Lattice-based Signatures

Phong Nguyễn

October 2020

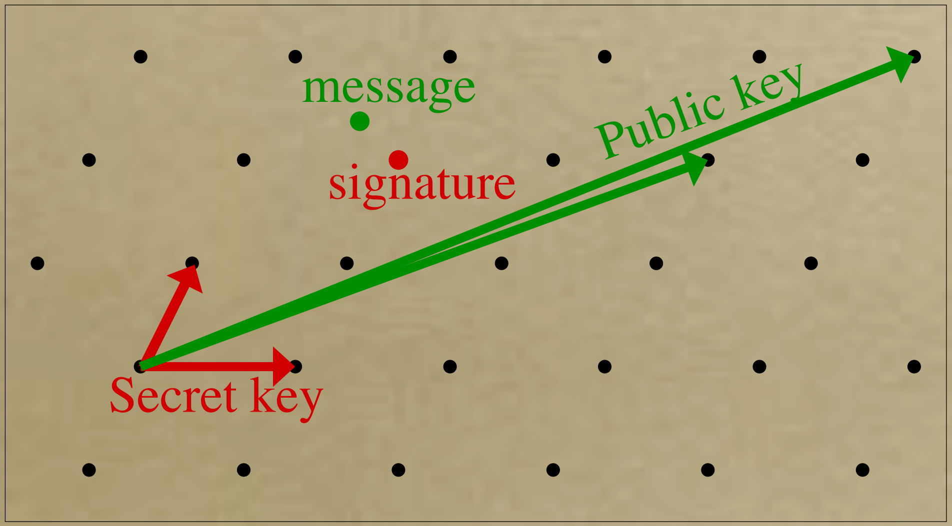
Today

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

The Early Days:
Insecure Lattice Signature

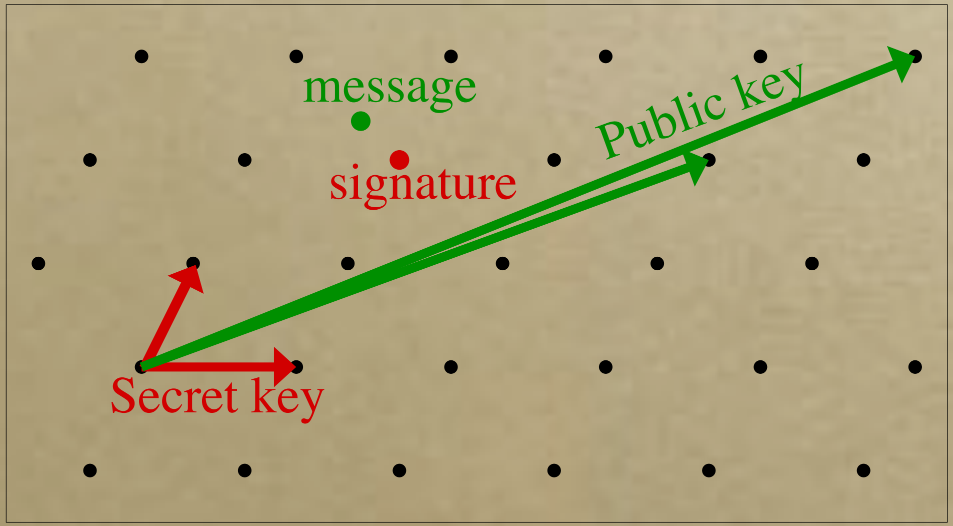
GGH Signature

- Message = m in $\mathbf{Z}^n/L$
  - Sign m into a close lattice point, using Babai's approx-CVP.
  - A signature must belong to the lattice, and be close to the message.



Key Generation in GGH

- Pick some high-dim lattice
  - Secret key = very good basis
  - Public key = very bad basis



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

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

- Generated by the rows of:

