Κρυπτογραφία

Εργαστηριακό μάθημα 9 (Πρωτόκολλα πιστοποίησης ταυτότητας μηδενικής γνώσης – Fiat-Shamir)

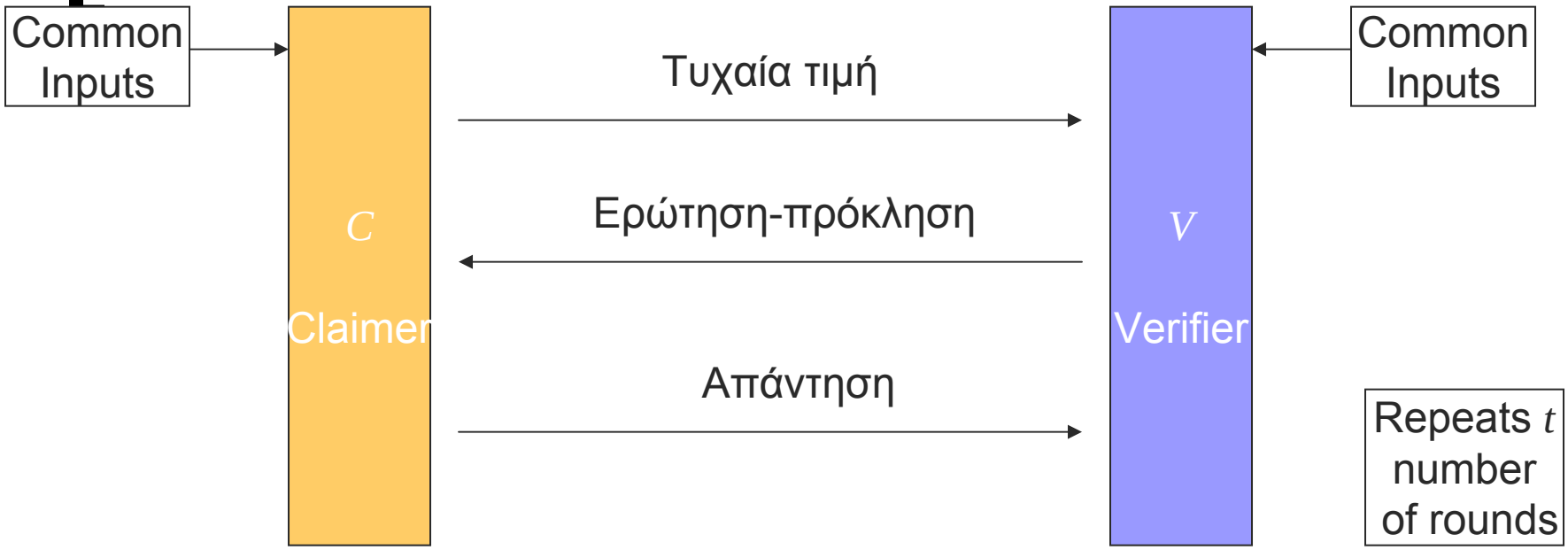
Πρωτόκολλα μηδενικής γνώσης

- Βασική ιδέα: Ένας χρήστης Α (claimant) αποδεικνύει την ταυτότητά του σε κάποιον άλλο Β (verifier) αποδεικνύοντάς του ότι κατέχει μία μυστική γνώση, χωρίς όμως να αποκαλύπτει τη γνώση αυτή. Αυτό επιτυγχάνεται με το να απαντά σε μία «ερώτηση-πρόκληση» του verifier, η απάντηση της οποίας εξαρτάται, εκτός από την ερώτηση, και από τη μυστική γνώση.
- Πρωτόκολλα με αυτά τα χαρακτηριστικά ονομάζονται μηδενικής γνώσης (zero-knowledge (ZK))

Γενικά χαρακτηριστικά πρωτοκόλλων ZK

- Ο Α (claimant) από το ιδιωτικό του κλειδί (μυστική πληροφορία που την κατέχει μόνο αυτός), παράγει τυχαία μία πληροφορία-βεβαίωση (witness). Ο Α στέλνει την βεβαίωση στον Β (verifier)
- Με βάση την βεβαίωση, ο Β κάνει μία ερώτηση-πρόκληση (challenge) στον Α. Το πρωτόκολλο πρέπει να είναι έτσι σχεδιασμένο ώστε μόνο κάποιος που κατέχει το μυστικό κλειδί του Α να μπορεί να απαντήσει σωστά σε όλες τις προκλήσεις, ενώ επίσης να μην μπορεί να εξαχθεί καμία πληροφορία για το ιδιωτικό κλειδί του Α από τις απαντήσεις.
- Ο Α στέλνει στον Β την απάντηση (response) στην πρόκληση. Ο Β πρέπει να είναι σε θέση να επιβεβαιώσει την ορθότητα της απάντησης.

