

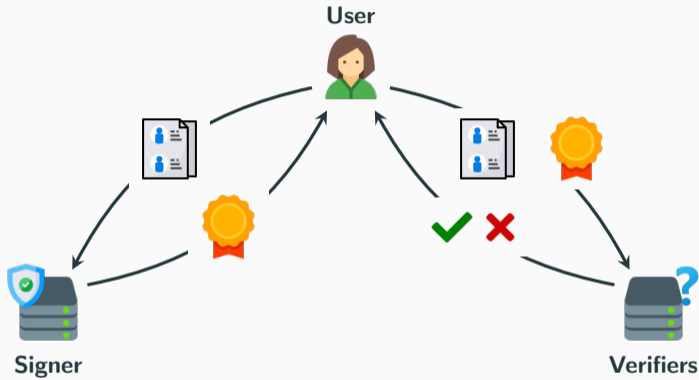
Improved Lattice Blind Signatures from Recycled Entropy

Crypto'25 - August 20th 2025

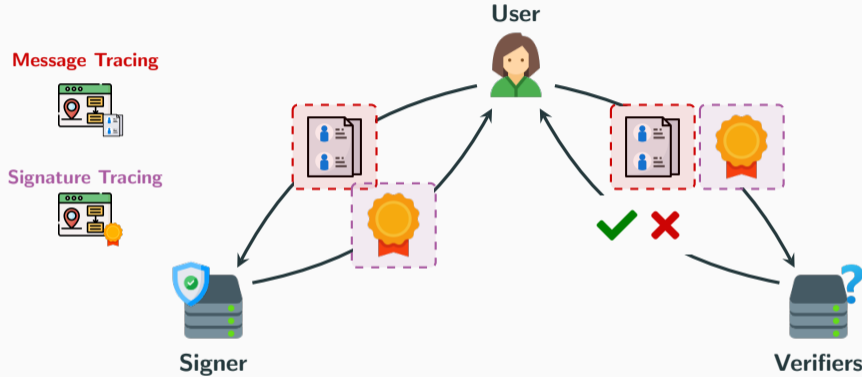
Corentin Jeudy¹, Olivier Sanders¹

¹ Orange, Applied Crypto Group





Digital Signatures



Message Tracing: Signer can trace user based on signed message

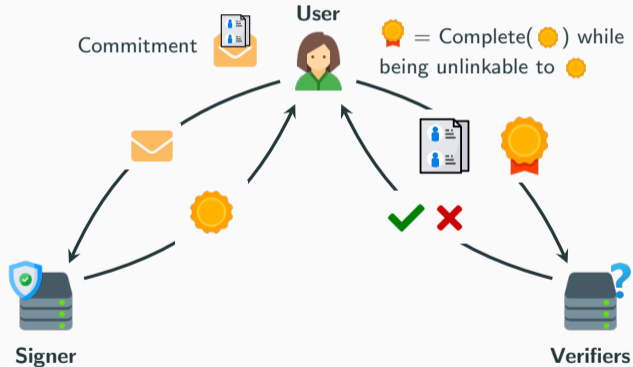
Signature Tracing: Signer can trace user based on emitted signatures

Blind Signatures in a Nutshell

Requirements: **Blindness** (a signature can't be traced back to its issuance), and
One-More Unforgeability (can't produce more valid blind signatures than was lawfully emitted).

Blind Signatures in a Nutshell

Requirements: **Blindness** (a signature can't be traced back to its issuance), and **One-More Unforgeability** (can't produce more valid blind signatures than was lawfully emitted).



Project Tourbillon: "Further research is needed to ready [PQ eCash] for [...] operational usage."
⇒ requires improvement on Post-Quantum Blind Signatures 🔗

ISIS _{m, d, q, β}

Given $(\mathbf{A}, \mathbf{u}) \leftarrow U(R_q^{d \times m+1})$, find $\mathbf{x} \in R^m$ such that $\mathbf{Ax} = \mathbf{u} \bmod q$, $\|\mathbf{x}\| \leq \beta$.

When $\mathbf{u} = \mathbf{0}$, we ask $\mathbf{x} \neq \mathbf{0}$.

Decision: Distinguish $\mathbf{Ax} \bmod q$ for a random short \mathbf{x} from a random $\mathbf{u} \rightarrow \text{LWE}$.

