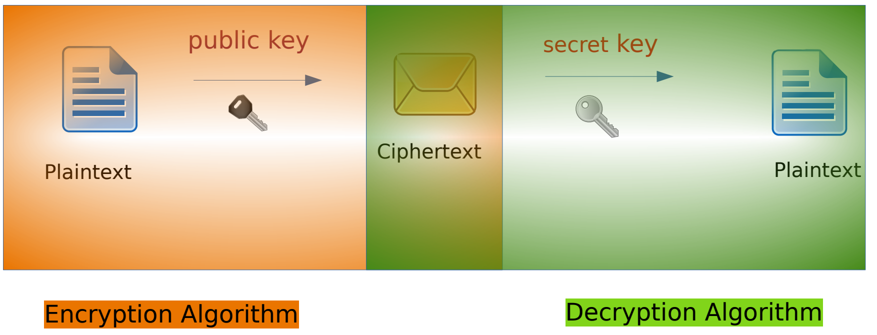
Post Quantum Cryptography

Meenakshi Kansal

Rashtriya Raksha University Gandhinagar

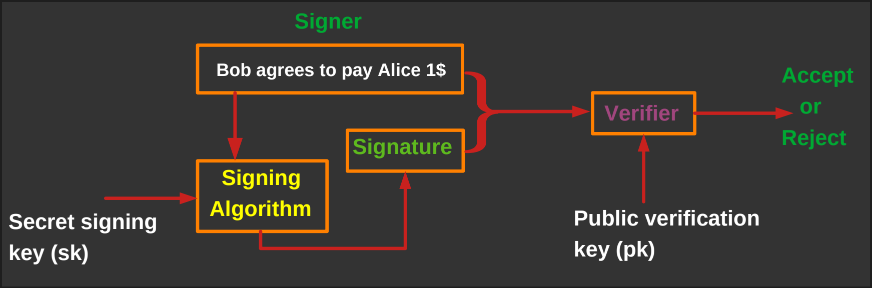
Encryption

- Encryption : Aims to provide privacy of documents



Digital Signature

- Digital Signature : Validate the authenticity of documents



Modern Cryptography

- Hard Mathematical Problem
  - * Factoring: Given pq find p, q.
  - * Discrete log problem: Given g, g^a find a.
- Proof of Security

If you can break encryption	$\Longrightarrow$	you can factor numbers

the encryption is secure	$\Longleftarrow$	If factoring is hard

Modern Cryptography

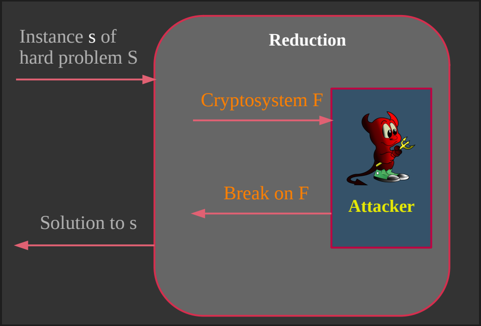
- Hard Mathematical Problem
  - Factoring: Given pq find p, q.
  - Discrete log problem: Given g, g^a find a.
- Proof of Security

If you can break encryption $\Longrightarrow$ you can factor numbers

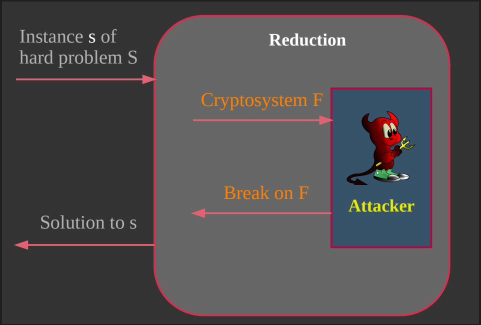
the encryption is secure $\Longleftarrow$ If factoring is hard

We are safe till this moment as there is no polynomial time algorithm to solve these problems on a classical machine.

- Cryptography assures that breaking a cryptosystem is atleast as hard as solving some difficult mathematical problem.

