

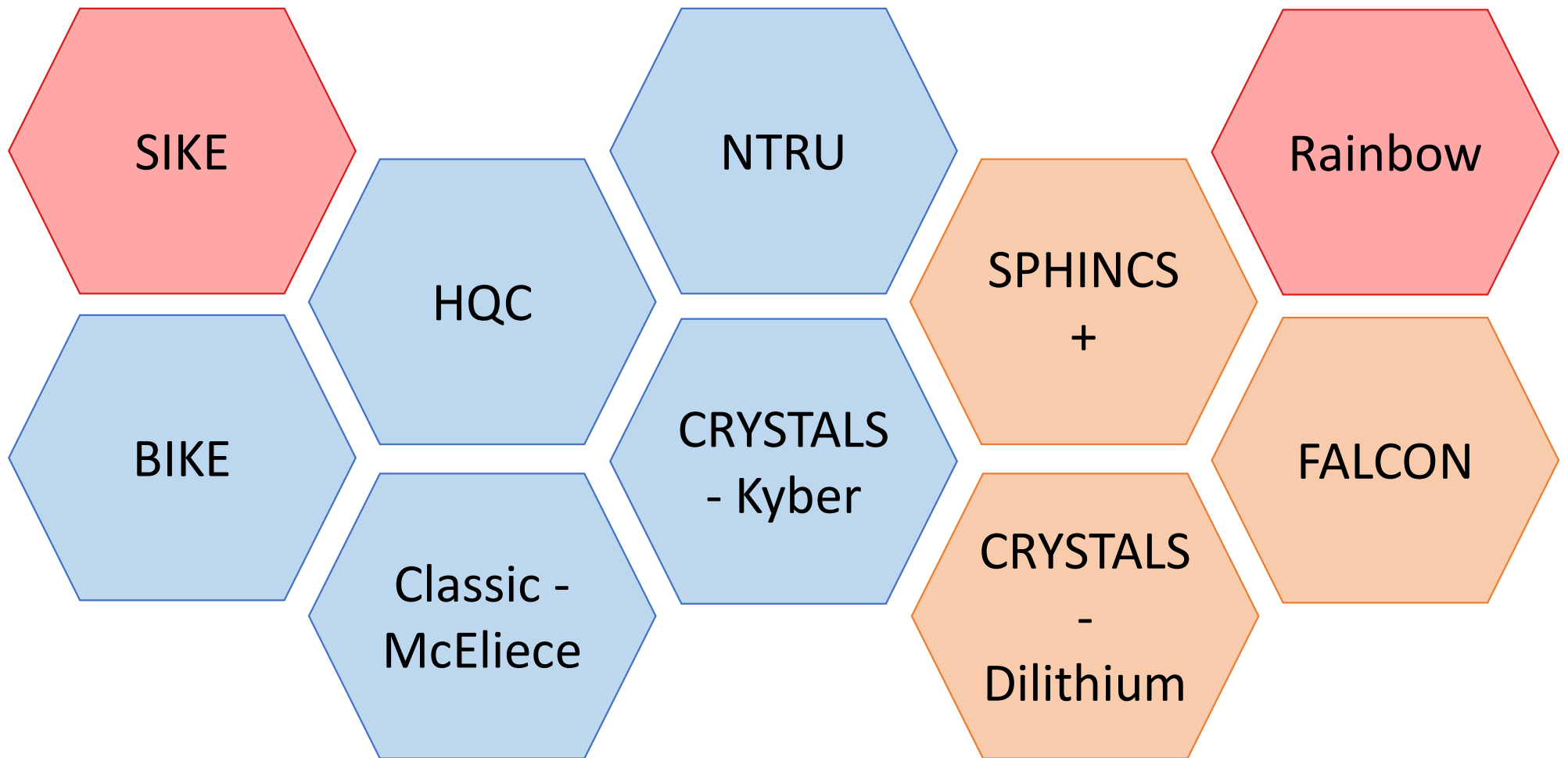


Evaluating the security of CRYSTALS-Dilithium in the QRROM

K. A. Jackson¹, Carl A. Miller^{2,3}, Daochen
Wang⁴

University of Maryland: Department of Physics¹ and
UMIACS², National Institute of Standards and
Technology³, University of British Columbia:
Department of Computer Science⁴

Cryptography must adapt to a post-quantum setting



Quantum-accessible hash functions are constructed from classical hash functions

Classical:

$$H_C: \{0,1\}^* \rightarrow \{0,1\}^n, n \in \mathbb{Z}^+$$

Quantum:

$$H_Q: \sum_{j \in \{0,1\}^n} \alpha_j |j\rangle |0\rangle \mapsto \sum_{j \in \{0,1\}^n} \alpha_j |j\rangle |H_C(j)\rangle$$

The (Quantum) Random Oracle Model is a useful post-quantum tool

Classical:

$$H_C: \{0,1\}^* \rightarrow \{0,1\}^n, n \in \mathbb{Z}^+$$

Quantum:

$$H_Q: \sum_{j \in \{0,1\}^n} \alpha_j |j\rangle |0\rangle \mapsto \sum_{j \in \{0,1\}^n} \alpha_j |j\rangle |H_C(j)\rangle$$

Standard Model:

$$\Pr[H \text{ "breaks"}] \leq \text{Adv}[\textit{Assumption}] + \text{negl}(n)$$

Random Oracle Model:

$$\Pr[H \text{ "breaks"}] \leq \text{negl}(n)$$

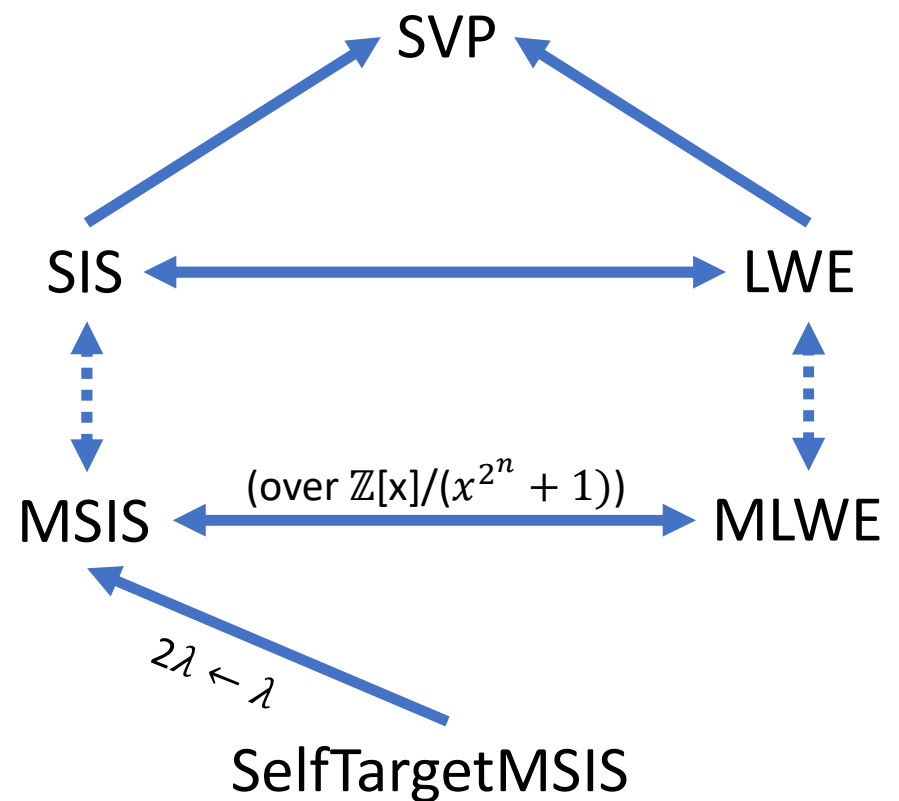
CRYSTALS-Dilithium's security depends on a novel problem

$$\begin{aligned} \mathit{Adv}_{\mathit{Dilithium}}^{\mathit{SEUF-CMA}}(A) \leq & \\ & \mathit{Adv}_{k,l,D}^{\mathit{MLWE}}(B) \\ & + \mathit{Adv}_{q,k,l+1,\gamma}^{\mathit{SelfTargetMSIS}}(C) \\ & + \mathit{Adv}_{q,k,l,\gamma'}^{\mathit{MSIS}}(D) \\ & + 2^{-254} \end{aligned}$$

