LATTICE-BASED SIGNATURES

PHONG NGUYEN

http://www.di.ens.fr/~pnguyen

October 2024

TODAY

- Lattice Analogues of:
  - Rabin signatures
  - Schnorr signatures
- Identity-based Encryption with Lattices

TODAY

- GGH/NTRU signatures
- Breaking GGH/NTRU signatures
- Rabin's signature with Lattices
- Lattice Identity-based Encryption

- **Signatures from Zero-Knowledge**
  - Schnorr's identification and signature
  - Lyubashevsky's identification and signature

TODAY

- **Trapdoor Signatures**
  - GGH/NTRU signatures
  - Breaking GGH/NTRU signatures
  - Rabin's signature with Lattices
  - Lattice Identity-based Encryption
- **Signatures from Zero-Knowledge**
  - Schnorr's identification and signature
  - Lyubashevsky's identification and signature

TRAPDOOR SIGNATURES

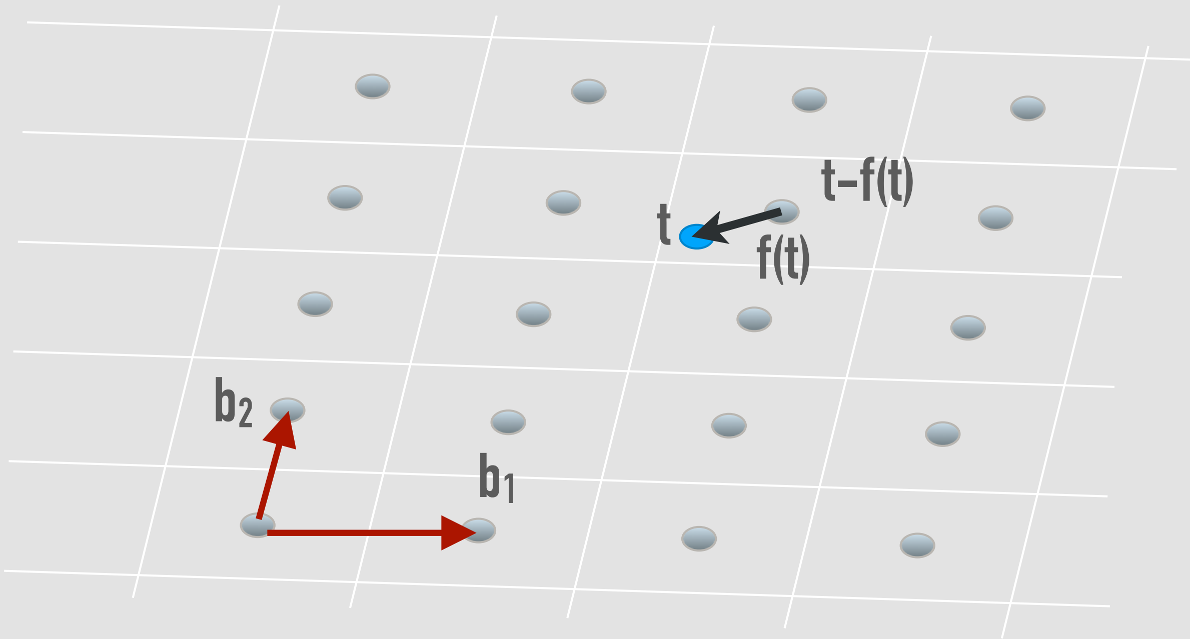
THE EARLY DAYS:
INSECURE LATTICE SIGNATURE

BE LIKE RSA

- We saw how to trapdoor lattice encryption like RSA: L-reduction was the analogue of modular exponentiation.
- RSA encryption is transformed into a signature by swapping encryption and decryption
  - Can we do the same with lattices?
  - Encryption was $f_{\text{public key}}$ and decryption was $f_{\text{secret key}}$

REMEMBER L-REDUCTIONS

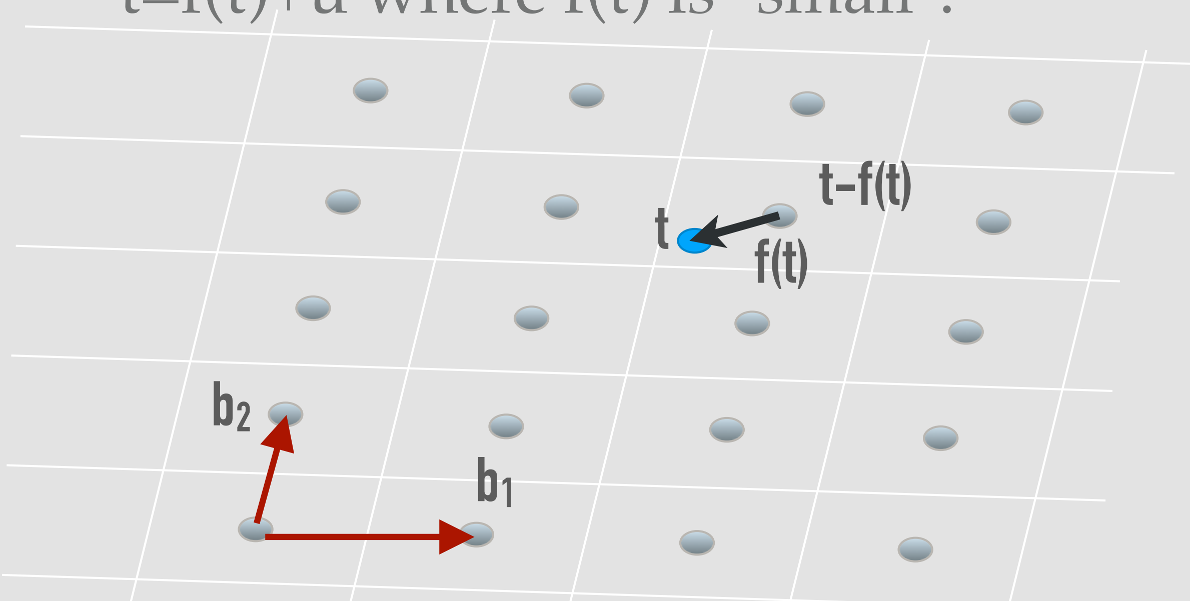
- Any basis provides two L-reductions, thanks to Babai's nearest plane algorithm and rounding-off algorithm.
- We call L-reduction any efficiently computable map $f : \mathbf{Z}^n \rightarrow \mathbf{Z}^n$ s.t. $f(x)-x \in L$ and $f(x)=f(y)$ iff $x-y \in L$.



- Rounding-off
  Choose $f(t)$ in the basis parallelepiped s.t. $t-f(t) \in L$

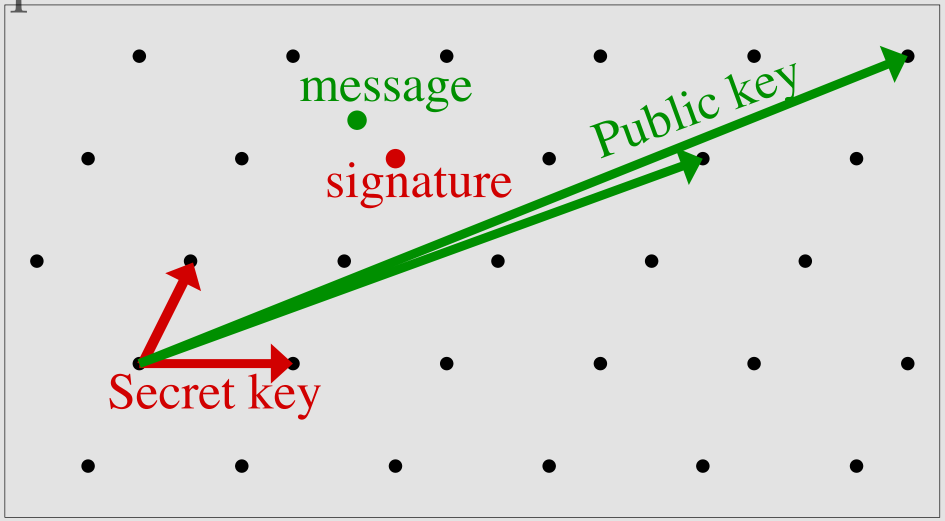
APPROX-CVP FROM L-REDUCTIONS

- L-reductions allow to solve BDD when the noise is sufficiently small.
- L-reductions also allow to approximate CVP: the size of the image dictates the quality of the approximation.
  - If t is the target, t-f(t) is a lattice point u close to t, because t=f(t)+u where f(t) is "small".



