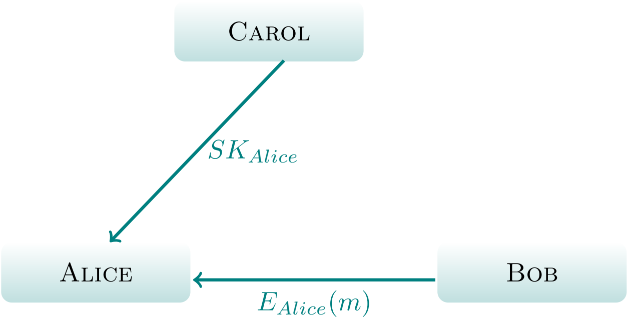
Efficient Identity-Based Encryption using NTRU Lattices

Léo Ducas, Vadim Lyubashevsky and Thomas Prest

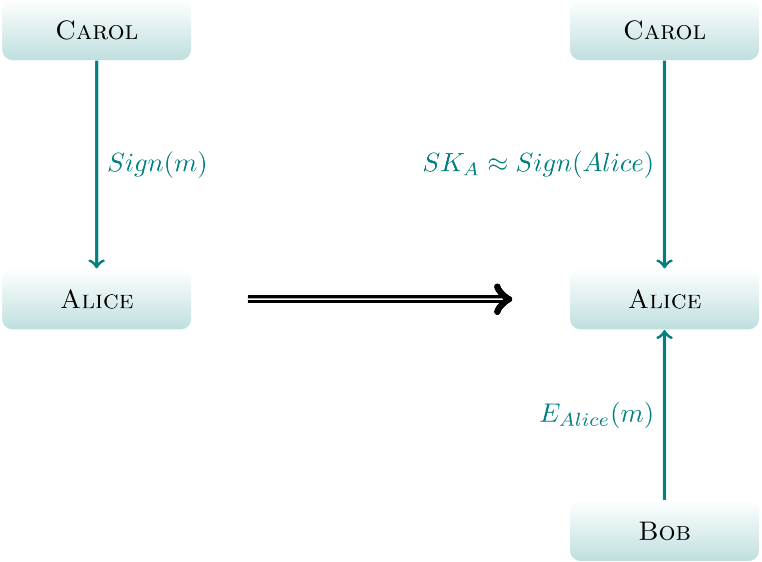
December 10, 2014

Identity-based encryption (IBE)

