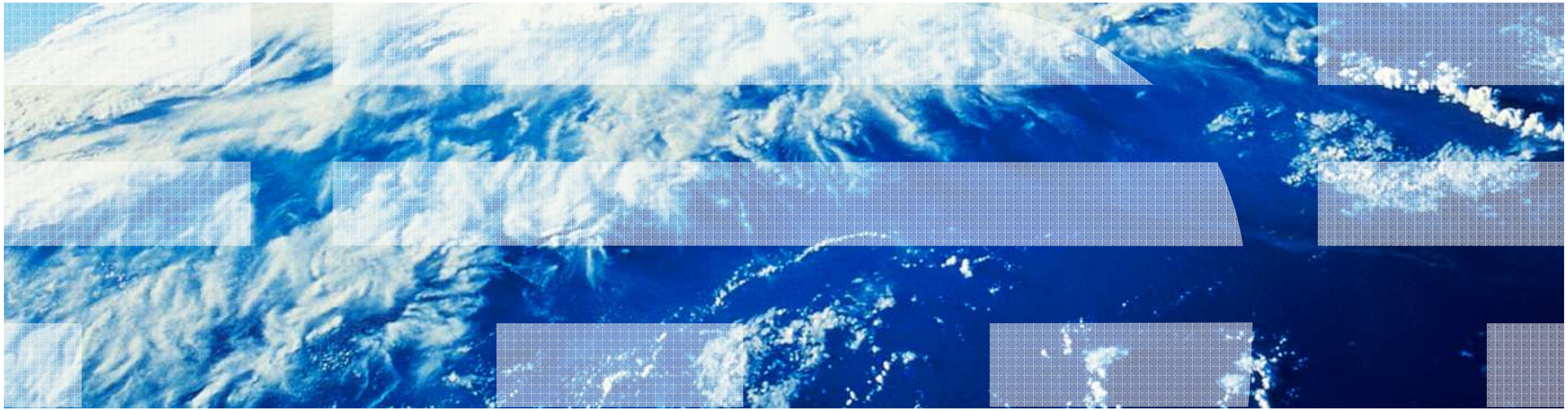
Fully anonymous attribute tokens from lattices

Jan Camenisch (IBM Research – Zurich)
Gregory Neven (IBM Research – Zurich)
Markus Rückert



“Elevator pitch”

- Goal:

  Anonymous credentials from lattices

- Starting point:

  GKV group signatures [Gordon, Katz, Vaikuntanathan, Asiacrypt 2010]

- Our contributions:
  - Anonymous attribute tokens (AAT)