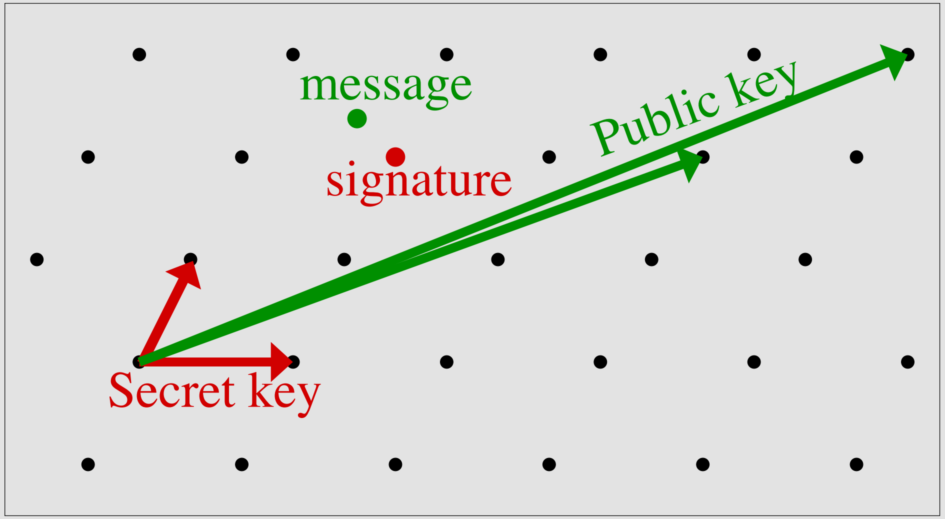
GGH SIGNATURE

- Message = m in $\mathbf{Z}^n$
  - Sign m into f(m), using Babai's approx-CVP.
  - The signature s must be small and m-s must belong to the lattice: here, the signature is the "error", but it can instead be the "lattice point".



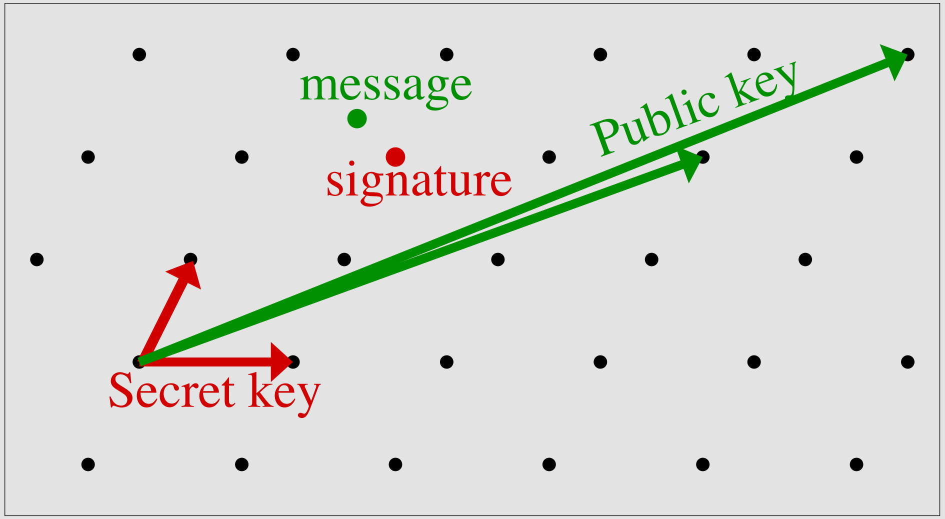
KEY GENERATION IN GGH

- Pick some high-dim lattice:
  - ➤ Secret key = very good basis e.g. qI_n + small coeffs
  - ➤ Public key = very bad basis



KEY GENERATION IN GGH

- Pick some high-dim lattice:
  - Secret key = very good basis e.g. qI_n + small coeffs
  - Public key = very bad basis



- The Secret key allows to approximate CVP within a good factor.

WHAT IS NTRUSIGN?

WHAT IS NTRUSIGN?

- NTRUSign [CT-RSA 2003] was an efficient signature scheme considered by IEEE P1363 standards.

WHAT IS NTRUSIGN?

- NTRUSign [CT-RSA 2003] was an efficient signature scheme considered by IEEE P1363 standards.
- It is a compact instantiation of the GGH signature scheme.

WHAT IS NTRUSIGN?

- NTRUSign [CT-RSA 2003] was an efficient signature scheme considered by IEEE P1363 standards.
- It is a compact instantiation of the GGH signature scheme.

➤ Former (very technical) NTRU signature schemes (2001) did not really correspond to NTRU encryption, and were shown to be totally insecure.

THE NTRUSIGN SECRET BASIS

- Pick some high-dim lattice

$$\begin{bmatrix} f_0 & f_1 & \cdots & f_{n-1} & g_0 & g_1 & \cdots & g_{n-1} \\ f_{n-1} & f_0 & \cdots & f_{n-2} & g_{n-1} & g_0 & \cdots & g_{n-2} \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ f_1 & \cdots & f_{n-1} & f_0 & g_1 & \cdots & g_{n-1} & g_0 \\ F_0 & F_1 & \cdots & F_{n-1} & G_0 & G_1 & \cdots & G_{n-1} \\ F_{n-1} & F_0 & \cdots & F_{n-2} & G_{n-1} & G_0 & \cdots & G_{n-2} \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ F_1 & \cdots & F_{n-1} & F_0 & G_1 & \cdots & G_{n-1} & G_0 \end{bmatrix} \qquad n = 251$$

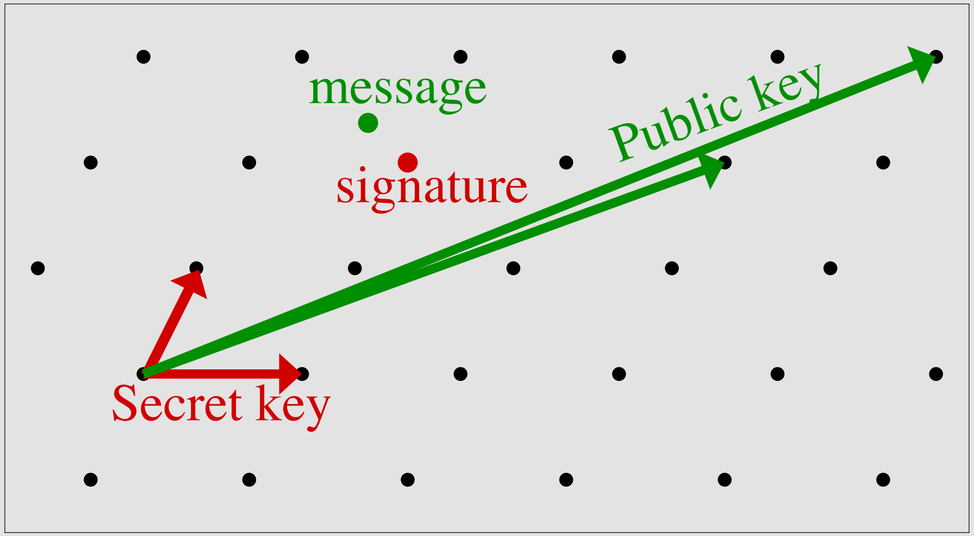
SECURITY OF GGH/NTRU SIGNATURES

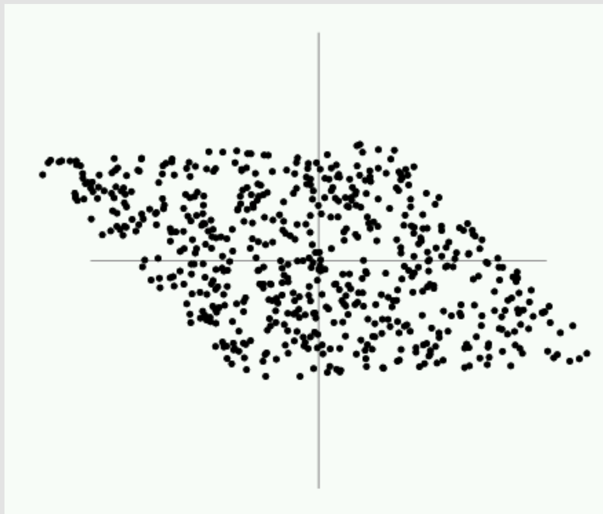
- GGH signatures leak information on the secret key [GentrySzzydlo02]: potential attack in [Szydlo03].
- [NguyenRegev06]: an efficient key-recovery attack.
- The analogues of GGH-encryption challenges have been solved.
- Half of NTRUSign parameter sets have been attacked (400 signatures).

