ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ & ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

"Ψηφιακές Πληρωμές στον Μετα-κβαντικό κόσμο"
"Digital Payments in a Post-Quantum World"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Μαυρογένη Γαρυφαλιά-Αγγελική

Επιβλέπων : : Μαλιάτσος Κωνσταντίνος, Επίκουρος Καθηγητής

Μέλη εξεταστικής επιτροπής: : Μαρία Καρύδα, Βασιλική Διαμαντοπούλου

Σάμος, [ΜΑΡΤΙΟΣ 2024]

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε κατά την χειμερινή περίοδο του Ακαδημαϊκού Έτους 2023-2024, στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών με τίτλο «Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων» του Τμήματος Μηχανικών Πληροφορικής του Πανεπιστημίου Αιγαίου. Η εργασία πραγματοποιήθηκε υπό την επίβλεψη του κ. Κωνσταντίνου Μαλιάτσου. Αντικείμενο της εργασίας αποτελεί η εφαρμογή της Κβαντικής Κρυπτογραφίας στα πλαίσια των σύγχρονων ψηφιακών πληρωμών.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν στην εκπόνηση της παρούσας διπλωματικής εργασίας. Οφείλω να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή κ. Κωνσταντίνο Μαλιάτσο για την καθοδήγηση και την πολύτιμη βοήθεια που προσέφερε σε όλα τα στάδια εκπόνησης της εργασίας αυτής.

Τέλος, θα ήθελα να ευχαριστήσω θερμά την οικογένεια και τους φίλους για την κατανόηση και συμπαράσταση που έδειξαν όλη αυτή την περίοδο.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Σχημάτων

Λίστα Πινάκων

Ακρωνύμια

NSA	National Security Agency
DES	Data Encryption Standard
RSA	Rivest-Shamir-Adleman
PGP	Pretty Good Privacy
ΥΔΚ	Υποδομή Δημοσίου Κλειδιού
PQC	Post Quantum Cryptography
ECDSA	Elliptic Curve Digital Signature
QKD	Quantum Key Distribution
DV-QKD	Discrete Variable Quantum Key Distribution
CV-QKD	Continuous Variable Quantum Key Distribution
TTP	Trusted Token Provider
GPS	Global Positioning System
TLS	Transport Layer Security
EMV	Europay Mastercard & Visa
CDA	Combined Data Authentication
SDA	Static Data Authentication
DDA	Dynamic Data Authentication
BDH	Blinded Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
KEM-TLS	Key Encapsulation Mechanism-Transport Layer Security
ct	Ciphertext
PQ KEM	Post Quantum Key Encapsulation Mechanism
TC	Κρυπτογράφημα
MAC	Message Authentication Code
CID	Current Interrupt Device
IPSEC	Internet Protocol Security
AES	Advanced Encryption Standard
API	Application Programming Interface
ECC	Elliptic Curve Cryptography
NIST	National Institute of Standards and Technology
ISO	International Organization for Standardization

Περίληψη

Η παρούσα διπλωματική εργασία αναφέρεται στον τρόπο με τον οποίο η Κβαντική Κρυπτογραφία μπορεί να εφαρμοστεί στις σύγχρονες ψηφιακές συναλλαγές. Ξεκινώντας γίνεται μια σύντομη αναδρομή στην ιστορία της Κρυπτογραφίας, ώστε να γίνει πλήρως κατανοητή η μετάβαση στα σημερινά δεδομένα. Παράλληλα εξετάζονται οι κατηγορίες και τα είδη των κρυπτογραφικών συστημάτων, καθώς και οι ιδιομορφίες που έχει το καθένα προκειμένου να κατανοήσουμε τον βαθμό στον οποίο αυτά μπορούν να συμβαδίσουν με την κβαντική μέθοδο. Γίνεται αναφορά στα κβαντικά πρωτόκολλα, καθώς και στα πλεονεκτήματα και μειονεκτήματά τους, όπως επίσης και κατατοπιστικά παραδείγματα για την πρακτική εφαρμογή τους στις ψηφιακές πληρωμές. Τέλος, παρουσιάζονται αναλυτικά οι προκλήσεις μετάβασης στην Κβαντική Κρυπτογραφία, αλλά και μερικά πεδία της που χρήζουν περαιτέρω έρευνας και δοκιμής.

Abstract

This project is about how Quantum Cryptography can be applied to synchronous digital transactions. Starting with a brief review of the history of Cryptography, in order to fully understand the transition to today's situation. At the same time, the categories and types of cryptographic systems are examined, as well as the peculiarities that each one has in order to understand the extent to which they can keep up with the quantum method. Reference is made to quantum protocols, as well as their advantages and disadvantages, and also illustrative examples of their practical application in digital payments. Finally, the challenges of moving to Quantum Cryptography are presented in detail, as well as some of its fields that need further research and testing.

1 *Εισαγωγή*

1.1 "Κβαντική Κρυπτογραφία και Ψηφιακές Πληρωμές»

Στην παρούσα διπλωματική εργασία μελετάμε το πώς η κβαντική κρυπτογραφία θα μπορέσει να εφαρμοστεί στις σύγχρονες ψηφιακές πληρωμές. Μελετάμε τα ήδη υπάρχοντα κρυπτογραφικά συστήματα, μαζί με τους αλγορίθμους που τα συνοδεύουν και εξετάζουμε τις τρωτότητες που αυτά παρουσιάζουν, αλλά και τους κινδύνους που ελοχεύουν. Δεδομένης της ιδιαίτερης φύσης των ψηφιακών πληρωμών η μετάβαση στην κβαντική μεθοδολογία πρέπει να γίνει με ομαλό τρόπο,καθώς και με πλήρη διαφάνεια απέναντι στους χρήστες. Η εξέλιξη των κβαντικών υπολογιστών είναι ιδιαίτερα αβέβαη όον αφορά το χρονικό διάστημα που θα διαρκέσει,με αποτέλεσμα να δυσχεραίνει ακόμη περισσότερο τα δεδομένα.

1.2 Αντικείμενο διπλωματικής

Πιο συγκεκριμένα στην εργασία αυτή θα μελετήσουμε λεπτομερώς τα ήδη υπάρχοντα κρυπτογραφικά συστήματα και το κατά πόσο αυτά είναι σε θέση να ικανοποιήσουν τις ανάγκες της σύγχρονης ψηφιακής εποχής. Έπειτα παρουσιάζονται κάποια πρωτόκολλα που σχετίζονται με ψηφιακές πληρωμές και εφαρμόζονται ακόμη και τώρα σε πληρωμές, αλλά και το πώς αυτά θα αλλάξουν αν μετεγκατασταθούμε στην κβαντική κρυπτογραφία. Δίνεται μάλιστα ένα χαρακτηριστικό παράδειγμα ανταλλαγής μηνυμάτων μέσω της κβαντικής κρυπτογραφίας ώστε να γίνει πιο κατανοητός ο τρόπος που λειτουργεί. Σε τελική φάση αναλύονται όλα τα σημεία που χρήζουν ιδιαίτερης προσοχής, προκειμένου να γίνει όσο το δυνατόν ομαλότερα αυτή η μετάβαση.

1.3 Δομή της διπλωματικής

Στο ΚΕΦΑΛΑΙΟ 1 ξεκινάμε με την ορολογία του όρου Κρυπτογραφία, κάνοντας μια σύντομη ιστορική αναδρομή και βλέποντας τα βασικότερα σημεία. Έπειτα περιγράφονται οι 2

μεγάλες κατηγορίες κρυπτογραφικών συστημάτων, μαζί με τα μειονεκτήματά τους, αλλά και το ποιοι είναι οι στόχοι τους συνολικά. Στο ΚΕΦΑΛΑΙΟ 2 ξεκινάμε βλέποντας πώς ακριβώς φτάσαμε στην κβαντική κρυπτογραφία, αλλά και το ποια είναι τα βασικά σχήματα-κατηγορίες της *Διανομής Κβαντικού Κλειδιού.* Λόγος γίνεται για τις βασικές αρχές κβαντικής επεξεργασίας των πληροφοριών. Συνεχίζουμε στο ΚΕΦΑΛΑΙΟ 3 με μια σύγκριση ανάμεσα στις κλασικές και στις κβαντικές πληρωμές και εξετάζουμε πώς λειτουργούν ορισμένα πρωτόκολλα με την κβαντική κρυπτογραφία. Κλείνοντας την εργασία στο ΚΕΦΑΛΑΙΟ 4 καταλήγουμε σε ορισμένα συμπεράσματα, βάσει όλων όσων έχουν αναφερθεί και επισημαίνονται κάποια κομμάτια που χρήζουν περαιτέρω έρευνας.

2

«Ορολογία»

Ο όρος ***κρυπτογραφία*** προέρχεται από τα συνθετικά μέρη "κρυπτός" και "γράφω", όπου μαζί με την *κρυπτολογία* αποτελούν κλάδους της *κρυπτανάλυσης.* Η κρυπτογραφία ασχολείται με την μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την προστασία του περιεχομένου των μηνυμάτων από το ευρύ κοινό. Αυτό που ουσιαστικά κάνει η κρυπτογραφία είναι να μετατρέπει πληροφορίες μέσω ενός μυστικού κώδικα από μια κανονική μορφή σε μια πιο *"δυσνόητη"* , όπου εάν δεν είναι γνωστός αυτός ο μυστικός κώδικας η αρχική πληροφορία θα παραμένει ακατανόητη.

Στα αρχικά στάδια ανάπτυξης της κρυπτογραφίας η επεξεργασία των μηνυμάτων βασιζόταν στην γλωσσική τους υποδομή, όμως μετέπειτα εγκαταλείφθηκε αυτή η μέθοδος και προχωρήσαμε σε αριθμητικούς αλγορίθμους. Μεγαλύτερη έμφαση έχει δοθεί σε κλάδους των Μαθηματικών όπως είναι *η Θεωρία Αριθμών, τα Διακριτά Μαθηματικά, η Θεωρία της Πληροφορίας, η Υπολογιστική Πολυπλοκότητα, η Στατιστική και η Συνδυαστική Ανάλυση.*

2.1«Στόχοι Κρυπτογραφίας»

- **Εμπιστευτικότητα**: Η μετατροπή της πληροφορίας σε μη κατανοητή μορφή μέσω ενός αλγορίθμου την καθιστά προσβάσιμη μόνο σε εξουσιοδοτημένους παραλήπτες, οι οποίοι με τη βοήθεια του αλγορίθμου θα ανακαλύψουν την αρχική μορφή της πληροφορίας.
- **Ακεραιότητα**: Οποιαδήποτε "αλλοίωση" - "αλλαγή" μπορεί να πραγματοποιηθεί μονάχα από νόμιμους χρήστες. Σε περίπτωση που πραγματοποιηθεί κάποια τροποποίηση από μη εξουσιοδοτημένο χρήστη, αυτή η τροποποίηση πρέπει οπωσδήποτε να είναι ανιχνεύσιμη.
- **Μη αποποίηση**: Ο παραλήπτης δεν θα μπορεί να αρνηθεί την μετάδοση της πληροφορίας και αντίστοιχα ο αποστολέας δεν θα είναι σε θέση να αρνηθεί την δημιουργία της.
- **Πιστοποίηση**: Αμφότεροι αποστολέας και παραλήπτης είναι σε θέση να επιβεβαιώνουν αμοιβαία τις ταυτότητες τους , καθώς και την πηγή/προορισμό της πληροφορίας έτσι ώστε να είναι σίγουροι ότι δεν έχουν να κάνουν με πλαστές ταυτότητες.

2.2«Η Κρυπτογραφία από το 1949 μέχρι σήμερα»

Η κρυπτογραφία είναι μια έννοια που είχε ήδη αναφερθεί από τον Ηρόδοτο στα χρόνια των Περσικών Πολέμων. Έπαιξε σημαντικό ρόλο στην εξέλιξη της παγκόσμιας ιστορίας και

μάλιστα μέχρι σήμερα αποτελεί ανάγκη του απλού ανθρώπου. Γυρνώντας αρκετά χρόνια πίσω και συγκεκριμένα στο 1950, παρατηρείται το πόσο σημαντική ήταν η συμβολή των Μαθηματικών και συγκεκριμένα ο κλάδος της Θεωρίας Αριθμών. Η κρυπτογραφία κυρίως ήταν χρήσιμη σε κυβερνήσεις και στρατιωτικούς, όσον αφορά την κατασκοπεία και την έκβαση πολέμων. Αδιαμφισβήτητα *πατέρας* των μαθηματικών συστημάτων κρυπτογραφίας είναι ο *Claud Shannon,* ο οποίος το 1949 δημοσίευσε το έγγραφο "*Θεωρία Επικοινωνίας των Συστημάτων Μυστικότητας*"(Communication Theory of Secrecy Systems). Μάλιστα ήταν αυτός που καθιέρωσε μια σταθερή θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση.

Η αλήθεια είναι πως τη δεκαετία 50-60 σημειώθηκαν ελάχιστες εξελίξεις, όπως για παράδειγμα το ότι *από το 1960 και έπειτα κάθε εταιρία χρησιμοποιούσε το δικό της τρόπο κρυπτογράφησης*. Αντίθετα, από την δεκαετία του 70 και έπειτα είχαμε πληθώρα νέων πληροφοριών και εξελίξεων. Πιο συγκεκριμένα:

- ***1975:*** *Κρυπτογράφηση Εωσφόρος IBM:*
  - Η σειρά των δυαδικών ψηφίων χωρίζεται σε 64-άδες
  - Σε κάθε 64-άδα τα ψηφία διατάσσονται σε
  - 32-άδες
  - Μέσω μεταθέσεων γίνονται αλλαγές στη σειρά των ψηφίων
  - Προστίθεται η νέα σειρά των ψηφίων στην παλαιά
  - Η παραπάνω διαδικασία πραγματοποιείται
  - 16 φορές
  - **Κλειδί**: Ο τρόπος που ακολουθούμε για να φτάσουμε στην τελευταία 64-άδα

- Δημιουργία της NSA(National Security Agency): Κρατική κεντρική υπηρεσία του Υπουργείου Άμυνας των ΗΠΑ , που είναι αρμόδια για την προστασία των κυβερνητικών πληροφοριακών συστημάτων.
- **Horst Feistel**(1915-1990): κρυπτογράφος, ο οποίος εργάστηκε στους ciphers.
- Έναρξη ποικίλων ερευνών που κορυφώθηκαν με την ανακάλυψη του DES(Data Encryption Standard).
- **Whitfield Diffie**: Αφιερώθηκε κυρίως στο σημαντικότερο κομμάτι της κρυπτογραφίας που είναι η μεταφορά του κλειδιού.
- **Clifford Christopher Cocks:** Βρετανός μαθηματικός και κρυπτογράφος, ο οποίος το 1973 εφηύρε αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού , γνωστός ως RSA.
- 1976: Diffie και Hellman παίρνουν βραβείο στο Διεθνές Συνέδριο Πληροφορικής.
  - **Philip Zimmermann**: Επιχείρησε να ενθαρρύνει την κρυπτογράφηση για τη διαφύλαξη του προσωπικού απορρήτου και για αυτόν ακριβώς το λόγο η NSA κινήθηκε νομικά εναντίον του. Το 1990 εφηύρε το Pretty Good Privacy (PGP) , το οποίο συνδυάζει το RSA με το κλασικό DES.

2.3«Κρυπτογραφικά Συστήματα»

Ένα από τα σημαντικότερα κομμάτια που μας απασχολούν είναι η ισχύς των κρυπτογραφικών συστημάτων. Την απάντηση έρχεται να δώσει *η αρχή του Kerchoff:* "Η ασφάλεια ενός κρυπτοσυστήματος δεν εξαρτάται από την μυστικότητα του αλγορίθμου κρυπτογράφησης, αλλά έγκειται στο κατά πόσο μπορεί να διατηρηθεί μυστικό το *κλειδί.*" Είναι σημαντικό να τονιστεί το ότι η *ισχύς* του αλγορίθμου προέρχεται από την *μυστικότητα του κλειδιού, το μήκος του, τον αλγόριθμο,* αλλά και με το πώς λειτουργούν αυτά από κοινού. Η *ισχύς έχει να κάνει με τη δυσκολία στον υπολογισμό του αλγορίθμου ή του κλειδιού.*

Ο *Shannon* θεμελιώνοντας την *Θεωρία της Πληροφορίας,* το 1949 εξέφρασε ορισμένα κριτήρια τα οποία καθιστούν έναν αλγόριθμο κρυπτογράφησης άρτια σχεδιασμένο. Τα κριτήρια του είναι τα εξής:

- *Βαθμός κρυπτογραφικής ασφάλειας:* Έχει να κάνει με το ποιες πληροφορίες εκμαιεύει ο αντίπαλος όταν παρατηρεί το κρυπτοκείμενο.
- Μήκος κλειδιού: Το μήκος του κλειδιού επηρεάζει το κατά πόσο είναι εύκολο να τα διαχειριστούμε.
- Ευκολία εκτέλεσης κρυπτογράφησης & αποκρυπτογράφησης: Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης πόσο χρόνο απαιτούν, αλλά και ποιες λειτουργίες απαιτείται να εκτελεστούν.
- Διόγκωση κρυπτοκειμένου: Θέλουμε το κρυπτοκείμενο μας να έχει ίδιο μήκος με το αρχικό ή έστω συγκρίσιμο μέγεθος με το αρχικό ;
- Διάδοση σφαλμάτων κρυπτογράφησης: Ιδανικά αυτό που πρέπει να συμβαίνει είναι το οποιοδήποτε σφάλμα στην κρυπτογράφηση να επηρεάζει στο ελάχιστο την έκβαση της αποκρυπτογράφησης.

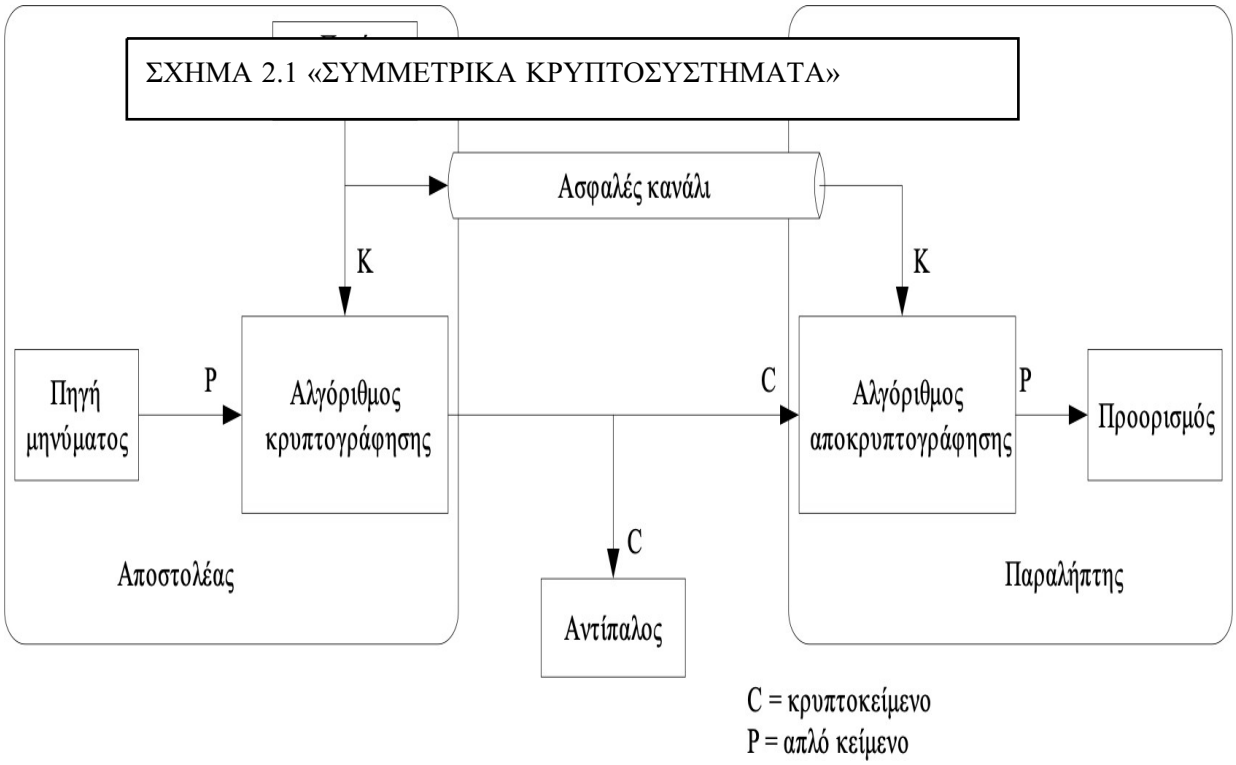
Είναι βέβαια γεγονός το ότι στα περισσότερα συστήματα κρυπτογράφησης δεν είναι εφικτό να πληρούνται όλες οι προηγούμενες ιδιότητες. Δύο πάντως είναι οι καθοριστικές ιδιότητες της κρυπτογραφικής ισχύος: η διάχυση και η σύγχυση. Όσον αφορά την διάχυση , αυτή σχετίζεται με την ικανότητα του αλγορίθμου να χρησιμοποιήσει ένα συγκεκριμένο τμήμα του αρχικού κειμένου και να καταφέρει να επηρεάσει όσο το δυνατόν περισσότερα κομμάτια του κρυπτοκειμένου. Η σύγχυση από την άλλη είναι η ικανότητα του αλγορίθμου να "μπερδέψει" τον αντίπαλο και έτσι αν γίνει κάποια αλλαγή στο αρχικό κείμενο να ΜΗΝ είναι εύκολο να προβλεφθεί η αντίστοιχη αλλαγή στο κρυπτοκείμενο.

