ΤΕΧΝΟΛΟΓΙΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ

ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

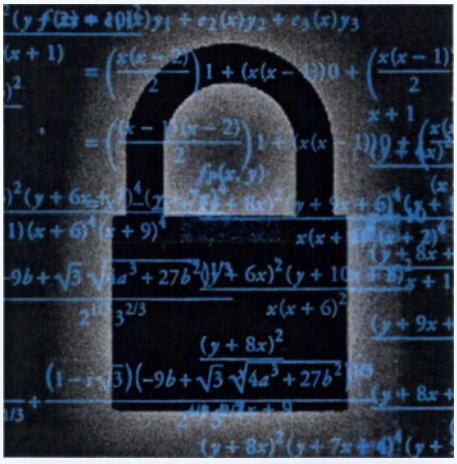
ΤΕΙ ΚΑΛΑΜΑΤΑΣ-

ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ

<<Πρωτόκολλα μηδενικής γνώσης>>

Δάνου Γεωργία

Α.μ:2007023



Επόπτης:

Πατσάκης Κωνσταντίνος

Σεπτέμβριος 2 011

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος

Η παρούσα πτυχιακή ασχολείται με τα πρωτόκολλα μηδενικής γνώσης

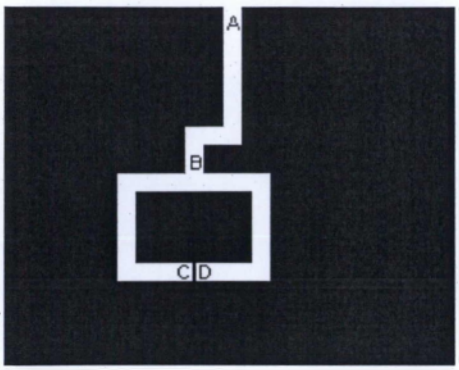
. Ένα πρωτόκολλο αποκαλείται πρωτόκολλο μηδενικής γνώσης αν και μόνο εάν υπάρχει αλγόριθμος ο οποίος λειτουργεί σε πολυωνυμικό χρόνο και έχει την δυνατότητα να παράγει σύνολο μηνυμάτων του πρωτοκόλλου χωρίς τη γνώση του μυστικού απόδειξης, έτσι ώστε το σύνολο των μηνυμάτων να μην είναι δυνατόν να διακριθεί από ένα σύνολο <<πραγματικών >> μηνυμάτων που προέρχονται από την εκτέλεση πρωτοκόλλου με το μέλος που γνωρίζει το μυστικό απόδειξης. Τα πιο γνωστά πρωτόκολλα είναι το πρωτόκολλο Fiat-shamir ,Feige-fiat –shamir , Okamoto . Guillou-Quisquarter , Schnoor και το πρωτόκολλο ισομορφισμού γράφων.

Εισαγωγή

Τα πρωτόκολλα μηδενικής γνώσης έχουν ως κύριο σκοπό την αυθεντικοποίηση. Επομένως μια οντότητα θα πρέπει να αποδείξει στην άλλη την κατοχή ενός μυστικού και όχι να επιδείξουν το μυστικό αυτό .Αυτό έχει ως αποτέλεσμα ,σε κανένα σημείο του πρωτοκόλλου να μην γίνεται αποκάλυψη του μυστικού από καμία οντότητα και έτσι καμία οντότητα δεν μαθαίνει κάτι καινούργιο .

Προκειμένου να γίνει σαφές θα χρησιμοποιήσουμε ένα παράδειγμα. Έστω η Άλικη που θέλει να πείσει τον Μπόμπ ότι ξέρει το μυστικό και να περάσει μέσα από την πόρτα μεταξύ των σημείων C και D της σπηλιάς . Ο Μπόμπ αφήνει την Άλικη να πάει στη σπήλια είτε από το σημείο C ή το σημείο D . Όταν η Άλικη πάει εκεί , φωνάζει τον Μπόμπ να πάει στο σημείο B. Μόλις ο Μπόμπ φτάσει εκεί δεν μπορεί να γνωρίζει αν η Άλικη είναι στο σημείο C ή D . Ο Μπόμπ τώρα φωνάζει <<δεξιά >> ή <<αριστερά>>, και αν η Άλικη γνωρίζει το μυστικό μονοπάτι τότε μπορεί να ακολουθήσει την εντολή του Μπόμπ. Στην συνέχεια βγαίνουν έξω από την σπηλιά με τα πόδια (Σχήμα 1) . Επαναλαμβάνουν την διαδικασία αρκετές φορές ,αν η Άλικη ξέρει το μυστικό τότε περνάει την δοκιμασία (πληρότητα). Αν όχι, τότε μπορεί να συμμορφωθεί με το αίτημα του Μπόμπ .

Τα πρωτόκολλα μηδενικής γνώσης κατατάσσονται στην κατηγορία πρωτοκόλλων απόδειξης με αλληλεπίδραση (Interactive Proof), που σημαίνει ότι τα συμμετέχοντα μέλη ανταλλάσσουν πλήθος μηνυμάτων τα οποία βασίζονται σε τυχαίους αριθμούς και σε οποιαδήποτε στιγμή μπορεί οποιοδήποτε από τα μέλη να τερματίσει το πρωτόκολλο .Αρχικά μια έμπιστη οντότητα η οποία δημιουργεί κάποια δεδομένα τα οποία είναι γνωστά σε όλους και κάποια τα κατέχουν μόνο εξουσιοδοτημένες οντότητες . Προκειμένου δυο οντότητες να αποδείξουν την γνώση της μυστικής πληροφορίας , η μια στέλνει στην άλλη ένα τυχαίο αριθμό .Η οντότητα που τον παραλαμβάνει ,στέλνει στην πρώτη μια πρόσκληση , στην οποία πρέπει να απαντήσει σωστά προκειμένου να αποδείξει τη γνώση του μυστικού .Οι δύο οντότητες θα καλούνται η μια ως μάρτυρας και η άλλη ως επιβεβαιωτής ανάλογα με το ποια οντότητα επιβεβαιώνει τη γνώση του μυστικού σε ποια. Το κίνητρο της ανάπτυξης των πρωτοκόλλων μηδενικής γνώσης είναι το γεγονός ότι στα «συμβατικά» πρωτόκολλα αυθεντικοποίησης, κατά την ολοκλήρωση της εκτέλεσής 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.