THE ATTACK:
HOW TO LEARN A PARALLELEPIPED

LEARNING A PARALLELEPIPED FROM (MESSAGES,SIGNATURES)

- Each difference message-signature lies in the parallelepiped spanned by the secret basis. Likely to have uniform distribution over the secret parallelepiped.

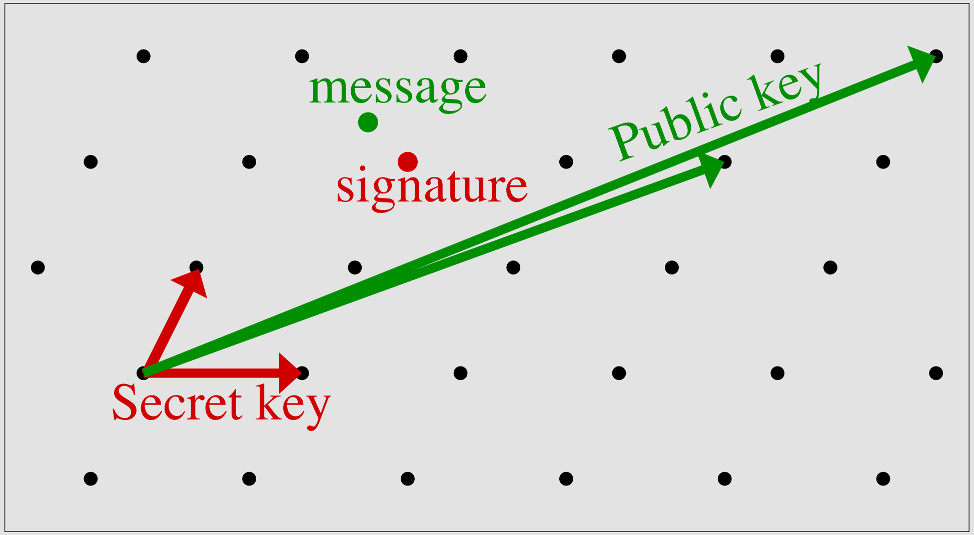


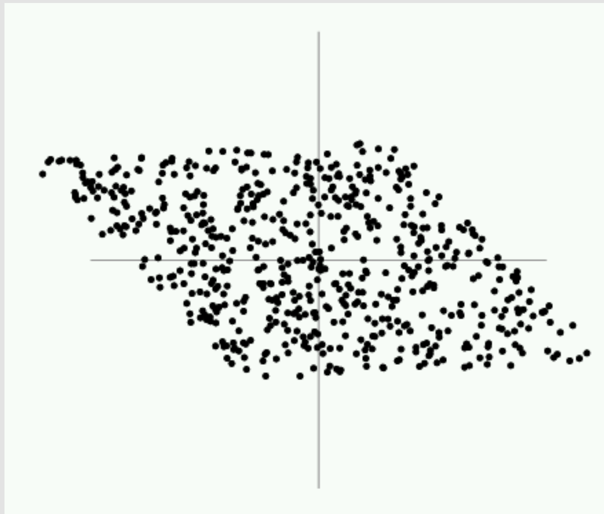


LEARNING A PARALLELEPIPED FROM (MESSAGES,SIGNATURES)

- Each difference message-signature lies in the parallelepiped spanned by the secret basis. Likely to have uniform distribution over the secret parallelepiped.

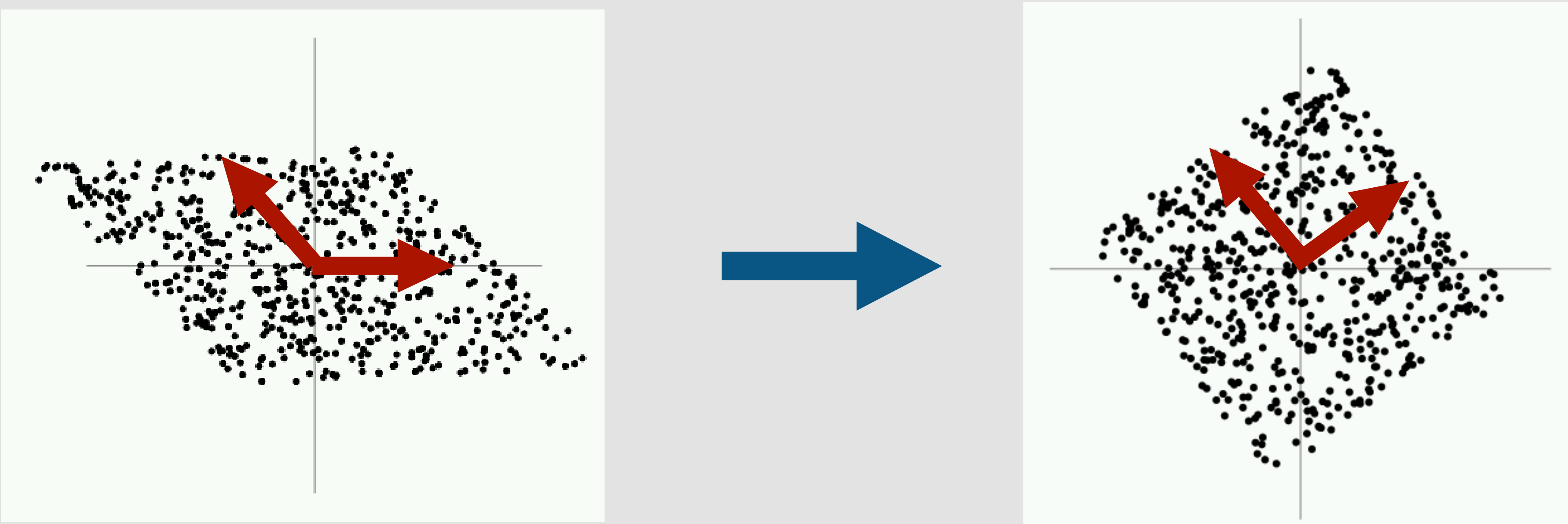
- An attacker faces a learning problem.





STAGE 1: MORPHING

- It is not difficult to reduce the general case to the case where the parallelepiped is an n-dim centered unit hypercube.



STAGE 1: MORPHING

- Consider $y = xB$ where $x \in_R [-1,1]^n$
- Then $y^t y = B^t x^t x B$

STAGE 1: MORPHING

- Consider $y=xB$ where $x \in_R [-1,1]^n$
- Then $y^t y = B^t x^t x B$
- $Exp(y^t y)$ is a multiple of $G = B^t B$: why?

STAGE 1: MORPHING

- Consider $y = xB$ where $x \in_R [-1,1]^n$
- Then $y^t y = B^t x^t x B$
- $Exp(y^t y)$ is a multiple of $G = B^t B$: why?
- Now compute a matrix L s.t. $G^{-1} = L L^t$
- Then $C = BL$ satisfies $C C^t = BG^{-1}B^t = I_n$.

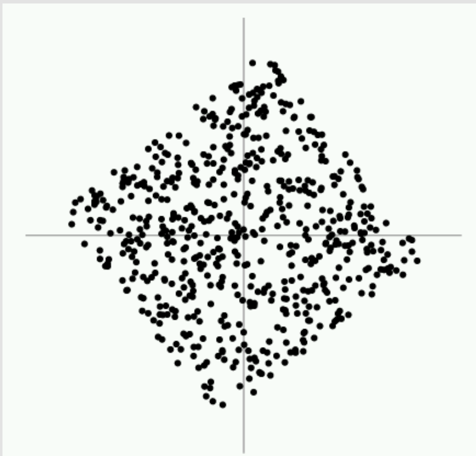
STAGE 1: MORPHING

- Consider $y=xB$ where $x \in_R [-1,1]^n$
- Then $y^t y = B^t x^t x B$
- $Exp(y^t y)$ is a multiple of $G = B^t B$: why?
- Now compute a matrix L s.t. $G^{-1} = L L^t$
- Then $C=BL$ satisfies $C C^t = BG^{-1}B^t = I_n$.
- So C is orthogonal and $yL = xC$ is uniformly distributed over some hypercube.

TOWARDS STAGE 2

- Let D be the uniform distribution over an n-dim centered unit hypercube.
- Let $\vec{u}$ be a unit vector in $\mathbb{R}^n$.
- For any k in **N**, it is easy to compute:

$$\mathrm{Exp}_{\vec{v}\in D}\left(\langle \vec{u}, \vec{v}\rangle^k\right)$$



- It is zero if k is odd.

