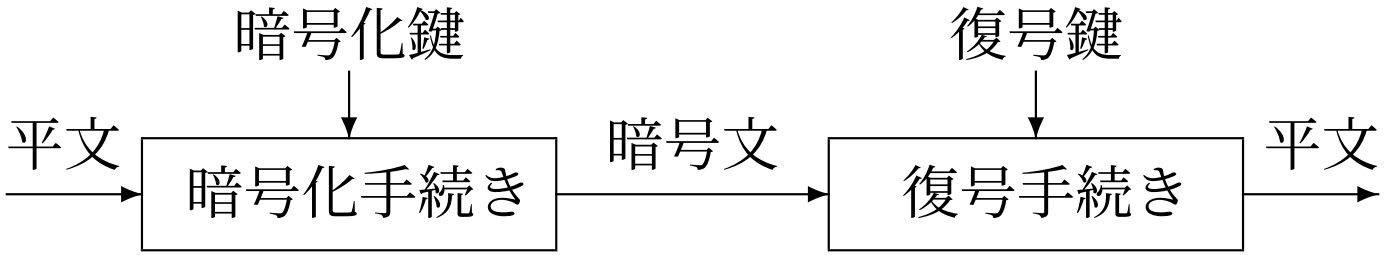
公開鍵暗号

廣瀬勝一

公開鍵暗号と共通鍵暗号



- 暗号化手続き，復号手続きは公開
- 復号鍵は受信者の秘密

暗号化鍵による暗号系の分類

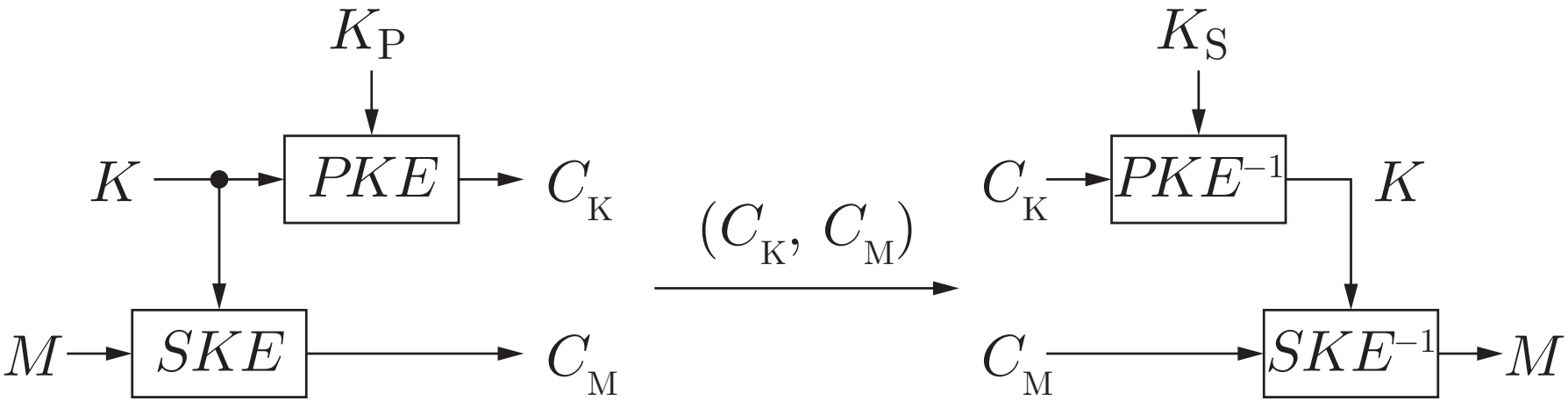
- 共通鍵暗号系（対称暗号系）
  暗号化鍵も秘密
  暗号化鍵 ＝ 復号鍵
- 公開鍵暗号系（非対称暗号系）
  暗号化鍵は公開
  暗号化鍵 ≠ 復号鍵

公開鍵暗号では

- 誰でも送りたいメッセージを暗号化できる．
- 送信者はあらかじめ受信者と秘密鍵を共有する必要はない．

ハイブリッド暗号

共通鍵暗号と公開鍵暗号の組み合わせ



- メッセージは高速な共通鍵暗号で暗号化
- 共通鍵暗号で使用する秘密鍵を公開鍵暗号で暗号化

公開鍵暗号系

鍵生成アルゴリズム Gen（確率的アルゴリズム）

$$(pk, sk) \leftarrow \mathsf{Gen}(1^{\ell})$$

ℓ はセキュリティパラメータ（例えば，生成する鍵の長さ）
(pk, sk) は公開鍵・秘密鍵の組

暗号化アルゴリズム Enc（確率的または決定的アルゴリズム）

$$C \leftarrow \mathsf{Enc}(pk, M)$$

M は平文，C は暗号文

復号アルゴリズム Dec（決定的アルゴリズム）

$$M \leftarrow \mathsf{Dec}(pk, sk, C)$$

落し戸付き一方向関数 (Trapdoor one-way function)

暗号化関数 $\mathsf{Enc}(pk, \cdot)$ は一方向関数.

