Ring Signatures

Panagiotis Grontas

15/04/2021

ΕΜΠ - Κρυπτογραφία ΙΙ (2020-2021)

Introduction

Motivation

- Ψηφιακές Υπογραφές: Δημόσια επαληθεύσιμες
  - Ακεραιότητα
  - Αυθεντικότητα
  - Μη - Αποκήρυξη
- Χωρίς ανωνυμία όμως...
- Η επαλήθευση γίνεται με συγκεκριμένο δημόσιο κλειδί, που δείχνει ποιος υπέγραψε

Δύο λύσεις:

- Ομαδικές υπογραφές (Group signatures)
- Υπογραφές δακτυλίου (Ring signatures) ή SAG (Spontaneous Anonymous Group signatures)

Group Signatures - [CH91]

- Η υπογραφή προέρχεται από μια ομάδα, όπου υπάρχει αρχηγός
- Διατηρείται ανωνυμία, ως προς το ποιο μέλος υπέγραψε
- Τα μέλη ορίζονται εξ'αρχής από τον αρχηγό
- Δυναμική ομάδα: Μπορούν να ανακληθούν (revocation) ή να προστεθούν καινούρια
- Ο αρχηγός μπορεί να αποκαλύψει ποιος υπέγραψε (traceability)

Ring Signatures - How to leak a secret [RST2001]

Οι ομάδες σχηματίζονται ad hoc από τον υπογράφοντα κατά την υπογραφή

- Η Alice είναι μέλος του υπουργικού συμβουλίου και θέλει να αποκαλύψει ένα σκάνδαλο στον Bob
- Ο Bob θέλει να πειστεί ότι η αποκάλυψη έρχεται από κάποιο μέλος του υπουργικού συμβουλίου
- Η Alice δεν μπορεί να υπογράψει κάποιο μήνυμα, γιατί θα αποκαλυφθεί από την επαλήθευση
- Δημιουργία δακτυλίου με όλα τα δημόσια κλειδιά των υπουργών
- Υπογραφή προέρχεται από το δακτύλιο
  - έγκυρη,
  - αλλά χωρίς να είναι δυνατόν να ταυτοποιηθεί ποιο μέλος του υπέγραψε

Ring signatures με Σ - Πρωτόκολλα [CDS94]

- Σ-Πρωτόκολλα: Honest Verifier Zero-Knowledge Proofs of Knowledge
- Fiat-Shamir heuristic: NIZK Δημιουργία υπογραφών
- Ύπαρξη simulator: Παραγωγή μη-διαχωρίσιμων συζητήσεων χωρίς witness
- Παραδείγματα:
  - Schnorr proof DLOG
  - Chaum-Pedersen proof of EQDLOG
- Συνδυασμός με secret-sharing scheme: Witness indistinguishable Proof of Knowledge

Ring signatures από OR-Schnorr [CDS94]

$$\text{NIZK}\{(L = \{y_i\}_{i=1}^n, \mathbb{G}, q, g), (x_k), y_k = g^{x_k}, k \in [n]\}$$

$\mathcal{S}$		V
Select $\{s_i, c_i \leftarrow\$ \mathbb{Z}_q\}\ i \in [n] \setminus \{k\}$		
Compute $\{z_i = g^{s_i} y_i^{c_i}\}\ i \in [n] \setminus \{k\}$		
Select $\{r_k \leftarrow\$ \mathbb{Z}_q\}$		
Compute $\{z_k = g^{r_k}\}$		
	$\xrightarrow{\{z_i\}_{i=1}^n}$	
		Compute $c = \mathrm{H}(L, m, \{z_i\}_{i=1}^n)$
	$\xleftarrow{c}$	
$c_k = c \oplus (\bigoplus_{i=1, i\neq k}^{n} c_i)$		
$s_k = r_k - x_k c_k$		
	$\xrightarrow{\sigma = \{(c_i, s_i)\}_{i=1}^n}$	
		Verify iff: $(\bigoplus_{i=1}^{n} c_i), \mathrm{H}(L, m, \{g^{s_i} y_i^{c_i}\}_{i=1}^n)$

Ring Signatures - Formal Definition

- $(\mathsf{sk}, \mathsf{pk}, \mathsf{prms}) \leftarrow \mathsf{KGen}(1^\lambda)$
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{prms}, \mathsf{sk}, L, m)$ με την προϋπόθεση ότι $\mathsf{pk} \in L$
- $\{0, 1\} \leftarrow \textbf{Verify}(\mathsf{prms}, L, m, \sigma)$

Ορθότητα:

$$\forall m, \forall (\mathsf{sk}, \mathsf{pk}, \mathsf{prms}) \leftarrow \mathsf{KGen}(1^\lambda), \forall L : \mathsf{pk} \in L :$$
$$\textbf{Verify}(\mathsf{prms}, L, m, \mathsf{Sign}(\mathsf{prms}, \mathsf{sk}, L, m)) = 1$$