2.1 «Κατηγορίες Κρυπτογραφικών Συστημάτων»

Τα κρυπτογραφικά συστήματα χωρίζονται σε 2 κατηγορίες: τα **συμμετρικά** και **τα ασύμμετρα**

2.4.1 «Συμμετρικά Κρυπτοσυστήματα»

- Μερικές εναλλακτικές ονομασίες τους είναι: συστήματα συμμετρικού κλειδιού (symmetric-key), μονού κλειδιού (single-key) και μυστικού κλειδιού (secret-key), ακριβώς επειδή το κλειδί κρυπτογράφησης και αποκρυπτογράφησης είναι κοινό. Το αρχικό κείμενο εισάγεται στον αλγόριθμο μαζί με το κλειδί και έτσι προκύπτει το κρυπτοκείμενο. Αντίστοιχα η διαδικασία αποκρυπτογράφησης δέχεται ως είσοδο το κρυπτοκείμενο και το κοινό κλειδί. Με λίγα λόγια εφαρμόζονται οι αντίστροφες διαδικασίες για την αποκρυπτογράφηση του αρχικού κειμένου.

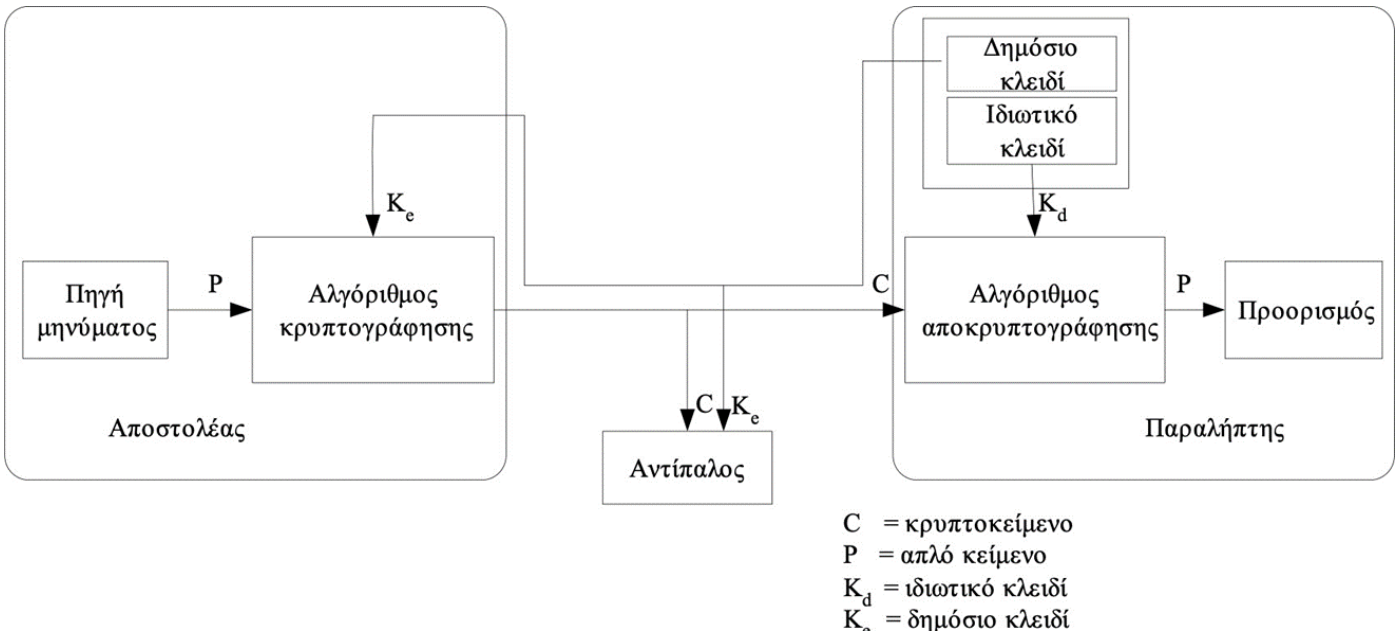


Από το προηγούμενο σχήμα παρατηρούμε ότι είναι αναγκαίο αποστολέας και παραλήπτης να διαθέτουν μια ασφαλή μέθοδο ώστε να μοιράζονται την κοινή μυστική πληροφορία, που είναι το κλειδί. Στο σημείο αυτό δημιουργείται το ερώτημα: *"Γιατί να κρυπτογραφηθεί το μήνυμα από τη στιγμή που θεωρητικά υπάρχει ασφαλές κανάλι επικοινωνίας;"*. Άλλο αδύναμο σημείο των συμμετρικών συστημάτων είναι η ανεπάρκεια τους σε περιπτώσεις ανοικτών δικτύων επικοινωνίας, στα οποία είναι μεγάλο το πλήθος των μελών. Το συγκεκριμένο πρόβλημα είναι

γνωστό και ως *"πρόβλημα τετραγώνου"*

2.4.2 *«Ασύμμετρα Κρυπτοσυστήματα»(Συστήματα δημοσίου κλειδιού)*

Σε αυτά τα κρυπτοσυστήματα ο αλγόριθμος κρυπτογράφησης είναι ίδιος με τον αλγόριθμο αποκρυπτογράφησης, με τη διαφορά ότι στην αποκρυπτογράφηση χρησιμοποιείται διαφορετικό κλειδί. Βασίζεται κυρίως σε μαθηματικές υποθέσεις μιας και ανάμεσα σε δημόσιο(κρυπτογράφηση) και ιδιωτικό (αποκρυπτογράφηση) κλειδί υπάρχουν μαθηματικές εξαρτήσεις.



ΣΧΗΜΑ 2.2 «ΑΣΥΜΜΕΤΡΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ»

Να τονιστεί ότι στα ασύμμετρα κρυπτογραφικά συστήματα το *δημόσιο κλειδί* διατίθεται ελεύθερα , χωρίς να απαιτείται ασφαλές κανάλι επικοινωνίας, ενώ το *ιδιωτικό κλειδί* παραμένει στην κατοχή του παραλήπτη. Εν ολίγοις στα ασύμμετρα κρυπτοσυστήματα δεν υπάρχει ασφαλές κανάλι. Η ασύμμετρη κρυπτογράφηση βασίζεται σε μια *one-way συνάρτηση* για την οποία είναι απλό να βρεθεί η τιμή της αλλά δύσκολο να αντιστραφεί. Δηλαδή: *για δοθέν yi, δεν μπορεί να βρεθεί xi, τέτοιο ώστε f(xi)=yi.* Για να ήμασταν σε θέση να αντιστρέψουμε τη συνάρτηση, θα

έπρεπε να γνωρίζαμε μια πρόσθετη πληροφορία, δηλαδή να είχαμε μια *συνάρτηση με καταπακτή(trapdoor).* Μάλιστα οι *trapdoor συναρτήσεις* αποτελούν τη βάση των Συστημάτων Δημοσίου Κλειδιού. Αξίζει να αναφερθούν ορισμένοι *συμμετρικοί αλγόριθμοι,* οι οποίοι τη δεδομένη χρονική στιγμή έχουν καθαρά **εμπορική χρήση:**

ΠΙΝΑΚΑΣ ΣΥΜΜΕΤΡΙΚΩΝ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΩΝ(*Πίνακας 1)*

ΑΛΓΟΡΙΘΜΟΣ	**ΜΗΚΟΣ ΚΛΕΙΔΙΟΥ**	**ΙΣΧΥΣ**	**ΠΑΡΑΤΗΡΗΡΣΕΙΣ**
DES	64	Αδύναμος	Πρότυπο ασυμ. Κρυπτ., ο οποίος είναι ο πιο διαδεδομένος block cipher
3DES	161,112,168	Ισχυρός	Τριπλή κρυπτογράφηση του κειμένου με διαφορετικό κλειδί κάθε φορά
AES	28,192,256	Ισχυρός	Επέκταση του DES
IDEA	64,128	Ισχυρός	Φτιάχτηκε το 1990 από τους Lai & Massey, έχει παρόμοια δομή με τον DES
BLOWFISH	32,448	Αδύναμος	Φτιάχτηκε από τον Schneier, έχει μεταβλητό μήκος κλειδιού, ταχύτερος του DES
RC5	32,64,128	Αδύναμος	Φτιάχτηκε από τον Ron Rivest για τη εταιρία RSA.Έχει μεταβλητό μήκος κλειδιού

2.4.3 «Μειονεκτήματα Υποδομής Δημοσίου Κλειδιού»

Η Υποδομή Δημοσίου Κλειδιού(*Public Key Infrastructure*), παρουσιάζει αρκετές αδυναμίες. Μερικές εξ' αυτών είναι οι παρακάτω:

- Πολυπλοκότητα: Τα συστατικά μέρη μιας υποδομής δημοσίου κλειδιού είναι ποικίλα, όπως για παράδειγμα το εργατικό δυναμικό, καθώς και τα συστήματα υλικού και λογισμικού. Τα συστήματα αυτά δεν είναι δυνατό να ενσωματωθούν με τρόπο αποσπασματικό.
- Κόστος: Οι δαπάνες για την επέκταση μιας υποδομής δημοσίου κλειδιού(ΥΔΚ) εξαρτώνται από το πώς ο εκάστοτε οργανισμός έχει σκοπό να χρησιμοποιήσει την ΥΔΚ.
- Αποδοχή Χρηστών: Ένα ευνοϊκό σημείο της ΥΔΚ είναι ότι χρησιμοποιεί τα ίδια πιστοποιητικά για να επικυρώσει ανθρώπους και συσκευές. Σημαντικό ρόλο παίζει εδώ το κατά πόσο η ΥΔΚ γίνεται αποδεκτή από τους χρήστες, διότι εάν δεν υπάρχει η απαιτούμενη αποδοχή, με την έννοια ότι δεν ακολουθούνται οι πολιτικές και τα μέτρα ασφαλείας, τότε το σύστημα οδηγείται τόσο σε εξωτερικές , όσο και σε εσωτερικές επιθέσεις.
- Κλιμάκωση: Η ΥΔΚ οφείλει να είναι σε θέση να υποστηρίζει και μικρό αλλά και μεγάλο αριθμό χρηστών.
- Εφαρμογές: Ένα σημαντικό ζήτημα είναι η δημιουργία εφαρμογών, οι οποίες να αποτελούν πόλο έλξης για τους χρήστες, με αποτέλεσμα να παρακινούν τους χρήστες να χρησιμοποιούν την ΥΔΚ, αλλά και να επενδύουν χρόνο στην εφαρμογή και διατήρηση της. Εν ολίγοις η ΥΔΚ χρειάζεται τις εφαρμογές και αντίστοιχα οι εφαρμογές χρειάζονται την ΥΔΚ.
- Ετερογένεια: Η ΥΔΚ θα πρέπει να υποστηρίζει ένα ευρύ φάσμα λειτουργικών συστημάτων, μηχανημάτων αλλά και πελατών.
- Εμπιστοσύνη: Στόχος της ΥΔΚ είναι να καταφέρει να υλοποιήσει τις κρίσεις εμπιστοσύνης

2.4.4 *«Μειονεκτήματα Συμμετρικών Κρυπτοσυστημάτων»*

- Εάν το συμμετρικό κλειδί "πέσει" στα χέρια ενός κακόβουλου χρήστη, τότε εκείνος θα είναι σε θέση να αποκρυπτογραφήσει όλα τα κρυπτογραφημένα περιεχόμενα.
- Η συμμετρική κρυπτογράφηση σε αμφίδρομες επικοινωνίες θέτει σε κίνδυνο και τις δύο πλευρές.
- Δεδομένου ότι η επικοινωνία αποστολέα και παραλήπτη βασίζεται στην συμφωνία ενός κοινού κλειδιού, η ασφάλεια των συστημάτων αυτών βασίζεται στην μυστικότητα του κλειδιού, δηλαδή σε ένα ασφαλές κανάλι επικοινωνίας. Για όσο διάστημα επιθυμούμε να διατηρηθεί η επικοινωνία, είμαστε υποχρεωμένοι να διατηρήσουμε μυστικό το κλειδί.
- Η μετάδοση πληροφοριών μέσω του Διαδικτύου δεν είναι ιδιαίτερα ασφαλής μιας και οποιοσδήποτε έχει τα κατάλληλα μέσα είναι σε θέση να εκμαιεύσει πληροφορίες που ανταλλάσσονται.
- Ένας κακόβουλος χρήστης είναι σε θέση επίσης να τροποποιεί και να πλαστογραφεί όλα τα μηνύματα που ανταλάσσουν οι 2 ανυποψίαστοι χρήστες.

3

3.1 «Ιστορική Αναδρομή της Post Quantum Cryptography(PQC)»

Το Nist ενέκρινε τους αλγορίθμους RSA & ECDSA ως κύριους αλγορίθμους δημοσίου κλειδιού και ψηφιακής υπογραφής αντίστοιχα. Ωστόσο, λόγω της εξέλιξης των κβαντικών υπολογιστών και του κρυπταναλυτικού κινδύνου, το NIST κατέληξε στο συμπέρασμα ότι μια εντελώς κβαντική ανθεκτική κρυπτογράφηση(όπως η PQC) έπρεπε να αντικαταστήσει την ήδη υπάρχουσα. Τον Δεκέμβριο του 2016, το NIST ανακοίνωσε την πρόσκληση για αλγορίθμους PQC και ένα σχέδιο για μετάβαση σε νέους αλγορίθμους, μετά τη δημιουργία ενός νέου προτύπου. . Το NIST και η National Security Agency(Υπηρεσία Εθνικής Ασφάλειας) προέβλεψαν ότι ίσως και να χρειαστούν 20-30 χρόνια για να ολοκληρωθεί η μετάβαση στους νέους αλγορίθμους, εξαιτίας του μεγάλου κύκλου ζωής των κυβερνητικών συστημάτων πληροφορικής. Συνυπολογίστηκε επίσης και ο κίνδυνος της εμφάνισης των κβαντικών υπολογιστών πολύ νωρίτερα από το προβλεπόμενο. Η πρόσκληση υποβολής προτάσεων έληξε τον Νοέμβριο του 2017. Οι αλγόριθμοι περιελάμβαναν μηχανισμούς δημοσίου κλειδιού, ενθυλάκωσης και ψηφιακής υπογραφής. Το NIST επέλεξε 29 από τους αλγορίθμους που παρουσιάστηκαν και σε δεύτερη φάση μονάχα 15(7 τελικοί & 8 αναπληρωματικοί). Δηλώθηκε μάλιστα από το NIST η σημαντικότητα της ποικιλομορφίας της PQC, ώστε να αποφευχθεί ο κίνδυνος μιας καινοτομίας που θα "σπάσει" τους αλγορίθμους.

(Finalists: 7)

	Name of algorithm	Underlying mathematical problem	Institution which submitters joined
Public-key encryption/KEM	CRYSTALS-KYBER	Lattice problem (e.g., SVP)	Radboud University
	NTRU		University of Waterloo
	SABER		KU Leuven, etc.
	Classic McEliece	Error correcting code problem	Eindhoven University of Technology, etc.
Digital signature	CRYSTALS-DILITHIUM	Lattice problem (e.g., SVP)	IBM Research
	FALCON		Thales Communications & Security, etc.
	Rainbow	MQ problem	University of Cincinnati

Πίνακας 2 «Τελικοί Αλγόριθμοι του NIST»

(Alternate candidates: 8)

	Name of algorithm	Underlying mathematical problem	Institution which submitters joined
Public-key encryption/KEM	FrodoKEM	Lattice problem (e.g., SVP)	Microsoft Research
	NTRU Prime		Eindhoven University of Technology, etc.
	BIKE	Error correcting code problem	Intel Corporation, etc.
	HQC		University of Limoges, etc.
	SIKE	Isogeny graph path-finding problem	University of Waterloo
Digital signature	GeMSS	MQ problem	Sorbonne University, etc.
	Picnic	Symmetric-key decryption problem	Microsoft Research
	SPHINCS+	Hash function collision search problem	Eindhoven University of Technology

Πίνακας 3 «Αναπληρωματικοί Αλγόριθμοι του NIST»

- **«Post Quantum Cryptography»**

Η κρυπτογράφηση Δημοσίου Κλειδιού έχει ποικίλα μειονεκτήματα, όπως για παράδειγμα ότι είναι δύσκολη η εφαρμογή της σε συσκευές χαμηλής μνήμης και περιορισμένων διεργασιών. Το *Μοντέλο Αναφοράς Ανοικτού Συστήματος(Open System Inter-connection, OSI)* ορίζει 7

στρώματα , από τα οποία τα 5 σχετίζονται με θέματα ασφαλείας. Μάλιστα στο αρχικό μοντέλο OSI δεν γινόταν καν λόγος για θέματα ασφαλείας. Αυτά άρχισαν να αναφέρονται από το πρότυπο X.800. Παρόλα αυτά η *Ασφάλεια Φυσικού Επιπέδου(Physical Layer Security,PLS)* και η *Διανομή Κβαντικού Κλειδιού(Quantum Key Distribution)* δεν έχουν φανεί στο συγκεκριμένο πρότυπο. Η χρήση των *PLS* και *QKD* είναι σε θέση να βελτιώσει τα ζητήματα ασφαλείας σε αυτά τα 5 επίπεδα του OSI , αλλά επίσης υπάρχει η δυνατότητα και για ανεξάρτητη λειτουργία ανάμεσα σε *PLS* και *QKD.*

3.2 «Βασικά Στοιχεία του Quantum Key Distribution (QKD)»

Είναι γεγονός ότι ο κβαντικός υπολογισμός αποτελεί μια μεγάλη πρόκληση για τα σύγχρονα συστήματα κυβερνοασφάλειας. Το QKD με συμμετρική κρυπτογράφηση μπορεί να θεωρηθεί ως ένα από τα σχήματα ασφαλείας φυσικού επιπέδου που παρέχει αποδεδειγμένη ασφάλεια απέναντι σε επιθέσεις που εκκινούνται από κβαντικούς υπολογιστές. Το πρώτο QKD σχήμα εισήχθη από τους Bennett και Brassard, οι οποίοι το 1984 πρότειναν το πρωτόκολλο που είναι γνωστό ως BB84. Η ασφάλεια στο QKD έγκειται στους νόμους κβαντικής μηχανικής. Διαφορετικοί βαθμοί ελευθερίας σε φωτόνια(όπως πόλωση και τροχιακή γωνιακή ορμή) , χρησιμοποιούνται στην εφαρμογή διαφόρων πρωτοκόλλων.

«Βασικά Σχήματα QKD»

A. Διακριτή Μεταβλητή Discrete Variable QKD: Ένας ανιχνευτής ενός φωτονίου(*Single-Photon Detector)* εφαρμόζεται στην πλευρά του Bob(*παραλήπτης)* , με αποτέλεσμα να επιτυγχάνεται η άνευ όρων ασφάλεια μέσω του *Θεωρήματος Μη-Κλωνοποίησης* και του *Θεωρήματος Δυσδιάκριτης Ικανότητας Αυθαίρετων Κβαντικών Καταστάσεων.* Το *Θεώρημα Μη- Κλωνοποίησης* ισχυρίζεται ότι οι αυθαίρετες κβαντικές καταστάσεις δεν μπορούν να κλωνοποιηθούν- αντιγραφούν, υποδεικνύοντας ότι η Eve δεν μπορεί να αντιγράψει ορθογώνιες κβαντικές καταστάσεις ακόμα και με τη χρήση κβαντικού υπολογιστή. Από την άλλη πλευρά το *Θεώρημα Δυσδιάκριτης Ικανότητας Αυθαίρετων Κβαντικών Καταστάσεων* υποστηρίζει ότι οι μη-ορθογώνιες καταστάσεις δεν διακρίνονται με σαφήνεια. Δηλαδή όταν η Eve αλληλεπιδράσει στην προσπάθεια της να πάρει πληροφορίες, θα διαταράξει την πιστότητα των κβαντικών καταστάσεων που θα ανιχνεύσει ο Bob(*παραλήπτης).*

- **Κβαντική Κατάσταση**: Μια αφηρημένη έννοια την οποία χρησιμοποιούμε για να περιγράψουμε σε ποια ακριβώς κατάσταση βρίσκεται ένα κβαντικό αντικείμενο. Η κβαντική κατάσταση αναπαρίσταται από ένα μαθηματικό αντικείμενο, όπως μια κυματοσυνάρτηση ή ένα density operator(τελεστής πυκνότητας που βοηθά στον εξορθολογισμό υπολογισμών στην κβαντομηχανική πολλών σωματιδίων).