Σχήμα 1: σπηλιά

ΚΕΦΑΛΑΙΟ 1: ΔΙΑΔΡΑΣΤΙΚΗ ΑΝΑΓΝΩΡΙΣΗ

Α. ΕΙΣΑΓΩΓΗ

Στη διαδραστική αναγνώριση[5] υποθέτουμε ότι υπάρχει ένα έμπιστο κέντρο (μια κυβέρνηση , μια εταιρία έκδοσης πιστωτικών καρτών , μια στρατιωτική βάση ,κτλ) το οποίο εκδίδει τις έξυπνες κάρτες για τους χρήστες μετά από σωστό έλεγχο των φυσικών τους ταυτοτήτων. Καμία επιπλέον αλληλεπίδραση με το κέντρο δεν απαιτείται είτε για την παραγωγή ή για την απόδειξη της ταυτότητας . Ένας απεριόριστος αριθμός χρηστών μπορεί να συμμετέχει στο σύστημα χωρίς να υποβαθμίσει την απόδοση του , και δεν είναι πάντα απαραίτητο να κρατάει μια λίστα με όλους τους έγκυρους χρήστες .

Η αλληλεπίδραση με τις έξυπνες κάρτες δεν επιτρέπει στους επαληθευτές την αναπαραγωγή τους ακόμα και την πλήρης γνώση των μυστικών περιεχομένων όλων των καρτών που εκδίδονται από το κέντρο ,επίσης δεν θα είναι δυνατόν οι αντίπαλοι να δημιουργήσουν νέες κάρτες ή να τροποποιήσουν ήδη υπάρχοντες ταυτότητες . Ακόμα καμία πληροφορία απολύτως δεν διαρρέει κατά την διάρκεια της αλληλεπίδρασης. Οι έξυπνες κάρτες μπορούν να διαρκέσουν μια ζωή ,ανεξάρτητα από το πόσο συχνά χρησιμοποιούνται .

Β.ΤΟ ΣΥΣΤΗΜΑ

Πριν το κέντρο αρχίζει να εκδίδει κάρτες , αυτό επιλέγει και φτιάχνει ένα δημόσιο modulous n και μια ψευδό-τυχαία συνάρτηση f η όποια είναι χάρτης αυθαίρετων σειρών στο εύρος [0,n].

Το modulous n είναι προϊόν δυο μυστικών τιμών των p και q και μόνο το κέντρο γνωρίζει την παραγοντοποίηση του modulous n και επομένως ο καθένας μπορεί να χρησιμοποιήσει το ίδιο n. Η συνάρτηση f θα πρέπει να είναι δυσδιάκριτη από μια πραγματικά τυχαία συνάρτηση από οποιοδήποτε πολυωνυμικό οριοθετημένο υπολογισμό.

Όταν ένας επιλέξιμος χρήστης υποβάλει αίτηση για μια έξυπνη κάρτα , το κέντρο προετοιμάζει μια σταθερά I η οποία περιέχει όλες τις πληροφορίες σχετικά με τον χρήστη (όνομα ,επώνυμο, διεύθυνση ,ID αριθμό ,φυσική περιγραφή , εκκαθάριση για λόγους ασφαλείας ,κτλ) και για την κάρτα (ημερομηνία έκδοσης , περιορισμούς ως προς το κύρος , κτλ).

Οι ανωτέρω πληροφορίες επαληθεύεται από το σύστημα και αυτό που είναι σημαντικό είναι ο λεπτομερής και ο διπλός έλεγχος για ορθότητα των στοιχείων. Το κέντρο στη συνέχεια εκτελεί τα ακόλουθα βήματα:

1. *Υπολογίζει τις τιμές $v_j=f(I,j)$ για μικρές τιμές του j.*
2. *Παίρνει k διακριτές τιμές του j για το οποίο v_j είναι τετραγωνικό υπόλειμμα (mod n) και υπολογίζει την μικρότερη τετραγωνική ρίζα s_j του v_j^{-1} (mod n).*
3. *Εκδίδει μια έξυπνη κάρτα η οποία περιέχει το I , τους k s_j τιμές και τους δείκτες τους .*

   Όταν η κάρτα εισαχτεί στο μηχάνημα επιβεβαίωσης τα οποία είναι πανομοιότυπα αυτόνομα μηχανήματα και τα οποία περιέχουν μικροεπεξεργαστή , μια μικρή μνήμη , και μια διεπαφή I/O .Η μόνη πληροφορία που αποθηκεύεται σε αυτά είναι το modulous n καθώς και η συνάρτηση f .Όταν η έξυπνη κάρτα εισέρχεται μέσα στο μηχάνημα ,αυτό αποδεικνύει ότι γνωρίζει s_1,s_2,s_k χωρίς να δίνει καμία πληροφορία για τις τιμές αυτές. .Αυτό επιτυγχάνεται με τον ακόλουθο τρόπο :

   - *Ο Α στέλνει το I στον Β.*
   - *Ο Β παράγει $v_j=f(I,j)$ για j=1,……,k.*

     Επαναλαμβάνει τα βήματα 3 εώς 6 για i= 1,……,t:

     - *Επιλέγει τυχαιά $r_i \in [0,n)$ και στέλνει $x_i=r_i^2 (mod\ n)$ στον Β.*
     - *Β στέλνει ένα τυχαίο δυαδικό διάνυσμα*
     - *Ο Α στέλνει στον Β :*

$y_i= r_i \Pi_{eij=1} s_j (mod n)$

   - *Ο Β ελέγχει ότι :*

     $x_i= y_i^2 \Pi_{eij=1} v_j (mod\ n)$.

Πρέπει να τονιστεί ότι ο επιβεβαιωτής δέχεται την απόδειξη ταυτότητας του Α μόνο όταν όλα τα t είναι σωστά .

Επίσης ο Α μπορεί να πιστοποιήσει την αυθεντικότητα ενός συγκεκριμένου μηνύματος (λ.χ τις οδηγίες για ένα απομακρυσμένο σύστημα ελέγχου ή για ένα πρόγραμμα το οποίο τοποθετείται σε ένα απομακρυσμένο υπολογιστή) χωρίς να έχει εξάγει νέες τετραγωνικές ρίζες με την αποστολή στον Β

των πρώτων 128 bits της $f(m,x_i)$ στο βήμα 3. Ένα ο Β γνωρίζει το m ,αυτός μπορεί εύκολα να ελέγξει την τιμή στο βήμα 6.

Η διαδραστική αναγνώριση έχει χρήση στα πρωτόκολλα που ακολουθούν.

