暗号入門

教科書・参考書

- Oded Goldreich:
  Foundations of Cryptography,
  Volume I Basic Tools, Cambridge, 2001
- Oded Goldreich:
  Foundations of Cryptography,
  Volume II Basic Applications, Cambridge, 2004
- J. A. ブーフマン 著, 林 芳樹 訳:
  暗号理論入門, 原著第3版,
  暗号アルゴリズム, 署名と認証, その数学的基礎,
  Springer, シュプリンガー・ジャパン, 2007

あらすじ

- 暗号化スキーム
  - 定義
    - Private-Key vs. Public-Key
    - ブロック暗号
  - 対称鍵暗号
    - DES, AES, 疑似乱数
  - 公開鍵暗号
    - RSA, 落し戸付き置換, ElGamal
  - 公開鍵暗号を使ったプロトコル
    - Needham-Schroeder公開鍵認証プロトコル
- 署名スキーム
- ハッシュ関数

暗号化スキーム

- 暗号化スキームとは、確率的多項式時間アルゴリズムの三つ組 (G, E, D) で、以下の二つの条件を満たすもののことである。
  - 1^n が入力されたとき、鍵生成アルゴリズム G は、ビット列の対を返す。
  - G が返した任意の対 (e, d) と任意の $\alpha \in \{0,1\}^*$ に対して、暗号化アルゴリズム E と、復号アルゴリズム D は、以下の等式を満たす。

    $$\Pr[D(d, E(e, \alpha))=\alpha] = 1$$

    ただし、確率はアルゴリズム D と E の内部的なコイン投げに従う。
- n はセキュリティ・パラメタ。

暗号化スキーム

- 暗号化スキームとは、確率的多項式時間アルゴリズムの三つ組 (G, E, D) で、以下の二つの条件を満たすもののことである。
  - 1^n が入力されたとき、鍵生成アルゴリズム G は、ビット列の対を返す。
  - G が返した任意の対 (e, d) と任意の $\alpha \in \{0,1\}^*$ に対して、暗号化アルゴリズム E と、復号アルゴリズム D は、以下の等式を満たす。

    $$\Pr[D_d(E_e(\alpha)) = \alpha] = 1$$

    ただし、確率はアルゴリズム D と E の内部的なコイン投げに従う。
- n はセキュリティ・パラメタ。

確率的多項式時間アルゴリズム

- ある多項式 $p(n)$ が存在して、
  - 入力の大きさが n であるとき、たかだか $p(n)$ ステップで終了する（多項式時間）。
  - コイン（乱数）を持っていて、コイン投げに従って次の動作を決めることができる（確率的）。
- より具体的には、確率的多項式時間チューリング機械によって実現される。
  - 1^n（1 の n 個の並び）は、チューリング機械へのセキュリティ・パラメタの入力を表す。

