ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Πρωτόκολλο Μηδενικής Γνώσης και Ανάλυση Πρωτοκόλλων Αυθεντικοποίησης

Χαρίλαος Κουτσίκος

Α.Μ. 2008055

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Πρωτόκολλο Μηδενικής Γνώσης και Ανάλυση Πρωτοκόλλων Αυθεντικοποίησης

Χαρίλαος Κουτσίκος, Α.Μ.: 2008055

Επιβλέπων καθηγήτρια: Ελένη Κουτσούκου

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

Όνομα και Επώνυμο Συγγραφέα (Με Κεφαλαία):

ΚΟΥΤΣΙΚΟΣ ΧΑΡΙΛΑΟΣ

……

Υπογραφή (Ολογράφως, χωρίς μονογραφή):

ΚΟΥΤΣΙΚΟΣ ΧΑΡΙΛΑΟΣ

……

Ημερομηνία (Ημέρα – Μήνας – Έτος):

04-01-2016

……

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους γονείς μου για την συνεχή υποστήριξη και την επιβλέποντα καθηγήτρια Ελένη Κουτσούκου για την αμέριστη βοήθειά της στην εκπόνηση της πτυχιακής εργασίας μου.

Περιεχόμενα

Πίνακας περιεχομένων

Περίληψη

Οι διαλογικές αποδείξεις μηδενικής γνώσης (ή αλλιώς πρωτόκολλα μηδενικής γνώσης – zero knowledge protocols, ZKP) αποτελούν ένα εξαιρετικα ενδιαφέρον πεδίο της σύγχρονης κρυπτογραφίας. Από την ανάλυση της κρυπτογραφίας, των αποδείξεων μηδενικής γνώσης και των κρυπτογραφικών εφαρμογών, και τα παραδείγματα των αποδείξεων μηδενικής γνώσης, θα κατανοήσουμε καλύτερα και ορθά τον τρόπο λειτουργίας τους και τα σημαντικότερα προβλήματα που μπορούμε να λύσουμε στην ασφάλεια: τη μυστικότητα, τη πιστοποίηση, την ακεραιότητα, τη ταυτοποίηση, αλλά και τη σημαντικότητα ύπαρξής τους στη σημερινή, γεμάτη τεχνολογία, εποχή μας. Στο $1^{ο}$ κεφάλαιο θα ασχοληθούμε με τους βασικούς ορισμούς και έννοιες τις κρυπτογραφίας και στην συνέχεια με το σημαντικό κομμάτι της ψηφιακής υπογραφής. Στο $3^{ο}$ κεφάλαιο θα αναλύσουμε τα κρυπτογραφικά πρωτόκολλα και τη δομή τους ενώ στο $4^{ο}$ κεφάλαιο θα ασχοληθούμε με τα πρωτόκολλα μηδενικής γνώσης. Στη συνέχεια θα παρουσιάσουμε κάποια παραδείγματα για την καλύτερη κατανόηση ενώ θα αναλύσουμε σε βάθος τα πρωτόκολλα αυθεντικοποίησης. Στο τελευταίο κεφάλαιο θα δούμε τη χρήση της κρυπτογραφίας και των πρωτοκόλλων μηδενικής γνώσης στη σύγχρονη εποχή με παραδείγματα και ανάλυση για τις ψηφιακές υπογραφές.

Λέξεις Κλειδιά

Πρωτόκολλο, Πρωτόκολλο μηδενικής γνώσης, Κρυπτογραφία, Αλγόριθμος, Μηδενική γνώση, Κρυπτογράφηση, Αποκρυπτογράφηση, Κλειδί, Υπογραφή, Ψηφιακή υπογραφή, Κρυπτογραφικό Πρωτόκολλο, Απόδειξη μηδενικής γνώσης, Συμμετρική κρυπτογραφία, ασύμμετρη κρυπτογραφία, πρωτόκολλο αναγνώρισης, Πρωτόκολλο αυθεντικοποίησης Fiat – Shamir, πρωτόκολλο αυθεντικοποίησης Feige – Fiat – Shamir, Πρωτόκολλο αυθεντικοποίησης Guillou – Quisquater, Πρωτόκολλο αυθεντικοποίησης Schnorr, ηλεκτρονική ψηφοφορία

Abstract

The interactive proof (or zero knowledge protocols, ZKP) represent a very interesting field of modern cryptography. From analysing cryptography, zero knowledge proofs, cryptographic practises and examples we will understand clearly and correctly the sufficient way to operate and the major problems that we can solve safely: secrecy, authentication, integrity and the significance of their existence in our time. In the first chapter we will deal with the basic definitions and concepts of cryptography and then the important part of the digital signature. In the third chapter we will analyse cryptographic protocols and their structure while in the fourth chapter will deal with the zero-knowledge protocols. Then we will present some examples to better understand and we will analyse in depth the authentication protocols. In the last chapter we will see the use of cryptography and zero knowledge protocols in modern times with examples and analysis on digital signatures.

Κεφάλαιο 1ο

Για να κατανοήσουμε καλύτερα και πιο εύκολα το πρωτόκολλο μηδενικής γνώσης, καλό θα ήταν να αναφερθούμε πρώτα σε κάποιες βασικές έννοιες της Κρυπτογραφίας και της Ασφάλειας Πληροφοριακών Συστημάτων.

1.1 Κρυπτογραφία

Ένα σημαντικό μέρος της προσπάθειας για μεγαλύτερη ασφάλεια αποτελεί η επιστήμη της κρυπτογραφίας (cryptography). Η κρυπτογραφία αποτελεί κλάδο των μαθηματικών και μέρος της κρυπτολογίας (cryptology). Η κρυπτολογία έχει ένα ακόμα παιδί, την κρυπτανάλυση (cryptanalysis), που είναι η επιστήμη της ανάλυσης και τελικώς του σπασίματος των αλγορίθμων κρυπτογράφησης.

Με την βοήθεια της κρυπτογραφίας μπορούμε να αντιμετωπίσουμε τα σημαντικότερα προβλήματα ασφαλείας.

- Μυστικότητα (secrecy). Η κρυπτογραφημένη πληροφορία θα πρέπει να είναι προσιτή μόνο στο πρόσωπο που κατέχει το μυστικό της αποκρυπτογράφησης του κώδικα.
- Πιστοποίηση (authentication). Θα πρέπει ο παραλήπτης ενός μηνύματος να μπορεί να βεβαιωθεί για την προέλευση του, αποκλείοντας την περίπτωση να χρησιμοποιεί κάποιος την ταυτότητα άλλου.
- Ακεραιότητα (integrity). Θα πρέπει να μπορεί ο παραλήπτης να βεβαιώνεται ότι τα δεδομένα που παρέλαβε δεν τροποποιήθηκαν στην μεταφορά.
- Ταυτοποίηση (non-repudiation). Δεν θα πρέπει να είναι δυνατόν για τον αποστολέα ενός μηνύματος να αρνηθεί αργότερα την πράξη του.

1.2 Αλγόριθμοι κρυπτογράφησης – αποκρυπτογράφησης

Ένας κρυπτογραφικός αλγόριθμος, ή απλά κώδικας (cryptographic algorithm ή cipher), είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση (γενικά υπάρχουν δύο συσχετιζόμενες συναρτήσεις: μία για κρυπτογράφηση και μία για αποκρυπτογράφηση).

1.3 Κλειδί κρυπτογράφησης – αποκρυπτογράφησης

Το πρόβλημα της γνωστοποίησης του κλειδιού του αλγορίθμου έχει λυθεί από την σύγχρονη κρυπτογραφία με το κλειδί, δηλούμενο με το K (από το key). Το κλειδί παίρνει τιμή από ένα πεδίο ορισμού (keyspace), που γενικά διαφέρει από αλγόριθμο σε αλγόριθμο. Τόσο κατά την κρυπτογράφηση όσο και κατά την αποκρυπτογράφηση χρησιμοποιούνται κλειδιά. Τα κλειδιά αυτά μπορεί να είναι ίδια ή διαφορετικά. Στους αλγόριθμους αυτούς όλη η ασφάλεια έγκειται στο κλειδί και όχι στον ίδιο τον αλγόριθμο. Μόνο η γνώση του κλειδιού επιτρέπει ανάκτηση του αρχικού κειμένου.

1.4 Συμμετρική Κρυπτογράφηση

Η κρυπτογράφηση συμμετρικού κλεισιού ή αλλιώς συμμετρική κρυπτογράφηση (Symmetric Cryptography), βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, γνωστό ως μυστικό ή συμμετρικό κλειδί (secret key), το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος. Ο αποστολές και ο παραλήπτης είναι οι μόνοι που πρέπει να γνωρίζουν και να χρησιμοποιήσουν το μυστικό κλειδί. Το παρακάτω σχήμα θα μας βοηθήσει στην καλύτερη κατανόηση της διαδικασίας.

Το μήνυμα προς κρυπτογράφηση, γνωστό ως σαφες κείμενο (plaintext), κρυπτογραφήται με τη χρήση του συμμετρικού (ή αλλιώς μυστικού) κλειδιού. Ηδιαδικασία της κρυπτογράφησης παράγει ένα νέο κείμενο σε ακατανόητη μορφή, γνωστό ως κρυπτογράφημα (ciphertext). Η διαδικασία για την ανάκτηση του αρχικού μηνύματος γίνεται με τη χρήση ξανά του ίδιου συμμετρικου κλειδιού και ονομάζεται αποκρυπτογράφηση.

Σχήμα 1: Απλοποιημένο μοντέλο συμμετρικής κρυπτογραφίας

Ένα σχήμα συμβατικής κρυπτογραφίας αποτελείται από πέντε επιμέρους οντότητες:

- Αρχικό κείμενο (plaintext): Αποτελεί το αρχικό μήνυμα ή τα αρχικά δεδομένα που εισάγονται στον αλγόριθμο κρυπτογράφησης.
- Αλγόριθμος κρυπτογράφησης (encryption algorithm): Πραγματοποιεί τους απαραίτητους μετασχηματισμούς του αρχικού κειμένου για την επίτευξη κρυπτογράφησης ενός μηνύματος.
- Μυστικό κλειδί ή συμμετρικό κλειδί (secret key): Αποτελεί το μυστικό κλειδί, το οποίο εισάγεται επίσης στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό το μυστικό κλειδί.
- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphertext): Είναι το μετασχηματισμένο μήνυμα που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης. Το κρυπτογράφημα αυτό εξαρτάται τόσο από το αρχικό μήνυμα όσο και από το μυστικό κλειδί, συνεπώς δοθέντος ενός μηνύματος διαφορετικά κλειδιά παράγουν διαφορετικά κρυπτογραφήματα.

- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): Πρόκειται για έναν αλγόριθμο που πραγματοποιεί την αντίστροφη διαδικασία, δηλαδή λαμβάνει το κρυπτογράφημα και το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης και παράγει το αρχικό κείμενο.

Για την ασφαλή χρήση της συμμετρικής κρυπτογραφίας πρέπει να ακολουθήσουμε ορισμένες προϋποθέσεις όπως:

- Πρέπει να υπάρχει ένας ισχυρός αλγόριθμος κρυπτογράφησης. Ως ελάχιστη απαίτηση αναφέρεται η ύπαρξη αλγορίθμου για τον οποίο ακόμη και αν είναι γνωστός σε έναν κακόβουλο και υπάρχει πρόσβαση σε ένα ή περισσότερα κρυπτογραφήματα, αυτός δεν δύναται ούτε να υπολογίσει το μυστικό κλειδί, ούτε να διαβάσει το αρχικό κείμενο.

- Ο πομπός και ο δέκτης πρέπει να έχουν παραλάβει τα αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και να διαφυλάσσουν αυτό το μυστικό κλειδί σε ασφαλές μέρος. Εάν κάποιος γνωρίζει τον αλγόριθμο και ανακαλύψει το κλειδί, τότε όλη η επικοινωνία που χρησιμοποιεί αυτό το κλειδί μπορεί να παραβιαστεί.

Το μεγάλο πλεονέκτημα της συμμετρικής κρυπογραφίας είναι η μεγάλη ταχύτητα κρυπτογράφησης και αποκρυπτογραφησης και η μικρή απαίτηση σε μνήμα και υπολογιστική ισχύ. Το μειονέκτημα βεβαίως είναι η ανάγκη για την ανταλλαγή του μυστικού ή συμμετρικού κλειδιού μεταξύ αποστολέα και παραλήπτη. Η ασφάλεια της συμμετρικής κρυπτογραφίας βασίζεται στο γεγονός ότι ο αποστολέας και ο παραλήπτης μοιράζονται το συμμετρικό κλειδί πριν την αποστολή του μηνύματος.

Στην συνέχεια παρουσιάζονται και άλλες περίπλοκες περιπτώσεις για την ασφάλεια . Αν ο αποστολές και ο παραλήπτης είναι άγνωστοι μεταξύ τους θα πρέπει να υπάρχει κάποια πιστοποίηση της ταυτότητας καθ'ενός ώστε να αποφευχθει η διαβίβαση του κλειδιού σε κάποιον τρίτο. Ένας ακόμα περιορισμός είναι η αύξηση του πλήθους των χρηστών που θέλουν να επικοινωνήσουν μεταξύ τους. Αυτό σημαίνει και αύξηση του πλήθους των μυστικών κλειδιών που θα χρησιμοποιηθούν σε κάθε επιμέρους επικοινωνία.

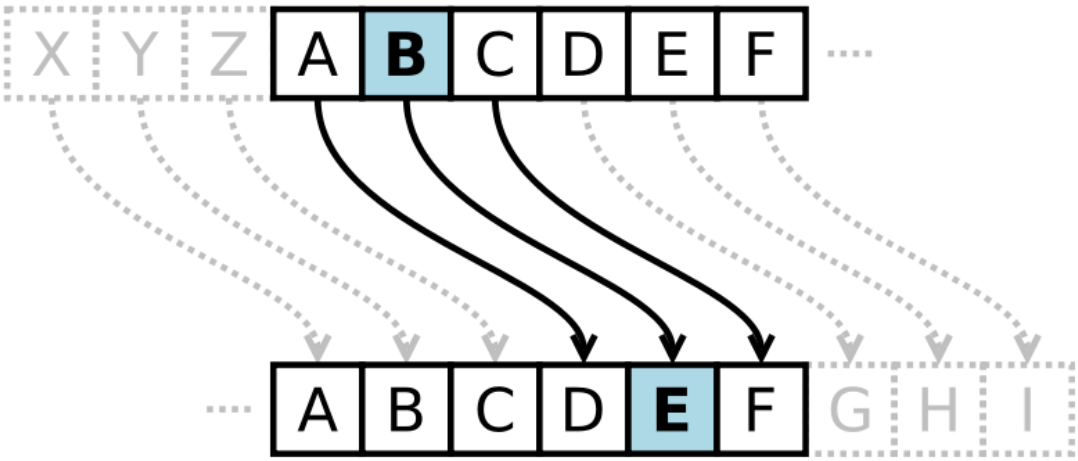
Η συμμετρική κρυπτογραφία χρησιμοποιήται εδώ και χιλιάδες χρόνια. Ο πιο διάσημος από τους κώδικες κρυπτογραφίας είναι ο αλγόριθμος του Καίσαρα.

Είναι κώδικας αντικατάστασης στον οποίο κάθε γράμμα του κειμένου αντικαθίσταται από κάποιο άλλο γράμμα με σταθερή απόσταση κάθε φορά στο αλφάβητο.

Ο αλγόριθμος του Καίσαρα αποτελεί ένα από τα παλαιότερα γνωστά παραδείγματα κρυπτογραφικού αλγόριθμου αντικατάστασης. Η μέθοδος έχει πάρει το όνομά της από τον Ιούλιο Καίσαρα, ο οποίος τη χρησιμοποιούσε για την προσωπική του επικοινωνία.

Κάθε χαρακτήρας του plaintext αντικαθίσταται από ένα χαρακτήρα 3 θέσεις πιο κάτω στο αλφάβητο.

- Plaintext: are you ready
- Ciphertext: duh brx uhdgb



Σχήμα 2: Κώδικας του Καίσαρα

1.5 Ασύμμετρη κρυπτογράφηση

Ένα συμαντικό βήμα για την εξέλιξη της ασφάλειας και της κρυπτογραφίας έγινε στο τέλος της δεκαετίας του 1970 όταν επινωήθηκε ο αλγόριθμος ασύμμετρης κρυπτογράφησης (ή δημόσιου κλειδιού) από τους Whitfield Diffie και Martin Hellman, δίνωντας μας έναν περιορισμό των προβλημάτων της συμμετρικής κρυπτογράφησης. Χρεισιμοποιεί ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης και αποκρυπτογράφησης από την κρυπτογράφηση δημόσιου κλειδιού.