PLAYING WITH MOMENTS

- The second moment is:

$$\mathrm{Var}(\langle \vec{u}, \rangle) = \mathrm{Exp}_{\vec{v}}\left(\langle \vec{u}, \vec{v}\rangle^2\right) = \cdots = 1/3$$ 🙁

PLAYING WITH MOMENTS

- The second moment is:

$$\mathrm{Var}(\langle \vec{u}, \rangle) = \mathrm{Exp}_{\vec{v}}\left(\langle \vec{u}, \vec{v} \rangle^2\right) = \cdots = 1/3$$ ☹️

- The fourth moment is:

$$\mathrm{Kur}(\langle \vec{u}, \rangle) = \mathrm{Exp}_{\vec{v}}\left(\langle \vec{u}, \vec{v} \rangle^4\right) = \cdots = \frac{1}{3} - \frac{2}{15}\sum_{i=1}^{n} u_i^4$$ 🙂

where $u_i = \langle \vec{u}, \vec{c}_i \rangle$

PLAYING WITH MOMENTS

- The second moment is:

$$\mathrm{Var}(\langle \vec{u}, \rangle) = \mathrm{Exp}_{\vec{v}}\left(\langle \vec{u}, \vec{v} \rangle^2\right) = \cdots = 1/3$$ ☹️

- The fourth moment is:

$$\mathrm{Kur}(\langle \vec{u}, \rangle) = \mathrm{Exp}_{\vec{v}}\left(\langle \vec{u}, \vec{v} \rangle^4\right) = \cdots = \frac{1}{3} - \frac{2}{15}\sum_{i=1}^{n} u_i^4$$ 🙂

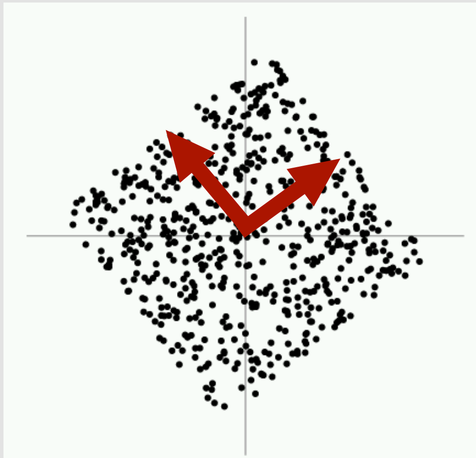
where $u_i = \langle \vec{u}, \vec{c}_i \rangle$

- In a random direction: ≈1/3
- In direction of any c_i: ≈1/3-2/15=1/5

STAGE 2: MINIMIZING A MULTIVARIATE FUNCTION

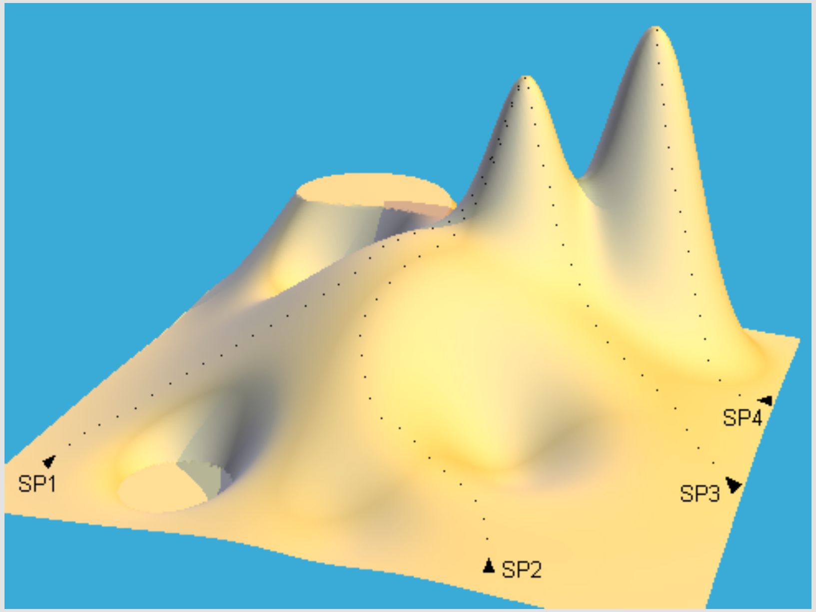
- Th: the 2n vectors $\pm \mathbf{c}_i$ are the only local minima of the fourth moment.

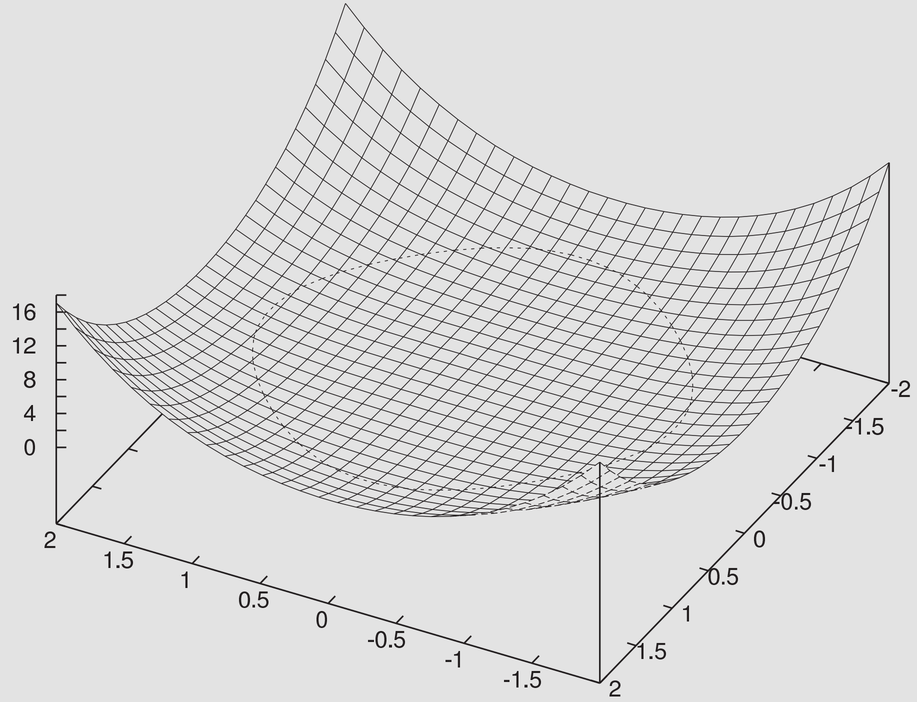
- Finding a basis of the parallelepiped amounts to finding sufficiently many local minima of the fourth moment.



STAGE 2: GRADIENT DESCENT

- We solve this minimization problem using a gradient descent.
- Here, the descent can be proved, because our function is very nice.





