ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Επισκόπηση Μηχανισμών Ενθυλάκωσης Κλειδιού

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Σιδηρόπουλου Ευθύμιου

Επιβλέπων : Κωνσταντίνου Ελισάβετ, Επίκουρη Καθηγήτρια

Μέλη εξεταστικής επιτροπής: Βλάχου Ακριβή, Αναπληρωτής Καθηγητής
Κρητικός Κυριάκος, Αναπληρωτής Καθηγητής

Σάμος, Φεβρουάριος 2021

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια, κα. Κωνσταντίνου Ελισάβετ για τις πολύτιμες συμβουλές και παρατηρήσεις, καθώς και για την βοήθεια της σε όλη την διάρκεια της παρούσας διπλωματικής εργασίας.

Επιπλέον, ευχαριστώ την οικογένειά μου για όλη την στήριξη τους σε όλη την πορεία του μεταπτυχιακού προγράμματος.

Σιδηρόπουλου Ευθύμιου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1 Εισαγωγή 9

1.1 Εισαγωγή στην Κρυπτογραφία 9

1.2 Συνεισφορά Μεταπτυχιακής Διατριβής 10

1.3 Δομή Διπλωματικής Εργασίας 10

2 Θεωρητικό Υπόβαθρο 11

2.1 Μαθηματικό Υπόβαθρο 11

2.1.1 Διαιρετότητα 11

2.1.2 Πρώτοι αριθμοί 12

2.1.3 Πρόβλημα Παραγοντοποίησης 12

2.1.4 Αριθμητική Modulo 12

2.1.5 Πρόβλημα διακριτού λογαρίθμου 15

2.2 Ασύμμετρη Κρυπτογραφία 15

2.2.1 Κρυπτοσυστήματα Δημοσίου Κλειδιού 16

2.2.2 Ασφάλεια κρυπτοσυστημάτων δημοσίου κλειδιού 18

2.2.3 Παραδείγματα κρυπτοσυστημάτων δημοσίου κλειδιού 19

2.2.3.1 Κρυπτοσύστημα RSA 19

2.2.3.2 Κρυπτοσύστημα ElGamal 21

2.2.3.3 Ανταλλαγή κλειδιού Diffie-Hellman 23

2.3 Θεωρία Ελλειπτικών καμπυλών 24

2.3.1 Γενικά Στοιχεία Ελλειπτικών Καμπυλών 24

2.3.2 Κρυπτογραφία ελλειπτικών καμπυλών 27

2.3.3 Ανταλλαγή κλειδιού Diffie-Hellman με ελλειπτικές καμπύλες 29

2.3.4 Κρυπτοσύστημα ElGamal με ελλειπτικές καμπύλες 30

3 Υβριδική Κρυπτογραφία 31

3.1 Μηχανισμοί Ενθυλάκωσης Κλειδιού 32

3.1.1 Επιθέσεις στους μηχανισμούς ενθυλάκωσης κλειδιού 33

3.2 Μηχανισμοί ενθυλάκωσης δεδομένων 35

3.2.1 Επιθέσεις στους μηχανισμούς ενθυλάκωσης δεδομένων 35

3.3 Μηχανισμοί KEM-DEM 38

3.3.1 Το μοντέλο Tag-KEM 39

4 Ανάλυση Μηχανισμών Ενθυλάκωσης Κλειδιού 41

4.1 Κρυπτογραφικά Εργαλεία Μηχανισμών Ενθυλάκωσης Κλειδιού 41

4.1.1 Παραδοχές ασφαλείας *44*
4.2 RSA-KEM 45
4.2.1 Ασφάλεια RSA-KEM *50*
4.3 ECIES-KEM 53
4.3.1 Ασφάλεια ECIES-KEM *64*
4.4 PSEC-KEM 66
4.4.1 Ασφάλεια PSEC-KEM *73*
4.5 ACE-KEM 78
4.5.1 Ασφάλεια ACE-KEM *83*
4.6 Σύγκριση μηχανισμών ενθυλάκωσης κλειδιού 86
5 Σύνοψη και Συμπεράσματα 90
Βιβλιογραφία 94

Λίστα Σχημάτων

Εικόνα 2.1: Δύο βασικές απεικονίσεις ελλειπτικών καμπυλών, α) Το κυβικό $\boldsymbol{y2 = x3 - x}$ και β) το κυβικό $\boldsymbol{y2 = x3 + x}$ [26].....25
Εικόνα 2.2: Πρόσθεση σημείων σε ελλειπτική καμπύλη [26]. 26
Εικόνα 3.1: Λειτουργία ενός KEM.....33
Εικόνα 3.2: Λειτουργία ενός DEM.....35
Εικόνα 3.3: Το κλειδί κρυπτογράφησης που χρησιμοποιείται στο σχήμα, κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη (KEM). Έπειτα, το αρχείο κρυπτογραφείται συμμετρικά με το κλειδί που δημιουργήθηκε στην προηγούμενη διαδικασία.....39
Εικόνα 3.4: Όταν ο παραλήπτης λάβει το κρυπτογραφημένο αρχείο μέσω του σχήματος KEM-DEM, χρησιμοποιεί το ιδιωτικό του κλειδί για την ανάκτηση του συμμετρικού κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση του αρχείου. Αφού λάβει το κλειδί είναι σε θέση να αποκρυπτογραφήσει το αρχείο που του απεστάλη.....39
Εικόνα 4.1: Λειτουργία Ενθυλάκωσης Κλειδιού στον μηχανισμό RSA-KEM σύμφωνα με το πρότυπο ISO []. 47
Εικόνα 4.2: Λειτουργία Απενθυλάκωσης Κλειδιού στον μηχανισμό RSA-KEM σύμφωνα με το πρότυπο ISO []. 47
Εικόνα 4.3: Λειτουργία Ενθυλάκωσης Κλειδιού στον μηχανισμό RSA-KEM σύμφωνα με το πρότυπο IETF[] 48
Εικόνα 4.4: Λειτουργία Απενθυλάκωσης Κλειδιού στον μηχανισμό RSA-KEM σύμφωνα με το πρότυπο IETF [].....49
Εικόνα 4.5: Διαδικασία κρυπτογράφησης με το κρυπτοσύστημα ECIES.....54
Εικόνα 4.6: Διαδικασία αποκρυπτογράφησης με το κρυπτοσύστημα ECIES.....56
Εικόνα 4.7: Διαδικασία κρυπτογράφησης με το κρυπτοσύστημα PSEC-3.....58
Εικόνα 4.8: Διαδικασία αποκρυπτογράφησης με το κρυπτοσύστημα PSEC-3.....59
Εικόνα 4.9: Ενθυλάκωση κλειδιού στον μηχανισμό ECIES-KEM σύμφωνα με το πρότυπο ISO. 61
Εικόνα 4.10: Απενθυλάκωση με το ECIES-KEM.....62

Λίστα Πινάκων

Πίνακας 4.1: Αριθμός λειτουργιών ομάδας των σχημάτων ECIES-KEM, PSEC-KEM και ACE-KEM. 88

Απόδοση Αγγλικών όρων στα Ελληνικά

Αδιακρισία	Indistinguishability
Ανθεκτικότητα Δεύτερης Προ-εικόνας	Second Preimage Resistance
Ανθεκτικότητα Προ-εικόνας	Preimage Resistance
Ανθεκτικότητα Σύγκρουσης	Collision Resistance
Αρχή Πιστοποίησης	Certificate Authority
Αρχικό κείμενο	Plaintext
Επίθεση Επιλεγμένου Αρχικού Κειμένου	Chosen Plaintext Attack
Επίθεση Επιλεγμένου Κρυπτοκειμένου	Chosen Ciphertext Attack
Επίθεση Προσαρμόσιμου Επιλεγμένου Κρυπτοκειμένου	Adaptive Chosen Ciphertext Attack
Επιλεγμένο Αρχικό Κείμενο	Chosen Plaintext
Ιδιότητα Ορθότητας	Correctness Property
Ιδιότητα Ορθότητας	Soundness Property
Κρυπτογραφική Συνάρτηση Κατακερματισμού	Cryptographic Hash Function
Κρυπτοκείμενο	Ciphertext
Μηχανισμός Ενθυλάκωσης Δεδομένων	Data Encapsulation Mechanism
Μηχανισμός Ενθυλάκωσης Κλειδιού	Key Encapsulation Mechanism
Διεκδικητής	Challenger
Συνάρτηση Δημιουργίας Κλειδιού	Key Derivation Function
Συνάρτηση Κατακερματισμού	Hash
Τάξη	Order
Ταυτοτικό στοιχείο	Identity Element
Υποδομή Δημοσίου Κλειδιού	Public Key Infrastructure
Χώρος Αρχικού Κειμένου	Plaintext Space
Χώρος Κλειδιού Αποκρυπτογράφησης	Decryption Key Space
Χώρος Κλειδιού Κρυπτογράφησης	Encrpytion Key Space
Χώρος Κρυπτοκειμένου	Ciphertext Space
Ωτακουστής	Eavesdropper

Ακρωνύμια

Key Encapsulation Mechanism	KEM
Data Encapsulation Mechanism	DEM
Public Key Infrastructure	PKI
Chosen Ciphertext Attack	CCA
Indistinguishability	IND
Elliptic Curve Cryptography	ECC
Πρόβλημα Διακριτού Λογαρίθμου σε ελλειπτικές καμπύλες	ECDLP
Key Derivation Function	KDF
Decisional Diffie Hellman	DDH
gap-Computational Diffie Hellman	gap-CDH
Elliptic Curve Integrated Encryption Scheme	ECIES
Discrete Logarithm Augmented Encryption Scheme	DLAES
Diffie-Hellman Integrated Encryption Scheme	DHIES
Provably Secure Elliptic Curve	PSEC

Περίληψη

Οι πληροφορίες που ανταλλάσσονται στο διαδίκτυο θεωρούνται ότι δεν είναι ασφαλής και επομένως, η εξασφάλιση των δεδομένων αποτελεί ένα από τα σημαντικότερα ζητήματα στον χώρο της ασφάλειας. Η ασφάλεια των δεδομένων στηρίζεται σε μεγάλο βαθμό σε κρυπτογραφικά σχήματα, τα οποία θεωρούνται αδιάσπαστα χωρίς την κατοχή των ιδιωτικών κλειδιών. Τα είδη κρυπτογραφίας που κυριαρχούν στις επικοινωνίες δεδομένων είναι η συμμετρική και η ασύμμετρη κρυπτογράφηση. Από την μία ,οι συμμετρικοί αλγόριθμοι προσφέρουν υψηλό επίπεδο ασφάλειας με γρήγορη επεξεργασία δεδομένων, ωστόσο η βασική αδυναμία τους έγκειται στο γεγονός μεταφοράς του μυστικού κλειδιού. Από την άλλη, η ασύμμετρη κρυπτογραφία προσπαθεί να επιλύσει το πρόβλημα μεταφοράς του μυστικού κλειδιού, ωστόσο απαιτούν υψηλούς υπολογιστικούς πόρους και δεν προσφέρουν γρήγορη επεξεργασία δεδομένων.

Τα προβλήματα που προκύπτουν από τα δύο παραπάνω σχήματα κρυπτογράφησης μπορούν να προσπεραστούν με την χρήση ενός σχήματος υβριδικής κρυπτογραφίας, δηλαδή τον συνδυασμό της μεταφοράς κλειδιού από ένα ασύμμετρο σχήμα και της απόδοσης των συμμετρικών σχημάτων. Ένα υβριδικό σχήμα αποτελείται από δύο υπο-κρυπτοσυστήματα: τον μηχανισμό ενθυλάκωσης κλειδιού και τον μηχανισμό ενθυλάκωσης δεδομένων, που αφορούν το ασύμμετρο και το συμμετρικό σχήμα, αντίστοιχα.

Παρόλες τις προτάσεις για την υλοποίηση και δημιουργία μηχανισμών ενθυλάκωσης κλειδιού, δεν υπάρχει επαρκή ανάλυση στην βιβλιογραφία όσον αφορά την επεξήγηση και σύγκριση των σχημάτων αυτών. Στην εργασία αυτή μελετώνται οι τέσσερις δημοφιλέστεροι αλγόριθμοι μηχανισμών ενθυλάκωσης κλειδιού, οι RSA-KEM, ECIES-KEM, PSEC-KEM και ACE-KEM, οι οποίοι είναι και προτυποποιημένοι. Για την πλήρη κατανόηση των σχημάτων αυτών, αναλύονται τα σχήματα δημοσίου κλειδιού στα οποία οι αλγόριθμοι αυτοί βασίζονται, καθώς και συζητούνται οι έννοιες ασφάλειας τους. Τέλος, παρουσιάζεται η σύγκριση μεταξύ τους όσον αφορά την απόδοση και αποτελεσματικότητά τους.

Λέξεις Κλειδιά: *Μηχανισμοί Ενθυλάκωσης Κλειδιού, Υβριδική Κρυπτογραφία, Ανταλλαγή Κλειδιού, IND-CCA Ασφάλεια*

Abstract

Exchanged information on the internet is considered to be unsafe and as a result, data security is one of the most important issues in the broader research area of cryptography and security. Data security heavily relies on cryptographic schemes, which are considered unbreakable without the possession of private keys. There are two encryption schemes in communications: symmetric and asymmetric encryption. On the one hand, symmetric algorithms offer a high security level with fast data processing. However, their main weakness lies in secret key transmission. A symmetric cryptography, on the other hand, tries to solve the problem of secret key transmission, but it requires high computational resources and does not offer fast data processing.

The problems arising from the two encryption schemes can be overcome by using a hybrid cryptography scheme. That is, the combination of an asymmetric scheme for key transfer and a symmetric key for fast data processing. A hybrid scheme consists of two sub-cryptosystems: the key encapsulation mechanism and the data encapsulation mechanism, which relate to the assymetric and symmetric scheme, respectively.

Despite the proposals and implementations of key encapsulation mechanisms in the bibliography, there is insufficient analysis regarding the explanation and comparison of these schemes. This work studies the four most popular key encapsulation mechanisms, namely, RSA-KEM, ECIES-KEM, PSEC-KEM and ACE-KEM, which are also standardized as ISO standard. To provide a full understanding of these schemes we discuss the public key algorithms on which these algorithms rely. Moreover, we discuss the properties and the security of these algorithms. Finally, we compare the key encapsulation mechanisms in terms of performance and effectiveness.

Keywords: *Key Encapsulation Mechanisms, Hybrid Cryptography, IND-CCA Security, Key Exchange*

1 *Εισαγωγή*

1.1 Εισαγωγή στην Κρυπτογραφία

Παρόλη την ραγδαία εξέλιξη στην γρήγορη μεταφορά και επεξεργασία πληροφοριών μέσω του διαδικτύου, ένα μεγάλο μέρος της πληροφορίας αποκαλύπτεται, παραποιείται, αλλοιώνεται ή και αποποιείται. Επομένως, η ασφάλεια γίνεται όλο ένα και μεγαλύτερο ζήτημα [1], με τους χρήστες να αποζητούν μέτρα εξασφάλισης της ιδιωτικότητας τους. Οι βασικές απαιτήσεις ασφαλείας μεταξύ άλλων, περιλαμβάνουν την αυθεντικοποίηση, εμπιστευτικότητα, ακεραιότητα και μη αποποίηση [2]. Η παροχή των συγκεκριμένων απαιτήσεων γίνεται κυρίως μέσω της χρήσης κρυπτογραφικών σχημάτων. Η κρυπτογραφία, τυπικά, αποτελεί την διαδικασία απόκρυψης ενός μηνύματος έτσι ώστε το περιεχόμενο του να μην είναι εύκολα προσπελάσιμο, ενώ η αποκρυπτογράφηση αποτελεί την αντίστροφη διαδικασία. Οι διαδικασίες αυτές στηρίζονται σε διάφορους αλγορίθμους, οι οποίοι, συνήθως, περιλαμβάνουν ένα μυστικό κλειδί, το οποίο καθορίζει την μετατροπή του αρχικού μηνύματος σε ένα κρυπτογραφημένο.

Υπάρχουν κυρίως δύο τεχνικές κρυπτογράφησης, αυτές που βασίζονται σε συμμετρικά συστήματα και αυτές που βασίζονται σε ασύμμετρα, γνωστά ως κρυπτοσυστήματα δημοσίου κλειδιού. Στην συμμετρική κρυπτογραφία χρησιμοποιείται το ίδιο κλειδί για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης μιας πληροφορίας. Το μυστικό κλειδί αυτό, χρησιμοποιείται με τέτοιο τρόπο ώστε να αλλάξει την πληροφορία με έναν συγκεκριμένο τρόπο. Επομένως, στα συστήματα αυτά απαραίτητη προϋπόθεση αποτελεί η γνώση του μυστικού κλειδιού από τον αποστολέα και τον παραλήπτη. Οι αλγόριθμοι που βασίζονται σε συμμετρική κρυπτογραφία έχουν αποδειχτεί ότι είναι αποτελεσματικοί, ασφαλής, εκτελούνται γρήγορα και απαιτούν λίγους υπολογιστικούς πόρους. Όμως, σε γενικότερο επίπεδο, η βασική τους αδυναμία έγκειται στο πρόβλημα της ασφαλούς μεταφοράς του μυστικού κλειδιού. Το πρόβλημα αυτό μπορεί να επιλυθεί με την χρήση ασύμμετρης κρυπτογραφίας όπου χρησιμοποιείται ένα ζεύγος κλειδιών, το δημόσιο και το ιδιωτικό. Το δημόσιο κλειδί είναι διαθέσιμο προς όλους τους χρήστες ενός συστήματος, ενώ το ιδιωτικό παραμένει μυστικό από τον ιδιοκτήτη. Οποιοδήποτε μήνυμα κρυπτογραφείται μέσω του δημοσίου κλειδιού, μπορεί να αποκρυπτογραφηθεί μόνο από τον κάτοχο του ιδιωτικού κλειδιού [3]. Το βασικότερο πρόβλημα που προκύπτει με την χρήση κρυπτογραφίας δημοσίου κλειδιού είναι ότι τα κρυπτοσυστήματα αυτά απαιτούν πολλούς υπολογιστικούς πόρους και δεν εκτελούνται με τόση μεγάλη ταχύτητα όσο οι συμμετρικοί αλγόριθμοι. Επομένως, τα ασύμμετρα συστήματα δεν μπορούν να διαχειριστούν μηνύματα μεγάλου μήκους.

Η λύση στις αδυναμίες των δύο παραπάνω μεθόδων αποτελεί η χρήση ενός σχήματος υβριδικής κρυπτογραφίας. Στην μέθοδο αυτή, το πρωτόκολλο ασφάλειας χρησιμοποιεί ένα κρυπτοσύστημα δημοσίου κλειδιού με σκοπό την ανταλλαγή ενός μυστικού κλειδιού και έπειτα το μυστικό κλειδί που δημιουργήθηκε, χρησιμοποιείται σε συμμετρικούς αλγορίθμους για την διασφάλιση της

εμπιστευτικότητας των δεδομένων. Συνήθως, η συμφωνία του μυστικού κλειδιού (ή κλειδιού συνόδου) συμβαίνει σε αρχική φάση σε δημοφιλή πρωτόκολλα ασφαλούς επικοινωνίας, όπως στα TLS, το IPSec και το SSH. Έτσι, στην υβριδική κρυπτογραφία, χρησιμοποιούνται δύο μηχανισμοί για την μεταφορά κλειδιού και κρυπτογράφηση των μηνυμάτων, ο μηχανισμός ενθυλάκωσης κλειδιού (KEM) και ο μηχανισμός ενθυλάκωσης δεδομένων (DEM), τα οποία προτάθηκαν από τον Shoup ως πρότυπα ISO ως μοντέλα υβριδικής κρυπτογράφησης δημοσίου κλειδιού [4]. Στην ουσία, το KEM είναι ένα τύπος ασύμμετρης κρυπτογραφίας, ο οποίος χρησιμοποιείται για την ασφαλή μεταφορά ενός κλειδιού, το οποίο μετέπειτα χρησιμοποιείται στο DEM, δηλαδή έναν συμμετρικό αλγόριθμο, ως κλειδί κρυπτογράφησης.

1.2 Συνεισφορά Μεταπτυχιακής Διατριβής

Στην εργασία αυτή, εστιάζουμε στον τρόπο λειτουργίας των δημοφιλέστερων υβριδικών σχημάτων που βασίζονται στο μοντέλο KEM-DEM, δίνοντας έμφαση στην περίπτωση δημιουργίας μυστικού κλειδιού χρησιμοποιώντας μηχανισμούς KEM. Είναι σημαντικό να αναφερθεί πως παρόλη την προτυποποίηση, δεν υπάρχουν πολλές βιβλιογραφικές αναφορές σχετικά με την υλοποίηση, εφαρμογή και ασφάλεια των μεθόδων που χρησιμοποιούν μοντέλα KEM για την εξασφάλιση μιας επικοινωνίας. Στην εργασία αυτή πραγματοποιείται ανάλυση των τρόπων εγκαθίδρυσης του μυστικού κλειδιού βάση των κρυπτοσυστημάτων στα οποία βασίζεται η λειτουργία τους και αξιολογείται ξεχωριστά η ασφάλεια κάθε μοντέλου.

Οι μηχανισμοί ενθυλάκωσης κλειδιού στηρίζονται σε κλασσικές μεθόδους ασύμμετρης κρυπτογραφίας. Έτσι, μελετήθηκε το θεωρητικό υπόβαθρο που αφορά τον τρόπο λειτουργίας των σχημάτων αυτών, καθώς και ορίζεται η έννοια ασφάλειας τους. Επιπλέον, είναι γνωστό πως τα κρυπτογραφικά σχήματα αυτά μπορούν να οριστούν πάνω από μια ελλειπτική καμπύλη. Επομένως, είναι απαραίτητη η παροχή θεωρητικού υπόβαθρου για τον τρόπο λειτουργίας των ελλειπτικών καμπυλών.

Τέλος, παρουσιάζεται συγκριτική μελέτη του επιπέδου ασφαλείας κάθε μοντέλου KEM του οποίου αναλύθηκε ο τρόπος λειτουργίας του, ώστε να διαπιστωθεί εάν κάποια από τις διαθέσιμες μεθόδους υπερισχύει έναντι άλλων, τουλάχιστον όσον αφορά θέματα ασφαλείας.

1.3 Δομή Διπλωματικής Εργασίας

Η διπλωματική εργασία οργανώνεται ως εξής:

Στο κεφάλαιο 2 παρουσιάζεται το θεωρητικό υπόβαθρο σχετικά με τις μαθηματικές ιδιότητες που είναι απαραίτητες για την κατανόηση της ασύμμετρης κρυπτογραφίας και την κρυπτογραφίας πάνω από ελλειπτικές καμπύλες.

Στο κεφάλαιο 3 περιγράφονται τα βασικά χαρακτηριστικά της υβριδικής κρυπτογραφίας, δηλαδή του συνδυασμού ασύμμετρης και συμμετρικής κρυπτογραφίας.

Στο κεφάλαιο 4 αναλύονται οι μηχανισμοί ενθυλάκωσης κλειδιού, καθώς και συζητείται η έννοια ασφάλειας κάθε ενός σχήματος.

Το κεφάλαιο 5 αποτελεί μια σύνοψη των κύριων στοιχείων των μηχανισμών ενθυλάκωσης κλειδιού και συζητούνται τα συμπεράσματα της εργασίας.

2 *Θεωρητικό Υπόβαθρο*

2.1 Μαθηματικό Υπόβαθρο

Στο κεφάλαιο αυτό παρουσιάζονται θεμελιώδες έννοιες μαθηματικού υπόβαθρου για την κατανόηση της λειτουργίας των δημοφιλέστερων κρυπτοσυστημάτων και ως αποτέλεσμα των εφαρμογών των μηχανισμών ενθυλάκωσης κλειδιού. Τα βασικά στοιχεία των αλγορίθμων κρυπτογραφίας επικεντρώνονται στην θεωρία αριθμών, δηλαδή τις ιδιότητες των φυσικών αριθμών. Στην συνέχεια, παρουσιάζονται τα μαθηματικά προβλήματα που στηρίζουν την λειτουργία τους, οι αλγόριθμοι συμφωνίας κρυπτογραφικών κλειδιών. Τα προβλήματα που αναφέρονται είναι το πρόβλημα της παραγοντοποίησης και το πρόβλημα του διακριτού λογαρίθμου, τα οποία θεωρούνται υπολογιστικά ανέφικτο να επιλυθούν. Είναι σημαντικό να σημειωθεί ότι η αναφορά στο μαθηματικό υπόβαθρο δεν είναι λεπτομερείς, αλλά απομονώθηκαν μόνο τα σημαντικότερα στοιχεία. Για την παροχή των παρακάτω στοιχείων, δόθηκε ιδιαίτερη έμφαση σε πληροφορίες που συλλέχθηκαν από τα [1], [2].

2.1.1 Διαιρετότητα

Πριν τον ορισμό της διαιρετότητας είναι σημαντικό να αναφερθεί πως το σύνολο των ακεραίων αριθμών $\{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ συμβολίζεται με $\mathbb{Z}$.

Ορισμός 2.1.1.1 Ένας ακέραιος αριθμός $a \neq 0$ διαιρεί έναν ακέραιο b αν υπάρχει ακέραιος m τέτοιος ώστε $b = ma$. Η διαιρετότητα του a με τον b (ο a διαιρεί τον b) συμβολίζεται ως $a|b$.

Σύμφωνα με τον παραπάνω ορισμό, ο ακέραιος αριθμός b αποτελεί ακέραιο πολλαπλάσιο του a. Για την διαιρετότητα των ακεραίων ισχύουν οι εξής ιδιότητες:

1. $1|a$ για κάθε a.
2. $a|b \Rightarrow |a| \leq |\mathrm{b}|$. Εφόσον $a|b$ τότε ισχύει ότι $\mathrm{b} = ma$. Γνωρίζοντας ότι $b \neq 0$, τότε και $m \neq 0$, οπότε και $q \geq 1$. Άρα, $|b| = |m|\,|a| \Rightarrow |\mathrm{b}| \geq |a|$.
3. Για κάθε $b \neq 0$, ισχύει ότι $b|b$ και $b|0$. Η συγκεκριμένη ιδιότητα ισχύει διότι κάθε ακέραιος b αποτελεί ακέραιο πολλαπλάσιο του εαυτού του. Με άλλα λόγια, $b = 1b$.
4. Αν $a > 0, b > 0, a|b, b|a$, ισχύει ότι $a = \pm b$. Λόγω της ιδιότητας 2, συμπεραίνεται πως $|a| \leq |b|$ και $|b| \geq |a|$. Άρα $|a| = |b|$, οπότε $a = \pm b$.
5. Αν $a, b \neq 0, a|b, b|c$, ισχύει ότι $a|c$. Παρατηρώντας ότι
$$\begin{cases} \alpha\nu\ a|b \Leftrightarrow \mathrm{b} = \mathrm{ma} \\ \alpha\nu\ b|c \Leftrightarrow \mathrm{c} = \mathrm{kb} \end{cases} \Rightarrow\ \mathrm{c} = (\mathrm{km})a \Rightarrow\ \mathrm{a}|c.$$
6. Για κάθε a, b, c με $a \neq 0$, αν $a|b$ και $a|c$, τότε $a|(xb + yc)$ για κάθε $x, y \epsilon \mathbb{Z}$. Η συγκεκριμένη ιδιότητα γενικεύεται για οποιοδήποτε πεπερασμένο πλήθος ακεραίων

αριθμών. Ειδικότερα αν d, $a_1, a_2, \dots, a_n \in \mathbb{Z}$ και $d|a_i$, $i = 1,2, \dots, n$ τότε $d|(t_1a_1 + t_2a_2 + \dots + t_na_n)$.

Ορισμός 2.1.1.2 *Αλγόριθμος του Ευκλείδη:* Αν $a, b \in \mathbb{Z}$ και $b \neq 0$, τότε υπάρχουν μοναδικοί ακέραιοι q, r ώστε $a = qb + r$. Το στοιχείο q ονομάζεται πηλίκο και το στοιχείο r το υπόλοιπο της $a|b$.

2.1.2 Πρώτοι αριθμοί

Ορισμός 2.1.2.1 *Πρώτος αριθμός* ονομάζεται ένας ακέραιος p, με $p > 1$, ο οποίος μπορεί να διαιρεθεί χωρίς να αφήνει υπόλοιπο μόνο με τον εαυτό του και το 1, συμπεριλαμβανομένων και των αρνητικών αυτών αριθμών. Οποιοσδήποτε θετικός ακέραιος αριθμός $n > 1$, που δεν είναι πρώτος, ονομάζεται σύνθετος.

Ορισμός 2.1.2.2 *Θεμελιώδες Θεώρημα Αριθμητικής*: Κάθε θετικός ακέραιος $n > 1$ μπορεί να αναλυθεί σε γινόμενο πρώτων παραγόντων, $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, όπου $p_1 < p_2 < p_3$ είναι πρώτοι αριθμοί και $e_i, r, 1 \leq i \leq r$ θετικοί ακέραιοι.

Ορισμός 2.1.2.3 Μέγιστος κοινός διαιρέτης $MK\Delta(a, b)$ δύο ακεραίων (a, b) ορίζεται ως ο μεγαλύτερος από τους κοινούς διαιρέτες των a και b.

Ορισμός 2.1.2.4 Πρώτοι μεταξύ τους (ή σχετικά πρώτοι) ονομάζονται δύο ακέραιοι a και b, αν $MK\Delta(a, b) = 1$.

2.1.3 Πρόβλημα Παραγοντοποίησης

Το πρόβλημα της παραγοντοποίησης ορίζεται ως εξής: Δεδομένου ενός θετικού ακεραίου n, είναι δύσκολη η ανάλυσή του σε γινόμενο πρώτων παραγόντων. Με άλλα λόγια, σκοπός είναι να βρεθούν οι πρώτοι αριθμοί $p_i, 1 \leq i \leq r$, ώστε $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, όπου e_i, r θετικοί ακέραιοι. Μέχρι και σήμερα δεν έχει ανακαλυφθεί αποδοτική μέθοδος που να μπορεί να επιλύσει το πρόβλημα παραγοντοποίησης σε εύλογο χρονικό διάστημα για μεγάλους αριθμούς n. Στο πρόβλημα αυτό βασίζονται δημοφιλής αλγόριθμοι δημοσίου κλειδιού, όπως ο RSA που θα συζητηθεί παρακάτω.

2.1.4 Αριθμητική Modulo

Ορισμός 2.1.4.1 Μια τιμή r ορίζεται ως το υπόλοιπο της διαίρεσης ενός ακεραίου a από τον n, $r = a \bmod n$.

Ορισμός 2.1.4.2 Ένας ακέραιος αριθμός $a' \in \mathbb{Z}$ είναι πολλαπλασιαστικός αντίστροφος του ακεραίου αριθμού a $modulo$ n, με $n > 0$, αν $a * a' \equiv 1 \bmod n$.

Ορισμός 2.1.4.3 Το σύνολο $\mathbb{Z}_n^*$ είναι το υποσύνολο του $\mathbb{Z}_n$ (το σύνολο των ακεραίων που είναι μικρότεροι από n), στο οποίο περιέχονται οι ακέραιοι που είναι σχετικά πρώτοι με τον n. Άρα, το σύνολο $\mathbb{Z}_p^*$ περιέχει τους ακέραιους αριθμούς από είναι μικρότερο από έναν πρώτο αριθμό p, $\mathbb{Z}_p^* = \{1,2, \dots, p-1\}$.

Ορισμός 2.1.4.4 *Θεώρημα Euler*: Ως συνάρτηση Euler $\varphi(n)$, ορίζεται το σύνολο των θετικών ακεραίων μικρότερων από το n, οι οποίοι δεν έχουν κοινούς διαιρέτες με αυτόν (είναι σχετικά πρώτοι με αυτόν). Για την συνάρτηση Euler, ισχύουν οι εξής ιδιότητες:

1. Αν p είναι πρώτος αριθμός τότε $\varphi(p) = p - 1$.

2. Αν p είναι πρώτος αριθμός και a είναι θετικός ακέραιος, τότε $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a(1-\frac{1}{p})$.
3. Αν n, m είναι θετικοί ακέραιοι με $MK\Delta(n,m) = 1$, τότε $\varphi(n*m) = \varphi(n)*\varphi(m)$.
4. Αν $n = p*q$, όπου p, qπρώτοι, τότε $\varphi(p*q) = (p-1)(q-1)$.

5. Αν $n = p_1^{a_1}p_2^{a_2}\dots p_t^{a_t}$, τότε $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots(1-\frac{1}{p_t})$

Το θεώρημα Euler δηλώνει ότι για κάθε a και n που είναι πρώτοι μεταξύ τους ισχύει:

$$a^{\varphi(n)} \equiv 1(modn).$$

Ορισμός 2.1.4.5 *Θεώρημα Fermat*: Για κάθε $a \in \mathbb{Z}$ και κάθε πρώτο αριθμό p ισχύει ότι $a^p \equiv a(modp)$.

Ορισμός 2.1.4.6 *Πολλαπλασιαστική τάξη* k ενός στοιχείου $a \in \mathbb{Z}_n^*$, $ord_n(a)$, ονομάζεται ο μικρότερος θετικός ακέραιος για τον οποίο ισχύει $a^k = 1(modn)$.

Ορισμός 2.1.4.7 *Πρωτεύουσα ρίζα* δεδομένου ενός θετικού ακεραίου n ονομάζεται ένας ακέραιος $g \in \mathbb{Z}_n^*\ modulo\ n$, αν $ord_n(g) = \varphi(N)$. Στην περίπτωση αυτή, οι δυνάμεις του $g, g^i modn$ για $1 \le i \le \varphi(N)$ δημιουργούν μια μετάθεση του $\mathbb{Z}_n^*$.

Ορισμός 2.1.4.8 *Ομάδα* $(G,\circ)$ ορίζεται ένα σύνολο στοιχείων G στο οποίο μπορεί να εφαρμοστεί μια πράξη $\circ: G\ x\ G \to G$, η οποία περιλαμβάνει την πράξη της πρόσθεσης (+) ή του πολλαπλασιασμού (*).

- Η πράξη που ορίζει η ομάδα είναι κλειστή, δηλαδή για κάθε $a, b \in G$, ισχύει ότι $a \circ b = c$, $c \in G$.
- Η ομάδα περιλαμβάνει ένα ταυτοτικό στοιχείο (identity element) $e \in G$, τέτοιο ώστε $a \circ e = e \circ a = a$, για κάθε $a \in G$.
- Η πράξη που ορίζει η ομάδα περιλαμβάνει την προσεταιριστική ιδιότητα, δηλαδή για κάθε $a, b, c \in G$, ισχύει ότι $a \circ (b \circ c) = (\text{a} \circ \text{b}) \circ \text{c}$.
- Για κάθε $a \in G$ υπάρχει ένα στοιχείο $b \in G$, που ονομάζεται αντίστροφο του a, τέτοιο ώστε $a \circ b = b \circ a = e$.
- Μια ομάδα ονομάζεται αβελιανή αν για όλα τα $a, b \in G$, ισχύει ότι $a \circ b = b \circ \text{a}$. Σημειώνεται ότι σε μια αβελιανή ομάδα ισχύουν και οι παραπάνω ιδιότητες της ομάδας.
- Μια ομάδα g λέγεται κυκλική, $\langle g \rangle$, αν υπάρχει ένα στοιχείο (γεννήτορας) $g \in G$, τέτοιο ώστε όλα τα στοιχεία της ομάδας μπορούν να βρεθούν αν εφαρμοστεί επαναληπτικά η αριθμητική πράξη που ορίζει την ομάδα. Σημειώνεται ότι κάθε κυκλική ομάδα είναι αβελιανή.

Σημειώνεται ότι αν στην ομάδα περιλαμβάνεται η πράξη της πρόσθεσης, η ομάδα ονομάζεται προσθετική. Σε αυτή το ταυτοτικό στοιχείο είναι 0, ενώ το αντίστροφο του a συμβολίζεται με $-\alpha$. Αντίστοιχα, αν περιλαμβάνεται η πράξη του πολλαπλασιασμού, η ομάδα ονομάζεται πολλαπλασιαστική, το ταυτοτικό στοιχείο είναι το 1, ενώ το αντίστροφο του a συμβολίζεται με a^{-1}. Η ομάδα ονομάζεται *πεπερασμένη* αν το G είναι ένα πεπερασμένο σύνολο, όπου ο αριθμός των στοιχείων που περιλαμβάνει το G ονομάζεται τάξη (order) του G.

Ορισμός 2.1.4.9 Υποομάδα της G ονομάζεται ένα υποσύνολο H αν στο H εφαρμόζεται η ιδιότητα της κλειστότητας ως προς την πράξη που ορίζει η ομάδα G, το ταυτοτικό στοιχείο της G ανήκει στο H και για κάθε $h \in H$, ισχύει ότι $h^{-1} \in H$.

Ορισμός 2.1.4.10 *Δακτύλιος* ονομάζεται μια αλγεβρική δομή R στην οποία ισχύουν οι πράξεις της πρόσθεσης και του πολλαπλασιασμού, $(R, +, *)$ που αποτελείται από το σύνολο R, στην οποία ισχύουν τα εξής:

1. $+: RxR \to R, (x, y) \to x + y.$
2. $*: RxR \to R, (x, y) \to x * y.$
   i. Ισχύει η προσεταιριστική ιδιότητα ως προς τον πολλαπλασιασμό, δηλαδή για όλα τα $a, b, c \in A$ $(a * b * c) = a * (b * c)$.
   ii. Το A είναι αβελιανό ως προς την πρόσθεση, δηλαδή για όλα τα $a, b \in A$, ισχύει ότι $a + b = b + a$.

Ορισμός 2.1.4.11 Σώμα ονομάζεται ένα σύνολο στοιχείων F με τις εξής ιδιότητες:

1. Όλα τα στοιχεία του F δημιουργούν μια προσθετική ομάδα με την πράξη $+$, $(F, +)$, με ταυτοτικό στοιχείο τον αριθμό 0.
2. Όλα τα στοιχεία του F εκτός από το 0 σχηματίζουν μια πολλαπλασιαστική ομάδα $*$, $(F\backslash\{0\}, *)$, με ταυτοτικό στοιχείο τον ακέραιο 1.
3. Τα σώματα διακρίνονται σε πεπερασμένα και άπειρα. Η διαφορά τους είναι το πλήθος των στοιχείων που περιλαμβάνουν. Για τους σκοπούς ανάλυσης των κρυπτογραφικών σχημάτων αρκεί η έννοια ενός πεπερασμένου σώματος.
   - Ένα πεπερασμένο σώμα είναι ένα σώμα το οποίο περιλαμβάνει πεπερασμένο αριθμό στοιχείων. Ένα παράδειγμα πεπερασμένου σώματος είναι το σύνολο των αριθμών $modulo\ p$, όπου p είναι πρώτος αριθμός.
   - Το πλήθος των στοιχείων ενός πεπερασμένου σώματος ονομάζεται τάξη. Η τάξη ενός στοιχείου $a \in \frac{Z_p[x]}{f(x)}$ είναι ένα ακέραιος e τέτοιος ώστε $a^e = 1 mod f(x)$.
   - Αν F_q είναι πεπερασμένο σώμα τάξης $q = p^m$, με p πρώτο αριθμό, τότε το χαρακτηριστικό του F_q είναι το p.
4. Κάθε σώμα F περιλαμβάνει δύο λειτουργίες, αυτή την πρόσθεσης και του πολλαπλασιασμού. Η αφαίρεση στοιχείων ορίζεται σε όρους πρόσθεσης. Δηλαδή, για $a, b \in F, a - b = a + (-b)$, όπου $-b$ είναι ένα μοναδικό στοιχείο στο F τέτοιο ώστε $b + (-b) = 0$. Παρόμοια, η πράξη της διαίρεσης ορίζεται σε όρους πολλαπλασιασμού. Δηλαδή, για $a, b \in F, \frac{a}{b} = a * b^{-1}$, με $b \neq 0$, όπου b^{-1} είναι ένα μοναδικό στοιχείο στο F τέτοιο ώστε $b * b^{-1} = 1$.

Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα πεπερασμένα σώματα τάξης p και τα σώματα Galois. Ως πεπερασμένο σώμα τάξης p, $GF(p)$, με p πρώτο αριθμό, ορίζεται η αλγεβρική δομή $(\mathbb{Z}_p, +_p, *_p)$, δηλαδή το σύνολο $\mathbb{Z}_p = \{0,1,2, \dots, p-1\}$ εφοδιασμένο με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού $modulo\ p$. Το σώμα Galois, $F_p m$, αποτελεί επέκταση του σώματος $\mathbb{Z}_p$ με βαθμό επέκτασης m. Ένα σώμα K ονομάζεται επέκταση ενός άλλου σώματος F αν το F είναι υποσύνολο

του K. Κάθε στοιχείο s του σώματος Galois αναπαρίσταται ως $s = \sum_{i=0}^{m-1} a_i x^i = a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}$, με $a_i \in F_p$.

2.1.5 Πρόβλημα διακριτού λογαρίθμου

Ένας λογάριθμος είναι η αντίστροφη διαδικασία από την πράξη της δύναμης. Έτσι, ο διακριτός λογάριθμος είναι η αντίστροφη διαδικασία από την πράξη της δύναμης σε έναν λογάριθμο. Οι παραπάνω ορισμοί (ομάδα, σώμα) είναι απαραίτητοι για την κατανόηση των προβλημάτων που βασίζονται στο πρόβλημα αυτό. Έτσι, δίνουμε ένα παράδειγμα για την καλύτερη κατανόηση αυτών.

Έστω ότι p είναι ένας πρώτος αριθμός και $F_p = \{0,1,2, \ldots, p-1\}$ συμβολίζει το σύνολο των ακεραίων $modulo\ p$. Τότε ο συμβολισμός $(F_p, +)$, όπου η πράξη της πρόσθεσης ορίζεται ως η πρόσθεση των ακεραίων $modulo\ p$, είναι μια πεπερασμένη προσθετική ομάδα τάξης p με ταυτοτικό στοιχείο τον αριθμό 0. Αντίστοιχα, ο συμβολισμός $(F_p^*, *)$, ο οποίος απεικονίζει όλα τα μη μηδενικά στοιχεία στο σύνολο F_p, όπου η πράξη του πολλαπλασιασμού ορίζεται ως ο πολλαπλασιασμός των ακεραίων $modulo\ p$, είναι μια πεπερασμένη πολλαπλασιαστική κυκλική ομάδα τάξης $p-1$ με ταυτοτικό στοιχείο τον ακέραιο αριθμό 1. Η τριπλέτα $(F_p, +, *)$ είναι ένα πεπερασμένο σώμα, το οποίο συνήθως συμβολίζεται με F_p.

Έστω ότι $(G, *)$ είναι μια πολλαπλασιαστική κυκλική ομάδα τάξης n, ένας γεννήτορας $g \in G$ και $h \in \langle g \rangle \subset G$. Σκοπός είναι να βρεθεί ένας αριθμός $k \in \mathbb{Z}$, ο οποίος ικανοποιεί την συνθήκη $k * g = h$. Η εύρεση του ακεραίου k αποτελεί το πρόβλημα του διακριτού λογαρίθμου. Επιπλέον, ο αριθμός αυτός ονομάζεται διακριτός λογάριθμος του h στην βάση g. Εναλλακτικά, η ταυτότητα του διακριτού λογαρίθμου μπορεί να γραφεί ως $g^k = h$.

2.2 Ασύμμετρη Κρυπτογραφία

Στο εισαγωγικό κεφάλαιο παρουσιάστηκε η βασική έννοια ενός σχήματος κρυπτογράφησης. Ειδικότερα, ως *σχήμα κρυπτογράφησης* ορίζεται μια πλειάδα (P, C, K_E, K_D, E, D) όπου P, K, K_E, K_D είναι αυθαίρετα σύνολα και E, D είναι ένα σύνολο συναρτήσεων, τέτοιες ώστε για κάθε D ορίζεται η συνάρτηση $E_k: P \to C$ όσον αφορά την E και για κάθε $k \in K_D$ ορίζεται η συνάρτηση $D_k: C \to D$ όσον αφορά την D. Η πλειάδα πρέπει να ικανοποιεί την συνθήκη ότι για κάθε $t \in K_E$ υπάρχει ένα μοναδικό $s \in K_D$, τέτοιο ώστε $D_s\big(E_t(p)\big) = p$ για κάθε $p \in P$ [5].

Τα σύνολα P, C, K_E, K_D στον παραπάνω ορισμό ονομάζονται χώρος αρχικού κειμένου (plaintext space), χώρος κρυπτοκειμένου (ciphertext space), χώρος κλειδιού κρυπτογράφησης (encryption key space) και χώρος κλειδιού αποκρυπτογράφησης (decryption key space), αντίστοιχα. Οι συναρτήσεις E, D είναι οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης.

Εξ' ορισμού, γίνεται εύκολα αντιληπτό ότι για την ασφαλή επικοινωνία μεταξύ δύο χρηστών δεν μπορούν να ληφθούν υπόψη όλα τα συστήματα κρυπτογράφησης. Αυτό συμβαίνει, διότι υπάρχουν σχήματα τα οποία δεν ικανοποιούν τις ανάγκες των δύο χρηστών. Για παράδειγμα, η πλειάδα $(A, A, 1, 1, \{E: x \to x\}, \{D: x \to x\})$ είναι ένα σχήμα κρυπτογράφησης με βάση τον ορισμό. Όμως, το σχήμα αυτό δεν μπορεί να προσφέρει ασφαλή επικοινωνία. Ο κύριος στόχος της κρυπτογραφίας είναι η αποφυγή γνώσης του αρχικού περιεχομένου σε περίπτωση που κάποιος κακόβουλος χρήστης παρέμβει στην επικοινωνία μεταξύ δύο χρηστών. Προφανώς κάτι τέτοιο δεν ισχύει στο προηγούμενο παράδειγμα, αφού το αρχικό κείμενο δε διαφέρει από το αντίστοιχο

κρυπτογράφημα. Επομένως, είναι απαραίτητη η απαίτηση δυσκολίας στην αποκρυπτογράφηση ενός μηνύματος σε έναν χρήστη, ο οποίος δεν είναι ενήμερος για το κλειδί κρυπτογράφησης. Για τον σκοπό αυτό είναι επιθυμητή η δυσκολία καθορισμού του κλειδιού ακόμη και σε περίπτωση που ένας επιτιθέμενος έχει γνώση για το αρχικό κείμενο και το αντίστοιχο κρυπτογράφημα. Ως «δυσκολία» νοείται ένα πρόβλημα το οποίο δε μπορεί να λυθεί σε πολυωνυμικό χρόνο.

Εκ πρώτης όψεως, η ιδέα ότι οι δύο χρήστες που θέλουν να επικοινωνήσουν μεταξύ τους κρατούν το σύστημα κρυπτογράφησης μυστικό φαίνεται λογική. Ωστόσο, σύμφωνα με την αρχή του Kerckhoff, η ασφάλεια μιας επικοινωνίας δε θα πρέπει να βασίζεται στην μυστικότητα ενός σχήματος κρυπτογράφησης [6]. Με άλλα λόγια, οι δύο χρήστες που θέλουν να επικοινωνήσουν μεταξύ τους πρέπει να υποθέσουν ότι ένας επιτιθέμενος έχει γνώση για το σχήμα κρυπτογραφίας που χρησιμοποιούν.

2.2.1 Κρυπτοσυστήματα Δημοσίου Κλειδιού

Ένα σχήμα κρυπτογράφησης μπορεί να χρησιμοποιεί το ίδιο κλειδί για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Ένα τέτοιο σχήμα, ονομάζεται συμμετρικό. Στην περίπτωση αυτή δεν υπάρχει διάκριση μεταξύ των κλειδιών κρυπτογράφησης και αποκρυπτογράφησης, καθώς συμπεριφέρονται σαν ένα αντικείμενο. Ένα από τα βασικότερα μειονεκτήματα της συμμετρικής κρυπτογραφίας είναι ότι το επιλεγμένο κλειδί πρέπει πάντα να παραμένει μυστικό. Ακόμη και αν το σχήμα προσφέρει την μέγιστη ασφάλεια που μπορεί να υπάρξει, αν το κλειδί διαρρεύσει, τότε υπάρχει παραβίαση της ασφάλειας.

Η μεγαλύτερη απειλή όσον αφορά την ασφάλεια είναι η υποκλοπή ενός κλειδιού κατά την διάρκεια την ανταλλαγής του. Όταν δύο χρήστες ανταλλάσσουν πληροφορίες σχετικά με το κλειδί που πρόκειται να χρησιμοποιηθεί για την εξασφάλιση της επικοινωνίας τους, υπάρχει πάντα η πιθανότητα υποκλοπής του από έναν κακόβουλο χρήστη. Για την αντιμετώπιση αυτού του μειονεκτήματος των συμμετρικών σχημάτων κρυπτογραφίας, δημιουργήθηκαν τα ασύμμετρα σχήματα (ή κρυπτοσύστημα δημοσίου κλειδιού).

Η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού προσφέρει κυρίως λύσεις στο πρόβλημα μεταφοράς κλειδιού, καθώς και έχει εφαρμογή σε συστήματα ψηφιακών υπογραφών [7]. Η διανομή κλειδιού είναι ένα άμεσο πρόβλημα που προκύπτει από την χρήση ενός συμμετρικού μηχανισμού κρυπτογράφησης [2]. Για την ασφαλή επικοινωνία μεταξύ δύο χρηστών, ένα μυστικό κλειδί θα πρέπει να μεταφερθεί μέσω ενός ασφαλούς καναλιού. Η λειτουργία της ασύμμετρης κρυπτογραφίας βασίζεται σε ένα ζεύγος κλειδιών, το δημόσιο κλειδί PK που χρησιμοποιείται για την κρυπτογράφηση ενός μηνύματος (ή ως υπογραφή) και το ιδιωτικό κλειδί SK, το οποίο χρησιμοποιείται για την αποκρυπτογράφηση (ή την επιβεβαίωση μιας υπογραφής). Επομένως, σε αντίθεση με τα συμμετρικά σχήματα, τα ασύμμετρα χρησιμοποιούν διαφορετικά κλειδιά για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Το δημόσιο κλειδί είναι διαθέσιμο σε όλους τους χρήστες έτσι ώστε να είναι σε θέση να κρυπτογραφήσουν ένα μήνυμα (ή να επιβεβαιώσουν μια υπογραφή). Από την άλλη, το ιδιωτικό κλειδί κρατείται μυστικό με τρόπο τέτοιο ώστε ο ιδιοκτήτης να είναι ο μόνος που να μπορεί να αποκρυπτογραφήσει μηνύματα τα οποία έχουν δημιουργηθεί με το αντίστοιχο δημόσιο κλειδί (ή να δημιουργήσει υπογραφές οι οποίες μπορούν να επιβεβαιωθούν από το αντίστοιχο δημόσιο κλειδί).

