Lattice-based Signature Schemes in the Fiat-Shamir Paradigm

PhD Defense

Julien Devevey¹, under the supervision of Damien Stehlé

Sep. 18, 2023

¹. École Normale Supérieure de Lyon
Mrs & Mr D.
Signing the Lease
Signing the Lease

J. Devevey - Defense
Use Cases of Digital Signatures

- First use: every visited website is \( \geq 1 \) signature published and multiple verifications

- Second use: The one on the lease is legally binding in many countries

- Both use cases relies on long-term security

However...
Use Cases of Digital Signatures

- First use: every visited website is \( \geq 1 \) signature published and multiple verifications
- Second use: The one on the lease is legally binding in many countries
- Both use cases relies on long-term security

However...quantum computing threatens the security of current standards!
Dilithium

- NIST holds a competition for new, quantum resistant standards

- Among the winners: Dilithium, Falcon are based on lattices
Dilithium

- NIST holds a competition for new, quantum resistant standards

- Among the winners: Dilithium

- Based on the “Fiat-Shamir with Aborts over Euclidean Lattices” framework by Lyubashevsky [Lyu09,Lyu12]

- We want to explore other directions than the one from Dilithium
How can we get rid of rejection sampling in Lyubashevsky’s signature while keeping signature sizes at least as small?

What is rejection sampling and why do we need it? (Preliminaries)

Why do we want to remove rejection sampling? (Contribution)

Answer: replace rejection sampling with convolution (Contribution)

What are the best achievable sizes with rejection sampling? (Contribution)
Preliminaries: the Fiat-Shamir Paradigm

What are we talking about?
Digital Signature

KeyGen(\(\lambda\)) → sk

Sign(sk, \(\mu\)) → \(\sigma\)

Verify(vk, \(\mu\), \(\sigma\)) → True or False

(For any message \(\mu\))
Properties of Digital Signatures

- **Correctness:**
  \[ \text{Verify}(vk, \mu, \text{Sign}(sk, \mu)) = \text{True} \]

- **Unforgeability:**
  \[ \text{Pr} \left[ \text{Verify}(vk, \mu^*, \sigma^*) = \text{True} \right] = \text{negl}(\lambda) \]
  when \((\mu^*, \sigma^*) = A(vk)\) for ppt \(A\) (EU-NMA) Add Sign oracle (EU-CMA)

```
KeyGen(1^\lambda) -> sk, vk
  sk -> Sign(sk) -> \sigma -> Verify(vk, \mu, \sigma) -> True
  vk -> Verify(vk, \mu, \sigma) -> True
```
Properties of Digital Signatures

KeyGen(1^λ) → vk → \mathcal{A}(vk) → \mu^*, \sigma^* → Verify(vk, \mu^*, \sigma^*) → \text{False}

- Correctness:
  \text{Verify}(vk, \mu, \text{Sign}(sk, \mu)) = True

- Unforgeability:
  \text{Pr}[\text{Verify}(vk, \mu^*, \sigma^*) = True] = \text{negl}(\lambda)
  \text{when } (\mu^*, \sigma^*) = \mathcal{A}(vk) \text{ for ppt } \mathcal{A}
  (EU-NMA)
Properties of Digital Signatures

- **Correctness:**
  \[
  \text{Verify}(vk, \mu, \text{Sign}(sk, \mu)) = \text{True}
  \]

- **Unforgeability:**
  \[
  \Pr[\text{Verify}(vk, \mu^*, \sigma^*) = \text{True}] = \text{negl}(\lambda)
  \]
  when \((\mu^*, \sigma^*) = \mathcal{A}(vk)\) for ppt \(\mathcal{A}\)
  (EU-NMA)
  Add Sign oracle (EU-CMA)
$\Sigma$-protocol

\[
P(sk) \quad V(vk)
\]

\[
c \leftarrow U(C)
\]

\[
w
\]

\[
z
\]
Properties

- Completeness: $V(vk)$ accepts after interacting with $P(sk)$

Diagram:

```
 P(sk) ------------------- V(vk)
    \       \            \    \   \  \\
     w         c         z
```