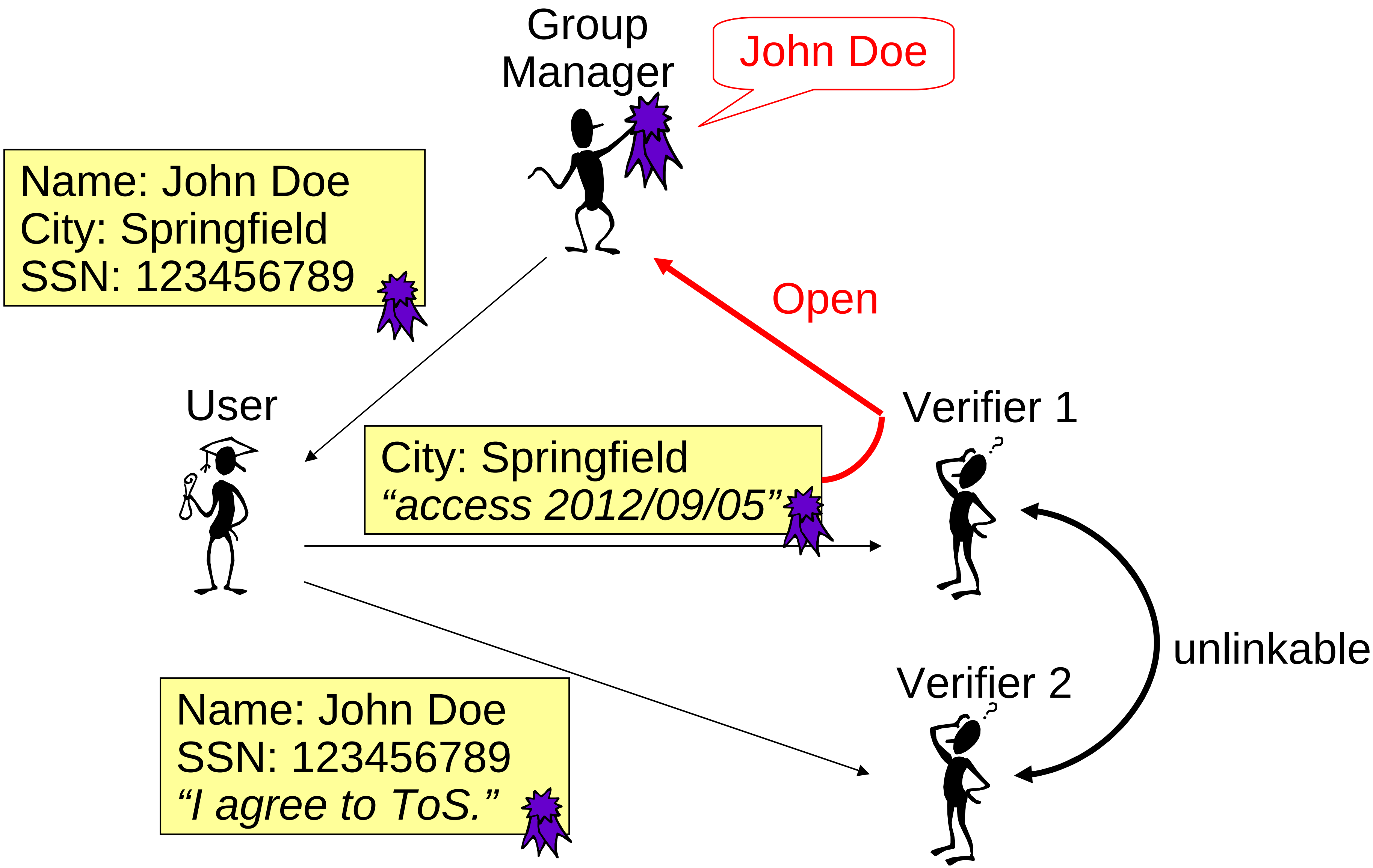
    ≈ anonymous credentials “light”
  - Scheme without opening (AAT−O)
  - Scheme with opening (AAT+O), full CCA anonymity
  - Extension adding non-frameability

- Open problems:
  - Constant token size, currently O(#users)
  - Full-fledged anonymous credentials

Overview

- Anonymous attribute tokens
- Lattice preliminaries
- GKV group signatures
- Our AAT−O scheme: construction sketch
- Our AAT+O scheme: construction idea
- Conclusion & open problems

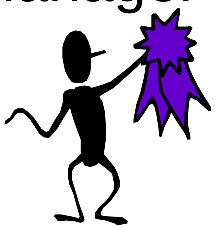
Usage scenario



Anonymous attribute tokens

without opening (AAT−O)

Group Manager



MKeyGen(1^n,U) → (mpk,msk)

