Lattice-based Signature Schemes in the Fiat-Shamir Paradigm

PhD Defense

Julien Devevey[1], under the supervision of Damien Stehlé

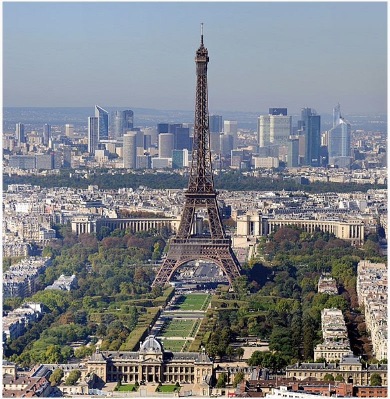
Sep. 18, 2023

1. École Normale Supérieure de Lyon

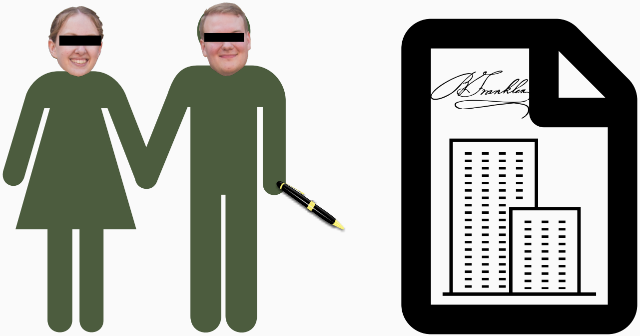
ENS DE LYON

Story Time

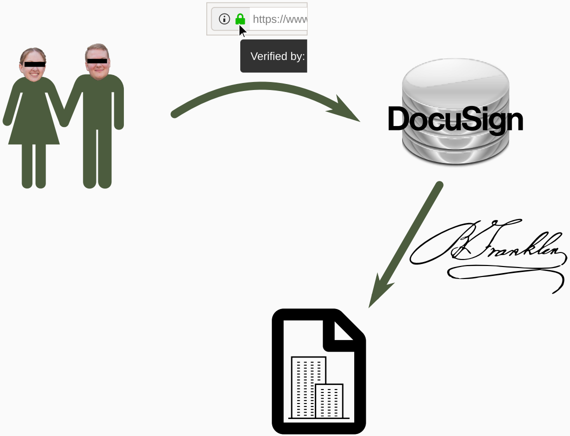
Mrs & Mr D.



Signing the Lease



Signing the Lease



Use Cases of Digital Signatures

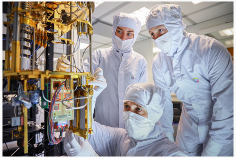
- First use: every visited website is ≥ 1 signature published and multiple verifications
- Second use: The one on the lease is legally binding in many countries
- Both use cases relies on long-term security

However…

Use Cases of Digital Signatures

- First use: every visited website is ≥ 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 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE holds a competition for new, quantum resistant standards
- Among the winners:
- 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

In the next 40 Minutes

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)

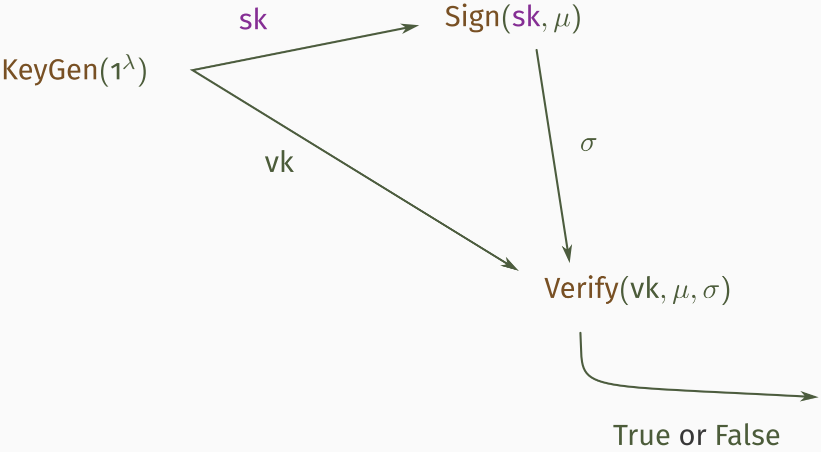
Answer: replace rejection sampling with convolution (Contribution)

What are the best achievable sizes with rejection sampling? (Contribution)

Preliminaries: the Fiat-Shamir Paradigm

What are we talking about?

Digital Signature



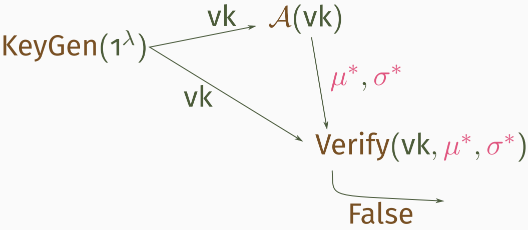
(For any message μ)

Properties of Digital Signatures

$$
\begin{tikzcd}
 & \mathsf{Sign}(\mathsf{sk}) \arrow[d, "\sigma"] \\
\mathsf{KeyGen}(1^{\lambda}) \arrow[ur, "\mathsf{sk}"] \arrow[r, "\mathsf{vk}"'] & \mathsf{Verify}(\mathsf{vk}, \mu, \sigma) \arrow[d] \\
 & \mathsf{True}
\end{tikzcd}
$$