Ένα κρυπτοσύστημα δημοσίου κλειδιού περιλαμβάνει μια τριπλέτα αλγορίθμων (G, E, D), δηλαδή, τους αλγορίθμους δημιουργίας κλειδιού (key generation), κρυπτογράφησης (encode) και αποκρυπτογράφησης (decode). Ο αλγόριθμος δημιουργίας κλειδιού, λαμβάνει ως είσοδο παραμέτρους ασφαλείας και αποφέρει ένα ζεύγος κλειδιών (PK, SK). Το δημόσιο κλειδί PK ορίζει το χώρο των αρχικών μηνυμάτων M, δηλαδή το σύνολο όλων των πιθανών αρχικών μηνυμάτων που μπορούν να προωθηθούν στον αλγόριθμο κρυπτογράφησης, καθώς και των χώρο των κρυπτοκειμένων C, δηλαδή το σύνολο των πιθανών κρυπτοκειμένων που μπορούν να προωθηθούν στον αλγόριθμο αποκρυπτογράφησης. Οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης λειτουργούν βάση του δημοσίου PK και ιδιωτικού κλειδιού SK που δημιουργήθηκαν από τον προηγούμενο αλγόριθμο. Η κρυπτογράφηση ενός αρχικού μηνύματος $m \in M$ σε ένα κρυπτοκείμενο (ciphertext) C με την χρήση του δημοσίου κλειδιού PK ορίζεται ως:

$$C = E(PK, m).$$

Αντίστοιχα, η διαδικασία αποκρυπτογράφησης ενός κρυπτοκειμένου $c \in C$ σε ένα αρχικό μήνυμα M με την χρήση του ιδιωτικού κλειδιού SK ορίζεται ως:

$$M = D(SK, c).$$

Μια αναλογία ενός κρυπτοσυστήματος δημοσίου κλειδιού στον πραγματικό κόσμο είναι ότι ένας φάκελος μπορεί να τοποθετηθεί στο γραμματοκιβώτιο ενός ατόμου από οποιονδήποτε (κρυπτογράφηση), αλλά μόνο η οντότητα (ιδιοκτήτης) που έχει το κλειδί (ιδιωτικό κλειδί) μπορεί να ανακτήσει (αποκρυπτογραφήσει) το περιεχόμενο του [13]. Γενικότερα, για να θεωρείται ένα κρυπτοσύστημα δημοσίου κλειδιού ασφαλές θα πρέπει να είναι υπολογιστικά αδύνατο να βρεθεί το αρχικό μήνυμα M χωρίς την γνώση του ιδιωτικού κλειδιού SK, ακόμη και αν το δημόσιο κλειδί PK είναι γνωστό [14]. Σε κάθε περίπτωση, για κάθε σχήμα ασύμμετρης κρυπτογραφίας (G, E, D) θα πρέπει να ισχύει η ιδιότητα της ορθότητας (correctness property), δηλαδή, για όλα τα ζεύγη (PK, SK), η αποκρυπτογράφηση $D(SK, c) = m$ πρέπει να ισχύει για όλες τις κρυπτογραφήσεις $c = E(PK, m)$.

Η ασύμμετρη κρυπτογραφία, όπως αναφέρθηκε προηγουμένως, λύνει το πρόβλημα διανομής κλειδιού. Το μόνο που απαιτείται από έναν χρήστη είναι να κάνει διαθέσιμο το δημόσιο κλειδί του. Οποιοσδήποτε χρήστης είναι ενήμερος για ένα δημόσιο κλειδί μπορεί να αποστείλει κρυπτογραφημένα μηνύματα. Όμως, το πρόβλημα που προκύπτει είναι ότι ένας ωτακουστής (eavesdropper) μπορεί να δημοσιεύσει ένα κλειδί παριστάνοντας κάποιον άλλον χρήστη. Το πρόβλημα αυτό λύνεται από την υποδομή δημοσίου κλειδιού (Public Key Infrastructure) - PKI.

Ένα σύστημα τύπου PKI πιστοποιεί την ιδιοκτησία του δημοσίου κλειδιού ενός χρήστη δια μέσου μιας αρχής πιστοποίησης (certificate authority), η οποία αποτελεί μια τρίτη έμπιστη οντότητα. Η αρχή πιστοποίησης εκδίδει και διαχειρίζεται ένα σύνολο πιστοποιητικών δημοσίου κλειδιού, τα οποία πιστοποιούν ότι ένα δημόσιο κλειδί ανήκει σε έναν συγκεκριμένο χρήστη. Το ψηφιακό αυτό πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί του χρήστη και την ταυτότητα του και είναι υπογεγραμμένο από την αρχή πιστοποίησης. Όποτε δύο χρήστες θέλουν να επικοινωνήσουν, ανταλλάσσουν τα πιστοποιητικά τους. Κάθε χρήστης επαληθεύει την υπογραφή από το πιστοποιητικό που παρέλαβε δια μέσω του δημοσίου κλειδιού της αρχής πιστοποίησης, το οποίο είναι γνωστό σε όλους τους χρήστες. Εάν η υπογραφή γίνει αποδεκτή, τότε το πιστοποιητικό θεωρείται έγκυρο και οι δύο χρήστες είναι σίγουροι για τις ταυτότητες και τα δημόσιο κλειδιά τους. Επομένως, μια ασφαλής επικοινωνία μπορεί να αρχικοποιηθεί.

2.2.2 Ασφάλεια κρυπτοσυστημάτων δημοσίου κλειδιού

Όσον αφορά τον ορισμό της ασφάλειας ενός σχήματος κρυπτογράφησης πρέπει να ληφθούν υπόψη οι στόχοι ασφάλειας καθώς και πιθανές επιθέσεις σε αυτό [8]. Βασικός στόχος της ασύμμετρης κρυπτογραφίας και εν γένει των κρυπτογραφικών σχημάτων είναι η χρήση ενός κλειδιού το οποίο μετατρέπει κατάλληλα τα μηνύματα επικοινωνίας μεταξύ δύο χρηστών με τρόπο τέτοιο ώστε ένας ωτακουστής να μην είναι σε θέση να αναγνωρίζει το αρχικό μήνυμα. Ωστόσο, όσο οι επικοινωνίες και τα δίκτυα γίνονται ευκολότερα προσβάσιμα, ένας επιτιθέμενος δε θα περιοριστεί στον παθητικό ρόλο του ωτακουστή, αλλά θα λάβει πιο ενεργητικό ρόλο. Για παράδειγμα, θα μπορούσε να επικοινωνήσει με έναν έγκυρο χρήστη, αποστέλλοντας του κρυπτογραφημένα μηνύματα με σκοπό την ανάλυση της απάντησης που θα λάβει. Τέτοιου είδους ενεργητικές επιθέσεις είναι πιο ισχυρές και δυσκολότερο να αντιμετωπιστούν από ότι οι παθητικές [9].

Για την μοντελοποίηση αυτών των τύπων επιθέσεων, η έννοια της ασφάλειας επιλεγμένου κρυπτοκειμένου (chosen-ciphertext) προτάθηκε από τους Naor και Yung [10] και έπειτα αναπτύχθηκε από διάφορους ερευνητές [11]. Η ασφάλεια έναντι της επίθεσης επιλεγμένου κρυπτοκειμένου (CCA) σημαίνει ότι ακόμη και αν ο επιτιθέμενος μπορεί να αποστείλει ερωτήματα αποκρυπτογράφησης στο σύστημα για ένα κρυπτοκείμενο της επιλογής του, δε θα μπορεί να λάβει καμία χρήσιμη πληροφορία για την αποκρυπτογράφηση άλλων μηνυμάτων στα αντίστοιχα κρυπτογραφήματά τους. Το πρώτο πρακτικό CCA-ασφαλές κρυπτοσύστημα, παρουσιάστηκε από τους Cramer και Shoup [12], ασφάλεια του οποίου βασίζεται στο πρόβλημα Diffie-Hellman, το οποίο θα παρουσιαστεί στην συνέχεια.

Για την περιγραφή της ασφάλειας των ασύμμετρων σχημάτων και εν συνεχεία των υβριδικών, αρκούμαστε σε έναν στόχο ασφάλειας, την αδιακρισία (indistinguishability). Η αδιακρισία (IND) αποδίδει την ανικανότητα ενός επιτιθέμενου να μάθει οποιαδήποτε πληροφορία για ένα αρχικό μήνυμα m με την γνώση ενός κρυπτοκειμένου c [14]. Με άλλα λόγια, η έννοια του συγκεκριμένου στόχου υποδηλώνει ότι ένα σύστημα είναι ασφαλές εάν το πλεονέκτημα του επιτιθέμενου για την εισβολή σε ένα σχήμα είναι αμελητέο (negligible). Μια συνάρτηση $f: \mathbb{Z} \to \mathbb{R}$ είναι αμελητέα εάν για κάθε πολυώνυμο p υπάρχει ένας ακέραιος N_p έτσι ώστε $|f(n)| \leq \frac{1}{p(n)}$ για κάθε $n \geq N_p$. Εν γένει, ο ορισμός της ασφάλειας σε ένα σχήμα κρυπτογραφίας εκφράζεται με ένα παιχνίδι μεταξύ ενός διεκδικητή (challenger) και ενός επιτιθέμενου. Το παιχνίδι λειτουργεί σε δύο στάδιο, το στάδιο εύρεσης (πριν την πρόκληση) και το στάδιο εικασίας (μετά την πρόκληση). Για μια παράμετρο ασφαλείας k (για παράδειγμα το μέγεθος του κλειδιού σε bits), το παιχνίδι IND-CCA εκτελείται ως εξής:

Ο διεκδικητής δημιουργεί ένα ζεύγος (PK, SK) μέσω του αλγορίθμου G και δημοσιοποιεί το PK στον επιτιθέμενο. Το SK παραμένει μυστικό στον διεκδικητή.

1. Ο επιτιθέμενος μπορεί να εκτελέσει οποιονδήποτε αριθμό κρυπτογραφήσεων βάση του PK. Επιπλέον, μπορεί να πραγματοποιήσει αποστολή κρυπτοκειμένων C για αποκρυπτογράφηση στο σύστημα, το οποίο επιστρέφει $D(SK, C)$.
2. Ο επιτιθέμενος υποβάλλει δύο διαφορετικά επιλεγμένα αρχικά μηνύματα m_0, m_1 στον διεκδικητή.
3. Ο διεκδικητής επιλέγει τυχαία ένα bit $b \in \{0,1\}$ και δημιουργεί την πρόκληση $C' = E(PK, m_b)$.

4. Ο επιτιθέμενος μπορεί να πραγματοποιήσει οποιονδήποτε αριθμό κρυπτογραφήσεων για την πρόκληση C'. Σε αυτή τη φάση επιτρέπεται η αποστολή κρυπτοκειμένων $C \neq C'$ στο σύστημα για αποκρυπτογράφηση, το οποίο αποφέρει $D(SK, C)$.

Ο επιτιθέμενος εικάζει για την τιμή του b και νικά το παραπάνω παιχνίδι αν $b' = b$. Το πλεονέκτημα του επιτιθέμενου ορίζεται ως $|\mathrm{P}[b = b'] - 1/2|$. Ένα ασύμμετρο σχήμα κρυπτογραφίας είναι ασφαλές στο μοντέλο επίθεσης IND-CCA αν για όλους τους πολυωνιμικούς επιτιθέμενους A, το πλεονέκτημα νίκης του A για το παιχνίδι IND-CCA είναι αμελητέο ως συνάρτηση της παραμέτρου ασφαλείας k.

Γενικότερα, για την δημιουργία ενός ασφαλούς κρυπτοσυστήματος δημοσίου κλειδιού, ο προσδιορισμός του μυστικού (ιδιωτικού) κλειδιού βάση του δημοσίου κλειδιού πρέπει να είναι ένα δύσκολο πρόβλημα. Για να επιτευχθεί αυτό, τα σχήματα ασύμμετρης κρυπτογραφίας βασίζουν την λειτουργία τους σε ένα δύσκολο μαθηματικό πρόβλημα. Το δημοφιλέστερο κρυπτοσύστημα δημοσίου κλειδιού είναι το RSA [15], το οποίο παρουσιάστηκε το 1978 και βασίζει την λειτουργία του στο πρόβλημα της παραγοντοποίησης. Από τότε, πολλά κρυπτοσυστήματα δημοσίου κλειδιού και ψηφιακών υπογραφών έχουν προταθεί στην βιβλιογραφία. Πολλά από αυτά βασίζονται στο πρόβλημα του διακριτού λογαρίθμου, όπως το κρυπτοσύστημα ElGamal [16] ή στο πρόβλημα Diffie-Hellman [7].

2.2.3 Παραδείγματα κρυπτοσυστημάτων δημοσίου κλειδιού

Στην ενότητα 2.2 παρουσιάστηκε η έννοια ενός κρυπτοσυστήμστος δημοσίου κλειδιού, ενώ στις ενότητες 2.1.3 και 2.1.5 παρουσιάστηκαν δύο θεμελιώδεις δύσκολα μαθηματικά προβλήματα, στα οποία στηρίζουν την λειτουργία τους τα σχήματα αυτά. Παρακάτω, παρουσιάζονται 3 παράδειγμα σχημάτων ασύμμετρης κρυπτογραφίας, το κρυπτοσύστημα RSA, το κρυπτοσύστημα ElGamal και η ανταλλαγή κλειδιού με το σχήμα Diffie-Hellman.

2.2.3.1 Κρυπτοσύστημα RSA

Το πρώτο κρυπτοσύστημα δημοσίου κλειδιού προτάθηκε από τους Rivest, Shamir και Adleman, γνωστό ως RSA (από τα αρχικά των δημιουργών) [15], αποτελώντας ένα από τα δημοφιλέστερα και πολυχρησιμοποιημένα κρυπτοσυστήματα μέχρι και την σημερινή εποχή. Η λειτουργία του βασίζεται στο πρόβλημα της παραγοντοποίησης μεγάλων πρώτων αριθμών: ο πολλαπλασιασμός δύο μεγάλων πρώτων αριθμών είναι υπολογιστικά εύκολος, αλλά η παραγοντοποίηση του αποτελέσματος της προηγούμενης πράξης απαιτεί ογκώδης υπολογιστική προσπάθεια. Έτσι, το αντίστοιχο ζεύγος δημοσίου και ιδιωτικού κλειδιού αποφέρεται βάση δύο μεγάλων πρώτων αριθμών. Τα κλειδιά που προκύπτουν είναι συνήθως μεγαλύτερα από 1024 bits και έτσι είναι αρκετά δύσκολο να πραγματοποιηθεί ανάκτηση ενός αρχικού μηνύματος βάση του δημοσίου κλειδιού [17].

Ο αλγόριθμος RSA αποτελείται από τρείς φάσεις, την δημιουργία κλειδιού, την κρυπτογράφηση και την αποκρυπτογράφηση. Τα βήματα για την υλοποίηση του συγκεκριμένου αλγορίθμου είναι τα εξής:

1. Γίνεται επιλογή δύο μεγάλων πρώτων αριθμών p και q, με τρόπο τέτοιο ώστε το πρόβλημα παραγοντοποίησης του $n = p * q$ να είναι δύσκολο στο Z_n^*.

2. Γίνεται υπολογισμός του $n = p * q$, καθώς και της τιμής Euler $\varphi(n) = (p-1) * (q-1)$.
3. Γίνεται επιλογή ενός σχετικώς πρώτου αριθμού e με τον $\varphi(N)$, με $1 < e < \varphi(N)$, τέτοιον ώστε $MK\Delta\big(e, \varphi(n)\big) = 1$.
4. Γίνεται υπολογισμός του πολλαπλασιαστικού αντιστρόφου του $\varphi(n)$, το οποίο συμβολίζεται με d, έτσι ώστε $e * d \equiv 1(mod(\varphi(n))$, με $1 < d < \varphi(n)$.
5. Το δημόσιο κλειδί αποτελείται από το ζεύγος (e, n) και το ιδιωτικό κλειδί είναι η τιμή d.

Αφού έχουν υπολογιστεί οι παραπάνω τιμές, για την κρυπτογράφηση ενός μηνύματος m από έναν αποστολέα ο οποίος είναι ενήμερος για το δημόσιο κλειδί του παραλήπτη ακολουθεί την εξής διαδικασία:

1. Υπολογίζεται το κρυπτοκείμενο $c = m^e mod n$.

Αντίστοιχα, για την αποκρυπτογράφηση ενός μηνύματος c, ο παραλήπτης, ο οποίος έχει στην διάθεση του το ιδιωτικό του κλειδί ακολουθεί την εξής διαδικασία:

1. Υπολογίζεται το αρχικό μήνυμα $m = c^d mod n$.

Για παράδειγμα έστω ότι ένας χρήστης επιλέγει $p = 7$ και $q = 13$. Υπολογίζει $n = 7 * 13 = 91$ και $\varphi(N) = 6 * 12 = 72$. Στη συνέχεια επιλέγει τον αριθμό $e = 5$, ελέγχοντας ότι $MK\Delta(5,72) = 1$ και υπολογίζει τον αντίστροφο του, modulo 72, $d = 29$. Οι τιμές $(5,72)$ αποτελούν το δημόσιο κλειδί του χρήστη, ενώ η τιμή 29 το ιδιωτικό του κλειδί. Για την κρυπτογράφηση του μηνύματος $m = 10$ από έναν άλλο χρήστη, ο οποίος είναι ενήμερος για το ζεύγος $(5,29)$, υπολογίζει την τιμή $c = 10^5 mod 91 = 82$. Όταν ο παραλήπτης λάβει το κρυπτοκείμενο, χρησιμοποιεί το ιδιωτικό του κλειδί και υπολογίζει την τιμή $m = 82^{29} mod 91 = 10$.

Η ασφάλεια του κρυπτοσυστήματος RSA βασίζεται στο γεγονός ότι για την ανάκτηση του μυστικού εκθέτη d από το ζεύγος δημοσίου κλειδιού (e, n), ο επιτιθέμενος θα πρέπει να πραγματοποιήσει παραγώγιση του δημοσίου modulus n, διαδικασία η οποία θεωρείται υπολογιστικά αδύνατη για μεγάλα modulus [18]. Εάν ένας επιτιθέμενος μπορεί να παραγοντοποιήσει τον δημόσιο αριθμό n, θα είναι σε θέση να γνωρίζει τις τιμές p και q, και ως αποτέλεσμα το $\varphi(n)$. Επομένως, βάση του $\varphi(n)$ και του e θα είναι εύκολη η εύρεση του d. Με άλλα λόγια, μια οντότητα η οποία έχει υποκλέψει το κρυπτοκείμενο $c = m^e mod n$, για την παραβίαση ασφαλείας του RSA θα πρέπει με κάποιο τρόπο να γνωρίζει είτε το αρχικό μήνυμα m, είτε το ιδιωτικό κλειδί d, κάτι το οποίο είναι υπολογιστικά ανέφικτο. Επομένως, μια οντότητα η οποία έχει γνώση μόνο για το δημόσιο κλειδί δε θα πρέπει να μπορεί να αποκρυπτογραφήσει ένα κρυπτοκείμενο.

Οι τύποι επιθέσεων που μπορούν να εφαρμοστούν στον αλγόριθμο RSA είναι [1]:

i. Ο εξαντλητικός έλεγχος όλων των πιθανών ιδιωτικών κλειδιών.
ii. Μαθηματικές επιθέσεις, οι οποίες έχουν άμεση σχέση με το πρόβλημα της παραγοντοποίησης.
iii. Επιθέσεις χρονισμού, οι οποίες εκμεταλλεύονται τον χρόνο εκτέλεσης του αλγορίθμου αποκρυπτογράφησης.
iv. Επιθέσεις τύπου CCA.

Οι επιθέσεις τύπου εξαντλητικής αναζήτησης έχουν άμεση σχέση με τον χώρο των κλειδιών d. Όσο μεγαλύτερο είναι το πλήθος bit, τόσο δυσκολότερη γίνεται η εξαντλητική αναζήτηση. Ο επίσημος οργανισμός NIST προτείνει την χρήση κλειδιών μήκους 2048 bits για τον RSA [19].

Για τις μαθηματικές επιθέσεις, υπάρχουν τρείς προσεγγίσεις επίθεσης:

- Ανάλυση του n σε πρώτους παράγοντες. Ως αποτέλεσμα, ο επιτιθέμενος να είναι σε θέση να υπολογίσει το $\varphi(n) = (p-1) * (q-1)$, το οποίο θα αποφέρει τον προσδιορισμό του $d = e^{-1} mod(\varphi(n))$.
- Προσδιορισμός του $\varphi(n)$, χωρίς την ανάλυση σε πρώτους παράγοντες. Έτσι, ο επιτιθέμενος και πάλι θα είναι σε θέση να προσδιορίσει το $d = e^{-1} mod(\varphi(n))$.
- Προσδιορισμός του d, χωρίς την εύρεση του $\varphi(n)$.

Το πρώτο σενάριο φαίνεται πιο ρεαλιστικό σε περίπτωση που δεν υπάρχει διαρροή ασφαλείας από το σύστημα. Ο προσδιορισμός του $\varphi(n)$, δεδομένου του n είναι ισοδύναμος με την παραγοντοποίηση του n, το οποίο αποτελεί ένα δύσκολο μαθηματικό πρόβλημα.

Οι επιθέσεις χρονισμού έχουν να κάνουν με τον προσδιορισμό του ιδιωτικού κλειδιού βάση παρατήρησης του χρόνου εκτέλεσης του αλγορίθμου αποκρυπτογράφησης.

Όπως αναφέρθηκε, η ισχυρότερη έννοια ασφάλειας είναι η απόδειξη ανθεκτικότητας ενός κρυπτοσυστήματος έναντι επιθέσεων τύπου CCA. Ο αλγόριθμος RSA έχει αποδειχτεί ότι είναι ευάλωτος σε μια τέτοια επίθεση. Αυτό συμβαίνει στον RSA διότι ισχύει ότι η συνένωση δύο κρυπτογραφημάτων με διαφορετικά αρχικά μηνύματα είναι ίδια με το κρυπτογράφημα της συνένωσης των δύο αυτών μηνυμάτων εξ' αρχής, $E(PK, M) * E(PK, M') = E(PK, [M * M'])$. Ένα επιτιθέμενος γνωρίζοντας ένα κρυπτοκείμενο $C = M^e mod n$, υπολογίζει:

1. $X = (C * 2^e)\ mod\ n.$
2. Το X αποτελεί το επιλεγμένο κρυπτοκείμενο για το οποίο είναι γνωστό το αρχικό μήνυμα $Y = X^d\ mod\ n$. Βάση της ιδιότητας του RSA, ισχύει ότι $X = (C\ mod\ n) * (2^e\ mod\ n) = (M^e\ mod\ n) * (2^e\ mod\ n) = (2M)^e\ mod\ n$. Έτσι, γνωρίζοντας το Y, ο επιτιθέμενος μπορεί να υπολογίσει το αρχικό μήνυμα M.

Για την αντιμετώπιση της παραπάνω επίθεσης, το αρχικό μήνυμα συμπληρώνεται με τυχαία δεδομένα πριν κρυπτογραφηθεί με την συμπλήρωση δεδομένων από μια συνάρτηση κατακερματισμού (hash). Η τεχνική αυτή είναι γνωστή ως RSA-OAEP [20].

2.2.3.2 Κρυπτοσύστημα ElGamal

Ένα από τα δημοφιλέστερα κρυπτοσυστήματα είναι ο αλγόριθμος ElGamal [16], λειτουργία του οποίου βασίζεται στο πρόβλημα του διακριτού λογαρίθμου: δοθείσης μιας κυκλικής ομάδας G τάξης n, ενός γεννήτορα a της G και ενός στοιχείου $b \in G$, είναι υπολογιστικά αδύνατο να βρεθεί ο ακέραιος $x, 0 \leq x \leq n-1$, τέτοιος ώστε $a^x = b$.

Τα βήματα για την υλοποίηση του συγκεκριμένου αλγορίθμου είναι τα εξής:

1. Γίνεται επιλογή ενός μεγάλου πρώτου αριθμού p και ενός γεννήτορα g της υποομάδας του $\mathbb{Z}_p^*$.
2. Γίνεται επιλογή ενός τυχαίου ακεραίου αριθμού k, $1 \leq \kappa \leq p-2$.
3. Γίνεται υπολογισμός του $y = g^{\kappa}(modp)$.

4. Το δημόσιο κλειδί δίνεται από την τριπλέτα (p, g, y), ενώ το ιδιωτικό κλειδί αντιστοιχεί στην τιμή k.

Αφού έχει υπολογιστεί το ζεύγος δημοσίου και ιδιωτικού κλειδιού, για την κρυπτογράφηση ενός μηνύματος m από έναν αποστολέα ο οποίος είναι ενήμερος για το δημόσιο κλειδί του παραλήπτη ακολουθεί την εξής διαδικασία:

1. Γίνεται επιλογή ενός τυχαίου αριθμού r, $1 \leq r \leq p-2$.
2. Γίνεται υπολογισμός των $y_1 = g^r mod p$ και $y_2 = m * y^r (mod p)$.
3. Αποφέρεται το κρυπτογράφημα $c = (y_1, y_2)$.

Αντίστοιχα, για την αποκρυπτογράφηση ενός μηνύματος c, ο παραλήπτης, ο οποίος έχει στην διάθεση του το ιδιωτικό του κλειδί ακολουθεί την εξής διαδικασία:

1. Γίνεται υπολογισμός του αρχικού μηνύματος $m = y_2 (y_1^k)^{-1} mod p$.

Για παράδειγμα, έστω ότι ένας χρήστης επιλέγει τον αριθμό $p = 11$, τον γεννήτορα $g = 6$ στο Z_{11}^* και στην συνέχεια, επιλέγει $k = 2$. Έπειτα, υπολογίζει $y = 6^2 \ mod \ 36 = 3$. Το δημόσιο κλειδί αποτελείται από την τριπλέτα (11,6,3), ενώ η τιμή $k = 2$ αποτελεί το ιδιωτικό κλειδί του χρήστη. Για την κρυπτογράφηση ενός μηνύματος $m = 9$ από έναν άλλο χρήστη, ο οποίος είναι ενήμερος για το δημόσιο κλειδί του παραλήπτη, επιλέγει έναν τυχαίο αριθμό $r = 2$ και υπολογίζει τις τιμές $y_1 = 6^2 \ mod \ 11 = 3$ και $y_2 = 9 * 3^2 \ mod \ 11 = 4$. Όταν ο παραλήπτης λάβει το κρυπτοκείμενο που αποτελείται από το ζεύγος (3,4), χρησιμοποιεί το ιδιωτικό του κλειδί και υπολογίζει την τιμή $m = 4 * (3^2)^{-1} \ mod \ 11$. Ο αντίστροφος του 9 mod 11 είναι το 5, άρα $m = 4 * 5 \ mod \ 11 = 9$.

Η ασφάλεια του κρυπτοσυστήματος ElGamal βασίζεται στις ιδιότητες της κυκλικής ομάδας G. Σαφώς, εάν ο επιτιθέμενος ανακτήσει το ιδιωτικό κλειδί k, θα μπορεί να αποκρυπτογραφεί οποιοδήποτε μήνυμα. Αφού, το δημόσιο κλειδί περιλαμβάνει την τιμή $y = g^\kappa$, η εύρεση του ιδιωτικού κλειδιού με την γνώση του δημοσίου βασίζεται στον υπολογισμό του διακριτού λογαρίθμου στην κυκλική ομάδα $\langle g \rangle$. Για τον λόγο αυτό, ο αριθμός p πρέπει να είναι αρκετά μεγάλος. Για την εισβολή σε ένα κρυπτοκείμενο $y = (y_1, y_2) = (g^\kappa, m * y^k)$ θα ήταν αρκετό να βρεθεί η τιμή y^{-k}, αφού $m = y_2 * y^{-k}$. Επομένως, αυτό που απαιτείται από τον επιτιθέμενο είναι η εύρεση του y^k, μιας και οι υπολογισμοί των αντιστρόφων μπορούν εύκολα να υπολογιστούν. Για την εύρεση του k αρκεί ο υπολογισμός του διακριτού λογαρίθμου $y_1 = g^\kappa$. Εν γένει, η εύρεση του αρχικού μηνύματος βάση του κρυπτοκειμένου είναι ισοδύναμο με το υπολογιστικό (computational) πρόβλημα Diffie-Hellman (το οποίο θα συζητηθεί στην επόμενη ενότητα), σύμφωνα με το οποίο: δοσμένου του (g, g^a, g^b) , είναι δύσκολος ο υπολογισμός του g^{ab}. Επιπλέον, ένας επιτιθέμενος ο οποίος δεν είναι ενήμερος για την τυχαία τιμή r, δε θα είναι σε θέση να γνωρίζει ένα αρχικό μήνυμα m' κρυπτογραφώντας με το δημόσιο κλειδί και συγκρίνοντας το με το κρυπτογράφημα που έχει υποκλέψει.

Μια από τις βασικότερες αδυναμίες του αλγορίθμου ElGamal είναι η χρήση του ίδιου κλειδιού σε διαφορετικά μηνύματα επικοινωνίας. Έστω ότι ένας χρήστης χρησιμοποιεί το ίδιο ιδιωτικό κλειδί για την αποστολή δύο διαφορετικών μηνυμάτων m_1 και m_2. Στην περίπτωση αυτή η τιμή y_1 θα είναι ίδια για τα δύο μηνύματα ($y_1 = y_1'$). Έτσι, τα ζεύγη κρυπτοκειμένων θα είναι (y, y_2) και (y, y_2'). Εάν ο επιτιθέμενος επιλέξει να επιτεθεί στο αρχικό μήνυμα m_1, θα μπορεί να καθορίσει και το μήνυμα m_2. Αυτό συμβαίνει διότι $\frac{y_2}{m_1} = y^k = \frac{y_2'}{m_2} (mod p)$. Αφού ο επιτιθέμενος γνωρίζει για τα y_2και y_2' θα είναι σε θέση να υπολογίσει το m_2 βάση της γνώσης που έχει αποκτήσει από το

m_1, $m_2 = \frac{y_2' * m_1}{y_2} (mod p)$. Επομένως, απαραίτητη προϋπόθεση για την αποτελεσματική χρήση του αλγορίθμου ElGamal είναι η αποφυγή χρήσης του ίδιου ιδιωτικού κλειδιού.

2.2.3.3 Ανταλλαγή κλειδιού Diffie-Hellman

Όπως αναφέρθηκε, το πρόβλημα ανταλλαγής κλειδιού αποτελεί ένα από τα μεγαλύτερα προβλήματα στα κρυπτοσυστήματα που χρησιμοποιούν ένα σχήμα συμμετρικής κρυπτογραφίας. Ο αλγόριθμος Diffie-Hellman [7] λύνει το συγκεκριμένο πρόβλημα, ο οποίος και αποτελεί ένα χαρακτηριστικό παράδειγμα κρυπτοσυστήματος δημοσίου κλειδιού. Ο συγκεκριμένος αλγόριθμος έχει σχεδιαστεί για την ανταλλαγή κλειδιών, χωρίς να μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση μηνυμάτων. Όπως και το κρυπτοσύστημα ElGamal, και ο αλγόριθμος Diffie-Hellman βασίζεται στο πρόβλημα υπολογισμού διακριτών λογαρίθμων.

Υποθέτοντας ότι δύο χρήστες θέλουν να συμφωνήσουν σε ένα μυστικό κρυπτογραφικό κλειδί, αρχικά συμφωνούν σε μια πεπερασμένη αβελιανή ομάδα G, έναν μεγάλο πρώτο αριθμό p και μια πρωτεύουσα ρίζα g στο σύνολο Z_p^*. Στη συνέχεια, ο αλγόριθμος λειτουργεί ως εξής:

1. Η πρώτη οντότητα επιλέγει ένα τυχαίο ακέραιο αριθμό $a \in Z_{p-1}^*$.
2. Υπολογίζει και αποστέλλει το g^a στην δεύτερη οντότητα.
3. Η δεύτερη οντότητα επιλέγει τυχαία έναν ακέραιο $b \in Z_{p-1}^*$.
4. Υπολογίζει την τιμή $(g^a)^b$ και αποστέλλει g^b στην πρώτη οντότητα.
5. Η πρώτη οντότητα υπολογίζει $(g^b)^a = g^{ab}$.
6. Η τιμή a^{ab} αποτελεί το διαμοιρασμένο μυστικό κλειδί.

Για παράδειγμα, έστω ότι οι χρήστες έχουν συμφωνήσει στην αβελιανή ομάδα $G = Z_{19}^*$, $p = 19 \in Z_{19}^*$ και από το σύνολο πρωτευουσών ριζών {2,3,10,13,14,15} επιλέγουν $g = 3$. Η πρώτη οντότητα επιλέγει τυχαία τον ακέραιο $a = 5$ και μεταδίδει $3^5 \ mod \ 19 = 15$. Η δεύτερη οντότητα επιλέγει τον αριθμό $b = 11$ και μεταδίδει $3^{11} \ mod \ 19 = 10$. Η δεύτερη οντότητα υπολογίζει το διαμοιρασμένο κλειδί ως $15^{11} \ mod \ 19 = 3$ και η πρώτη οντότητα ως $10^5 \ mod \ 19 = 3$.

Η ασφάλεια του αλγορίθμου Diffie-Hellman έγκειται στο πρόβλημα διακριτών λογαρίθμων. Το υπολογιστικό πρόβλημα Diffie-Hellman ορίζεται ως εξής: Δεδομένου ενός πρώτου αριθμού p, μιας πρωτεύουσας ρίζας g στο σύνολο Z_p^* και των τιμών g^a και g^b για τυχαίους ακέραιους αριθμούς a και b, με $0 \leq a, b \leq p-1$, να βρεθεί η τιμή g^{ab}. Όπως και στον αλγόριθμο ElGamal, η ασφάλεια είναι ισάξια με την δυσκολία επίλυσης του προβλήματος διακριτού λογαρίθμου.

Στον αλγόριθμο Diffie-Hellman, η ασφάλεια μπορεί επιπλέον να οριστεί με το πρόβλημα απόφασης (decisional) Diffie-Hellman, κάτι που εφαρμόζεται και στο κρυπτοσύστημα ElGamal. Στο πρόβλημα αυτό ο επιτιθέμενος είναι ενήμερος για τις τιμές (g, p, g^a, g^b, g^{ab}) και (g, p, g^a, g^b, g^z), όπου $a, b, z \in Z_{p-1}^*$ είναι τυχαίοι εκθέτες και καλείται να αποφασίσει ποια πεντάδα από τις δύο αποτελεί αυτή που ολοκληρώνουν τον αλγόριθμο με επιτυχία.

Η βασικότερη αδυναμία του συγκεκριμένου αλγορίθμου είναι ότι μπορεί να υποστεί επίθεση τύπου ενδιάμεσης οντότητας (man-in-the-middle). Ένας επιτιθέμενος υποκρινόμενος ταυτόχρονα την μια από τις δυο οντότητες στην άλλη, λαμβάνει τις τιμές g^a και g^b. Εφόσον ελέγχει την επικοινωνία μπορεί να αλλάξει τις τιμές αυτές στις g^{m_1} και g^{m_2}, όπου m_1, m_2 είναι οι τιμές που επιλέγει ο επιτιθέμενος στο Z_{p-1}^*. Έτσι, οι δύο οντότητες θα πιστεύουν ότι έχουν εδραιώσει ένα

κλειδί συνόδου μεταξύ τους, ενώ στην πραγματικότητα το κλειδί αυτό θα το διαμοιράζονται με τον επιτιθέμενο. Η πρώτη οντότητα θα έχει εδραιώσει το κλειδί g^{am_2} και η δεύτερη το κλειδί g^{am_1} με τον επιτιθέμενο. Εφόσον ο επιτιθέμενος αποτελεί την ενδιάμεση οντότητα στα μηνύματα που ανταλλάσουν μεταξύ τους οι δύο έγκυρες οντότητες μπορεί να λαμβάνει τα κρυπτογραφημένα μηνύματα τους, να τα αποκρυπτογραφεί και στην συνέχεια μπορεί κατά βούληση να τα τροποποιεί και να τα αποστέλλει στον προορισμό τους. Για την αντιμετώπιση της συγκεκριμένης επίθεσης τα μηνύματα στα οποία παρέχονται οι τιμές που έχουν επιλέξει οι δύο οντότητες πρέπει να είναι αυθεντικοποιημένα. Κάτι τέτοιο συμβαίνει στο πλαίσιο εγκαθίδρυσης κλειδιού συνόδου στο πρωτόκολλο TLS [21] με δύο τρόπους, το εφήμερο (ephemeral) και στατικό (static) Diffie-Hellman. Έτσι, η συγκεκριμένη αδυναμία μπορεί να επιλυθεί με την χρήση ψηφιακών υπογραφών ή πιστοποιητικών δημοσίου κλειδιού.

2.3 Θεωρία Ελλειπτικών καμπυλών

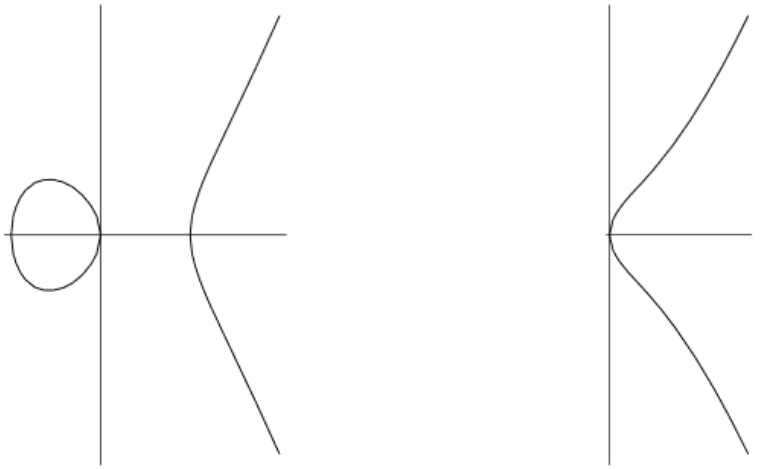
Στην ενότητα αυτή πραγματοποιείται μια συνοπτική μελέτη της θεωρίας ελλειπτικών καμπυλών. Οι ελλειπτικές καμπύλες προτάθηκαν αρχικά ως η βάση δημιουργίας κρυπτογραφικών σχημάτων δημοσίου κλειδιού στα μέσα της δεκαετίας του 1980 από τον Miller [22] και Koblitz [23]. Η χρήση τους παρέχει ασύμμετρα κρυπτοσυστήματα βασισμένα στον διακριτό λογάριθμο, τα οποία μπορούν να χρησιμοποιούν μικρότερο μήκος κλειδιού από άλλα ασύμμετρα σχήματα, παρέχοντας ισότιμο επίπεδο ασφαλείας. Για παράδειγμα με την χρήση κρυπτογραφίας ελλειπτικών καμπυλών (ECCs) με μήκος κλειδιού 160 bit, παρέχεται το ίδιο επίπεδο ασφαλείας με την χρήση ενός κλασσικού κρυπτοσυστήματος RSA με μήκος κλειδιού 1024 bits [24]. Έτσι, τα ECCs παρέχουν γρηγορότερη υλοποίηση για τις μεθόδους διαμοιρασμού κλειδιού, κρυπτογράφησης και αποκρυπτογράφησης από άλλα σχήματα όπως τον RSA ή συστήματα βασισμένα στον διακριτό λογάριθμο.

2.3.1 Γενικά Στοιχεία Ελλειπτικών Καμπυλών

Η κύρια διαφορά των ελλειπτικών καμπυλών έναντι συμβατικών κρυπτογραφικών σχημάτων είναι ότι χρησιμοποιούνται πεπερασμένα σώματα που έχουν τάξη έναν πρώτο αριθμό ή σώματα Galois αντί δακτυλίων της μορφής $\mathbb{Z}_n$. Έτσι, οι ελλειπτικές καμπύλες είναι ομάδες που ορίζονται σε ένα σώμα K και περιγράφονται από κυβικές εξισώσεις. Με άλλα λόγια, μια ελλειπτική καμπύλη είναι μια εξίσωση δευτέρου βαθμού ως προς μια μεταβλητή y και τρίτου βαθμού ως προς μια μεταβλητή x, με συντελεστές τα στοιχεία του σώματος K. Όπως έχει αναφερθεί σώμα ονομάζεται ένα σύνολο στοιχείων F. Ειδικά για τις ελλειπτικές καμπύλες ως K θεωρείται ένα πεπερασμένο σώμα ακεραίων υπολοίπων $modulo\ p$, το οποίο συμβολίζεται με F_p και ισχύει ότι $F_p = \mathbb{Z}/p\mathbb{Z}$, με p πρώτο αριθμό. Γενικότερα, τα σώματα στα οποία ορίζονται οι ελλειπτικές καμπύλες συμβολίζονται με F_q.

Εν γένει, η κυβική εξίσωση που περιγράφει μια ελλειπτική καμπύλη E σε ένα πεπερασμένο σώμα (ή σώμα Galois) GF δίνεται από την εξίσωση Weierstrass $y^2 + axy + by = x^3 + cx^2 + dx + e$ [27], όπου $a, b, c, d, e \in GF$. Για τον σκοπό περιγραφής των ελλειπτικών καμπυλών, αρκεί η εξίσωση $y^2 = x^3 + ax + b$, όπου οι μεταβλητές x, y και οι σταθερές τιμές a, b ανήκουν σε ένα πεπερασμένο σώμα F_p, με p πρώτο αριθμό και ικανοποιούν την συνθήκη $4a^3 + 27b^2 \neq 0$ [25]. Τα σημεία που ικανοποιούν την προηγούμενη συνθήκη ονομάζονται αφινικά (affine), ενώ σε κάθε ελλειπτική καμπύλη ορίζεται ένα σημείο 0, το οποίο ονομάζεται και σημείο απείρου.

Για την απεικόνιση μιας ελλειπτικής καμπύλης πρέπει να υπολογιστεί η εξίσωση $y = \sqrt{x^3 + ax + b}$. Για δεδομένες τιμές των σταθερών τιμών a, b η γραφική παράσταση αποτελείται από τις θετικές και αρνητικές τιμές του y για κάθε τιμή του x. Έτσι, κάθε ελλειπτική καμπύλη είναι συμμετρική ως προς τον άξονα $y = 0$. Δύο βασικές μορφές των ελλειπτικών καμπυλών απεικονίζονται στην παρακάτω εικόνα. Το κυβικό $y^2 = x^3 - x = x(x-1)(x+1)$ έχει τρείς μοναδικές πραγματικές ρίζες και το κυβικό $y^2 = x^3 + x = x(x^2+1)$ έχει μια πραγματική ρίζα.



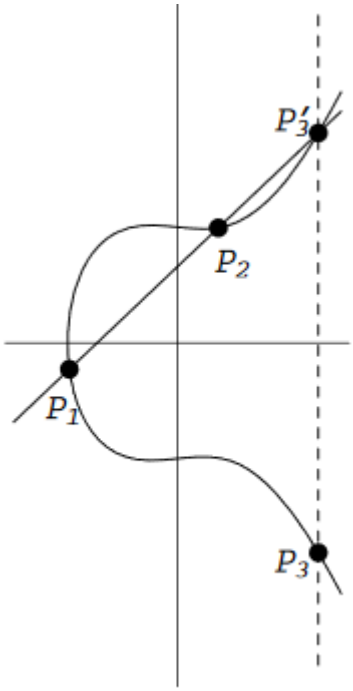
$(a) \quad y^2 = x^3 - x$ $(b) \quad y^2 = x^3 + x$

Εικόνα 2.1: Δύο βασικές απεικονίσεις ελλειπτικών καμπυλών, α) Το κυβικό $\boldsymbol{y^2 = x^3 - x}$ και β) το κυβικό $\boldsymbol{y^2 = x^3 + x}$ [26].

Δεν επιτρέπουμε πολλαπλές ρίζες για το κυβικό, υποθέτοντας ότι η διακρίνουσα της E, $\Delta = -(4a^3 + 27b^2) \neq 0$. Επομένως, οι ρίζες του κυβικού πρέπει να είναι μοναδικές.

Δοθείσης μιας ελλειπτικής καμπύλης $E(F_p)$ με τον περιορισμό της μη μηδενικής διακρίνουσας, μπορεί να οριστεί μια αβελιανή ομάδα με μεταβλητές τα σημεία (x, y) στην $E(F_p)$. Η πράξη της πρόσθεσης της ομάδας μπορεί να αναπαρασταθεί γραφικά ως εξής:

- Γίνεται λήψη ενός σημείου $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$ στην ελλειπτική καμπύλη $E(K)$, η οποία δίνεται από την εξίσωση $y^2 = x^3 + ax + b$. Τα σημεία P_1 και P_2 ενώνονται με μια ευθεία, με $m = \frac{y_2 - y_1}{x_2 - x_1}$, όπου m είναι η κλίση της συνάρτησης (slope).
- Η ευθεία τέμνει την E σε ακριβώς ένα σημείο, $P_3{}'$.
- Το σημείο αυτό αντικατοπτρίζεται στον άξονα x (πραγματοποιείται αλλαγή του πρόσημου στον άξονα y) και έτσι λαμβάνεται το σημείο P_3. Στην ουσία, το σημείο P_3 είναι το αποτέλεσμα της πρόσθεσης των σημείων P_1 και P_2, $P_3 = P_1 + P_2$.



Εικόνα 2.2: Πρόσθεση σημείων σε ελλειπτική καμπύλη [26].

Η παραπάνω μέθοδος είναι λειτουργική σε γενικότερο επίπεδο, ωστόσο, εξακολουθούν να υπάρχουν σημεία στην καμπύλη τα οποία δίνουν απροσδιόριστα αποτελέσματα. Για παράδειγμα, αν $P_1 = P_2$ με συντεταγμένη $y = 0$, τότε η εφαπτομένη δε θα τέμνει κανένα σημείο στην $E(F_p)$, εκτός από το ίδιο το σημείο. Για τον λόγο αυτό το σημείο απείρου (0), προστίθεται ως στοιχείο, το οποίο ονομάζεται και ταυτοτικό. Το σημείο αυτό είναι στην ουσία η κορυφή και το τέλος του άξονα y. Επιπλέον, το σημείο αυτό λειτουργεί ως μηδενικό στοιχείο, ορίζοντας $P + 0 = P$ για όλα τα $P \in E(K)$.

Ενναλακτικά, η πρόσθεση δύο σημείων μπορεί να γίνει αλγεβρικά, όπου και ορίζεται ο νόμος ομάδας (group law) ως εξής:

Έστω ότι E είναι η ελλειπτική καμπύλη, η οποία ορίζεται ως $y^2 = x^3 + Ax + B$.

Έστω ότι $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$ είναι τα σημεία της E με $P_1, P_2 \neq 0$.

Η πρόσθεση των δύο σημείων $P_1 + P_2 = P_3 = (x_3, y_3)$ ορίζεται ως εξής:

1. Αν $x_1 \neq x_2$, τότε $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$, όπου $m = \frac{y_2 - y_1}{x_2 - x_1}$.
2. Αν $x_1 = x_2$ και $y_1 \neq y_2$, τότε $P_1 + P_2 = 0$.
3. Αν $P_1 = P_2$ με $y_1 \neq 0$, τότε $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$, όπου $m = \frac{3x_1^2 + A}{2y_1}$.
4. Αν $P_1 = P_2$ με $y_1 = 0$, τότε $P_1 + P_2 = 0$.

Σε διαφορετική περίπτωση ορίζεται $P + 0 = P$ για όλα τα $P \in E(K)$.

Το αντίστροφο ενός σημείου P σε μια ελλειπτική καμπύλη που ορίζεται με την εξίσωση Weierstrass είναι ισοδύναμο με την εύρεση του αντίστροφου P' τέτοιο ώστε $P + P' = 0$. Το σημείο αυτό ονομάζεται και αρνητικό του P ή $-P$. Ακολουθώντας τον νόμο ομάδας, δύο σημεία $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$, όπου $x_1 = x_2$ και $y_1 \neq y_2$, αποφέρουν $P_1 + P_2 = 0$. Επειδή $x_1 = x_2$, τα y_1, y_2 είναι οι δύο ρίζες της εξίσωσης Weierstrass τέτοια ώστε $y_2 = -y_1$. Επομένως το σημείο $P' =$

$(x_1, -y_1)$ είναι το αντίστροφο του P. Επιπλέον, το αντίστροφο ενός σημείου ορίζεται και για $y_1 = y_2 = 0$ λόγω της τέταρτης περίπτωσης από τον νόμο ομάδας. Ο κανόνας αντιστρόφου μπορεί να συνοψιστεί στο ακόλουθο θεώρημα:

- Έστω ότι έχει υπολογιστεί ένα σημείο $P = (x, y)$ σε μια ελλειπτική καμπύλη, το αντίστροφό του P' είναι το σημείο $P' = (x, -y)$.

Το παραπάνω θεώρημα εφαρμόζεται στην εξίσωση Weierstrass $y^2 = x^3 + ax + b$. Για ελλειπτικές καμπύλες με διαφορετικές εξισώσεις, το αντίστροφο βρίσκεται διαφορετικά, ωστόσο δεν κρίνεται αναγκαία η παρουσίαση του για τους σκοπούς της εργασίας αυτής.

2.3.2 Κρυπτογραφία ελλειπτικών καμπυλών

Ο ορισμός της πρόσθεσης δύο σημείων επιτρέπει σε μια ελλειπτική καμπύλη να δημιουργήσει μια πεπερασμένη αβελιανή ομάδα με την πρόσθεση και τον πολλαπλασιασμό να είναι η λειτουργία της ομάδας, ενώ το σημείο απείρου να είναι το ταυτοτικό στοιχείο. Πολλά πρωτόκολλα χρησιμοποιούν μια πεπερασμένη αβελιανή ομάδα για την παροχή εμπιστευτικότητας και αυθεντικότητας. Ωστόσο, τα πρωτόκολλα αυτά απαιτούν λειτουργία υψηλότερου επιπέδου από την πρόσθεση σημείων, κάτι που στην περίπτωση των ελλειπτικών καμπυλών, ονομάζεται βαθμιαίος πολλαπλασιασμός (scalar multiplication). Βαθμιαίος πολλαπλασιασμός ενός σημείου P με βαθμό k, συμβολίζεται με $[k]P$ και ορίζεται ως $[k]P = P + P + \cdots + P$. Στην πράξη, με την πρόσθεση του ίδιου σημείου πολλαπλές φορές στην αβελιανή ομάδα μιας ελλειπτικής καμπύλης, η πράξη της πρόσθεσης μετατρέπεται σε βαθμιαίο πολλαπλασιασμό. Αυτό επιτρέπει τον πολλαπλασιασμό ενός σημείου P της ελλειπτικής καμπύλης με έναν ακέραιο αριθμό k, κάτι που αποφέρει την δημιουργία ενός άλλου σημείου στην ελλειπτική καμπύλη, $Q = k * P$. Η λειτουργία αυτή μπορεί να παρομοιαστεί με τον ορισμό των κρυπτοσυστημάτων που βασίζονται στον διακριτό λογάριθμο. Στην πραγματικότητα, οι περισσότεροι αλγόριθμοι που βασίζονται στον διακριτό λογάριθμο, όπως η ανταλλαγή κλειδιού Diffie-Hellman [7] μπορούν να μετατραπούν σε μια μορφή, κατάλληλη για χρήση από ελλειπτικές καμπύλες. Έτσι, η ασφάλεια των ελλειπτικών καμπυλών βασίζεται στην αδυναμία επίλυσης του προβλήματος διακριτού λογαρίθμου για ελλειπτικές καμπύλες.

Το πρόβλημα διακριτού λογαρίθμου σε ελλειπτικές καμπύλες (ECDLP) ορίζεται ως εξής: Δοθείσης μιας ελλειπτικής καμπύλης E, η οποία ορίζεται σε ένα πεπερασμένο σώμα F_q, ένα σημείο $P \in E(F_q)$ τάξης n και ένα σημείο $Q \in \langle P \rangle$, είναι δύσκολο να βρεθεί ένας ακέραιος $l \in [0, n-1]$ τέτοιος ώστε $Q = l * P$. Ο αριθμός l ονομάζεται διακριτός λογάριθμος του Q με βάση το P, $\mathrm{l} = log_p Q$.