Issue(msk,u,a_1,…,a_ℓ) → $cred_u$

mpk, $cred_u$

mpk

User u

$(a_i)_{i\in R}$,M,t

Verifier

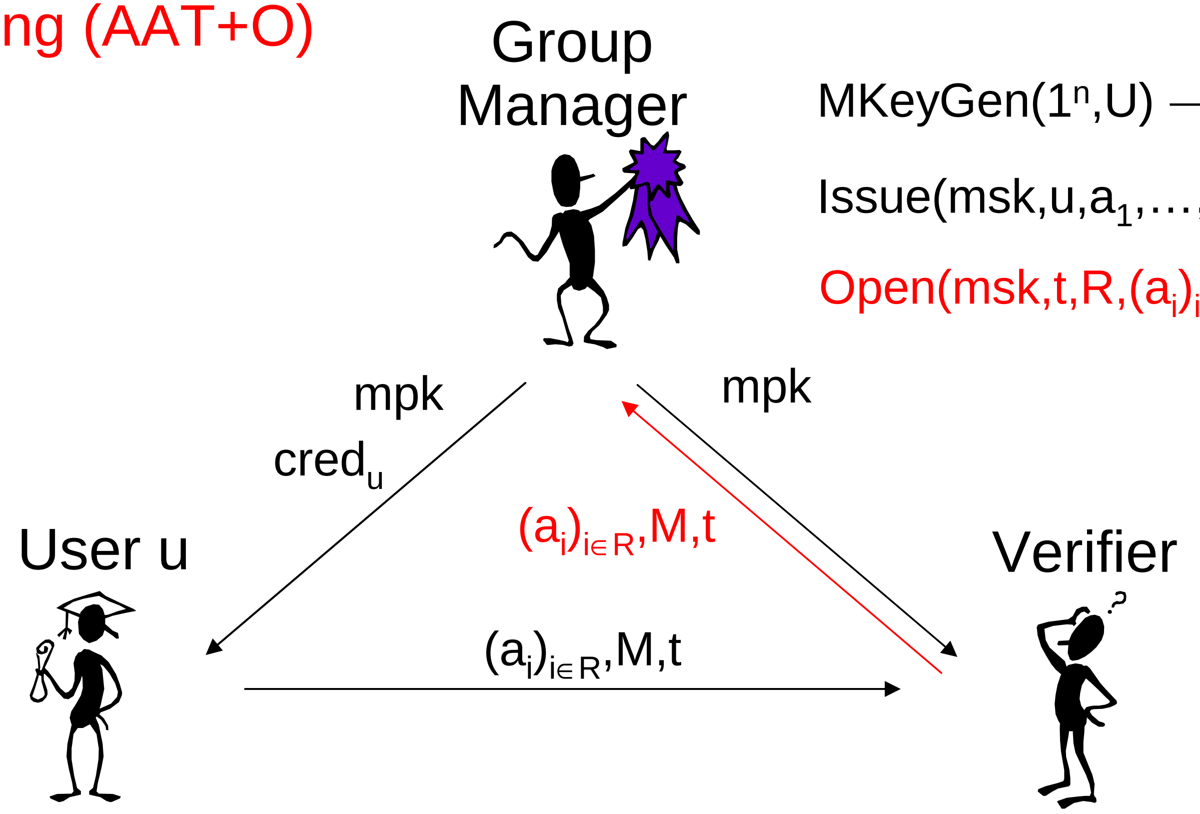
GenToken(mpk,$cred_u$,R,M) → t
where R ⊆ [1,ℓ]

VToken(mpk,t,R,$(a_i)_{i\in R}$,M) → 0/1

cf. minimal disclosure tokens (U-Prove), anonymous credentials [Cha81], attribute-based signatures [MPR11]

Anonymous attribute tokens

with opening (AAT+O)



$MKeyGen(1^n, U) \rightarrow (mpk, msk)$

$Issue(msk, u, a_1, \ldots, a_\ell) \rightarrow cred_u$

$Open(msk, t, R, (a_i)_{i \in R}, M) \rightarrow u$

$GenToken(mpk, cred_u, R, M) \rightarrow t$
where $R \subseteq [1, \ell]$

$VToken(mpk, t, R, (a_i)_{i \in R}, M) \rightarrow 0/1$

cf. anonymous credentials [Cha81], attribute-based group signatures

Security of anonymous attribute tokens

With opening (AAT+O)

- Full anonymity (CCA):

  Tokens are unlinkable, "modulo" revealed attributes

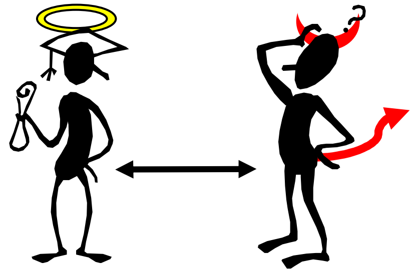
  – Input mpk

  – Oracles Init($u,a_1,\ldots,a_\ell$), Issue(u) $\rightarrow$ $cred_u$, Open($t,R,(a_i)_{i\in R},M$) $\rightarrow$ u