CRYSTALS-Dilithium's security depends on a novel problem

$$\begin{aligned} \text{Adv}_{\text{Dilithium}}^{\text{SEUF-CMA}}(A) \leq & \\ & \text{Adv}_{k,l,D}^{\text{MLWE}}(B) \\ & + \text{Adv}_{q,k,l+1,\gamma}^{\text{SelfTargetMSIS}}(C) \\ & + \text{Adv}_{q,k,l,\gamma'}^{\text{MSIS}}(D) \\ & + 2^{-254} \end{aligned}$$

ROM: $X \rightarrow Y$, X at least as hard as Y



Structure Definitions

$$R_q := Z_q[X]/(X^n + 1)$$

Structure Definitions

$$R_q := Z_q[X]/(X^n + 1)$$

$$S_\lambda := \{p \in R_q : |p|_\infty \leq \lambda\} \quad (\text{Small})$$


Structure Definitions


$$R_q := Z_q[X]/(X^n + 1)$$

$$S_\lambda := \{p \in R_q : |p|_\infty \leq \lambda\} \quad (\text{Small})$$

$$B_\tau := \{p \in R_q : |p|_\infty \leq 1 \wedge |p|_1 = \tau\} \quad (\text{Short})$$

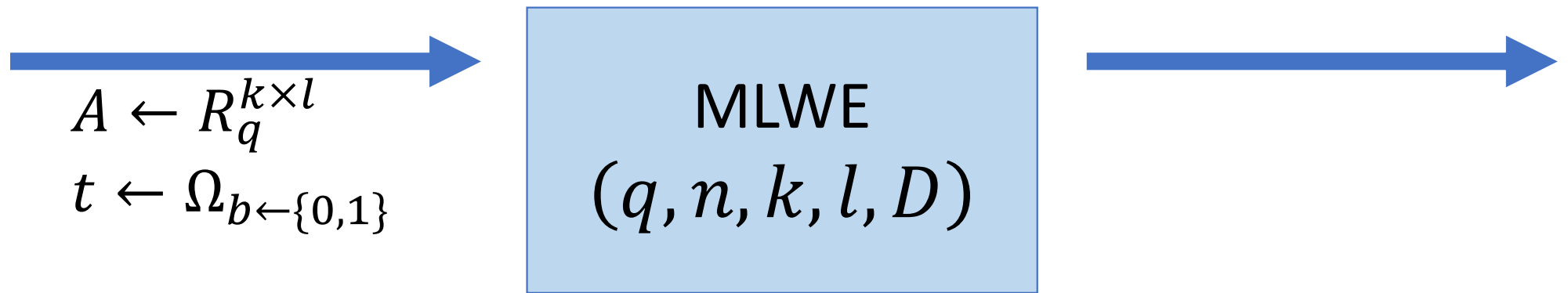
Definition of MLWE


$$A \leftarrow R_q^{k \times l}$$
$$t \leftarrow \Omega_{b \leftarrow \{0,1\}}$$



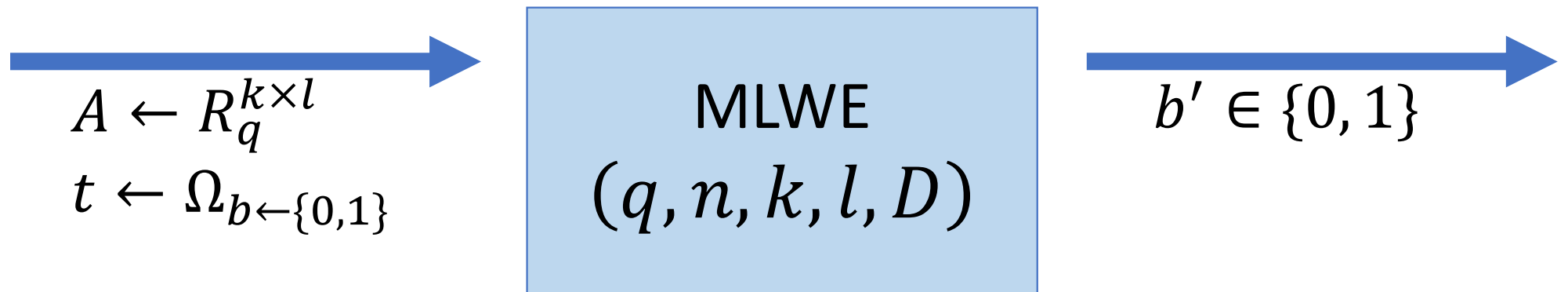
MLWE
 (q, n, k, l, D)

Definition of MLWE



$$\Omega_b := \begin{cases} R_q^k & b = 0 \\ \{As_1 + s_2 : s_1 \leftarrow D^l, s_2 \leftarrow D^k\} & b = 1 \end{cases}$$

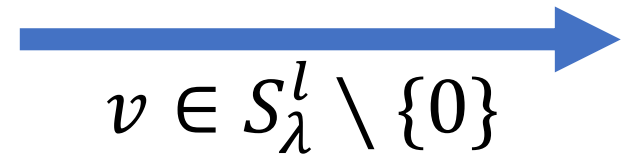
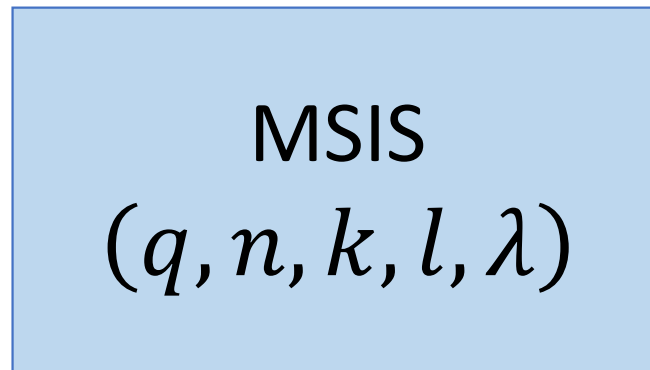
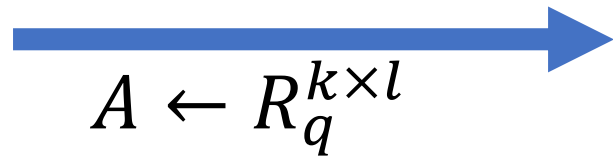
Definition of MLWE



$$\Omega_b := \begin{cases} R_q^k & b = 0 \\ \{As_1 + s_2 : s_1 \leftarrow D^l, s_2 \leftarrow D^k\} & b = 1 \end{cases}$$