J. Devevey - Defense
Properties

- **Completeness:** $V(vk)$ accepts after interacting with $P(sk)$
- **Soundness:** $V(vk)$ rejects after interacting with $A(vk)$
Properties

\[ \approx \varepsilon_{zk} \]

where does not use \( sk \)

- **Completeness**: \( V(vk) \) accepts after interacting with \( P(sk) \)
- **Soundness**: \( V(vk) \) rejects after interacting with \( A(vk) \)
- **HVZK**: Nothing is revealed on \( sk \)
From $\Sigma$-protocol to Signature

$\text{Sign}(sk, \mu)$:

\[
\text{Output } \sigma = (w, c, z)
\]

\[\mathcal{U}(c)\]

$\text{Verify}(vk, \mu, \sigma)$:

Check that $V$ accepts $\sigma = (w, c, z)$
Easy forgery:

\[ A(vk, \mu): \]

Output \( \sigma = (w, c, z) \)

\[ \text{Verify}(vk, \mu, \sigma): \]

Check that \( V \) accepts \( \sigma = (w, c, z) \)
Simulation relies on **changing the order in which the transcript is generated**

\[
P(\text{sk}) \rightarrow V(\text{vk})
\]

\[
w \rightarrow H(w, \mu) = c
\]

\[
z
\]

\[H\] prevents the use of the simulator while keeping uniform challenges.
The Fiat-Shamir Transform [FS86]

Sign$(sk, \mu)$:

Output $\sigma = (w, c, z)$

Verify$(vk, \mu, \sigma)$:

Check that $V$ accepts $\sigma = (w, c, z)$ and that $c = H(w, \mu)$

Properties:

• Completeness implies correctness
• Soundness implies EU-NMA
• Add HVZK to get EU-CMA
The Fiat-Shamir Transform [FS86]

\textbf{Sign}(sk, \mu):$

Output $\sigma = (w, c, z)$

\textbf{Verify}(vk, \mu, \sigma):$

Check that $V$ accepts $\sigma = (w, c, z)$ and that $c = H(w, \mu)$

\textbf{Properties:}$

- Completeness implies correctness
- Soundness implies EU-NMA
- Add HVZK to get EU-CMA

*(Simulate the Sign oracle to make it useless)*
Preliminaries: the Fiat-Shamir Paradigm, the Lattice Case

What is rejection sampling?
Lattice-based Assumptions

Learning with Errors $\text{LWE}_{m,k,q,\chi}$

Given $A_0 \leftarrow U(\mathbb{Z}_q^{m \times (k-m)})$, $A = (A_0 | I_m)$ and $t \in \mathbb{Z}_q^m$, find if $t \leftarrow U(\mathbb{Z}_q^m)$ or if $t = As$ for short $s \leftarrow \chi^k$
### Learning with Errors LWE_{m,k,q,\chi}

Given $A_0 \leftarrow U(\mathbb{Z}_q^{m \times (k-m)})$, $A = (A_0 | I_m)$ and $t \in \mathbb{Z}_m$, find if $t \leftarrow U(\mathbb{Z}_q^m)$ or if $t = As$ for short $s \leftarrow \chi^k$.

### Short Integer Solution SIS_{m,k,\gamma}

Given $A \leftarrow U(\mathbb{Z}_q^{m \times k})$, find $x \in \mathbb{Z}^k$ such that $\|x\| \leq \gamma$ and $Ax = 0 \mod q$. 
Lyubashevsky’s Protocol [Lyu09,Lyu12]

\[ P(A, S) \quad V(A, T) \]

\[ y \leftarrow Q \]

\[ w = Ay \mod q \]

\[ c \]

\[ z = y + Sc \]

- \[ AS = T \mod q \] and \( S \) is short
- Short \( y \) sampled from distribution \( Q \)
- \( c \) is binary or ternary
Lyubashevsky’s Protocol [Lyu09,Lyu12]

\[ P(A, S) \quad V(A, T) \]

