

Ελλειπτικές καμπύλες

Παναγιώτης Γροντάς

ΕΜΠ - Κρυπτογραφία

- Η ομάδα ελλειπτικών καμπυλών
- Κρυπτογραφικά πρωτόκολλα
- Pairings
- Εφαρμογές PBC

Μαθηματικό υπόβαθρο

Γενικά

- Πλούσιο σε ιστορία μαθηματικό αντικείμενο
 - Πρώτη εμφάνιση Διόφαντος 3 αιώνας πΧ (ρητές ρίζες της $y^2 = x^3 - x + 9$)
 - Μελέτη εδώ και 300 έτη

Γενικά

- Πλούσιο σε ιστορία μαθηματικό αντικείμενο
 - Πρώτη εμφάνιση Διόφαντος 3 αιώνας πΧ (ρητές ρίζες της $y^2 = x^3 - x + 9$)
 - Μελέτη εδώ και 300 έτη
- Κρυπτογραφία: 80s (Neil Koblitz, Victor Miller)

Γενικά

- Πλούσιο σε ιστορία μαθηματικό αντικείμενο
 - Πρώτη εμφάνιση Διόφαντος 3 αιώνας πΧ (ρητές ρίζες της $y^2 = x^3 - x + 9$)
 - Μελέτη εδώ και 300 έτη
- Κρυπτογραφία: 80s (Neil Koblitz, Victor Miller)
- Βασίζεται στο πρόβλημα του Διακριτού Λογάριθμου

Γενικά

- Πλούσιο σε ιστορία μαθηματικό αντικείμενο
 - Πρώτη εμφάνιση Διόφαντος 3 αιώνας πΧ (ρητές ρίζες της $y^2 = x^3 - x + 9$)
 - Μελέτη εδώ και 300 έτη
- Κρυπτογραφία: 80s (Neil Koblitz, Victor Miller)
- Βασίζεται στο πρόβλημα του Διακριτού Λογάριθμου
 - Αντικατάσταση του \mathbb{Z}_p με σημεία τους

Γενικά

- Πλούσιο σε ιστορία μαθηματικό αντικείμενο
 - Πρώτη εμφάνιση Διόφαντος 3 αιώνας πΧ (ρητές ρίζες της $y^2 = x^3 - x + 9$)
 - Μελέτη εδώ και 300 έτη
- Κρυπτογραφία: 80s (Neil Koblitz, Victor Miller)
- Βασίζεται στο πρόβλημα του Διακριτού Λογάριθμου
 - Αντικατάσταση του \mathbb{Z}_p με σημεία τους
 - Μόνο γενικευμένοι αλγόριθμοι DLP $O(2^{\frac{\lambda}{2}})$ - όχι υποεκθετικοί

Γενικά

- Πλούσιο σε ιστορία μαθηματικό αντικείμενο
 - Πρώτη εμφάνιση Διόφαντος 3 αιώνας πΧ (ρητές ρίζες της $y^2 = x^3 - x + 9$)
 - Μελέτη εδώ και 300 έτη
- Κρυπτογραφία: 80s (Neil Koblitz, Victor Miller)
- Βασίζεται στο πρόβλημα του Διακριτού Λογάριθμου
 - Αντικατάσταση του \mathbb{Z}_p με σημεία τους
 - Μόνο γενικευμένοι αλγόριθμοι DLP $O(2^{\frac{\lambda}{2}})$ - όχι υποεκθετικοί
 - Ίδια επίπεδα ασφάλειας με μικρότερη παράμετρο - καλύτερη απόδοση

RSA	EC
1024	160
2048	224
3072	256

Έστω \mathbb{F} ένα σώμα.

Έστω \mathbb{F} ένα σώμα.

Ορισμός $\mathcal{E}(\mathbb{F})$

Μια ελλειπτική καμπύλη \mathcal{E} πάνω από το \mathbb{F} είναι το σύνολο των σημείων $(x, y) \in \mathbb{F}$, που ικανοποιούν την εξίσωση Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{F}$$

και ένα στοιχείο \mathcal{O} , (- σημείο στο άπειρο)

Έστω \mathbb{F} ένα σώμα.

Ορισμός $\mathcal{E}(\mathbb{F})$

Μια ελλειπτική καμπύλη \mathcal{E} πάνω από το \mathbb{F} είναι το σύνολο των σημείων $(x, y) \in \mathbb{F}$, που ικανοποιούν την εξίσωση Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

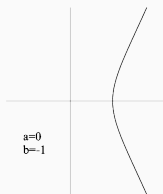
$$a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{F}$$

και ένα στοιχείο \mathcal{O} , (- σημείο στο άπειρο)

Πρακτικά

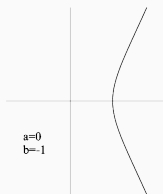
$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}$$

Ελλειπτικές καμπύλες στο \mathbb{R} (μορφή)

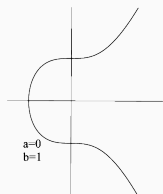


$$y^2 = x^3 - 1$$

Ελλειπτικές καμπύλες στο \mathbb{R} (μορφή)

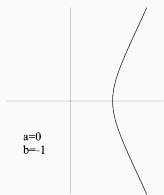


$$y^2 = x^3 - 1$$

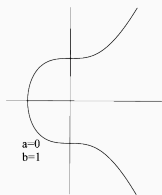


$$y^2 = x^3 + 1$$

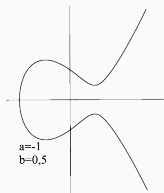
Ελλειπτικές καμπύλες στο \mathbb{R} (μορφή)



$$y^2 = x^3 - 1$$

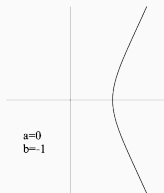


$$y^2 = x^3 + 1$$

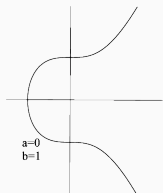


$$y^2 = x^3 - x + \frac{1}{2}$$

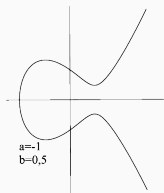
Ελλειπτικές καμπύλες στο \mathbb{R} (μορφή)



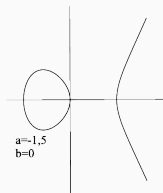
$$y^2 = x^3 - 1$$



$$y^2 = x^3 + 1$$



$$y^2 = x^3 - x + \frac{1}{2}$$



$$y^2 = x^3 - \frac{3}{2}x$$

Παρατηρήσεις στη μορφή ελλειπτικών καμπυλών

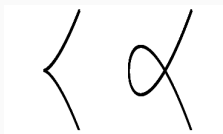
- Συμμετρία ως προς άξονα x

Παρατηρήσεις στη μορφή ελλειπτικών καμπυλών

- Συμμετρία ως προς άξονα x
- Συμπίεση σημείου: Αποθηκεύουμε τετμημένη και 1 bit για πάνω ή κάτω από τον άξονα των x (δηλ. $(x, 0)$ ή $(x, 1)$)

Παρατηρήσεις στη μορφή ελλειπτικών καμπυλών

- Συμμετρία ως προς άξονα x
- Συμπίεση σημείου: Αποθηκεύουμε τετμημένη και 1 bit για πάνω ή κάτω από τον άξονα των x (δηλ. $(x, 0)$ ή $(x, 1)$)
- **Προς αποφυγή** Singular καμπύλες: Πολλαπλές ρίζες, σημεία τομής



Πρέπει $4a^3 + 27b^2 \neq 0$

Ομάδα Σημείων Ελλειπτικής καμπύλης

Τα σημεία μιας ελλειπτικής καμπύλης αποτελούν αβελιανή ομάδα ως προς την πρόσθεση

Ομάδα Σημείων Ελλειπτικής καμπύλης

Τα σημεία μιας ελλειπτικής καμπύλης αποτελούν αβελιανή ομάδα ως προς την πρόσθεση

- ουδέτερο στοιχείο \mathcal{O}

Ομάδα Σημείων Ελλειπτικής καμπύλης

Τα σημεία μιας ελλειπτικής καμπύλης αποτελούν αβελιανή ομάδα ως προς την πρόσθεση

- ουδέτερο στοιχείο \mathcal{O}
- αντίθετο σημείου P στην $\mathcal{E}(\mathbb{R})$:
 - Αν $P = \mathcal{O}$, τότε $-P = \mathcal{O}$
 - Αν $P = (x, y)$ τότε $-P = (x, -y)$
(ανήκει στην \mathcal{E} λόγω συμμετρίας)

Ομάδα Σημείων Ελλειπτικής καμπύλης

Τα σημεία μιας ελλειπτικής καμπύλης αποτελούν αβελιανή ομάδα ως προς την πρόσθεση

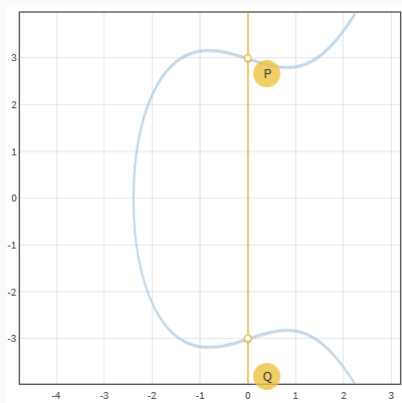
- ουδέτερο στοιχείο \mathcal{O}
- αντίθετο σημείου P στην $\mathcal{E}(\mathbb{R})$:
 - Αν $P = \mathcal{O}$, τότε $-P = \mathcal{O}$
 - Αν $P = (x, y)$ τότε $-P = (x, -y)$
(ανήκει στην \mathcal{E} λόγω συμμετρίας)
- πρόσθεση: Για τρία σημεία P, Q, R στην ίδια ευθεία:
 $P + Q + R = \mathcal{O}$
- πρόσθεση: προσεταιριστική και αντιμεταθετική