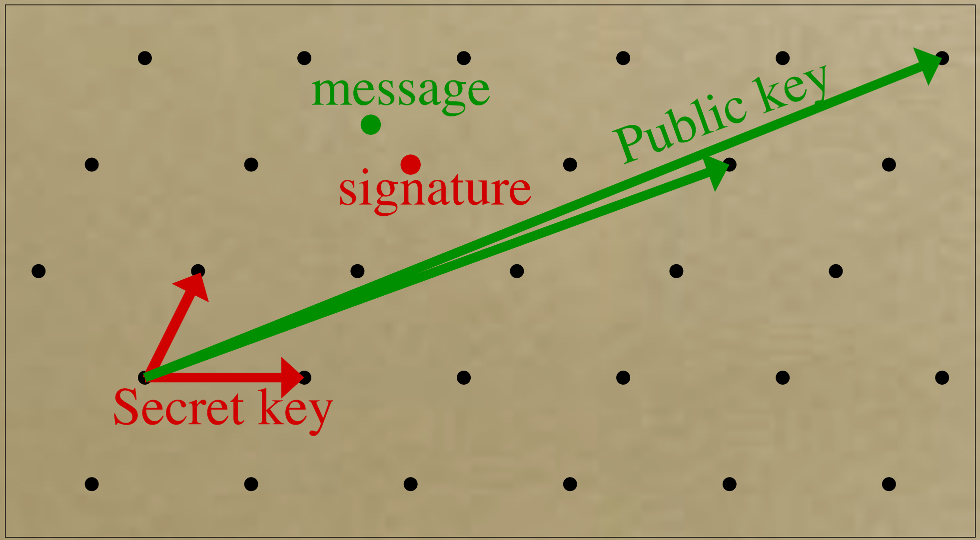
$$\begin{bmatrix} f_0 & f_1 & \cdots & f_{n-1} & g_0 & g_1 & \cdots & g_{n-1} \\ f_{n-1} & f_0 & \cdots & f_{n-2} & g_{n-1} & g_0 & \cdots & g_{n-2} \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ f_1 & \cdots & f_{n-1} & f_0 & g_1 & \cdots & g_{n-1} & g_0 \\ F_0 & F_1 & \cdots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

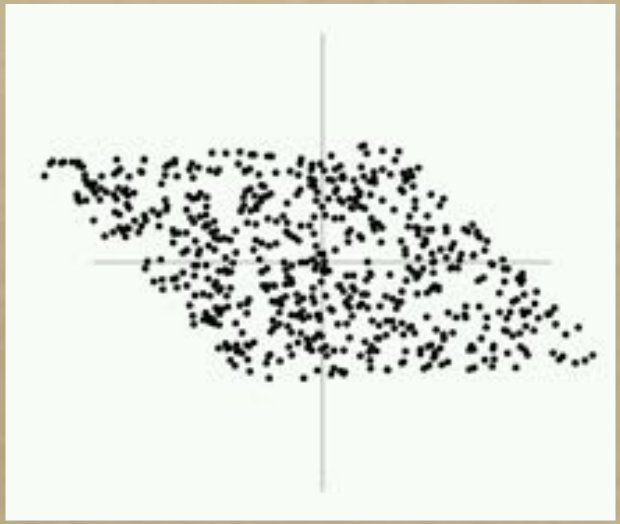
Security of GGH/NTRU Signatures

- GGH signatures leak information on the secret key [GeSz02]: potential attack in [Szydlo03].
- [NgRe06]: an efficient key-recovery attack.
- The analogues of GGH-encryption challenges have been solved.
- Half of NTRUSign parameter sets have been attacked (400 signatures).

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.

