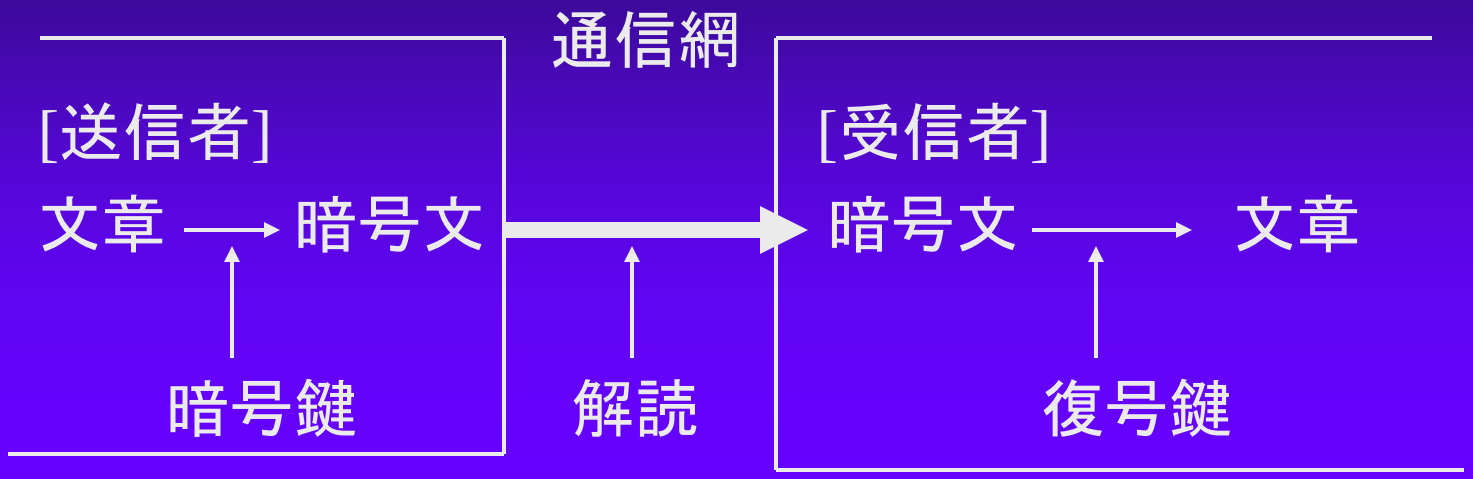
暗号理論
(研究内容の紹介)

原澤研究室

暗号とは

- 情報を送る際、送信者，受信者以外の人物が、その情報の内容を理解することが困難となるように構成されたもの
  （葉書の内容ならば、郵便局員にばれる）
- 重要な情報を送るためには、暗号の技術が必要不可欠

暗号システム



[解読されないためには] 復号鍵の計算が困難
(当事者(本人)以外: 復号鍵は分からない)