Παρατήρηση:

Το L σχηματίζεται κατά τη διάρκεια της υπογραφής

Ring Signatures - Unforgeability

Existential Unforgeability under Chosen Message Attack:
$\mathbf{Pr}[\text{EUF-CMA}_{\mathcal{A},\Pi}(\lambda) = 1] = \text{negl}(\lambda)\ \forall PPT\mathcal{A}$

Algorithm 1: $\text{EUF-CMA}_{\mathcal{A},\Pi}$

Input : λ

Output: $\{0, 1\}$

$\text{prms} \leftarrow \Pi.\text{KGen}(1^{\lambda})$

$(n, L = \{\text{pk}_i\}_{i=1}^{n}, m) \leftarrow \mathcal{A}(\textbf{choose})$

$(L', m, \sigma) \leftarrow \mathcal{A}^{SO}(\textbf{forge}, \text{prms}, L)$

$\mu\varepsilon\ \sigma' \leftarrow SO(L'', m') : \Pi.\textbf{Verify}(L'', m', \sigma') = 1$

if $\Pi.\textbf{Verify}(L', m, \sigma) = 1$ **AND** $L' \subseteq L$ **AND** $(L', m, \sigma) \notin SO$ **then**
  return 1

else
  return 0

end

Ring Signatures - Signer ambiguity

Αδύνατο να ταυτοποιηθεί ποια οντότητα υπέγραψε
$\mathbf{Pr}[\mathrm{SA}_{\mathcal{A},\Pi}(\lambda) = 1] = \frac{1}{n}\ \forall \mathcal{A}$

Algorithm 2: $\mathrm{SA}_{\mathcal{A},\Pi}$

Input : λ

Output: $\{0, 1\}$

$\mathrm{prms} \leftarrow \Pi.\mathrm{KGen}(1^{\lambda})$

$(n, L = \{\mathrm{pk}_i\}_{i=1}^{n}, m) \leftarrow \mathcal{A}(\textbf{choose})$

$k \leftarrow\!\!\$\ [n]$

$\sigma \leftarrow \Pi.\mathrm{Sign}(\mathrm{sk}_k, L, m)$

$i \leftarrow \mathcal{A}(\textbf{guess}, L, m, \sigma)$

if $i = k$ **then**
  return 1
else
  return 0
end

Linkable Ring Signatures

Linkable Ring Signatures

Ring signatures όπου δίνεται η δυνατότητα να ελεγχθεί αν δύο υπογραφές προέρχονται από το ίδιο μέλος (χωρίς να αποκαλυφθεί η ταυτότητά του)

$$\mathsf{Link}(\mathsf{prms}, L, m_1, \sigma_1, m_2, \sigma_2) = 1 \Leftrightarrow$$
$$\sigma_1 = \mathsf{Sign}(\mathsf{prms}, \mathsf{sk}, L, m_1) \text{ AND } \sigma_2 = \mathsf{Sign}(\mathsf{prms}, \mathsf{sk}, L, m_2)$$
$$\mathsf{Verify}(\mathsf{prms}, L, m_1, \sigma_1) = 1 \text{ AND } \mathsf{Verify}(\mathsf{prms}, L, m_2, \sigma_2) = 1$$

Linkable Ring Signatures - Signer Ambiguity

Algorithm 3: $\mathsf{SA}_{\mathcal{A},\Pi,t}$

Input : λ, n

Output: $\{0,1\}$

$\mathsf{prms} \leftarrow \Pi.\mathsf{KGen}(1^\lambda)$

$(n, L = \{\mathsf{pk}_i\}_{i=1}^{n}, m) \leftarrow \mathcal{A}(\textbf{choose})$

$D_t = \{\hat{s_1}, \cdots, \hat{s_t}\} \leftarrow \mathcal{A}(\textbf{corrupt})$

$k \leftarrow\$ [n]$

$\sigma \leftarrow \Pi.\mathsf{Sign}(\mathsf{sk}_k, L, m)$

$i \leftarrow \mathcal{A}(\textbf{guess}, L, m, \sigma, D_t)$

return

$i = k \,\textbf{AND}\, i \notin D_t \,\textbf{AND}\, 0 \leq t < n-1$

$\textbf{Pr}[\mathsf{SA}_{\mathcal{A},\Pi}(\lambda) = 1] \leq \frac{1}{n-t} - \mathsf{negl}(\lambda)$

- Ο $\mathcal{A}$ μπορεί να εκμεταλλευθεί το linkability συγκρίνοντας με όλους τους δακτύλιους που αποτελούνται από ένα κλειδί
- Απενοχοποίηση (exculpability): Ακόμα και αν ο $\mathcal{S}$ αποκαλύψει το ιδιωτικό του κλειδί δεν μπορεί να πείσει ότι υπέγραψε
- Σε κάποιες περιπτώσεις μπορεί να απαιτείται ενοχοποίηση (culpability)

