LWE暗号入門

DiKO

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

Twitter

今日の資料

Name : DiKO

Like　: 暗号と猫

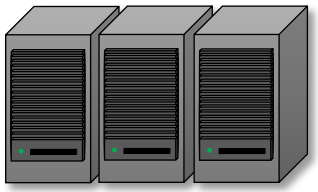
CTF　: Crypto

Study : 暗号のハードウェア実装(RNS)
カードベース暗号

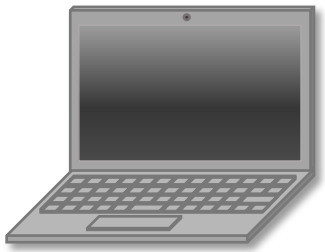
その他
Seccamp2020：完全準同型暗号のC++実装
Seccamp2021：TA

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

RSA暗号

楕円曲線上の
離散対数問題

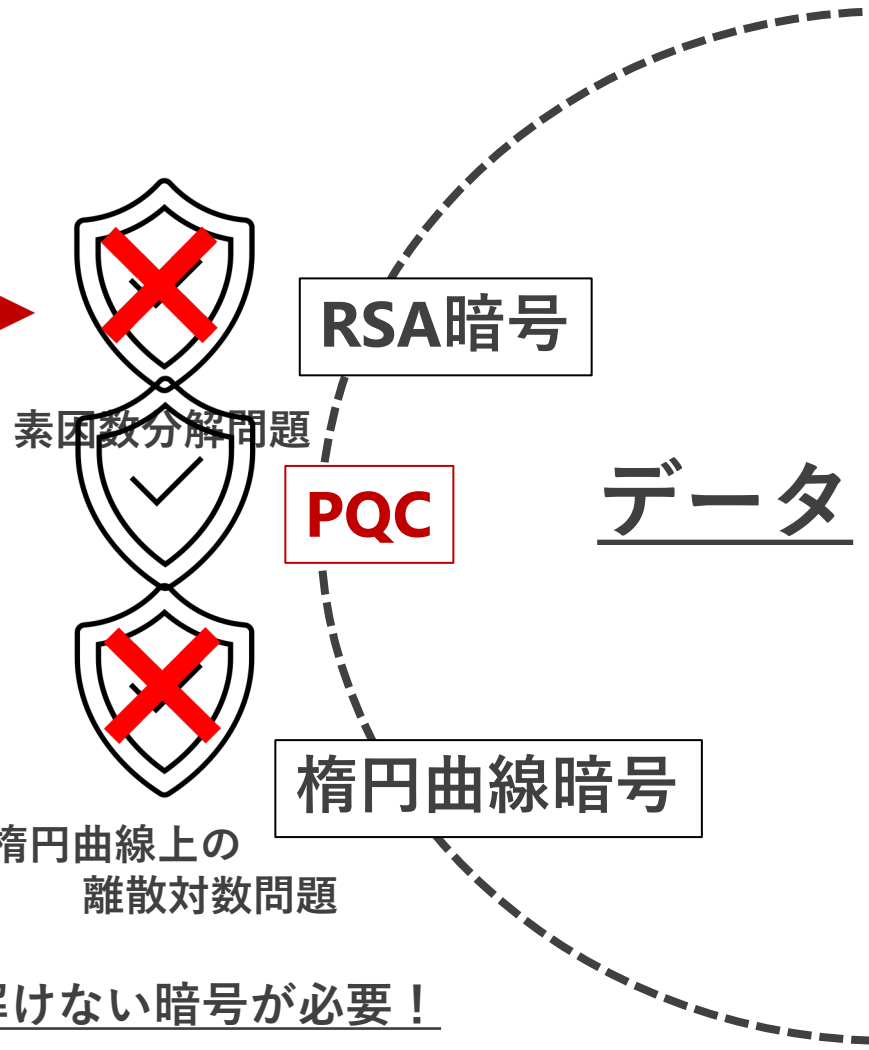
楕円曲線暗号

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



量子コンピュータでも解けない暗号が必要！

NIST PQC Standardization

2016 公募開始

2024年までに決定，2030年までに移行

2017 **First Round**

PKE/ KEMsとして45方式
Signaturesとして19方式

2018

2019 **Second Round**

PKE/ KEMsとして16方式
Signaturesとして10方式

2020

2021 **Third Round (Finalists)**

PKE/ KEMsとして4方式
Signaturesとして3方式

Table.1 Third Round Candidate

Type	PKE/KEMs	Signatures
Lattice	CTYSTALS-Kyber NTRU Saber	Dilithium Falcon
Code-based	Classic McEliece	
Multivariate		Rainbow