B. . Συνεχής Μεταβλητή Continuous Variable QKD: Στο σχήμα αυτό χρησιμοποιείται η *αρχή της αβεβαιότητας,* η οποία θεωρεί ότι τόσο τα στοιχεία εντός φάσης, όσο και τα τετραγωνικά στοιχεία μιας συνεκτικής κατάστασης δεν μπορούν να μετρηθούν ταυτόχρονα με πλήρη ακρίβεια. Να τονιστεί ότι αυτό το είδος σχήματος δεν

περιορίζεται χρονικά. Καθώς μη-ορθογώνιες καταστάσεις μεταδίδονται ανάμεσα σε Alice και Bob και ελέγχοντας για διαταραχή στην κατάσταση εκπομπής, η οποία διαταραχή προκαλείται από το κανάλι ή από δραστηριότητα της Eve, μπορούν να καθορίσουν ένα ανώτερο όριο υποκλοπής/θορύβου στο κανάλι κβαντικής επκοινωνίας. Όσον αφορά το όριο για το μέγιστο αποδεκτό ποσοστό σφάλματος αυτό εξαρτάται από την αποτελεσματικότητα των καλύτερων βημάτων μετά την επεξεργασία.

3.2 «Γενικές Κατηγορίες του QKD»

a) Device-dependent QKD: Τυπικά η κβαντική πηγή τοποθετείται στην πλευρά της Alice(αποστολέας) και ο κβαντικός ανιχνευτής στην πλευρά του Bob(παραλήπτης). Οι δημοφιλείς κατηγορίες περιλαμβάνουν DV-QKD, CV-QKD, υποβοηθούμενη από εμπλοκή QKD, αναφορά κατανεμημένης φάσης και πολλές άλλες.

b) Source-device independent QKD: Στην κβαντική πηγή τοποθετείται η πλευρά της Eve, ενώ οι κβαντικοί ανιχνευτές τοποθετούνται στις πλευρές των Alice και Bob.

c) Measurement-device independent QKD: Οι κβαντικοί ανιχνευτές τοποθετούνται στην πλευρά της Eve, ενώ οι κβαντικές πηγές διατάσσονται στην πλευρά της Alice και του Bob. Οι κβαντικές καταστάσεις προετοιμάζονται στις πλευρές των νόμιμων επικοινωνούντων οντοτήτων(Alice & Bob) και μεταδίδονται προς τους ανιχνευτές της Eve. Η Eve με τη σειρά της πραγματοποιεί κάποιες μετρήσεις και έπειτα ανακοινώνει πότε εντοπίζονται οι επιθυμητές καταστάσεις.

Το QKD είναι ικανό να επιβάλει την άνευ όρων ασφάλεια, πράγμα που σημαίνει ότι η ασφάλεια του επαληθεύεται χωρίς περιορισμούς ούτε στην υπολογιστική ισχύ της Eve, αλλά ούτε και στην στρατηγική υποκλοπής. Η πιο συνηθισμένη κατάσταση είναι αυτή στην οποία η Alice και ο Bob διατηρούν το κλειδί αναφοράς και στέλνουν τις κλασικές πληροφορίες στο άλλο μέρος μέσω ενός καναλιού. Παράλληλα το άλλο μέρος εκτελεί συγκεκριμένη διαδικασία πάνω στα δεδομένα , δίχως να παρέχει ανάδραση.

3.4 «Post Quantum Information Theory»

Στην κβαντομηχανική οι βασικές απροσδιόριστες έννοιες είναι το φυσικό σύστημα, το παρατηρήσιμο και η κατάσταση. Ένα φυσικό σύστημα είναι οποιοδήποτε επαρκώς απομονωμένο κβαντικό αντικείμενο, όπως ένα ηλεκτρόνιο, ένα φωτόνιο ή ένα μόριο. Το παρατηρήσιμο σχετίζεται με μια μετρήσιμη ιδιότητα ενός φυσικού συστήματος , όπως για παράδειγμα η ενέργεια. Τέλος, η κατάσταση ενός φυσικού συστήματος είναι περισσότερο πολύπλοκη έννοια και κυρίως όταν ασχολούμαστε με σύνθετα φυσικά συστήματα. Συγκεκριμένα, υπάρχουν καταστάσεις στις οποίες κανένα από τα υποσυστήματα δεν είναι σε καθορισμένη κατάσταση. Οι κατηγορίες των καταστάσεων που συναντάμε είναι: *καθαρή* και *μικτή*.

3.4.1 «Βασικές Αρχές Κβαντικής Επεξεργασίας Πληροφοριών(Quantum Information Processing Fundamentals)»

Γραμμική Υπέρθεση(Linear Superposition): Σε αντίθεση με το τετριμμένο bit, το κβαντικό bit ή αλλιώς qubit μπορεί να λάβει πέρα από τις διακριτές τιμές 0 και 1 και άλλους πιθανούς συνδυασμούς τους. Αυτό βασίζεται σε μια ιδιότητα των κβαντικών καταστάσεων, που αναφέρει το εξής: "Είναι εφικτό να δημιουργηθεί μια γραμμική υπέρθεση της κβαντικής κατάστασης |0> και της κβαντικής κατάστασης |1>.

|0>: Το διάνυσμα (0,1)

|1>: Το διάνυσμα (1,0)

Κβαντικός Παραλληλισμός(Quantum Parallelism): Πρόκειται για μια δυνατότητα εκτέλεσης μεγάλου αριθμού λειτουργιών *ταυτόχρονα,* που είναι και η ειδοποιός διαφορά από τον κλασικό υπολογισμό. Στους κλασικούς υπολογιστές υπάρχει η δυνατότητα να γνωρίζουμε την εσωτερική κατάσταση του υπολογιστή. Στον αντίποδα, εξαιτίας του Θεωρήματος Μη-Κλωνοποίησης , δεν είμαστε σε θέση να γνωρίζουμε την τρέχουσα κατάσταση του κβαντικού υπολογιστή. Αυτό έχει οδηγήσει στην ανάπτυξη του *Αλγορίθμου Παραγοντοποίησης Schor ,* ο οποίος χρησιμοποιείται για να σπάσει το πρωτόκολλο κρυπτογράφησης *RSA(Rivest-Shamir-Adleman).* Υπάρχουν κβαντικοί αλγόριθμοι οι οποίοι αξιοποιούν τον *Αλγόριθμο Αναζήτησης Grover* , που βοηθά στην εκτέλεση αναζήτησης σε μια βάση δεδομένων μη- δομημένη. Ο κβαντικός υπολογιστής μπορεί να κωδικοποιεί τις εισαγόμενες σειρές εισόδου *μήκους N* παράλληλα σε ένα μόνο βήμα υπολογισμού. Η ιδιότητα αυτή τον καθιστά σαφώς ισχυρότερο από τον κλασικό.

Entanglement("Διεμπλοκή ή εναγκαλεισμός"):Σε κβαντικό επίπεδο φαίνεται πως 2 κβαντικά αντικείμενα μπορούν να σχηματίσουν 1 ενιαία οντότητα, ακόμη και στην περίπτωση που μεταξύ τους είναι άρτια διαχωρισμένα. Εάν επιχειρήσουμε αυτή την ενιαία οντότητα να την θεωρήσουμε ως συνδυασμό 2 ανεξάρτητων κβαντικών αντικειμένων, θα αποτύχουμε. Η μοναδική εξαίρεση είναι στην περίπτωση που επιτρέπεται η διάδοση σήματος σε υπερφωτεινή ταχύτητα. Τα κβαντικά αντικείμενα δεν θα είναι σε θέση να αποσυντεθούν σε μεμονωμένα ανεξάρτητα κβαντικά αντικείμενα. Αυτός είναι και ο λόγος που ονομάζονται "μπλεγμένα αντικείμενα". Αποδεικνύεται ότι η ποσότητα των πληροφοριών που υπάρχουν σε μια "μπερδεμένη" κατάσταση N-qubits, αυξάνεται εκθετικά και όχι γραμμικά, όπως θα συνέβαινε με τα κλασικά bit.

3.4.2 «Εναρμόνιση Πληροφοριών και Ενίσχυση Ασφάλειας»

Δεδομένου ότι το ακατέργαστο κλειδί είναι ατελές, είναι απαραίτητο να εκτελεστεί εναρμόνιση πληροφοριών και να ενισχυθεί το απόρρητο έτσι ώστε να εξασφαλιστεί η συσχέτιση των ακολουθιών X που δημιουργήθηκαν από την Alice(αποστολέας) και των αντίστοιχων Y που έλαβε ο Bob(παραλήπτης).Παράλληλα μειώνει τις αμοιβαίες πληροφορίες της Eve αναφορικά με

το επιθυμητό επίπεδο ασφάλειας. Η συμφωνία πληροφοριών δεν είναι τίποτα άλλο πέρα από την διόρθωση σφάλματος που εκετλείται μέσω ενός δημόσιου καναλιού, το οποίο εναρμονίζει τα σφάλματα ανάμεσα στις ακολουθίες X και Y. Με αυτό τον τρόπο αποκτάται μια συμβολοσειρά από bit K, ενώ ταυτόχρονα όσο το δυνατόν λιγότερες πληροφορίες στην Eve. Η ενίσχυση απορρήτου χρησιμοποιείται από την Alice και τον Bob για να πάρει από το K ένα μικρότερο σύνολο bits S, των οποίων η συσχέτιση με την συμβολοσειρά Z της Eve έχει κάποιο άνω φράγμα. Για το σκοπό αυτό υπάρχουν οι *συναρτήσεις κατακερματισμού G* , των οποίων η λειτουργία είναι οι εξής: Αντιστοιχίζουν το σύνολο των συμβολοσειρών n-bit A σε ένα σύνολο συμβολοσειρών m-bit.

3.4.3 «Πρωτόκολλο BB84»

Το πρωτόκολλο αυτό πήρε το όνομα του από τους Bennett και Brassard. Τρεις βασικές αρχές του είναι οι εξής:

- Θεώρημα Κλωνοποίησης
- Κατάρρευση Κατάστασης κατά τη Μέτρηση
- Μη Αναστρέψιμη Λειτουργία Μετρήσεων

Το πρωτόκολλο μπορεί να χρησιμοποιηθεί με διαφορετικούς βαθμούς ελευθερίας(**D**egree **O**f **F**reedom). Πειραματικά το BB84 έχει αποδειχθεί τόσο σε κανάλια οπτκών ινών, όσο και σε οπτικά κανάλια ελεύθερου χώρου.

- **<u>Επίσημη Περιγραφή Πρωτοκόλλου</u>**

Η Alice δημιουργεί 2 κλασικές ακολουθίες bit: την ακολουθία δεδομένων d και την ακολουθία βάσεων b, μήκους N > 4n (όπου n είναι το μήκος του κλειδιού) η καθεμία και τις κωδικοποιεί ως μπλοκ N-qubits ως εξής:

$$|\boldsymbol{\psi}\rangle = \bigotimes_{k=1} |\psi_{d_k b_k}\rangle$$

$$|\psi_{00}\rangle = |0\rangle \qquad |\psi_{10}\rangle = |1\rangle$$

$$|\psi_{01}\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \; |\psi_{11}\rangle = (|0\rangle - |1\rangle)/\sqrt{2}.$$

- Η Alice δημιουργεί 2 κλασικές ακολουθίες μήκους N η καθεμία(N>4n), την d και την d'.
- Η Alice επιλέγει τυχαία ακολουθία μήκους N bit των βάσεων b και κωδικοποιεί τα δεδομένα di ως εξής: {|0> , |1>} εάν το αντίστοιχο bit στο b είναι 0 ή {|+> , |->} εάν το bit στο b είναι 1.
- Το αποτέλεσμα στέλνεται στον Bob από την Alice
- Όταν ο Bob λάβει τα N-qubits, το ανακοινώνει και έπειτα μετρά κάθε qubit είτε στην CB είτε στην

DB, με τυχαίο τρόπο.

- Η Alice ανακοινώνει την ακολουθία βάσεων b που χρησιμοποίησε

- Οι Alice και Bob θα απορρίψουν εκείνα τα κομμάτια, στα οποία χρησιμοποιήθηκαν διαφορετικές βάσεις. Με μεγάλη πιθανότητα θα έχουν απομείνει τουλάχιστον 2n bits, διαφορετικά το πρωτόκολλο θα ακυρωθεί. Τα 2n bits που απέμειναν θα τα αξιοποιήσουν ώστε να προχωρήσει το πρωτόκολλο.
- Από τα 2n bit που έμειναν, η Alice θα επιλέξει n bit τα οποία θα τα χρησιμοποιήσει ενάντια στην Eve και στις παρεμβολές στο κανάλι και έπειτα ενημερώνει τον Bob ποια bit χρησιμοποίησε.
- Τα δύο μέρη της επικοινωνίας θα συγκρίνουν τις τιμές των n-bit που επιλέχθηκαν και θα εκτιμήσουν τη τιμή του ρυθμού κβαντικών σφαλμάτων. Εάν ο αριθμός αυτός των σφαλμάτων ξεπεράσει κάποιο όριο, το πρωτόκολλο διακόπτεται.
- Διαφορετικά η Alice και ο Bob προχωρούν στην εναρμόνιση των πληροφοριών και την ενίσχυση απορρήτου στα υπόλοιπα n-bit για να ληφθούν τα m-bits του μυστικού κοινού κλειδιού.

3.4.4 «Η αναγκαιότητα της Post Quantum Cryptography(PQC)»

Η ανάπτυξη των υπολογιστών έχει συγκεντρώσει μεγάλη προσοχή τα τελευταία χρόνια. Συγκεκριμένα στο πλαίσιο της κρυπτολογίας οι κβαντικοί υπολογιστές αποτελούν σημαντική απειλή για τους τρέχοντες αλγορίθμους κρυπτογράφησης δημόσιου κλειδιού. Αν ποτέ κατασκευαστεί ο ιδανικός κβαντικός υπολογιστής, η ασφάλεια της τρέχουσας κρυπτογραφίας δημόσιου κλειδιού θα επιδεινωθεί. Δεδομένης λοιπόν της κατάστασης καταλήγουμε στο συμπέρασμα ότι είναι αναγκαία η μετάβαση στην PQC για τους παρακάτω λόγους:

- Η μετάβαση αυτή αναμένεται να διαρκέσει τουλάχιστον 10 έτη, συνεπώς απαιτείται ένα σημαντικό χρονικό διάστημα. Επίσης απαιτείται μεγάλη ανανέωση συστήματος, αντικατάσταση υλικού και λογισμικού, καθώς και η συμμετοχή διαφόρων ενδιαφερομένων στον χρηματοπιστωτικό κλάδο. Η υποδομή πληροφορικής για την εθνική άμυνα θα μπορούσε να διαρκέσει από 20 έως και 30 χρόνια. Εάν οι προετοιμασίες της μετάβασης ξεκινήσουν, με την προϋπόθεση ότι έχουν ήδη γίνει οι καινοτομίες που οδηγούν σε κβαντικούς υπολογιστές, η μετάβαση ενδέχεται να μην ολοκληρωθεί πριν τη δημιουργία των ιδανικών μηχανών.
- Η μετάβαση πρέπει να ξεκινήσει εγκαίρως για να μετριαστεί η απειλή μιας επίθεσης, η οποία συλλέγει και αποθηκεύει κρυπτογραφημένα δεδομένα σε ένα δημόσιο κανάλι επικοινωνίας και προσπαθεί να τα ανακτήσει αφού η υπολογιστική ισχύς του εισβολέα θα αυξηθεί στο μέλλον. Τα κρυπτογραφημένα δεδομένα θα πρέπει να έχουν λήξει νωρίτερα από την εμφάνιση των κβαντικών υπολογιστών. Για παράδειγμα εάν το απόρρητο πρέπει να διατηρηθεί για 10 χρόνια και οι ιδανικές μηχανές εμφανιστούν 30 χρόνια μετά η μετάβαση στο PQC είναι απαραίτητο να ολοκληρωθεί εντός 20 ετών.
- Ο κίνδυνος της εμφάνισης ιδανικών μηχανών δεν μπορεί να αγνοηθεί, λαμβάνοντας υπόψη την ραγδαία πρόοδο της τεχνολογίας και την αύξηση στον κβαντικό υπολογισμό. Το 2014 οι κβαντικοί υπολογιστές εξόπλιζαν μόνο 5 qubits. Τον Σεπτέμβριο του 2019 εμφανίστηκαν 53 qubit και η κβαντική υπεροχή θεωρήθηκε ότι είχε επιτευχθεί. Οι πρόσφατες μηχανές εξοπλίζουν περίπου 70 qubits. Με τον τρόπο αυτό, η τεχνολογική πρόοδος ήταν αξιοσημείωτη τα τελευταία χρόνια, υποστηριζόμενη από αυξημένες

επενδύσεις στον κβαντικό τομέα.

- Χρειάζεται χρόνος για να τελειοποιηθεί η εφαρμογή της κρυπτογραφίας και να ενισχυθεί η αξιοπιστίας της νέας τεχνολογίας έτσι ώστε να μπορεί να ενσωματωθεί στην κοινωνική υποδομή. Όπως έχει ήδη αναφερθεί, η ασφάλεια της κρυπτογραφίας δημόσιου κλειδιού δεν μπορεί να αποδειχθεί καθαρά θεωρητικά. Επίσης, μια θεωρητική αξιολόγηση της ασφάλειας δεν είναι αρκετή για την επαλήθευση της αντίστασης σε επιθέσεις πλευρικού καναλιού, που εξαρτώνται από την υλοποίηση. Είναι απαραίτητο ακόμη, να αξιολογηθεί η απόδοση ορισμένων υπολογιστικών πόρων, όπως οι IoT. Συνεπώς συνιστούμε την εισαγωγή της PQC σε νέες υπηρεσίες και συστήματα πληροφορικής, πρωτίστως για τον εντοπισμό και αντιμετώπιση προβλημάτων κατά την πρακτική χρήση και στη συνέχεια για την ενίσχυση της αξιοπιστίας,καθώς εξελίσσεται η κοινωνική υποδομή.

3.4.5«Παράδειγμα Ανταλλαγής Μηνύματος»

Φανταστείτε ότι η Alice θέλει να στείλει στον Bob ένα κρυπτογραφημένο μήνυμα που αποτελείται από μια σειρά μονάδων και μηδενικών. Παριστά λοιπόν τις μονάδες και τα μηδενικά στέλνοντας φωτόνια με συγκεκριμένες πολώσεις. Η Alice έχει να επιλέξει ανάμεσα σε δύο σχήματα σύνδεσης των πολώσεων των φωτονίων με το 1 ή το 0. Στο πρώτο σχήμα, το λεγόμενο ευθύγραμμο, ή σχήμα +, στέλνει ένα φωτόνιο πόλωσης ↕ για να εκπροσωπεί το 1 κι ένα πόλωσης ↔ για το 0.Για να στείλει ένα δυαδικό μήνυμα, εναλλάσσει τα δύο σχήματα με απρόβλεπτο τρόπο. Έτσι το δυαδικό μήνυμα 10101101001 θα μπορούσε να μεταδοθεί ως εξής:

Μήνυμα 1101101001 **Σχήμα**+x+xxx++xx

Μετάδοση ↕ / ↔ / \ ↕↔ \ /

Η Alice μεταδίδει το πρώτο 1 χρησιμοποιώντας το σχήμα δεύτερο 1 χρησιμοποιώντας το σχήμα x.

Κατά συνέπεια, το 1 μεταδίδεται και στις δύο περιπτώσεις, αλλά κάθε φορά εκπροσωπείται από διαφορετικής πόλωσης φωτόνια. Η συνταγή τους για την κβαντική κρυπτογραφία απαιτεί τρία προπαρασκευαστικά στάδια. Παρότι τα στάδια αυτά δεν περιλαμβάνουν αποστολή κρυπτογραφημένου μηνύματος, επιτρέπουν την ασφαλή ανταλλαγή ενός κλειδιού το οποίο στη συνέχεια θα χρησιμοποιηθεί για την κρυπτογράφηση ενός μηνύματος.

<u>*Στάδιο 1.*</u> Η Αλίκη αρχίζει μεταδίδοντας μια τυχαία ακολουθία μονάδων και μηδενικών (bit), χρησιμοποιώντας μια τυχαία επιλογή ευθύγραμμων (κάθετων και οριζόντιων) και διαγώνιων σχημάτων πόλωσης.