Ασφαλής ελλειπτικές καμπύλες θεωρούνται αυτές στις οποίες το ECDLP είναι αδύνατο και η αδυναμία αυτή επιτρέπει στον βαθμιαίο πολλαπλασιασμό να αποτελεί την βασική κρυπτογραφική λειτουργία μιας ελλειπτικής καμπύλης. Σαφώς, οι παράμετροι της ελλειπτικής καμπύλης πρέπει να διαλέγονται με τέτοιο τρόπο ώστε η εξίσωση της ελλειπτικής καμπύλης να είναι ανθεκτική σε γνωστές επιθέσεις. Η πιο απλή επίθεση που λύνει το ECDLP είναι η εξαντλητική αναζήτηση όπου αυτό που έχει να κάνει ο επιτιθέμενος είναι να υπολογίσει την αλληλουχία των σημείων $P, 2P, 3P, \ldots$ έως ότου βρεθεί το σημείο Q. Ο εκτιμώμενος χρόνος εντοπισμού του σημείου Q είναι n βήματα, ενώ στην χειρότερη περίπτωση $n/2$ βήματα. Επομένως, η εξαντλητική αναζήτηση μπορεί να είναι εφικτή μόνο αν η τάξη n είναι μικρή. Οι πιο γνωστές επιθέσεις μείωσης του υπολογισμού του

αριθμού l είναι ο αλγόριθμος Pohlig-Hellman και ο αλγόριθμος rho του Pollard [27]. Και οι δύο επιθέσεις αυτές μειώνουν τον χρόνο υπολογισμού του l σε $\sqrt{n}$ [27].

Εν γένει, οι παράμετροι που χρησιμοποιούνται από οποιονδήποτε τύπο ελλειπτικής καμπύλης εξαρτώνται από το πεπερασμένο σώμα στο οποίο έχει οριστεί η E. Όπως αναφέρθηκε, δύο τύποι ελλειπτικών καμπυλών μπορούν να οριστούν σε ένα πεπερασμένο σώμα $GF(q)$, με $q = p^m$ στοιχεία, το πεπερασμένο σώμα $GF(p)$, όπου p είναι ένας πρώτος αριθμός με $m = 1$ και το πεπερασμένο σώμα Galois, $GF(2^m)$, όπου $m \geq 1$ είναι ένας ακέραιος αριθμός. Στην πρώτη περίπτωση, το σύνολο των παραμέτρων που ορίζουν την καμπύλη είναι (p, a, b, G, n, h), ενώ για το σώμα Galois το σύνολο των παραμέτρων είναι $(m, f(x), a, b, G, n, h)$, όπου:

- $p \in GF(p)$ είναι ένας πρώτος αριθμός.
- a και b είναι στοιχεία του πεπερασμένου σώματος.
- $G = (G_x, G_y)$ είναι ένα σημείο στην ελλειπτική καμπύλη που χρησιμοποιείται ως γεννήτορας των σημείων που για την αναπαράσταση των δημοσίων κλειδιών.
- n είναι ένας πρώτος αριθμός ο οποίος αναπαριστά την τάξη του σημείου G. Υπενθυμίζεται ότι η τάξη ενός σημείου G, το οποίο ανήκει σε μια ελλειπτική καμπύλη E είναι ο μικρότερος ακέραιος n ο οποίος αποφέρει $n * Q = 0$.
- h είναι ο συμπαράγοντας της καμπύλης, ο οποίος υπολογίζεται ως $h = \#E/n$, όπου $\#E$ είναι ο αριθμός των σημείων (τάξη) της ελλειπτικής καμπύλης.
- m είναι ένας ακέραιος που ορίζει το πεπερασμένο σώμα $GF(2^m)$.
- $f(x)$ είναι ένα πολυώνυμο βαθμού m, το οποίο ορίζει το σώμα $GF(2^m)$.

Σε ένα πρωτόκολλο δημοσίου κλειδιού, πριν τις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης πρέπει να δημιουργηθεί το ζεύγος δημοσίου και ιδιωτικού κλειδιού. Ειδικά για τις ελλειπτικές καμπύλες αυτά θα πρέπει να υπολογιστούν βάση αυτής. Για την δημιουργία ενός ζεύγους δημοσίου και ιδιωτικού κλειδιού, αρχικά, επιλέγεται το ιδιωτικό κλειδί. Αυτό είναι ένας ακέραιος αριθμός, ο οποίος συμβολίζεται ως d και επιλέγεται τυχαία στο πεδίο $[1, n-1]$. Το αντίστοιχο δημόσιο κλειδί είναι το σημείο της ελλειπτικής καμπύλης που ικανοποιεί την συνθήκη $W = [d]G$, όπου G είναι ένα σημείο στην ελλειπτική καμπύλη.

Ειδικότερα, έστω ότι E είναι μια ελλειπτική καμπύλη που ορίζεται σε ένα πεπερασμένο σώμα F_p, G ένα σημείο στην $E(F_p)$ τάξης n. Τότε η κυκλική υπο-ομάδα του $E(F_p)$ που δημιουργείται από το σημείο G είναι η $\langle G \rangle = \{\infty, G, 2G, 3G, \dots, (n-1)G\}$. Ο πρώτος αριθμός p, η εξίσωση της ελλειπτικής καμπύλης E, το σημείο G και η αντίστοιχη τάξη του n αποτελούν τις δημόσιες παραμέτρους. Το ιδιωτικό κλειδί είναι ένας ακέραιος αριθμός d, ο οποίος επιλέγεται τυχαία στο πεδίο $[1, n-1]$ και το αντίστοιχο δημόσιο κλειδί είναι το σημείο $W = dG$. Όπως αναφέρθηκε, το πρόβλημα καθορισμού του d βάση των δημόσιων παραμέτρων και του σημείου W είναι το πρόβλημα διακριτού λογαρίθμου σε ελλειπτικές καμπύλες [27].

Αλγόριθμος 1: Δημιουργία ζεύγους κλειδιών σε ελλειπτικές καμπύλες

Είσοδος: Δημόσιοι παράμετροι (p, E, G, n).

Έξοδος: Δημόσιο κλειδί W και ιδιωτικό κλειδί d.

1. Επιλογή ενός ακεραίου $d \in [1, n-1]$.
2. Υπολογισμός $W = dG$.
3. Έξοδος (W, d).

2.3.3 Ανταλλαγή κλειδιού Diffie-Hellman με ελλειπτικές καμπύλες

Όπως έχει ήδη αναφερθεί στην ενότητα 2.2.3.3 το σχήμα Diffie-Hellman έχει στόχο τον διαμοιρασμό ενός μυστικού κλειδιού σε δύο οντότητες που επικοινωνούν μέσω ενός μη ασφαλούς καναλιού, το οποίο προσφέρει εμπιστευτικότητα και ακεραιότητα των πληροφοριών που ανταλλάσσουν οι οντότητες αυτές [28]. Όπως και στην αρχική του μορφή, ο αλγόριθμος Diffie-Hellman με την χρήση ελλειπτικών καμπυλών έχει στόχο την δημιουργία ενός διαμοιρασμένου μυστικού κλειδιού, το οποίο μετέπειτα χρησιμοποιείται για την εξασφάλιση των επικοινωνιών μεταξύ δύο χρηστών.

Αρχικά, οι δύο χρήστες πρέπει να συμφωνήσουν στις παραμέτρους του συστήματος, οι οποίες ορίζονται στο πεπερασμένο σώμα $GF(q)$. Όπως αναφέρθηκε, οι παράμετροι αυτοί είναι είτε η πλειάδα (p, a, b, G, n, h) για την περίπτωση του πεπερασμένου σώματος $GF(p)$ είτε η πλειάδα $(m, f(x), a, b, G, n, h)$ για την περίπτωση του πεπερασμένου σώματος $GF(2^m)$. Επιπλέον κάθε ένας από τους δύο χρήστες που θέλουν να επικοινωνήσουν πρέπει να έχει στην διάθεση του ένα ζεύγος κλειδιών. Επομένως, κάθε χρήστης διαθέτει ένα ιδιωτικό κλειδί $d \in [1, n-1]$, το οποίο έχει επιλεγεί τυχαία και το αντίστοιχο δημόσιο κλειδί $W = d * G$, το οποίο, ουσιαστικά, είναι η επαναλαμβανόμενη πρόσθεση του σημείου G στον εαυτό του d φορές.

Υποθέτοντας ότι οι δύο χρήστες έχουν δημιουργήσει το ζεύγος κλειδιών, (d_A, W_A) και (d_B, W_B), αντίστοιχα ο αλγόριθμος λειτουργεί ως εξής:

1. Η πρώτη οντότητα υπολογίζει το σημείο $K = (x_K, y_K) = d_A * W_B$.
2. Αντίστοιχα, η δεύτερη οντότητα υπολογίζει το σημείο $K = (x_K, y_K) = d_B * W_A$.
3. Το μυστικό κλειδί που οι δύο οντότητες μοιράζονται είναι η x-συντεταγμένη του σημείου K, x_K.

Αξίζει να σημειωθεί ότι το τελικό διαμοιρασμένο κλειδί μετατρέπεται μέσω μιας συνάρτησης κατακερματισμού. Από τους παραπάνω υπολογισμούς, οι δύο χρήστες υπολογίζουν το σημείο K, διότι $d_A * W_B = d_A * d_B * G = d_B * d_A * G = d_B * W_A$. Έτσι, για το κλειδί που συμφωνούν οι δύο χρήστες, το μόνο που απαιτείται για τον υπολογισμό του είναι το δημόσιο κλειδί του καθενός. Ο μόνος τρόπος απόκτησης του ιδιωτικού κλειδιού είναι η επίλυση του ECDLP, κάτι το οποίο είναι υπολογιστικά αδύνατο.

Όπως είναι γνωστό, η βασικότερη αδυναμία του αλγορίθμου είναι η επίθεση ενδιάμεση οντότητας. Η επίθεση αυτή μπορεί να εφαρμοστεί και σε περίπτωση που χρησιμοποιούνται ελλειπτικές καμπύλες για τον υπολογισμό του διαμοιρασμένου μυστικού κλειδιού. Ένας επιτιθέμενος υποκρινόμενος ταυτόχρονα την μια οντότητα στην άλλη και αντίστροφα, λαμβάνει τις τιμές W_A και W_B και μπορεί να αλλάξει τις τιμές αυτές. Όπως και στην περίπτωση του Diffie-Hellman χωρίς την χρήση ελλειπτικών καμπυλών, για την αντιμετώπιση της επίθεσης, οι οντότητες θα πρέπει να αυθεντικοποιούν κατάλληλα τα μηνύματα.

Ειδικά για τις ελλειπτικές καμπύλες, άλλη μια επίθεση είναι εφικτή. Υποθέτοντας ότι ένας χρήστης έχει επιλέξει εσκεμμένα λανθασμένα σημεία στην καμπύλη για την δημιουργία του ιδιωτικού του κλειδιού και ο δεύτερος χρήστης δεν αυθεντικοποιήσει τα σημεία αυτά με τρόπο τέτοιο ώστε να διαπιστώσει ότι είναι μέρος της επιλεγμένης ομάδας, τότε ο πρώτος χρήστης μπορεί να λάβει σημαντικές πληροφορίες για το ιδιωτικό κλειδί του άλλου χρήστη. Έχει αποδειχτεί ότι τέτοιες επιθέσεις είναι εφικτές στο πρωτόκολλο SSL/TLS [29].

2.3.4 Κρυπτοσύστημα ElGamal με ελλειπτικές καμπύλες

Όπως αναφέρθηκε στην ενότητα 2.2.3.2, το κρυπτοσύστημα ElGamal βασίζεται στο πρόβλημα του διακριτού λογαρίθμου. Το συγκεκριμένο σχήμα, καθώς και άλλα που βασίζονται στο πρόβλημα του διακριτού λογαρίθμου μπορούν εύκολα να μεταφραστούν σε σχήματα που ορίζονται πάνω από ελλειπτικές καμπύλες (παρόμοια με την ανταλλαγή κλειδιού Diffie-Hellman που αναφέρθηκε προηγουμένως).

Αρχικά, όπως και στην περίπτωση της ανταλλαγής κλειδιού Diffie-Hellman πάνω από ελλειπτικές καμπύλες οι δύο χρήστες πρέπει να συμφωνήσουν στις παραμέτρους του συστήματος, υπό την έννοια ότι πρέπει να δημιουργηθεί η ελλειπτική καμπύλη E πάνω από ένα πεπερασμένο σώμα F_q αι να επιλεχθεί ένα σημείο G τάξης n. Επιπλέον, οι δύο χρήστες που θέλουν να εδραιώσουν ένα ασφαλές κανάλι πρέπει να δημιουργήσουν το αντίστοιχο ζεύγος δημοσίου-ιδιωτικού κλειδιού, καθώς και να συμφωνήσουν σε μια δημόσια συνάρτηση $f: m \rightarrow G_m$, η οποία μετατρέπει ένα αρχικό μήνυμα m σε ένα σημείο G_m στην ελλειπτική καμπύλη [23].

Η διαδικασία δημιουργίας κλειδιών ακολουθεί την τυπική διαδικασία που παρουσιάστηκε στην ενότητα 2.3.2, δηλαδή κάθε χρήστης επιλέγει τυχαία έναν αριθμό $d \in [1, n-1]$ και δημοσιοποιεί το σημείο $W = dG$, το οποίο αποτελεί το δημόσιο κλειδί του.

Για την κρυπτογράφηση ενός μηνύματος ο πρώτος χρήστης επιλέγει τυχαία έναν αριθμό $r \in [1, n-1]$ και υπολογίζει τα σημεία $C = rP$ και $C' = kY$. Στην συνέχεια, υπολογίζει το σημείο $G_m = f(m)$. Το τελικό κρυπτογράφημα αποτελείται από το ζεύγος (C, C_0), όπου $C_0 = C' + G_m$.

Όσον αφορά την διαδικασία αποκρυπτόγραφησης, ο παραλήπτης εφόσον λάβει το ζεύγος (C, C_0), υπολογίζει το σημείο C' βάση του ιδιωτικού του κλειδιού, $C' = dC$. Έπειτα, ανακτά το σημείο $G_m = C_0 - C = (r(dG) + G_m - (d(dG))$. Τέλος, ανακτά το μήνυμα m από την αντίστροφη συνάρτηση της f, $m = f^{-1}(G_m)$.

3 *Υβριδική Κρυπτογραφία*

Ένα κρυπτοσύστημα δημοσίου κλειδιού, τυπικά, λειτουργεί με μηνύματα σταθερού μεγέθους. Όποτε ένα μήνυμα μεγαλύτερου μεγέθους πρέπει να κρυπτογραφηθεί, συνήθως χρησιμοποιείται υβριδική κρυπτογράφηση: ένας συμμετρικός αλγόριθμος χρησιμοποιείται για την κρυπτογράφηση του μηνύματος με ένα τυχαίο μυστικό κλειδί K, το οποίο έχει κρυπτογραφηθεί με ένα κρυπτοσύστημα δημοσίου κλειδιού. Ο παραλήπτης χρησιμοποιεί το ιδιωτικό του κλειδί για την ανάκτηση του K, το οποίο μετέπειτα χρησιμοποιείται για την αποκρυπτογράφηση του μηνύματος. Η υβριδική κρυπτογραφία χρησιμοποιείται κυρίως για λόγους αποδοτικότητας, αφού η συμμετρική κρυπτογράφηση είναι γρηγορότερη σε σχέση με την χρήση ενός ασύμμετρου σχήματος.

Υπάρχουν κυρίως δύο λόγοι για τους οποίους η κρυπτογραφία δημοσίου κλειδιού δεν μπορεί να αποτελέσει αντικατάσταση των αλγορίθμων συμμετρικού κλειδιού [17]:

- Τα κρυπτοσυστήματα δημοσίου κλειδιού λειτουργούν πολύ πιο αργά από ότι τα συμμετρικά σχήματα. Αυτό συμβαίνει διότι απαιτούν περισσότερους πόρους λόγω της χρήσης δυο διαφορετικών κλειδιών.
- Οι αλγόριθμοι δημοσίου κλειδιού είναι αδύναμοι στις επιθέσεις τύπου επιλεγμένου αρχικού κειμένου (chosen plaintext). Το κλειδί κρυπτογράφησης είναι δημόσιο και το κρυπτοκείμενο δημιουργείτε βάση αυτού ($c = E(PK)$). Επομένως, ένας επιτιθέμενος θα μπορούσε να κρυπτογραφήσει όλα τα πιθανά αρχικά κείμενα και να συγκρίνει το αποτέλεσμα με το κρυπτοκείμενο. Έτσι, ακόμη και αν ο επιτιθέμενος δεν είναι σε θέση να αναπαράγει το ιδιωτικό κλειδί, με την προηγούμενη μέθοδο μπορεί να βρει το αρχικό κείμενο.

Στους αλγορίθμους υβριδικής κρυπτογραφίας λαμβάνει χώρα ένα συνδυασμός συμμετρικού κλειδιού με κρυπτογραφία δημοσίου κλειδιού. Επομένως, η υβριδική κρυπτογράφηση αποτελείται από δύο υπο-συστήματα: τον (ασύμμετρο) μηχανισμό ενθυλάκωσης κλειδιού (KEM) και τον (συμμετρικό) μηχανισμό ενθυλάκωσης δεδομένων (DEM). Στο KEM εκτελείται κρυπτογράφηση δημοσίου κλειδιού για να εξασφαλιστεί το (συμμετρικό) κλειδί συνόδου (session key). Με άλλα λόγια, το KEM είναι μια τεχνική υβριδικής κρυπτογραφίας με την οποία δημιουργείται ένα κλειδί συνόδου προς χρήση από συμμετρικούς αλγόριθμους μέσω ενός συστήματος κρυπτογραφίας δημοσίου κλειδιού. Αντίστοιχα, το DEM αποτελεί ένα κρυπτοσύστημα συμμετρικού κλειδιού, το οποίο κρυπτογραφεί τις πληροφορίες βάση του κλειδιού συνόδου που δημιουργήθηκε από την προηγούμενη διαδικασία [26],[31]. Οι Cramer και Shoup [26],[32] έδειξαν πως τα αυτά τα δύο υπο-συστήματα ενός σχήματος υβριδικής κρυπτογραφίας μπορούν να διαχωριστούν και οι απαιτήσεις ασφαλείας μπορούν να οριστούν ξεχωριστά.

Γενικότερα, για την κρυπτογράφηση ενός μηνύματος m, χρησιμοποιείται ο μηχανισμός KEM με το δημόσιο κλειδί του παραλήπτη για την δημιουργία του συμμετρικού κλειδιού K, καθώς και για την ασύμμετρη κρυπτογράφηση (ή ενθυλάκωση) αυτού του κλειδιού C_1. Έπειτα, το μήνυμα m κρυπτογραφείται συμμετρικά μέσω του DEM και του τυχαίου κλειδιού K που δημιουργήθηκε από το KEM, από όπου αποφέρεται το κρυπτογράφημα C_2. Το τελικό κρυπτογράφημα είναι το ζεύγος (C_1, C_2). Το ζεύγος αυτό αποκρυπτογραφείται αφού γίνει απενθυλάκωση του C_1 με το KEM και το ιδιωτικό κλειδί, έτσι ώστε να γίνει ανάκτηση του συμμετρικού κλειδιού K. Έπειτα με την χρήση του DEM και του συμμετρικού κλειδιού K γίνεται ανάκτηση του μηνύματος M από το κρυπτογράφημα C_2.

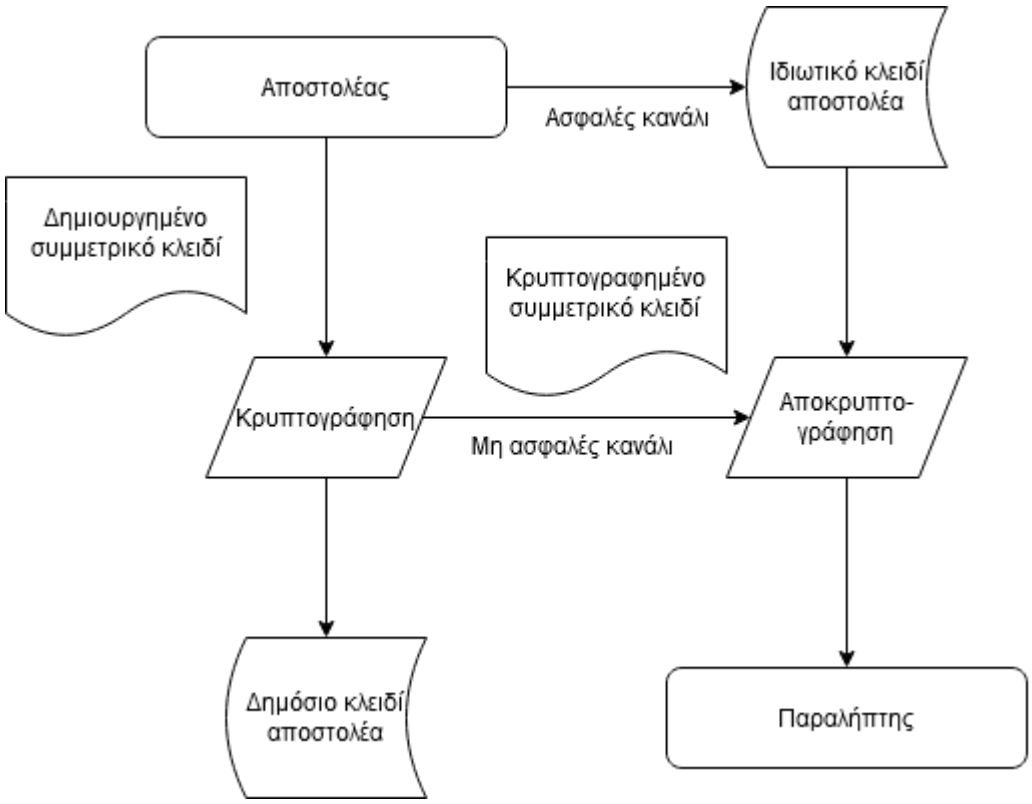
Το κίνητρο για την χρήση υβριδικής κρυπτογράφησης είναι να γίνει εκμετάλλευση των δυνατών σημείων των δύο μεθόδων κρυπτογράφησης, δηλαδή την ταχύτητα από την χρήση συμμετρικού κλειδιού και την ασφάλεια που παρέχει η ασύμμετρη κρυπτογραφία.

3.1 Μηχανισμοί Ενθυλάκωσης Κλειδιού

Οι μηχανισμοί τύπου KEM, αποτελούν, στην πράξη, σχήματα κρυπτογραφίας δημοσίου κλειδιού και προτάθηκαν από τον Shoup ως πρότυπα ISO [33]. Τυπικά, ένα KEM αποτελείται από μια τριπλέτα αλγορίθμων [34]:

1. $Generate_{KEM}(D)$: Αλγόριθμος δημιουργίας του ζεύγους δημοσίου και ιδιωτικού κλειδιού (PK, SK), με D τις παραμέτρους ασφαλείας (για παράδειγμα το μήκος του κλειδιού που πρόκειται να δημιουργηθεί).
2. $Encapsulate_{KEM}(PK)$: Αλγόριθμος ενθυλάκωσης (κρυπτογράφησης), ο οποίος αποφέρει το ζεύγος κλειδιού συνόδου και κρυπτογραφήματος του κλειδιού (K, C_1) με βάση το δημόσιο κλειδί PK.
3. $Decapsulate_{KEM}(SK, C_1)$: Αλγόριθμος απενθυλάκωσης (αποκρυπτογράφησης), ο οποίος αποφέρει το κλειδί συνόδου K με βάση το ιδιωτικό κλειδί SK και την κρυπτογραφημένη πληροφορία C_1.

Έτσι, τα KEMs είναι παρόμοια με τα σχήματα ασύμμετρης κρυπτογραφίας. Η διαφορά μεταξύ της χρήσης ενός KEM και ενός κρυπτοσυστήματος δημοσίου κλειδιού είναι ότι στο KEM με την είσοδο του δημοσίου κλειδιού του παραλήπτη, δημιουργείται ένα κρυπτογραφημένο μήνυμα και ένα κλειδί συνόδου, όπου το κρυπτογραφημένο μήνυμα αποστέλλεται στον παραλήπτη, ενώ το κλειδί συνόδου παραμένει μυστικό στον αποστολέα και χρησιμοποιείται στην επακόλουθη διαδικασία για την κρυπτογράφηση των δεδομένων. Αντίθετα, στην κρυπτογραφία δημοσίου κλειδιού, με την είσοδο ενός αρχικού μηνύματος και του δημοσίου κλειδιού του παραλήπτη δημιουργείται ένα κρυπτογραφημένο μήνυμα. Από την άλλη, στην αποκρυπτογράφηση, στον KEM με βάση την είσοδο του κρυπτομηνύματος και του ιδιωτικού κλειδιού του παραλήπτη δίδεται το κλειδί συνόδου, ενώ στην κρυπτογραφία δημοσίου κλειδιού, με βάση το κρυπτοκείμενο και το μυστικό κλειδί, δίδεται το αρχικό μήνυμα.



Εικόνα 3.1: Λειτουργία ενός KEM

Βασική απαίτηση για την λειτουργία ενός KEM είναι ότι για όλα τα ζεύγη (PK, SK) που δημιουργήθηκαν από τον αλγόριθμο δημιουργίας κλειδιού $Generate$ και για όλα τα ζεύγη (K, C_1) που δημιουργήθηκαν από τον αλγόριθμο ενθυλάκωσης $Encapsulate$, ισχύει ότι $Encapsulate_{KEM}(PK), Decapsulate_{KEM}(SK, C_1) = K$. Με άλλα λόγια, ένα KEM πρέπει να ικανοποιεί την ιδιότητα της ορθότητας, δηλαδή το κρυπτοκείμενο C_1 πρέπει να αποκρυπτογραφείται με βάση το δημόσιο κλειδί PK και να αποφέρει το κλειδί K.

3.1.1 Επιθέσεις στους μηχανισμούς ενθυλάκωσης κλειδιού

Μια κατασκευή ενός σχήματος υβριδικής κρυπτογραφίας, όπως αναφέρθηκε, επιτρέπει την δημιουργία των μηχανισμών KEM και DEM ξεχωριστά. Επομένως, και η ασφάλεια τους μπορεί να αξιολογηθεί ξεχωριστά. Υπάρχουν τρείς τύποι επιθέσεων που μπορούν να εφαρμοστούν στα KEMs, οι οποίες είναι [35]:

- *Επίθεση Επιλεγμένου μηνύματος* (Chosen Plaintext Attack) - CPA, ένας τύπος επίθεσης όπου ο επιτιθέμενος μπορεί να έχει πρόσβαση στην διαδικασία κρυπτογράφησης αλλά όχι στην αποκρυπτογράφηση. Σε αυτόν τον τύπο ο αντίπαλος έχει την δυνατότητα απόκτησης κρυπτοκειμένων για μηνύματα της επιλογής του.
- *Επίθεση Επιλεγμένου Κρυπτοκειμένου* (Chosen Ciphertext Attack) - CCA1, ένας τύπος επίθεσης όπου ο επιτιθέμενος μπορεί να λάβει πρόσβαση στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης. Σε αυτόν τον τύπο ο αντίπαλος έχει την δυνατότητα απόκτησης ενός ζεύγους αρχικού μηνύματος – κρυπτοκειμένου. Όμως, ο αντίπαλος δε μπορεί να λάβει πρόσβαση στην αποκρυπτογράφηση όταν λάβει ένα

κρυπτοκείμενο-στόχο. Σκοπός του είναι η αποκάλυψη του κλειδιού αποκρυπτογράφησης με βάση το ζεύγος που του έχει γίνει γνωστό.

- Επίθεση Προσαρμόσιμου Επιλεγμένου Κρυπτοκειμένου (Adaptive Chosen Ciphertext Attack)- CCA2, ένας τύπος επίθεσης όπου ο επιτιθέμενος μπορεί να λάβει πρόσβαση στην κρυπτογράφηση και αποκρυπτογράφηση ακόμη και αν έχει λάβει ένα κρυπτοκείμενο-στόχο.

Κάθε τύπος επίθεσης ορίζεται λαμβάνοντας υπόψη ότι ο αντίπαλος μπορεί να λάβει πρόσβαση στην διαδικασία κρυπτογράφησης ή/και αποκρυπτογράφησης. Η κρυπτογράφηση λαμβάνει ένα αρχικό μήνυμα και αποφέρει το κρυπτοκείμενο. Από την άλλη, η αποκρυπτογράφηση λαμβάνει κρυπτοκείμενα και αποφέρει τα αρχικά μηνύματα.

Γενικότερα, η ασφάλεια ενός KEM ορίζεται από το πλεονέκτημα που έχει ο επιτιθέμενος να κερδίσει ένα παιχνίδι ενάντια σε ένα σύστημα. Στόχος ενός επιτιθέμενου σε ένα KEM είναι η διάκριση του κλειδιού που αντιστοιχεί στην ενθυλάκωση δεδομένων. Το παιχνίδι μεταξύ διεκδικητή και επιτιθέμενου είναι παρόμοιο με αυτό που περιγράφηκε στην ενότητα 2.2.2, γνωστό ως IND-CCA και δοθείσης μιας παραμέτρου ασφαλείας k λειτουργεί ως εξής:

1. Ο διεκδικητής δημιουργεί ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού (PK, SK) βάση του αλγορίθμου $Generate_{KEM}(k)$ και το δημοσιοποιεί το PK στον επιτιθέμενο. Το SK παραμένει μυστικό στον διεκδικητή.
2. Ο επιτιθέμενος μπορεί να εκτελέσει οποιονδήποτε αριθμό ενθυλακώσεων βάση του PK. Στο μεταξύ, ο επιτιθέμενος μπορεί να αποστείλει ερωτήματα απενθυλάκωσης C στο σύστημα, το οποίο επιστρέφει $Decapsulate_{KEM}(SK, C)$. Με άλλα λόγια, ο επιτιθέμενος μπορεί να αποστείλει ερωτήματα ενθυλάκωσης και απενθυλάκωσης στο σύστημα. Το σύστημα εκτελεί τις απαραίτητες λειτουργίες και αποφέρει τα αποτελέσματα στον επιτιθέμενο.
3. Ο διεκδικητής δημιουργεί μια έγκυρη ενθυλάκωση (K_0, C') μέσω του αλγορίθμου $Encapsulate_{KEM}(PK)$. Επιπλέον, δημιουργεί ένα τυχαίο κλειδί K_1 με μήκος όσο το K_0. Έπειτα, επιλέγει τυχαία ένα bit $b \in \{0,1\}$ και θέτει $K' = K_b$. Τέλος, δημιουργεί την πρόκληση ενθυλάκωσης (K', C').
4. Ο επιτιθέμενος μπορεί να πραγματοποιήσει οποιονδήποτε αριθμό ενθυλακώσεων για την πρόκληση C'. Σε αυτή τη φάση ο επιτιθέμενος μπορεί να αποστείλει ερωτήματα απενθυλάκωσης $C \neq C'$ στο σύστημα, το οποίο θα επιστρέψει $Decapsulate_{KEM}(SK, C)$.

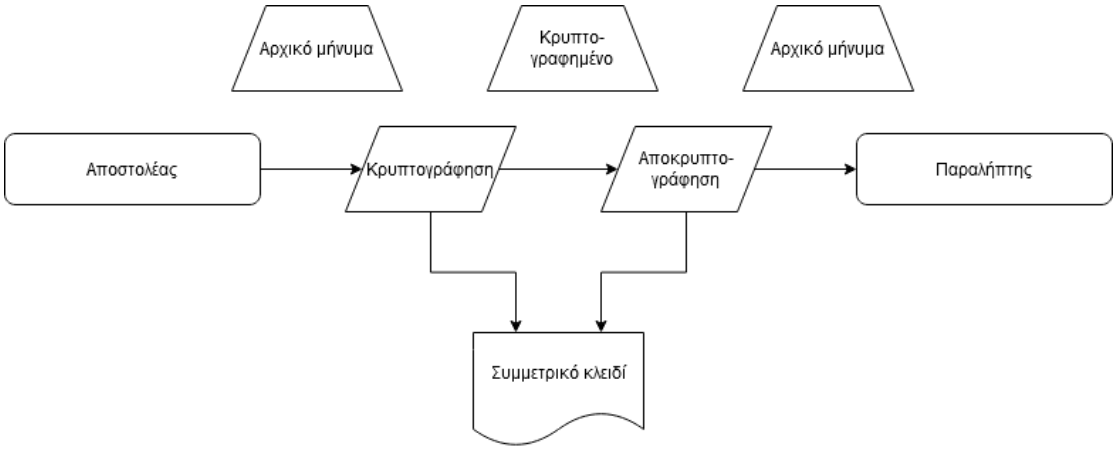
Ο επιτιθέμενος εικάζει για την τιμή του b και νικά το παιχνίδι αν $b' = b$. Το πλεονέκτημα του επιτιθέμενου ορίζεται ως $|\,\mathrm{P}[b = b'] - \frac{1}{2}|$. Ένα KEM είναι ασφαλές στο μοντέλο επίθεσης IND-CCA για όλους τους πολυωνιμικούς επιτιθέμενους A, όταν το πλεονέκτημα νίκης του A για το παιχνίδι IND-CCA είναι αμελητέο ως συνάρτηση της παραμέτρου ασφαλείας k [36].

3.2 Μηχανισμοί ενθυλάκωσης δεδομένων

Οι μηχανισμοί τύπου DEM, όπως και τα KEMs, επίσης, προτάθηκαν από τον Shoup ως πρότυπα ISO [33]. Ένα DEM αποτελείται από ένα ζεύγος αλγορίθμων:

1. $Encpypt_{DEM}(K, M)$: Αλγόριθμος κρυπτογράφησης, ο οποίος αποφέρει το κρυπτοκείμενο C_2, με βάση το μυστικό κλειδί K, το οποίο έχει δημιουργηθεί από το KEM, και το αρχικό μήνυμα M.
2. $Decrypt_{DEM}(K, C_2)$: Αλγόριθμος αποκρυπτογράφησης, ο οποίος αποφέρει το αρχικό μήνυμα Mβάση του μυστικού κλειδιού K και του κρυπτοκειμένου C_2.

Ουσιαστικά, τα DEMs είναι αλγόριθμοι συμμετρικής κρυπτογραφίας, με την διαφορά ότι το κλειδί που πρόκειται να χρησιμοποιηθεί, δημιουργείται από την προηγούμενη διεργασία του KEM και δεν έχει προ-συμφωνηθεί από τις οντότητες που συμμετέχουν σε μια συνομιλία.



Εικόνα 3.2: Λειτουργία ενός DEM

Βασική απαίτηση για την λειτουργία ενός DEM είναι ότι για κάθε κρυπτοκείμενο C_2 που δημιουργείται από τον αλγόριθμο κρυπτογράφησης $Encrypt$, ισχύει ότι $Encrypt_{DEM}(K, M), Decrypt_{DEM}(K, C_2) = M$. Με άλλα λόγια, για όλα τα κλειδιά K, ο αλγόριθμος αποκρυπτογράφησης πρέπει να αποφέρει το αρχικό μήνυμα M.

3.2.1 Επιθέσεις στους μηχανισμούς ενθυλάκωσης δεδομένων

Η κατασκευή ενός σχήματος υβριδικής κρυπτογραφίας, όπως αναφέρθηκε, εκτός από το μέρος του ασύμμετρου σχήματος KEM, βασίζεται και στην ύπαρξη τύπων συμμετρικής κρυπτογραφίας. Το μέρος αυτό των υβριδικών σχημάτων είναι το DEM και περιλαμβάνει συμμετρικά σχήματα ή/και σχήματα MAC. Πριν την ανασκόπηση ασφαλείας των μηχανισμών DEM πρέπει να ορίσουμε τις έννοιες ασφάλειας για τα σχήματα κρυπτογραφίας στα οποία βασίζονται.

Ένα συμμετρικό σχήμα κρυπτογραφίας αποτελείται από ένα ζεύγος αλγορίθμων (ENC, DEC). Ο αλγόριθμος κρυπτογράφησης ENC λαμβάνει ως είσοδο ένα μήνυμα m σε δυαδική μορφή, $m \in \{0,1\}$, οποιουδήποτε μεγέθους και ένα κλειδί K σταθερού μεγέθους και αποφέρει το κρυπτογράφημα $C = ENC(K, m)$. Ο αλγόριθμος αποκρυπτογράφησης DEC λαμβάνει ως είσοδο το κρυπτογράφημα C, το οποίο βρίσκεται επίσης σε δυαδική μορφή, $c \in \{0,1\}$, και το ίδιο κλειδί K και αποφέρει το αρχικό μήνυμα $m = DEC(K, C)$. Βασική απαίτηση για την λειτουργία ενός

συμμετρικού σχήματος κρυπτογραφίας είναι η ικανοποίηση της απαίτησης ορθότητας (soundness property), δηλαδή, για οποιοδήποτε κλειδί K κατάλληλου μεγέθους και οποιοδήποτε μήνυμα $m \in \{0,1\}$ πρέπει να ισχύει ότι ο αλγόριθμος αποκρυπτογράφησης ενός μηνύματος που κρυπτογραφήθηκε με το ίδιο κλειδί K πρέπει να αποφέρει το αρχικό μήνυμα m, $DEC(K, ENC(K, m)) = m$.

Όπως και στα ασύμμετρα σχήματα, τα συμμετρικά πρέπει να ικανοποιούν μια έννοια ασφάλειας. Για την ασφάλεια των σχημάτων αυτών, ορίζομε δύο έννοιες, τις IND-PA και IND-CCA, οι οποίες είναι παρόμοιες με την IND-CCA ασφάλεια που ορίστηκε κατά την περιγραφή των ασύμμετρων σχημάτων. Επομένως, τα μοντέλα επιθέσεων βασίζονται σε ένα παιχνίδι μεταξύ ενός διεκδικητή και ενός επιτιθέμενου, βάση μιας παραμέτρου ασφαλείας k. Το παιχνίδι IND-PA λειτουργεί ως εξής:

1. Ο διεκδικητής δημιουργεί τυχαία ένα συμμετρικό κλειδί K κατάλληλου μεγέθους.
2. Ο επιτιθέμενος αποφέρει ένα ζεύγος μηνυμάτων (m_0, m_1) ίδιου μεγέθους.
3. Ο διεκδικητής επιλέγει τυχαία ένα bit, $b \in \{0,1\}$ και δημιουργεί την πρόκληση $C' = ENC(K, m_b)$.
4. Ο επιτιθέμενος αποφέρει την εικασία b' για το b.

Ο επιτιθέμενος κερδίζει το παιχνίδι αν $b = b'$.

Το παιχνίδι IND-CCA είναι παρόμοιο με την διαφορά ότι ο επιτιθέμενος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης αφού έχει λάβει την πρόκληση κρυπτοκειμένου, χωρίς ωστόσο να μπορεί να αποστείλει ερωτήματα για το κρυπτοκείμενο C'. Με άλλα λόγια, στο βήμα 4, ο επιτιθέμενος έχει πρόσβαση σε ένα περιορισμένο αλγόριθμο αποκρυπτογράφησης, το οποίο βάση του κρυπτοκειμένου $C \neq C'$, θα αποφέρει $DEC(K, C)$. Από την άλλη, στο βήμα 2, ο επιτιθέμενος δεν έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης. Και στις παραπάνω δύο περιπτώσεις το πλεονέκτημα του επιτιθέμενου να κερδίζει το παιχνίδι ορίζεται από τον τύπο $|\mathrm{P}[b = b'] - \frac{1}{2}|$.

Ένα συμμετρικό σχήμα κρυπτογραφίας είναι IND-PA ασφαλές αν για όλους τους πολυωνιμικούς επιτιθέμενους A, το πλεονέκτημα νίκης του A στο παιχνίδι IND-PA είναι αμελητέο ως συνάρτηση της παραμέτρου ασφαλείας k. Παρομοίως, ένα συμμετρικό σχήμα είναι IND-CCA ασφαλές αν για όλους τους πολυωνιμικούς επιτιθέμενους A, το πλεονέκτημα νίκης του A στο παιχνίδι IND-CCA είναι αμελητέο ως συνάρτηση της παραμέτρου ασφαλείας k.

Όπως αναφέρθηκε ένα DEM μπορεί να απαιτεί την χρήση ενός σχήματος MAC. Ένα σχήμα MAC είναι ένας αλγόριθμος, ο οποίος λαμβάνει ως είσοδο ένα μήνυμα $m \in \{0,1\}$ οποιουδήποτε μεγέθους και ένα κλειδί K σταθερού μεγέθους και αποφέρει την ετικέτα MAC τ, η οποία είναι σταθερού μεγέθους. Όπως και στις προηγούμενες περιπτώσεις, βασική προϋπόθεση για την λειτουργία ενός αλγορίθμου MAC είναι ότι τόσο το μήκος του κλειδιού όσο και η ετικέτα εξαρτώνται από μια παράμετρο ασφαλείας k. Η ασφάλεια ενός αλγορίθμου MAC ορίζεται ως ένα παιχνίδι μεταξύ ενός διεκδικητή και ενός επιτιθέμενου ως εξής:

1. Ο διεκδικητής δημιουργεί τυχαία ένα κλειδί K κατάλληλου μεγέθους.
2. Ο επιτιθέμενος αποφέρει ένα μήνυμα m.
3. Ο διεκδικητής υπολογίζει την ετικέτα MAC για το m, $\tau = MAC(K, m)$.
4. Ο επιτιθέμενος αποφέρει οποιοδήποτε ζεύγος (m_i, τ_i).

Ο επιτιθέμενος νικά το παιχνίδι αν οποιαδήποτε έξοδος του (m_i, τ_i) ικανοποιεί την συνθήκη $\tau_i = MAC(K, m_i)$. Επομένως, ένα σχήμα MAC είναι ασφαλές αν για όλους τους πολυωνιμικούς επιτιθέμενους A, η πιθανότητα νίκης του A το παραπάνω παιχνίδι ασφαλείας είναι αμελητέο ως συνάρτηση της παραμέτρου ασφαλείας k.

Γενικότερα, η ασφάλεια ενός DEM είναι ίδια με αυτή ενός συμμετρικού σχήματος κρυπτογράφησης. Επομένως, τα DEMs πρέπει να είναι IND-PA και IND-CCA ασφαλή.

Σύμφωνα με το θεώρημα του Cramer και Shoup [26] Ένα σχήμα ασύμμετρης κρυπτογραφίας που δημιουργήθηκε από ένα IND-CCA KEM και ένα IND-CCA DEM είναι IND-CCA ασφαλές. Ωστόσο, υπάρχει ένα πρόβλημα στην κατασκευή ενός συμμετρικού αλγορίθμου που λαμβάνει αυθαίρετα μεγάλα μηνύματα και είναι IND-CCA ασφαλές. Εκ πρώτης όψεως, αν και ένα συμμετρικός αλγόριθμος μπορεί να είναι IND-CCA ασφαλές, στην πραγματικότητα, δεν μπορεί να διαχειριστεί μηνύματα μεγάλου μεγέθους. Ομοίως, αν ένας συμμετρικός αλγόριθμος μπορεί να διαχειριστεί μηνύματα μεγάλου μεγέθους, δεν θα είναι IND-CCA ασφαλής ακόμη και αν θεωρείται IND-CCA ασφαλής.

Οι Cramer και Shoup [26] όρισαν την κατασκευή ενός ασφαλούς IND-CCA DEM με την χρήση ενός IND-PA συμμετρικού σχήματος κρυπτογράφησης και έναν ασφαλή αλγόριθμο MAC. Στο σχήμα αυτό, η κρυπτογράφηση ενός μηνύματος m με ένα κλειδί K γίνεται ως εξής:

1. Το κλειδί K διαχωρίζεται σε δύο κλειδιά κατάλληλου μεγέθους $K = K_1||K_2$, όπου K_1 είναι το κλειδί για το συμμετρικό σχήμα και K_2 είναι το κλειδί για το σχήμα MAC.
2. Ορισμός του $C = E(K_1, m)$.
3. Ορισμός του $t = MAC(K_2, C)$.
4. Επιστροφή του κρυπτογραφήματος (C, t).

Η αποκρυπτογράφηση του (C, t) με βάση το κλειδί K γίνεται ως εξής:

1. Το κλειδί K διαχωρίζεται σε δύο κλειδιά κατάλληλου μεγέθους $K = K_1||K_2$, όπου K_1 είναι το κλειδί για το συμμετρικό σχήμα και K_2 είναι το κλειδί για το σχήμα MAC.
2. Έλεγχος ότι $t = MAC(K_2, C)$.
3. Ορισμός του $m = D(K_1, C)$.
4. Επιστροφή του αρχικού μηνύματος m.

Απαραίτητη προϋπόθεση για τα κλειδιά K_1 και K_2 είναι να έχουν προκαθορισμένο μέγεθος και να μην εξαρτώνται από το μήνυμα. Το σχήμα αυτό έχει αποδειχτεί ότι είναι IND-CCA ασφαλές, με την προϋπόθεση ότι το σύστημα κρυπτογράφησης είναι IND-PA ασφαλής και ο αλγόριθμος MAC είναι ασφαλής.

Η κατασκευή του παραπάνω σχήματος encrypt-then-MAC είναι IND-CCA ασφαλής διότι προσφέρει, εκτός από εμπιστευτικότητα, και υπηρεσίες ακεραιότητα/αυθεντικότητας [37]. Σύμφωνα με τον ορισμό ενός DEM, δεν απαιτείται από αυτό να παρέχει υπηρεσίες αυθεντικοποίησης. Ωστόσο, η παροχή αυτής της υπηρεσίας, σημαίνει ότι είναι αδύνατο για έναν επιτιθέμενο να δημιουργήσει ένα νέο έγκυρο κρυπτογράφημα χωρίς την αποστολή ερωτημάτων στο σύστημα κρυπτογράφησης. Έτσι, το σύστημα αποκρυπτογράφησης είναι άχρηστο για τον επιτιθέμενο, αφού ο μόνος τρόπος δημιουργίας ενός κρυπτογραφήματος που μπορεί να αποκρυπτογραφηθεί από τον επιτιθέμενο είναι να αποστείλει ερωτήματα στο σύστημα κρυπτογράφησης και στην περίπτωση αυτή ο επιτιθέμενος θα πρέπει να γνωρίζει την

αποκρυπτογράφηση του μηνύματός του. Έτσι, το σχήμα IND-CCA είναι ασφαλές, παρόλο που το σχήμα κρυπτογράφησης είναι μόνο IND-PA ασφαλές.

3.3 Μηχανισμοί KEM-DEM

Με την χρήση ενός συνδυασμού των KEM και DEM, λαμβάνεται ένα σχήμα υβριδικής κρυπτογράφησης. Έστω ότι $KEM = (Generate, Encapsulate, Decapsulate)$ και $DEM = (Encrypt, Decrypt)$. Για την συνένωση των δύο αυτών μηχανισμών απαραίτητη προϋπόθεση αποτελεί το κριτήριο συμβατότητας του κλειδιού που δημιουργείται από το KEM να μπορεί να χρησιμοποιηθεί από το DEM. Με άλλα λόγια το μέγεθος του κλειδιού $KEM.KeyLength = DEM.KeyLength$. Ένα σύστημα υβριδικής κρυπτογραφίας δημοσίου κλειδιού με βάση τα KEM και DEM ορίζεται ως εξής:

1. **Αλγόριθμος δημιουργίας κλειδιού**

   Ο αλγόριθμος δημιουργίας κλειδιού είναι ο ίδιος με αυτόν του KEM, $Generate_{KEM}(D)$. Το ζεύγος κλειδιών που δημιουργείται (PK, SK) από το $Generate_{KEM}(D)$ αναπαριστά το δημόσιο και ιδιωτικό κλειδί, αντίστοιχα.

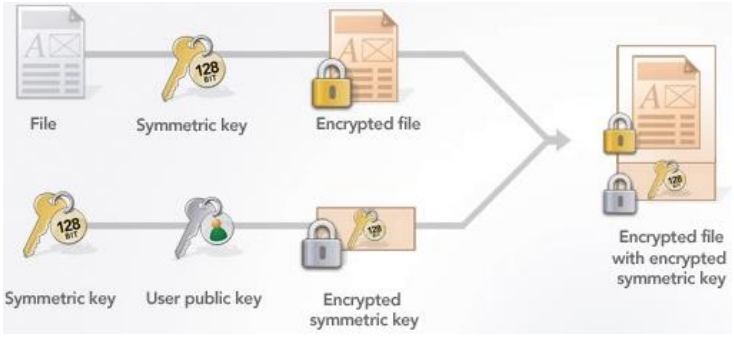
   Αλγόριθμος κρυπτογράφησης

2. Αρχικά, στο σχήμα της υβριδικής κρυπτογραφίας εκτελείται η ενθυλάκωση κλειδιού από το KEM, $Encapsulate_{KEM}(PK)$ για την δημιουργία του διαμοιρασμένου κλειδιού K και του κρυπτογραφήματος του, C_1. Έπειτα, γίνεται κρυπτογράφηση ενός μηνύματος M στο κρυπτοκείμενο C_2 με την χρήση του DEM, $Encpypt_{DEM}(K, M)$. Τέλος, αποφέρεται το τελικό κρυπτοκείμενο C, το οποίο αποτελείται από τα κρυπτογραφήματα C_1 και C_2.

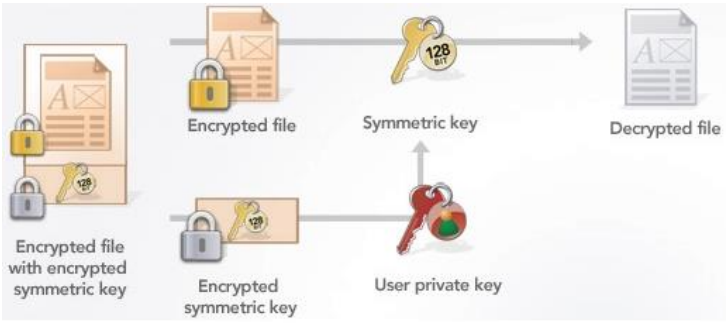
   Αλγόριθμος αποκρυπτογράφησης

3. Αρχικά, ο αλγόριθμος αποκρυπτογράφησης λαμβάνει το κρυπτοκείμενο $C = C_1||C_2$. Στην συνέχεια, αποκρυπτογραφεί το C_1 για να ληφθεί το διαμοιρασμένο κλειδί K με βάση το ιδιωτικό κλειδί SK, μέσω του KEM, $Decapsulate_{KEM}(SK, C_1)$. Τέλος, αποκρυπτογραφείται το C_2 για να ληφθεί το αρχικό μήνυμα Mμε την χρήση του DEM, $Decrypt_{DEM}(K, C_2)$.

Όπως αναφέρθηκε, η χρήση ενός σχήματος υβριδικής κρυπτογραφίας μπορεί να προσπελάσει τα αδύναμα σημεία της μεταφοράς κλειδιού (συμμετρική κρυπτογραφία) και της κρυπτογράφησης μηνυμάτων μεγάλου μεγέθους (ασύμμετρη κρυπτογραφία). Στην παρακάτω εικόνες φαίνεται πως ένα αρχείο μεγάλου μεγέθους μπορεί να κρυπτογραφηθεί και αποκρυπτογραφηθεί με την χρήση ενός σχήματος KEM/DEM.



