Mersenne 数を用いた公開鍵暗号システムについて

AJPS Public-Key Cryptosystem

手塚 真徹　　　田中 圭介

東京工業大学

Version: 2020/12/23

※ 本スライドは2018年CREST暗号数理ミニワークショップ
「未解決問題ワークショップ」の前半スライドである.

Mersenne 数を用いた公開鍵暗号システム

Aggrawal，Joux，Prakash，Sanatha [AJP+18] (CRYPTO 2018)

メルセンヌ数に関連する，新たな計算困難な問題を

ベースとした暗号方式を提案した.

本発表では AJPS 公開鍵暗号方式の概略を解説する.

[AJP+18] Divesh Aggarwal, Antoine Joux, Anupam Prakash, Miklos Santha:
A New Public-Key Cryptosystem via Mersenne Numbers: CRYPTO2018

AJPS 暗号方式の解説

- □ AJPS 公開鍵暗号方式の提案の動機
- □ メルセンヌ数の性質
- □ メルセンヌ数に関連した計算困難な問題
- □ 1ビットメッセージ AJPS 公開鍵暗号方式
- □ 多ビットメッセージ AJPS 公開鍵暗号方式

公開鍵暗号の歴史

1976年　Diffie，Hellman

➡ 公開鍵暗号の概念を提案

1978年　Rivest，Shamir，Adleman

➡ RSA暗号：　RSA仮定（素因数分解と関連あり）

1984年　ElGamal

➡ エルガマル暗号：　離散対数問題

公開鍵暗号の歴史

1976年　Diffie，Hellman

➡ 公開鍵暗号の概念を提案

量子コンピュータ
1997年
Shorのアルゴリズム

1978年　Rivest，Shamir，Adleman

➡ RSA暗号：　~~RSA仮定（素因数分解と関連あり）~~

1984年　ElGamal

➡ エルガマル暗号：　~~離散対数問題~~

耐量子暗号

暗号に利用される数学問題の種類

- 格子
- 符号
- 多変数多項式
- ハッシュ関数
- 同種写像
- その他

耐量子暗号

暗号に利用される数学問題の種類

- 格子
- 符号
- 多変数多項式
- ハッシュ関数
- 同種写像
- その他

本発表の暗号

AJPS

AJPS 暗号方式の解説

- □ AJPS 公開鍵暗号方式の提案の動機
- □ メルセンヌ数の性質
- □ メルセンヌ数に関連した計算困難な問題
- □ 1ビットメッセージ AJPS 公開鍵暗号方式
- □ 多ビットメッセージ AJPS 公開鍵暗号方式

メルセンヌ素数とは

メルセンヌ素数 p とは

$$p = 2^n - 1 \quad (n\text{: 素数})$$

の形で表せる素数のこと.

メルセンヌ素数 $p = 2^n - 1$ を n bit で表すと,

$$\underbrace{11 \ldots \ldots \ldots 1}_{n}$$

となる.

メルセンヌ素数を法とした算術

メルセンヌ素数: $p = 2^n - 1$

$A, B \ \in \ \{0,1\}^n$

加法 $A + B$, 乗法　$A \times B$ を次のように定める.

$$A + B = seq(int(A) + int(B) \ \ mod\, p)$$

$$A \cdot B = seq(int(A) \cdot int(B)\, mod\, p)$$

ハミング重み

二進文字列 A のハミング重みとは

文字列 A の中の 1 であるビットの総数.

例.

$A = \boxed{1\,0\,1\,1\,0\,0\,1}$ $Ham(A) = 4$

※（メルセンヌ素数: $p = 2^n - 1$に対して

文字列(1^n) のハミング重みは 0 とする.

$\rightarrow Ham(1^n) = Ham(seq(int\ (1^n)\ mod\ p) = Ham(0)$.