Πρόσθεση Σημείων i

(Γεωμετρική) Ερμηνεία

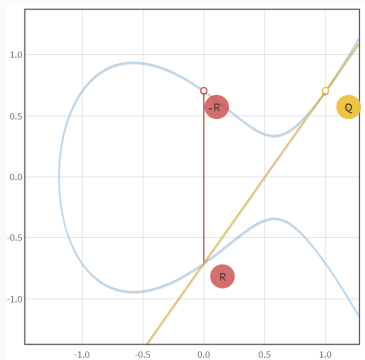
Το άθροισμα $P + Q$

Αν $P = \mathcal{O}$, τότε $\mathcal{O} + Q = Q$
Αν $Q = -P$, τότε $P + Q = \mathcal{O}$.
Το σημείο \mathcal{O} υπάρχει σε **κάθε**
κατακόρυφη



Αν $P = Q$ τότε:

- Θεωρούμε την εφαπτομένη στο P
- Βρίσκουμε το σημείο τομής R με την \mathcal{E} .
- Βρίσκουμε το αντίθετο

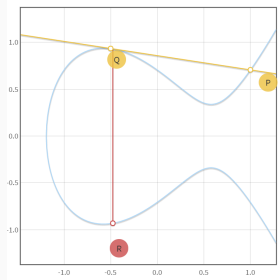
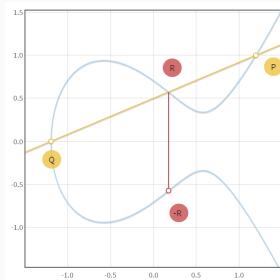


Elliptic Curve point addition

Πρόσθεση Σημείων iii

Αν $P \neq Q$ τότε:

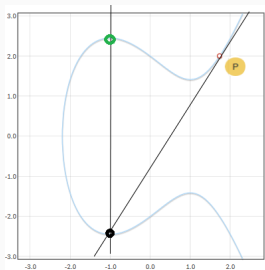
- Θεωρούμε την \overline{PQ}
- Αν υπάρχει σημείο τομής R με την \mathcal{E} :
 - Βρίσκουμε το αντίθετο
- Αν δεν υπάρχει σημείο τομής τομής:
 - Σε ένα εκ των P, Q η \overline{PQ} θα εφάπτεται με την \mathcal{E}
 - Βρίσκουμε το αντίθετο



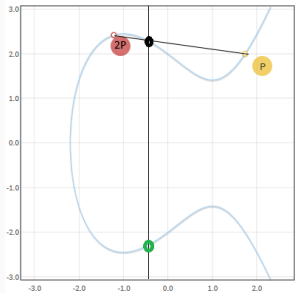
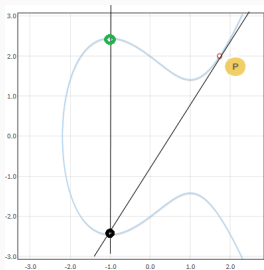
Αλγεβρική αναπαράσταση

- Συντελεστής ευθείας \overline{PQ} : $m = \frac{y_P - y_Q}{x_P - x_Q}$
- Εύρεση σημείου τομής (x_R, y_R) με ελλειπτική καμπύλη
- Επίλυση τριτοβάθμιας εξίσωσης

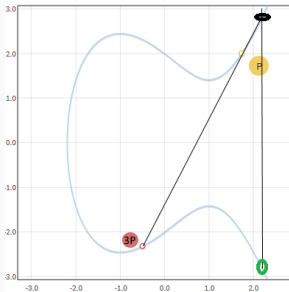
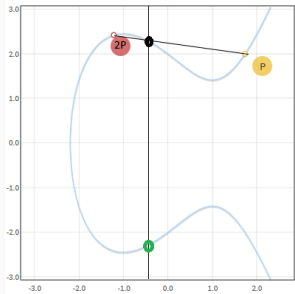
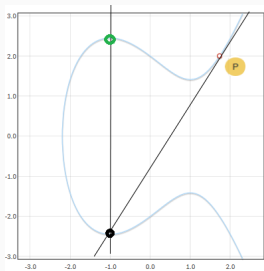
Πολλαπλασιασμός σημείου με ακέραιο $nP = P + P + \dots + P$



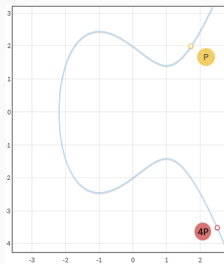
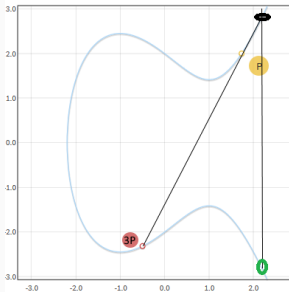
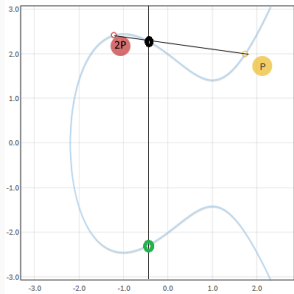
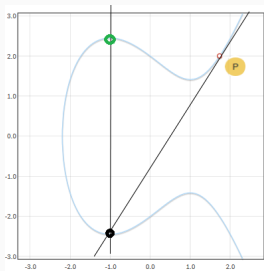
Πολλαπλασιασμός σημείου με ακέραιο $nP = P + P + \dots + P$



Πολλαπλασιασμός σημείου με ακέραιο $nP = P + P + \dots + P$



Πολλαπλασιασμός σημείου με ακέραιο $nP = P + P + \dots + P$



Υπολογισμός nP

Απαιτούνται $n - 1$ προσθέσεις

Λύση: Square and multiply - Double and add

$$17P = P + 16P$$

$$2P = P + P$$

$$4P = 2P + 2P$$

$$8P = 4P + 4P$$

$$16P = 8P + 8P$$

Ελλειπτικές καμπύλες στο \mathbb{F}_p

Ορισμός $\mathcal{E}(\mathbb{F}_p)$

$$\mathcal{E} = \mathcal{O} \cup \{y^2 = x^3 + ax + b \pmod{p}, \\ (x, y) \in \mathbb{F}_p^2, (a, b) \in \mathbb{F}_p^2 : 4a^3 + 27b^2 \not\equiv 0 \pmod{p}\}$$

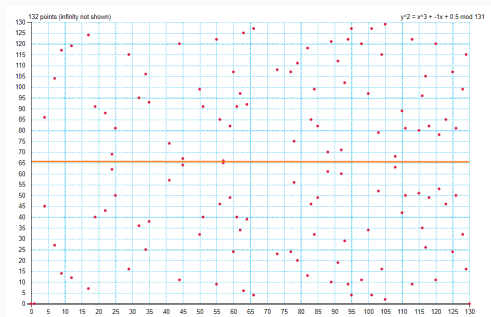
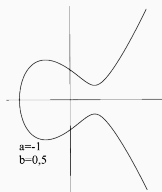
Ελλειπτικές καμπύλες στο \mathbb{F}_p

Ορισμός $\mathcal{E}(\mathbb{F}_p)$

$$\mathcal{E} = \mathcal{O} \cup \{y^2 = x^3 + ax + b \pmod{p}, \\ (x, y) \in \mathbb{F}_p^2, (a, b) \in \mathbb{F}_p^2 : 4a^3 + 27b^2 \neq 0 \pmod{p}\}$$

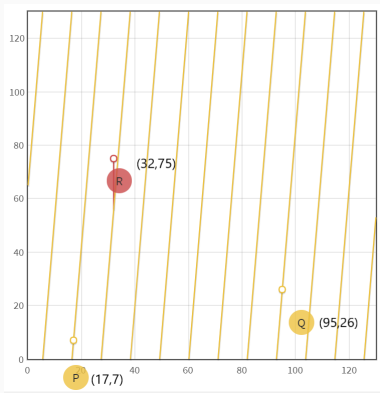
Παράδειγμα: $y^2 = x^3 - x + \frac{1}{2} \pmod{131}$

Discrete Elliptic Curve Plotter



Πρόσθεση σημείων στο \mathbb{F}_p

Η ευθεία που συνδέει τα P, Q, R επαναλαμβάνεται



Η ομάδα των σημείων $\mathcal{E}(\mathbb{F}_p)$ i

Εύρεση τάξης ομάδας

Εκθετικός αλγόριθμος

Δοκιμές όλων των $x \in \{0, \dots, p-1\}$ για το ποια ικανοποιούν την εξίσωση της καμπύλης

Το πολύ $2p + 1$ σημεία (συμμετρία +)

Hasse bound

$$p + 1 - 2\sqrt{p} \leq |\mathcal{E}(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$$

Υπολογισμός

Αλγόριθμος Schoof σε $O(\log(p))$ με βελτιώσεις Elkies, Atkin (SEA)

Η ομάδα των σημείων $\mathcal{E}(\mathbb{F}_p)$ ii

Κυκλικές υποομάδες

Κάθε σημείο μιας καμπύλης $\mathcal{E}(\mathbb{F}_p)$ παράγει μια κυκλική υποομάδα

Εύρεση σημείων βάσης

Θέλουμε γεννήτορες μεγάλων υποομάδων

- Επιλογή τάξης υποομάδας (μεγάλος πρώτος q): $q \mid |\mathcal{E}|$
- Υπολογισμός cofactor $h = \frac{|\mathcal{E}|}{q}$
- Επιλογή τυχαίου σημείου P
- Υπολογισμός $G = hP$
- Αν $G = \mathcal{O}$ επανάληψη

Βελτιστοποίηση πρόσθεσης σημείων και πολλαπλασιασμού σημείου με ακέραιο

- Koblitz curves: $y^2 + xy = x^3 + ax^2 + 1, a \in \{0, 1\}$
- Binary curves: $y^2 + xy = x^3 + x^2 + b, b \in \mathbb{Z}$
- Edwards curves: $y^2 + x^2 = 1 + dx^2y^2, d \in \{0, 1\}$ (προστασία από side channels)

Δίνονται:

- Μία ελλειπτική καμπύλη \mathcal{E} ορισμένη πάνω από το \mathbb{F}_p
($p, a, b, \#\mathcal{E}$)
- Μία μεγάλη υποομάδα της με τάξη q
- ένα σημείο βάσης G και
- ένα σημείο Y .