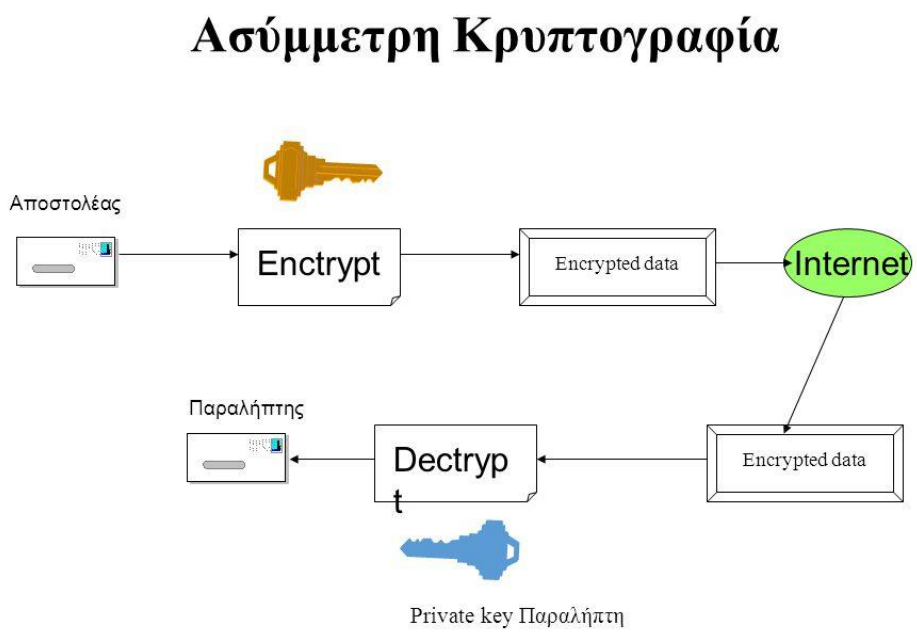
Οι αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται σε μαθηματικές συναρτήσεις. Η χρήση δύο κλειδιών επιφέρει σημαντικές αλλαγές σε βασικά θέματα όπως η εμπιστευτικότητα, η αυθεντικότητα και η διανομή των κλειδιών. Τα δύο αυτά κλειδιά είναι επαρκώς διαφορετικά ώστε η γνώση τους ενός να μην επιτρέπει την παραγωγή ή τον υπολογισμό του άλλου. Αυτό σημαίνει ότι ένα από τα δύο κλειδιά μπορεί να είναι δημόσια γνωστό και διαθέσιμο. Το κλειδί αυτό ονομάζεται δημόσιο (public key) και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Το δεύτερο κλειδί είναι απαραίτητο να μείνει ιδιωτικό και κρυφό, γι'αυτό και ονομάζεται ιδιωτικό κλειδί (private key) και χρησιμοποιείται στην αποκρυπτογράφηση των δεδομένων.

Μία δομή δημοσίου κλειδιού είναι η ακόλουθη

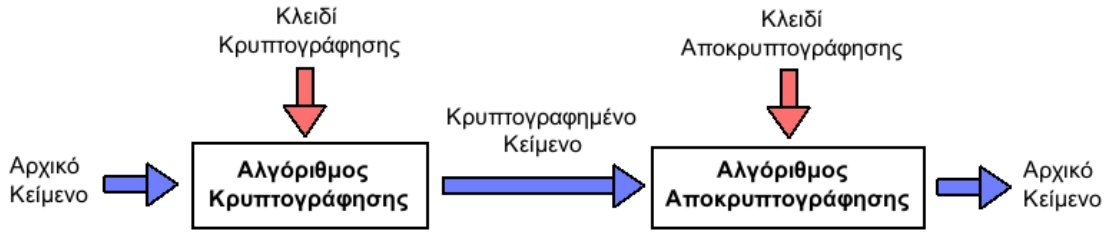
- Αλγόριθμος κρυπτογράφησης (encryption algorithm): ο αλγόριθμος με τον οποίον πραγματοποιούνται οι διάφοροι μετασχηματισμοί στο αρχικό μήνυμα.
- Αρχικό κείμενο (plaintext): είναι το μη κρυπτογραφημένο μήνυμα που αποτελεί στοιχείο εισόδου στον αλγόριθμο κρυπτογράφησης.
- Ζεύγος δημόσιου (public) και ιδιωτικού (private) κλειδιού: Ζεύγος κλειδιών, που έχει επιλεγεί με τρόπον ώστε, το δημόσιο κλειδί του παραλήπτη να χρησιμοποιηθεί για κρυπτογράφηση και το ιδιωτικό κλειδί του παραλήπτη για αποκρυπτογράφηση. Οι ακριβείς μετασχηματισμοί πραγματοποιούνται από τον αλγόριθμο κρυπτογράφησης/αποκρυπτογράφησης, εξαρτώμενοι από τις τιμές του δημόσιου και του ιδιωτικού κλειδιού που παρέχονται ως είσοδοι.

- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphertext): Είναι το μήνυμα που παράγεται από τον αλγόριθμο κρυπτογράφησης ως έξοδος. Εξαρτάται από το αρχικό μήνυμα και το δημόσιο κλειδί του παραλήπτη. Για ένα συγκεκριμένο μήνυμα από δύο διαφορετικά κλειδιά παράγονται από τη συνάρτηση κρυπτογράφησης δύο διαφορετικά κρυπτογραφημένα κείμενα.

- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): Είναι ο αλγόριθμος που δέχεται ως είσοδο το κρυπτογραφημένο μήνυμα και το ιδιωτικό κλειδί και παράγει το πρωτότυπο αρχικό μήνυμα.



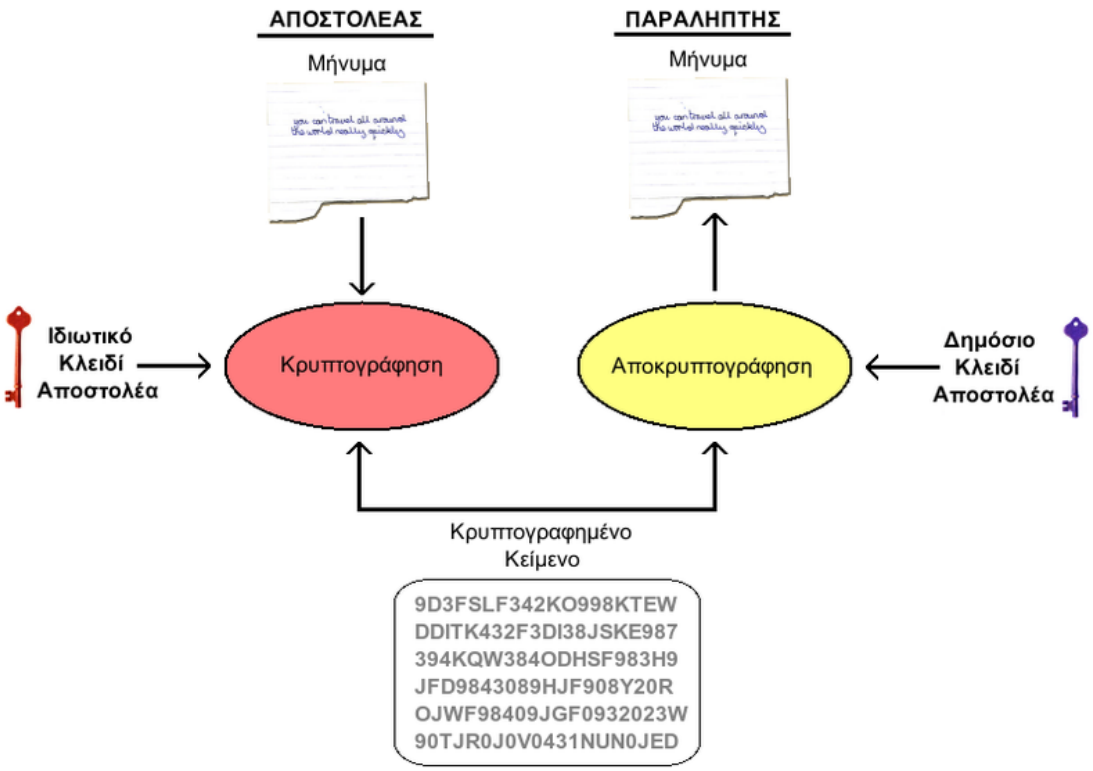
Σχήμα 3: Δομή ασύμμετρης κρυπτογραφίας



Σχήμα 4 :Δομή ασύμμετρης κρυπτογραφίας

Η παραπάνω μέθοδος μπορεί να εξασφαλίσει την εμπιστευτικότητα αλλά όχι την πιστοποίηση του αποστολέα. Αυτό με λίγα λόγια σημαίνει πως η παραπάνω μέθοδος δεν μπορεί να εγγυηθεί την ταυτότητα του αποστολέα. Πράγματι, ο αποστολέας μπορεί να δηλώσει ψευδή ταυτότητα και ο παραλήπτης να νομίσει ότι το συγκεκριμένο μήνυμα προήλθε από άλλο πρόσωπο.

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στη συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.



Σχήμα 5: Επιτυχία στη πιστοποίηση

Παρόλο που η παραπάνω μέθοδος εγγυάται την ταυτοποίηση του αποστολέα, δεν δύναται να εγγυηθεί την εμπιστευτικότητα του μηνύματος. Πράγματι, το μήνυμα μπορεί να το αποκρυπτογραφήσει οποιοσδήποτε διαθέτει το δημόσιο κλειδί του αποστολέα. Όπως έχει ήδη ειπωθεί, το δημόσιο κλειδί είναι γνωστό σε όλη τη

διαδικτυακή κοινότητα, άρα πρακτικά ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος.

Συνδυάζοντας τις δύο τεχνικές που παρουσιάστηκαν παραπάνω είναι εφικτό να επιτύχουμε εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή αφενός το μήνυμα παραμένει γνωστό μονάχα στον αποστολέα και τον παραλήπτη και αφετέρου ο παραλήπτης γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα. Για να επιτευχθεί αυτό ο αποστολέας μπορεί να κρυπτογραφήσει το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στη συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση).

Ένα σημαντικό πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι οτι δεν χρειάζεται ανταλλαγή μυστικού κλειδιού.

ΚΕΦΑΛΑΙΟ 2ο

Αυτό σημαίνει ότι ο αλγόριθμος μπορεί να δημοσιευτεί και να αναλυθεί, όπως επίσης μπορεί να χρησιμοποιηθεί σε προϊόντα μαζικής παραγωγής. Ένας αλγόριθμος μαζί με όλα τα δυνατά κείμενα, κρυπτογραφήματα και κλειδιά λέγεται κρυπτοσύστημα (cryptosystem).

2.1 Ψηφιακή υπογραφή

Η ψηφιακή υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε – παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφημένης συνάρτησης κατατεμαχισμού (hash function) για την δημιουργία της σύνοψης (hash) σε συνδυασμό με ασύμμετρη κρυπτογραφία για κρυπτογράφηση και αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασύμμετρη κρυπτογραφία αποδεικνύει την ακεραιότητα του εγγράφου αλλά και την απόδειξη ταυτότητας του αποστολέα). Σε μερικές χώρες όπως τις ΗΠΑ και κάποιες χώρες της Ευρωπαϊκής ένωσης, οι ψηφιακές υπογραφές έχουν και νομική υπόσταση. Οι ψηφιακές υπογραφές σε ψηφιακά έγγραφα είναι παρόμοιες με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Όταν οι ψηφιακές υπογραφές υλοποιούνται - εφαρμόζονται σωστά (με χρήση ασφαλών κρυπτογραφικών αλγορίθμων), είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες χειρόγραφες. Επίσης το φυσικό πρόσωπο που ψηφιακά υπογράφει το ψηφιακό έγγραφο δεν μπορεί να ισχυριστεί ότι δεν το υπόγραψε (όσο το ιδιωτικό κλειδί που χρησιμοποίησε δεν υποκλάπηκε). Κάποιες υλοποιήσεις των ψηφιακών υπογραφών προσθέτουν και την ημερομηνία υπογραφής του εγγράφου, ώστε και τον ιδιωτικό κλειδί να υποκλαπεί, η ψηφιακή υπογραφή να είναι έγκυρη. Η ψηφιακή υπογραφή μπορεί να προστεθεί σε οποιαδήποτε σειρά από bits (δηλαδή δεδομένα): παραδείγματα χρήσης είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, μηνύματα που στέλνονται στο

Διαδίκτυο κλπ. Πολλοί οργανισμοί υιοθετούν την χρήση των ψηφιακών υπογραφών ώστε να αποφεύγεται η αποστολή τυπωμένων εγγράφων (επικυρωμένα με χρήση σφραγίδων και υπογραφών).

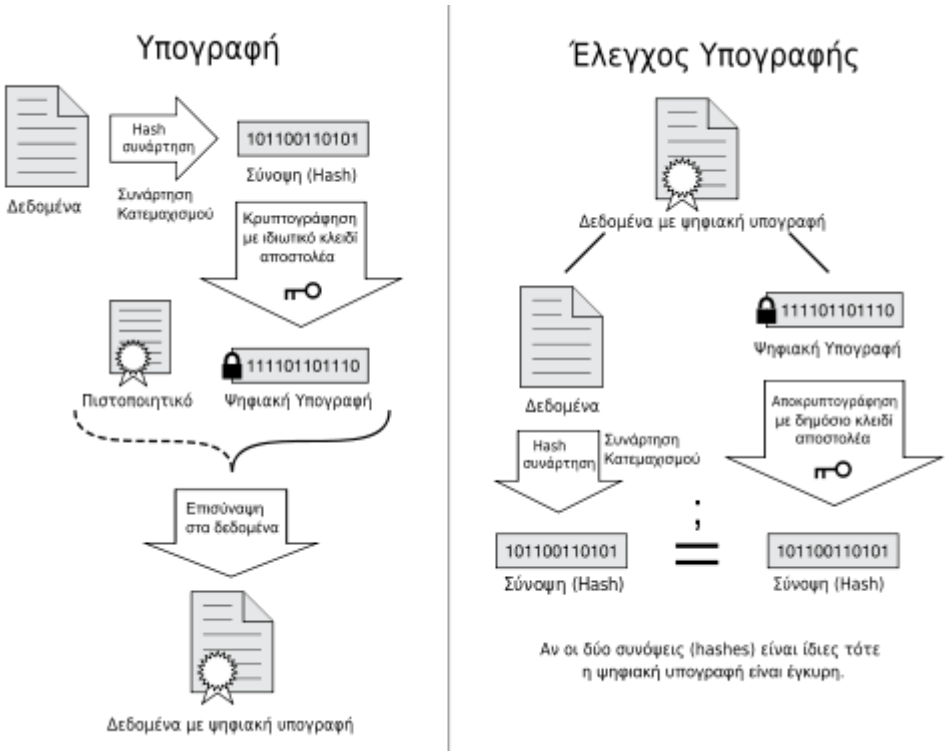
2.2 Ορισμός

Η ψηφιακή υπογραφή αποτελείται από τρείς αλγορίθμους:

- Ο αλγόριθμος δημόσιου και ιδιωτικού κλειδιού: Ο αλγόριθμος αυτός χρησιμοποιεί μια γεννήτρια τυχαίων αριθμών και με βάση αυτόν τον τυχαίο αριθμό δημιουργεί το δημόσιο και ιδιωτικό κλειδί (με το ιδιωτικό κλειδί δημιουργείτε η ψηφιακή υπογραφή και με το δημόσιο κλειδί ελέγχεται η ψηφιακή υπογραφή).
- Ο αλγόριθμος προσθήκης ψηφιακής υπογραφής σε μηνύματα ή έγγραφα: Χρησιμοποιώντας το μήνυμα/έγγραφο και το ιδιωτικό κλειδί (το οποίο ανήκει μόνο σε αυτόν που υπογράφει το έγγραφο), δημιουργεί την ψηφιακή υπογραφή.
- Ο αλγόριθμος ελέγχου ψηφιακής υπογραφής μηνύματος ή εγγράφου: Χρησιμοποιώντας το μήνυμα/έγγραφο και το δημόσιο κλειδί (το δημόσιο κλειδί είναι διαθέσιμο σε όλους, και συσχετίζεται με το ιδιωτικό κλειδί και ανήκει σε αυτόν που υπέγραψε ψηφιακά το μήνυμα/έγγραφο), ελέγχει την αυθεντικότητα (ποιος το υπέγραψε) αλλά και ακεραιότητα (ότι το μήνυμα δεν παραποιήθηκε) του μηνύματος/εγγράφου.