Linkable Ring Signatures - Linkability 1

Αποσύνδεση 'συνδεδεμένων' υπογραφών

Algorithm 4: $\mathsf{LinkGame}_{\mathcal{A},\Pi}$

Input : λ

Output: $\{0,1\}$

$\mathsf{prms} \leftarrow \Pi.\mathsf{KGen}(1^\lambda)$

$(n, L = \{\mathsf{pk}_i\}_{i=1}^{n}, m_1, m_2) \leftarrow \mathcal{A}(\textbf{choose})$

$\mathsf{sk}_{k_1} \leftarrow \mathcal{A}(\textbf{corrupt})$

if $\mathsf{sk}_{k_1} \notin L$ **then**

  abort

end

$(\sigma_1, \sigma_2) \leftarrow \mathcal{A}(\mathsf{sk}_{k_1}, L, m_1, m_2)$

return $\Pi.\textbf{Verify}(L, m_1, \sigma_1) = 1$ **AND** $\Pi.\textbf{Verify}(L, m_2, \sigma_2) = 1$ **AND** $\Pi.\mathsf{Link}(L, m_1, \sigma_1, m_2, \sigma_2) = 0$

$\textbf{Pr}[\mathsf{LinkGame}_{\mathcal{A},\Pi}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$

Unforgeability $\Rightarrow$ 2 ασύνδετες υπογραφές δημιουργούνται με διαφορετικά κλειδιά

Linkable Ring Signatures - Linkability 2

Σύνδεση 'ασύνδετων' υπογραφών - Παγίδευση έντιμων χρηστών (non slanderability)

Algorithm 5: $\mathsf{LinkGame}_{\mathcal{A},\Pi}$

Input : λ

Output: $\{0,1\}$

$\mathsf{prms} \leftarrow \pi.\mathsf{KGen}(1^\lambda)$

$(n, L = \{\mathsf{pk}_i\}_{i=1}^{n}, m_1, m_2) \leftarrow \mathcal{A}(\textbf{choose})$

$\mathsf{pk}_{k_1} \leftarrow \mathcal{A}(\textbf{choose})$ // *Επιλογή θύματος*

$\sigma_1 \leftarrow \Pi.\mathsf{Sign}(\mathsf{sk}_{k_1}, L, m_1)$

$\sigma_2 \leftarrow \mathcal{A}(L, m_1, m_2, \sigma_1)$

return $\sigma_1 \neq \sigma_2$ **AND** $\Pi.\mathsf{Verify}(L, m_1, \sigma_2) =$
1 **AND** $\Pi.\mathsf{Link}(L, m_1, \sigma_1, m_2, \sigma_2) = 1$

$\mathbf{Pr}[\mathsf{LinkGame}_{\mathcal{A},\Pi}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$

