Group Signatures from Lattices: Simpler, Tighter, Shorter, Ring-based

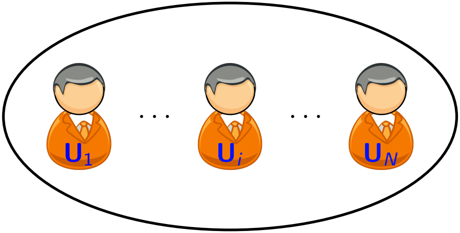
San Ling and **Khoa Nguyen** and Huaxiong Wang

Nanyang Technological University, Singapore

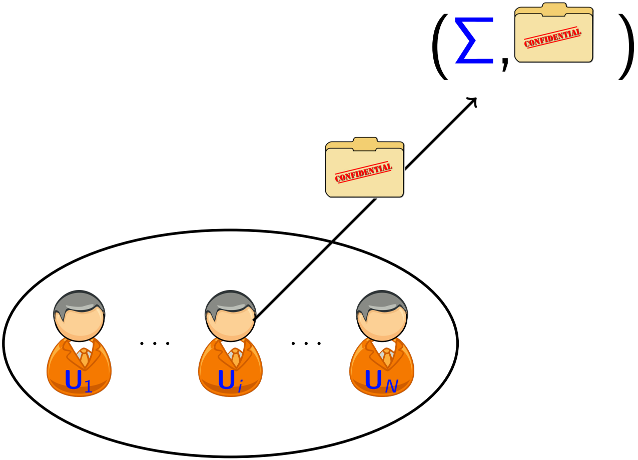
PKC 2015

Content

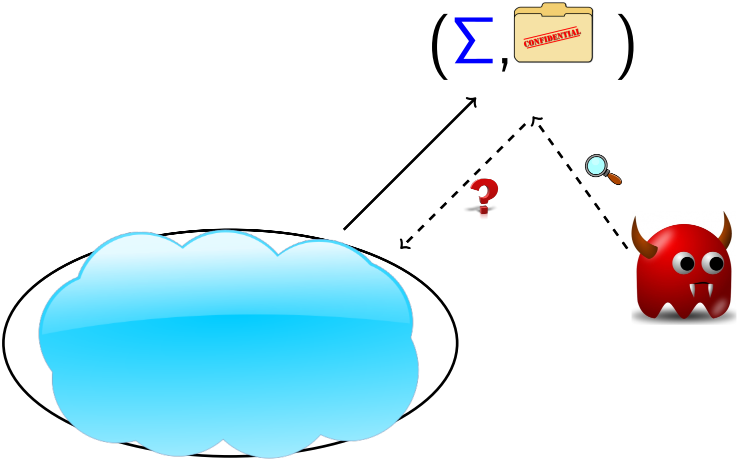
Group Signatures [CH91]



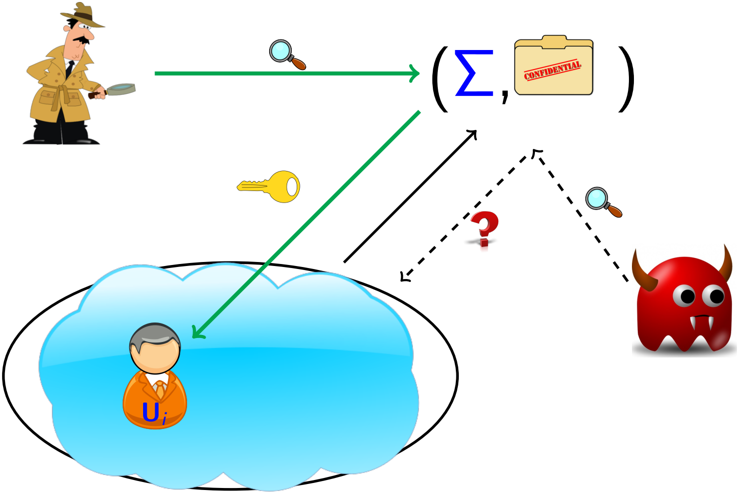
Group Signatures [CH91]



Group Signatures [CH91]



Group Signatures [CH91]



The [BMW'03] Model

Four algorithms:

1. $\mathsf{KeyGen}(n, N) \longrightarrow \big(\mathsf{gpk}, \mathsf{gmsk}, \{\mathsf{gsk}[i]\}_{i=0}^{N-1}\big)$.
2. $\mathsf{Sign}(\mathsf{gsk}[i], M) \longrightarrow \Sigma$.
3. $\mathsf{Verify}(\mathsf{gpk}, M, \Sigma) \longrightarrow \{0, 1\}$.
4. $\mathsf{Open}(\mathsf{gmsk}, M, \Sigma) \longrightarrow \{i, \perp\}$.