ISIS _{m, d, q, β}

Given $(\mathbf{A}, \mathbf{u}) \leftarrow U(R_q^{d \times m+1})$, find $\mathbf{x} \in R^m$ such that $\mathbf{Ax} = \mathbf{u} \bmod q$, $\|\mathbf{x}\| \leq \beta$.

When $\mathbf{u} = \mathbf{0}$, we ask $\mathbf{x} \neq \mathbf{0}$.

Decision: Distinguish $\mathbf{Ax} \bmod q$ for a random short \mathbf{x} from a random $\mathbf{u} \rightarrow \text{LWE}$.

Gadget-based trapdoors [MP12]¹ lead to signatures that smoothly interact with NIZKs

[MP12]: Matrices of the form

$$\mathbf{A}_t = [\mathbf{A} \mid t\mathbf{G} - \mathbf{AR}]$$

with $\mathbf{A} = [\mathbf{I} \mid \mathbf{A}']$, \mathbf{A}' uniform, t tag, \mathbf{R} trapdoor, $\mathbf{G} = [b^0 \mathbf{I} \mid \dots \mid b^{k-1} \mathbf{I}]$ public gadget for $k = \log_b q$.

Sampler: Allows to sample random short \mathbf{v} s.t. $\mathbf{A}_t \mathbf{v} = \mathbf{u} \bmod q$ for any \mathbf{u} , without leaking \mathbf{R} .

\rightarrow notation: $\mathbf{v} = \text{SampPre}(\mathbf{R}, \mathbf{A}_t, \mathbf{u})$



¹Micciancio, Peikert. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. Eurocrypt 2012

We use the [LNP22]² lattice zero-knowledge proof framework.



- ② Proves quadratic equations modulo q , e.g.,
$$[\mathbf{A} | t\mathbf{G} - \mathbf{B}]\mathbf{w} = \mathbf{u} \bmod q, \quad \text{or} \quad \langle \mathbf{w}, \mathbf{w} \rangle = B^2 \bmod q \quad (\text{i.e., } \|\mathbf{w}\|_2^2 = B^2 \bmod q)$$
- ||·|| Proves ℓ_2 norms exactly by lifting over \mathbb{Z} : $\langle \mathbf{w}, \mathbf{w} \rangle = B^2 \bmod q \implies \|\mathbf{w}\|_2 = B$ if $q > \Omega(B^2)$

²Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022

We use the [LNP22]² lattice zero-knowledge proof framework.



-  Proves quadratic equations modulo q , e.g.,
$$[\mathbf{A} | \mathbf{t}\mathbf{G} - \mathbf{B}]\mathbf{w} = \mathbf{u} \bmod q, \quad \text{or} \quad \langle \mathbf{w}, \mathbf{w} \rangle = B^2 \bmod q \quad (\text{i.e., } \|\mathbf{w}\|_2^2 = B^2 \bmod q)$$
-  Proves ℓ_2 norms exactly by lifting over \mathbb{Z} : $\langle \mathbf{w}, \mathbf{w} \rangle = B^2 \bmod q \implies \|\mathbf{w}\|_2 = B$ if $q > \Omega(B^2)$

Proof π contains many elements including



-  Masked opening of the witness $\mathbf{z} = \mathbf{y} + c\mathbf{w}$
→ Size depends linearly on dimension of \mathbf{w}
-  Commitments, all-but-one-coefficient masks which are uniform-looking modulo q
→ Size depends on how big q is

²Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022

We use the [LNP22]² lattice zero-knowledge proof framework.

-  Proves quadratic equations modulo q , e.g.,
$$[\mathbf{A}|\mathbf{t}\mathbf{G} - \mathbf{B}]\mathbf{w} = \mathbf{u} \bmod q, \quad \text{or} \quad \langle \mathbf{w}, \mathbf{w} \rangle = B^2 \bmod q \quad (\text{i.e., } \|\mathbf{w}\|_2^2 = B^2 \bmod q)$$
-  Proves ℓ_2 norms exactly by lifting over \mathbb{Z} : $\langle \mathbf{w}, \mathbf{w} \rangle = B^2 \bmod q \implies \|\mathbf{w}\|_2 = B$ if $q > \Omega(B^2)$

