



@魔女のお茶会 #3

# LWE暗号入門

DiKO



2022/5/22



# Outline

- 自己紹介
- 背景
- **LWE問題**
- **LWE問題を利用した公開鍵暗号方式**





# 自己紹介

Name : DiKO

Like : 暗号と猫

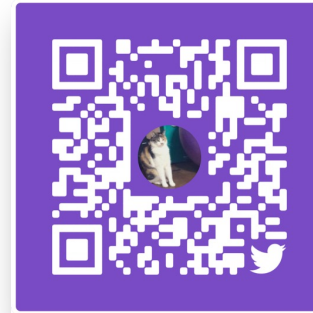
CTF : Crypto

Study : 暗号のハードウェア実装(RNS)  
カードベース暗号

その他

Seccamp2020 : 完全準同型暗号のC++実装

Seccamp2021 : TA



Twitter



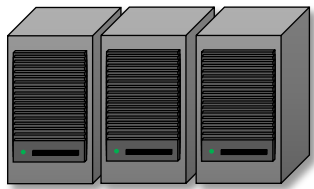
今日の資料



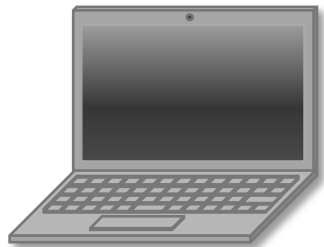


# 背景：Why Post Quantum Cryptography?

これまでの暗号解析

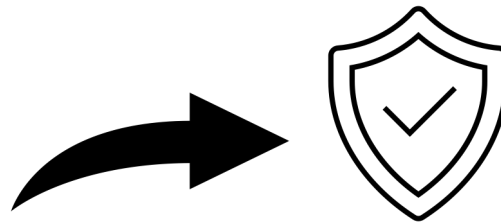


サーバー

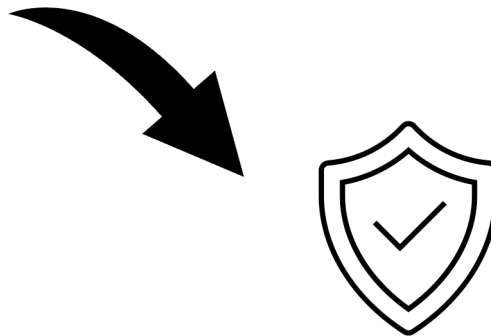


PC

古典計算機



素因数分解問題



楕円曲線上の  
離散対数問題

RSA暗号

楕円曲線暗号

データ





# 背景：Why Post Quantum Cryptography?

量子コンピュータの研究開発



<https://www.ibm.com>



素因数分解問題

楕円曲線上の  
離散対数問題

RSA暗号

PQC

楕円曲線暗号

データ

量子コンピュータでも解けない暗号が必要！





# NIST PQC Standardization

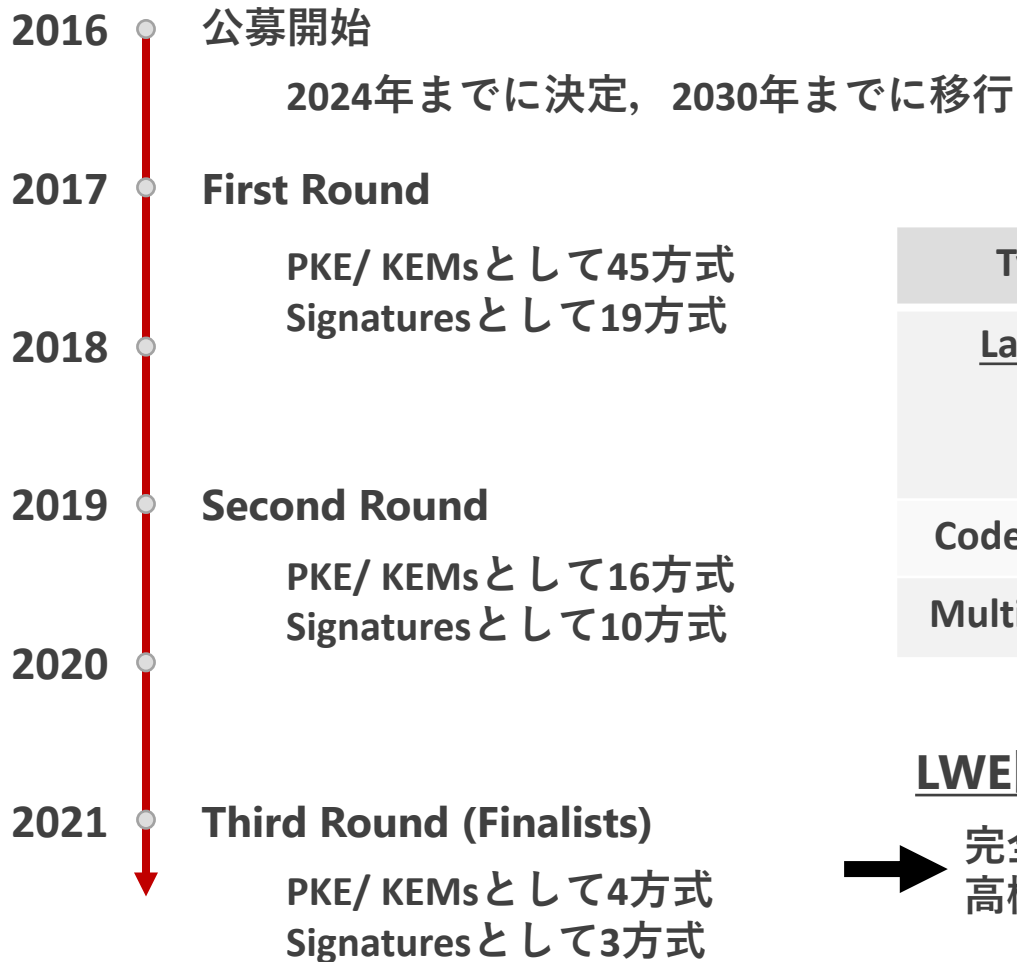


Table.1 Third Round Candidate

Type	PKE/KEMs	Signatures
<u>Lattice</u>	<u>CRYSTALS-Kyber</u> NTRU <u>Saber</u>	<u>Dilithium</u> Falcon
