Εργασία Κρυπτογραφίας– Απρίλιος 2023

Παράδοση: Παρασκευή 28/4/2023 1:00μμ

Οδηγίες:

- Όπου απαιτούνται πράξεις, θα πρέπει να εξηγείτε τους υπολογισμούς σας.
- Να απαντάτε στο ζητούμενο με σαφήνεια, και να εξηγείτε τη σκέψη σας.

1. Εξετάστε τις παρακάτω παραλλαγές για το σχήμα του Pedersen. Για κάθε μία ελέγξτε εάν διατηρούνται οι ιδιότητες της δέσμευσης και της απόκρυψης.

   (α□) Αλλάζουμε το χώρο μηνυμάτων $\mathcal{M}$ ώστε να γίνονται δεκτά μόνο $m \in \{0, 1\}$.

   (β□) Αλλάζουμε την επιλογή της τυχαίας τιμής r στην Com ώστε να έχουμε $r \leftarrow \{0, 1\}$.

   (γ□) Στις παραμέτρους, θέτουμε $h \leftarrow g$.

   (α□) Αλλάζουμε το χώρο μηνυμάτων $\mathcal{M}$ ώστε να γίνονται δεκτά μόνο $m \in \{0, 1\}$.

   Παρατηρούμε ότι ο ορισμός της δέσμευσης αλλά και της απόκρυψης προβλέπει ότι τα m_0, m_1 επιλέγονται από τον αντίπαλο. Οπότε, αν υπάρχει αντίπαλος $\mathcal{A}$ ο οποίος παραβιάζει μια από τις δύο ιδιότητες για τον περιορισμένο χώρο μηνυμάτων, ο ίδιος αντίπαλος παραβιάζει την ίδια ιδιότητα και για τον πλήρη χώρο.

   (β□) Αλλάζουμε την επιλογή της τυχαίας τιμής r στην Com ώστε να έχουμε $r \leftarrow \{0, 1\}$.

   Η δέσμευση δεν πλήττεται. Με ανάλυση όπως παραπάνω, κάθε αντίπαλος που επιτυγχάνει στον περιορισμένο χώρο, επιτυγχάνει και στον πλήρη.

   Η απόκρυψη όμως παύει να ισχύει. Υπάρχουν μόλις δύο δεσμεύσεις για κάθε m, και, αφού ο χώρος των μηνυμάτων είναι μεγάλος, οι πιθανές δεσμεύσεις για δύο διαφορετικά μηνύματα είναι σχεδόν πάντα σύνολα με μηδενική τομή (πιο συγγεκριμένα, έχουμε μη μηδενική τομή ανν οι λογάριθμοι των h^{m_0}, h^{m_1} έχουν διαφορά 1). Οπότε, μπορούμε εύκολα να περιγράψουμε έναν αντίπαλο που επιλέχει δύο τυχαία m_0, m_1. Η πιθανότητα να είναι η διαφορά 1 είναι η πιθανότητα να ισχύει:

   $$(m_0 - m_1) \cdot t = 1 \mod q \quad \text{ή} \quad (m_1 - m_0) \cdot t = 1 \mod q$$

   Άρα πρέπει το $(m_0 - m_1)$ να είναι ο αντίστροφος του t ή ο αντιθετός του. Αυτό συμβαίνει με πιθανότητα $\frac{2}{q}$, και επιπλέον μπορεί να ελεγχθει από τον $\mathcal{A}$ ώστε να αλλάξει επιλογές.

   (γ□) Στις παραμέτρους, θέτουμε $h \leftarrow g$.

   Αυτή η αλλαγή είναι αντίστοιχη με το να θέσουμε $t = 1$ και να το γνωστοποιήσουμε στον αντίπαλο από πριν.

   Η δέσμευση δεν ισχύει πλέον, αφού ο αντίπαλος μπορεί πχ να θέσει επιλέξει τυχαία (m_1, r_1) με περιορισμό $m_1 \neq r_1$ και να θέσει $(m_2, r_2) = (r_1, m_1)$.

