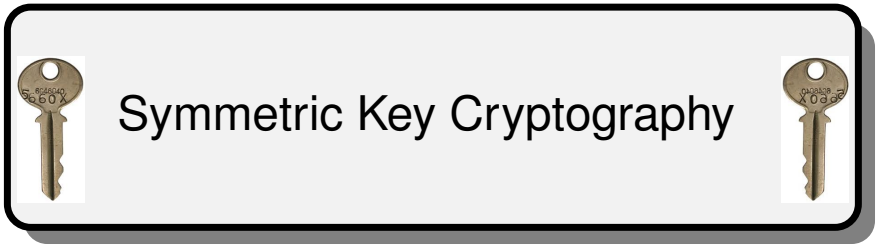
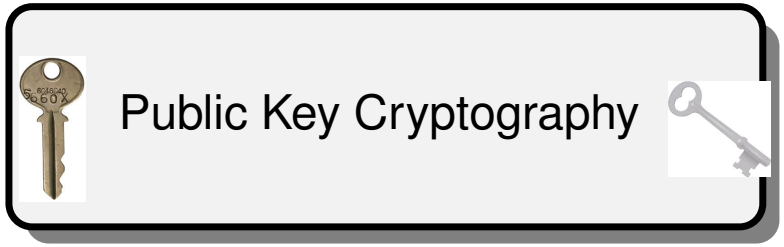
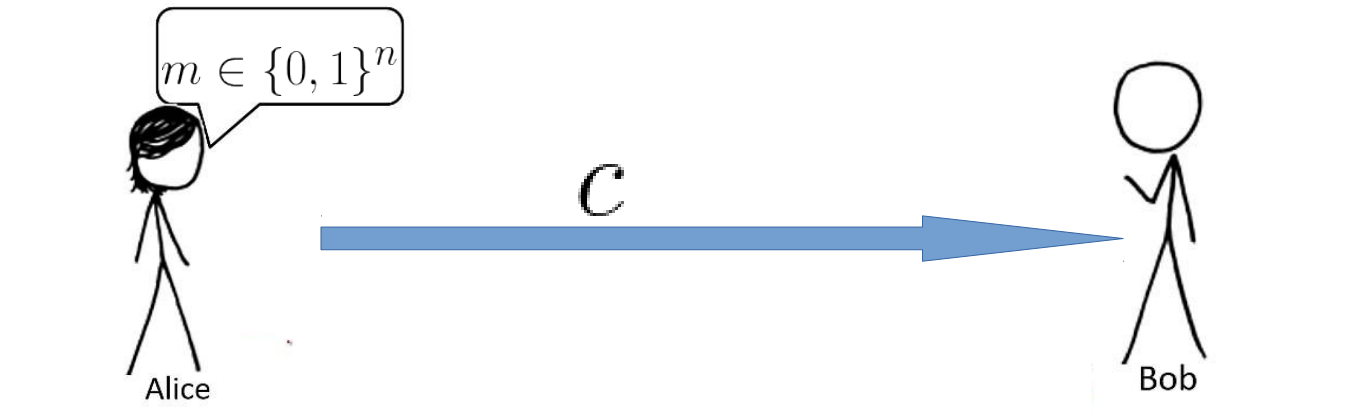
Lattice-Based Cryptography: A Primer