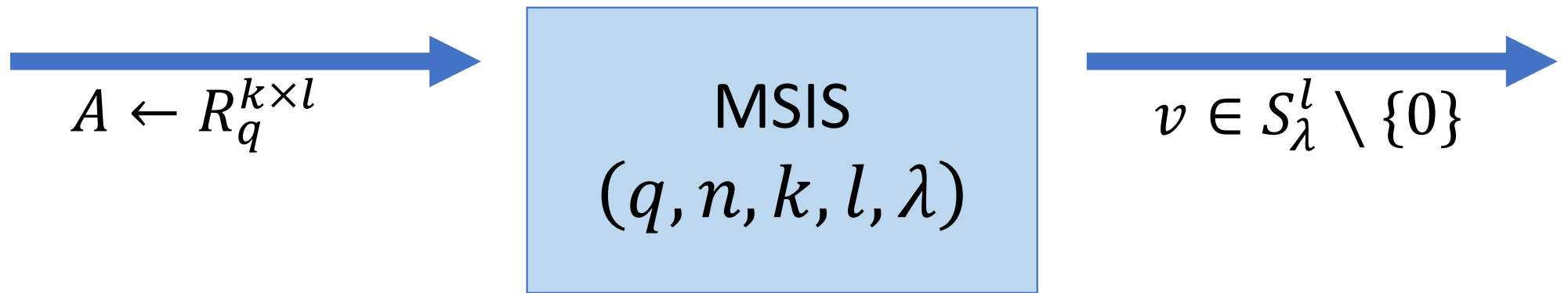
Definition of MSIS

$S_\lambda := \{p \in R_q \mid 0 \leq |p|_\infty \leq \lambda\}$, set of “small” vectors



Definition of MSIS

$S_\lambda := \{p \in R_q \mid 0 \leq |p|_\infty \leq \lambda\}$, set of “small” vectors



Requires: $A \cdot v = 0$

Definition of SelfTargetMSIS

$S_\lambda := \{p \in R_q \mid 0 \leq |p|_\infty \leq \lambda\}$, set of “small” vectors

$B_\tau := \{p \in R_q \mid \tau \text{ elements} = 1\}$, set of “short” vectors



SelfTargetMSIS
 $(q, n, \lambda, k, l, \tau)$



Definition of SelfTargetMSIS

$S_\lambda := \{p \in R_q \mid 0 \leq |p|_\infty \leq \lambda\}$, set of “small” vectors

$B_\tau := \{p \in R_q \mid \tau \text{ elements} = 1\}$, set of “short” vectors

$H \leftarrow \text{Func}(R_q^k, B_\tau)$


$A \leftarrow R_q^{k \times l}$

SelfTargetMSIS
 $(q, n, \lambda, k, l, \tau)$

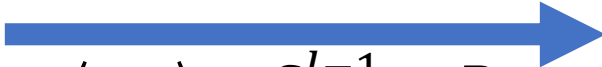
Definition of SelfTargetMSIS

$S_\lambda := \{p \in R_q \mid 0 \leq |p|_\infty \leq \lambda\}$, set of “small” vectors

$B_\tau := \{p \in R_q \mid \tau \text{ elements} = 1\}$, set of “short” vectors


$$H \leftarrow \text{Func}(R_q^k, B_\tau)$$
$$A \leftarrow R_q^{k \times l}$$


SelfTargetMSIS
 $(q, n, \lambda, k, l, \tau)$


$$\langle r, c \rangle \in S_\lambda^{l-1} \times B_\tau$$


Definition of SelfTargetMSIS

$S_\lambda := \{p \in R_q \mid 0 \leq |p|_\infty \leq \lambda\}$, set of “small” vectors

$B_\tau := \{p \in R_q \mid \tau \text{ elements} = 1\}$, set of “short” vectors


$$H \leftarrow \text{Func}(R_q^k, B_\tau)$$
$$A \leftarrow R_q^{k \times l}$$

SelfTargetMSIS
 $(q, n, \lambda, k, l, \tau)$


$$\langle r, c \rangle \in S_\lambda^{l-1} \times B_\tau$$

Requires: $H(A \cdot \langle r, c \rangle) = c$

Proof Roadmap

$$1. \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{SelfTargetMSIS}}(A|H) \leq \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{Chosen Coordinate Binding}}(B)$$

$$2. \leq \text{Adv}_{q,n,k,l,\lambda}^{\text{Collapsing}}(C)$$

$$3. \leq \text{Adv}_{q,n,k,l,S_\eta}^{\text{MLWE}}(D), \eta < \left\lfloor \frac{q}{32} \right\rfloor / 2\lambda nl$$

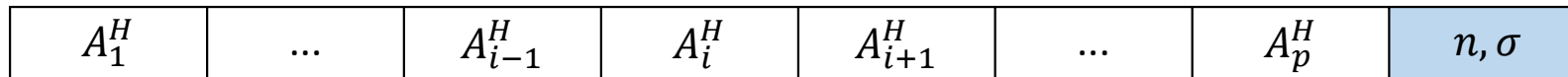
Proof Roadmap

$$1. \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{SelfTargetMSIS}}(A|H) \leq \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{Chosen Coordinate Binding}}(B)$$

$$2. \leq \text{Adv}_{q,n,k,l,\lambda}^{\text{Collapsing}}(C)$$

$$3. \leq \text{Adv}_{q,n,k,l,S_\eta}^{\text{MLWE}}(D), \eta < \left\lfloor \frac{q}{32} \right\rfloor / 2\lambda nl$$

Rewinding works in the ROM, but not the QRROM

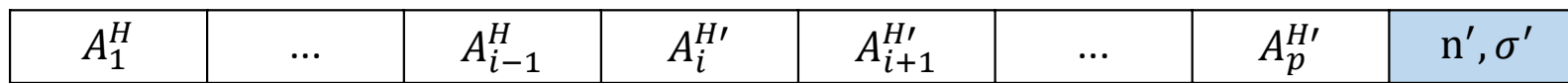
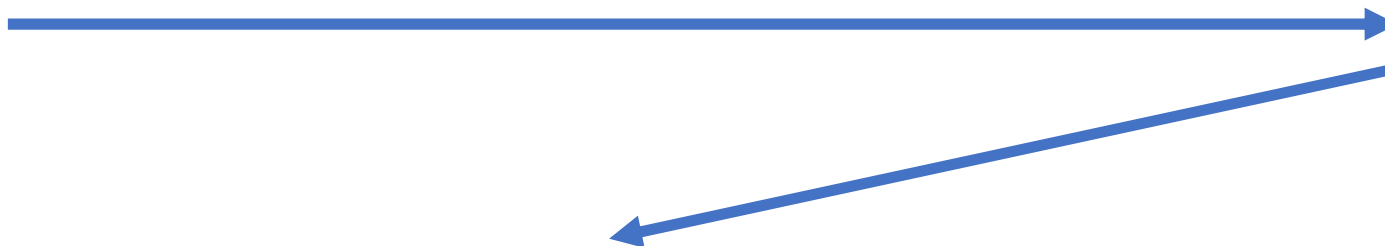
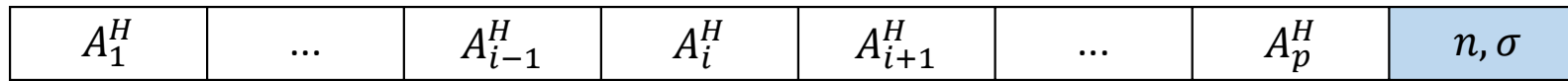


Glossary:

$H: X \rightarrow Y$

A : p -classical
query alg. with
 δ success prob.

