SQIsign with Fixed-Precision Integer Arithmetic

Won Kim, Jeonghwan Lee,
Hyeonhak Kim, Changmin Lee

SQIsign

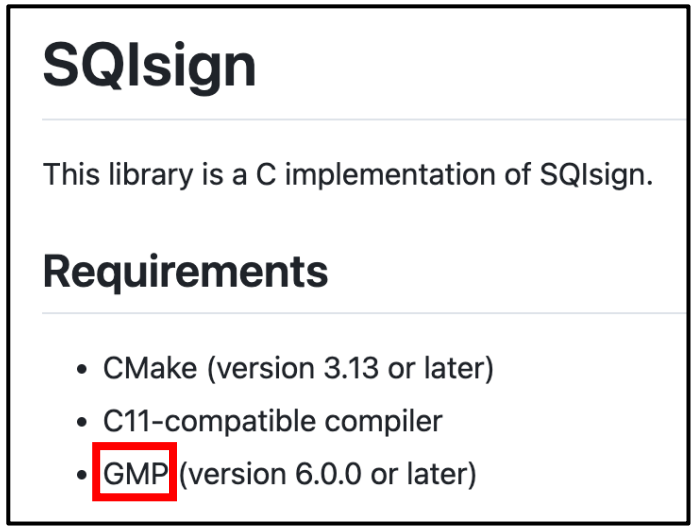
- Isogeny-based (Post-Quantum) digital signature scheme
- A candidate of NIST PQC standard
- **Small Key & Signature sizes**

Algorithm	Public Key (bytes)			Signature (bytes)		
	NIST-I	NIST-III	NIST-V	NIST-I	NIST-III	NIST-V
SQIsign	**65**	**97**	**129**	**148**	**224**	**292**
ML-DSA	1312	1952	2592	2420	3309	4627
Falcon	897		1793	666		1280
SLH-DSA	32	48	64	7856	16224	29792

Challenges

- SQIsign needs quaternion arithmetic over **field of rational numbers** $\mathbb{Q}$
- $\mathbb{Q}$: **No size bound** on numerators, denominators

  ∴ Fixed-precision implementation of SQIsign is challenging

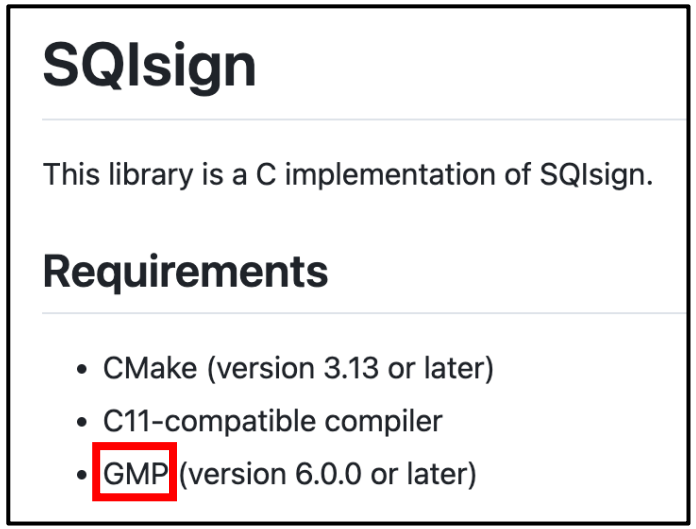


Challenges

- SQIsign needs quaternion arithmetic over **field of rational numbers** $\mathbb{Q}$
- $\mathbb{Q}$: **No size bound** on numerators, denominators

  ∴ Fixed-precision implementation of SQIsign is challenging

- **Why Fixed-Precision?**
  - Constant-time implementation
  - Implementation for memory-constrained devices