Σχηματική αναπαράσταση



- *Και οι δύο έχουν κάποια πληροφορία από κοινού (common inputs)*
- Αν όλες οι απαντήσεις είναι αποδεκτές (δηλαδή σωστές), γίνεται η πιστοποίηση ταυτότητας

Σχήμα πιστοποίησης ταυτότητας Fiat-Shamir

Έστω ***N=p×q****, όπου* ***p,q*** είναι πολύ μεγάλοι πρώτοι αριθμοί (το N τουλάχιστον 512 bits)

O claimant A ***επιλέγει τυχαία s μικρότερο του N και υπολογίζει υ*** τέτοιο ώστε:

- $\upsilon = s^2 \pmod N$

Δημόσιο κλειδί : ***N, υ (τα ξέρει και ο Verifier)***

ιδιωτικό κλειδί : ***s (το ξέρει μόνο ο Claimant)***

Σχήμα πιστοποίησης ταυτότητας Fiat-Shamir (II)

- Κάθε φορά, ο C γεννάει έναν τυχαίο αριθμό r και αποστέλλει στον V τον αριθμό $x=r^2 \bmod N$.
- Ο V αποστέλλει στον C έναν αριθμό e, είτε 0 είτε 1
- Ο C υπολογίζει τον αριθμό $y=rs^e \bmod N$ και τον στέλνει στον V. Αφού μόνο ο C ξέρει το s, είναι ο μόνος που μπορεί να υπολογίσει το y
- Ο V κάνει, από το y που λαμβάνει, τον υπολογισμό $y^2 \bmod N$. Αν ισχύει $y^2=xu^e \pmod N$ τότε επιβεβαιώνει την ταυτότητα του C.
  - Πράγματι, $y^2=r^2s^{2e} \pmod N = x\, u^e \pmod N$

Fiat-Shamir (διάγραμμα)

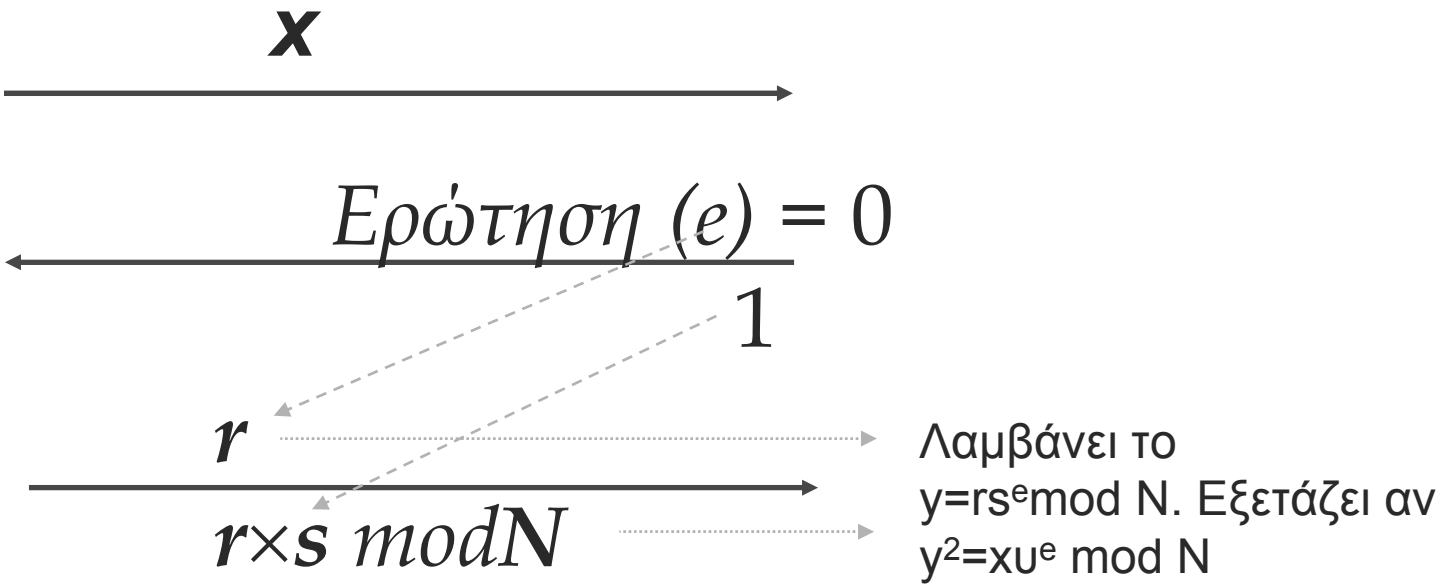
Claimant (C)