  – Output (u_0,u_1,R,M) where $a_{0,i} = a_{1,i}$ for all $i\in R$

  – Challenge $t^* \leftarrow$ GenToken($mpk,cred_{ub},R,M$)

  – Guess b



- Traceability:

  Can't create token with new attributes or opening to honest user

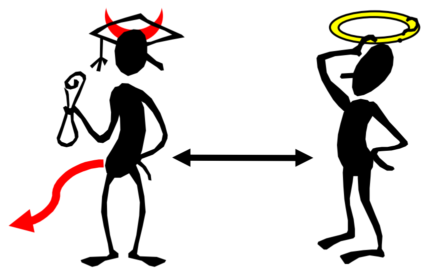
  – Input mpk

  – Oracles Init, Issue, Open, GenToken(u,R,M) $\rightarrow$ t

  – Output t^*, R^*, $(a_i^*)_{i\in R^*}$, M^* such that t^* opens to u^* and

    • u^* was never queried to Issue, or

    • u^* was initialized with $a_i \neq a_i^*$



Without opening (AAT−O): anonymity & unforgeability

Overview

- Anonymous attribute tokens
- Lattice preliminaries
- GKV group signatures
- Our AAT−O scheme: construction idea
- Our AAT+O scheme: construction idea
- Conclusion & open problems

Lattice preliminaries

Trapdoor one-way function from short integer solution (SIS) [GPV08]

$\mathbf{A} \in Z_q^{n \times m}$ with trapdoor $\mathbf{T} \in Z_q^{m \times m}$

$\mathbf{y} = \mathbf{A}\mathbf{x} \pmod q$ for $\mathbf{x}$ short, Gaussian distribution

invert using

- trapdoor $\mathbf{T} \rightarrow$ short preimage $\mathbf{x}$
- Gaussian elimination $\rightarrow$ long preimage $\mathbf{x}$

FDH-signature: $\mathbf{A}\boldsymbol{\sigma} = H(M)$ and $\boldsymbol{\sigma}$ short

“Verifiable encryption” from learning with errors (LWE) [Reg09,GKV10]

$\mathbf{B} \in Z_q^{n \times m}$ with trapdoor $\mathbf{S} \in Z_q^{m \times m}$

$\mathrm{Enc}_{\mathbf{B}}(\boldsymbol{\sigma}) = \boldsymbol{\tau}$ such that $\mathbf{A}\boldsymbol{\tau} = H(M) \bmod q$

decrypt using $\mathbf{S}$

Overview

- Anonymous attribute tokens
- Lattice preliminaries
- GKV group signatures
- Our AAT−O scheme: construction idea
- Our AAT+O scheme: construction idea
- Conclusion & open problems

GKV group signatures: construction idea

- Key generation

  For all users u = 1,…,U generate $(\mathbf{A}_u,\mathbf{T}_u)$, $(\mathbf{B}_u,\mathbf{S}_u)$

  $$\text{mpk} = (\mathbf{A}_u,\mathbf{B}_u)_{u=1\ldots U} \quad ; \quad \text{msk} = (\mathbf{S}_u)_{u=1\ldots U} \quad ; \quad \text{sk}_u = \mathbf{T}_u$$

- Group signature by user u on message M

  Compute short $\boldsymbol{\sigma}_u$: $\mathbf{A}_u\boldsymbol{\sigma}_u = H(M)$ using $\mathbf{T}_u$

  For v ≠ u compute long $\boldsymbol{\sigma}_v$: $\mathbf{A}_v\boldsymbol{\sigma}_v = H(M)$ using Gaussian elimination

  For v = 1,…,U encrypt $\boldsymbol{\tau}_v = \text{Enc}_{\mathbf{B}v}(\boldsymbol{\sigma}_v)$

  Non-interactive witness-indistinguishable proof (NIWIP)

  $$\pi_{OR} \leftarrow \text{NIWIP}\{\boldsymbol{\tau}_1 \text{ encrypts short } \boldsymbol{\sigma}_1 \vee \ldots \vee \boldsymbol{\tau}_U \text{ encrypts short } \boldsymbol{\sigma}_U\}$$