The [BMW'03] Model

Four algorithms:

1. $\mathsf{KeyGen}(n, N) \longrightarrow \big(\mathsf{gpk}, \mathsf{gmsk}, \{\mathsf{gsk}[i]\}_{i=0}^{N-1}\big)$.
2. $\mathsf{Sign}(\mathsf{gsk}[i], M) \longrightarrow \Sigma$.
3. $\mathsf{Verify}(\mathsf{gpk}, M, \Sigma) \longrightarrow \{0, 1\}$.
4. $\mathsf{Open}(\mathsf{gmsk}, M, \Sigma) \longrightarrow \{i, \perp\}$.

Correctness requirement:

$$\begin{aligned} \mathsf{Verify}\big(\mathsf{gpk}, M, \mathsf{Sign}(\mathsf{gsk}[i], M)\big) &= 1, \\ \mathsf{Open}\big(\mathsf{gmsk}, M, \mathsf{Sign}(\mathsf{gsk}[i], M)\big) &= i. \end{aligned}$$

The [BMW'03] Model

Four algorithms:

1. $\mathsf{KeyGen}(n, N) \longrightarrow \left(\mathsf{gpk}, \mathsf{gmsk}, \{\mathsf{gsk}[i]\}_{i=0}^{N-1}\right)$.
2. $\mathsf{Sign}(\mathsf{gsk}[i], M) \longrightarrow \Sigma$.
3. $\mathsf{Verify}(\mathsf{gpk}, M, \Sigma) \longrightarrow \{0, 1\}$.
4. $\mathsf{Open}(\mathsf{gmsk}, M, \Sigma) \longrightarrow \{i, \perp\}$.

Correctness requirement:

$$\begin{aligned} \mathsf{Verify}\big(\mathsf{gpk}, M, \mathsf{Sign}(\mathsf{gsk}[i], M)\big) &= 1, \\ \mathsf{Open}\big(\mathsf{gmsk}, M, \mathsf{Sign}(\mathsf{gsk}[i], M)\big) &= i. \end{aligned}$$

Security requirements:

1. **CCA-anonymity:** Signatures generated by two distinct group users are computationally indistinguishable to an adversary who:
   - Knows all the user secret keys.
   - Has access to Opening oracle. (**CPA-anonymity** ([BBS'04]), otherwise.)
2. **Traceability:** All signatures, even those produced by a coalition, can be traced to a member of the coalition.

Previous Lattice-based Group Signatures

Schemes in the [BMW'03] model:

Scheme	GKV10	CNR12	LLLS13
Signature	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n^2)$
Public key	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n^2)$
User secret key	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$
Anonymity	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^8)}$
Traceability	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^{1.5})}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^{7.5})}$

- Encryption layer to be initialized in accordance with signature layer; long user secret keys; long ciphertexts.
- None of previous schemes simultaneously achieves logarithmic signature size and weak hardness assumptions.
- Another open question raised in [LLLS'13]: Ring-based group signature?

Our Results and Comparison with Previous Works

Lattice-based group signature (in the [BMW'03] model) with:

1. Logarithmic signature and public key sizes + short user secret key.
2. Weak hardness assumptions: CCA-anonymous and traceable if the underlying encryption and standard signature schemes are secure, respectively (i.e., no overhead!).
3. Easy transformation into the ring setting.
4. Encryption layer and signature layer are independent. Only $\log N$ bits have to be encrypted.