N*, *s*, *u

Verifier (V)

N

Σε κάθε βήμα, επιλογή τυχαίου αριθμού **r** **μικρότερου του** N και $x=r^2 \bmod N$ **(witness)**



Παράδειγμα

- $N=17 \times 19 = 323$
- $s=25$
- $u=s^2 \bmod N = 302$
- Γέννηση τυχαίου αριθμού $r=12$ και αποστολή του $x=r^2 \bmod N = 144$
- Ο V στέλνει τον αριθμό $e=1$
- Ο C απαντάει με τον $y=rs^e \bmod N =$
  $12 \times 25 \bmod 323 = 300$
- Ο V υπολογίζει τον αριθμό $y^2 \bmod N = 206$ και εξετάζει αν ισούται με τον $xu^e \pmod N = 144 \times 302 \bmod 323 = 206$ (άρα, αποδεκτή η απάντηση $y=300$ του C).

Σχόλια πάνω στον Fiat – Shamir

- Ένας επιτιθέμενος που θέλει να προσποιηθεί ότι είναι ο C, μπορεί να επιλέξει τυχαίο r, να στείλει $x=r^2/u$ και σε κάθε πρόκληση e=1 να απαντά y=r, κάτι που ο V θα το ανιχνεύει ως σωστή απάντηση. Όμως δεν θα μπορεί να απαντήσει σωστά για e=0.

Σχόλια πάνω στον Fiat – Shamir (2)

- Ένας επιτιθέμενος που θέλει να προσποιηθεί ότι είναι ο C, μπορεί να επιλέξει τυχαίο r, να στείλει $x=r^2$ και σε κάθε πρόκληση e=0 να απαντά y=r, κάτι που ο V θα το ανιχνεύει ως σωστή απάντηση. Όμως δεν θα μπορεί να απαντήσει σωστά για e=1.

Σχόλια πάνω στον Fiat – Shamir (3)

- Με βάση τις προηγούμενες δύο διαφάνειες, καταλήγουμε ότι πάντα θα μπορεί κάποιος να ξεγελάσει το σύστημα, αρκεί να ξέρει από πριν ποια θα είναι η ερώτηση e που θα κάνει ο Verifier (το οποίο όμως δεν το ξέρει!!). Για αυτό ακριβώς είναι πολύ κρίσιμο το ότι πρώτα ο Claimant στέλνει το witness x και μετά δέχεται την ερώτηση/πρόκληση e. Τη στιγμή που στέλνει το x, δεν ξέρει ποια ερώτηση θα δεχτεί μετέπειτα, ως εκ τούτου δεν ξέρει ποιο x να στείλει ($x=r^2/v$ ή $x=r^2$) για να ξεγελάσει τον Verifier.
- Γίνεται κατανοητό λοιπόν γιατί ο «διάλογος» μεταξύ των δύο γίνεται πολλές φορές προτού ο Verifier εγκρίνει πρόσβαση στον Claimant, έτσι ώστε να ελαχιστοποιηθεί η πιθανότητα εξαπάτησης (δηλαδή η πιθανότητα ο εχθρός να μαντεύει συνέχεια σωστά το e)

Σχόλια πάνω στον Fiat-Shamir

- Δεν πρέπει να χρησιμοποιείται πάνω από μία φορά το ίδιο r, γιατί με αυτό τον τρόπο ένας εισβολέας μπορεί να παρακολουθεί τη συνομιλία, να μάθει τις απαντήσεις του claimant για τις εκάστοτε ερωτήσεις του verifier και να τις επαναλάβει

Ασφάλεια Fiat-Shamir

Έγκειται στην παραγοντοποίηση:

- ένας αλγόριθμος που «σπάει» τον *Fiat-Shamir είναι ισοδύναμος με έναν αλγόριθμο που παραγοντοποιεί τον* ***N.*** Κι αυτό γιατί για να βρει κάποιος το ιδιωτικό κλειδί s από τα υ, Ν πρέπει να γνωρίζει τα p,q (αυτό έχει εξηγηθεί στη θεωρία, κατά την περιγραφή του αλγορίθμου Rabin, και δεν θα αναλυθεί περαιτέρω εδώ στο εργαστήριο)

Εφαρμογές του Fiat-Shamir πρωτοκόλλου

- VideoCrypt (κρυπτογράφηση αναλογικού τηλεοπτικού σήματος – π.χ. Filmnet).
- Σε εφαρμογές e-voting