  Return $(\boldsymbol{\tau}_1,\ldots,\boldsymbol{\tau}_U,\pi_{OR})$

- Verification

  For v = 1,…,U check $\mathbf{A}\boldsymbol{\tau}_v = H(M)$

  Verify π_{OR}

- Opening

  For v = 1,…,U decrypt $\boldsymbol{\sigma}_v = \text{Dec}_{\mathbf{S}v}(\boldsymbol{\tau}_v)$ until $\boldsymbol{\sigma}_v$ short

Overview

- Anonymous attribute tokens
- Lattice preliminaries
- GKV group signatures
- Our AAT−O scheme: construction idea
- Our AAT+O scheme: construction idea
- Conclusion & open problems

Our AAT−O scheme: construction sketch

- Master key generation

  mpk = $\mathbf{A}$; msk = $\mathbf{T}$; common reference string $\mathbf{B}$

- Issuance for attributes $a_1,\ldots,a_\ell$

  For $i = 1,\ldots,\ell$ compute short $\boldsymbol{\sigma}_{u,i}$: $\mathbf{A}\boldsymbol{\sigma}_{u,i} = H(u,i,a_i)$ using $\mathbf{T}$

  Return $\text{cred}_u = (a_1,\ldots,a_\ell, \boldsymbol{\sigma}_{u,1},\ldots,\boldsymbol{\sigma}_{u,\ell})$

- Token generation by user u revealing attributes $R \subseteq [1,\ell]$, message M

  For $i \in R$ use $\boldsymbol{\sigma}_{u,i}$ from cred_u

  For $v \neq u$, $i \in R$ compute $\boldsymbol{\sigma}_{v,i}$: $\mathbf{A}\boldsymbol{\sigma}_{v,i} = H(v,i,a_i)$ using Gaussian elimination

Same-signer aggregation

If $\mathbf{A}\boldsymbol{\sigma}_i = H(M_i)$ with short $\boldsymbol{\sigma}_i$

Then $\mathbf{A}\boldsymbol{\alpha} = \mathbf{A} \sum \boldsymbol{\sigma}_i = \sum H(M_i)$ with "somewhat short" $\boldsymbol{\alpha}$

Our AAT−O scheme: construction sketch

- Master key generation

  mpk = $\mathbf{A}$; msk = $\mathbf{T}$; common reference string $\mathbf{B}$

- Issuance for attributes $a_1,\ldots,a_\ell$

  For $i = 1,\ldots,\ell$ compute short $\boldsymbol{\sigma}_{u,i}$: $\mathbf{A}\boldsymbol{\sigma}_{u,i} = H(u,i,a_i)$ using $\mathbf{T}_u$

  Return $\text{cred}_u = (a_1,\ldots,a_\ell, \boldsymbol{\sigma}_{u,1},\ldots,\boldsymbol{\sigma}_{u,\ell})$

- Token generation by user u revealing attributes $R \subseteq [1,\ell]$, message M

  Compute short $\boldsymbol{\alpha}_u \leftarrow \sum_{i\in R} \boldsymbol{\sigma}_{u,i}$

  For $v \neq u$, compute long $\boldsymbol{\alpha}_v$: $\mathbf{A}\boldsymbol{\alpha}_v = \sum_{i\in R} H(v,i,a_i)$ using Gaussian elim.

  For $v = 1,\ldots,U$ encrypt $\boldsymbol{\tau}_v = \text{Enc}_{\mathbf{B}}(\boldsymbol{\alpha}_v)$

Not a real encryption – linkable!