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

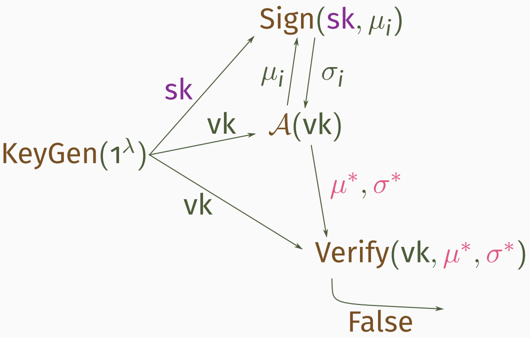
Properties of Digital Signatures



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

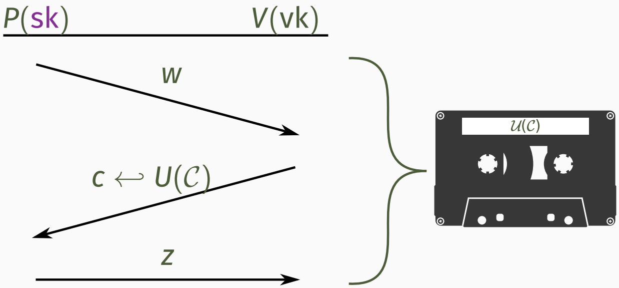
- **Unforgeability:**
  $\Pr[\mathsf{Verify}(\mathsf{vk}, \mu^*, \sigma^*) = \mathsf{True}] = \mathsf{negl}(\lambda)$
  when $(\mu^*, \sigma^*) = \mathcal{A}(\mathsf{vk})$ for ppt $\mathcal{A}$
  (EU-NMA)

Properties of Digital Signatures

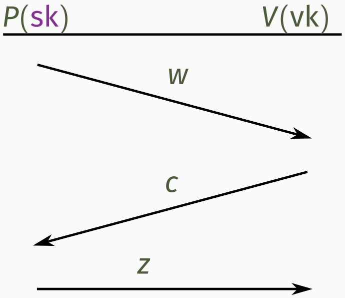


- **Correctness:**
  $\mathsf{Verify}(\mathsf{vk}, \mu, \mathsf{Sign}(\mathsf{sk}, \mu)) = \mathsf{True}$

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

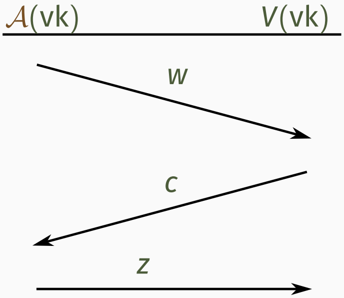

$P(\mathsf{sk})$
$V(\mathsf{vk})$
w
$c \hookleftarrow U(\mathcal{C})$
z
$\mathcal{U}(\mathcal{C})$

Properties



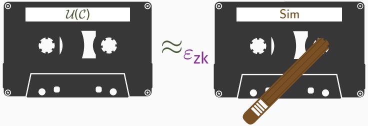
- Completeness: $V(\mathsf{vk})$ accepts after interacting with $P(\mathsf{sk})$

Properties



- **Completeness**: $V(\mathsf{vk})$ accepts after interacting with $P(\mathsf{sk})$
- **Soundness**: $V(\mathsf{vk})$ rejects after interacting with $\mathcal{A}(\mathsf{vk})$

Properties



where  does not use sk

- Completeness: $V(\mathsf{vk})$ accepts after interacting with $P(\mathsf{sk})$
- Soundness: $V(\mathsf{vk})$ rejects after interacting with $\mathcal{A}(\mathsf{vk})$
- HVZK: Nothing is revealed on sk

From Σ-protocol to Signature

Sign(sk, μ):

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

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

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

From Σ-protocol to Signature?

Easy forgery:

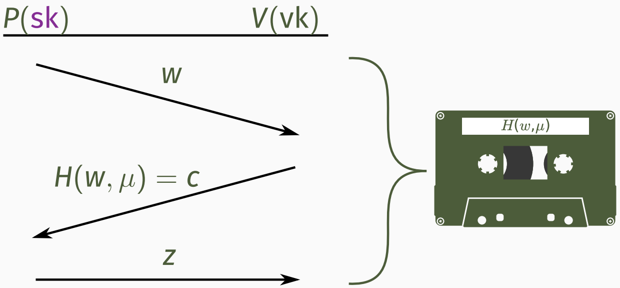
$\mathcal{A}(\mathsf{vk}, \mu)$:

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

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

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

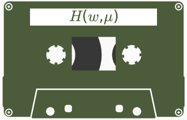
Simulation relies on changing the order in which the transcript is generated



H prevents the use of the simulator while keeping uniform challenges

The Fiat-Shamir Transform [FS86]

Sign(sk, μ):



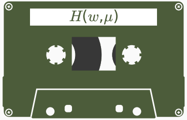
Output $\sigma = (w, c, z)$

Verify(vk, μ, σ):

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

The Fiat-Shamir Transform [FS86]

Sign(sk, μ):



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

Verify(vk, μ, σ):

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

(Simulate the Sign oracle to make it useless)

Preliminaries: the Fiat-Shamir Paradigm, the Lattice Case

What is rejection sampling?