Contributions

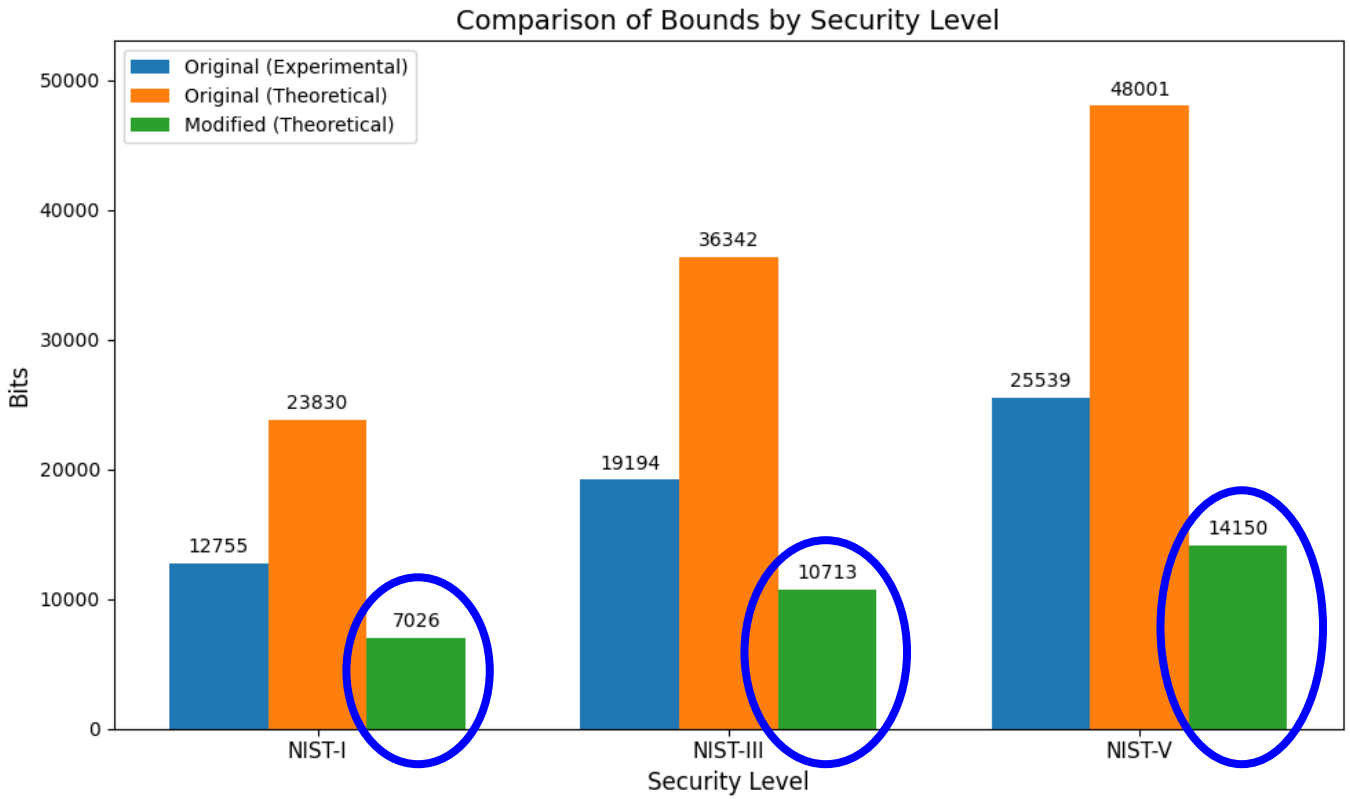
PQSnC
Post-Quantum Security and Cryptography

- **First theoretical uniform bound on KeyGen and Sign of SQIsign**
  - KeyGen bound : $\mathbf{2^{50}} p^{14} (log\ p)^{96}$
  - Sign bound : $\mathbf{2^{50}} p^{95}$

Contributions

PQSnC
Post-Quantum Security and Cryptography

- **First theoretical uniform bound on KeyGen and Sign of SQIsign**
  - KeyGen bound : $\boldsymbol{2^{50}p^{14}(log\ p)^{96}}$
  - Sign bound : $\boldsymbol{2^{50}p^{95}}$
- **Reducing the necessary precision**
  - **Improved KeyGen bound:** $2^{68}p^{9}$
  - **Improved Sign bound:** $2^{16}p^{28}$



Quaternion Algebras in SQIsign

PQSnC
Post-Quantum Security and Cryptography

Elliptic-curve world	Quaternion-algebra world
E (supersingular)	$\mathcal{O} = \mathrm{End}(E) \subset B_{p,\infty}$
$\varphi : E \to E'$	Left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\deg(\varphi)$	$\mathrm{nrd}(I_\varphi)$
$\varphi, \psi : E \to E'$ equivalent	$I_\varphi \sim I_\psi$
$\hat{\varphi} : E' \to E$	$I_{\hat{\varphi}}$
$\varphi \circ \psi$	$I_\psi \cdot I_\varphi$

- **Deuring correspondence:** 1-1 between elliptic-curve objects and quaternion-algebra objects
- SQIsign accelerates isogeny computations by replacing them with (quaternion) ideal computations.