Rewinding works in the ROM, but not the QRROM

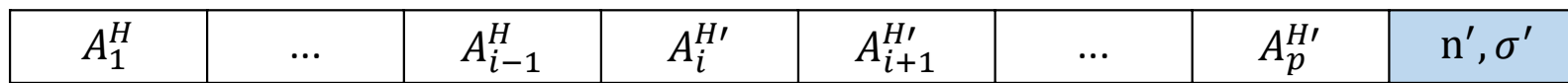
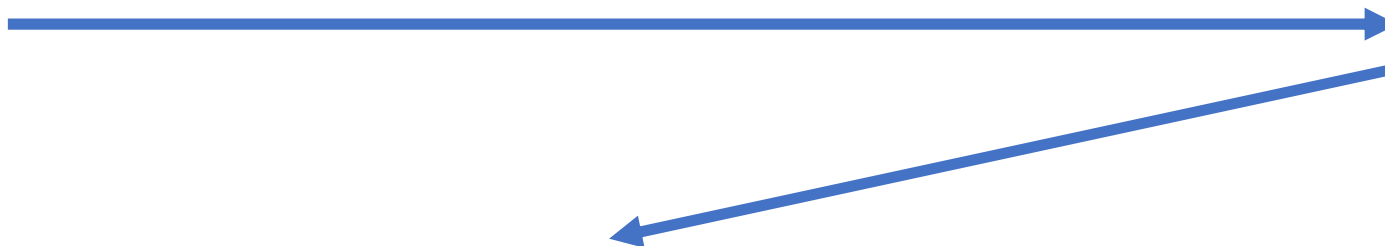


Glossary:

$$H: X \rightarrow Y$$

A : p -classical query alg. with δ success prob.

Rewinding works in the ROM, but not the QRROM



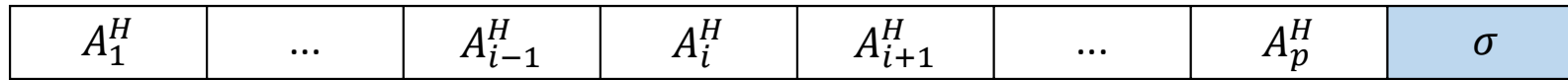
Glossary:

$H: X \rightarrow Y$

$A: p$ -classical query alg. with δ success prob.

$$\text{ROM: } \Pr[n = n' \wedge \sigma \neq \sigma'] \geq \delta \left(\frac{\delta}{p} - \frac{1}{|X|} \right)$$

Reprogramming can be used in the QRROM



Glossary:

$H: X \rightarrow Y$

$A: p$ -quantum
query alg. with
 δ success
prob.

Reprogramming can be used in the QRROM



$$H[x, y](x') := \begin{cases} H(x'), & x' \neq x \\ y, & x' = x \end{cases}$$

Glossary:

$H: X \rightarrow Y$

$A: p$ -quantum query alg. with δ success prob.

We map quantum-query SelfTargetMSIS to classical-query SelfTargetMSIS

| | | | | | | | |
|---------|-----|-------------|---------|-------------|-----|---------|----------|
| A_1^H | ... | A_{i-1}^H | A_i^H | A_{i+1}^H | ... | A_p^H | σ |
|---------|-----|-------------|---------|-------------|-----|---------|----------|



| | | | | | | | |
|---------|-----|-------------|------------|-------------|-----|---------|-----------|
| A_1^H | ... | A_{i-1}^H | $A_i^{H'}$ | A_{i+1}^H | ... | A_p^H | σ' |
|---------|-----|-------------|------------|-------------|-----|---------|-----------|



$$\delta_S \geq \frac{\delta_A}{(2p + 1)^2}$$

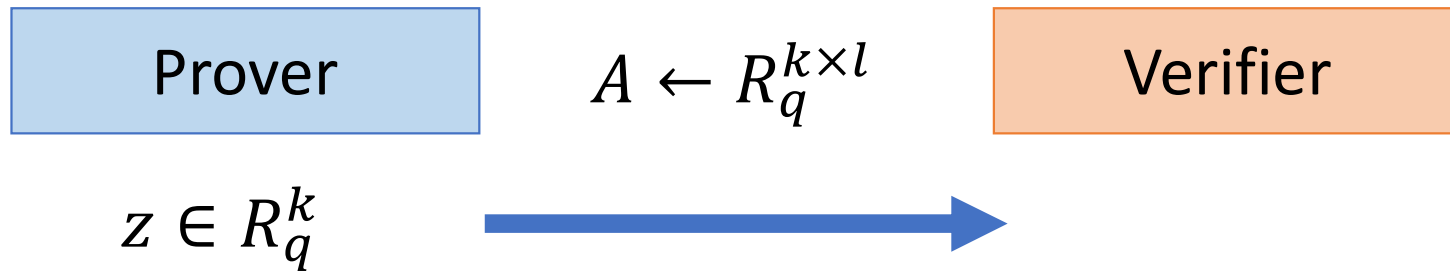
Glossary:

$H: X \rightarrow Y$

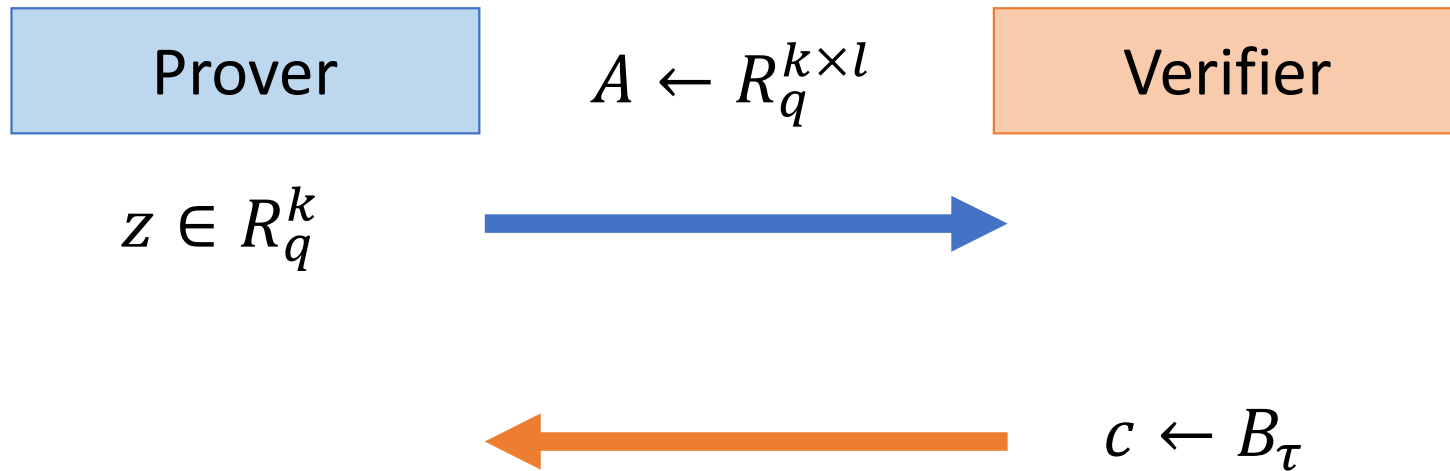
A : p -quantum
query quantum alg.

S : 1-classical query
quantum alg.