\( y \leftarrow Q \)

\( w = Ay \mod q \)

\( z = y + Sc \)

- \( AS = T \mod q \) and \( S \) is short
- \( z = y + Sc \) is small
- \( Az = Ay + ASc = w + Tc \mod q \)
- \( V \) checks \( \|z\| \leq \gamma \) and \( Az - Tc = w \mod q \)
Lyubashevsky’s Protocol [Lyu09,Lyu12]

\[ y \leftarrow Q \]
\[ w = Ay \mod q \]
\[ z = y + Sc \]

- \( AS = T \mod q \) and \( S \) is short
- \( V \) checks \( ||z|| \leq \gamma \) and \( Az - Tc = w \mod q \)
- The protocol is complete
- Soundness based on SIS
HVZK for Lyubashevsky’s Protocol

\[ z \leftarrow ??? \]
\[ c \leftarrow U(C) \]
\[ w = Az - Tc \pmod{q} \]

Return \((w, c, z)\)

- \(z \leftarrow P\) where \(P\) is independent of \(S\)
- Impact on the security of the signature?
HVZK for Lyubashevsky’s Protocol

\[
\begin{align*}
  z & \leftarrow \text{??}
  \\
  c & \leftarrow U(C)
  \\
  w & = Az - Tc \mod q
  \\
  \text{Return } (w, c, z)
\end{align*}
\]

- \[ z \leftarrow P \text{ where } P \text{ is independent of } S \]
- Impact on the security of the signature?
- \[ z = y + Sc \text{ actually leaks } Sc \]
- Key recovery attacks
Technique 1: HVZK via Flooding

$$z = y + Sc$$

Large sizes due to large standard deviation ⇒ Impractical parameters
Technique 1: HVZK via Flooding

Simulated $z$

$z = y + Sc$

Large sizes due to large standard deviation ⇒ Impractical parameters
Technique 1: HVZK via Flooding

Simulated $z$

$z = y + Sc$

Large sizes due to large standard deviation $⇒$ Impractical parameters
Technique 1: HVZK via Flooding

Simulated \( z \)

\[ z = y + Sc \]

Large sizes due to large standard deviation $\Rightarrow$ Impractical parameters

J. Devevey - Defense
Technique 2: Rejection Sampling

Monte-Carlo sampling

\[ M \cdot Q_{Sc} \]
Technique 2: Rejection Sampling

- “Monte-Carlo” sampling

$M \cdot Q_{Sc}$
Technique 2: Rejection Sampling

- “Monte-Carlo” sampling
- $M = \text{number of expected repetitions}$
Technique 2: Rejection Sampling

- $M \approx$ number of expected repetitions
- $\varepsilon$ controls the quality
Technique 2: Rejection Sampling

- $M \approx$ number of expected repetitions
- $\varepsilon(Sc)$ controls the quality (*may vary*)
Non-aborting Simulation

\[
P(A, S) \quad V(A, T)
\]

\[
y \leftarrow Q \\
w = Ay \mod q
\]

\[
z = y + Sc \quad \text{w.p.} \quad \frac{P(z)}{MQ(y)}
\]

Else

For \( M > 1 \) take \( \varepsilon = \max \varepsilon(S, c) \).
Non-aborting Simulation

\[ P(A, S) \quad V(A, T) \]
\[ y \leftarrow Q \quad w = Ay \mod q \]
\[ w.p. \quad z = y + Sc \]
\[ z \leftarrow P \quad \text{else} \]

For \( M > 1 \) take \( \varepsilon = \max \varepsilon(S, c) \).

