Κρυπτογραφικά Πρωτόκολλα

Παναγιώτης Γροντάς

05/12/2017

ΕΜΠ - Κρυπτογραφία - (2017-2018)

Το πρόβλημα

- m παίκτες θέλουν να υπολογίσουν από κοινού την τιμή της συνάρτησης $f(x_1, x_2, \cdots x_m)$
- Κάθε παίκτης P_i συνεισφέρει την είσοδο x_i
- Γενίκευση: κάθε παίκτης διαθέτει τη δική του συνάρτηση f_i, αλλά χρειάζεται είσοδο από όλους
- Μπορεί να γίνει;
    - Χωρίς να αποκαλυφθεί καμία πληροφορία εκτός από το αποτέλεσμα
    - Υποθέσεις ασφάλειας
    - Πολυπλοκότητα: Υπολογισμών / Επικοινωνίας
- Δεν είναι αποδεκτή η χρήση TTP

Το πρόβλημα των εκατομμυριούχων (Yao-1982)

- Δύο εκατομμυριούχοι (Alice, Bob) θέλουν να δουν ποιος είναι πιο πλούσιος
- Χωρίς να αποκαλυφθεί η περιουσία τους
- $f(a, b) =$ if $a < b$ then 1 else 0
- Υπόθεση: $1 \leq a, b \leq n$

Το πρόβλημα των εκατομμυριούχων - Η λύση του Yao

- Ο Bob
    - Δημιουργεί n ταυτόσημα κουτιά (σχήμα δέσμευσης)
    - Διαλέγει έναν αριθμό x και τον τοποθετεί στο κουτί b
    - Στα υπόλοιπα τοποθετεί τυχαίους αριθμούς

Το πρόβλημα των εκατομμυριούχων - Η λύση του Yao

- Ο Bob
    - Δημιουργεί n ταυτόσημα κουτιά (σχήμα δέσμευσης)
    - Διαλέγει έναν αριθμό x και τον τοποθετεί στο κουτί b
    - Στα υπόλοιπα τοποθετεί τυχαίους αριθμούς
- Η Alice
    - Ανοίγει όλες τις δεσμεύσεις
    - Αφήνει τα πρώτα a κουτιά ίδια
    - Προσθέτει 1 στα υπόλοιπα $n - a$
    - Τα στέλνει πίσω στον Bob

Το πρόβλημα των εκατομμυριούχων - Η λύση του Yao

- Ο Bob
    - Δημιουργεί n ταυτόσημα κουτιά (σχήμα δέσμευσης)
    - Διαλέγει έναν αριθμό x και τον τοποθετεί στο κουτί b
    - Στα υπόλοιπα τοποθετεί τυχαίους αριθμούς
- Η Alice
    - Ανοίγει όλες τις δεσμεύσεις
    - Αφήνει τα πρώτα a κουτιά ίδια
    - Προσθέτει 1 στα υπόλοιπα $n - a$
    - Τα στέλνει πίσω στον Bob
- Ο Bob
    - Ελέγχει τα κουτιά
    - Αν στο κουτί b υπάρχει το $x + 1$ είναι πλουσιότερος
    - Αλλιώς: Η Alice είναι

Το πρόβλημα των εκατομμυριούχων - Η λύση του Yao

- Ο Bob
  - Δημιουργεί n ταυτόσημα κουτιά (σχήμα δέσμευσης)
  - Διαλέγει έναν αριθμό x και τον τοποθετεί στο κουτί b
  - Στα υπόλοιπα τοποθετεί τυχαίους αριθμούς
- Η Alice
  - Ανοίγει όλες τις δεσμεύσεις
  - Αφήνει τα πρώτα a κουτιά ίδια
  - Προσθέτει 1 στα υπόλοιπα $n - a$
  - Τα στέλνει πίσω στον Bob
- Ο Bob
  - Ελέγχει τα κουτιά
  - Αν στο κουτί b υπάρχει το $x + 1$ είναι πλουσιότερος
  - Αλλιώς: Η Alice είναι
- Προβλήματα