<u>*Στάδιο 2.*</u> Ο Bob πρέπει να μετρήσει την ποσότητα των φωτονίων. Εφόσον δε γνωρίζει ποιο σχήμα πόλωσης χρησιμοποίησε η Αλίκη για το κάθε φωτόνιο, ανταλλάσσει τυχαία τους δύο ανιχνευτές του, τον

+ και τον x. Μερικές φορές ο Μπομπ επιλέγει το σωστό ανιχνευτή και κάποιες άλλες όχι. Αν ο Bob

χρησιμοποιήσει λάθος ανιχνευτή, μπορεί να ερμηνεύσει εσφαλμένα το φωτόνιο της Αλίκης.

<u>*Στάδιο 3.*</u> Στο σημείο αυτό, η Αλίκη έχει στείλει μια σειρά από μονάδες και μηδενικά και ο Bob έχει ανιχνεύσει ορισμένα από αυτά σωστά και κάποια άλλα λάθος. Στη συνέχεια, για να

ξεκαθαρίσει την κατάσταση, η Αλίκη τηλεφωνεί στον Μπομπ σε μια κοινή, μη ασφαλή γραμμή και του λέει ποιο σχήμα πόλωσης χρησιμοποίησε για το κάθε φωτόνιο – όχι όμως και τι είδους πόλωση του έδωσε. Έτσι θα μπορούσε να του πει ότι έστειλε το πρώτο φωτόνιο χρησιμοποιώντας το ευθύγραμμο σχήμα, αλλά όχι αν έστειλε ↕ ή ↔. Τότε ο Bob λέει στην Αλίκη σε ποιες περιπτώσεις μάντεψε το σωστό σχήμα πόλωσης. Στις περιπτώσεις αυτές μέτρησε σωστά την πόλωση και σημείωσε ορθά το 1 ή το 0. Τέλος, η Αλίκη και ο Bob αγνοούν όλα τα φωτόνια για τα οποία ο Bob χρησιμοποίησε εσφαλμένο σχήμα και συγκεντρώνονται μόνο σε εκείνα για τα οποία μάντεψε το σωστό. Στην πραγματικότητα, δημιούργησαν μια νέα, βραχύτερη ακολουθία μπιτ, αποτελούμενη μόνο από τις σωστές μετρήσεις του Bob.

3.4.6 «Εναλλακτική Προσέγγιση Κβαντικής Κρυπτογραφίας»

Ένας άλλος τρόπος να σκεφτούμε την κβαντική κρυπτογραφία είναι με όρους μιας τράπουλας, αντί για τα πολωμένα φωτόνια. Κάθε χαρτί της τράπουλας έχει ένα φύλλο και ένα χρώμα, όπως βαλές κούπα ή έξι μπαστούνι και συνήθως κοιτάζοντας ένα χαρτί βλέπουμε ταυτόχρονα το φύλλο και το χρώμα του. Φαντασθείτε, ωστόσο, ότι μπορούμε να μετρήσουμε μόνο το φύλλο ή μόνο το χρώμα. Ας υποθέσουμε ότι επιλέγει να μετρήσει το χρώμα, που είναι "σπαθί", το οποίο και καταγράφει. Το χαρτί τυχαίνει να είναι το τέσσερα σπαθί, όμως η Alice ξέρει μόνο ότι είναι σπαθί. Στη συνέχεια μεταδίδει το χαρτί μέσω μιας τηλεφωνικής γραμμής στον Bob. Ενώ γίνεται αυτό, η Eve προσπαθεί να μετρήσει το χαρτί, δυστυχώς όμως γι' αυτή, επιλέγει να μετρήσει το φύλλο του, που είναι "τέσσερα". Όταν το χαρτί φτάνει στον Bob, εκείνος αποφασίζει να μετρήσει το χρώμα του, που είναι πάντα "σπαθί", το οποίο και σημειώνει. Κατόπιν η Alice τηλεφωνεί στον Bob και τον ρωτάει αν μέτρησε το χρώμα, πράγμα που έκανε κι έτσι τώρα η Αλίκη και ο Bob ξέρουν ότι μοιράζονται μια κοινή γνώση – και οι δύο τους έχουν γραμμένο στο σημειωματάριό τους "σπαθί".

Αντίθετα, η Eve έχει γραμμένο στο σημειωματάριό της "τέσσερα", που της είναι εντελώς άχρηστο. Στη συνέχεια, η Alice παίρνει από την τράπουλα άλλο ένα χαρτί, ας πούμε τον ρήγα καρό και πάλι όμως μπορεί να μετρήσει μόνο μία από τις δύο ιδιότητες. Τη φορά αυτή επιλέγει να μετρήσει το φύλλο, που είναι "ρήγας" και μεταδίδει το χαρτί μέσω μιας τηλεφωνικής γραμμής στον Bob. Η Eve επιχειρεί να μετρήσει το χαρτί και επιλέγει και αυτή να μετρήσει το φύλλο: "ρήγας". Όταν το χαρτί φτάνει στον Bob, εκείνος αποφασίζει να μετρήσει το χρώμα, που είναι "καρό". Κατόπιν η Alice τηλεφωνεί στον Bob και τον ρωτάει αν μέτρησε το φύλλο του χαρτιού. Εκείνος τότε παραδέχεται ότι μάντεψε λάθος και μέτρησε το χρώμα του. Η Alice και ο Bob δεν ενοχλούνται, επειδή μπορούν να αγνοήσουν εντελώς το συγκεκριμένο χαρτί και να δοκιμάσουν με κάποιο άλλο, επιλεγμένο στην τύχη από την τράπουλα. Στην περίπτωση αυτή η Eve μάντεψε σωστά και μέτρησε την ίδια ιδιότητα με την Alice, "ρήγας", όμως το χαρτί ακυρώθηκε επειδή ο Bob δεν το μέτρησε σωστά. Έτσι ο Bob δε χρειάζεται να ανησυχεί για τα λάθη του, επειδή ο ίδιος και η Alice μπορούν να συμφωνήσουν να τα αγνοούν, ενώ η Eve είναι παγιδευμένη στα δικά της. Στέλνοντας αρκετές κάρτες, η Alice και ο Bob μπορούν να συμφωνήσουν σε μια ακολουθία φύλλων και χρωμάτων, η οποία στη συνέχεια μπορεί να χρησιμοποιηθεί ως βάση για ένα είδος κλειδιού.

Η κβαντική κρυπτογραφία επιτρέπει στην Alice και τον Bob να συμφωνήσουν σε ένα κλειδί, το οποίο η Eve δε μπορεί να υποκλέψει χωρίς να κάνει λάθη. Η κβαντική κρυπτογραφία έχει και ένα επιπλέον πλεονέκτημα: επιτρέπει στην Alice και τον Bob να καταλάβουν αν η Eve

κρυφακούει. Η παρουσία της Eve στη γραμμή γίνεται εμφανής επειδή κάθε φορά που μετράει ένα φωτόνιο, κινδυνεύει να το αλλοιώσει και οι αλλοιώσεις αυτές γίνονται αντιληπτές από την Alice και τον Bob.

4

4.1 «Κλασικές Ψηφιακές Πληρωμές»

Βήμα 1: Ο πελάτης δημιουργεί έναν λογαριασμό στον Trusted Token Provider(TTP), παρέχοντας το μυστικό αναγνωριστικό του και τις ευαίσθητες πληροφορίες της πιστωτικής του κάρτας , μέσω ενός πιστοποιημένου και κρυπτογραφημένου καναλιού.

Βήμα 2: Ο πελάτης πραγματοποιεί έλεγχο ταυτότητας με τον TTP και έπειτα ζητά ένα *διακριτικό κατόχου κάρτας C* , το οποίο ο TTP θα το στείλει μέσω ενός ασφαλούς καναλιού.

Βήμα 3: Ο TTP δημιουργεί τυχαία ένα διακριτικό P και το στέλνει στον πελάτη μέσω ασφαλούς καναλιού.

Βήμα 4: Η συσκευή του πελάτη χρησιμοποιεί το αποθηκευμένο μυστικό διακριτικό C , το δημόσιο αναγνωριστικό εμπόρου *Mi* και το διακριτικό πληρωμής P. Η σύνθεση όλων αυτών θα δώσει το κρυπτόγραμμα*(C,Mi,P)*.

Βήμα 5: Ο πελάτης ξοδεύει το κρυπτογράφημα στον επιλεγμένο έμπορο

Βήμα 6: Ο έμπορος επαληθεύει το κρυπτόγραμμα με το TTP και αποδέχεται ή απορρίπτει τη συναλλαγή.

Τα *αποθηκευμένα δεδομένα του πελάτη* μπορεί να είναι ένα ηλεκτρονικό πορτοφόλι ή μια εικονική πιστωτική κάρτα που είναι αποθηκευμένη σε ένα smartphone, ρολόι κ.λ.π

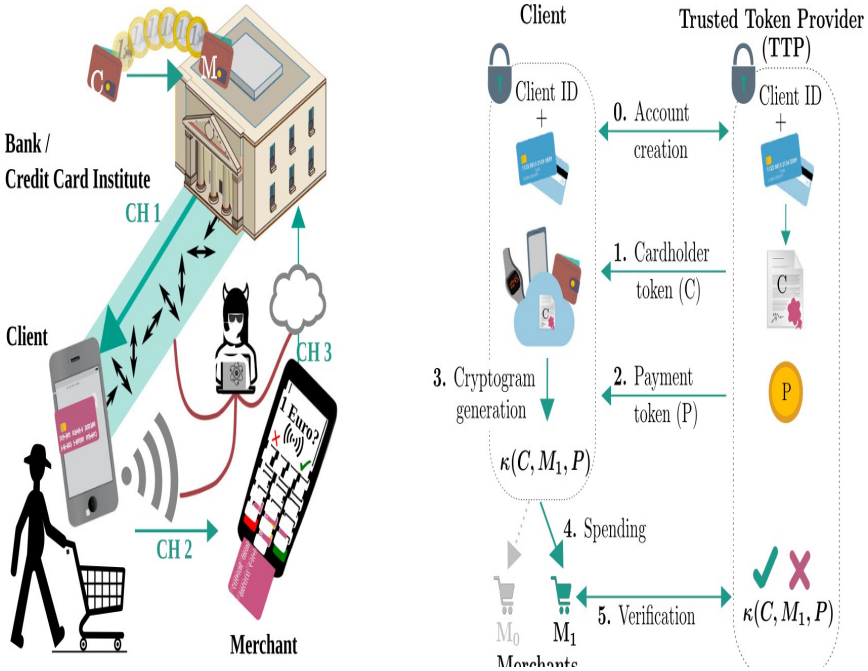
4.2 «Κβαντικές Πληρωμές»

Είναι γεγονός ότι οι ψηφιακές πληρωμές έχουν αντικαταστήσει τα φυσικά τραπεζογραμμάτια σε πολλούς τομείς της καθημερινής ζωής. Όπως και στα τραπεζογραμμάτια, έτσι και στις ψηφιακές πληρωμές θέλουμε να υπάρχει ευχρηστία, μοναδικότητα, ασφάλεια και ανθεκτικότητα απέναντι σε εισβολείς και παραβιάσεις δεδομένων. Η τρέχουσα τεχνολογία αντικαθιστά τα ευαίσθητα δεδομένα των πελατών τυχαιοποιημένα διακριτικά και διασφαλίζει την μοναδικότητα της πληρωμής με μια κρυπτογραφικό λειτουργία, που λέγεται κρυπτογράφημα. Παρόλα αυτά, υπολογιστικά ισχυρές επιθέσεις παραβιάζουν αυτές τις λειτουργίες.

Η κβαντική τεχνολογία έχει τη δυνατότητα να προστατεύει και από άπειρη υπολογιστική ισχύ. Με τη βοήθεια του κβαντικού φωτός μπορούν να εξασφαλιστούν καθημερινές ψηφιακές πληρωμές, μέσω της δημιουργίας κβαντικών κρυπτογραφημάτων. Εφαρμόζεται ένα σχέδιο σύνδεσης μιας οπτικής ίνας και του πόσο αυτή είναι ανθεκτική απέναντι σε επιθέσεις που σχετίζονται με θόρυβο και απώλεια. Δεν υπάρχει εξάρτηση από μακροπρόθεσμη κβαντική αποθήκευση ή από αξιόπιστους πράκτορες και πιστοποιημένα κανάλια. Βασίζεται σε βραχυπρόθεσμη τεχνολογία και μπορεί να προαναγγέλει μια εποχή κβαντικής ασφάλειας.

Η ανάπτυξη κβαντικών αλγορίθμων που διακυβεύουν την σύγχρονη κρυπτογραφία, έχει πυροδοτήσει την προσπάθεια ανάπτυξης ισχυρών μαθηματικά κρυπτογραφιών συστημάτων. Παρόλα αυτά όμως κάποια από αυτά τα σχήματα που έχουν αναπτυχθεί, έχουν σπάσει από υπολογιστικές επιθέσεις. Η ασφάλεια που προσφέρουν οι κβαντομηχανικοί νόμοι είναι γνωστή και ως ασφάλεια θεωρητικής πληροφορίας.

- Στη σύγχρονη εποχή των ψηφιακών πληρωμών που υλοποιούνται από ανέπαφες συναλλαγές μέχρι και ηλεκτρονικές τραπεζικές συναλλαγές, αναδύεται μια πληθώρα νέων απειλών όσον αφορά την ασφάλεια. Η σημαντικότερη απειλή εντοπίζεται στην αλληλεπίδραση του πελάτη με αναξιόπιστους εμπόρους, οι οποίοι παρουσιάζουν ανεπάρκειες στο να προστατεύσουν τους πελάτες τους από επίδοξους hackers ή μπορεί ακόμη να είναι και οι ίδιοι κακόβουλοι. Σε αυτή την περίπτωση απαιτείται κάποια δέσμευση ανάμεσα σε πελάτη-έμπορο-τράπεζα ή του δικτύου πληρωμών, ώστε να εξασφαλιστεί η εγκυρότητα της συναλλαγής. Ένας δεσμός αυτού του είδους εμφανίζεται. Συνήθως με τη μορφή κρυπτογραφήματος, το οποίο αποτελεί την έξοδο μιας συνάρτησης κατακερματισμού, που εξασφαλίζει την εφάπαξ φύση της κάθε συναλλαγής. Επειδή δεν είναι αξιόπιστα όλα τα εμπλεκόμενα μέλη, το QKD δεν μπορεί να δώσει την απαιτούμενη ασφάλεια και για αυτό το λόγο εισάγονται κάποιες επιπλέον κβαντικές λύσεις.
- Στόχος είναι η μη-κλωνοποίηση της κβαντικής μηχανής. Για αυτό το σκοπό λοιπόν αξιοποιείται το κβαντικό φως για την πρόληψη της παραχάραξης τραπεζογραμματίων με πιστωτικές κάρτες. Βέβαια, η εφαρμογή αυτής της μεθόδου κρύβει και ορισμένες αδυναμίες, μιας και είναι απαραίτητο οι κβαντικές καταστάσεις να αποθηκεύονται σε ημέρες ή μήνες για να διασφαλιστεί η ευελιξία των δαπανών. Ένα νέο σχετικά κβαντικό σχήμα που προτάθηκε έχει ως εξής: ένα δίκτυο αξιόπιστων πρακτόρων και πιστοποιημένων καναλιών, τοποθετημένων σε ακριβείς τοποθεσίες σε σχέση με τα σημεία των δαπανών, θα αντικαταστήσει την κβαντική αποθήκευση. Τα μειονεκτήματα βέβαια εδώ είναι ότι δεν δημιουργείται ασφαλές δίκτυο εμπιστοσύνης για καθημερινές συναλλαγές και επιπλέον ότι οι χωρικές και χρονικές συντεταγμένες απαιτούν ένα Παγκόσμιο Σύστημα Εντοπισμού Θέσης(GPS), το οποίο μπορεί να οδηγήσει σε επιθέσεις πλαστογράφησης.



ΣΧΗΜΑ 4.1 «ΚΒΑΝΤΙΚΕΣ ΨΗΦΙΑΚΕΣ ΠΛΗΡΩΜΕΣ & ΚΛΑΣΙΚΕΣ ΨΗΦΙΑΚΕΣ ΠΛΗΡΩΜΕΣ»

4.2.1 «Post-Quantum Protocols for Banking Applications»

Δεδομένου του αβέβαιου ρυθμού ανάπτυξης των κβαντικών υπολογιστών είναι απαραίτητο να προετοιμαστούν τα συστήματα για μια μετάβαση. Έτσι λοιπόν κρίνεται αναγκαίο το να υιοθετηθούν εκείνοι οι αλγόριθμοι που θα οδηγήσουν στα πιο ισχυρά μετακβαντικά

πρωτόκολλα. Παράλληλα πρέπει να εντοπιστούν και πιθανές τρωτότητες που θα παρουσιαστούν κατά τη φάση αυτής της μετάβασης. Πράγματι, οι μετακβαντικοί αλγόριθμοι έχουν πολύ μεγαλύτερα κλειδιά, κείμενα και υπογραφές , για αυτό και είναι περισσότερες οι απαιτήσεις όσον αφορά τους υπολογισμούς και την κατανάλωση μνήμης. Εξαιτίας αυτής της νέας κατάστασης, οι εταιρίες ζητούν να εφαρμοστούν *υβριδικά πρωτόκολλα* τα οποία θα συνδυάζουν την κλασική-δοκιμασμένη κρυπτογραφία με την PQC. Να σημειωθεί το γεγονός ότι έχουν πραγματοποιηθεί ορισμένα πειράματα πάνω σε αυτά τα υβριδικά πρωτόκολλα. Το 2016 η Google ανέπτυξε ένα υβριδικό σχήμα για την εγκατάσταση κλειδιών στο TLS, με όνομα *PQC New Hope.* Στο σχήμα αυτό ο έλεγχος ταυτότητας πραγματοποιείται με ενθυλάκωση κλειδιού και όχι με υπογραφή.

Στην παρούσα ενότητα βέβαια αυτό που θα εξετάσουμε είναι πρωτόκολλα που χρησιμοποιούνται στις πληρωμές με κάρτα. Θα παρατηρήσουμε ότι ο αλγόριθμος RSA χρησιμοποιείται αρκετά σε ό,τι έχει να κάνει με τον έλεγχο ταυτότητας κάρτας και συμμετρική κρυπτογραφία για πιστοποιητικά συναλλαγών που προορίζονται για τον εκδότη. Τα κρυπτογραφικά δεδομένα που εμπλέκονται σε μια τραπεζική συναλλαγή είναι πολύτιμα για ένα σύντομο χρονικό διάστημα, καθώς μετά την επικύρωση τους από την τράπεζα καθίστανται άχρηστα. Αυτό σημαίνει ότι οι τραπεζικές συναλλαγές παραμένονυ απρόσβλητες σε απειλές. Από την άλλη οι *συναλλαγές εκτός σύνδεσης* βασίζονται αποκλειστικά στον έλεγχο ταυτότητας της κάρτας. Στην περίπτωση αυτή η επικύρωση από την τράπεζα καθυστερεί.

Τα πιστοποιητικά συναλλαγών αποθηκεύονται λίγες ώρες στο τερματικό πριν διαβιβαστούν στην τράπεζα. Αυτό συμβαίνει προκειμένου να επιταχυνθούν οι εμπορικές συναλλαγές που σχετίζονται με μικρά ποσά. Εδώ, ο έλεγχος ταυτότητας της κάρτας είναι κρίσιμος για την ασφάλεια του συστήματος. Αν και δεν υπάρχει βραχυπρόθεσμη απειλή για τον έλεγχο ταυτότητας που βασίζεται σε RSA, η βιομηχανία θα πρέπει να αρχίσει σήμερα να εξερευνά την κρυπτογράφηση PQ για αυτό το βήμα ελέγχου ταυτότητας, ώστε να είναι έτοιμη για την «ημέρα Q». Αυτό ισχύει ιδιαίτερα επειδή υπάρχουν αυστηρές απαιτήσεις για τους χρονισμούς των συναλλαγών και οι πιο απαιτητικοί υπολογισμοί θα μπορούσαν να έχουν δραματικό αντίκτυπο, στο βαθμό που απαιτούν αλλαγές στο υλικό των εμπλεκόμενων συσκευών. Η έγκαιρη προετοιμασία και ο εντοπισμός των εμποδίων μπορεί μόνο να διευκολύνει αυτήν την προσπάθεια.