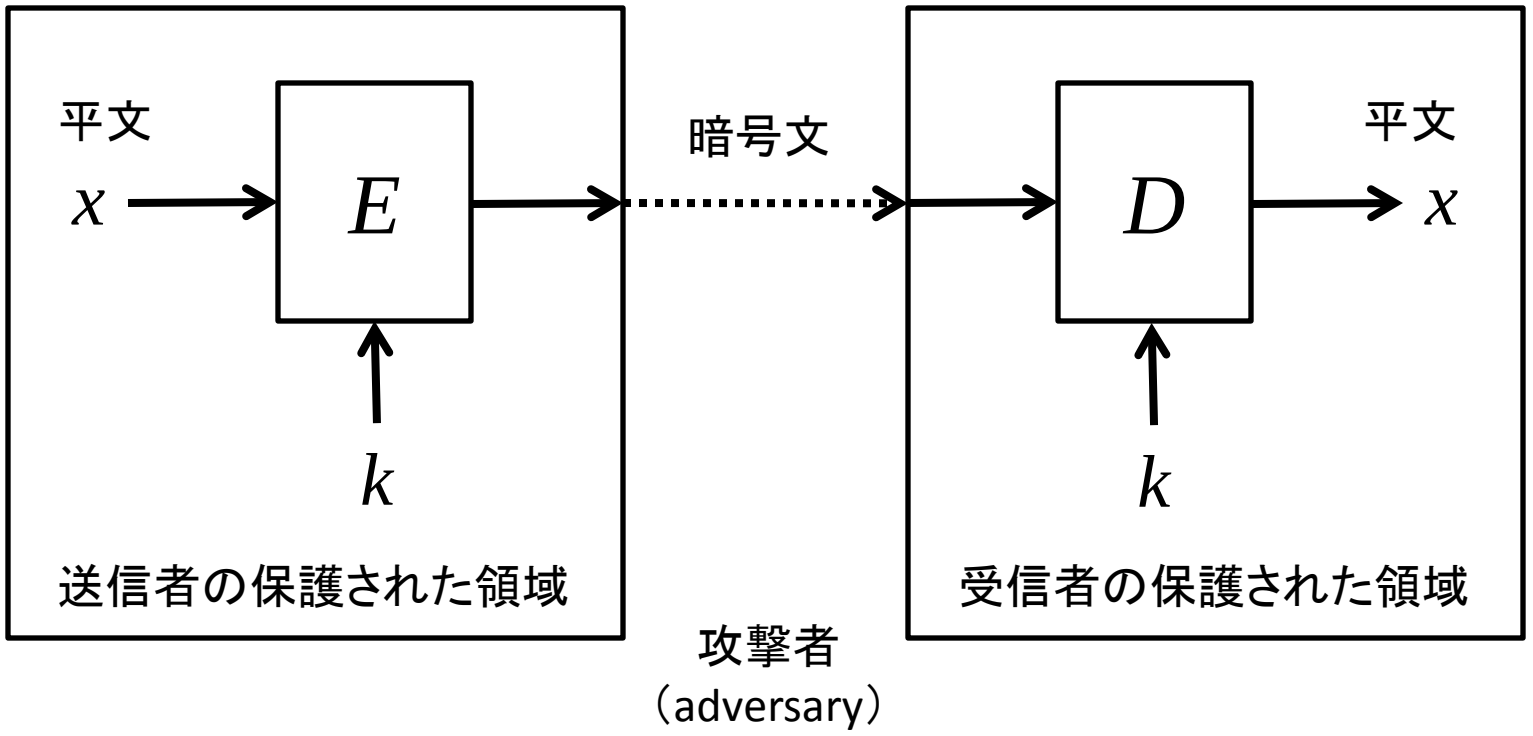
セキュリティ・パラメタ

- 暗号の強さを決めるパラメタ
- n とか η
- たとえば、鍵の長さ（ビット数）。
  - 鍵の空間は、その長さに従って、指数的に大きくなる。
- 暗号への攻撃は、セキュリティ・パラメタが大きくなっても、その多項式の時間に限定されていると仮定する。
  - 指数時間を許せば、鍵をすべて試せてしまう。

