On Rejection Sampling in Lyubashevsky's Signature Scheme

Julien Devevey[1] Omar Fawzi[1,2] Alain Passelègue[1,2] Damien Stehlé[1]

ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, Inria, UCBL), France

INRIA, Laboratoire LIP, France

Our Results

1. Lower bounds on the compactness of Lyubashevsky's signatures
2. Proposal of distributions reaching them
3. Optimality of rejection sampling runtime
4. Similar results for the BLISS `(Ducas et al.; Crypto'13)` variant
5. Proposal of a variant with bounded runtime

Rejection Sampling for Lyubashevsky's Signatures

- Widely studied and folklore technique from probabilities,
- Used for signatures in `(Lyubashevsky; AC'09)`,
- Widely used since then, but almost as a black-box and only with Gaussians/Hypercubes-Uniforms,
- Implemented in a NIST PQC finalist (Dilithium).

Is the way we use rejection sampling "optimal" (in some sense)?
Could we use other distributions?
Which ones are the best suited for the task?

Lyubashevsky’s Signature Scheme

Intuition

sk	vk
$\mathbf{A}$, $\mathbf{S}$ where **S** is "small."	$\mathbf{A}$, $\mathbf{T} = \mathbf{A}\mathbf{S}$

A signature σ for a message μ is comprised of

c	z
$\mathbf{c} = \mathbf{H}\left(\mathbf{A}\mathbf{y}, \mu\right)$	$\mathbf{y} + \mathbf{S}\mathbf{c}$

Intuition

sk	vk
${}_{n}\underset{m}{\mathbf{A}}, \; {}_{m}\underset{k}{\mathbf{S}}$ where **S** is "small."	$\mathbf{A}, \; {}_{n}\underset{k}{\mathbf{T}} = \mathbf{A}\mathbf{S}$

A signature σ for a message μ is comprised of

$\mathbf{c}$	$\mathbf{z}$
${}_{k}\mathbf{c} = \mathbf{H}\left(\mathbf{A}\mathbf{y}, \mu\right)$	$\mathbf{y} + \mathbf{S}\mathbf{c}$

Intuition (2)

To verify, check that $\|\mathbf{z}\| \leq \gamma$ and that

$$\mathbf{c} = H\left(\mathbf{A} \mathbf{z} - \mathbf{T} \mathbf{c}, \mu \right)$$

The security relies on the hardness of

$\mathsf{SIS}_{n,m,\beta}$

Given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find nonzero $\mathbf{s} \in \mathbb{Z}_q^{m}$ s.t. $\|\mathbf{s}\| \leq \beta$ and

$$\mathbf{A} \mathbf{s} = \mathbf{0}$$

Intuition (2)

To verify, check that $\|\mathbf{z}\| \leq \gamma$ and that

$$\mathbf{c} = \mathbf{H}\left(\mathbf{A}\,\mathbf{z} - \mathbf{T}\,\mathbf{c}, \mu \right)$$

The security relies on the hardness of

$\mathrm{SIS}_{n,m,\beta}$

Given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find nonzero $\mathbf{s} \in \mathbb{Z}_q^m$ s.t. $\|\mathbf{s}\| \leq \beta$ and

$$\mathbf{A}\,\mathbf{s} = \mathbf{0}$$

Signature Scheme (Lyubashevsky; AC'09),(Lyubashevsky; EC'11),...

Sign$(\mu, \mathbf{A}, \mathbf{S})$:

1: $\mathbf{y} \hookleftarrow Q$
2: $\mathbf{c} \leftarrow H(\mathbf{Ay}, \mu)$
3: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc}$
4: With probability $\min\left(\frac{P(\mathbf{z})}{M \cdot Q(\mathbf{y})}, 1\right)$, return $(\mathbf{z}, \mathbf{c})$
5: **else** go to Step 1

- P and Q are either Gaussian or Hypercubes-Uniforms,
- Most of the correctness, runtime and security proofs are *flawed*.

Sign$(\mu, \mathbf{A}, \mathbf{S})$:

1: $\mathbf{y} \hookleftarrow Q$
2: $\mathbf{c} \leftarrow H(\mathbf{Ay}, \mu)$
3: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc}$
4: With probability $\min\left(\frac{P(\mathbf{z})}{M \cdot Q(\mathbf{y})}, 1\right)$, return $(\mathbf{z}, \mathbf{c})$
5: **else** go to Step 1

- P and Q are either Gaussian or Hypercubes-Uniforms,
- Most of the correctness, runtime and security proofs are *flawed*.