ΚΕΦΑΛΑΙΟ 2: ΔΟΜΗ ΠΡΩΤΟΚΟΛΛΩΝ ΜΗΔΕΝΙΚΗΣ ΓΝΩΣΗΣ

ΠΡΩΤΟΚΟΛΛΟ FIAT –SHAMIR

ΔΟΜΗ ΠΡΩΤΟΚΟΛΛΩΝ ΜΗΔΕΝΙΚΗΣ ΓΝΩΣΗΣ

Θεωρούμε ότι ένα άτομο Α[1] έχει ένα μυστικό και θέλει να αποδείξει την κατοχή του σε ένα άτομο Β με τη χρήση πρωτοκόλλου μηδενικής γνώσης. Ένας κύκλος ενός πρωτόκολλου αποτελείται από τα εξής στάδια:

1. *στάδιο μαρτυρίας, όπου το άτομο Α στέλνει μήνυμα δέσμευσης στον Β. 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 του Α, από την οποία ο Β επιλέγει την πρόκληση στο επόμενο στάδιο.*

   2.στάδιο πρόκλησης, όπου ο Β στέλνει την πρόκλησή του στον Α. Η πρόκληση επιλέγεται από το μήνυμα δέσμευσης του Α. Ο Α δεν είναι σε θέση να γνωρίζει εκ των προτέρων ποια θα είναι η πρόκληση του Β. 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 ο Α καλείται να υπολογίσει τη σωστή απάντηση της πρόκλησης του Β σε πολυωνυμικό χρόνο και να ενημερώσει τον Β για τη λύση.

Επίσης τα γενικά χαρακτηριστικά των πρωτόκολλων μηδενικής γνώσης είναι:

- *Είναι καθορισμένο εκ των προτέρων. Δηλαδή ο σχεδιασμός ενός πρωτοκόλλου έχει ολοκληρωθεί προτού το πρωτόκολλο χρησιμοποιηθεί.*

- *Αμοιβαία συμφωνία. Όλα τα μέλη συμφωνούν να εκτελέσουν τα βήματα του πρωτοκόλλου με τη σειρά που υποδεικνύει το πρωτόκολλο*

- *Σαφήνεια. Η εκτέλεση όλων των βημάτων του πρωτοκόλλου θα πρέπει να είναι σαφής, έτσι ώστε κανένα από τα μέλη να μην παρερμηνεύσει τα βήματα που του αναλογούν.*

- *Πληρότητα. Για οποιαδήποτε κατάσταση που μπορεί να βρεθεί οποιοδήποτε μέλος, θα πρέπει να υπάρχουν προκαθορισμένες ενέργειες.*

2.2 ΠΡΩΤΟΚΟΛΛΟ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ FIAT -SHAMIR

*Το πρωτόκολλο αυθεντικοποίησης Fiat-Shamir [4,1] δημιουργήθηκε το 1987 και βασίζεται στη δυσκολία εύρεσης της τετραγωνικής ρίζας modulo ενός μεγάλου ακεραίου ,ο όποιος είναι γινόμενο δυο μεγάλων πρώτων. Το πρωτόκολλο περιλαμβάνει μια εμπιστευτική οντότητα δημιουργεί και ανακοινώνει τον n=p*q με τον p,q πρώτους καθώς και καταχωρεί τα δημόσια κλειδιά των μελών.*

Ένα άτομο A εγγράφεται στο σύστημα επιλέγοντας ένα μυστικό αριθμό s για τον όποιο ισχύει 0 <s < n – 1 .Στην συνέχεια υπολογίζει το τετράγωνο της μυστικής ποσότητας:

$v=s^2 mod n$ ο όποιος αντιπροσωπεύει το δημόσιο κλειδί της. Τέλος δημοσιεύει τον αριθμό v στην έμπιστη οντότητα . Στο πρωτόκολλο αυτό κάθε οντότητα προσπαθεί να αποδείξει τη γνώση του s.

Τα βήματα από τα οποία αποτελείται το πρωτόκολλο είναι τα εξής:

1. Ο επιβεβαιωτής διαλέγει ένα τυχαίο αριθμό r και στέλνει στο

μάρτυρα τον αριθμό $r^2 mod n$.

2. Ο μάρτυρας επιλέγει τυχαία μία τιμή e, η οποία είναι είτε 0

είτε 1 και τη στέλνει στον επιβεβαιωτή.

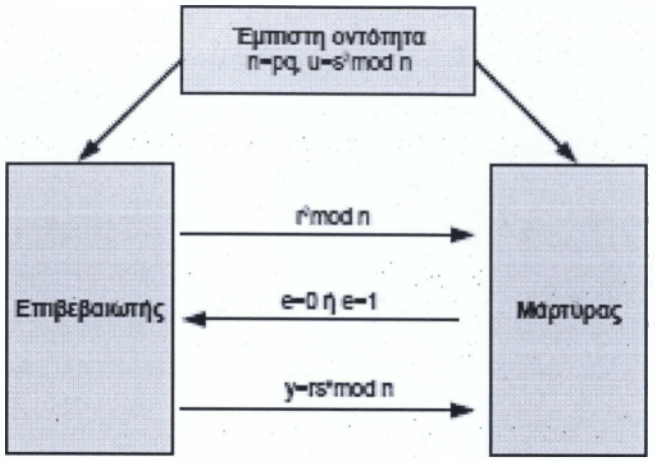
3. Ο επιβεβαιωτής υπολογίζει με τη σειρά του τη τιμή $y \equiv rs^e mod n$

και τη στέλνει στον μάρτυρα.

4. Ο μάρτυρας ελέγχει αν ισχύει η σχέση

$y^2 \equiv r^2 v^e \ mod \ n$

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



Εικόνα 1 Σχηματική αναπαράσταση Fiat-Shamir

2.3 Αναλύση πρωτοκόλλου Fiat-shamir

Αρχικά παρατηρούμε ότι σε έναν κύκλο του πρωτοκόλλου [1] ο επιβεβαιωτής θα πρέπει να γνωρίζει και τις δύο προκλήσεις, για e= 0 και για e = 1. Για e = 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 ο επιβεβαιωτής καλείται να απαντήσει μόνο στην πρόκληση για e= 1, ο αντίπαλος μπορεί να προσποιηθεί την ταυτότητα του επιβεβαιωτή επιλέγοντας τυχαίο r και στέλνοντας την ποσότητα $x=r^2v^{-1}(mod\ n)$

αντί του τετραγώνου του r. Έτσι θα ισχύει:

$x=r^2v^{-1}v^{-1}modn= r^2modn$

Επειδή όμως ο μάρτυρας έχει την επιλογή να ζητήσει απόδειξη ότι ο επιβεβαιωτής γνωρίζει την τετραγωνική ρίζα του x, ο αντίπαλος θα πρέπει να λύσει το δύσκολο πρόβλημα υπολογισμού της τετραγωνικής ρίζας του r2v-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 μάρτυρας 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 του επιβεβαιωτή και του μάρτυρα . 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 e ∈{0, 1}.