Code-based	Classic McEliece	
Multivariate		Rainbow

## LWE問題ベース



完全準同型暗号を構成可能なことから  
高機能暗号としても注目







# LWE問題

$e$ があることで困難化

$(\text{mod } q)$

$$\begin{array}{c} n \times 1 \\ \text{B} \end{array} - \begin{array}{c} n \times n \\ \text{A} \end{array} \times \begin{array}{c} n \times 1 \\ \text{S} \end{array} = \begin{array}{c} n \times 1 \\ \text{e} \end{array}$$

秘密ベクトル

$s$ を知っていれば  $B - A \cdot s = e$  で  $e$  を計算し、 $B$  から  $e$  を取り除くことができる  
 $e$  を取り除くことができれば、 $(A, B)$  から  $s$  を求めることができる！







# LWE問題を用いた公開鍵暗号

どうやって暗号を作るか？

## Regev方式

- 最初に提案されたLWE問題ベースの公開鍵暗号方式
- 平文を1bit ずつ暗号化
- 今日はこれ

## Peikert方式

- LWE問題を少し拡張して平文をまとめて暗号化できる
- GitHubに簡単な実装を書いたので興味があれば  
(暗号化して復号できるレベル)

## その他沢山





# LWE問題を用いた公開鍵暗号

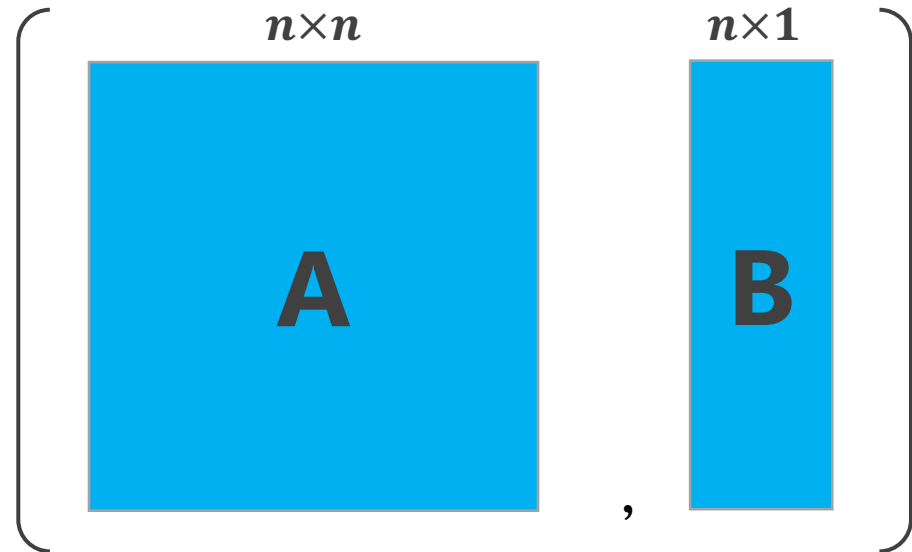
## 鍵生成

秘密鍵は  $sk = s \leftarrow \mathbb{F}_q^n$   
公開鍵は  $pk = (A, B) = (A, A \cdot s + e \pmod{q})$  探索問題の困難性から  $s$  は漏れない