- $\mathsf{Enc}(pk, \cdot)$ は容易に計算できる.
- $\mathsf{Enc}(pk, \cdot)$ の逆関数は計算が困難.

$\mathsf{Enc}(pk, \cdot)$ は落し戸付き一方向関数.

- $\mathsf{Enc}(pk, \cdot)$ の逆関数，即ち，復号関数は sk を知っていれば容易に計算できなければならない.
- sk は落し戸と呼ばれる.

但し，一方向関数でさえ，本当に存在するかどうかは未解決問題！

RSA 方式

Rivest, Shamir, Adleman 1977

公開鍵 n, e

- $n = pq$. ここで，p, q は相異なる奇素数
- $\gcd(e, \phi(n)) = 1$. ここで，$\phi(n) = (p-1)(q-1)$

秘密鍵 d

- $de \equiv 1 \pmod{\phi(n)}$

暗号化 平文 $M \in \mathbb{Z}_n$ は以下のように暗号文 C に暗号化される.

$$C = M^e \bmod n$$

復号 暗号文 C は以下のように平文 M に復号される.

$$M = C^d \bmod n$$

安全性の根拠

非常に大きな整数について，素因数分解問題を解くことが困難

RSA 方式

Theorem

すべての $M \in \mathbb{Z}_n$ について $(M^e)^d \bmod n = M$ である.

（証明）$e\,d \equiv 1 \pmod{\phi(n)}$ より，ある k について $e\,d = k\,\phi(n) + 1$.
$M \in \mathbb{Z}_n^*$ のときは，$M^{\phi(n)} \equiv 1 \pmod{n}$ より明らか.
一方，$M \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$ のときは，$p \,|\, M$ または $q \,|\, M$ である．$p \,|\, M$ ならば

$$\begin{cases} M^{k\,\phi(n)+1} \equiv M (\equiv 0) \pmod{p} \\ M^{k\,\phi(n)+1} \equiv M \pmod{q} \end{cases}$$

したがって，中国人剰余定理より,

$$M^{k\,\phi(n)+1} \bmod n = M$$

$q \,|\, M$ のときも同様に証明できる. □

素因数分解と RSA

素因数分解問題

入力： $n(=pq)$

出力： p, q

RSA 問題

入力： n, e, C

出力： $C^{\frac{1}{e}} \bmod n$

素因数分解問題が解ける $\Rightarrow$ RSA 問題が解ける

問題の困難さを不等号で表すと

$$\text{RSA 問題} \leq \text{素因数分解問題}$$

「素因数分解問題 $\leq$ RSA 問題」かどうかは未解決問題

素因数分解問題を解かずに RSA を破れる可能性は否定されていない.

RSA の誤用 (共通の法の使用)

Alice と Bob が同じ法を使用するとき

n, e_{A}　Alice の公開鍵
n, e_{B}　Bob の公開鍵

Alice と Bob の両方に同じメッセージを安全に送ることができない.

$$\begin{cases} C_{\mathrm{A}} = M^{e_{\mathrm{A}}} \bmod n \\ C_{\mathrm{B}} = M^{e_{\mathrm{B}}} \bmod n \end{cases}$$

$\gcd(e_{\mathrm{A}}, e_{\mathrm{B}}) = 1$ ならば, $a\,e_{\mathrm{A}} + b\,e_{\mathrm{B}} = 1$ を満たす a, b が計算できる.
$a < 0$ かつ $b > 0$ のとき

$$(C_{\mathrm{A}}{}^{-1})^{-a} C_{\mathrm{B}}{}^{b} \bmod n = M^{a\,e_{\mathrm{A}}}\, M^{b\,e_{\mathrm{B}}} \bmod n = M$$

$a > 0$ かつ $b < 0$ のときも同様.

RSA の誤用 (小さなべき指数の使用)

Alice, Bob, Carol が 3 をべき指数として使用するとき

$n_{\mathrm{A}}, 3$　Alice の公開鍵
$n_{\mathrm{B}}, 3$　Bob の公開鍵
$n_{\mathrm{C}}, 3$　Carol の公開鍵

Alice, Bob, Carol のすべてに同じメッセージを安全に送ることができない.