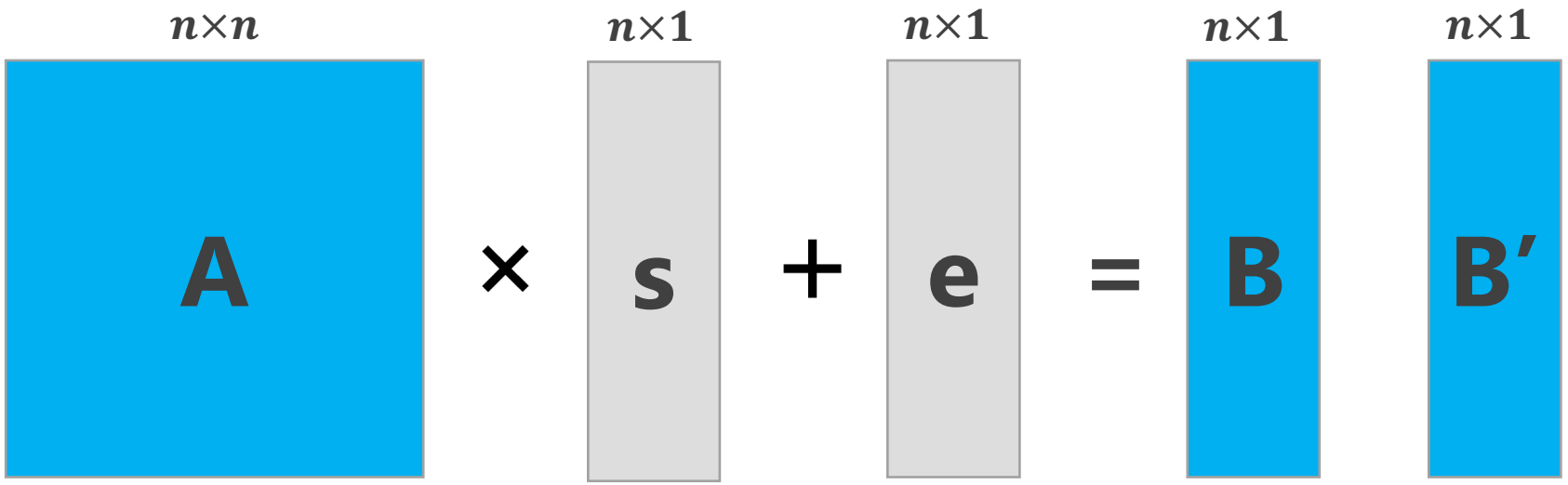
LWE問題ベース

→ 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

$(\mathrm{mod}\ q)$



秘密ベクトル

ランダム

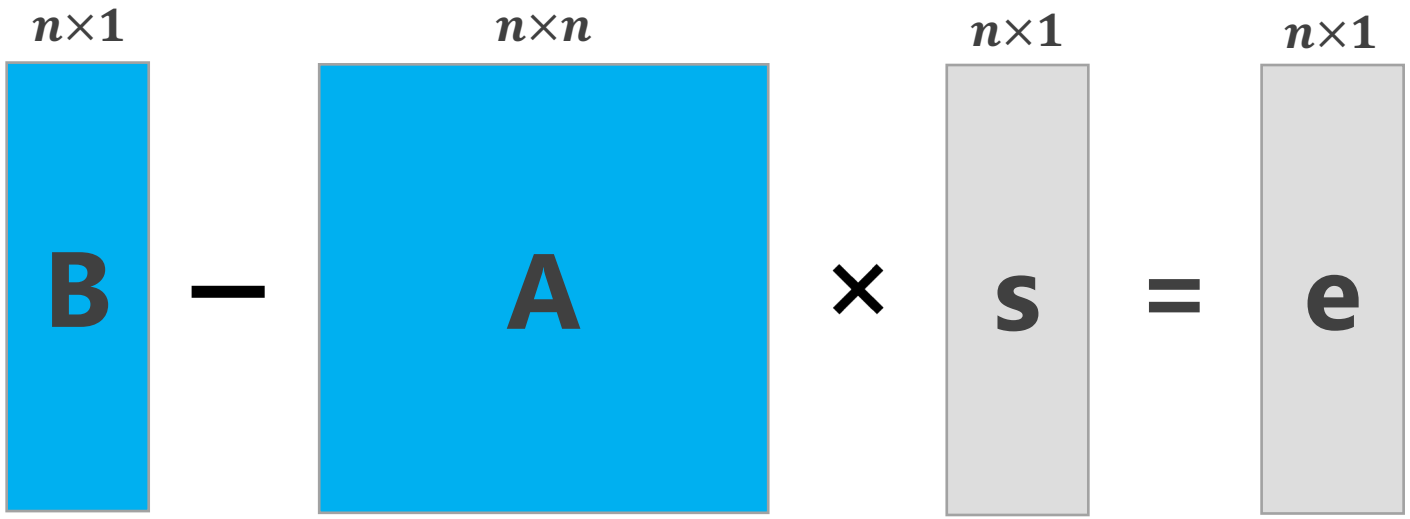
探索問題：A,Bが与えられたとき，sを求める問題

判定問題：B,B′が与えられたとき，Bがどちらか判定する問題

LWE問題

eがあることで困難化

$(\mathrm{mod}\ q)$



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てみたので興味があれば（暗号化して復号できるレベル）

LWE問題を用いた公開鍵暗号

Alice

鍵生成

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

$sk = s$

pk →

Bob

$m = \{110100 \cdots\}$

