On Rejection Sampling in Lyubashevsky's Signature Scheme

Julien Devevey Omar Fawzi Alain Passelègue Damien Stehlé

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

Our Questions

1. Can we make rejection sampling faster?
2. How compact can Lyubashevsky's signatures get?
3. How to reach this compactness?
4. Bonus:
    4.1 Are the proofs in the litterature flawed?
    4.2 Similar questions for the BLISS `(Ducas et al.; Crypto'13)` variant
5. Can we do rejection sampling with bounded runtime?

Motivations

- Already implemented in practice.
- NIST PQC standardisation project finalist:
- Rejection sampling has been widely used since its introduction in cryptography (Lyubashevsky; AC'09)...
- ... but mostly in a black-box manner, and only with very few distributions.

Table of contents

Definitions

Definitions

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

Results on Rejection Sampling

Minimizing Signature Size

Digital Signature

- KeyGen
  - **Input**: Security parameter 1^λ
  - **Output**: Signing key sk and verification key vk

- Sign
  - **Input**: sk and message μ
  - **Output**: Signature σ

- Verify
  - **Input**: vk and μ and σ
  - **Output**: True or False

Properties of Digital Signatures

- Correctness: Verify(vk , μ , Sign(sk , μ)) returns False with negligible probability.

- Unforgeability: Without sk , it is hard to produce an unseen valid pair (μ^* , σ^*) even with a signing oracle.

Security Assumption

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

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

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

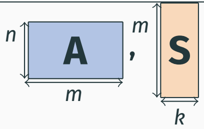
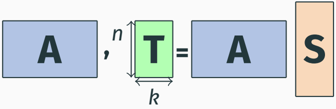
- Post-quantum assumption based on Euclidean Lattices.
- Gets harder when β is smaller.

Lyubashevsky's Signature Scheme

(Lyubashevsky; AC'09),

(Lyubashevsky; EC'11)...

KeyGen

sk	vk
	
where **S** is “small.”	

Sign

On input sk, μ, sample a small

$$\mathbf{y} \hookleftarrow Q.$$

A signature σ for a message μ is of the form

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

Verify

vk	**c**	**z**
$\mathbf{A}$, $\mathbf{T} = \mathbf{A}\mathbf{S}$	$H(\mathbf{A}\mathbf{y}, \mu)$	$\mathbf{y} + \mathbf{S}\mathbf{c}$

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

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

Properties

Correctness

$\forall \mathbf{S}, \mathbf{c} : \Pr_{\mathbf{y} \hookleftarrow Q}(\|\mathbf{y} + \mathbf{S}\mathbf{c}\| > \gamma) \leq \mathrm{negl}(\lambda) \implies$ the scheme is correct.

- Instantiated with Q either Gaussian or Hypercube-Uniform,
- This version is not secure:
  the distribution of $\mathbf{z}$ heavily depends on $\mathbf{S}$.

Making the Scheme secure

Ideal signature:

$\mathsf{Sign}_2(\mu, \mathbf{A}, \mathbf{S})$:

1: $\mathbf{z} \hookleftarrow P$
2: $\mathbf{c} \leftarrow U(\mathcal{C})$
3: set $H(\mathbf{Az} - \mathbf{Tc}, \mu) = \mathbf{c}$
4: return $(\mathbf{z}, \mathbf{c})$

Intuition

- If Q Gaussian, take $P = Q$ with standard deviation such that the shift $\mathbf{Sc}$ is not noticeable.
- If $Q = U([-\gamma_1, \gamma_1]^m)$, reject the signature if $\mathbf{z} \notin [\gamma_2, \gamma_2]^m$.
  - Value of γ_1, γ_2?
  - Generalise for Gaussians and other distributions?