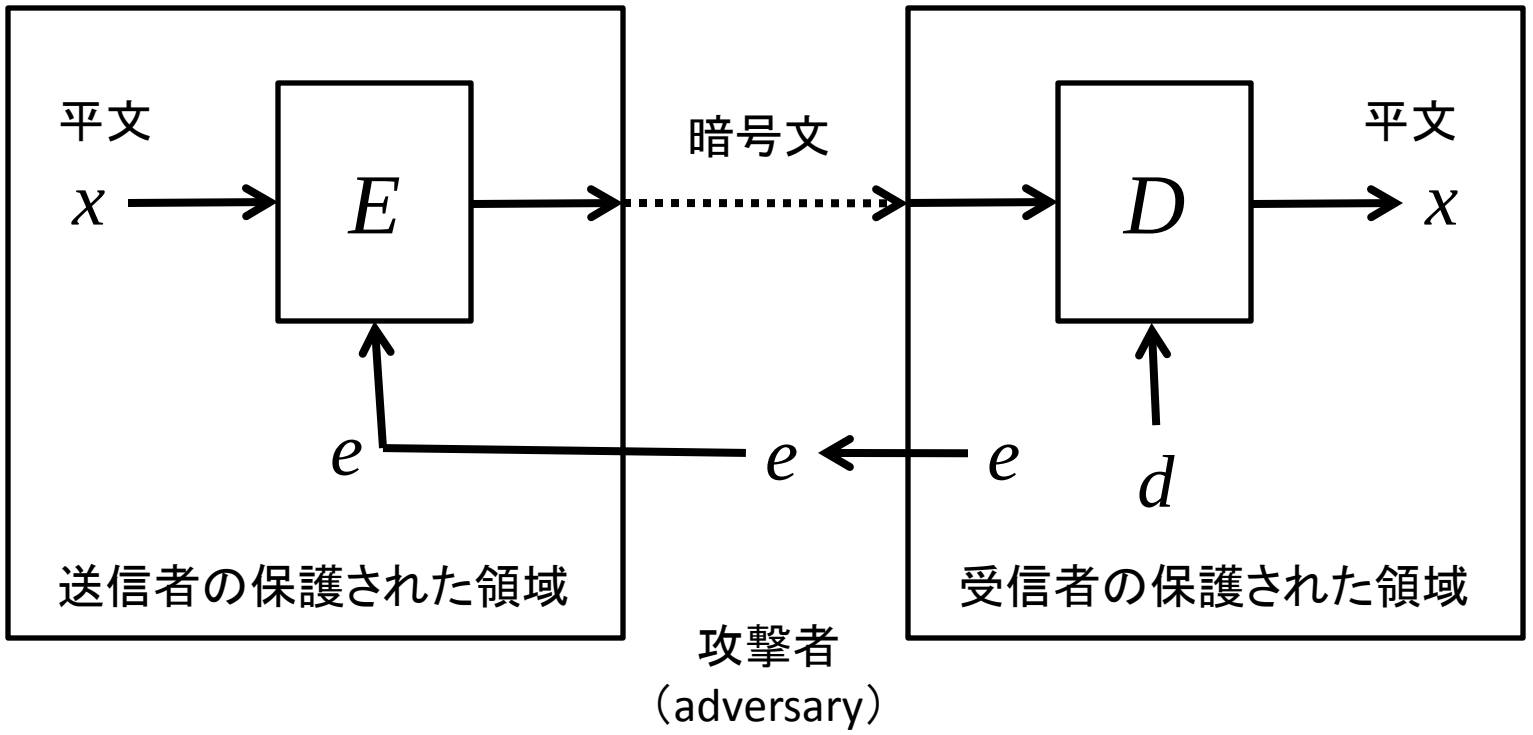
Private-Key vs. Public-Key

- Private-key --- 秘密鍵・個別鍵・共通鍵
- Public-key --- 公開鍵
- 暗号化スキームの定義に両者の違いはない。
- 両者の違いは、各種の安全性定義の違いとなって現れる。
- ただし、$e = d$ の場合は必然的に private-key となる。この場合、暗号化スキームは symmetric（対称鍵）という。

Private-Key



Public-Key



ブロック暗号

- ブロック暗号とは、確率的多項式時間アルゴリズムの三つ組 (G, E, D) で、以下の二つの条件を満たすもののことである。
  - 1^n が入力されたとき、鍵生成アルゴリズム G は、ビット列の対を返す。
  - ブロック長と呼ばれる多項式有界関数 $\ell: \mathbf{N} \to \mathbf{N}$ が存在して、G が返した任意の対 (e, d) と任意の $\alpha \in \{0,1\}^{\ell(n)}$ に対して、暗号化アルゴリズム E と、復号アルゴリズム D は、以下の等式を満たす。

$$\Pr[D_d(E_e(\alpha)) = \alpha] = 1$$

  - 典型的には、$\ell(n) = n$ もしくは $\ell(n) = 1$

ブロック暗号

- ブロック暗号とは、確率的多項式時間アルゴリズムの三つ組 (G, E, D) で、以下の二つの条件を満たすもののことである。
  - 1^n が入力されたとき、鍵生成アルゴリズム G は、ビット列の対を返す。
  - ブロック長と呼ばれる多項式有界関数 $\ell: \mathbf{N} \to \mathbf{N}$ が存在して、G が返した任意の対 (e, d) と任意の $\alpha \in \{0,1\}^{\ell(n)}$ に対して、暗号化アルゴリズム E と、復号アルゴリズム D は、以下の等式を満たす。