[秘密鍵暗号] 暗号鍵: 秘密
（暗号鍵が分かると，復号鍵が容易に分かる）

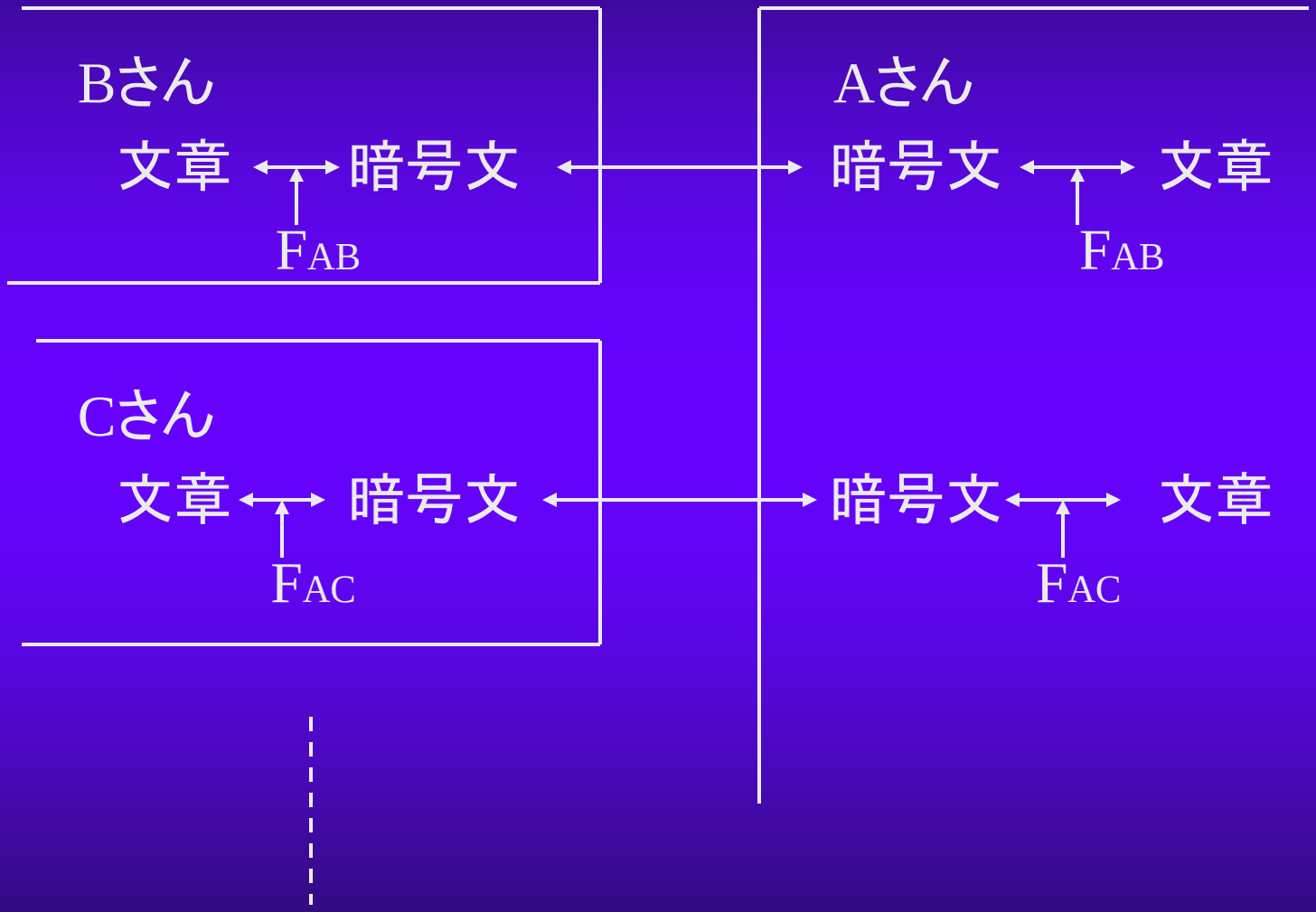
[公開鍵暗号] 暗号鍵：公開
（暗号鍵が分かっても，復号鍵を求めることが困難）

秘密鍵暗号系

登録者	暗号鍵＝復号鍵
Aさん	F_{AB} , F_{AC}, … (F_{AB}：Bさんとの通信用, F_{AC}：Cさんとの通信用, …)
Bさん	F_{AB}, F_{BC}, … (F_{AB}：Aさんとの通信用, F_{BC}：Cさんとの通信用, …)
Cさん	F_{AC}, F_{BC}, … (F_{AC}：Aさんとの通信用, F_{BC}：Bさんとの通信用, …)
⋮	⋮