3. – Αν e = 0 τότε:

$X=y^2modn$

– Αν e = 1 τότε:

$X=y^2v^{-1}modn$

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

Παράδειγμα

Έστω ότι n = 19×29 = 551 και ότι το μυστικό s εί-

ναι ο αριθμός 111. Τότε u ≡ 1112 mod 551 ≡ 199. Ο επιβεβαιωτής

καλείται να αποδείξει γνώση της τ ιμής s, επιλέγει ένα τυχαίο αριθ-

μό r, τον 257 και αποστέλλει στον μάρτυρα την τιμή r2 mod 551 ≡ 2572 mod 551 ≡ 480. Ο μάρτυρας επιλέγει τυχαία την τιμή e = 1

και την αποστέλλει στον επιβεβαιωτή. Αυτός με τη σειρά του υπο-

λογίζει την τιμή $y \equiv rs^e \bmod n \equiv 257 \times 111 \bmod 551 \equiv 426$. *Ο*

μάρτυρας αρκεί πλέον να υπολογίσει αν ισχύει ότι

$y2 \equiv r^2 u^e \bmod n$

Πράγματι έχουμε ότι :

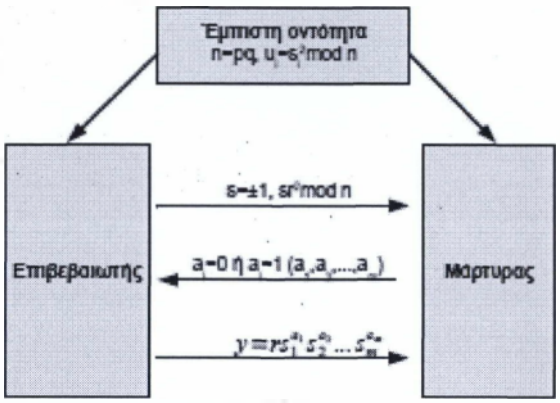
$426^2 = 257^2 199^1 \bmod n$

ΚΕΦΑΛΑΙΟ 3 ΠΡΩΤΟΚΟΛΛΟ FEIGE –FIAT – SHAMIR

3.1 Τρόπος λειτουργίας

Το πρωτόκολλο των Feige-fiat-shamir [4]δημιουργήθηκε το 1988 και βασίζεται στη δυσκολία εύρεσης τετραγωνικής ρίζας modulo ενός ακέραιου ο οποίος είναι γινόμενο δυο μεγάλων αριθμών.

*Έτσι αρχικά η έμπιστη οντότητα κατασκευάζει το n=p*q, p,q πρώτους. Έπειτα κατασκευάζονται το μυστικοί αριθμοί si που δεν διαιρούν το n και μένουν μυστικοί .Η οντότητα δημοσιεύει το $u_i = s_i^2 mod n$. Στο πρωτόκολλο αυτό κάθε οντότητα καλείται να αποδείξει τη γνώση του si .*



Εικόνα 2 σχηματική αναπαράσταση του feige-fiat –shamir

Το πρωτόκολλο αποτελείται από τα εξής βήματα :

1. *Ο επιβεβαιωτής επιλέγει έναν αριθμό r τυχαία και ένα αριθμο $s\begin{cases}1\\-1\end{cases}$ και στέλνει στον μάρτυρα τον αριθμό $v=sr^2 mod n$.*
2. *Ο μάρτυρας κατασκευάζει ένα τυχαίο διάνυσμα με συντεταγμένες (α1, α2,…,…..αm) είτε 0 είτε 1 και τις στέλνει στον επιβεβαιώτη.*
3. *Ο επιβεβαιωτής υπολογίζει με τη σειρά του την τιμή y= $r*s_1^{a1}*s_2^{a2}\ldots\ldots\ldots*s_m^{am} mod n$*
4. *Ο μάρτυρας ελέγχει αν ισχύει η σχέση :$y^2=\pm r^2*u_1^{a1}*u_2^{a}\ldots\ldots*u_m^{am}$ mod n*
   Αν δεν ισχύει το πρωτόκολλο σταματά.

3.2 Ανάλυση πρωτοκόλου feige-fiat –shamir

Η ασφάλεια του πρωτοκόλλου[1] έγκειται στο γεγονός τις δυσκολίας εύρεσης της τετραγωνικής ρίζας μεγάλων σύνθετων ακέραιων αριθμών.
Στο πλαίσιο όλης της διαδικασίας ο μάρτυρας δεν παρέχει καμία χρήσιμη πληροφορία στον επιβεβαιωτή. Το μόνο που κάνει είναι να αποδεικνύει την κατοχή των μυστικών αριθμών χωρίς να υποδεικνύει ποιοι είναι . Ένας υποκλοπέας θα μάθαινε ακριβώς τα ίδια πράγματα.
Ας υποθέσουμε ότι μεταξύ της Αλίκης ,επιβεβαιωτής , και του Βύρωνα ,μάρτυρας , επεμβαίνει η Εύα ,υποκλοπέας. Αν θέλει η Εύα να προσποιηθεί στον Βύρωνα την Αλίκη, θα πρέπει να μαντεύει σωστά τους αριθμούς αi .Έπειτα να παίρνει ένα τυχαίο αριθμό
$x=y^2u_1^{-a1}u_2^{-a2}u_m^{-am} mod n$ *και να τον στέλνει στον Βύρωνα.*
Κάθε φορά που ο Βύρωνα στέλνει ένα αi η Εύα να στέλνει το y της .Ο Βύρωνα μένει ικανοποιημένος και κατανοεί ότι η Εύα που προσποιείται την Αλίκη ξέρει τους μυστικούς αριθμούς
Ωστόσο η πιθανότητα να μαντεύει η Εύα τους σωστούς αi είναι της τάξης 2^{-kt}
Στη περίπτωση που η διαδικασία επαναλαμβάνεται πολλές φορές η πιθανότητα να μαντέψει σωστά τα αi είναι της τάξης 2^{-kt} *τα k =-4 και t=5 και έχουν γινόμενο ίσο με 20 , η πιθανότητα πλαστογραφίας είναι μια στο εκατομμύριο.*

3.3 Εναλλακτική έκδοση

Μια εναλλακτική έκδοση του Feige –Fiat- Shamir [3]δίνεται από τον Schneier [BS94]. Στην έκδοση του Schneier , ο επιβεβαιωτής επιλεγεί k τυχαίους αριθμούς S1 , ……s_k , όπου Sj είναι ένα ακέραιο υπόλοιπο του modulous n και δημοσιεύει αυτά ως δημόσια κλειδιά. Στη συνέχεια ο επιβεβαιωτής υπολογίζει το μικρότερο Ij το οποίο ισούται με I_j = $cb\sqrt{1/S_j}$ modn και στην συνέχεια κρατάει το I_1,I_2 , ……I_j ως ιδιωτικά κλειδιά. Έπειτα ακολουθούν τα βήματα που περιγράφονται παραπάνω. Η δυσκολία αυτής της έκδοσης του πρωτοκόλλου έγκειται στη δυσκολία του υπολογισμού του τετραγωνικού υπόλοιπου.