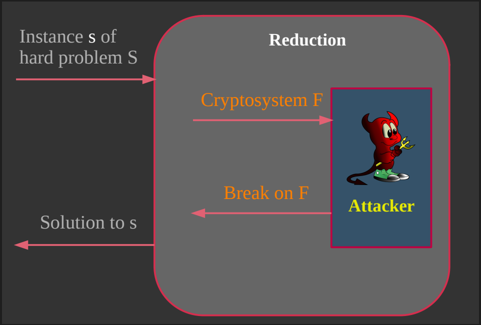


- Cryptography assures that breaking a cryptosystem is atleast as hard as solving some difficult mathematical problem.



- We normally model it as a classical computer.

- Cryptography assures that breaking a cryptosystem is atleast as hard as solving some difficult mathematical problem.



- We normally model it as a classical computer.

What if the attacker is quantum?

Factoring and Quantum (In)Security

- Shor (1994)
  - efficient quantum algorithms to factor integers.

Factoring and Quantum (In)Security

- Shor (1994)
  - efficient quantum algorithms to factor integers.
- Is this threat real?

Factoring and Quantum (In)Security

- Shor (1994)
  - efficient quantum algorithms to factor integers.
- Is this threat real? Yes!
- Google claims it has reached quantum supremacy.
  https://www.nature.com/articles/s41586

Factoring and Quantum (In)Security

- Shor (1994)
  - efficient quantum algorithms to factor integers.
- Is this threat real? Yes!
- Google claims it has reached quantum supremacy.
  https://www.nature.com/articles/s41586
- Assumption that factoring is hard does not hold in a "Post Quantum World".
- Same holds for most other mathematical problems currently in use.
  - discrete logarithm and their variants
- Need for new mathematical problems that are not solvable by quantum algorithms.
  - Post Quantum Cryptography
- Families of post quantum cryptography:
  - Code based cryptography
  - Hash based cryptography
  - Isogeny based cryptography
  - Lattice based cryptography
  - Multivariate cryptography

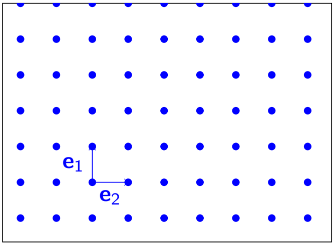
Factoring and Quantum (In)Security

- Shor (1994)
    - efficient quantum algorithms to factor integers.
- Is this threat real? Yes!
- Google claims it has reached quantum supremacy.
  https://www.nature.com/articles/s41586
- Assumption that factoring is hard does not hold in a "Post Quantum World".
- Same holds for most other mathematical problems currently in use.
    - discrete logarithm and their variants
- Need for new mathematical problems that are not solvable by quantum algorithms.
    - Post Quantum Cryptography
- Families of post quantum cryptography:
    - Code based cryptography
    - Hash based cryptography
    - Isogeny based cryptography
    - Lattice based cryptography
    - Multivariate cryptography

Impact of Quantum Computing on Common Cryptographic Algorithms

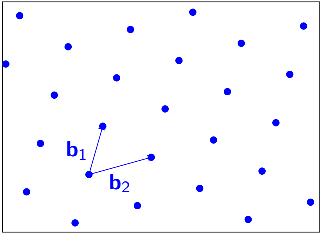
Cryptographic Algorithm	Type	Purpose	Impact from large scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA	——	Hash functions	Larger output needed
RSA	Public key	Signatures, Key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, Key exchange	No longer secure

What is a Lattice?