Making the Scheme secure

Ideal signature:

$\text{Sign}_2(\mu, \mathbf{A}, \mathbf{S})$:

1: $\mathbf{z} \hookleftarrow P$
2: $\mathbf{c} \leftarrow U(\mathcal{C})$
3: set $H(\mathbf{Az} - \mathbf{Tc}, \mu) = \mathbf{c}$
4: return $(\mathbf{z}, \mathbf{c})$

Two solutions:

1. Flooding
   - Set the standard deviation of Q really large
   - Consequence: γ is really large
   - Used by (Damgård et al.; CRYPTO12), (Agrawal et al.; ICALP22)
2. Rejection Sampling (Lyubashevsky; AC'09)

Making the Scheme secure

Ideal signature:

$\text{Sign}_2(\mu, \mathbf{A}, \mathbf{S})$:

$\mathbf{z} \hookleftarrow P$
$\mathbf{c} \leftarrow U(\mathcal{C})$
set $H(\mathbf{Az} - \mathbf{Tc}, \mu) = \mathbf{c}$
return $(\mathbf{z}, \mathbf{c})$

Two solutions:

1. Flooding
   - Set the standard deviation of Q really large
   - Consequence: γ is really large
   - Used by (Damgård et al.; CRYPTO12), (Agrawal et al.; ICALP22)

2. Rejection Sampling (Lyubashevsky; AC'09)

Results on Rejection Sampling

Rejection Sampling for Lyubashevsky's Signatures

- Widely studied and folklore technique from probabilities
- Turns the distribution of $(\mathbf{z}, \mathbf{c})$ into $P \otimes U(\mathcal{C})$
- First used for signatures in `(Lyubashevsky; AC'09)`

Is the way we use rejection sampling "optimal" (in some sense)?
What distributions can we use?

Context

- Given access to many samples distributed following $\tilde{D}$...
- ... How to find a sample distributed following D?
- ⚠ Without modifying the samples!

Setting

- $D, \tilde{D}$ two probability distributions,
- $X_1, \ldots, X_i, \ldots,$ i.i.d. random variables following $\tilde{D}$.

Rejection Sampling Strategy

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

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

Goal: minimize $\mathbb{E}(i^*)$.

Standard Rejection Sampling

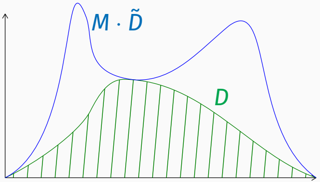


Figure 1: Acceptance zone and sampling domain

Standard Rejection Sampling

$$A_i : (X_1, \ldots, X_i) \mapsto \begin{cases} i & \text{w.p. } \frac{D(X_i)}{M \cdot \tilde{D}(X_i)}, \\ \perp & \text{otherwise.} \end{cases}$$

Works if $D(x) \leq M \cdot \tilde{D}(x)$ for all x. In this case $\mathbb{E}(i^*) = M$.

Imperfect Rejection Sampling (Lyubashevsky; EC'11)

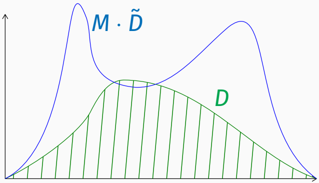


Figure 2: Acceptance zone and sampling domain

$$A_i : (X_1, \ldots, X_i) \mapsto \begin{cases} i & \text{w.p. } \min\left(\frac{D(X_i)}{M \cdot \tilde{D}(X_i)}, 1\right), \\ \perp & \text{otherwise.} \end{cases}$$

Closeness of Imperfect Rejection Sampling

If $\Pr_{x \hookleftarrow D}(D(x) \leq M \cdot \tilde{D}(x)) \geq 1 - \varepsilon$ then the resulting distribution P_{X_J} is such that $\Delta(P_{X_J}, D) \leq \varepsilon$.