_for non-in Lyubashevsky’s scheme_

Sample \( z \leftarrow P \)
and \( c \leftarrow U(C) \).
Set \( w = Az - Tc \mod q \)
Return \((w, c, z)\).
One Instance: Dilithium

Goal: Easy implementation

- $P$ and $Q$ are uniform over hypercubes
- $P(z)/MQ(y)$ is 0 or 1 depending on $\|z\|_{\infty}$
- Average rejection probability is $\beta = 3/4$
Goal: Easy implementation

- $P$ and $Q$ are uniform over hypercubes
- $P(z)/MQ(y)$ is 0 or 1 depending on $\|z\|_\infty$
- Average rejection probability is $\beta = 3/4$
One Instance: Dilithium

Goal: Easy implementation

- $P$ and $Q$ are uniform over hypercubes
- $P(z)/MQ(y)$ is 0 or 1 depending on $\|z\|_\infty$
- Average rejection probability is $\beta = 3/4$
Difficulties in the Analysis of Fiat-Shamir with Aborts

Why do we want to remove it?

*Based on a work with P. Fallahpour, A. Passelège and D. Stehlé*
From Aborting $\Sigma$-protocol to Signature

<table>
<thead>
<tr>
<th></th>
<th>Fiat-Shamir</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Sign}(sk, \mu)$</td>
<td>![Diagram]</td>
</tr>
<tr>
<td>Repetitions</td>
<td>1</td>
</tr>
<tr>
<td>Intuition</td>
<td>Unif. challenge</td>
</tr>
<tr>
<td>Drawback</td>
<td>$\Pr(\text{Unif. challenge}) = \beta$</td>
</tr>
</tbody>
</table>
## From Aborting $\Sigma$-protocol to Signature

<table>
<thead>
<tr>
<th></th>
<th>Fiat-Shamir</th>
<th>Unbounded FS$_\infty$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sign</strong>($\text{sk}, \mu$)</td>
<td><img src="image1" alt="Fiat-Shamir Sign" /></td>
<td><img src="image2" alt="Unbounded FS$_\infty$ Sign" /></td>
</tr>
<tr>
<td>Repetitions</td>
<td>1</td>
<td>While</td>
</tr>
<tr>
<td>Intuition</td>
<td>Unif. challenge</td>
<td>Correct</td>
</tr>
<tr>
<td>Drawback</td>
<td>$\Pr(\text{foo}) = \beta$</td>
<td>No analysis</td>
</tr>
</tbody>
</table>

J. Devevey - Defense
From Aborting $\Sigma$-protocol to Signature

<table>
<thead>
<tr>
<th></th>
<th>Fiat-Shamir</th>
<th>Bounded FS$_B$</th>
<th>Unbounded FS$_\infty$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sign</strong>(sk, $\mu$)</td>
<td>![Diagram 1]</td>
<td>![Diagram 2] at most $B$</td>
<td>![Diagram 3] While</td>
</tr>
<tr>
<td><strong>Repetitions</strong></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Intuition</strong></td>
<td>Unif. challenge</td>
<td></td>
<td>Correct</td>
</tr>
<tr>
<td><strong>Drawback</strong></td>
<td>$\Pr\left(\text{Unif. challenge}\right) = \beta$</td>
<td>$\Pr\left(\begin{array}{c} \text{Unif. challenge} \ 1 \ldots B \end{array}\right) = \beta^B$</td>
<td>Not used in practice</td>
</tr>
</tbody>
</table>
A False Intuition

Those events are non-independent due to the use of $H$

In particular when the same $w$ is used twice

Problem$_\infty$: counter-example with infinite runtime
A False Intuition

Those events are non-independent due to the use of $H$

In particular when the same $w$ is used twice

Problem\(_\infty\): counter-example with infinite runtime
Problem\(_B\): all previous security proofs for FS\(_B\) are void!
The security proof can be patched if works for.

For Lyubashevsky’s protocol, we only have for non-.
Solution for $FS_B$

The security proof can be patched if works for Lyubashevsky. For Lyubashevsky's protocol, we only have for non-

**Aborting case analysis**

When $w, w \approx U(\mathbb{Z}_q^m)$

**Leveraged Simulator**

Run with proba $1/M$. Else, output uniform $(w, c, z) \in \mathbb{Z}_q^m \times C \times \{\perp\}$
Reasons to remove Rejection Sampling

- The base $\Sigma$-protocol is not complete.
- The analysis is tedious (imagine for advanced protocols!).
- Rejected signatures are “wasted” resources.
G+G: a Convolution Approach to Lattice-based Fiat-Shamir

How can we get rid of rejection sampling while keeping signature sizes at least as small?