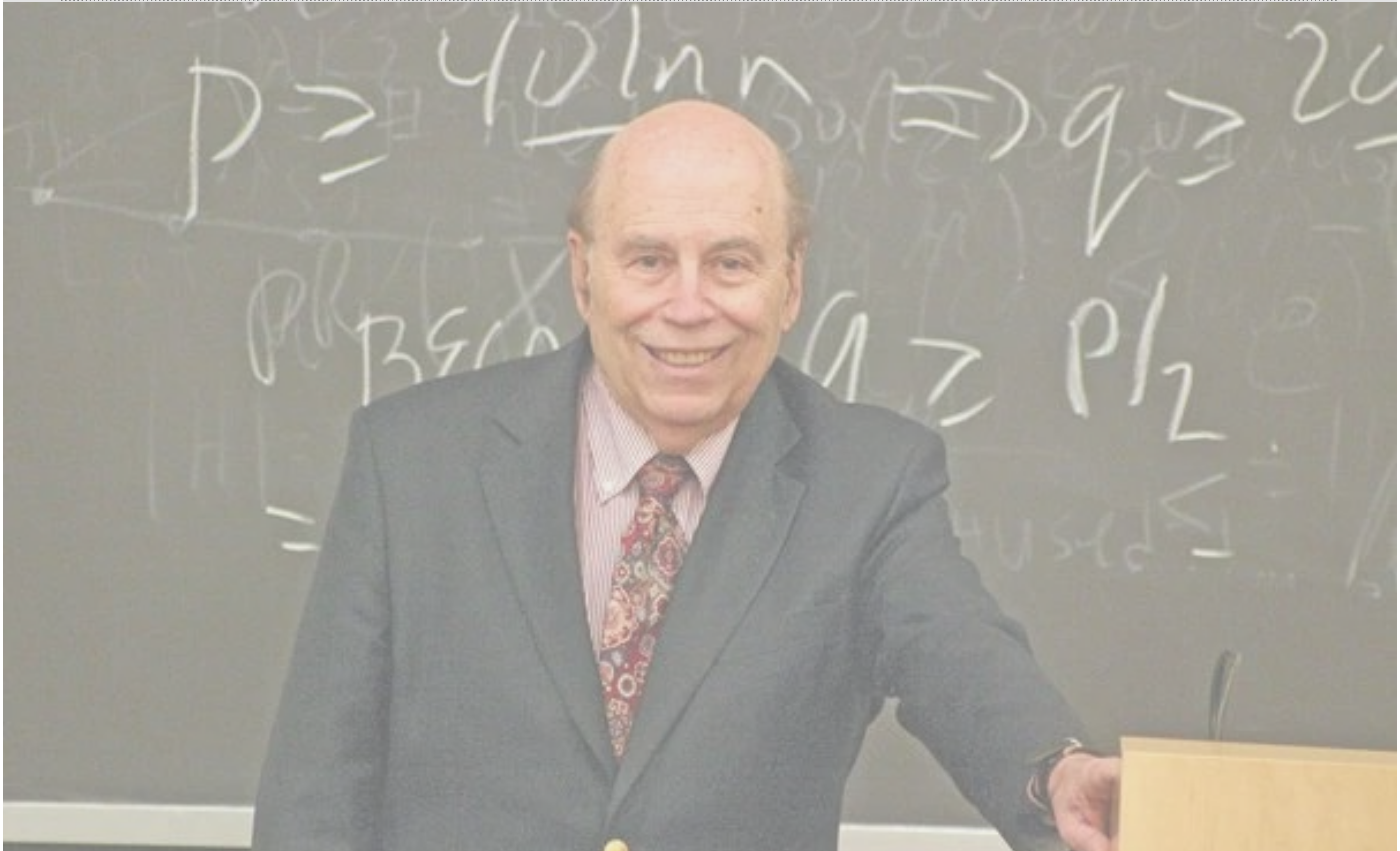
COUNTERMEASURES

- Signatures should not leak information on the secret key.
- Practical countermeasures by IEEE-IT and NTRUSign were also broken in [DuNg12].
- But there is a secure countermeasure…

RABIN’S SIGNATURE WITH LATTICES

proposed by Michael O.
digital signature schemes

RABIN SIGNATURE



proposed by Michael O.
digital signature schemes

RABIN SIGNATURE

- Let $N=pq$. where $p \neq q$ large primes.
- Then $f(x)=x^2 \bmod N$ is a one-way function over $\{0,\ldots,N-1\}$.
- If one knows the trapdoor (p,q), one can invert f: each square has 4 pre-images, and one can select one pre-image uniformly at random.

proposed by Michael O.
digital signature schemes

RABIN SIGNATURE

- Let N=pq. where $p \neq q$ large primes.
- Then $f(x)=x^2$ mod N is a one-way function over {0,…,N-1}.
- If one knows the trapdoor (p,q), one can invert f: each square has 4 pre-images, and one can select one pre-image uniformly at random.
- Rabin uses this pre-image sampling to give a provably-secure signature scheme based on factoring in the random-oracle model: the distributions (x,f(x)) and $(f^{-1}(H(m)),H(m))$ are statistically close.

RABIN SIGNATURE

RABIN SIGNATURE

- Random collisions in f allow to factor.

RABIN SIGNATURE

- Random collisions in f allow to factor.
- This Rabin signature is randomized but it is essential if you sign the same message twice, the signature remains the same: to do that, one can use a PRF.

LATTICE SIGNATURE USING TRAPDOOR

- [GPV08] is a lattice analogue of Rabin signature.

LATTICE SIGNATURE USING TRAPDOOR

- [GPV08] is a lattice analogue of Rabin signature.

➤ What will replace the Rabin squaring function?

LATTICE SIGNATURE USING TRAPDOOR

- [GPV08] is a lattice analogue of Rabin signature.

➤ What will replace the Rabin squaring function?

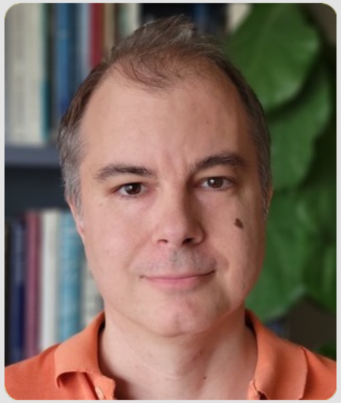
➤ What will replace square root sampling?

LATTICE SIGNATURE USING TRAPDOOR

- [GPV08] is a lattice analogue of Rabin signature.
  - What will replace the Rabin squaring function?
  - What will replace square root sampling?
- The security proof is essentially the same.

LATTICE SIGNATURE USING TRAPDOOR

- [GPV08] is a lattice analogue of Rabin signature.



Craig Gentry

Chris Peikert

Vinod Vaikuntanathan

LATTICE SIGNATURE USING TRAPDOOR

- [GPV08] is a lattice analogue of Rabin signature.

➤ What will replace the Rabin squaring function?

LATTICE SIGNATURE USING TRAPDOOR

- [GPV08] is a lattice analogue of Rabin signature.

➤ What will replace the Rabin squaring function?

➤ What will replace square root sampling?

LATTICE SIGNATURE USING TRAPDOOR

- [GPV08] is a lattice analogue of Rabin signature.

  ➤ What will replace the Rabin squaring function?

  ➤ What will replace square root sampling?

- The security proof is essentially the same.

INVERTING ISIS/SIS

- Pick $g=(g_1,\ldots,g_m)$ uniformly at random from G^m.
- $f_g(x_1,\ldots,x_m)=\Sigma_i\, x_i\, g_i$ where $x_1,\ldots,x_m$ are small integers.

INVERTING ISIS/SIS

- Pick $g=(g_1,\ldots,g_m)$ uniformly at random from G^m.
- $f_g(x_1,\ldots,x_m)=\Sigma_i\, x_i\, g_i$ where $x_1,\ldots,x_m$ are small integers.

- f_g is surjective with many preimages: inverting f_g means finding a preimage with suitable distribution, namely, some discrete Gaussian distribution. Inverting can be done by Gaussian sampling.

GAUSSIAN MEASURE

GAUSSIAN MEASURE

- Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.

GAUSSIAN MEASURE

- Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.
- This Gaussian measure was implicitly used in [Klein00]'s randomized variant of Babai's nearest-plane algorithm to solve BDD.

GAUSSIAN MEASURE

- Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.
- This Gaussian measure was implicitly used in [Klein00]'s randomized variant of Babai's nearest-plane algorithm to solve BDD.
- [Regev2005] noted that the Gaussian measure could sometimes be sampled.

GAUSSIAN MEASURE

- Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.
- This Gaussian measure was implicitly used in [Klein00]'s randomized variant of Babai's nearest-plane algorithm to solve BDD.
- [Regev2005] noted that the Gaussian measure could sometimes be sampled.
- [GPV2008] rediscovered [Klein00] and showed that it samples from the Gaussian measure.

GAUSSIAN MEASURE

GAUSSIAN MEASURE

- Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.

Wojciech Banaszczyk

GAUSSIAN MEASURE

- Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.
- This Gaussian measure was implicitly used in [Klein00]'s randomized variant of Babai's nearest-plane algorithm to solve BDD.

Philip N. Klein

Wojciech Banaszczyk

GAUSSIAN MEASURE

- Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.
- This Gaussian measure was implicitly used in [Klein00]'s randomized variant of Babai's nearest-plane algorithm to solve BDD.
- [Regev2005] noted that the Gaussian measure could sometimes be sampled.

Oded Regev

GAUSSIAN MEASURE

- Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.
- This Gaussian measure was implicitly used in [Klein00]'s randomized variant of Babai's nearest-plane algorithm to solve BDD.
- [Regev2005] noted that the Gaussian measure could sometimes be sampled.
- [GPV2008] rediscovered [Klein00] and showed that it samples from the Gaussian measure.