Rishiraj Bhattacharyya


Symmetric Key Cryptography

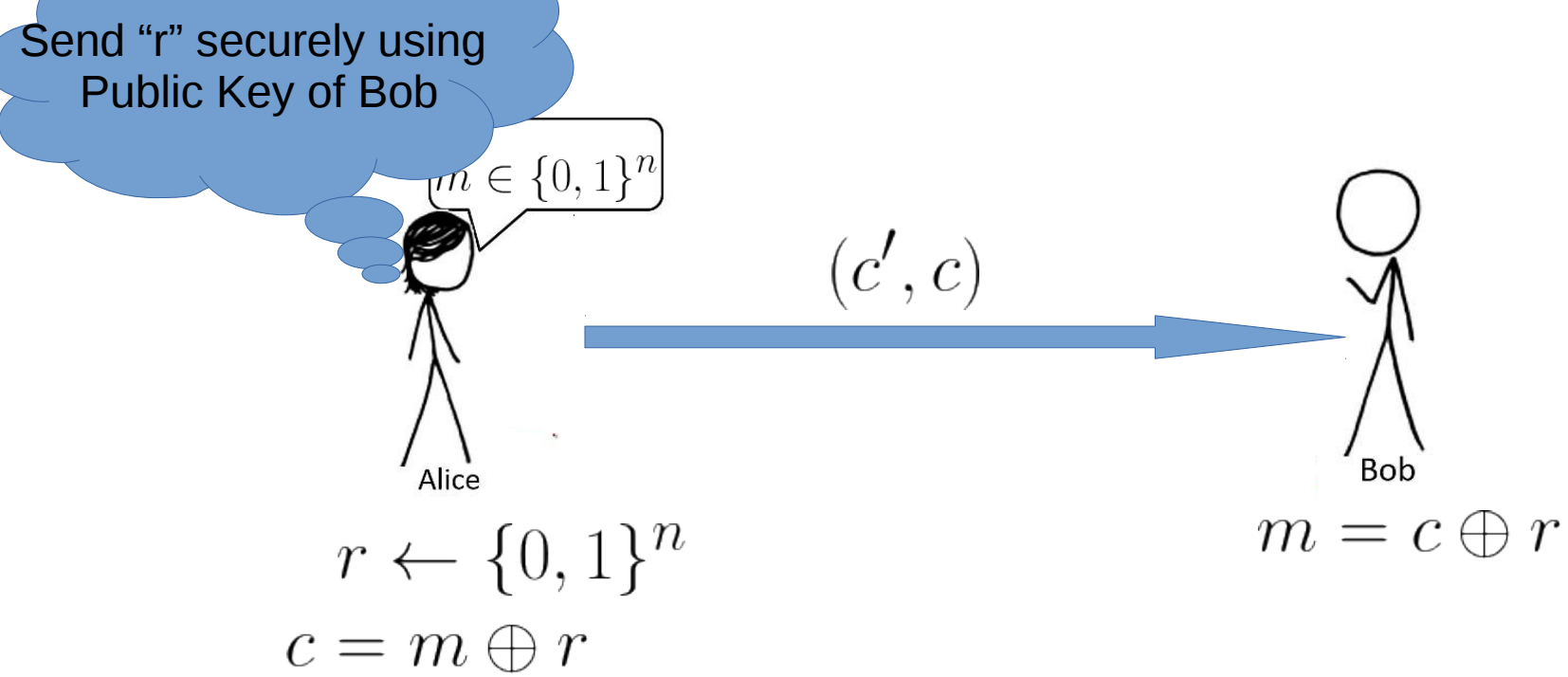

Public Key Cryptography



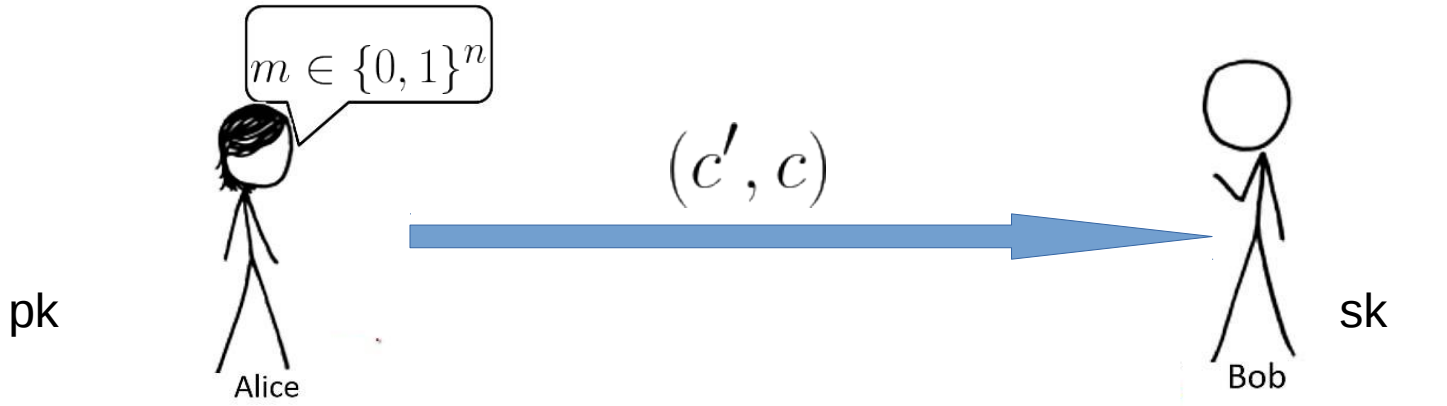
Symmetric Key Crypto:

1. One Time Pad: “r” is the key.
2. Stream Cipher: Both Alice and Bob generate “r” from the key using a pseudorandom generator

Send “r” securely using Public Key of Bob



Semantic Security: r is pseudorandom, given (pk,c’,c)



Public Key Crypto

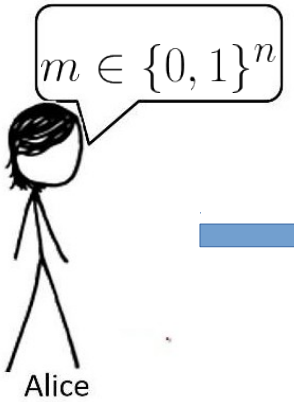
1.

$$c' = f(pk, r'), r = H(r')$$

Bob recovers r using trapdoor

Example

$$c' = r^e \pmod N$$



(c', c)

$r \leftarrow \{0,1\}^n$

$c = m \oplus r$

$m = c \oplus r$

Public Key Crypto

1.

$c' = f(pk, r'), r = H(r')$

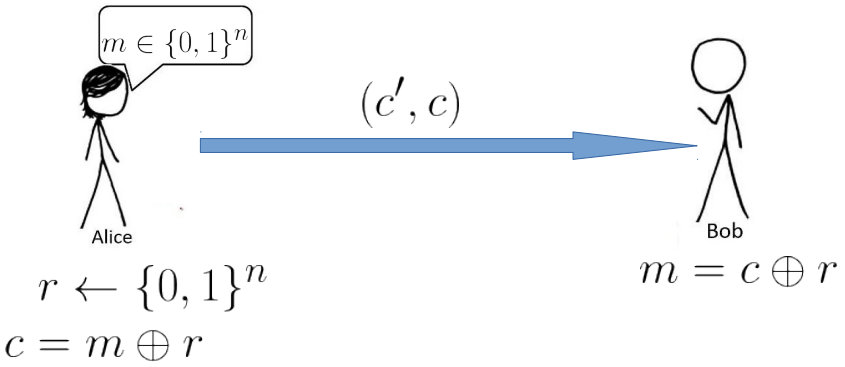
$c' = r^e \pmod N$

2.

c' such that $F(sk, c') = r$

Example

$pk = g^X, r = g^{XY}, c' = g^Y$



Public Key Crypto

1.

$$c' = f(pk, r'), r = H(r')$$

Example

$$c' = r^e \pmod{N}$$

Requires Trapdoor Functions like RSA

2.

$$c' \text{ such that } F(sk, c') = r$$

Example

$$pk = g^X, r = g^{XY}, c' = g^Y$$

Requires one way functions and Key Exchange

Why Post Quantum

- Crypto Motto: Ready for the worst
- Efficient Quantum Algorithm for Factorisation and Discrete Logarithm Problems
  - Shor, Peter W. (1997), "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM J. Comput. 26 (5): 1484–1509, arXiv:quant-ph/9508027v2

Alternatives: Code Based and Lattice Based

- Similar Basic Idea:
  - Error Correcting random code
  - Solving approximate linear equations
- Fast Implementation: Linear operations over a Finite Field.