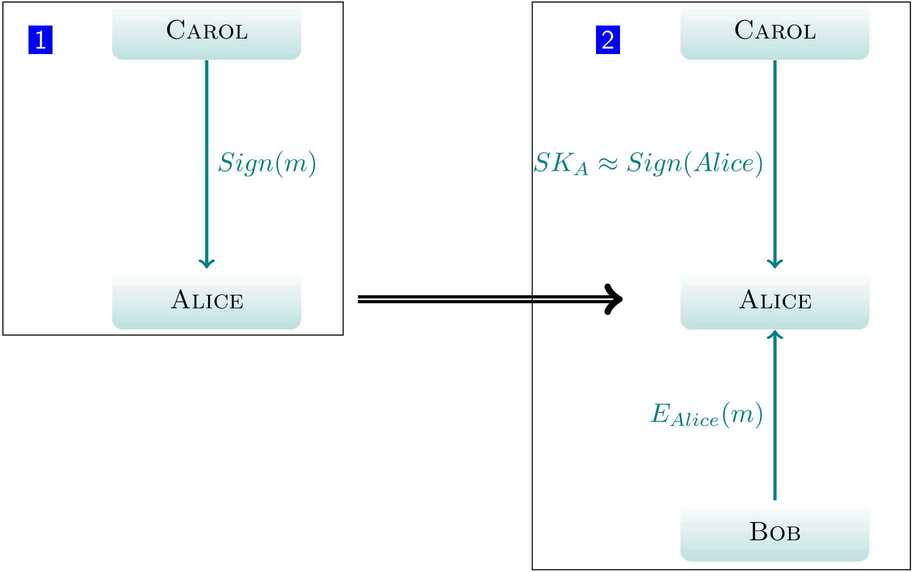


An Identity-based encryption scheme

[GPV]: Signature scheme $\implies$ IBE



[GPV]: Signature scheme $\Longrightarrow$ IBE



1 Gaussian Sampling and KL-Divergence

2 An IBE scheme over NTRU lattices

A signature scheme: GGH/NTRUSign [GGH, HHP$^+$]

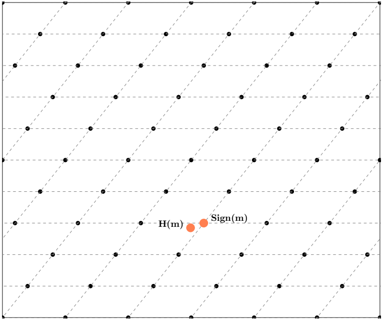


Figure : Only one possible signature

How to sign m with a short basis $\mathbf{B}$ of a lattice $\Lambda \supset q\mathbb{Z}^n$:

1. $H(m) \xleftarrow{\$} \mathbb{Z}_q^n$
2. $Sign(m) \leftarrow$ a point $\mathbf{v} \in \Lambda$ s.t. $\|\mathbf{v} - H(m)\|$ is small

What GGH/NTRUSign does

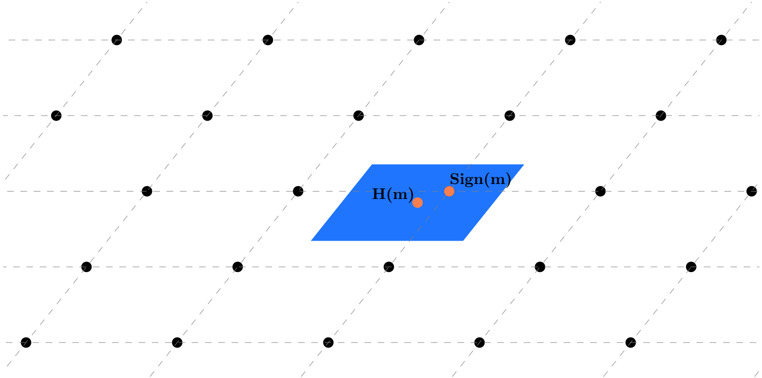


Figure : Only one possible signature

1. $H(m) \xleftarrow{\$} \mathbb{Z}_q^n$
2. Let  be the fundamental parallelepiped of $\mathbf{B}$ centered over $H(m)$
3. $Sign(m) \leftarrow$  $\cap \Lambda$

Information leakage in GGH/NTRUSign

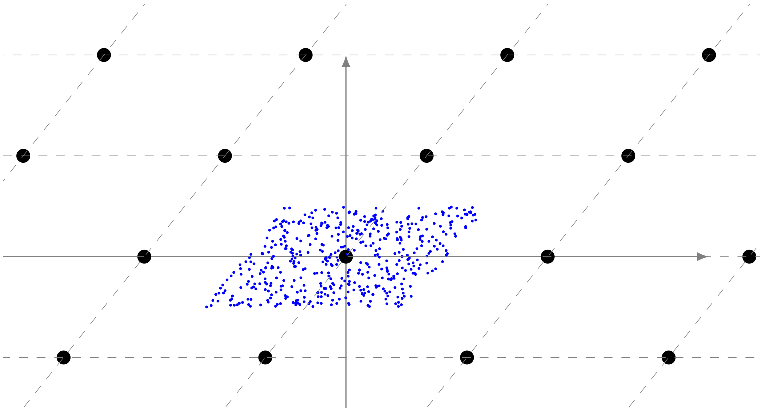


Figure : Distribution of the $H(m_i) - sign(m_i)$

- One can recover the short base [NR]
- Countermeasures are ineffective [DNb]