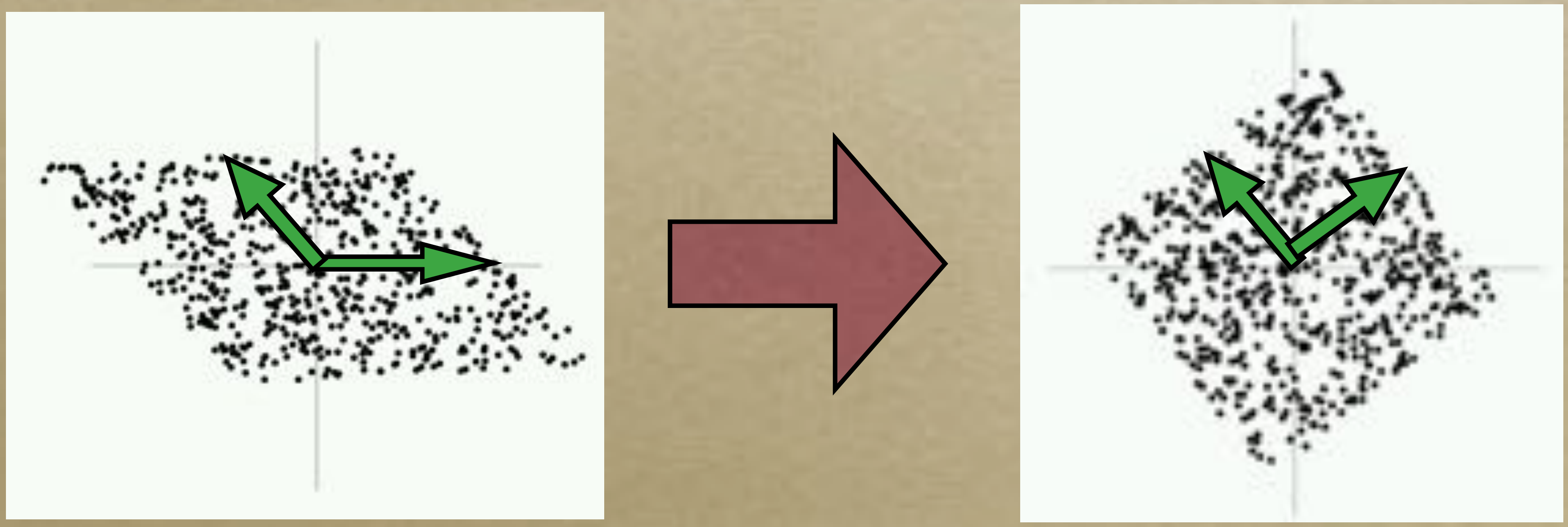




The Attack:
How to Learn a Parallelepiped

Stage 1: Morphing

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



Stage 1: Morphing

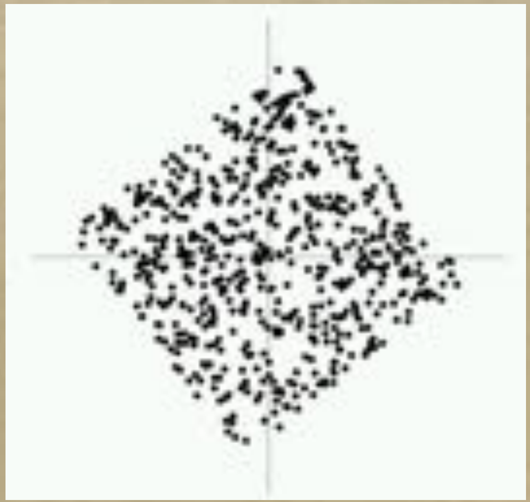
- Consider $y=xB$ where $x \in_R [-1,1]^n$
- Then $y^t y = B^t x^t x B$
- $Exp(y^t y)$ converges to a multiple of $G = B^t B$.
- Now compute a matrix L s.t. $G^{-1} = L L^t$
- Then $C=BL$ satisfies $C C^t = BG^{-1}B^t = I_n$.
- So C is orthogonal and $yL = xC$ is uniformly distributed over some hypercube.

Towards Stage 2

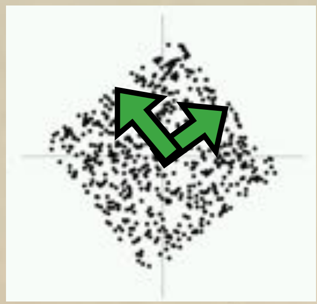
- Let D be the uniform distribution over an n-dim centered unit hypercube.
- Let $\vec{u}$ be a unit vector.
- For any k in **N**, it is easy to compute:

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

- It is zero if k is odd.

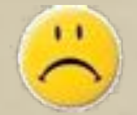


Playing with Moments



- The second moment is:

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



- The fourth moment is:

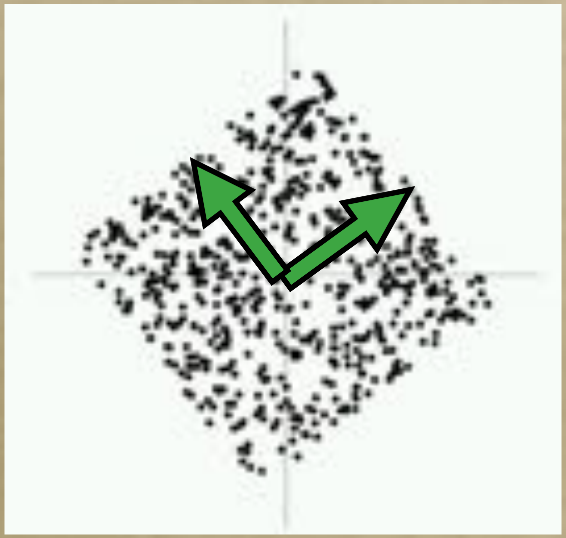
$$\mathrm{Kur}(\langle \vec{u}, \rangle) = \mathrm{Exp}_{\vec{v}}\left(\langle \vec{u}, \vec{v} \rangle^4\right) = \cdots = \frac{1}{3} - \frac{2}{15} \sum_{i=1}^{n} u_i^4$$