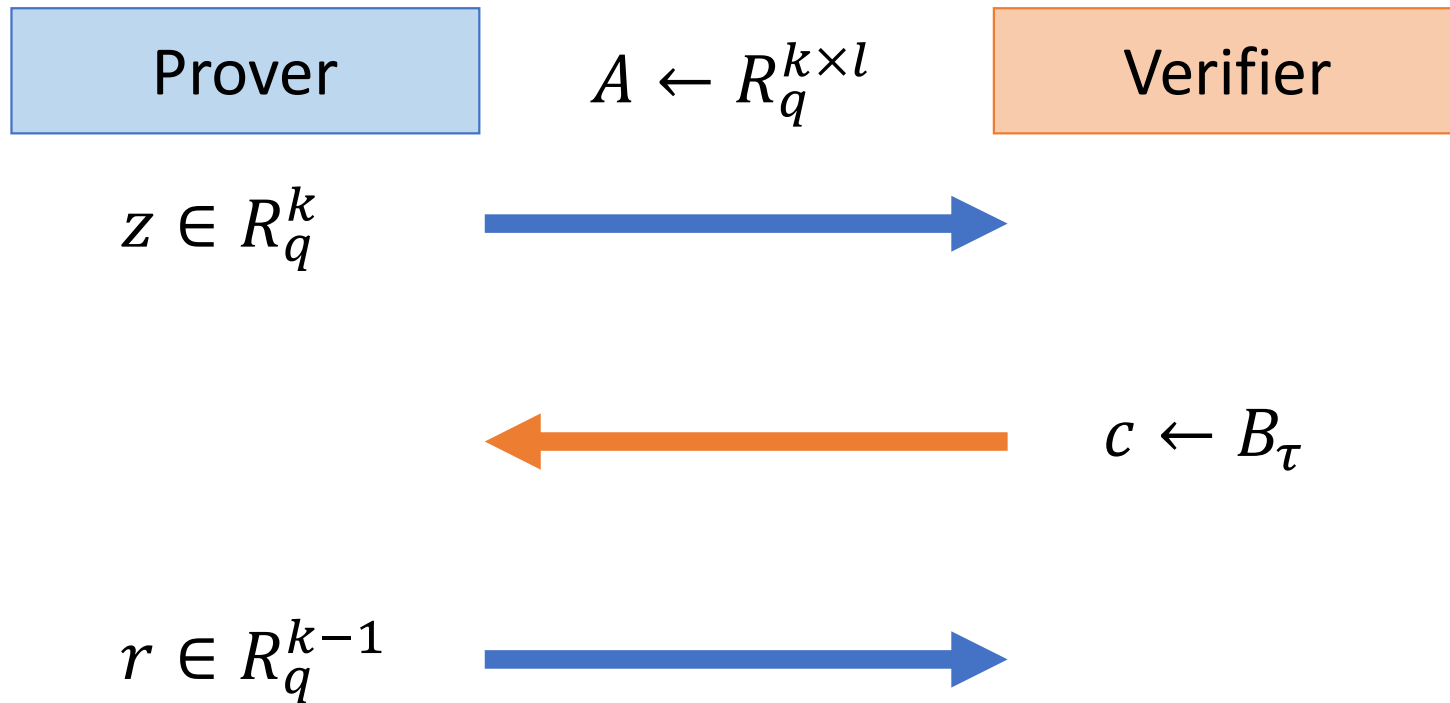
Mapping SelfTargetMSIS to a Chosen-Coordinate Binding Experiment



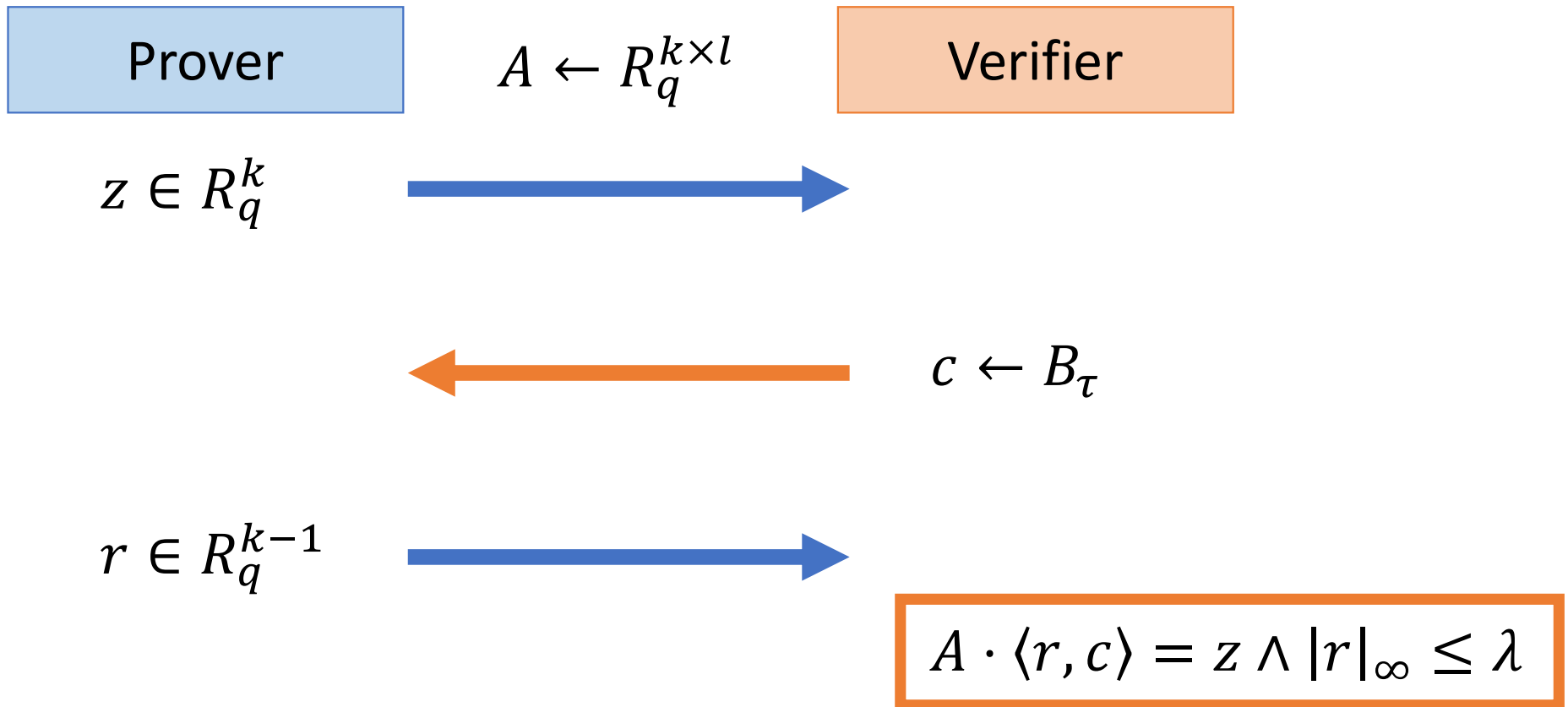
Mapping SelfTargetMSIS to a Chosen-Coordinate Binding Experiment



Mapping SelfTargetMSIS to a Chosen-Coordinate Binding Experiment



Mapping SelfTargetMSIS to a Chosen-Coordinate Binding Experiment



Proof Roadmap

$$1. \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{SelfTargetMSIS}}(A|H) \leq \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{Chosen Coordinate Binding}}(B)$$

$$2. \leq \text{Adv}_{q,n,k,l,\lambda}^{\text{Collapsing}}(C)$$

$$3. \leq \text{Adv}_{q,n,k,l,S_\eta}^{\text{MLWE}}(D), \eta < \left\lfloor \frac{q}{32} \right\rfloor / 2\lambda nl$$