Quaternion Algebras in SQIsign

PQSnC
Post-Quantum Security and Cryptography

- $B_{p,\infty}$: Quaternion algebra, with $\mathbb{Q}$-basis $\{1, i, j, k\}$ for $(i^2 = -1, j^2 = -p, k \coloneqq ij = -ji$ with $p \equiv 3 \pmod 4)$
- Reduced norm $\mathrm{nrd}(\alpha) \coloneqq \alpha\bar{\alpha} \in \mathbb{Q}$ where $\bar{\alpha} \coloneqq a - bi - cj - dk$ for $(\alpha = a + bi + cj + dk)$

Quaternion Algebras in SQIsign

- $B_{p,\infty}$: Quaternion algebra, with $\mathbb{Q}$-basis $\{1, i, j, k\}$ for $(i^2 = -1, j^2 = -p, k \coloneqq ij = -ji$ with $p \equiv 3 \pmod 4)$
- Reduced norm $\mathrm{nrd}(\alpha) \coloneqq \alpha\bar{\alpha} \in \mathbb{Q}$ where $\bar{\alpha} \coloneqq a - bi - cj - dk$ for $(\alpha = a + bi + cj + dk)$

- Ideals : Quaternion lattices $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3 + \mathbb{Z}\alpha_4$
- Reduced norm $\mathrm{nrd}(I) \coloneqq \gcd\{\mathrm{nrd}(\alpha) : \alpha \in I\}$
- Ideal Multiplication $I_1 I_2 \coloneqq \{\alpha\beta : \alpha \in I_1, \beta \in I_2\}$

Quaternion Algebras in SQIsign

PQSnC
Post-Quantum Security and Cryptography

- Representing ideals = Representing $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \rightarrow$ **4x4 integer matrix** (after clearing denominators)
  - $\alpha_\ell = (a_\ell + b_\ell \cdot i + c_\ell \cdot j + d_\ell \cdot k)/r_\ell$
  - $M = \frac{1}{r}\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{pmatrix}$ $\quad r = \mathrm{lcm}(r_1, \ldots, r_4)$

Quaternion Algebras in SQIsign

PQSnC
Post-Quantum Security and Cryptography

- Representing ideals = Representing $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \rightarrow$ **4x4 integer matrix** (after clearing denominators)
  - $\alpha_\ell = (a_\ell + b_\ell \cdot i + c_\ell \cdot j + d_\ell \cdot k)/r_\ell$
  - $M = \frac{1}{r}\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{pmatrix}$ $\quad r = \mathrm{lcm}(r_1, \ldots, r_4)$

- Computing ideal multiplication = Computing **the basis** of ideal multiplication
  - $I_1 I_2 = \{\alpha\beta : \alpha \in I_1, \beta \in I_2\} = \langle \alpha_s \beta_t \rangle_{1 \le s,t \le 4}$ $\quad$ where $I_1 = \langle \alpha_1, \cdots, \alpha_4 \rangle,\ I_2 = \langle \beta_1, \cdots, \beta_4 \rangle$
  - HNF algorithm: Computes a basis of a lattice with given generate set
  - HNF algorithm for a lattice I can be performed by integer arithmetics over $\mathbb{Z}_m$ where $m = \det(I)$

Idea on Contribution 1: First theoretical bound on SQIsign

- ∄ **bound on** $\mathbb{Q}$: field of rational numbers is an infinite set
- ∃ **bound on SQIsign** : algorithm is a finite sequence of statements

- How can we compute the existing bound?

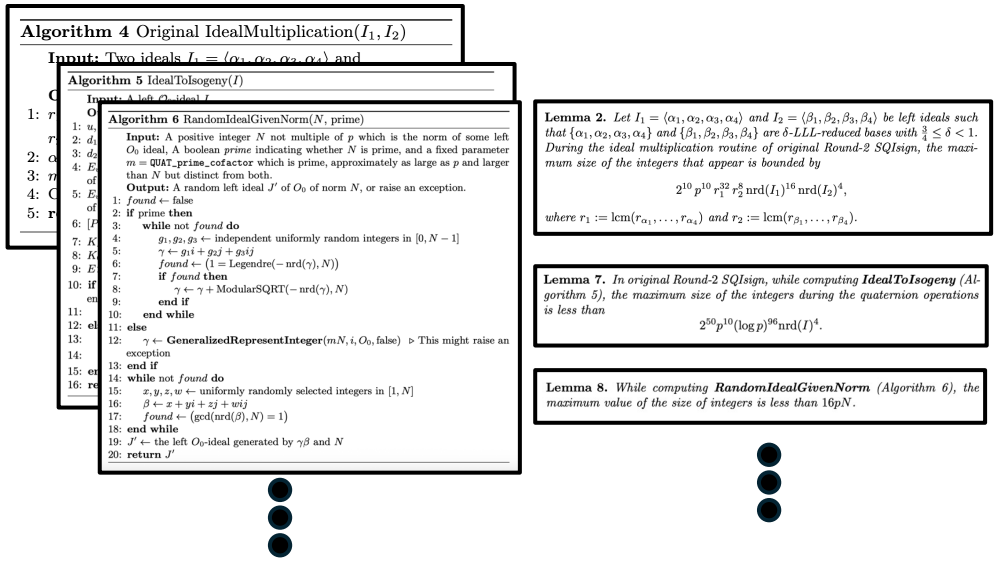
Idea on Contribution 1: First theoretical bound on SQIsign