   Η απόκρυψη όπως είχαμε αναλύσει ισχύει και όταν ο αντίπαλος επιλέγει την τιμή του t άρα δεν είναι δυνατό να παραβιαστεί: το να σταθεροποιήσουμε $t = 1$ εν γνώσει του αντιπάλου είναι υποπερίπτωση του να αφήσουμε τον αντίπαλο να διαλέξει, οπότε βάσει της προηγούμενης ανάλυσης το σχήμα είναι ασφαλές ως προς την απόκρυψη.

2. Μία παρέα φοιτητών θέλει να παίξει ένα επιτραπέζιο παιχνίδι, αλλά ανακαλύπτει ότι δεν έχει στη διάθεσή της εξάπλευρα ζάρια.

   Η Μαρία προτείνει να χρησιμοποιήσουν κέρματα ως εξής: αντί για ένα ζάρι θα ρίχνονται 3 ανεξάρτητα και αμερόληπτα κέρματα, όπου κάθε πλευρά με όψη «κεφάλι» θα ισοδυναμεί με 0 και κάθε πλευρά με όψη «γράμματα» θα ισοδυναμεί με 1. Το αποτέλεσμα θα είναι το άθροισμα των όψεων συν 2.

   Η Στέλλα, προτείνει να χρησιμοποιήσουν 5 κέρματα συν 1 (με τις ίδιες αξίες ανα όψη).

(α□) Υπολογίστε τη μέση τιμή κάθε κατανομής: ζάρι, 3 κέρματα +2, 5 κέρματα +1.

(β□) Με τη βοήθεια της στατιστικής απόστασης, υπολογίστε ποιά πρόταση είναι καλύτερη.

(α□) Και στις 3 περιπτώσεις είναι 3.5 μετά από υπολογισμούς. Αν μια από τις δύο εναλακτικές είχε διαφορετική μέση τιμή, θα ήταν μια ένδειξη ότι δεν είναι καλή προσέγγιση για το ζάρι.

(β□) Με τη βοήθεια της στατιστικής απόστασης, υπολογίστε ποιά πρόταση είναι καλύτερη.

Έχουμε να υπολογίσουμε δύο αποστάσεις, πρώτον την $\Delta[Z, M]$ και την $\Delta[Z,]$.

Για κάθε μια από τις επιλογές, προετοιμάζουμε τις πιθανότητες ανα ενδεχόμενο.

Για το ζάρι έχουμε Pr $= [Z = t] = \frac{1}{6}$ για t=1,2,3,4,5,6.

Για τη Μαρία έχουμε: Pr$[M = 1] = 0$, Pr$[M = 2] = \frac{1}{8}$, Pr$[M = 3] = \frac{3}{8}$, Pr$[M = 4] = \frac{3}{8}$, Pr$[M = 5] = \frac{1}{8}$,Pr$[M = 6] = 0$.

Για τη Στέλλα έχουμε: Pr$[M = 1] = \frac{1}{32}$, Pr$[M = 2] = \frac{5}{32}$, Pr$[M = 3] = \frac{10}{32}$, Pr$[M = 4] = \frac{10}{32}$, Pr$[M = 5] = \frac{5}{32}$,Pr$[M = 6] = \frac{1}{32}$

3. Στον ορισμό της απόκρυψης για σχήματα δέσμευσης (¶3.2 σελ 21) ζητάμε ο αντίπαλος να μην μπορεί να "μαντέψει" την τιμή του b Με πιθανότητα σημαντικά καλύτερη από $\frac{1}{2}$. Μπορούμε να περιγράψουμε την ιδιότητα της απόκρυψης με έναν εναλλακτικό τρόπο: ζητάμε κανένας (πολυωνυμικός) αντίπαλος να μην αλλάζει τη συμπεριφορά του ανάλογα με την τιμή του b. Για να το περιγράψουμε και τυπικά, ορίζουμε την παραλλαγή $hiddingattack_x^{\mathcal{B}}$ ως το παιχνίδι $hiddingattack^{\mathcal{B}}$ αλλά στη γραμμή 3 θέτουμε $d \leftarrow x$. Επίσης, ορίζουμε $out_{\mathcal{B}}(hiddingattack_b^{\mathcal{B}}(1^\lambda))$ να είναι η τελευταία έξοδος του $\mathcal{B}$ σε αυτό το παιχνίδι.