The simplest lattice in n-dimensional space is the integer lattice

$$\Lambda = \mathbb{Z}^n$$



Other lattices are obtained by applying a linear transformation

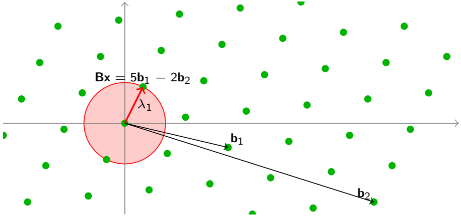
$$\Lambda = \mathbf{B}\mathbb{Z}^n \qquad (\mathbf{B} \in \mathbb{R}^{d \times n})$$

slides (9-24) credit: Daniele Micciancio

Shortest Vector Problem

Definition (Shortest Vector Problem, SVP)

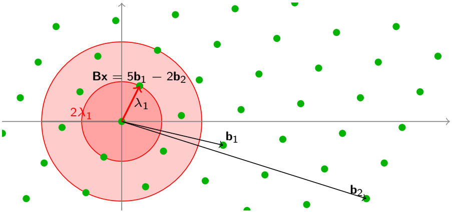
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \lambda_1$



Approximate Shortest Vector Problem

Definition (Shortest Vector Problem, SVP$_\gamma$)

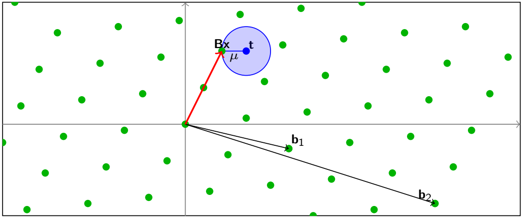
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \gamma\lambda_1$



Closest Vector Problem

Definition (Closest Vector Problem, CVP)

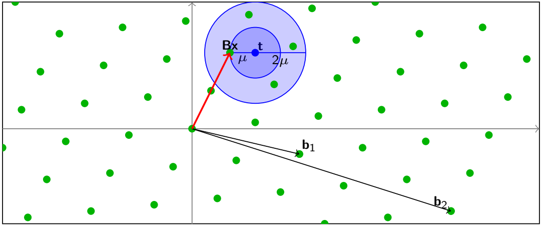
Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \mu$ from the target



Approximate Closest Vector Problem

Definition (Closest Vector Problem, CVP_γ)

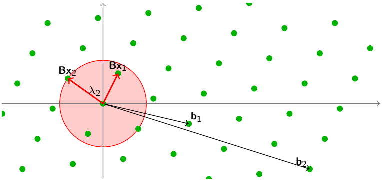
Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \gamma\mu$ from the target



Shortest Independent Vectors Problem

Definition (Shortest Independent Vectors Problem, SIVP)

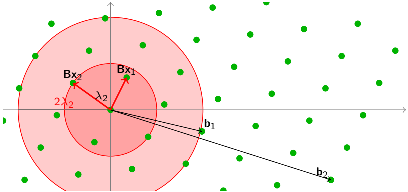
Given a lattice $\mathcal{L}(\mathbf{B})$, find n linearly independent lattice vectors $\mathbf{Bx}_1, \ldots, \mathbf{Bx}_n$ of length (at most) $\max_i \|\mathbf{Bx}_i\| \leq \lambda_n$



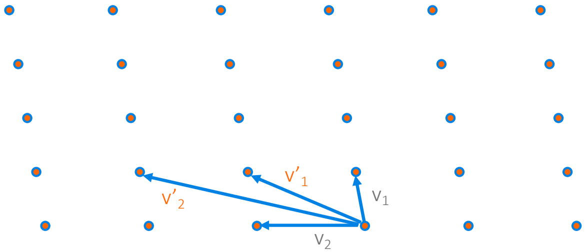
Approximate Shortest Independent Vectors Problem

Definition (Shortest Independent Vectors Problem, SIVP$_\gamma$)

Given a lattice $\mathcal{L}(\mathbf{B})$, find n linearly independent lattice vectors $\mathbf{Bx}_1, \ldots, \mathbf{Bx}_n$ of length (at most) $\max_i \|\mathbf{Bx}_i\| \leq \gamma\lambda_n$