3. 4 ΠΡΟΒΛΗΜΑΤΑ ΜΕ ΠΡΩΤΟΚΟΛΛΑ ΜΗΔΕΝΙΚΗΣ ΓΝΩΣΗΣ

Το βασικό πρόβλημα αυτού του είδους εξακρίβωσης της ταυτότητας είναι το θέμα των man-in-the-middle επιθέσεων ,στις οποίες ένας ανέντιμος επιβεβαιωτής φτιάχνει ένα αντίγραφο της απόδειξη της ταυτότητας που δίνεται από τον μάρτυρα , για να την παραποιήσει με επιτυχία σε έναν αλλό επιβεβαιωτής . Αυτό το πετυχαίνει με την μετεγκατάσταση κάθε μόνου μηνύματος που δέχεται ο επιβεβαιωτής από τον μάρτυρα . Η αντεπίθεση για αυτό το είδος της επίθεσης είναι μια ισχυρή μέθοδος συγχρονισμού: επιβάλλεται ένα ορισμένο
χρονικό περιθώριο για τις απαντήσεις, με σκοπό να μην υπάρχει αρκετά χρόνος για τη μεταβίβαση των επικοινωνιών. Μια άλλη αντεπίθεση, που μπορούν να χρησιμοποιηθούν εκτός από το πρώτο, είναι να απαιτούν από όλες τις ταυτοποιήσεις να λάβει χώρα μέσασε προστατευόμενες ζώνες (θωρακισμένο δωμάτια, κλωβοί Faraday) για την πρόληψη της επικοινωνίας.

ΚΕΦΑΛΑΙΟ 4 ΠΡΩΤΟΚΟΛΛΟ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ GUILLOU-OUISQUARTER

4.1 Τρόπος λειτουργίας

Το πρωτόκολλο του Guillou και Quisquarter[1,4,2] κατασκευάστηκε το 1988 και αποτελεί επέκταση του πρωτοκόλλου Fiat- Shamir . Η ασφαλειά του βασίζεται στη δυσκολία εύρεσης των πρώτων παραγόντων ενός σύνθετου αριθμού. Η βασική διαφορά του GQ και του Fiat-Shamir έγκειται στο γεγονός ότι ο χώρος

πρόσκλησης είναι μεγαλύτερος από ενα(1) bits,με αποτέλεσμα να χρειάζονται λιγότερες επαναλήψεις του πρωτοκόλου προκειμένου να επιτευχθει μικρή πιθανότητα πλαστοπροσωπίας.

*Αρχικά μια οντότητα (Trusted authority) κατασκευάζει το n=p*q η οποία είναι μια δημόσια παράμετρο. Στη συνέχεια επιλέγει το b€ ZØ(n) ο οποίος είναι μυστικός και εκθέτης κρυπτογράφησης.*

Οι παράμετροι p,q παραμένουν κρυφοί ενώ το n ,b είναι δημοσιές παραμέτροι.

Το επόμενο στάδιο είναι η εγγραφή του μέλους. Η έμπιστη οντότητα επιλέγει την ταυτότητα του μέλους, η οποία είναι ένας ακέραιος αριθμός IDA, έτσι ώστε 1< IDA <n . Στη συνέχεια η μυστική οντότητα υπολογίζει το μυστικό απόδειξης του μέλους :

$s_a=(ID_A)$ *^-s modn*

$S=b^{-1} mod\ \varphi(n)$ *το gcd (b ,φ(n))=1*

Την οποία και παραδίδει στο εγραφόμενο μέλος εμπιστευτικά.

Τέλος η εμπιστευτική οντότητα δημοσιεύει την ταυτότητα του μέλους μαζί με τα στοιχεία του σε ένα δημόσιο ευρετήριο.

Η διαδικασία αυθεντικοποίησης αποτελείται από τα ακόλουθα βήματα :

- *Ο επιβεβαιωτής επιλέγει έναν τυχαίο αριθμό k για τον οποίο ισχύει 1≤ k ≤n. Στη συνέχεια υψώνει τον αριθμό αυτό στο δημόσιο εκθέτη και στέλνει το αποτέλεσμα στον μάρτυρα .*
  X=k^b(modn)

- *Ο μάρτυρας επιλέγει την πρόσκληση e,για την οποία ισχύει*
  1≤e≤ b και την αποστέλνει στον επιβεβαιωτή.
  Μάρτυρας->επιβεβαιωτή : e
- *Ο επιβεβαιωτής υπολογίζει την απόκριση και την στέλνει στον μάρτυρα :*
  Y=ks_A^b(mod n)
- *Ο μάρτυρας προμηθεύεται την ταυτότητα του επιβεβαιώτη από το ευρετήριο και ελέγχει αν ισχύει :*
  X= (ID_A^b)y^bmodn ,
  Απορρίπτοντας την περίπτωση οπού x=0(modn).
  Η πιθανότητα επιτυχούς πλαστοπροσωπίας από τον αντίπαλο για t γύρους είναι ίση με (1/e)-t.

ΚΕΦΑΛΑΙΟ 5 ΠΡΩΤΟΚΟΛΛΟ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ SCHNORR

5.1Τρόπος λειτουργίας πρωτοκόλλου schnorr

Το πρωτόκολλο δημιουργήθηκε το 1991 από τον Schnoor[4 ,1]

Και πήρε το όνομα του. Τα πρωτόκολλα που παρουσιάσαμε προηγουμένως (Fiat-Shamir , Feige –Fiat –Shamir ,Guillou- Quisquarter) βασίζονται στο πρόβλημα της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων .

Η ασφάλεια του πρωτοκόλλου αυτού βασίζεται στο πρόβλημα του διακριτού αλγορίθμου. 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 .Καταρχήν η οντότητα T επιλέγει ένα μεγάλο αριθμό p και ένα μεγάλο πρώτο διαιρέτη q του p-1. Στη συνέχεια επιλέγει η εμπιστευτική οντότητα ένα στοιχείο β το οποίο να έχει την τάξη q. Για να επετεύχθη κάτι τέτοιο αρκεί να βρει ένα στοιχείο γεννήτορας της πολλαπλασιαστικής ομάδας modulo p και να υψωθεί στη p-1 /q δύναμη. Τέλος η T επιλέγει δύο αλγόριθμους, τον sigT για υπογραφή και τον verT για επικύρωση καθώς και ένα αριθμό t, για τον οποίο έχουμε ότι $2t < q$. Όλες οι παράμετροι εκτός του αλγόριθμου sigT δημοσιοποιούνται από την T. Για να αποκτήσει μια οντότητα β ένα πιστοποιητικό από την T, επιλέγει έναν αριθμό $d \in Z_q$ και υπολογίζει την ποσότητα:

$v = \beta^{-c} \bmod p$ και στη συνέχεια τη στέλνει στην οντότητα T.