Σύμφωνα με την ασύμμετρη κρυπτογράφηση κάποιος που γνωρίζει το δημόσιο κλειδί δεν μπορεί να δημιουργήσει (είναι υπολογιστικά ανέφικτο) το αντίστοιχο ιδιωτικό κλειδί. Επίσης κάποιος ο οποίος έχει το δημόσιο κλειδί μπορεί να ελέγξει την αυθεντικότητα και ακεραιότητα ενός μηνύματος/εγγράφου το οποίο είναι ψηφιακά υπογεγραμμένο.

Ένα πρόβλημα με τις ψηφιακές υπογραφές είναι ότι δεν γνωρίζουμε αν το δημόσιο κλειδί (κατά την διάρκεια του ελέγχου της υπογραφής) που έχουμε ανήκει σε αυτό που ισχυρίζεται ότι είναι. Για αυτό ακριβώς τον λόγο υπάρχει ο Πάροχος Υπηρεσιών Πιστοποίησης ο οποίος είναι ένας οργανισμός-οντότητα όπου πιστοποιεί την σχέση ενός ανθρώπου με το δημόσιο κλειδί του.



Σχήμα 6: Ανάλυση ψηφιακής υπογραφής

2.3 Ιστορικά στοιχεία

Το 1976 ο Whitfield Diffie και ο Martin Hellman για πρώτη φορά παρουσίασαν την ιδέα των ψηφιακών υπογραφών, αν και η κεντρική ιδέα των τέτοιων συστημάτων προϋπήρχε. Λίγο αργότερα ο Ronald Rivest, ο Adi Shamir και ο Len Adleman παρουσίασαν τον αλγόριθμο RSA ο οποίος χρησιμοποιήθηκε στις πρώτες ψηφιακές υπογραφές. Οι πρώτες ψηφιακές υπογραφές με τον αλγόριθμο RSA αποδείχθηκαν ότι δεν ήταν ασφαλείς. Το πρώτο, ευρέος γνωστό στην αγορά, λογισμικό που χρησιμοποίησε τέτοιες ψηφιακές υπογραφές ήταν τον Lotus Notes 1.0, το οποίο κυκλοφόρησε το 1989.Η χρήση της συνάρτησης κατατεμαχισμού στις ψηφιακές προστέθηκε αργότερα για λόγους ασφάλειας. Η ιδέα είναι ότι υπολογίζεται η σύνοψη (hash) του μηνύματος/εγγράφου και η ψηφιακή υπογραφή υπολογίζεται πάνω στην σύνοψη (hash) και όχι στο μήνυμα/έγγραφο. Άλλοι αλγόριθμοι που αναπτύχθηκαν μετά το RSA ήταν οι ψηφιακές υπογραφές Lamport, οι ψηφιακές υπογραφές Merkle (γνωστές ως δένδρα Merkle ή απλούστερα "δένδρα συνόψεων/hash") και οι ψηφιακές υπογραφές Rabin. Το 1988 ο Shafi Goldwasser, ο Silvio Micali και ο Ronald Rivest ήταν οι πρώτοι που δημοσίευσαν ολοκληρωμένη μελέτη για τις απαιτήσεις ασφάλειας των ψηφιακών υπογραφών. Παρουσίασαν με ποιους τρόπους κάποιος μπορεί να παραβιάσει τις υπάρχουσες υλοποιήσεις ψηφιακών υπογραφών και παρουσίασαν το μοντέλο ψηφιακών υπογραφών GMR.

Οι πρόσφατες υλοποιήσεις ψηφιακών υπογραφών είναι παρόμοιας τεχνικής: χρησιμοποιούν μια συνάρτηση της οποίας η έξοδος δεν είναι προβλέψιμη από την είσοδο (trapdoor function), όπως η συνάρτηση RSA. Η κύρια τεχνική είναι ότι η ψηφιακή υπογραφή είναι η σύνοψη (hash) του μηνύματος κρυπτογραφημένη με το ιδιωτικό κλειδί (χρησιμοποιώντας ασυμμετρική κρυπτογραφία). Υπάρχουν διάφοροι λόγοι που ουσιαστικά εφαρμόζεται η ψηφιακή υπογραφή στην σύνοψη του μηνύματος (hash) και όχι σε ολόκληρο το μήνυμα/έγγραφο:

- Αποτελεσματικότητα (efficiency): Η ψηφιακή υπογραφή είναι πολύ μικρότερη σε μέγεθος και χρειάζεται λιγότερο χρόνος για να εφαρμοστεί η ψηφιακή υπογραφή (η σύνοψη (hash)) έχει πολύ μικρότερο μέγεθος από ότι ολόκληρο το μήνυμα/έγγραφο).
- Συμβατότητα (compartibility): Τα μηνύματα/έγγραφα είναι ουσιαστικά μεταβλητές δέσμες bits. Ο αλγόριθμος κατατεμαχισμού μπορεί να μετατρέψει μεταβλητού μεγέθους δέσμες bits σε συγκεκριμένο αριθμό bits (σύνοψη - hash).
- Ακεραιότητα (integrity): Αν δεν εφαρμοστεί η συνάρτηση κατατεμαχισμού το αρχικό μήνυμα/έγγραφο θα πρέπει να διαιρεθεί σε μικρότερα μεγέθη bits (πακέτα bits) ώστε ο αλγόριθμος ψηφιακών υπογραφών να εφαρμοστεί σε αυτά. Ο αποδέκτης των πακέτων bits δεν είναι σε θέση να αναγνωρίσει αν όλα τα πακέτα έχουν έρθει και αν βρίσκονται στη σωστή σειρά.

ΚΕΦΑΛΑΙΟ 3^{Ο}

Σε αυτό το κεφάλαιο θα ορίσουμε τις έννοιες του πρωτοκόλλου, του κρυπτογραφικού πρωτοκόλλου και των πρωτοκόλλων μηδενικής γνώσης όπου θα αναλύσουμε και τα μέλη από οποία αποτελείται το πρωτόκολλο μηδενικής γνώσης. Θα δοθεί παράδειγμα για τα κρυπτογραφικά πρωτόκολλα.

3.1 Ορισμός πρωτοκόλλου

Ως Πρωτόκολλο επικοινωνίας ορίζεται ένα σύνολο κανόνων συμφωνημένων και από τα δυο επικοινωνούντα μέρη και που εξυπηρετούν την μεταξύ τους ανταλλαγή πληροφοριών. Το πρωτόκολλο επικοινωνίας είναι δηλαδή μια δέσμη κανόνων στους οποίους στηρίζεται η επικοινωνία των υπολογιστών σε ένα δίκτυο. Οι κανόνες αυτοί καθορίζουν τη μορφή, το χρόνο και τη σειρά μετάδοσης των πληροφοριών στο δίκτυο. Εκτελούν, επίσης, έλεγχο και διόρθωση σφαλμάτων στη διάρκεια μετάδοσης των πληροφοριών στο δίκτυο.

3.2 Ορισμός κρυπτογραφικού πρωτοκόλλου

Κρυπτογραφικό πρωτόκολλο είναι η πλήρως αποσαφηνισμένη διαδικασία που πρέπει να ακολουθήσουν τα επικοινωνούντα μέλη, προκειμένου να επιτύχουν μια συγκεκριμένη κρυπτογραφική υπηρεσία. Το βασικό χαρακτηριστικό του κρυπτογραφικού πρωτοκόλλου είναι ότι πρέπει το κάθε μέλος να γνωρίζει σε κάθε χρονική στιγμή (κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου) πιο βήμα πρέπει να εκτελεστεί και πως πρέπει να εκτελεστεί. Οποιαδήποτε παρέκκλιση από τη διαδικασία που απαιτεί το κρυπτογραφικό πρωτόκολλο έχει ως αποτέλεσμα την κατάρρευση της επικοινωνίας ή της υποκείμενης κρυπτογραφικής υπηρεσίας.

Παράδειγμα 1 – Απλό πρωτόκολλο ανταλλαγής κλειδιών. Η Αλίκη και ο Βύρων αποφασίζουν να χρησιμοποιήσουν ένα συμμετρικό κρυπτοσύστημα για να ανταλλάξουν εμπιστευτικά μηνύματα. Η διανομή του κλειδιού γίνεται μέσω ασύμμετρου κρυπτοσυστήματος με το ακόλουθο πρωτόκολλο:

1. Η Αλίκη δημιουργεί ένα συμμετρικό κλειδί.
2. Η Αλίκη ζητά το δημόσιο κλειδί του Βύρωνα.
3. Ο Βύρωνας στέλνει το δημόσιό του κλειδί στην Αλίκη
4. Η Αλίκη κρυπτογραφεί το συμμετρικό κλειδί με το κλειδί του Βύρωνα.
5. Η Αλίκη στέλνει το κρυπτογραφημένο κλειδί στον Βύρωνα σε μορφή κρυπτογραφημένου μηνύματος.
6. Ο Βύρωνας αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα και ανακτά το συμμετρικό κλειδί.

Με την ολοκλήρωση του πρωτοκόλλου η Αλίκη και ο Βύρων έχουν ένα κοινό συμμετρικό κλειδί το οποίο το μοιράστηκαν με εμπιστευτικότητα.

3.3 Τα Μέλη του πρωτοκόλλου μηδενικής γνώσης.

- Ο Αποδείκτης (Αλίκη), ο οποίος έχει μία πληροφορία που επιθυμεί να αποδείξει στον Επαληθευτή (Βύρων), χωρίς όμως να αποκαλύψει το μυστικό σε αυτόν.
- Ο Επαληθευτής (Βύρων), ο οποίος ρωτά κάποιες ερωτήσεις τον Αποδείκτη (Αλίκη), προσπαθώντας να μάθει εάν όντως ο Αποδείκτης έχει στη κατοχή του το μυστικό. Ο Επαληθευτής δεν μαθαίνει καμία πληροφορία για το μυστικό, ακόμα και αν απατήσει ή δεν ακολουθήσει τους κανόνες του πρωτοκόλλου.

3.4 Επισκόπηση

Ένα μειονέκτημα των πρωτοκόλλων τα οποία είναι κρυπτογραφημένα με απλό κωδικό (Simple password protocols) είναι ότι όταν ο αποδείκτης (Prover) δώσει στον

επαληθευτή (Verifier) τον κωδικό τους, τότε ο αποδείκτης μπορεί να υποδύεται τον επαληθευτή. Το πρωτόκολλο μηδενικής γνώσης (Zero-Knowledge protocol) επιτρέπει στον αποδείκτη να αποδείξει ότι κατέχει γνώση ενός μυστικού στον επαληθευτή, χωρίς να αποκαλύψει καμία χρήσιμη πληροφορία για αυτό το μυστικό. Πρωτόκολλα απόδειξης με αλληλεπίδραση χρησιμοποιούνται ως η βάση των πρωτοκόλλων μηδενικής γνώσης.

ΚΕΦΑΛΑΙΟ 4ο

4.1 Πρωτόκολλα Μηδενικής Γνώσης

Μεγάλο Ενδιαφέρον παρουσιάζουν τα πρωτόκολλα μηδενικής γνώσης (Zero Knowledge protocols). Τα πρωτόκολλα μηδενικής γνώσης κατατάσσονται στην κατηγορία πρωτοκόλλων **απόδειξης με αλληλεπίδραση** (Interactive Proof), που σημαίνει ότι τα συμμετέχοντα μέλη ανταλλάσουν πλήθος μηνυμάτων τα οποία βασίζονται σε τυχαίους αριθμούς και σε οποιαδήποτε στιγμή μπορεί οποιοδήποτε από τα μέλη να τερματίσει το πρωτόκολλο.

Τα πρωτόκολλα μηδενικής γνώσης αναφέρονται κυρίως σε πρωτόκολλα αυθεντικοποίησης ταυτότητας. Το κίνητρο της ανάπτυξης των πρωτοκόλλων μηδενικής γνώσης είναι το γεγονός ότι στα «συμβατικά» πρωτόκολλα αυθεντικοποίησης, κατά την ολοκλήρωση της εκτέλεσης τους, το μέλος το οποίο επαληθεύει την ταυτότητα του ομότιμού του έχει στην κατοχή του μηνύματα και μυστικά τα οποία μπορεί να τα χρησιμοποιήσει για πλαστοπροσωπία. Στα πρωτόκολλα μηδενικής γνώσης , το μυστικό το οποίο χρησιμοποιείται για να αποδειχθεί η ταυτότητα ενός μέλους, εξαρτάται από συγκεκριμένη χρονική στιγμή, έτσι ώστε σε άλλη στιγμή να είναι άχρηστο. Με άλλα λόγια η Αλίκη μπορεί να αποδείξει στον Βύρωνα ότι γνωρίζει κάποιο μυστικό, χωρίς να του αποκαλύψει καμία πληροφορία για το μυστικό αυτό. Προκειμένου να κατανοήσουμε την έννοια του πρωτοκόλλου μηδενικής γνώσης είναι αναγκαίο να δώσουμε τον ορισμό από τον οποίο μπορούμε να χαρακτηρίσουμε ένα πρωτόκολλο ως πρωτόκολλο μηδενικής γνώσης. Ως μυστικό απόδειξης ορίζουμε το μυστικό το οποίο είναι γνωστό μόνο στο τέλος το οποίο προκαλούμε να μας αποδείξει ότι έχει στην κατοχή του το μυστικό αυτό.

4.2 Ορισμός Πρωτοκόλλου Μηδενικής γνώσης

Ένα πρωτόκολλο χαρακτηρίζεται ως πρωτόκολλο μηδενικής γνώσης, αν και μόνο αν υπάρχει αλγόριθμος ο οποίος λειτουργεί σε πολυωνυμικό χρόνο και έχει την δυνατότητα να παράγει σύνολο μηνυμάτων του πρωτοκόλλου χωρίς τη γνώση του μυστικού απόδειξης, έτσι ώστε το σύνολο των μηνυμάτων να μην είναι δυνατό να διακριθεί από ένα σύνολο «πραγματικών» μηνυμάτων που προέρχονται από την εκτέλεση του πρωτοκόλλου με το μέλος που γνωρίζει τον μυστικό απόδειξης.

Ισοδύναμα αυτό σημαίνει ότι όλα τα μηνύματα που ανταλλάσσονται σε ένα πρωτόκολλο μηδενικής γνώσης δε δίνουν απολύτως καμία πληροφορία για το μυστικό απόδειξης. Από τον παραπάνω ορισμό μπορούμε να κατανοήσουμε τη διαφορά ενός πρωτοκόλλου μηδενικής γνώσης από ένα πρωτόκολλο αυθεντικοποίησης πρόκλησης-απόκρισης με ψηφιακές υπογραφές. Αν και ο κάτοχος του ιδιωτικού κλειδιού δε φανερώνει ποτέ το κλειδί αυτό, είναι πολύ εύκολο να ελέγξουμε αν ένα μήνυμα είναι μέρος του πρωτοκόλλου. Για παράδειγμα, η ψηφιακή υπογραφή της Αλίκης επάνω στην πρόκληση του Βύρωνα, αποδεικνύει ότι η Αλίκη κατέχει το ιδιωτικό της κλειδί, αλλά το μήνυμα της ψηφιακής υπογραφής της Αλίκης δεν είναι δυνατό να δημιουργηθεί χωρίς τη συμμετοχή του ιδιωτικού κλειδιού (σε πολυωνυμικό χρόνο). Αυτή η χαρακτηριστική διαφορά μεταξύ ενός πρωτοκόλλου μηδενικής γνώσης και ενός πρωτοκόλλου αυθεντικοποίησης με ψηφιακές υπογραφές, είναι ο λόγος όπου σε ένα πρωτόκολλο μηδενικής γνώσης δεν υπάρχει υποβάθμιση της ασφάλειας ως προς τον χρόνο, καθώς δεν υπάρχει διαρροή της πληροφορίας του μυστικού απόδειξης. Αντίθετα, σε ένα πρωτόκολλο ψηφιακών υπογραφών, κάποιος αντίπαλος ο οποίος υποκλέπτει τα μηνύματα, μπορεί σε κάποια χρονική στιγμή να τα χρησιμοποιήσει για να επιτύχει πλαστοπροσωπία.