GAUSSIAN MEASURE

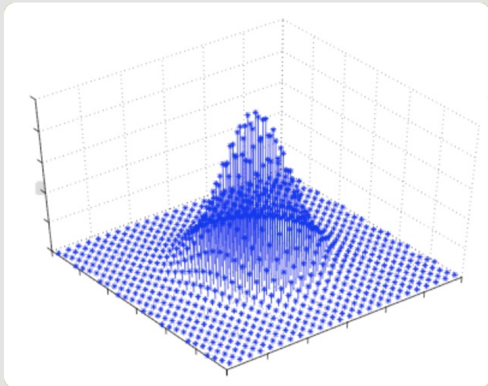
- Center c, parameter s
- Mass of x∈L proportional to

$$\rho_{s,\vec{c}}(\vec{x}) = e^{-\pi \| \frac{\vec{x}-\vec{c}}{s} \|^2}$$

GAUSSIAN MEASURE

- Center c, parameter s
- Mass of x∈L proportional to

$$\rho_{s,\vec{c}}(\vec{x}) = e^{-\pi \| \frac{\vec{x}-\vec{c}}{s} \|^2}$$

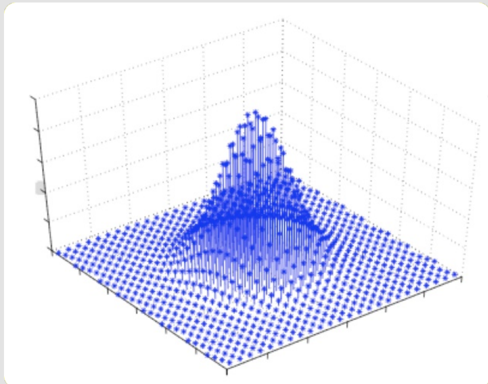


- The distribution is independent of the basis.

GAUSSIAN MEASURE

- Center c, parameter s
- Mass of x∈L proportional to

$$\rho_{s,\vec{c}}(\vec{x}) = e^{-\pi \| \frac{\vec{x}-\vec{c}}{s} \|^2}$$



- The distribution is independent of the basis.

- Introduced in [Ba93], then used in cryptography in [Cai99,Regev03,MiRe04,…]

GAUSSIAN SAMPLING

- [GPV08] rediscovered [Kl00] but provided a more complete analysis:
- Given a lattice basis, one can sample lattice points according to the discrete Gaussian distribution in poly-time, as long as the mean norm is somewhat larger than the basis norms.

SAMPLING AND PUBLIC-KEY CRYPTO

- Security proofs require (rigorous) probability distributions and efficient sampling.
- In classical PKC, a typical distribution is the uniform distribution over a finite group.

SAMPLING AND PUBLIC-KEY CRYPTO

- Security proofs require (rigorous) probability distributions and efficient sampling.
- In classical PKC, a typical distribution is the uniform distribution over a finite group.

➤ Example: The lack of nice probability distribution was problematic for braid cryptography.

SAMPLING AND PUBLIC-KEY CRYPTO

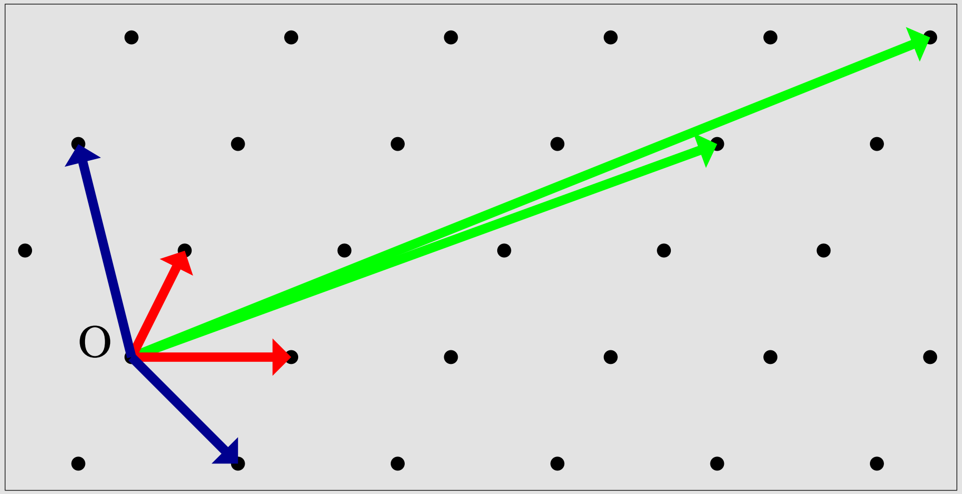
- Security proofs require (rigorous) probability distributions and efficient sampling.
- In classical PKC, a typical distribution is the uniform distribution over a finite group.

➤ Example: The lack of nice probability distribution was problematic for braid cryptography.

- Gaussian lattice sampling is a crucial tool for lattice-based cryptography.

LATTICE SIGNATURE [GPV08]

- **Secret key** = Good basis
- **Public key** = Bad basis
- **Message** = m in $\mathbf{Z}^n/L$
- **Signature** = a lattice point chosen with discrete Gaussian distribution close to m.
- **Verification** = check that the signature is a lattice point, close to m.



LATTICE SIGNATURE WITH SIS [GPV08]

- **Public key** $g=(g_1,\ldots,g_m)$ uniformly distributed over G^m.

  This generates a SIS lattice L.

- **Secret key** = Short basis of L.

- **Hashed message** = $m \in G$

- **Signature** = $(x_1,\ldots,x_m) \in \mathbf{Z}^m$ produced by Gaussian sampling over L s.t. $m=\Sigma_i\, x_i\, g_i$

- **Verification** = Check $m=\Sigma_i\, x_i\, g_i$ with $(x_1,\ldots,x_m)$ small.

SECURITY ARGUMENT IN THE ROM

- Same as Rabin:

➤ The distributions $((x_1,...,x_m),f_g(x_1,...,x_m))$ and $(f_g^{-1}(H(m)),H(m))$ are statistically close.

➤ Random collisions in $f_g(x_1,\ldots,x_m)$ allow to solve SIS, like in the lattice-based hash function.

➤ Again, if you sign the same message twice, you should output the same signature.

FALCON (2017)

FALCON

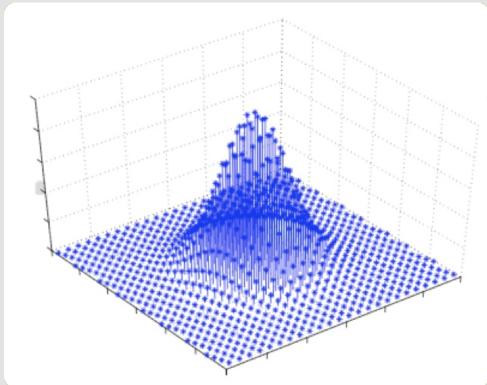
Fast-Fourier Lattice-based
Compact Signatures over NTRU

FALCON (2017)

- More-or-less NTRUSign with the GPV08 provably-secure fix:

FALCON (2017)

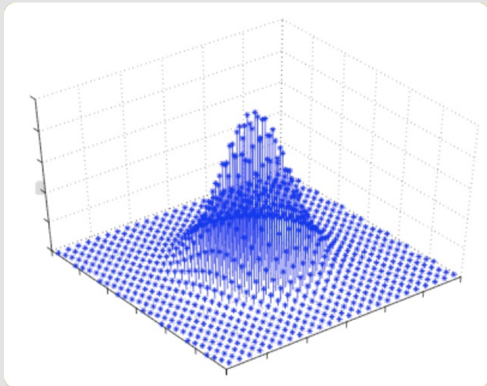
- More-or-less NTRUSign with the GPV08 provably-secure fix:
  - Sign by discrete Gaussian sampling, instead of Babai's algorithms.



FALCON (2017)

- More-or-less NTRUSign with the GPV08 provably-secure fix:

➤ Sign by discrete Gaussian sampling, instead of Babai's algorithms.



➤ ROM security proof similar to Rabin's factoring signature.

FALCON SETTINGS

- Different from NTRU encryption

➤ Uses NTT rings $\mathbf{Z}_q[X]/(X^n+1)$ with $q=12289\equiv 1 \pmod{2n}$ and 2-power n.

➤ Secret (f,g) has discrete Gaussian distribution with $||(f,g)|| \approx 1.17\sqrt{q}$

➤ The signature is not a lattice point: it is a short element in the message coset m+L.

