The 23rd Annual International Conference on Information Security and Cryptology

ICISC 2020

December 2 (Wed) ~ December 4 (Fri), 2020 | Virtual Conference

Hosted by
Korea Institute of Information Security and Cryptology (KIISC)
National Security Research Institute (NSR)

Korea Institute of Information Security & Cryptology

A Sub-linear Lattice-based Submatrix Commitment Scheme

Huang Lin

Mercury's Wing & Suterusu Project

Summary

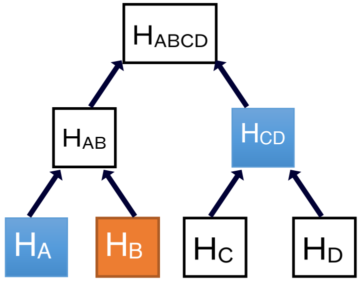
- Motivation
- Preliminaries
- Scheme
- Proof
- Performance

Motivation: submatrix commitment for post-quantum secure zero-knowledge proof scheme with transparent setup

- One way to construct post-quantum secure ZKP with transparent setup: “CS proofs” paradigm based on probabilistically checkable proofs (PCP)+Merkle Treee Commitment (MTC).

- A PCP scheme allows the prover to efficiently compute a PCP string which encodes the witness of the statement to be proven. The verifier can then decide whether the statement is true with probability close to 1 by *randomly inspecting* q entries of the PCP string.

“CS proofs” paradigm



Prover

PCP: {A,B,C,D}

Verifier

Com(PCP)=H_{ABCD} →

← Show me the ***second*** character of the PCP string.

Open:=B

Proof:={H_A, H_{CD}} →

Accept if

$$H_{ABCD} = H\left(H\left(H_A, H_B\right), H_{CD}\right)$$

Verify PCP

Motivation: submatrix commitment for post-quantum secure zero-knowledge proof scheme with transparent setup

- Problem with Merkle Tree Commitment: can only open one position at a time, and hence the space cost incurred due to the Merkle tree commitment is around $q\lambda \log \ell$ bits, where ℓ is the size of PCP and λ is the security parameter.

- A submatrix commitment scheme (an improvement of MTC) commits to a message vector and opens to multiple entries of the message vector simultaneously.

- The security of our proposed scheme is reduced to Module-SIS Assumption, which is believed to be post-quantum secure. Both the commitment and opening size of our proposed scheme is sublinear, i.e., proportional to the square root of the message size. To the best of our knowledge, this is the first post-quantum submatrix commitment scheme with sublinear performance.

Preliminaries

For $a, b \in \mathbb{N}$, we use $[a, b]$ to denote the set $\{a, a+1, \cdots, b-1, b\}$. Given a matrix

$$\mathbf{w} = \begin{pmatrix} w_{0,0} & w_{0,1} & \cdots & w_{0,N-1} \\ w_{1,0} & w_{1,1} & \cdots & w_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{h-1,0} & w_{h-1,1} & \cdots & w_{h-1,N-1} \end{pmatrix}$$

that is also denoted as $\left\{ \left\langle w_{i,0}, w_{i,1}, \dots, w_{i,N-1} \right\rangle_{i \in [0,h-1]} \right\}$, we define a submatrix $\mathbf{w}_{\mathbf{I},\mathbf{J}} = \left\{ \left\langle w_{i,j} \mid j \in \mathbf{J} \right\rangle_{i \in \mathbf{I}} \right\}$ as an ordered subset of the entries of the matrix indexed by $\mathbf{I} \subseteq [0, h-1]$ and $\mathbf{J} \subseteq [0, N-1]$.