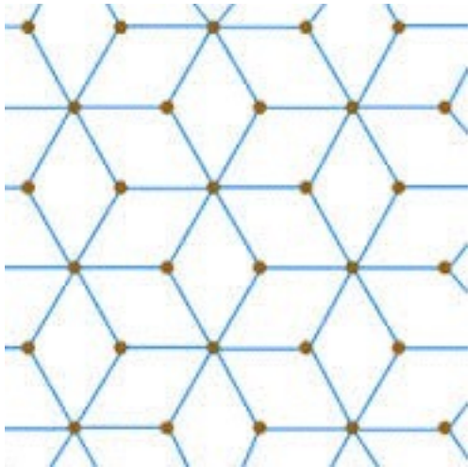
Agenda

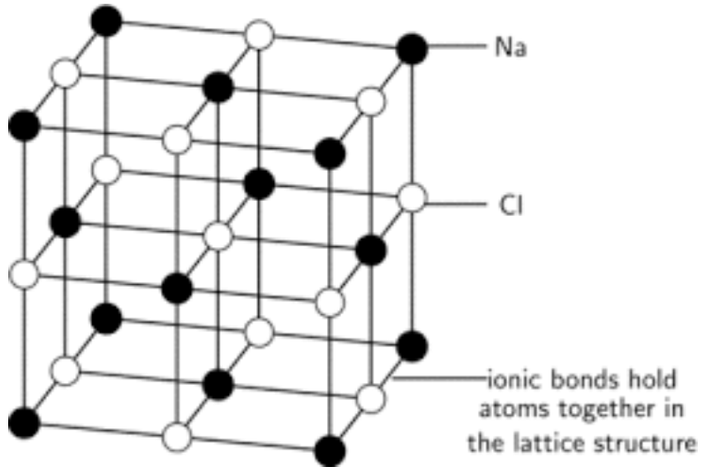
1. A short review of Cryptographic Design
2. Lattice based Encryptions
3. Lattice based Signatures
4. Available Implementations