Based on a work with A. Passelègue and D. Stehlé
Leaks in rejectionless Lyubashevsky’s protocol

- \( z = y + Sc \) is centered around \( Sc \)

- This can be learnt with sufficiently many signatures
Leaks in rejectionless Lyubashevsky’s protocol

- $z = y + Sc$ is centered around $Sc$

- This can be learnt with sufficiently many signatures

Solution: Sample $h$ centered around $-c$ to compensate
Set $z = y + Sc + Sh$

New problem: $Az - Tc = Ay + Th \mod q$. How to make the scheme correct?
Changing the Key Generation

Problem: \( Th = 0 \mod q \)
Solution: Take \( AS = 0 \mod q \)
Changing the Key Generation

Problem: \( Th = 0 \mod q \)
Solution: Take \( AS = 0 \mod q \)

Problem: \( Sc \) can be omitted from \( z \) as \( Az = Ay \mod q \)
More Solutions, More Problems

**Changing the Key Generation**

Problem: \( Th = 0 \mod q \)
Solution: Take \( AS = 0 \mod q \)

Problem: \( Sc \) can be omitted from \( z \) as \( Az = Ay \mod q \)
Solution: Use \( 2q \) and \( 2AS = 0 \mod 2q \) while \( AS \neq 0 \mod 2q \)

Sample \( h \) centered around \(-c/2\) and set \( z = y + Sc + 2Sh \)
Changing the Key Generation

Problem: $Th = 0 \mod q$
Solution: Take $AS = 0 \mod q$

Problem: $Sc$ can be omitted from $z$ as $Az = Ay \mod q$
Solution: Use $2q$ and $2AS = 0 \mod 2q$ while $AS \neq 0 \mod 2q$

Sample $h$ centered around $-c/2$ and set $z = y + Sc + 2Sh$

New Problem: Covariance matrix of $2Sh$ dependent on $S$

What is the final distribution of $z = y + Sc + 2Sh$?
Gaussian Convolution (Continuous Case)

\[ y + (Sc + 2Sh) = z \]
Gaussian Convolution (Continuous Case)

\[ y \text{ var}(y) + \text{Sc} + 2 \text{Sh} \text{ var}(\text{Sc} + 2 \text{Sh}) = z \text{ var}(z) \]
Set $\Sigma(S) = \sigma^2 I_k - 4S^2 SS^T$. Sample $y \leftarrow D_{\mathbb{Z}^k, \Sigma(S)}$ and $h \leftarrow D_{\mathbb{Z}^n, s, -c/2}$.

- $\sigma \geq \sqrt{8} \sigma_1(S) \cdot s$

(Positive definite)
Discrete Gaussian Case

Set $\Sigma(S) = \sigma^2 I_k - 4s^2 SS^\top$.
Sample $y \leftarrow D \mathbb{Z}^k, \Sigma(S)$ and $h \leftarrow D \mathbb{Z}^n, s_{-c/2}$.
Set $z = y + Sc + 2Sh$.

• $\sigma \geq \sqrt{8}\sigma_1(S) \cdot s$ (Positive definite)
• $s \geq \sqrt{2 \ln(d - 1 + 2d/\varepsilon)}/\pi$ (Smoothing quality)