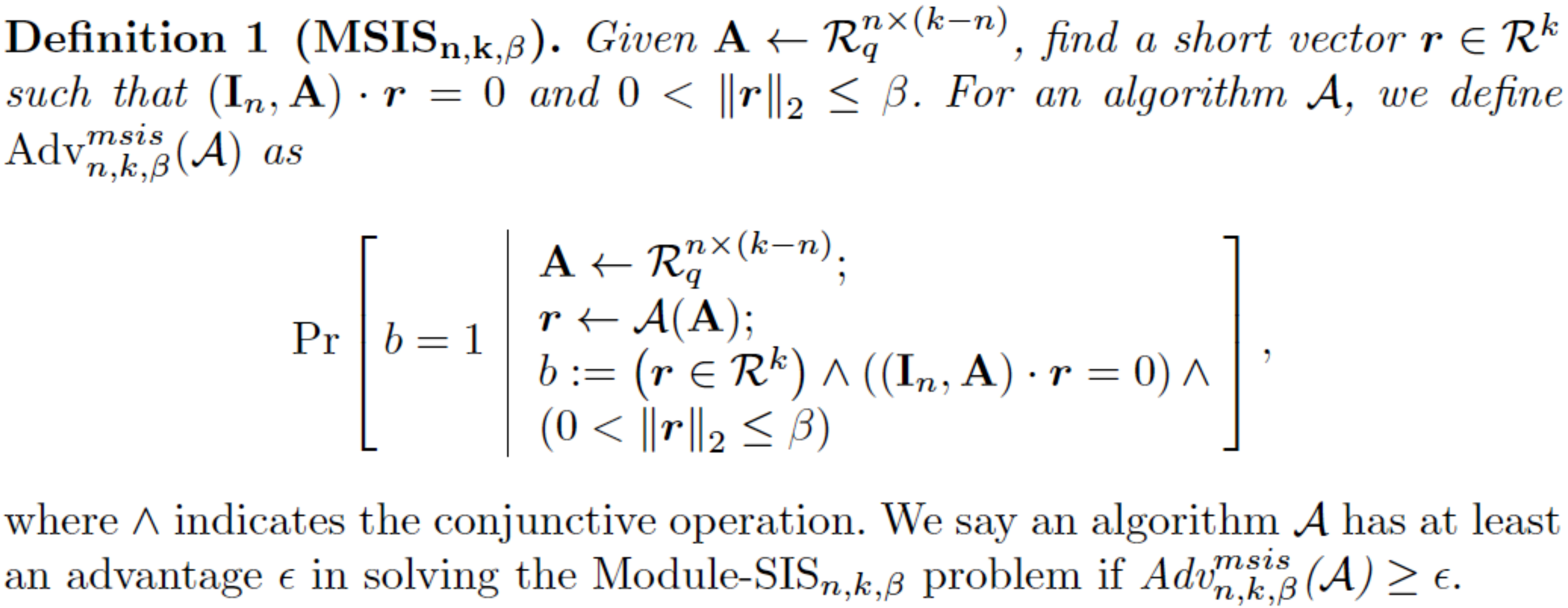
Preliminaries

Let $\mathcal{R}$ be the cyclotomic ring $\mathcal{R} = \mathbb{Z}[X]/\langle X^N + 1\rangle$, where N is a power of 2. Let *q* be a positive integer and define $\mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle$. Here $\mathbb{Z}_q$ denotes the integers modulo *q*. For $f(X) = \sum_i f_i X^i \in \mathcal{R}$, the norms of *f* are defined as

$l_1 : \|f\|_1 = \sum_i |f_i|,\ l_2 : \|f\|_2 = \left(\sum_i |f_i|^2\right)^{1/2},\ l_\infty : \|f\|_\infty = \max_i |f_i|.$

In our system, *q* is a product of two primes p_1 and p_2. For a positive integer β, we write S_β to be the set of all elements in $\mathcal{R}_{p_2}$ with l_1-norm at most β.

Preliminaries



Definition 1 **($\mathbf{MSIS}_{\mathbf{n},\mathbf{k},\beta}$).** *Given* $\mathbf{A} \leftarrow \mathcal{R}_q^{n\times(k-n)}$*, find a short vector* $\boldsymbol{r} \in \mathcal{R}^k$ *such that* $(\mathbf{I}_n, \mathbf{A}) \cdot \boldsymbol{r} = 0$ *and* $0 < \|\boldsymbol{r}\|_2 \leq \beta$*. For an algorithm* $\mathcal{A}$*, we define* $\mathrm{Adv}_{n,k,\beta}^{msis}(\mathcal{A})$ *as*

