LWE and cryptography

June 5, 2019

Motivation

- Originally as an attempt to solve lattice problems

Motivation

- Originally as an attempt to solve lattice problems
- RSA broken by Shor's algorithm

Intuition

$$14s_1 + 15s_2 + 5s_3 + 2s_4 \approx 8 \pmod{17}$$

$$13s_1 + 14s_2 + 14s_3 + 6s_4 \approx 16 \pmod{17}$$

$$6s_1 + 10s_2 + 13s_3 + s_4 \approx 3 \pmod{17}$$

$$10s_1 + 4s_2 + 12s_3 + 16s_4 \approx 12 \pmod{17}$$

$$9s_1 + 5s_2 + 9s_3 + 6s_4 \approx 9 \pmod{17}$$

$$3s_1 + 6s_2 + 4s_3 + 5s_4 \approx 16 \pmod{17}$$

$$\vdots$$

$$6s_1 + 7s_2 + 16s_3 + 2s_4 \approx 3 \pmod{17}$$

Definition

Let $A_{\vec{s},\chi}$ be a distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ as follows:

Definition

Let $A_{\vec{s},\chi}$ be a distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ as follows:

- Pick $\vec{a} \in \mathbb{Z}_q^n$ uniformly randomly

Definition

Let $A_{\vec{s},\chi}$ be a distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ as follows:

- Pick $\vec{a} \in \mathbb{Z}_q^n$ uniformly randomly
- Pick e according to χ

Definition

Let $A_{\vec{s},\chi}$ be a distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ as follows:

- Pick $\vec{a} \in \mathbb{Z}_q^n$ uniformly randomly
- Pick e according to χ
- Output $(\vec{a}, \langle \vec{a}, \vec{s} \rangle + e)$

Search vs. Decision

Assymetric cryptography

Enc and Dec are separate functions, each parametrized by a key. For a valid key pair (pk, sk), $\mathrm{Dec}_{sk}^{-1} = \mathrm{Enc}_{pk}$.

1. Alice generates "public key" and "secret key"

Assymetric cryptography

Enc and Dec are separate functions, each parametrized by a key. For a valid key pair (pk, sk), $\mathrm{Dec}_{sk}^{-1} = \mathrm{Enc}_{pk}$.

1. Alice generates "public key" and "secret key"
2. Alice sends the public key to Bob

Assymetric cryptography

Enc and Dec are separate functions, each parametrized by a key. For a valid key pair (pk, sk), $\mathrm{Dec}_{sk}^{-1} = \mathrm{Enc}_{pk}$.

1. Alice generates "public key" and "secret key"
2. Alice sends the public key to Bob
3. Bob encrypts the message using public key

Assymetric cryptography

Enc and Dec are separate functions, each parametrized by a key. For a valid key pair (pk, sk), $\mathrm{Dec}_{sk}^{-1} = \mathrm{Enc}_{pk}$.

1. Alice generates "public key" and "secret key"
2. Alice sends the public key to Bob
3. Bob encrypts the message using public key
4. Bob sends the ciphertext to Alice

Assymetric cryptography

Enc and Dec are separate functions, each parametrized by a key. For a valid key pair (pk, sk), $\mathrm{Dec}_{sk}^{-1} = \mathrm{Enc}_{pk}$.

1. Alice generates "public key" and "secret key"
2. Alice sends the public key to Bob
3. Bob encrypts the message using public key
4. Bob sends the ciphertext to Alice
5. Alice decrypts it using the secret key.

Safety

- CPA
- CCA1
- CCA2

Malleability

Homomorphic encryption

References

- O. Regev. The Learning with Errors Problem.
- C. Gentry, A. Sahai, B. Waters. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based.