Imperfect Rejection Sampling (Lyubashevsky; EC'11)

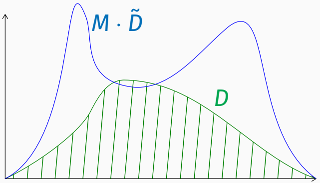


Figure 2: Acceptance zone and sampling domain

$$A_i : (X_1, \ldots, X_i) \mapsto \begin{cases} i & \text{w.p. } \min\left(\frac{D(X_i)}{M \cdot \tilde{D}(X_i)}, 1\right), \\ \perp & \text{otherwise.} \end{cases}$$

Closeness of Imperfect Rejection Sampling

If $\Pr_{x \hookleftarrow D}(D(x) \leq M \cdot \tilde{D}(x)) \geq 1 - \varepsilon$ then the resulting distribution P_{X_J} is such that $\Delta(P_{X_J}, D) \leq \varepsilon$.

Let $D, \tilde{D}$ be two probability distributions.

Definition

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

Our generalization for any $\varepsilon > 0$:

ε-smooth Rényi divergence

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

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

Rényi Divergence

Let $D, \tilde{D}$ be two probability distributions.

Definition

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

Our generalization for any $\varepsilon > 0$:

ε-smooth Rényi divergence

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

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

Optimality of perfect Rejection Sampling

Rejection Sampling Strategy

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

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

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

Reached for $M = R_\infty(D \| \tilde{D})$.

Imperfect RS in terms of Divergence

Contribution: computing the Divergence

$$R_\infty(P_{X_J} \| D) \leq \frac{1}{1-\varepsilon}.$$

Comparisons

- $P_{X_J}(E) \leq D(E) + \varepsilon$ with SD.
- $P_{X_J}(E) \leq \frac{D(E)}{1-\varepsilon} \approx (1+\varepsilon) \cdot D(E)$ with RD.

If Q_s signatures are produced,

$$\varepsilon = \begin{cases} O(2^{-\lambda}) & \text{with SD,} \\ O(1/Q_s) & \text{with RD.} \end{cases}$$

Imperfect RS in terms of Divergence

Contribution: computing the Divergence

$$R_\infty(P_{X_J} \| D) \leq \frac{1}{1-\varepsilon}.$$

Comparisons

- $P_{X_J}(E) \leq D(E) + \varepsilon$ with SD.
- $P_{X_J}(E) \leq \frac{D(E)}{1-\varepsilon} \approx (1+\varepsilon) \cdot D(E)$ with RD.

If Q_s signatures are produced,

$$\varepsilon = \begin{cases} O(2^{-\lambda}) & \text{with SD,} \\ O(1/Q_s) & \text{with RD.} \end{cases}$$

Minimizing Signature Size

Definitions

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

Results on Rejection Sampling

Minimizing Signature Size

Instantiating Rejection Sampling

Take any discrete P and Q and set

- $\tilde{D}$ distribution of $(\mathbf{z}, \mathbf{c})$ where $\mathbf{y} \hookleftarrow Q$, $\mathbf{c} \hookleftarrow U(\mathcal{C})$ and $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$,
- $D = P \otimes U(\mathcal{C})$,
- $\frac{D(\mathbf{z},\mathbf{c})}{\tilde{D}(\mathbf{z},\mathbf{c})} = \frac{P(\mathbf{z})}{Q(\mathbf{y})}$.

Set $M \geq R_{\infty}^{\varepsilon}(D \| \tilde{D})$ for some $\varepsilon \geq 0$.

Instantiating Rejection Sampling

Take any discrete P and Q and set

- $\tilde{D}$ distribution of $(\mathbf{z}, \mathbf{c})$ where $\mathbf{y} \hookleftarrow Q$, $\mathbf{c} \hookleftarrow U(\mathcal{C})$ and $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$,
- $D = P \otimes U(\mathcal{C})$,
- $\frac{D(\mathbf{z},\mathbf{c})}{\tilde{D}(\mathbf{z},\mathbf{c})} = \frac{P(\mathbf{z})}{Q(\mathbf{y})}$.

Set $M \geq R_\infty^\varepsilon(D \| \tilde{D})$ for some $\varepsilon \geq 0$.