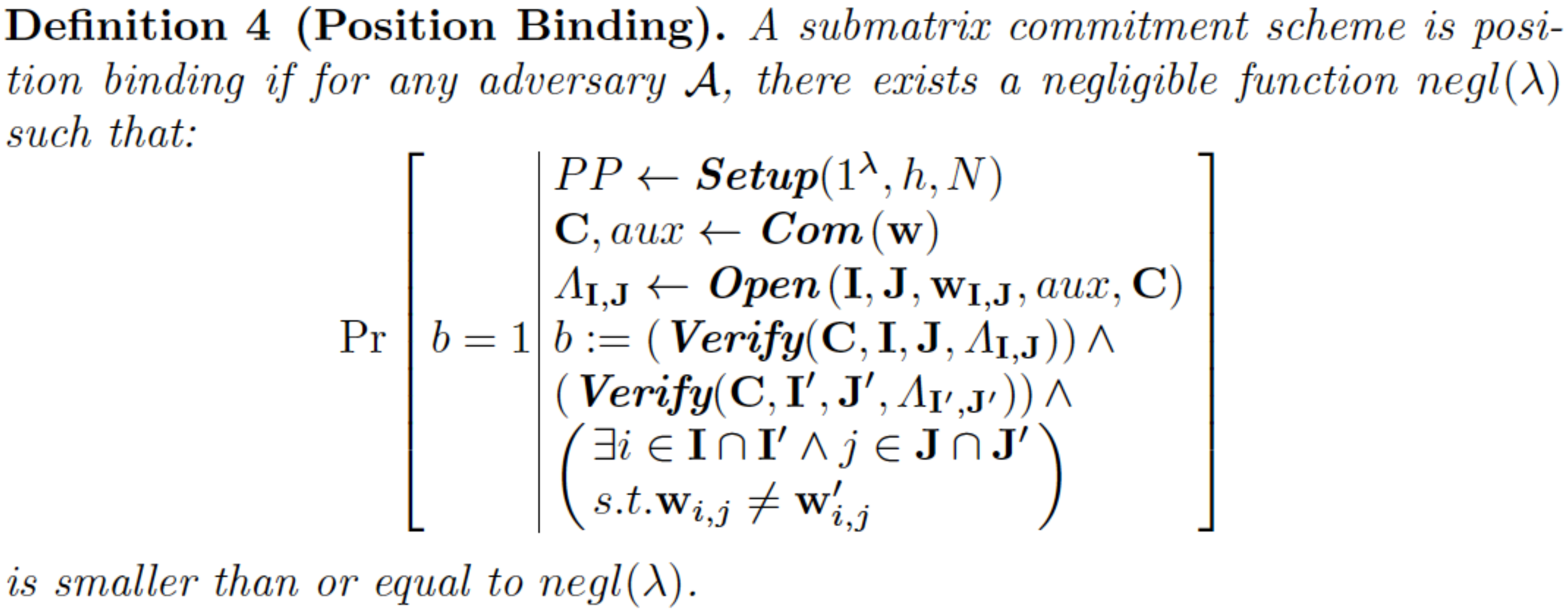
$$\Pr\left[b = 1 \;\middle|\; \begin{array}{l} \mathbf{A} \leftarrow \mathcal{R}_q^{n\times(k-n)}; \\ \boldsymbol{r} \leftarrow \mathcal{A}(\mathbf{A}); \\ b := \left(\boldsymbol{r} \in \mathcal{R}^k\right) \wedge ((\mathbf{I}_n, \mathbf{A}) \cdot \boldsymbol{r} = 0) \wedge \\ (0 < \|\boldsymbol{r}\|_2 \leq \beta) \end{array} \right],$$

where $\wedge$ indicates the conjunctive operation. We say an algorithm $\mathcal{A}$ has at least an advantage ϵ in solving the Module-SIS$_{n,k,\beta}$ problem if $Adv_{n,k,\beta}^{msis}(\mathcal{A}) \geq \epsilon$.

Sub-linear lattice-based submatrix commitment

- Submatrix commitment syntax: A submatrix commitment scheme consists of five algorithms:
- $\mathbf{Setup}(1^{\lambda}, h, N)$: Given security parameter λ, the dimension of a matrix h and N, outputs the public parameters PP.
- $\mathbf{Com}(\mathbf{w})$: Given a matrix w, outputs a commitment C and an auxiliary message aux.
- $\mathbf{Open}\left(\mathbf{I}, \mathbf{J}, \mathtt{w}_{\mathrm{I,J}}, aux, \mathbf{C}\right)$: Given two order index sets I, J and the auxiliary message aux, outputs an opening $\Lambda_{\mathbf{I,J}}$ that proves $\mathtt{W}_{\mathrm{I,J}}$ is the submatrix of the message committed under C.
- $\mathbf{Verify}(\mathbf{C}, \mathbf{I}, \mathbf{J}, \mathtt{w}_{\mathrm{I,J}}, \Lambda_{\mathbf{I,J}})$: Given inputs commitment C, two order index sets I and J, the submatrix of the message $\mathtt{W}_{\mathrm{I,J}}$ and opening $\Lambda_{\mathbf{I,J}}$, outputs 1 (accept) or 0 (reject).