Εικόνα 3.3: Το κλειδί κρυπτογράφησης που χρησιμοποιείται στο σχήμα, κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη (KEM). Έπειτα, το αρχείο κρυπτογραφείται συμμετρικά με το κλειδί που δημιουργήθηκε στην προηγούμενη διαδικασία.



Εικόνα 3.4: Όταν ο παραλήπτης λάβει το κρυπτογραφημένο αρχείο μέσω του σχήματος KEM-DEM, χρησιμοποιεί το ιδιωτικό του κλειδί για την ανάκτηση του συμμετρικού κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση του αρχείου. Αφού λάβει το κλειδί είναι σε θέση να αποκρυπτογραφήσει το αρχείο που του απεστάλη.

Όπως έχει αναφερθεί στην βιβλιογραφία, για την δημιουργία ενός CCA-ασφαλούς σχήματος υβριδικής κρυπτογραφίας, αρκεί τα υποσυστήματα KEM και DEM να είναι CCA-ασφαλή. Σε περίπτωση που ένα από τα δύο συστήματα δεν είναι CCA-ασφαλή, ένας επιτιθέμενος ο οποίος προσπαθεί να αποκρυπτογραφήσει ένα κρυπτοκείμενο-στόχο, θα μπορούσε να τροποποιήσει το αντίστοιχο τμήμα του κρυπτοκειμένου και να χρησιμοποιήσει το σύστημα αποκρυπτογράφησης για να λάβει πολύτιμες πληροφορίες. Βέβαια, υβριδικά σχήματα κρυπτογράφησης, τα οποία είναι CCA-ασφαλή, χωρίς το ένα από δύο υποσυστήματα να είναι CCA-ασφαλές έχουν προταθεί [38],[39]. Παρόλα αυτά, το προηγούμενο σχήμα είναι εν γένει CCA-ασφαλή, αλλά και πιο αποδοτικό από ότι αυτά που έχουν προταθεί ως πρότυπα ISO. Επομένως, το σχήμα Kurosawa-Desmedt παραθέτει ότι ναι μεν μπορούμε να αρκεστούμε στην CCA-ασφάλεια των υποσυστημάτων KEM-DEM για την δημιουργία ενός ασφαλούς σχήματος υβριδικής κρυπτογραφίας, ωστόσο η CCA-ασφάλεια δεν είναι απαραίτητη [47].

3.3.1 Το μοντέλο Tag-KEM

Το 2005, το υβριδικό μοντέλο υβριδικής κρυπτογράφησης για τα ασύμμετρα σχήματα γενικεύτηκε [47]. Το νέο μοντέλο ονομάστηκε tag-KEM και αποτελείται από μια τετράδα αλγορίθμων:

- Τον αλγόριθμο δημιουργίας κλειδιού, $Generate$, ο οποίος λαμβάνει ως είσοδο μια παράμετρο ασφαλείας k και αποφέρει το ζεύγος δημοσίου και ιδιωτικού κλειδιού (PK, SK).

- Τον αλγόριθμο δημιουργίας κλειδιού, Key, ο οποίος λαμβάνει ως είσοδο το δημόσιο κλειδί PK και αποφέρει το κλειδί K.
- Τον αλγόριθμο ενθυλάκωσης, $Encapsulate$, ο οποίος λαμβάνει ως είσοδο μια ετικέτα τ και αποφέρει το κρυπτογράφημα C.
- Τον αλγόριθμο απενθυλάκωσης, $Decapsulate$, ο οποίος λαμβάνει ως είσοδο το ιδιωτικό κλειδί SK, το κρυπτογράφημα C και την ετικέτα τ και αποφέρει το κλειδί K.

Προφανώς, από ένα τέτοιο σύστημα απαιτείται η ιδιότητα της ορθότητας. Δηλαδή, για όλα τα ζεύγη δημοσίου και ιδιωτικού κλειδιού (PK, SK), ισχύει ότι $K = Decapsulate(SK, C, \tau)$ για όλα τα κλειδιά K που δημιουργούνται από τον αλγόριθμο Key, $K = Key(PK)$ και για όλες τις ετικέτες τ που δημιουργούν το κρυπτογράφημα C βάση του αλγορίθμου $Encapsulate$, $C = Encapsulate(\tau)$.

Ένα ασύμμετρο σχήμα κρυπτογραφίας μπορεί να δημιουργηθεί με τον συνδυασμό του μηχανισμού tag-KEM και DEM. Για την κρυπτογράφηση ενός μηνύματος m με την χρήση ενός δημοσίου κλειδιού PK, ακολουθείται η εξής διαδικασία:

1. Ορισμός του $K = Key(PK)$.
2. Ορισμός του $C_2 = Encrypt(K, m)$.
3. Ορισμούς του $C_1 = Encapsulate(C_2)$.
4. Έξοδος του κρυπτογραφήματος $C = (C_1, C_2)$.

Αξίζει να σημειωθεί ότι η συμμετρική κρυπτογράφηση του κρυπτογραφήματος χρησιμοποιείται ως ετικέτα με την χρήση του μηχανισμού tag-KEM. Έτσι, ο ορισμός του tag-KEM είναι πιο γενικευμένος από την έννοια του KEM. Επιπλέον, οποιοδήποτε KEM μπορεί να εκφραστεί ως tag-KEM, εάν η ετικέτα είναι προκαθορισμένη. Στην πραγματικότητα, η ετικέτα φέρει την ταυτότητα του αποστολέα και πρέπει να προκαθοριστεί πριν επιλεχθεί ένα κλειδί για χρήση στο DEM.

Όσον αφορά την ασφάλεια του μηχανισμού, τα κριτήρια είναι αυστηρότερα από ότι ένα KEM. Έτσι, ένα ασφαλές KEM ίσως να μην είναι ασφαλές όταν χρησιμοποιείται στο σύστημα tag-KEM, ωστόσο, επιτρέπεται η χρήση ενός DEM, το οποίο είναι ασφαλές μόνο έναντι παθητικών επιθέσεων (IND-PA ασφαλές) [47].

4 *Ανάλυση Μηχανισμών Ενθυλάκωσης Κλειδιού*

Στο κεφάλαιο αυτό περιγράφεται η λειτουργία των δημοφιλέστερων μηχανισμών ενθυλάκωσης κλειδιού, οι οποίοι έχουν προταθεί από τον Shoup ως πρότυπα ISO. Ονομαστικά, οι μηχανισμοί αυτοί είναι οι RSA-KEM, ECIES-KEM, PSEC-KEM και ACE-KEM [33]. Σαφώς, κατά καιρούς έχουν προταθεί και άλλοι μηχανισμοί τύπου KEM, όπως ο μηχανισμός που προτάθηκε από τον Kiltz [40], ο μηχανισμός BEG-KEM [41], ο μηχανισμός Rabin-KEM [34] και ο μηχανισμός Kurosawa-Desmedt KEM [42]. Δημοφιλέστερος μεταξύ αυτών είναι ο μηχανισμός Kurosawa-Desmedt KEM οποίος αποδείχτηκε ότι δεν είναι IND-CCA ασφαλής [43], [44], κάτι που οδήγησε στην αναθεώρηση του [45]. Για άλλους μηχανισμούς τύπου KEM εκτός από αυτούς που έχουν προταθεί στο πρότυπο ISO που εξετάζουμε [33] δεν έχει γίνει εκτενής ανάλυση και έτσι δεν αναλύονται περεταίρω η λειτουργία τους.

4.1 Κρυπτογραφικά Εργαλεία Μηχανισμών Ενθυλάκωσης Κλειδιού

Πριν την ανάλυση του τρόπου λειτουργίας των κυριότερων μηχανισμών ενθυλάκωσης κλειδιού, είναι απαραίτητη η αναφορά στα κρυπτογραφικά εργαλεία που απαιτούνται για την κατασκευή τους.

Στα συστήματα τύπου KEM/DEM, τυπικά, χρησιμοποιείται μια συνάρτηση δημιουργίας κλειδιού (Key Derivation Function), KDF, η οποία μετατρέπει ένα κλειδί K που δημιουργήθηκε από ένα KEM σε μια κωδικοποίηση, η οποία αποτελεί το τελικό κλειδί που πρόκειται να χρησιμοποιηθεί από το DEM. Η KDF είναι συνήθως μια κρυπτογραφική συνάρτηση κατακερματισμού η οποία προέρχεται από ένα μυστικό κλειδί. Πριν τον ορισμό μιας συνάρτηση KDF ορίζεται οι κρυπτογραφική συνάρτηση κατακερματισμού (cryptographic hash function).

Ορισμός 6.1.1 Μια κρυπτογραφική συνάρτηση κατακερματισμού είναι μια συνάρτηση που μετατρέπει ένα αλφαριθμητικό x οποιουδήποτε μεγέθους σε ένα αλφαριθμητικό σταθερού μεγέθους, $h = hash(x)$.

Όσον αφορά τις συναρτήσεις κατακερματισμού αυτές περιλαμβάνουν τις εξής παραμέτρους:

1. Μήκος κατακερματισμού (HashLen): ένας ακέραιος αριθμός ο οποίος δηλώνει το μέγεθος εξόδου της συνάρτησης κατακερματισμού.
2. Μέγιστο μέγεθος εισόδου κατακερματισμού (HashMaxInputLen): ένας ακέραιος αριθμός ο οποίος δηλώνει το μέγιστο επιτρεπόμενο μήκος του αλφαριθμητικού x στην συνάρτηση κατακερματισμού.

Ουσιαστικά, μια συνάρτηση κατακερματισμού μετατρέπει ένα αλφαριθμητικό x μέγιστου μεγέθους HashMaxInputLen σε ένα αλφαριθμητικό μήκους HashLen. Η συνάρτηση αποτυγχάνει μόνο εάν το μήκος εισόδου είναι μεγαλύτερο από το HashMaxInputLen.

Μια κρυπτογραφική συνάρτηση κατακερματισμού υποθέτουμε ότι ικανοποιεί τις βασικές απαιτήσεις ασφαλείας [46]:

- Είναι ανθεκτική σε συγκρούσεις (collision resistant). Δηλαδή είναι δύσκολο να βρεθούν δύο είσοδοι x, y με $x \neq y$ τέτοιοι ώστε $Hash(x) = Hash(y)$.
- Είναι ανθεκτική σε προ-εικόνα (preimage resistant). Δηλαδή, δοθέντος όλων τον εξόδων, είναι δύσκολο να βρεθεί οποιαδήποτε είσοδος της οποίας η έξοδος είναι κάποια από τις προκαθορισμένες εισόδους. Με άλλα λόγια, δοθέντος οποιασδήποτε εξόδου h της οποία η είσοδος x δεν είναι γνωστή, είναι αδύνατο να βρεθεί y τέτοιο ώστε $hash(y) = h$.
- Είναι ανθεκτική σε δεύτερη προ-εικόνα (second-preimage resistant). Δηλαδή, είναι δύσκολο να βρεθεί να βρεθεί οποιαδήποτε είσοδος διαφορετική της πρώτης η οποία είναι γνωστή, τέτοια ώστε οι έξοδοι των συναρτήσεων κατακερματισμού και των δύο εισόδων να είναι ίδιοι. Με άλλα λόγια, δοθέντος μιας εισόδου x, είναι αδύνατο να βρεθεί μια είσοδος y, με $x \neq y$, τέτοια ώστε $Hash(x) = Hash(y)$.

Όσον αφορά ποιες συναρτήσεις κατακερματισμού πρέπει να χρησιμοποιούνται αυτές που προτείνονται μπορούν να βρεθούν στην πρότυπη έκδοση του επίσημου οργανισμού NIST 180-4 [47]. Εφόσον έχει οριστεί η κρυπτογραφική συνάρτηση κατακερματισμού και οι βασικές απαιτήσεις της μπορούμε να προχωρήσουμε στον ορισμό μιας KDF.

Ορισμός 6.1.2 Μια KDF είναι μια συνάρτηση που λαμβάνει ως είσοδο ένα αλφαριθμητικό x και έναν ακέραιο αριθμό $l \geq 0$ και αποφέρει ένα αλφαριθμητικό μεγέθους $l, KDF(x, l)$.

Μια KDF μοντελοποιείται ως τυχαία συνάρτηση και ικανοποιεί την ιδιότητα εξομάλυνσης εντροπίας (entropy smoothing property), δηλαδή, για ένα x επιλεγμένο τυχαία, η έξοδος της KDF πρέπει να είναι υπολογιστικά αδιάκριτη από το τυχαίο αλφαριθμητικό μεγέθους l. Επομένως, οι συναρτήσεις κατακερματισμού με αυθαίρετο μέγεθος εξόδου, φαίνεται να ταιριάζουν στις απαιτήσεις μιας KDF.

Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι όλοι οι μηχανισμοί KEM σύμφωνα με το πρότυπο ISO χρησιμοποιούν μια KDF. Επιπλέον, όλοι οι μηχανισμοί αυτοί, εκτός από τον RSA-KEM είναι βασισμένοι στον αλγόριθμο ElGamal. Όπως αναφέρθηκε στον ενότητα 3.3.2 ο αλγόριθμος χρησιμοποιεί μια κυκλική ομάδα και επομένως βασίζεται σε μια πεπερασμένη ομάδα. Επιπλέον, ο αλγόριθμος αυτός μπορεί εύκολα να υλοποιηθεί σε ελλειπτικές καμπύλες. Σύμφωνα με το πρότυπο ISO [33] για την περιγραφή των μηχανισμών ενθυλάκωσης βασισμένων στο κρυπτοσύστημα ElGamal ορίζεται μια αφηρημένη ομάδα (abstract group) Γ για λόγους απλότητας της περιγραφής των μηχανισμών που την χρησιμοποιούν. Στην ομάδα αυτή ορίζεται η πράξη της πρόσθεσης, ενώ το 0 αποτελεί το ταυτοτικό στοιχείο.

Ορισμός 6.1.3 Η αφηρημένη ομάδα Γ είναι μια πλειάδα αλγορίθμων $(H, G, g, \mu, \nu, E, D, E', D')$ όπου,

- H είναι μια πεπερασμένη αβελιανή ομάδα στην οποία πραγματοποιούνται όλοι οι υπολογισμοί της ομάδας.
- G είναι μια κυκλική υπό-ομάδα της ομάδας H.
- g είναι ένας γεννήτορας για της κυκλικής ομάδας G.
- μ είναι ένας πρώτος αριθμός, ο οποίος συμβολίζει την τάξη (το μέγεθος) της G.

- ν είναι μια μεταβλητή της G, όπου $\nu = |H|/\mu$.
- $E(a, format)$ είναι μια συνάρτηση κωδικοποίησης, η οποία κωδικοποιεί ένα στοιχείο $a \in H$ σε ένα αλφαριθμητικό. Η μεταβλητή $format$ είναι ένα προσδιοριστικό μορφής (format specifier) για την κωδικοποίηση ενός στοιχείου, ενώ οι επιτρεπτές τιμές για την μεταβλητή αυτή εξαρτώνται από την ομάδα. Για την συνάρτηση E, ισχύουν οι παρακάτω απαιτήσεις:
    - Το ταυτοτικό στοιχείο 0 έχει μοναδική κωδικοποίηση. Δηλαδή, για όλους τους προσδιοριστές μορφής $format, format'$, ισχύει ότι $E(0, format) = E(0, format')$.
    - Για οποιοδήποτε άλλο στοιχείο εκτός του ταυτοτικού, η συνάρτηση κωδικοποίησης είναι ένα-προς-ένα. Δηλαδή, για κάθε $a, a' \in H$ και για όλους του προσδιοριστές μορφής $format, format'$, αν $(a, format) \neq (a', format')$ και $\alpha \neq 0$ ή $\alpha' \neq 0$, τότε $E(a, format) \neq E(a', format')$.
- $D(x)$ είναι μια συνάρτηση η οποία επιστρέφει το στοιχείο $a \in H$ τέτοιο ώστε $E(a, format) = x$. Σε περίπτωση που το στοιχείο $x = E(a, format)$ δεν αποτελεί έγκυρη κωδικοποίηση στο H, επιστρέφεται μήνυμα σφάλματος. Σημειώνεται ότι έγκυρη κωδικοποίηση ενός στοιχείου $\alpha \in H$ θεωρείται το αλφαριθμητικό x για το οποίο ισχύει ότι $x = E(a, format)$.
- $E'(a)$ είναι μια συνάρτηση μερικής κωδικοποίησης, η οποία κωδικοποιεί ένα στοιχείο $a \in H$ σε ένα αλφαριθμητικό.
- $D'(x)$ είναι μια συνάρτηση η οποία επιστρέφει το στοιχείο $a \in H$ τέτοιο ώστε $E'(a) = x$. Σε περίπτωση που το στοιχείο $x = E(a)$ δεν αποτελεί έγκυρη μερική κωδικοποίηση στο H, επιστρέφεται μήνυμα σφάλματος. Σημειώνεται ότι έγκυρη μερική κωδικοποίηση ενός στοιχείου $\alpha \in H$ θεωρείται το αλφαριθμητικό x για το οποίο ισχύει ότι $x = E'(a)$. Επιπλέον, αξίζει να σημειωθεί ότι η συγκεκριμένη συνάρτηση δεν υλοποιείται από τα σχήματα που περιγράφονται στη συνέχεια. Ωστόσο, ο ορισμός της συνάρτησης αυτής είναι απαραίτητος για την απόδειξη ασφάλειας τους.

Ο ορισμός της παραπάνω αφηρημένης ομάδας καλύπτει την μοντελοποίηση δύο υπο-ομάδων, αυτών των πεπερασμένων ομάδων Z_p^* και των ελλειπτικών καμπυλών.

Ο ορισμός μιας πεπερασμένης ομάδας και εν γένει μιας ομάδας έχει δοθεί στην ενότητα 2.3 (ορισμός 2.3.8). Ειδικά η ομάδα Z_p^*, ορίζεται ως εξής:

Ορισμός 6.1.4 Έστω ότι p είναι ένας πρώτος αριθμός και η πολλαπλιαστική ομάδα των στοιχείων $modulo\ p$ συμβολίζεται με Z_p^*.

Για την προσαρμογή του ορισμού στην αφηρημένη ομάδα Γ, θεωρούμε H την αναπαράσταση της ομάδας Z_p^*. Επιπλέον, θεωρούμε ότι G αναπαριστά οποιαδήποτε υπο-ομάδα πρώτης τάξης της ομάδας H και g είναι ένας γεννήτορας για το G. Έτσι, $\mu = |G|$ και $\nu = (p-1)/\mu$.

Η ομάδα H είναι κυκλική και επομένως η κυκλική υπο-ομάδα G περιλαμβάνει όλα τα στοιχεία της ομάδας H της οποίας η τάξη διαιρεί την τάξη της ομάδας G (μ). Επομένως μπορούν να οριστούν οι συναρτήσεις E, D, E', D'. Στην πράξη, όλα τα στοιχεία της ομάδας κωδικοποιούνται σε

αλφαριθμητικά μεγέθους $log_{256}p$, ενώ επιτρέπεται μόνος ένα προσδιοριστικό μορφής. Άρα, οι συναρτήσεις E', D' υλοποιούνται με τον ίδιο τρόπο όπως και οι συναρτήσεις E, D, αντίστοιχα.

Όσον αφορά τις ελλειπτικές καμπύλες που ορίζονται σε ένα πεπερασμένο σώμα F_q, οι οποίες ζητήθηκαν στην ενότητα 4, θεωρούμε ότι H την αναπαράσταση της ομάδας, η οποία μπορεί να μην είναι κυκλική. Επιπλέον, θεωρούμε ότι G αναπαριστά μια υπο-ομάδα πρώτη τάξης της ομάδας H και g είναι ένας γεννήτορας για το G. Αντίστοιχα, θεωρούμε ότι μ είναι η τάξη της G και ν είναι ο λογάριθμος της στο H, $\nu = log_{\mu}H$.

Στην περίπτωση των ελλειπτικών καμπυλών, η ομάδα H δεν είναι απαραίτητα κυκλική. Έτσι, η κωδικοποίηση ενός σημείου μπορεί να έχει μέγεθος 1 ή $1 + log_{256}|F|$ ή $2 + log_{256}|F|$. Άρα για τις συναρτήσεις E, D υπάρχει η δυνατότητα επιλογής μεταξύ τριών προσδιοριστικών μορφής. Σημειώνεται ότι η υλοποίηση τους μπορεί να πραγματοποιηθεί με τρόπο τέτοιο ώστε να επιτρέπονται πολλαπλοί προσδιοριστές μορφής, το οποίο, ωστόσο, δεν είναι απαραίτητο. Όσον αφορά την συνάρτηση μερικής κωδικοποίησης E', αυτή αποφέρει ένα κωδικοποιημένο αλφαριθμητικό σταθερού μεγέθους της x-συντεταγμένης του σημείου, με την προϋπόθεση ότι το σημείο αυτό δεν είναι το ταυτοτικό. Εννοιολογικά, βάση ενός σημείου $P \in E$, με $P(x, y) \neq 0$, όπου $(x, y) \in H$, επιστρέφεται ένα κωδικοποιημένο αλφαριθμητικό. Σε διαφορετική περίπτωση, επιστρέφεται ένα προκαθορισμένο αλφαριθμητικό ίδιου μεγέθους. Αντίστοιχα, η συνάρτηση D' μετατρέπει το κωδικοποιημένο αλφαριθμητικό στο στοιχείο της ομάδας H. Όπως αναφέρθηκε, η συνάρτηση E' κωδικοποιεί την x-συντεταγμένη. Άρα, η D' για να επιστρέψει το αρχικό σημείο πρέπει να λύσει την κυβική εξίσωση της καμπύλης για να βρεθούν οι πιθανές y-συντεταγμένες, οι οποίες μπορεί να είναι το μέγιστο δύο.

4.1.1 Παραδοχές ασφαλείας

Πριν την περιγραφή των μηχανισμών ενθυλάκωσης κλειδιού, πρέπει να γίνει προσαρμογή των δύσκολων μαθηματικών προβλημάτων για να ταιριάζουν με την ομάδα Γ που ορίστηκε προηγουμένως, έτσι ώστε να μπορεί να αξιολογηθεί η ασφάλεια τους. Όπως αναφέρθηκε η ομάδα Γ χρησιμοποιείται από όλα τα σχήματα KEM που ορίζονται στο πρότυπο ISO, εκτός από το RSA-KEM. Μιας και όλα τα υπόλοιπα βασίζονται στο κρυπτοσύστημα ElGamal, μας αρκεί ο προσδιορισμός των προβλημάτων που βασίζονται στο πρόβλημα Diffie-Hellman. Εν γένει, το πρόβλημα Diffie-Hellman προέρχεται από την δυσκολία υπολογισμού του διακριτού λογαρίθμου σε κυκλικές ομάδες [7].

Αρχικά, θα ορίσουμε το υπολογιστικό πρόβλημα Diffie-Hellman (CDH), στο οποίο έγινε αναφορά στην ενότητα 3.3.2.

Ορισμός 6.1.1.1 Δοθείσης μιας κυκλικής ομάδας G τάξης q, ενός γεννήτορα $g \in G$ και των υπολογισμών g^a, g^b, με τα στοιχεία $a, b \in \{0, \dots, q-1\}$ τυχαία επιλεγμένα, είναι υπολογιστικά αδύνατος ο υπολογισμός g^{ab}.

Το πρόβλημα CDH ειδικά για την ομάδα $\Gamma = (H, G, g, \mu, \nu, E, D, E', D')$, μπορεί εύκολα να οριστεί ως εξής: Δοθείσης της κυκλικής υπο-ομάδας ομάδας $G \in H$ τάξης μ, ενός γεννήτορα $g \in G$ και των υπολογισμών g^a, g^b, με $a, b \in \{0, \dots, \mu-1\}$ τυχαία επιλεγμένα, είναι υπολογιστικά αδύνατος ο υπολογισμός g^{ab}.

Από τον παραπάνω ορισμό είναι προφανές ότι το πρόβλημα CDH είναι άμεσα συνδεδεμένο με το πρόβλημα διακριτού λογαρίθμου. Για τον υπολογισμό του g^{ab} πρέπει αρχικά να υπολογιστεί το στοιχείο a, το οποίο υπολογίζεται λαμβάνοντας τον διακριτό λογάριθμο του g^a με βάση το g. Εάν υπολογιστεί το στοιχείο a τότε λόγω των ιδιοτήτων των δυνάμεων μπορεί να υπολογιστεί και το g^{ab}.

Στην πράξη, δεν μπορεί να υπολογιστεί μια σωστή λύση για το CDH πρόβλημα. Οι αλγόριθμοι οι οποίοι μπορούν να επιλύσουν το πρόβλημα, ουσιαστικά, δημιουργούν μια λίστα αποτελεσμάτων για ένα πρόβλημα CDH. Επομένως, οποιοσδήποτε αλγόριθμος A, ο οποίος επιλύει το CDH, επιστρέφει μια λίστα πιθανών λύσεων μέγιστου μεγέθους l. Η πιθανότητα εύρεσης της σωστής λύσης στην λίστα αποτελεσμάτων θεωρείται αμελητέα, κάτι το οποίο και αποτελεί την βάση για το πρόβλημα απόφασης Diffie-Hellman (DDH).

Ορισμός 6.1.1.2 Δοθείσης μιας κυκλικής ομάδας G τάξης q, ενός γεννήτορα $g \in G$ και των υπολογισμών g^a, g^b, με τα στοιχεία $a, b \in \{0, \dots, q-1\}$ τυχαία επιλεγμένα, το g^{ab} φαίνεται ως ένα τυχαίο στοιχείο της ομάδας G. Δηλαδή, δοθέντων των στοιχείων (g^a, g^b, g^{ab}) με $a, b \in \{0, \dots, q-1\}$ τυχαία επιλεγμένα και των στοιχείων $(g^a, g^b g^c)$ με $a, b, c \in \{0, \dots, q-1\}$ τυχαία επιλεγμένα είναι δύσκολο να διαπιστωθεί εάν ο υπολογισμός g^{ab} αφορά ένα τυχαία επιλεγμένο στοιχείο.

Αντίστοιχα, το πρόβλημα DDH για την ομάδα $\Gamma = (H, G, g, \mu, \nu, E, D, E', D')$ ορίζεται ως εξής: Δοθείσης της κυκλικής υπο-ομάδας ομάδας $G \in H$ τάξης μ, ενός γεννήτορα $g \in G$ και των υπολογισμών g^a, g^b, με τα στοιχεία $a, b \in \{0, \dots, \mu-1\}$ τυχαία επιλεγμένα, το g^{ab} φαίνεται ως ένα τυχαίο στοιχείο της ομάδας G.

Το πρόβλημα CDH ειδικά για την ομάδα $\Gamma = (H, G, g, \mu, \nu, E, D, E', D')$, μπορεί εύκολα να οριστεί ως εξής: Δοθείσης της κυκλικής υπο-ομάδας $G \in H$ τάξης μ, ενός γεννήτορα $g \in G$ και των υπολογισμών g^a, g^b, με $a, b \in \{0, \dots, \mu-1\}$ τυχαία επιλεγμένα, είναι υπολογιστικά αδύνατος ο υπολογισμός g^{ab}. Δηλαδή, δοθέντων των στοιχείων (g^a, g^b, g^{ab}) με $a, b \in \{0, \dots, \mu-1\}$ τυχαία επιλεγμένα και των στοιχείων $(g^a, g^b g^c)$ με $a, b, c \in \{0, \dots, \mu-1\}$ τυχαία επιλεγμένα είναι δύσκολο να διαπιστωθεί εάν ο υπολογισμός g^{ab} αφορά ένα τυχαία επιλεγμένο στοιχείο.

Τέλος, ειδικά για τις ομάδες των ελλειπτικών καμπυλών, οι δημιουργοί του σχήματος PSEC, το οποίο συζητείται παρακάτω, πρότειναν ένα νέο δύσκολο πρόβλημα, το κενό υπολογιστικό (gap-Computational) Diffie-Hellman (gap-CDH) [49]. Σύμφωνα με τους δημιουργούς, είναι δύσκολο να λυθεί το CDH πρόβλημα ακόμη και υπάρχει κάποιος αλγόριθμος ο οποίος επιλύει το DDH πρόβλημα.

Στο σημείο αυτό είμαστε σε θέση να προχωρήσουμε στην περιγραφή των σχημάτων KEM που έχουν προτυποποιηθεί, παρέχοντας παράλληλα αποδείξεις για την ασφάλεια τους.

4.2 RSA-KEM

Από την ονομασία του συγκεκριμένου μηχανισμού γίνεται εύκολο αντιληπτό ότι χρησιμοποιείται το δημόσιο RSA κλειδί του παραλήπτη για την ασφαλή μεταφορά ενός κλειδιού. Στην άλλη πλευρά, ο παραλήπτης εξάγει το κλειδί που δημιουργήθηκε από το KEM με την χρήση του ιδιωτικού του κλειδιού [50]. Όπως αναφέρθηκε στην ενότητα 3.3.1 η γενικότερη λειτουργία του RSA αλγορίθμου έχει ως εξής:

1. Αναπαράσταση ενός μηνύματος με έναν ακέραιο αριθμό m.

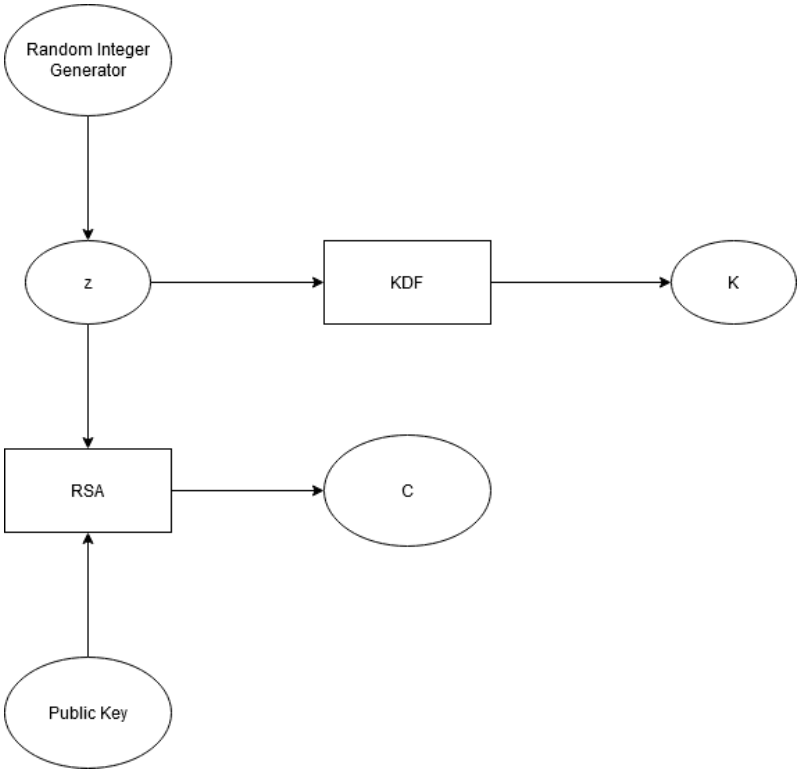
2. Κρυπτογράφηση του ακεραίου αριθμού m με το δημόσιο κλειδί του παραλήπτη, $c = m^e mod n$.
3. Το c αποτελεί το κρυπτογράφημα του μηνύματος m.

Ο μηχανισμός RSA-KEM ακολουθεί μια παρόμοια διαδικασία, με την διαφορά ότι χρησιμοποιείται ένα τυχαίος αριθμός z, αντί του μηνύματος m. Σύμφωνα με τον Shoup [33] ο μηχανισμός RSA-KEM αποτελείται από τις εξής τρείς παραμέτρους:

1. **Αλγόριθμος Δημιουργίας κλειδιού RSA (RSAKeyGen)**: όπως αναφέρθηκε στην ενότητα 3.3.1, ο συγκεκριμένος αλγόριθμος αποφέρει μια τριπλέτα (e, n, d), όπου το ζεύγος (e, n) αποτελεί το δημόσιο κλειδί ενός χρήστη, ενώ η τιμή d, αποτελεί το αντίστοιχο ιδιωτικό κλειδί. Στην πράξη, ο ακέραιος αριθμός n είναι το αποτέλεσμα του πολλαπλασιασμού δύο μεγάλων πρώτων αριθμών p και q. Ο ακέραιος αριθμός e υπολογίζεται με τέτοιο τρόπο ώστε $MK\Delta(e, (p-1)(q-1)) = 1$ και ο αριθμός d είναι ο ακέραιος αριθμός τέτοιος ώστε $e * d \equiv 1(mod((p-1)(q-1))$.
2. **Συνάρτηση Δημιουργίας κλειδιού (KDF)**: μια συνάρτηση κατακερματισμού όπως ορίστηκε στην αρχή αυτού του κεφαλαίου.
3. **Μήκος Κλειδιού (KeyLen)**: ένας θετικός ακέραιος αριθμός.

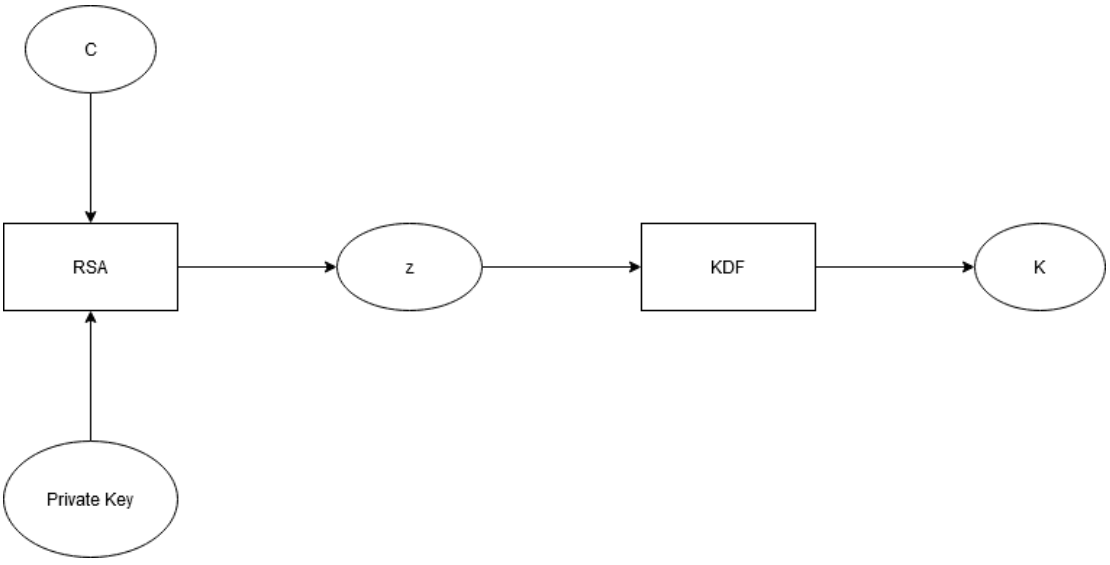
Όπως είναι γνωστό, ένας μηχανισμός KEM αποτελείται από τρεις αλγορίθμους: $Generate_{KEM}()$,$Encapsulate_{KEM}(PK)$, $Decapsulate_{KEM}(SK, C)$. Έτσι, η λειτουργία του RSA-KEM έχει ως εξής:

1. Ο αλγόριθμος $Generate_{RSA-KEM}()$ αποφέρει την τριπλέτα (e, n, d) βάση του αλγορίθμου δημιουργίας κλειδιού RSA (RSAKeyGen), όπου το ζεύγος (e, n) αποτελεί το δημόσιο κλειδί ενός χρήστη, ενώ το ζεύγος (n, d) το αντίστοιχο ιδιωτικό.
2. Ο αλγόριθμος $Encapsulate_{RSA-KEM}(PK)$ λαμβάνει ως είσοδο το δημόσιο κλειδί του παραλήπτη $PK = (e, n)$ και λειτουργεί ως εξής:
    a. Επιλέγεται ένας τυχαίος αριθμός $z \in [0 \dots n)$.
    b. Ο ακέραιος αριθμός z κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη (n, e), $C = z^e mod n$.
    c. Υπολογίζεται το κλειδί κρυπτογράφησης K βάση της συνάρτησης KDF, λαμβάνοντας ως είσοδο τον ακέραιο αριθμό z και το μήκος κλειδιού που οι δύο χρήστες θέλουν να δημιουργήσουν, $K = KDF(z, KeyLen)$.
    d. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το κρυπτογράφημα C και το μυστικό κλειδί K.



Εικόνα 4.1: Λειτουργία Ενθυλάκωσης Κλειδιού στον μηχανισμό RSA-KEM σύμφωνα με το πρότυπο ISO [].

3. Ο αλγόριθμος $Decapsulate_{RSA-KEM}(SK, C)$ λαμβάνει ως είσοδο το ιδιωτικό κλειδί του παραλήπτη, $SK = (n, d)$ και το κρυπτογράφημα C και λειτουργεί ως εξής:
    a. Πραγματοποιείται αποκρυπτογράφηση του C με το ιδιωτικό κλειδί του παραλήπτη (n, d), $z = C^d mod n$.
    b. Υπολογίζεται το κλειδί κρυπτογράφησης βάση της συνάρτησης KDF, λαμβάνοντας ως είσοδο τον ακέραιο αριθμό z και το μήκος κλειδιού, $K = KDF(z, KeyLen)$.
    c. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το μυστικό κλειδί K.

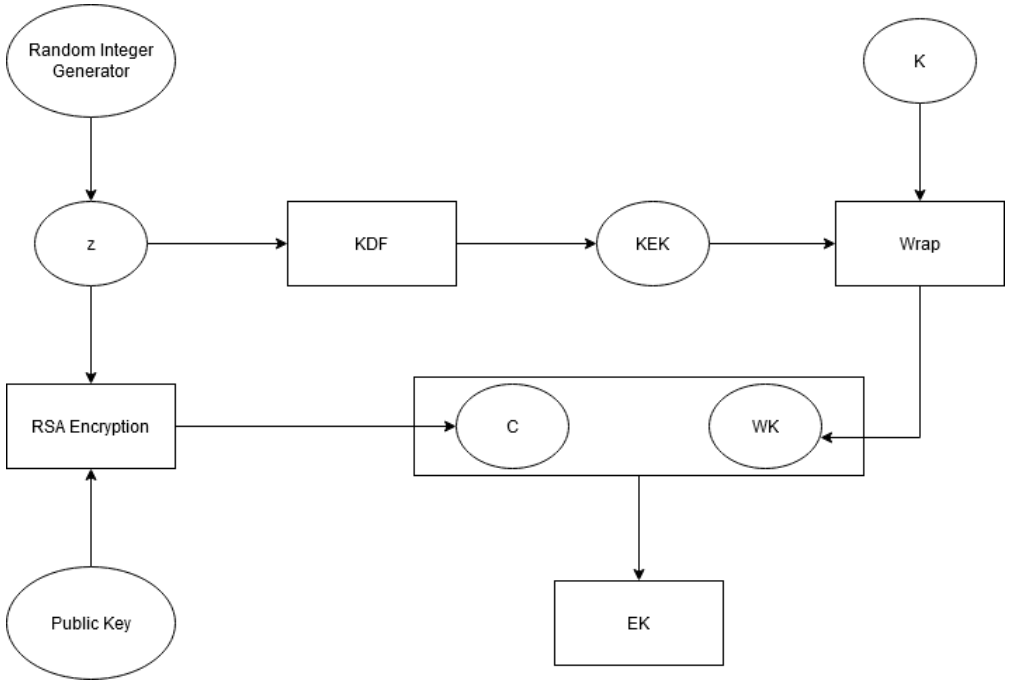


Εικόνα 4.2: Λειτουργία Απενθυλάκωσης Κλειδιού στον μηχανισμό RSA-KEM σύμφωνα με το πρότυπο ISO [].

Η παραπάνω λειτουργία του RSA-KEM παρουσιάστηκε βάση του προτύπου ISO που έχει προταθεί από τον Shoup [33]. Σύμφωνα με τον επίσημο οργανισμό IETF για την ασφαλή ανταλλαγή μηνυμάτων χρησιμοποιείται μια παραλλαγή της παραπάνω διαδικασίας [50]. Σύμφωνα με το πρότυπο αυτό, χρησιμοποιείται ένα επιπλέον σχήμα συμμετρικής κρυπτογράφησης για την κρυπτογράφηση του κλειδιού. Επομένως ο μηχανισμός RSA-KEM, εκτός της συνάρτησης KDF, περιλαμβάνει και έναν αλγόριθμο επικάλυψης κλειδιού (Wrap). Ο συγκεκριμένος αλγόριθμος κρυπτογραφεί το μυστικό κλειδί που έχει υπολογιστεί με την χρήση ενός συμμετρικού σχήματος κρυπτογράφησης.

Υποθέτοντας ότι το ζεύγος (n, e) αποτελεί το δημόσιο κλειδί του παραλήπτη που δημιουργήθηκε από την τυπική διαδικασία δημιουργίας κλειδιού RSA και K το κλειδί που πρόκειται να μεταφερθεί, η διαδικασία που πραγματοποιείται στην πλευρά του αποστολέα είναι η εξής:

1. Επιλέγεται ένας τυχαίος αριθμός $z \in [0 \dots n)$.
2. Πραγματοποιείται κρυπτογράφηση του ακεραίου αριθμού z με το δημόσιο κλειδί του παραλήπτη (n, e), $C = z^e mod n$.
3. Γίνεται απόκτηση του κλειδιού κρυπτογράφησης KEK βάση του ακεραίου z από τον αλγόριθμο KDF, $KEK = KDF(z, KekLen)$. Σημειώνεται ότι το κλειδί που πρόκειται να συμφωνηθεί είναι ήδη δημιουργημένο. Έτσι, το μήκος κλειδιού που εισάγεται στην συνάρτηση KDF είναι το μήκος του κλειδιού KEK, $KekLen$.
4. Το κλειδί K με την χρήση του αλγορίθμου Wrap κρυπτογραφείται με το κλειδί κρυπτογράφησης KEK για την απόκτηση του επικαλυμμένου κλειδιού WK, $WK = Wrap(KEK, K)$.
5. Πραγματοποιείται συγχώνευση του κρυπτογραφήματος C και του επικαλυμμένου κλειδιού WK για την απόκτηση του κλειδιού EK, $EK = C||WK$.
6. Το EK αποτελεί την τελική έξοδο που περιλαμβάνει το κρυπτογραφημένο κλειδί.

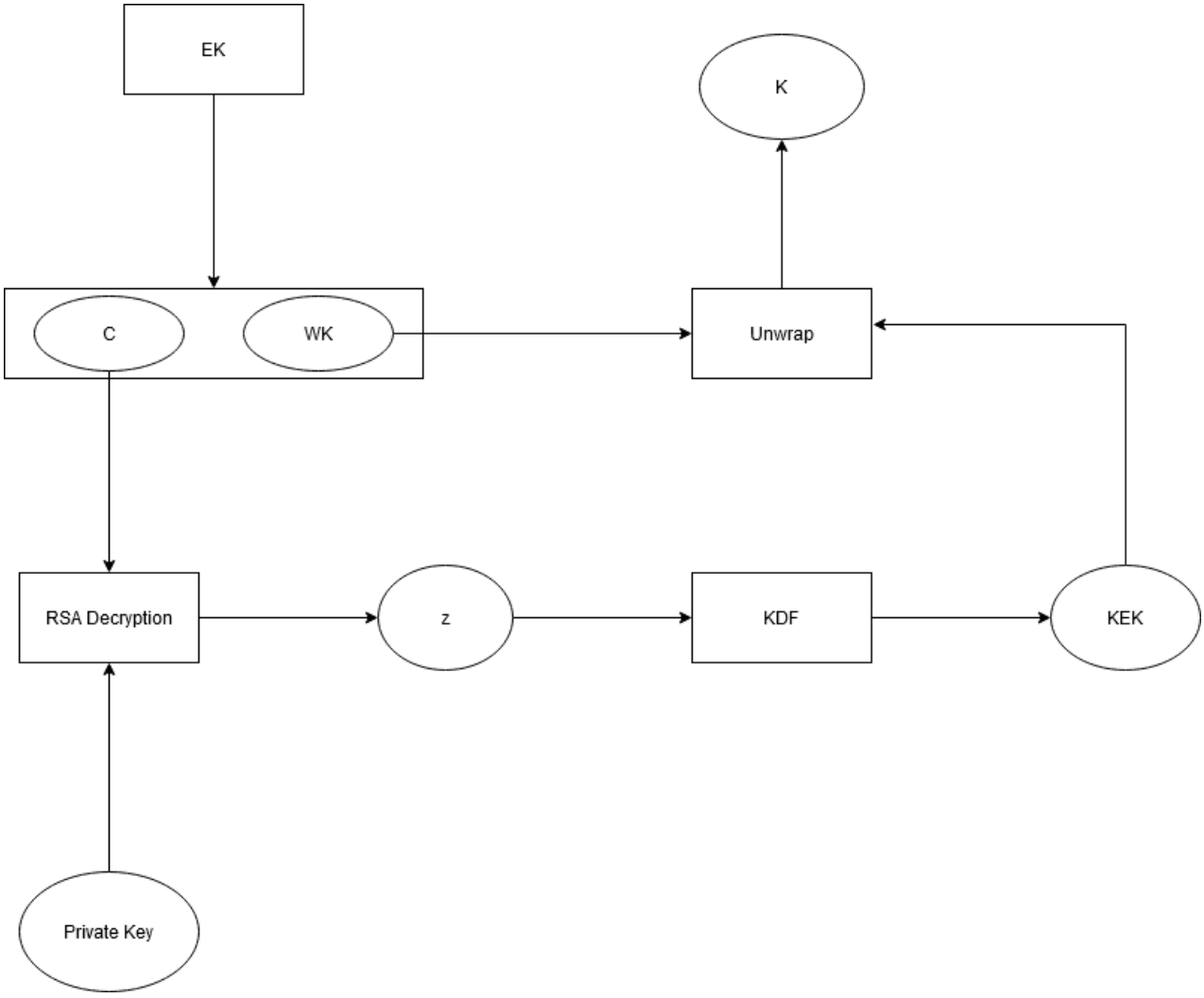


Εικόνα 4.3: Λειτουργία Ενθυλάκωσης Κλειδιού στον μηχανισμό RSA-KEM σύμφωνα με το πρότυπο IETF[] .

Στην άλλη πλευρά, η διαδικασία που πραγματοποιείται στην πλευρά του παραλήπτη είναι η εξής:

Έστω ότι (n, d) είναι το ιδιωτικό κλειδί του παραλήπτη και EK το κρυπτογραφημένο κλειδί που έχει ληφθεί από τον αποστολέα.

1. Διαχώριση του κρυπτογραφήματος EK στο κρυπτοκείμενο C και το επικαλυμμένο κλειδί $WK, C||WK = EK$.
2. Το κρυπτογράφημα C αποκρυπτογραφείται με το ιδιωτικό κλειδί (n, d) ώστε να ανακτηθεί ο ακέραιος αριθμός $z, z = C^d mod n$.
3. Απόκτηση του κλειδιού κρυπτογράφησης KEK από το z με την χρήση του KDF αλγορίθμου, $KEK = KDF(z, KekLen)$.
4. Εκτύλιξη του επικαλυμμένου κλειδιού WK με το κλειδί κρυπτογράφησης KEK με την χρήση του αλγορίθμου Wrap για την ανάκτηση του κλειδιού $K, K = Unwrap(KEK, WK)$.
5. Το K αποτελεί την τελική έξοδο, δηλαδή το κλειδί κρυπτογράφησης που δημιουργήθηκε στην πλευρά του αποστολέα.



Εικόνα 4.4: Λειτουργία Απενθυλάκωσης Κλειδιού στον μηχανισμό RSA-KEM σύμφωνα με το πρότυπο IETF [].

4.2.1 Ασφάλεια RSA-KEM

Γενικότερα, η ασφάλεια της συγκεκριμένης τεχνικής βασίζεται τόσο στην δυσκολία επίλυσης του προβλήματος RSA (πρόβλημα παραγοντοποίησης) όσο και στην δυσκολία αντιστροφής του κλειδιού εφόσον αυτό έχει τροποποιηθεί μέσω της συνάρτησης KDF. Όπως παρουσιάστηκε στην προηγούμενη ενότητα, η διαδικασία ενθυλάκωσης κλειδιού, γενικά, μπορεί να συνοψιστεί σε 3 βήματα:

1. Δημιουργία ενός τυχαίου ακεραίου αριθμού z (κατάλληλου μεγέθους).
2. Κρυπτογράφηση του z με την χρήση του RSA για την μεταφορά του στον παραλήπτη.
3. Δημιουργία του κλειδιού $y = KDF(w)$ για χρήση του στην υποκείμενη διαδικασία συμμετρικής κρυπτογράφησης.

Γίνεται εύκολα αντιληπτό ότι ο παραλήπτης μπορεί να ανακτήσει το z από τον κρυπτοκειμένο που παρέλαβε και στην συνέχει να υπολογίζει το y έτσι ώστε και ο αποστολέας και ο ίδιος να συμφωνήσουν στο ίδιο συμμετρικό κλειδί. Ο υπολογισμός του κλειδιού y βασίζεται στην συνάρτηση KDF. Επομένως, η ασφάλεια του RSA-KEM σχετίζεται με την δυσκολία εύρεσης του αντιστρόφου του RSA. Παρακάτω αποδεικνύεται ότι το πλεονέκτημα ενός επιτιθέμενου να κερδίσει το IND-CCA παιχνίδι στο μοντέλο RSA-KEM είναι αμελητέα [33].

Υποθέτουμε πως υπάρχει μια δημόσια συνάρτηση με τις εξής ιδιότητες:

1. Για κάθε νέα μεταβλητή, η συνάρτηση επιστρέφει μια νέα τιμή. Όλες οι τιμές αποθηκεύονται ως ζεύγος (μεταβλητή, τιμή).
2. Σε περίπτωση που η νέα τιμή έχει ήδη αποθηκευτεί, η συνάρτηση επιστρέφει την τιμή που αντιστοιχεί στην μεταβλητή αυτή.

Η απόδειξη ασφαλείας του μοντέλου RSA-KEM βασίζεται στην υπόθεση ότι η αντιστροφή του προβλήματος RSA είναι αδύνατη, καθώς και την υπόθεση ότι η συνάρτηση KDF ικανοποιεί τις απαιτήσεις ασφαλείας μιας συνάρτησης κατακερματισμού.

Για τον αλγόριθμο δημιουργίας κλειδιού RSA (ο οποίος επιστρέφει την τριπλέτα (n, e, d)), θεωρούμε ότι υπάρχει ένα μικρότερο επιτρεπόμενο όριο για τους αριθμούς n, $nBound \leq n$. Για την απόδειξη ασφαλείας στο μοντέλο IND-CCA αρκεί να αποδειχτεί ότι για οποιονδήποτε επιτιθέμενο A ισχύει ότι $Adv_{RSA-KEM}(A) \leq Adv_{RSAKeyGen}(A') + qD/nBound$, όπου:

- qD είναι ο μέγιστος αριθμός επιτρεπόμενων ερωτημάτων που μπορεί να αποστείλει ο επιτιθέμενος με σκοπό να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα c.
- A' είναι ένας αλγόριθμος για την επίλυση του προβλήματος RSA. Με άλλα λόγια η μεταβλητή $Adv_{RSAKeyGen}(A')$ αποδίδει την πιθανότητα επιτυχημένης επίλυσης του προβλήματος RSA. Σε αυτό το σημείο θα πρέπει να τονιστεί πως η παραπάνω ανισότητα δεν λαμβάνει υπόψη το γεγονός ότι ο αλγόριθμος δημιουργίας κλειδιού RSA μπορεί να επιστρέψει μη επιτρεπτά κλειδιά. Για να ληφθεί το γεγονός αυτό υπόψη, αρκεί τα προστεθεί η πιθανότητα αυτή στην παραπάνω ανισότητα.