Instantiating Rejection Sampling

Take any discrete P and Q and set

- $\tilde{D}$ distribution of $(\mathbf{z}, \mathbf{c})$ where $\mathbf{y} \hookleftarrow Q, \mathbf{c} \hookleftarrow U(\mathcal{C})$ and $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$,
- $D = P \otimes U(\mathcal{C})$,
- $\frac{D(\mathbf{z},\mathbf{c})}{\tilde{D}(\mathbf{z},\mathbf{c})} = \frac{P(\mathbf{z})}{Q(\mathbf{y})}$.

Set $M \geq R_\infty^\varepsilon(D \| \tilde{D})$ for some $\varepsilon \geq 0$.

Generic Signature

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

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

$\approx \text{Sign}_1(\mu, \mathbf{A}, \mathbf{S})$:

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

Can be adapted to work with continuous P and Q.

Generic Signature

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

1: $\mathbf{y} \hookleftarrow Q$
2: $\mathbf{c} \leftarrow H(\mathbf{A}\mathbf{y}, \mu)$
3: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$
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

$\approx \mathsf{Sign}_1(\mu, \mathbf{A}, \mathbf{S})$:

1: $\mathbf{y} \hookleftarrow Q$
2: $\mathbf{c} \leftarrow U(\mathcal{C})$
3: $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{S}\mathbf{c}$
4: set $H(\mathbf{A}\mathbf{y}, \mu) = \mathbf{c}$
5: With probability $\min\left(\frac{P(\mathbf{z})}{M \cdot Q(\mathbf{y})}, 1\right)$ return $(\mathbf{z}, \mathbf{c})$
6: **else** go to Step 1

Can be adapted to work with continuous P and Q.

Generic Signature

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

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

$\approx \mathsf{Sign}_1(\mu, \mathbf{A}, \mathbf{S})$:

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

Can be adapted to work with continuous P and Q.

Contribution: Understanding how to set the Parameters

Probability Preservation Property

If $\mathcal{A}$ makes Q_s signature queries:

$$\Pr(\mathcal{A}^{\mathsf{Sign}_1} \text{ forges}) \leq \frac{\Pr(\mathcal{A}^{\mathsf{Sign}_2} \text{ forges})}{(1-\varepsilon)^{Q_s}}.$$

Set $\varepsilon = O(1/Q_s)$ (as opposed to $\varepsilon = 2^{-\Omega(\lambda)}$ before).

Multiplicativity

$$R_\infty^\varepsilon(D \| \tilde{D}) \leq \max_{\mathbf{S},\mathbf{c}} R_\infty^\varepsilon(P \| Q_{\mathbf{Sc}}).$$

Set $M \geq \max_{\mathbf{S},\mathbf{c}} R_\infty^\varepsilon(P \| Q_{\mathbf{Sc}})$.

Contribution: Understanding how to set the Parameters

Probability Preservation Property

If $\mathcal{A}$ makes Q_s signature queries:

$$\Pr(\mathcal{A}^{\mathsf{Sign}_1} \text{ forges}) \leq \frac{\Pr(\mathcal{A}^{\mathsf{Sign}_2} \text{ forges})}{(1-\varepsilon)^{Q_s}}.$$

Set $\varepsilon = O(1/Q_s)$ (as opposed to $\varepsilon = 2^{-\Omega(\lambda)}$ before).

Multiplicativity

$$R_\infty^\varepsilon(D \| \tilde{D}) \leq \max_{\mathbf{s},\mathbf{c}} R_\infty^\varepsilon(P \| Q_{\mathbf{sc}}).$$

Set $M \geq \max_{\mathbf{s},\mathbf{c}} R_\infty^\varepsilon(P \| Q_{\mathbf{sc}})$.