PQSnC
Post-Quantum Security and Cryptography

- ∄ **bound on** $\mathbb{Q}$: field of rational numbers is an infinite set
- ∃ **bound on SQIsign** : algorithm is a finite sequence of statements

- How can we compute the existing bound?
  - Analyze each subroutine algorithm
  - Recursively apply them to get a bound on

    KeyGen and Sign of SQIsign



Algorithm 4 Original IdealMultiplication(I_1, I_2)

Input: Two ideals $I_1 = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ and

Algorithm 5 IdealToIsogeny(I)

Input: A left $\mathcal{O}_0$-ideal I

Algorithm 6 RandomIdealGivenNorm(N, prime)

Input: A positive integer N not multiple of p which is the norm of some left $\mathcal{O}_0$ ideal, A boolean *prime* indicating whether N is prime, and a fixed parameter $m =$ `QUAT_prime_cofactor` which is prime, approximately as large as p and larger than N but distinct from both.
Output: A random left ideal J' of $\mathcal{O}_0$ of norm N, or raise an exception.

1: *found* ← false
2: **if** prime **then**
3: **while** not *found* **do**
4: $g_1, g_2, g_3 \leftarrow$ independent uniformly random integers in $[0, N-1]$
5: $\gamma \leftarrow g_1 i + g_2 j + g_3 ij$
6: *found* ← $(1 = \text{Legendre}(-\text{nrd}(\gamma), N))$
7: **if** *found* **then**
8: $\gamma \leftarrow \gamma + \text{ModularSQRT}(-\text{nrd}(\gamma), N)$
9: **end if**
10: **end while**
11: **else**
12: $\gamma \leftarrow$ **GeneralizedRepresentInteger**$(mN, i, O_0, \text{false})$ ▷ This might raise an exception
13: **end if**
14: **while** not *found* **do**
15: $x, y, z, w \leftarrow$ uniformly randomly selected integers in $[1, N]$
16: $\beta \leftarrow x + yi + zj + wij$
17: *found* ← $(\gcd(\text{nrd}(\beta), N) = 1)$
18: **end while**
19: $J' \leftarrow$ the left O_0-ideal generated by $\gamma\beta$ and N
20: **return** J'

Lemma 2. *Let $I_1 = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ and $I_2 = \langle \beta_1, \beta_2, \beta_3, \beta_4 \rangle$ be left ideals such that $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ are δ-LLL-reduced bases with $\frac{3}{4} \leq \delta < 1$. During the ideal multiplication routine of original Round-2 SQIsign, the maximum size of the integers that appear is bounded by*

$$2^{10}\, p^{10}\, r_1^{32}\, r_2^{8}\, \text{nrd}(I_1)^{16}\, \text{nrd}(I_2)^{4},$$

where $r_1 := \text{lcm}(r_{\alpha_1}, \ldots, r_{\alpha_4})$ and $r_2 := \text{lcm}(r_{\beta_1}, \ldots, r_{\beta_4})$.

Lemma 7. *In original Round-2 SQIsign, while computing **IdealToIsogeny** (Algorithm 5), the maximum size of the integers during the quaternion operations is less than*

$$2^{50} p^{10} (\log p)^{96} \text{nrd}(I)^4.$$

Lemma 8. *While computing **RandomIdealGivenNorm** (Algorithm 6), the maximum value of the size of integers is less than $16pN$.*

Idea on Contribution 2: reducing the precision budgets

PQSnC
Post-Quantum Security and Cryptography

- By our analysis, the **main bottleneck is ideal multiplication**
- Original ideal multiplication algorithm uses **too large intermediate value:**

Algorithm 4 Original IdealMultiplication(I_1, I_2)

Input: Two ideals $I_1 = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ and $I_2 = \langle \beta_1, \beta_2, \beta_3, \beta_4 \rangle$ such that $O_R(I_1) = O_L(I_2)$.
Output: An ideal $I_1 I_2 = \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4 \rangle$.