Quality

$$P_z \approx \varepsilon \cdot D_{\mathbb{Z}^k, \sigma}$$
## The G+G Scheme

<table>
<thead>
<tr>
<th>P(A, S)</th>
<th>V(A, T = AS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( y \leftarrow D_{\mathbb{Z}^k}^{\Sigma(s)} )</td>
<td>( w \leftarrow A y \mod 2q )</td>
</tr>
<tr>
<td>( w \leftarrow A y \mod 2q )</td>
<td>( w \rightarrow )</td>
</tr>
<tr>
<td>( h \leftarrow D_{\mathbb{Z}^n}^{s,-c/2} )</td>
<td>( c \leftarrow U(C) )</td>
</tr>
<tr>
<td>( z \leftarrow y + 2Sh + S c \mod 2q )</td>
<td>( z \rightarrow )</td>
</tr>
<tr>
<td>( \text{Accept if } Az = w + Tc \mod 2q )</td>
<td>( |z| \leq \gamma )</td>
</tr>
<tr>
<td>( \text{and } |z| \leq \gamma )</td>
<td></td>
</tr>
</tbody>
</table>
Properties

- **Completeness:** $A_z - T_c = A_y + (A - S - T)c + 2A_S h = A_y = w \mod 2q$

- **Soundness:** Based on SIS, as before

- **HVZK:** Sample $z \leftarrow D_{\mathbb{Z}_k, \sigma}$ and $c \leftarrow U(C)$. Set $w = A_z - T_c \mod 2q$
Performances

Signature Size vs Security Level graph showing performances of Dilithium and G+G.

- Dilithium
- G+G

J. Devevey - Defense
Haetae: Shorter Fiat-Shamir with Aborts Signature

What are the best achievable sizes with rejection sampling?

Haetae is a work with J.H. Cheon, H. Choe, T. Güneysu, D. Hong, M. Krausz, G. Land, M. Möller, D. Stehlé, M. Yi

Based on a theoretical work with O. Fawzi, A. Passelègue and D. Stehlé
Dilithium is not the best you can do
Goal of Dilithium was not short signatures, contrary to:

- Submitted to NIST and Korean PQ Competition
- Theory-backed choice of distributions for $P$ and $Q$
Optimal Choice of Distribution

Our choice for $Q$ and $P$: $U(\cdot)$

- Most compact choice \[\text{DFPS22}\]
- Easier rejection probability than Gaussians

Use of bimodal setting: more compact \[\text{DFPS22}\]
Switching to Bimodal Distributions

\[
z = y + Sc \text{ or } z = y - Sc \quad \text{(with probability } 1/2 \text{ each)}
\]
Switching to Bimodal Distributions

\[ z = y + Sc \text{ or } z = y - Sc \] (with probability 1/2 each)

- Adapt KeyGen
- Work \( \mod 2q \) to have \( AS = -AS \mod 2q \)

- Adapt rejection probability
Sizes for Haetae

- Dilithium-G
- Dilithium
- Haetae
- G+G

Security Level vs. Signature Size graph.
## Final Comparison

<table>
<thead>
<tr>
<th>Haetae</th>
<th>G+G</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Already implemented</td>
<td>+ No rejection sampling</td>
</tr>
<tr>
<td>+ No involved operation on secret values</td>
<td>+ Smaller sizes</td>
</tr>
</tbody>
</table>

J. Devevey - Defense
<table>
<thead>
<tr>
<th>Publication</th>
<th>Conference/Preprint</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Rejection Sampling in Lyubashevsky’s Signature Scheme</td>
<td>Asiacrypt’22</td>
<td>O. Fawzi, A. Passelège and D. Stehlé</td>
</tr>
<tr>
<td>A Detailed Analysis of Fiat-Shamir with Aborts</td>
<td>Crypto’23</td>
<td>P. Fallahpour, A. Passelège and D. Stehlé</td>
</tr>
<tr>
<td>G+G: A Fiat-Shamir Lattice Signature Based on Convolved Gaussians</td>
<td>Asiacrypt’23</td>
<td>A. Passelège and D. Stehlé</td>
</tr>
</tbody>
</table>
On the Integer Polynomial Learning with Errors Problem
*PKC’21*. With A. Sakzad, D. Stehlé and R. Steinfeld

*PKC’21*. With B. Libert, K. Nguyen, T. Peters, M. Yung

Rational Modular Encoding in the DCR Setting: Non-Interactive Range Proofs and Paillier-Based Naor-Yung in the Standard Model
*PKC’22*. With B. Libert and T. Peters
Thank you! Any questions?