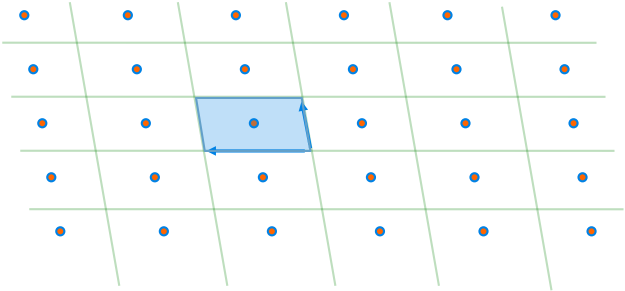


Lattice Trapdoors: Geometric View

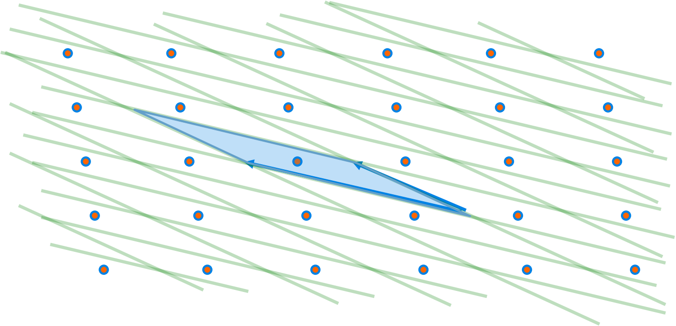


Multiple Bases

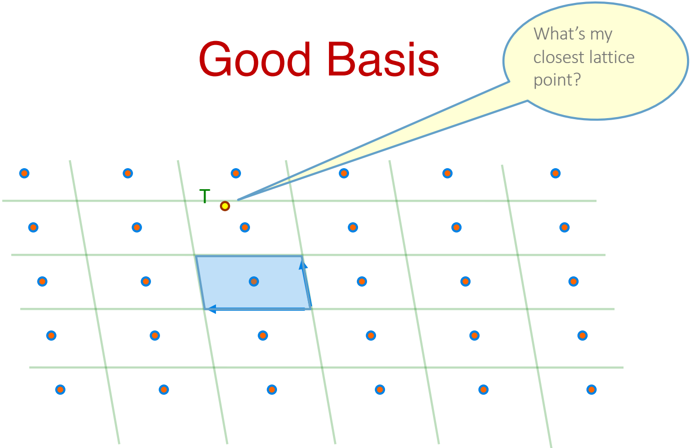
Parallelopipeds



Parallelopipeds

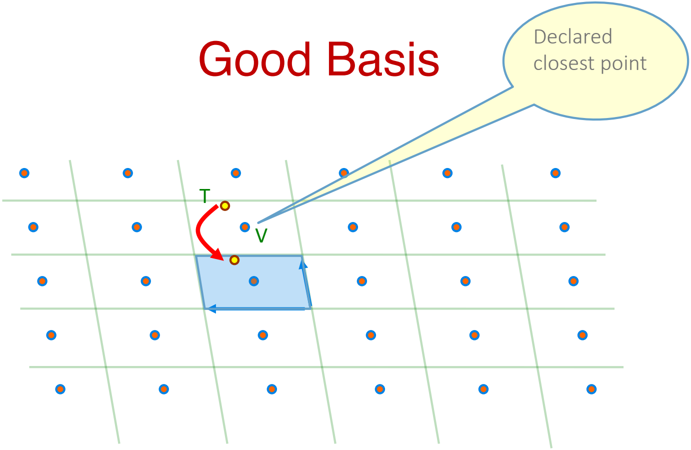


Good Basis



"Quite short" and "nearly orthogonal"