Linkable Ring Signatures Construction - LWW04 - KGen

Algorithm 6: KGen

Input : λ

Output: prms

/* $\mathbb{G}$ *ομάδα τάξης* q *πρώτου και γεννήτορα* g *με δύσκολο DDH* */

/* $\mathrm{H}_{\mathbb{G}}$ *Συνάρτηση σύνοψης* $\{0,1\}^* \to \mathbb{G}$ */

/* H_q *Συνάρτηση σύνοψης* $\{0,1\}^* \to \mathbb{Z}_q$ */

return $\mathbb{G}, g, q, \mathrm{H}_{\mathbb{G}}, \mathrm{H}_q$

/* *Each user:* */

$x \leftarrow\$ \mathbb{Z}_q$

$y \leftarrow g^x$

Linkable Ring Signatures Construction - LWW04 - Sign

Algorithm 7: Sign_k

Input : $m \in \{0,1\}^*, x_k, \text{prms}$

Output: σ

/ Επιλογή δημοσίων κλειδιών και σχηματισμός L */*

$L \leftarrow \{y_1, y_2, \cdots, y_n\}$

$h \leftarrow H_{\mathbb{G}}(L)$

$\hat{y} \leftarrow h^{x_k}$

$u \leftarrow\$ \mathbb{Z}_q$

$c_{k+1} \leftarrow H_q(L, \hat{y}, m, g^u, h^u)$

for $i \in \{k+1 \cdots n, 1 \cdots k-1\}$ **do**

  $s_i \leftarrow\$ \mathbb{Z}_q$

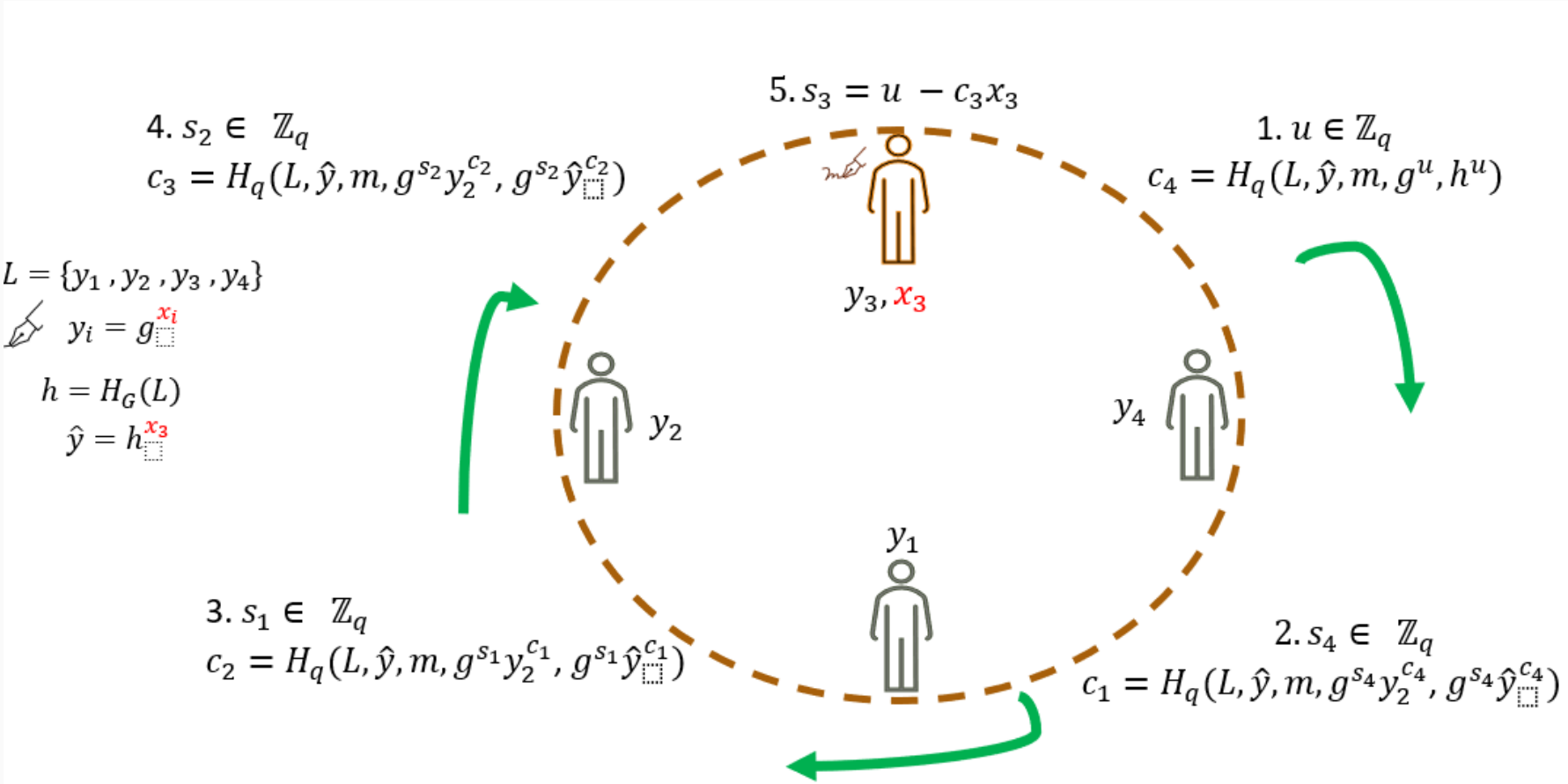
  $c_{i+1} \leftarrow H_q(L, \hat{y}, m, g^{s_i} y_i^{c_i}, g^{s_i} \hat{y}^{c_i})$

end

$s_k \leftarrow u - x_k c_k$

return $\sigma_L = (c_1, s_1, \cdots, s_n, \hat{y}, L)$

Linkable Ring Signatures Construction - LWW04 - Sign



Linkable Ring Signatures Construction - LWW04 - Verify

Algorithm 8: Verify

Input : $m \in \{0,1\}^*, \sigma_L, m, \text{prms}$

Output: $\{0,1\}$

/ Υπενθύμιση:* $\sigma_L = (c_1, s_1, \cdots, s_n, \hat{y}, L)$ **/*

$h \leftarrow H_{\mathbb{G}}(L)$

for $i \in \{1 \cdots n\}$ **do**

  $c_{i+1} \leftarrow H_q(L, \hat{y}, m, g^{s_i} y_i^{c_i}, g^{s_i} \hat{y}^{c_i})$

end

if $c_{n+1} = c_1$ **then**

  return 1

else

  return 0

end

Linkable Ring Signatures Construction - LWW04 - *Link*

Algorithm 9: *Link*

Input : $L, \sigma_L, \sigma'_L, m, m'$

Output: $\{0, 1\}$

/ Υπενθύμιση:* $\sigma_L = (c_1, s_1, \cdots, s_n, \hat{y}, L)$ **/*

if Verify$(\text{prms}, L, m, \sigma_L) =$ Verify$(\text{prms}, L, m', \sigma'_L) = 1$ **AND** $\hat{y} = \hat{y}'$

then

  return 1

else

  return 0

end

Culpability: Με δεδομένο ένα ιδιωτικό κλειδί x_i έλεγχος αν

$\exists y_i \in L : y_i = g^{x_i}$ **AND** $\hat{y} = \mathrm{H}_{\mathbb{G}} L^{x_i}$