Lattice

$$\mathbb{R}^n$$

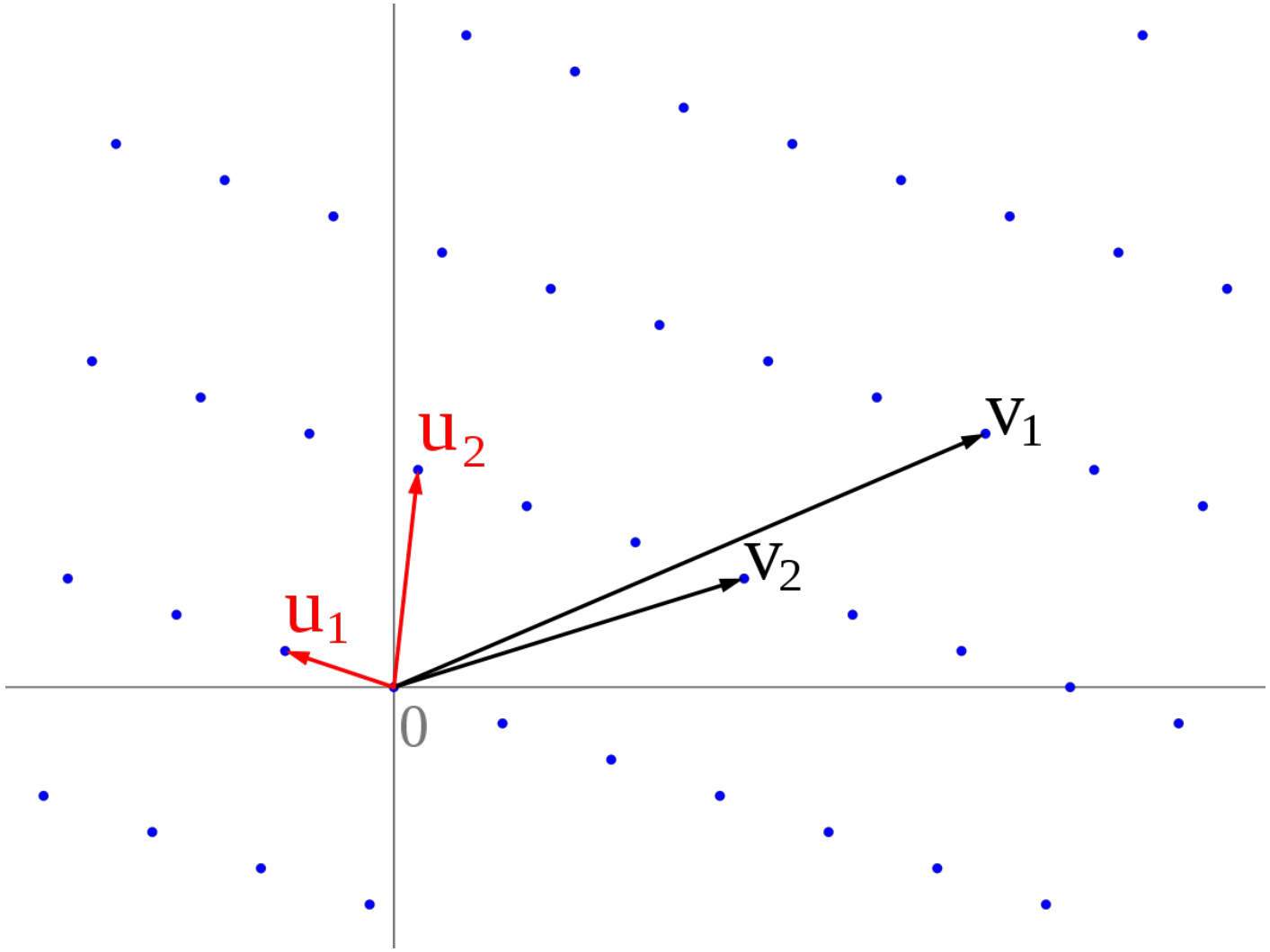
- Discrete Subgroup of





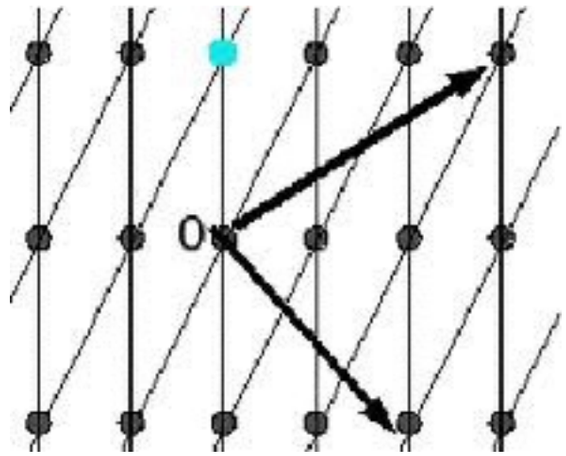
- $$L = \sum_{i=1}^{n} \alpha_i v_i, \alpha_i \in \mathbb{Z}$$

Lattice has Multiple Basis

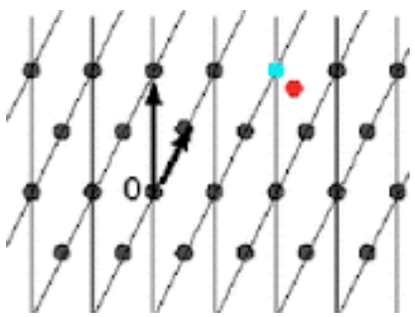


Classical Hard Problems

- Shortest (linearly independent) vector problem



- Closest Vector Problem



Short Integer Solutions

- Solving linear equation is easy.
- What about additional constraints?
- $z = \{-1, 0, 1\}^n$

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Dual Approach: Learning with Error

- How about correcting errors?
- Find solution of approximate linear equations?
- $A \leftarrow \mathbb{Z}_q^{m \times n}$
- $s \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \chi^n$
- $b = As + e$

Question

Distinguish b from uniform.

RoadMap

- Encryption Schemes
  - Regev's Encryption and its dual
  - Subset Sum Encryption
  - Regev's Encryption in Ring-LWE
  - Stehle-Steinfield Encryption
  - NTRU.

RoadMap

- Encryption Schemes
  - Regev's Encryption and its dual
  - Subset Sum Encryption
  - Regev's Encryption in Ring-LWE
  - Stehle-Steinfield Encryption
  - NTRU.
- Signature Schemes
  - Lattice Trapdoor and Hash and Sign
  - Fiat-Shamir with Lattices.