メルセンヌ素数とハミング重み

メルセンヌ素数: $p = 2^n - 1,\ \ A, B\ \in\ \{0,1\}^n$

次のハミング重みの評価式が成り立つ.

$$Ham(A + B) \leq Ham(A) + Ham(B)$$

$$Ham(A \cdot B) \leq Ham(A) \times Ham(B)$$

$$Ham(-A) \leq n - Ham(A) \quad (\ A \neq\ 0^n\ )$$

AJPS 暗号方式の解説

- □ AJPS 公開鍵暗号方式の提案の動機
- □ メルセンヌ数の性質
- □ メルセンヌ数に関連した計算困難な問題
- □ 1ビットメッセージ AJPS 公開鍵暗号方式
- □ 多ビットメッセージ AJPS 公開鍵暗号方式

Mersenne Low Hamming Ratio Assumption

メルセンヌ素数: $p = 2^n - 1$, パラメータ: h

R : ランダム n bit 文字列

A, B : ハミング重み h のランダム n bit 文字列

Mersenne Low Hamming Ratio Assumption

$$R \;\; and \;\; seq\left(\frac{int(A)}{int(B)}\right)$$

を識別することが困難である.

Mersenne Low Hamming Combination Assumption

メルセンヌ素数: $p = 2^n - 1$, パラメータ: h

R_1, R_2, R_3, R_4: ランダム n bit 文字列

A, B_1, B_2 : ハミング重み h のランダム n bit 文字列

Mersenne Low Hamming Combination Assumption

$$\begin{pmatrix} R_1 & R_1 \cdot A + B_1 \\ R_2 & R_2 \cdot A + B_2 \end{pmatrix} \ and \ \begin{pmatrix} R_1 & R_3 \\ R_2 & R_4 \end{pmatrix}$$

を識別することが困難である.

AJPS 暗号方式の解説

- □ AJPS 公開鍵暗号方式の提案の動機
- □ メルセンヌ数の性質
- □ メルセンヌ数に関連した計算困難な問題
- □ 1ビットメッセージのAJPS公開鍵暗号方式
- □ 多ビットメッセージのAJPS公開鍵暗号方式

公開鍵暗号方式

公開鍵暗号方式 PKE = (KeyGen, Enc, Dec)

$$pp \longrightarrow \boxed{\text{KeyGen}} \longrightarrow (pk, sk)$$

$$(pk, m) \longrightarrow \boxed{\text{Enc}} \longrightarrow c$$

$$(sk, c) \longrightarrow \boxed{\text{Dec}} \longrightarrow m \ \ or \ \ \perp$$

公開鍵暗号方式

公開鍵暗号方式 PKE = (KeyGen, Enc, Dec)

$$pp \longrightarrow \boxed{\text{KeyGen}} \longrightarrow (pk, sk)$$

$$(pk, m) \longrightarrow \boxed{\text{Enc}} \longrightarrow c$$

$$(sk, c) \longrightarrow \boxed{\text{Dec}} \longrightarrow m \ \ or \ \ \perp$$