Rejection Sampling

Rényi Divergence

Let P, Q be two probability distributions.

Definition

$$R_\infty(P\|Q) = \sup_{x \in \mathrm{Supp}(P)} \frac{P(x)}{Q(x)}.$$

Our generalization for any $\varepsilon > 0$:

ε-smooth Rényi divergence

$$R_\infty^\varepsilon(P\|Q) = \inf_{\substack{S \\ P(S) \geq 1-\varepsilon}} \sup_{x \in S} \frac{P(x)}{Q(x)}.$$

Example: $R_\infty(D^m_{\sigma,\mathbf{c}} \| D^m_\sigma) = +\infty$ whereas $R^\varepsilon_\infty(D^m_{\sigma,\mathbf{c}} \| D^m_\sigma) < +\infty$.

Setting

- P, Q two probability distributions,
- $X_1, \ldots, X_i, \ldots,$ i.i.d. random variables following Q.

Rejection Sampling Strategy

A family $(A_i : \mathrm{Supp}(Q)^i \to [i] \cup \{\perp\})_{i \geq 1}$ of randomized algorithms such that $X_J \hookleftarrow P$, where

- $i^* = \min\{i | A_i(X_1, \ldots, X_i) \neq \perp\}$,
- $J = A_{i^*}(X_1, \ldots, X_{i^*})$.

Example

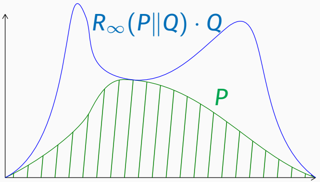


Figure 1: Acceptance zone and sampling domain

Usual Rejection Sampling

$$A_i : (X_1, \ldots, X_i) \mapsto \begin{cases} X_i & \text{w.p. } \frac{P(X_i)}{R_\infty(P\|Q)\cdot Q(X_i)}, \\ 0 & \text{otherwise.} \end{cases}$$

In this case $\mathbb{E}(i^*) = R_\infty(P\|Q)$.

Optimality

Rejection Sampling Strategy

A family $(A_i : \mathrm{Supp}(Q)^i \to [i] \cup \{\perp\})_{i \geq 1}$ of randomized algorithms such that $X_J \hookleftarrow P$, where

- $i^* = \min\{i | A_i(X_1, \ldots, X_i) \neq \perp\}$,
- $J = A_{i^*}(X_1, \ldots, X_{i^*})$.

Contribution: Optimality of the usual strategy

Given any strategy $(A_i)_{i \geq 1}$,

$$\mathbb{E}(i^*) \geq R_\infty(P \| Q).$$

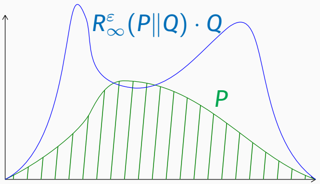


Figure 2: Acceptance zone and sampling domain

Imperfect Rejection Sampling

$$A_i : (X_1, \ldots, X_i) \mapsto \begin{cases} X_i & \text{w.p. } \min\left(\frac{P(X_i)}{R_\infty^\varepsilon(P\|Q)\cdot Q(X_i)}, 1\right), \\ 0 & \text{otherwise.} \end{cases}$$

Resulting distribution: P_{X_j} such that $R_\infty(P_{X_j}\|P) \le \frac{1}{1-\varepsilon}$.

Back to the Signature Scheme

Modified Scheme

Sign$(\mu, \mathbf{A}, \mathbf{S})$:

1: $\mathbf{y} \hookleftarrow Q$
2: $\mathbf{c} \leftarrow H(\mathbf{A}\lceil \mathbf{y} \rfloor, \mu)$
3: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc}$
4: With probability $\min\left(\frac{P(\mathbf{z})}{M \cdot Q(\mathbf{y})}, 1\right)$
return $(\lceil \mathbf{z} \rfloor, \mathbf{c})$
5: **else** go to Step 1

Figure 3: Modified Signature Algorithm.

- P, Q two (possibly continuous) distributions,
- $\forall \mathbf{S}, \mathbf{c} : R_\infty^\varepsilon(P \| Q_{\mathbf{Sc}}) \leq M$,
- $\Pr_{\mathbf{z} \hookleftarrow P}(\|\lceil \mathbf{z} \rfloor\| \geq \gamma) \leq \mathrm{negl}(\lambda)$.