この名簿は非公開（秘密）

秘密鍵暗号システム



秘密鍵暗号の問題点

- ユーザの人数分だけ秘密鍵を所有
  ⟶　不特定多数との通信には不向き
- 秘密鍵の送信方法(共有方法)の実現性

↓

公開鍵暗号の登場

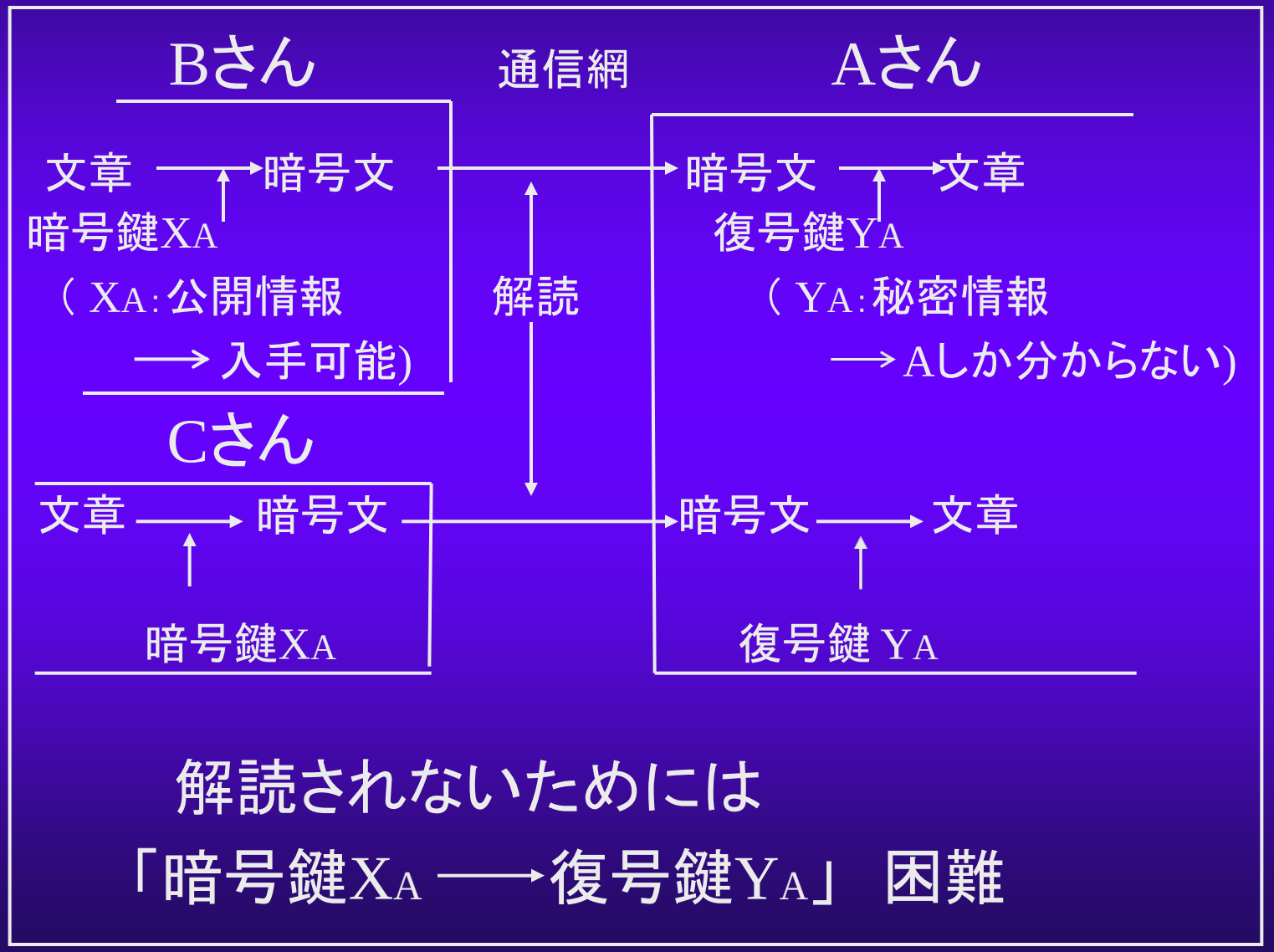
公開鍵暗号系

登録者	暗号鍵 (公開)	復号鍵 (秘密)
Aさん	X_A	Y_A
Bさん	X_B	Y_B
Cさん	X_C	Y_C
⋮	⋮	⋮

各ユーザの暗号鍵は電話帳（などの形）で公開しておく

→　公開鍵認証局の必要性(公開鍵の正当性を保証するため)

公開鍵暗号システム



解読されないためには

「暗号鍵X_A ⟶ 復号鍵Y_A」 困難

[応用] ディジタル署名

・ディジタル署名（電子印鑑）

→ 本人確認

[暗号と逆の手順]