Solution: randomize the signature! [GPV]

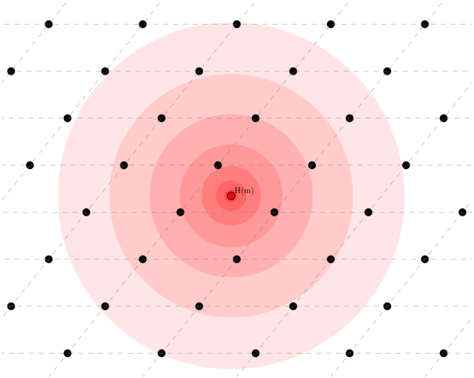


Figure : Gaussian Sampling: several possible signatures

- No more information leakage [GPV]

Solution: randomize the signature! [GPV]

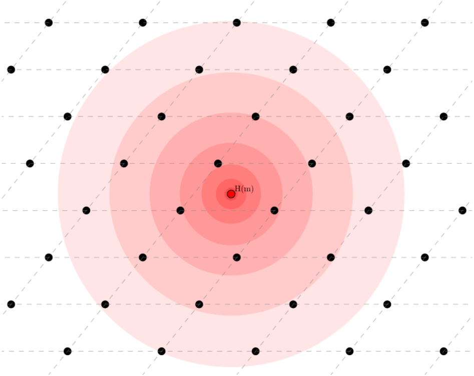


Figure : Gaussian Sampling: several possible signatures

- No more information leakage [GPV]
- The larger the standard deviation σ, the looser the security
- If σ is too small, the simulated gaussian leaks the basis again

Distinguishing two distributions

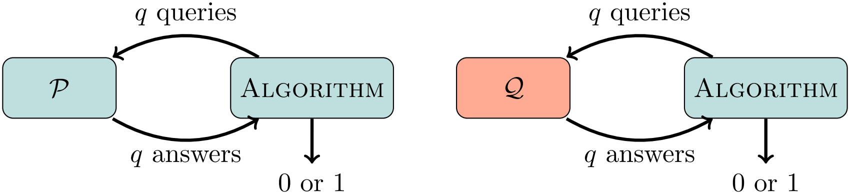


Figure : Are $\mathcal{P}$ and $\mathcal{Q}$ indistinguishable?

In our case, $\mathcal{P}$ = perfect Gaussian, $\mathcal{Q}$ = simulated Gaussian from [GPV]

Distinguishing two distributions

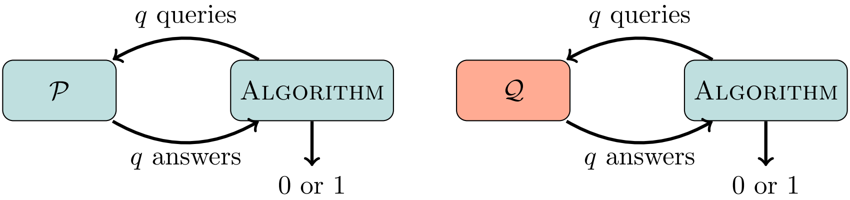


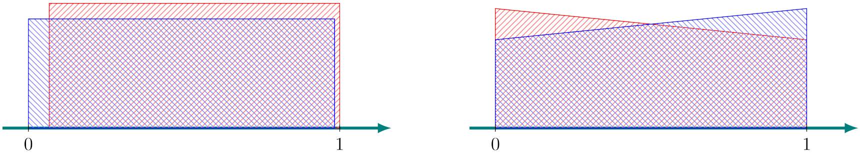
Figure : Are $\mathcal{P}$ and $\mathcal{Q}$ indistinguishable?
In our case, $\mathcal{P}$ = perfect Gaussian, $\mathcal{Q}$ = simulated Gaussian from [GPV]

Let the algorithm $\mathcal{A}^{\mathcal{P}}$ do at most q queries to $\mathcal{P}$ and output a bit. Let x (resp. y) be the probability that $\mathcal{A}^{\mathcal{P}}$ (resp. $\mathcal{A}^{\mathcal{Q}}$) outputs 1.