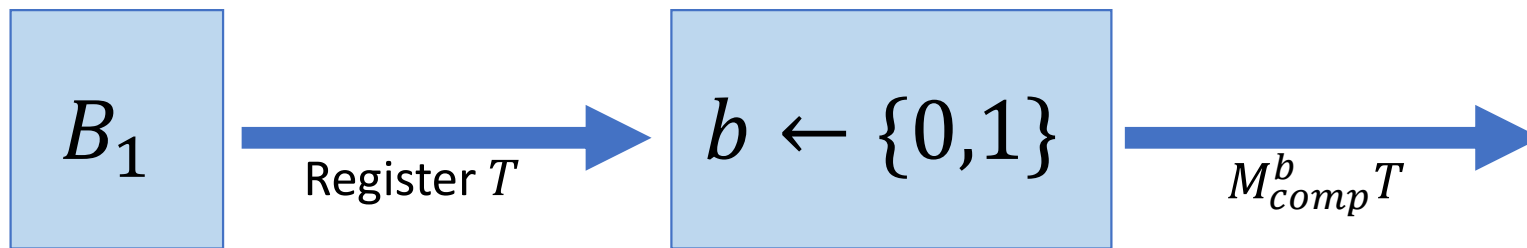
What is a Collapsingness Experiment?

- Algorithm (B_1, B_2) passes the collapsingness experiment iff B_1 can construct a register such that B_2 has a better than random chance of detecting if a verifier has destructively measured the register



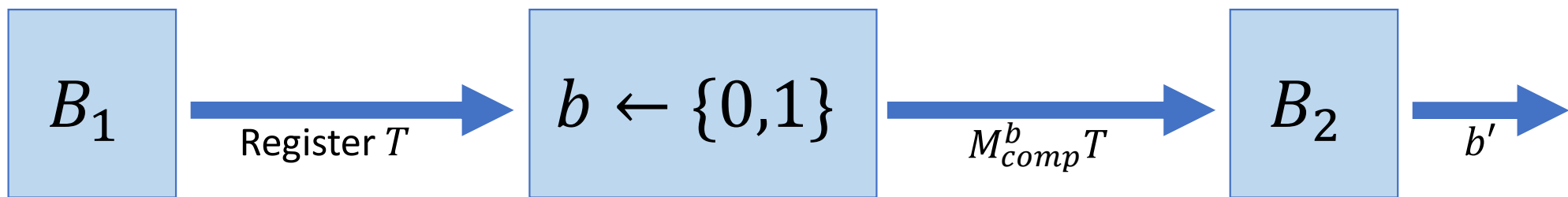
What is a Collapsingness Experiment?

- Algorithm (B_1, B_2) passes the collapsingness experiment iff B_1 can construct a register such that B_2 has a better than random chance of detecting if a verifier has destructively measured the register



What is a Collapsingness Experiment?

- Algorithm (B_1, B_2) passes the collapsingness experiment iff B_1 can construct a register such that B_2 has a better than random chance of detecting if a verifier has destructively measured the register



$$\delta_{collapse} := \Pr[b' = b]$$

Mapping the Chosen-Coordinate Binding Experiment to a Collapsingness Experiment

$$A = (A_1, A_2)$$

Builds registers over $R_q^k, R_q^l, B_\tau, \{0, 1\}^*$

Mapping the Chosen-Coordinate Binding Experiment to a Collapsingness Experiment

$$A = (A_1, A_2)$$

U

Apply Π

Builds registers over $R_q^k, R_q^l, B_\tau, \{0, 1\}^*$

$$\Pi := \sum_{c \in B_\tau} \sum_{\substack{(z,y) \in R_q^k \times R_q^l \\ |y|_\infty \leq \tau, Ay=z, y_l=c}} |z, y\rangle\langle z, y| \otimes |c\rangle\langle c| \otimes I_T$$

Mapping the Chosen-Coordinate Binding Experiment to a Collapsingness Experiment

$$A = (A_1, A_2)$$

U

Apply Π

U^\dagger

Measure B_τ register

Builds registers over $R_q^k, R_q^l, B_\tau, \{0, 1\}^*$

$$\Pi := \sum_{c \in B_\tau} \sum_{\substack{(z,y) \in R_q^k \times R_q^l \\ |y|_\infty \leq \tau, Ay=z, y_l=c}} |z, y\rangle\langle z, y| \otimes |c\rangle\langle c| \otimes I_T$$

$$\delta_{collapse} - \frac{1}{2} \geq \frac{\delta_{CCB}}{2} \left(\delta_{CCB} - \frac{1}{|B_\tau|} \right)$$

Proof Roadmap

$$1. \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{SelfTargetMSIS}}(A|H) \leq \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{Chosen Coordinate Binding}}(B)$$

$$2. \leq \text{Adv}_{q,n,k,l,\lambda}^{\text{Collapsing}}(C)$$

$$3. \leq \text{Adv}_{q,n,k,l,S_\eta}^{\text{MLWE}}(D), \eta < \left\lfloor \frac{q}{32} \right\rfloor / 2\lambda nl$$

A Collapsingness Distinguisher Implies an MLWE Distinguisher

$$B = (B_1, B_2)$$

I

vs.

M_{comp}

$MLWE$

$$(A, b) \\ b := Ax + \epsilon$$

vs.

$$(A, b) \\ b \leftarrow R_q^k$$

A Collapsingness Distinguisher Implies an MLWE Distinguisher

$$B = (B_1, B_2)$$



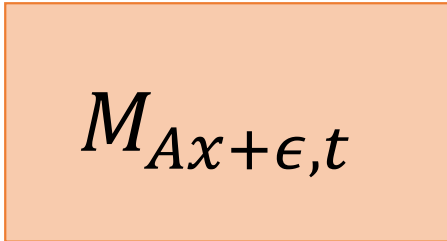
I

vs.



M_{comp}

$MLWE$



$M_{Ax+\epsilon,t}$

vs.

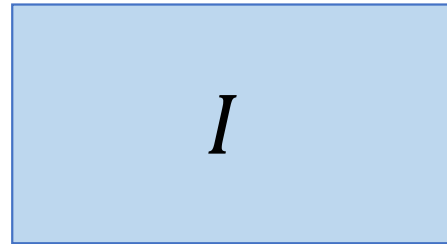


$M_{R_q^k,t}$

$M_{D,t} := b \leftarrow D, s \leftarrow R_q$ then measure $y \mapsto \text{Round}_t(b \cdot y + s)$

A Collapsingness Distinguisher Implies an MLWE Distinguisher

$$B = (B_1, B_2)$$



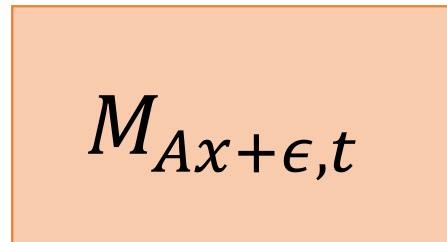
vs.