Our Goal

Let $\varepsilon \geq 0$ and $M > 1$, fixing the runtime.
Let $\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| > \gamma) = \mathrm{negl}(\lambda)$.
Goal: find P, Q such that $\max_{\mathbf{s},\mathbf{c}} R_\infty^\varepsilon(P \| Q_{\mathbf{sc}}) \leq M$ minimizing γ.

Minimize γ

$\Downarrow$

Cryptanalysis becomes more costly

$\Downarrow$

Smaller parameters overall for the same level of security

Our Goal

Let $\varepsilon \geq 0$ and $M > 1$, fixing the runtime.
Let $\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| > \gamma) = \mathrm{negl}(\lambda)$.
Goal: find P, Q such that $\max_{\mathbf{s},\mathbf{c}} R_\infty^\varepsilon(P \| Q_{\mathbf{sc}}) \leq M$ minimizing γ.

Minimize γ

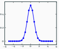
$\Downarrow$

Cryptanalysis becomes more costly

$\Downarrow$

Smaller parameters overall for the same level of security

Current choices of Distributions

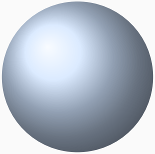
P, Q	Sampling	Rejection	$O(\gamma)_{(\varepsilon=0)}$	$O(\gamma)_{(\varepsilon=\frac{1}{Q_s})}$
$U($$)$	Easy	Deterministic	$\frac{t\sqrt{mm}}{\log M}$	Same
	Cumbersome	Probabilistic	∞	$\frac{t\sqrt{m\log\frac{1}{\varepsilon}}}{\sqrt{\log M}}$

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

The first distribution is used in the Dilithium signature scheme.

Our proposal

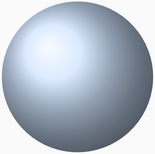
Use the uniform continuous distribution over

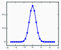


P, Q	Sampling	Rejection	$O(\gamma)_{(\varepsilon=0)}$	$O(\gamma)_{(\varepsilon=\frac{1}{Q_S})}$
$U($$)$	Easy	Deterministic	$\frac{t\sqrt{mm}}{\log M}$	Same
	Cumbersome	Probabilistic	∞	$\frac{t\sqrt{m\log\frac{1}{\varepsilon}}}{\sqrt{\log M}}$
$U($$)$	Cumbersome	Deterministic	$\frac{tm}{\log M}$	$\frac{t\sqrt{m\log\frac{1}{\varepsilon}}}{\log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

Our proposal

Use the uniform continuous distribution over



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

Intuition

Hyperballs versus hypercubes:

- $\{\mathbf{Sc}\} \approx \mathcal{B}_m(t) \cap \mathbb{Z}^m$ and γ is a bound on the Euclidean norm.
- Factor $\sqrt{m}$ gained because of $\|\cdot\| \leq \sqrt{m}\|\cdot\|_\infty$.

Cut and smooth divergence:

- Remove a hyperspherical cap opposed to $\mathbf{Sc}$.
- Volume allowed depends on ε.

Continuous versus discrete hyperballs:

- Easier to study.
- Easier to sample from.

Intuition

Hyperballs versus hypercubes:

- $\{\mathbf{Sc}\} \approx \mathcal{B}_m(t) \cap \mathbb{Z}^m$ and γ is a bound on the Euclidean norm.
- Factor $\sqrt{m}$ gained because of $\|\cdot\| \leq \sqrt{m}\|\cdot\|_\infty$.

Cut and smooth divergence:

- Remove a hyperspherical cap opposed to $\mathbf{Sc}$.
- Volume allowed depends on ε.

Continuous versus discrete hyperballs:

- Easier to study.
- Easier to sample from.

Intuition

Hyperballs versus hypercubes:

- $\{\mathbf{Sc}\} \approx \mathcal{B}_m(t) \cap \mathbb{Z}^m$ and γ is a bound on the Euclidean norm.
- Factor $\sqrt{m}$ gained because of $\|\cdot\| \leq \sqrt{m}\|\cdot\|_\infty$.