- If $SD(\mathcal{P}, \mathcal{Q}) \leqslant \delta$, then $|x - y| \leqslant q\delta$
- If $D_{KL}(\mathcal{P} \| \mathcal{Q}) \leqslant \delta$, then $|x - y| \leqslant \frac{1}{2}\sqrt{q\delta}$ [PDG]

$\Rightarrow$ We can replace Statistical Distance with KL-Divergence.

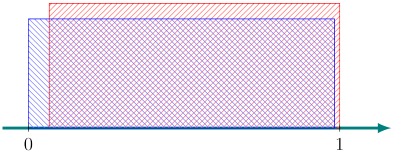
Statistical Distance or KL-Divergence?



$\Delta(\mathcal{P}, \mathcal{Q}) < D_{KL}(\mathcal{P} \| \mathcal{Q})$ $\qquad$ $\Delta(\mathcal{P}, \mathcal{Q}) > D_{KL}(\mathcal{P} \| \mathcal{Q})$

Figure : The "best" measure depends on the distributions

Statistical Distance or KL-Divergence?



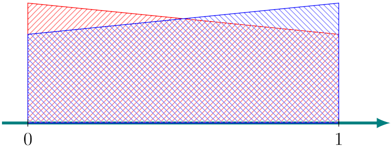


Figure : The "best" measure depends on the distributions

Let $\mathcal{P}$ the perfect Gaussian of st. dev. σ, $\mathcal{Q}$ the output of the Gaussian Sampler.

[GPV, DNa] $\rightarrow$ If $\sigma \geqslant \sqrt{\frac{\lambda \ln 2}{2\pi^2}} \cdot \|\tilde{\mathbf{B}}\|$, then $SD(\mathcal{P}, \mathcal{Q}) \leqslant 2^{-\lambda}$

Our results $\rightarrow$ If $\sigma \geqslant \frac{1}{\sqrt{2}} \sqrt{\frac{\lambda \ln 2}{2\pi^2}} \cdot \|\tilde{\mathbf{B}}\|$, then $D_{KL}(\mathcal{P} \| \mathcal{Q}) \leqslant 2^{-\lambda}$

Practical impact of KL-Divergence

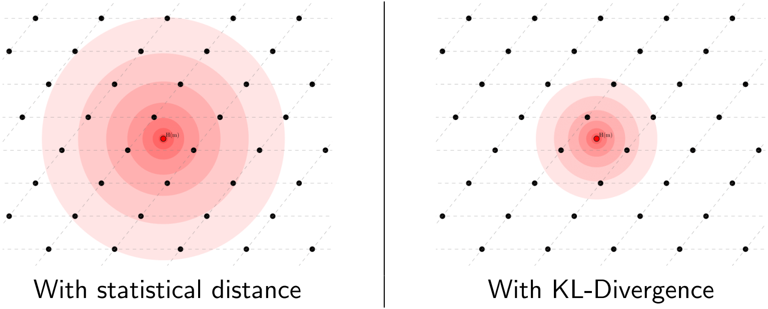


Figure : Sizes of the signatures

- Smaller signatures
- Gain for free!