$pk = (A, B)$

暗号化

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

if $m[i] = 0$

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

if $m[i] = 1$

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

← $c[i]$

復号

$\mathrm{tmp} = b - a \cdot s \pmod q$

if $\mathrm{tmp} < \lfloor q/2 \rfloor$

$m[i] = 0$

else

$m[i] = 1$

⋮

LWE問題を用いた公開鍵暗号

鍵生成

秘密鍵は $sk = s$

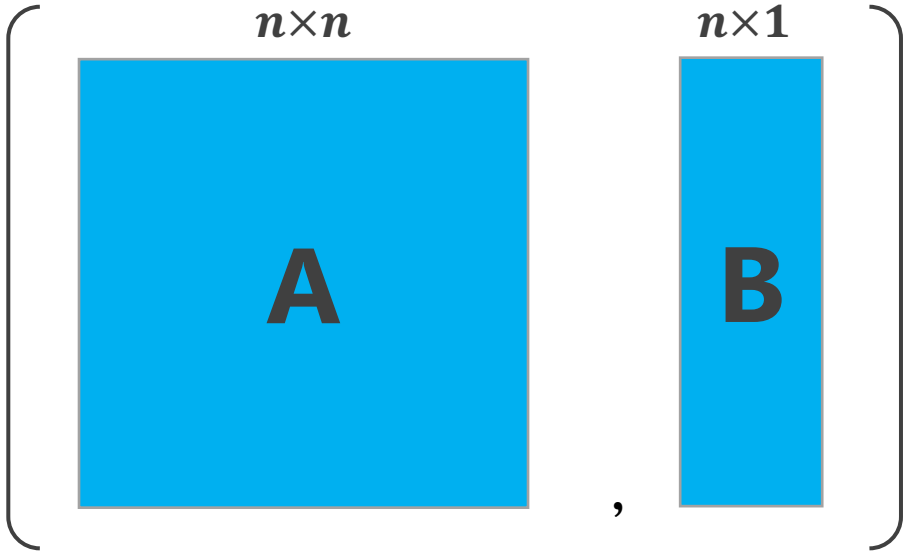
公開鍵は $pk = (A, B) = (A, A \cdot s + e \pmod q)$　探索問題の困難性から s は漏れない