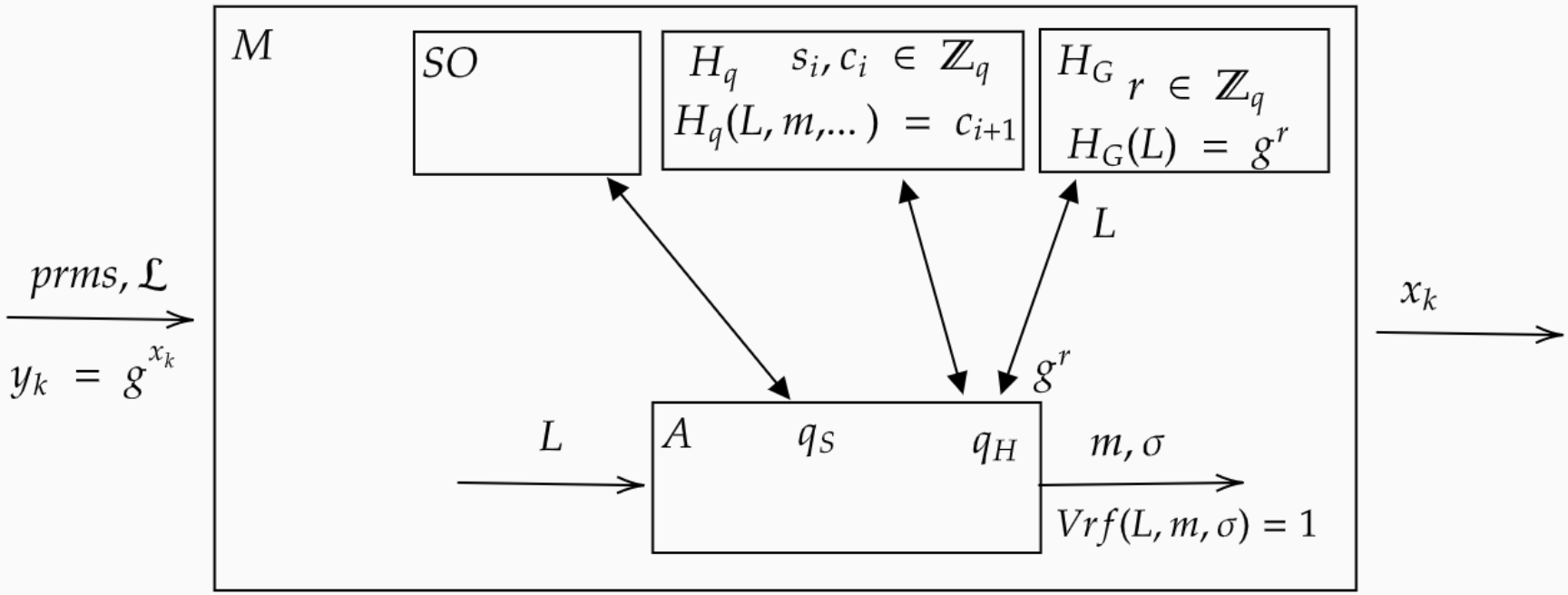
Ανάλυση Ασφάλειας

Theorem
Αν DLP δύσκολο στην $\mathbb{G}$ τότε οι LSAG διαθέτουν EUF-CMA.

Theorem
Αν ισχύει η υπόθεση DDH στην $\mathbb{G}$ τότε οι LSAG διαθέτουν signer-ambiguity.

Theorem
Αν DLP δύσκολο στην $\mathbb{G}$ τότε οι LSAG είναι linkable για τον ίδιο δακτύλιο.

Unforgeability analysis i



Αν ο $\mathcal{A}$ καταφέρει να δημιουργήσει πλαστογράφηση με μη-αμελητέα πιθανότητα, τότε ο $\mathcal{M}$ μπορεί να λύσει τον διακριτό λογάριθμο για κάποιο στοιχείο της $\mathbb{G}$.