$$\Pr[D_d(E_e(\alpha)) = \alpha] = 1$$

暗号化スキームでは
$\alpha \in \{0,1\}^*$

  - 典型的には、$\ell(n) = n$ もしくは $\ell(n) = 1$

ブロック暗号から暗号化スキームへ

- ブロック暗号 (G, E, D) から暗号化スキーム (G', E', D') を構成する。
  - G' は G に等しい。
  - 暗号化は、メッセージ α を長さ $\ell(n)$ のブロック $\alpha_1, \ldots, \alpha_t$ に分解し（最後のブロックには余白を埋めて）、

$$E'_e(\alpha) = (|\alpha|, E_e(\alpha_1), \ldots, E_e(\alpha_t))$$

  - 復号は、暗号文 $(m, \beta_1, \ldots, \beta_t)$ が与えられたとき、$\alpha_i = D_d(\beta_i)$ として、連結した結果 $\alpha_1 \ldots \alpha_t$ の最初の m ビットを返す。

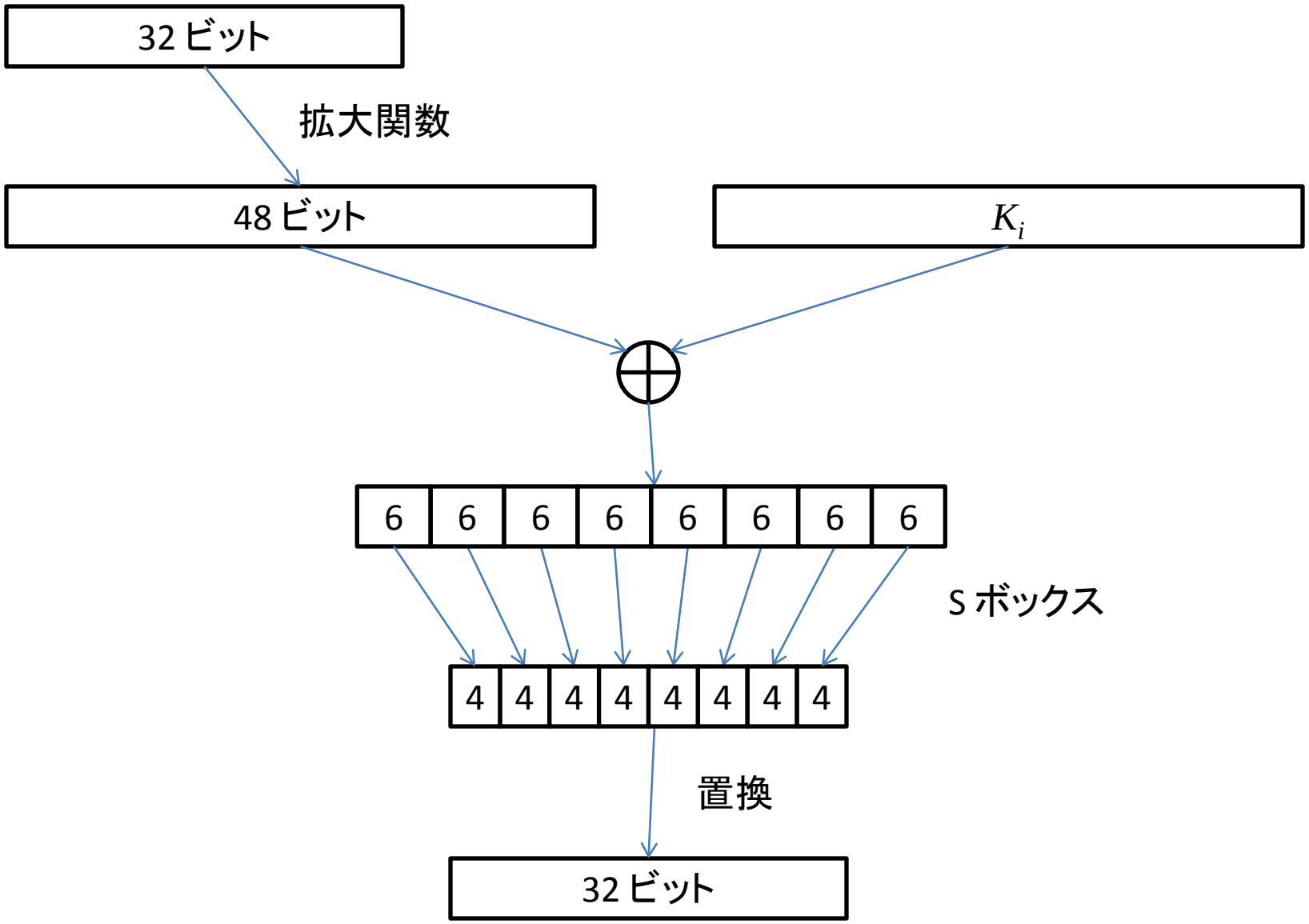
対称鍵のブロック暗号の例

乱数化していない

- アフィン線形ブロック暗号
  - ヴィジュネル暗号
  - ヒル暗号
  - 置換暗号 --- ビット位置の置換
- DES
  - Data Encryption Standard
  - Feistel 暗号の一種
- AES
  - Advanced Encryption Standard
  - Rijmen と Daemen（Rijndael ）

DES

- ブロック 64 ビット・鍵 64 ビット
- おおよその構成
  - 初期置換 IP を適用。結果を L_0R_0 とする。
  - 16 段の Feistel 暗号
    - $(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus f_{K_i}(R_{i-1}))$
    - 巡回鍵 K_i は、DES 鍵から関数 PC1 と PC2 により作る。
    - f_{K_i} は 32 ビットに対して以下のように定義される。
      - 32 ビットを 48 ビットに拡大し、K_i との排他的論理和をとる。
      - 6 ビットの 8 ブロックに 8 個の S ボックスという関数を適用。
      - 結果は 4 ビットの 8 ブロックとなる。
      - これに置換を適用。
  - 最後に $R_{16}L_{16}$ に IP^{-1} を適用