Για την απόδειξη ασφαλείας στο μοντέλο IND-CCA θεωρούμε πως υπάρχει μια σειρά παιχνιδιών G_i για τα οποία υπάρχει ένας αντίπαλος A, ο οποίος πραγματοποιεί μια επίθεση. Κάθε ένα από τα παιχνίδια λαμβάνει χώρα σε ένα χώρο πιθανοτήτων και στην πράξη, σε κάθε παιχνίδι αλλάζει ο τρόπος υποβολής ερωτημάτων από τον επιτιθέμενο. Επιπλέον, κάθε παιχνίδι έχει ένα ενδεχόμενο S_i σε αντιστοιχία με το ενδεχόμενο S_0 του αρχικού παιχνιδιού. Σκοπός είναι να

αποδειχτεί πως η διαφορά $|\mathrm{P}[S_i] - \mathrm{P}[S_{i-1}]|$ είναι αμελητέα, κάτι το οποίο θα σημαίνει πως για το τελευταίο παιχνίδι ισχύει ότι $\mathrm{P}[S_k] = 1/2$.

Έστω ότι G_0 είναι το αρχικό παιχνίδι και S_0 το ενδεχόμενο ότι ο επιτιθέμενος A έχει μαντέψει σωστά το κρυφό bit b στο παιχνίδι G_0. Υποθέτουμε ότι η μεταβλητή H συμβολίζει την τυχαιότητα μετατροπής των στοιχείων του Z_n στα bit μεγέθους $KeyLen$. Επιπλέον, θεωρούμε πως $y' \in Z_n$ συμβολίζει το κρυπτοκείμενο στόχο και $\mathrm{r}' = (y')^{1/e} \in Z_n$.

Έπειτα, ορίζουμε ένα παιχνίδι G_1 ίδιο με το αρχικό παιχνίδι G_0, με την διαφορά ότι αν το κρυπτοκείμενο στόχος y' έχει υποβληθεί για αποκρυπτογράφηση πριν γίνει επίκληση στον αλγόριθμο κρυπτογράφησης, το παιχνίδι τερματίζεται. Θεωρούμε ότι S_1 είναι ένα ενδεχόμενο του παιχνιδιού G_1, το οποίο αντιστοιχεί με το γεγονός S_0.

Υποθέτοντας ότι το παιχνίδι τερματίζεται στο ενδεχόμενο F_1, το πλεονέκτημα του επιτιθέμενου ορίζεται από την ανισότητα $\mathrm{P}[F_1] \leq q_D/nBound$. Εφόσον τα παιχνίδια G_0 και G_1 είναι πανομοιότυπα μέχρι να συμβεί το ενδεχόμενο F_1, ισχύει ότι $|\mathrm{P}[S_0] - \mathrm{P}[S_1]| \leq q_D/nBound$, βάση του παρακάτω λήμματος [33].

Λήμμα 6.2.1.1: Έστω ότι E, E', F, F' είναι ενδεχόμενα σε ένα χώρο πιθανοτήτων τέτοια ώστε $P[E \wedge \neg F] = P[E' \wedge \neg F]$ και $\mathrm{P}[F] = \mathrm{P}[F']$. Για τα ενδεχόμενα αυτά ισχύει ότι $|\mathrm{P}[E] - \mathrm{P}[E']| \leq \mathrm{P}[F]$.

Σημειώνεται ότι $P[E \wedge \neg F]$ συμβολίζει την πιθανότητα να συμβεί το ενδεχόμενο E και ταυτόχρονα να μην συμβαίνει το ενδεχόμενο E.

Η απόδειξη του παραπάνω λήμματος ακολουθεί έναν απλό υπολογισμό. Έχουμε:

- $P[E] = P[E \wedge \neg \mathrm{F}](1 - \varepsilon) + P[E \wedge \mathrm{F}]\varepsilon$, όπου $\varepsilon = \mathrm{P}[F]$,
- $P[E'] = P[E' \wedge \neg \mathrm{F}'](1 - \varepsilon) + P[E' \wedge \mathrm{F}']\varepsilon$.

Αφαιρώντας τις παραπάνω εξισώσεις και παίρνοντας τις απόλυτες τιμές, έχουμε:

- $|\mathrm{P}[E] - \mathrm{P}[E']| = \varepsilon|P[E \wedge \mathrm{F}] - P[E' \wedge \mathrm{F}']| \leq \varepsilon = \mathrm{P}[F]$.

Βάση του παραπάνω λήμματος, για το RSA-KEM ισχύει ότι $|\mathrm{P}[S_0] - \mathrm{P}[S_1]| \leq q_D/nBound$.

Στην συνέχεια, ορίζεται το παιχνίδι G_2, το οποίο είναι πανομοιότυπο με το παιχνίδι G_1, με την διαφορά ότι το κρυπτοκείμενο στόχος έχει δημιουργηθεί κατά την έναρξη του παιχνιδιού και ότι αν ο επιτιθέμενος αποστείλει ερωτήματα H για το r', το παιχνίδι τερματίζεται. Θεωρούμε ότι S_2 είναι το ενδεχόμενο του παιχνιδιού G_2 σε αντιστοιχία με το S_0. Γίνεται εύκολα αντιληπτό ότι $\mathrm{P}[S_2] = 1/2$, αφού το κλειδί $H(r')$ είναι ανεξάρτητο στο παιχνίδι G_2. Αυτό συμβαίνει διότι το H για το r' καλείται μόνο για λόγους κρυπτογράφησης.

Υποθέτοντας ότι το παιχνίδι G_2 τερματίζεται στο γεγονός F_2, το πλεονέκτημα του επιτιθέμενου ορίζεται από το $\mathrm{P}[F_2]$. Τα παιχνίδια G_1 και G_2 είναι πανομοιότυπα μέχρι να συμβεί το γεγονός F_2 και έτσι ισχύει ότι $|\mathrm{P}[S_1] - \mathrm{P}[S_2]| \leq \mathrm{P}[F_2]$.

Για τον αλγόριθμο A' θεωρούμε πως $\mathrm{P}[F_2] \leq Advantage_{RSA}(A')$, χρόνος εκτέλεσης του οποίου περιορίζεται από τον χρόνο που περιεγράφηκε προηγουμένως. Ο αλγόριθμος A' λειτουργεί ως εξής:

Λαμβάνει ως είσοδο ένα τυχαίο RSA $modulus\ n$, μια δύναμη RSA e και ένα τυχαίο στοιχείο $y' \in Z_n$.

Δημιουργεί το δημόσιο κλειδί χρησιμοποιώντας τα στοιχεία n, e και επιτρέπει στον επιτιθέμενο A να ξεκινήσει το παιχνίδι G_2.

Όταν ο επιτιθέμενος αποστέλλει ερωτήματα κρυπτογράφησης, ο αλγόριθμος A' αποφέρει ένα ζεύγος (K', y'), όπου K' είναι ένα αλφαριθμητικό τυχαίων bit, μεγέθους $KeyLen$. Ο αλγόριθμος A' προσομοιώνει την τυχαιότητα H, καθώς και την διαδικασία αποκρυπτογράφησης ως εξής:

Για κάθε είσοδο $r \in Z_n$, ο αλγόριθμος A' υπολογίζει $y = r^e \in Z_n$ και αποθηκεύει την τριπλέτα $(r, y, K = H(r))$.

Σε περίπτωση που $y' = y$, ο αλγόριθμος αποφέρει r και τερματίζει.

Όποτε ένας επιτιθέμενος αποστέλλει ένα ερώτημα αποκρυπτογράφησης $y \in Z_n$, ο αλγόριθμος αναζητά την μεταβλητή y στα αποθηκευμένα στοιχεία για να διαπιστωθεί αν έχει δημιουργηθεί η μεταβλητή $r = y^{1/e} \in Z_n$. Αν έχει δημιουργηθεί η μεταβλητή r, ο αλγόριθμος επιστρέφει $H(r)$. Διαφορετικά, δημιουργεί ένα νέο κλειδί $K = H(r)$ και αποθηκεύει το ζεύγος (y, K). Μελλοντικά, αν ο επιτιθέμενος αξιολογήσει τον αλγόριθμο για το στοιχείο $r \in Z_n$, τέτοιο ώστε $r^e = y$, το κλειδί K θα χρησιμοποιηθεί για την τιμή του $H(r)$.

Η παραπάνω προσομοίωση του αλγορίθμου A' είναι κατάλληλη για έναν επιτιθέμενο A και έτσι το πλεονέκτημα ορίζεται $\mathrm{P}[F_2]$. Έτσι, αποδεικνύεται η ασφάλεια του μηχανισμού RSA-KEM.

Επομένως, εφόσον έχει οριστεί η ασφάλεια του RSA-KEM βάση της δυσκολίας επίλυσης του προβλήματος RSA μπορούμε να οδηγηθούμε στο παρακάτω λήμμα:

Λήμμα 6.2.1.2: Αν το πρόβλημα RSA είναι υπολογιστικά δύσκολο, τότε ο μηχανισμός RSA-KEM ικανοποιεί τις απαιτήσεις ασφαλείας IND-CCA για το KEM, εφόσον η συνάρτηση KDF ικανοποιεί τις απαιτήσεις ασφαλείας μιας συνάρτησης κατακερματισμού.

Όπως παρουσιάστηκε στην περιγραφή λειτουργίας του RSA-KEM, σύμφωνα με το πρότυπο RFC 5990 [50], ο μηχανισμός RSA-KEM μπορεί να χρησιμοποιείται με την προσθήκη ενός σχήματος συμμετρικής κρυπτογράφησης για την προστασία του μυστικού κλειδιού. Στην περίπτωση αυτή εκτός από την δυσκολία επίλυσης του προβλήματος RSA και την δυσκολία αντιστροφής του κλειδιού, πρέπει να παρέχεται εγγύηση ασφάλειας στο σχήμα επικάλυψης του κλειδιού. Έτσι, βασική προϋπόθεση αποτελεί ότι το σχήμα αυτό ικανοποιεί τις απαιτήσεις ασφαλείας ενός συμμετρικού αλγορίθμου (ή ενός DEM).

Όσον αφορά τα μεγέθη των κλειδιών που πρέπει να χρησιμοποιούνται για τον αλγόριθμο RSA, καθώς και για το σχήμα επικάλυψης κλειδιού αν αυτό προστεθεί, σύμφωνα με τον οργανισμό NIST [51], αυτά (σε επίπεδο συμμετρικής ασφάλειας) είναι:

- Ασφάλεια 80-bit: Το κλειδί RSA πρέπει να είναι κατ' ελάχιστο 1024 bits και η συνάρτηση κατακερματισμού που χρησιμοποιείται από τον αλγόριθμο KDF να είναι τουλάχιστον η SHA-1.
- Ασφάλεια 112-bit: Το κλειδί RSA πρέπει να είναι κατ' ελάχιστο 2048 bits και η συνάρτηση κατακερματισμού που χρησιμοποιείται από τον αλγόριθμο KDF να είναι τουλάχιστον η SHA-224.
- Ασφάλεια 128-bit: Το κλειδί RSA πρέπει να είναι κατ' ελάχιστο 3072 bits και η συνάρτηση κατακερματισμού που χρησιμοποιείται από τον αλγόριθμο KDF να είναι τουλάχιστον η SHA-256.

Για κάθε μια από τις παραπάνω περιπτώσεις, εάν χρησιμοποιηθεί το υποκείμενο σχήμα επικάλυψης κλειδιού, ο αλγόριθμος συμμετρικής κρυπτογράφησης πρέπει να είναι είτε ο AES είτε Camellia.

Προφανώς, απαραίτητη προϋπόθεση για το RSA-KEM είναι η προστασία του ιδιωτικού κλειδιού, καθώς και η προστασία του κλειδιού κρυπτογράφησης σε περίπτωση που χρησιμοποιηθεί το σχήμα Wrap. Η απόκτηση του ιδιωτικού κλειδιού οδηγεί στην αποκάλυψη όλων των μηνυμάτων που έχουν προστατευτεί με το κλειδί αυτό, ενώ η αποκάλυψη του κλειδιού κρυπτογράφησης για τον αλγόριθμο Wrap οδηγεί στην αποκάλυψη όλων των μηνυμάτων που έχουν κρυπτογραφηθεί με αυτό. Επίσης, δε θα πρέπει να δίνεται καμία πληροφορία για τον υπολογισμό των ενδιάμεσων τιμών, καθώς και ένας επιτιθέμενος δε θα πρέπει να λαμβάνει καμιά πληροφορία όσον αφορά τον χρόνο υπολογισμού των τιμών. Σε διαφορετική περίπτωση επιθέσεις χρονισμού είναι εφικτές και έτσι ο επιτιθέμενος θα μπορεί να διαπιστώσει πληροφορίες σχετικά με το ιδιωτικό κλειδί του παραλήπτη.

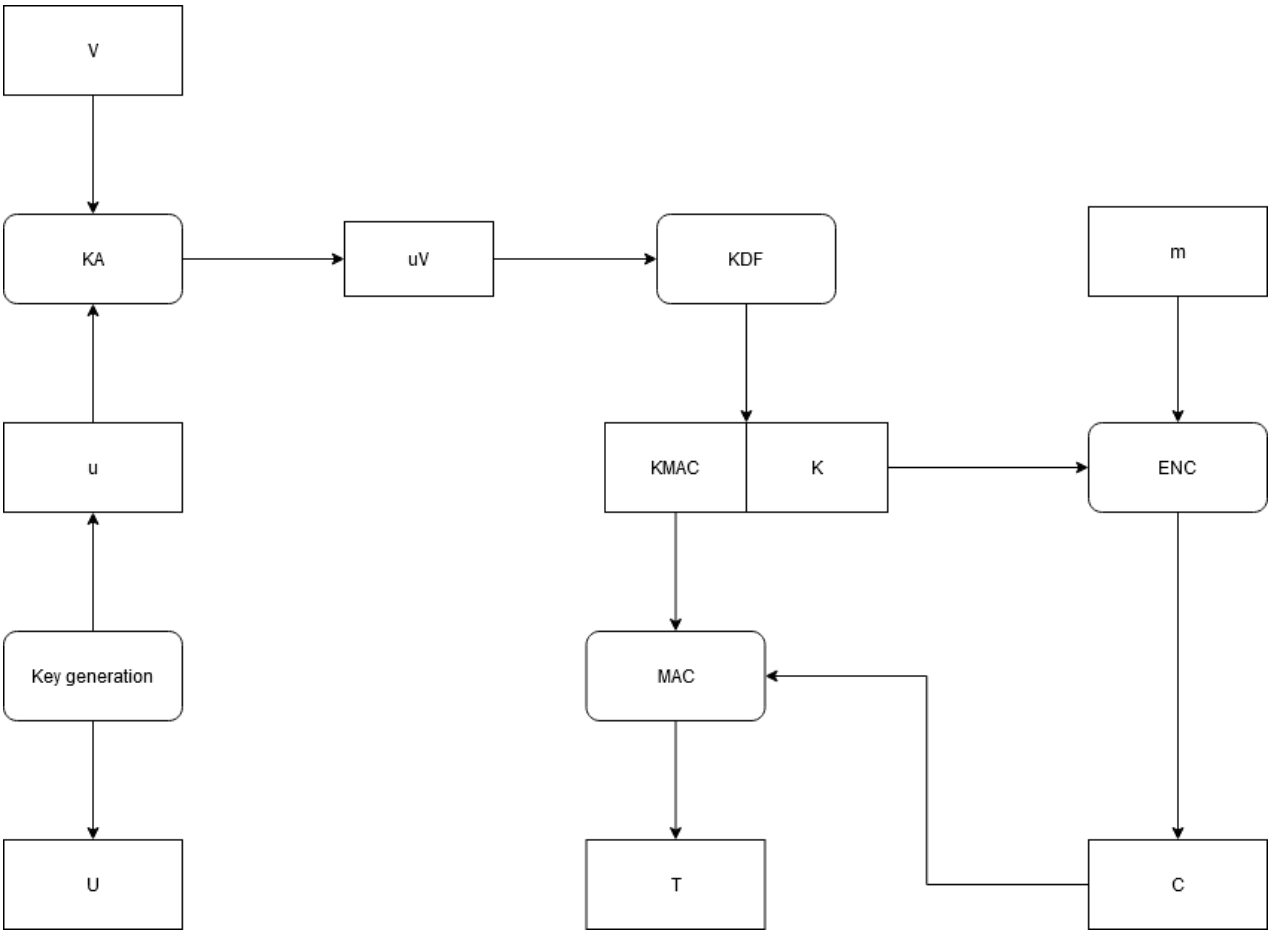
4.3 ECIES-KEM

Ένα από τα εκτενέστερα σχήματα κρυπτογραφίας βασισμένο σε ελλειπτικές καμπύλες είναι το Elliptic Curve Integrated Encryption Scheme (ECIES). Το συγκεκριμένο σχήμα αποτελεί μια παραλλαγή του σχήματος ElGamal και αρχικά παρουσιάστηκε το 1997 με την ονομασία Discrete Logarithm Augmented Encryption Scheme (DLAES) [52]. Ένα χρόνο μετά, η αρχική έκδοση του αλγορίθμου βελτιώθηκε από τους ίδιους ερευνητές και μετονομάστηκε σε Diffie-Hellman Augmented Encryption Scheme (DHAES) και αργότερα, το 2001 μετονομάστηκε σε Diffie-Hellman Integrated Encryption Scheme (DHIES) [53]. Το συγκεκριμένο σχήμα μπορεί να βρεθεί σε διάφορες παραλλαγές σε πρότυπα επικοινωνιών και σε γενικότερο επίπεδο, αναφέρεται με το όνομα ECIES. Το σχήμα ECIES αποτελείται από τις εξής πέντε παραμέτρους :

1. Συνάρτηση Συμφωνίας Κλειδιού (KA): συνάρτηση που χρησιμοποιείται για την δημιουργία ενός κοινού μυστικού κλειδιού στην επικοινωνία δύο χρηστών. Στην πράξη ο αλγόριθμος Diffie-Hellman υλοποιεί την συγκεκριμένη συνάρτηση.
2. Συνάρτηση Δημιουργίας κλειδιού (KDF): μια συνάρτηση κατακερματισμού όπως παρουσιάστηκε στην αρχή αυτού του κεφαλαίου.
3. Κρυπτογράφηση (E): Αλγόριθμος συμμετρικής κρυπτογράφησης.
4. Συνάρτηση αυθεντικοποιήσης μηνύματος (MAC): Συνάρτηση η οποία αποφέρει δεδομένα, τα οποία αυθεντικοποιούν την προέλευση των μηνυμάτων.

Για την περιγραφή της λειτουργίας του σχήματος ECIES, όπως και στις υπόλοιπες περιπτώσεις, υποθέτουμε ότι ένας χρήστης θέλει να επικοινωνήσει με έναν άλλο. Το ζεύγος δημοσίου και ιδιωτικού κλειδιού των δύο χρηστών αναπαρίστανται με (U, u) και (V, v), αντίστοιχα. Όπως είδαμε στην ενότητα 4.1, τα ιδιωτικά κλειδιά πάνω σε ελλειπτικές καμπύλες είναι στοιχεία ενός πεπερασμένου σώματος, του $GF(p)$ ή του $GF(2^m)$, ενώ τα δημόσια κλειδιά είναι σημεία που ανήκουν στην ελλειπτική καμπύλη και υπολογίζονται ως το γινόμενο του ιδιωτικού κλειδιού και του γεννήτορα G της ελλειπτικής καμπύλης. Τα βήματα που ακολουθούνται για την λειτουργία του σχήματος ECIES είναι τα εξής:

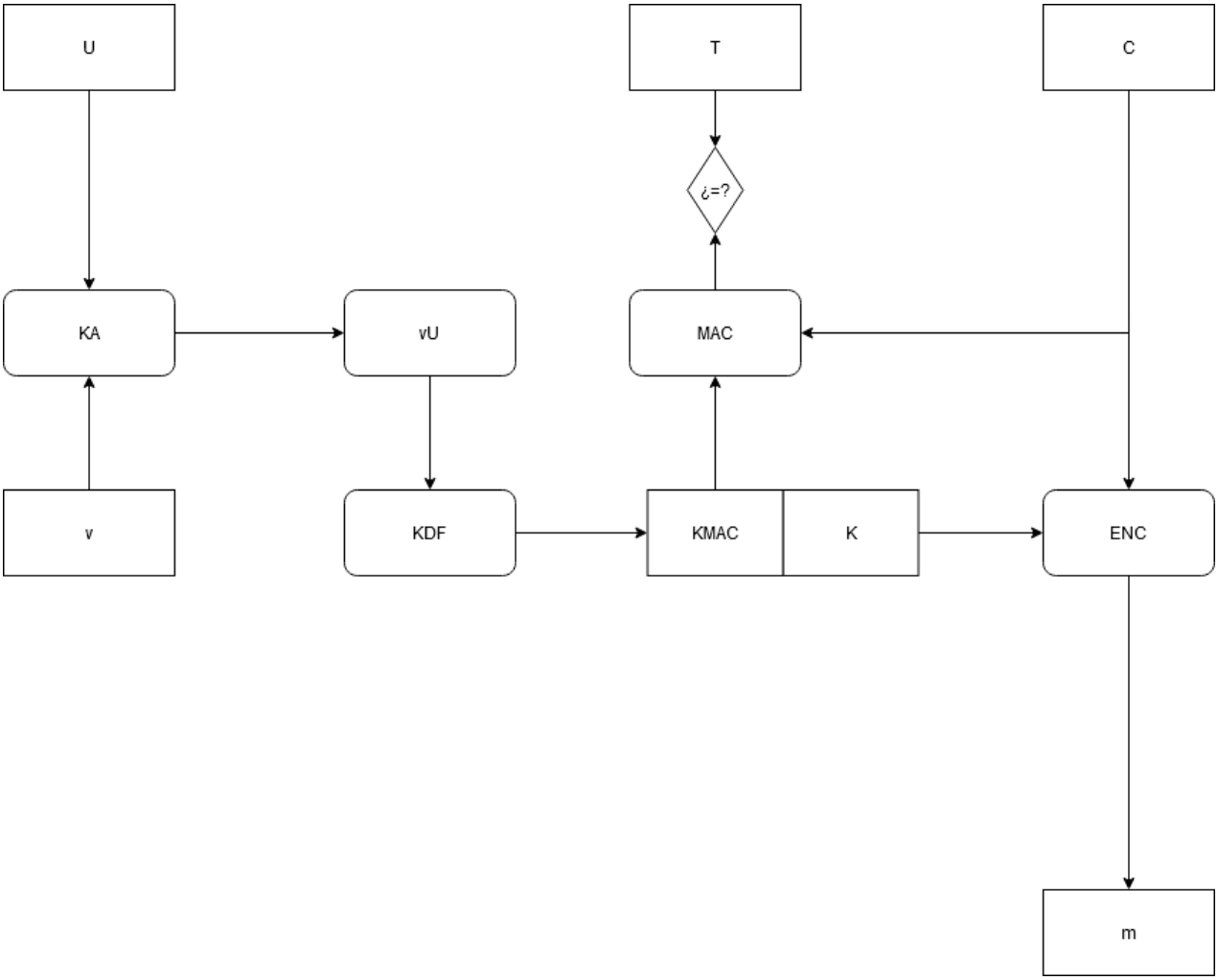
- Ο πρώτος χρήστης δημιουργεί ένα επίκαιρο ζεύγος δημοσίου-ιδιωτικού κλειδιού (U, u), όπου $U = uG$. Στην πράξη ο ακέραιος αριθμός $u \in [1, n-1]$ επιλέγεται τυχαία.
- Αφού έχει δημιουργηθεί το ζεύγος δημοσίου-ιδιωτικού κλειδιού, χρησιμοποιείται η συνάρτηση KA ώστε να δημιουργηθεί η διαμοιρασμένη μυστική τιμή. Η συνάρτηση αυτή λαμβάνει ως είσοδο το ιδιωτικό κλειδί u του χρήστη και το δημόσιο κλειδί του παραλήπτη V. Η μυστική τιμή υπολογίζεται από τον πολλαπλασιασμό των τιμών αυτών, $S = uV$.
- Στην συνέχεια, η τιμή που υπολογίστηκε εισάγεται ως είσοδος στην συνάρτηση KDF. Η συνάρτηση αυτή επιστρέφει δύο μεταβλητές, το συμμετρικό κλειδί κρυπτογράφησης K και το κλειδί για χρήση από τον αλγόριθμο MAC, ΚMAC, $KDF(uV) = K||KMAC$.
- Το κλειδί K που υπολογίστηκε χρησιμοποιείται για την συμμετρική κρυπτογράφηση του αρχικού μηνύματος m, $C = E(K, m)$.
- Το κλειδί $KMAC$ που υπολογίστηκε μαζί με το κρυπτογράφημα C χρησιμοποιείται για την δημιουργία της ετικέτας MAC, $T = MAC(C, KMAC)$.
- Αποστέλλεται στον παραλήπτη μια τιμή που αποτελείται από το δημόσιο κλειδί του αποστολέα U, την ετικέτα MAC T και το κρυπτοκείμενο C, $Output = (U||T||C)$.



Εικόνα 4.5: Διαδικασία κρυπτογράφησης με το κρυπτοσύστημα ECIES.

Όσον αφορά την αποκρυπτογράφηση, η διαδικασία που ακολουθείται στην πλευρά του παραλήπτη αφού πραγματοποιηθεί παραλαβή της τιμής $Output$ είναι η εξής:

- Γίνεται ανάκτηση του δημοσίου κλειδιού του αποστολέα U, της ετικέτας T και το κρυπτογραφημένου μηνύματος C.
- Με την χρήση του δημοσίου κλειδιού U του αποστολέα και του ιδιωτικού κλειδιού v του παραλήπτη, υπολογίζεται η κοινή μυστική τιμή $S = vU$ μέσω της συνάρτησης KA. Το αποτέλεσμα του πολλαπλασιασμού αυτού είναι ίδιο με την πράξη που πραγματοποιήθηκε στην πλευρά του αποστολέα ($S = uV$). Στην πράξη, η συνάρτηση συμφωνίας κλειδιού είναι το κρυπτοσύστημα Diffie-Hellman.
- Με την χρήση του μυστικού κλειδιού στην συνάρτηση KDF, ο παραλήπτης θα πρέπει να υπολογίσει το ίδιο κλειδί κρυπτογράφησης, καθώς και το αντίστοιχο κλειδί MAC, $KDF(vU) = K||KMAC$.
- Στην συνέχεια, βάση του κλειδιού MAC και του κρυπτοκειμένου C, υπολογίζεται η ετικέτα T και συγκρίνεται η τιμή που υπολογίστηκε με αυτή που έχει παραληφθεί, $T = MAC(C, KMAC)$. Σε περίπτωση που οι τιμές είναι διαφορετικές, ο παραλήπτης απορρίπτει την επικοινωνία λόγω σφάλματος στην ετικέτα MAC.
- Εάν η ετικέτα που υπολογίστηκε είναι ίδια με αυτή που έχει αποσταλεί, η διαδικασία συνεχίζει στην αποκρυπτογράφηση του μηνύματος C, με την χρήση του κλειδιού που υπολογίστηκε από την συνάρτηση KDF, $m = E(C, K)$.



Εικόνα 4.6: Διαδικασία αποκρυπτογράφησης με το κρυπτοσύστημα ECIES.

Όπως παρουσιάστηκε, η λειτουργία του συγκεκριμένου σχήματος περιλαμβάνει λειτουργίες δημοσίου κλειδιού, αλγορίθμους κρυπτογράφησης, επαλήθευση ετικέτας και υπολογισμούς βάση συναρτήσεων κατακερματισμού. Λόγω της προσαρμογής των διάφορων συναρτήσεων, το σχήμα ECIES θεωρείται ασφαλές έναντι επιθέσεων επιλεγμένου κρυπτοκειμένου χωρίς να απαιτείται να αυξηθεί ο αριθμός των υπολογισμών ή του μήκους του κλειδιού [53].

Μια παραλλαγή του παραπάνω αλγορίθμου προτάθηκε από τον Shoup ως μηχανισμός ενθυλάκωσης κλειδιού, το οποίο ονομάστηκε ECIES-KEM [33]. Ο συγκεκριμένος μηχανισμός έχει πολλές ομοιότητες με το κρυπτοσύστημα PSEC-3 (Provably Secure Elliptic Curve) [54], το οποίο στηρίζεται σε ελλειπτικές καμπύλες. Έτσι, πριν την περιγραφή του ECIES-KEM, αναφέρεται ο τρόπος λειτουργίας του κρυπτοσυστήματος PSEC-3.

Το σχήμα PSEC-3, μοιάζει αρκετά με το σχήμα ECIES, αφού χρησιμοποιεί παρόμοιες παραμέτρους συστήματος. Συγκεκριμένα, αποτελείται από τις εξής παραμέτρους :

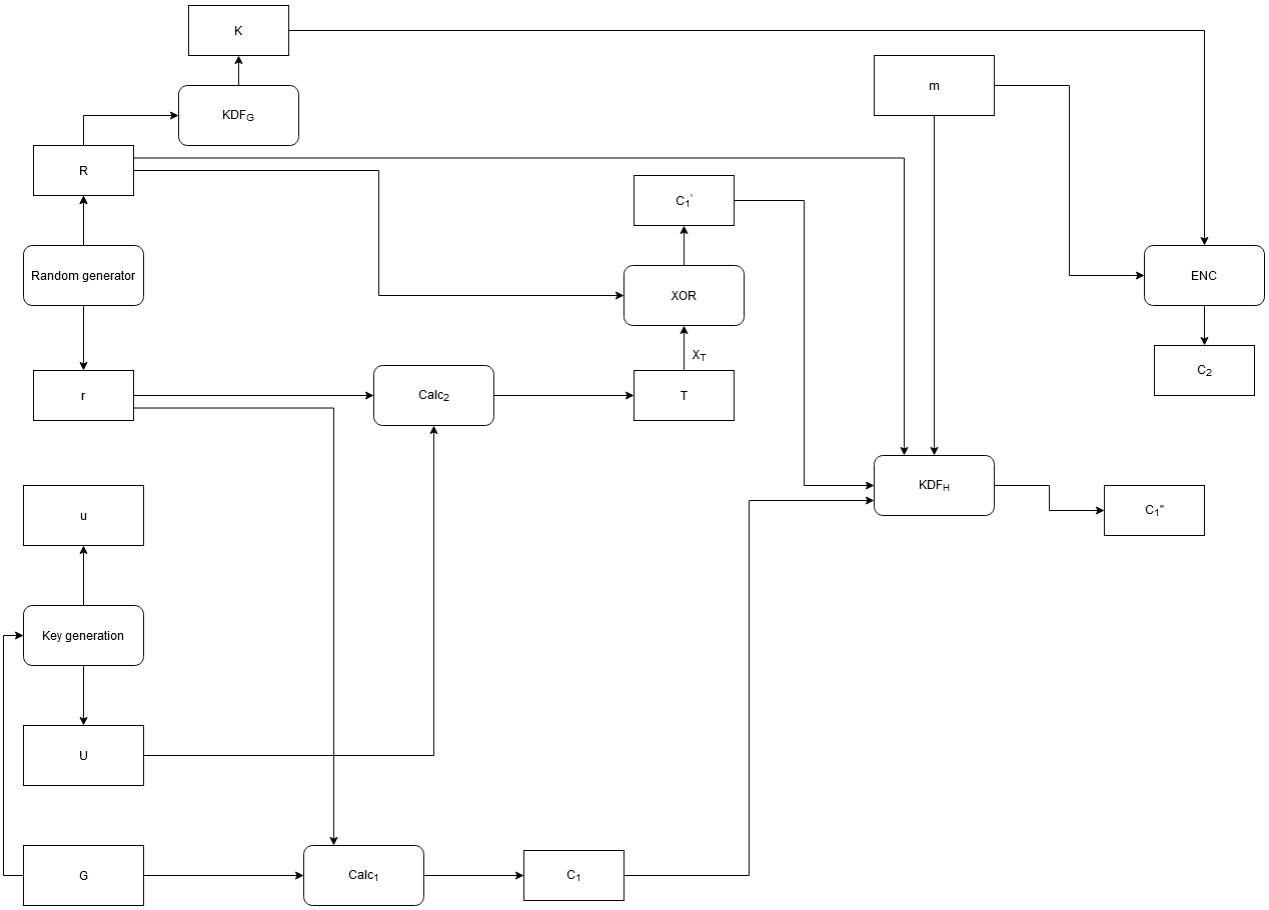
1. Συνάρτηση Δημιουργίας κλειδιού (KDF): το σχήμα PSEC-3 χρησιμοποιεί δύο συναρτήσεις KDF (συναρτήσεις κατακερματισμού), την KDF_G και την KDF_H. Η πρώτη, εξάγει το κλειδί όπως σε όλες τις περιπτώσεις που χρησιμοποιούνται συναρτήσεις KDF, ενώ η KDF_H χρησιμοποιείται για την εξαγωγή δεδομένων αυθεντικοποίησης.

2. Κρυπτογράφηση (E): Αλγόριθμος συμμετρικής κρυπτογράφησης/αποκρυπτογράφησης. Στην πράξη ο αλγόριθμος αυτός αποτελείται από το ζεύγος αλγορίθμων κρυπτογράφησης και αποκρυπτογράφησης. Ο αλγόριθμος κρυπτογράφησης λαμβάνει ως είσοδο το κλειδί K που δημιουργείται από την KDF_G και ένα αρχικό μήνυμα και επιστρέφει το αντίστοιχο κρυπτογράφημα. Αντίστοιχα, ο αλγόριθμος αποκρυπτογράφησης λαμβάνει ως είσοδο το κρυπτογράφημα και το κλειδί K και επιστρέφει το αρχικό μήνυμα.

Όπως σε όλες τις περιπτώσεις περιγραφής κρυπτοσυστημάτων, υποθέτουμε ότι δύο χρήστες θέλουν να επικοινωνήσουν μεταξύ τους, για τους οποίους το ζεύγος δημοσίου και ιδιωτικού κλειδιού αναπαρίστανται με (U, u) και (V, v), αντίστοιχα. Όπως αναφέρθηκε και στην περιγραφή του κρυπτοσυστήματος ECIES, αλλά και γενικότερα για τα κρυπτοσυστήματα που βασίζονται σε ελλειπτικές καμπύλες, τα ιδιωτικά κλειδιά είναι στοιχεία ενός πεπερασμένου σώματος και τα δημόσια κλειδιά σημεία που υπολογίζονται ως γινόμενο του ιδιωτικού κλειδιού και ενός γεννήτορα G της ελλειπτικής καμπύλης. Τα βήματα που ακολουθούνται για την λειτουργία του σχήματος PSEC-3 είναι τα εξής:

- Ο πρώτος χρήστης δημιουργεί ένα επίκαιρο ζεύγος δημοσίου-ιδιωτικού κλειδιού (U, u), όπου $U = uG$. Στην πράξη ο ακέραιος αριθμός $u \in [1, n-1]$.
- Αφού έχει δημιουργηθεί το ζεύγος δημοσίου-ιδιωτικού κλειδιού, επιλέγονται τυχαία δύο αριθμοί $R \in \{0,1\}^{qLen}$, όπου $qLen$ είναι το μέγεθος $|q|$ της τάξης q του πεπερασμένου πεδίου F_q και r $\in \mathbb{Z}_p^*$.
- Έπειτα, υπολογίζονται τα σημεία στην ελλειπτική καμπύλη $C_1 = rG$ και $T = rU$.
- Στην συνέχεια υπολογίζονται οι εξής τιμές:
  - $C_1{}' = R \oplus \mathrm{x}_T$, όπου x_T είναι η x-συντεταγμένη του σημείου T.
  - $K = KDF_G(R)$. Σημειώνεται ότι η συνάρτηση KDF_G υλοποιείται με τρόπο ώστε να μετατρέπει έναν αριθμό $a \in \{0,1\}^{qLen}$ στο $a' \in \{0,1\}^{kLen}$, όπου $kLen$, είναι το μέγεθος του κλειδιού που πρόκειται να δημιουργηθεί.
  - $C_1{}'' = KDF_H(C_1||C_1'||R||m)$. Σημειώνεται ότι η συνάρτηση KDF_H λαμβάνει ως εισόδους το σημείο C_1, την τιμή $C_1{}'$, τον τυχαίο αριθμό R και το αρχικό μήνυμα m. Η τιμή $C_1{}'$ και R έχουν μέγεθος $qLen$ και το μήνυμα m έχει μέγεθος $mLen$. Όσον αφορά το μέγεθος του σημείου C_1, $|C_1|$, αυτό είναι είτε $|C_1| = qLen + 1$ αν το σημείο αναπαρίσταται από την x-συντεταγμένη του και 1 bit υπογραφής, είτε $|C_1| = 2qLen$ αν το σημείο αναπαρίσταται από το ζεύγος (x-συντεταγμένη, y-συντεταγμένη). Επομένως η συνάρτηση KDF_H υλοποιείται με τρόπο τέτοιο ώστε να μετατρέπει έναν αριθμό $a \in \{0,1\}^{|C_1|+2qLen+mLen}$ στο $a' \in \{0,1\}^{hLen}$, όπου $hLen$, είναι το μέγεθος της ετικέτας που δημιουργείται. Ουσιαστικά, η συνάρτηση KDF_H, ικανοποιεί τις απαιτήσεις αυθεντικοποίησης και χρησιμοποιείται έναντι μιας συνάρτησης MAC.
- Το κλειδί K που υπολογίστηκε χρησιμοποιείται για την συμμετρική κρυπτογράφηση του αρχικού μηνύματος m, $C_2 = E(K, m)$.

- Αποστέλλεται στον παραλήπτη μια τιμή που αποτελείται από το δημόσιο κλειδί του αποστολέα U, το σημείο C_1, την τιμή $C_1{}'$, την έξοδο της συνάρτησης KDF_H, $C_1{}''$ και το κρυπτογράφημα C_2, $Output = (U, C_1, C_1', C_1'', C_2)$.

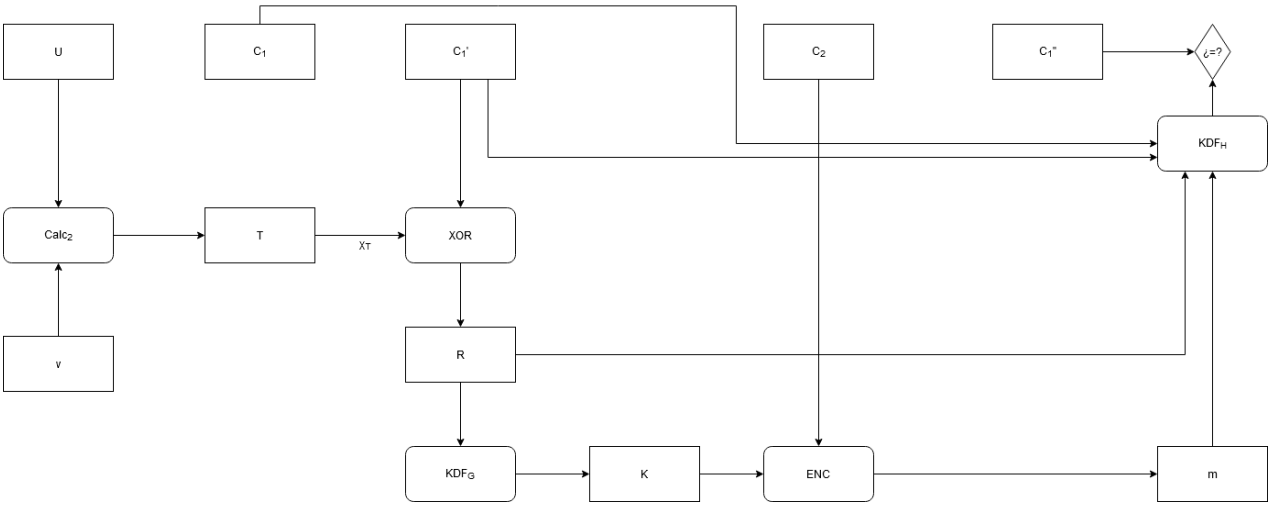


Εικόνα 4.7: Διαδικασία κρυπτογράφησης με το κρυπτοσύστημα PSEC-3.

Όσον αφορά την διαδικασία αποκρυπτογράφησης, στην πλευρά του παραλήπτη, αφού γίνει λήψη της τιμής $Output$, πραγματοποιούνται τα εξής:

- Γίνεται ανάκτηση του δημοσίου κλειδιού του αποστολέα U, του σημείου C_1 της ελλειπτικής καμπύλης που υπολογίστηκε στην πλευρά του αποστολέα, της τιμής C_1', της ετικέτας C_1'' και του κρυπτογραφημένου μηνύματος C_2.
- Υπολογίζεται το σημείο της ελλειπτικής καμπύλης $T = vU$, με την χρήση του δημοσίου κλειδιού U του αποστολέα και του ιδιωτικού κλειδιού v του παραλήπτη. Το αποτέλεσμα του υπολογισμού είναι με τον υπολογισμό που πραγματοποιήθηκε στην πλευρά του αποστολέα ($T = rU$).
- Εφόσον πραγματοποιηθεί ανάκτηση του σημείου T, ο αποστολέας είναι σε θέση να υπολογίσει την τιμή $R = C_1' \oplus \mathrm{x}_T$, όπου x_T είναι η x-συντεταγμένη του σημείου T.
- Στην συνέχεια, υπολογίζεται το κλειδί K βάση της συνάρτησης KDF_G, $K = KDF_G(R)$.
- Η διαδικασία συνεχίζει στην αποκρυπτογράφηση του μηνύματος C_2, με την χρήση του κλειδιού που υπολογίστηκε από την συνάρτηση KDF_G, $m = E(K, C_2)$.
- Πριν την επιστροφή της υπολογισμένης τιμής του αρχικού μηνύματος, υπολογίζεται η ετικέτα C_1'' μέσω της συνάρτηση KDF_H, $C_1'' = KDF_H(C_1||C_1'||R||m)$ και ελέγχεται εάν

η τιμή της είναι ίδια με αυτή που υπολογίστηκε. Σε περίπτωση που οι τιμές είναι διαφορετικές, ο παραλήπτης απορρίπτει την επικοινωνία λόγω σφάλματος στην ετικέτα C_1''. Διαφορετικά, επιστρέφεται το αρχικό μήνυμα m.



Εικόνα 4.8: Διαδικασία αποκρυπτογράφησης με το κρυπτοσύστημα PSEC-3.

Όσον αφορά την ασφάλεια του κρυπτοσυστήματος PSEC-3, έχει αποδειχτεί ότι είναι ασφαλές στο μοντέλο IND-CCA, με την προϋπόθεση ότι το πρόβλημα gap-CDH είναι υπολογιστικά αδύνατο να επιλυθεί [54].

Εφόσον έχει αναφερθεί η λειτουργία των κρυπτοσυστημάτων ECIES και PSEC-3, στα οποία στηρίζεται το σχήμα ECIES-KEM, μπορούμε να προχωρήσουμε στην περιγραφή του.

Σύμφωνα με το πρότυπο ISO που προτάθηκε από τον Shoup [33] ο μηχανισμός ECIES-KEM αποτελείται από τις εξής παραμέτρους:

1. Ομάδα $\Gamma = (H, G, g, \mu, \nu, E, D, E', D')$, όπως αυτή ορίστηκε στην αρχή του κεφαλαίου.
2. Συνάρτηση Δημιουργίας κλειδιού (KDF): μια συνάρτηση κατακερματισμού, όπως παρουσιάστηκε στην αρχή του κεφαλαίου.
3. Μεταβλητή Λειτουργίας Συμπαράγοντα (CofactorMode): οι τιμές της μεταβλητής είναι είτε 0 είτε 1.
4. Μεταβλητή Ελέγχου Λειτουργίας (CheckMode): οι τιμές τις μεταβλητής είναι είτε 0 είτε 1.
5. Μήκος Κλειδιού (KeyLen): ένας θετικός ακέραιος αριθμός.

Σημειώνεται ότι οι επιπλέον μεταβλητές που ορίστηκαν στο παραπάνω σύστημα παραμέτρων, δηλαδή η $CofactorMode$ και η $CheckMode$ χρησιμοποιούνται μόνο κατά την διαδικασία απενθυλάκωσης. Οι μεταβλητές αυτές απαιτούνται για την αξιολόγηση ασφαλείας του σχήματος και έχουν άμεση σχέση με την μεταβλητή ν της ομάδας Γ. Ειδικότερα, ισχύουν οι εξής ιδιότητες όσον αφορά την σχέση των μεταβλητών αυτών:

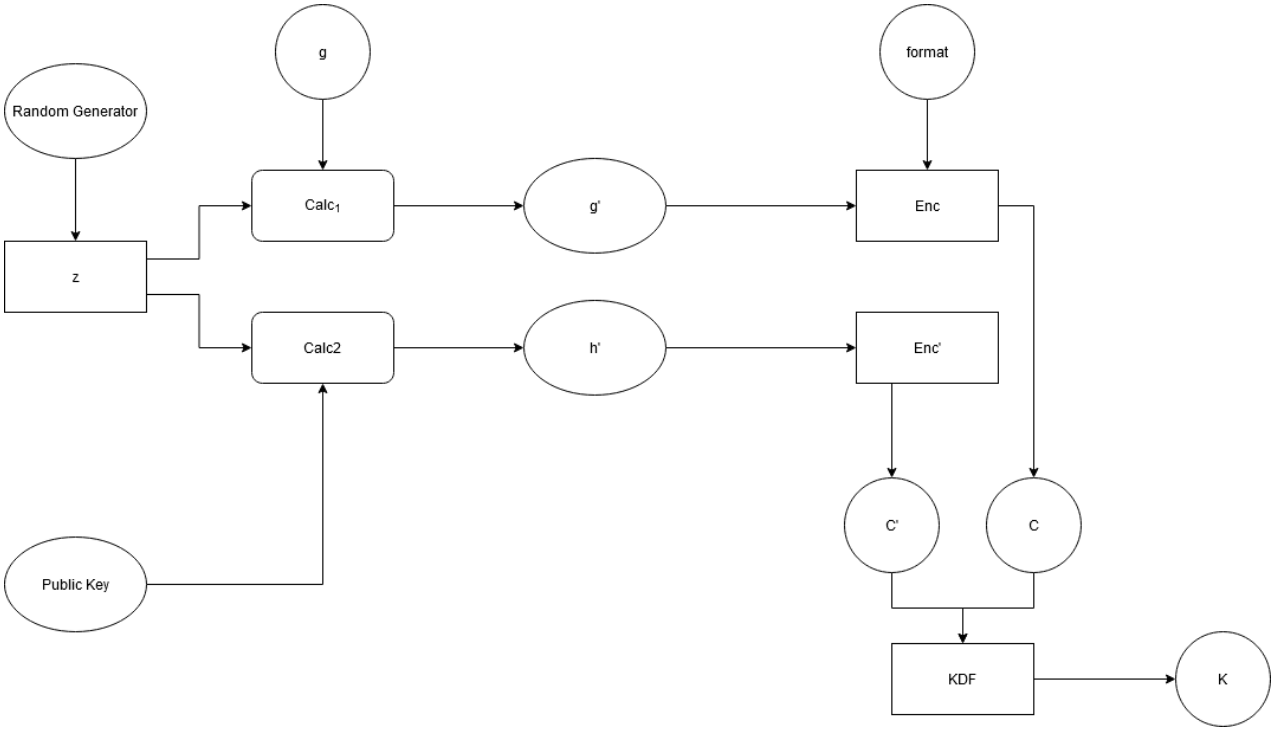
- Αν $\nu = 0$, τότε $CofactorMode = 0$ και $CheckMode = 0$.
- Αν $\nu > 1$ και $MK\Delta(\mu, \nu) = 1$, τότε οι μεταβλητές μπορούν να τεθούν ως $CofactorMode = 0$ ή $CofactorMode = 1$ και $CheckMode = 0$.

- Μόνο μια μεταβλητή εκ των $CofactorModer$ και $CheckMode$ μπορεί να τεθεί ίση με 1.

Από τις παραπάνω ιδιότητες μπορούμε να εξάγουμε δύο συμπεράσματα. Σύμφωνα με την τελευταία ιδιότητα, μόνο μια μεταβλητή εκ των $CofactorMode$ και $CheckMode$ μπορεί να είναι ίση με 1. Επίσης, σύμμφωνα με την δεύτερη ιδιότητα, αν $v > 1$ και $CheckMode = 0$, τότε πρέπει $MK\Delta(\mu, v) = 1$.