メッセージMに対して

[暗号] Aさんにメッセージを送る

M → 暗号文 → M

Aの公開鍵　　Aの秘密鍵

[署名] Aさんがメッセージを送る

M → (M, 署名) → (M, 本人確認)

Aの秘密鍵　　Aの公開鍵

・受信者はAからのメッセージだと確認できる

(Aの秘密鍵を知っているのはAのみ)

公開鍵暗号の構成(概要)

[前提] 攻撃者(解読者)が，暗号鍵(公開鍵)を得ている

「暗号鍵X_A ⟶ 復号鍵Y_A」 困難？

復号鍵: 暗号鍵の逆の手順で得られる

暗号化(容易)

文章 ⇄ 暗号文

復号(困難)

- 一方向性関数の必要性

⟶ 数学 (数の構造，etc)

一方向性関数の例(RSA暗号)

- 2つの大きな素数 p, q (300桁以上)

積(容易)

$$p, q \rightleftharpoons n = p\,q$$

因数分解(困難)

- 例) p=47459, q=53087

$\longleftrightarrow$ n=2519455933

数の特徴(ほんの一例)

[素数の性質]

- p: 素数,　a: 自然数(整数)

↓

a^p を p で割った余り ＝ a を p で割った余り

→ 元に戻る（復号可能)

例） p = 5

$1^5 = 1$,　$2^5 = 32$,　$3^5 = 243$,　$4^5 = 1024$

$5^5 = 3125$,　$6^5 = 7776$,　---------

一方向性関数の例
(離散対数型暗号)

- p: 大きな素数(600桁以上)，　a: 整数

指数計算(容易)

x:整数 ⇄ $y = a^x$ を p で割った余り

対数計算(困難)

指数(累乗)計算

例: a^{12}の計算に必要な乗算回数

1) $a \longrightarrow a^2 \longrightarrow a^3 \longrightarrow \cdots\cdots \longrightarrow a^{11} \longrightarrow a^{12}$

$\longrightarrow$ 11回の乗算

2) $a \longrightarrow a^2 \longrightarrow a^3 \xrightarrow{2乗} a^6 \xrightarrow{2乗} a^{12}$