秘密鍵  $sk$



公開鍵  $pk$

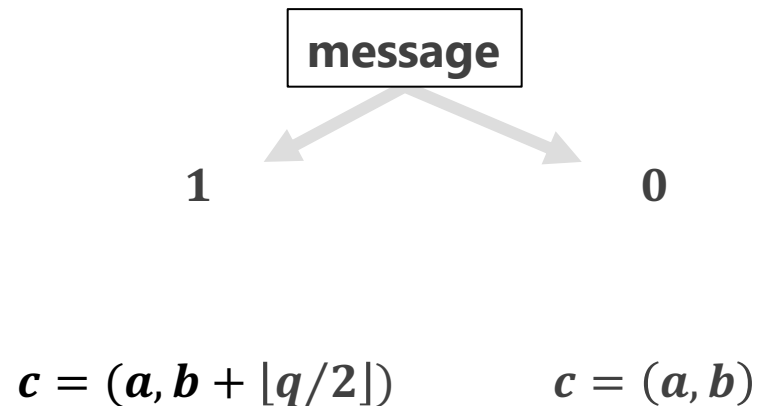
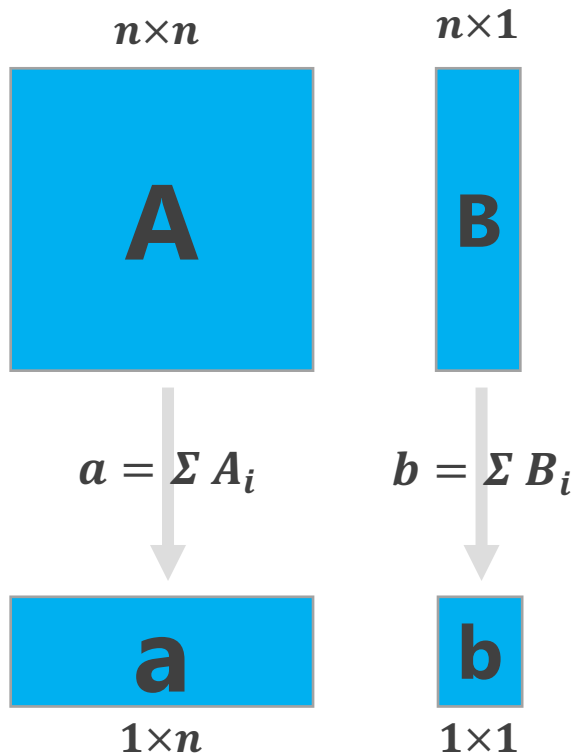




# LWE問題を用了公開鍵暗号

## 暗号化

✖ 平文を1bitずつ暗号化する





# LWE問題を用いた公開鍵暗号

復号

$$sk = s, c = (a, b)$$

1×1

**b**

−

**a**

×

**s**

=

?

$< \lfloor q/2 \rfloor$

0

$> \lfloor q/2 \rfloor$

1

$$b - a \cdot s < \lfloor q/2 \rfloor$$

Yes

No

0

1

$$b - a \cdot s = (a \cdot s + e) - a \cdot s$$

0の時

or

$$= (a \cdot s + \underline{e + \lfloor q/2 \rfloor}) - a \cdot s \quad 1の時$$

ここで $\lfloor q/2 \rfloor$ より大きくなっている





# LWE問題を用いた公開鍵暗号

Alice

鍵生成

$$pk = (A, B = A \cdot s + e) \pmod{q}$$

$$sk = s$$

復号

$$\text{if } b - a \cdot s \pmod{q} < \lfloor q/2 \rfloor$$

$$m[i] = 0$$

else

$$m[i] = 1$$

Bob

$$m = \{110100 \dots\}$$

$$pk = (A, B)$$

暗号化

$$a = \sum A_i, b = \sum B_i$$

if  $m[i] = 0$

$$c = (a, b) \pmod{q}$$

if  $m[i] = 1$

$$c = (a, b + \lfloor q/2 \rfloor) \pmod{q}$$

⋮

$c[i]$

$pk$





# 最近はRing-LWE問題が人気！

全て多項式環  $\mathbb{Z}_q/x^n + 1$  上の計算に置き換えた

$$\begin{array}{c} n \\ \text{A} \end{array} \times \begin{array}{c} n \\ \text{s} \end{array} + \begin{array}{c} n \\ \text{e} \end{array} = \begin{array}{c} n \\ \text{B} \end{array} \quad \begin{array}{c} n \\ \text{B}' \end{array}$$

探索問題：  $(A[x], B[x] = A[x] \cdot s[x] + e[x])$  が与えられたとき，  $s$  を求める問題

判定問題：  $(A, B), (A, B')$  が与えられたとき， どちらが  $B$  かを判定する問題