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

Given $\mathbf{A}_0 \hookleftarrow U(\mathbb{Z}_q^{m\times(k-m)})$, $\mathbf{A} = (\mathbf{A}_0|\mathbf{I}_m)$ and $\mathbf{t} \in \mathbb{Z}_q^m$, find if $\mathbf{t} \hookleftarrow U(\mathbb{Z}_q^m)$ or if $\mathbf{t} = \mathbf{A}\mathbf{s}$ for short $\mathbf{s} \hookleftarrow \chi^k$

Lattice-based Assumptions

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

Given $\mathbf{A}_0 \hookleftarrow U(\mathbb{Z}_q^{m\times(k-m)})$, $\mathbf{A} = (\mathbf{A}_0|\mathbf{I}_m)$ and $\mathbf{t} \in \mathbb{Z}_q^m$, find if $\mathbf{t} \hookleftarrow U(\mathbb{Z}_q^m)$ or if $\mathbf{t} = \mathbf{A}\mathbf{s}$ for short $\mathbf{s} \hookleftarrow \chi^k$

Short Integer Solution $\mathsf{SIS}_{m,k,\gamma}$

Given $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times k})$, find $\mathbf{x} \in \mathbb{Z}^k$ such that $\|\mathbf{x}\| \leq \gamma$ and $\mathbf{A}\mathbf{x} = 0 \bmod q$

Lyubashevsky's Protocol [Lyu09,Lyu12]

$P(\mathbf{A}, \mathbf{S})$		$V(\mathbf{A}, \mathbf{T})$
$\mathbf{y} \hookleftarrow Q$		
	$\xrightarrow{\mathbf{w} = \mathbf{A}\mathbf{y} \bmod q}$	
	$\xleftarrow{\mathbf{c}}$	
	$\xrightarrow{\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}}$	

- $\mathbf{A}\mathbf{S} = \mathbf{T} \bmod q$ and $\mathbf{S}$ is short
- Short $\mathbf{y}$ sampled from distribution Q
- $\mathbf{c}$ is binary or ternary

$$
\begin{array}{lcr}
P(\mathbf{A}, \mathbf{S}) & & V(\mathbf{A}, \mathbf{T}) \\
\hline
\mathbf{y} \hookleftarrow Q & & \\
 & \xrightarrow{\mathbf{w} = \mathbf{A}\mathbf{y} \bmod q} & \\
 & \xleftarrow{\mathbf{c}} & \\
 & \xrightarrow{\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}} &
\end{array}
$$

- $\mathbf{A}\mathbf{S} = \mathbf{T} \bmod q$ and $\mathbf{S}$ is short
- $\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ is small
- $\mathbf{A}\mathbf{z} = \mathbf{A}\mathbf{y} + \mathbf{A}\mathbf{S}\mathbf{c} = \mathbf{w} + \mathbf{T}\mathbf{c} \bmod q$
- V checks $\|\mathbf{z}\| \leq \gamma$ and $\mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} = \mathbf{w} \bmod q$

Lyubashevsky's Protocol [Lyu09,Lyu12]

$P(\mathbf{A}, \mathbf{S})$		$V(\mathbf{A}, \mathbf{T})$
$\mathbf{y} \hookleftarrow Q$		
	$\xrightarrow{\mathbf{w} = \mathbf{A}\mathbf{y} \bmod q}$	
	$\xleftarrow{\mathbf{c}}$	
	$\xrightarrow{\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}}$	

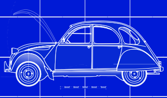
- $\mathbf{A}\mathbf{S} = \mathbf{T} \bmod q$ and $\mathbf{S}$ is short
- V checks $\|\mathbf{z}\| \leq \gamma$ and $\mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} = \mathbf{w} \bmod q$
- The protocol is complete
- Soundness based on SIS

$\mathbf{z} \hookleftarrow ???$

$\mathbf{c} \hookleftarrow U(\mathcal{C})$

$\mathbf{w} = \mathbf{Az} - \mathbf{Tc} \bmod q$

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$



- $\mathbf{z} \hookleftarrow P$ where P is independent of $\mathbf{S}$
- Impact on the security of the signature?

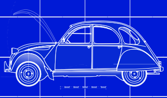
HVZK for Lyubashevsky's Protocol

$\mathbf{z} \hookleftarrow ???$

$\mathbf{c} \hookleftarrow U(\mathcal{C})$

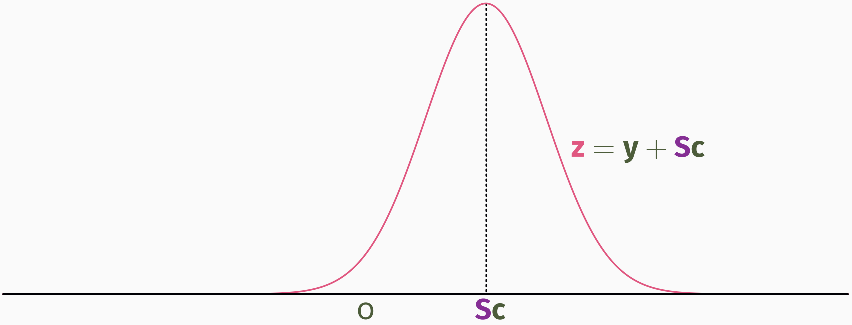
$\mathbf{w} = \mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} \bmod q$

Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$

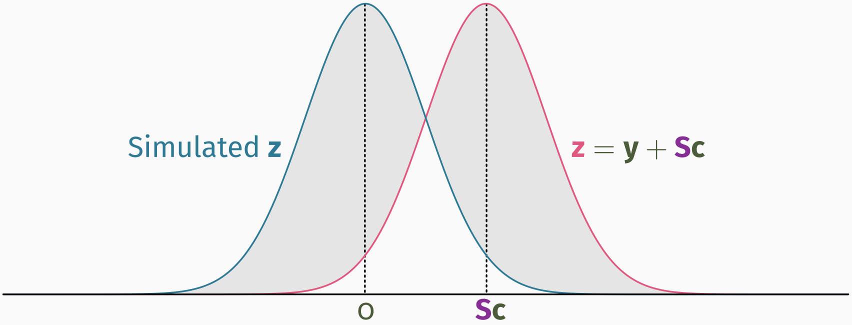


- $\mathbf{z} \hookleftarrow P$ where P is independent of $\mathbf{S}$
- Impact on the security of the signature?
- $\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ actually leaks $\mathbf{S}\mathbf{c}$
- Key recovery attacks