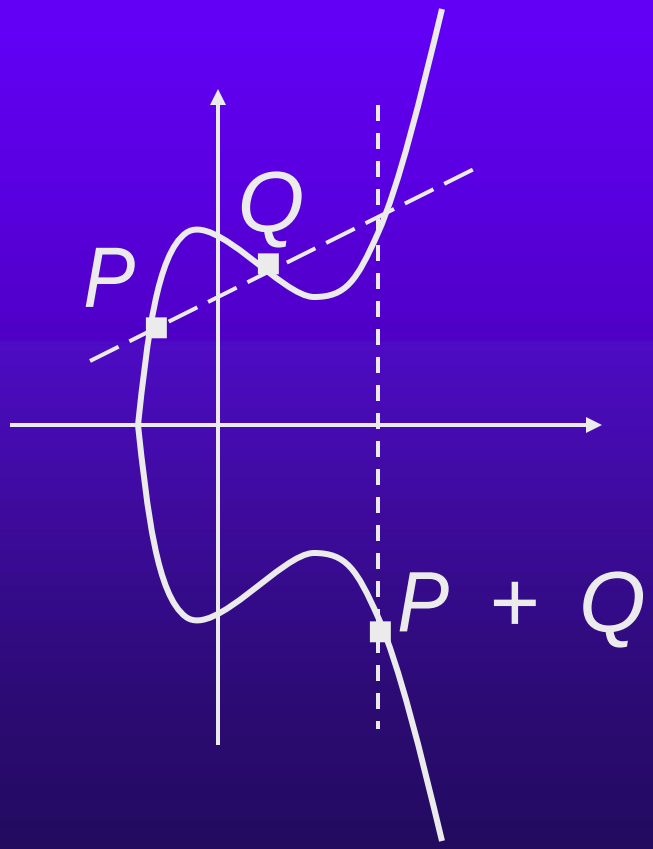
$\longrightarrow$ 4回の乗算

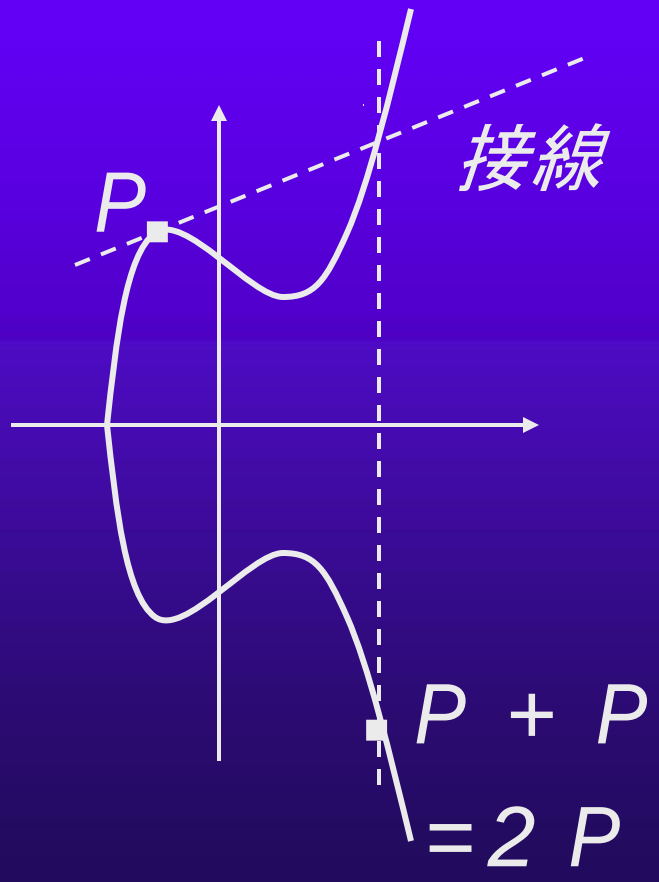
- x乗 $\Longrightarrow$ 約 $\log_2 x$ 回の乗算
  (xの2進表記の桁数)

楕円曲線: $y^2 = x^3 + ax + b$

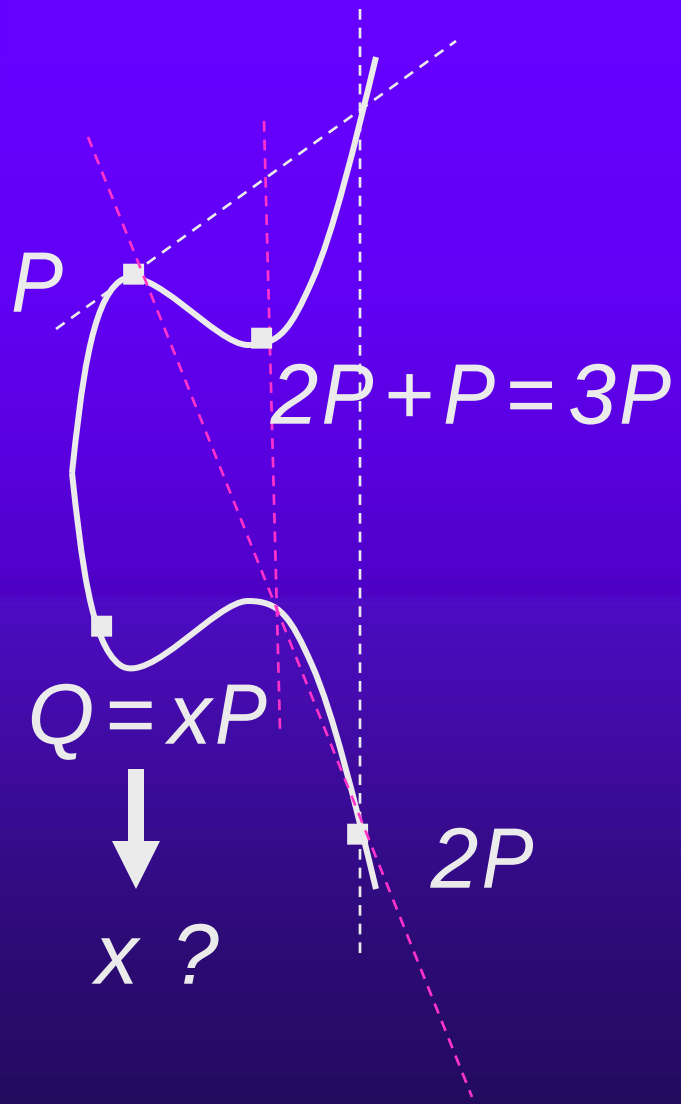
- 曲線上に演算(加法)が定義できる

  (ちょっと複雑)