From a signature scheme to an IBE scheme

Keygen:

$$SK \leftarrow \begin{bmatrix} g & G \\ -f & -F \end{bmatrix}, PK \leftarrow h$$

Where $f * G - g * F = q$ and $h = g * f^{-1} \mod q$ (NTRU basis)
Sign:

$$t \leftarrow H(m)$$

$$Sign(m) = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \text{s.t. } s_1 + s_2 * h = t$$

From a signature scheme to an IBE scheme

Setup:

$$MSK \leftarrow \begin{bmatrix} g & G \\ -f & -F \end{bmatrix}, MPK \leftarrow h$$

Where $f * G - g * F = q$ and $h = g * f^{-1} \mod q$ (NTRU basis)

Extract:

$$t \leftarrow H(id)$$

$$SK_{id} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \text{s.t. } s_1 + s_2 * h = t$$

From a signature scheme to an IBE scheme

Setup:

$$MSK \leftarrow \begin{bmatrix} g & G \\ -f & -F \end{bmatrix}, MPK \leftarrow h$$

Where $f * G - g * F = q$ and $h = g * f^{-1} \mod q$ (NTRU basis)
Extract:

$$t \leftarrow H(id)$$

$$SK_{id} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \text{s.t. } s_1 + s_2 * h = t$$

[LPR] Encrypt:

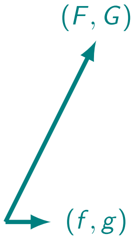
$$\begin{aligned} u &\leftarrow r * h + e_1 \\ v &\leftarrow r * t + e_2 + \left\lfloor \frac{q}{2} \right\rfloor \cdot b \end{aligned}$$

[LPR] Decrypt:

$$v - u * s_2 = \left\lfloor \frac{q}{2} \right\rfloor \cdot b + \underbrace{e_2 + r * s_1 - e_1 * s_2}_{\|\|_\infty \text{ small}}$$

Optimal NTRU bases

Which NTRU lattices should we use for signature (or IBE)?

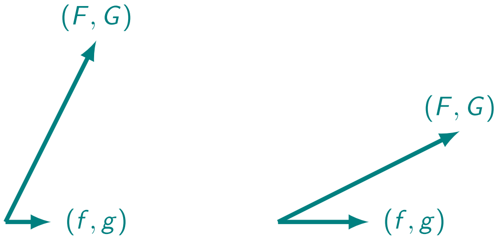


NTRUEncrypt

$\|(f, g)\|$ minimal

Optimal NTRU bases

Which NTRU lattices should we use for signature (or IBE)?

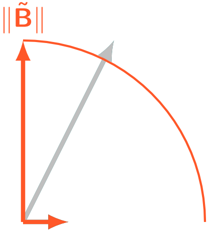


NTRUEncrypt	Our paper
$\|(f,g)\|$ minimal	$\|(f,g)\| \approx 1.17\sqrt{q}$

Optimal NTRU bases

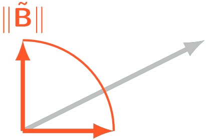
Which NTRU lattices should we use for signature (or IBE)?

$$\sigma \geqslant \frac{1}{\sqrt{2}} \sqrt{\frac{\lambda \ln 2}{2\pi^2}} \cdot \|\tilde{\mathbf{B}}\|$$



NTRUEncrypt

$\|(f,g)\|$ minimal



Our paper

$\|(f,g)\| \approx 1.17\sqrt{q}$

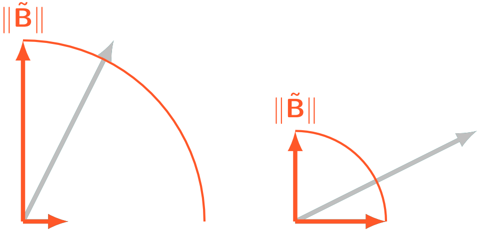
$\|\tilde{\mathbf{B}}\| = \max_{\tilde{\mathbf{b}}_i \in \tilde{\mathbf{B}}} \|\tilde{\mathbf{b}}_i\|$, where $\tilde{\mathbf{B}}$ is the Gram-Schmidt orthogonalization of $\mathbf{B}$

For NTRU lattices, $\|\tilde{\mathbf{B}}\| \approx \max(\|(f,g)\|, \frac{(1.17)^2 q}{\|(f,g)\|})$