1: $r_1 \leftarrow \mathrm{lcm}(r_{\alpha_1}, r_{\alpha_2}, r_{\alpha_3}, r_{\alpha_4})$,
$r_2 \leftarrow \mathrm{lcm}(r_{\beta_1}, r_{\beta_2}, r_{\beta_3}, r_{\beta_4})$
2: $\alpha_i \leftarrow r_1 \alpha_i, \quad \beta_j \leftarrow r_2 \beta_j \quad (1 \le i, j \le 4)$
3: $m \leftarrow \left|\det\left(\alpha_1\beta_1 \ \alpha_1\beta_2 \ \alpha_1\beta_3 \ \alpha_1\beta_4\right)\right|$
4: Compute $M \leftarrow \mathbf{HNF}((\alpha_i \beta_j)_{1 \le i,j \le 4})$ over $\mathbb{Z}_m$.
5: **return** $\frac{1}{r_1 r_2} M$

Idea on Contribution 2: reducing the precision budgets

PQSnC
Post-Quantum Security and Cryptography

- By our analysis, the **main bottleneck is ideal multiplication**
- Original ideal multiplication algorithm uses **too large intermediate value:**

Algorithm 4 Original IdealMultiplication(I_1, I_2)

Input: Two ideals $I_1 = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ and $I_2 = \langle \beta_1, \beta_2, \beta_3, \beta_4 \rangle$ such that $O_R(I_1) = O_L(I_2)$.
Output: An ideal $I_1 I_2 = \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4 \rangle$.

1: $r_1 \leftarrow \mathrm{lcm}(r_{\alpha_1}, r_{\alpha_2}, r_{\alpha_3}, r_{\alpha_4})$, $r_2 \leftarrow \mathrm{lcm}(r_{\beta_1}, r_{\beta_2}, r_{\beta_3}, r_{\beta_4})$
2: $\alpha_i \leftarrow r_1 \alpha_i, \quad \beta_j \leftarrow r_2 \beta_j \quad (1 \le i, j \le 4)$
3: $m \leftarrow \left|\det\left(\alpha_1\beta_1 \ \alpha_1\beta_2 \ \alpha_1\beta_3 \ \alpha_1\beta_4\right)\right|$
4: Compute $M \leftarrow \mathbf{HNF}((\alpha_i \beta_j)_{1 \le i,j \le 4})$ over $\mathbb{Z}_m$.
5: **return** $\frac{1}{r_1 r_2} M$

Algorithm 5 Modified IdealMultiplication(I_1, I_2)

Input: Two ideals $I_1 = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ and $I_2 = \langle \beta_1, \beta_2, \beta_3, \beta_4 \rangle$ such that $O_R(I_1) = O_L(I_2)$.
Output: An ideal $I_1 I_2 = \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4 \rangle$.

1: $r_1 \leftarrow \mathrm{lcm}(r_{\alpha_1}, r_{\alpha_2}, r_{\alpha_3}, r_{\alpha_4})$, $r_2 \leftarrow \mathrm{lcm}(r_{\beta_1}, r_{\beta_2}, r_{\beta_3}, r_{\beta_4})$
2: $\alpha_i \leftarrow r_1 \alpha_i, \quad \beta_j \leftarrow r_2 \beta_j \quad (1 \le i, j \le 4)$
3: $m \leftarrow \mathrm{nrd}(r_1 I_1)^2 \, \mathrm{nrd}(r_2 I_2)^2$
4: Compute $M \leftarrow \mathbf{HNF}((\alpha_i \beta_j)_{1 \le i,j \le 4})$ over $\mathbb{Z}_m$.
5: **return** $\frac{1}{r_1 r_2} M$

$$\det(\boldsymbol{\alpha_1\beta_1}, \ldots, \boldsymbol{\alpha_1\beta_4}) \gg \mathrm{nrd}(\boldsymbol{r_1 I_1})^2 \mathrm{nrd}(\boldsymbol{r_2 I_2})^2$$

Conclusion

PQSnC
Post-Quantum
Security and
Cryptography

Summary

- We derive the theoretical size bound on SQIsign
- We modify the subroutine of SQIsign, reducing the necessary precision budget.
- We implement the first fixed-precision implementation of SQIsign

Conclusion

PQSnC
Post-Quantum
Security and
Cryptography

❑ Summary

- We derive the theoretical size bound on SQIsign
- We modify the subroutine of SQIsign, reducing the necessary precision budget.
- We implement the first fixed-precision implementation of SQIsign

❑ Following works

- Constant-time implementation of quaternion algorithms for SQIsign
- Implementation of SQIsign KeyGen and Sign in memory-constrained devices
- Reducing precision budgets reasonably

Thank you for listening

PQSnC Lab

Won Kim

Paper