Unforgeability analysis ii

Βήμα 1: Αν γίνει πλαστογράφηση με μη αμελητέα πιθανότητα, τότε προηγουμένως έχουν ρωτηθεί τα oracles $H_q, H_{\mathbb{G}}$ για όλες τις τιμές που εμφανίζονται στην επαλήθευση

Βήμα 2: Καταγράφουμε τα queries που γίνονται για την επαλήθευση της πλαστογράφησης σε δείκτες $i_1, \cdots, i_n$. Για κάθε επιτυχή πλαστογράφηση (με transcript T) κάνουμε rewind τον $\mathcal{A}$ στην θέση i_1. Με μη αμελητέα πιθανότητα θα ξαναγίνει πλαστογράφηση (με transcript T').

Unforgeability analysis iii

Βήμα 3: Για κάποιο στοιχείο $g^u = g^{s_k + x_k c_k}$ στο T και $g^u = g^{s'_k + x_k c'_k}$ και στο T'. Από αυτά υπολογίζουμε το x_k:

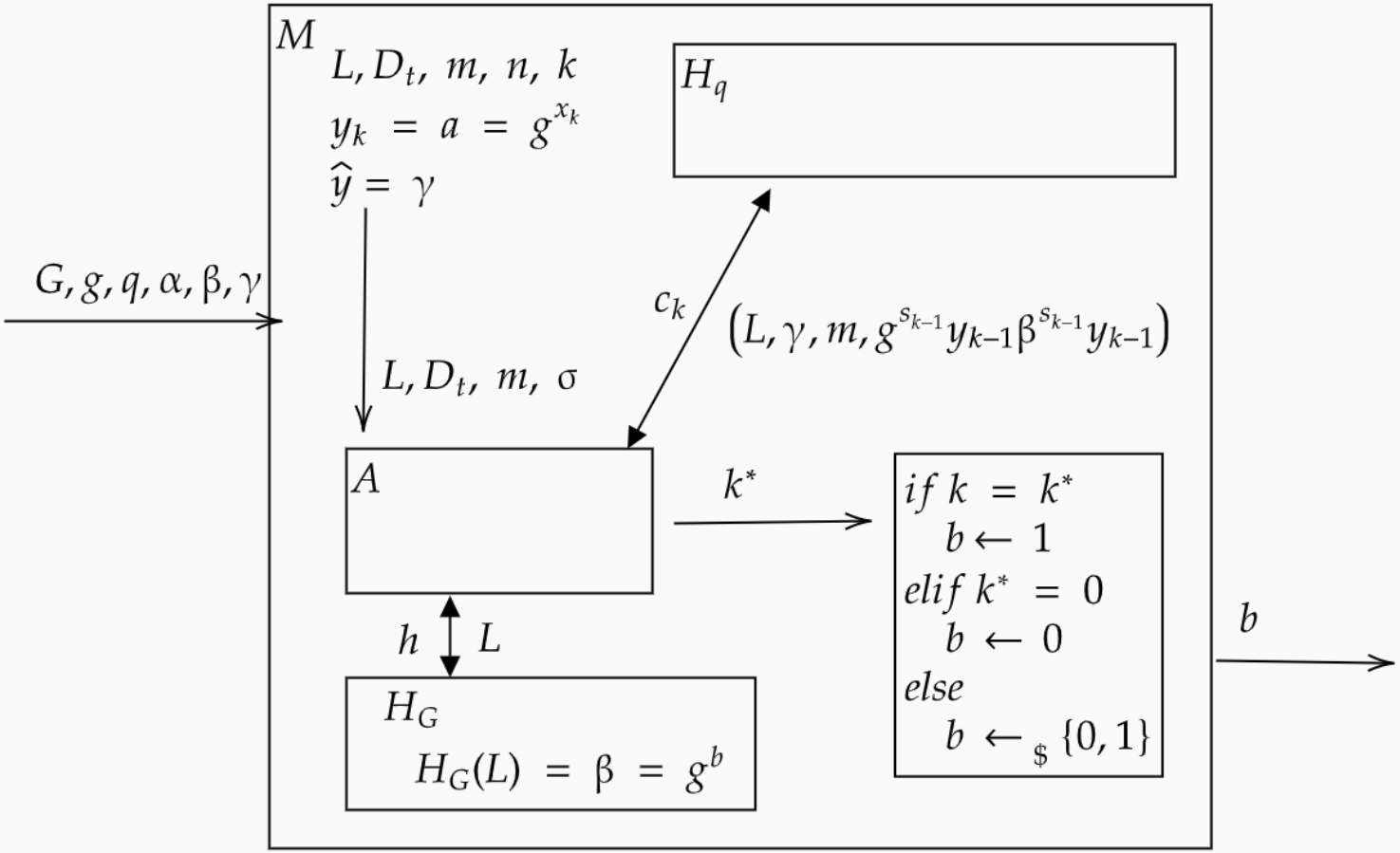
$$
\begin{aligned}
g^{s_k + x_k c_k} = g^{s'_k + x_k c'_k} &\Rightarrow \\
s_k + x_k c_k = s'_k + x_k c'_k &\Rightarrow \\
x_k (c_k - c'_k) = s'_k - s_k &\Rightarrow \\
x_k = \frac{s'_k - s_k}{c_k - c'_k}
\end{aligned}
$$