Rabin 方式

Rabin 1979

公開鍵 $n = pq$

- p と q は相異なる素数で $p \equiv 3 \pmod 4$ かつ $q \equiv 3 \pmod 4$.

秘密鍵 p, q

暗号化 平文 $M \in \mathbb{Z}_n^*$ は以下のように暗号文 C に暗号化される.

$$C = M^2 \bmod n$$

復号 暗号文 C は以下のように復号される.

$$C^{\frac{1}{2}} \bmod n$$

安全性の根拠

非常に大きな整数について，素因数分解問題を解くことが困難

復号法

平文は以下の方程式を解くことによって得られる.

$$x^2 \equiv C \pmod{n} \Leftrightarrow \begin{cases} x^2 \equiv C \pmod{p} \\ x^2 \equiv C \pmod{q} \end{cases}$$

$p \equiv 3 \pmod{4}$ のとき，p を法とする C の平方根は容易に得られる.

$$\begin{cases} x \equiv \pm C^{\frac{p+1}{4}} \pmod{p} \\ x \equiv \pm C^{\frac{q+1}{4}} \pmod{q} \end{cases}$$

中国人剰余定理により n を法とする C の平方根が 4 個得られる.

- 任意の暗号文に対して 4 個の可能な平文が存在する.
- 一意に復号するためには，平文に冗長性を持たせなければならない.

素因数分解と Rabin 方式

素因数分解問題

入力： $n(=pq)$
出力： p, q

Rabin 問題

入力： n, C
出力： $x^2 \equiv C \pmod{n}$ を満たす x

Rabin 問題と素因数分解問題は同程度に難しい.

Theorem

Rabin 問題が解けるならば，素因数分解問題が確率 *1/2* で解ける.

（証明）与えられた n について，無作為に $r \in \mathbb{Z}_n^*$ を選び，$C = r^2 \bmod n$ を計算する．次に，Rabin 問題を解くアルゴリズムに n, C を入力として与え，その出力 x を得る．このとき，$x \not\equiv \pm r \pmod{n}$ ならば $\gcd(x + r, n) \in \{p, q\}$ である．$x \not\equiv \pm r \pmod{n}$ の確率は $1/2$. □

ElGamal 方式

ElGamal 1982

公開鍵 p, g, y（すべての利用者が同一の p と g を利用できる）

- p は素数，g は乗法群 $\mathbb{Z}_p^*$ の原始元
- $y = g^x \bmod p$

秘密鍵 $x \in \mathbb{Z}_{p-1}$

暗号化 平文 $M \in \mathbb{Z}_p^*$ は以下のように暗号文 (a, b) に暗号化される．

1. $k \in \mathbb{Z}_{p-1}$ を無作為に選ぶ．
2. $a = g^k \bmod p$, $b = y^k M \bmod p$

復号 暗号文 (a, b) は以下のように平文 $M \in \mathbb{Z}_p^*$ に復号される．

$$M = b/a^x \bmod p$$

安全性の根拠

離散対数問題を解くことが困難

剰余べき乗算の計算法

square-and-multiply 法

$g^x \bmod p$ は，高々$2|x|$ 回の剰余乗算で計算できる．
（より正確には $|x| + (x$ のハミング重み$)$ 回）

x の 2 進数表記を $(x_{\ell-1}, x_{\ell-2}, \ldots, x_1, x_0)$ とする．

$$x = x_0 + 2x_1 + 2^2 x_2 + \cdots + 2^{\ell-2} x_{\ell-2} + 2^{\ell-1} x_{\ell-1} \qquad (x_i \in \{0, 1\})$$

【例】$\ell = 4$

1. $1^2 = 1$
2. $g^{x_3}\, 1 = g^{x_3}$
3. $(g^{x_3})^2 = g^{2x_3}$
4. $g^{x_2} g^{2x_3} = g^{x_2+2x_3}$
5. $(g^{x_2+2x_3})^2 = g^{2x_2+2^2x_3}$
6. $g^{x_1} g^{2x_2+2^2x_3} = g^{x_1+2x_2+2^2x_3}$
7. $(g^{x_1+2x_2+2^2x_3})^2 = g^{2x_1+2^2x_2+2^3x_3}$
8. $g^{x_0} g^{2x_1+2^2x_2+2^3x_3} = g^{x_0+2x_1+2^2x_2+2^3x_3}$