Τότε πλέον ορίζουμε την ιδιότητα απόκρυψη* ως εξής:

$$|\text{Prob}[out_{\mathcal{B}}(hiddingattack_0^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(hiddingattack_1^{\mathcal{B}}(1^\lambda)) = 1]| = \text{negl}(1^\lambda)$$

(α□) Δείξτε ότι ο νέος ορισμός είναι ισοδύναμος με τον αρχικό.

Πρώτα επαναδιατυπώνουμε τον αρχικό ορισμό, διαχωρίζοντας περιπτώσεις για το τυχαίο bit b. Για συντομία όπου $hiddingattack^{\mathcal{B}}$ γράφουμε $ha^{\mathcal{B}}$.

$$\begin{aligned}
\text{Prob}[ha^{\mathcal{B}}(1^\lambda) = 1] &= \text{Prob}[ha^{\mathcal{B}}(1^\lambda) = 1 \cap (b = 0)] + \text{Prob}[ha^{\mathcal{B}}(1^\lambda) = 1 \cap (b = 1)] \\
&= \text{Prob}[ha^{\mathcal{B}}(1^\lambda) = 1 | b = 0] \cdot \text{Prob}[b = 0] + \text{Prob}[ha^{\mathcal{B}}(1^\lambda) = 1 \cap (b = 1)] \\
&= \text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 0] \cdot \frac{1}{2} + \text{Prob}[ha^{\mathcal{B}}(1^\lambda) = 1 \cap (b = 1)] \\
&= \frac{1}{2}\left(\text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 0] + \text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1]\right) \\
&= \frac{1}{2}\left(1 - \text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 1] + \text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1]\right) \\
&= \frac{1}{2} - \frac{1}{2}\left(\text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1]\right)
\end{aligned}$$

Εύκολα λοιπόν βλέπουμε ότι όταν ικανοποιείται ο νέος ορισμός, η ποσότητα $|\text{Prob}[out_{\mathcal{B}}(hiddingattack_0^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(hiddingattack_1^{\mathcal{B}}(1^\lambda)) = 1]|$ είναι αμελητέα, άρα και η ποσότητα $\frac{1}{2}(\text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 1])$ που εμφανίζεται παραπάνω. Άρα, όποτε ικανοποιείται ο νέος ορισμός, ικανοποιείται και ο αρχικός.

Μένει να δείξουμε ότι εάν ικανοποιείται ο αρχικός, θα ικανοποιείται και ο νέος. Όταν ικανοποιείται ο αρχικός ορισμός έχουμε:

$$\text{Prob}[ha^{\mathcal{B}}(1^\lambda)] \leq \frac{1}{2} + \text{negl}(1^\lambda)$$

$$\frac{1}{2} - \frac{1}{2}\left(\text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1]\right) \leq \frac{1}{2} + \text{negl}(1^\lambda)$$

$$-\frac{1}{2}\left(\text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1]\right) \leq \text{negl}(1^\lambda)$$

$$\frac{1}{2}\left(\text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 1]\right) \leq \text{negl}(1^\lambda)$$

$$\left(\text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 1]\right) \leq \text{negl}(1^\lambda)$$

Από τον παραπάνω υπολογισμό έχουμε μέρος του ζητουμένου.

Έστω $AM = \left(\text{Prob}[out_{\mathcal{B}}(ha_1^{\mathcal{B}}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(ha_0^{\mathcal{B}}(1^\lambda)) = 1]\right)$. Ξέρουμε λοιπό ότι το AM είναι αμελητέο αλλά το ζητούμενο για να ικανοποιείται ο νέος ορισμός είναι να δείξουμε ότι το $|AM|$ είναι αμελητέο. Αρκεί συνεπώς, να δείξουμε ότι το $-AM$ είναι αμελητέο.