Privacy analysis i

Τρεις περιπτώσεις:

- $\mathrm{sk}_\pi \in D_t$
  Ανάκτηση $\hat{y}$ από υπογραφή.
  Δοκιμή $\forall \mathrm{sk} \in D_t$ αν $\hat{y} = h^{\mathrm{sk}}$
- $|D_t| = n - 1$
  Ο χρήστης που μένει είναι ο υπογράφων
- $0 \leq |D_t| < n - 1$
  Χρήση $\mathcal{A}$ που σπάει το signer ambiguity
  Κατασκευή μιας υπογραφής σ τέτοιας ώστε για $\pi \in [n]$:
  $\mathrm{pk}_\pi = \alpha \in \mathbb{G} = g^a, a \in \mathbb{Z}_q (a = \mathrm{sk}_\pi)$
  $h = \beta \in \mathbb{G} = g^b, b \in \mathbb{Z}_q$ με προγραμματισμό του RO $\mathrm{H}_{\mathbb{G}}$ για είσοδο L
  $\hat{y} = \gamma = h^a = g^{ab}$
  Χρήση $\mathcal{A}$ για εντοπισμό π
  Επίλυση προβλήματος DDH

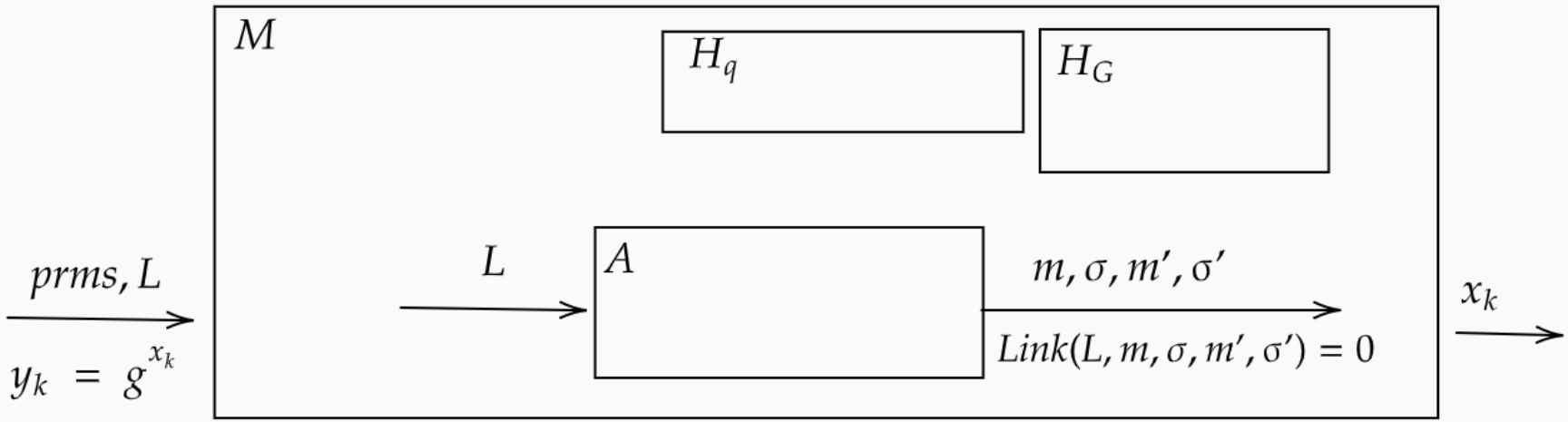
Privacy analysis ii



Μη αμελητέα πιθανότητα σπασίματος signer ambiguity $\Rightarrow$ Μη αμελητέα πιθανότητα επίλυσης DDH problem

Linkability analysis

1. Αν το DLP είναι δύσκολο και ο $\mathcal{A}$ γνωρίζει μόνο ένα κλειδί sk_k τότε για μια έγκυρη υπογραφή που παράγει σ_{sk_k} ισχύει $\hat{y} = \mathsf{H}_{\mathbb{G}}(L)^{\mathsf{sk}_k}$



2. Αν ο $\mathcal{A}$ δημιουργήσει δύο unlinkable υπογραφές τότε $\hat{y} \neq \hat{y}' \Rightarrow \mathsf{sk} \neq \mathsf{sk}'$. Αλλά ο $\mathcal{A}$ διαθέτει μόνο ένα ιδιωτικό κλειδί.