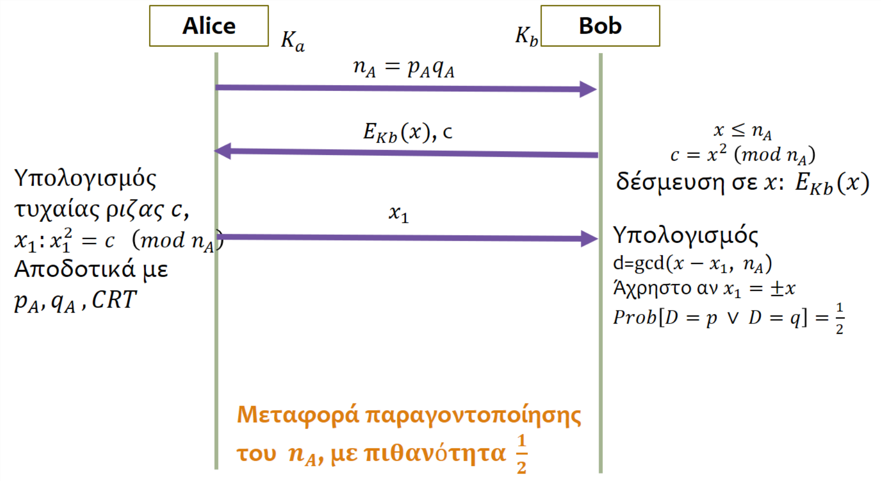
Το πρόβλημα των εκατομμυριούχων - Η λύση του Yao

- Ο Bob
  - Δημιουργεί n ταυτόσημα κουτιά (σχήμα δέσμευσης)
  - Διαλέγει έναν αριθμό x και τον τοποθετεί στο κουτί b
  - Στα υπόλοιπα τοποθετεί τυχαίους αριθμούς
- Η Alice
  - Ανοίγει όλες τις δεσμεύσεις
  - Αφήνει τα πρώτα a κουτιά ίδια
  - Προσθέτει 1 στα υπόλοιπα $n - a$
  - Τα στέλνει πίσω στον Bob
- Ο Bob
  - Ελέγχει τα κουτιά
  - Αν στο κουτί b υπάρχει το $x + 1$ είναι πλουσιότερος
  - Αλλιώς: Η Alice είναι
- Προβλήματα
  - Εκθετικό πλήθος δεσμεύσεων (ως προς τα bits της περιουσίας)
  - Ενεργοί αντίπαλοι (τερματισμός πριν την αποκάλυψη)

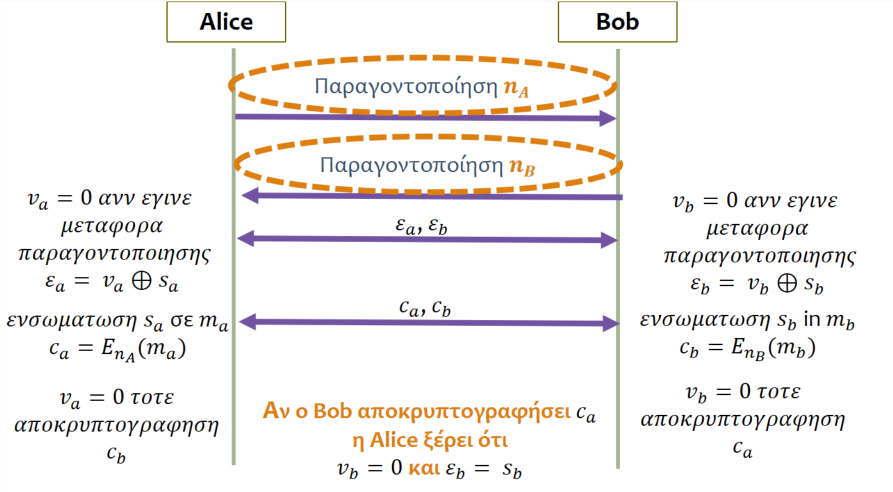
Γενίκευση: ανταλλαγή μυστικών

- Οι Alice, Bob θέλουν να ανταλλάξουν τα μυστικά s_a, s_b χωρίς TTP
- Ταυτόχρονη ανταλλαγή (ο ένας μαθαίνει αν ο άλλος έλαβε το μυστικό)
- Αποφυγή τερματισμού
- Πρόβλημα
    - $s_a = f(a_1, \cdots, a_n)$
    - $s_b = f(b_1, \cdots, b_n)$
    - $\exists k$: ώστε να μπορεί να υπολογιστεί το s_a, αλλά όχι το s_b