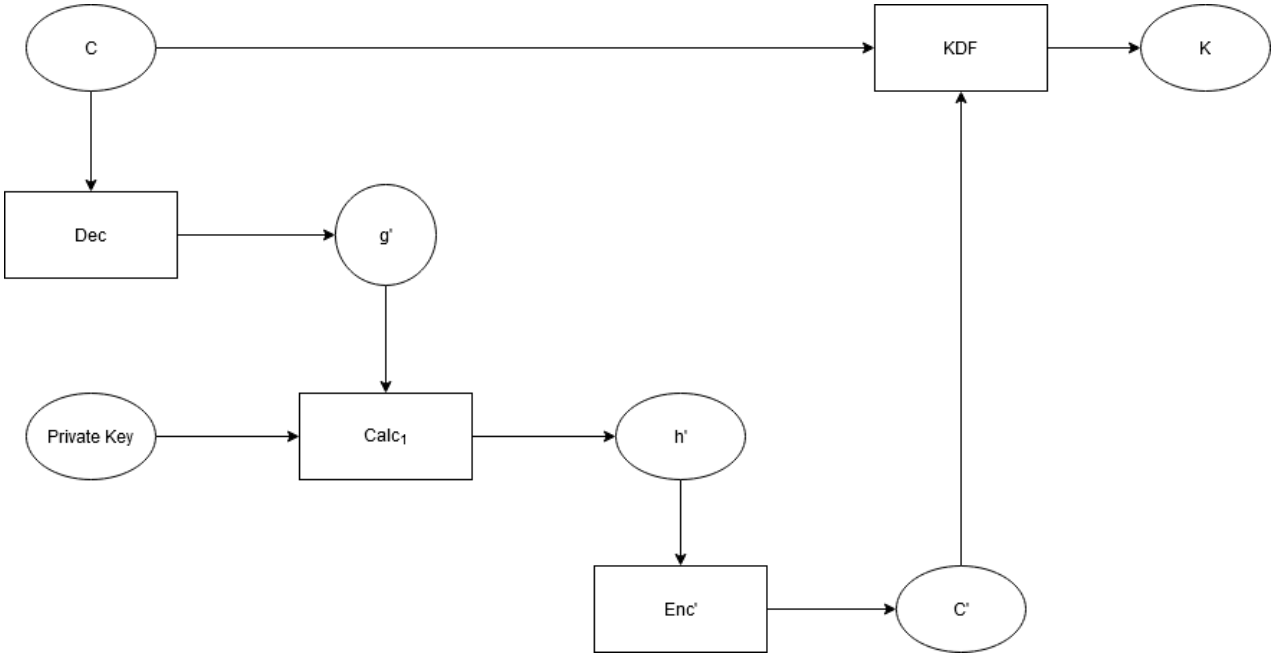
Όπως σε όλα τα σχήματα τύπου KEM, η λειτουργία τους περιγράφεται σε τρία στάδια, την δημιουργία κλειδιών, την διαδικασία ενθυλάκωσης και την διαδικασία απενθυλάκωσης. Έτσι, η λειτουργία του ECIES-KEM έχει ως εξής:

1. Ο αλγόριθμος $Generate_{ECIES-KEM}()$ αποφέρει το ζεύγος (U, u) βάση του αλγορίθμου δημιουργίας κλειδιού, όπου η τιμή U αποτελεί το δημόσιο κλειδί ενός χρήστη, ενώ η τιμή u το αντίστοιχο ιδιωτικό. Ο αλγόριθμος δημιουργίας κλειδιού λειτουργεί ως εξής:
    a. Επιλέγεται ένας τυχαίος ακέραιος αριθμός $u \in [1 \dots \mu)$.
    b. Υπολογίζεται το στοιχείο $U = u * g$.
    c. Ο ακέραιος αριθμός u αποτελεί το ιδιωτικό κλειδί του χρήστη, ενώ το στοιχείο $U \in G$, το αντίστοιχο δημόσιο κλειδί. Σημειώνεται ότι το ιδιωτικό κλειδί εκτός του τυχαίου αριθμού u, περιλαμβάνει και τις τιμές των μεταβλητών $CofactorMode$ και $CheckMode$.
2. Ο αλγόριθμος $Encapsulate_{ECIES-KEM}(U)$ λαμβάνει ως είσοδο το δημόσιο κλειδί του παραλήπτη $U = u * g$ και λειτουργεί ως εξής:
    a. Επιλέγεται ένας τυχαίος αριθμός $z \in [1 \dots \mu)$.
    b. Υπολογίζονται τα στοιχεία $g' = z * g$ και $h' = z * U$.
    c. Υπολογίζεται το κρυπτογράφημα $C = E(g', format)$. Σημειώνεται ότι στο σχήμα ECIES-KEM ο αλγόριθμος ενθυλάκωσης λαμβάνει ως είσοδο μια προαιρετική μεταβλητή $format$, η οποία καθορίζει τη μορφή κωδικοποίησης για τα στοιχεία της ομάδας.
    d. Υπολογίζεται το κρυπτογράφημα $C' = E'(h')$.
    e. Υπολογίζεται το κλειδί κρυπτογράφησης βάση της συνάρτησης KDF, λαμβάνοντας ως είσοδο τις τιμές που υπολογίστηκαν στα προηγούμενα βήματα και το μήκος κλειδιού που πρόκειται να δημιουργηθεί, $K = KDF(C||C', KeyLen)$.
    f. Ο αλγόριθμος τερματίζει εφόσον υπολογιστεί το κρυπτογράφημα C και το μυστικό κλειδί K.



Εικόνα 4.9: Ενθυλάκωση κλειδιού στον μηχανισμό ECIES-KEM σύμφωνα με το πρότυπο ISO.

3. Ο αλγόριθμος $Decapsulate_{ECIES-KEM}(u, C)$ λαμβάνει ως είσοδο το ιδιωτικό κλειδί, $u \in [1 \dots \mu)$ και το κρυπτογράφημα C και λειτουργεί ως εξής:
    a. Υπολογίζεται το στοιχείο $g' = D(C) \in H$, ελέγχοντας αν το κρυπτογράφημα C έχει κατάλληλη μορφή κωδικοποίησης. Σε διαφορετική περίπτωση ο αλγόριθμος τερματίζει και επιστρέφεται μήνυμα σφάλματος.
    b. Αν $CheckMode = 1$, ελέγχεται αν $g' \in G$. Σε διαφορετική περίπτωση ο αλγόριθμος τερματίζει την λειτουργία του και επιστρέφεται μήνυμα σφάλματος.
    c. Αν $CofactorMode = 1$, τότε υπολογίζεται το στοιχείο $g'' = \nu * g'$ και το στοιχείο $u' = \nu^{-1} u \; mod \; \mu$, όπου u είναι το ιδιωτικό κλειδί του παραλήπτη. Διαφορετικά, τίθεται $g'' = g'$ και $u' = u$.
    d. Υπολογίζεται το στοιχείο $\mathrm{h}' = u' g''$. Παράλληλα, ελέγχεται αν $h' = 0$. Στην περίπτωση αυτή ο αλγόριθμος τερματίζει και επιστρέφεται μήνυμα σφάλματος.
    e. Υπολογίζεται το κρυπτογράφημα $C' = E'(h')$.
    f. Υπολογίζεται το κλειδί ενθυλάκωσης $K = KDF(C||C', KeyLen)$.
    g. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το μυστικό κλειδί K.



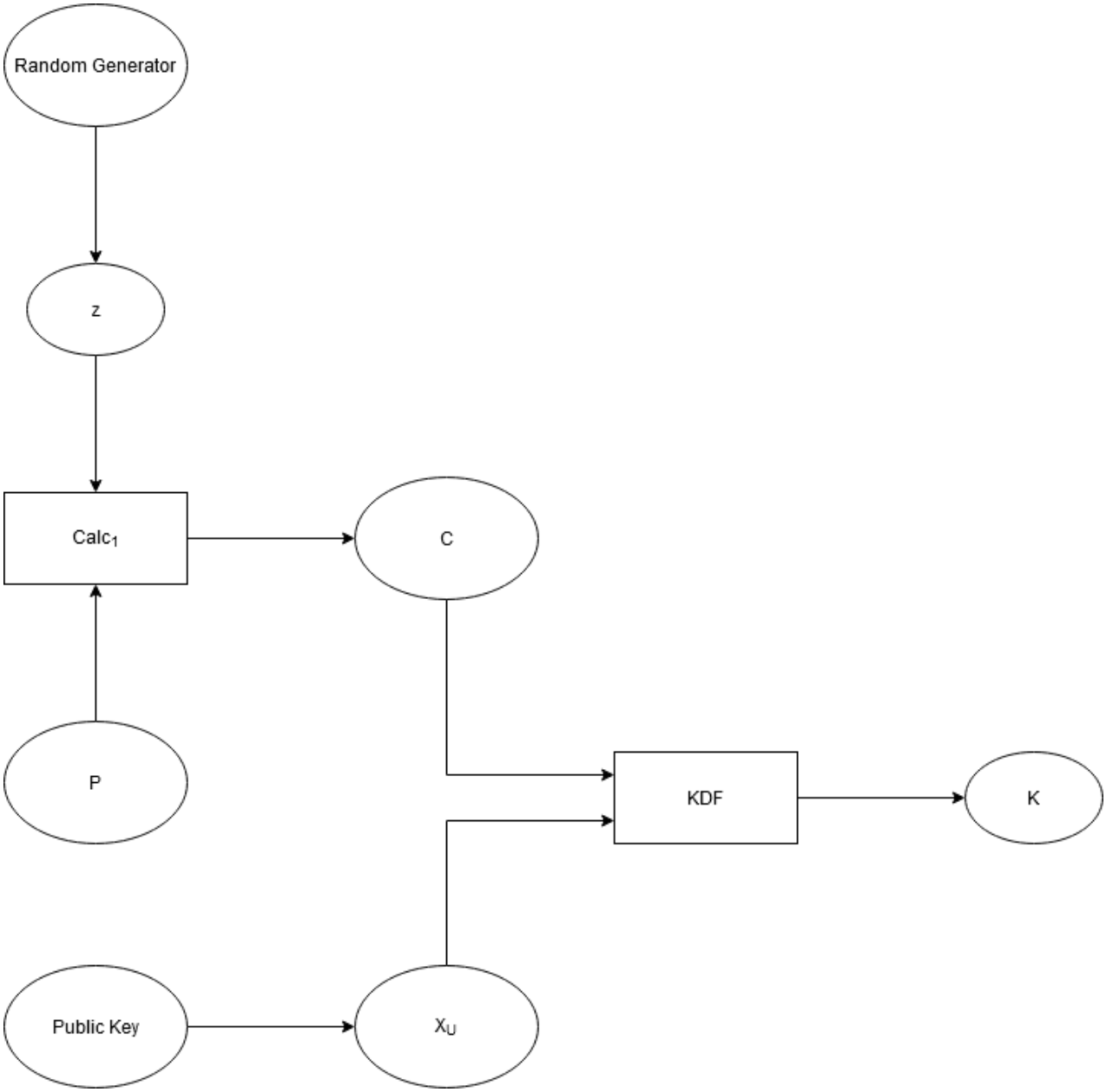
Εικόνα 4.10: Απενθυλάκωση με το ECIES-KEM.

Η παραπάνω περιγραφή του σχήματος ECIES-KEM, όπως αναφέρθηκε, αφορά την λειτουργία του μηχανισμού λαμβάνοντας υπόψη την ομάδα Γ, όπως αναγράφεται στο πρότυπο ISO [33]. Μιας και το σχήμα αφορά υπολογισμούς σε ελλειπτικές καμπύλες, η λειτουργία του μπορεί να γενικευτεί πέρα από την ομάδα Γ ως εξής [56]:

1. Ο αλγόριθμος $Generate_{ECIES-KEM}()$ αποφέρει το ζεύγος (U, u) βάση της τυπικής διαδικασίας δημιουργίας ζεύγους κλειδιών σε ελλειπτικές καμπύλες, όπου η τιμή U αποτελεί το δημόσιο κλειδί ενός χρήστη, ενώ η τιμή u το αντίστοιχο ιδιωτικό. Ο μηχανισμός ECIES-KEM, όπως και ο ECIES, είναι ένα σχήμα ελλειπτικών καμπυλών. Επομένως, πρέπει να έχει δημιουργηθεί μια κατάλληλη ελλειπτική καμπύλη E και να επιλεχθεί ένα σημείο $P \in E$ πρώτης τάξης p. Ειδικότερα, ο αλγόριθμος δημιουργίας κλειδιού λειτουργεί ως εξής:
    a. Επιλέγεται ένας τυχαίος ακέραιος αριθμός $u \in [1 \dots p)$.
    b. Υπολογίζεται το δημόσιο κλειδί $U = u * P$
    c. Ο ακέραιος αριθμός u αποτελεί το ιδιωτικό κλειδί του χρήστη, ενώ το στοιχείο U, το αντίστοιχο δημόσιο κλειδί. Στην πράξη το δημόσιο κλειδί αποτελείται από την τετράδα (E, P, p, U).
2. Ο αλγόριθμος $Encapsulate_{ECIES-KEM}(U)$ λαμβάνει ως είσοδο το δημόσιο κλειδί του παραλήπτη $U = u * P$ και λειτουργεί ως εξής:
    a. Επιλέγεται ένας τυχαίος αριθμός $z \in [1 \dots p)$.
    b. Υπολογίζεται το σημείο $C = z * P$.
    c. Λαμβάνεται η μεταβλητή x, η οποία αποτελεί την x-συντεταγμένη του σημείου U.
    d. Υπολογίζεται το κλειδί ενθυλάκωσης βάση της συνάρτησης KDF, λαμβάνοντας ως είσοδο τις τιμές C, x (που υπολογίστηκαν στα προηγούμενα βήματα) και το

μήκος του κλειδιού που οι δύο χρήστες πρόκειται να δημιουργήσουν, $K = KDF(C||x, KeyLen)$.

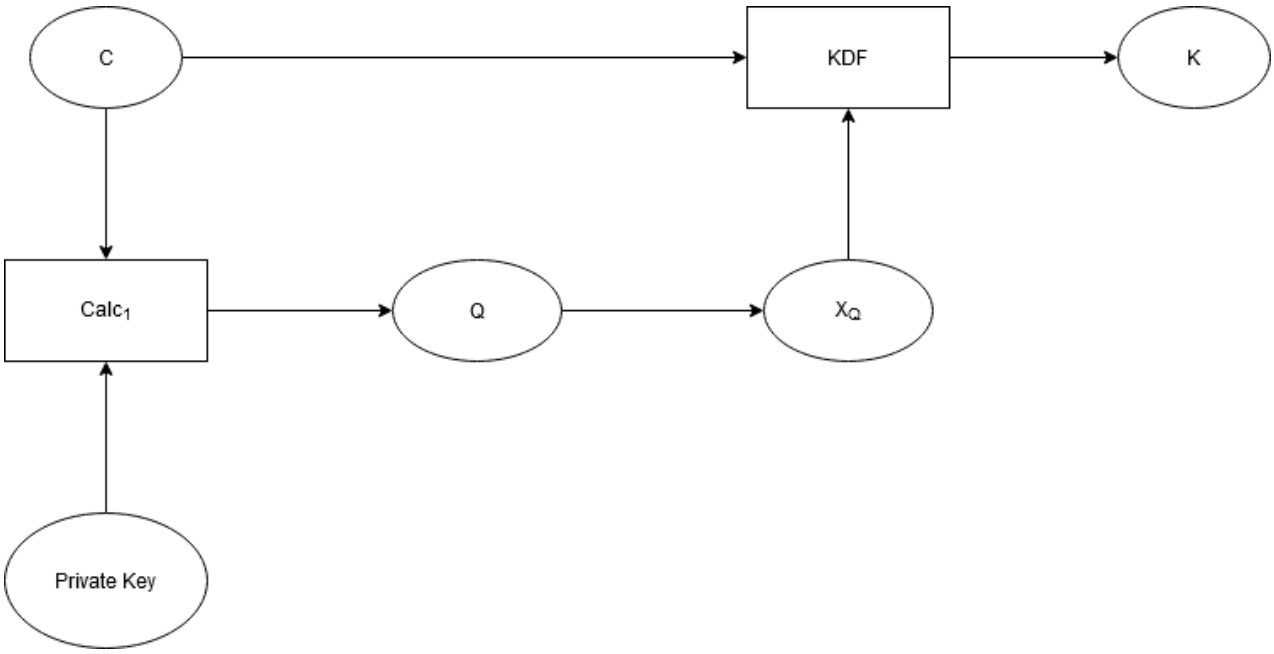
e. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το κρυπτογράφημα C και το μυστικό κλειδί K.



3. Ο αλγόριθμος $Decapsulate_{ECIES-KEM}(u, C)$ λαμβάνει ως είσοδο το ιδιωτικό κλειδί του παραλήπτη, $u \in [1 \dots p)$ και το κρυπτογράφημα C και λειτουργεί ως εξής:
   a. Υπολογίζεται το στοιχείο $Q = u * C$. Σε περίπτωση που το στοιχείο Q εμπίπτει στο ταυτοτικό σημείο 0, ο αλγόριθμος τερματίζει την λειτουργία του αποφέροντας μήνυμα σφάλματος.
   b. Λαμβάνεται η μεταβλητή μεταβλητή x, η οποία αποτελεί την x-συντεταγμένη του σημείου Q.

c. Υπολογίζεται το κλειδί απενθυλάκωσης βάση της συνάρτησης KDF, λαμβάνοντας ως είσοδο το κρυπτογράφημα C, την μεταβλητή x και το μήκος του κλειδιού που οι δύο χρήστες θέλουν να συμφωνήσουν, $K = KDF(C||x, KeyLen)$.

d. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το μυστικό κλειδί K.



4.3.1 Ασφάλεια ECIES-KEM

Όπως αναφέρθηκε, το σχήμα ECIES-KEM αποτελεί μια παραλλαγή του σχήματος ECIES, καθώς και μοιάζει αρκετά με το σχήμα PSEC-3. Έτσι, το σχήμα μπορεί να αποδειχτεί ότι είναι ασφαλές, υποθέτοντας πως το πρόβλημα gap-CDH είναι δύσκολο να επιλυθεί [49]. Σαφώς, για απόδειξη ασφαλείας απαιτείται η δυσκολία αντιστροφής της συνάρτησης KDF. Επομένως, η ασφάλεια του ECIES-KEM βασίζεται στην υπόθεση ότι το πρόβλημα gap-CDH είναι υπολογιστικά αδύνατο, καθώς και στην υπόθεση ότι η συνάρτηση KDF ικανοποιεί τις απαιτήσεις μιας συνάρτησης κατακερματισμού.

Για την απόδειξη ασφαλείας στο μοντέλο IND-CCA αρκεί να αποδειχτεί ότι $Adv_{ECIES-KEM}(A) = O(Adv_{gap-CDH}(A', q_{KDF})$, όπου:

- A' είναι ένας αλγόριθμος επίλυσης του προβλήματος DDH, του οποίου ο χρόνος εκτέλεσης είναι ίδιος με αυτόν του A.
- q_{KDF} είναι ο μέγιστος αριθμός ερωτημάτων.
- $Adv_{gap-CDH}$ είναι το πλεονέκτημα νίκης έναντι του προβλήματος gap-CDH.

Σημειώνεται ότι με την περιγραφή του αλγορίθμου σύμφωνα με το πρότυπο ISO υπάρχουν δύο επιπλέον μεταβλητές στο σχήμα ECIES-KEM, το οποίο ορίζεται στην ομάδα Γ και ειδικότερα η $CofactorMode$ και η $CheckMode$. Σύμφωνα με την περιγραφή αυτή και αν μια από τις δύο προαναφερθείσες μεταβλητές ισούται με 1, η ασφάλεια του ECIES-KEM σχετίζεται με την μεταβλητή v της ομάδας Γ και συγκεκριμένα, $Adv_{ECIES-KEM}(A) = O(v * Adv_{gap-CDH}(A', q_{KDF})$.

Υποθέτοντας ότι υπάρχει ένας επιτιθέμενος A έναντι της IND-CCA ασφάλειας του ECIES-KEM ο οποίος έχει το πλεονέκτημα $Adv_{ECIES-KEM}(A)$ και πραγματοποιεί τα μέγιστα q_D ερωτήματα απενθυλάκωσης και q_{KDF} ερωτήματα στην συνάρτηση KDF, τότε υπάρχει ένας αλγόριθμος A' του οποίου ο χρόνος εκτέλεσης είναι ίδιο με αυτόν του A και επιλύει το πρόβλημα gap-CDH.

Για την απόδειξη ασφαλείας του σχήματος ECIES μοντελοποιούμε ένα παιχνίδι IND-CCA, όπως σε όλες τις περιπτώσεις αξιολόγησης ασφαλείας κρυπτοσυστημάτων δημοσίου κλειδιού. Για την απόδειξη αυτή λαμβάνουμε υπόψη την γενική περίπτωση υλοποίησης και λειτουργίας του σχήματος ECIES-KEM, χωρίς τον περιορισμό της ομάδας Γ. Υποθέτοντας ότι ένας επιτιθέμενος έχει πρόσβαση την τριπλέτα (P, aP, bP), η οποία αντιστοιχεί σε σημεία της ελλειπτικής καμπύλης E, όπου $P \in E$ είναι ένα σημείο πρώτης τάξης p, σκοπός είναι τα υπολογιστεί το σημείο abP.

Για την έναρξη του παιχνιδιού ορίζεται ως δημόσιο κλειδί το σημείο $U = aP$ και στην πράξη το δημόσιο κλειδί αποτελείται από την εξίσωση της ελλειπτικής καμπύλης E, το σημείο $P \in E$, την τάξη p και το σημείο W, $PK = (E, P, p, W)$. Στην συνέχεια ετοιμάζονται δύο λίστες $DecList$ και $KDFList$. Τέλος, επιτρέπεται στον αλγόριθμο A να εκτελεστεί μέχρι να είναι σε θέση να λάβει μια πρόκληση.

Σε περίπτωση που ο αλγόριθμος A αποστείλει ερώτημα απενθυλάκωσης για μια ενθυλάκωση C τότε ελέγχεται αν το ζεύγος (C, K) βρίσκεται στην λίστα $DecList$ και αν ναι, τότε επιστρέφεται το κλειδί ενθυλάκωσης K. Σε διαφορετική περίπτωση, επιλέγεται ένα τυχαίο δημιουργημένο κλειδί K και εισάγεται το ζεύγος (C, K) στην $DecList$.

Εναλλακτικά, αλγόριθμος A μπορεί να αποστείλει ερώτημα κατακερματισμού στην συνάρτηση KDF για μια είσοδο X. Αν το ζεύγος (X, K) βρίσκεται στη λίστα $KDFList$ τότε επιστρέφεται το κλειδί ενθυλάκωσης K. Σε διαφορετική περίπτωση, ο επιτιθέμενος αναλύει την είσοδο X ως η συνένωση ενός σημείου και μιας x-συντεταγμένης, $X = C||x$, όπου C είναι ένα σημείο της ελλειπτικής καμπύλης και x είναι η x-συντεταγμένη ενός σημείου στην ελλειπτική καμπύλη. Αν η ανάλυση δεν μπορεί να πραγματοποιηθεί τότε επιλέγει τυχαία ένα κλειδί K, το οποίο προστίθεται στην λίστα $KDFList$ ως ζεύγος (X, K). Στην συνέχεια υπολογίζονται δύο σημεία Q και $-Q$, τα οποία έχουν x-συντεταγμένη την παραπάνω μεταβλητή x, $Q_x = x$ και ελέγχεται αν η τετράδα (P, aP, C, Q) αποτελεί έγκυρη τριπλέτα Diffie-Hellman χρησιμοποιώντας το gap oracle. Στην πράξη ελέγχεται αν υπάρχει c τέτοιο ώστε $C = cP$ και $Q = acP$. Αν η τετράδα δεν αποτελεί έγκυρη τριπλέτα Diffie-Hellman τότε επιλέγεται ένα τυχαίο κλειδί K και εισάγεται ως ζεύγος (X, K) στην λίστα $KDFList$.

Υποθέτοντας ότι η τετράδα (P, aP, C, Q) αποτελεί έγκυρη τριπλέτα και αν $\mathrm{C} = bP$, τότε το σημείο Q αποτελεί την λύση στο πρόβλημα gap-CDH. Επομένως, καταλήγουμε ότι αν ο αλγόριθμος A μπορεί να αποστείλει ερώτημα απενθυλάκωσης για το C, τότε πρέπει να επιστρέφεται $KDF(X)$, ώστε να επιλεχθεί ένα τυχαίο K και να προστεθεί το ζεύγος (X, K) στην λίστα $KDFList$ και το ζεύγος (C, K) στην $DecList$.

Όταν ο αλγόριθμος A είναι έτοιμος να δεχθεί μια πρόκληση ενθυλάκωσης επιλέγεται τυχαία ένα κλειδί K και επιστρέφεται το ζεύγος (K, C). Στην συνέχεια επιτρέπουμε στον A να εκτελεστεί απαντώντας σε οποιοδήποτε ερώτημα με την προυπόθεση ότι δεν θα ζητηθεί απενθυλάκωση του bP.

Έστω ότι S είναι το ενδεχόμενο στο οποίο έχει ερωτηθεί η μεταβλητή $bP||x$, όπου x είναι η x-συντεταγμένη του σημείο abP. Μέχρι να συμβεί αυτό, ο αλγόριθμος A, δεν έχει πλεονέκτημα απόφασης για το ζεύγος (K, bP), αποτελεί μια έγκυρη ενθυλάκωση διότι δεν είναι σε θέση να γνωρίζει την έξοδο της KDF. Όταν το ενδεχόμενο S συμβεί, τότε ο αλγόριθμος τερματίζεται και επιστρέφεται η τιμή abP. Η πιθανότητα να συμβεί το S είναι τουλάχιστον ίδιο με την πιθανότητα νίκης έναντι του ECIES-KEM και επομένως η πιθανότητα να επιτύχει ο αλγόριθμος A' είναι ίδια με αυτή νίκης στο ECIES-KEM.

4.4 PSEC-KEM

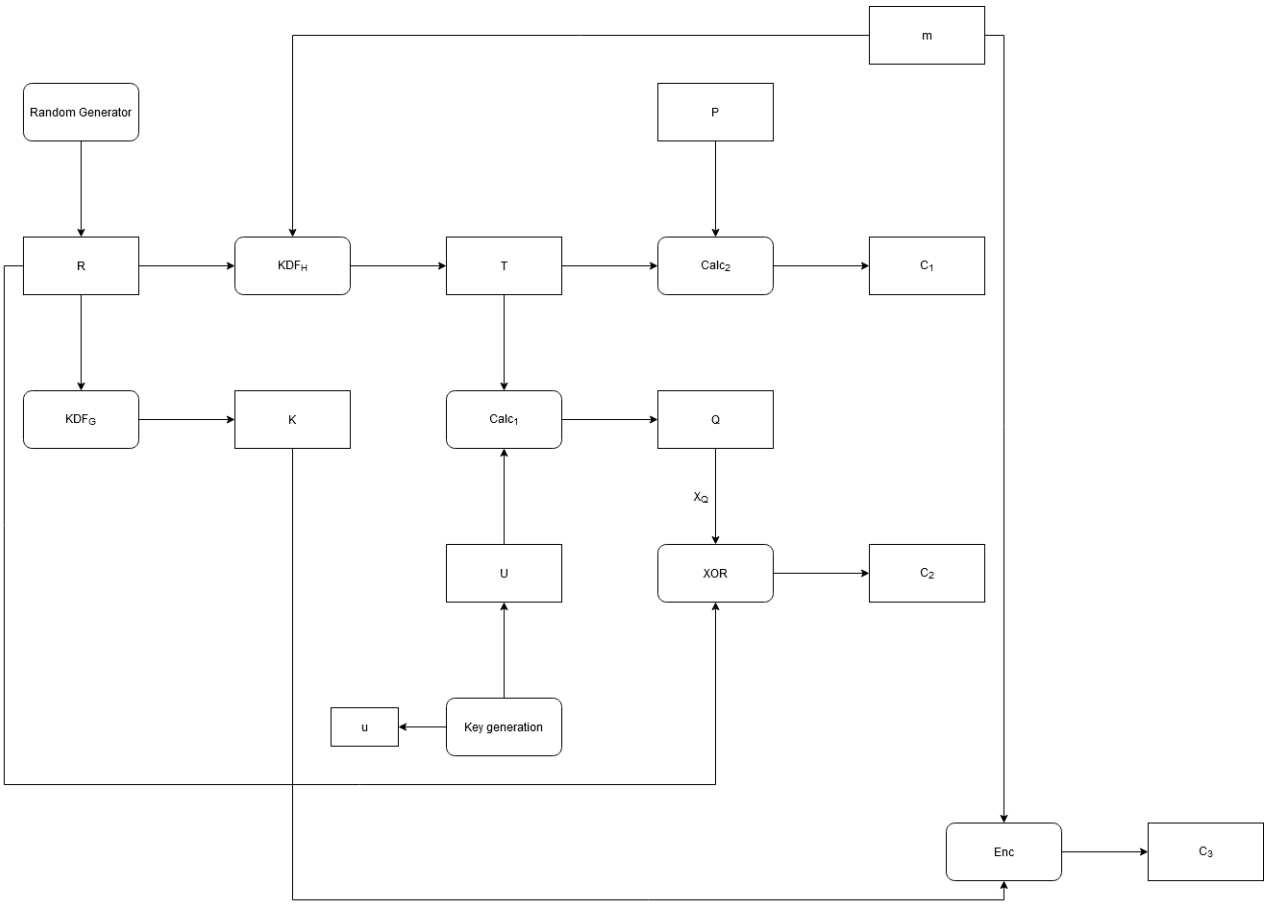
Το σχήμα PSEC-KEM που έχει προταθεί ως πρότυπο ISO αποτελεί μια παραλλαγή του σχήματος PSEC-2 [33]. Για καλύτερη περιγραφή και κατανόηση του PSEC-KEM, αρχικά, αναφέρουμε την λειτουργία του κρυπτοσυστήματος PSEC-2. Οι παράμετροι του σχήματος είναι οι εξής [57]:

1. Συνάρτηση Δημιουργίας Κλειδιού (KDF): Το σχήμα PSEC-2, όπως και το PSEC-3 που συζητήθηκε στην προηγούμενη ενότητα, χρησιμοποιεί δύο συναρτήσεις KDF (συναρτήσεις κατακερματισμού), την KDF_G και την KDF_H. Η πρώτη, εξάγει το κλειδί που πρόκειται να χρησιμοποιηθεί στην διαδικασία κρυπτογράφησης, ενώ η KDF_H χρησιμοποιείται για την εξαγωγή δεδομένων αυθεντικοποίησης.
2. Κρυπτογράφηση (E): Αλγόριθμος συμμετρικής κρυπτογράφησης/αποκρυπτογράφησης. Στην πράξη ο αλγόριθμος αυτός αποτελείται από το ζεύγος αλγορίθμων κρυπτογράφησης και αποκρυπτογράφησης. Ο αλγόριθμος κρυπτογράφησης λαμβάνει ως είσοδο το κλειδί K που δημιουργείται από την KDF_G και ένα αρχικό μήνυμα και επιστρέφει το αντίστοιχο κρυπτογράφημα. Αντίστοιχα, ο αλγόριθμος αποκρυπτογράφησης λαμβάνει ως είσοδο το κρυπτογράφημα και το κλειδί K και επιστρέφει το αρχικό μήνυμα.

Υποθέτοντας ότι δύο χρήστες που έχουν ήδη δημιουργήσει το ζεύγος κλειδιών τους, (U, u) και (V, v), αντίστοιχα, πάνω σε μια ελλειπτική καμπύλη E, επιθυμούν να εδραιώσουν μια ασφαλή επικοινωνία μεταξύ τους. Υπενθυμίζεται ότι για τον ορισμό μιας ελλειπτικής καμπύλης E, επιλέγεται ένα πεπερασμένο σώμα F_q, οι συντελεστές $a, b \in F_q$, ένας πρώτος αριθμός p, ο οποίος διαιρεί τον αριθμό των σημείων της ελλειπτικής καμπύλης και ένα σημείο P τάξης p. Τέλος, για την δημιουργία των κλειδιών επιλέγεται ένας τυχαίος αριθμός d και υπολογίζεται το σημείο $U = dP$, όπου το U αποτελεί το δημόσιο κλειδί του χρήστη και d το αντίστοιχο ιδιωτικό. Τα βήματα που ακολουθούνται για την λειτουργία του σχήματος PSEC-2 είναι τα εξής:

- Ο πρώτος χρήστης δημιουργεί ένα επίκαιρο ζεύγος δημοσίου-ιδιωτικού κλειδιού (U, u).
- Αφού έχει δημιουργηθεί το ζεύγος δημοσίου-ιδιωτικού κλειδιού, επιλέγονται τυχαία ένας αριθμός $R \in \{0,1\}^{rLen}$, όπου $rLen \leq qLen$, όπου $qLen$ είναι το μέγεθος $|q|$ της τάξης q του πεπερασμένου πεδίου F_q και r $\in \mathbb{Z}_p^*$.
- Υπολογίζεται το κλειδί κρυπτογράφησης $K = KDF_G(R)$. Σημειώνεται ότι η συνάρτηση KDF_G υλοποιείται με τρόπο ώστε να μετατρέπει έναν αριθμό $a \in \{0,1\}^{rlen}$ στο $a' \in \{0,1\}^{qLen}$, όπου $qLen$, είναι το μέγεθος του κλειδιού που πρόκειται να δημιουργηθεί.

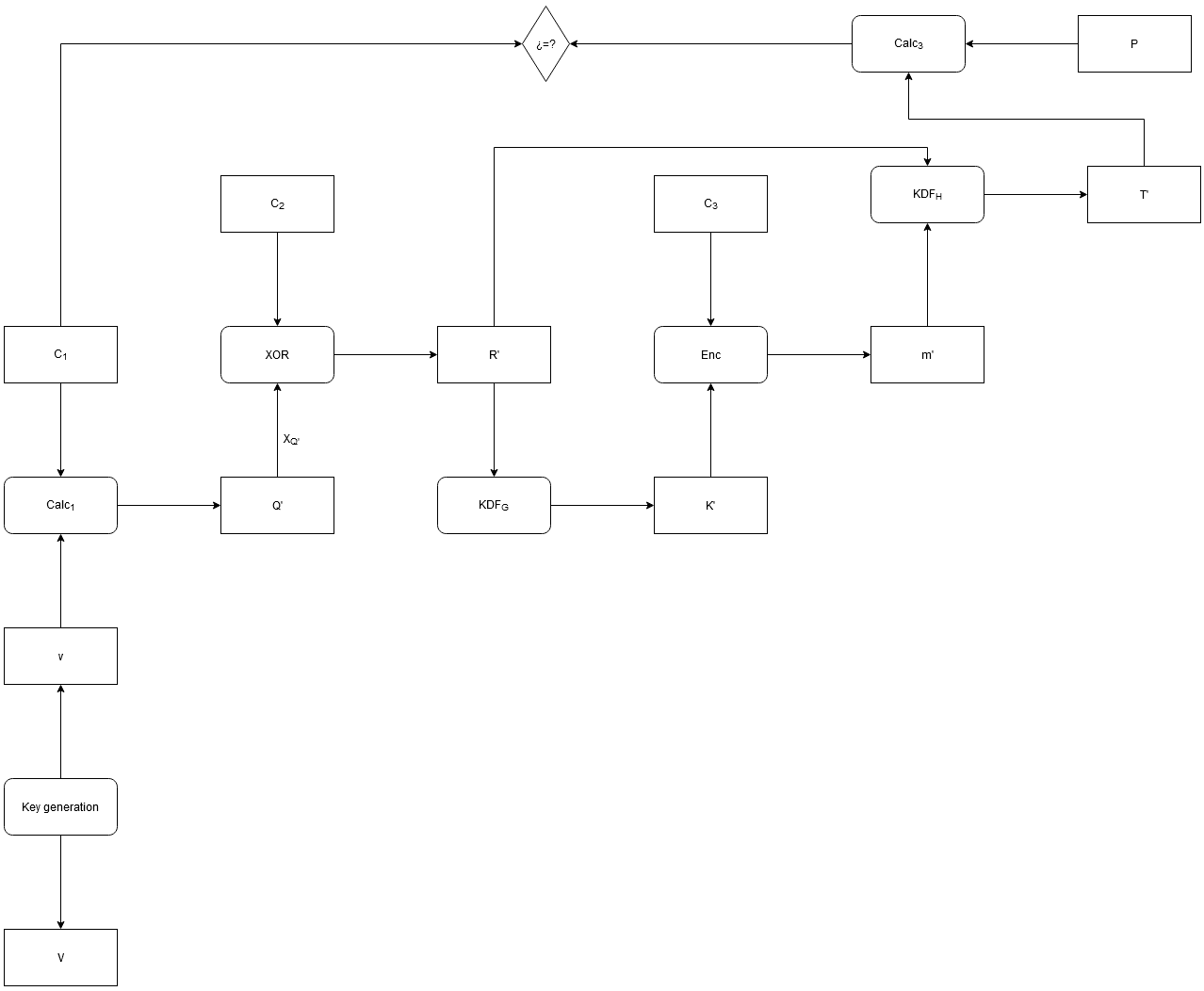
- Υπολογίζεται η ετικέτα $T = KDF_H(m||R)$, όπου m είναι το αρχικό μήνυμα. Σημειώνεται ότι η συνάρτηση KDF_H υλοποιείται με τέτοιο τρόπο ώστε να μετατρέπει έναν αριθμό $a \in \{0,1\}^{mLen+rLen}$ στο $a' \in \{0,1\}^{hLen}$, όπου $hLen$, είναι το μέγεθος της ετικέτας που δημιουργείται.
- Στην συνέχεια, υπολογίζονται τα σημεία της ελλειπτικής καμπύλης $Q = TU$ και $C_1 = TP$.
- Υπολογίζεται η τιμή $C_2 = R \oplus \mathrm{x}_Q$, όπου x_Q είναι η x-συντεταγμένη του σημείου Q.
- Το κλειδί K που υπολογίστηκε χρησιμοποιείται για την συμμετρική κρυπτογράφηση του αρχικού μηνύματος m, $C_3 = E(K, m)$.
- Αποστέλλεται στον παραλήπτη μια τιμή που αποτελείται από το δημόσιο κλειδί U του αποστολέα, το σημείο C_1, την τιμή C_2 και το κρυπτογράφημα C_3, $Output = (U, C_1, C_2, C_3)$.



Όσον αφορά την διαδικασία αποκρυπτογράφησης, στην πλευρά του παραλήπτη, αφού γίνει λήψη της τιμής $Output$, πραγματοποιούνται τα εξής:

- Γίνεται ανάκτηση του δημοσίου κλειδιού του αποστολέα U, του σημείου C_1 που υπολογίστηκε στην πλευρά του παραλήπτη, της τιμής C_2 και του κρυπτογραφημένου μηνύματος C_3.
- Υπολογίζεται το σημείο της ελλειπτικής καμπύλης $Q' = vC_1$, με την χρήση του ιδιωτικού κλειδιού v του παραλήπτη και σημείου C_1.

- Εφόσον πραγματοποιηθεί ο υπολογισμός του σημείου Q', ο αποστολέας είναι σε θέση να υπολογίσει την τιμή $R' = C_2 \oplus \mathrm{x}_{Q'}$, όπου x_q, είναι η x-συντεταγμένη του σημείου Q'.
- Στην συνέχεια, υπολογίζεται το κλειδί K' βάση της συνάρτησης KDF_G, $K' = KDF_G(R')$.
- Η διαδικασία συνεχίζει με την αποκρυπτογράφηση του μηνύματος C_3, με την χρήση του κλειδιού που υπολογίστηκε από την συνάρτηση KDF_G, $m' = E(K', C_3)$.
- Πριν την επιστροφή της υπολογισμένης τιμής του αρχικού μηνύματος, υπολογίζεται η ετικέτα T' μέσω της συνάρτηση KDF_H, $T' = KDF_H(m'|R')$ και ελέγχεται αν ισχύει ότι $C_1 = T'P$. Σε περίπτωση που οι τιμές είναι διαφορετικές, ο παραλήπτης απορρίπτει την επικοινωνία λόγω σφάλματος στην ετικέτα T. Διαφορετικά, επιστρέφεται το αρχικό μήνυμα m.



Όσον αφορά την ασφάλεια του κρυπτοσυστήματος PSEC-2, έχει αποδειχτεί ότι είναι ασφαλές στο μοντέλο IND-CCA, με την προϋπόθεση ότι το πρόβλημα CDH σε ελλειπτικές καμπύλες είναι υπολογιστικά αδύνατο να επιλυθεί [57].

Όπως αναφέρθηκε προηγουμένως, το σχήμα PSEC-KEM αποτελεί παραλλαγή του PSEC-2. Σύμφωνα με το πρότυπο ISO που προτάθηκε από τον Shoup [33] ο μηχανισμός PSEC-KEM αποτελείται από τις εξής παραμέτρους:

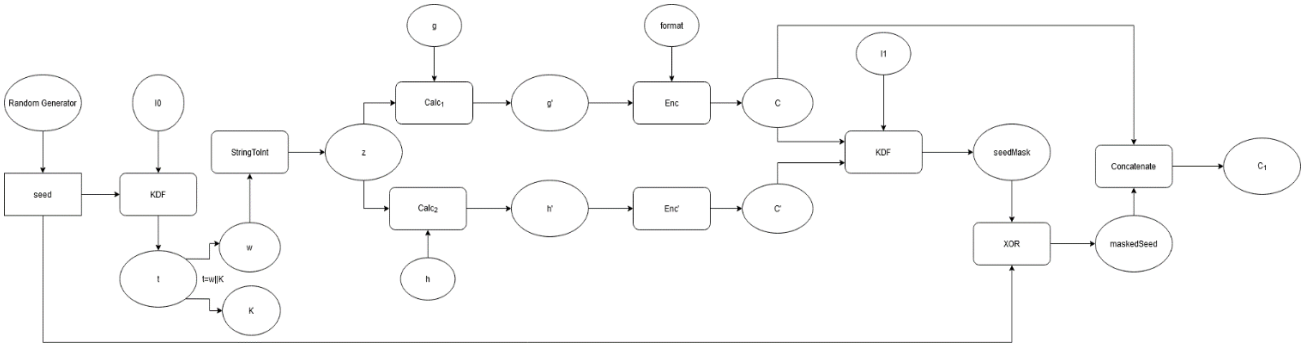
1. Ομάδα $\Gamma = (H, G, g, \mu, \nu, E, D, E', D')$, όπως αυτή ορίστηκε στην αρχή του κεφαλαίου.
2. Συνάρτηση Δημιουργίας Κλειδιού (KDF): μια συνάρτηση κατακερματισμού, όπως παρουσιάστηκε στην αρχή του κεφαλαίου.
3. Μήκος τυχαίας τιμής (seedLen): ένας θετικός ακέραιος αριθμός.
4. Μήκος Κλειδιού (keyLen): ένας θετικός ακέραιος αριθμός.

Βάση των παραπάνω παραμέτρων, η λειτουργία του PSEC-KEM έχει ως εξής:

1. Ο αλγόριθμος $Generate_{PSEC-KEM}()$ αποφέρει το ζεύγος (U, u) βάση του αλγορίθμου δημιουργίας κλειδιού, όπου η τιμή U αποτελεί το δημόσιο κλειδί ενός χρήστη, ενώ η τιμή u το αντίστοιχο ιδιωτικό. Ο αλγόριθμος δημιουργίας κλειδιού λειτουργεί ως εξής:
    a. Επιλέγεται ένας τυχαίος ακέραιος αριθμός $u \in [0 \dots \mu)$.
    b. Υπολογίζεται το σημείο $U = u * g$.
    c. Ο ακέραιος αριθμός u αποτελεί το ιδιωτικό κλειδί του χρήστη, ενώ το σημείο $U \in G$, το αντίστοιχο δημόσιο κλειδί.
2. Ο αλγόριθμος $Encapsulate_{PSEC-KEM}(U)$ λαμβάνει ως είσοδο το δημόσιο κλειδί του παραλήπτη $U = u * g$ και λειτουργεί ως εξής:
    a. Επιλέγεται ένα τυχαίο αλφαριθμητικό $seed$, μήκους $seedLen$.
    b. Υπολογίζεται η έξοδος της συνάρτησης KDF, $t = KDF(I0||seed, \lceil log_{256}\mu \rceil + 16 + keyLen)$, όπου $I0$ είναι ένα αλφαριθμητικό s μήκους 4 τέτοιο ώστε η συνάρτηση μετατροπής του s σε ακέραιο αριθμό να επιστρέφει τον αριθμό 0, $StringToInt(s) = 0$ και $\lceil log_{256}\mu \rceil$ είναι ο μικρότερος θετικός ακέραιος i τέτοιος ώστε $i \geq log_{256}\mu$ (για παράδειγμα, $\lceil 5 \rceil = 5, \lceil 5.3 \rceil = 6, \lceil -5.3 \rceil = -5$). Σημειώνεται ότι $\lceil log_{256}\mu \rceil + 16 + keyLen$ αναπαριστά το μήκος της ετικέτας που δημιουργείται.
    c. Η προηγούμενη υπολογισμένη τιμή t αναλύεται ως $t = w||K$, όπου w είναι ένα αλφαριθμητικό μεγέθους $\lceil log_{256}\mu \rceil + 16$ και K είναι μεγέθους $keyLen$.
    d. Υπολογίζεται η τιμή $z = StringToInt(w)\ mod\ \mu$.
    e. Υπολογίζονται τα σημεία της ελλειπτικής καμπύλης $g' = zg$ και $h' = zh$.
    f. Υπολογίζεται το κρυπτογράφημα $C = E(g', format)$. Σημειώνεται ότι στο σχήμα PSEC-KEM ο αλγόριθμος ενθυλάκωσης λαμβάνει ως είσοδο μια προαιρετική μεταβλητή $format$, η οποία καθορίζει τη μορφή κωδικοποίησης για τα στοιχεία της ομάδας.
    g. Υπολογίζεται το κρυπτογράφημα $C' = E'(h')$.
    h. Υπολογίζεται η τιμή $seedMask = KDF(I1||C||C', seedLen)$, όπου $I1$ είναι ένα αλφαριθμητικό s' μεγέθους τέτοιο ώστε η συνάρτηση μετατροπής του s' σε ακέραιο αριθμό να επιστρέφει τον αριθμό 1.
    i. Υπολογίζεται η τιμή $maskedSeed = seed \oplus seedMask$.

j. Υπολογίζεται η τιμή $C_1 = C||maskedSeed$.

k. Ο αλγόριθμος τερματίζει εφόσον υπολογιστεί το κρυπτογράφημα C_1 και το κλειδί K.



3. Ο αλγόριθμος $Decapsulate_{PSEC-KEM}(u, C_1)$ λαμβάνει ως είσοδο το ιδιωτικό κλειδί, $u \in [0 \dots \mu)$ και το κρυπτογράφημα C_1:

   a. Αναλύεται το κρυπτογράφημα C_1 ως $C_1 = C||maskedSeed$, όπου C είναι η κωδικοποίηση του στοιχείου g' και $maskedSeed$ είναι ένα αλφαριθμητικό μεγέθους $seedLen$. Γίνεται εύκολα αντιληπτό ότι το βήμα αυτό αποτυγχάνει αν $|C| < seedLen$.

   b. Υπολογίζεται το σημείο g' από την διαδικασία αποκωδικοποίησης $g' = D(C)$. Το βήμα αυτό αποτυγχάνει αν το στοιχείο C δεν αποτελεί έγκυρη κωδικοποίηση.

   c. Υπολογίζεται το σημείο $h' = ug'$.

   d. Υπολογίζεται το κρυπτογράφημα $C' = E'(h')$.

   e. Υπολογίζεται η τιμή $seedMask = KDF(I1||C||C', seedLen)$

   f. Υπολογίζεται η τιμή $seed = maskedSeed \oplus seedMask$.

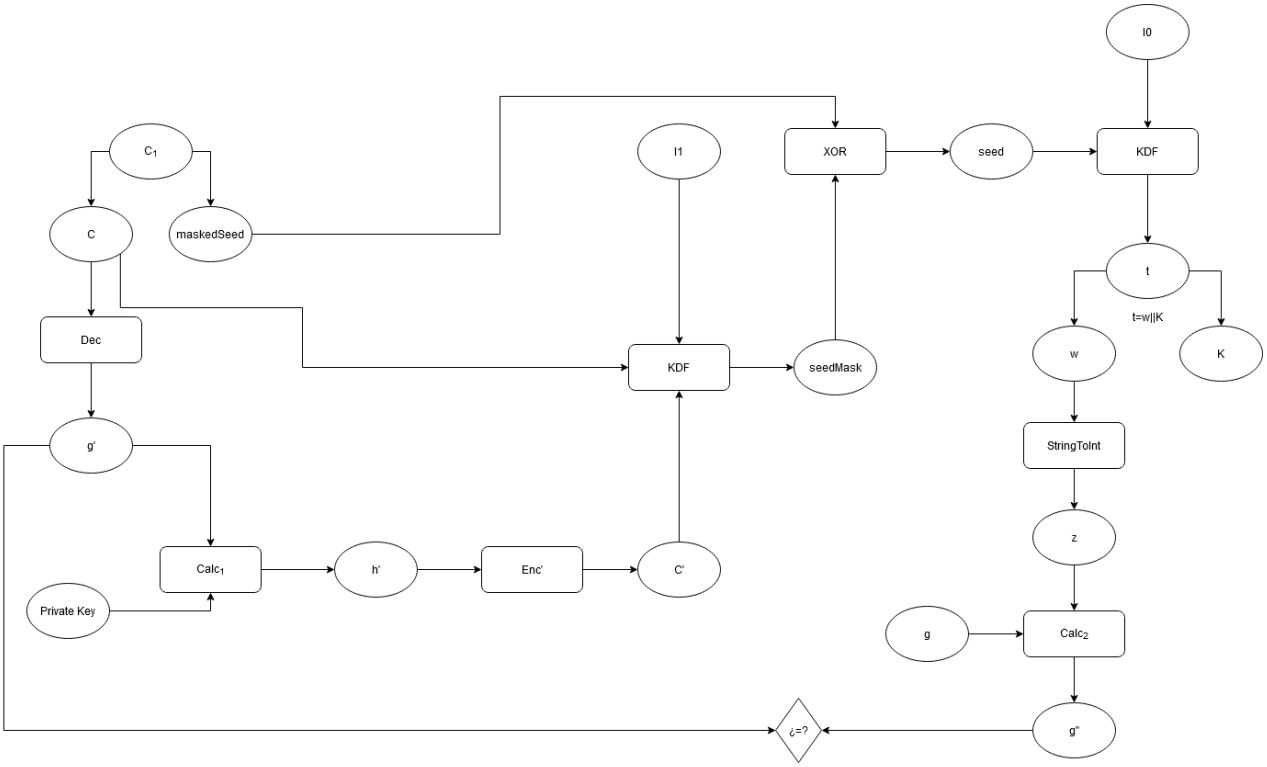
   g. Υπολογίζεται η ετικέτα $t = KDF(I0||seed, \lceil log_{256}\mu \rceil + 16 + keyLen)$.

   h. Αναλύεται η ετικέτα t, ως $t = w||K$, όπου w είναι ένα αλφαριθμητικό μεγέθους $\lceil log_{256}\mu \rceil + 16$ και K είναι μεγέθους $keyLen$.

   i. Υπολογίζεται η τιμή $z = StringToInt(w)\ mod\ \mu$.

   j. Υπολογίζεται το σημείο $g'' = zg$ και ελέγχεται αν $g'' = g'$. Σε διαφορετική περίπτωση ο αλγόριθμος τερματίζει την λειτουργία του και επιστρέφεται μήνυμα σφάλματος.

   k. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το μυστικό κλειδί K.



Η παραπάνω περιγραφή του σχήματος PSEC-KEM, όπως αναφέρθηκε, αφορά την λειτουργία του μηχανισμού λαμβάνοντας υπόψη την ομάδα Γ, όπως αναγράφεται στο πρότυπο ISO [33]. Μιας και το σχήμα αφορά υπολογισμούς σε ελλειπτικές καμπύλες, η λειτουργία του μπορεί να γενικευτεί πέρα από την ομάδα Γ ως εξής [56]:

1. Ο αλγόριθμος $Generate_{PSEC-KEM}()$ αποφέρει το ζεύγος (U, u) βάση της τυπικής διαδικασίας δημιουργίας ζεύγους κλειδιών σε ελλειπτικές καμπύλες, όπου η τιμή U αποτελεί το δημόσιο κλειδί ενός χρήστη, ενώ η τιμή u το αντίστοιχο ιδιωτικό. Ο μηχανισμός PSEC-KEM, όπως και κρυπτοσύστημα PSEC-2 αποτελεί ένα σχήμα ελλειπτικών καμπυλών. Επομένως, πρέπει να έχει δημιουργηθεί μια κατάλληλη ελλειπτική καμπύλη E και να επιλεχθεί ένα σημείο $P \in E$ πρώτης τάξης p. Ειδικότερα, ο αλγόριθμος δημιουργίας κλειδιού λειτουργεί ως εξής:
    a. Επιλέγεται ένας τυχαίος ακέραιος αριθμός $u \in [1 \dots p)$.
    b. Υπολογίζεται το δημόσιο κλειδί $U = u * P$
    c. Ο ακέραιος αριθμός u αποτελεί το ιδιωτικό κλειδί του χρήστη, ενώ το στοιχείο U, το αντίστοιχο δημόσιο κλειδί. Στην πράξη το δημόσιο κλειδί αποτελείται από την τετράδα (E, P, p, U).
2. Ο αλγόριθμος $Encapsulate_{PSEC-KEM}(U)$ λαμβάνει ως είσοδο το δημόσιο κλειδί του παραλήπτη $U = u * P$ και λειτουργεί ως εξής:
    a. Επιλέγεται ένα τυχαίο αλφαριθμητικό $seed$ σταθερού μεγέθους $seedLen$.
    b. Υπολογίζεται το στοιχείο $H = KDF(0_{32}||seed)$, όπου 0_{32} αποτελεί την 32-bit αναπαράσταση του αριθμού 0.

c. Το στοιχείο H αναλύεται ως $H = t||K$ όπου t αποτελεί την ετικέτα μήκους $p + 128$ και K αποτελεί το κλειδί κατάλληλου μεγέθους που οι δύο χρήστες πρόκειται να συμφωνήσουν.

d. Υπολογίζεται το στοιχείο $z = t \bmod p$.