鍵長（NIST SP 800-57 より）

安全性	SKA	FFC	IFC	ECC
80	2TDEA	$(1024, 160)$	1024	$160 \sim 223$
112	3TDEA	$(2048, 224)$	2048	$224 \sim 255$
128	AES-128	$(3072, 256)$	3072	$256 \sim 383$
192	AES-192	$(7680, 384)$	7680	$384 \sim 511$
256	AES-256	$(15360, 512)$	15360	$512 \sim$

安全性は $\log_2$(攻撃計算量)

SKA: Symmetric Key Algorithms
FFC: Finite-Field Cryptography (DSA, DH), (公開鍵長, 秘密鍵長)
IFC: Integer-Factorization Cryptography (RSA)
ECC: Elliptic Curve Cryptography

2TDEA: 2-key Triple DES
3TDEA: 3-key Triple DES

公開鍵暗号方式の安全性

安全性の達成度

- 一方向性（one-wayness）
- 識別不能性（indistinguishability）
- 頑強性（non-malleability）

攻撃

- 選択平文攻撃
  暗号化鍵は公開なので常に適用可能
- 選択暗号文攻撃

一方向性 (One-wayness)

$(pk, sk) \leftarrow \mathsf{Gen}(1^\ell)$ と無作為に選ばれた平文 M について，

$$C \leftarrow \mathsf{Enc}(pk, M)$$

Definition (一方向性)