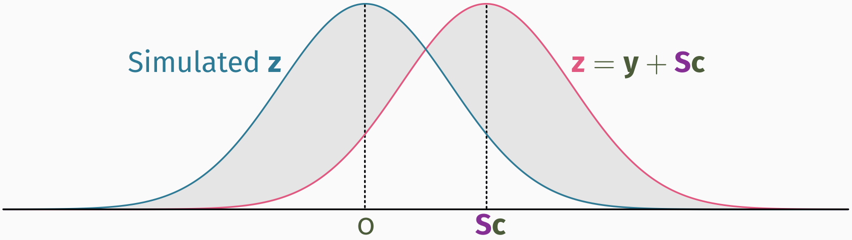
Technique 1: HVZK via Flooding



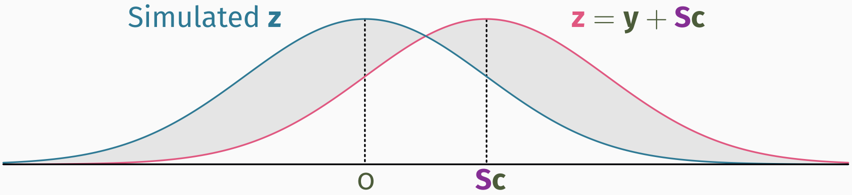
Technique 1: HVZK via Flooding



Technique 1: HVZK via Flooding

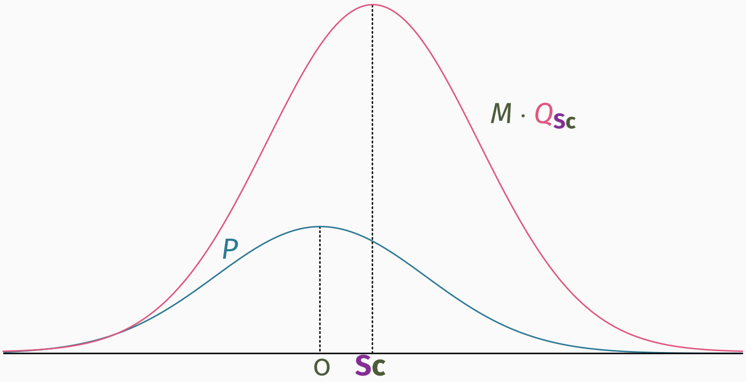


Technique 1: HVZK via Flooding

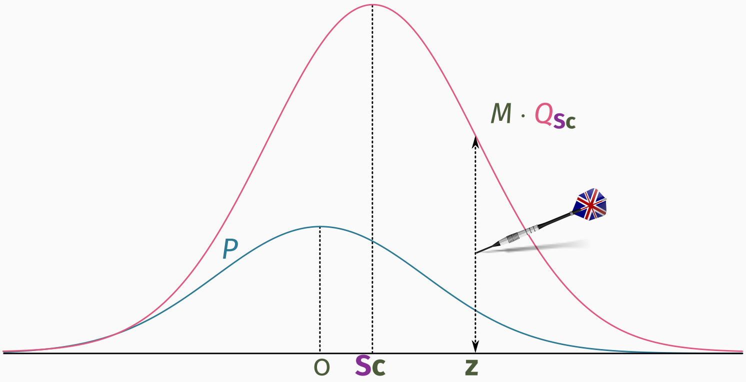


Large sizes due to large standard deviation $\implies$ **Impractical parameters**

Technique 2: Rejection Sampling

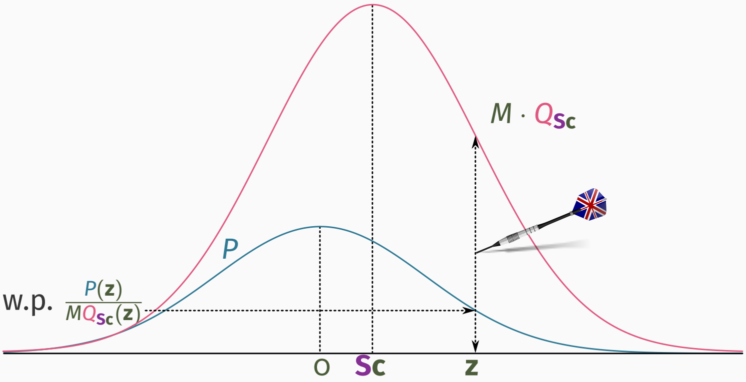


Technique 2: Rejection Sampling



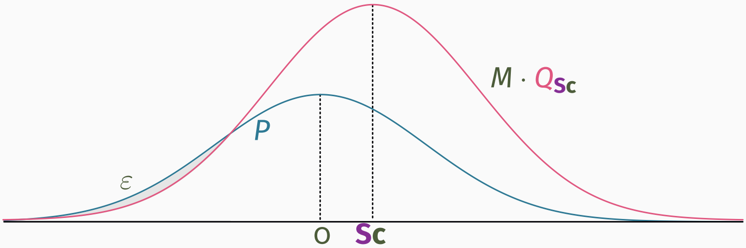
- "Monte-Carlo" sampling

Technique 2: Rejection Sampling



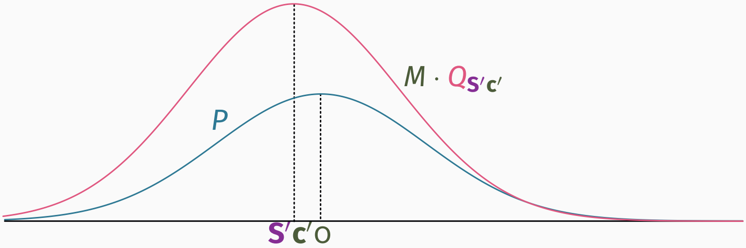
- “Monte-Carlo” sampling
- $M =$ number of expected repetitions