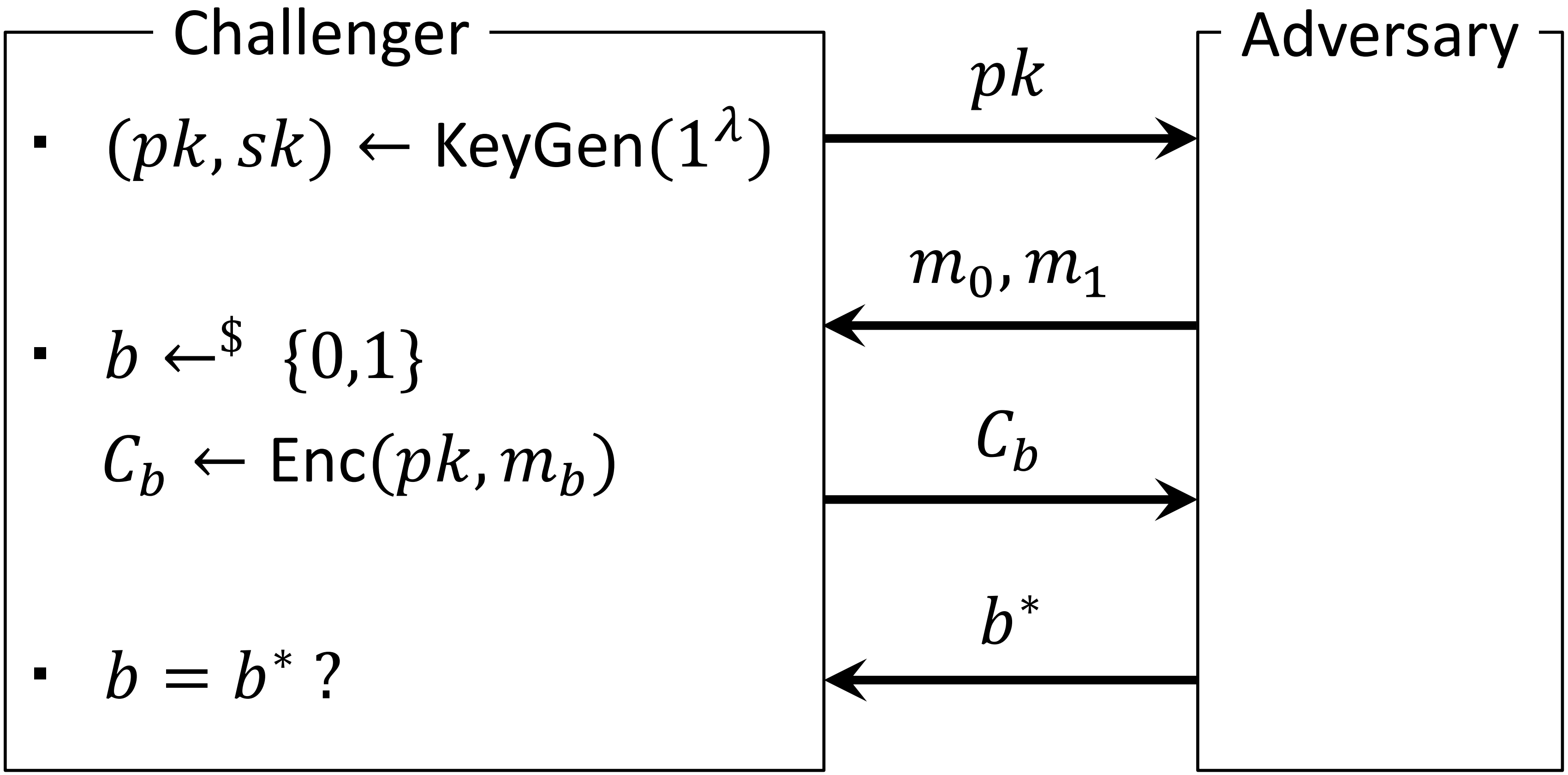
正当性

$\forall m \in M, \quad \forall (pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$ に対し,

$\text{Dec}(sk, \text{Enc}(pk, m)) = m$

公開鍵暗号方式の安全性

Semantically security (IND-CPA)



1ビットメッセージ AJPS 公開鍵暗号方式

$pp = (\lambda, p = 2^n - 1, h)$

KeyGen(pp)

- Choose n bits strings F, G s.t

  $\mathrm{Ham}(F) = \mathrm{Ham}(G) = h$

- $pk := H = seq\left(\dfrac{int(F)}{int(G)}\right), \quad sk := G$

- Return (pk, sk)