Scheme	GKV10	CNR12	LLLS13	Scheme (I)	Scheme (II)
Signature	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n)$	$\log N \cdot \widetilde{\mathcal{O}}(n)$
Public key	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n)$
User secret key	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	$\widetilde{\mathcal{O}}(n)$
Anonymity	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^8)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SVP}^{\infty}_{\widetilde{\mathcal{O}}(n^{3.5})}$
Traceability	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^{1.5})}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^{7.5})}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SVP}^{\infty}_{\widetilde{\mathcal{O}}(n^2)}$

Note: All known lattice-based group signatures are proven secure only in the ROM.

A Simple Design Approach

Choose $N = 2^\ell$, user $j \in [0, N-1]$ is equivalently indexed by $d \in \{0,1\}^\ell$.

1. Group public key consists of verification key of the Boyen signature scheme ([Boyen'10]), and encrypting key of a lattice-based PKE $\mathcal{E}$. Opening key is the decrypting key of $\mathcal{E}$.
2. Secret key of user with index $d \in \{0,1\}^\ell$ is a Boyen signature $\mathbf{z}$ on "message" d.
3. To sign any message, encrypt d to obtain a ciphertext $\mathbf{c}$ and generate a zero-knowledge argument π to prove that:
   (i) **The user possesses a valid message-signature pair $(d, \mathbf{z})$ for the Boyen signature scheme.**
   (ii) $\mathbf{c}$ is a correct encryption of d.

   Then using the Fiat-Shamir heuristic to get a NIZKAoK π. The signature is $\Sigma = (\mathbf{c}, \pi)$.
4. To verify Σ, check π.
5. To open Σ, decrypt $\mathbf{c}$.

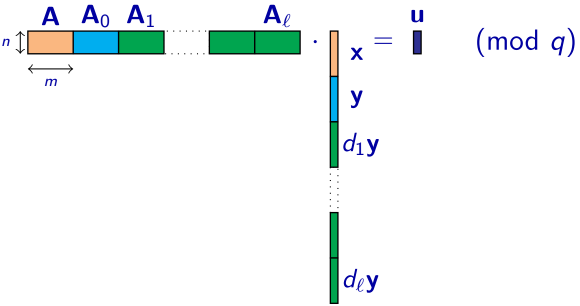
Main Technical Contribution

We introduce a statistical ZK argument for a valid message-signature pair $(d, \mathbf{z})$ for the Boyen signature (i.e., both d and $\mathbf{z}$ are hidden), which might be of independent interest.

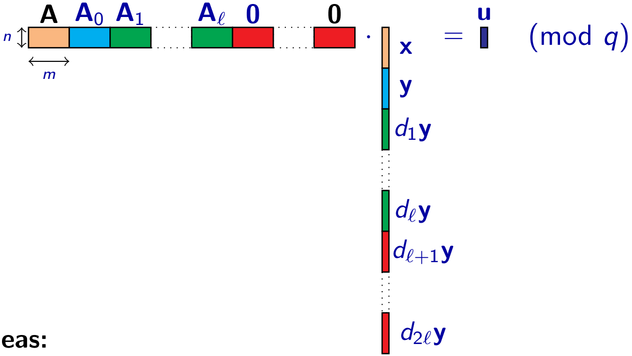
Main Technical Contribution

We introduce a statistical ZK argument for a valid message-signature pair $(d, \mathbf{z})$ for the Boyen signature (i.e., both d and $\mathbf{z}$ are hidden), which might be of independent interest.

Specifically, given public matrices $\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell \in \mathbb{Z}_q^{n \times m}$ and vector $\mathbf{u} \in \mathbb{Z}_q^n$, we prove in ZK the possession of $d = (d_1, \ldots, d_\ell) \in \{0,1\}^\ell$ and small $\mathbf{z} = (\mathbf{x} \| \mathbf{y}) \in \mathbb{Z}^{2m}$ s.t. $\mathbf{A}\mathbf{x} + \big(\mathbf{A}_0 + \sum_{i=1}^{\ell} d_i \mathbf{A}_i\big)\mathbf{y} = \mathbf{u} \bmod q$.