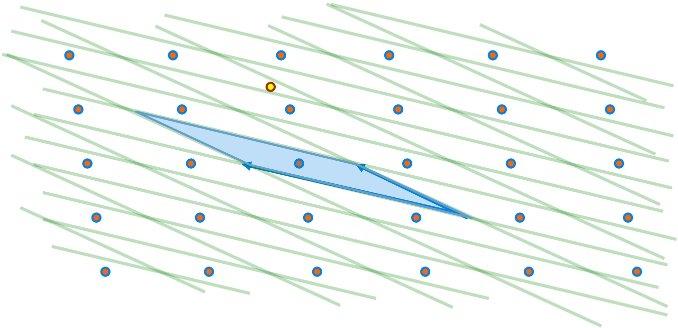
Good Basis

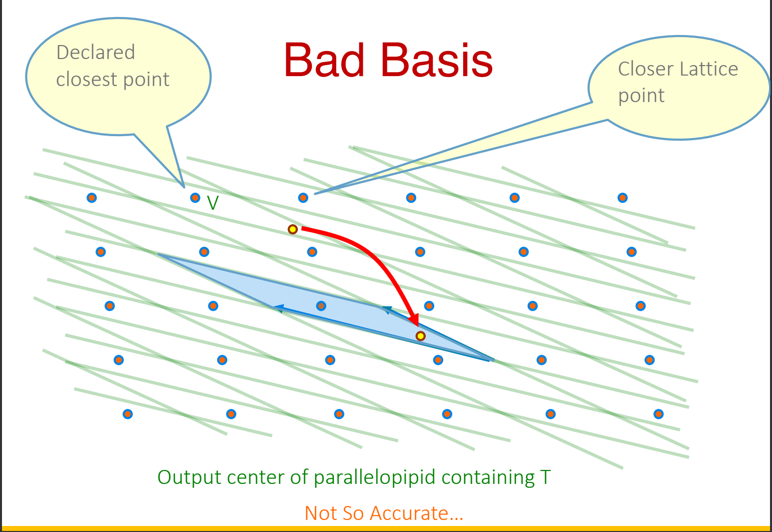


Output center of parallelopipid containing T

Pretty Accurate...

Bad Basis



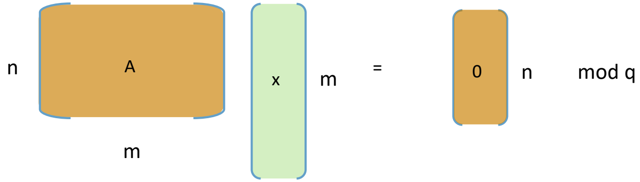

Bad Basis
Declared closest point
Closer Lattice point
V
Output center of parallelopipid containing T
Not So Accurate...

Short Integer Solution Problem

Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}, q = \text{poly}(n), m = \Omega(n \log q)$

Given matrix **A**, find "short" (low norm) vector **x** such that

$$\mathbf{Ax} = 0 \;\; mod \;\; q \in \mathbb{Z}_q^n$$



Learning With Errors Problem

Distinguish "noisy inner products" from uniform

Fix uniform $s \in Z_q^n$

a_1 , $b_1 = \langle a_1, s\rangle + e_1$
a_2 , $b_2 = \langle a_2, s\rangle + e_2$
⋮
a_m , $b_m = \langle a_m, s\rangle + e_m$

vs

a'_1 , b'_1
a'_2 , b'_2
⋮
a'_m , b'_m

uniform $\in Z_q^n$, $e_i \sim \phi \in Z_q$

a_i uniform $\in Z_q^n$, b_i uniform $\in Z_q$

Syntax and Correctness of Digital Signatures

Syntax

- $(vk, sk) \leftarrow$ keygen
- $\sigma \leftarrow$ sign(sk, m)
- $d \in \{0,1\} \leftarrow$ verify(vk, m, σ)

Correctness Requirement

$$\Pr\Big[\text{verify}\big(vk, m, \text{sign}(sk, m)\big) = 1\Big] = 1$$

for all $(vk, sk) \leftarrow$ keygen and all $m \in$ message space

Security

- Existential Forgery: given (m_i, σ_i) for $i = 1, 2, \ldots, q$, attacker cannot produce a valid signature for a new message.
- Strong Existential Forgery: given (m_i, σ_i) for $i = 1, 2, \ldots, q$, attacker cannot produce a new and valid signature on any m_i.

Simplified Version of CRYSTALS-Dilithium

Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé

- Finalists of Round three in a competition organised by NIST Post-Quantum Cryptography Standardization

Important Criteria for the Design

- Simple to implement securely.
- Be conservative with parameters.
- Minimize the size of public key and signature.
- Be modular - easy to vary security.