Ζητείται: Να βρεθεί, αν υπάρχει, ακέραιος x τέτοιος ώστε $xG = Y$.

Δίνονται:

- Μία ελλειπτική καμπύλη \mathcal{E} ορισμένη πάνω από το \mathbb{F}_p
($p, a, b, \#\mathcal{E}$)
- Μία μεγάλη υποομάδα της με τάξη q
- ένα σημείο βάσης G και
- ένα σημείο Y .

Ζητείται: Να βρεθεί, αν υπάρχει, ακέραιος x τέτοιος ώστε $xG = Y$.

Εικασία

Το πρόβλημα ECDLP είναι υπολογιστικά απρόσιτο

Δίνονται:

- Μία ελλειπτική καμπύλη \mathcal{E} ορισμένη πάνω από το \mathbb{F}_p
($p, a, b, \#\mathcal{E}$)
- Μία μεγάλη υποομάδα της με τάξη q
- ένα σημείο βάσης G και
- ένα σημείο Y .

Ζητείται: Να βρεθεί, αν υπάρχει, ακέραιος x τέτοιος ώστε $xG = Y$.

Εικασία

Το πρόβλημα ECDLP είναι υπολογιστικά απρόσιτο

Όχι όμως σε κάθε καμπύλη:

- MOV's attack (pairings) - υποεκθετικό DLP
- Smart's attack ($\#\mathcal{E}(\mathbb{F}_p) = p$) - πολυωνυμικό DLP

Συνέπεια: Δεν προτείνεται η παραγωγή καμπυλών, αλλά η χρήση έτοιμων

Συνέπεια: Δεν προτείνεται η παραγωγή καμπυλών, αλλά η χρήση έτοιμων

Πρότυπο **NIST FIPS186-3**

15 ελλειπτικές καμπύλες. Οι πιο γνωστές:

- **NIST P-256** ή **secp256r1**

$$y^2 = x^3 - 3x + b \pmod{(2^{256} - 2^{224} + 2^{192} + 2^{96} - 1)}$$

με $b = 41\ 058\ 363\ 725\ 152\ 142\ 129\ 326\ 129\ 780\ 047\ 268\ 409$
 $114\ 441\ 015\ 993\ 725\ 554\ 835\ 256\ 314\ 039\ 467\ 401\ 291$

- **NIST P-384**

$$y^2 = x^3 - 3x + b \pmod{(2^{384} - 2^{128} - 2^{96} + 2^{32} - 1)}$$

με $b = 27\ 580\ 193\ 559\ 959\ 705\ 877\ 849\ 011\ 840\ 389\ 048\ 093$
 $056\ 905\ 856\ 361\ 568\ 521\ 428\ 707\ 301\ 988\ 689\ 241\ 309\ 860$
 $865\ 136\ 260\ 764\ 883\ 745\ 107\ 765\ 439\ 761\ 230\ 575$

Εναλλακτικά:

secp256k1 (OpenSSL, Bitcoin)

$$y^2 = x^3 + 0x + 7 \pmod{(2^{256} - 2^{32} - 977)}$$

Curve25519 (OpenSSH)

$$y^2 = x^3 + 486662 \cdot x^2 + x \pmod{(2^{255} - 19)}$$

Κρυπτογραφικά πρωτόκολλα

Στόχοι

- Κατασκευή κοινού κλειδιού πάνω από δημόσιο κανάλι επικοινωνίας
- Σε EC: Το κοινό κλειδί είναι σημείο της καμπύλης
- Δημόσια επικοινωνία και συμφωνία σε σημείο P μιας ελλειπτικής καμπύλης \mathcal{E}

Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#\mathcal{E}, q, G)$

Πρωτόκολλο

- Η Alice επιλέγει έναν ακέραιο $a \in \{1, \dots, q - 1\}$
- Υπολογίζει το $aG \in \mathcal{E}$ και το δημοσιοποιεί.
- Ο Bob επιλέγει έναν ακέραιο $b \in \{1, \dots, q - 1\}$ και δημοσιοποιεί το $bG \in \mathcal{E}$
- Το δημόσιο κλειδί που θα χρησιμοποιούν στη συνέχεια είναι το $P = a(bG) = b(aG) \in \mathcal{E}$

Παραλλαγή Κρυπτοσυστήματος ElGamal

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$

Παραλλαγή Κρυπτοσυστήματος ElGamal

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q - 1\}$

Παραλλαγή Κρυπτοσυστήματος ElGamal

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q - 1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in E$

Παραλλαγή Κρυπτοσυστήματος ElGamal

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q - 1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in E$

Κρυπτογράφηση

- Κωδικοποίηση μηνύματος ως σημείο P_m της E

Παραλλαγή Κρυπτοσυστήματος ElGamal

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q - 1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in E$

Κρυπτογράφηση

- Κωδικοποίηση μηνύματος ως σημείο P_m της E
- Επιλέγεται ένας τυχαίος ακέραιος $k \in \{1, \dots, q - 1\}$

Παραλλαγή Κρυπτοσυστήματος ElGamal

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q - 1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in E$

Κρυπτογράφηση

- Κωδικοποίηση μηνύματος ως σημείο P_m της E
- Επιλέγεται ένας τυχαίος ακέραιος $k \in \{1, \dots, q - 1\}$
- Κρυπτογράφημα: $\text{Enc}(Y, m) = (kG, P_m + kY)$

Παραλλαγή Κρυπτοσυστήματος ElGamal

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q - 1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in E$

Κρυπτογράφηση

- Κωδικοποίηση μηνύματος ως σημείο P_m της E
- Επιλέγεται ένας τυχαίος ακέραιος $k \in \{1, \dots, q - 1\}$
- Κρυπτογράφημα: $\text{Enc}(Y, m) = (kG, P_m + kY)$

Αποκρυπτογράφηση

- Υπολογισμός

$$P_m + kY - x(kG) = P_m$$

Κωδικοποίηση μηνύματος σε σημείο

- 1ος τρόπος: Hashed Elgamal
 - Χρήση συνάρτησης $\mathcal{H} : \mathcal{E} \rightarrow \mathcal{M}$
 - Κρυπτογράφηση: $\text{Enc}(Y, m) = (kG, m \oplus \mathcal{H}(kY))$
 - Αποκρυπτογράφηση;

Κωδικοποίηση μηνύματος σε σημείο

- 1ος τρόπος: Hashed Elgamal
 - Χρήση συνάρτησης $\mathcal{H} : \mathcal{E} \rightarrow \mathcal{M}$
 - Κρυπτογράφηση: $\text{Enc}(Y, m) = (kG, m \oplus \mathcal{H}(kY))$
 - Αποκρυπτογράφηση;
- 2ος τρόπος
 - Επιλογή τυχαίου x_p και αντικατάσταση των bits χαμηλής τάξης του με το m
 - Επιλογή ενός από τα δύο πιθανά σημεία της καμπύλης
 - Αν δεν ανήκει τότε επανάληψη

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q - 1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in E$

Υπογραφή

- Υπολογισμός σύνοψης του μηνύματος $h = \mathcal{H}(M)$ και προσαρμογή της στο $[0, \dots, q - 1]$
- Επιλογή τυχαίου αριθμού k στο σύνολο $\{1, \dots, q - 1\}$
- Υπολογισμός του σημείου $P = kG = (x_P, y_P)$.
- Υπολογισμός του $r = x_P \bmod q$
- Αν $r = 0 \pmod{q}$ τότε επανάληψη με καινούριο k .
- Υπολογισμός του $s = k^{-1}(h + r \cdot x) \bmod q$
- Αν $s = 0$ τότε επανάληψη με καινούριο k .
- Η υπογραφή είναι το ζεύγος (r, s)

Επαλήθευση

- Υπολογισμός του $u_1 = s^{-1}h \bmod q$
- Υπολογισμός του $u_2 = s^{-1}r \bmod q$
- Υπολογισμός του σημείου $P' = u_1G + u_2Y$
- Η υπογραφή είναι έγκυρη αν $r = x_{P'} \pmod{q}$

Ορθότητα: Υπολογισμός ίδιου σημείου με 2 τρόπους:

- Υπογραφή $P = kG$
- Επαλήθευση $P' = u_1G + u_2Y$

$$P' = u_1G + u_2Y = s^{-1}(h + rx)G = k(h + rx)^{-1}(h + rx)G = kG = P$$

Ασφάλεια: Επιλογή διαφορετικού k ανά υπογραφή

Αλλιώς: Ανάκτηση ιδιωτικού κλειδιού!