4.3 Δομή πρωτοκόλλων μηδενικής γνώσης

Θεωρούμε ότι η Αλίκη έχει ένα μυστικό και θέλει να το αποδείξει στον Βύρων με τη χρήση πρωτοκόλλου μηδενικής γνώσης. Ένας κύκλος ενός πρωτοκόλλου μηδενικής γνώσης αποτελείται από τρία στάδια:

1. **Στάδιο μαρτυρίας**, όπου η Αλίκη στέλνει μήνυμα δέσμευσης στον Βύρωνα. Το στάδιο αυτό αρχικοποιεί το πρωτόκολλο εισάγοντας τυχαιότητα. Το στάδιο αυτό περιλαμβάνεται για δύο λόγους. Πρώτον, τα μηνύματα που θα επακολουθήσουν δεν θα μπορούν να χρησιμοποιηθούν στο μέλλον από τον αντίπαλο. Δεύτερον, η μαρτυρία είναι η δημοσίευση της δέσμευσης της Αλίκης, από την οποία ο Βύρων επιλέγει την πρόκληση στο επόμενο στάδιο.
2. **Στάδιο πρόκλησης**, όπου ο Βύρων στέλνει την πρόκληση του στην Αλίκη. Η πρόκληση επιλέγεται από τον μήνυμα δέσμευσης της Αλίκης. Η Αλίκη δεν είναι σε θέση να γνωρίζει εκ των προτέρων ποια θα είναι η πρόκληση του Βύρωνα. Τα δύο στάδια παρομοιάζονται με την αρχή της «κοπής και επιλογής» (cut-and-choose), όπου ένας κόβει μια πίτα σε δύο κομμάτια, αλλά ο άλλος επιλέγει πρώτος το κομμάτι.
3. **Στάδιο απόκρισης,** όπου η Αλίκη καλείται να υπολογίσει τη σωστή απάντηση της πρόκλησης του Βύρωνα σε πολυωνυμικό χρόνο και να ενημερώσει τον Βύρωνα για τη λύση.

ΚΕΦΑΛΑΙΟ 5ο

Σε αυτό το κεφάλαιο θα δώσουμε μερικά παραδείγματα αποδείξεων μηδενικής γνώσης.Θα αναλύσουμε τις ιδιότητες και τα χαρακτηριστικά των πρωτοκόλλων μηδενικής γνώσης.

Επίσης θα αναλύσουμε το πρόβλημα Ισομορφισμού Γραφημάτων, το πρωτόκολλο αυθεντικοποίησης Fiat – Shamir,το πρωτόκολλο αναγνώρισης Feige – Fiat – Shamir, το πρωτόκολλο αυθεντικοποίησης Guillou – Quisquater και το Πρωτόκολλο αυθεντικοποίησης του Schnorr.Τέλος θα ασχοληθούμε με την ασφάλεια των πρωτοκόλλων Fiat – Shamir και Feige – Fiat – Shamir

5.1 Παραδείγματα αποδείξεων μηδενικής γνώσης

Θα δούμε εδώ μερικά παραδείγματα πρωτοκόλλων μηδενικής γνώσης. Τα παραδείγματά μας προέρχονται κυρίως από την Υπολογιστική Πολυπλοκότητα. Αλλά αφορούν και κρυπτογραφικές εφαρμογές : (i) τα συγκεκριμένα παραδείγματα αποδίδουν πολύ καλύτερα τη διαίσθηση των αποδείξεων μηδενικής γνώσης σε σύγκριση με τα παραδείγματα που αφορούν σε αριθμοθεωρητική κρυπτογραφία, (ii) υπάρχει μία βαθύτερη σχέση των NP-πλήρων προβλημάτων με τις κρυπτογραφικές εφαρμογές

Παράδειγμα 1 - Πού είναι ο Waldo**;**

Στο παιχνίδι Πού είναι ο Waldo, υπάρχει ένα μεγάλο ταμπλό που απεικονίζει μια σκηνή με πολλούς χαρακτήρες που μοιάζουν με τον "Waldo". Στόχος του παιχνιδιού είναι να βρούμε τον Waldo.

Υποθέτουμε ότι η Αλίκη και ο Βύρωνας παίζουν αυτό το παιχνίδι. Η Αλίκη υποστηρίζει ότι έχει βρει που βρίσκεται ο Waldo αλλά δεν θέλει να το πει στο Βύρωνα. Η υπόθεση ότι ο Waldo υπάρχει είναι η πρόταση, οι συντεταγμένες (x, y)

της θέσης του Waldo είναι ο μάρτυρας, και η διαδικασία λήψης των (x, y) και η επιβεβαίωση ότι ο Waldo είναι όντως εκεί σχετίζεται με το κατηγόρημα R.

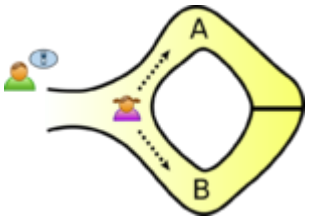
Μια πιθανή λύση και όχι μοναδική είναι η Αλίκη να καλύψει το ταμπλό με ένα μεγάλο κομμάτι χαρτί και μια μικρή τρύπα στο κέντρο. Η Αλίκη θα τοποθετήσει το χαρτί στο ταμπλό έτσι ώστε να εμφανιστεί μόνο ο Waldo. Η λύση θα είναι αποτελεσματική αν το χαρτί έχει τουλάχιστον διπλάσιες διαστάσεις από το ταμπλό.

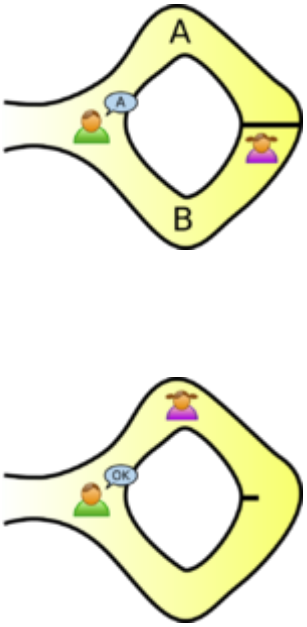
Παράδειγμα 2– Η μαγική πόρτα

Το επόμενο παιχνίδι που θα μας απασχολήσει είναι το εξής.

1. Στο βάθος μιας σπηλιάς υπάρχει μια μαγική πόρτα που μπορεί να ανοίξει χρησιμοποιώντας ένα μυστικό κωδικό. Ο Βύρωνας προσπαθεί να πείσει την Αλίκη ότι γνωρίζει τον κωδικό και συνεπώς πως μπορεί να ανοίξει την μαγική πόρτα.

1. Η Αλίκη κάθεται στο σημείο 1.
2. Ο Βύρωνας μπαίνει στην σπηλιά και κάθεται στα σημεία 3 ή 4.
3. Όταν ο Βύρωνας εξαφανίζεται, η Αλίκη προχωρά στο σημείο 2.
4. Η Αλίκη φωνάζει τον Βύρωνα, ρωτώντας τον να βγει είτε από το αριστερό μονοπάτι είτε από το δεξί.
5. Ο Βύρωνας δρα σύμφωνα με αυτό χρησιμοποιώντας τον μυστικό κωδικό αν είναι αναγκαίο.





Σχήμα 7 Παράδειγμα: Η μαγική πόρτα

Αυτό το παιχνίδι μας δείχνει μια απόδειξη γνώσης μέσω μιας πιθανοτικής διαδικασίας. Συγκεκριμένα, μετά από k επαναλήψεις, ο Βύρωνας μπορεί να πείσει την Αλίκη πως ξέρει τον μυστικό κωδικό με πιθανότητα $1 - 1/2k$.

5.2 Ιδιότητες πρωτοκόλλων μηδενικής γνώσης

Πληρότητα (Completeness): Αν $x \in L$ και $R(x, w) = 1$ για κάποιο μάρτυρα w, τότε out $VP,V(x, w, z) = 1$ για κάθε συμβολοακολουθία z με συντριπτική πιθανότητα v.

Ορθότητα (Soundness): Για κάθε πολυωνυμικού χρόνου πρόγραμμα $P*$ ορίζουμε $\pi.x.\ w, z = \text{Prob}[\text{out } VP*,V(x, w, z) = 1]$.
Ένα πρωτόκολλο EP,VI ικανοποιεί την ορθότητα αν για κάθε $P*$ υπάρχει πρόγραμμα, μια πιθανοτική Turing machine (PTM), που ονομάζεται ***knowledge extractor (εξαγωγέας γνώσης)*** με την ακόλουθη ιδιότητα. Έστω ότι
$\pi\, x, w, z = \text{Prob}[\, K(x, w, z) = w\, O : R(x, w\, O) = 1\,]$.

Τότε ισχύει ότι αν το $\pi.x.\ ,w\ ,z$ είναι μη αμελητέο, τότε και το $\pi.x.\ ,w\ ,z$ είναι μη αμελητέο.

(Στατιστική) Μηδενική Γνώση ((Statistical) Zero-Knowledge) (SZK): Για κάθε πολυωνυμικού χρόνου πρόγραμμα $V*$, υπάρχει ένα PTM πρόγραμμα S, που ονομάζεται ***simulator (προσομοιωτής)***, τέτοιο ώστε για κάθε x, w με $R(x, w) = 1$, οι τυχαίες μεταβλητές $S(x, z)$ και out $V^* P V^* (x, w, z)$ είναι
στατιστικά αδιαχώριστες για όλες τις συμβολοακολουθίες z: A

Prob $[A(S(x, z)) = 1]$ – Prob $[A(\text{out } V* P, V* (x, w, z)) = 1] < \varepsilon$

Η **πληρότητα** είναι όμοια με την σωστή λειτουργία του πρωτοκόλλου. Υποθέτοντας ότι ο prover και ο verifier ακολουθούν το πρωτόκολλο πιστά, η πληρότητα εγγυάται πως το πρωτόκολλο θα επιτύχει με ικανοποιητικά μεγάλη πιθανότητα.

Η διαισθητική ερμηνεία της **ορθότητας** διασφαλίζει πως το πρωτόκολλο θα αποτύχει όταν εκτελείται από έναν prover που χρησιμοποιεί έναν ψεύτικο μάρτυρα και από έναν τίμιο verifier. Αυτή είναι μια ελάχιστη απαίτηση. Ο τυπικός ορισμός που δώσαμε απαιτεί κάτι ισχυρότερο. Εγγυάται πως ένας εξαγωγέας γνώσης K
μπορεί να εξάγει έναν έγκυρο μάρτυρα από κάθε πειστικό prover. Αυτό συνεπάγεται πως ο K πρέπει να έχει παραπάνω ισχύ από τον verifier. Συγκεκριμένα ο K έχει πρόσβαση στο πρόγραμμα του prover σε αντίθεση με τον verifier (ο verifier είναι ένα πρόγραμμα που αλληλεπιδρά με τον prover, ενώ ο εξαγωγέας γνώσης είναι
ένα πρόγραμμα που προέρχεται από το πρόγραμμα του prover).

Η **στατιστική μηδενική γνώση** είναι η ιδιότητα που απαγορεύει την εξαγωγή κάποιας γνώσης ενός verifier από έναν τίμιο prover. Αν ο verifier μπορεί να μάθει κάτι θα πρέπει να υπάρχει ένας αλγόριθμος που προσομοιώνει το πρωτόκολλο χωρίς πρόσβαση σε έναν μάρτυρα. Επιπλέον η εκτέλεση του αλγορίθμου είναι αδιαχώριστη από αυτή του πρωτοκόλλου.

Μια ασθενέστερη εκδοχή της μηδενικής γνώσης είναι η μηδενική γνώση τίμιου verifier (honest-verifier zero-knowledge) (HVZK). Σε αυτήν υποθέτουμε πως ο verifier εκτελεί το πρωτόκολλο τίμια, αλλά κάνει επιπλέον υπολογισμούς.

Ειδικότερα, αυτό απεικονίζεται στον ορισμό μας περιορίζοντας τον V ∗ να προσομοιώνει τον verifier V και στο τέλος, να επιστρέφει ολόκληρη την επικοινωνία. Το να επιτύχουμε την ασθενέστερη ιδιότητα ονομάζεται μερικές φορές μηδενική γνώση ημι-τίμιου (semi-honest) verifier. Αν και αυτό χαλαρώνει τις προδιαγραφές του SZK, μπορεί να χρησιμοποιηθεί για να επιτύχουμε αποδείξεις μηδενικής γνώσεις σε καταστάσεις, χρησιμοποιώντας γενικές μεθόδους. Η απόδειξη μηδενικής γνώσης τίμιου verifier ανάγεται στην δημιουργία συνομιλιών πρωτοκόλλων αποδοχής τα οποία είναι αδιαχώριστα από τις συνομιλίες του πρωτοκόλλου μεταξύ τίμιου prover-verifier, χωρίς τη γνώση μάρτυρα.

5.3 Χαρακτηριστικά πρωτοκόλλου μηδενικής γνώσης

Το πρωτόκολλο μηδενικής γνώσης μπορεί να περιγραφεί ως ένα πρωτόκολλα κρυπτογράφησης που έχει τα ακόλουθα χαρακτηριστικά:

- Ο επαληθευτής δεν μαθαίνει κάτι από το πρωτόκολλο. Ο επαληθευτής δεν μπορεί να μάθει κάτι από το πρωτόκολλο, το οποίο που δεν θα μπορούσε να μάθει από μόνος του. Αυτή είναι η κεντρική ιδέα της μηδενικής γνώσης.
- Ο αποδείκτης δεν μπορεί να εξαπατήσει τον επαληθευτή. Αν ο αποδείκτης δεν γνωρίζει το μυστικό απόδειξης, τότε μπορεί να το επιτύχει μόνο με πολλή καλή τύχη . Μετά από αρκετούς γύρους του πρωτοκόλλου οι πιθανότητες μιας τέτοιας περίπτωσης είναι πολύ μικρή . Τα πρωτόκολλα ακολουθούν την αρχή "κοπής και επιλογής" δηλαδή την πρώτη φορά που ο αποδείκτης αποτύχει, ο επαληθευτής ξέρε ι ότι ο αποδείκτη ς δεν είναι αξιόπιστος. Έτσι, με κάθε γύρο του πρωτοκόλλου η βεβαιότητα γίνεται όλο και μεγαλύτερη .
- Ο επαληθευτής δεν μπορεί να εξαπατήσει τον αποδείκτη. Ο επαληθευτής δεν μπορεί να πάρει καμία πληροφορία που προβλέπεται έξω από το πρωτόκολλο, ακόμη και αν δεν ακολουθήσει το πρωτόκολλο . Το μόνο πράγμα που ο επαληθευτής μπορεί να κάνει είναι να πείσει τον εαυτό του ότι ο αποδείκτης ξέρει το μυστικό απόδειξης . Ο αποδείκτης πάντα αποκαλύπτει μόνο μία λύση από τις πολλές ενός προβλήματος και ποτέ δεν επιτρέπει να αποκαλυφτεί το μυστικό απόδειξης.
- Ο επαληθευτής δεν μπορεί να υποκριθεί ότι είναι ο αποδείκτης σε κάποιο τρίτο μέλος. Επειδή καμία πληροφορία δ ε μπορεί να διαρρεύσει από τον

αποδείκτη στο επαληθευτή, ο επαληθευτής δεν μπορεί να μεταμφιεστεί ω ς αποδείκτη ς σε κάποιο τρίτο μέλος. Σε μερικά από αυτά τα πρωτόκολλα το να υπάρξει ένας άνθρωπος στη μέση της επίθεσης είναι πολύ πιθανό. Κάποιος δηλαδή μπορεί να μεταδώσει την συνομιλία από το αληθινό αποδείκτη και να προσπαθήσει να πείσει ότι έναν άλλο επαληθευτή ότι αυτός είναι ο αποδείκτης. Επίσης , εάν ο επαληθευτής καταγράφει τη συνομιλία μεταξύ αυτού και του αποδείκτη, η εγγραφή αυτή δεν μπορεί να χρησιμοποιηθεί για να πείσει κάποιο άλλο τρίτο πρόσωπο .

- Ο επαληθευτής μπορεί να πεισθεί μόνο από αληθείς καταστάσεις. Αυτή η ιδιότητα ονομάζεται ορθότητα (όπως έχουμε ήδη αναφέρει) και λαμβάνεται ουσιαστικά η ικανότητα κάποιων αποδεικτών να πείσουν τον επαληθευτή για μια αληθή κατάσταση.

.

5.4 Το πρόβλημα Ισομορφισμού Γραφημάτων

Ας δούμε ένα πρωτόκολλο για το πρόβλημα του Ισομορφισμού Γραφημάτων (GI, Graph Isomorphism). Στο πρωτόκολλο που παρατίθεται ο prover ξεκινά ενώ κάνει και χρήση τυχαίων bits:

Είσοδος: γραφήματα G1 = (V1 , E1) και G2 = (V2 , E2). Δίχως βλάβη της γενικότητας, θεωρούμε πως αν το Gi έχει n κορυφές, αυτές είναι οι V,: = { 1, 2, .. . , n}. Ερώτημα: υπάρχει ισομορφισμός ανάμεσα στα G1 και G2 , δηλ. υπάρχει συνάρτηση f : Vi → V2 που να είναι 1-1 και επί, τέτοια ώστε να υπάρχει ακμή ανάμεσα στις κορυφές u, υ αν και μόνον αν υπάρχει ακμή ανάμεσα στις κορυφές f (u) , f (υ).