Technique 2: Rejection Sampling



- $M \approx$ number of expected repetitions
- ε controls the quality

Technique 2: Rejection Sampling



- $M \approx$ number of expected repetitions
- $\varepsilon(\mathbf{Sc})$ controls the quality *(may vary)*

Non-aborting Simulation

$P(\mathbf{A}, \mathbf{S})$	$V(\mathbf{A}, \mathbf{T})$
$\mathbf{y} \hookleftarrow Q$	
$\xrightarrow{\mathbf{w} = \mathbf{A}\mathbf{y} \bmod q}$	
$\xleftarrow{\mathbf{c}}$	
$\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ w.p. $\frac{P(\mathbf{z})}{MQ(\mathbf{y})}$ $\longrightarrow$	
Else 	

For $M > 1$ take $\varepsilon = \max \varepsilon(\mathbf{S}, \mathbf{c})$.

Non-aborting Simulation

$P(\mathbf{A}, \mathbf{S})$		$V(\mathbf{A}, \mathbf{T})$
$\mathbf{y} \hookleftarrow Q$		
	$\xrightarrow{\mathbf{w} = \mathbf{A}\mathbf{y} \bmod q}$	
	$\xleftarrow{\mathbf{c}}$	
	$\xrightarrow{\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c} \text{ w.p. } \frac{P(\mathbf{z})}{MQ(\mathbf{y})}}$	
	Else 	

For $M > 1$ take $\varepsilon = \max \varepsilon(\mathbf{S}, \mathbf{c})$.

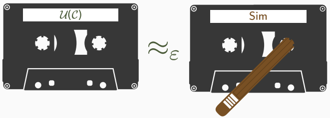
for non-abort in Lyubashevsky's scheme

Sample $\mathbf{z} \hookleftarrow P$

and $\mathbf{c} \hookleftarrow U(\mathcal{C})$.

Set $\mathbf{w} = \mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} \bmod q$

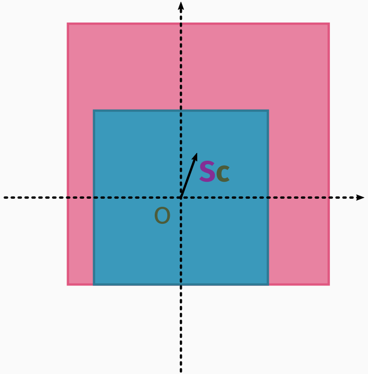
Return $(\mathbf{w}, \mathbf{c}, \mathbf{z})$.



One Instance: Dilithium

Goal: Easy implementation

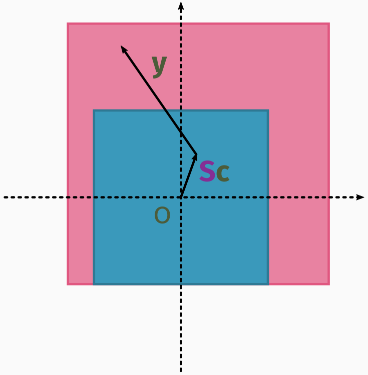
- P and Q are uniform over hypercubes
- $P(\mathbf{z})/MQ(\mathbf{y})$ is 0 or 1 depending on $\|\mathbf{z}\|_\infty$
- Average rejection probability is $\beta = 3/4$



One Instance: Dilithium

Goal: Easy implementation

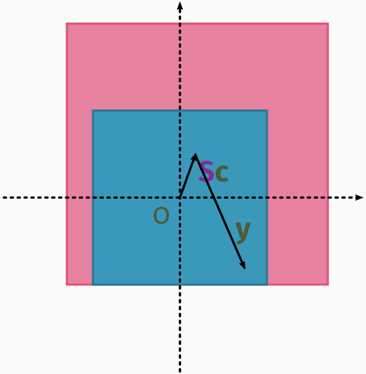
- P and Q are uniform over hypercubes
- $P(\mathbf{z})/MQ(\mathbf{y})$ is 0 or 1 depending on $\|\mathbf{z}\|_\infty$
- Average rejection probability is $\beta = 3/4$



One Instance: Dilithium

Goal: Easy implementation

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

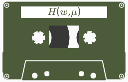


Difficulties in the Analysis of Fiat-Shamir with Aborts

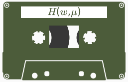
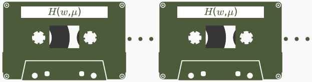
Why do we want to remove it?

Based on a work with P. Fallahpour, A. Passelègue and D. Stehlé

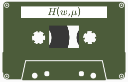
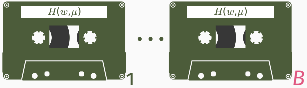
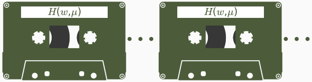
From Aborting Σ-protocol to Signature

	Fiat-Shamir		
Sign(sk, μ)			
Repetitions	1		
Intuition	Unif. challenge		
Drawback	Pr() $= \beta$		

From Aborting Σ-protocol to Signature

	Fiat-Shamir		Unbounded FS_∞
Sign(sk, μ)			
Repetitions	1		While 
Intuition	Unif. challenge		Correct
Drawback	Pr() $= \beta$		No analysis

From Aborting Σ-protocol to Signature

	Fiat-Shamir	Bounded FS_B	Unbounded FS_∞
Sign(sk, μ)			
Repetitions	1	at most B	While 
Intuition	Unif. challenge	Pr  $= \beta^B$	Correct
Drawback	Pr  $= \beta$	Not used in practice	No analysis

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

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!