1ビットメッセージ AJPS 公開鍵暗号方式

$\mathrm{Enc}(pk = H, b)$

- Choose n bits strings A, B s.t

  $\mathrm{Ham}(A) = \mathrm{Ham}(B) = h$

- Return $C \coloneqq (-1)^b (A \cdot H + B)$

$\mathrm{Dec}(sk = G, C)$

- Compute $C \cdot G = (-1)^b (A \cdot F + B \cdot G)$
- If $\mathrm{Ham}(C \cdot G) \leq 2h^2$, return 1
- If $\mathrm{Ham}(C \cdot G) \geq n - 2h^2$, return 0

1ビットメッセージ AJPS の正当性

正当性　（ $b=0$ のとき）　$H=seq\left(\frac{int(F)}{int(G)}\right)$

- $C\cdot G=(A\cdot H+B)\cdot G=(A\cdot F+B\cdot G)$

$$Ham(C\cdot G)\le Ham(A\cdot F)+Ham(B\cdot G)$$
$$\le Ham(A)\times Ham(F)$$
$$+Ham(B)\times Ham(G)\le 2h^2$$

$$\boxed{\begin{aligned}&Ham(A+B)\le Ham(A)+Ham(B)\\&Ham(A\cdot B)\le Ham(A)\times Ham(B)\end{aligned}}$$

1ビットメッセージ AJPS の正当性

正当性　（ $b=1$ のとき）　$H = seq\left(\dfrac{int(F)}{int(G)}\right)$

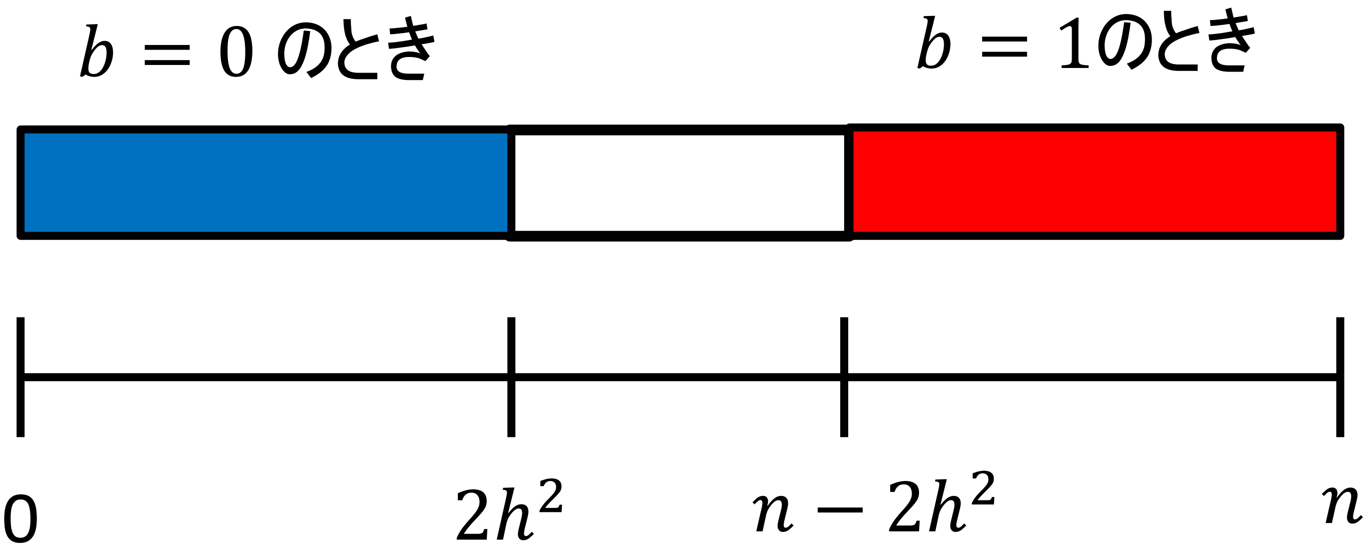
- $C \cdot G = -(A \cdot F + B \cdot G)$

$$Ham(C \cdot G) = n - Ham(A \cdot F + B \cdot G)$$
$$\geq n - 2h^2$$

$$\boxed{Ham(-A) \leq n - Ham(A) \quad (A \neq 0^n)}$$

1ビットメッセージ AJPS の正当性

$Ham(C \cdot G)$



正当性は，$4h^2 < n$ のときに成り立つ.