Ο ακόλουθος πίνακας διατυπώνει σε διαλογική μορφή το πρωτόκολλο για το πρόβλημα GI.

Πρέπει να προσέξουμε πως ο prover διαλέγει τυχαία ένα από τα δύο γραφήματα, έπειτα δημιουργεί ένα ισομορφικό του αντίγραφο (με μία τυχαία μετάθεση των κορυφών { 1, 2, ... , n}) και το αποστέλλει στον verifier. Αυτός απαντά έχοντας επιλέξει τυχαία ένα από τα δύο γραφήματα τη ς εισόδου και ο prover καλείται τώρα

να επιδείξει έναν ισομορφισμό ανάμεσα στο γράφημα που επέλεξε ο verifier και σε αυτό που του απέστειλε ο ίδιος στον πρώτο γύρο επικοινωνίας.

Prover	Επικοινωνία	Verifier
Διάλεξε τυχαίο i E {1 , 2}, διάλεξε τυχαία μετάθεση π του {1, 2, .. n} και υπολόγισε το γράφημα π(*Gi)* = H		
	→H→	
		Διάλεξε τυχαίο j E {1, 2}
	←j←	
Υπολόγισε μετάθεση σ τέτοια ώστε σ(Gj) =H		
	→σ→	
		Αποδοχή αν σ(Gj) =H

Θεώρημα 1- Το ανωτέρω πρωτόκολλο είναι ένα πρωτόκολλο μηδενικής γνώσης για το πρόβλημα GI

Απόδειξη

- **Πληρότητα**: Αν τα δύο γραφήματα που δίδονται στην είσοδο είναι ισομορφικά, τότε το τυχαίο ισομορφικό αντίγραφο H που θα αποσταλεί θα είναι ισομορφικό και προς τα δύο γραφήματα της εισόδου. Αν λοιπόν ένας έντιμος επαληθευτή ς ακολουθήσει τα βήματα του πρωτοκόλλου, θα αποδεχθεί με πιθανότητα 1.

- **Ορθότητα**: Έστω (G1 , G2) ~ GI (τα γραφήματα δεν είναι ισομορφικά). Τότε ο verifier θα απορρίψει το στιγμιότυπο με πιθανότητα τουλάχιστον ~ και η πιθανότητα λάθους μπορεί να μειωθεί περαιτέρω με διαδοχικές επαναλήψεις του αλγορίθμου. Όντως, στην περίπτωση μη ισομορφικών γραφημάτων, ανεξάρτητα από την στρατηγική του prover, το γράφημα H που αποστέλλεται στο πρώτο μήνυμα δεν μπορεί να είναι ισομορφικό ταυτόχρονα με το G1 και το G2 . Άρα υπάρχει j E {1, 2} τέτοιο ώστε το H να μην είναι ισομορφικό με το Gj. Ο verifier όμως επιλέγει το j αυτό με πιθανότητα ~ και τότε ο prover δεν μπορεί να βρει μετάθεση σ τέτοια ώστε σ (G j) = H. Προφανώς, ο verifier σε αυτή τη περίπτωση απορρίπτει.

- **Μηδενική γνώση** : Θα περιγράψουμε τη λειτουργία ενός προσομοιωτή , ενός αλγορίθμου δηλαδή ο οποίος παράγει ανάμεσα σε prover και σε verifier ένα πρακτικό επικοινωνίας, το οποίο έχει την ίδια ακριβώς πιθανοτική κατανομή με αυτό που παράγεται από το πρωτόκολλο μηδενικής γνώση ς για το πρόβλημα GI. Ο προσομοιωτής S * διαλέγει τυχαία i' Ε { 1, 2} και μια τυχαία μετάθεση π του { 1, 2, . .. , n}. Κατόπιν υπολογίζει το π(Gi') = Η και το αποστέλλει στον verifier V'. Ο V', ανεξαρτήτως στρατηγικής θα απαντήσει με τυχαίο j' Ε {1, 2}. Αν i' = j', τότε ο S* στέλνει τη μετάθεση π στο V' και δέχεται την απόφασή του . Αλλιώς, i' #- j' και ο S* ξαναρχίζει από την αρχή. Η κρίσιμη ιδιότητα εδώ είναι πως το πρώτο μήνυμα του προσομοιωτή έχει ακριβώς την ίδια κατανομή με το πρώτο μ~Ινυμα του prover, το οποίο είναι τυχόν ένα ισομορφικό αντίγραφο του G1 ή του G2 . Προφανώς , το γράφημα Η που αποστέλλεται δεν αποκαλύπτει τίποτα για την επιλογή του j' και άρα η πιθανότητα του γεγονότος i' = j' είναι ακριβώς ~. Αυτό σημαίνει, πως ο verifier V' βλέπει μηνύματα Η και π τα οποία έχουν ακριβώς την ίδια κατανομή με αυτά που παρατηρεί σε μια πραγματική επικοινωνία με τον prover στο πλαίσιο του zero-knowledge protocol. Άρα « βλέπει» πράγματα τα οποία θα μπορούσε να έχει υπολογίσει και μόνος του.

Το παραπάνω πρωτόκολλο είναι ένα παράδειγμα πρωτοκόλλου PZK (τέλειας μηδενικής γνώσης). Η παραπάνω απόδειξη όμως δεν είναι πλήρης, αφενός διότι δεν περιλαμβάνει τις λεπτομέρειες του επιχειρήματος περί (απολύτως) ίδιας κατανομής των μηνυμάτων που παράγει ο προσομοιωτής με αυτά που παράγονται από το πρωτόκολλο και αφετέρου διότι δεν αντιμετωπίζει το ενδεχόμενο ενός «ανέντιμου » επαληθευτή (dishonest varifier).

5.5 Πρωτόκολλο αυθεντικοποίησης Fiat – Shamir

Το πρωτόκολλο αυθεντικοποίησης ταυτότητας των Fiat και Shamir είναι ένα πρωτόκολλο μηδενικής γνώσης που βασίζεται στο δύσκολο πρόβλημα υπολογισμού της τετραγωνικής ρίζας, modulo n, για μεγάλο n με άγνωστους πρώτους παράγοντες. Το πρωτόκολλο περιλαμβάνει έμπιστη οντότητα η οποία υπολογίζει και ανακοινώνει το n και καταχωρεί τα δημόσια κλειδιά των μελών. Αρχικά, η έμπιστη οντότητα επιλέγει δύο μεγάλους πρώτους αριθμούς p, q και ανακοινώνει το n = p * q.
Η Αλίκη εγγράφεται στο σύστημα επιλέγοντας έναν μυστικό αριθμό s τέτοιον ώστε $0 < s < n - 1$. Στη συνέχεια υπολογίζει το τετράγωνο της μυστικής ποσότητας:

$V \equiv s^2 \pmod n$

το οποίο αντιπροσωπεύει το δημόσιο κλειδί της. Τέλος, στέλνει το δημόσιο κλειδί v στην έμπιστη οντότητα.
Κατά τη διαδικασία αυθεντικοποίησης στον Βύρωνα, εκτελούνται t κύκλοι του πρωτοκόλλου. Ο κάθε κύκλος του πρωτοκόλλου αποτελείται από τα ακόλουθα βήματα:

1. Η Αλίκη δεσμεύεται με έναν τυχαίο αριθμό r, όπου $0 < r < n$ και στη συνέχεια υπολογίζει το τετράγωνο αυτού, το οποίο και στέλνει στον Βύρωνα:
   Αλίκη → Βύρων: $x \equiv r^2 \pmod n$

2. Ο Βύρων επιλέγει τυχαία πρόκληση $b \in \{0, 1\}$, δηλαδή b = 1 ή b = 0 και τη στέλνει στην Αλίκη:
   Βύρων → Αλίκη: b

3. Η Αλίκη υπολογίζει την απόκριση y και τη στέλνει στον Βύρωνα:

Αλίκη → Βύρων: y

όπου:

$$y = \begin{cases} r & \text{αν } b = 0 \\ rs \bmod n & \text{αν } b = 1 \end{cases}$$

4. Ο Βύρων ελέγχει αν ισχύει:

   $y^2 \equiv x v^b \pmod n$

   Στην ειδική περίπτωση όπου y = 0, το πρωτόκολλο ακυρώνεται.

5.6 Ανάλυση του πρωτοκόλλου των Fiat – Shamir

Αρχικά παρατηρούμε ότι σε έναν κύκλο του πρωτοκόλλου η Αλίκη θα πρέπει να γνωρίζει και τις δύο προκλήσεις, για b = 0 και για b = 1. Για b = 0, η λύση είναι εύκολη για οποιονδήποτε που επιλέγει τυχαία r, επομένως εύλογα αναρωτιόμαστε ποιο είναι το κέρδος σε μια τέτοια δοκιμή. Η απάντηση είναι ότι στην περίπτωση όπου η Αλίκη καλείται να απαντήσει μόνο στην πρόκληση για b = 1, ο αντίπαλος μπορεί να προσποιηθεί την ταυτότητα της Αλίκης επιλέγοντας τυχαίο r και στέλνοντας την ποσότητα

X ≡ $r^2 v v^{-1} \equiv r^2$

Αντί του τετραγώνου του r. Έτσι θα ισχύει:

$y^2 \equiv r^2 v v^{-1} \equiv r^2 \pmod n$

Επειδή όμως ο Βύρων έχει την επιλογή να ζητήσει απόδειξη ότι η Αλίκη γνωρίζει την τετραγωνική ρίζα του x, ο αντίπαλος θα πρέπει να λύσει το δύσκολο πρόβλημα υπολογισμού της τετραγωνικής ρίζας του $r^2 v^{-1}$ mod n.

Το πρωτόκολλο μπορεί να επαναληφθεί περισσότερες από μία φορές. Μάλιστα είναι επιθυμητό να επαναληφθεί περισσότερες από μία φορές, διότι λόγω των παραπάνω, ο αντίπαλος έχει πιθανότητα 0.5 να επιτύχει πλαστοπροσωπία, με μία και μόνο εκτέλεση του πρωτοκόλλου. Αν το πρωτόκολλο επαναληφθεί t φορές, τότε η πιθανότητα επιτυχίας του αντιπάλου θα είναι ίση με 2^{-t}. Είναι ευνόητο πως αν υπάρξει έστω και μια εσφαλμένη απάντηση, ο Βύρων τερματίζει το πρωτόκολλο και απορρίπτει την απόπειρα απόδειξης.

Το πρωτόκολλο των Fiat και Shamir κατατάσσεται στην κατηγορία των πρωτοκόλλων μηδενικής γνώσης. Αυτό σημαίνει ότι μπορούμε να κατασκευάσουμε αλγόριθμο ο οποίος παράγει τα μηνύματα του πρωτοκόλλου χωρίς τη γνώση του μυστικού s και χωρίς να έχουμε τη δυνατότητα να διακρίνουμε ότι τα μηνύματα παράχθηκαν από τον αλγόριθμο και όχι από την εκτέλεση του πρωτοκόλλου μεταξύ της Αλίκης και του Βύρωνα. Όντως, ο παρακάτω αλγόριθμος έχει τη δυνατότητα παραγωγής των μηνυμάτων του πρωτοκόλλου, χωρίς τη γνώση του s:

1. Επιλογή τυχαίου y, τέτοιου ώστε $0 < y < n$.
2. Επιλογή τυχαίας πρόκλησης $b \in \{0, 1\}$.
3. – Αν $b = 0$ τότε:

   $x \leftarrow y^2 \bmod n$

   -Αν $b = 1$ τότε:

   $x \leftarrow y^2 v^{-1} \bmod n$

Ο παραπάνω αλγόριθμος παράγει τριάδες (x, b, y) οι οποίες ικανοποιούν τους ελέγχους του πρωτοκόλλου των Fiat και Shamir.

5.7 Ασφάλεια του πρωτοκόλλου Fiat – Shamir

Η ασφάλεια του πρωτοκόλλου αυθεντικοποίησης Fiat και Shamir έγκειται στα εξής:

- Δυσκολία στην παραγοντοποίηση:
  - Ένας αλγόριθμος που «σπάει» τον Fiat – Shamir είναι ισοδύναμος με έναν αλγόριθμο που παραγοντοποιεί τον **N**
- Τυχαιότητα:
  - Του r (όσον αφορά τη μηδενική γνώση)
  - Της ερώτησης (αυτό εμποδίζει τον αποδείκτη να εξαπατήσει)

5.8 Πρωτόκολλο αναγνώρισης Feige – Fiat – Shamir

Μία παραλλαγή του Fiat – Shamir πρωτοκόλλου, αποτελεί το Feige-Fiat-Shamir όπου εμπλέκει μια οντότητα αυτό-αναγνώρισης αποδεικνύοντας τη γνώση ενός μυστικού χρησιμοποιώντας μια απόδειξη μηδενικής γνώσης.

Πρωτόκολλο: Η Αλίκη αποδεικνύει την ταυτότητα της στον Βύρωνα σε t εκτελέσεις.

1. Επιλογή παραμέτρων συστήματος
   I. Επιλέγεται και δημοσιοποιείται ένας σύνθετος ακέραιος n=pq, αλλά κρατούνται μυστικοί οι πρώτοι παράγοντες p και q. Ακέραιοι k, t ορίζονται ως παράμετροι ασφάλειας.
2. Επιλογή μυστικών ανά οντότητα.
   i. Επιλέγονται k τυχαίοι ακέραιοι $s_1, s_2, ...s_k$ με 1≤s≤n-1 και τυχαία bits $b_1, b_2, ..., b_k$

      Απαιτείται για τεχνικούς λόγους gcd(s_j n)=1
   ii. Υπολογισμός του $U_i = (-1)^{b_i} \bullet (s_i^2)^{-1} \bmod n$ για 1≤s_j≤n-1. Αυτό χρησιμεύει για να αποδείξει ότι δεν υπάρχει διαρροή μυστικής πληροφορίας, αφού με την επιλογή του n, ακριβώς ένα έχει τετραγωνική ρίζα.
   iii. Η Αλίκη ταυτοποιεί τον εαυτό της με μη κρυπτογραφικούς τρόπους και στη συνέχεια δηλώνεται το δημόσιο κλειδί ($\nu_1, ...\nu_\kappa, n$) της Αλίκης, ενώ τα μυστικά της κλειδιά ($s_1, ...s_k$) τα γνωρίζει μόνο εκείνη.
3. Μηνύματα πρωτοκόλλου

   Κάθε ένας από τους t γύρους έχει τρία μηνύματα με την εξής μορφή:

   i. $A \to B : x(= \pm r^2 \bmod n)$ (1)

   $A \leftarrow B : (e_1, ..., e_k), e_i \in \{0,1\}$ (2)

   $A \to B : y(= r \bullet \Pi_{ej} = 1^{s_j} \bmod n)$ (3)
4. Ενέργειες πρωτοκόλλου

   Τα επόμενα βήματα εκτελούνται t φορές. Ο Βύρων αποδέχεται την ταυτότητα της Αλίκης εάν όλοι οι γύροι επιτύχουν.

   i. Η Αλίκη επιλέγει τυχαία έναν ακέραιο r με 1 ≤ r ≤ n-1 και έναν τυχαίο bit b. Υπολογίζει το x = $(-1)^b r^2$ mod n και αποστέλλει το x στον Βύρωνα.

ii. Ο Βύρωνας στέλνει στην Αλίκη ένα άνυσμα k-bit (e1,……,ek)(πρόκληση)

iii. Η Αλίκη υπολογίζει και στέλνει στον Βύρωνα την απάντηση:

$$y = r \bullet \Pi_j^k = 1^{s_j^{e_j}} \bmod n$$

iv. Ο Βύρωνας υπολογίζει το $z = y^2 \bullet \Pi_j^k = 1^{u_j^{e_j}} \bmod n$ και εξακριβώνει ότι z= ±x και $z \neq 0$

5.9 Ασφάλεια του Feige – Fiat – Shamir

1. Η ασφάλειά του στηρίζεται στη δυσκολία εύρεσης τετραγωνικής ρίζας modulo μεγάλων σύνθετων ακεραίων.
2. Η πιθανότητα επιτυχούς πλαστογραφίας είναι μικρή, και αν σκεφτούμε τη δυσκολία του προβλήματος της εύρεσης είναι στην καλύτερη περίπτωση 2^{-kt}
3. Είναι αρκετά ασφαλές σε επιθέσεις προεπιλεγμένων μηνυμάτων
4. Η επιλογή των παραμέτρων k και t, έτσι ώστε το γινόμενο kt να ισούται με το 20, ελαχιστοποιεί την πιθανότητα πλαστοπροσωπίας σε μία στο εκατομμύριο.
5. Είναι πιθανόν επίσης να μειωθεί η πολυπλοκότητα της επικοινωνίας της Αλίκης και του Βύρωνα, εάν η Αλίκη αποστείλει στον Βύρωνα μια hash τιμή H(x) αντί για ένα μήνυμα x. Αυτό βέβαια απαιτεί και την αντίστοιχη τροποποίηση στην διαδικασία εξακρίβωσης του Βύρωνα.