$\boldsymbol{\tau}_u = \text{Enc}_{\mathbf{B}}(\boldsymbol{\alpha}) = \mathbf{B}^T\mathbf{s} + \boldsymbol{\alpha}$

Encrypt twice $\Rightarrow$ $\boldsymbol{\tau}_u - \boldsymbol{\tau}'_u = \mathbf{B}^T(\mathbf{s} - \mathbf{s}')$ is lattice point

Our AAT−O scheme: construction sketch

- Master key generation

  mpk = **A** ; msk = **T** ; common reference string **B**

- Issuance for attributes $a_1,\ldots,a_\ell$

  For i = 1,…,ℓ compute short $\boldsymbol{\sigma}_{u,i}$: $\mathbf{A}\boldsymbol{\sigma}_{u,i} = H(u,i,a_i)$ using $\mathbf{T}_u$

  Return $cred_u = (a_1,\ldots,a_\ell, \boldsymbol{\sigma}_{u,1},\ldots,\boldsymbol{\sigma}_{u,\ell})$

- Token generation by user u revealing attributes $R \subseteq [1,\ell]$, message M

  Compute short $\boldsymbol{\alpha}_u \leftarrow \sum_{i\in R} \boldsymbol{\sigma}_{u,i}$

  For $v \neq u$, compute long $\boldsymbol{\alpha}_v$: $\mathbf{A}\boldsymbol{\alpha}_v = \sum_{i\in R} H(v,i,a_i)$ using Gauss elimination

  Choose short random **x**, compute $\mathbf{y} = \mathbf{A}\mathbf{x}$

  For v = 1,…,U encrypt $\boldsymbol{\tau}_v = Enc_{\mathbf{B}}(\boldsymbol{\alpha}_v+\mathbf{x})$

  $\pi_{OR} \leftarrow NIWIP\{\boldsymbol{\tau}_1$ encrypts short $\boldsymbol{\alpha}_1 \vee \ldots \vee \boldsymbol{\tau}_U$ encrypts short $\boldsymbol{\alpha}_U\}$

  Compute signature of knowledge [Lyu08]

  $$\pi_{\mathbf{y}} \leftarrow SoK\{\mathbf{x} : \mathbf{A}\mathbf{x} = \mathbf{y}\}(M)$$

  Return $t = (\mathbf{y},\boldsymbol{\tau}_1,\ldots,\boldsymbol{\tau}_U,\pi_{OR},\pi_{\mathbf{y}})$

Our AAT−O scheme: construction sketch

- Token generation by user u revealing attributes $R \subseteq [1,\ell]$, message M

  Compute short $\boldsymbol{\alpha}_u \leftarrow \sum_{i\in R} \boldsymbol{\sigma}_{u,i}$

  For $v \neq u$, compute long $\boldsymbol{\alpha}_v$: $\mathbf{A}\boldsymbol{\alpha}_v = \sum_{i\in R} H(v,i,a_i)$ using Gauss elimination

  Choose short random $\mathbf{x}$, compute $\mathbf{y} = \mathbf{A}\mathbf{x}$

  For $v = 1,\ldots,U$ encrypt $\boldsymbol{\tau}_v = \mathrm{Enc}_{\mathbf{B}}(\boldsymbol{\alpha}_v+\mathbf{x})$

  $\pi_{OR} \leftarrow \mathrm{NIWIP}\{\boldsymbol{\tau}_1 \text{ encrypts short } \boldsymbol{\alpha}_1 \vee \ldots \vee \boldsymbol{\tau}_U \text{ encrypts short } \boldsymbol{\alpha}_U\}$

  Compute signature of knowledge [Lyu08]

  $$\pi_{\mathbf{y}} \leftarrow \mathrm{SoK}\{\mathbf{x} : \mathbf{A}\mathbf{x} = \mathbf{y}\}(M)$$

  Return $t = (\mathbf{y},\boldsymbol{\tau}_1,\ldots,\boldsymbol{\tau}_U,\pi_{OR},\pi_{\mathbf{y}})$

- Token verification for revealed attributes $(a_i)_{i\in R}$, message M

  For $v = 1,\ldots,U$ check $\mathbf{A}\boldsymbol{\tau}_v = \sum_{i\in R} H(v,i,a_i) + \mathbf{y}$

  Verify π_{OR} and $\pi_{\mathbf{y}}(M)$

Our AAT−O scheme: security

- Anonymity

  Learning with errors (LWE) hard in the random-oracle model

- Unforgeability

  Short integer solution (SIS) and learning with errors (LWE) hard in the random-oracle model