Proof π contains many elements including

-  Masked opening of the witness $\mathbf{z} = \mathbf{y} + c\mathbf{w}$
→ Size depends linearly on dimension of \mathbf{w}
-  Commitments, all-but-one-coefficient masks which are uniform-looking modulo q
→ Size depends on how big q is

Smaller dimension \implies Smaller proof size

Smaller modulus \implies Smaller proof size

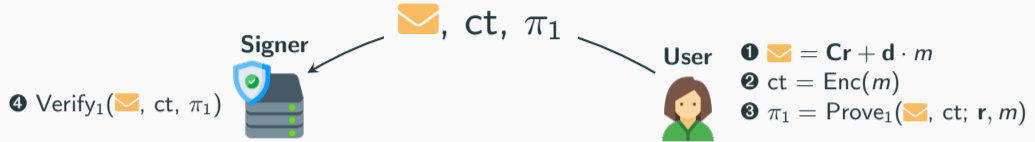
²Lyubashevsky, Nguyen, Plançon. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. Crypto 2022

Constructing Blind Signatures from Gadgets



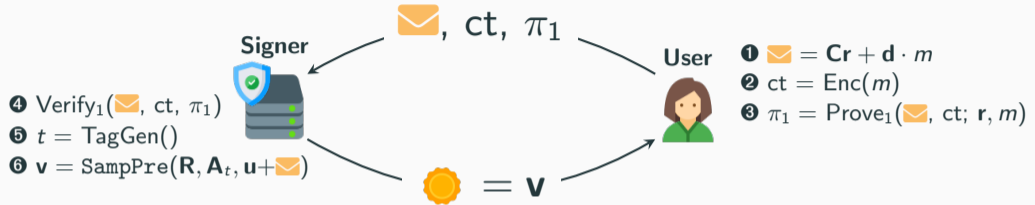
Step ③ proves the commitment and encryption-to-the-sky are well-formed.

Constructing Blind Signatures from Gadgets



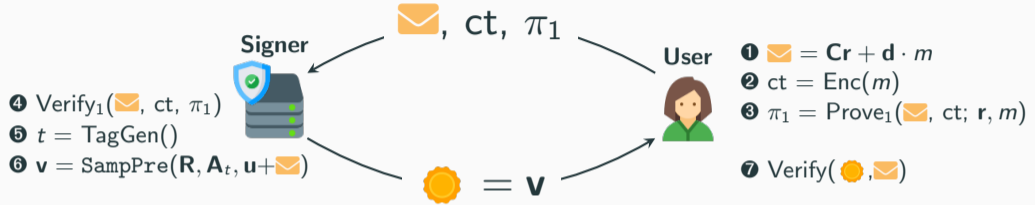
Step 3 proves the commitment and encryption-to-the-sky are well-formed.

Constructing Blind Signatures from Gadgets



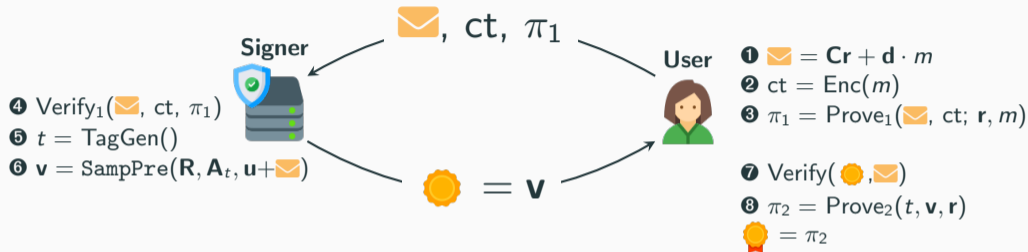
Step ③ proves the commitment and encryption-to-the-sky are well-formed.

Constructing Blind Signatures from Gadgets



Step ③ proves the commitment and encryption-to-the-sky are well-formed.

Constructing Blind Signatures from Gadgets



Step ③ proves the commitment and encryption-to-the-sky are well-formed.