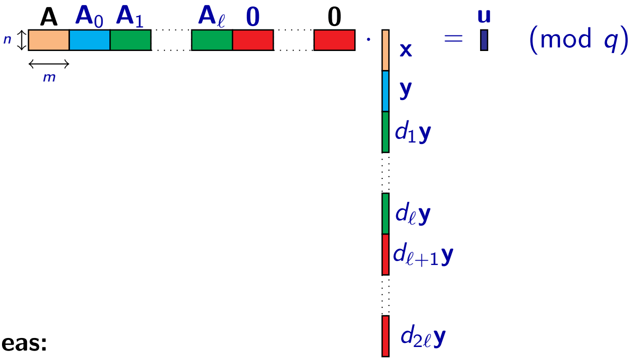


Observation: This is essentially an ISIS relation $\mathbf{A}^*\mathbf{z}^* = \mathbf{u} \bmod q$, where the ISIS solution $\mathbf{z}^*$ has a special structure.



Main ideas:

- After extensions, we still have an ISIS relation. Here, $d_{\ell+1}, \ldots, d_{2\ell}$ are bits s.t. the extended vector $d^* = (d_1, \ldots, d_\ell, d_{\ell+1}, \ldots, d_{2\ell}) \in \{0,1\}^{2\ell}$ has weight exactly equal to ℓ.



Main ideas:

- After extensions, we still have an ISIS relation. Here, $d_{\ell+1}, \ldots, d_{2\ell}$ are bits s.t. the extended vector $d^* = (d_1, \ldots, d_\ell, d_{\ell+1}, \ldots, d_{2\ell}) \in \{0,1\}^{2\ell}$ has weight exactly equal to ℓ.
- We develop the Stern-type protocol for ISIS from [LNSW'13].
  - Proving the knowledge of $\mathbf{x}$ and $\mathbf{y}$ is a simple adaptation.
  - We randomly permute the blocks of $(d_1\mathbf{y}, \ldots, d_\ell\mathbf{y}, d_{\ell+1}\mathbf{y}, \ldots, d_{2\ell}\mathbf{y})$ and show that it has exactly ℓ blocks equal to $\mathbf{y}$. This convinces the verifier that the original vector has the form $(d_1\mathbf{y}, \ldots, d_\ell\mathbf{y})$ for certain hidden $(d_1, \ldots, d_\ell) \in \{0,1\}^\ell$.

Scheme Developments

- We have a flexible choice for encryption layer. For the Dual-Regev encryption [GPV'08], we obtain a Stern-type ZK argument for proving that a given ciphertext $\mathbf{c}$ is a valid encryption of d.

Scheme Developments

- We have a flexible choice for encryption layer. For the Dual-Regev encryption [GPV'08], we obtain a Stern-type ZK argument for proving that a given ciphertext $\mathbf{c}$ is a valid encryption of d.
- The two Stern-type protocols can be combined together to result in a CPA-anonymous group signature.

Scheme Developments

- We have a flexible choice for encryption layer. For the Dual-Regev encryption [GPV'08], we obtain a Stern-type ZK argument for proving that a given ciphertext $\mathbf{c}$ is a valid encryption of d.
- The two Stern-type protocols can be combined together to result in a CPA-anonymous group signature.
- To achieve CCA-anonymity, we employ the IBE version of Dual-Regev [GPV08], and the technique from [BCHK07].

Scheme Developments

- We have a flexible choice for encryption layer. For the Dual-Regev encryption [GPV'08], we obtain a Stern-type ZK argument for proving that a given ciphertext $\mathbf{c}$ is a valid encryption of d.
- The two Stern-type protocols can be combined together to result in a CPA-anonymous group signature.
- To achieve CCA-anonymity, we employ the IBE version of Dual-Regev [GPV08], and the technique from [BCHK07].
- We obtain a ring-based group signature scheme, in which the public key and signature both have asymptotically size $\log N \cdot \widetilde{\mathcal{O}}(n)$. Key points:
  1. Boyen's signature can be transformed into the ring setting.
  2. We use an efficient variant of Dual-Regev encryption presented in [LPR13].
  3. Our ZK protocol basically works as for general lattices.
  4. CPA-anonymity and traceability can be based on the worst-case hardness of $\mathsf{SVP}_{\gamma}^{\infty}$ on ideal lattices, for relatively small γ. (Also, no overhead in security assumptions.)

A Brief Comparison with [NZZ'15]

In a concurrent and independent work, Nguyen, Zhang, and Zhang also obtain a lattice-based group signature scheme which is simpler than [GKV'10],[LLLS'13].