Τέλος η εμπιστευτική οντότητα T παράγει την υπογραφή S.

S=sig(ID(β) ,v) καθώς και την ψηφιακή υπογραφή της έμπιστης οντότητας στα στοιχεία αυτά και δημοσιεύει το ακόλουθο πιστοποιητικό για την οντότητα β.

Cert α=(ID(β), v,s).

Κατά την εκτέλεση του πρωτόκολλου αυθεντικοποίησης , ο επιβεβαιωτής αποδεικνύει την ταυτότητα του στο μάρτυρα με τον ακόλουθα βήματα:

[1] Ο επιβεβαιωτής επιλέγει έναν τυχαίο αριθμό r για τον οποίο ισχύει $0<r<q$ τον οποίο χρησιμοποιεί ως εκθέτη στη δημόσια παράμετρο u και στέλνει το αποτέλεσμα στον μάρτυρα μαζί με το πιστοποιητικό της
Επιβεβαιωτής →μάρτυρα : cert α, $x \equiv u^r \pmod p$

[2] Στην συνέχεια ο μάρτυρας επιλέγει την πρόκληση b ,με $1 \le b \le 2^t$, την οποία την στέλνει στον επιβεβαιωτή
Μάρτυρας→ επιβεβαιωτής :b

[3] Ο επιβεβαιωτής στην συνέχεια υπολογίζει την απόκριση y την οποία την στέλνει στον μάρτυρα :
Επιβεβαιωτής→ μάρτυρας: $y = \beta * b + r \pmod p$

[4] Τέλος ο μάρτυρας αφού λάβει την ταυτότητα του επιβεβαιωτή ελέγχει αν ισχύει η σχέση :
$w \equiv \beta^y u^r \bmod n$

5.2 Ανάλυση πρωτοκόλλου Schnoor

Είναι φανερό ότι η επιτυχής εκτέλεση πρωτοκόλλου [1] απαιτεί τη γνώση μυστικού απόδειξης B 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 στον επιβεβαιωτη. Επομένως, τα μηνύματα του πρωτοκόλλου δεν αποκαλύπτουν καμία μυστική παράμετρο.

Ώστοσο ,για μεγάλη τιμη της προκλήσης b , ο μάρτυρας στο τέλος του πρωτοκόλλου έχει τη λύση της εξίσωσης (x, y,b) , της εξίσωσης

$X=u^y v^b (mod\ p)$.

Το οποίο 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:

$x \equiv u^y v^b (mod\ p)$

3. Ο αντίπαλος έχει μια τριάδα (x, y, b) η οποία πληρεί τις απαιτήσεις του πρωτοκόλλου αυθεντικοποίησης και μπορεί να εκτελέσει το πρωτόκολλο με τον μάρτυρα. Ο αλγόριθμος του αντιπάλου ολοκληρώνεται σε πολυωνυμικό χρόνο, παράγοντας τα επιθυμητά μηνύματα του πρωτοκόλλου

ΚΕΦΑΛΑΙΟ 6 ΠΡΩΤΟΚΟΛΛΟ ΜΗΔΕΝΙΚΗΣ ΓΝΩΣΗΣ ΒΑΣΙΣΜΕΝΟ ΣΤΗ ΘΕΩΡΙΑ ΓΡΑΦΩΝ

6.1 ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ

Το πρωτόκολλο αυτό δημιουργήθηκε από τους Goldreich, Michali και Wigderson [4] και βασίζεται στη θεωρία του ισομορφισμού γράφων η οποία μας λέει ότι δυο γράφοι είναι ισομορφισμοί αν υπάρχει μια αμφιμονοσήμαντη αντιστοιχία f από τους κόμβους του G στους κόμβους του H έτσι ώστε να υπάρχει ακμή uv στον γράφο G αν και μονό εάν υπάρχει ακμή f(u) ,f(v) στον H(u,v κόμβοι του G).

Στο πρωτόκολλο αυτό ο μάρτυρας θέλει να δείξει στον επιβεβαιωτή ότι γνωρίζει τον ισομορφισμό δύο γράφων G1 ,G2.Για να το πετύχει αυτό δημιουργεί έναν γράφο H ο οποιός είναι ισόμορφος με το G1 αυτό επιτυγχάνεται με αντιμετάθεση στοιχείων του G1. Ο H θα είναι ισομορφικός με τον G1 και κατ επέκταση και με τον G2.

Στην συνέχεια στέλνει αυτόν τον γράφο H στον επιβεβαιωτή

Μάρτυράς →επιβεβαιωτής : H

Έπειτα ο επιβεβαιωτής επιλέγει την τυχαία πρόκληση b€{1,2} την οποία στέλνει στον μάρτυρα

Επιβεβαιωτή → μάρτυρα:b

Έπειτα ο μάρτυρας υπολογίζει τον ισομορφισμό του Gb και του H και τον στέλνει στον επιβεβαιωτή.

Και τέλος ο επιβεβαιωτής ελέγχει αν ο ισομορφισμός είναι σωστός.

Το πρωτόκολλο αυτό επαναλαμβάνεται n φορές.

Η πιθανότητα για επιτυχής πλαστογραφία είναι 2^{-n} .

Ο επιβεβαιωτής εφόσον έχει στην κατοχή του μόνο τον ισομορφισμό μεταξύ του Gi και H δεν μπορεί να υπολογίσει κανέναν άλλο ισομορφισμό μεταξύ των τριών γράφων.

<u>*Παράδειγμα*</u>

Η Πάτυ επιλέγει μυστικά το γράφο G1={1,4,5,7,2,6} και στην συνέχεια στέλνει στον Τομ τον H={1,4,5,7,2,6}.

Ο Τομ στη συνέχεια επιλέγει το bι=1 κι το στέλνει στην Πάτυ.

Έπειτα η Πάτυ υπολογίζει τον ισομορφισμο του Gb ={1,4,5,7,2,6} και του H={1,4,5,7,2,6}.

Τρ.οπος 2:

Η Πάτυ υπολογίζει τον π={2,4,1,3,5}.Αυτή στέλνει τον H=π 0G1={2,4,1,3,5} στον Τομ

Ο Τομ επιλέγει b=2 και ον στέλνει στην Πάτυ.

Η Πάτυ υπολογίζει ρ=π0σ={2,4,1,3,5}0{5,4,3,2,1}={4,2,5,3,1} και τα στέλνει στον Τομ.