秘密鍵 sk

$n \times 1$

公開鍵 pk

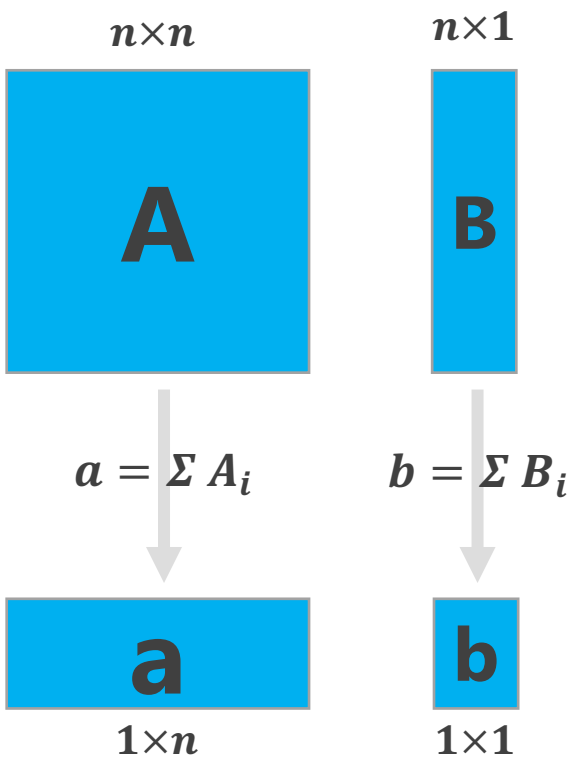
$n \times n$　　$n \times 1$

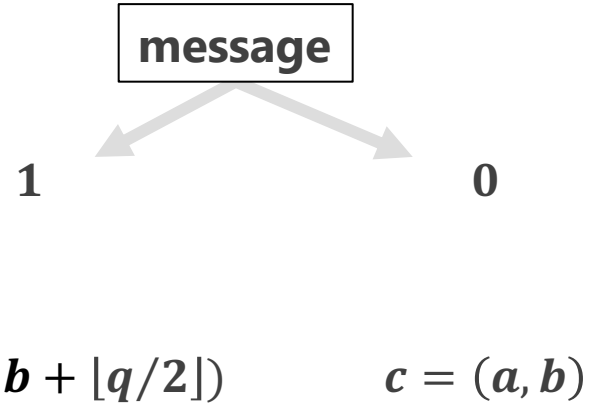


LWE問題を用いた公開鍵暗号

暗号化

※ 平文を1bitずつ暗号化する

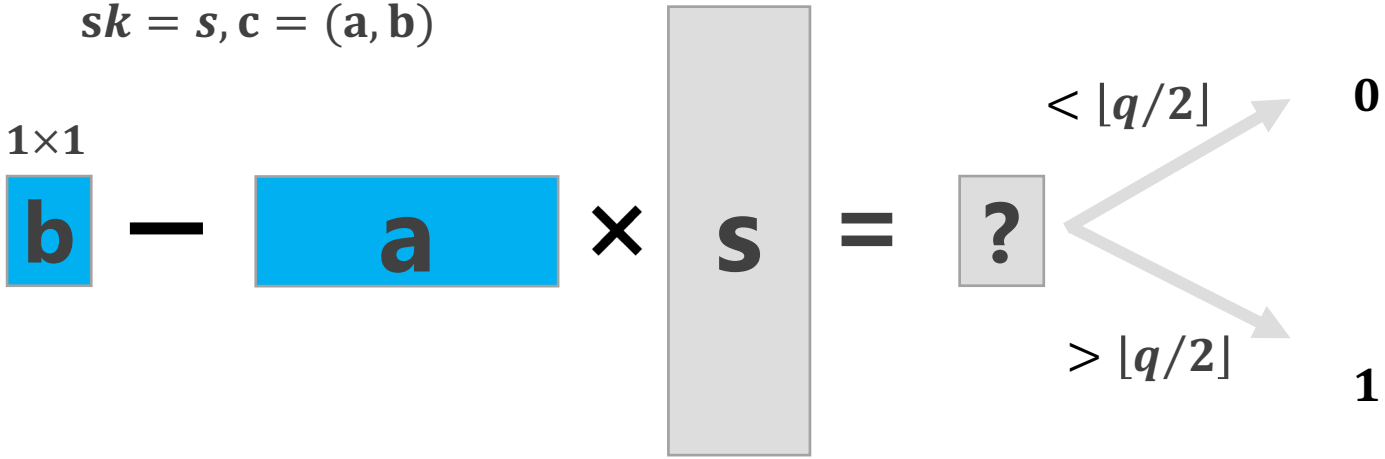




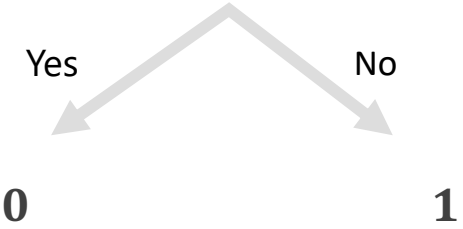
LWE問題を用いた公開鍵暗号

復号

$sk = s, \mathbf{c} = (\mathbf{a}, \mathbf{b})$