Solution for FS_B

The security proof can be patched if  works for 

For Lyubashevsky's protocol,
we only have  for non-

The security proof can be patched if 

works for 

For Lyubashevsky's protocol,
we only have 

for non-

Aborting case analysis

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

Leveraged Simulator

Run 

with proba $1/M$.
Else, output uniform $(\mathbf{w}, \mathbf{c}, z) \in \mathbb{Z}_q^m \times \mathcal{C} \times \{\perp\}$

Reasons to remove Rejection Sampling

- The base Σ-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

Back to Basics

Leaks in rejectionless Lyubashevsky's protocol

- $\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ is centered around $\mathbf{S}\mathbf{c}$
- This can be learnt with sufficiently many signatures

Leaks in rejectionless Lyubashevsky's protocol

- $\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ is centered around $\mathbf{S}\mathbf{c}$
- This can be learnt with sufficiently many signatures

Solution: Sample $\mathbf{h}$ centered around $-\mathbf{c}$ to compensate

Set $\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c} + \mathbf{S}\mathbf{h}$

New problem: $\mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c} = \mathbf{A}\mathbf{y} + \mathbf{T}\mathbf{h} \bmod q$. How to make the scheme correct?

More Solutions, More Problems

Changing the Key Generation

Problem: $\mathbf{Th} = 0 \bmod q$

Solution: Take $\mathbf{AS} = 0 \bmod q$

More Solutions, More Problems

Changing the Key Generation

Problem: $\mathbf{Th} = 0 \bmod q$

Solution: Take $\mathbf{AS} = 0 \bmod q$

Problem: $\mathbf{Sc}$ can be omitted from $\mathbf{z}$ as $\mathbf{Az} = \mathbf{Ay} \bmod q$

More Solutions, More Problems

Changing the Key Generation

Problem: $\mathbf{Th} = 0 \bmod q$

Solution: Take $\mathbf{AS} = 0 \bmod q$

Problem: $\mathbf{Sc}$ can be omitted from $\mathbf{z}$ as $\mathbf{Az} = \mathbf{Ay} \bmod q$

Solution: Use $2q$ and $2\mathbf{AS} = 0 \bmod 2q$ while $\mathbf{AS} \neq 0 \bmod 2q$

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

More Solutions, More Problems

Changing the Key Generation

Problem: $\mathbf{Th} = 0 \bmod q$

Solution: Take $\mathbf{AS} = 0 \bmod q$

Problem: $\mathbf{Sc}$ can be omitted from $\mathbf{z}$ as $\mathbf{Az} = \mathbf{Ay} \bmod q$

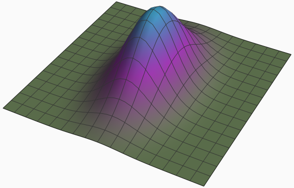
Solution: Use $2q$ and $2\mathbf{AS} = 0 \bmod 2q$ while $\mathbf{AS} \neq 0 \bmod 2q$

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

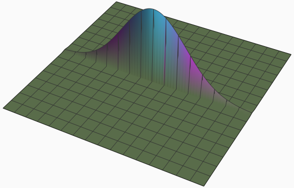
New Problem: Covariance matrix of $2\mathbf{Sh}$ dependent on $\mathbf{S}$

What is the final distribution of $\mathbf{z} = \mathbf{y} + \mathbf{Sc} + 2\mathbf{Sh}$?

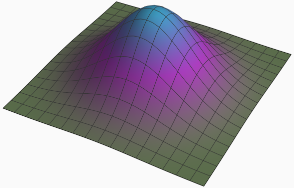
Gaussian Convolution (Continuous Case)



$+$

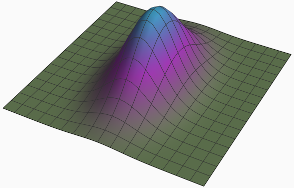


$=$

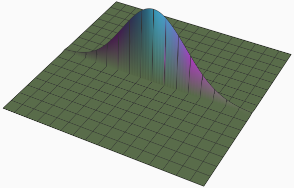


$\mathbf{y}$ $\qquad$ $\mathbf{Sc} + 2\mathbf{Sh}$ $\qquad$ $\mathbf{z}$

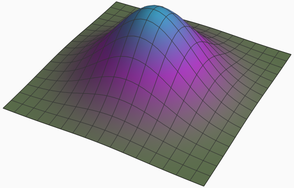
Gaussian Convolution (Continuous Case)



$+$



$=$



$\mathbf{y}$

$\mathrm{var}(\mathbf{y})$

$\mathbf{Sc} + 2\mathbf{Sh}$

$\mathrm{var}(\mathbf{Sc} + 2\mathbf{Sh})$

$\mathbf{z}$

$\mathrm{var}(\mathbf{z})$

Discrete Gaussian Case

Set $\Sigma(\mathbf{S}) = \sigma^2 \mathbf{I}_k - 4s^2 \mathbf{S}\mathbf{S}^\top$.
Sample $\mathbf{y} \hookleftarrow D_{\mathbb{Z}^k, \Sigma(\mathbf{S})}$ and $\mathbf{h} \hookleftarrow D_{\mathbb{Z}^n, s, -\mathbf{c}/2}$.