Optimal NTRU bases

Which NTRU lattices should we use for signature (or IBE)?

$$\sigma \geqslant \frac{1}{\sqrt{2}}\sqrt{\frac{\lambda \ln 2}{2\pi^2}} \cdot \|\tilde{\mathbf{B}}\|$$



NTRUEncrypt	Our paper
$\|(f,g)\|$ minimal	$\|(f,g)\| \approx 1.17\sqrt{q}$

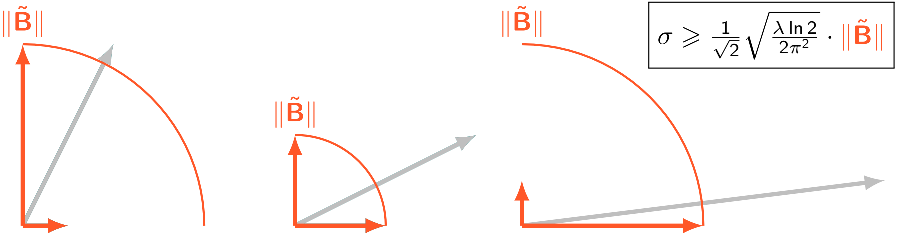
$\|\tilde{\mathbf{B}}\| = \max_{\tilde{\mathbf{b}}_i \in \tilde{\mathbf{B}}} \|\tilde{\mathbf{b}}_i\|$, where $\tilde{\mathbf{B}}$ is the Gram-Schmidt orthogonalization of $\mathbf{B}$

For NTRU lattices, $\|\tilde{\mathbf{B}}\| \approx \max(\|(f,g)\|, \frac{(1.17)^2 q}{\|(f,g)\|})$

$\Rightarrow \|\tilde{\mathbf{B}}\|$ is minimal for $\|(f,g)\| \approx 1.17\sqrt{q}$

Optimal NTRU bases

Which NTRU lattices should we use for signature (or IBE)?



$$\sigma \geqslant \frac{1}{\sqrt{2}} \sqrt{\frac{\lambda \ln 2}{2\pi^2}} \cdot \|\tilde{\mathbf{B}}\|$$

NTRUEncrypt	Our paper	[SS]
$\|(f,g)\|$ minimal	$\|(f,g)\| \approx 1.17\sqrt{q}$	$\|(f,g)\| \geqslant 2n\sqrt{q}$

$\|\tilde{\mathbf{B}}\| = \max_{\tilde{\mathbf{b}}_i \in \tilde{\mathbf{B}}} \|\tilde{\mathbf{b}}_i\|$, where $\tilde{\mathbf{B}}$ is the Gram-Schmidt orthogonalization of $\mathbf{B}$

For NTRU lattices, $\|\tilde{\mathbf{B}}\| \approx \max(\|(f,g)\|, \frac{(1.17)^2 q}{\|(f,g)\|})$

$\Rightarrow \|\tilde{\mathbf{B}}\|$ is minimal for $\|(f,g)\| \approx 1.17\sqrt{q}$

KL-Divergence + optimal NTRU bases

Let $\mathcal{P}$ the perfect Discrete Gaussian, $\mathcal{Q}$ the output of the Gaussian Sampler.

[GPV, DNa] $\rightarrow$ If $\sigma \geqslant \sqrt{\frac{\lambda \ln 2}{2\pi^2}} \cdot \|\tilde{\mathbf{B}}\|$, then $SD(\mathcal{P}, \mathcal{Q}) \leqslant 2^{-\lambda}$

Our results $\rightarrow$ If $\sigma \geqslant \frac{1}{\sqrt{2}} \sqrt{\frac{\lambda \ln 2}{2\pi^2}} \cdot 1.17\sqrt{q}$, then $D_{KL}(\mathcal{P}\|\mathcal{Q}) \leqslant 2^{-\lambda}$