5.10 Πρωτόκολλο αυθεντικοποίησης Guillou – Quisquater

Το πρωτόκολλο αυθεντικοποίησης μηδενικής γνώσης των Guillou και Quisquater (GQ) είναι επέκταση του πρωτοκόλλου των Fiat και Shamir που αναλύσαμε στο προηγούμενο κεφάλαιο. Η ασφάλεια του πρωτοκόλλου GQ βασίζεται στη δυσκολία εύρεσης των πρώτων παραγόντων ενός σύνθετου αριθμού. Η βασική διαφορά των δύο πρωτοκόλλων είναι ότι στο πρωτόκολλο GQ ο χώρος της πρόκλησης αποτελείται από περισσότερα από 1 bits, με αποτέλεσμα να απαιτούνται λιγότερες επαναλήψεις του πρωτοκόλλου προκειμένου να επιτευχθεί μικρή πιθανότητα πλαστοπροσωπίας.
Το πρωτόκολλο περιλαμβάνει έμπιστη οντότητα η οποία καθορίζει τις δημόσιες παραμέτρους και απονέμει ταυτότητες στα μέλη. Οι δημόσιες παράμετροι προκύπτουν με βάση το κρυπτοσύστημα RSA. Η έμπιστη οντότητα επιλέγει δύο μεγάλους πρώτους αριθμούς p και q οι οποίοι καθορίζουν το δημόσιο modulus n = pq. Στη συνέχεια, επιλέγει ένα δημόσιο εκθέτη e > 2 με gcd (e, φ(ν)) = 1 και υπολογίζει τον ιδιωτικό εκθέτη s = e^{-1} mod φ (n). Οι δημόσιες παράμετροι είναι οι (e, n)

Το επόμενο στάδιο είναι η διαδικασία εγγραφής του μέλους. Έστω ότι η Αλίκη επιθυμεί να εγγραφεί στο σύστημα αυθεντικοποίησης. Η έμπιστη οντότητα επιλέγει την ταυτότητα της Αλίκης, η οποία είναι ένας ακέραιος ID_A, έτσι ώστε $1 < ID_A < n$. Στη συνέχεια, η έμπιστη οντότητα υπολογίζει το μυστικό απόδειξης της Αλίκης:

$$S_A = (ID_A)^{-5} \bmod n$$

την οποία και παραδίδει εμπιστευτικά στην Αλίκη. Τέλος, η έμπιστη οντότητα δημοσιεύει την ταυτότητα της Αλίκης μαζί με τα στοιχεία της σε κάποιο δημόσιο ευρετήριο.
Κατά τη διαδικασία αυθεντικοποίησης στον Βύρωνα, εκτελούνται t κύκλοι του πρωτοκόλλου αυθεντικοποίησης. Ο κάθε κύκλος του πρωτοκόλλου αποτελείται από τα ακόλουθα βήματα:

1. Η Αλίκη δεσμεύεται με έναν τυχαίο αριθμό r, όπου 0 < r < n. Στη συνέχεια υψώνει τον αριθμό αυτό στο δημόσιο εκθέτη, και στέλνει το αποτέλεσμα στον Βύρωνα:

   Αλίκη → Βύρων: $x \equiv r^e \pmod n$

2. Η Αλίκη δεσμεύεται με έναν τυχαίο αριθμό r, όπου 0 < r < n. Στη συνέχεια υψώνει τον αριθμό αυτό στο δημόσιο εκθέτη, και στέλνει το αποτέλεσμα στον Βύρωνα:

Αλίκη → Βύρων: b

3. Η Αλίκη υπολογίζει την απόκριση y και τη στέλνει στον Βύρωνα
   Αλίκη → Βύρων: $y \equiv r s_A^{\,e} \pmod n$

4. Ο Βύρων προμηθεύεται την ταυτότητα της Αλίκης από το ευρετήριο και ελέγχει αν ισχύει:
   $X \equiv (ID_A)^b y^e \pmod n$

   απορρίπτοντας την περίπτωση όπου $x \equiv 0 \pmod n$.

   Η ανάλυση του πρωτοκόλλου GQ είναι παρόμοια με την ανάλυση του πρωτοκόλλου των Fiat και Shamir. Η πιθανότητα επιτυχούς πλαστοπροσωπίας από τον αντίπαλο για t γύρους είναι ίση με $(1/e)^{-t}$.

5.11 Πρωτόκολλο αυθεντικοποίησης του Schnorr

Το πρωτόκολλο των Fiat και Shamir καθώς και το πρωτόκολλο των Guillou και Quisquater που αναλύσαμε βασίζονται στο πρόβλημα της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων. Η ασφάλεια του πρωτοκόλλου του Schnorr που θα παρουσιάσουμε στη συνέχεια βασίζεται στο πρόβλημα του διακριτού λογάριθμου. Σε αντίθεση με τα πρωτόκολλα μηδενικής γνώσης που παρουσιάσαμε, το πρωτόκολλο του Schnorr δεν απαιτεί επαναληπτική εκτέλεση του πρωτοκόλλου προκειμένου να μειωθεί η πιθανότητα πλαστοπροσωπίας. Η πιθανότητα καθορίζεται από την επιλογή μίας εκ των παραμέτρων, όπως θα δούμε παρακάτω.

Το πρωτόκολλο αυθεντικοποίησης απαιτεί τη συμμετοχή τρίτης έμπιστης οντότητας, προκειμένου να καθοριστούν οι δημόσιες παράμετροι. Επιπλέον, η έμπιστη οντότητα λειτουργεί και ως Αρχή Πιστοποίησης, εκδίδοντας ψηφιακά πιστοποιητικά στα μέλη της.

Αρχικά, η έμπιστη οντότητα επιλέγει δύο πρώτους αριθμούς p και q τέτοιους ώστε ο q να είναι παράγοντας του (p–1). Στη συνέχεια, επιλέγει u τέτοιο ώστε η πολλαπλασιαστική τάξη να είναι q και $0 < u < p$.

Η παραμετροποίηση του επιπέδου της ασφάλειας γίνεται με τον q. Αν θέσουμε

$t = [\log_2(q)]$

τότε θα ισχύει και $2 \wedge t \leq q$. Η παράμετρος t καθορίζει το επίπεδο ασφαλείας. Έτσι θα μπορούμε να εργαστούμε αντίστροφα, δηλαδή να ορίσουμε το t και στη συνέχεια να επιλέξουμε q τέτοιο ώστε $2 \wedge t \leq q$.

Οι δημόσιοι παράμετροι είναι η τριάδα (p, q, u) καθώς και το δημόσιο κλειδί της οντότητας το οποίο χρησιμοποιείται για την επαλήθευση των πιστοποιητικών των μελών. Κατά την εγγραφή ενός μέλους, η έμπιστη οντότητα την ταυτότητα ID_A ενώ το μέλος (για παράδειγμα η Αλίκη) επιλέγει έναν ακέραιο α τέτοιον ώστε $0 < a < q$. Στη συνέχεια η Αλίκη υπολογίζει το: $v = u^{-a} \bmod p$

το οποίο στέλνει στην έμπιστη οντότητα. Τέλος, η έμπιστη οντότητα εκδίδει πιστοποιητικό για την Αλίκη το οποίο αποτελείται από τα στοιχεία ID_A και v, καθώς και την ψηφιακή υπογραφή της έμπιστης οντότητας στα στοιχεία αυτά. Έστω $cert_A$ το πιστοποιητικό που προκύπτει.

Κατά την εκτέλεση του πρωτοκόλλου αυθεντικοποίησης, η Αλίκη αποδεικνύει την ταυτότητά της στον Βύρων με τα ακόλουθα βήματα:

1. Η Αλίκη επιλέγει τυχαίο ακέραιο r με $0 < r < q$ τον οποίο χρησιμοποιεί ως εκθέτη στη δημόσια παράμετρο u και στέλνει το αποτέλεσμα στον Βύρωνα μαζί με το πιστοποιητικό της:

Αλίκη → Βύρων: $cert_A$, $x \equiv u^r \pmod p$

2. Ο Βύρων επιλέγει πρόκληση b, με $1 \leq b \leq 2^t$, την οποία στέλνει στην Αλίκη:

Βύρων → Αλίκη: b.

3. Η Αλίκη υπολογίζει την απόκριση y την οποία στέλνει στον Βύρωνα:

Αλίκη → Βύρων: $y \equiv a * b + r \pmod q$

4. Ο Βύρων δέχεται την ταυτότητα της Αλίκης ελέγχοντας αν ισχύει η σχέση:

$x \equiv u^y \ v^b \pmod p$

Είναι φανερό ότι η επιτυχής εκτέλεση του πρωτοκόλλου απαιτεί τη γνώση του μυστικού απόδειξης a από το μέλος του οποίου αυθεντικοποιείται η ταυτότητα. Ο συνυπολογισμός της δέσμευσης r στα μηνύματα x και y έχει ως αποτέλεσμα την απόκρυψη του μυστικού απόδειξης, εφόσον ο r είναι τυχαίος και δεν είναι γνωστό σε κανέναν παρά μόνο στην Αλίκη. Επομένως, τα μηνύματα του πρωτοκόλλου δεν αποκαλύπτουν καμία μυστική παράμετρο.
Ωστόσο, για μεγάλη τιμή της πρόκλησης b, ο Βύρων στο τέλος του πρωτοκόλλου έχει τη λύση (x, y, b) της εξίσωσης:

$x \equiv u^y \ v^b \pmod{p}$

που σημαίνει ότι μπορεί να αποδείξει ότι γνωρίζει τη λύση (την οποία δεν μπορούσε να υπολογίσει πριν ολοκληρωθεί το πρωτόκολλο),οπότε και το πρωτόκολλο χάνει την ιδιότητα της μηδενικής γνώσης.

Από πλευράς ασφάλειας, η πιθανότητα επιτυχίας του αντιπάλου είναι της τάξης του 2^{-t}. Αυτό αναλύεται με τον ακόλουθο αλγόριθμο επίθεσης του αντιπάλου (ο οποίος συμπίπτει και με την απόδειξη της ιδιότητας της μηδενικής γνώσης) :

1. Ο αντίπαλος επιλέγει μια πρόκληση b. Η πιθανότητα να επιλέξει τη σωστή πρόκληση είναι 2^{-t}
2. Ο αντίπαλος επιλέγει τυχαία απόκριση y και υπολογίζει τη δέσμευση x όπως απαιτεί η προεπιλεγμένη απόκριση:

$x \equiv u^y \ v^b \pmod{p}$

3. Ο αντίπαλος έχει μια τριάδα (x, y, b) η οποία πληροί τις απαιτήσεις του πρωτοκόλλου αυθεντικοποίησης και μπορεί να εκτελέσει το πρωτόκολλο με τον Βύρωνα.

Ο αλγόριθμος του αντιπάλου ολοκληρώνεται σε πολυωνυμικό χρόνο, παράγοντας τα επιθυμητά μηνύματα του πρωτοκόλλου.

ΚΕΦΑΛΑΙΟ 6ο

6.1 Ηλεκτρονική ψηφοφορία και μηδενική γνώση

Οι τεχνολογίες του Διαδικτύου έχουν παρεισφρήσει σε κάθε τομέα της οικονομικής και εκπαιδευτικής ζωής, κυρίως στις προηγμένες χώρες. Ο όρος ηλεκτρονική δημοκρατία (e-democracy) αναφέρεται στην χρήση των τεχνολογιών του Διαδικτύου για την επικοινωνία των πολιτών με την κυβέρνηση και τους πολιτικούς, την εξυπηρέτηση του πολίτη από τις δημόσιες υπηρεσίες, και τη συμμετοχή του στις αποφάσεις (π.χ. δημοψηφίσματα, συλλογή υπογραφών, δημοσκοπήσεις). Στα σημερινά αντιπροσωπευτικά δημοκρατικά καθεστώτα όπου οι πολίτες ψηφίζουν τους εκπροσώπους τους στην κυβέρνηση, επικρατεί ανησυχία για τα αυξανόμενα ποσοστά αποχής από τις εθνικές εκλογές, καθώς και γενικότερα για τη διαφαινόμενη τάση αποστασιοποίησης από τα πολιτικά δρώμενα. Για να αντιστραφεί το κλίμα αυτό αναζητούνται αλλαγές στον τρόπο συμμετοχής των πολιτών στα κοινά.

Ένα από τα μέτρα υπό συζήτηση είναι και η απλοποίηση της διαδικασίας των εκλογών, με τα συστήματα ηλεκτρονικής ψηφοφορίας (e-voting). Η καθιέρωση της ηλεκτρονικής ψηφοφορίας, και μάλιστα της ψηφοφορίας μέσω του Διαδικτύου (Internet voting), αναμένεται να απλοποιήσει την διαδικασία υποβολής των ψήφων και να αυξήσει την εμπιστοσύνη των ψηφοφόρων στην ορθότητα των αποτελεσμάτων. Ωστόσο, οι επικριτές των συστημάτων ηλεκτρονικής ψηφοφορίας θεωρούν ότι οι υπάρχουσες τεχνολογίες δεν είναι ακόμα ώριμες να αντιμετωπίσουν τα προβλήματα ασφάλειας που προκύπτουν, να εξασφαλίσουν την ακρίβεια των αποτελεσμάτων και να επιλύσουν ζητήματα όπως αυτά του κοινωνικού αποκλεισμού των λεγόμενων «ψηφιακά αναλφάβητων» πολιτών και της αντιμετώπισης των «ευπαθών» κοινωνικών ομάδων .

Τα συστήματα ηλεκτρονικής ψηφοφορίας χρησιμοποιούν ψηφιακά δεδομένα για να αποτυπώσουν τις επιλογές του ψηφοφόρου. Στην ηλεκτρονική ψηφοφορία μέσω Διαδικτύου οι ψηφοφόροι έχουν την επιπλέον δυνατότητα χρησιμοποίησης του Διαδικτύου για την αποστολή των ψήφων τους στις Εκλογικές Αρχές. Έως σήμερα έχουν διεξαχθεί αρκετές εκλογές μέσω Διαδικτύου, αν και οι περισσότερες από αυτές

είχαν ανεπίσημο χαρακτήρα, ενώ αρκετά συστήματα σχεδιάζονται και εφαρμόζονται πιλοτικά με σκοπό τη μελλοντική τους υλοποίηση σε συστήματα μεγάλης κλίμακα. Σε γενικές γραμμές, κάθε ηλεκτρονική ψηφοφορία αποτελείται από τέσσερα (4) διακριτά στάδια:

- Εγγραφή. Πριν από τη διεξαγωγή των εκλογών, οι ψηφοφόροι αποδεικνύουν την αληθινή τους ταυτότητα και τη νομιμότητα του
- δικαιώματος τους να ψηφίσουν (π.χ. όριο ηλικίας). Όσοι πληρούν τις προϋποθέσεις εγγράφονται στον εκλογικό κατάλογο.
- Επικύρωση. Πριν την υποβολή της ψήφου ελέγχεται η ταυτότητα των ψηφοφόρων (ταυτοποίηση – identification).
- Υποβολή Ψήφου. Οι ψηφοφόροι υποβάλλουν την ψήφο τους. Μόνο μια ψήφος επιτρέπεται για κάθε ψηφοφόρο.
- Καταμέτρηση Ψήφων. Μόλις εκπνεύσει η προθεσμία υποβολής ψήφων, οι ψήφοι καταμετρούνται και ανακοινώνεται το αποτέλεσμα των εκλογών.