Ο Τομ υπολογίζει τον H={2,4,1,3,5} =p0G2={4,2,5,3,1}0{1,2,3,4,5} ={4,2,5,3,1}.

Παρατρούμε οτί όταν ο Τομ έχει να υπολογίσει για b=1 ισχύει H = π0 *G*ι το οποίο σημαίνει ότι ο H είναι ισομορφικός του G1 . Όταν ο b=2 η Πάτυ δείχνει ότι το H= π0G1 είναι ισομορφικό του (π0σ) 0 G2 , κ.τ.λ

ΚΕΦΑΛΑΙΟ 7: ΠΡΩΤΟΚΟΛΟ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ ΤΟΥ ΟΚΑΜΟΤΟ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΠΡΩΤΟΚΟΛΩΝ

7.1 ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΠΡΩΤΟΚΟΛΟΥ ΟΚΑΜΟΤΟ

Το πρωτόκολλο αυτό αναπτύχτηκε από τον T. Okamoto το 1992.[4]

Πρώτα η οντότητα Τ επιλέγει ένα πρώτο αριθμό p καθώς επίσης και ένα μεγάλο πρώτο διαιρέτη q του p-1. Επιπλέον η οντότητα Τ επιλέγει δυο στοιχεία α1 ,α2 τα οποία έχουν τάξη q και ένα στοιχείο c με $a2=a_1^{\xi} \bmod p$.

Τέλος η οντότητα Τ επιλέγει δύο αλγόριθμους , τον sig_t για υπογραφή και τον ver_t για επικύρωση καθώς και έναν αριθμό τ , για τον οποίο ισχύει $2^{\tau}<q$. Οι παράμετροι α1, α2 και το t δημοσιοποιούνται ενώ οι παράμετροι sigt και η σταθερά c δημοσιοποιούνται από την Τ.

Έστω ότι ένα μέλος θέλει να γραφτεί στο σύστημα. Πρέπει να επιλέξει δύο αριθμούς d1 ,d2 £ Z_q και στην συνέχεια υπολογίζει την ποσότητα

$U= d_1^{a1} * d_2^{a2} \bmod p$ και στην συνέχεια την στέλνει στην οντότητα Τ.

Έπειτα η οντότητα Τ παράγει την υπογραφή s η οποία αποτελείται από την υπογραφή της οντότητας Τ , την ταυτότητα του μέλους Α καθώς και το U.

S=sigt(ID(A) ,U)

Και δημοσιοποιεί το πιστοποιητικό για την οντότητα Α που περιλαμβάνει την ταυτότητα του μέλους Α το u καθώς και υπογραφή s

Certa= ((ID (A), u, s).

Στην συνέχεια ο επιβεβαιωτής για την αυθεντικοποίηση επιλέγει δύο αριθμούς k1 ,k2 €Z_q και υπολογίζει την τιμή $w= d_1^{k1} * d_2^{k2} \bmod p$ και στην συνέχεια στέλνει την τιμή w και το πιστοποιητικό του μέλους Α δηλαδή το c (a) στον μάρτυρα.

Στην συνέχεια ο μάρτυρας ελέγχει την εγκυρότητα του πιστοποιητικού c(a) και επιλέγει μια τυχαία τιμή έστω r για την οποία ισχύει $1 \le r \le 2^t$ και την αποστέλλει στον επιβεβαιωτή .

Ο επιβεβαιωτής με τη σειρά υπολογίζει τις τιμές y1 και y2 και τις στέλνει στον μάρτυρα .

$y_1= k1 + a1r \bmod q$

$y_{2=}k2+ a2r \bmod q$

Τέλος ο μάρτυρας επιβεβαιώνει εάν ισχύει η ακόλουθη σχέση

$W= a1^{y1} a2^{y2} u^{r} \bmod q$.

7.2 ΕΦΑΡΜΟΓΕΣ ΟΛΩΝ ΤΩΝ ΠΡΩΤΟΚΟΛΩΝ ΜΗΔΕΝΙΚΗΣ ΓΝΩΣΗΣ

Τα πρωτόκολλα μηδενικής γνώσης χρησιμοποιούνται σε περιπτώσεις που χρειάζεται να γίνει αυθεντικοποίηση σε κάποια οντότητα χωρίς να υπάρχει εμπιστοσύνη ότι το μυστικό δεν θα διαρρεύσει [1,5,4].

Το πιο χαρακτηριστικό παράδειγμα είναι τα ATM καθώς και οι έξυπνες κάρτες . Η τράπεζα που εξέδωσε την κάρτα δεν θέλει ο κωδικός της κάρτας να διαρρεύσει σε ένα οποιοδήποτε ATM , διότι μπορεί κάποιος να το έχει πειράξει προκειμένου να κλέψει τους κωδικούς καρτών. Έτσι λοιπόν η κάρτα αναλαμβάνει να αποδείξει στο ATM ότι προέρχεται από μια τράπεζα χωρίς να αποκαλύψει το μυστικό της κλειδί .

Επίσης μια άλλη εφαρμογή των πρωτοκόλλων είναι στην έξυπνη κάρτα . Η έξυπνη κάρτα μοιάζει εξωτερικά με πιστωτική κάρτα εσωτερικά διαφέρει από αυτήν . Η πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία (magnetic stripe), στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη. Η έξυπνη κάρτα, αντίθετα, ενσωματώνει ένα μικροεπεξεργαστή ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Η βασική διαφορά των δύο τύπων καρτών είναι ότι, ενώ τα δεδομένα στη μαγνητική ταινία είναι εύκολο να παραλλαχθούν ή και να διαγραφούν (ακόμη και τυχαία), αυτό δεν είναι δυνατό στην έξυπνη κάρτα, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη: Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια. Η τροφοδοσία της κάρτας με ενέργεια εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας (smart card reader), στον οποίο εισάγεται η κάρτα προκειμένου να χρησιμοποιηθεί. Αυτός μπορεί να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη, προκειμένου να εξασφαλιστεί η πρόσβαση σε δεδομένα. Η έξυπνη κάρτα χρησιμοποιείται κυρίως σε τραπεζικές συναλλαγές , σε συναλλαγές με υπηρεσίες κοινής ωφέλειας(στην Γερμανία κάθε ασφαλισμένος διαθέτει έξυπνη κάρτα περίθαλψης) καθώς και σε συστήματα απαγόρευσης πρόσβασης σε μη εξουσιοδοτημένο προσωπικό.