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

Discrete Gaussian Case

Set $\Sigma(\mathbf{S}) = \sigma^2 \mathbf{I}_k - 4s^2 \mathbf{S}\mathbf{S}^\top$.
Sample $\mathbf{y} \hookleftarrow D_{\mathbb{Z}^k, \Sigma(\mathbf{S})}$ and $\mathbf{h} \hookleftarrow D_{\mathbb{Z}^n, s, -\mathbf{c}/2}$.
Set $\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c} + 2\mathbf{S}\mathbf{h}$.

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

Quality

$$P_{\mathbf{z}} \approx_\varepsilon D_{\mathbb{Z}^k, \sigma}$$

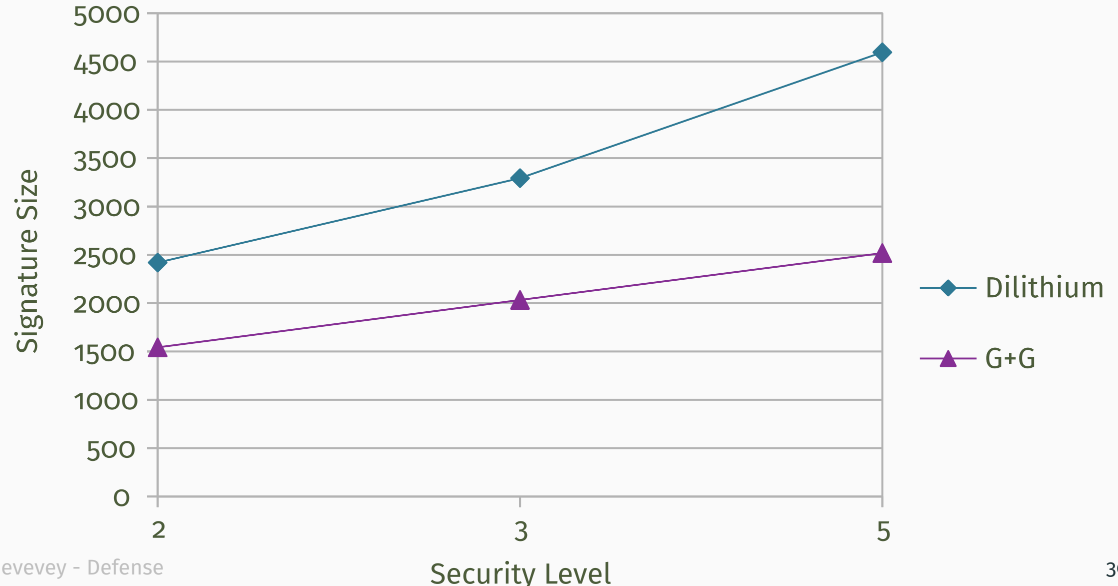
The G+G Scheme

$\mathsf{P}(\mathbf{A}, \mathbf{S})$		$\mathsf{V}(\mathbf{A}, \mathbf{T} = \mathbf{AS})$
$\mathbf{y} \hookleftarrow D_{\mathbb{Z}^k, \Sigma(\mathbf{S})}$		
$\mathbf{w} \leftarrow \mathbf{Ay} \bmod 2q$	$\xrightarrow{\mathbf{w}}$	
	$\xleftarrow{\mathbf{c}}$	$\mathbf{c} \hookleftarrow U(\mathcal{C})$
$\mathbf{h} \hookleftarrow D_{\mathbb{Z}^n, s, -\mathbf{c}/2}$		
$\mathbf{z} \leftarrow \mathbf{y} + 2\mathbf{Sh} + \mathbf{Sc} \bmod 2q$	$\xrightarrow{\mathbf{z}}$	Accept if
		$\mathbf{Az} = \mathbf{w} + \mathbf{Tc} \bmod 2q$
		and $\\|\mathbf{z}\\| \leq \gamma$

Properties

- Completeness: $\mathbf{Az} - \mathbf{Tc} = \mathbf{Ay} + (\mathbf{AS} - \mathbf{T})\mathbf{c} + 2\mathbf{ASh} = \mathbf{Ay} = \mathbf{w} \bmod 2q$
- Soundness: Based on SIS, as before
- HVZK: Sample $\mathbf{z} \hookleftarrow D_{\mathbb{Z}^k,\sigma}$ and $\mathbf{c} \hookleftarrow U(\mathcal{C})$. Set $\mathbf{w} = \mathbf{Az} - \mathbf{Tc} \bmod 2q$

Performances

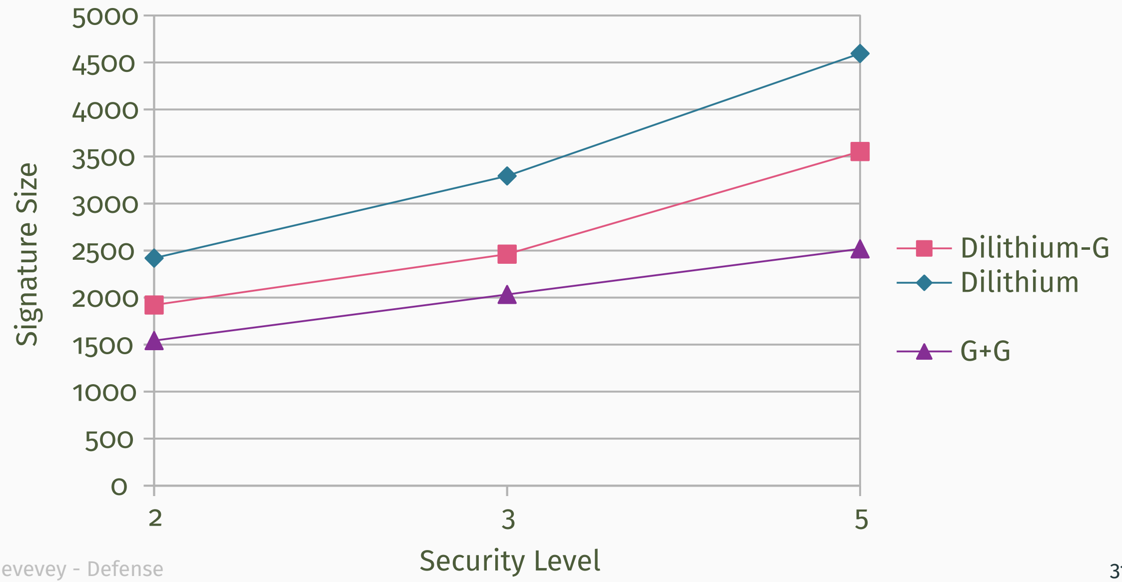


Haetae: Shorter Fiat-Shamir with Aborts Signature

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:

HAETAE

HEAAN CRYPTO LAB

- 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: $U(\bullet)$

- Most compact choice [**D**FPS22]
- Easier rejection probability than Gaussians

Use of bimodal setting: more compact [**D**FPS22]

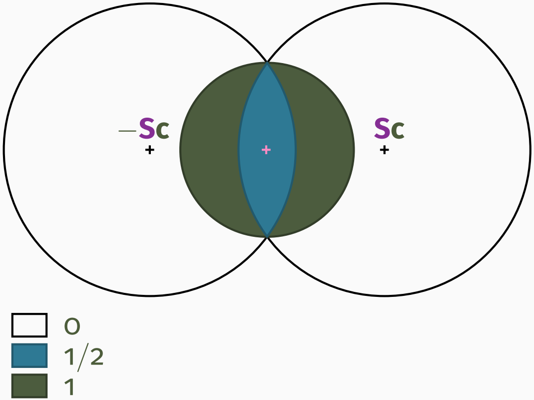
Switching to Bimodal Distributions

$\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ or $\mathbf{z} = \mathbf{y} - \mathbf{S}\mathbf{c}$ (with probability $1/2$ each)

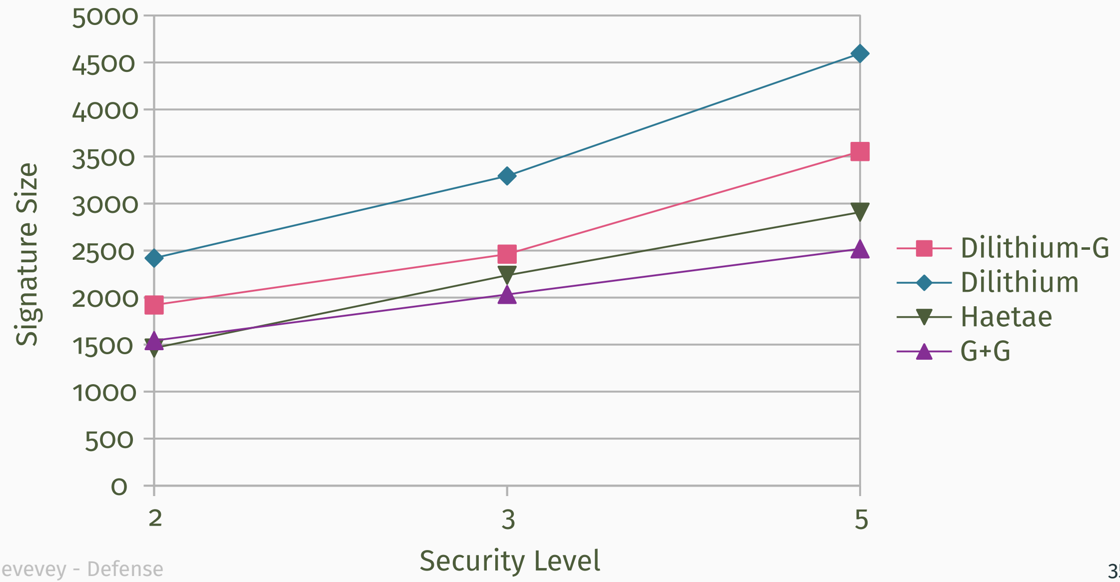
Switching to Bimodal Distributions

$\mathbf{z} = \mathbf{y} + \mathbf{S}\mathbf{c}$ or $\mathbf{z} = \mathbf{y} - \mathbf{S}\mathbf{c}$ (with probability $1/2$ each)

- Adapt KeyGen
- Work $\bmod 2q$ to have $\mathbf{A}\mathbf{S} = -\mathbf{A}\mathbf{S} \bmod 2q$
- Adapt rejection probability



Sizes for Haetae



Final Comparison

Haetae	G+G
+ Already implemented	+ No rejection sampling
+ No involved operation on secret values	+ Smaller sizes

Publications (1)

- On Rejection Sampling in Lyubashevsky's Signature Scheme
  Asiacrypt'22. With O. Fawzi, A. Passelègue and D. Stehlé

- A Detailed Analysis of Fiat-Shamir with Aborts
  Crypto'23. With P. Fallahpour, A. Passelègue and D. Stehlé

- G+G: A Fiat-Shamir Lattice Signature Based on Convolved Gaussians
  Asiacrypt'23. With A. Passelègue and D. Stehlé

- HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures
  Preprint. With JH. Cheon, H. Choe, T. Güneysu, D. Hong, M. Krausz, G. Land, M. Möller, D. Stehlé and M. Yi

Publications (2)

- On the Integer Polynomial Learning with Errors Problem
  PKC'21. With A. Sakzad, D. Stehlé and R. Steinfeld
- Non-Interactive CCA2-Secure Threshold Cryptosystems: Achieving Adaptive Security in the Standard Model Without Pairings
  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?