Sub-linear lattice-based submatrix commitment



Definition 4 (Position Binding). *A submatrix commitment scheme is position binding if for any adversary $\mathcal{A}$, there exists a negligible function negl(λ) such that:*

$$\Pr\left[b = 1 \;\middle|\; \begin{array}{l} PP \leftarrow \boldsymbol{Setup}(1^{\lambda}, h, N) \\ \mathbf{C}, aux \leftarrow \boldsymbol{Com}\,(\mathbf{w}) \\ \Lambda_{\mathbf{I},\mathbf{J}} \leftarrow \boldsymbol{Open}\,(\mathbf{I}, \mathbf{J}, \mathbf{w}_{\mathbf{I},\mathbf{J}}, aux, \mathbf{C}) \\ b := (\boldsymbol{Verify}(\mathbf{C}, \mathbf{I}, \mathbf{J}, \Lambda_{\mathbf{I},\mathbf{J}})) \wedge \\ (\boldsymbol{Verify}(\mathbf{C}, \mathbf{I}', \mathbf{J}', \Lambda_{\mathbf{I}',\mathbf{J}'})) \wedge \\ \left(\begin{array}{l} \exists i \in \mathbf{I} \cap \mathbf{I}' \wedge j \in \mathbf{J} \cap \mathbf{J}' \\ s.t. \mathbf{w}_{i,j} \neq \mathbf{w}'_{i,j} \end{array} \right) \end{array} \right]$$

is smaller than or equal to negl(λ).

Our design: primitive idea

- We exploit a conceptual similarity between Single-Instruction Multiple-Data (SIMD) in homomorphic encryption and submatrix commitment, and develops a novel position binding technique based on the Chinese Remainder Theorem.

- In our scheme, the modulus q is a product of two primes p_1 and p_2. The committed message of our scheme is an element in Z_{p_1}, where p_1 can be set to 2. The cyclotomic polynomial $\phi(X)$ is chosen to split into linear terms modulo q,

$$\Phi(X) = \left[\prod_{i=0}^{N-1}(X - \varsigma_i)\right]_{p_1 p_2}$$

- From the Chinese Remainder Theorem (CRT), one can define an isomorphism:

$$\mathbb{Z}_q[X]/\langle\Phi(X)\rangle \mapsto \left(\mathbb{Z}_q[X]/\langle X - \varsigma_0\rangle, \ldots, \mathbb{Z}_q[X]/\langle X - \varsigma_{N-1}\rangle\right)$$

Our design: primitive idea

$$\mathbf{m}\left(X\right)\times\mathbf{J}\left(X\right)\overset{CRT}{\longleftrightarrow}\mathbf{m}\otimes\mathbf{J}=\left\langle m_0*\mathbf{J}_0,m_1*\mathbf{J}_1,\cdots,m_{N-1}*\mathbf{J}_{N-1}\right\rangle$$

$$\mathbf{J}=\left\langle 0,1,1,\cdots,0\right\rangle\Rightarrow\mathbf{m}\otimes\mathbf{J}=\left\langle 0,m_1,m_2,\cdots,0\right\rangle$$

Similarly, when the message polynomial **m**(X) is replaced by the commitment **C**, then we have $\mathbf{J}(X)\mathbf{C}$ as a commitment of the respective subvector.

Our design: commitment algorithm

- The underlying lattice-based commitment scheme: $\mathbf{C} = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix} \mathbf{r}(X) + \begin{pmatrix} 0 \\ \mathbf{w}(X) \end{pmatrix}$, where $\mathbf{A}_1$ and $\mathbf{A}_2$ are both matrix of ring elements in $\mathcal{R}_q$

- $\mathbf{w}(X) \in (\mathcal{R}_q)^\ell$ is the message vector, where the p_1 component, i.e., $[\mathbf{w}(X)]_{(X-\varsigma_j, p_1)} = H'(w_{0,j} \| w_{1,j} \| \cdots \| w_{h-1,j})$ and the p_2 component is set to be 0.

- The p_2 component of $\mathbf{r}(X)$ belongs to S_β, i.e., $[\mathbf{r}(X)]_{p_2} = H(\rho)$ and the p_1 component is set to be 0.

Our design: opening algorithm

- The opening would be the column vector, i.e., $\Lambda_{\mathrm{I,J}} = \left(\left\langle w_{i,j} \mid i \in [0, h-1], j \in \mathbf{J} \right\rangle, \rho\right)$, which amounts to the message column vector with column indexes belonging to J and the random seed.