Ας εξετάσουμε 2 πρωτόκολλα πληρωμής ***EMV(Europay, Mastercard & Visa), CDA*** με επαλήθευση PIN εκτός σύνδεσης και συναλλαγή εκτός σύνδεσης και μια παραλλαγή που παρέχει προστασία έναντι της παρακολούθησης χρηστών. Αυτά τα πρωτόκολλα προσφέρουν διαφορετικές ιδιότητες ασφαλείας και λειτουργούν με διαφορετικούς (κλασικούς) κρυπτογραφικούς αλγόριθμους. Είναι επομένως σημαντικό να δούμε πώς συμπεριφέρονται με τους αλγόριθμους PQ. Προτείνουμε PQ και υβριδικές εκδόσεις αυτών των πρωτοκόλλων. Και για τα δύο, προσθέτουμε την αντίσταση PQ με προσεκτική προσθήκη κρυπτογραφικών λειτουργιών. Αυτό το κάνουμε έχοντας κατά νου πολλούς στόχους. Πρώτον, διατηρούμε τους στόχους ασφαλείας των αρχικών πρωτοκόλλων. Δεύτερον, σεβόμαστε όσο το δυνατόν περισσότερο τη γενική δομή όσον αφορά τις εντολές και τις ανταλλαγές. Αυτό στοχεύει στη διευκόλυνση της μετανάστευσης, περιορίζοντας τις τροποποιήσεις και επιτρέποντας την συμβατότητα. Τέλος, προσπαθούμε να μειώσουμε τα γενικά έξοδα για τους χρονισμούς συναλλαγών και για το σκοπό αυτό σχεδιάζουμε προσεκτικά την έκδοση PQ των πρωτοκόλλων. Επιλέγουμε διαφορετικούς αλγορίθμους PQ και

υλοποιούμε το αποτέλεσμα σε έξυπνες κάρτες. Στη συνέχεια, αναλύουμε τις επιπτώσεις όσον αφορά το μέγεθος των δεδομένων (μέγεθος κώδικα, εξατομίκευση κάρτας και επικοινωνίες) και τους χρόνους υπολογισμών και εκθέτουμε ορισμένους τομείς εργασίας που πρέπει να ληφθούν υπόψη εάν θέλουμε να επιτύχουμε καλές επιδόσεις με καθαρά PQ ή υβριδικά πρωτόκολλα.

- **Πρωτόκολλα EMV**

Το πρότυπο αυτό δημιουργήθηκε το 1996. Τα στάδια στο πρωτόκολλο αυτό είναι τα εξής:

Initialization: Στη φάση αυτή ο πελάτης επιλέγει τη σωστή εφαρμογή στην κάρτα και κάποια δεδομένα μεταδίδονται από την κάρτα, συμπεριλαμβανομένου του αριθμού κάρτας, της ημερομηνίας λήξης της και των υποστηριζόμενων λειτουργιών.

Έλεγχος Ταυτότητας Δεδομένων: Στο στάδιο αυτό εξασφαλίζεται η γνησιότητα της κάρτας. Υποστηρίζονται 3 διαφορετικές μέθοδοι:

- Στατικός Έλεγχος Ταυτότητας(Static Data Authentication,SDA): Εδώ παρέχονται υπογεγραμμένα δεδομένα στο τερματικό, για να ελεγχθεί η αυθεντικότητα τους. Φυσικά η μέθοδος αυτή είναι επιρρεπής στην κλωνοποίηση.
- Δυναμικός Έλεγχος Ταυτότητας(Dynamic Data Authentication,DDA): Η κάρτα εδώ είναι εξοπλισμένη με ένα ασύμμετρο ζεύγος κλειδιών, το αντίστοιχο πιστοποιητικό και τη δυνατότητα εκτέλεσης των υπογραφών. Μια ανταλλαγή "πρόκλησης-απόκρισης" όπου η κάρτα υπογράφει μια πρόκληση που αποστέλλεται από το τερματικό επιτρέπει τον έλεγχο ταυτότητας της κάρτας – με τρόπο που αποτρέπει την κλωνοποίηση. Ωστόσο, υπάρχει ένα ζήτημα ασφαλείας με το DDA: αν και επιτρέπει τον έλεγχο ταυτότητας της κάρτας, το τερματικό δεν έχει καμία διαβεβαίωση ότι η ίδια κάρτα εμπλέκεται σε επόμενες ανταλλαγές.
- Συνδυασμένος Έλεγχος Ταυτότητας(Combined Data Authentication,CDA): Είναι παρόμοια με την μέθοδο DDA , με τη μόνη διαφορά ότι η υπογραφή της κάρτας χρησιμοποιείται και για τον έλεγχο ταυτότητας κάποιων δεδομένων, ώστε να επιδιορθωθεί το ελάττωμα του DDA.

Επαλήθευση Κατόχου Κάρτας: Αυτό μπορεί να γίνει είτε με PIN, είτε με χειρόγραφη υπογραφή. Στην περίπτωση του PIN, αυτό θα εισαχθεί στο τερματικό και η επαλήθευση θα γίνει *ηλεκτρονικά* με το PIN να αποστέλλεται και να ελέγχεται από τον εκδότη ή *εκτός σύνδεσης,* όπου το PIN αποστέλλεται στην κάρτα. Το PIN μεταδίδεται cleartext ή σε κρυπτογραφημένη μορφή. Το τερματικό κάνει χρήση του δημόσιου κλειδιού για να κρυπτογραφήσει το PIN.

Συναλλαγή: Αυτό είναι και το τελικό βήμα το οποίο μπορεί να γίνει *online,* αλλά και *εκτός σύνδεσης*.

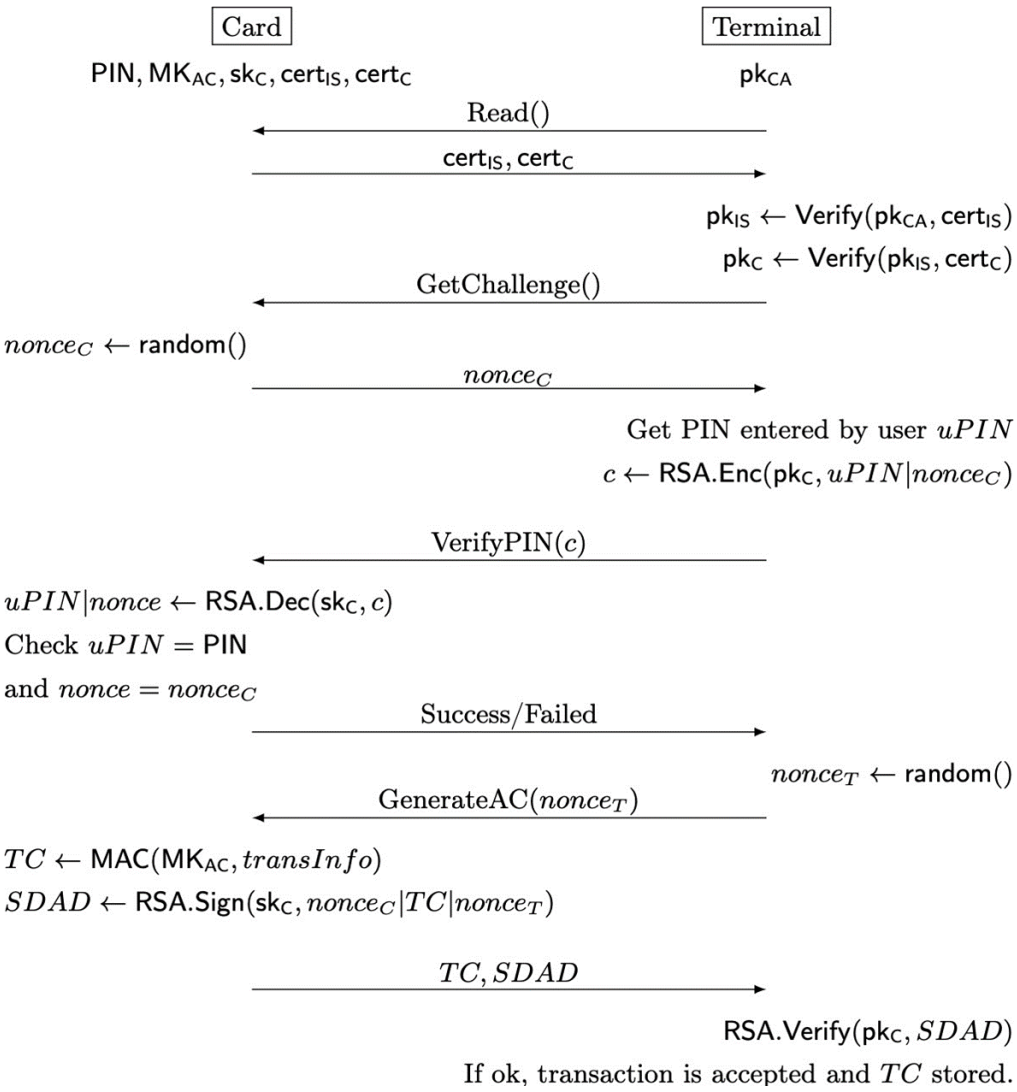
- Διαδικτυακή Συναλλαγή: Η κάρτα παρέχει ένα κρυπτόγραμμα αίτησης εξουσιοδότησης, που δημιουργείται χάρη σε ένα συμμετρικό κλειδί που μοιράζεται με τον εκδότη. Το τερματικό το προωθεί στον εκδότη, ο οποίος το επαληθεύει. Σε περίπτωση έγκρισης η κάρτα παρέχει Πιστοποιητικό Συναλλαγής ως απόδειξη ολοκλήρωσης.
- Συναλλαγή Εκτός Σύνδεσης: Η κάρτα παρέχει απευθείας ένα Πιστοποιητικό Συναλλαγής, το οποίο μετατρέπεται και αργότερα αποστέλλεται στον εκδότη. Η εμπορική συναλλαγή επιτρέπεται μόνο με βάση τον έλεγχο ταυτότητας της κάρτας.

Στις διαδικτυακές συναλλαγές χρησιμοποιείται συμμετρική κρυπτογραφία με μήκος κλειδιού στα 256 bit, παρέχοντας έτσι μια κβαντική αντίσταση. Ωστόσο, οι συναλλαγές αυτές δεν μπορούν να εκτελεστούν σε όλα τα περιβάλλοντα και δεν είναι τόσο φιλικές στη χρήση μιας και απαιτούν αρκετό χρόνο για να υλοποιηθούν. Αυτός είναι και ένας από τους λόγους που προτιμώνται οι συναλλαγές εκτός σύνδεσης. Έτσι λοιπόν είναι αναγκαίο να ενσωματωθούν νέοι αλγόριθμοι Post Quantum.

EMV CDA PROTOCOL

Έστω μια συναλλαγή εκτός σύνδεσης στην οποία το PIN κρυπτογραφείται. Το πρωτόκολλο βασίζεται στον αλγόριθμο RSA τόσο για την κρυπτογράφηση όσο και για την υπογραφή. Η κάρτα είναι εξοπλισμένη με ένα *μυστικό κλειδί skC* και το αντίστοιχο *πιστοποιητικό certC* που εκπέμπεται από τον εκδότη. Το *πιστοποιητικό certIS* του εκδότη παρέχεται και από την κάρτα. Το **πρώτο βήμα** έχει να κάνει με το τερματικό που ελέγχει την αλυσίδα μέχρι την αρχή πιστοποίησης (*όλα τα πιστοποιητικά είναι υπογεγραμμένα με RSA).* Για το σκοπό αυτό υπάρχει η συνάρτηση *Verify:* παίρνει ως είσοδο ένα δημόσιο κλειδί και ένα πιστοποιητικό, επαληθεύει την υπογραφή του πιστοποιητικού και εξάγει το πιστοποιημένο δημόσιο κλειδί σε περίπτωση επιτυχίας. Η συνάρτηση *RSA.Enc (αντίστοιχα RSA.Dec)* λαμβάνει ως είσοδο ένα δημόσιο κλειδί RSA (αντίστοιχα ιδιωτικό κλειδί RSA) και ένα μήνυμα για κρυπτογράφηση(αντίστοιχα για αποκρυπτογράφηση) και εξάγει το κρυπτογραφημένο κείμενο(αντίστοιχα το απλό κείμενο).

Σε δεύτερη φάση το τερματικό χρησιμοποιεί το PIN που έχει εισάγει ο χρήστης για να κρυπτογραφήσει. Έπειτα η κάρτα εκτελεί την αποκρυπτογράφηση και ελέγχει το PIN που έλαβε σε σχέση με την τιμή αναφοράς. Η κάρτα είναι εξοπλισμένη με ένα συμμετρικό κλειδί MKAC κοινόχρηστο με τον εκδότη, το οποίο χρησιμοποιείται για τον υπολογισμό των κρυπτογραφημάτων. Τα κρυπτογραφήματα υπολογίζονται με τη βοήθεια μιας συνάρτησης MAC που βασίζεται στο DES ή στο Triple-DES. Η κάρτα υπολογίζει το κρυπτόγραμμα TC και το υπογράφει με το μυστικό κλειδί RSA skC, χάρη στη λειτουργία RSA.Sign. Η τιμή nonceT που αποστέλλεται από το τερματικό περιλαμβάνεται στην υπογραφή. Αυτό επιτρέπει στο τερματικό να πιστοποιεί την ταυτότητα της κάρτας επαληθεύοντας την υπογραφή με το δημόσιο κλειδί της κάρτας pkC , χάρη στη λειτουργία RSA.Verify. Σε περίπτωση επιτυχίας το TC αποθηκεύεται.

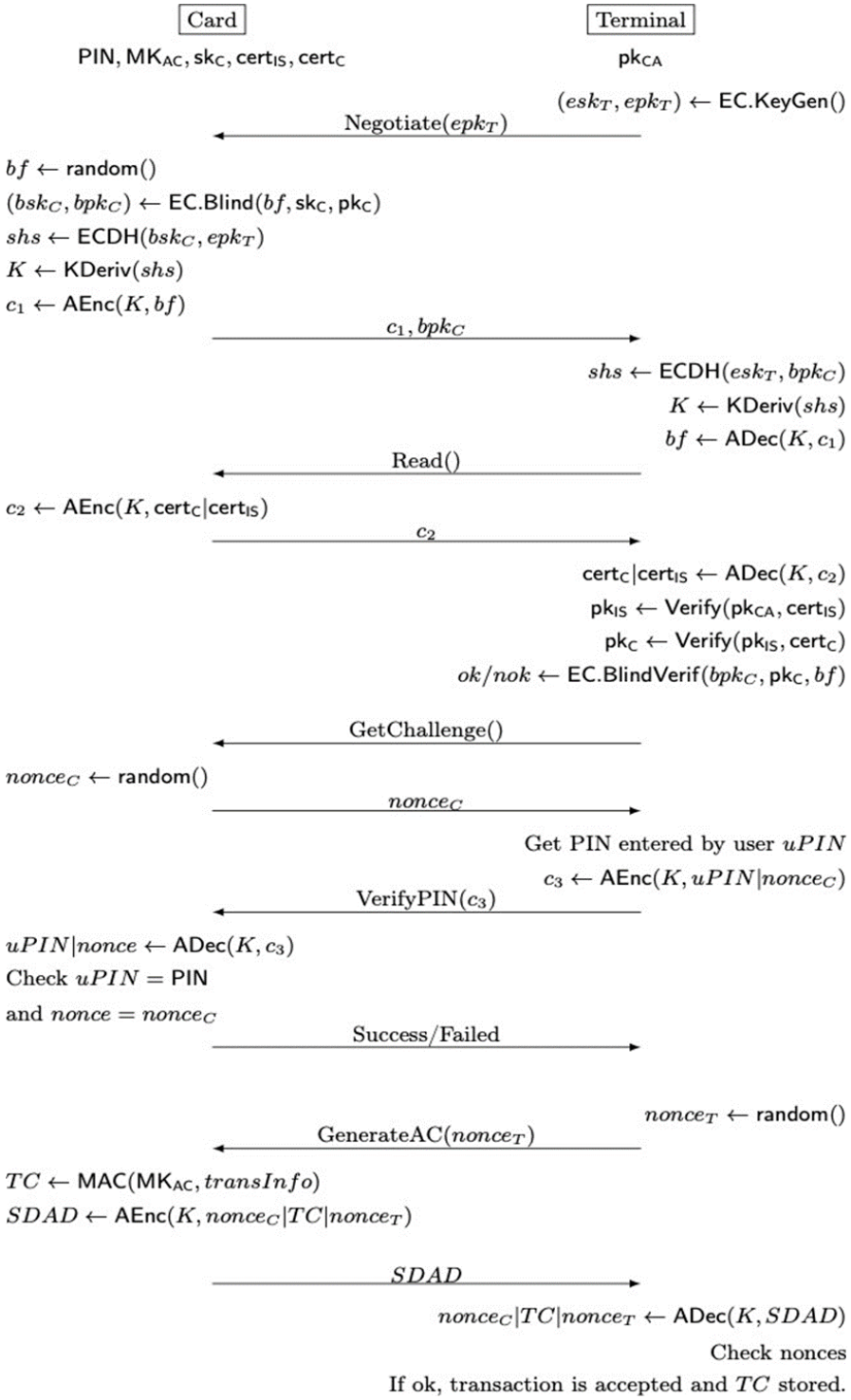


ΣΧΗΜΑ 4.2 «EMV CDA PROTOCOL»

BDH-based Protocol

Με το πρωτόκολλο αυτό δημιουργείται ένα ασφαλές κανάλι επικοινωνίας ανάμεσα σε κάρτα και τερματικό, αποτρέποντας ταυτόχρονα την παρακολούθηση της κάρτας. Στο BDH(Blinded Diffie-Hellman) η κάρτα χρησιμοποιεί στατικό κλειδί Diffie-Hellman για τον έλεγχο ταυτότητας. Στο επόμενο σχήμα βλέπουμε όλα τα βήματα του πρωτοκόλλου στην περίπτωση που χρησιμοποιείται για να ολοκληρωθεί μια συναλλαγή εκτός σύνδεσης με κρυπτογράφηση PIN. Το μυστικό κλειδί skC είναι ένα ιδιωτικό κλειδί ECDH(Elliptic Curve Diffie-Hellman). Δεδομένης ελλειπτικής καμπύλης E πάνω από πεδίο F και σημείου G της καμπύλης , η συνάρτηση EC-Blind παίρνει ως είσοδο ένα στοιχείο bf του F, το οποίο ονομάζεται *συντελεστής τύφλωσης,* ένα ιδιωτικό κλειδί sk επίσης μέσα στο F και το αντίστοιχο δημόσιο κλειδί pk, με *pk=[sk]*G.* . Ως έξοδο η συνάρτηση δίνει τις *τυφλές τιμές bsk=bf*sk* και *bpk=[bf]*pk.* . Η κάρτα χρησιμοποιεί αυτή τη συνάρτηση ώστε να υπολογίσει μια τυφλή τιμή του στατικού ζεύγους κλειδιών *(bskC,bpkC).*

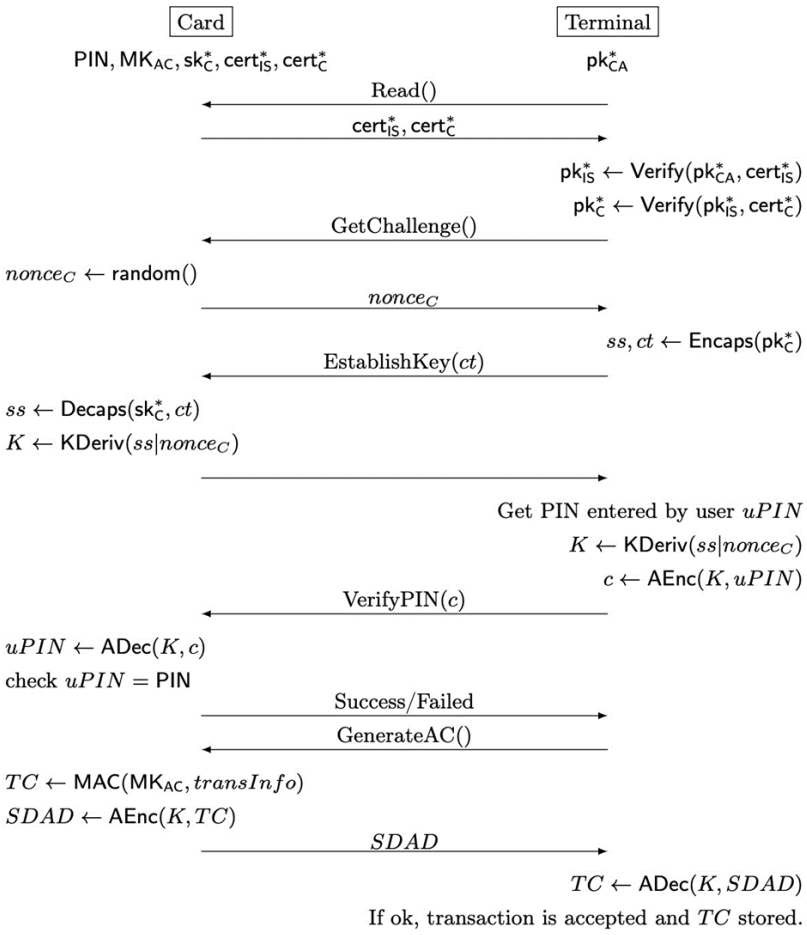
). Έπειτα συνάπτεται μια συμφωνία ανάμεσα ECDH μεταξύ bskC και του μόλις ληφθέντος τερματικού προσωρινού δημόσιου κλειδιού epkT. Με τον τρόπο αυτό δημιουργείται ένα ασφαλές κανάλι επικοινωνίας από τα κοινόχρηστα μυστικά κλειδιά shs. Το σύνολο των κλειδιών αυτών το συμβολίζουμε με K. Οι συναρτήσεις *AEnc και ADec* χρησιμοποιούνται για επικυρωμένη κρυπτογράφηση και αποκρυπτογράφηση αντίστοιχα. Η κάρτα θα κρυπτογραφήσει το bf και θα το στείλει στο τερματικό μαζί με το τυφλό δημόσιο κλειδί bpkC και έτσι επιτρέπει στο τερματικό να φτιάξει το σύνολο K και να ανακτήσει το bf. Στη συνέχεια η αλυσίδα πιστοποιητικών της κάρτας αποστέλλεται κρυπτογραφημένη στο τερματικό, το οποίο τα επαληθεύει και επιβεβαιώνει την ταυτότητα της κάρτας, μέσω της συνάρτησης *EC.BlindVerif* . Αυτή η συνάρτηση παίρνει ως είσοδο 2 σημεία *p1,p2* και ένα βαθμωτό *s* και ελέγχει εάν *p1=[s]*p2.* Το ασφαλές κανάλι χρησιμοποιείται για από το τερματικό για την ασφαλή επικοινωνία του PIN που έχει εισάγει ο χρήστης στην κάρτα.