楕円曲線暗号(離散対数型)



◆スカラー倍(掛け算)

P: 曲線上の点

k: 自然数(整数)

⟶ k Pは容易

例) 12Pの計算(先と同様):

P ⟶ 2P ⟶ 3P $\xrightarrow{2倍}$ 6P $\xrightarrow{2倍}$ 12P

逆に,

◆離散対数(割り算)

Q=x P ⟶ x:困難

ペアリングを用いた暗号システム(1)

- ペアリング(Pairing): 双線形写像

  ⟶　楕円曲線(代数曲線)に付随

  $e: G \times G \longrightarrow G'$

  (G: 楕円曲線の点からなる集合)

  (G´: 1のベキ乗根からなる集合)

[性質]

・$e(P+Q, R) = e(P, R) \cdot e(Q, R)$

・$e(P, Q+R) = e(P, Q) \cdot e(P, R)$

ペアリングを用いた暗号システム(2)

[具体例]

- 三者間鍵配送
  → 1回のラウンドで実現可能
  (従来法では2回必要)
- ID情報を基にした(公開鍵)暗号システム
  → 任意の文字列を暗号鍵として使用可能
  → ID情報(例:メールアドレス)を使用
  → 公開鍵認証局を必要としない

その他, 多数の暗号システムが提案されている

(公開鍵)暗号の安全性(1)

[理想]

攻撃者(解読者)に有利な環境を提供しても,
暗号文から元の文章のいかなる情報
(すなわち, 1ビット分の情報)も推測できない.

→「IND-CCA2を満たす暗号」という

[疑問]

IND-CCA2を満たすか否かを,
どのようにして判定するのか？

(公開鍵)暗号の安全性(2)

[暗号システム]

b (0 or 1)を選択

C*：M_b の暗号文

M_0, M_1 ←

→ C*

[攻撃者(解読者)]

文章M_0, M_1を作成

b を推測 (0 or 1)

[攻撃者の環境]

・文章M (M_0, M_1 以外) に対する暗号文の入手

・暗号文C (C*以外) に対する文章の入手

[IND－CCA2となるためには]

攻撃者が b を当てる確率が 1/2

(公開鍵)暗号の安全性(3)

[安全性証明の流れ：背理法を用いる]

暗号が安全でないと仮定する

↓

(数学の)未解決問題が解決する

↓

矛盾が生じる

↓

暗号は安全である

数学の未解決問題(1)

- RSA暗号関連 (n=pq, p, q:素数)

  (1) 因数分解問題:

  入力値:n , 出力値:p, q

  (2) RSA問題(RSA暗号の解読問題):

  入力値:n, e, $m^e \bmod n$, 出力値: m

  ($m^e \bmod n$:暗号文, m:メッセージ に相当)

注: (1)は(2)より難しい

(すなわち, (1)が解けると(2)も解ける)

数学の未解決問題(2)

- 楕円曲線暗号関連 (P : 曲線上の点, k,h: 自然数)

  (1) 離散対数問題 :

  入力値 : kP , 出力値 : k

  (2) Diffie-Hellman問題 :

  入力値 : kP, hP, 出力値 : (kh)P

  (楕円曲線暗号では, (kh)Pが分かると解読可能)

注 : (1)は(2)より難しい

(すなわち, (1)が解けると(2)も解ける)

研究内容

- 公開鍵暗号の構成･設計，安全性の考察
  高速演算法，素数判定，
  因数分解，位数計算，攻撃法，
  ペアリング計算および曲線の構成, etc

- その周辺(応用)
  符号理論，電子署名，計算数論, etc