Our design: verification algorithm

- Since $\left[\mathbf{w}(X)\mathbf{J}(X)\right]_{p_1}$ can be recovered from the above column vector and $\left[\mathbf{w}(X)\mathbf{J}(X)\right]_{p_2}=0$, hence we can recover $\mathbf{w}(X)\mathbf{J}(X)$.

- Since the seed ρ is included in the opening, $\mathbf{r}(X)\mathbf{J}(X)$ can be recovered.

- The verification checks whether $\mathbf{J}(X)\mathbf{C}=\begin{pmatrix}\mathbf{A}_1\\ \mathbf{A}_2\end{pmatrix}\mathbf{J}(X)\mathbf{r}(X)+\begin{pmatrix}0\\ \mathbf{w}(X)\mathbf{J}(X)\end{pmatrix}$

Our design: security proof

- Assuming an adversary outputs $\mathbf{C},\mathbf{I},\mathbf{J},\mathbf{w}_{\mathbf{I},\mathbf{J}},\Lambda_{\mathbf{I},\mathbf{J}},\mathbf{I'},\mathbf{J'},\mathbf{w'}_{\mathbf{I'},\mathbf{J'}},\Lambda'_{\mathbf{I'},\mathbf{J'}}$ such that $\mathbf{Verify}(\mathbf{C},\mathbf{I},\mathbf{J},\mathbf{w}_{\mathbf{I},\mathbf{J}},\Lambda_{\mathbf{I},\mathbf{J}})=\mathbf{Verify}(\mathbf{C},\mathbf{I'},\mathbf{J'},\mathbf{w'}_{\mathbf{I'},\mathbf{J'}},\Lambda'_{\mathbf{I'},\mathbf{J'}})=1$ and $\exists i\in\mathbf{I}\cap\mathbf{I'}\wedge j\in\mathbf{J}\cap\mathbf{J'}$ such that $w_{i,j}\neq w'_{i,j}$, we can construct an algorithm C to solve the $\mathrm{MSIS}_{n,k,\beta}$ problem over $\mathcal{R}_{p_2}$ with non-negligible prob.

Our design: security proof

According to the verification equation, we have

$$\mathbf{J}(X)\mathbf{C} = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix} \mathbf{J}(X)\mathbf{r}(X) + \begin{pmatrix} 0 \\ \mathbf{w}(X)\mathbf{J}(X) \end{pmatrix}$$

$$\mathbf{J}'(X)\mathbf{C} = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix} \mathbf{J}'(X)\mathbf{r}'(X) + \begin{pmatrix} 0 \\ \mathbf{w}'(X)\mathbf{J}'(X) \end{pmatrix}$$

By multiplying J'(x) with the first equation and J(x) with the second one and minus the first with the second, we have

$$\begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix} \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{r}(X) - \mathbf{r}'(X)) \\ + \begin{pmatrix} \vec{0} \\ \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{w}(X) - \mathbf{w}'(X)) \end{pmatrix} = 0$$

Our design: security proof

$$\begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix} \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{r}(X)-\mathbf{r}'(X)) + \begin{pmatrix} \vec{0} \\ \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{w}(X)-\mathbf{w}'(X)) \end{pmatrix} = 0$$

First we prove that $\mathbf{J}(X)\mathbf{J}'(X)(\mathbf{w}(X)-\mathbf{w}'(X)) \neq \mathbf{0} \bmod q$ by contradiction. Since if $\mathbf{J}(X)\mathbf{J}'(X)\mathbf{w}(X) = \mathbf{J}(X)\mathbf{J}'(X)\mathbf{w}'(X) \bmod q$, we have $\left[\mathbf{w}(\varsigma_j)\right]_{p_1} = \left[\mathbf{w}'(\varsigma_j)\right]_{p_1}, \forall j \in \mathbf{J} \cap \mathbf{J}'$, but since the p1 component of w(x) is the hash of the message column vector, i.e., $\left[\mathbf{w}(X)\right]_{(X-\varsigma_j, p_1)} = H'\left(w_{0,j} \parallel w_{1,j} \parallel \cdots \parallel w_{h-1,j}\right)$ and we assume $\exists i \in \mathbf{I} \cap \mathbf{I}' \wedge j \in \mathbf{J} \cap \mathbf{J}'$ such that $w_{i,j} \neq w'_{i,j}$, therefore unless we have found a collision of the hash function, we found a contradiction.