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

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

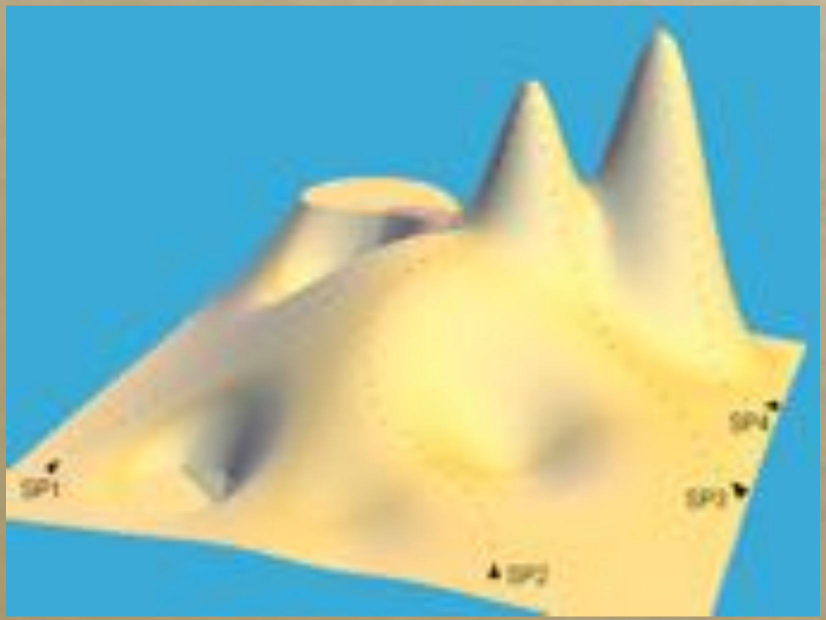
Stage 2: Minimizing a Multivariate Function

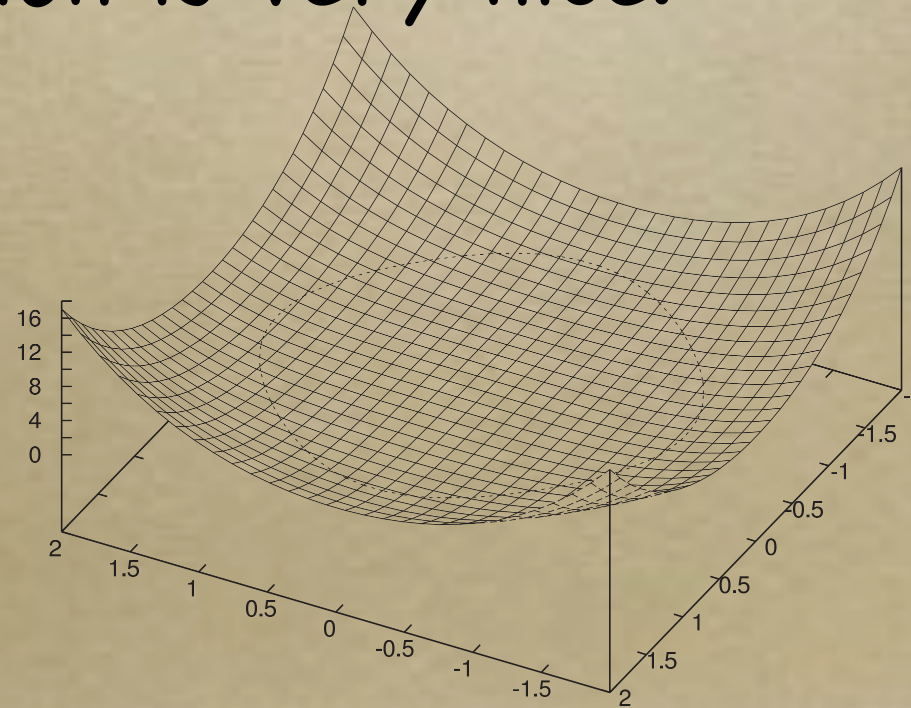
- Th: the 2n vectors $\pm c_i$ are the only local minima of the fourth moment.
- Finding a basis of the parallelepiped amounts to finding sufficiently many local minima of the fourth moment.



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

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 preimages, and one can select one preimage uniformly at random.
- Rabin uses this preimage 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.
- Random collisions in f allow to factor.

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.