\gg

\gg

MLWE



vs.



$$M_{D,t} := b \leftarrow D, s \leftarrow R_q \text{ then measure } y \mapsto \text{Round}_t(b \cdot y + s)$$

Details on *Collapse* \rightarrow *MLWE*

I : identity operator

M_0 : computational basis measurement

M_{MLWE}^t : $[y \mapsto [(b \cdot y + s)_0]_t | s \leftarrow R_q, e_1 \leftarrow S_\eta^m, e_2 \leftarrow S_\eta^l, b := e_1^T A + e_2^T \in R_q^l]$

M_{rand}^t : $[y \mapsto [(b \cdot y + s)_0]_t | s \leftarrow R_q, b \leftarrow R_q^l]$

Details on *Collapse* \rightarrow *MLWE*

I : identity operator

M_0 : computational basis measurement

M_{MLWE}^t : $[y \mapsto [(b \cdot y + s)_0]_t | s \leftarrow R_q, e_1 \leftarrow S_\eta^m, e_2 \leftarrow S_\eta^l, b := e_1^T A + e_2^T \in R_q^l]$

M_{rand}^t : $[y \mapsto [(b \cdot y + s)_0]_t | s \leftarrow R_q, b \leftarrow R_q^l]$

We can prove that for some parameters:

$$\begin{array}{l} M_{MLWE}^t = \frac{1}{d} M_{MLWE}^{td}(\rho) + \left(1 - \frac{1}{d}\right) \rho \\ M_{rand}^t = \frac{1}{d} M_0 \left(M_{MLWE}^{td}(\rho) \right) + \left(1 - \frac{1}{d} - p_t\right) M_0(\rho) + p_t \rho \end{array} \xrightarrow{p_t \ll 1 \ll d} \begin{array}{l} M_{MLWE}^t \approx \rho \\ M_{rand}^t \approx M_0(\rho) \end{array}$$

SelfTargetMSIS to MLWE Reduction for Security Applications

Conclusion: An algorithm that solves $SelfTargetMSIS_{H,\tau,m,k}$ with advantage ϵ from p queries reduces to $MLWE_{m+k,m,\eta}$ with advantage like $O(\epsilon^2/p^4)$ for $\eta = O(q/n(m+k)\gamma)$.

We can approximate quantum Core-SVP security like:

$$z_{STMSIS} \geq \frac{z_{MLWE}}{2} - \frac{3}{2} \log(p_{max}) - 3$$

Proof Roadmap

$$1. \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{SelfTargetMSIS}}(A|H) \leq \text{Adv}_{q,n,k,l,\lambda,\tau}^{\text{Chosen Coordinate Binding}}(B)$$

$$2. \leq \text{Adv}_{q,n,k,l,\lambda}^{\text{Collapsing}}(C)$$

$$3. \leq \text{Adv}_{q,n,k,l,S_\eta}^{\text{MLWE}}(D), \eta < \left\lfloor \frac{q}{32} \right\rfloor / 2\lambda nl$$

Conclusions

- We provide the first proof that SelfTargetMSIS is hard in the QROM

Conclusions

- We provide the first proof that SelfTargetMSIS is hard in the QRROM
- Compared to original Dilithium:

- Increase q $2^{23} \rightarrow 2^{43}$
- Increase size of pk $\approx 12.1 \times$
- Increase size of σ $\approx 3.7 \times$

Conclusions

- We provide the first proof that SelfTargetMSIS is hard in the QROM
- Compared to original Dilithium:

- Increase q $2^{23} \rightarrow 2^{43}$
- Increase size of pk $\approx 12.1 \times$
- Increase size of σ $\approx 3.7 \times$

- Provable security

Dilithium-QROM reformulates Dilithium in a different ring

- CRYSTALS-Dilithium

$$q = 1 \pmod{2n}$$
$$R_q \simeq Z_q^{(1)} \otimes \dots \otimes Z_q^{(1)}$$

- Dilithium-QROM

$$q = 5 \pmod{8}$$
$$R_q \simeq F_q^{(n/2)} \otimes F_q^{(n/2)}$$

Conclusions

- We provide the first proof that SelfTargetMSIS is hard in the QRROM
- Compared to Dilithium-QRROM:

- Increase size of pk $\approx 2.9 \times$

- Increase size of σ $\approx 1.3 \times$

Conclusions

- We provide the first proof that SelfTargetMSIS is hard in the QRROM
- Compared to Dilithium-QRROM:

- Increase size of pk $\approx 2.9 \times$

- Increase size of σ $\approx 1.3 \times$

- Better-studied ring structure

- Faster *KeyGen* $1.9 \times, 3.4 \times$

- Faster *Sign* $1.9 \times, 3.4 \times$

- Faster *Verify* $2.0 \times, 3.6 \times$

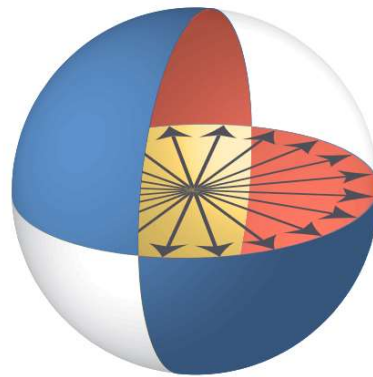
Conclusions

- We provide the first proof that SelfTargetMSIS is hard in the QRROM
- Our version of Dilithium is:
 - Provably secure under safer assumptions than CRYSTALS-Dilithium
 - More efficient to implement than Dilithium-QRROM

Acknowledgements



NIST



JOINT CENTER FOR
QUANTUM INFORMATION
AND COMPUTER SCIENCE



Questions?



1. Boneh et al. “Random Oracles in a Quantum World”. ASIACRYPT 2011. DOI: 10.1007/978-3-642-25385-0_3
2. Bai et al. “CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation, Round 3.1”. NIST: Post Quantum Cryptography. URL: <https://pq-crystals.org/dilithium/>
3. Langlois & Stehlé. “Worst-Case to Average-Case Reductions for Module Lattices”. Designs, Codes and Cryptography. DOI: 10.1007/s10623-014-9938-4
4. Bellare and Neven. “Multi-Signatures in the Plain Public-Key Model and a General Forking Lemma”. CCS '06. DOI: 10.1145/1180405.1180453
5. Don et al. “The Measure-and-Reprogram Technique 2.0: Multi-round Fiat-Shamir and More”. CRYPTO 2020. DOI: 10.1007/978-3-030-56877-1_21
6. Dall’Agnol & Spooner. “On the Necessity of Collapsing for Post-Quantum and Quantum Commitments”. TQC 2023. DOI: 10.4230/LIPIcs.TQC.2023.2
7. Jackson, Miller, & Wang. “Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model”. EUROCRYPT 2024. DOI:10.48550/arXiv.2312.16619

Define “breaking” a hash function

Assume:

- Realizable, Deterministic, Surjective
- Computationally Efficient
- $H: X \rightarrow Y$

$$\Pr[H \text{ "breaks"}] := \Pr[A, \text{Pre-Image}] + \Pr[B, \text{Collision}]$$

$$\Pr[A, \text{Pre-Image}] := \Pr[H(x') = y: x \leftarrow X, y := H(x), x' \leftarrow A^H(y)]$$

$$\Pr[B, \text{Collision}] := \Pr[H(x_1) = H(x_2) \wedge x_1 \neq x_2: (x_1, x_2) \leftarrow A^H]$$

The Forking Lemma is technically sound

Let A^H be a randomized p -query algorithm with access to $H: X \rightarrow Y$ that with given input χ and random queries $\{x_i: i \in [p]\} \in X^p$ outputs $(n, \sigma) \in Z \times Y^n$ for arbitrary constant n with success probability δ .