Step ⑧ proves the partial signature verification equation while hiding (t, \mathbf{v}, r) but revealing m :

$$\mathbf{A}_t \mathbf{v} - \mathbf{C}r = \mathbf{u} + d \cdot m \bmod q$$

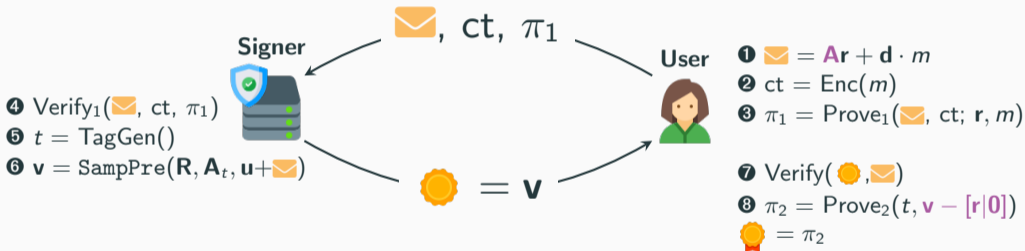
$$t \in \mathcal{T}, \quad \|(\mathbf{v}, r)\|_2 \text{ small}$$

Reducing the Witness Dimension

- ✗ Witness in π_2 includes the randomness \mathbf{r} , increasing the proof size.
- 💡 We can reuse $\mathbf{A} = [\mathbf{I}_d | \mathbf{A}']$ from \mathbf{A}_t with uniform \mathbf{A}' to keep hiding commitment, but merge \mathbf{r} to the top part of \mathbf{v} .

Reducing the Witness Dimension

- ❌ Witness in π_2 includes the randomness \mathbf{r} , increasing the proof size.
- 💡 We can reuse $\mathbf{A} = [\mathbf{I}_d | \mathbf{A}']$ from \mathbf{A}_t with uniform \mathbf{A}' to keep hiding commitment, but merge \mathbf{r} to the top part of \mathbf{v} .



Vector $\mathbf{w} = \mathbf{v} - [\mathbf{r}|0]$ slightly larger in norm, but reduces witness dimension.
Equation becomes

$$\mathbf{A}_t \mathbf{w} = \mathbf{u} + \mathbf{d} \cdot m$$

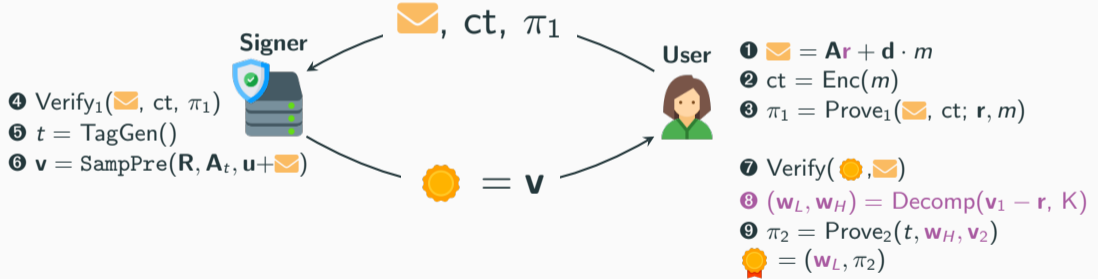
Randomness Injection for Smaller Blind Signature

- ❓ \mathbf{r} is small (ternary). Can we inject more randomness without increasing the norm of \mathbf{w} too much?
- 💡 Compute $\mathbf{v} = \mathbf{A}(\mathbf{K}\mathbf{r}_{hid} + \mathbf{r}_{mask}) + \mathbf{d} \cdot m$, where \mathbf{r}_{hid} is small (ternary) to keep a hiding commitment, and \mathbf{r}_{mask} **as large as possible to mask the top of \mathbf{v}** in the end. Base K lifts \mathbf{r}_{hid} to the high bits of $\mathbf{r} = \mathbf{K}\mathbf{r}_{hid} + \mathbf{r}_{mask}$.

Randomness Injection for Smaller Blind Signature

❓ \mathbf{r} is small (ternary). Can we inject more randomness without increasing the norm of \mathbf{w} too much?

💡 Compute $\text{📧} = \mathbf{A}(\mathbf{K}\mathbf{r}_{hid} + \mathbf{r}_{mask}) + \mathbf{d} \cdot m$, where \mathbf{r}_{hid} is small (ternary) to keep a hiding commitment, and \mathbf{r}_{mask} as large as possible to mask the top of \mathbf{v} in the end. Base K lifts \mathbf{r}_{hid} to the high bits of $\mathbf{r} = \mathbf{K}\mathbf{r}_{hid} + \mathbf{r}_{mask}$.