Η λύση του Rabin με τετραγωνικά υπόλοιπα i



Η λύση του Rabin με τετραγωνικά υπόλοιπα ii



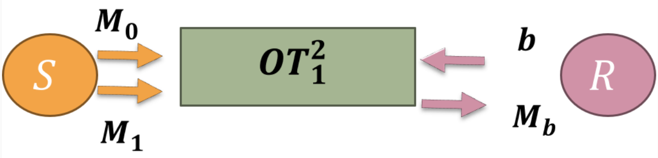
Ορισμός $OT(S, R, M)$ (Even, Goldreich, Lempel)
Μη συνειδητή μεταφορά $OT(S, R, M)$ είναι ένα πρωτόκολλο με το οποίο ο αποστολέας S μεταφέρει ένα μηνυμα M στον παραλήπτη R έτσι ώστε ο R λαμβάνει το μήνυμα με πιθανότητα $1/2$ και:

- Αν ο R δεν λάβει το μήνυμα, δεν μαθαίνει ούτε κάποια χρήσιμη πληροφορία
- Οποιαδήποτε προσπαθεια μη εκτέλεσης του πρωτοκόλλου γίνεται αντιληπτή

Αφαιρετική αναπαράσταση καναλιού με θόρυβο

Παραλλαγή: 1-από-2 Μη-Συνειδητή Μεταφορά

$OT_1^2(S, R, M_1, M_2)$
Ο R επιλέγει μεταξύ δύο μηνυμάτων για μεταφορά με πιθανότητα $1/2$ και ο S το μεταφέρει χωρίς ασφαλώς να γνωρίζει ποιο μετέφερε. Μπορούμε να προσομοιώσουμε την τυχαία επιλογή χρησιμοποιώντας ένα bit.



Άλλες παραλλαγές

$OT_1^n(S, R, M_1, \cdots, M_n)$
Ο R επιλέγει μεταξύ n μηνυμάτων να λάβει το i. Φυσικά ο S δεν το μαθαίνει, ενώ ο R δεν μαθαίνει τα $M_j, j \neq i$

k-από-n Μη-Συνειδητή Μεταφορά

- Ο R λαμβάνει ταυτόχρονα k μηνύματα
- Ο R λαμβάνει σειριακά k μηνύματα που μπορούν να τροποποιηθούν με βάση τα προηγούμενα (adaptive)

Πρακτική κατασκευή OT_1^2

- Χρήση κρυπτοσυστήματος δημοσίου κλειδιού με $\mathcal{M} = \mathcal{C}$
- Τυχαία επιλογή $x_0, x_1 \in \{0,1\}^*$
- Για να ληφθεί το M_0 ο R:
    - Στέλνει στον S το $(Enc(x_0), x_1)$
    - Ο S αποκρυπτογραφεί, παράγοντας το $(x_0, Dec(x_1))$.
    - Τελικά ο S αποστέλλει το $(M_0 \oplus x_0, M_1 \oplus Dec(x_1))$
    - Τελικά ο R ανακτά το M_0 με XOR του πρώτου συστατικού: $M_0 \oplus x_0 \oplus x_0$

- Χρήση *OT* για κατασκευή κυκλώματος C που υπολογίζει ασφαλώς ως προς παθητικό αντίπαλο μια συνάρτηση f
- Οι παίκτες παρέχουν στο C τις εισόδους
- Μαθαίνουν το αποτέλεσμα χωρίς να αποκαλυφθεί οποιαδήποτε ενδιάμεση τιμή ή είσοδος

Βασική ιδέα
Κατασκευή αλλοιωμένων πινάκων τιμών για τις λογικές πύλες του κυκλώματος με χρήση *OT*