ΣΧΗΜΑ 4.3 «BDH-based PROTOCOL»

4.2.2 «PQ Version Of EMV CDA Protocol»

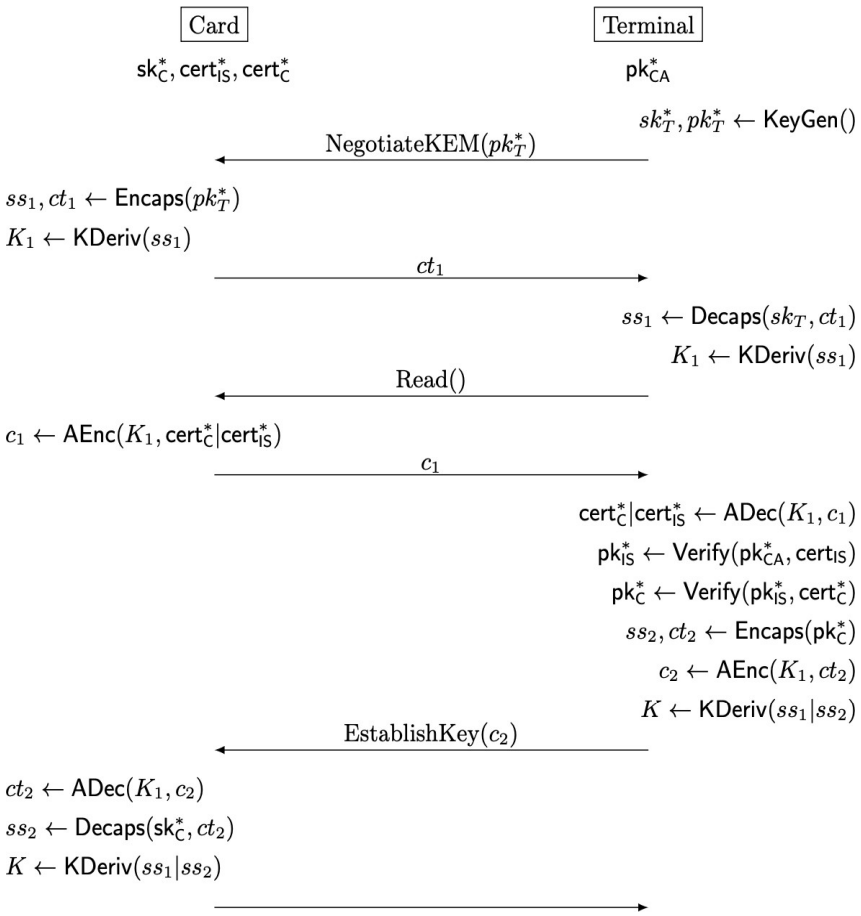
Στην έκδοση αυτή το τερματικό προκαλεί την κάρτα ζητώντας της να κάνει *"decapsulate"* ένα κρυπτογραφημένο κείμενο που δημιουργήθηκε για το δημόσιο κλειδί της κάρτας. Με τον τρόπο αυτό ελέγχεται η κάρτα σε σχέση με το δημόσιο κλειδί της, αλλά το κοινό μυστικό μπορεί να χρησιμοποιηθεί για μετάβαση σε συμμετρική κρυπτογραφία για τις υπόλοιπες ανταλλαγές αντί για χρήση δημόσιου κλειδιού. Προκειμένου η κάρτα να εισάγει δική της τυχαιότητα,το *nonceC* που δημιουργείται στο *GetChallenge* ενσωματώνεται και από τα 2 μέρη στην παραγωγή του κοινόχρηστου κλειδιού K. Αυτή η τιμή K μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση και τον έλεγχο ταυτότητας του κωδικού PIN που έχει εισαχθεί από τον χρήστη και υποδηλώνεται με *uPIN* για την κάρτα, ενώ συνεχίζει να παρέχει προστασία κατά της επανάληψης. Χρησιμοποιείται επίσης για τον έλεγχο ταυτότητας της κάρτας και του TC προς το τερματικό. Υπάρχει η εντολή *EstablishKey* μετά το *GetChallenge* για το τερματικό, ώστε να στείλει το κρυπτοκείμενο στην κάρτα. Οι 2 εντολές GetChallenge και EstablishKey μπορούν να συγχωνευθούν για να μειωθεί ο αριθμός των ανταλλαγών.



ΣΧΗΜΑ 4.4 «PQ analog of CDA PROTOCOL»

4.2.3 «PQ Version Of BDH-based Protocol»

Το πρωτόκολλο BDH βασίζεται σε μαθηματικές ιδιότητες των ελλειπτικών καμπυλών για να εξάγει ένα έγκυρο εφήμερο δημόσιο κλειδί από ένα στατικό δημόσιο κλειδί χρησιμοποιώντας τον blind factor. Με αλγορίθμους Post Quantum δεν είναι δυνατό να επιτευχθεί ο έλεγχος ταυτότητας. Για να γίνει αυτό μπορούμε να κάνουμε χρήση ενός πρωτοκόλλου που προέρχεται από το KEM- TLS. Το τερματικό δημιουργεί ένα εφήμερο ζεύγος κλειδιών και στέλνει το δημόσιο μέρος στην κάρτα. Η κάρτα μπορεί να ενθυλακώσει ένα μυστικό και να αντλήσει ένα πρώτο κοινόχρηστο σύνολο κλειδιών K1 για ασφαλή επικοινωνία με το τερματικό. Το σύνολο K1 χρησιμοποιείται από την κάρτα για να στείλει το στατικό δημόσιο κλειδί της κρυπτογραφημένο, έτσι ώστε να μην μπορεί να συνδεθεί με τον πραγματικό χρήστη από κάποιον που παρακολουθεί. Έπειτα το τερματικό ελέγχει την ταυτότητα του δημόσιου κλειδιού της κάρτας και να αμφισβητήσει την τελευταία , ζητώντας την αποκρυπτογράφηση του κρυπτογραφημένου τμήματος. Για να διασφαλιστεί πλήρως το απόρρητο, η τιμή αυτή αποστέλλεται κρυπτογραφημένη μαζί με το σύνολο K1. Το πρωτόκολλο προσφέρει σιωπηρό έλεγχο ταυτότητας με κοινή χρήση του κοινού μυστικού κλειδιού K.

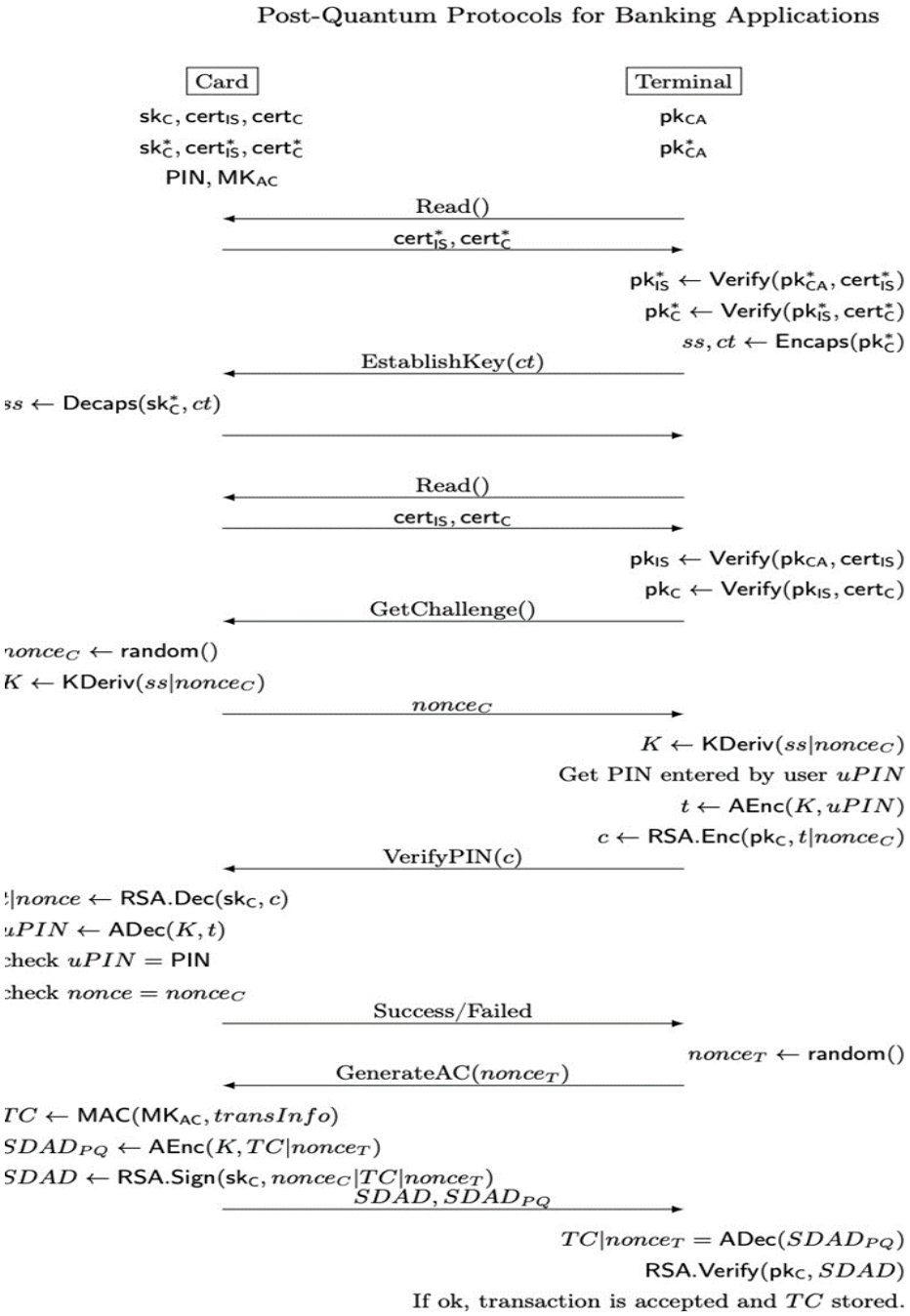


ΣΧΗΜΑ 4.5 «PQ analog of BDH-based PROTOCOL»

4.2.4 «ΥΒΡΙΔΙΚΕΣ ΜΕΘΟΔΟΙ»

Παρά το ότι τα Post Quantum πρωτόκολλα δεν χρησιμοποιούν υπογραφές, αυτές είναι σημαντικές για τα πιστοποιητικά. Πράγματι, 2 πιστοποιητικά αποστέλλονται από την κάρτα και επαληθεύονται από το τερματικό: αυτό του εκδότη και αυτό της κάρτας. Για τις υβριδικές εκδόσεις οι προσεγγίσεις είναι ποικίλες, η μία έχει 2 χωριστές αλυσίδες και άλλες κάνουν χρήση *υβριδικών πιστοποιητικών.* Σε όλες τις περιπτώσεις ο αριθμός των δημόσιων κλειδιών και των υπογραφών είναι ο ίδιος.

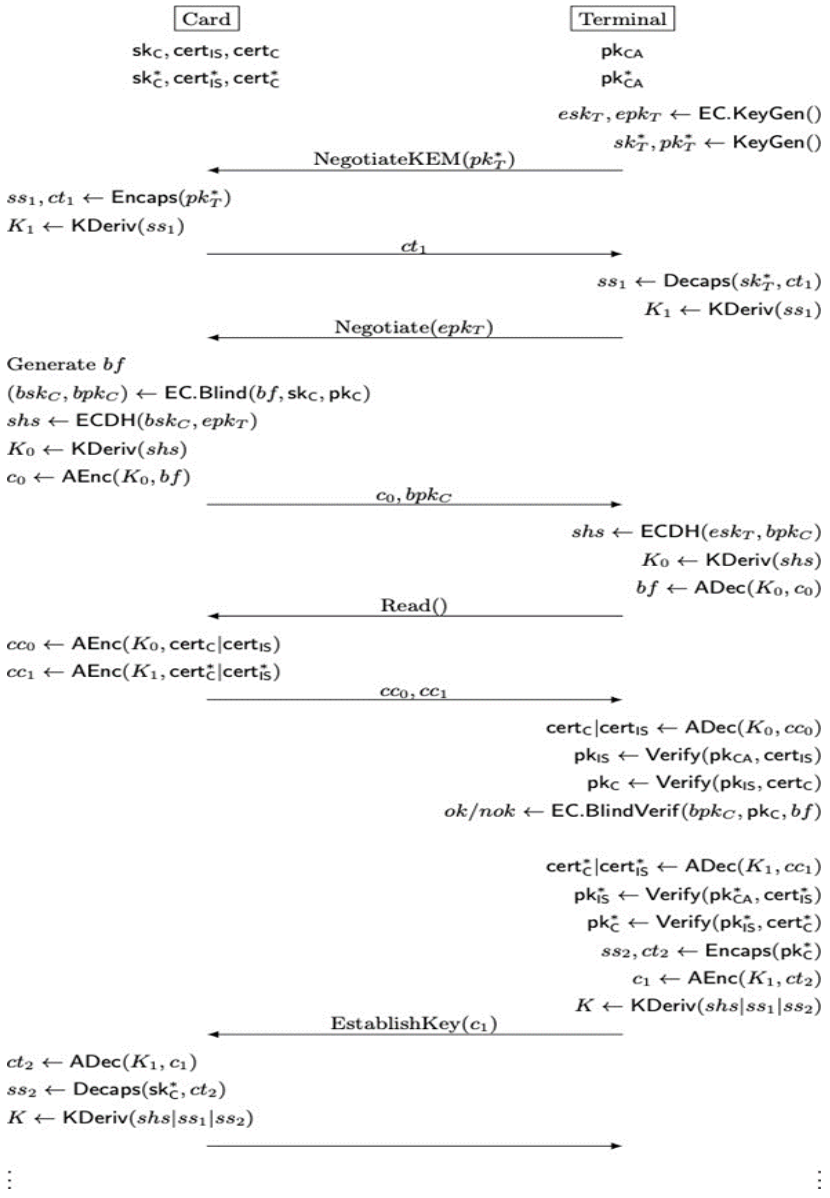
- **<u>Υβριδική Μορφή του CDA Πρωτοκόλλου</u>**
  1. Η κάρτα αποθηκεύει ζεύγη κλειδιών και πιστοποιητικά RSA & PQ KEM
  2. Στην πρώτη εντολή READ, η αλυσίδα πιστοποιητικών του στατικού δημόσιου κλεδιού PQ αποστέλλεται στο τερματικό. Στη συνέχεια το τερματικό επαληθεύει την αλυσίδα των πιστοποιητικών.
  3. Έπειτα το τερματικό ζητά από την κάρτα να κάνει decapsulate το ct(ciphertext) και το κρυπτογραφημένο κοινόχρηστο μυστικό ss.
  4. Σε μια δεύτερη εντολή READ, η αλυσίδα πιστοποιητικών του κλασικού στατικού δημόσιου κλειδιού αποστέλλεται στο τερματικό. Εν συνεχεία το τερματικό επαληθεύει αυτή την αλυσίδα πιστοποιητικών.
  5. Αφού το τερματικό λάβει nonceC , ένα κλειδί K(προέρχεται από το nonceC και το κοινό μυστικό ss του PQ). Το uPIN που εισάγεται από τον χρήστη κρυπτογραφείται πρώτα με τη βοήθεια του K(ασφάλεια PQ) και μετά γίνεται χρήση του αλγορίθμου RSA(κλασική ασφάλεια): c ← RSA.Enc(pkC,AEnc(K,uPIN))
  6. Το TC(κρυπτογράφημα) ελέγχεται με χρήση του K και υπογράφεται με επίσης χρησιμοποιώντας το RSA ιδιωτικό κλειδί: ***RSA.Sign(skC , nonceC |T C |nonceT).*** Και οι 2 τιμές αποστέλλονται ως απάντηση στην εντολή *GenerateAC.*



ΣΧΗΜΑ 4.6 «HYBRID version of CDA PROTOCOL»

Υβριδική Μορφή Του BDH Πρωτοκόλλου

1. Η κάρτα αποθηκεύει ζεύγη κλειδιών και πιστοποιητικά RSA & PQ KEM
2. Χρησιμοποιούνται τα Negotiate και NegotiateKEM αμετάβλητα σε σχέση με τις κλασικές εκδόσεις PQ, έτσι ώστε η κάρτα να μπορεί να στέλνει κλασικά πιστοποιητικά κρυπτογραφημένα με κλειδί K0 που προέρχεται από ECDH και πιστοποιητικά PQ κρυπτογραφημένα με κλειδί K1 που προέρχεται από KEM.
3. Το τερματικό μπορεί να ελέγξει όλα τα πιστοποιητικά και να αντλήσει το μυστικό K όχι μόνο από τα κοινόχρηστα μυστικά PQ ss1 & ss2, αλλά και από τα κοινόχρηστα μυστικά shs που λαμβάνονται από το κλασικό BDH: K ← KDeriv(shs|ss1|ss2)



ΣΧΗΜΑ 4.7«HYBRID vrsion of BDH-based PROTOCOL»

4.2.5

«ΜΕΤΑΚΒΑΝΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ»

Ορισμένοι αλγόριθμοι υπογραφής βασισμένοι σε κατακερματισμό έχουν ήδη τυποποιηθεί από το NIST. Απολαμβάνουν υψηλή εμπιστοσύνη από την κοινότητα και έτσι μπορούν να χρησιμοποιηθούν μόνοι τους μέσω της υβριδικής οδού. Θα εξετάσουμε 2 αλγορίθμους υπογραφής που έχουν επιλεγεί για τυποποίηση: *Falcon & CRYSTALS-Dilithium.* Να τονιστεί ότι στους παραπάνω αλγορίθμους έπαιξε σημαντικό ρόλο το μήκος των πιστοποιητικών όσον αφορά τον χρόνο των συναλλαγών. Απαιτούνται επίσης διαφορετικά επίπεδα ασφαλείας για τους διαφορετικούς φορείς στην αλυσίδα πιστοποιητικών, ανάλογα με τη διάρκεια ζωής τους.