A Brief Comparison with [NZZ'15]

In a concurrent and independent work, Nguyen, Zhang, and Zhang also obtain a lattice-based group signature scheme which is simpler than [GKV'10],[LLLS'13].

In their scheme:

- Group public key and signature sizes are shorter than ours.
- The secret key of each group user is still a matrix in $\mathbb{Z}^{2m \times 2m}$ of bit-size $\widetilde{\mathcal{O}}(n^2)$.
- Parameters are required to be larger than ours, e.g., $q = m^{2.5} \max(m^6 \omega(\log^{2.5} m), 4N)$.
- Security assumptions are stronger than ours, e.g., traceability is based on the worst-case hardness of $\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^{8.5})}$.

Some Open Questions

Constructing lattice-based group signatures with:

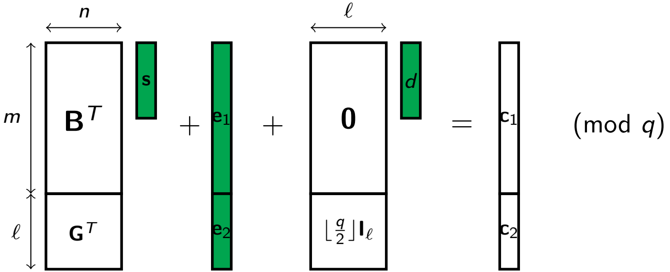
- Dynamic enrollment of users ([BSZ'05], [SSEHO'12] models)?
- Signatures size independent of N?
- Provable security in the standard model?

Scheme	GKV10	CNR12	LLLS13	Scheme (I)	Scheme (II)
Signature	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n)$	$\log N \cdot \widetilde{\mathcal{O}}(n)$
Public key	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n^2)$	$\log N \cdot \widetilde{\mathcal{O}}(n)$
User secret key	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	$\widetilde{\mathcal{O}}(n)$
Anonymity	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^8)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SVP}^{\infty}_{\widetilde{\mathcal{O}}(n^{3.5})}$
Traceability	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^{1.5})}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^{7.5})}$	$\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n^2)}$	$\mathsf{SVP}^{\infty}_{\widetilde{\mathcal{O}}(n^2)}$

A Zero-knowledge Protocol for the GPV-IBE

Given public key $(\mathbf{B}, \mathbf{G})$ and ciphertext $(\mathbf{c}_1, \mathbf{c}_2)$, prove in ZK the knowledge of $\mathbf{s} \in \mathbb{Z}_q^n$ (might be small), small $(\mathbf{e}_1 \in \mathbb{Z}^m, \mathbf{e}_2 \in \mathbb{Z}^\ell)$ and $d \in \{0,1\}^\ell$ s.t.

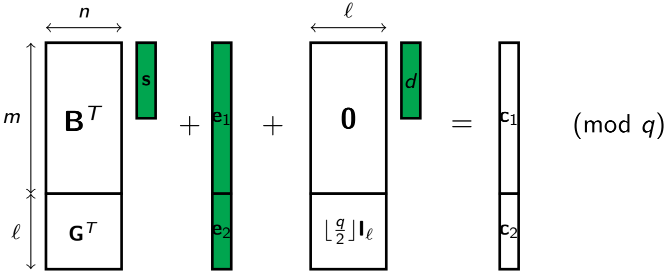
$$\left(\mathbf{c}_1 = \mathbf{B}^T\mathbf{s} + \mathbf{e}_1, \mathbf{c}_2 = \mathbf{G}^T\mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor d\right).$$



A Zero-knowledge Protocol for the GPV-IBE

Given public key $(\mathbf{B}, \mathbf{G})$ and ciphertext $(\mathbf{c}_1, \mathbf{c}_2)$, prove in ZK the knowledge of $\mathbf{s} \in \mathbb{Z}_q^n$ (might be small), small $(\mathbf{e}_1 \in \mathbb{Z}^m, \mathbf{e}_2 \in \mathbb{Z}^\ell)$ and $d \in \{0,1\}^\ell$ s.t.

$$\left(\mathbf{c}_1 = \mathbf{B}^T\mathbf{s} + \mathbf{e}_1, \mathbf{c}_2 = \mathbf{G}^T\mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor d\right).$$



- This can be done by adapting the techniques from [LNSW13].