1ビットメッセージ AJPS の安全性

Mersenne Low Hamming Ratio Assumption が成り立つ

⇨ 1ビットメッセージ AJPS は Semantically Secure

である.

Mersenne Low Hamming Ratio Assumption

$$R \quad and \quad seq\left(\frac{int(A)}{int(B)}\right)$$

を識別することが困難である.

AJPS 暗号方式の解説

- □ AJPS 公開鍵暗号方式の提案の動機
- □ メルセンヌ数の性質
- □ メルセンヌ数に関連した計算困難な問題
- □ 1ビットメッセージ AJPS 公開鍵暗号方式
- □ 多ビットメッセージ AJPS 公開鍵暗号方式

誤り訂正符号 (Error Correcting Code)

誤り訂正符号

データを記録・伝送する際に発生する誤りを
受け手の側で検出し、訂正することができる
ように付加される符号.

多ビットメッセージ AJPS 公開鍵暗号方式

$pp = (\lambda, p = 2^n - 1, h)$

KeyGen(pp)

- Choose n bits strings F, G s.t

  $\mathrm{Ham}(F) = \mathrm{Ham}(G) = h$

- Choose n bits string R
- $pk \coloneqq (R, T) = (R, F \cdot R + G), \quad sk \coloneqq F$
- Return (pk, sk)

多ビットメッセージ AJPS 公開鍵暗号方式

$\mathcal{E}$: error correcting encoding algorithm

Enc$(pk = (R, T), m)$

- Choose n bits strings A, B_1, B_2 s.t

  $$\mathrm{Ham}(A) = \mathrm{Ham}(B_1) = \mathrm{Ham}(B_2) = h$$

- $C_1 \coloneqq A \cdot R + B_1$
- $C_2 \coloneqq (A \cdot T + B_2) \oplus \mathcal{E}(m)$
- Return $C \coloneqq (C_1, C_2)$

多ビットメッセージ AJPS 公開鍵暗号方式

$\mathcal{D}$: error correcting decoding algorithm

Dec$(sk = F, C)$

- Parse C as (C_1, C_2)
- Compute $\widetilde{m} := \mathcal{D}((F \cdot C_1) \oplus C_2)$
- Return $\widetilde{m}$

多ビットメッセージ AJPS の復号

$$(F \cdot C_1) \oplus C_2$$

$$= F \cdot (A \cdot R + B_1) \oplus (A \cdot T + B_2) \oplus \mathcal{E}(m)$$

$$= (A \cdot F \cdot R + B_1 \cdot F) \oplus (A \cdot T + B_2) \oplus \mathcal{E}(m)$$

$$= (A \cdot (T - G) + B_1 \cdot F)\,) \oplus (A \cdot T + B_2) \oplus \mathcal{E}(m)$$

$$= \boxed{((A \cdot T + B_2)\ \boxed{- B_2 - A \cdot G + B_1 \cdot F})}$$

$$\oplus \boxed{(A \cdot T + B_2)} \oplus \mathcal{E}(m)$$

復号は $\boxed{F \cdot C_1}$ と $\boxed{C_2}$ のハミング距離が低くなると

期待できることを利用．（復号の失敗の可能性あり）

多ビットメッセージ AJPS の安全性

Mersenne Low Hamming Combination Assumption

が成り立つ.

⇨ 多ビットメッセージ AJPS は Semantically Secure .

Mersenne Low Hamming Combination Assumption

$$\begin{pmatrix} R_1 & R_1 \cdot A + B_1 \\ R_2 & R_2 \cdot A + B_2 \end{pmatrix} \ and \ \begin{pmatrix} R_1 & R_3 \\ R_2 & R_4 \end{pmatrix}$$

を識別することが困難である.