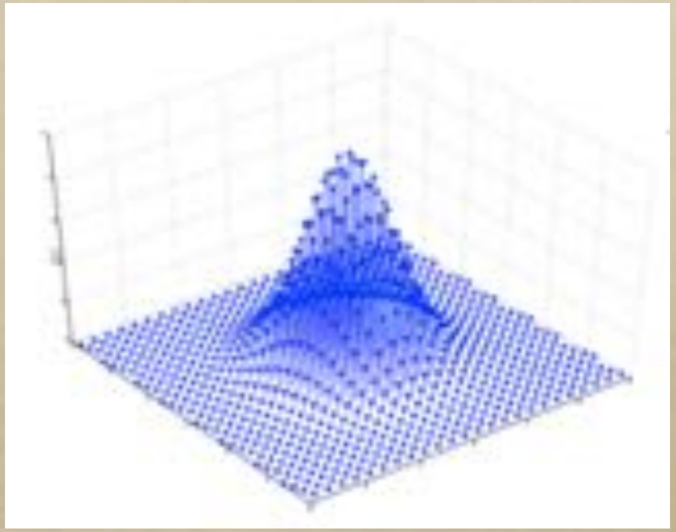
Inverting ISIS/SIS

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

- 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



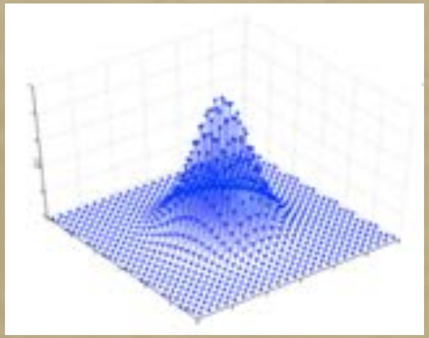
- Center c, parameter s
- Mass of x∈L proportional to

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

- The distribution is independent of the basis.
- Introduced in [Ba93], then used in cryptography in [Cai99,Regev03,MiRe04,...]

Gaussian Sampling

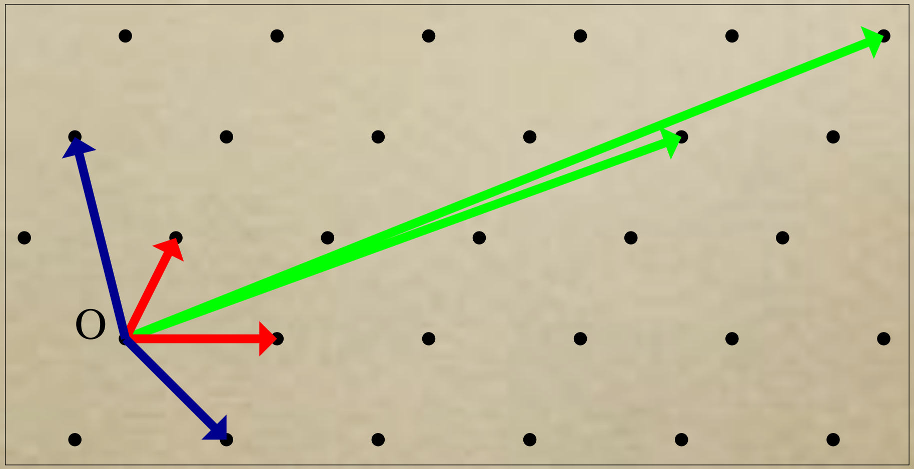
- [GPV08] rediscovered [Kl00] but provided a more complete analysis: given a lattice basis, one can sample lattice points according to the discrete Gaussian distribution in poly-time, as long as the mean norm is somewhat larger than the basis norms.



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.
- Ex: 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]

- Secret key = Trapdoor
- Public key = $g=(g_1,\ldots,g_m)$ uniformly distributed over G^m
- Hashed message = $m\in G$
- Signature = $(x_1,\ldots,x_m)\in \mathbf{Z}^m$ produced by Gaussian sampling s.t. $m = \sum_i x_i g_i$
- Verification = Check $m=\sum_i x_i g_i$ with $(x_1,\ldots,x_m)$ small.

Security Argument in the ROM

- Same as Rabin:
  - The distributions $((x_1,\ldots,x_m), f_g(x_1,\ldots,x_m))$ 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.

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: $g=(g_1,\ldots,g_m)$ uniformly distributed over G^m
  - Secret-key extraction=$(x_1,\ldots,x_m)\in\mathbf{Z}^m$ produced by Gaussian sampling s.t. ID = $\Sigma\ x_i\ g_i$

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.