Παράδειγμα: Πύλη OR

- Υπολογισμός $x = s\ \boldsymbol{OR}\ r$
- Ο S παρέχει το s
- Ο R παρέχει το r

s	r	s OR r
0	0	0
0	1	1
1	0	1
1	1	1

Figure 1: Αρχικός πίνακας υπολογισμού OR

Παράδειγμα: Garbled OR

- Επιλογή δύο τυχαίων μεταθέσεων $v_s, v_r : \{0,1\} \to \{0,1\}$
- Εφαρμογή στον πίνακα
- Επιλογή 4 ζευγών συναρτήσεων κρυπτογράφησης και αποκρυπτογράφησης $(E_0^S, D_0^S), (E_1^S, D_1^S), (E_0^R, D_0^R), (E_1^R, D_1^R)$
- Εφαρμογή στο αποτέλεσμα της μετάθεσης
- Αποστολή στον R μαζί με τη v_r

s	**r**	**s *OR* r**
$v_s(0)$	$v_r(0)$	$E^S_{v_s(0)}(E^R_{v_r(0)}(0))$
$v_s(0)$	$v_r(1)$	$E^S_{v_s(0)}(E^R_{v_r(1)}(1))$
$v_s(1)$	$v_r(0)$	$E^S_{v_s(1)}(E^R_{v_r(0)}(1))$
$v_s(1)$	$v_r(1)$	$E^S_{v_s(1)}(E^R_{v_r(1)}(1))$

Figure 2: Αλλοιωμένος πίνακας υπολογισμού OR

Υπολογισμός με Garbled OR

- Ο S υπολογίζει το $v_s(s)$
- Στέλνει στον R το ζεύγος $(v_s(s), D^S_{v_s}(s))$
- Ο R υπολογίζει το $v_r(r)$
- Για να αποκρυπτογραφήσει χρειάζεται την συνάρτηση $D^R_{(v_r(r))}$
- Πρέπει να την πάρει από τον S χωρίς να αποκαλυφθεί το $v_r(r)$
- Χρήση $OT^2_1(S, R, D^R_0, D^R_1)$
- Τελικά ο R μπορεί να υπολογίσει το αποτέλεσμα $D^R_{v_r(r)}(D^S_{v_s(s)}(E^S_{v_s(s)}(E^R_{v_r(r)}(x))))$ και να το επιστρέψει στον S.

Γενίκευση

- Αλλοίωση όλων των πυλών
- Για κάθε πύλη
  - Μετάθεση γραμμών πίνακα αλήθειας $\rightarrow$ τυχαία μετάθεση αποτελέσματος
  - Θεώρουμε αποτέλεσμα και εισόδους ως τυχαία κλειδιά
  - Χρειάζονται 6 κλειδιά (4 είσοδοι - 2 αποτέλεσμα)
  - Υπολογισμός πύλης: γνώση κλειδιού αποτελέσματος
  - Τροφοδοσία επόμενης
- Οι τελικές έξοδοι αποκρυπτογραφούνται

Βιβλιογραφία i

1. St. Zachos and Aris Pagourtzis. Στοιχεία Θεωρίας Αριθμών και Εφαρμογές στην Κρυπτογραφία. Πανεπιστημιακές Σημειώσεις
2. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography 2nd edition, Chapman and Hall/CRC, 2015
3. M. Ben-Or, S. Goldwasser and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation," Proceedings of the 20th Annual ACM Symposium on Theory of Computing, Chicago, 1988, pp. 1-10.
4. Yao, A. C. "Protocols for secure computations" (FOCS 1982): 160–164
5. Rabin M. O. "How to exchange secrets by oblivious transfer." ,TR-81, Harvard University, 1981
6. S. Even, O. Goldreich, and A. Lempel. 1985. A randomized protocol for signing contracts. Commun. ACM 28, 6 (June 1985), 637-647
7. Claude Crépeau. 1987. Equivalence Between Two Flavours of Oblivious Transfers. In A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology (CRYPTO '87, UK, 350-354.
8. Yehuda Lindell and Benny Pinkas. 2009. A Proof of Security of Yao's Protocol for Two-Party Computation. J. Cryptol. 22, 2 (April 2009), 161-188 Ostrofski R., CS 282A/MATH 209A: Foundations of Cryptography, Lecture 10, Oblivious Transfer
9. Gabriel Bender, Cryptography and Secure Two-Party Computation, August 21, 2006
10. Ronald Cramer, Ivan Damgård, Jesper Buus Nielsen Multiparty Computation, an Introduction