Επίθεση επανάληψης τυχειότητας

Δίνονται δύο υπογραφές $(r_1, s_1)(r_2, s_2)$

Παρατήρηση: $r_1 = r_2 = x_{kG}$

Τότε: $s_1 - s_2 = k^{-1}(h_1 - h_2) \pmod{q}$

Ανάκτηση $k = (h_1 - h_2)(s_1 - s_2)^{-1} \pmod{q}$

Ανάκτηση $x = (ks_1 - h_1)r^{-1}$

Sony PlayStation 3 hack (2011): Υπογραφή όλων των παιχνιδιών με ίδιο k

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
             // guaranteed to be random.  
}
```

<https://xkcd.com/221/>

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#E, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q - 1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in E$

Υπογραφή Μηνύματος m

- Επιλογή τυχαίου αριθμού k στο σύνολο $\{1, \dots, q - 1\}$
- Υπολογισμός του σημείου $P = kG$.
- Υπολογισμός του $s = k + x \cdot \mathcal{H}(P||Y||m)$
- Η υπογραφή είναι το ζεύγος (P, s) (σημείο και τιμή)

Επαλήθευση υπογραφής στο m

$$\text{Verify}(\mathcal{H}, m, (P, s)) = \begin{cases} 1, & s \cdot G = P + \mathcal{H}(P||Y||m) \cdot Y \\ 0, & \text{αλλιώς} \end{cases}$$

Ορθότητα:

$$\begin{aligned} s \cdot G &= (k + x \cdot \mathcal{H}(P||Y||m)) \cdot G \\ &= kG + xG \cdot \mathcal{H}(P||Y||m) \\ &= P + Y \cdot \mathcal{H}(P||Y||m) \end{aligned}$$

Βελτίωση απόδοσης: Batch validation (ακόμα και με διαφορετικά κλειδιά)

$$\begin{aligned} \text{Verify}(\mathcal{H}, (m_1, P_1, s_1), \dots, (m_n, P_n, s_n)) : \\ (s_1 + \dots + s_n) \cdot G = \\ P_1 + \mathcal{H}(P_1 || Y_1 || m_1) \cdot Y_1 + \dots + P_n + \mathcal{H}(P_n || Y || m_n) \cdot Y_n \end{aligned}$$

Pairing Based Cryptography

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ πεπερασμένες κυκλικές ομάδες

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ πεπερασμένες κυκλικές ομάδες

Ζεύξη (pairing-bilinear map): Μία αποδοτικά υπολογίσιμη συνάρτηση

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ πεπερασμένες κυκλικές ομάδες

Ζεύξη (pairing-bilinear map): Μία αποδοτικά υπολογίσιμη συνάρτηση

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

1) Διγραμμική (bilinear):

$$e(g_1 \cdot g_2, h_1) = e(g_1, h_1) \cdot e(g_2, h_1) \text{ και}$$

$$e(g_1, h_1 \cdot h_2) = e(g_1, h_1) \cdot e(g_1, h_2)$$

ή ισοδύναμα $e(g^a, h^b) = e(g, h)^{ab} \quad \forall g \in \mathbb{G}_1, h \in \mathbb{G}_2, a, b \in \mathbb{Z}$

Ορισμός

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ πεπερασμένες κυκλικές ομάδες

Ζεύξη (pairing-bilinear map): Μία αποδοτικά υπολογίσιμη συνάρτηση

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

1) Διγραμμική (bilinear):

$$e(g_1 \cdot g_2, h_1) = e(g_1, h_1) \cdot e(g_2, h_1) \text{ και}$$

$$e(g_1, h_1 \cdot h_2) = e(g_1, h_1) \cdot e(g_1, h_2)$$

ή ισοδύναμα $e(g^a, h^b) = e(g, h)^{ab} \quad \forall g \in \mathbb{G}_1, h \in \mathbb{G}_2, a, b \in \mathbb{Z}$

2) Μη εκφυλισμένη (non-degenerate):

Αν $\mathbb{G} = \langle g \rangle$ τότε $\mathbb{G}_T = \langle e(g, g) \rangle$

Ορισμός (2)

Μπορεί και $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$

Συνήθως: $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G} \subseteq \mathcal{E}(\mathbb{F}_p), \mathbb{G}_T \subseteq \mathbb{F}_{p^a}^*$

Ορισμός (2)

Μπορεί και $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$

Συνήθως: $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G} \subseteq \mathcal{E}(\mathbb{F}_p), \mathbb{G}_T \subseteq \mathbb{F}_{p^a}^*$

Συνέπεια ορισμού: Συμμετρία $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$

Ορισμός (2)

Μπορεί και $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$

Συνήθως: $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G} \subseteq \mathcal{E}(\mathbb{F}_p)$, $\mathbb{G}_T \subseteq \mathbb{F}_{p^a}^*$

Συνέπεια ορισμού: Συμμετρία $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$

Pairings: ένα απλό παράδειγμα

$e(x, y) = 2^{xy}$ Τότε:

$e(a, b + c) = 2^{a(b+c)}$ και: $e(a, b) \cdot e(a, c) = 2^{ab} \cdot 2^{ac} = 2^{a(b+c)}$

Διαίσθηση: πολλαπλασιασμός σε κρυπτογραφημένες τιμές

Ζεύξεις στην κρυπτογραφία

- Στο \mathbb{G} κάποια προβλήματα είναι δύσκολα, αλλά στο \mathbb{G}_T μπορεί να είναι εύκολα

Ζεύξεις στην κρυπτογραφία

- Στο \mathbb{G} κάποια προβλήματα είναι δύσκολα, αλλά στο \mathbb{G}_T μπορεί να είναι εύκολα
- Λόγω της απεικόνισης e μπορούμε να μεταβούμε αποδοτικά από την δύσκολη εκδοχή στην εύκολη

Ζεύξεις στην κρυπτογραφία

- Στο \mathbb{G} κάποια προβλήματα είναι δύσκολα, αλλά στο \mathbb{G}_T μπορεί να είναι εύκολα
- Λόγω της απεικόνισης e μπορούμε να μεταβούμε αποδοτικά από την δύσκολη εκδοχή στην εύκολη
- Χρήσιμη ασυμμετρία για την κατασκευή κρυπτογραφικών πρωτοκόλλων
- Πχ: Υπογραφές:

Ζεύξεις στην κρυπτογραφία

- Στο \mathbb{G} κάποια προβλήματα είναι δύσκολα, αλλά στο \mathbb{G}_T μπορεί να είναι εύκολα
- Λόγω της απεικόνισης e μπορούμε να μεταβούμε αποδοτικά από την δύσκολη εκδοχή στην εύκολη
- Χρήσιμη ασυμμετρία για την κατασκευή κρυπτογραφικών πρωτοκόλλων
- Πχ: Υπογραφές:
 - Κατασκευή υπογραφής στο \mathbb{G}
 - Επαλήθευση στο \mathbb{G}_T μέσω του pairing

Ζεύξεις στην κρυπτογραφία

- Στο \mathbb{G} κάποια προβλήματα είναι δύσκολα, αλλά στο \mathbb{G}_T μπορεί να είναι εύκολα
- Λόγω της απεικόνισης e μπορούμε να μεταβούμε αποδοτικά από την δύσκολη εκδοχή στην εύκολη
- Χρήσιμη ασυμμετρία για την κατασκευή κρυπτογραφικών πρωτοκόλλων
- Πχ: Υπογραφές:
 - Κατασκευή υπογραφής στο \mathbb{G}
 - Επαλήθευση στο \mathbb{G}_T μέσω του pairing
- Αρνητικές συνέπειες: Κάποια προβλήματα γίνονται ευκολότερα αν όχι εύκολα

Το DDHP είναι εύκολο...

...αν υπάρχει pairing

...αν υπάρχει pairing

Θέλουμε να ελέγξουμε αν $g^c = g^{ab}$, με δεδομένα τα g^a, g^b, g^c .

...αν υπάρχει pairing

Θέλουμε να ελέγξουμε αν $g^c = g^{ab}$, με δεδομένα τα g^a, g^b, g^c .

Αποδοτικός υπολογισμός μέσω ζεύξης: $e(g^a, g^b) = e(g, g)^{ab}$

...αν υπάρχει pairing

Θέλουμε να ελέγξουμε αν $g^c = g^{ab}$, με δεδομένα τα g^a, g^b, g^c .

Αποδοτικός υπολογισμός μέσω ζεύξης: $e(g^a, g^b) = e(g, g)^{ab}$

Σύγκριση με το $e(g, g^c) = e(g, g)^c$

Όχι όμως και το DLP...

...παρά την ύπαρξη pairing

...παρά την ύπαρξη pairing

Αντί για εύρεση x από g, g^x στην \mathbb{G} (ελλειπτική καμπύλη)

Όχι όμως και το DLP...

...παρά την ύπαρξη pairing

Αντί για εύρεση x από g, g^x στην \mathbb{G} (ελλειπτική καμπύλη)

εύρεση x από $e(g, g), e(g, g^x)$ στην \mathbb{G}_T (πεπερασμένο σώμα)

Όχι όμως και το DLP...

...παρά την ύπαρξη pairing

Αντί για εύρεση x από g, g^x στην \mathbb{G} (ελλειπτική καμπύλη)

εύρεση x από $e(g, g), e(g, g^x)$ στην \mathbb{G}_T (πεπερασμένο σώμα)

Το DLP έγινε ευκολότερο (υποεκθετικοί αλγόριθμοι, MOV attack), όχι όμως εύκολο

Όχι όμως και το DLP...

...παρά την ύπαρξη pairing

Αντί για εύρεση x από g, g^x στην \mathbb{G} (ελλειπτική καμπύλη)

εύρεση x από $e(g, g), e(g, g^x)$ στην \mathbb{G}_T (πεπερασμένο σώμα)