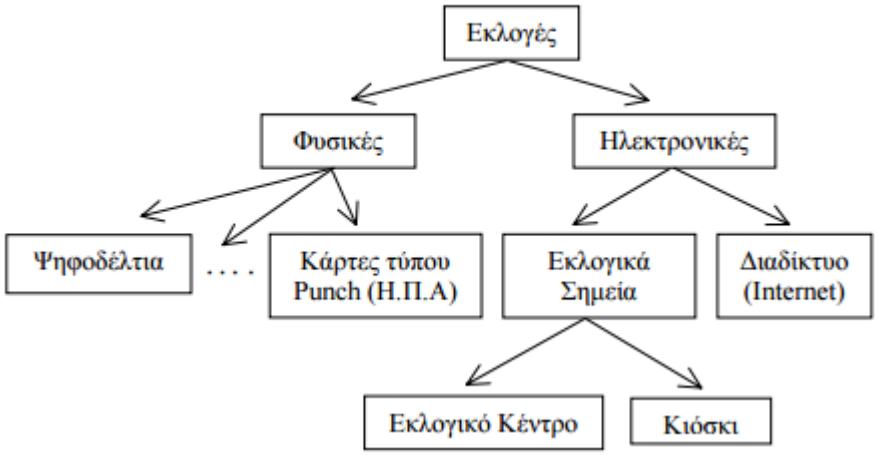
Κάθε ένα από τα παραπάνω στάδια μπορεί να εκτελεστεί με χρήση φυσικών ή ηλεκτρονικών διαδικασιών. Η έρευνα μας επικεντρώθηκε στη διεξαγωγή ηλεκτρονικής ψηφοφορίας και συγκεκριμένα σε εκείνους τους τύπους ηλεκτρονικής ψηφοφορίας που περιλαμβάνουν τουλάχιστον μια απομακρυσμένη (remote) επικοινωνία μέσω ενός ανοικτού δικτύου όπως το Διαδίκτυο. Διακρίνουμε δύο τύπους ηλεκτρονικής ψηφοφορίας:

Την Ηλεκτρονική Ψηφοφορία σε Εκλογικά Σημεία (Polling Place E-Voting) και την Ηλεκτρονική Ψηφοφορία μέσω Διαδικτύου (Internet Voting)

6.2 Ηλεκτρονική Ψηφοφορία σε Εκλογικά Σημεία.

Σε ένα εκλογικό σημείο, τόσο τα συστήματα-πελάτες (voting clients) που χρησιμοποιούν οι ψηφοφόροι για να υποβάλλουν ηλεκτρονικά την ψήφο τους, όσο και το φυσικό περιβάλλον στο οποίο διεξάγεται η ψηφοφορία, επιβλέπονται από εξουσιοδοτημένες οντότητες (π.χ. εκλογικοί υπάλληλοι, αντιπρόσωποι, αστυνομία). Ανάλογα με το είδος του εκλογικού σημείου, π.χ. Εκλογικό Κέντρο (Precinct) ή

Κιόσκι , το στάδιο της Επικύρωσης μπορεί να γίνει είτε με φυσικές διαδικασίες (έλεγχος απ' ευθείας από τους εκλογικούς υπευθύνους) είτε με ηλεκτρονικές (με κάποια ψηφιακή μέθοδο ταυτοποίησης). Τα στάδια της Υποβολής και της Καταμέτρησης ψήφου γίνονται εξ' ολοκλήρου με ηλεκτρονικές διαδικασίες: τα εκλογικά μηχανήματα (συστήματα-πελάτες) μπορεί να είναι Συσκευές Άμεσης Καταμέτρησης (Direct Recording Equipment) , που χρησιμοποιούνται ευρέως στις Η.Π.Α, ή επίσης ενδέχεται να στέλνουν την ηλεκτρονική κάλπη σε ένα κεντρικό εξυπηρετητή (server) μέσω μιας «ασφαλούς» σύνδεσης Διαδικτύου ή μέσω του δικτύου ATM.



Σχήμα 8: Ηλεκτρονική ψηφοφορία

6.3 Ψηφοφορία μέσω Διαδικτύου.

Η ψήφος υποβάλλεται μέσω Διαδικτύου και τα συστήματα-πελάτες βρίσκονται υπό χαλαρή ή μηδαμινή επίβλεψη (τα συστήματα-πελάτες μπορεί να βρίσκονται στο σπίτι, στον χώρο εργασίας, σε βιβλιοθήκες, σχολεία, πανεπιστήμια). Η Εγγραφή μπορεί να γίνει με φυσικές (π.χ. σε ένα εκλογικό γραφείο) ή με ηλεκτρονικές διαδικασίες (με κάποια ψηφιακή μέθοδο ταυτοποίησης). Τα στάδια της Επικύρωσης, της Υποβολής και της Καταμέτρησης γίνονται εξ' ολοκλήρου με ηλεκτρονικές διαδικασίες. Η ψηφοφορία μέσω Διαδικτύου απαιτεί ένα μεγαλύτερο επίπεδο ασφάλειας από αυτό που απαιτείται σε συνήθεις συναλλαγές ηλεκτρονικού εμπορίου. Ενώ η ταυτοποίηση των ψηφοφόρων και η εξασφάλιση της μοναδικότητας της ψήφου ανά ψηφοφόρο, μπορούν να αντιμετωπιστούν με τεχνικές που ήδη

χρησιμοποιούνται σε εφαρμογές ηλεκτρονικών συστημάτων πληρωμών (π.χ. ψηφιακές υπογραφές - ψηφιακά πιστοποιητικά), οι επιπλέον απαιτήσεις όπως η μυστικότητα (secrecy) και η ανωνυμία (anonymity) της ψήφου, η οικουμενική επαληθευσιμότητα (universal verifiability), καθώς και η προστασία από καταναγκασμό (uncoercibility), συνθέτουν ένα πολύπλοκο μοντέλο απαιτήσεων ασφάλειας το οποίο έως σήμερα δεν έχει αντιμετωπιστεί με μεθόδους που να είναι ασφαλείς και παράλληλα πρακτικές.

6.4 Απαιτήσεις Ασφάλειας και Πρακτικότητας

Για τη σχεδίαση ενός συστήματος ηλεκτρονικής ψηφοφορίας που πρόκειται να χρησιμοποιηθεί σε εκλογές μεγάλης κλίμακας, είναι σημαντικό να καθορίσουμε τις απαιτήσεις ασφάλειας και πρακτικότητας.

Οι απαιτήσεις αυτές πρέπει να είναι κοινώς αποδεκτές και τεχνολογικά ουδέτερες .

Ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει λοιπόν να είναι:

α) Ασφαλές, δηλαδή:

- Δημοκρατικό (Democratic).

  - Μόνο εξουσιοδοτημένοι ψηφοφόροι δικαιούνται να υποβάλλουν ψήφους.
  - Κανένας ψηφοφόρος δε δικαιούται να υποβάλλει περισσότερες από μια ψήφους.

- Ακριβές (Accurate). Καμία ψήφος δεν είναι δυνατόν ο να αλλοιωθεί, ο να καταμετρηθεί περισσότερες από μια φορές, ο να διαγραφεί από τις Εκλογικές Αρχές ή άλλους εσωτερικούς/εξωτερικούς εχθρούς.

- Μυστικό (Secret). ο Όλες οι ψήφοι παραμένουν μυστικές για όσο διάστημα διαρκεί η περίοδος υποβολής ψήφων. ο Καμία ψήφος δεν είναι δυνατόν να συνδεθεί με τον ψηφοφόρο που την υπέβαλλε.

- Προστατευμένο από Καταναγκασμό (Uncoercible). Κανένας χρήστης δεν έχει τη δυνατότητα να αποδείξει τη ψήφο του σε κάποιον τρίτο.

- Οικουμενικά Επαληθεύσιμο (Universally Verifiable). Κάθε εξωτερικός παρατηρητής μπορεί να πειστεί6 ότι το σύστημα είναι ακριβές και ότι το αποτέλεσμα του υπολογισμού των ψήφων της κάλπης αντανακλά τη βούληση των ψηφοφόρων που τις υπέβαλλαν.

- Ανθεκτικό (Robust). Όλες οι απαιτήσεις ασφάλειας ικανοποιούνται πλήρως, παρά τα όποια τυχαία σφάλματα ή τις κακόβουλες συμπεριφορές κάποιων οντοτήτων (ψηφοφόροι, Αρχές, εσωτερικοί/εξωτερικοί εχθροί).

β) Πρακτικό,

δηλαδή:

- Εύκολα υλοποιήσιμο, συμβατό με τις διάφορες τεχνολογίες και πλατφόρμες (λειτουργικά συστήματα, αρχιτεκτονικές, εργαλεία πλοήγησης στο Web κ.λ.π).

- Λειτουργικό για όλους τους ψηφοφόρους και ιδιαίτερα για τους ψηφοφόρους με ειδικές ανάγκες.

- Να υποστηρίζει μια ποικιλία από μορφοποιήσεις (format) ψήφων.

- Η αποδοτικότητα του να μην επηρεάζεται δραστικά από το μέγεθος του εκλογικού σώματος (scalability).

- Να υπόκειται σε ελέγχους αξιοπιστίας ώστε να εμπνέει εμπιστοσύνη.

6.5 ΠλεονεκτήΜατα ΣυστηΜάτων Ηλεκτρονικής Ψηφοφορίας

α) Ηλεκτρονική Ψηφοφορία (Γενικά).

Ορισμένα από τα πλεονεκτήματα των συστημάτων ηλεκτρονικής ψηφοφορίας προκύπτουν με βάση τη σύγκριση τους με παραδοσιακά εκλογικά συστήματα, τα οποία και ενέχουν σημαντικά προβλήματα αξιοπιστίας. Για παράδειγμα στις εκλογές του 2000 στις Η.Π.Α παρουσιάστηκε ένας αρκετά μεγάλος αριθμός προβληματικών ψήφων (residual votes), όπως αποκαλούνται οι ψήφοι με λιγότερες επιλογές υποψηφίων από τις προβλεπόμενες (under votes), οι αλλοιωμένες ψήφοι (spoiled votes), οιψήφοι που δε λήφθηκαν υπ’ όψιν κατά την καταμέτρηση (uncounted votes) κ.λ.π. Τα συστήματα ηλεκτρονικής ψηφοφορίας αναμένεται να μειώσουν σημαντικά

τα ποσοστά λάθους στην υποβολή και καταμέτρηση των ψήφων . Επίσης υπόσχονται μεγαλύτερη προσβασιμότητα σε ευπαθείς ομάδες ψηφοφόρων. Επιπλέον, η καταμέτρηση των ψήφων και η δημοσίευση των αποτελεσμάτων θα γίνονται εύκολα, γρήγορα, με μικρότερη πιθανότητα λάθους, αλλά και μικρότερο (μακροπρόθεσμα) οικονομικό κόστος, σε σχέση π.χ. με το κόστος εκτύπωσης ψηφοδελτίων στις παραδοσιακές εκλογές.

β) Ψηφοφορία μέσω Διαδικτύου.

Το μεγάλο ποσοστό διείσδυσης του Διαδικτύου, ιδιαίτερα στις ανεπτυγμένες χώρες, καθιστά επωφελή τη μετάβαση στα συστήματα ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου. Με τα συστήματα αυτά η διαδικασία υποβολής της ψήφου θα είναι φιλική προς τον χρήστη, με αποτέλεσμα να ευνοηθεί η αύξηση του ποσοστού συμμετοχής των πολιτών στις εκλογές. Ένας μεγάλος αριθμός υπολογιστών που είναι σήμερα διαθέσιμοι σε εύκολα προσβάσιμους χώρους (π.χ. βιβλιοθήκες, σχολεία, πανεπιστήμια) μπορούν να γίνονται διαθέσιμοι στο εκλογικό σώμα την ημέρα των εκλογών. Επίσης, η ψηφοφορία μέσω Διαδικτύου θα μπορούσε να διαδραματίσει σημαντικό ρόλο σε εκλογές μικρής κλίμακας, π.χ. φοιτητικές εκλογές, ανάδειξη αντιπροσώπων ή/και λήψη αποφάσεων σε συλλόγους, κοινότητες, οργανισμούς κ.λ.π.

6.8 Μειονεκτήματα Συστημάτων Ηλεκτρονικής Ψηφοφορίας

Οι απειλές ασφάλειας που ελλοχεύουν στα συστήματα ηλεκτρονικής ψηφοφορίας είναι ιδιαίτερα σημαντικές :

α) Ηλεκτρονική Ψηφοφορία (Γενικά). Είναι γνωστό ότι τα ηλεκτρονικά δεδομένα αντιγράφονται, αλλοιώνονται και καταστρέφονται πολύ πιο εύκολα από ότι οι φυσικές ψήφοι. Επιπλέον, όλα τα ηλεκτρονικά συστήματα είναι ευάλωτα σε επιθέσεις από εσωτερικούς εχθρούς (insider attacks) καθώς και σε επιθέσεις Άρνησης Εξυπηρέτησης (Denial Of Service – DOS) που έχουν ως στόχο τους υπολογιστικούς πόρους ενός ηλεκτρονικού υπολογιστή (σύστημα-πελάτης ή σύστημα-εξυπηρετητής). Τα σημερινά ηλεκτρονικά συστήματα ψηφοφορίας διαθέτουν ανεπαρκή στοιχεία ελέγχου (audit trail) και δεν παρέχουν οικουμενική επαληθευσιμότητα, με συνέπεια τα αποτελέσματα της ψηφοφορίας να τίθενται υπό αμφισβήτηση. Επιπλέον, παρότι

σήμερα υπάρχουν ασφαλείς κρυπτογραφικοί αλγόριθμοι, δεν υπάρχουν επαρκώς ασφαλή συστήματα (π.χ. πλατφόρμες, λειτουργικά συστήματα) στα οποία να μπορούμε να ενσωματώσουμε την κρυπτογραφία .

β) Ψηφοφορία μέσω Διαδικτύου. Τα συστήματα ψηφοφορίας αυτού του τύπου θα γίνουν ευρέως αποδεκτά μόνον όταν σχεδόν όλοι οι ψηφοφόροι θα μπορούν να έχουν εύκολη και γρήγορη πρόσβαση στο Διαδίκτυο, κάτι που δεν ισχύει σήμερα. Επίσης, η μετάβαση σε εκλογές μέσω Διαδικτύου πιθανόν να συνεπάγεται υψηλό κόστος αγοράς και συντήρησης υπολογιστικών μηχανών, λογισμικού βάσεων δεδομένων και συστημάτων δρομολόγησης . Από τη σκοπιά της ασφάλειας, οι εκλογές μέσω Διαδικτύου είναι περισσότερο ευάλωτες σε επιθέσεις καταναγκασμούόπου οι χρήστες αναγκάζονται ή συναλλάσσονται με κάποιον τρίτο για την υποβολή μιας προσυμφωνημένης ψήφου. Επιπρόσθετα, οι χρήστες πρέπει να δημιουργούν οι ίδιοι ένα ασφαλές περιβάλλον στις υπολογιστικές τους μηχανές (συστήματα πελάτες), προτού υποβάλλουν τη ψήφο τους. Οι έλεγχοι και η πιστοποίηση λογισμικού στα συστήματα ψηφοφορίας μέσω Διαδικτύου παρουσιάζουν επίσης ιδιαίτερες δυσκολίες, καθώς τα συστατικά μέρη των συστημάτων αυτών είναι συνήθως διαφορετικής προέλευσης και έχουν μυστικό (κλειστό) κώδικα, όπως για παράδειγμα τα σύγχρονα λειτουργικά συστήματα Windows και τα προγράμματα πλοήγησης στο Web . Παράλληλα, τα συστήματα ψηφοφορίας μέσω Διαδικτύου είναι περισσότερο ευάλωτα, σε σχέση με τις υπόλοιπες κατηγορίες ηλεκτρονικής ψηφοφορίας, στα εξής σημεία: - Στα συστήματα-πελάτες (clients): Ιοί τύπου «σκουλήκια» (worms) ή «δούρειοι ίπποι» (trojan horses) μπορούν να αλλοιώσουν τη ψήφο, πολύ πριν αυτή κρυπτογραφηθεί ή αυθεντικοποιηθεί. Επίσης, ο επιτιθέμενος μπορεί εξ' αποστάσεως να εκμεταλλευτεί «τρύπες» ή λάθη στο σχεδιασμό του λειτουργικού συστήματος ή του προγράμματος πλοήγησης στο Web. - Στο επίπεδο της επικοινωνίας: Οι κυριότερες επιθέσεις στο επίπεδο της επικοινωνίας είναι οι επιθέσεις πλαστοπροσωπίας (spoofing) ονομάτων DNS ή διευθύνσεων IP, καθώς και οι επιθέσεις ενδιάμεσης οντότητας (man in the middle attacks) . Κατά τη διάρκεια μιας τέτοιας επίθεσης, για παράδειγμα, ο επιτιθέμενος στέλνει στο σύστημα-πελάτης μια φαινομενικά έγκυρη σελίδα Web. Ο χρήστης νομίζει ότι ο δικτυακός τόπος που εμφανίζεται στο πρόγραμμα πλοήγησης είναι ο επίσημος δικτυακός τόπος για την υποβολή της ψήφου. Αυτό μπορεί να είναι αρκετό για να μη ληφθεί καθόλου υπ' όψιν η ψήφος του χρήστη. Αργότερα ο επιτιθέμενος μπορεί να χρησιμοποιήσει τα

ψηφιακά πιστοποιητικά που θα του έχει ήδη υποβάλλει ο ανυποψίαστος χρήστης, ώστε να ταυτοποιηθεί στον server του συστήματος και να υποβάλλει μια «πλαστή» ψήφο εκ μέρους του χρήστη. Η επικοινωνία μεταξύ client και server μπορεί επίσης να απειληθεί και από επιθέσεις τύπου TCP SYN/ACK στο επίπεδο δικτύου του μοντέλου TCP/IP, από επιθέσεις πλαστοπροσωπίας στο φυσικό επίπεδο του μοντέλου OSI (ARP spoofing) κ.λ.π.