Then, the forking algorithm $R(A)[.]$ acts as follows:

1. Set random tape r for A and select inputs $\{x_i: i \in [p]\} \leftarrow X$ accordingly
2. Output $(n, \sigma) \leftarrow A(\chi, x_1, \dots, x_p: r)$. If $n = 0$, break and return $(0, \sigma, \sigma)$.
3. Select new inputs for A at random like $\{x'_j: j \in [n, p]\} \leftarrow X$
4. Output $(n', \sigma') \leftarrow A(\chi, x_1, \dots, x_{n-1}, x'_n, \dots, x'_p: r)$.
5. If $n = n'$ and $x_n \neq x'_n$, return $(1, \sigma, \sigma')$. Else return $(0, \sigma, \sigma')$

$$\Pr[b = 1: (b, \sigma, \sigma') \leftarrow R(A)[x]] \geq \delta \left(\frac{\delta}{p} - \frac{1}{|X|} \right) \forall x$$

Details on $CCB \rightarrow Collapse$

Lemma (Dall'Agnol & Spooner, 2023): Let P, Q be projectors in $C^{d \times d}$ and ρ be a density matrix in C^d such that $\rho Q = \rho$. Then, $\text{tr}(QP\rho P) \geq \text{tr}(P\rho)^2$.

1. Prep states with (A_1, A_2) , then apply U
2. Make projective measurement Π .
3. If measurement outputs $\Pi \leftrightarrow (A_1, A_2)$ passes:
 - $b := 1$.
 - Apply U^\dagger
 - Make projective measurement $|\psi\rangle\langle\psi|$ on the bound coordinate register.
 - If measurement outputs $|\psi\rangle\langle\psi|$:
 - $b' := 0$
 - Else, if measurement outputs $1 - |\psi\rangle\langle\psi|$:
 - $b' := 1$
- Else, if measurement outputs $1 - \Pi \leftrightarrow (A_1, A_2)$ fails:
 - $b := 0$
 - $b' \leftarrow \{0, 1\}$.

$$\delta_B \geq \frac{1}{2} + \frac{\delta_A}{2} \left(\delta_A - \frac{1}{|B_\tau|} \right)$$

$$\begin{aligned} \text{Time}(B) &\leq \text{Time}(A_1) \\ &+ 2\text{Time}(A_1) \\ &+ O(ml \log(q) \log(|B_\tau|)) \end{aligned}$$

Details on *Collapse* \rightarrow *MLWE*

I : identity operator

M_0 : computational basis measurement

M_{MLWE}^t : $[y \mapsto [(b \cdot y + s)_0]_t | s \leftarrow R_q, e_1 \leftarrow S_\eta^m, e_2 \leftarrow S_\eta^l, b := e_1^T A + e_2^T \in R_q^l]$

M_{rand}^t : $[y \mapsto [(b \cdot y + s)_0]_t | s \leftarrow R_q, b \leftarrow R_q^l]$

We can prove that for some parameters:

$$\begin{array}{l} M_{MLWE}^t = \frac{1}{d} M_{MLWE}^{td}(\rho) + \left(1 - \frac{1}{d}\right) \rho \\ M_{rand}^t = \frac{1}{d} M_0 \left(M_{MLWE}^{td}(\rho) \right) + \left(1 - \frac{1}{d} - p_t\right) M_0(\rho) + p_t \rho \end{array} \xrightarrow{p_t \ll 1 \ll d} \begin{array}{l} M_{MLWE}^t \approx \rho \\ M_{rand}^t \approx M_0(\rho) \end{array}$$

Concrete Parameter Tables

| | Dilithium [Bai+21] | | | Our Work | | |
|-----------------------|--------------------|-----------------|-----------------|----------|----------|----------|
| | SL2 | SL3 | SL5 | SL2 | SL3 | SL5 |
| q | $2^{23} - 8191$ | $2^{23} - 8191$ | $2^{23} - 8191$ | q_0 | q_0 | q_0 |
| n | 256 | 256 | 256 | 256 | 256 | 256 |
| (k, l) | (4, 4) | (6, 5) | (8, 7) | (20, 15) | (24, 24) | (32, 32) |
| d | 13 | 13 | 13 | 17 | 17 | 17 |
| τ | 39 | 49 | 60 | 45 | 45 | 45 |
| γ_1 | 2^{17} | 2^{19} | 2^{19} | 357889 | 515361 | 687147 |
| γ_2 | 95232 | 261888 | 261888 | 715778 | 1030722 | 1374294 |
| ζ | 350209 | 724481 | 769537 | 4380677 | 5010565 | 5697709 |
| ζ' | 380930 | 1048184 | 1048336 | 2863114 | 4122890 | 5497178 |
| η | 2 | 4 | 2 | 2 | 2 | 2 |
| η' | N/A | N/A | N/A | 5 | 3 | 2 |
| pk size (bytes) | 1312 | 1952 | 2592 | 17952 | 21536 | 28704 |
| σ size (bytes) | 2464 | 3272 | 4561 | 10757 | 16933 | 23589 |
| Expected Repeats | 4.25 | 5.10 | 3.85 | 5.00 | 5.00 | 5.00 |
| LWE BKZ block-Size | 448 | 669 | 911 | 1044 | 1823 | 2581 |
| Quantum Core-SVP | 118 | 177 | 241 | 276 | 483 | 683 |
| "SelfTargetMSIS" BKZ | N/A | N/A | N/A | 1720 | 2186 | 3020 |
| Quantum Core-SVP | N/A | N/A | N/A | 96 | 143 | 205 |
| SIS BKZ Block-Size | 363 | 533 | 773 | 4746 | 5550 | 7449 |
| Quantum Core-SVP | 96 | 141 | 204 | 1257 | 1470 | 1973 |

| Dilithium-QROM [KLS18] | | Our Work | |
|------------------------|------------------|----------|-----------|
| recc. | very high | recc. | very high |
| $2^{45} - 21283$ | $2^{45} - 21283$ | q_0 | q_0 |
| 256 | 256 | 256 | 256 |
| (8, 8) | (10, 10) | (26, 26) | (32, 31) |
| 15 | 15 | 17 | 17 |
| 46 | 46 | 45 | 45 |
| 905679 | 905679 | 558307 | 672832 |
| 905679 | 905679 | 1116614 | 1345664 |
| 2565023 | 2565023 | 5182349 | 5640449 |
| 3622718 | 3622718 | 4466458 | 5382658 |
| 7 | 3 | 2 | 2 |
| N/A | N/A | 3 | 2 |
| 7712 | 9632 | 23328 | 28704 |
| 5670 | 7078 | 19173 | 22885 |
| 4.29 | 2.18 | 5.00 | 5.00 |
| 499 | 620 | 2009 | 2487 |
| 132 | 164 | 532 | 659 |
| N/A | N/A | 2408 | 3000 |
| N/A | N/A | 129 | 158 |
| 1557 | 2038 | 6025 | 7475 |
| 412 | 540 | 1596 | 1980 |

Concrete Complexity Tables

| | Dilithium-QROM [KLS18] | | Our Work | | |
|------------------------------------|-------------------------|-----------|----------|-----------|---------|
| | recc. | very high | recc. | very high | |
| $q = 1 \bmod 2n$ | Integer Multiplications | | | | |
| NTT +: $\frac{3}{2}n \log n + 2n$ | Gen | 863089 | 1348576 | 348902 | 604764 |
| NTT ×: $3n \log n$ | Sign | 3640076 | 3112514 | 988556 | 1447944 |
| $q = 5 \bmod 8$ | Verify | 1078861 | 1618291 | 377978 | 651284 |
| | Integer Additions | | | | |
| HTT +: $\frac{3}{2}n \log n + 96n$ | Gen | 2883298 | 4504512 | 577484 | 1000631 |
| HTT ×: $3n \log n + 333n$ | Sign | 12178026 | 10407247 | 1685272 | 2460175 |
| | Verify | 3603610 | 5404902 | 625395 | 1077288 |

| | | |
|--------|--------------------|--------|
| Gen | Sign | Verify |
| • kl | • $kl + (l + 2k)r$ | • kl |