Modified Scheme

Sign$(\mu, \mathbf{A}, \mathbf{S})$:

1: $\mathbf{y} \hookleftarrow Q$
2: $\mathbf{c} \leftarrow H(\mathbf{A}\lceil \mathbf{y} \rfloor, \mu)$
3: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{Sc}$
4: With probability $\min\left(\frac{P(\mathbf{z})}{M \cdot Q(\mathbf{y})}, 1\right)$ return $(\lceil \mathbf{z} \rfloor, \mathbf{c})$
5: **else** go to Step 1

Figure 3: Modified Signature Algorithm.

- P, Q two (possibly continuous) distributions,
- $\forall \mathbf{S}, \mathbf{c} : R_\infty^\varepsilon(P \| Q_{\mathbf{Sc}}) \leq M$,
- $\Pr_{\mathbf{z} \hookleftarrow P}(\| \lceil \mathbf{z} \rfloor \| \geq \gamma) \leq \mathrm{negl}(\lambda)$.

Properties

Contribution: Fix the proofs

In the Random Oracle Model, for $\varepsilon = 1/Q_s$ and $t = \max_{\mathbf{s},\mathbf{c}} \|\mathbf{Sc}\|$, the scheme is

- *correct*,
- *sEU-CMA secure* under the $\mathrm{SIS}_{n,m,2(\gamma+t)}$ assumption,
- and the number of iterations i^* of a call to Sign is such that

$$\Pr(i^* \geq i) \leq \left(1 - \frac{1-\varepsilon}{M}\right)^i + \mathrm{negl}(\lambda).$$

Our Goal

Minimize γ

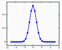
$\Downarrow$

Reduction from harder SIS

$\Downarrow$

Smaller parameters overall for the same level of security

Current choices of Distributions

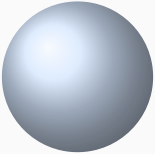
P, Q	Sampling	Rejection	$O(\gamma)_{(\varepsilon=0)}$	$O(\gamma)_{(\varepsilon=\frac{1}{Q_S})}$
U()	Easy	Deterministic	$\frac{t\sqrt{m}m}{\log M}$	Same
	Cumbersome	Probabilistic	∞	$\frac{t\sqrt{m}\sqrt{\log\frac{1}{\varepsilon}}}{\sqrt{\log M}}$

(where $t = \max_{\mathbf{s},\mathbf{c}}\|\mathbf{Sc}\|$)

The first distribution is used in the Dilithium signature scheme.

Our proposal

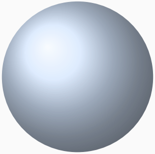
Use the uniform continuous distribution over

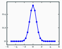


P, Q	Sampling	Rejection	$O(\gamma)_{(\varepsilon=0)}$	$O(\gamma)_{(\varepsilon=\frac{1}{Q_s})}$
$U($$)$	Easy	Deterministic	$\frac{t\sqrt{mm}}{\log M}$	Same
	Cumbersome	Probabilistic	∞	$\frac{t\sqrt{m}\sqrt{\log\frac{1}{\varepsilon}}}{\sqrt{\log M}}$
$U($$)$	Cumbersome	Deterministic	$\frac{tm}{\log M}$	$\frac{t\sqrt{m}\sqrt{\log\frac{1}{\varepsilon}}}{\log M}$

Our proposal

Use the uniform continuous distribution over



P, Q	Sampling	Rejection	$O(\gamma)_{(\varepsilon=0)}$	$O(\gamma)_{(\varepsilon=\frac{1}{Q_S})}$
$U($$)$	Easy	Deterministic	$\frac{t\sqrt{m}m}{\log M}$	Same
	Cumbersome	Probabilistic	∞	$\frac{t\sqrt{m}\sqrt{\log\frac{1}{\varepsilon}}}{\sqrt{\log M}}$
$U($$)$	Cumbersome	Deterministic	$\frac{tm}{\log M}$	$\frac{t\sqrt{m}\sqrt{\log\frac{1}{\varepsilon}}}{\log M}$

Optimality

Contribution: Lower bounds on compactness

When $\varepsilon = 0$, for fixed $M > 1$ and any choice of P and Q such that $\max_{\mathbf{s},\mathbf{c}} R_\infty(P \| Q_{\mathbf{sc}}) \leq M$:

$$\gamma \geq \frac{t(m-1)}{\log M}.$$

Conclusion and Open Questions

Open questions:

1. Concrete instantiation?
2. Efficient sampling from the continuous ball?
3. Totally removing rejection while keeping compactness?
4. Automatisation of rejection-based signature design?

Thank you for your attention!