Μια άλλη επίσης πολύ σημαντική εφαρμογή των πρωτοκόλλων μηδενικής γνώσης είναι η ψηφοφορία μέσω διαδικτύου 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

- *Επικύρωση. Πριν την υποβολή της ψήφου ελέγχεται η ταυτότητα των*

Ψηφοφόρων

- Υποβολή Ψήφου. Οι ψηφοφόροι υποβάλλουν την ψήφο τους. Μόνο μια

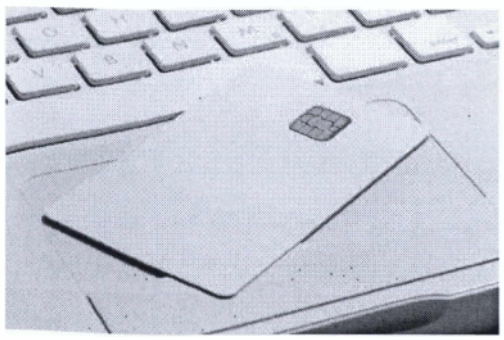
ψήφος επιτρέπεται για κάθε ψηφοφόρο.

- Καταμέτρηση Ψήφων. Μόλις εκπνεύσει η προθεσμία υποβολής ψήφων,

οι ψήφοι καταμετρούνται και ανακοινώνεται το αποτέλεσμα των εκλογών.

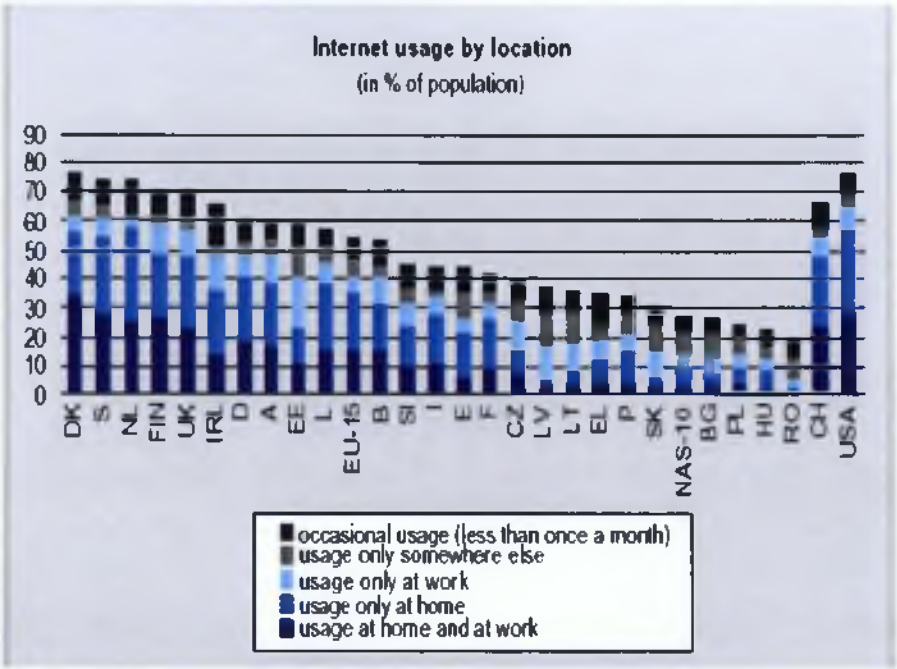
Η ψηφοφορία μέσω Διαδικτύου απαιτεί ένα μμεγαλύτερο επίπεδο ασφάλειας από αυτό που απαιτείται σε συνήθεις συναλλαγές ηλεκτρονικού εμπορίου.

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 αντιμετωπίζεται σε μεγάλο βαθμό με τις τεχνικές των πρωτοκολλων μηδενικής γνώσης .Το ηλεκτρονικό σύστημα ψηφοφορίας δεν είναι τοσό διαδεδομένο στην Ελλάδα όσο στο εξωτερικό.



Έξυπνη κάρτα

Κάρτα ATM



ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ ΣΤΙΣ ΧΩΡΕΣ ΤΗΣ Ε.Ε

ΚΕΦΑΛΑΙΟ 8: ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΒΙΒΛΙΟΓΡΑΦΙΑ

8.1 ΣΥΜΠΕΡΑΣΜΑ

Στην εργασία αυτή προσπαθήσαμε να αναλύσουμε τις τεχνικές που χρησιμοποιούν τα πρωτόκολλα μηδενικής γνώσης προκειμένου να μεταφέρουν μια πληροφορία με ασφάλεια.

Καταλήγουμε λοιπόν στο συμπέρασμα ότι εάν τα κλειδιά η τα μηνύματα δεν αλλάζουν συχνά ένας κακόβουλος ωτακουστής μπορεί πολύ εύκολα να βρει το μυστικό κάνοντας επίθεση στις ηχογραφημένες συνομιλίες .Ειδικά στην περίπτωση που το μέγεθος του κλειδιού είναι μικρό επομένως όχι και τόσο ισχυρό κυρίως λόγω του περιορισμού υλικού που υπάρχει στον πραγματικό κόσμο ,υπάρχει σοβαρό πρόβλημα .

Είναι εμφανές από την μελέτη αυτή ότι σε εφαρμογές που απαιτείται πραγματική ασφάλεια πρέπει να έχουμε αρκετά μεγάλο υπολογιστική μνήμη καθώς και να έχουν επιλέξει συστήματα ενσωματωμένου ελέγχου ώστε να λειτουργούν με την πλήρη δύναμη των πρωτόκολλων κρυπτογράφησης.

Τέλος συνδυάζοντας τη δύναμη των πρωτοκόλλων, τα κλειδιά σας και το υλικό και να είναι σε θέση να ισορροπήσει έχουμε ένα σύστημα που μπορεί να ανταποκριθεί στις πραγματικές ανάγκες σας και αυτό είναι ακόμα πιο σημαντικό από ότι στις παραδοσιακές εφαρμογές της κρυπτογραφίας.

8.2 ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Τεχνικές κρυπτογραφίας και κρυπτανάλυσης εκδόσεις Κάτος Α.Β page331-339

[2]A practical zero –knowledge protocol fitted to security microprocessor minimizing both transmission and memory Louis C. Guillou and Jeans-Jasques Quisquater

[3] Digital Certificates and the Feige-Fiat-Shamir zero-knowledge protocol , Daniele Raffo Supervisor: François Morain, July 11, 2002

[4] Κωνσταντίνος Πατσάκης, Ευάγγελος Φούντας, «Κρυπτογραφία και Εφαρμογές, Τόμος Β» , εκδόσεις Varmar, 200A. Fiat, A. Shamir, σελ.156-311

[5] "How to prove yourself: Practical solutions

to identification and signature problems", Advances in

Cryptology, Crypto86, Lecture Notes in Computer Science,

vol. 263 ed. A. Odlyzko, Springer-Verlag, Santa Barbara,

CA, 19879.