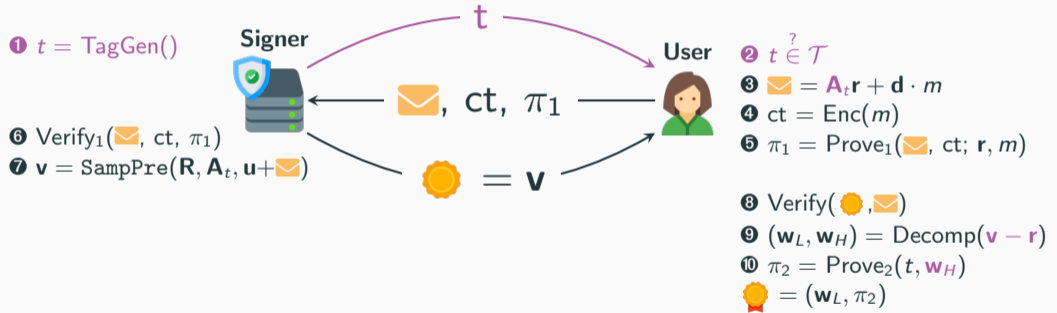
$\mathbf{w}_L = \text{Low}(\mathbf{v}_1, K) + \mathbf{r}_{mask} \bmod K$, which can be revealed if \mathbf{r}_{mask} uniform modulo K .
 Reduces witness norm as $\|\mathbf{w}_H\|_2 \approx \|\mathbf{w}\|_2 / K$. Reduces the proof modulus and thus proof size.

💡 We can push the idea further to hide \mathbf{v}_2 as well. But the user needs to know the tag t that will be used, making our scheme 3-round.



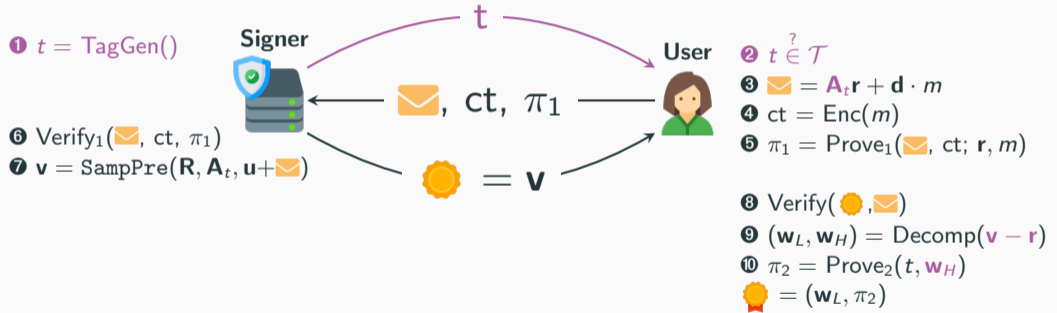
Making it 3-Round for Smaller Sizes

💡 We can push the idea further to hide \mathbf{v}_2 as well. But the user needs to know the tag t that will be used, making our scheme 3-round.



Making it 3-Round for Smaller Sizes

💡 We can push the idea further to hide \mathbf{v}_2 as well. But the user needs to know the tag t that will be used, making our scheme 3-round.



Albeit 3-round, we are not subject to attacks on Schnorr-like 3-round blind signatures.

Performance Comparison

	Assumptions	Round	iss. NIZK	transcript	bsig
[AKSY22] ³	Std. + One-More-ISIS	2	-	1.37 KB	45.19 KB
[dPK22] ⁴	Std.	2	Algebraic	932 KB	102.6 KB
[BLNS23] ⁵	Std.	2	General	60 KB	22 KB
Ours	Std.	3	Algebraic	59.63 KB	41.12 KB

Further optimization: Replace gadget sampler with recent truncated gadget sampler of [JS24]⁶

→ No impact on security

→ Smaller dimensional witness gives: |transcript| \approx 53.21 KB, and |bsig| \approx 36.28 KB.