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



$b - a \cdot s = (a \cdot s + e) - a \cdot s$ 0の時

or

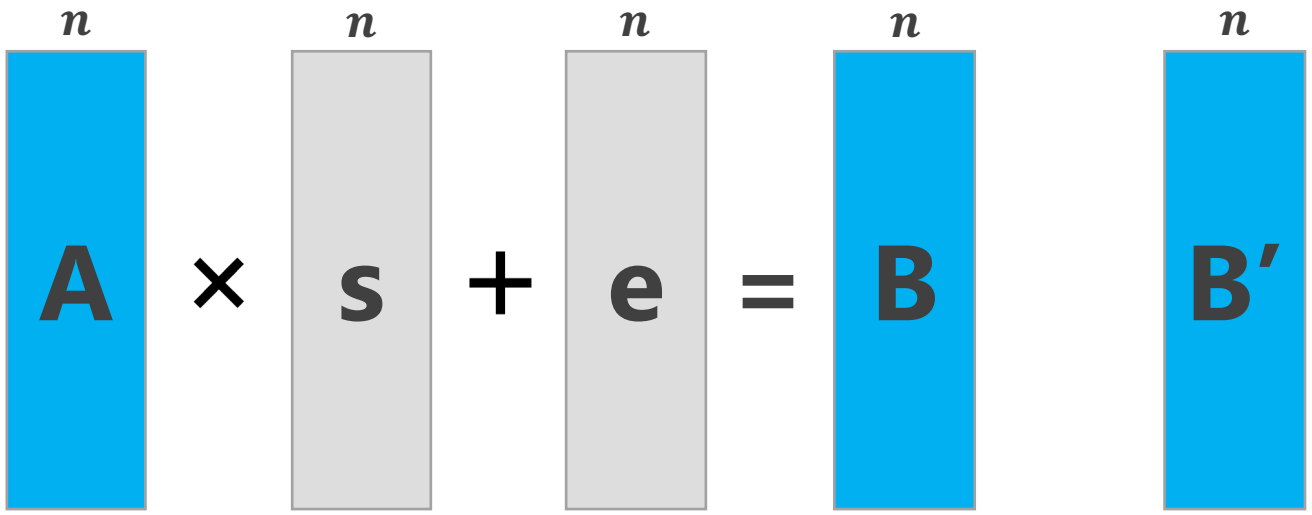
$= (a \cdot s + e + \lfloor q/2 \rfloor) - a \cdot s$ 1の時

ここで$\lfloor q/2 \rfloor$より大きくなっている

終わり

R-LWE問題

多項式環 $\mathbb{Z}_q/x^n+1$ 上の計算



探索問題：A,Bが与えられたとき，sを求める問題

判定問題：B,B′が与えられたとき，Bがどちらか判定する問題