Our AAT+O scheme: construction idea

- Correlated trapdoor one-way function [RS09, Pei09]

  $\mathrm{Enc}_{\mathbf{B}0\ldots k}(\mathbf{s},\boldsymbol{\rho}_1,\ldots,\boldsymbol{\rho}_k) = (\mathbf{B}_i^{T}\mathbf{s} + \boldsymbol{\rho}_i)_{i=0\ldots k}$

  CCA2 encryption: $\mathbf{B}_i = \mathbf{B}_{i,vki}$ for one-time verification key vk

- AAT+O token generation:

  For v=1,…,U let

  $\mathbf{B}_{vk} \leftarrow [\,\mathbf{B}_0 \mid \mathbf{B}_{1,vk1} \mid \ldots \mid \mathbf{B}_{k,vkk}\,]$

  $\boldsymbol{\rho}_v \leftarrow [\boldsymbol{\alpha}_v + \mathbf{x} \mid \boldsymbol{\rho}_{v,1} \mid \ldots \mid \boldsymbol{\rho}_{v,|vk|}\,]$ where $\boldsymbol{\rho}_{v,i}$ short random

  $\boldsymbol{\tau}_v \leftarrow \mathbf{B}_{vk}^{T}\,\mathbf{s}_v + \boldsymbol{\rho}_v$

  Then have that $\boldsymbol{\rho}_u$ "somewhat short", so

  $$\pi_{OR} \leftarrow \mathrm{NIWIP}\{\boldsymbol{\tau}_1 \text{ encrypts short } \boldsymbol{\rho}_1 \vee \ldots \vee \boldsymbol{\tau}_U \text{ encrypts short } \boldsymbol{\rho}_U\}$$

  proves correct correlation for free

- AAT+O opening:

  Decrypt $\boldsymbol{\tau}_v$ using $\mathbf{S}_0$ (trapdoor for $\mathbf{B}_0$) until $\boldsymbol{\rho}_{v,0}$ short

Our AAT+O scheme: security

- Anonymity

  Learning with errors (LWE) hard and one-time signature scheme existentially unforgeable in the random-oracle model

- Traceability

  Short integer solution (SIS) and learning with errors (LWE) hard in the random-oracle model

Conclusion & open problems

IBM

Contributions

- AAT schemes as “anonymous credentials light”
  - without opening (AAT−O): anonymity cannot be lifted
  - with opening (AAT+O): full anonymity (CCA)

    $\Rightarrow$ first fully anonymous group signature scheme
- Schemes based on SIS and LWE in the random-oracle model
- Extension: non-frameability

Open problems

- Full-fledged credential systems from lattices

  attribute predicates, pseudonyms, blind issuing, …
- Token/signature size independent of total #users

Lattice preliminaries

Trapdoor one-way function from short integer solution (SIS) [GPV08]

$\mathbf{A} \in Z_q^{n \times m}$ (uniform) with trapdoor $\mathbf{T} \in Z_q^{m \times m}$ (short) such that $\mathbf{AT} \equiv \mathbf{0} \pmod{q}$

$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{Ax} \pmod{q}$ ($\mathbf{x}$: short, Gaussian), invert using

- Gaussian elimination → long $\mathbf{x}$
- trapdoor $\mathbf{T}$ → short $\mathbf{x}$

Encryption from learning with errors (LWE) [Reg09]

$\mathbf{B} \in Z_q^{n \times m}$ with trapdoor $\mathbf{S} \in Z_q^{m \times m}$ such that $\mathbf{AS} \equiv \mathbf{0} \pmod{q}$

$\mathrm{Enc}(\mathbf{s}) = \mathbf{B}^T\mathbf{s} + \mathbf{e} \pmod{q}$ ($\mathbf{e}$: short, Gaussian), decrypt using $\mathbf{S}$

Related trapdoor sampling [GKV10]

Given $\mathbf{B}$, generate $\mathbf{A}$ with trapdoor $\mathbf{T}$ such that $\mathbf{AB}^T \equiv \mathbf{0} \pmod{q}$