Όσα έχουμε γράψει ως τώρα ισχύουν για έναν οποιοδήποτε πολυωνυμικό αντίπαλο $\mathcal{B}$. Για να ολοκληρώσουμε την απόδειξη, επιστρέφουμε στον αρχικό ορισμό, και επαναλαμβάνουμε την διερεύνηση για ένα αντίπαλο $\mathcal{B}'$ ο οποίος επιστρέφει την τιμή 0 όποτε ο $\mathcal{B}$ επιστρέφει 1 και αντίστροφα. Προφανώς θα συμπεράνουμε ότι η αντίστοιχη ποσότητα AM' θα είναι αμελητέα, δηλαδή $AM' = \left(\text{Prob}[out_{\mathcal{B}}(ha_1^{B'}(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{B}}(ha_0^{B'}(1^\lambda)) = 1]\right)$. Όμως από κατασκευή $out_{\mathcal{B}}(ha_1^{B'}(1^\lambda)) = 1$ μόνο όποτε $out_{\mathcal{B}}(ha_1^{B}(1^\lambda)) = 0$ και αντίστροφα, οπότε $AM' = -AM$, και άρα το $-AM$ είναι αμελητέο.

4. Συχνά, οι κρυπτογραφικοί ορισμοί επιτρέπουν μια μικρή πιθανότητα ο αντίπαλος να λύσει κάποιο υπολογιστικό πρόβλημα. Δε δίνουν όμως εγγυήσεις για την κατανομή αυτής της πιθανότητας. Πχ μπορεί ένας αντίπαλος να λύνει κάθε εκδοχή του προβλήματος με πιθανότητα p ενώ ένας άλλος, να λύνει ένα κλάσμα $1/p$ των εκδοχών του προβλήματος με πιθανότητα 1. Δείξτε ότι στο πρόβλημα του διακριτού λογαρίθμου, αυτό το ζήτημα ουσιαστικά δεν υπάρχει.

   (α□) (Μόνο προπτυχιακοί). Έστω ένας πολυωνυμικός αλγόριθμος $\mathcal{E}$ ο οποίος υπολογίζει διακριτούς λογάριθμους με μη αμελητέα πιθανότητα p οταν ο διακριτός λογάριθμος του στοιχείου που δίνεται είναι άρτιος και με πιθανότητα 0 όταν είναι περιττός. Περιγράψτε έναν πολυωνυμικό αλγόριθμο που υπολογίζει διακριτούς λογαρίθμους με μη αμελητέα πιθανότητα για κάθε στοιχείο.

   (β□) Δείξτε τη γενική περίπτωση του παραπάνω: δηλαδή αν ισχύει[1] ότι $\text{Prob}[h \leftarrow \mathbb{G}; E(\mathbb{G}, g, q, h) = x : g^x = h] = p$, οπου p μη αμελητέο τότε μπορούμε να φτιάξουμε αλγόριθμο $\mathcal{D}$ ώστε $min_{h\in\mathbb{G}}(\text{Prob}[h \leftarrow \mathbb{G}; D(\mathbb{G}, g, q, h) = x : g^x = h]) = p'$, οπου p' μη αμελητέο.

   (α□) Χρειαζόμαστε μια μετατροπή μέσω της οποίας τα ερωτήματα που θα κάνουμε στον $\mathcal{E}$ θα είναι άρτια ή περιττά με παρόμοια πιθανότητα, ανεξάρτητα από το h που μας δίνεται. Ο πιο απλός τρόπος, είναι με πιθανότητα $\frac{1}{2}$ να αλλάξουμε το h ώστε να αλλάξει από άρτιο σε περιττό και αντίστροφα (στο αντίθετο ενδεχόμενο διατηρούμε την αρχική τιμή). Για να το κάνουμε αυτό, θέτουμε $h' = h \cdot g$. Ευκολα συμπεραίνουμε ότι γενικά, αν ο λογάριθμος του h είναι λ, όπου λ περιττός, τότε ο λογάριθμος του $g \cdot h$ θα είναι $\lambda + 1 \mod q$ ο οποίος θα είναι άρτιος[2].