Applications

Το Bitcoin δεν είναι ανώνυμο

Επιθέσεις:

- Linkability: έλεγχος αν δύο συναλλαγές καταλήγουν στην ίδια διεύθυνση
- Traceability: προσδιορισμός ποιες συναλλαγές ξοδεύονται σε μια συναλλαγή

Οι προσωρινές διεύθυνσεις που παρέχει το Bitcoin δεν είναι ασφαλείς απέναντι σε σοβαρή Ανάλυση

Λύσεις:

- Mixers
- Zerocash
- Monero: Ring signatures for untraceability

Monero Ring Confidential Transactions

Βασική ιδέα: Απόκρυψη δημόσιου κλειδιού μιας συναλλαγής σε ring με δημόσια κλειδιά.

Υλοποίηση: LSAG με δύο τροποποιήσεις.

1. Linkability με μεταβλητο δακτύλιο (Back LSAG)

$$\hat{y} \leftarrow \mathrm{H}(y_k)^{x_k}$$
$$c_{k+1} \leftarrow H_q(m, g^u, \mathrm{H}(y_k)^u)$$
$$c_{i+1} \leftarrow H_q(m, g^{s_i} y_i^{c_i}, \mathrm{H}(y_i{}^{s_i})\hat{y}^{c_i})$$

Monero Ring Confidential Transactions

2. Multilayer LSAG: Δυνατότητα δημιουργίας *multi-input transactions* - Δυνατότητα υπογραφής με m ιδιωτικά κλειδιά

Δακτύλιος $L = \{y_{ij}\}_{i=1,j=1}^{n,m}$ για τα οποία είναι γνωστά τα ιδιωτικά κλειδιά $\{x_{kj}\}_{j=1}^{m}$

Linkability: Χρήση οποιουδήποτε από τα γνωστά κλειδιά

$$\{\hat{y}_j \leftarrow \mathrm{H}(y_{kj})^{x_{kj}}\}_{j\in[m]}$$
$$c_{k+1} \leftarrow H_q(m, \{(g^{u_j}, \mathrm{H}({y_{kj}}^{u_j}))\}_{j\in[m]}$$
$$c_{i+1} \leftarrow H_q(m, \{g^{s_{ij}} y_{ij}^{c_i}, \mathrm{H}({y_{ij}}^{s_{ij}})\hat{y}_j^{c_i}\}_{j\in[m]}) \qquad i \in [n]$$
$$\sigma = (\{\hat{y}_j\}_{j\in[m]}, c_1, \{s_{ij}\}_{i\in[n],j\in[m]})$$

Πολυπλοκότητα: $\mathcal{O}(mn)$

Ανώνυμα Δημοψηφίσματα - Εκλογές

Βασική υπόθεση: Όλοι οι n ψηφοφόροι έχουν μια λίστα από ιδιωτικά και δημόσια κλειδιά (x_i, y_i)

L: Όλα τα δημόσια κλειδιά

- Κωδικοποίηση m_{yes}, m_{no}
- Ψηφοφορία: Δημιουργία υπογραφής LSAG για την επιλογή του ψηφοφόρου. Κατάθεση σε ανώνυμο κανάλι.
- Καταμέτρηση: Επαλήθευση υπογραφών και καταμέτρηση.

Ανώνυμα Δημοψηφίσματα - Εκλογές

Ιδιότητες:

- Ορθότητα: Διπλοψηφίες αποτρέπονται λόγω linkability
- Επαληθευσιμότητα: Η καταμέτρηση είναι δημόσια και μπορεί να γίνει από τον καθένα
- Ανωνυμία: Signer ambiguity + ανώνυμο κανάλι

Προβλήματα:

- Vote selling-coercion: Μπορεί να αποδειχθεί πώς ψήφισε κάποιος αποκαλύπτοντας το ιδιωτικό κλειδί x_i
- (In)Efficiency: Δημιουργία υπογραφής $\mathcal{O}(n)$

Open questions

- Συνδυασμός Ring Signatures με Decentralized Voting για να επιτευχθούν ισχυρότερες εγγυήσεις ιδιωτικότητας
- Για παράδειγμα: αντίσταση στον εξαναγκασμό (coercion resistance)
- Χρειάζεται ιδιωτικό κανάλι με τον καταμέτρηση
- Ασύμβατο με το self tallying

Βιβλιογραφία

1. Rivest R.L., Shamir A., Tauman Y. (2001) How to Leak a Secret. In ASIACRYPT 2001.
2. Chaum D., van Heyst E. (1991) Group Signatures. In EUROCRYPT '91. EUROCRYPT 1991.
3. Cramer R., Damgård I., Schoenmakers B. (1994) Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In CRYPTO 1994
4. Abe M., Ohkubo M., Suzuki K. (2002) 1-out-of-n Signatures from a Variety of Keys. In ASIACRYPT 2002.
5. Liu J.K., Wei V.K., Wong D.S. (2004) Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups. In ACISP 2004.
6. Liu J.K., Wong D.S. (2005) In ICCSA 2005.
7. Shen Noether (2015), Ring Signature Confidential Transactions for Monero, eprint 2015/1098