Overview

- strongly secure under chosen message attacks based on the hardness of lattice problems over module lattices
- based on the scheme proposed in [Lyu09]
- resemblance to the schemes proposed in [GLP12], [BG14]
- uses rejection sampling
- uses uniform distribution

[BG14] Shi Bai and Steven D. Galbraith. An improved compression technique for signatures based on learning with errors. In CT-RSA, pages 28–47, 2014.

[GLP12] Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In CHES, pages 530–547, 2012.

[Lyu09] Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In ASIACRYPT, pages 598–616, 2009.

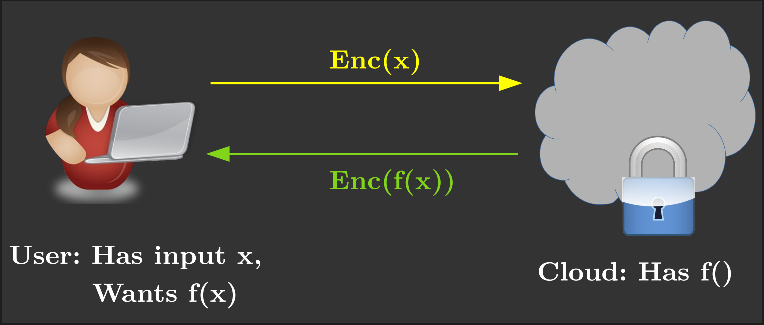
Lattice based Digital Signature

Let R be a polynomial ring.

- keygen(1^λ)
  - short $\mathbf{s}_1, \mathbf{s}_2 \leftarrow R_1$
  - $\mathbf{a} \leftarrow R$
  - compute $\mathbf{t} = \mathbf{a}\mathbf{s}_1 + \mathbf{s}_2$
  - $pk = (\mathbf{a}, \mathbf{t}), sk = (\mathbf{a}, \mathbf{t}, \mathbf{s}_1, \mathbf{s}_2)$
- sign(sk, m)
  - pick $\mathbf{y}_1, \mathbf{y}_2 \leftarrow R_k$
  - $\mathbf{c} \leftarrow H(\mathbf{a}\mathbf{y}_1 + \mathbf{y}_2, m)$
  - set $\mathbf{z}_1 \leftarrow \mathbf{s}_1\mathbf{c} + \mathbf{y}_1$, $\mathbf{z}_2 \leftarrow \mathbf{s}_2\mathbf{c} + \mathbf{y}_2$ (Rejection Sampling)
  - output $\sigma = (\mathbf{z}_1, \mathbf{z}_2, \mathbf{c}, m)$
- verify(pk, m, σ)
  - check that $||\mathbf{z}_1||, ||\mathbf{z}_2||$ are small
  - $\mathbf{c} = H(\mathbf{a}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{t}\mathbf{c}, m)$

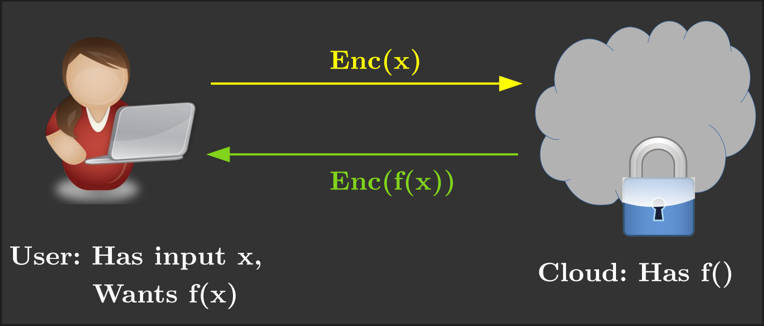
Cryptography from Lattices

- Remake old cryptography
- Get new primitives – Fully Homomorphic Encryption



Cryptography from Lattices

- Remake old cryptography
- Get new primitives – Fully Homomorphic Encryption



Thank you!