LATTICE IDENTITY-BASED ENCRYPTION

ID-BASED ENCRYPTION FROM LATTICES [GPV08]

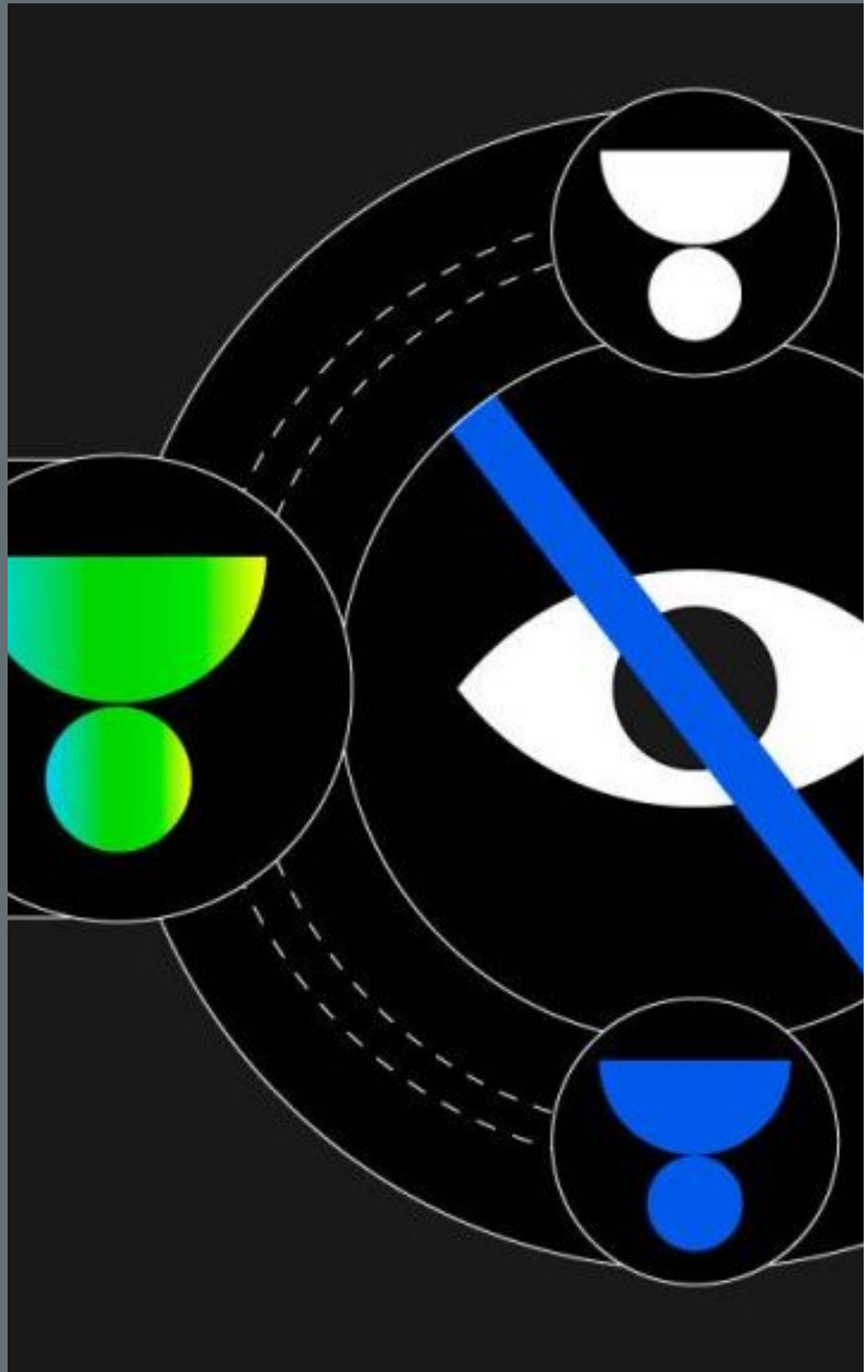
- It turns out that the GPV signature is compatible with dual GLWE encryption.

➤ Master key = Lattice trapdoor

➤ Parameters: $g=(g_1,\dots,g_m)$ uniformly distributed over G^m

➤ Secret-key extraction=$(x_1,\dots,x_m)\in \mathbf{Z}^m$ produced by Gaussian sampling s.t. $ID = \Sigma\, x_i\, g_i$

SIGNATURES FROM ZERO-KNOWLEDGE



NON-TRAPDOOR SIGNATURES

- There is another design for lattice-based signatures based on identification schemes from the Discrete Log world.

- ➤ This is related to Fiat-Shamir and proofs of knowledge.
- ➤ NIST's finalist Dilithium is based on this philosophy.

DILITHIUM SIGNATURE

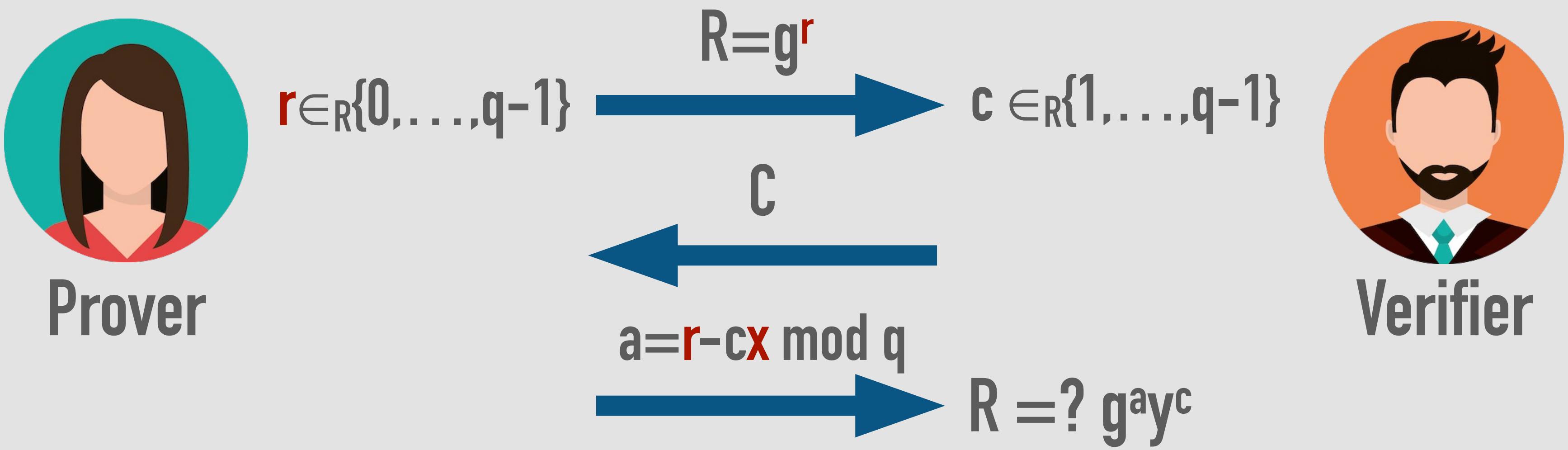
SCHNORR'S IDENTIFICATION (1989)

SCHNORR'S IDENTIFICATION (1989)

- $G=\langle g \rangle$ generated by g of order q.
- Proves knowledge of $x \in \{0,\ldots,q-1\}$ s.t. $y=g^x$

SCHNORR'S IDENTIFICATION (1989)

- $G=\langle g \rangle$ generated by g of order q.
- Proves knowledge of $x \in \{0,\ldots,q\text{-}1\}$ s.t. $y=g^x$



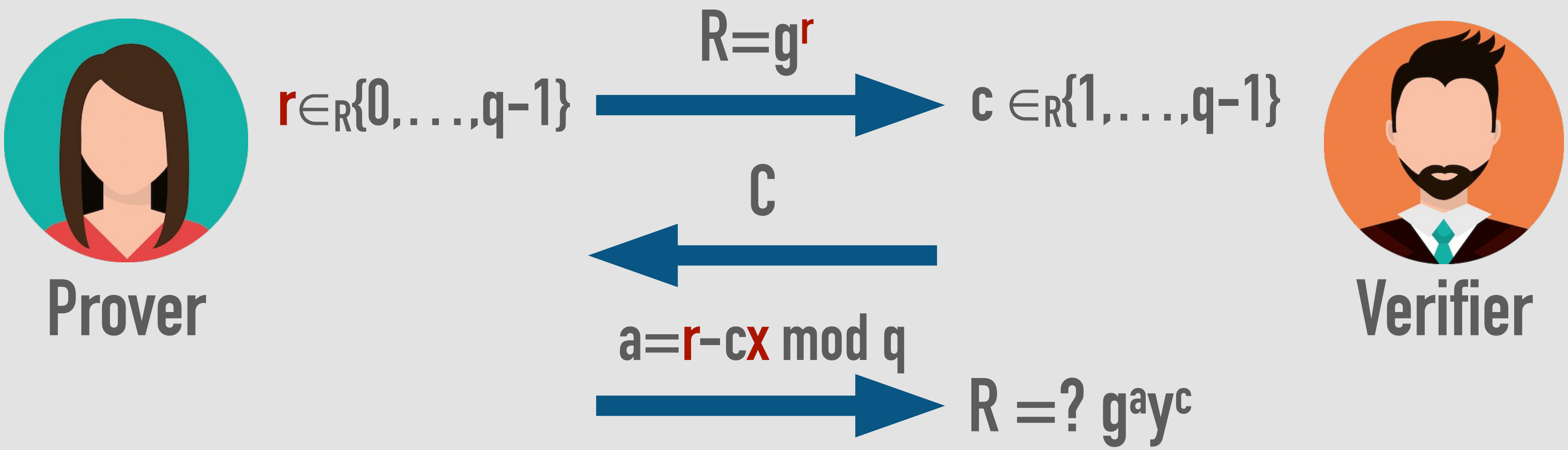
SCHNORR'S SIGNATURE (1989)