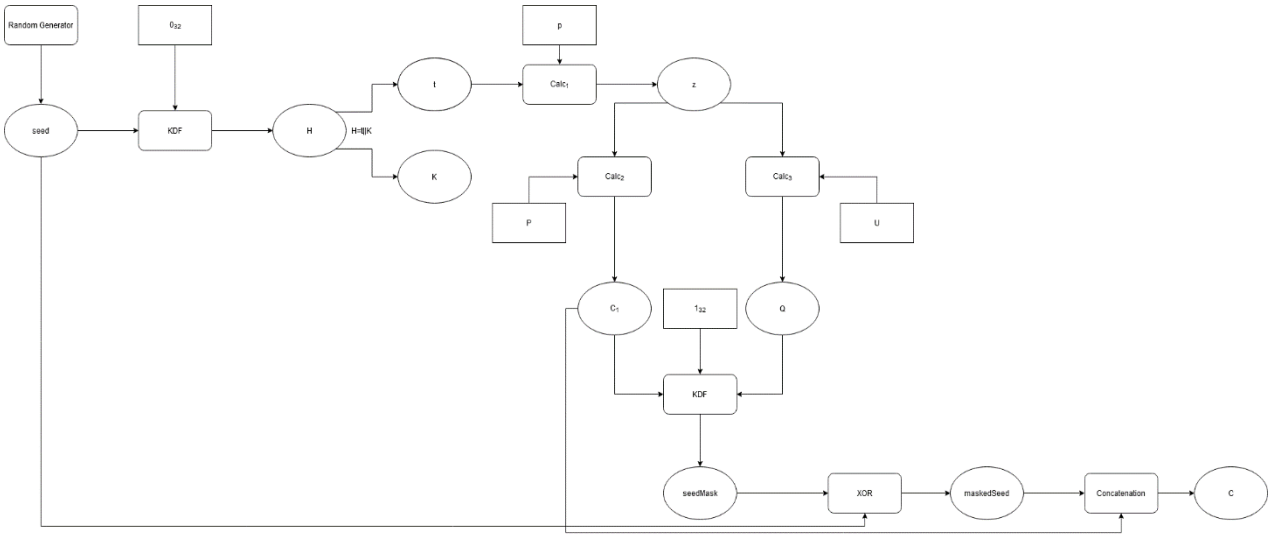
e. Υπολογίζονται τα σημεία της ελλειπτικής καμπύλης $Q = zU$ και $C_1 = zP$.

f. Υπολογίζεται η τιμή $seedMask = KDF(1_{32}||C_1||Q)$, όπου 1_{32} είναι η 32-bit αναπαράσταση του αριθμού 1.

g. Υπολογίζεται η τιμή $\mathrm{m}askedSeed = seed \oplus seedMask$.

h. Υπολογίζεται η τιμή $C = C_1||maskedSeed$.

i. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το κρυπτογράφημα C και το μυστικό κλειδί K.



3. Ο αλγόριθμος $Decapsulate_{PSEC-KEM}(u, C)$ λαμβάνει ως είσοδο το ιδιωτικό κλειδί του παραλήπτη, $u \in [1 \dots p)$ και το κρυπτογράφημα C και λειτουργεί ως εξής:

a. Αναλύεται το κρυπτογράφημα C, ως $C = C_1||maskedSeed$.

b. Υπολογίζεται το σημείο $Q = uC_1$.

c. Υπολογίζεται η μεταβλητή $seedMask = KDF(1_{32}||C_1||Q)$.

d. Υπολογίζεται η μεταβλητή $seed = maskedSeed \oplus seedMask$.

e. Υπολογίζεται το στοιχείο $H = KDF(0_{32}||seed)$.

f. Το στοιχείο H αναλύεται ως $H = t||K$ όπου t αποτελεί την ετικέτα μήκους $p + 128$ και K αποτελεί το κλειδί κατάλληλου μεγέθους που οι δύο χρήστες πρόκειται να συμφωνήσουν.

g. Υπολογίζεται το στοιχείο $z = t \bmod p$.

h. Ελέγχεται αν $C_1 = zP$.Σε διαφορετική περίπτωση ο αλγόριθμος τερματίζει και επιστρέφεται μήνυμα σφάλματος.

i. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το μυστικό κλειδί K.

4.4.1 Ασφάλεια PSEC-KEM

Όπως αναφέρθηκε, το σχήμα PSEC-KEM, αποτελεί παραλλαγή του κρυπτοσυστήματος PSEC-2, το οποίο βασίζεται στην δυσκολία επίλυσης του προβλήματος CDH [57]. Επομένως, η απόδειξη ασφαλείας του PSEC-KEM στηρίζεται στο δύσκολο αυτό πρόβλημα. Εκτός από το πρόβλημα CDH, όπως σε όλα τα σχήματα τύπου KEM η απόδειξη ασφαλείας βασίζεται στην δυσκολία αντιστροφής της συνάρτησης KDF. Επομένως η συνάρτηση KDF πρέπει να ικανοποιεί τις απαιτήσεις ασφαλείας μιας συνάρτησης κατακερματισμού.

Όπως παρουσιάστηκε προηγουμένως, στο σχήμα PSEC-KEM γίνεται χρήση της συνάρτησης KDF δύο φορές. Αρχικά, η KDF χρησιμοποιείται για την δημιουργία μιας ετικέτας t μεγέθους $\lceil log_{256}\mu \rceil + 16 + keyLen$, η οποία λαμβάνει ως είσοδο ένα αλφαριθμητικό μεγέθους 4 και το αλφαριθμητικό $seed$, μεγέθους $seedLen$. Στην συνέχεια η KDF χρησιμοποιείται για την δημιουργία της μεταβλητής $maskedSeed$, μεγέθους $seedLen$, η οποία λαμβάνει ως είσοδο τις εξόδους των συναρτήσεων E και E' και ένα αλφαρηθμητικό μεγέθους 4. Επομένως, έχουμε:

- $KDF_0 : S^{seedLen+4} \rightarrow S^{\lceil log_{256}\mu \rceil + 16 + keyLen}$, όπου S δηλώνει το αλφαρηθμητικό στην είσοδο και έξοδο αντίστοιχα.
- $KDF_1 : E(H) + E'(H) + S^4 \rightarrow S^{seedLen}$, όπου $E(H)$ δηλώνει το σύνολο όλων των κωδικοποίησεων των στοιχείων στο H και $E'(H)$ το σύνολο όλων των μερικών κωδικοποίησεων των στοιχείων στο H.

Για την μοντελοποίηση της IND-CCA ασφάλειας υποθέτουμε ότι υπάρχει ένας επιτιθέμενος A, στον οποίον επιτρέπεται να πραγματοποιήσει το μέγιστο qD ερωτήματα με σκοπό την αποκρυπτογράφηση του κρυπτογραφημένου μηνύματος C_1. Επιπλέον, θεωρούμε ότι q_0 συμβολίζει τον μέγιστο επιτρεπόμενο αριθμό ερωτημάτων στην KDF_0 και q_1 δηλώνει τον μέγιστο επιτρεπόμενο αριθμό ερωτημάτων στην KDF_1.

Για την απόδειξη ασφαλείας στο μοντέλο IND-CCA θεωρούμε πως υπάρχει μια σειρά παιχνιδιών G_i για τα οποία ο επιτιθέμενος A πραγματοποιεί μια επίθεση. Κάθε ένα από τα παιχνίδια λαμβάνει χώρα σε ένα χώρο πιθανοτήτων και στην πράξη, σε κάθε παιχνίδι αλλάζει ο τρόπος υποβολής ερωτημάτων από τον επιτιθέμενο. Επιπλέον, κάθε παιχνίδι έχει ένα ενδεχόμενο S_i σε αντιστοιχία με το ενδεχόμενο S_0 του αρχικού παιχνιδιού. Σκοπός είναι να αποδειχτεί πως η διαφορά $|\mathrm{P}[S_i] - \mathrm{P}[S_{i-1}]|$ είναι αμελητέα, κάτι το οποίο θα σημαίνει πως για το τελευταίο παιχνίδι ισχύει ότι $\mathrm{P}[S_k] = 1/2$. Αυτό με την σειρά του θα σημαίνει πως το πλεονέκτημα νίκης στο σχήμα PSEC-KEM είναι $Advantage_{PSEC-KEM}(A) = |\mathrm{P}[S_0] - 1/2|$ είναι αμελητέο.

Έστω ότι G_0 είναι το αρχικό παιχνίδι και S_0 το ενδεχόμενο ότι ο επιτιθέμενος A έχει μαντέψει σωστά το κρυφό bit b στο παιχνίδι G_0. Σημειώνεται ότι G_0 μοντελοποιείται ακριβώς όπως αναφέρθηκε κατά την περιγραφή ασφαλείας IND-CCA στην ενότητα 5.1.1.

Όπως περιεγράφηκε στην λειτουργία απενθυλάκωσης χρησιμοποιούνται οι συμβολισμοί $C, maskedSeed, g', h', C', seed, t, w, K, z, g''$, οι οποίοι συμβολίζουν τις τιμές που υπολογίζονται από τον αλγόριθμο απενθυλάκωσης με σκοπό την αποκρυπτογράφηση ενός κρυπτοκειμένου C_1. Αντίστοιχα, το κρυπτοκειμένο στόχος συμβολίζεται ως ${C_1}^*$ και αντίστοιχες τιμές ως $C^*, maskedSeed^*, g'^*, h'^*, C'^*, seed^*, t^*, w^*, K^*, z^*, g''^*$.

Τα κρυπτοκείμενα C_1 που αποστέλλονται στην διαδικασία κρυπτογράφησης ταξινομούνται σε τρείς κατηγορίες:

1. $g' \neq g'^*$.
2. $C = C^*$.
3. $g' = g'^*$, με $C \neq C^*$.

Σημειώνεται ότι για την περίπτωση 1, όλα τα κρυπτοκείμενα C_1 αποστέλλονται στην διαδικασία αποκρυπτογράφησης πριν γίνει επίκληση στην διαδικασία κρυπτογράφησης. Επιπλέον, για την περίπτωση 3, τα κρυπτοκείμενα μπορούν να δημιουργηθούν μόνο αν υποστηρίζονται πολλαπλοί τύποι μορφής κωδικοποίησης.

Έστω ότι $SEED$ δηλώνει το σύνολο των σημείων $seed$ στα οποία η συνάρτηση KDF_0 έχει ερωτηθεί είτε απευθείας από τον επιτιθέμενο είτε έχει πραγματοποιηθεί επίκληση αποκρυπτογράφησης του τύπου 3. Το σύνολο $SEED$ αυξάνεται με την πάροδο του χρόνου, όσο αποστέλλονται ερωτήματα στην KDF_0. Για οποιοδήποτε αλφαριθμητικό μεγέθους $seedLen$, ορίζεται το $\rho(seed)$, το οποίο συμβολίζει τον αριθμό που λαμβάνεται από το πρώτα $\lceil log_{256}\mu \rceil +$ 16 bytes της συνάρτησης KDF_0, αφού γίνει ανάλυση της ετικέτας $t = w||K$ και το στοιχείο w μετατραπεί στον αριθμό $z = StringToInt(w)\ mod\ \mu$.

Για την απόδειξη ασφαλείας εφαρμόζεται το λήμμα 6.2.1.1 που αναφέρθηκε κατά την απόδειξη ασφαλείας του σχήματος RSA-KEM. Υπενθυμίζεται το λήμμα 6.2.1.1: *Έστω ότι E, E', F είναι ενδεχόμενα σε ένα χώρο πιθανοτήτων τέτοια ώστε $P[E \wedge \neg F] = P[E' \wedge \neg F]$. Για τα ενδεχόμενα αυτά ισχύει ότι $|P[E] - P[E']| \leq P[F]$.*

Στο σημείο αυτό μπορούμε να ορίσουμε την ακολουθία παιχνιδιών $G_1, G_2, \dots, G_k$.

Στο παιχνίδι G_1 μεταβάλλεται η διαδικασία αποκρυπτογράφησης. Ειδικότερα, αν ο επιτιθέμενος αποστείλει ένα κρυπτογράφημα C_1 τύπου 2, το C_1 απορρίπτεται χωρίς να εκτελεσθεί ο αλγόριθμος αποκρυπτογράφησης. Έστω ότι F_1 είναι το ενδεχόμενο στο παιχνίδι G_1, στο οποίο ένα κρυπτοκείμενο απορρίπτεται, χωρίς ωστόσο αυτό να έχει απορριφθεί κατά το παιχνίδι G_0. Εφόσον τα δύο αυτά παιχνίδια είναι πανομοιότυπα μέχρι να συμβεί το ενδεχόμενο F_1 ισχύει ότι $P[S_0 \wedge \neg F_1] = P[S_1 \wedge \neg F_1]$. Εφαρμόζοντας το λήμμα 6.2.1.1 ισχύει ότι $|P[S_0] - P[S_1]| \leq P[F_1]$.

Υποθέτοντας ότι έχει αποσταλεί ένα κρυπτοκείμενο C_1 τύπου 2 στην διαδικασία αποκρυπτογράφησης του παιχνιδιού G_1, τότε θα ισχύει ότι $maskedSeed \neq maskedSeed^*$ και κατά συνέπεια $seed \neq seed^*$, διότι $C_1 \neq {C_1}^*$. Για την αποδοχή του C_1 σύμφωνα με τους κανόνες του παιχνιδιού G_0 πρέπει να ισχύει ότι $z = z^*$. Για να συμβεί αυτό, ο επιτιθέμενος θα πρέπει να βρει μια είσοδο $seed \neq seed^*$, η οποία θα προωθηθεί στην KDF_0 τέτοια ώστε $\rho(seed) = z^*$. Επομένως, ισχύει ότι $P[F_1] \leq (g_0 + g_D)\mu^{-1}(1 + 2^{-128})$. Ο παράγοντάς $(1 + 2^{-128})$ προέρχεται από το γεγονός ότι η τιμή z δεν είναι ομοιόμορφα κατανεμημένη. Έτσι, καταλήγουμε στο $|P[S_0] - P[S_1]| \leq (g_0 + g_D)\mu^{-1}(1 + 2^{-128})$.

Στην συνέχεια ορίζουμε το παιχνίδι G_2, πανομοιότυπο με το αρχικό, με την διαφορά ότι ο τύπος 1 κρυπτοκειμένου έχει αποσταλεί και ισχύει ότι $\text{seed} \notin SEED$. Επομένως, το κρυπτοκείμενο απορρίπτεται πριν φτάσει στο σημείο υπολογισμού της ετικέτας κατά την διαδικασία απενθυλάκωσης.

Έστω ότι F_2 είναι το ενδεχόμενο στο παιχνίδι G_2, στο οποίο ένα κρυπτοκείμενο απορρίπτεται, χωρίς ωστόσο αυτό να έχει απορριφθεί κατά το παιχνίδι G_1. Τα παιχνίδια αυτά εκτελούνται όμοια

μέχρι να συμβεί το ενδεχόμενο F_2. Έτσι, ισχύει ότι $P[S_1 \wedge \neg F_2] = P[S_2 \wedge \neg F_2]$ και εφαρμόζοντας το λήμμα 6.2.1.1 προκύπτει ότι $P[S_1] - P[S_2]| \leq P[F_2]$.

Υποθέτοντας ότι έχει αποσταλεί ένα κρυπτοκείμενο C_1 τύπου 1 με $\text{seed} \notin SEED$ στην διαδικασία αποκρυπτογράφησης του παιχνιδιού G_2 μπορούν να συμβούν τα παρακάτω ενδεχόμενα:

- Αν έχει πραγματοποιηθεί επίκληση στην διαδικασία κρυπτογράφησης πριν αποσταλεί το κρυπτογράφημα C_1 με $seed = seed^*$, τότε σύμφωνα με τους κανόνες του παιχνιδιού G_1, το κρυπτογράφημα θα απορριπτόταν διότι $g' \neq g'^*$.
- Αν δεν έχει γίνει προηγουμένως επίκληση στην διαδικασία αποκρυπτογράφησης ή έχει γίνει και ισχύει $seed \neq seed^*$, τότε δεν έχει πραγματοποιηθεί ερώτημα στην KDF_0 για το $seed$ ούτε από την διαδικασία κρυπτογράφησης, ούτε από την διαδικασία αποκρυπτογράφησης, ούτε από τον επιτιθέμενο. Επομένως, η τιμή z είναι ανεξάρτητη από οποιαδήποτε άλλη μεταβλητή, τουλάχιστον από την οπτική του επιτιθέμενου.

Επομένως, η πιθανότητα να μην απορριφθεί το συγκεκριμένο κρυπτοκείμενο σύμφωνα με τους κανόνες του παιχνιδιού G_1 είναι το πολύ $\mu^{-1}(1 + 2^{-128})$. Άρα, ισχύει ότι $|P[S_1] - P[S_2]| \leq g_D\mu^{-1}(1 + 2^{-128})$.

Στην συνέχεια ορίζουμε το παιχνίδι G_3, πανομοιότυπο με το αρχικό, με την διαφορά ότι ο τύπος 1 κρυπτοκειμένου έχει αποσταλεί και ισχύουν οι παρακάτω κανόνες:

- Αν $g' \neq \rho(seed')g$ για οποιοδήποτε $seed' \in SEED$, τότε το κρυπτογράφημα απορρίπτεται.
- Αν $g' = \rho(seed')g$ για κάποιο $seed' \in SEED$, υπολογίζεται το σημείο $h' = \rho(seed')h$ και η διαδικασία συνεχίζει στην αποκρυπτογράφηση, όπως στο παιχνίδι G_2, ξεκινώντας από τον υπολογισμό του στοιχείου C'.

Υποθέτοντας ότι έχει αποσταλεί ένα κρυπτοκείμενο C_1 για το οποίο $g' \neq \rho(seed^*)g$ για οποιοδήποτε $seed' \in SEED$, τότε το κρυπτογράφημα αυτό απορρίπτεται σύμφωνα με τους κανόνες του παιχνιδιού G_2. Για να διαπιστωθεί αυτό, θεωρούμε ότι $g' = z'g$, όπου $\mathrm{z}' \in \{0, \dots, \mu - 1\}$. Έτσι, $\mathrm{z}' \neq \rho(seed')$ για οποιοδήποτε $seed' \in SEED$. Υποθέτουμε ότι υπάρχει η μεταβλητή $seed$. Αν $seed \in SEED$, τότε το κρυπτογράφημα θα απορριπτόταν λόγω των κανόνων του παιχνιδιού G_2, επειδή θα αποτύγχανε ο έλεγχος $\mathrm{g}' = g''$ στην διαδικασία απενθυλάκωσης. Σε διαφορετική περίπτωση, θα ισχύει ότι $\text{seed} \notin SEED$, κάτι που θα οδηγούσε και πάλι στην απόρριψη του κρυπτογραφήματος σύμφωνα με τους κανόνες του παιχνιδιού G_2. Τέλος, λαμβάνεται υπόψη η περίπτωση όπου $\mathrm{g}' = \rho(seed')g$ για κάποιο $seed' \in SEED$. Στην περίπτωση αυτή, η διαδικασία απενθυλάκωσης εκτελείται πανομοιότυπα με αυτή του παιχνιδιού G_2.

Σύμφωνα με τα παραπάνω, μπορεί να διαπιστωθεί ότι τα παιχνίδια G_2 και G_3 είναι πανομοιότυπα και επομένως ισχύει ότι $P[S_3] = P[S_2]$.

Επιπλέον, ορίζουμε το παιχνίδι G_4,το οποίο αποτελεί παραλλαγή του παιχνιδιού G_3. Ειδικά για το παιχνίδι ορίζονται οι εξής νέες 4 μεταβλητές:

- Ένα τυχαίο αλφαριθμητικό $seed^+$ μεγέθους $seedLen$.
- Ένα τυχαίο αλφαριθμητικό w^+ μεγέθους $\lceil log_{256}\mu \rceil + 16$.
- Ένα τυχαίο αλφαριθμητικό K^+ μεγέθους $KeyLen$.

- Μια συνάρτηση KDF^+, η οποία λαμβάνει ως είσοδο την έξοδο της συνάρτησης κωδικοποίησης και αποφέρει ένα αλφαριθμητικό μεγέθους $seedLen$, $KDF^+: E(H) \rightarrow S^{seedLen}$.

Θεωρούμε ότι το παιχνίδι G_4 είναι πανομοιότυπο με το G_3 με την διαφορά των παρακάτω κανόνων:

1. Στην διαδικασία ενθυλάκωσης εκτελούνται τα εξής:
   a. $z^+ = StringToInt(w^+)\ mod\ \mu$.
   b. $g'^* = z^+ g$.
   c. $C^* = E(g'^*, format)$.
   d. $seedMask^+ = KDF^+(C^*)$
   e. $maskedSeed^* = seed^+ \oplus seedMask^+$.
   f. Επιστρέφεται το κλειδί K^+ και το κρυπτοκείμενο $C_0' = C^* || maskedSeed^*$.
2. Στην διαδικασία αποκρυπτογράφησης, όταν γίνεται επεξεργασία ενός κρυπτοκειμένου τύπου 3, χρησιμοποιείται η συνάρτηση $KDF^+(C)$, αντί της $KDF_1(C, C')$.
3. Όποτε η KDF_0 δεχθεί κάποιο ερώτημα, είτε από τον επιτιθέμενο είτε από την διαδικασία αποκρυπτογράφησης κρυπτοκειμένου τύπου 3, αντί για $KDF(seed^+)$, επιστρέφει με $u^+ || K^+$.
4. Όποτε η KDF_1 δεχθεί κάποιο ερώτημα, είτε από τον επιτιθέμενο είτε από την διαδικασία αποκρυπτογράφησης κρυπτοκειμένου τύπου 1, αντί για την απάντηση $KDF_1(C, C')$, επιστρέφει $KDF^+(C)$.

Τα παιχνίδια G_3 και G_4 είναι πανομοιότυπα, αφού η μόνη αλλαγή αφορά την αντικατάσταση τυχαίων τιμών με άλλες τυχαίες τιμές. Έτσι, ισχύει ότι $P[S_4] = P[S_3]$.

Τέλος, ορίζουμε το παιχνίδι G_5, πανομοιότυπο με το παιχνίδι G_4, με την διαφορά ότι δεν ισχύουν οι κανόνες 3 και 4. Στο παιχνίδι αυτό το κρυπτοκείμενο C_1^* δεν αποτελεί πλέον έγκυρο κρυπτογράφημα και επίσης δεν ισχύει ότι $seed^* = seed^+$ και $t^* = w^+ || K^+$. Αυτά συμβαίνουν διότι πλέον οι αρχικές διαδικασίες ενθυλάκωσης – απενθυλάκωσης δεν είναι σύμφωνες με τις αλλαγές που πραγματοποιήθηκα. Στην πράξη το κλειδί K^+ και επομένως το κρυφό bit που επιτιθέμενος καλείται να μαντέψει είναι ανεξάρτητα στο παιχνίδι G_5, όπως και το αλφαριθμητικό $seed^+$. Επιπλέον, η διαδικασία απενθυλάκωσης για τον τύπο 3 κρυπτογραφήματος δεν έρχεται σε συμφωνία με τις αρχικές διαδιακασίες ενθυλάκωσης – απενθυλάκωσης.

Τα παιχνίδια G_4 και G_5 λειτουργούν πανομοιότυπα έως ότου το αλφαριθμητικό $seed^+$ εμφανιστεί στο σύνολο $SEED$ ή αν ο επιτιθέμενος ή η διαδικασία αποκρυπτογράφησης αποστείλει ερώτημα στην συνάρτηση KDF_1 για τις εισόδους (C, C'), όπου C είναι η κωδικοποίηση του στοιχείου g'^* και C' είναι η μερική κωδικοποίηση του σημείου ug'^*.

Έστω ότι F_{5a} είναι το ενδεχόμενο εμφάνισης του αλφαριθμητικού $seed^+$ στο σύνολο $SEED$ στο παιχνίδι G_5. Έστω ότι F_{5b} είναι το ενδεχόμενο αποστολής ερωτήματος στην συνάρτηση KDF_1 για τις εισόδους (C, C'), όπου C είναι η κωδικοποίηση του στοιχείου g'^* και C' είναι η μερική κωδικοποίηση του σημείο ug'^*, είτε από τον επιτιθέμενο, είτε από την διαδικασία αποκρυπτογράφησης για τον τύπο 1 κρυπτογραφήματος. Έτσι, θεωρούμε ότι $F_5 = F_{5a} \vee F_{5b}$.

Εφόσον τα παιχνίδια G_4 και G_5 εκτελούνται πανομοιότυπα μέχρι να συμβεί το ενδεχόμενο F_5, ισχύει ότι $P[S_4 \wedge \neg F_5] = P[S_5 \wedge \neg F_5]$ και εφαρμόζοντας το λήμμα 6.2.1.1 προκύπτει ότι $P[S_4] - P[S_5]| \leq P[F_5]$.

Αφού το αλφαριθμητικό $seed^+$είναι ανεξάρτητο, ισχύει ότι $P[F_{5a}] \leq (g_0 + g_D)2^{-seedLen}$. Για την πιθανότητα $P[F_{5b}]$, ισχύει ότι $P[F_{5b}] \leq (1 + 2^{-128}) * P[A']$, όπου $P[A']$ είναι η πιθανότητα κατασκευής μιας λίστας με σύνολο στοιχείων $O(q_1 + q_D)$, ένα από τα οποία περιλαμβάνει μια λύση για το πρόβλημα CDH, από έναν επιτιθέμενο A', το οποίου ο χρόνος επίθεσης είναι περίπου ίδιος με αυτόν του επιτιθέμενου A.

Ο αλγόριθμος A' εκτελείται λαμβάνοντας ως είσοδο μια τυχαία τριπλέτα (g, h, g'^+) του προβλήματος CDH και τρέχει τον αλγόριθμο A έναντι μιας παραλλαγής του παιχνιδιού G_5. Στην παραλλαγή του παιχνιδιού, γίνεται χρήση των στοιχείων g, h για την κατασκευή του δημοσίου κλειδιού. Επιπλέον, χρησιμοποιείται απευθείας η μεταβλητή g'^+, αντί αυτή να προέρθει από το w^+. Ο παράγοντας $(1 + 2^{-128})$ προέρχεται από το γεγονός ότι η κατανομή g'^+ δεν είναι ομοιόμορφη, ενώ υποθέτουμε ότι η αντίστοιχη τιμή στο πρόβλημα CDH είναι ομοιόμορφα κατανεμημένη. Επομένως, συμπεραίνουμε ότι

$$P[S_4] - P[S_5] \leq Advantage_{CDH}(A', O(g_1 + g_D))(1 + 2^{-128}) + (g_0 + g_D)2^{-seedLen}.$$

Ακόμη, στο παιχνίδι G_5 το κρυφό bit είναι ανεξάρτητο από τις υπόλοιπες τιμές και επομένως ισχύει ότι $P[S_5] = 1/2$.

Λαμβάνοντας υπόψη τα συμπεράσματα από κάθε παιχνίδι, δηλαδή τα:

1. $|P[S_0] - P[S_1]| \leq (g_0 + g_D)\mu^{-1}(1 + 2^{-128})$.
2. $|P[S_1] - P[S_2]| \leq g_D\mu^{-1}(1 + 2^{-128})$.
3. $P[S_3] = P[S_2]$.
4. $P[S_4] = P[S_3]$.
5. $P[S_4] - P[S_5] \leq Advantage_{CDH}(A', O(g_1 + g_D))(1 + 2^{-128}) + (g_0 + g_D)2^{-seedLen}$.
6. $P[S_5] = 1/2$.

συμπεραίνεται ότι

$$Advantage_{PSEC-KEM}(A) \leq (g_0 + 2g_D)\mu^{-1}(1 + 2^{-128}) + Advantage_{CDH}(A', O(g_1 + g_D))(1 + 2^{-128}) + (g_0 + g_D)2^{-seedLen}.$$

Έτσι, το σχήμα PSEC-KEM είναι ασφαλές με την υπόθεση ότι το πρόβλημα CDH είναι αδύνατο να επιλυθεί.

Συνοψίζοντας, η απόδειξη ασφαλείας του PSEC-KEM λαμβάνει υπόψη δύο συναρτήσεις KDF, KDF_0 και KDF_1, για τις οποίες οι έξοδοι είναι εντελώς διαφορετικές μεταξύ τους. Από την παραπάνω απόδειξη, γίνεται εύκολα αντιληπτό ότι το πρόβλημα εισβολής στο σχήμα PSEC-KEM είναι ισοδύναμο με το πρόβλημα επίλυσης CDH για ελλειπτικές καμπύλες.

4.5 ACE-KEM

Το σχήμα ACE-KEM αποτελεί μια παραλλαγή του κρυπτοσυστήματος ACE (Advanced Cryptographic Engine), το οποίο αποτελεί ένα σχήμα υβριδικής κρυπτογραφίας δημοσίου κλειδιού, ενώ διαθέτει την επιλογή μετατροπής του σε σχήμα ψηφιακών υπογραφών [58]. Προτάθηκε από τον δημιουργό του πρότυπο ISO που μελετάτε στην παρούσα εργασία και αποτελεί μια παραλλαγή του σχήματος δημοσίου κλειδιού που προτάθηκε από τον ίδιο μερικά χρόνια νωρίτερα [12], το οποίο, στην πράξη, αποτελεί παραλλαγή του κρυπτοσυστήματος El Gamal. Για την περιγραφή του σχήματος ACE-KEM αρκεί η αναφορά στο κρυπτοσύστημα δημοσίου κλειδιού ACE-Encrypt.

Το σχήμα ACE-Encrypt αποτελείται από τις εξής παραμέτρους :

1. Συνάρτηση Υπολογισμού Ακεραίου $A\ rem\ n$: συνάρτηση που χρησιμοποιείται για τον υπολογισμό ενός ακέραιου αριθμού r, με $0 \leq r \leq n-1$, τέτοιος ώστε $A \equiv r\ mod\ n$, με $n > 0$ και $A \in \mathbb{Z}$.
2. Συνάρτηση Δημιουργίας κλειδιού (KDF): μια συνάρτηση κατακερματισμού όπως παρουσιάστηκε στην αρχή αυτού του κεφαλαίου. Το σχήμα ACE-Encrypt, χρησιμοποιεί δύο συναρτήσεις KDF (συναρτήσεις κατακερματισμού), την KDF_0 και την KDF_1. Η KDF_0 χρησιμοποιείται για την εξαγωγή δεδομένων αυθεντικοποίησης, ενώ η KDF_1 εξάγει το κλειδί που πρόκειται να χρησιμοποιηθεί στην διαδικασία κρυπτογράφησης.
3. Κρυπτογράφηση (E): Αλγόριθμος συμμετρικής κρυπτογράφησης.
4. Συνάρτηση Κωδικοποίησης (Encode): Αλγόριθμος κωδικοποίησης, ο οποίος μετατρέπει ένα κρυπτογράφημα στην αναπαράσταση του σε bytes.

Εν γένει, για την δημιουργία του ζεύγους δημοσίου-ιδιωτικού κλειδιού επιλέγεται μια παράμετρος m, η οποία αποτελεί έναν ακέραιο αριθμό, με $1024 \leq m \leq 16384$, ένα πρώτος αριθμός q μεγέθους 256-bit και ένας ακέραιος αριθμός P μεγέθους m-bit τέτοιος ώστε $P \equiv 1\ mod\ q$. Ειδικότερα, τα βήματα που ακολουθούνται για την δημιουργία του ζεύγους κλειδιών είναι τα εξής:

- Δημιουργία ενός τυχαίου πρώτου αριθμού q, με $2^{255} < q < 2^{256}$.
- Δημιουργία ενός τυχαίου πρώτου αριθμού P, με $2^{m-1} < P < 2^m$, τέτοιος ώστε $P \equiv 1\ mod\ q$.
- Δημιουργία ενός τυχαίου ακεραίου g_1, με $2 \leq g_1 \leq P-1$, τέτοιος ώστε $g_1^q \equiv 1\ mod\ P$.
- Δημιουργία των τυχαίων ακεραίων w, με $1 \leq w \leq q-1$ και $x, y, z_1, z_2 \in [0, \dots, q-1]$.
- Υπολογίζονται οι εξής ακέραιοι αριθμοί:
  - $g_2 = g_1^w\ rem\ P$,
  - $c = g_1^x\ rem\ P$,
  - $d = g_1^y\ rem\ P$,
  - $h_1 = g_1^{z_1}\ rem\ P$,
  - $h_2 = g_1^{z_2}\ rem\ P$.

- Δημιουργούνται τα τυχαία αλφαριθμητικά $k_1 \in B^{20l'+64}$ και $k_2 \in B^{2\lceil l/16 \rceil+40}$, όπου $l = L_B(P)$, όπου $L_B(P)$ είναι το μέγεθος του αριθμού P σε bytes και $l' = L_B(\lceil(2\lceil l/4\rceil + 4/16\rceil)$.
- Επιστρέφεται το δημόσιο κλειδί $PK = (P, q, g_1, g_2, c, d, h_1, h_2, k_1, k_2)$ και το ιδιωτικό κλειδί $SK = (w, x, y, z_1, z_2)$.

Για την διαδικασία κρυπτογράφησης με το σχήμα ACE και εφόσον έχουν δημιουργηθεί το αντίστοιχο ζεύγος κλειδιών για δύο χρήστες που θέλουν να εγκαθιδρύσουν ένα ασφαλές κανάλι μεταξύ τους, ο αλγόριθμος λαμβάνει ως είσοδο το δημόσιο κλειδί του παραλήπτη, $PK = (P, q, g_1, g_2, c, d, h_1, h_2, k_1, k_2)$ και ένα αρχικό μήνυμα M και επιστρέφει το κρυπτοκείμενο C. Ειδικότερα, η διαδικασία που ακολουθείται στην πλευρά του αποστολέα είναι η εξής:

- Επιλέγεται ένας τυχαίος αριθμός $r \in \{0, \dots, q-1\}$.
- Δημιουργείται το πρόθεμα (preamble) του κρυπτοκειμένου ως εξής:
  - Επιλέγεται ένα τυχαίο αλφαριθμητικό $s \in W^4$, όπου W είναι ένα σύνολο αλφαριθμητικών μεγέθους 32-bit και W^4 είναι ένα σύνολο αλφαριθμητικών μεγέθους 4*32=128 bit.
  - Υπολογίζονται οι ακέραιοι $u_1 = g_1^r \; rem \; P$ και $u_2 = g_2^r \; rem \; P$.
  - Υπολογίζεται ο ακέραιος αριθμός $a = KDF_0(k_1, L_B(P), s, u_1, u_2)$, με $0 < a < 2^{160}$. Σημειώνεται ότι η KDF_0 υλοποιείται με τέτοιο τρόπο ώστε να μετατρέπει μια πλειάδα $(k, l, s, u, u') \in B^* \times Z \times W^4 \times Z \times Z$, με $l > 0$, $0 \leq u, u' \leq 256^l$ σε έναν ακέραιο αριθμό a, με $0 < a < 2^{160}$.
  - Υπολογίζεται ο ακέραιος αριθμός $v = c^r d^{ar} \; rem \; P$.
- Αφού υπολογιστεί το πρόθεμα του κρυπτοκειμένου, υπολογίζεται το κλειδί που θα χρησιμοποιηθεί στην διαδικασία συμμετρικής κρυπτογράφησης ως εξής:
  - Υπολογίζονται οι ακέραιοι $h_1' = h_1^r \; rem \; P$ και $h_2' = h_2^r \; rem \; P$.
  - Υπολογίζεται το κλειδί κρυπτογράφησης $K = KDF_1(k_2, L_B(P), s, u_1, h_1', h_2') \in W^8$, όπου W^8 είναι ένα σύνολο αλφαριθμητικών μεγέθους 8*32=256 bit. Σημειώνεται ότι η KDF_1 υλοποιείται με τέτοιο τρόπο ώστε να μετατρέπει μια πλειάδα $(k, l, s, u, h, h') \in B^* \times Z \times W^4 \times Z \times Z \times Z$, με $0 \leq u, h, h' < 256^l$ σε ένα αλφαριθμητικό h, με $h \in W^8$.
- Υπολογίζεται το κρυπτογράφημα $e = E(k, s, 1024, M)$. Σημειώνεται ότι ο αλγόριθμος συμμετρικής κρυπτογράφησης Ε λαμβάνει ως είσοδο μια πλειάδα $(k, s, m, M) \in W^8 \times W^4 \times Z \times B^*$, με $m > 0$ και επιστρέφει ένα κρυπτογράφημα $e \in B^l$, όπου $l = L(M) + 16\lceil L(M)/m \rceil$.
- Υπολογίζεται η κωδικοποίηση του κρυπτογραφήματος σε bytes, $c = Encode(L_B(P), s, u_1, u_2, v, e)$.
- Ο αλγόριθμος τερματίζει εφόσον υπολογιστεί το κρυπτογράφημα c.

Όσον αφορά την διαδικασία αποκρυπτογράφησης, στην πλευρά του παραλήπτη, αφού έχει ήδη δημιουργηθεί το ζεύγος δημοσίου - ιδιωτικού κλειδιού, $(PK = (P, q, g_1, g_2, c, d, h_1, h_2, k_1, k_2), SK = (w, x, y, z_1, z_2))$ και πραγματοποιηθεί λήψη του κρυπτογραφήματος c, πραγματοποιούνται τα εξής:

- Ελέγχεται αν $L(C) \geq 3 * L_B(P) + 16$. Σε διαφορετική περίπτωση, το κρυπτογράφημα απορρίπτεται και επιστρέφεται μήνυμα σφάλματος.

- Υπολογίζεται η πλειάδα (s, u_1, u_2, v, e) από την συνάρτηση κωδικοποίησης, $(s, u_1, u_2, v, e) = Encode(L_B(P), c)$, με $0 \leq u_1, u_2, v < 256^l$, όπου $l = L_B(P)$. Σημειώνεται ότι η συνάρτηση κωδικοποίησης, στην πράξη, αποτελείται από το ζεύγος αλγορίθμων κωδικοποίησης-αποκωδικοποίησης.
- Ελέγχεται το πρόθεμα του κρυπτοκειμένου ως εξής:
  - Ελέγχεται αν $u_1 < P$ ή $u_1 < P$ ή $v < P$. Σε διαφορετική περίπτωση ο αλγόριθμος τερματίζει και επιστρέφεται μήνυμα σφάλματος.
  - Ελέγχεται αν $u_1^q = 1 \; rem \; P$. Σε διαφορετική περίπτωση ο αλγόριθμος τερματίζει και επιστρέφεται μήνυμα σφάλματος.
  - Αρχικοποιείται μια τιμή $r = 0$.
  - Ελέγχεται αν $u_2 \neq u_1^w \; rem \; P$. Αν ισχύει, τότε τίθεται $r = 1$.
  - Υπολογίζεται ο ακέραιος αριθμός $a = KDF_0(k_1, L_B(P), s, u_1, u_2)$.
  - Ελέγχεται αν $v \neq u_1^{x+ay} \; rem \; P$. Αν ισχύει, τότε τίθεται $r = 1$.
  - Ελέγχεται αν $r = 1$. Αν ισχύει, τότε ο αλγόριθμος τερματίζει και επιστρέφεται μήνυμα σφάλματος.
- Ο αλγόριθμος συνεχίζει στον υπολογισμό του κλειδιού συμμετρικής κρυπτογράφησης:
  - Υπολογίζονται οι ακέραιοι $h_1' = u_1^{z_1} \; rem \; P$ και $h_2' = u_1^{z_2} \; rem \; P$.
  - Υπολογίζεται το κλειδί κρυπτογράφησης $K = KDF_1(k_2, L_B(P), s, u_1, h_1', h_2') \in W^8$.
- Υπολογίζεται το αρχικό μήνυμα $M = E(k, s, 1024, e)$. Σημειώνεται ότι ο αλγόριθμος συμμετρικής κρυπτογράφησης Ε, στην πράξη, αποτελείται από το ζεύγος αλγορίθμων κρυπτογράφησης-αποκρυπτογράφησης.
- Ο αλγόριθμος τερματίζει εφόσον υπολογιστεί το αρχικό μήνυμα M.

Όσον αφορά την ασφάλεια του κρυπτοσυστήματος ACE-Encrypt, έχει αποδειχτεί ότι είναι ασφαλές στο μοντέλο IND-CCA, με την προϋπόθεση ότι το πρόβλημα DDH είναι υπολογιστικά αδύνατο να επιλυθεί [58].

Όπως αναφέρθηκε προηγουμένως, το σχήμα ACE-KEM αποτελεί παραλλαγή του σχήματος υβριδικής κρυπτογραφίας ACE-Encrypt. Σύμφωνα με το πρότυπο ISO που προτάθηκε από τον Shoup [33] ο μηχανισμός ACE-KEM αποτελείται από τις εξής παραμέτρους:

1. Ομάδα $\Gamma = (H, G, g, \mu, \nu, E, D, E', D')$, όπως αυτή ορίστηκε στην αρχή του κεφαλαίου.
2. Συνάρτηση Δημιουργίας Κλειδιού (KDF): μια συνάρτηση κατακερματισμού, όπως παρουσιάστηκε στην αρχή του κεφαλαίου. Όπως και το σχήμα ACE-Encrypt, ο μηχανισμός ACE-KEM χρησιμοποιεί δύο συναρτήσεις KDF (συναρτήσεις κατακερματισμού), την KDF_0 και την KDF_1. Η KDF_0 χρησιμοποιείται για την εξαγωγή δεδομένων αυθεντικοποίησης, ενώ η KDF_1 εξάγει το κλειδί που πρόκειται να χρησιμοποιηθεί στην διαδικασία κρυπτογράφησης. Σημειώνεται ότι για την KDF_0 πρέπει να ισχύει ότι το μήκος της εξόδου της KDF_0. $OutputLen < log_{256}\mu$.
3. Μεταβλητή Λειτουργίας Συμπαράγοντα (CofactorMode): οι τιμές της μεταβλητής είναι είτε 0 είτε 1.
4. Μήκος Κλειδιού (keyLen): ένας θετικός ακέραιος αριθμός.

Βάση των παραπάνω παραμέτρων, η λειτουργία του ACE-KEM έχει ως εξής:

1. Ο αλγόριθμος $Generate_{ACE-KEM}()$ αποφέρει το ζεύγος δημοσίου-ιδιωτικού κλειδιού. Ο αλγόριθμος δημιουργίας κλειδιού λειτουργεί ως εξής:
    a. Επιλέγονται 4 ακέραιοι αριθμοί $w, x, y, z \in [0 \dots \mu)$.
    b. Υπολογίζονται τα στοιχεία της ομάδας G:
        i. $g' = w * g$,
        ii. $c = x * g$,
        iii. $d = y * g$,
        iv. $h = z * g$.
    c. Το δημόσιο κλειδί του χρήστη PK αποτελείται από τα στοιχεία $g', c, d, h \in G$, ενώ το αντίστοιχο ιδιωτικό SK από τους ακεραίους w, $x, y, z \in [0 \dots \mu)$.
2. Ο αλγόριθμος $Encapsulate_{ACE-KEM}(PK)$ λαμβάνει ως είσοδο το δημόσιο κλειδί του παραλήπτη $PK = (g', c, d, h) \in G$ και λειτουργεί ως εξής:
    a. Επιλέγεται ένας τυχαίος αριθμός $r \in [0, \dots, \mu)$.
    b. Υπολογίζονται τα στοιχεία της ομάδας H:
        i. $u = r * g$,
        ii. $u' = r * g'$,
        iii. $h' = r * h$.
    c. Υπολογίζονται τα αλφαριθμητικά $C = E(u, format)$ και $C' = E(u', format)$ μέσω της συνάρτησης κωδικοποίησης. Σημειώνεται ότι στο σχήμα ACE-KEM ο αλγόριθμος κωδικοποίησης λαμβάνει ως είσοδο μια προαιρετική μεταβλητή $format$, η οποία καθορίζει τη μορφή κωδικοποίησης για τα στοιχεία της ομάδας.
    d. Υπολογίζεται η έξοδος της συνάρτησης KDF_0, $EC = KDF_0(C||C')$.
    e. Υπολογίζεται ο ακέραιος $a = StringToInt(EC)$.
    f. Υπολογίζεται ο ακέραιος $r' = a * r \; mod \; \mu$.
    g. Υπολογίζεται το στοιχείο της ομάδας G, $v = r * c + r' * d$.
    h. Υπολογίζονται το αλφαριθμητικό $EV = E(v, format)$ μέσω της συνάρτησης κωδικοποίησης.
    i. Υπολογίζεται το αλφαριθμητικό $PEH = E'(h')$, μέσω της συνάρτησης μερικής κωδικοποίησης.
    j. Υπολογίζεται το αλφαριθμητικό $C_0 = C||C'||EV$.
    k. Υπολογίζεται το κλειδί K μέσω της συνάρτησης KDF_1, $K = KDF_1(C||PEH, keyLen)$.
    l. Ο αλγόριθμος τερματίζει εφόσον υπολογιστεί το αλφαριθμητικό C_0 και το κλειδί K.
3. Ο αλγόριθμος $Decapsulate_{ACE-KEM}(SK, C_0)$ λαμβάνει ως είσοδο το ιδιωτικό κλειδί του παραλήπτη, $SK = (w, z, y, z) \in [0 \dots \mu)$ και το κρυπτογράφημα C_0 και λειτουργεί ως εξής:

a. Αναλύεται το κρυπτογράφημα C_0, ως $C_0 = C||C'||EV$, όπου C, C', EV είναι οι κωδικοποιήσεις των στοιχείων της ομάδας H, $u, u', v \in H$.
b. Από την συνάρτηση αποκωδικοποίησης υπολογίζονται τα στοιχεία $u, u', v \in H$:
   i. $u = D(C)$,
   ii. $u' = D(C')$,
   iii. $v = D(EV)$.
c. Ελέγχεται αν τα στοιχεία C, C', EV αποτελούν έγκυρες κωδικοποιήσεις. Σε διαφορετική περίπτωση, ο αλγόριθμος τερματίζει την λειτουργία του και επιστρέφεται μήνυμα σφάλματος.
d. Αν $CofactorMode = 1$, τότε υπολογίζονται τα εξής:
   i. $u'' = v * u$,
   ii. $w' = v^{-1} * w \ mod \ \mu$,
   iii. $x' = v^{-1} * x \ mod \ \mu$,
   iv. $y' = v^{-1} * y \ mod \ \mu$,
   v. $z' = v^{-1} * z \ mod \ \mu$.

   Σε διαφορετική περίπτωση, δηλαδή αν $CofactorMode = 0$, τότε:
   i. $u'' = u$,
   ii. $w' = w$,
   iii. $x' = x$,
   iv. $y' = y$,
   v. $z' = z$.
e. Αν $CofactorMode = 0$ και $v > 1$, ελέγχεται αν $u \in G$. Σε διαφορετική περίπτωση, ο αλγόριθμος τερματίζεται και επιστρέφεται μήνυμα σφάλματος.
f. Υπολογίζεται η έξοδος της συνάρτησης KDF_0, $EC = KDF_0(C||C')$.
g. Υπολογίζεται ο ακέραιος $a = StringToInt(EC)$.
h. Υπολογίζεται ο ακέραιος $\mathrm{t} = x' + y' * a \ mod \ \mu$.
i. Ελέγχεται αν $w' * u'' = u'$ και $t * u'' = v$. Σε διαφορετική περίπτωση, ο αλγόριθμος τερματίζει και επιστρέφεται μήνυμα σφάλματος.
j. Υπολογίζεται το στοιχείο της ομάδας H, $\mathrm{h}' = z' * u''$.
k. Υπολογίζεται το αλφαριθμητικό $PEH = E'(h')$, μέσω της συνάρτησης μερικής κωδικοποίησης.
l. Υπολογίζεται το κλειδί K μέσω της συνάρτησης $KDF_1 = KDF(C||PEH, keyLen)$.
m. Ο αλγόριθμος τερματίζει εφόσον υπολογιστεί το κλειδί K.

Ο παραπάνω μηχανισμός, όπως και τα υπόλοιπα σχήματα KEM που περιγράφηκαν προηγουμένως (εκτός του RSA-KEM) μπορεί να περιγράφει χωρίς να ληφθεί υπόψη η ομάδα Γ που έχει οριστεί στο πρότυπο ISO. Επίσης, μιας και το ACE-KEM στηρίζεται στο κρυπτοσύστημα ElGamal, η λειτουργία του μπορεί να περιγράφει και πάνω από ελλειπτικές καμπύλες [59].

1. Ο αλγόριθμος $Generate_{ACE-KEM}()$ πάνω σε μια ελλειπτική καμπύλη E, ορισμένη σε ένα πεπερασμένο σώμα F_q, με G ένα σημείο στην ελλειπτική καμπύλη που χρησιμοποιείται ως γεννήτορας και n έναν πρώτο αριθμό ο οποίος αναπαριστά την τάξη του σημείου G, λειτουργεί ως εξής:
    a. Επιλέγονται τέσσερις τυχαίοι ακέραιοι αριθμοί $d, x, y, z \in [1 \dots n)$.
    b. Υπολογίζονται τα σημεία $Q = d * G, X = X * G, Y = y * G$ και $Z = z * G$
    c. Η τετράδα (d, x, y, z) αποτελεί το ιδιωτικό κλειδί του χρήστη, ενώ η τετράδα σημείων (Q, X, Y, Z), το αντίστοιχο δημόσιο κλειδί.
2. Ο αλγόριθμος $Encapsulate_{ACE-KEM}(PK)$ λαμβάνει ως είσοδο το δημόσιο κλειδί του παραλήπτη που αποτελείται από τα σημεία (Q, X, Y, Z) και λειτουργεί ως εξής:
    a. Επιλέγεται ένας ακέραιος αριθμός $t \in [0 \dots n)$.
    b. Υπολογίζονται τα σημεία $T = t * G, U_1 = t * Q$ και $U_2 = t * Z$.
    c. Υπολογίζεται ο ακέραιος αριθμός $a = KDF_0(T, U_1)$.
    d. Υπολογίζεται ο ακέραιος αριθμός $t' = a * t \; mod \; n$.
    e. Υπολογίζεται το σημείο $V = t * X + t' * Y$.
    f. Υπολογίζεται το κλειδί κρυπτογράφησης $K = KDF_1(T, U_2)$.
    g. Ο αλγόριθμος τερματίζει εφόσον υπολογιστεί η τριπλέτα (T, U_1, V) και το κλειδί K.
3. Ο αλγόριθμος $Decapsulate_{ACE-KEM}(SK, C)$ λαμβάνει ως είσοδο το ιδιωτικό κλειδί του παραλήπτη που αποτελείται από τους ακέραιους (d, x, y, z) και το κρυπτογράφημα $C = (T, U_1, V)$ και λειτουργεί ως εξής:
    a. Υπολογίζεται ο ακέραιος αριθμός $a = KDF_0(T, U_1)$.
    b. Υπολογίζεται ο ακέραιος αριθμός $r = x + a * y \; mod \; n$.
    c. Υπολογίζονται τα σημεία ${U_1}' = d * T$ και $V' = r * T$.
    d. Ελέγχεται αν $U_1' = U_1$ και αν $V' = V$. Σε διαφορετική περίπτωση, ο αλγόριθμος τερματίζει την λειτουργία του και επιστρέφεται μήνυμα σφάλματος.
    e. Υπολογίζεται το σημείο $U_2 = z * T$.
    f. Υπολογίζεται το κλειδί $K = KDF_1(T, U_2)$.
    g. Ο αλγόριθμος τερματίζεται εφόσον υπολογιστεί το μυστικό κλειδί K.