Cut and smooth divergence:

- Remove a hyperspherical cap opposed to $\mathbf{Sc}$.
- Volume allowed depends on ε.

Continuous versus discrete hyperballs:

- Easier to study.
- Easier to sample from.

Optimality

Contribution: Lower bounds on compactness

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

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

Intuition of the proof

1. Do the proof for continuous distributions then discretize the result.
2. Model $\{\mathbf{Sc}\}$ as $U(\mathcal{B}_m(t))$.
3. Isotropise P and Q.
4. Deduce a functional inequality on P from the constraint.
5. Solve it.

Bonus: Fixing the Proofs

Claims from the Litterature

Claims

In the standard model for $\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| \geq \gamma) \leq \mathrm{negl}(\lambda)$ and $t = \max_{\mathbf{S},\mathbf{c}} \|\mathbf{Sc}\|$, the scheme is

- *correct*,
- has expected *number of iterations* M,

thanks to the properties of rejections sampling.

Flaw

- ⚠ D and $\tilde{D}$ are chosen for Sign_1.
- H not a random oracle $\implies$ $\mathbf{z}$ is not distributed following P and expected number of iterations is not M.
- Correctness and runtime analysis relying on this in the litterature are flawed.
- There are examples for which the expected runtime is infinite.

Flaw

- ⚠ D and $\tilde{D}$ are chosen for Sign_1.
- H not a random oracle $\implies$ $\mathbf{z}$ is not distributed following P and expected number of iterations is not M.
- Correctness and runtime analysis relying on this in the litterature are flawed.
- There are examples for which the expected runtime is infinite.

Properties

Contribution: Fix the proofs

In the Random Oracle Model, for $\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| \geq \gamma) \leq \mathrm{negl}(\lambda)$ 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

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

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!

BLISS

Definitions

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

Results on Rejection Sampling

Minimizing Signature Size

BLISS Variant (Ducas et al.; Crypto'13)

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

1: $\mathbf{y} \hookleftarrow Q$
2: $\mathbf{c} \leftarrow H(\mathbf{A}\lceil \mathbf{y} \rfloor, \mu)$
3: $b \hookleftarrow U(\{0,1\})$
4: $\mathbf{z} \leftarrow \mathbf{y} + (-1)^b \mathbf{S}\mathbf{c}$
5: With probability $\min\left(\frac{P(\mathbf{z})}{M \cdot (Q(\mathbf{z}+\mathbf{S}\mathbf{c}) + Q(\mathbf{z}-\mathbf{S}\mathbf{c}))/2}, 1\right)$ return $(\lceil \mathbf{z} \rfloor, \mathbf{c})$
6: **else** go to Step 1

- KeyGen and Verify are adapted to keep correctness and security,

Contribution: Lower bounds

$$\gamma \geq \frac{t\sqrt{m-2}}{\log(M/2)}.$$

- Reached for Gaussians and continuous Hyperball-Uniforms.

BLISS Variant (Ducas et al.; Crypto'13)

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

1: $\mathbf{y} \hookleftarrow Q$
2: $\mathbf{c} \leftarrow H(\mathbf{A}\lceil \mathbf{y} \rfloor, \mu)$
3: $b \hookleftarrow U(\{0, 1\})$
4: $\mathbf{z} \leftarrow \mathbf{y} + (-1)^b \mathbf{Sc}$
5: With probability $\min\left(\frac{P(\mathbf{z})}{M \cdot (Q(\mathbf{z}+\mathbf{Sc}) + Q(\mathbf{z}-\mathbf{Sc}))/2}, 1\right)$ return $(\lceil \mathbf{z} \rfloor, \mathbf{c})$
6: **else** go to Step 1

- KeyGen and Verify are adapted to keep correctness and security,

Contribution: Lower bounds

$$\gamma \geq \frac{t\sqrt{m-2}}{\log(M/2)}.$$

- Reached for Gaussians and continuous Hyperball-Uniforms.