Η *μετακβαντική* και *υβριδική* μορφή των πρωτοκόλλων CDA & BDH χρησιμοποιούν KEM(*Key Encapsulation Mechanism).* Ορισμένα από τα χαρακτηριστικά του αλγορίθμου πρέπει να είναι τα παρακάτω:

1. Η κάρτα πρέπει να αποθηκεύσει το μυστικό κλειδί KEM
2. Το δημόσιο κλειδί KEM μεταδίδεται ως μέρος του πιστοποιητικού της κάρτας
3. Ανταλλάσσονται 1(στο PQ CDA) ή 2(στο PQ BDH) κρυπτογραφημένα κείμενα KEM
4. Η κάρτα θα εκτελέσει μια λειτουργία Decaps και μια Encaps σε περίπτωση PQ BDH

ΠΑΡΑΤΗΡΗΣΕΙΣ ΓΙΑ ΤΟΝ ΑΛΓΟΡΙΘΜΟ FALCON

- Τα τσιπ που χρησιμοποιήθηκαν απαιτούν αρκετές εκατοντάδες kilobyte μνήμης Flash
- Τα δεδομένα που εξαρτώνται από τον χρήστη πρέπει να φορτωθούν στην κάρτα κατά τη διάρκεια μιας συγκεκριμένης λειτουργίας που λέγεται *εξατομίκευση*
- Το τμήμα PQ των πρωτοκόλλων προσθέτει:
    1. certIS το οποίο περιλαμβάνει κυρίως το δημόσιο κλειδί υπογραφής του εκδότη και την υπογραφή
    2. certC το οποίο περιλαμβάνει το δημόσιο κλειδί KEM της κάρτας και την υπογραφή του εκδότη
    3. skC , το μυστικό κλειδί KEM της κάρτας

4.3«Quantum Advantage»

1. Ο TTP δημιουργεί μια τυχαία συμβολοσειρά bit b και μια τυχαία συζυγή συμβολοσειρά βάσης B μήκους L. Κάθε bit bj κωδικοποιείται σε μια κβαντική κατάσταση προετοιμασμένη σε Bj. Αυτό αποτελεί την κλασική περιγραφή (d,B) του κβαντικού διακριτικού |P>, το οποίο ο TTP αποθηκεύει κάτω από το αναγνωριστικό CID του πελάτη. Το μήκος L εξαρτάται από την ανεκτή πιθανότητα επιτυχίας μιας επίθεσης και τον αροθμό των διαθέσιμων εμπόρων.
2. Με τη λήψη του |P>, ο πελάτης επιλέγει το Mi από μια βάση δεδομένων που είχε προκαθοριστεί με ασφάλεια από τον TTP. Έπειτα γίνεται ο εξής υπολογισμός: mi=MAC(C,Mi) που είναι η ετικέτα εξόδου ενός i.t secure MAC(Message Authentication Code). Το MAC παίρνει το μυστικό διακριτικό C και το δημόσιο αγνωριστικό Mi του επιλεγμένου εμπόρου ως είσοδο. Ο πελάτης ερμηνεύει το mi ως συμβολοσειρά βάσης και ιδιωτικά μετρά ολόκληρη την ακολουθία |P> σύμφωνα με το mi.
3. Ο πελάτης στέλνει το Ki μαζί με το αναγνωριστικό CID στον έμπορο, ο οποίος μαζί με το Mi τα προωθεί στονTTP για επαλήθευση.
4. Για να εξουσιοδοτηθεί η αγορά , ο TTP ζητά το CID και το (b,B) προκειμένου να υπολογίσει το mi για τον εκάστοτε πελάτη. Η συναλλαγή γίνεται αποδεκτή ΜΟΝΟ ΟΤΑΝ , όταν $(m_i)_j = \mathcal{B}_j$.
5. Σε διαφορετική περίπτωση η συναλλαγή απορρίπτεται.

• Η ασφάλεια έγκειται στο ανώτερο όριο της πιθανότητας να παραχθούν 2 έγκυρες και διακριτές κρυπτογραφημένες τιμές ki,kj για 2 διακριτούς εμπόρους Mi,Mj. Επίσης να τονιστεί ότι η απόκρυψη του CID εγγυημένη , συν το ότι η δέσμευση του Mi εξασφαλίζεται από τη μη-αναστρέψιμη φύση των κβαντικών μετρήσεων. Συγκεκριμένα η κβαντική μας δέσμευση δεν περιορίζεται από το θεώρημα αδυναμίας της δέσμευσης κβαντικών δυαδικών ψηφίων, στο οποίο το ένα από τα δύο μέρη μπορεί να καθυστερήσει να τις κβαντικές του μετρήσεις. Αυτό συμβαίνει επειδή ένα από τα μέρη που αλληλεπιδρούν θεωρείται ότι είναι ειλικρινές(το TTP). Οι βάσεις μέτρησης δεν θα αποκαλυφθούν στον πελάτη έως ότου απαιτηθεί επαλήθευση.

«<u>Ασφάλεια εξαρτώμενη από απώλειες</u>»

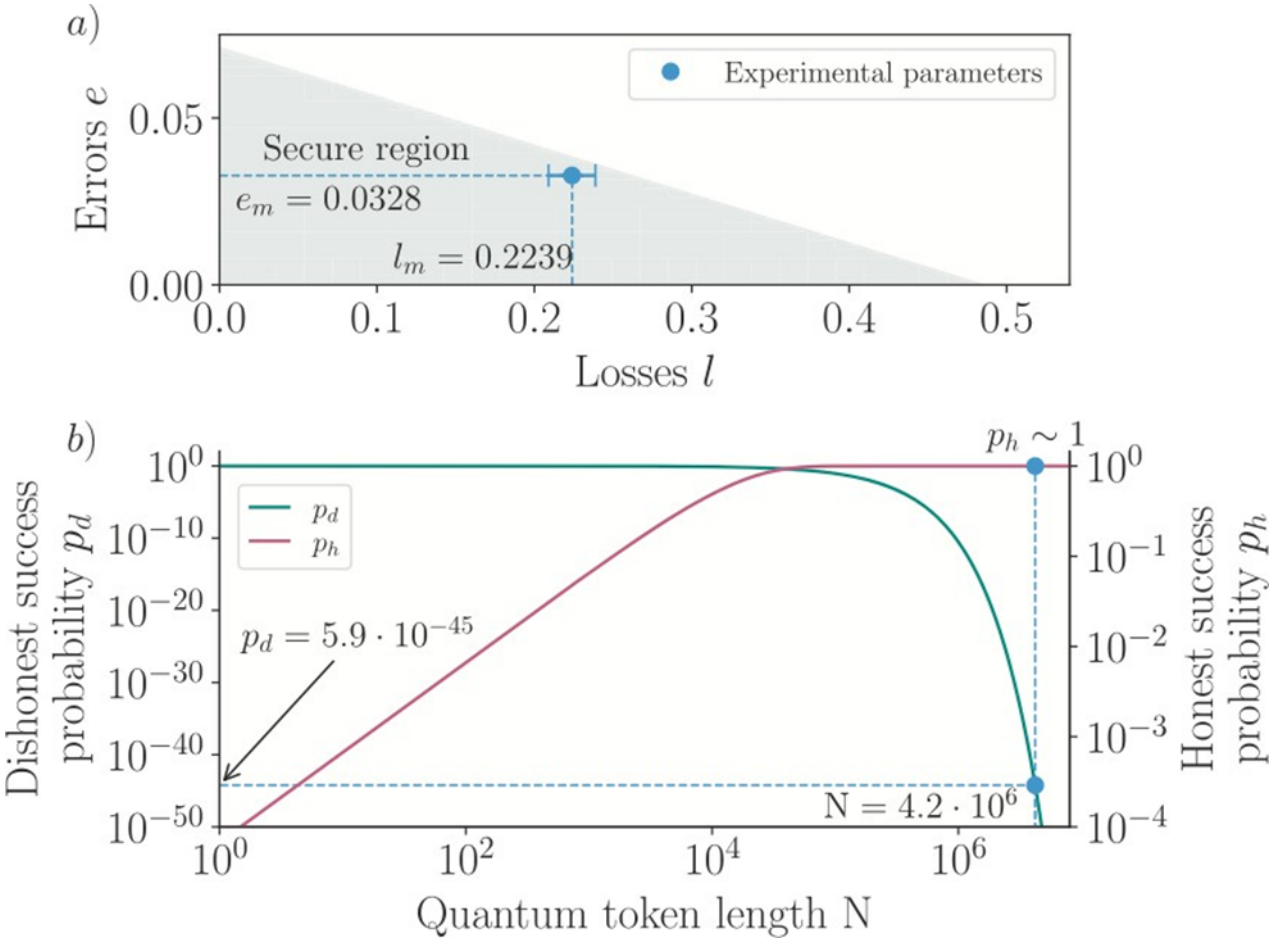
Παρόλο που η ασφάλεια είναι εγγυημένη από τους νόμους της κβαντικής μηχανικής, οι ατέλειες των πραγματικών συσκευών(*ανακριβής προετοιμασία κατάστασης, κβαντικά κανάλια με απώλειες)* οδηγούν στο να αποκλίνουν ορισμένες κβαντικές καταστάσεις. Παραδείγματος χάριν, στο βήμα 4 κάποια bit θα είναι άνισα παρόλο που μετρώνται στην ίδια βάση

$(\kappa_i)_j \neq \upsilon_j$ when $(m_i)_j = \upsilon_j$

Για τον λόγο αυτό είναι σωστό να επιτρέψουμε λάθη και απώλειες κατά τη διαδικασία της επαλήθευσης. Με τη σειρά του ένα μέρος κακόβουλο θα μπορούσε να το εκμεταλλευτεί για να παρακάμψει τη δέσμευση ή να δαπανήσει εις διπλούν το κρυπτογράφημα.

ΠΑΡΑΔΕΙΓΜΑ

Εάν υποθέσουμε ότι ο TTP δέχεται μέχρι και 50% απώλειες, τότε ένας κακόβουλος πελάτης θα ήταν σε θέση να μετρήσει το μισό του κβαντικού διακριτικού |Pi> στη βάση M0 και το άλλο μισό στη βάση M1, δημιουργώντας έτσι δυο επιτυχώς δεσμευμένα διακριτικά. Διαισθητικά, αναζητούμε τη στρατηγική εξαπάτησης που ελαχιστοποιεί την εισαγωγή υπερβολικών σφαλμάτων και απωλειών από την πλευρά του κακόβουλου μέρους. Σημειώνεται ότι τόσο ισχυρές επιθέσεις που εξαρτώνται από απώλειες δεν ελήφθησαν υπόψη σε προηγούμενες υλοποιήσεις κβαντικών διακριτικών.



ΣΧΗΜΑ 4.8 ««Ανέντιμη και Ειλικρινής Πιθανότητα Επιτυχίας»

4.4«Συστήματα Πληρωμών με Κάρτα σε έναν Μετα-κβαντικό Κόσμο»

4.4.1 «Κβαντικές Απειλές για Συμμετρική Κρυπτογραφία»

Είναι γεγονός πως εμπορικοί κβαντικοί υπολογιστές δεν υπάρχουν σήμερα, πράγμα που δίνει τη δυνατότητα στους hackers να χρησιμοποιήσουν την μέθοδο "capture now , decrypt later". Αυτό σημαίνει ότι μπορούν να συλλεχθούν ιδιαίτερα εμπιστευτικές πληροφορίες (όπως για παράδειγμα αρχεία που περιέχουν εφευρέσεις, βιομηχανικά στοιχεία ή ακόμη και κυβερνητικά μυστικά). Η ανάπτυξη αυτής της επίθεσης δεν έχει νόημα στα συστήματα πληρωμών με κάρτα, εξαιτίας του μικρού χρονικού διαστήματος που μεσολαβεί για να εξουσιοδοτηθεί μια πληρωμή με τη δημιουργία κρυπτογραφήματος και την παρουσίαση του στην τράπεζα. Με την ολοκλήρωση της πληρωμής τα κρυπτογραφήματα είναι άχρηστα για οποιαδήποτε εξαπάτηση. Υπάρχει όμως η δυνατότητα τα κρυπτογραφήματα να αποθηκευτούν για μερικές ώρες. Στην περίπτωση της συμμετρικής κρυπτογράφησης δεν βασιζόμαστε σε "σκληρά μαθηματικά προβλήματα". Οι συμμετρικοί αλγόριθμοι είναι έτσι σχεδιασμένοι, ώστε η ευκολότερη μέθοδος για να σπάσουν είναι η δοκιμή όλων των πιθανών κλειδιών. Βρέθηκε μάλιστα ότι στο AES 128 οι πιθανοί συνδυασμοί είναι 2128 , ενώ στο AES 256 είναι 2256.

4.4.2«Κβαντικές Απειλές για Ασύμμετρη Κρυπτογραφία»

Είναι απόλυτα προφανές πως όσα περισσότερα είναι τα κλειδιά, τόσο μεγαλύτερη είναι και η ασφάλεια που προσφέρει ένα κρυπτοσύστημα. Εάν τα πιστοποιητικά κάρτας είναι σπασμένα, τότε πλαστές πληρωμές με κάρτες που εμφανίζονται ως αυθεντικές θα μπορούσαν να χρησιμοποιηθούν, για παράδειγμα, για την εκτέλεση συναλλαγών εκτός σύνδεσης όπου το (συμμετρικό) κρυπτόγραμμα εφαρμογής δεν επικυρώνεται σε πραγματικό χρόνο τη στιγμή της αγοράς. Πρόσφατα κυκλοφόρησαν προδιαγραφές για την εφαρμογή του *ECC* σε κάρτες και τερματικά. Το *ECC* παρέχει ισοδύναμη υπολογιστική ισχύ με το *RSA,* απλώς με μικρότερα μήκη κλειδιού. Η ασφάλεια του βασίζεται στην επίλυση ενός δύσκολου μαθηματικού προβλήματος με κλασικούς υπολογιστές. Μέσω όμως των κβαντικών υπολογιστών οι hackers μπορούν να λύσουν αυτό το μαθηματικό πρόβλημα και να σπάσουν τον αλγόριθμο. Το 19994 ο Shor κατασκεύασε έναν αλγόριθμο ο οποίος εκτελείται σε κβαντικό υπολογιστή και σπάει τον ECC και τον RSA. Βέβαια για να γίνει αυτό απαιτούνται μερικές χιλιάδες σταθερά qubits. Να σημειωθεί σε αυτό το σημείο ότι τέτοιου είδους πρότυπα λειτουργούν σε ένα εξαιρετικά ελεγχόμενο εργαστηριακό περιβάλλον και όχι σε εμπορικό επίπεδο. Για να πραγματοποιηθεί αυτή η μετάβαση σε έναν μετα-κβαντικό κόσμο είναι απαραίτητο να χρησιμοποιηθούν *κρυπτοευκίνητα συστήματα πληρωμών.* Ως *κρυπτοευκινησία* θεωρούμε ένα λειτουργικό χαρακτηριστικό ενός κρυπτογραφικού συστήματος που επιτρέπει τη μεταγωγή από τη χρήση ενός αρχικού κρυπτομηχανισμού σε έναν άλλο, με αντίκτυπο στο υπάρχον στοιχείο του συστήματος υλικού και λογισμικού και ιδανικά κατά τρόπο διαφανή για τους τελικούς χρήστες. Εξαιτίας του ότι οι κάρτες πληρωμής αντικαθίστανται και έχουν σχετικά μικρή διάρκεια(3 έως 5 χρόνια), το *crypto-agility* επικεντρώνεται στα συστήματα επεξεργασίας πληρωμών με κάρτα, ξεκινώντας με το τερματικό.

4.4.3 «Cryptographic Agility»

"Mosca's Theorem"

Η ανακάλυψη νέων κρυπτογραφικών αδυναμιών ή προόδων στις τεχνολογίες που υποστηρίζουν την κρυπτογράφηση, οδηγούν στην ανάγκη αντικατάστασης του παλιού κρυπτογραφικού αλγορίθμου. Η έλευση του κβαντικού, καθώς και η τεχνολογία των υπολογιστών θέτουν σε κίνδυνο πολλούς από τους ήδη υπάρχοντες αλγορίθμους , ιδίως αυτούς που ανήκουν στην κατηγορία δημοσίου κλειδιού, μέθοδος η οποία χρησιμοποιείται συχνά για την προστασία ψηφιακών πληροφοριών. Πρωτόκολλα που βασίζονται σε κρυπτογραφία δημόσιου κλειδιού, όπως TLS, IPSEC, ψηφιακές υπογραφές θα γίνουν ευάλωτα σε υποκλοπές, καθώς δεν μπορούν να αποτρέψουν μια κβαντική επίθεση. Κρίνεται λοιπόν απαραίτητη η λήψη δραστικών μέτρων. Βέβαια το αν θα υπάρξει καθυστέρηση στη λήψη μέτρων εξαρτάται από 3 ερωτήσεις:

- Πόσο διάστημα χρειάζονται τα κρυπτογραφικά κλειδιά ώστε να διατηρηθεί η ασφάλεια; Ας συμβολίσουμε με x το διάστημα αυτό. Υπάρχει περίπτωση x=0, όταν η ασφάλεια απαιτείται σε πραγματικό χρόνο. Μπορεί ακόμη x=10, 20, 100, σε προσωπικά δεδομένα υγείας, εμπορικά μυστικά ή πληροφορίες εθνικής ασφάλειας. Η τιμή του x είναι είτε προσωπική, είτε επιχειρηματική.
- Πόσος χρόνος θα χρειαστεί για να αναπτυχθεί ένα σύνολο από εργαλεία που είναι κβαντικά ασφαλή. Έστω ότι τον χρόνο αυτό τον συμβολίζουμε με y. Εάν y=0 σημαίνει ότι πρόκειται για αυτόματη ενημέρωση, που αντικαθιστά τον AES-128 με τον AES-256 σε ένα σύστημα που ελέγχεται από έναν μόνο προμηθευτή.

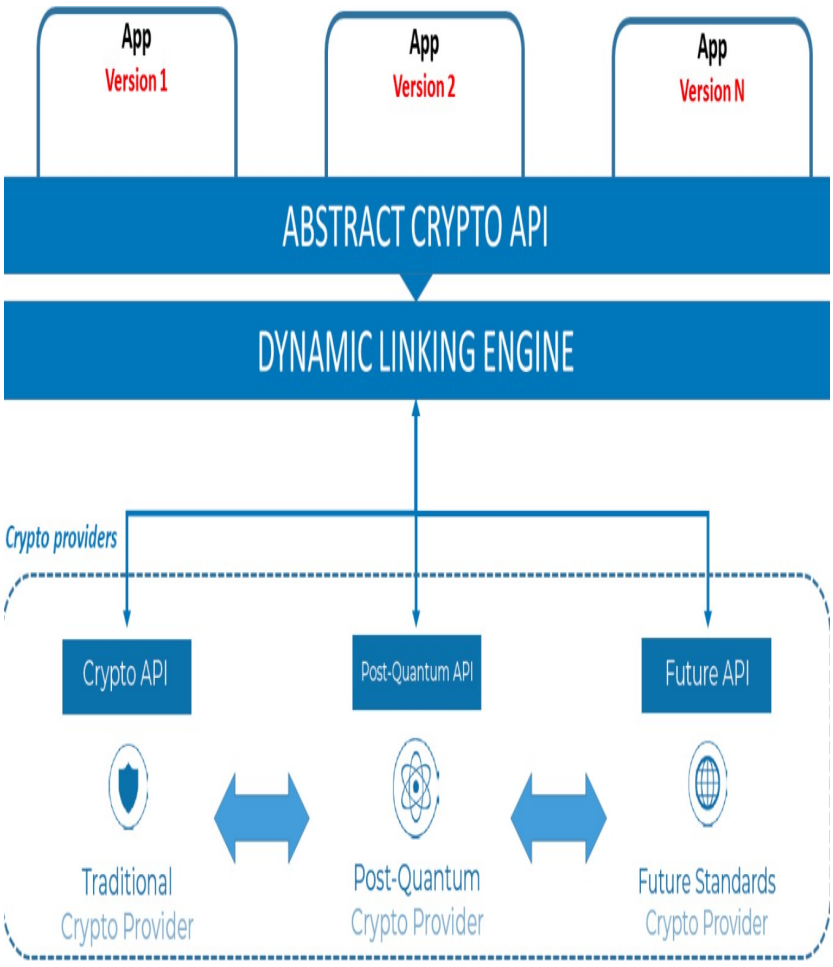
Ωστόσο μπορεί y>=15 εάν τυχόν χρησιμοποιείται μια μη-δοκιμασμένη μέθοδος κρυπτογράφησης δημοσίου κλειδιού που πρέπει να προσαρμοστεί για περιβάλλον με περισσότερους χρήστες , οι οποίοι πρέπει να συμφωνήσουν σε ένα πρότυπο.

- Πόσος καιρός θα περάσει πριν ένας κβαντικός υπολογιστής ή κάποια άλλη μέθοδος να σπάσει. Ας συμβολίσουμε με z αυτό το χρονικό διάστημα.

Εάν **x+y>z** υπάρχει σοβαρό πρόβλημα, διότι οι πληροφορίες προστατεύονται ευάλωτα κβαντικά εργαλεία και έτσι υπάρχει πιθανότητα σε επόμενα έτη τα εργαλεία αυτά να σπάσουν σε λιγότερο από x χρόνια.