SCHNORR'S SIGNATURE (1989)

- Fiat-Shamir: $c = H(R \mid\mid msg)$ $y=g^{x}$

SCHNORR'S SIGNATURE (1989)

- Fiat-Shamir: $c = H(R \mid\mid msg)$ $y=g^x$



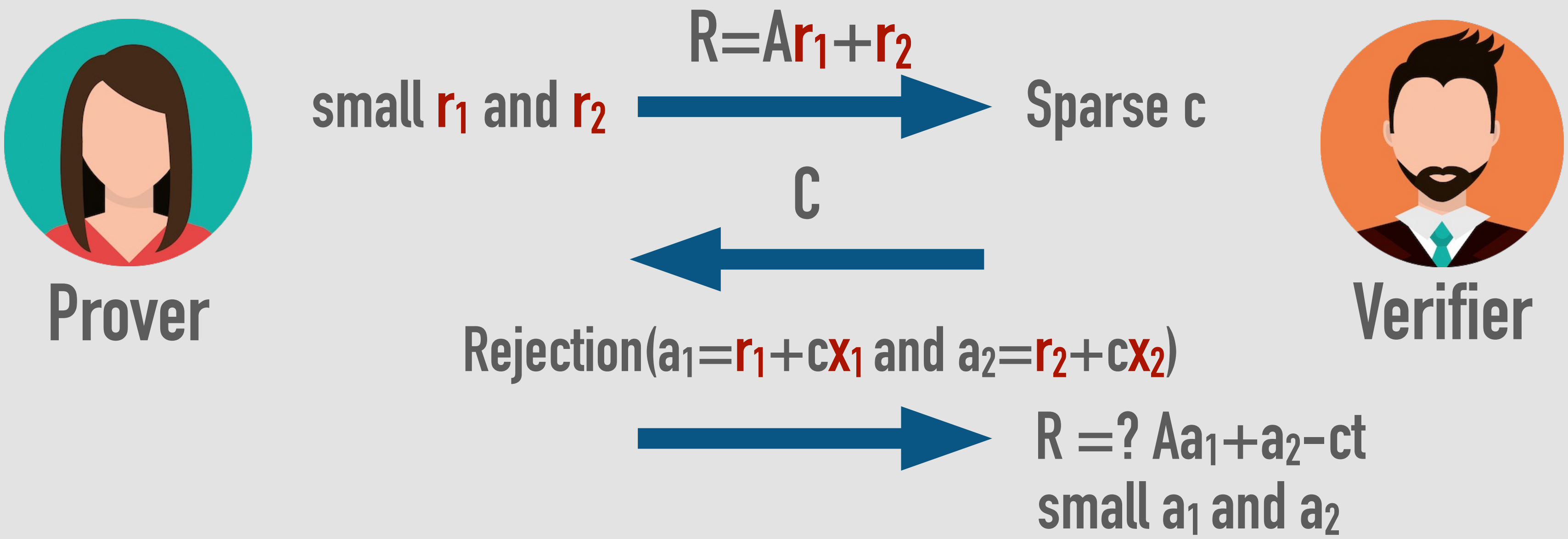
LYUBASHEVSKY’S IDENTIFICATION (2009–2012)

LYUBASHEVSKY'S IDENTIFICATION (2009-2012)

- A is an arbitrary matrix over $R=\mathbf{Z}_q[X]/(X^{256}+1)$
- $y=Ax_1+x_2$ with small x_1 and x_2.

LYUBASHEVSKY'S IDENTIFICATION (2009-2012)

- A is an arbitrary matrix over $R=\mathbf{Z}_q[X]/(X^{256}+1)$
- $y=Ax_1+x_2$ with small x_1 and x_2.



LYUBASHEVSKY'S IDENTIFICATION (2009–2012)

LYUBASHEVSKY'S IDENTIFICATION (2009-2012)

- Finding the secret (x_1, x_2) is MLWE.

LYUBASHEVSKY'S IDENTIFICATION (2009-2012)

- Finding the secret (x_1,x_2) is MLWE.
- If one can break the protocol, one can find $||.||_\infty$-short vectors in the MSIS lattice related to the matrix A over $R=\mathbf{Z}_q[X]/(X^{256}+1)$

LYUBASHEVSKY'S IDENTIFICATION (2009-2012)

- Finding the secret (x_1,x_2) is MLWE.
- If one can break the protocol, one can find $||.||_\infty$-short vectors in the MSIS lattice related to the matrix A over $R=\mathbf{Z}_q[X]/(X^{256}+1)$
  - True in the ROM
  - Not so much in the QROM

LYUBASHEVSKY'S IDENTIFICATION (2009-2012)

- Finding the secret (x_1, x_2) is MLWE.
- If one can break the protocol, one can find $||.||_\infty$-short vectors in the MSIS lattice related to the matrix A over $R=\mathbf{Z}_q[X]/(X^{256}+1)$
  - True in the ROM
  - Not so much in the QROM
- MSIS attacks are presumed to be harder than MLWE attacks.

DILITHIUM SETTINGS

DILITHIUM SETTINGS

- Ring $\mathbf{Z}_q[X]/(X^{256}+1)$ with $q=8380417\equiv 1 \pmod{512}$ instead of 3329 allows full-NTT.

DILITHIUM SETTINGS

- Ring $\mathbf{Z}_q[X]/(X^{256}+1)$ with $q=8380417 \equiv 1 \pmod{512}$ instead of 3329 allows full-NTT.
- 4x4, 6x5 and 8x7 matrices

DILITHIUM SETTINGS

- Ring $\mathbf{Z}_q[X]/(X^{256}+1)$ with $q=8380417\equiv 1 \pmod{512}$ instead of 3329 allows full-NTT.
- 4x4, 6x5 and 8x7 matrices
- Small distribution = uniform narrow. Sparse challenges with prescribed ± 1

DILITHIUM SETTINGS

- Ring $\mathbf{Z}_q[X]/(X^{256}+1)$ with $q=8380417\equiv 1 \pmod{512}$ instead of 3329 allows full-NTT.
- 4x4, 6x5 and 8x7 matrices
- Small distribution = uniform narrow. Sparse challenges with prescribed ±1
- Approx 4 repetitions

DILITHIUM SETTINGS

- Ring $\mathbf{Z}_q[X]/(X^{256}+1)$ with $q=8380417\equiv 1 \pmod{512}$ instead of 3329 allows full-NTT.
- 4x4, 6x5 and 8x7 matrices
- Small distribution = uniform narrow. Sparse challenges with prescribed ±1
- Approx 4 repetitions
- Many optimizations over [L09-L12]

DILITHIUM VS FALCON

- Falcon

- Dilithium

DILITHIUM VS FALCON

- Falcon
  - 3.5-smaller signatures: 600-1200 bytes
  - 30% smaller public keys: 900-1800 bytes
  - Faster verification
- Dilithium

DILITHIUM VS FALCON

- Falcon
  - 3.5-smaller signatures: 600-1200 bytes
  - 30% smaller public keys: 900-1800 bytes
  - Faster verification
- Dilithium
  - Faster signing and much faster key generation
  - Simpler signing: no Gaussian sampling, no floating-point arithmetic

FOOD FOR THOUGHT

FOOD FOR THOUGHT

- How hard are lattice problems, especially with structured lattices?

FOOD FOR THOUGHT

- How hard are lattice problems, especially with structured lattices?
- How risky is $\mathbf{Z}_q[X]/(X^n+1)$?

FOOD FOR THOUGHT

- How hard are lattice problems, especially with structured lattices?
- How risky is $\mathbf{Z}_q[X]/(X^n+1)$?
- How powerful are quantum algorithms?

FOOD FOR THOUGHT

- How hard are lattice problems, especially with structured lattices?
- How risky is $\mathbf{Z}_q[X]/(X^n+1)$?
- How powerful are quantum algorithms?
- How should we measure security?