- Στα συστήματα-εξυπηρετητές (servers): Οι επιθέσεις σε αυτό το επίπεδο είναι παρόμοιες με αυτές στα συστήματα-πελάτες. Εδώ βέβαια οι επιθέσεις Άρνησης Εξυπηρέτησης (DOS), όπως IP fragmentation ή υπερχείλιση καταχωρητών (buffer overflow), έχουν μεγάλη επικινδυνότητα, αφού μπορούν να υπονομεύσουν ολόκληρη την εκλογική διαδικασία. Το πρόβλημα της συμφόρησης (bottleneck) είναι παρόμοιο, ως προς τις συνέπειες που έχει, με μια επίθεση Άρνησης Εξυπηρέτησης, με τη διαφορά ότι η συμφόρηση προκαλείται από υπερβολικά μεγάλο αριθμό ταυτόχρονων νομίμων αιτήσεων για σύνδεση με τον server, και όχι απαραίτητα από κακόβουλη επίθεση .

6.9 Βασικά Κρυπτογραφικά Εργαλεία

Τα βασικά εργαλεία που χρησιμοποιούνται από τα περισσότερα κρυπτογραφικά πρωτόκολλα ηλεκτρονικής ψηφοφορίας είναι τα έξης:

6.9.1 Πίνακες Ανακοινώσεων (Bulletin Boards).

Πρόκειται για κανάλια δημόσιας εκπομπής (public broadcast channels) που επιτρέπουν στους χρήστες (π.χ. ψηφοφόροι) να επικοινωνούν με τις Αρχές του συστήματος, με πλήρη διαφάνεια. Στα κανάλια αυτά η επικοινωνία αυθεντικοποιείται με τη χρήση ψηφιακών υπογραφών. Μια πρακτική και ασφαλής υλοποίηση των πινάκων ανακοινώσεων αποτελεί το κατανεμημένο σύστημα Rampart

6.9.2 Ανώνυμα Κανάλια Επικοινωνίας (Anonymous Channels).

Τα κανάλια αυτά εξασφαλίζουν την ανωνυμία των χρηστών του συστήματος. Εκτός από τα δίκτυα MIX-net, υπάρχουν και τα συστήματα ανωνυμίας με τη χρήση διαμεσολαβητή (proxy systems) , όπως επίσης και τα υβριδικά συστήματα

6.9.3 Κρυπτογραφία τύπου Threshold (threshold cryptography)

Τα συστήματα κρυπτογράφησης τύπου threshold κατανέμουν τη λειτουργικότητα των κρυπτογραφικών πρωτοκόλλων ώστε να επιτύχουν ανθεκτικότητα (robustness). Για παράδειγμα, σε μια ψηφοφορία η διαδικασία της καταμέτρησης μπορεί να κατανεμηθεί μεταξύ Αρχών Ψηφοφορίας, με τη χρήση ενός threshold κρυπτογραφικού συστήματος δημοσίου κλειδιού (π.χ. threshold ElGamal). Σε αυτήν την περίπτωση υπάρχει μόνον ένα δημόσιο κλειδί, ενώ το ιδιωτικό κλειδί διαμοιράζεται στις Αρχές με τη χρήση τεχνικών διαμοιρασμού μυστικού n (t,n) n 9 . Κάθε ψηφοφόρος κρυπτογραφεί τη ψήφο του με το δημόσιο κλειδί των Αρχών, και η τελική κάλπη αποκρυπτογραφείται από κοινού με τη συνεργασία τουλάχιστον t Αρχών. Η μυστικότητα της ψήφου και η ακρίβεια των αποτελεσμάτων εξασφαλίζεται εφόσον δεν υπάρχουν περισσότερες από κακόβουλες ή απλά δυσλειτουργικές Αρχές. Ο αριθμός αποτελεί τη τιμή threshold του κρυπτογραφικού συστήματος. Τα συστήματα threshold μπορούν να ενισχυθούν, για προστασία από επιθέσεις υποκλοπής κλειδιού (key confiscation), με μηχανισμούς όπως προενεργή ασφάλεια t−1 t 9 (proactive security) καθώς και με τεχνικές ισχυρής χρονικής ασφάλειας (strong forward security)

6.10 Αποδείξεις με Μηδενική Γνώση (Zero Knowledge Proofs)

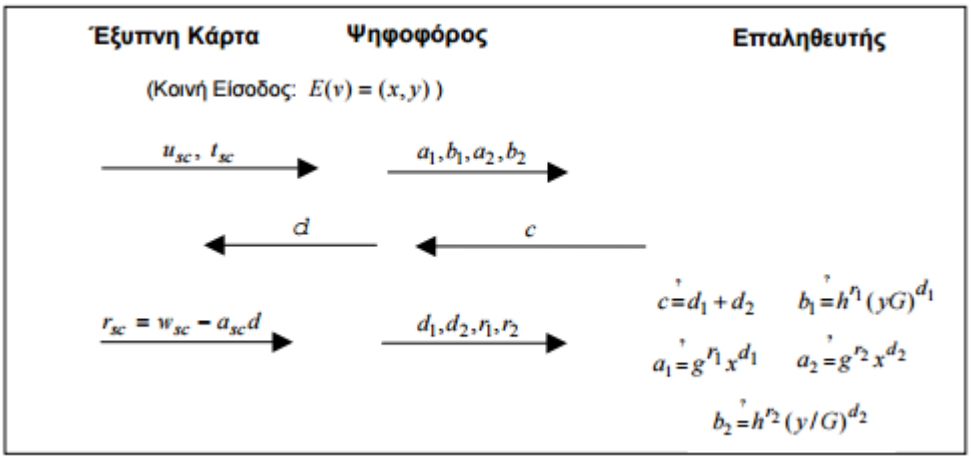
Οι αποδείξεις αυτές χρησιμοποιούν πρωτόκολλα Απόδειξης/Επαλήθευσης με αλληλεπίδραση (interactive), στα οποία ο Αποδεικνύων (Prover) επιβεβαιώνει σε έναν Επαληθευτή (Verifier) την ορθότητα μιας δήλωσης, κατά τέτοιον τρόπο ώστε ο Επαληθευτής να μη μπορεί να μάθει τίποτε περισσότερο, εκτός από το γεγονός ότι η δήλωση είναι ορθή. Τα πρωτόκολλα απόδειξης με μηδενική γνώση χρησιμοποιούνται ευρέως σε ηλεκτρονικά πρωτόκολλα ψηφοφορίας. Για παράδειγμα, τέτοια πρωτόκολλα χρησιμοποιούνται προκειμένου να αποδειχθεί η ορθότητα των μετασχηματισμών στα συστήματα ψηφοφορίας που χρησιμοποιούν δίκτυα MIX-net για την ανωνυμία των ψήφων , για να αποδειχτεί η εγκυρότητα των κρυπτογραφημένων ψήφων στις ομομορφικές εκλογές , για την ορθότητα των κρυπτογραφήσεων στα πρωτόκολλα προστασίας από καταναγκασμό , καθώς και για την ορθότητα των επικυρωμένων ψήφων στα συστήματα που βασίζονται στο μοντέλο των «τυφλών» υπογραφών. Οι αλληλεπιδραστικές αποδείξεις με μηδενική γνώση είναι μη μεταφέρσιμες (non transferable): ο Επαληθευτής δε μπορεί να αποδείξει σε κάποιον τρίτο την ορθότητα μιας δήλωσης. Εν τούτοις είναι δυνατόν αυτές οι αποδείξεις να μετασχηματιστούν σε αποδείξεις που είναι μεταφέρσιμες, επομένως οικουμενικά επαληθεύσιμες, με την ευριστική προσέγγιση των Fiat-Shamir. Στην περίπτωση αυτή η ασφάλεια βασίζεται στο μοντέλο random oracle10

6.11 Προστασία Από Καταναγκασμό

Στις παραδοσιακές εκλογές, ο ρόλος του εκλογικού παραβάν (voting booth) δεν περιορίζεται απλώς στο να επιτρέπει στους ψηφοφόρους να επιλέξουν με απόλυτη μυστικότητα τη ψήφο τους: ουσιαστικά η ύπαρξη του παραβάν αποτρέπει γεγονότα όπως η πώληση της ψήφου (vote selling) και ο καταναγκασμός (coercion) των ψηφοφόρων. Η αποτροπή τέτοιων επιθέσεων αποτελεί σημαντικό κομμάτι της έρευνας για ασφαλή συστήματα ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου.

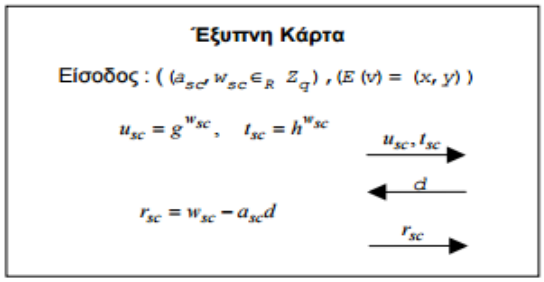
6.12 Απόδειξη Εγκυρότητας Ψήφου σε Εκλογές Προστατευμένες από Καταναγκασμό

Το πρωτόκολλο, με αλληλεπίδραση, της απόδειξης εγκυρότητας της ψήφουE(v) με μηδενική γνώση (IZKP), αποτελεί μια τροποποίηση για δύο-αποδεικνύοντες (two-prover), του πρωτοκόλλου των Cramer, Gennaro και Schoenmakers .

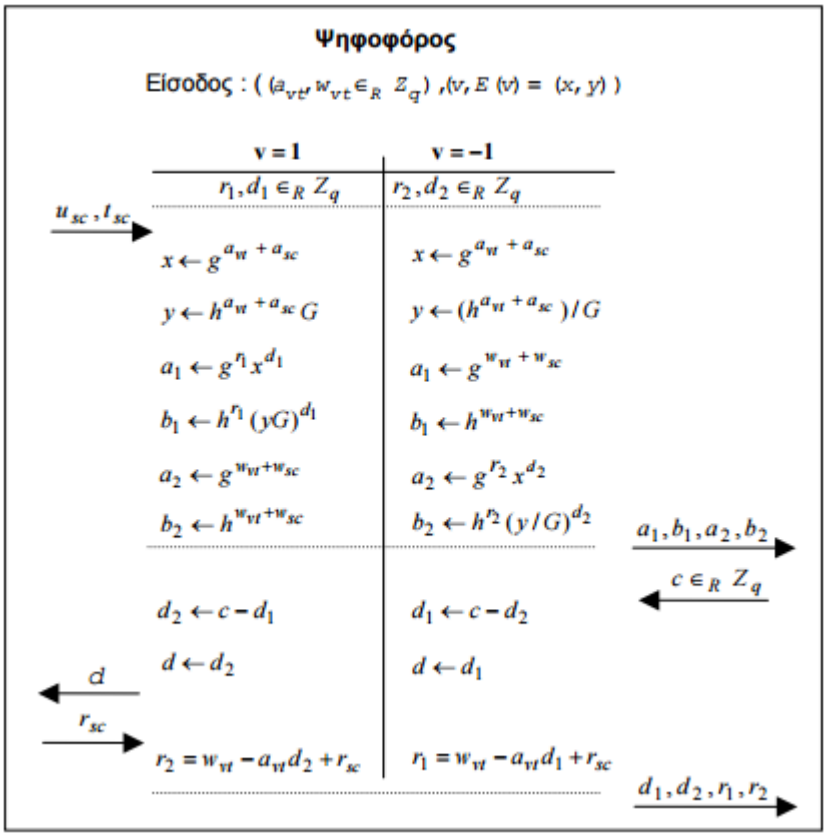


Σχήμα 9: Έξυπνη κάρτα

Η κοινή είσοδος του ψηφοφόρου και της Κάρτας είναι το ( ) (,) (,) όπου a a a a v E v x y g sc vt h sc vtG + + = = v∈{−1,+1}. Η συμμετοχή της Κάρτας στην απόδειξη εγκυρότητας περιγράφεται από την υπορουτίνα . Η συμμετοχή του ψηφοφόρου στην απόδειξη εγκυρότητας περιγράφεται από την υπορουτίνα .



Σχήμα 12: Συμμετοχή της Έξυπνης Κάρτας στην απόδειξη εγκυρότητας



Σχήμα 11: Συμμετοχή του Ψηφοφόρου στην απόδειξη εγκυρότητας

Θεώρημα.

Το πρωτόκολλο απόδειξης με μηδενική γνώση, που περιγράφεται στο Σχήμα 6, αποδεικνύει ότι το είναι κρυπτογράφηση μιας έγκυρης ψήφου (δηλαδή, μιας ψήφου που ανήκει στο σύνολο {-1,1}) [Mag01]. E(v) = (x, y) Μηδενική Γνώση. Η απόδειξη ότι το ζεύγος (x,y) είναι της σωστής μορφής, χωρίς να αποκαλυφθεί η τιμή της ψήφου v, ανάγεται στην απόδειξη γνώσης της σχέσης: log log(/) log log(/)−1 g x= h y G Þ g x= h y G (1) Οι αποδεικνύοντες, δηλαδή ο Ψηφοφόρος και η Κάρτα, είτε έχουν τη γνώση να αποδείξουν την ισότητα στο αριστερό τμήμα της σχέσης (1), είτε την ισότητα στο δεξί τμήμα της (1), αλλά όχι και τις δύο ισότητες ταυτόχρονα ανάλογα με την τιμή της ψήφου που έχει προεπιλεγεί. Για να αποδείξουν οποιαδήποτε από τις δυο ισότητες της (1), οι αποδεικνύοντες πρέπει να χρησιμοποιήσουν την απόδειξη με μηδενική γνώση για την ισότητα των διακριτών λογαρίθμων που προτάθηκε από τους Chaum και Pedersen . Στην απόδειξη , οι τυχαιότητες των μηνυμάτων που αποστέλλονται στον Επαληθευτή είναι συνδυασμός των τυχαιοτήτων του Ψηφοφόρου και της Κάρτας, κατά τρόπο ώστε κανείς από τους

δυο δε μπορεί να μάθει την τυχαιότητα του άλλου, αφού κάτι τέτοιο θα παραβίαζε την Προστασία από Καταναγκασμό. Στην εργασία αποδεικνύεται η ιδιότητα της μηδενικής γνώσης για την απόδειξη των Chaum και Pedersen στην περίπτωση ενός τίμιου επαληθευτή (honest-verifier). Αυτό εξυπηρετεί το σκοπό μας, αφού το πρωτόκολλο απόδειξης που περιγράψαμε θα μετατραπεί σε απόδειξη χωρίς αλληλεπίδραση, προκειμένου να υπάρχει οικουμενική επαληθευσιμότητα. Για τη μετατροπή αυτή, ο Επαληθευτής μπορεί να υλοποιηθεί είτε ως μια έμπιστη πηγή τυχαίων συμβολοσειρών είτε με την ευριστική προσέγγιση των Fiat και Shamir , όπου και γίνεται χρήση συναρτήσεων κατακερματισμού. Στην τελευταία περίπτωση η ασφάλεια βασίζεται στο μοντέλο random oracle11.

Βιβλιογραφία

- Cryptanalysis of a Zero – knowledge Identification Protocol of Eurocrypt ‘95
  Jean – Sebastian Coron and David Naccache
- Overview of Zero – Knowledge Protocols
  Jeffry Knapp 2003
- O Goldreich foundations of Cryptography vol. 1 Basic Tools
  Cambridge University Press, 2001
- Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης
  Β.Α. Κάτος, Γ.Χ. Στεφανίδης, 2003
- Computational Complexity: A Modern Approach
  Sanjeev Arora and Boaz Barak, 2007
- How to Cut a Cake: And Other Mathematical Conundrums
  Ian Stewart, 2006
- Εφαρμογές της κρυπτογραφίας
  https://dspace.lib.uom.gr/efarmogestiskriptografias
- Κρυπτογράφηση δημόσιου κλειδιού
  https://skytal.es/wiki/kriptografiaDimosiouKleidiou
- Συμμετρική Κρυπτογραφία http://users.auth.gr/symmetrikikriptografia.pdf
- Συμμετρική – Ασύμμετρη κρυπτογράφιση http://diktya.gr/assymetri
- Έννοιες της Κρυπτογραφίας
- Ηλεκτρονική ψηφοφορία **http://users.ionio.gr/~emagos/web_psifofories.pdf**