Implementation and comparison with a pairing-based IBE

Scheme	This paper	BF-192
Parameters	$2n = 2048$ $q \approx 2^{27}$	$\log p = 640$ $k \log p = 7680$
User Key	27 kbits	0.62 kbits
Ciphertexts	30 kbits	15 kbits
Extract	**32.7 ms**	**3.3 ms**
Encrypt	**0.033 ms**	**38.7 ms**
Decrypt	**0.012 ms**	**32.7 ms**

Implementation[1] in `C++` with `NFLlib`[2] [ABFK].
Comparison with Boneh-Franklin (implementation by [Gui]) for $\lambda = 192$.

[1] Material: Intel Core i5-3210M 2.5GHz and 6GB RAM
[2] NTT-based Fast Lattice library (only for Encrypt, Decrypt)

Implementation and comparison with a pairing-based IBE

Scheme	**This paper**	**BF-192**
Parameters	$2n = 2048$ $q \approx 2^{27}$	$\log p = 640$ $k \log p = 7680$
User Key	27 kbits	0.62 kbits
Ciphertexts	30 kbits	15 kbits
Extract	**32.7 ms**	**3.3 ms**
Encrypt	**0.033 ms**	**38.7 ms**
Decrypt	**0.012 ms**	**32.7 ms**

For 192 bits of security:

- **Extract:** **10× slower**
- **Encrypt:** **1200× faster**
- **Decrypt:** **2700× faster**

Implementation and comparison with a pairing-based IBE

Scheme	This paper	BF-128
Parameters	$2n = 2048$ $q \approx 2^{27}$	$\log p = 256$ $k \log p = 3072$
User Key	27 kbits	0.25 kbits
Ciphertexts	30 kbits	3 kbits
Extract	**32.7 ms**	**0.52 ms**
Encrypt	**0.033 ms**	**7.21 ms**
Decrypt	**0.012 ms**	**4.78 ms**

192 bits of security for us, 128 for Boneh-Franklin:

- **Extract: 60× slower**
- **Encrypt: 200× faster**
- **Decrypt: 400× faster**

Thank you! Any questions?

- ePrint: http://eprint.iacr.org/2014/794
- Article and slides: http://www.di.ens.fr/~prest/
- Implementation: https://github.com/tprest/Lattice-IBE/
- Contact: lducas[at]eng.ucsd.edu, vadim.lyubashevsky[at]inria.fr, thomas.prest[at]ens.fr

C. Aguilar, J. Barrier, L. Fousse, and M.O. Killijian.
Xpire : Private information retrieval for everyone. *IACR eprint XXX/2014*.

Léo Ducas and Phong Q. Nguyen.
Faster gaussian lattice sampling using lazy floating-point arithmetic. *ASIACRYPT'12*.

Léo Ducas and Phong Q. Nguyen.
Learning a zonotope and more: cryptanalysis of ntrusign countermeasures. *ASIACRYPT'12*.

Oded Goldreich, Shafi Goldwasser, and Shai Halevi.
Public-key cryptosystems from lattice reduction problems. *CRYPTO'97*.

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
Trapdoors for hard lattices and new cryptographic constructions. *STOC'08*.

Aurore Guillevic.
Étude de l'arithmétique des couplages sur les courbes algébriques pour la cryptographie.
PhD thesis.

Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte.
Ntrusign: digital signatures using the ntru lattice. *CT-RSA'03*.

Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
A toolkit for ring-lwe cryptography. *EUROCRYPT'13*.

Phong Q. Nguyen and Oded Regev.
Learning a parallelepiped: cryptanalysis of ggh and ntru signatures. *EUROCRYPT'06*.

Thomas Pöppelmann, Léo Ducas, and Tim Güneysu.
Enhanced lattice-based signatures on reconfigurable hardware. *CHES'14*.

Damien Stehlé and Ron Steinfeld.
Making ntru as secure as worst-case problems over ideal lattices. *EUROCRYPT'11*.