   Τυπικά, περιγράφουμε τον ζητούμενο αλγόριθμο παρακάτω:

   Αλγόριθμος $\mathcal{D}(h)$

   $b \leftarrow \{0, 1\}$

[1] Για ευκολία έχουμε σταθεροποιήσει την επιλογή της ομάδας.

[2] Το αντίστροφο δεν ισχύει όταν θεωρήσουμε τον λογάριθμο ως ακέραιο $< q$. Ο $q - 1$ είναι άρτιος (αφού q πρώτος), αλλά και ο επόμενος του είναι άρτιος αφού $q - 1 + q = 0 \mod q$.

$h' \leftarrow h \cdot g^b$
$\lambda' \leftarrow \mathcal{E}(h')$
$\lambda \leftarrow \lambda' - b$
Return λ

Άρα, για h με άρτιους λογάριθμους έχουμε τουλάχιστον $p/2$ πιθανότητα επιτυχίας: αρχικά $1/2$ για να επιλέξουμε να $h' = h$, και όταν καλέσουμε την $\mathcal{E}(h')$ θα πάρουμε τη σωστή απάντηση με πιθανότητα p.

Για h με περιττό λογάριθμο, έχουμε αντίστοιχα πιθανότητα $\frac{1}{2}$ να επιλέξουμε $h' = h \cdot g$ και άρα να "διορθώσουμε" το h, οπότε και στο επόμενο βήμα θα πάρουμε σωστή απάντηση με πιθανότητα p. Τελικά, σε οποιαδήποτε περίπτωση για το h, θα πάρουμε σωστή απάντηση με πιθανότητα $p/2$ η οποία είναι πράγματι μη αμελητέα όταν η p είναι μη αμελητέα.

(β□) Στη γενική περίπτωση το ζητούμενο είναι παρόμοιο: Ενώ η $\mathcal{E}$ έχει τη δυνατότητα σε μερικές εισόδους να μην απαντά ποτέ σωστά, προσπαθούμε να σχεδιάσουμε ένα αλγόριθμο $\mathcal{D}$ που αποδίδει σχετικά καλά σε όλες τις εισόδους. Ένα βήμα προς αυτό είναι όπως παραπάνω, τα ερωτήματα που θα κάνουμε στην $\mathcal{E}$ να είναι ανεξάρτητα από το (αρχικό) h.

Ο κατάλληλος αλγόριθμος είναι ιδιαίτερα απλός: χρησιμοποιούμε τον ψευδοκώδικα του προηγούμενου ερωτήματος με μόνη αλλαγή το $b \leftarrow \{0,1\}$ σε $b \leftarrow \mathbb{Z}_q$. Ευκολα μπορούμε να δείξουμε ότι το h' είναι ομοιόμορφα κατανεμημένο στο $\mathbb{G}$, αφού η στατιστική του απόσταση από την ομοιόμορφη κατανομή στο $\mathbb{G}$ είναι 0. Άρα, στην ανάλυση του $\mathcal{D}$ μπορούμε να συμπεράνουμε ότι η πιθανότητα το $\mathcal{E}(h')$ να είναι σωστό είναι ακριβώς ίση με την πιθανότητα Prob$[z \leftarrow \mathbb{G}; E(\mathbb{G}, g, q, z) = x : g^x = z]$ αφού και στις δύο περιπτώσεις τρέχουμε την $\mathcal{E}$ με είσοδο ομοιόμορφη στο $\mathbb{G}$. Οπότε η πιθανότητα η τιμή του λ' να είναι σωστή είναι p. Θέτοντας $\lambda \leftarrow \lambda' - b$ υπολογίζουμε τον λογάριθμο του h από τον λογάριθμο του $h \cdot g^b$ αφαιρόντας τον λογάριθμο του g^b, δηλαδή το b.