4.5.1 Ασφάλεια ACE-KEM

Όπως αναφέρθηκε, το σχήμα ACE-KEM, αποτελεί παραλλαγή του κρυπτοσυστήματος ACE-Encrypt, το οποίο βασίζεται στην δυσκολία επίλυσης του προβλήματος DDH [58]. Επομένως, η απόδειξη ασφαλείας του ACE-KEM στηρίζεται στο δύσκολο αυτό πρόβλημα. Εκτός από το πρόβλημα DDH, όπως σε όλα τα σχήματα τύπου KEM η απόδειξη ασφαλείας βασίζεται στην δυσκολία αντιστροφής των συναρτήσεων KDF. Σημειώνεται ότι η πρώτη KDF αφορά ένα κλασικό

τύπο συνάρτησης κατακερματισμού. Επομένως, οι δύο αυτές συναρτήσεις KDF πρέπει να ικανοποιούν τις απαιτήσεις ασφαλείας μιας συνάρτησης κατακερματισμού.

Όπως παρουσιάστηκε προηγουμένως, στο σχήμα ACE-KEM γίνεται χρήση μιας συνάρτησης κατακερματισμού (την οποία ονομάσαμε KDF_0) και μιας συνάρτησης KDF, KDF_1. Για την μοντελοποίηση της IND-CCA ασφάλειας υποθέτουμε ότι υπάρχει ένας επιτιθέμενος A, στον οποίον επιτρέπεται να πραγματοποιήσει το μέγιστο qD ερωτήματα με σκοπό την αποκρυπτογράφηση του μηνύματος C_0. Επομένως, γίνεται εύκολα αντιληπτό ότι το πλεονέκτημα νίκης έναντι του παιχνιδιού IND-CCA που ορίζεται για το σχήμα ACE-KEM έχει άμεση σχέση με το πλεονέκτημα νίκης έναντι του προβλήματος DDH και της αντιστροφής των συναρτήσεων KDF_0 και KDF_1. Ειδικότερα, $Advantage_{ACE-KEM}(A) = 0(Advantage_{DDH}(A_1) + Advantage_{KDF_0}(A_2) + Advantage_{KDF_1}(A_3))$, όπου:

- A_1, A_2, A_3 είναι επιτιθέμενοι που εκτελούν την επίθεση στο ίδιο χρονικό διάστημα με τον επιτιθέμενο A,
- $Advantage_{DDH}(A)$ είναι το πλεονέκτημα νίκης έναντι του προβλήματος DDH,
- $Advantage_{KDF_0}(A)$ είναι η πιθανότητα ενός επιτιθέμενου A να βρει δεύτερη προ-εικόνα στην συνάρτηση κατακερματισμού. Ειδικότερα, δοθέντων των C^* και C'^*, τα οποία αποτελούν κωδικοποιήσεις δύο τυχαίων στοιχείων της ομάδας G, σκοπός του επιτιθέμενου είναι να βρει δύο κωδικοποιήσεις C και C' τέτοιες ώστε $KDF_0(C||C') = KDF_0(C^*||C'^*)$, με $(C, C') \neq (C^*, C'^*)$. Σημειώνεται ότι το πρόβλημα εύρεσης δεύτερης προ-εικόνας είναι δυσκολότερο από το πρόβλημα εύρεσης συγκρούσεων.
- $Advantage_{KDF_1}(A)$ είναι το πλεονέκτημα ενός επιτιθέμενου A να διαχωρίζει μεταξύ των δύο ακόλουθων κατανομών: Έστω ότι u_1 και h' είναι τυχαία στοιχεία της ομάδας G και C είναι η κωδικοποίηση του στοιχείου u_1. Έστω ότι R είναι ένα τυχαίο αλφαριθμητικό μεγέθους $keyLen$. Η πρώτη κατανομή είναι το ζεύγος (R, C) και η δεύτερη το ζεύγος $(KDF_1(C||E'(h'), keyLen), C)$.
- qD είναι ο μέγιστος αριθμός ερωτημάτων αποκρυπτογράφησης που μπορούν να πραγματοποιηθούν από έναν επιτιθέμενο A.

Για την απόδειξη ασφαλείας στο μοντέλο IND-CCA θεωρούμε πως υπάρχει μια σειρά παιχνιδιών G_i για τα οποία ο επιτιθέμενος A πραγματοποιεί μια επίθεση. Κάθε ένα από τα παιχνίδια λαμβάνει χώρα σε ένα χώρο πιθανοτήτων και στην πράξη, σε κάθε παιχνίδι αλλάζει ο τρόπος υποβολής ερωτημάτων από τον επιτιθέμενο. Επιπλέον, κάθε παιχνίδι έχει ένα ενδεχόμενο S_i σε αντιστοιχία με το ενδεχόμενο S_0 του αρχικού παιχνιδιού. Σκοπός είναι να αποδειχτεί πως η διαφορά $|\mathrm{P}[S_i] - \mathrm{P}[S_{i-1}]|$ είναι αμελητέα, κάτι το οποίο θα σημαίνει πως για το τελευταίο παιχνίδι ισχύει ότι $\mathrm{P}[S_k] = 1/2$. Αυτό με την σειρά του θα σημαίνει πως το πλεονέκτημα νίκης στο σχήμα ACE-KEM είναι $Advantage_{ACE-KEM}(A) = |\mathrm{P}[S_0] - 1/2|$ είναι αμελητέο.

Υπενθυμίζεται ότι κατά την διαδικασία ενθυλάκωσης το κρυπτογράφημα C_0 αποτελείται από τις τιμές C, C' και EV, όπου:

- C είναι η κωδικοποίηση του στοιχείου $u = r * g$, όπου r είναι ένας τυχαίος επιλεγμένος ακέραιος αριθμός και g, από τον ορισμό της ομάδας Γ είναι ένας γεννήτορας της κυκλικής ομάδας G,
- C' είναι η κωδικοποίηση του στοιχείου $u' = r * g'$, όπου $g' = w * g$, όπου w είναι ένας τυχαίος επιλεγμένος ακέραιος αριθμός,

- EV είναι η κωδικοποίηση του στοιχείου $v = r * c + r' * d$, όπου $c = x * g$, όπου x είναι ένας τυχαία επιλεγμένος ακέραιος αριθμός, $r' = a * r \; mod \; \mu$, όπου a είναι η μετατροπή της εξόδου της συνάρτησης $KDF_0(C||C')$ σε έναν ακέραιο.

Βάση των παραπάνω, θεωρούμε το κρυπτοκείμενο στόχο ${C_0}^*$, το οποίο αποτελείται από τις αντίστοιχες τιμές C^*, C'^* και EV^*, στις οποίες αντιστοιχούν οι ανάλογες τιμές $u^*, u'^*, a^*, v^*, EV^*$.

Έστω ότι G_0 είναι το αρχικό παιχνίδι και S_0 το ενδεχόμενο ότι ο επιτιθέμενος A έχει μαντέψει σωστά το κρυφό bit b στο παιχνίδι G_0, επομένως, το πλεονέκτημα του επιτιθέμενου ορίζεται ως $|P[S_0] - 1/2|$. Σημειώνεται ότι το παιχνίδι G_0 μοντελοποιείται ακριβώς όπως αναφέρθηκε κατά την περιγραφή ασφαλείας IND-CCA στην ενότητα 5.1.1.

Για την απόδειξη ασφαλείας εφαρμόζεται το λήμμα 6.2.1.1 που αναφέρθηκε κατά την απόδειξη ασφαλείας του σχήματος RSA-KEM. Υπενθυμίζεται το λήμμα 6.2.1.1: *Έστω ότι E, E', F είναι ενδεχόμενα σε ένα χώρο πιθανοτήτων τέτοια ώστε $P[E \wedge \neg F] = P[E' \wedge \neg F]$. Για τα ενδεχόμενα αυτά ισχύει ότι $|P[E] - P[E']| \leq P[F]$.*

Στο σημείο αυτό μπορούμε να ορίσουμε την ακολουθία παιχνιδιών $G_1, G_2, \dots, G_k$.

Στο παιχνίδι G_1 μεταβάλλεται το ιδιωτικό κλειδί του χρήστη από w, x, y, z σε $x_1, x_2, y_1, y_2, z_1, z_2$, όπου όλα τα στοιχεία έχουν επιλεχθεί τυχαία. Επιπλέον, μεταβάλλεται ο τρόπος υπολογισμού του δημοσίου κλειδιού. Ειδικότερα,

- Υπολογίζονται οι εξής τιμές:
  - $c = x_1 * x_2 * g$,
  - $d = y_1 * y_2 * g$,
  - $h = z_1 * z_2 * g$.
- Στην διαδικασία απενθυλάκωσης υπολογίζονται οι εξής τιμές:
  - $u'' = v * u * u'$.
  - Αν $CofactorModer = 1$, τότε $z' = v^{-1} * z_1 * z_2$. Σε διαφορετική περίπτωση $z' = z_1 * z_2$.
  - $h' = z' * u''$.

Οι παραπάνω μετατροπές ολοκληρώνουν την περιγραφή του παιχνιδιού G_1, στο οποίο η σημαντικότερη μετατροπή αφορά το ιδιωτικό κλειδί ενός χρήστη, το οποίο μετατρέπεται στην πλειάδα $x_1, x_2, y_1, y_2, z_1, z_2$.

Έστω ότι F_1 είναι το ενδεχόμενο στο παιχνίδι G_1, στο οποίο ένα κρυπτοκείμενο απορρίπτεται, χωρίς ωστόσο αυτό να έχει απορριφθεί κατά το παιχνίδι G_0. Εφόσον τα παιχνίδια G_0 και G_1 είναι πανομοιότυπα μέχρι να συμβεί το ενδεχόμενο F_1 ισχύει ότι $P[S_0 \wedge \neg F_1] = P[S_1 \wedge \neg F_1]$. Εφαρμόζοντας το λήμμα 6.2.1.1 ισχύει ότι $|P[S_0] - P[S_1]| \leq P[F_1]$.

Στην συνέχεια ορίζουμε το παιχνίδι G_2, πανομοιότυπο με το αρχικό, με την διαφορά ότι αντί να υπολογίζονται τα στοιχεία u^* και u'^*, αυτά επιλέγονται τυχαία. Υπενθυμίζεται ότι οι κωδικοποιήσεις των στοιχείων u^* και u'^*, δηλαδή οι C^* και C'^*, αντίστοιχα, χρησιμοποιούνται για τον υπολογισμό του κρυπτογραφήματος στόχου ${C_0}^*$. Για το παιχνίδι αυτό ισχύει ότι $|P[S_2] - P[S_1]| \leq Advantage_{DDH}$.

Στην συνέχεια ορίζουμε το παιχνίδι G_3, πανομοιότυπο με το προηγούμενο, με τον εξής κανόνα: Έστω ότι F_3 είναι το ενδεχόμενο στο οποίο ο επιτιθέμενος στο παιχνίδι G_2 απέστειλε το

κρυπτοκείμενο C_0 τέτοιο ώστε $(u, u') \neq (u^*, u'^*)$ και $a = a^*$. Το παιχνίδι αυτό είναι πανομοιότυπο με το G_2 με την διαφορά ότι αν συμβεί το ενδεχόμενο F_3, η επίθεση τερματίζεται. Για το ενδεχόμενο αυτό ισχύει ότι $P[F_3] \leq Advantage_{KDF_0}$. Επιπλέον, επειδή το παιχνίδι G_3 έχει προέλθει από το παιχνίδι G_2, ισχύει ότι $P[S_2 \wedge \neg F_3] = P[S_3 \wedge \neg F_3]$. Εφαρμόζοντας το λήμμα 6.2.1.1 ισχύει ότι $|P[S_3] - P[S_2]| \leq Advantage_{KDF_0}$.

Θεωρούμε ότι το παιχνίδι G_4 είναι πανομοιότυπο με το G_3 με την διαφορά ότι η τιμή h'^* επιλέγεται τυχαία. Έστω ότι F_4 στο οποίο συμβαίνει ένα από τα παρακάτω:

- $log_g u^* = log_g u'^*$. Σημειώνεται ότι το κρυπτοκείμενο στόχος ${C_0}^*$ δεν είναι έγκυρο όταν $log_g u^* = log_g u'^*$.
- Ένα μη έγκυρο κρυπτοκείμενο C_0 με $(u_1, u_2, v) \neq ({u_1}^*, {u_2}^*, v^*)$ δεν έχει απορριφθεί από το παιχνίδι G_3.

Επομένως, ισχύει ότι $P[S_4 \wedge \neg F_4] = P[S_3 \wedge \neg F_4]$. Εφαρμόζοντας το λήμμα 6.2.1.1 ισχύει ότι $|P[S_4] - P[S_3]| \leq P[F_4]$.

Εν συνεχεία, ορίζουμε το παιχνίδι G_5, το οποίο είναι πανομοιότυπο με το G_4, με την διαφορά ότι μεταβάλλεται ο τρόπος υπολογισμού του κλειδιού K', το οποίο αντί να εξάγεται από την συνάρτηση KDF_1, επιλέγεται τυχαία. Επιπλέον, σε περίπτωση που στην διαδικασία απενθυλάκωσης αποσταλεί από έναν επιτιθέμενο το κρυπτογράφημα C_0, τότε στο παιχνίδι G_5 απορρίπτεται το κρυπτογράφημα αυτό. Έστω ότι F_5 συμβολίζει το γεγονός στο οποίο το κρυπτοκείμενο C_0 δεν έχει απορριφθεί από το παιχνίδι G_4. Επομένως, θα ισχύει ότι $P[S_4 \wedge \neg F_5] = P[S_5 \wedge \neg F_5]$ και εφαρμόζοντας το λήμμα 6.2.1.1 ισχύει ότι $|P[S_5] - P[S_4]| \leq P[F_5]$.

Επιπλέον, στο παιχνίδι G_5 το κρυφό bit είναι ανεξάρτητο από τις υπόλοιπες τιμές και επομένως ισχύει ότι $P[S_5] = 1/2$.

Λαμβάνοντας υπόψη τα συμπεράσματα από κάθε παιχνίδι, συμπεραίνεται ότι

$$Advantage_{ACE-KEM}(A) = Advantage_{DDH}(A_1) + Advantage_{KDF_0}(A_2) + Advantage_{KDF_1}(A_3)$$

Έτσι, το σχήμα PSEC-KEM είναι ασφαλές με την υπόθεση ότι το πρόβλημα CDH είναι αδύνατο να επιλυθεί.

Συνοψίζοντας, η απόδειξη ασφαλείας του ACE-KEM λαμβάνει υπόψη δύο συναρτήσεις KDF, KDF_0 και KDF_1, για τις οποίες οι έξοδοι είναι εντελώς διαφορετικές μεταξύ τους. Από την παραπάνω απόδειξη, γίνεται εύκολα αντιληπτό ότι το πρόβλημα εισβολής στο σχήμα ACE-KEM είναι ισοδύναμο με το πρόβλημα επίλυσης DDH, καθώς και στην δυσκολία αντιστροφής των συναρτήσεων KDF_0 και KDF_1. Ειδικά για την KDF_0, η οποία υλοποιείται ως συνάρτηση κατακερματισμού, απαιτείται η δυσκολία επίλυσης του προβλήματος δεύτερης προ-εικόνας.

4.6 Σύγκριση μηχανισμών ενθυλάκωσης κλειδιού

Όλα τα σχήματα που εξετάστηκαν, συμπεριλαμβανομένου και του RSA-KEM, το οποίο δεν βασίζεται στην λειτουργία ελλειπτικών καμπυλών, στηρίζονται κυρίως στην τυχαιότητα των συναρτήσεων KDF. Για την γενικότερη αξιολόγηση τους λαμβάνουμε υπόψη ότι οι συναρτήσεις

αυτές δεν δημιουργούν μοτίβα, για παράδειγμα σταθερά αλφαριθμητικά στις τελευταίες θέσεις τα οποία προκύπτουν με μεγαλύτερη συχνότητα από ότι θα έπρεπε για μια τυχαία συνάρτηση. Λαμβάνοντας υπόψιν το σενάριο ότι υπάρχουν μοτίβα κατά την έξοδο των συναρτήσεων KDF, μπορούμε εύκολα να συμπεράνουμε ότι τα κλειδιά που δημιουργούνται από ένα σχήμα KEM (τα οποία χρησιμοποιούνται μετέπειτα από το σχήμα DEM), οδηγούν σε κλειδιά κρυπτογράφησης που θα έχουν ένα μοτίβο με μεγάλη συχνότητα εμφάνισης. Βέβαια, κάτι τέτοιο δεν ισχύει σε σχήματα που χρησιμοποιούν περισσότερες από μια KDF, όπως το PSEC-KEM. Για τα σχήματα αυτά, αναλόγως της υλοποίησης κάθε μηχανισμού, κάθε μοτίβο αντιστοιχεί είτε στο κλειδί της διαδικασίας κρυπτογράφησης από τον μηχανισμό DEM, όπως και στην προηγούμενη περίπτωση, είτε αντιστοιχούν σε εισόδους σε άλλες λειτουργίες των σχημάτων. Σε κάθε περίπτωση ένα μοτίβο ίσως αποκαλύπτει σημαντικές πληροφορίες για τον τρόπο του υπολογισμού ενός κλειδιού. Επομένως, είναι σημαντικό να διασφαλίζεται η τυχαιότητα στις συναρτήσεις KDF, κάτι το οποίο είναι εφικτό μιας και στην πράξη, οι συναρτήσεις KDF αποτελούν κρυπτογραφικές συναρτήσεις κατακερματισμού.

Όσον αφορά την αξιολόγηση και σύγκριση των μηχανισμών KEM που μελετήθηκαν σε θέματα ασφάλειας, αυτές είναι δύσκολο να μελετηθούν διότι κάθε ένας μηχανισμός βασίζεται σε διαφορετικά ασύμμετρα σχήματα ή/και χρησιμοποιούνται διαφορετικές παραδοχές ασφαλείας. Για παράδειγμα είναι δύσκολο να συγκρίνουμε τον μηχανισμό RSA-KEM με έναν από τους υπόλοιπους, μιας και το μαθηματικό πρόβλημα (παραγοντοποίησης) στο οποίο στηρίζεται είναι πολύ διαφορετικό από το πρόβλημα (διακριτού λογαρίθμου), στο οποίο στηρίζονται τα υπόλοιπα σχήματα. Μια γενικευμένη σύγκριση μπορεί να γίνει στα σχήματα ACE-KEM, ECIES-KEM και PSEC-KEM, αφού και τα τρία στηρίζονται στο πρόβλημα επίλυσης διακριτού λογαρίθμου και ειδικότερα το πρόβλημα επίλυσης Diffie-Hellman. Η ασφάλεια του μηχανισμού ACE-KEM, ο οποίος βασίζεται την δυσκολία επίλυσης του προβλήματος Diffie-Hellman πάνω από ελλειπτικές καμπύλες, μπορεί να δειχθεί ότι είναι τουλάχιστον όσο ασφαλής όσο και ο μηχανισμός ECIES-KEM. Στην πράξη, ένας αλγόριθμος ο οποίος είναι ικανός να εισβάλει στο ACE-KEM μπορεί να προσαρμοστεί για την εισβολή του στον αλγόριθμο ECIES-KEM με το ίδιο πλεονέκτημα. Κάτι τέτοιο ωστόσο, δεν ισχύει για την περίπτωση του PSEC-KEM. Αυτό συμβαίνει διότι για να πραγματοποιηθεί η μετατροπή της πρόκλησης του ECIES-KEM σε πρόκληση PSEC-KEM πρέπει να υπολογιστεί ένα κατάλληλο ζεύγος (K, C_2) από μια πρόκληση (K, C_1). Το σενάριο αυτό μοιάζει αδύνατο λόγω της τυχαίας μεταβλητής $seed$ η οποία μετατρέπεται στο αλφαριθμητικό $t||K$ δια μέσου της συνάρτησης KDF_0, όπου η μεταβλητή t είναι ένα τυχαίο αλφαριθμητικό που χρησιμοποιείται από τον αλγόριθμο ECIES-KEM. Είναι προφανές ότι το PSEC-KEM βασίζεται σε αδύναμες παραδοχές ασφαλείας τουλάχιστον σε σχέση με το ECIES-KEM. Επομένως, είναι πιο ισχυρός αλγόριθμος, Ωστόσο, το τίμημα είναι η αργοπορία στην διαδικασία απενθυλάκωσης, διότι το PSEC-KEM πρέπει να υπολογίσει έναν επιπλέον πολλαπλασιασμό σε σχέση με το ECIES-KEM.

Με αφετηρία το παραπάνω συμπέρασμα, δηλαδή ότι μπορούμε να ισχυριστούμε ότι ο μηχανισμός PSEC-KEM είναι πιο ισχυρός όσον αφορά τις παραδοχές ασφαλείας, όμως είναι πιο αργός σε σχέση με τους μηχανισμούς ACE-KEM και ECIES-KEM, η σύγκριση των πρωτοκόλλων μπορεί να γίνει με βάση την απόδοση τους όσους αφορά τον χρόνο απόκρισης, καθώς και με βάση το μέγεθος των μηνυμάτων που ανταλλάσσουν δύο χρήστες μεταξύ τους έως ότου τερματίσει η λειτουργία του επιλεγμένου μηχανισμού. Στο σημείο αυτό είναι σημαντικό να τονιστεί ότι οι συγκρίσεις που ακολουθούν αφορούν τους μηχανισμούς KEM οι οποίοι υλοποιούνται παρόμοια,

δηλαδή βασίζονται στο πρόβλημα Diffie-Hellman. Δεν συμπεριλαμβάνουμε τον μηχανισμό RSA-KEM διότι αποτελεί μια ξεχωριστή κατηγορία.

Εφόσον έχουμε ήδη αναλύσει τους μηχανισμούς KEM, οι οποίοι βασίζονται σε παραλλαγές του προβλήματος Diffie-Hellman πάνω από ελλειπτικές καμπύλες οι κύριες διαφορές που εντοπίζονται είναι οι εξής [60]:

- Το δημόσιο κλειδί του μηχανισμού ACE-KEM αποτελείται από τέσσερα σημεία της ελλειπτικής καμπύλης (βλέπε ενότητα 4.5), ενώ για τους μηχανισμούς ECIES-KEM και PSEC-KEM, το δημόσιο κλειδί αποτελείται από ένα σημείο (βλέπε ενότητες 4.3 και 4.4).
- Ο μηχανισμός PSEC-KEM χρησιμοποιεί μια συνάρτηση KDF δύο φορές για την δημιουργία ενός ζεύγους κλειδιών, ένα για την συνάρτηση αυθεντικοποίησης MAC και ένα που θα χρησιμοποιηθεί ως συμμετρικό κλειδί κρυπτογράφησης. Αντίθετα, ο μηχανισμός ECIES-KEM χρησιμοποιεί μια συνάρτηση KDF, ενώ ο μηχανισμός ACE-KEM δύο διαφορετικές συναρτήσεις KDF.
- Το μήνυμα που στέλνει ο αποστολέας στον παραλήπτη σύμφωνα με τον μηχανισμό ECIES-KEM αποτελείται από το δημόσιο κλειδί του αποστολέα, το κρυπτογραφημένο μήνυμα και ένα μήνυμα αυθεντικοποίησης τύπου MAC. Στο σχήμα PSEC-KEM περιλαμβάνεται ακόμη μια επιπλέον μεταβλητή, ενώ στο ACE-KEM περιλαμβάνονται δύο επιπλέον σημεία της ελλειπτικής καμπύλης.
- Ο μηχανισμός PSEC-KEM είναι το μόνο σχήμα που χρησιμοποιεί την συνάρτηση XOR κατά την διαδικασία δημιουργίας κλειδιού.

Ανεξάρτητα από τις παραπάνω διαφορές που αφορούν κυρίως θέματα υλοποίησης, στον παρακάτω πίνακα, αναγράφεται ο αριθμός των λειτουργιών που απαιτούνται για την κρυπτογράφηση ενός μηνύματος όσον αφορά τις πράξεις που εκτελούνται και τον αριθμό επικλήσεων σε συναρτήσεις KDF [61].

Σχήμα	**Ύψωση σε δύναμη κατά την ενθυλάκωση**	**Ύψωση σε δύναμη κατά την απενθυλάκωση**	**Επίκληση σε συνάρτηση KDF**
ECIES-KEM	2	1	1
PSEC-KEM	2	2	2
ACE-KEM	5	3	1

Πίνακας 4.1: Αριθμός λειτουργιών ομάδας των σχημάτων ECIES-KEM, PSEC-KEM και ACE-KEM.

Όσον αφορά την απόδοση σύμφωνα με πείραμα που πραγματοποιήθηκε [61], ο μηχανισμός ACE-KEM έχει την χειρότερη απόδοση μιας και ο χρόνος πραγματοποίησης των διαδικασιών ενθυλάκωσης και απενθυλάκωσης ήταν 12.5 ms και 7.5 ms, αντίστοιχα. Πιο γρήγορος μηχανισμός φαίνεται να είναι ο ECIES-KEM με χρόνους απόκρισης 5ms και 2.5 ms, αντίστοιχα, ενώ πολύ κοντά στους χρόνους αυτούς είναι ο μηχανισμός PSEC-KEM με 5 ms και στις δύο διαδικασίες. Επομένως, ο μηχανισμός ECIES-KEM φαίνεται να είναι η καλύτερη επιλογή, διότι παρέχει την γρηγορότερη απόκριση όσον αφορά τον χρόνο εκτέλεσης του, αλλά και πραγματοποιούνται

λειτουργίες στην ομάδα. Συγκρίνοντας τον με τον μηχανισμό ACE-KEM, μπορεί εύκολα να ειπωθεί ότι είναι 2.5 με 3 φορές γρηγορότερος.

5 *Σύνοψη και Συμπεράσματα*

Στην παρούσα εργασία εξετάστηκαν οι μηχανισμοί ενθυλάκωσης κλειδιού για την επιτυχή μεταφορά ενός κλειδιού κατά την υβριδική κρυπτογράφηση. Αρχικά, εστιάσαμε στα προβλήματα που δημιουργούνται από τις κλασσικές τεχνικές μεταφοράς κλειδιού μέσω ασύμμετρων σχημάτων καθώς και προβλήματα που εντοπίζονται στη χρήση συμμετρικών αλγορίθμων κρυπτογράφησης. Τα προβλήματα και των δύο αυτών κατηγοριών φαίνεται να εξαλείφονται με την χρήση της υβριδικής κρυπτογραφίας και ειδικότερα με την χρήση μηχανισμών τύπου KEM/DEM, οι οποίοι προσφέρουν υψηλή ασφάλεια και μεγάλη αποδοτικότητα. Στην συνέχεια, εξετάστηκαν ξεχωριστά οι δημοφιλέστεροι μηχανισμοί ενθυλάκωσης κλειδιού οι οποίοι έχουν προταθεί ως πρότυπα ISO, όσον αφορά τα (ασύμμετρα) σχήματα στα οποία βασίζονται, το τρόπο λειτουργίας τους, καθώς και μελετήθηκαν οι αποδείξεις ασφαλείας τους.

Παρόλο που τα σχήματα που εξετάστηκαν βασίζονται είτε στο πρόβλημα της παραγοντοποίησης ή προβλήματα σχετικά με το Diffie-Hellman, τα οποία θεωρούνται ανέφικτο να επιλυθούν, υπάρχουν διαφορές μεταξύ τους, όσον αφορά ζητήματα απόδοσης και αριθμού υπολογισμών κατά τις διαδικασίες ενθυλάκωσης και απενθυλάκωσης. Ναι μεν τα σχήματα που εξετάστηκαν στηρίζονται σε διαφορετικά δύσκολα προβλήματα, ωστόσο όλα έχουν αποδειχθεί ότι ικανοποιούν τις απαιτήσεις IND-CCA ασφάλειας. Κύριος σκοπός του πρότυπου ISO που μελετήθηκε ήταν να γενικεύσει σχήματα που στηρίζονται σε κρυπτογραφία δημοσίου κλειδιού, έτσι ώστε να είναι συγκρίσιμα μεταξύ τους όσον αφορά την ασφάλεια και την αποδοτικότητα τους και ως αποτέλεσμα να επιτρέπεται η υλοποίηση ενός υβριδικού σχήματος κρυπτογραφίας, στο οποίο ο αλγόριθμος δημοσίου κλειδιού χρησιμοποιείται για την κρυπτογράφηση ενός κλειδιού, το οποίο μετέπειτα χρησιμοποιείται από ένα συμμετρικό σχήμα.

Τα επιλεγμένα σχήματα που χρησιμοποιήθηκαν για την δημιουργία του προτύπου ISO έχουν τις παρακάτω ιδιότητες:

- Τα σχήματα βασισμένα στην ανταλλαγή κλειδιού Diffie-Hellman ορίζονται σε μια ομάδα, η οποία μπορεί να υλοποιηθεί με διάφορους τρόπους, συμπεριλαμβανομένης της υλοποίησης ως υπο-ομάδα πάνω σε ελλειπτικές καμπύλες ή υπο-ομάδα του $\mathbb{Z}_p^*$.
- Όλα τα σχήματα είναι σε θέση να επεξεργαστούν αρχικά μηνύματα αυθαίρετου μεγέθους.
- Όλα τα σχήματα είναι αποδεδειγμένα ασφαλή έναντι της επίθεσης επιλεγμένου κρυπτοκειμένου (CCA).
- Όλα τα σχήματα παρέχουν ισορροπία αποδοτικότητάς – ασφάλειας.

Γενικά, ένα KEM λειτουργεί ως ένα σχήμα κρυπτογραφίας δημοσίου κλειδιού, με την διαφορά ότι ο αλγόριθμος κρυπτογράφησης λαμβάνει ως είσοδο μόνο το δημόσιο κλειδί του παραλήπτη και δημιουργεί ένα κλειδί, αντί να λαμβάνει και ένα αρχικό μήνυμα και να αποφέρει ένα

κρυπτογράφημα όπως στην περίπτωση κρυπτογραφίας δημοσίου κλειδιού. Ένα KEM αποτελείται από τους εξής τρείς αλγορίθμους:

- Αλγόριθμος δημιουργίας κλειδιού, ο οποίος αποφέρει το ζεύγος δημοσίου-ιδιωτικού κλειδιού.
- Αλγόριθμος ενθυλάκωσης, ο οποίος λαμβάνει ως είσοδο το δημόσιο κλειδί και αποφέρει το ζεύγος κλειδιού – κρυπτογραφήματος.
- Αλγόριθμος απενθυλάκωσης, ο οποίος λαμβάνει ως είσοδο το ιδιωτικό κλειδί και το κρυπτοκείμενο και αποφέρει το κλειδί.

Δοθέντος ενός KEM όπως περιγράφηκε παραπάνω, στην γενική του μορφή, και με την προσθήκη ενός μηχανισμού συμμετρικής κρυπτογραφίας και ενός αλγορίθμου αυθεντικοποίησης MAC, μπορεί να δημιουργηθεί ένα σχήμα υβριδικής κρυπτογραφίας το οποίο είναι ασφαλές έναντι της επίθεσης επιλεγμένου κρυπτοκειμένου. Βασική απαίτηση για την λειτουργία του νέου σχήματος είναι το μέγεθος του κλειδιού που δημιουργείται από τον αλγόριθμο ενθυλάκωσης να μπορεί να διαχωριστεί έτσι ώστε να είναι εφικτό να χρησιμοποιηθεί από τους αλγορίθμους συμμετρικής κρυπτογράφησης και MAC. Επομένως, από ένα σχήμα υβριδικής κρυπτογραφίας απαιτείται ότι το μέγεθος του κλειδιού εξόδου του μηχανισμού KEM θα πρέπει να ισούται με το μέγεθος του κλειδιού κρυπτογράφησης που δημιουργείται συν το μέγεθος του κλειδιού MAC, $KEM.OutputKeyLen = Enc.KeyLen + MAC.KeyLen$. Επομένως, δοθέντος ενός αρχικού μηνύματος M, ο αλγόριθμος KEM δημιουργεί ένα κλειδί K μήκους $Enc.KeyLen + MAC.KeyLen$ και ένα κρυπτοκείμενο C. Στην συνέχεια το κλειδί K αναλύεται ως $K = k||k'$, όπου k είναι το κλειδί που πρόκειται να χρησιμοποιηθεί από τον αλγόριθμο κρυπτογράφησης μεγέθους $Enc.KeyLen$ και k' είναι το κλειδί που πρόκειται να χρησιμοποιηθεί από τον αλγόριθμο MAC, $MAC.KeyLen$. Το αρχικό μήνυμα M κρυπτογραφείται με την χρήση του αλγορίθμου συμμετρικής κρυπτογραφίας, το οποίο αποφέρει ένα κρυπτοκείμενο C'. Στην συνέχεια, εφαρμόζεται ο αλγόριθμος MAC στο κρυπτοκείμενο αυτό με την χρήση του κλειδιού k' ώστε να ληφθεί η ετικέτα αυθεντικοποίησης. Το τελικό κρυπτοκείμενο που λαμβάνει ο παραλήπτης είναι το $C^* = C||C'||tag$.

Για την διαδικασία αποκρυπτογράφησης ακολουθείται η αντίθετη διαδικασία. Αν τα συστατικά στοιχεία του σχήματος υβριδικής κρυπτογραφίας είναι ασφαλή, δηλαδή αν ο αλγόριθμος KEM, ο αλγόριθμος συμμετρικής κρυπτογραφίας και ο αλγόριθμος MAC είναι IND-CCA ασφαλείς, τότε και όλο το σχήμα υβριδικής κρυπτογραφίας είναι ασφαλή.

Για την δημιουργία του προτύπου ISO λήφθηκαν υπόψη οι αλγόριθμοι δημοσίου κλειδιού RSA, ECIES, PSEC-2 και ACE-Encrypt, οι οποίοι τροποποιήθηκαν ώστε να ταιριάζουν στις απαιτήσεις σχημάτων υβριδικής κρυπτογραφίας. Η παραμετροποίηση των παραπάνω αλγορίθμων οδήγησε στην δημιουργία των εξής μηχανισμών ενθυλάκωσης κλειδιού:

- **RSA-KEM**

  Ο μηχανισμός RSA-KEM αποτελεί παραλλαγή του κρυπτοσυστήματος RSA, έτσι ώστε να ταιριάζει στις απαιτήσεις υλοποίησης ενός σχήματος υβριδικής κρυπτογραφίας. Ο αλγόριθμος RSA σε συνδυασμό με μια συνάρτηση δημιουργίας κλειδιού χρησιμοποιείται για την δημιουργία του ζεύγους (C, K) έτσι ώστε ο RSA να μετατρέπεται σε μηχανισμό ενθυλάκωσης κλειδιού. Το βασικό πλεονέκτημα του συγκεκριμένου σχήματος είναι η απλότητα που προσφέρει, καθώς και η εγγύηση ασφάλειας έναντι άλλων παρόμοιων μηχανισμών όπως το RSA-OAEP.

Αναφορικά με την ασφάλεια του RSA-KEM, η απόδειξη βασίζεται στην παραδοχή αδυναμίας επίλυσης του προβλήματος παραγοντοποίησης, δηλαδή, δοθέντος μιας ενθυλάκωσης κλειδιού η καλύτερη τεχνική διαχωρισμού μεταξύ του πραγματικού κλειδιού και ενός τυχαίου δημιουργημένου κλειδιού είναι να υπολογιστή η i-ρίζα της ενθυλάκωσης.

- **ECIES-KEM**

Ο μηχανισμός ECIES-KEM αποτελεί παραλλαγή του κρυπτοσυστήματος ECIES, το οποίο ορίζεται πάνω σε ελλειπτικές καμπύλες. Η κύρια διαφορά του σχήματος που ορίστηκε στο πρότυπο ISO με το κρυπτοσύστημα ECIES είναι ότι για την υλοποίηση του ορίζεται μια αφηρημένη ομάδα Γ, η οποία δεν ορίζεται απαραίτητα πάνω από ελλειπτικές καμπύλες. Βέβαια, η περιγραφή του σχήματος έγινε με βάση τον ορισμό του σε ελλειπτικές καμπύλες για λόγους απλότητας. Επιπλέον, στο σχήμα KEM προστέθηκε ο κατακερματισμός του κρυπτογραφήματος μέσω μιας συνάρτησης KDF.

Η ασφάλεια του σχήματος αυτού βασίζεται σε μια νέα σχετικά παραδοχή, αυτή του προβλήματος gap-Diffie Hellman. Σύμφωνα με αυτή

- **PSEC-KEM**

Ο μηχανισμός PSEC-KEM αποτελεί μια παραλλαγή του κρυπτοσυστήματος PSEC-2, το οποίο αποτελεί ένα σχήμα υβριδικής κρυπτογραφίας. Η κύρια διαφορά των δύο συστημάτων έγκειται στο γεγονός ότι το σχήμα KEM δημιουργεί ένα κρυπτοκείμενο μεγαλύτερου μεγέθους, καθώς και μια ετικέτα αυθεντικοποίησης μεγαλύτερου μεγέθους. Επιπλέον το σχήμα KEM μπορεί να υλοποιηθεί σε οποιαδήποτε κυκλική ομάδα και όχι μόνο πάνω από ελλειπτικές καμπύλες ή ομάδες πρώτης τάξης.

Όσον αφορά την ασφάλεια του συγκεκριμένου μηχανισμού, η απόδειξη βασίζεται στην παραδοχή αδυναμίας επίλυσης του προβλήματος Diffie-Hellman πάνω από ελλειπτικές καμπύλες. Σύμφωνα με αυτή, δοθέντος της ενθυλάκωσης ενός κλειδιού, η καλύτερη τεχνική για την διάκριση μεταξύ του πραγματικού κλειδιού και ενός τυχαίου δημιουργημένου κλειδιού είναι η αντιστροφή του πρωτοκόλλου Diffie-Hellman κάτι που μέχρι και σήμερα θεωρείται αδύνατο. Τέλος, ο μηχανισμός PSEC-KEM υλοποιείται με λίγους υπολογισμούς κατά την διάρκεια την ενθυλάκωσης και απενθυλάκωσης και επομένως, έχει υψηλή αποδοτικότητα.

- **ACE-KEM**

Ο μηχανισμός ACE-KEM αποτελεί μια παραλλαγή του κρυπτοσυστήματος ACE-Encrypt, το οποίο αποτελεί ένα σχήμα που ορίζεται πάνω από ελλειπτικές καμπύλες. Ο αλγόριθμος για το KEM γενικεύτηκε έτσι ώστε να λειτουργεί με την αφηρημένη ομάδα Γ που ορίστηκε στο πρότυπο ISO, καθώς και με οποιονδήποτε αλγόριθμο συμμετρικής κρυπτογράφησης και αλγόριθμο MAC.

Για την απόδειξη ασφαλείας του μηχανισμού χρησιμοποιείται το πρόβλημα απόφασης Diffie-Hellman. Με άλλα λόγια, αποδεικνύεται ότι για να επιτύχει μια επίθεση στο συγκεκριμένο σχήμα θα πρέπει να χρησιμοποιείται είτε μια αδύναμη συνάρτηση κατακερματισμού είτε μια αδύναμη συνάρτηση δημιουργίας κλειδιού. Παρόλη την απόδειξη ασφάλειας η απόδοση του ACE-KEM φαίνεται να είναι περιορισμένη, τουλάχιστον σε σχέση με τα υπόλοιπα σχήματα KEM που εξετάστηκαν. Έτσι, η χρήση του

δεν προτείνεται σε συσκευές με περιορισμένους πόρους παρά μόνο σε περιπτώσεις όπου η ασφάλεια είναι μείζον ζήτημα.

Τέλος, η σύγκριση μεταξύ των σχημάτων είναι δύσκολη να πραγματοποιηθεί διότι κάθε ένα βασίζεται σε κάποιο πρόβλημα το οποίο είναι ανέφικτο να επιλυθεί, τουλάχιστον μέχρι και σήμερα. Επομένως, ο μόνος τρόπος σύγκρισης τους, μιας και η ασφάλεια τους είναι αποδεδειγμένη, είναι η αποδοτικότητα τους. Αποδοτικότερο σχήμα φαίνεται να είναι ο μηχανισμός PSEC-KEM, ο οποίος βασίζεται στο πρόβλημα επίλυσης gap-Diffie-Hellman, ενώ κοντά σε αυτόν είναι ο μηχανισμός ECIES-KEM, ο οποίος βασίζεται στο πρόβλημα επίλυσης απόφασης Diffie-Hellman. Ο μηχανισμός RSA-KEM φαίνεται να είναι αρκετά αποδοτικός, ωστόσο δε μπορούμε να οδηγηθούμε σε ένα ασφαλές συμπέρασμα διότι υλοποιείται εντελώς διαφορετικά από τους υπόλοιπους μηχανισμούς και η απόδειξη ασφαλείας έγκειται στο πρόβλημα της παραγοντοποίησης. Τέλος, ο μηχανισμός ACE-KEM είναι ο πιο αργός και επομένως δε θα πρέπει να χρησιμοποιείται σε συστήματα όπου η ταχύτητα είναι το απαιτούμενο.

Τα σχήματα που εξετάστηκαν αν και θεωρούνται ασφαλή την δεδομένη χρονική στιγμή, είναι ευάλωτα σε κβαντικές επιθέσεις. Επομένως, ως μελλοντική έρευνα, κρίνεται απαραίτητη η σύγκριση της ήδη υπάρχουσας έρευνας γύρω από τους μηχανισμούς ενθυλάκωσης κλειδιού για κβαντικούς υπολογιστές ή/και η πρόταση νέων ισχυρών μηχανισμών.

Βιβλιογραφία

[1] Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.

[2] Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[3] Bauer, F. L. (2002). *Decrypted secrets: methods and maxims of cryptology*. Springer Science & Business Media.

[4] Shoup, V. (2001). A proposal for an ISO standard for public key encryption (version 2.1). *IACR e-Print Archive*, *112*.

[5] Buchmann, J. (2013). *Introduction to cryptography*. Springer Science & Business Media.

[6] Hoffstein, J., Pipher, J., Silverman, J. H., & Silverman, J. H. (2008). *An introduction to mathematical cryptography* (Vol. 1). New York: Springer.

[7] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.

[8] Bellare, M., & Sahai, A. (1999, August). Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. In *Annual International Cryptology Conference* (pp. 519-536). Springer, Berlin, Heidelberg.

[9] Bleichenbacher, D. (1998, August). Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1. In *Annual*

[10] Naor, M., & Yung, M. (1990, April). Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing* (pp. 427-437).

[11] Rackoff, C., & Simon, D. R. (1991, August). Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Annual International Cryptology Conference* (pp. 433-444). Springer, Berlin, Heidelberg.

[12] Cramer, R., & Shoup, V. (1998, August). A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Annual International Cryptology Conference* (pp. 13-25). Springer, Berlin, Heidelberg.

[13] Vaudenay, S. (2006). *A classical introduction to cryptography: Applications for communications security*. Springer Science & Business Media.

[14] Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. *Journal of computer and system sciences*, *28*(2), 270-299.

[15] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

[16] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, *31*(4), 469-472.

[17] Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons.

[18] Coron, J. S., & May, A. (2007). Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. *Journal of Cryptology*, *20*(1), 39-50

[19] Barker, E., Barker, W., Burr, W., Polk, W., & Smid, M. (2007). NIST special publication 800-57. *NIST Special publication*, *800*(57), 1-142.

[20] Bellare, M., & Rogaway, P. (1994, May). Optimal asymmetric encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 92-111). Springer, Berlin, Heidelberg.

[21] Dierks, T., & Rescorla, E. (2008). The transport layer security (TLS) protocol version 1.2.

[22] Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417-426). Springer, Berlin, Heidelberg.

[23] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), 203-209.

[24] Cohen, H., Miyaji, A., & Ono, T. (1998, October). Efficient elliptic curve exponentiation using mixed coordinates. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 51-65). Springer, Berlin, Heidelberg.

[25] Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., & Vercauteren, F. (Eds.). (2005). *Handbook of elliptic and hyperelliptic curve cryptography*. CRC press.

[26] Washington, L. C. (2008). *Elliptic curves: number theory and cryptography*. CRC press.

[27] Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). *Guide to elliptic curve cryptography*. Springer Science & Business Media.

[28] Barker, E., Chen, L., Keller, S., Roginsky, A., Vassilev, A., & Davis, R. (2017). *Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography* (No. NIST Special Publication (SP) 800-56A Rev. 3 (Draft)). National Institute of Standards and Technology.

[29] Jager, T., Schwenk, J., & Somorovsky, J. (2015, September). Practical invalid curve attacks on TLS-ECDH. In *European Symposium on research in computer security* (pp. 407-425). Springer, Cham.

[30] Cramer, R., & Shoup, V. (2003). Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, *33*(1), 167-226.

[31] Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014). *Encyclopedia of cryptography and security*. Springer Science & Business Media.

[32] Shoup, V. (2000, May). Using hash functions as a hedge against chosen ciphertext attack. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 275-288). Springer, Berlin, Heidelberg.

[33] Shoup, V. (2001). A proposal for an ISO standard for public key encryption (version 2.1). *IACR e-Print Archive*, *112*.

[34] Dent, A. W. (2003, December). A designer's guide to KEMs. In *IMA International Conference on Cryptography and Coding* (pp. 133-151). Springer, Berlin, Heidelberg.

[35] Nagao, W., Manabe, Y., & Okamoto, T. (2005, February). A universally composable secure channel based on the KEM-DEM framework. In *Theory of Cryptography Conference* (pp. 426-444). Springer, Berlin, Heidelberg.

[36] Dent, A. W. (2002). *ECIES-KEM vs. PSEC-KEM*. Technical Report NES/DOC/RHU/WP5/028/2, NESSIE.

[37] Bellare, M., & Namprempre, C. (2000, December). Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 531-545). Springer, Berlin, Heidelberg.

[38] Kurosawa, K., & Desmedt, Y. (2004, August). A new paradigm of hybrid encryption scheme. In *Annual International Cryptology Conference* (pp. 426-442). Springer, Berlin, Heidelberg.

[39] J. Herranz, D. Hofheinz, and E. Kiltz. The Kurosawa-Desmedt key encapsulation is notchosen-ciphertext secure. IACR e-print Archive 2006/207, 2005. (Cited on page1,15.

[40] Kiltz, E. (2007, April). Chosen-ciphertext secure key-encapsulation based on gap hashed Diffie-Hellman. In International Workshop on Public Key Cryptography (pp. 282-297). Springer, Berlin, Heidelberg.

[41] Kiltz, E., & Pietrzak, K. (2010, December). Leakage resilient elgamal encryption. In International conference on the theory and application of cryptology and information security (pp. 595-612). Springer, Berlin, Heidelberg.

[42] Kurosawa, K., & Desmedt, Y. (2004, August). A new paradigm of hybrid encryption scheme. In *Annual International Cryptology Conference* (pp. 426-442). Springer, Berlin, Heidelberg.

[43] Herranz, J., Hofheinz, D., & Kiltz, E. (2006). The Kurosawa-Desmedt Key Encapsulation is not Chosen-Ciphertext Secure. IACR Cryptology ePrint Archive, 2006, 207.

[44] Choi, S. G., Herranz, J., Hofheinz, D., Hwang, J. Y., Kiltz, E., Lee, D. H., & Yung, M. (2009). The Kurosawa–Desmedt key encapsulation is not chosen-ciphertext secure. Information Processing Letters, 109(16), 897-901.

[45] Kurosawa, K. (2014, May). Kurosawa-desmedt key encapsulation mechanism, revisited. In *International Conference on Cryptology in Africa* (pp. 51-68). Springer, Cham.

[46] Rogaway, P., & Shrimpton, T. (2004, February). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In International workshop on fast software encryption (pp. 371-388). Springer, Berlin, Heidelberg.

[47] Dang, Q. H. (2015). *Secure hash standard* (No. Federal Inf. Process. Stds.(NIST FIPS)-180-4).

[48] Abe, M., Gennaro, R., Kurosawa, K., & Shoup, V. (2005, May). Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 128-146). Springer, Berlin, Heidelberg.

[49] Okamoto, T., & Pointcheval, D. (2001, February). The gap-problems: A new class of problems for the security of cryptographic schemes. In International workshop on public key cryptography (pp. 104-118). Springer, Berlin, Heidelberg.

[50] Randall, J., Kaliski, B., Brainard, J., & Turner, S. (2010). Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS). *Proposed Standard, 5990*.

[51] Barker, E., Barker, W., Burr, W., Polk, W., & Smid, M. (2007). NIST special publication 800-57. *NIST Special publication*, *800*(57), 1-142.

[52] Bellare, M., & Rogaway, P. (1997, November). Minimizing the use of random oracles in authenticated encryption schemes. In *International Conference on Information and Communications Security* (pp. 1-16). Springer, Berlin, Heidelberg.

[53] Abdalla, M., Bellare, M., & Rogaway, P. (1999). DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem. *IACR Cryptology ePrint Archive*, *1999*, 7.

[54] Okamoto, T., & Pointcheval, D. (2000). PSEC-3: Provably secure elliptic curve encryption scheme-V3 (Submission to P1363a). IEEE P1363a.

[55] Gayoso Martínez, V., Hernández Encinas, L., & Sánchez Ávila, C. (2010). A survey of the elliptic curve integrated encryption scheme.

[56] Dent, A. W. (2002). *ECIES-KEM vs. PSEC-KEM*. Technical Report NES/DOC/RHU/WP5/028/2, NESSIE.

[57] Okamoto, T., Fujisaki, E., & Morita, H. (2000). PSEC: Provably secure elliptic curve encryption scheme. In *IEEE P1363a*.

[58] Schweinberger, T., & Shoup, V. (2000). ACE: the advanced cryptographic engine. In *Revised, August*.

[59] Menezes, A. (2001). Evaluation of security level of cryptography: The revised version of PSEC-2 (PSEC-KEM). Technical report, CRYPTREC, 2001. http://www. shiba. tao. go. jp/kenkyu/CRYPTREC/fy15/cryptrec20030424 outrep. html.

[60] Martínez, V. G., Encinas, L. H., & Muñoz, A. M. (2013). A comparative analysis of hybrid encryption schemes based on elliptic curves. *The Open Mathematics Journal*, *6*(1).

[61] Preneel, B., Biryukov, A., De Cannière, C., Örs, S. B., Oswald, E., Van Rompay, B., ... & Dent, A. (2004). Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. *Berlin Heidelberg NewYork London Paris Tokyo Hong Kong Barcelona Budapest: Springer-Verlag*.

[62] Galindo, D., Molleví, S. M., & Villar, J. L. (2004). Evaluating elliptic curve based KEMs in the light of pairings. IACR Cryptol. ePrint Arch., 2004, 84.