C が与えられたとき，M を得ることが困難である．

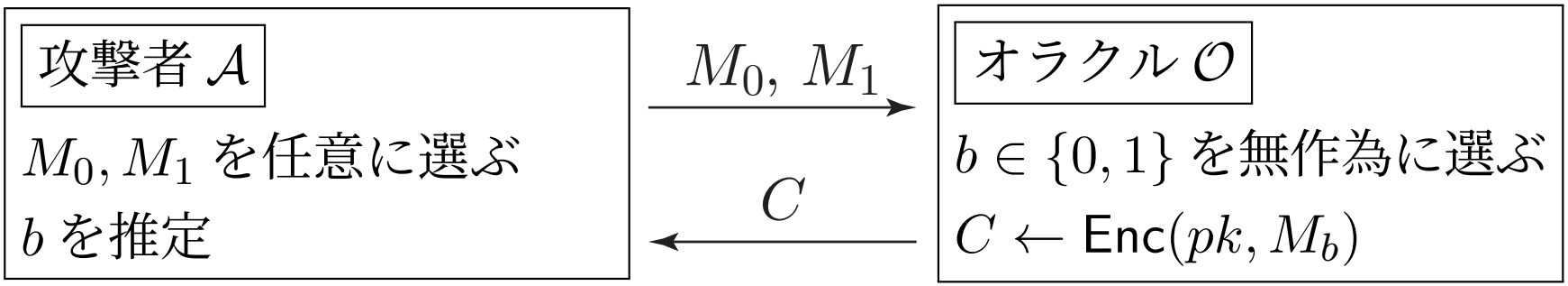
一方向性が満たされても，M の部分情報が得られる可能性がある．

【例】何ら脆弱性のない Enc について

$$\mathsf{Enc}'(pk, M) = M_{\mathrm{L}} \| \mathsf{Enc}(pk, M_{\mathrm{R}})$$

Enc' は一方向性を満たすが，安全な暗号化関数とは言えない．

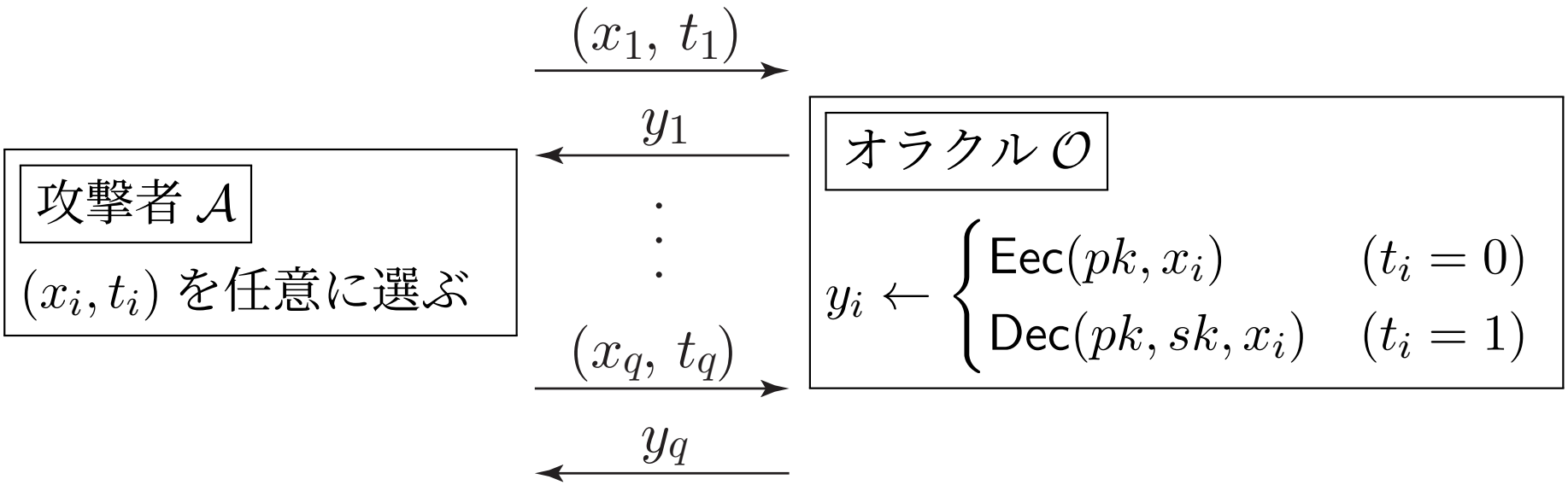
識別不能性 (Indistinguishability)



Definition (識別不能性)

1/2 より無視できない位大きな確率で b を正しく言い当てることが困難

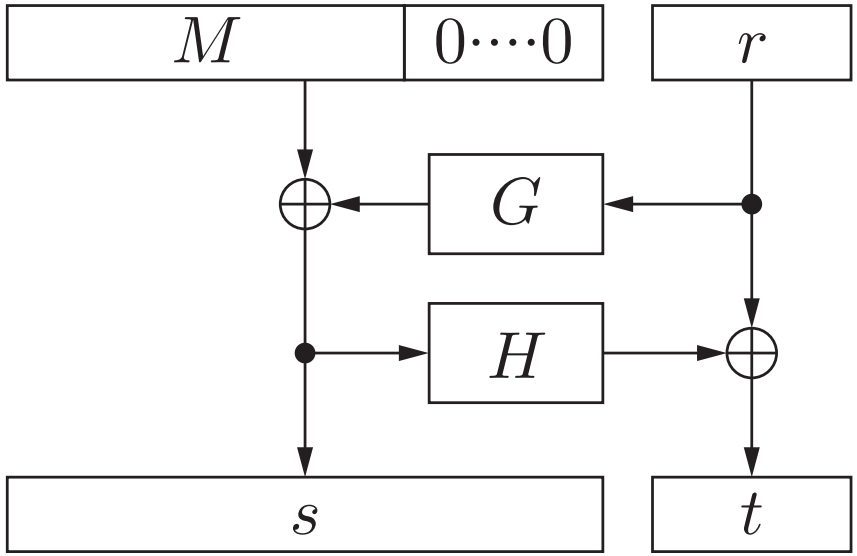
選択暗号文攻撃



- $\mathcal{A}$ は y_{i-1} を得た後にその情報を利用して (x_i, t_i) を選べる.
- $(x_i, 1)$ に対応する平文が存在しない場合，$y_i = \perp$（該当なし）.

RSA-OAEP [Bellare-Rogaway 1994]

OAEP (Optimal Asymmetric Encryption Padding)



RSA-OAEP

$$s = (M\|0\cdots0) \oplus G(r) \quad , \quad t = r \oplus H(s)$$

$$C = (s\|t)^e \bmod n$$

RSA-OAEP

Theorem

以下の条件が満たされるとき，*RSA-OAEP* は選択暗号文攻撃に対して識別不能性を満たす

- *RSA* 関数 $(x^e \bmod n)$ は一方向
- G と H はランダムオラクル

ランダムオラクルは以下を満たす理想的なブラックボックスである.

- 与えられた入力に対して無作為に選ばれた出力を返す.
- 同じ入力に対しては同じ出力を返す.

演習問題

1. RSA における小さなべき指数の使用が不都合であることを説明せよ.
2. Rabin 方式の復号アルゴリズムが正しく動作することを確認せよ.
3. 選択暗号文攻撃に対する以下の脆弱性を証明せよ.
   1. RSA 方式は一方向性を満たさない.
   2. ElGamal 方式は一方向性を満たさない.
   3. Rabin 方式は完全に解読可能である（秘密鍵が得られる）.