Το DLP έγινε ευκολότερο (υποεκθετικοί αλγόριθμοι, MOV attack), όχι όμως εύκολο

Επιλογή μεγαλύτερης τιμής για παράμετρο ασφάλειας

Διγραμμικό Πρόβλημα Απόφασης Diffie-Hellman

Διαχωρίζονται στοιχεία του \mathbb{G}_T

BDDHP

Δίνονται: δύο στοιχεία $h, g \in \mathbb{G}$ και τα στοιχεία $g^a, g^b, e(h, g)^c$.

Διγραμμικό Πρόβλημα Απόφασης Diffie-Hellman

Διαχωρίζονται στοιχεία του \mathbb{G}_T

BDDHP

Δίνονται: δύο στοιχεία $h, g \in \mathbb{G}$ και τα στοιχεία $g^\alpha, g^\beta, e(h, g)^c$.

Ζητείται: Ισχύει $c = \alpha\beta$;

- Συμμετρικά
- $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ (Weil pairing)

- Συμμετρικά
- $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ (Weil pairing)
- Ασύμμετρα $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$

- Συμμετρικά
- $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ (Weil pairing)
- Ασύμμετρα $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
 - Με εύκολο DDHP στο \mathbb{G}_1
 - Χωρίς εύκολο DDHP στο $\mathbb{G}_1, \mathbb{G}_2$
 - Tate pairing

Διαφορετικές υποθέσεις ασφάλειας

Εφαρμογές PBC

Έστω κυκλική ομάδα με $\mathbb{G} = \langle g \rangle$

Έστω κυκλική ομάδα με $\mathbb{G} = \langle g \rangle$

Τρεις οντότητες A, B, C με ζευγάρια ιδιωτικών - δημοσίων κλειδιών $(x_A, y_A = g^{x_A}), (x_B, y_B = g^{x_B}), (x_C, y_C = g^{x_C})$.

Τριμερής ανταλλαγή κλειδιού

Έστω κυκλική ομάδα με $\mathbb{G} = \langle g \rangle$

Τρεις οντότητες A, B, C με ζευγάρια ιδιωτικών - δημοσίων κλειδιών $(x_A, y_A = g^{x_A})$, $(x_B, y_B = g^{x_B})$, $(x_C, y_C = g^{x_C})$.

Μπορεί να συμφωνηθεί ένα κοινό κλειδί μεταξύ τους;

Χωρίς pairings - σε 3 γύρους

1. Ο A στέλνει το y_A στον B , ο B στέλνει το y_B στον C , ο C στέλνει το y_C στον A (κυκλικά).

Χωρίς pairings - σε 3 γύρους

1. Ο A στέλνει το y_A στον B , ο B στέλνει το y_B στον C , ο C στέλνει το y_C στον A (κυκλικά).
2. Ο A υπολογίζει το $t_A = y_C^{x_A} = g^{x_C x_A}$, ο B υπολογίζει το $t_B = y_A^{x_B} = g^{x_B x_A}$ και ο C υπολογίζει το $t_C = y_B^{x_C} = g^{x_B x_C}$

Χωρίς pairings - σε 3 γύρους

1. Ο A στέλνει το y_A στον B , ο B στέλνει το y_B στον C , ο C στέλνει το y_C στον A (κυκλικά).
2. Ο A υπολογίζει το $t_A = y_C^{x_A} = g^{x_C x_A}$, ο B υπολογίζει το $t_B = y_A^{x_B} = g^{x_B x_A}$ και ο C υπολογίζει το $t_C = y_B^{x_C} = g^{x_B x_C}$
3. Ο A στέλνει το t_A στον B , ο B στέλνει το t_B στον C , ο C στέλνει το t_C στον A (πάλι κυκλικά).

Χωρίς pairings - σε 3 γύρους

1. Ο A στέλνει το y_A στον B , ο B στέλνει το y_B στον C , ο C στέλνει το y_C στον A (κυκλικά).
2. Ο A υπολογίζει το $t_A = y_C^{x_A} = g^{x_C x_A}$, ο B υπολογίζει το $t_B = y_A^{x_B} = g^{x_B x_A}$ και ο C υπολογίζει το $t_C = y_B^{x_C} = g^{x_B x_C}$
3. Ο A στέλνει το t_A στον B , ο B στέλνει το t_B στον C , ο C στέλνει το t_C στον A (πάλι κυκλικά).
4. Όλοι υπολογίζουν το κοινό κλειδί ως εξής:
 - Ο A με $t_C^{x_A} = g^{x_B x_C x_A}$

Χωρίς pairings - σε 3 γύρους

1. Ο A στέλνει το y_A στον B , ο B στέλνει το y_B στον C , ο C στέλνει το y_C στον A (κυκλικά).
2. Ο A υπολογίζει το $t_A = y_C^{x_A} = g^{x_C x_A}$, ο B υπολογίζει το $t_B = y_A^{x_B} = g^{x_B x_A}$ και ο C υπολογίζει το $t_C = y_B^{x_C} = g^{x_B x_C}$
3. Ο A στέλνει το t_A στον B , ο B στέλνει το t_B στον C , ο C στέλνει το t_C στον A (πάλι κυκλικά).
4. Όλοι υπολογίζουν το κοινό κλειδί ως εξής:
 - Ο A με $t_C^{x_A} = g^{x_B x_C x_A}$
 - Ο B με $t_A^{x_B} = g^{x_C x_A x_B}$

Χωρίς pairings - σε 3 γύρους

1. Ο A στέλνει το y_A στον B , ο B στέλνει το y_B στον C , ο C στέλνει το y_C στον A (κυκλικά).
2. Ο A υπολογίζει το $t_A = y_C^{x_A} = g^{x_C x_A}$, ο B υπολογίζει το $t_B = y_A^{x_B} = g^{x_B x_A}$ και ο C υπολογίζει το $t_C = y_B^{x_C} = g^{x_B x_C}$
3. Ο A στέλνει το t_A στον B , ο B στέλνει το t_B στον C , ο C στέλνει το t_C στον A (πάλι κυκλικά).
4. Όλοι υπολογίζουν το κοινό κλειδί ως εξής:
 - Ο A με $t_C^{x_A} = g^{x_B x_C x_A}$
 - Ο B με $t_A^{x_B} = g^{x_C x_A x_B}$
 - Ο C με $t_B^{x_C} = g^{x_A x_B x_C}$

Χωρίς pairings - σε 3 γύρους

1. Ο A στέλνει το y_A στον B , ο B στέλνει το y_B στον C , ο C στέλνει το y_C στον A (κυκλικά).
2. Ο A υπολογίζει το $t_A = y_C^{x_A} = g^{x_C x_A}$, ο B υπολογίζει το $t_B = y_A^{x_B} = g^{x_B x_A}$ και ο C υπολογίζει το $t_C = y_B^{x_C} = g^{x_B x_C}$
3. Ο A στέλνει το t_A στον B , ο B στέλνει το t_B στον C , ο C στέλνει το t_C στον A (πάλι κυκλικά).
4. Όλοι υπολογίζουν το κοινό κλειδί ως εξής:
 - Ο A με $t_C^{x_A} = g^{x_B x_C x_A}$
 - Ο B με $t_A^{x_B} = g^{x_C x_A x_B}$
 - Ο C με $t_B^{x_C} = g^{x_A x_B x_C}$

Υποθέτουμε δύο ομάδες \mathbb{G}, \mathbb{G} με τάξη ένα πρώτο q και μία συμμετρική διγραμμική ζεύξη $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

Υποθέτουμε δύο ομάδες \mathbb{G}, \mathbb{G} με τάξη ένα πρώτο q και μία συμμετρική διγραμμική ζεύξη $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

- Όλοι οι συμμετέχοντες εκπέμπουν τα δημόσια κλειδιά τους $y_A = g^{x_A}, y_B = g^{x_B}, y_C = g^{x_C}$.

Με pairings - σε 1 γύρο (Joux-2000)

Υποθέτουμε δύο ομάδες \mathbb{G} , \mathbb{G} με τάξη ένα πρώτο q και μία συμμετρική διγραμμική ζεύξη $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

- Όλοι οι συμμετέχοντες εκπέμπουν τα δημόσια κλειδιά τους $y_A = g^{x_A}, y_B = g^{x_B}, y_C = g^{x_C}$.
- Με την βοήθεια της ζεύξης το κοινό κλειδί μπορεί να υπολογιστεί ως εξής:
 - $e(g^{x_B}, g^{x_C})^{x_A} = e(g, g)^{x_B x_C x_A}$

Με pairings - σε 1 γύρο (Joux-2000)

Υποθέτουμε δύο ομάδες \mathbb{G}, \mathbb{G} με τάξη ένα πρώτο q και μία συμμετρική διγραμμική ζεύξη $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

- Όλοι οι συμμετέχοντες εκπέμπουν τα δημόσια κλειδιά τους $y_A = g^{x_A}, y_B = g^{x_B}, y_C = g^{x_C}$.
- Με την βοήθεια της ζεύξης το κοινό κλειδί μπορεί να υπολογιστεί ως εξής:
 - $e(g^{x_B}, g^{x_C})^{x_A} = e(g, g)^{x_B x_C x_A}$
 - $e(g^{x_A}, g^{x_C})^{x_B} = e(g, g)^{x_A x_C x_B}$

Με pairings - σε 1 γύρο (Joux-2000)

Υποθέτουμε δύο ομάδες \mathbb{G} , \mathbb{G} με τάξη ένα πρώτο q και μία συμμετρική διγραμμική ζεύξη $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

- Όλοι οι συμμετέχοντες εκπέμπουν τα δημόσια κλειδιά τους $y_A = g^{x_A}, y_B = g^{x_B}, y_C = g^{x_C}$.
- Με την βοήθεια της ζεύξης το κοινό κλειδί μπορεί να υπολογιστεί ως εξής:
 - $e(g^{x_B}, g^{x_C})^{x_A} = e(g, g)^{x_B x_C x_A}$
 - $e(g^{x_A}, g^{x_C})^{x_B} = e(g, g)^{x_A x_C x_B}$
 - $e(g^{x_A}, g^{x_B})^{x_C} = e(g, g)^{x_A x_B x_C}$

- Boneh, Lynn και Shacham 2004
- Υπογραφές με βάση το DLP αλλά με μικρό μέγεθος
- Αντί για 2 στοιχεία, 1 στοιχείο με μέγεθος όσο η τάξη της ομάδας

- Δημιουργία κλειδιών: $KeyGen(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$

Υπογραφές BLS - Ορισμός

- Δημιουργία κλειδιών: $KeyGen(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH

- Δημιουργία κλειδιών: $KeyGen(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$

Υπογραφές BLS - Ορισμός

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συνάρτηση σύνοψης: $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{G}$

Υπογραφές BLS - Ορισμός

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συνάρτηση σύνοψης: $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{G}$
 - Κλειδί υπογραφής: $x \in_R \mathbb{Z}_q$

Υπογραφές BLS - Ορισμός

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συνάρτηση σύνοψης: $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{G}$
 - Κλειδί υπογραφής: $x \in_R \mathbb{Z}_q$
 - Κλειδί επαλήθευσης: $y = g^x$
- Υπογραφή:
 - Υπολογισμός $h = \mathcal{H}(m)$

Υπογραφές BLS - Ορισμός

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συνάρτηση σύνοψης: $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{G}$
 - Κλειδί υπογραφής: $x \in_R \mathbb{Z}_q$
 - Κλειδί επαλήθευσης: $y = g^x$
- Υπογραφή:
 - Υπολογισμός $h = \mathcal{H}(m)$
 - Υπολογισμός $s = h^x$

Υπογραφές BLS - Ορισμός

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συνάρτηση σύνοψης: $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{G}$
 - Κλειδί υπογραφής: $x \in_R \mathbb{Z}_q$
 - Κλειδί επαλήθευσης: $y = g^x$
- Υπογραφή:
 - Υπολογισμός $h = \mathcal{H}(m)$
 - Υπολογισμός $s = h^x$
 - Επιστροφή $s \in \mathbb{G}$
- Επαλήθευση:
 - Υπολογισμός $h = \mathcal{H}(m)$

Υπογραφές BLS - Ορισμός

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = (\mathbb{G}, \mathbb{G}_T, e, x, y)$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συνάρτηση σύνοψης: $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{G}$
 - Κλειδί υπογραφής: $x \in_R \mathbb{Z}_q$
 - Κλειδί επαλήθευσης: $y = g^x$
- Υπογραφή:
 - Υπολογισμός $h = \mathcal{H}(m)$
 - Υπολογισμός $s = h^x$
 - Επιστροφή $s \in \mathbb{G}$
- Επαλήθευση:
 - Υπολογισμός $h = \mathcal{H}(m)$
 - Έλεγχος $e(g, s) == e(y, h)$

Ορθότητα:

$$e(g, s) = e(g, h^x) = e(g, \mathcal{H}(m))^x \text{ και}$$

Ορθότητα:

$$e(g, s) = e(g, h^x) = e(g, \mathcal{H}(m))^x \text{ και}$$

$$e(y, h) = e(g^x, \mathcal{H}(m)) = e(g, \mathcal{H}(m))^x$$

Ορθότητα:

$$e(g, s) = e(g, h^x) = e(g, \mathcal{H}(m))^x \text{ και}$$

$$e(y, h) = e(g^x, \mathcal{H}(m)) = e(g, \mathcal{H}(m))^x$$

Ασφάλεια:

Ανάγεται στο CDH στην \mathbb{G}

Ορθότητα:

$$e(g, s) = e(g, h^x) = e(g, \mathcal{H}(m))^x \text{ και}$$

$$e(y, h) = e(g^x, \mathcal{H}(m)) = e(g, \mathcal{H}(m))^x$$

Ασφάλεια:

Ανάγεται στο CDH στην \mathbb{G}

Aggregation:

Χρήστες: $\{(x_i, y_i = g^{x_i})\}_{i=1}^n$, υπογραφές: $\{s_i\}_{i=1}^n$

Ορθότητα:

$$e(g, s) = e(g, h^x) = e(g, \mathcal{H}(m))^x \text{ και}$$

$$e(y, h) = e(g^x, \mathcal{H}(m)) = e(g, \mathcal{H}(m))^x$$

Ασφάλεια:

Ανάγεται στο CDH στην \mathbb{G}

Aggregation:

Χρήστες: $\{(x_i, y_i = g^{x_i})\}_{i=1}^n$, υπογραφές: $\{s_i\}_{i=1}^n$

Δημιουργία κοινής υπογραφής: $S = \prod_{i=1}^n s_i$

Ορθότητα:

$$e(g, s) = e(g, h^x) = e(g, \mathcal{H}(m))^x \text{ και}$$

$$e(y, h) = e(g^x, \mathcal{H}(m)) = e(g, \mathcal{H}(m))^x$$

Ασφάλεια:

Ανάγεται στο CDH στην \mathbb{G}

Aggregation:

Χρήστες: $\{(x_i, y_i = g^{x_i})\}_{i=1}^n$, υπογραφές: $\{s_i\}_{i=1}^n$

Δημιουργία κοινής υπογραφής: $S = \prod_{i=1}^n s_i$

Επαλήθευση: $\prod_{i=1}^n e(y_i, \mathcal{H}(m_i)) == e(g, S)$

- Signatures: Shamir 1984

Identity based cryptography

- Signatures: Shamir 1984
- Encryption: Boneh-Franklin (2001)

Identity based cryptography

- Signatures: Shamir 1984
- Encryption: Boneh-Franklin (2001)
- Οποιοδήποτε όνομα κάποιου χρήστη πχ. email είναι η ταυτότητα

Identity based cryptography

- Signatures: Shamir 1984
- Encryption: Boneh-Franklin (2001)
- Οποιοδήποτε όνομα κάποιου χρήστη πχ. email είναι η ταυτότητα
- Δεν χρειάζεται διανομή κλειδιού

Identity based cryptography

- Signatures: Shamir 1984
- Encryption: Boneh-Franklin (2001)
- Οποιοδήποτε όνομα κάποιου χρήστη πχ. email είναι η ταυτότητα
- Δεν χρειάζεται διανομή κλειδιού
- Χρειάζεται κεντρική ΤΤΡ

Identity based cryptography

- Signatures: Shamir 1984
- Encryption: Boneh-Franklin (2001)
- Οποιοδήποτε όνομα κάποιου χρήστη πχ. email είναι η ταυτότητα
- Δεν χρειάζεται διανομή κλειδιού
- Χρειάζεται κεντρική ΤΤΡ
- Παράγει τα ιδιωτικά κλειδιά από την ταυτότητα

Identity based cryptography

- Signatures: Shamir 1984
- Encryption: Boneh-Franklin (2001)
- Οποιοδήποτε όνομα κάποιου χρήστη πχ. email είναι η ταυτότητα
- Δεν χρειάζεται διανομή κλειδιού
- Χρειάζεται κεντρική TTP
- Παράγει τα ιδιωτικά κλειδιά από την ταυτότητα

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id
 - Επιλογή τυχαίου r

Identity based signatures

- TTP έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id
 - Επιλογή τυχαίου r
 - $t = r^e \bmod n$

Identity based signatures

- ΤΤΡ έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id
 - Επιλογή τυχαίου r
 - $t = r^e \bmod n$
 - $s = k r^{\mathcal{H}(m||t)} \bmod n$

Identity based signatures

- ΤΤΡ έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id
 - Επιλογή τυχαίου r
 - $t = r^e \bmod n$
 - $s = k r^{\mathcal{H}(m||t)} \bmod n$
 - Η υπογραφή είναι (t, s)

Identity based signatures

- ΤΤΡ έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id
 - Επιλογή τυχαίου r
 - $t = r^e \bmod n$
 - $s = k r^{\mathcal{H}(m||t)} \bmod n$
 - Η υπογραφή είναι (t, s)
- Επαλήθευση υπογραφής με την ταυτότητα:

Identity based signatures

- ΤΤΡ έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id
 - Επιλογή τυχαίου r
 - $t = r^e \bmod n$
 - $s = k r^{\mathcal{H}(m||t)} \bmod n$
 - Η υπογραφή είναι (t, s)
- Επαλήθευση υπογραφής με την ταυτότητα:
- Έλεγχος αν: $\mathcal{H}(id)t^{\mathcal{H}(m||t)} = s^e$

Identity based signatures

- ΤΡΡ έχει κλειδί RSA $((e, n), d)$
- Δημιουργία ιδιωτικού κλειδιού από ταυτότητα χρήστη id
 - Υπογραφή σύνοψης της ταυτότητας
 - $k = \mathcal{H}(id)^d \bmod n$
 - Ασφαλής Διανομή στον κάτοχο
- Υπογραφή από χρήστη id
 - Επιλογή τυχαίου r
 - $t = r^e \bmod n$
 - $s = k r^{\mathcal{H}(m||t)} \bmod n$
 - Η υπογραφή είναι (t, s)
- Επαλήθευση υπογραφής με την ταυτότητα:
- Έλεγχος αν: $\mathcal{H}(id)t^{\mathcal{H}(m||t)} = s^e$
- Ορθότητα: $\mathcal{H}(id)t^{\mathcal{H}(m||t)} = k^e r^{e\mathcal{H}(m||t)} = s^e$

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συναρτήσεις σύνοψης:
 - $\mathcal{H}_{\mathbb{G}} : \{0, 1\}^* \rightarrow \mathbb{G}$,
 - $\mathcal{H}_{\mathbb{G}_T} : \mathbb{G} \rightarrow \{0, 1\}^*$

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$
 - Ομάδες ($\mathbb{G} = \langle g \rangle, \mathbb{G}_T$) τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συναρτήσεις σύνοψης:
 - $\mathcal{H}_{\mathbb{G}} : \{0, 1\}^* \rightarrow \mathbb{G}$,