Προκειμένου να μειωθεί σημαντικά η μεταβλητή y του Mosca's Theorem θα πρέπει να γίνουν ριζικές αλλαγές στον τρόπο εφαρμογής των κρυπτογραφικών εργαλείων στα ποικίλα ΤΠΕ, ώστε να μειωθεί ο χρόνος που απαιτείται για την αντικατάσταση του μη-ασφαλή κρυπτογραφικού αλγορίθμου. Στο σημείο αυτό έρχεται η crypto-agility, δηλαδή η ικανότητα εφαρμογής, ενημέρωσης, αλλαγής και αφαίρεσης κρυπτογραφικών λειτουργιών από συστήματα και εφαρμογές κατά παραγγελία χωρίς να προκληθεί αλλαγή στο ίδιο το σύστημα ή την εφαρμογή. Για να επιτευχθεί η Crypto-agility πρέπει να δημιουργηθούν ένα ή περισσότερα επίπεδα αφαίρεσης μεταξύ εφαρμογών και κρυπτογραφικών λειτουργιών. Κρίνεται απαραίτητο λοιπόν να εντοπιστεί κρυπτογραφικό πάροχος, ο οποίος θα εφαρμόζει τους αλγορίθμους και έτσι θα

προσφέρει υπηρεσίες μέσω ενός αφηρημένου API.



ΣΧΗΜΑ 4.9 «Κρυπτογραφική Ευέλικτη Αρχιτεκτονική»

Το αφηρημένο API πρέπει να παρέχει κάποιες θεμελιώδεις αρχές που σχετίζονται με τυχαίους αριθμούς και διανομή κλειδιών κρυπτογράφησης. Οι πάροχοι κρυπτογράφησης συνδέονται με εφαρμογές κατά το χρόνο εκτέλεσης, δίχως να υπάρχουν τροποποιήσεις στον πηγαίο κώδικα.

Η μέθοδος που περιγράφεται στο προγούμενο σχήμα ενδέχεται να μην είναι αποτελεσματική σε συστήματα πληρωμών που βασίζονται σε τεχνολογία blockchain. Τα

συστήματα αυτά δεν μοιάζουν με άλλα, καθώς δεν προορίζονται μόνο για την προστασία μιας και μόνο πληροφορίας. Το blockchain είναι καθολικό και ως εκ τούτου είναι το περιουσιακό στοιχείο.

Θεωρητικά οι κβαντικοί υπολογιστές είναι σε θέση να σπάσουν τα κλασικά ασύμμετρα κρυπτογραφικά συστήματα, τα οποία χρησιμοποιούνται στα συστήματα πληρωμών με κάρτες(*RSA ή ECC)*. Αυτό συμβαίνει έχουν τη δυνατότητα να εκτελέσουν τον αλγόριθμο του Shor πολύ γρήγορα. Παρά το ότι οι κβαντικοί υπολογιστές δεν είναι ευρέως διαθέσιμοι, οι hackers μπορούν να συλλέγουν άκρως εμπιστευτικές κρυπτογραφημένες πληροφορίες και να περιμένουν έως ότου ένας κβαντικός υπολογιστής μπορέσει να αποκρυπτογραφήσει αυτά τα δεδομένα. Η δεδομένη απειλή είναι μακροπρόθεσμη και θα μπορούσε για παράδειγμα να αφορά μυστικά στρατιωτικά δεδομένα. Στην περίπτωση τώρα των συναλλαγών με κάρτα, τα δεδομένα κρυπτογραφούνται για αρκετά περιορισμένο χρόνο(*κάποιες ώρες το πολύ)* και έτσι για έναν κακόβουλο τα δεδομένα αυτά είναι άχρηστα. Συνεπώς δεν έχει νόημα να συλλέγουμε κρυπτογραφήματα που αφορούν πληρωμές με κάρτα και να περιμένουμε να τα αποκρυπτογραφήσουμε μελλοντικά. Βέβαια αναφορικά με τις πληρωμές με κάρτα υπάρχει ο κίνδυνος ένας κβαντικός υπολογιστής να παραβιάσει πιστοποιητικά καρτών ή τραπεζών και να τα χρησιμοποιήσει ώστε να κατασκευάσει ψεύτικες κάρτες πληρωμής.

5

«ΣΥΜΠΕΡΑΣΜΑΤΑ & ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ»

Γίνεται αντιληπτό το ότι οι κβαντικοί αλγόριθμοι είναι σε θέση να οδηγήσουν σε νέες και απρόβλεπτες επιθέσεις. Οι τόσο γρήγορες εξελίξεις καθιστούν τα ήδη υπάρχοντα συστήματα κρυπτογράφησης παρωχημένα. Η πιο σημαντική απειλή κατευθύνεται προς τα τρέχοντα συστήματα ψηφιακών υπογραφών RSA,ECC. Παρόμοιες απειλές αντιμετωπίζει και ο αλγόριθμος AES για τον οποίο μάλιστα έχει προταθεί ο διπλασιασμός του μεγέθους του κλειδιού, έχοντας πάντα κατά νου τους περιορισμούς των συστημάτων. Παραδείγματος χάριν, εάν ο αλγόριθμος AES-256 μετατραπεί στον AES-512 σημαίνει αυτόματα ότι αυξάνεται ο αριθμός των γύρων με συνέπεια να προκύπτουν περιορισμοί στην απόδοση. Όσο μεγαλύτερο είναι το κλειδί τόσο πιο ασφαλή είναι τα κρυπτογραφημένα δεδομένα, αλλά και τόσο περισσότεροι γύροι χρειάζονται. Από την άποψη *υλικού* μεγαλύτερο κλειδί σημαίνει μεγαλύτερη επιφάνεια και κατανάλωση ενέργειας.

Στην *ελλειπτική καμπύλη* τα ιδιωτικά κλειδιά είναι δυνατό να υπολογιστούν από κβαντικούς εισβολείς με την αποκάλυψη του αντίστοιχου δημόσιου κλειδιού. Το γεγονός αυτό απειλεί την ασφαλή φύλαξη των περιουσιακών στοιχείων. Ακόμη χειρότερα θα μπορούσε να οδηγήσει σε απώλεια κεφαλαίων χωρίς καμία απολύτως αλληλεπίδραση με τον χρήστη.

Μιλώντας για αναβαθμίσεις στους κρυπτογραφικούς αλγορίθμους πρέπει να τονιστεί ότι είναι απαραίτητο να γίνουν με πλήρη διαφάνεια προς τους χρήστες, προκειμένου να είναι εύκολη και η υιοθέτηση τους. Ένα οικοσύστημα ψηφιακού περιουσιακού στοιχείου συνοδεύεται από ένα μεγάλο μέρος βασικού υλικού με ποικίλες απαιτήσεις. Το να επιλεγεί ο σωστός αλγόριθμος κβαντικής ασφάλειας, σύμφωνα με τις συστάσεις του NIST δεν είναι τόσο απλή διαδικασία και χρήζει ιδιαίτερης προσοχής. Γενικά επικρατεί η άποψη ότι είναι ωφέλιμο η επιλογή του αλγορίθμου να γίνεται σύμφωνα με το σύνολο των στοιχείων, αντί για κάθε μεμονωμένο στοιχείο να επιλέγεται και από ένας αλγόριθμος. Στο συγκεκριμένο πλαίσιο θα κινηθούν *wallets υλικού & wallets λογισμικού.*

5.1 «Προκλήσεις Μετάβασης Στην Post Quantum Cryptography»\

Εξαιτίας της μεγάλης έκτασης του διαδικτύου και της ψηφιοποίησης των περισσότερων τομέων, η μετάβαση στην PQC θα είναι αρκετά περίπλοκη. Μερικές από τις σημαντικότερες προκλήσεις είναι οι παρακάτω:

- Απρόβλεπτο χρονοδιάγραμμα ανάπτυξης των κβαντικών υπολογιστών: Ο πρώτος κίνδυνος πηγάζει από ένα αβέβαιο χρονοδιάγραμμα ανάπτυξης της QC που αυξάνει τον ρυθμό ανάπτυξης σε σχέση με το αναμενόμενο.
- Πολύπλοκα κριτήρια μετεγκατάστασης για την PQC: Η μετάβαση από την κρυπτογραφία δημοσίου κλειδιού στην μετακβαντική κρυπτογραφία είναι περίπλοκη, γεγονός που έχει αναγνωριστεί από το NIST.
- Εκμετάλλευση μεταγενέστερων επιθέσεων: Στον συγκεκριμένο τύπο επίθεσης, μιας και οι περισσότερες ιδιωτικές πληροφορίες μοιράζονται σε κρυπτογραφημένη μορφή, συλλαμβάνονται και χρησιμοποιούνται μετά από χρόνια από κβαντικούς υπολογιστές.
- Επιλογή της συνάφειας των προτύπων NIST: Είναι κρίσιμο να αξιολογηθούν οι επιπτώσεις μετάβασης στην PQC.
- Θέματα Απόδοσης: Οι αλγόριθμοι PQC έχουν υψηλότερες απαιτήσεις υπολογισμού, αποθήκευσης, μνήμης και επικοινωνίας, επομένως οι εκτιμήσεις απόδοσης σε διάφορα σενάρια ανάπτυξης είναι σημαντικές.
- Θέματα Ασφαλείας: Είναι πολύ πιθανό να δημιουργηθούν ποικίλα ζητήματα ασφαλείας, εξαιτίας των αλλαγών στους αλγορίθμους κρυπτογράφησης δημοσίου κλειδιού. Λόγω του ότι ο αλγόριθμος PQC είναι λιγότερο κατανοητός σε σύγκριση με τους ήδη υπάρχοντες, όπως για παράδειγμα τους RSA και ECC, μπορεί να εγείρει ανησυχίες αναφορικά με το μέγεθος του κλειδιού και τον χρόνο υπολογισμού. Σημαντικός επίσης τομέας που χρήζει ιδιαίτερης προσοχής είναι η κρυπτανάλυση των αλγορίθμων PQC.
- Θέματα Υλοποίησης: Η υλοποίηση του αλγορίθμου PQC περιέχει πολύπλοκους μαθηματικούς αλγορίθμους , με αποτέλεσμα να απαιτείται συγκεκριμένη πλατφόρμα και περιβάλλοντα συσκευών.

Οι ήδη υπάρχοντες αλγόριθμοι έχουν περιθώρια βελτιστοποίησης με την εφαρμογή νέων σχεδίων υλικού και λογισμικού. Αυτό θα μπορούσε να βοηθήσει στη μείωση του χρόνου και του χώρου των αλγορίθμων. Θα μπορούσαμε επίσης να εστιάσουμε την προσοχή μας σε τεχνικές για τη μείωση των υπολογιστικών απαιτήσεων, κατασκευάζοντας εξειδικευμένο υλικό ή βελτιώνοντας το λογισμικό. Η θεωρητική και αλγοριθμική έρευνα αριθμών είναι ένα ακόμη πεδίο που θα απασχολήσει, όπως επίσης και η εφαρμογή νέων μαθηματικών τεχνικών που θα βοηθήσουν στην επίλυση δύσκολων προβλημάτων, στα οποία βασίζεται η ασφάλεια των μετακβαντικών συστημάτων.

Πολλές εταιρίες ανά τον κόσμο διαθέτουν πόρους για να προωθήσουν τις γνώσεις και τις πρακτικές που έχουν σχετικά με την Post Quantum Security. Οι αλγόριθμοι συμμετρικών κλειδιών είναι τόσο κλασικοί όσο και ανθεκτικοί κβαντικά(ο AES-256 έχει χρησιμοποιηθεί για τον χαρακτηρισμό του υψηλότερου επιπέδου ασφαλείας για

όλους τους νέους αλγορίθμους), αλλά είναι δύσκολο να εφαρμοστούν σε κβαντικά κυκλώματα, ειδικά δεδομένου ότι η κβαντική μηχανή έχει αναπτυχθεί μόνο για πολύ μικρό μέγεθος μηνύματος(περίπου 20 bit). Για τα συμμετρικά κρυπτοσυστήματα, οι κβαντικοί τρόποι διάρρηξης του αλγορίθμου απαιτούν έναν κβαντικό χρησμό. Εφόσον η συμμετρική κρυπτογραφία δεν εφαρμόζεται με κβαντικούς χρησμούς, είναι ασφαλής έναντι κβαντικών επιθέσεων. Οι επιπτώσεις κβαντικού υπολογισμού είναι πολύ πιο σοβαρές για τα κρυπτοσυστήματα δημοσίου κλειδιού. Μάλιστα ένας αντίπαλος με τοπικούς κβαντικούς πόρους μπορεί να εκμεταλλευτεί και να σπάσει τους αλγορίθμους.

Προς το παρόν, οι κβαντικοί αλγόριθμοι υπάρχουν για όλα τα μεγάλα Κρυπτοσυστήματα Δημοσίου Κλειδιού και είναι θέμα χρόνου να σπάσουν εντελώς. Οι ερευνητές είτε προσπαθούν να αυξήσουν τη σκληρότητα των προβλημάτων που χρησιμοποιούνται αυτή τη στιγμή(RSA,ECC), είτε να βρουν νέα προβλήματα που είναι αρκετά δύσκολα ακόμη και για έναν κβαντικό υπολογιστή. Οι τελευταίες έρευνες που έχουν πραγματοποιηθεί, ενθαρρύνουν τα πεδία των *προβλημάτων πλέγματος, των κωδικών διόρθωσης σφαλμάτων, των μη-μεταθετικών κρυπτοσυστημάτων και των κρυπτοσυστημάτων που βασίζονται σε κατακερματισμό.*

5.2 «Προοπτικές για Security Payment Association»

- Η ταχεία ανάπτυξη των κβαντικών υπολογιστών θέτει σε κίνδυνο τα κρυπτογραφικά συστήματα δημοσίου κλειδιού
- Οι τεχνικές κρυπτανάλυσης που κάνουν χρήση κλασικών υπολογιστών είναι πιθανό να έχουν πιο αδύναμες υλοποιήσεις δημοσίου κλειδιού. Τα οικονομικά αποδοτικά αντίμετρα υπάρχουν και θα πρέπει να λαμβάνονται σοβαρά υπόψιν από την κοινότητα πληρωμών.
- Τα κρυπτογραφήματα εφαρμογών εγκεκριμένων συναλλαγών με κάρτα είναι έγκυρα μόνο για μικρό χρονικό διάστημα. Με τον τρόπο αυτό μια γκάμα επιθέσεων θα καταστεί μη-εφαρμόσιμη στο οικοσύστημα πληρωμών με κάρτα.
- Υπάρχει η δυνατότητα οι κάρτες και τα τερματικά με κρυπτογράφηση να αναπτυχθούν σύμφωνα με την πρωτοβουλία τυποποίησης ISO.

Η βάση όλων των κρυπτογραφιών συστημάτων είναι η αποτελεσματική δημιουργία τυχαίων αριθμών, επομένως εισάγεται μια αρχιτεκτονική αναφοράς για τη δημιουργία και διανομή τυχαίων αριθμών. Είναι γεγονός ότι κβαντικές συσκευές που χρησιμοποιήθηκαν στη δημιουργία συστημάτων, έχουν φτάσει σε σημαντικό επίπεδο ωριμότητας και απόδοσης, με συνέπεια να δικαιολογείται η χρήση τους σε συστήματα πληρωμών.

5.3 «Τεχνικές Απάτης»

- Νιγηριανές Απάτες: Η συγκεκριμένες τεχνικές διαδόθηκαν μέσω των ταχυδρομείων, αλλά συνεχίζουν να γίνονται μέχρι και τις μέρες μας μέσω e-mail. Στην Αμερική, είναι γνωστές επίσης σαν "Advance Fee fraud" ή "419 fraud" (το 419 έρχεται από το άρθρο 419 του Νιγηριανού Ποινικού Κώδικα, το οποίο απαγορεύει και καθιστά παράνομες τέτοιες απάτες). Στη περίπτωση αυτή κάποιος στέλνει ένα e- mail σε πολλαπλούς αποστολείς, όπου αναπτύσσει μια ολόκληρη ιστορία για μια μεταφορά χρημάτων που δεν μπορεί να την κάνει ο ίδιος. Όποιος απαντήσει στο mail κινδυνεύει να του αποσπάσει τον τραπεζικό λογαριασμό ή τα στοιχεία της κάρτας του.
- Phising: Όπως το ίδιο το όνομά του υπονοεί, παραλλαγή του αγγλικού «fishing» (ψάρεμα), το Phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα. Το Phishing επιχειρείται συνήθως με τη αποστολή κάποιου spam e-mail, το οποίο ισχυρίζεται, ψευδώς, ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά θα χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση μη εξουσιοδοτημένων/παράνομων οικονομικών συναλλαγών. Τα e-mail αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, και τον οδηγούν μέσω συνδέσμων σε πλαστά web sites, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών.
- Γεννήτριες Τυχαίων Αριθμών: Χρησιμοποιούνται συνήθως στις απάτες μέσω Internet. Υπάρχει ειδικό λογισμικό, το οποίο «παράγει» τυχαία 16ψήφιους αριθμούς. Ορισμένοι από αυτούς τυχαίνουν να συμπίπτουν με πραγματικές πιστωτικές κάρτες. Οι κάρτες αυτές χρεώνονται όταν ο επιτήδειος κάνει αγορές μέσω Internet.

Η κβαντική κρυπτογραφία, υποτίθεται, πως έπρεπε να είναι απαραβίαστη και μάλιστα πολλές τράπεζες την χρησιμοποιούν για να μεταφέρουν δεδομένα. Όμως ανακοινώθηκε από το Νορβηγικό Πανεπιστήμιο Επιστήμης και Τεχνολογίας στο Τρόντχαϊμ, ότι ένας *"ωτακουστής"* μπορεί να παραβιάσει αυτού του είδους την κρυπτογραφία χωρίς να αφήσει κανένα ίχνος, εκμεταλλευόμενος αστοχίες στον τεχνολογικό εξοπλισμό. Ο καθηγητής Βαντίμ Μακάροφ υποστηρίζει ότι τυχόν κακόβουλοι είναι σε θέση να ελέγξουν από μακριά τον εξοπλισμό του λήπτη και να αποκωδικοποιούν σήματα που μέσω των φωτονίων τα στέλνει ο αποστολέας. Έχουν ανακαλύψει ότι 2 από τις 3 κβαντικές συσκευές που χρησιμοποιούνται είναι ευάλωτες από άποψη ασφαλείας.

Μέσα από την έρευνα φάνηκε ότι αρκετά μεγάλο μέρος της διεκπεραίωσης των τραπεζικών συναλλαγών καταναλώνεται στη διαβίβαση πιστοποιητικών. Στο πλαίσιο αυτό ένα σχέδιο υπογραφών Post Quantum με μικρές υπογραφές θα ήταν η καλύτερη επιλογή. Απαιτείται περαιτέρω εργασία για την εξασφάλιση ενσωματωμένης υλοποίησης από επιθέσεις πλευρικού καναλιού, καθώς και για την παροχή αποδείξεων ασφάλειας για τα πρωτόκολλα.

Βιβλιογραφία

1. Adams C. (2002), Undrestanding PKI: Concepts, Standards and Deployment Considerations, Addison Wesley
2. Bellare M., (2004), Introduction to Modern Cryptography , Course Notes , Mihir Bellare Homepage (ucsd.edu)
3. Λαμπρινή Χαρίτου, (2005), Πανεπιστήμιο Πατρών , Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων
4. Lorenzo Gaston, Technical Director of the Smart Payment Association , "A pathway to improve the security of card payment systems
5. "Evaluation Of Post-Quantum Distributed Ledger Cryptography", Robert e. , Campbell Sr. , Capitol Technology University, USA
6. "RecentTrends on Research and Development of Quantu Computers and Standardization of Post-Quantum Cryptography", Kazutoshi Kan and Masashi Une
7. "How does Post-Quantum Cryptography affect Central Bank Digital Currency?" , Lars Hupel, Makan Rafiee, Munchen, Germany
8. "Ασφάλεια στο Διαδίκτυο και στις Ηλεκτρονικές Συναλλαγές", Πολυχρονόπουλος Άγγελος
9. "Post-Quantum Cryptography: Techniques , Challenges, Standardization and Directions for Future Research", Ritik Bavdekar, Eashan Jayant Chopde, Ashutosh Bhatia, Kamlesh Tiwari, Sandeep Joshua Daniel, Atul
10. "Transitioning Organizations to Post-Quantum Cryptography", David Joseph, Rafael Misoczki, Mark Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, Royal Hansen
11. "Demonstration of Quantum-Digital Payments", Peter Schiansky, Julia Kalb, Esther Sztatecsny, Marie-Christine Roehsner, Tobias Guggemos, Allesandro Trenti, Mathieu Bozzio, Philip Walther
12. "The Security of Card Payment Systems in a Post-Quantum World", An SPA(Security Payment Association) Position Paper, October 2022
13. "Quantum Safe Payment Systems(Markets, Infrastructures, Payment Systems)", Elena Bucciol, Pietro Tiberi
14. "Privacy-Preserving Post-Quantum Credentials for Digital Payments", Raza Ali Kami, Duc-Phong Le, Cyrus Minwalla, Information Technology Services Department, Bank of Canada
15. "Post-Quantum Protocols for Banking Applications", Luk Bettale, Marco De Oliveira, Emmanuelle Dotax
16. "Physical-Layer Security and Quantum Key Distribution", Ivan B. Djordjevic, Department of Electrical and Computer Engineering, University of Arizona