Our design: security proof

$$\begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix} \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{r}(X)-\mathbf{r}'(X))$$

$$+\begin{pmatrix} \vec{0} \\ \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{w}(X)-\mathbf{w}'(X)) \end{pmatrix} = 0 \wedge \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{w}(X)-\mathbf{w}'(X)) \neq \mathbf{0} \bmod q$$

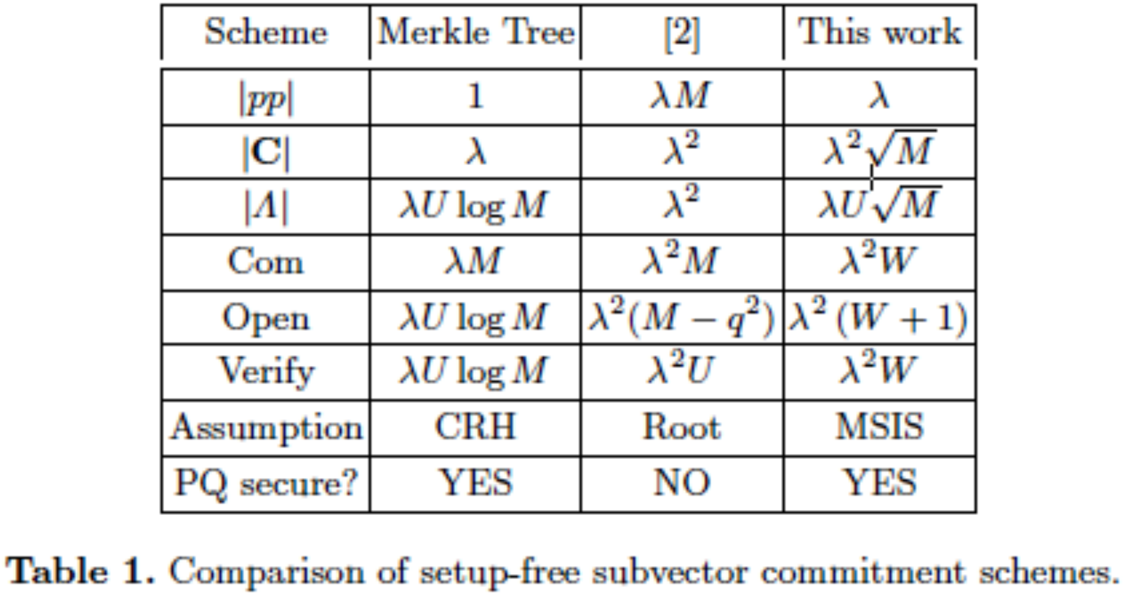
$$\left(\Rightarrow \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{r}(X)-\mathbf{r}'(X)) \neq \mathbf{0} \bmod q\right) \wedge [\mathbf{r}(X)]_{p_1} = [\mathbf{r}'(X)]_{p_1} = 0$$

$$\left(\Rightarrow \mathbf{J}(X)\mathbf{J}'(X)(\mathbf{r}(X)-\mathbf{r}'(X)) \neq \mathbf{0} \bmod p_2\right) \wedge [\mathbf{J}(X)]_{p_2} = [\mathbf{J}'(X)]_{p_2} = 1$$

$$\Rightarrow (\mathbf{r}(X)-\mathbf{r}'(X)) \neq \mathbf{0} \bmod p_2$$

The p_2 component of $\mathbf{r}(X)$ belongs to S_β, we have found a solution for the $\mathrm{MSIS}_{n,k,\beta}$ problem over $\mathcal{R}_{p_2}$

Our design: Performance analysis



Scheme	Merkle Tree	[2]	This work
$\|pp\|$	1	λM	λ
$\|\mathbf{C}\|$	λ	λ^2	$\lambda^2\sqrt{M}$
$\|\Lambda\|$	$\lambda U \log M$	λ^2	$\lambda U\sqrt{M}$
Com	λM	$\lambda^2 M$	$\lambda^2 W$
Open	$\lambda U \log M$	$\lambda^2(M-q^2)$	$\lambda^2\,(W+1)$
Verify	$\lambda U \log M$	$\lambda^2 U$	$\lambda^2 W$
Assumption	CRH	Root	MSIS
PQ secure?	YES	NO	YES

Table 1. Comparison of setup-free subvector commitment schemes.

When we set h and N to be equal, we have a commitment and opening size equal to the square root of the message matrix size, which is sublinear.

Thanks for your attention

Q&A