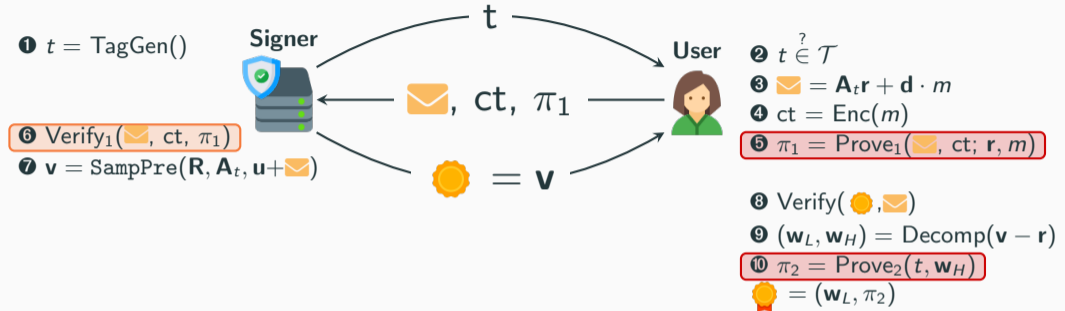
²Agrawal, Kirshanova, Stehlé, Yadav. Practical, Round-Optimal Lattice-Based Blind Signatures. CCS 2022

³del Pino, Katsumata. A New Framework for More Efficient Round-Optimal Lattice-Based (Partially) Blind Signature via Trapdoor Sampling. Crypto 2022

⁴Beullens, Lyubashevsky, Nguyen, Seiler. Lattice-Based Blind Signatures: Short, Efficient, and Round-Optimal. CCS 2023

⁶Judy, Sanders. Worst-Case Lattice Sampler with Truncated Gadgets and Applications. ePrint 2024/1952

Implementation Performance



Step	1+2	3+4	5	6	7	8	9	10	Total
Time (ms)	0	3	500	123	74	2	0	392	1094 ms

can be offline

Verification: 91 ms (verification of π_2 (≈ 90 ms) and that \mathbf{w}_L is in the correct interval (≈ 1 ms))



Full blind signature generation ≈ 1 second (non-optimized PoC implementation)



A new **Lattice Blind Signature**

- Based on standard post-quantum assumptions (M-SIS, M-LWE)
- Efficient issuance based only on algebraic proofs (no general-purpose NIZKs)
- Competitive sizes due to our entropy recycling technique
- 3-round but first round does not involve maintaining secret data (so it's more 2-ish)



Perspectives



More efficient proof systems for lattice relations?



Optimized implementation (dedicated backend, parallelization, parameter selection)



Implement using LaZer library [LSS24]⁷

⁷Lyubashevsky, Seiler, Steuer. The LaZer Library: Lattice-Based Zero-Knowledge and Succinct Proofs for Quantum-Safe Privacy. CCS 2024



A new **Lattice Blind Signature**

- Based on standard post-quantum assumptions (M-SIS, M-LWE)
- Efficient issuance based only on algebraic proofs (no general-purpose NIZKs)
- Competitive sizes due to our entropy recycling technique
- 3-round but first round does not involve maintaining secret data (so it's more 2-ish)



Perspectives



More efficient proof systems for lattice relations?




Optimized implementation (dedicated backend, parallelization, parameter selection)






Implement using LaZer library [LSS24]⁷

Thank You!

⁷Lyubashevsky, Seiler, Steuer. The LaZer Library: Lattice-Based Zero-Knowledge and Succinct Proofs for Quantum-Safe Privacy. CCS 2024

-  S. Agrawal, E. Kirshanova, D. Stehlé, and A. Yadav.
Practical, Round-Optimal Lattice-Based Blind Signatures.
In CCS, 2022.
-  J. Bootle, V. Lyubashevsky, N. K. Nguyen, and A. Sorniotti.
A Framework for Practical Anonymous Credentials from Lattices.
In CRYPTO, 2023.
-  R. del Pino and S. Katsumata.
A New Framework for More Efficient Round-Optimal Lattice-Based (Partially) Blind Signature via Trapdoor Sampling.
In CRYPTO, 2022.
-  C. Jeudy and O. Sanders.
Worst-Case Lattice Sampler with Truncated Gadgets and Applications.
IACR Cryptol. ePrint Arch., page 1952, 2024.

-  V. Lyubashevsky, N. K. Nguyen, and M. Plançon.
Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General.
CRYPTO, 2022.
-  V. Lyubashevsky, G. Seiler, and P. Steuer.
The LaZer Library: Lattice-Based Zero Knowledge and Succinct Proofs for Quantum-Safe Privacy.
In CCS, 2024.
-  D. Micciancio and C. Peikert.
Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller.
In EUROCRYPT, 2012.