 - $\mathcal{H}_{\mathbb{G}_T} : \mathbb{G} \rightarrow \{0, 1\}^*$
 - Ιδιωτικό κλειδί: $x \in_R \mathbb{Z}_q$ (TTP)

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συναρτήσεις σύνοψης:
 - $\mathcal{H}_{\mathbb{G}} : \{0, 1\}^* \rightarrow \mathbb{G}$,
 - $\mathcal{H}_{\mathbb{G}_T} : \mathbb{G} \rightarrow \{0, 1\}^*$
 - Ιδιωτικό κλειδί: $x \in_R \mathbb{Z}_q$ (TTP)
 - Δημόσιο κλειδί: $y = g^x$
- Δημιουργία ζεύγους κλειδιών για τον χρήστη ID:

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συναρτήσεις σύνοψης:
 - $\mathcal{H}_{\mathbb{G}} : \{0, 1\}^* \rightarrow \mathbb{G}$,
 - $\mathcal{H}_{\mathbb{G}_T} : \mathbb{G} \rightarrow \{0, 1\}^*$
 - Ιδιωτικό κλειδί: $x \in_R \mathbb{Z}_q$ (TTP)
 - Δημόσιο κλειδί: $y = g^x$
- Δημιουργία ζεύγους κλειδιών για τον χρήστη ID:
 - Υπολογισμός $h = \mathcal{H}_{\mathbb{G}}(ID)$

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συναρτήσεις σύνοψης:
 - $\mathcal{H}_{\mathbb{G}} : \{0, 1\}^* \rightarrow \mathbb{G}$,
 - $\mathcal{H}_{\mathbb{G}_T} : \mathbb{G} \rightarrow \{0, 1\}^*$
 - Ιδιωτικό κλειδί: $x \in_R \mathbb{Z}_q$ (TTP)
 - Δημόσιο κλειδί: $y = g^x$
- Δημιουργία ζεύγους κλειδιών για τον χρήστη ID:
 - Υπολογισμός $h = \mathcal{H}_{\mathbb{G}}(\text{ID})$
 - Δημόσιο κλειδί: $y_{\text{ID}} = h$

- Δημιουργία κλειδιών: $\text{KeyGen}(1^\lambda) = \mathbb{G}, \mathbb{G}_T, e, x, y$
 - Ομάδες $(\mathbb{G} = \langle g \rangle, \mathbb{G}_T)$ τάξης q με δύσκολο CDH
 - $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
 - Συναρτήσεις σύνοψης:
 - $\mathcal{H}_{\mathbb{G}} : \{0, 1\}^* \rightarrow \mathbb{G}$,
 - $\mathcal{H}_{\mathbb{G}_T} : \mathbb{G} \rightarrow \{0, 1\}^*$
 - Ιδιωτικό κλειδί: $x \in_R \mathbb{Z}_q$ (TTP)
 - Δημόσιο κλειδί: $y = g^x$
- Δημιουργία ζεύγους κλειδιών για τον χρήστη ID:
 - Υπολογισμός $h = \mathcal{H}_{\mathbb{G}}(ID)$
 - Δημόσιο κλειδί: $y_{ID} = h$
 - Ιδιωτικό κλειδί: $x_{ID} = y_{ID}^x$

- Κρυπτογράφηση από χρήστη ID:

- Κρυπτογράφηση από χρήστη ID:
 - Επιλογή $r \in \mathbb{Z}_q$

- Κρυπτογράφηση από χρήστη ID:
 - Επιλογή $r \in \mathbb{Z}_q$
 - Υπολογισμός $t = e(y_{ID}, y)^r$

- Κρυπτογράφηση από χρήστη ID:
 - Επιλογή $r \in \mathbb{Z}_q$
 - Υπολογισμός $t = e(y_{ID}, y)^r$
 - Κρυπτοκείμενο: $(g^r, m \oplus \mathcal{H}_{\mathbb{G}_T}(t))$
- Αποκρυπτογράφηση:

- Κρυπτογράφηση από χρήστη ID:
 - Επιλογή $r \in \mathbb{Z}_q$
 - Υπολογισμός $t = e(y_{ID}, y)^r$
 - Κρυπτοκείμενο: $(g^r, m \oplus \mathcal{H}_{\mathbb{G}_T}(t))$
- Αποκρυπτογράφηση:
 - Έστω κρυπτοκείμενο (a, b)

- Κρυπτογράφηση από χρήστη ID:
 - Επιλογή $r \in \mathbb{Z}_q$
 - Υπολογισμός $t = e(y_{ID}, y)^r$
 - Κρυπτοκείμενο: $(g^r, m \oplus \mathcal{H}_{G_T}(t))$
- Αποκρυπτογράφηση:
 - Έστω κρυπτοκείμενο (a, b)
 - Αποκρυπτογράφηση ως $b \oplus \mathcal{H}_{G_T}(e(x_{ID}, a))$

$$\begin{aligned}e(y_{ID}, y)^r &= e(h, g^x)^r = e(h, g)^{xr} \\e(x_{ID}, a) &= e(y_{ID}^x, g^r) = e(h, g)^{xr} \\b \oplus \mathcal{H}_{\mathbb{G}_T}(e(x_{ID}, a)) &= \\m \oplus \mathcal{H}_{\mathbb{G}_T}(e(y_{ID}, y)^r) \oplus \mathcal{H}_{\mathbb{G}_T}(e(x_{ID}, a)) &= \\m \oplus e(h, g)^{xr} \oplus e(h, g)^{xr} &= \\m &= m\end{aligned}$$

Η ασφάλεια του κρυπτοσυστήματος βασίζεται στο BDDH.

Στην παραδοσιακή κρυπτογραφία δημοσίου κλειδιού η αποκρυπτογράφηση είναι όλα ή τίποτα:

Functional Encryption: Γενίκευση IBE

Στην παραδοσιακή κρυπτογραφία δημοσίου κλειδιού η αποκρυπτογράφηση είναι όλα ή τίποτα:

Functional Encryption: Γενίκευση IBE

Γενικό σχήμα

- TTP έχει ένα master secret key sk

Στην παραδοσιακή κρυπτογραφία δημοσίου κλειδιού η αποκρυπτογράφηση είναι όλα ή τίποτα:

Functional Encryption: Γενίκευση IBE

Γενικό σχήμα

- TTP έχει ένα master secret key sk
- Για συνάρτηση f παραγωγή sk_f

Στην παραδοσιακή κρυπτογραφία δημοσίου κλειδιού η αποκρυπτογράφηση είναι όλα ή τίποτα:

Functional Encryption: Γενίκευση IBE

Γενικό σχήμα

- TTP έχει ένα master secret key sk
- Για συνάρτηση f παραγωγή sk_f
- Αποκρυπτογράφηση: $c = \text{Enc}(pk, m)$ και sk_f

Στην παραδοσιακή κρυπτογραφία δημοσίου κλειδιού η αποκρυπτογράφηση είναι όλα ή τίποτα:

Functional Encryption: Γενίκευση IBE

Γενικό σχήμα

- TTP έχει ένα master secret key sk
- Για συνάρτηση f παραγωγή sk_f
- Αποκρυπτογράφηση: $c = \text{Enc}(pk, m)$ και sk_f
- Λήψη $f(m)$
- Ασφάλεια: καμία άλλη γνώση για το m

- Spam filters on encrypted mail με βάση τα κριτήρια του χρήστη (sk_f παράγεται από χρήστη)
- Επεξεργασία σε ιατρικά δεδομένα: Απόκρυψη πληροφοριών που ταυτοποιούν τα υποκείμενα
- Εύκολο access control
 - Attribute Based Encryption
 - Predicate Based Encryption

Μπορούν να γίνουν και με την παραδοσιακή κρυπτογραφία αλλά με πρόβληματα διαχείρισης πολλών κλειδιών

Συνδυασμός ZK και Pairings (κά) για αποδοτική επαλήθευση υπολογισμών

Συνδυασμός ZK και Pairings (κά) για αποδοτική επαλήθευση υπολογισμών

Εφαρμογές:

- Cloud computing
- Anonymous bitcoin (ZCash)

Συνδυασμός ZK και Pairings (κά) για αποδοτική επαλήθευση υπολογισμών

Εφαρμογές:

- Cloud computing
- Anonymous bitcoin (ZCash)

Μοντέλο

- Ο client έχει είσοδο u (π.χ query)

Συνδυασμός ZK και Pairings (κά) για αποδοτική επαλήθευση υπολογισμών

Εφαρμογές:

- Cloud computing
- Anonymous bitcoin (ZCash)

Μοντέλο

- Ο client έχει είσοδο u (π.χ query)
- Ο server έχει ιδιωτική είσοδο w (π.χ. ΒΔ)

Συνδυασμός ZK και Pairings (κά) για αποδοτική επαλήθευση υπολογισμών

Εφαρμογές:

- Cloud computing
- Anonymous bitcoin (ZCash)

Μοντέλο

- Ο client έχει είσοδο u (π.χ query)
- Ο server έχει ιδιωτική είσοδο w (π.χ. ΒΔ)
- Ο client θέλει να μάθει $z = f(u, w)$ για δημόσια γνωστή f

Συνδυασμός ZK και Pairings (κά) για αποδοτική επαλήθευση υπολογισμών

Εφαρμογές:

- Cloud computing
- Anonymous bitcoin (ZCash)

Μοντέλο

- Ο client έχει είσοδο u (π.χ query)
- Ο server έχει ιδιωτική είσοδο w (π.χ. ΒΔ)
- Ο client θέλει να μάθει $z = f(u, w)$ για δημόσια γνωστή f
- Client: ενδιαφέρεται για ορθότητα (integrity)

Συνδυασμός ZK και Pairings (κά) για αποδοτική επαλήθευση υπολογισμών

Εφαρμογές:

- Cloud computing
- Anonymous bitcoin (ZCash)

Μοντέλο

- Ο client έχει είσοδο u (π.χ query)
- Ο server έχει ιδιωτική είσοδο w (π.χ. ΒΔ)
- Ο client θέλει να μάθει $z = f(u, w)$ για δημόσια γνωστή f
- Client: ενδιαφέρεται για ορθότητα (integrity)
- Server: ενδιαφέρεται για διατήρησης μυστικότητας w

Συνδυασμός ZK και Pairings (κά) για αποδοτική επαλήθευση υπολογισμών

Εφαρμογές:

- Cloud computing
- Anonymous bitcoin (ZCash)

Μοντέλο

- Ο client έχει είσοδο u (π.χ query)
- Ο server έχει ιδιωτική είσοδο w (π.χ. ΒΔ)
- Ο client θέλει να μάθει $z = f(u, w)$ για δημόσια γνωστή f
- Client: ενδιαφέρεται για ορθότητα (integrity)
- Server: ενδιαφέρεται για διατήρησης μυστικότητας w

- **Zero Knowledge:** Ο client (verifier \mathcal{V}) μαθαίνει το αποτέλεσμα και αν ο υπολογισμός έγινε σωστά (χωρίς να μάθει βοηθητικά inputs του server)

Χαρακτηριστικά zkSNARKS

- **Zero Knowledge:** Ο client (verifier \mathcal{V}) μαθαίνει το αποτέλεσμα και αν ο υπολογισμός έγινε σωστά (χωρίς να μάθει βοηθητικά inputs του server)
- **Succinct:** Μικρή απόδειξη σε σχέση με τον υπολογισμό

Χαρακτηριστικά zkSNARKS

- **Zero Knowledge:** Ο client (verifier \mathcal{V}) μαθαίνει το αποτέλεσμα και αν ο υπολογισμός έγινε σωστά (χωρίς να μάθει βοηθητικά inputs του server)
- **Succinct:** Μικρή απόδειξη σε σχέση με τον υπολογισμό
 - σταθερή απόδειξη εξαρτάται μόνο από το μέγεθος της παράμετρου ασφάλειας $O_\lambda(1)$ δηλ. 288 bytes
 - χρόνος επαλήθευσης $O_\lambda(|f| + |u| + |z|)$ ανεξάρτητος από χρόνο εκτέλεσης f - 10msec

Χαρακτηριστικά zkSNARKS

- **Zero Knowledge:** Ο client (verifier \mathcal{V}) μαθαίνει το αποτέλεσμα και αν ο υπολογισμός έγινε σωστά (χωρίς να μάθει βοηθητικά inputs του server)
- **Succinct:** Μικρή απόδειξη σε σχέση με τον υπολογισμό
 - σταθερή απόδειξη εξαρτάται μόνο από το μέγεθος της παράμετρου ασφάλειας $O_\lambda(1)$ δηλ. 288 bytes
 - χρόνος επαλήθευσης $O_\lambda(|f| + |u| + |z|)$ ανεξάρτητος από χρόνο εκτέλεσης f - 10msec
- **Non Interactive:** Οι αποδείξεις δημιουργούνται από τον server μόνο και είναι δημόσια επαληθεύσιμες

Χαρακτηριστικά zkSNARKS

- **Zero Knowledge:** Ο client (verifier \mathcal{V}) μαθαίνει το αποτέλεσμα και αν ο υπολογισμός έγινε σωστά (χωρίς να μάθει βοηθητικά inputs του server)
- **Succinct:** Μικρή απόδειξη σε σχέση με τον υπολογισμό
 - σταθερή απόδειξη εξαρτάται μόνο από το μέγεθος της παράμετρου ασφάλειας $O_\lambda(1)$ δηλ. 288 bytes
 - χρόνος επαλήθευσης $O_\lambda(|f| + |u| + |z|)$ ανεξάρτητος από χρόνο εκτέλεσης f - 10msec
- **Non Interactive:** Οι αποδείξεις δημιουργούνται από τον server μόνο και είναι δημόσια επαληθεύσιμες
- **Arguments**

Χαρακτηριστικά zkSNARKS

- **Zero Knowledge:** Ο client (verifier \mathcal{V}) μαθαίνει το αποτέλεσμα και αν ο υπολογισμός έγινε σωστά (χωρίς να μάθει βοηθητικά inputs του server)
- **Succinct:** Μικρή απόδειξη σε σχέση με τον υπολογισμό
 - σταθερή απόδειξη εξαρτάται μόνο από το μέγεθος της παράμετρου ασφάλειας $O_\lambda(1)$ δηλ. 288 bytes
 - χρόνος επαλήθευσης $O_\lambda(|f| + |u| + |z|)$ ανεξάρτητος από χρόνο εκτέλεσης f - 10msec
- **Non Interactive:** Οι αποδείξεις δημιουργούνται από τον server μόνο και είναι δημόσια επαληθεύσιμες
- **Arguments**
- **of Knowledge**

Γενικό σχήμα:

1. Μετατροπή ελέγχου εγκυρότητας υπολογισμού σε έλεγχο ισότητας πολυωνύμων: (Code \rightarrow R1CS \rightarrow QSP \rightarrow Pairings)
εγκυρότητα $\leftrightarrow p(x)q(x) = s(x)r(x)$

Γενικό σχήμα:

1. Μετατροπή ελέγχου εγκυρότητας υπολογισμού σε έλεγχο ισότητας πολυωνύμων: (Code \rightarrow R1CS \rightarrow QSP \rightarrow Pairings)
εγκυρότητα $\leftrightarrow p(x)q(x) = s(x)r(x)$
2. Ο client επιλέγει μυστικό σημείο αποτίμησης:
 $p(x_0)q(x_0) = s(x_0)r(x_0)$

Γενικό σχήμα:

1. Μετατροπή ελέγχου εγκυρότητας υπολογισμού σε έλεγχο ισότητας πολυωνύμων: (Code \rightarrow R1CS \rightarrow QSP \rightarrow Pairings)
εγκυρότητα $\leftrightarrow p(x)q(x) = s(x)r(x)$
2. Ο client επιλέγει μυστικό σημείο αποτίμησης:
 $p(x_0)q(x_0) = s(x_0)r(x_0)$
3. Ομομορφική αποτίμηση:
 $\text{Enc}(p(x_0))\text{Enc}(q(x_0)) = \text{Enc}(s(x_0))\text{Enc}(r(x_0))$

Γενικό σχήμα:

1. Μετατροπή ελέγχου εγκυρότητας υπολογισμού σε έλεγχο ισότητας πολυωνύμων: (Code \rightarrow R1CS \rightarrow QSP \rightarrow Pairings)
εγκυρότητα $\leftrightarrow p(x)q(x) = s(x)r(x)$
2. Ο client επιλέγει μυστικό σημείο αποτίμησης:
 $p(x_0)q(x_0) = s(x_0)r(x_0)$
3. Ομομορφική αποτίμηση:
 $\text{Enc}(p(x_0))\text{Enc}(q(x_0)) = \text{Enc}(s(x_0))\text{Enc}(r(x_0))$
4. Τυχαιότητα για ZK:
 $\text{Enc}(k + p(x_0))\text{Enc}(k + q(x_0)) = \text{Enc}(k + s(x_0))\text{Enc}(k_r(x_0))$

Task

Έστω $\text{Enc}(x) = g^x$ όπου g γεννήτορας και $p(x) = \sum_{i=0}^d a_i x^i$

Μία οντότητα \mathcal{V} με γνώση του x_0 και μία οντότητα \mathcal{P} με γνώση του p μπορούν να υπολογίσουν το $\text{Enc}(p(x_0))$

Task

Έστω $\text{Enc}(x) = g^x$ όπου g γεννήτορας και $p(x) = \sum_{i=0}^d a_i x^i$

Μία οντότητα \mathcal{V} με γνώση του x_0 και μία οντότητα \mathcal{P} με γνώση του p μπορούν να υπολογίσουν το $\text{Enc}(p(x_0))$

- Ο \mathcal{V} δημοσιοποιεί:

$$\text{Enc}(x_0^0), \text{Enc}(x_0^1), \dots, \text{Enc}(x_0^d)$$

- Ο \mathcal{P} υπολογίζει:

$$\prod_{i=0}^d \text{Enc}(x_0^i)^{a_i} = \text{Enc}\left(\sum_{i=0}^d a_i x_0^i\right) = \text{Enc}(p(x_0))$$

Pairings: Έλεγχος σωστής αποτίμησης πολυωνύμων i

- Ο \mathcal{V} (γνωρίζει x_0):
 - υπολογίζει και δημοσιοποιεί:

$$\text{Enc}(x_0^0), \text{Enc}(x_0^1), \dots, \text{Enc}(x_0^d)$$

- επιλέγει παράγοντα b
- υπολογίζει και δημοσιοποιεί:

$$\text{Enc}(bx_0^0), \text{Enc}(bx_0^1), \dots, \text{Enc}(bx_0^d)$$

- Ο \mathcal{P} που γνωρίζει το $p(x)$:
 - υπολογίζει και δημοσιοποιεί: $\text{Enc}(p(x_0)), \text{Enc}(bp(x_0))$
- Τα μυστικά b, x_0 καταστρέφονται

Ο έλεγχος γίνεται ως εξής:

- Η συνάρτηση pairing e υπολογίζει:
 - $e(\text{Enc}(p(x_0)), \text{Enc}(b)) = e(g, g)^{bp(x_0)}$
 - $e(\text{Enc}(bp(x_0)), \text{Enc}(1)) = e(g, g)^{bp(x_0)}$

Παρατήρηση

- Ομομορφική πρόσθεση
- Πολλαπλασιασμός από το pairing
- Έλεγχοι για soundness και blinding ZK

1. Παγουρτζής, Α., Ζάχος, Ε., ΓΠ, 2015. Υπολογιστική κρυπτογραφία. [ηλεκτρ. βιβλ.] Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
2. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography 2nd edition, Chapman and Hall/CRC, 2015
3. Neal Koblitz and Alfred J. Menezes, [A riddle wrapped in an enigma](#)
4. Jeremy Kun [Introducing Elliptic Curves](#)
5. Andrea Corbellini [Elliptic Curve Cryptography: a gentle introduction](#)
6. Dan Shumow and Niels Ferguson [On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng](#), Crypto 2007 Rump Session
7. Antoine Joux. A one round protocol for tripartite diffie-hellman. In Algorithmic Number Theory,4th International Symposium,ANTS-IV,Leiden, The Netherlands, July 2-7, 2000, Proceedings, pages 385–394, 2000.
8. Dan Boneh, Ben Lynn, and Hovav Shacham. [Short signatures from the Weil pairing](#). Journal of Cryptology, 17(4):297–319, 2004. ISSN 0933-2790.
9. Dan Boneh and Matthew K. Franklin. [Identity-based encryption from the weil pairing](#). In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '01, pages 213–229, London, UK, UK, 2001. Springer-Verlag. ISBN 3-540-42456-3.
10. Boneh, Dan, Amit Sahai, and Brent Waters. [Functional encryption: a new vision for public-key cryptography](#), Communications of the ACM 55, no. 11 (2012): 56-64.
11. Vitalik Buterin [zkSNARKs: under the hood](#)
12. Alfred Menezes [An introduction to pairing based crypto](#)
13. [An introduction to pairing based crypto](#)
14. [3rd BIU Winter School on Cryptography 2013](#)