32 ビット
拡大関数
48 ビット
K_i
6 6 6 6 6 6 6 6
S ボックス
4 4 4 4 4 4 4 4
置換
32 ビット

AES

- ブロック 32*Nb ビット・鍵 32*Nkビット

  $4 \leqq Nb \leqq 8, 4 \leqq Nk \leqq 8$

- 巡回の回数 Nr

  Nk = 4, 6, 8 に対して Nr = 10, 12, 14

  巡回のために鍵拡張。

- ブロックを 4 行 Nb 列のバイト行列と考える。
- 初期変換の後、Nr 回の巡回。
  - SubBytes
  - ShiftRows
  - MixColumns（最終巡回のときは適応せず）
  - AddRoundKey（初期変換でもある）

疑似乱数から private-key を構成

- $F = \{F_n\}$ を効率的計算可能関数アンサンブルとし、I と V を F に付随したアルゴリズムとする。
  - $I(1^n)$ は分布 F_n で関数を選択し、ビット列 s に付随する関数 f_s に対して $V(s, x)$ は $f_s(x)$ を計算する。
- Private-key ブロック暗号 (G, E, D) を以下のように定義する。
  - $G(1^n) = (k, k)$ where $k \Leftarrow I(1^n)$
  - $x \in \{0,1\}^n$ に対して、$E_k(x) = (r, V(k, r) \oplus x)$ where $r \Leftarrow \{0,1\}^n$
  - $D_k(r, y) = V(k, r) \oplus y$

疑似乱数から private-key を構成

- さらに、ブロック暗号から、一般的な暗号化スキームを構成することができる。
- アンサンブル F が（多項式回路に対して）pseudorandom ならば、以上のようにして構成された暗号化スキームは IND-CCA1 を満たす（Goldreich, Vol.II, Prop.5.4.18, p.450）。
  - F が（多項式回路に対して）pseudorandom であるとは、分布 F_n が一様分布 H_n と（多項式回路によって）区別できないということ。

乱数化された RSA

- RSA による落し戸付き置換を利用。
  - 鍵生成
    - n ビットの二つの素数 P と Q をランダムに選ぶ。
    - $N=PQ$ とおく。
    - $ed=1 \ (\mathbf{mod}\ (P-1)(Q-1))$ を満たす対 (e, d) をランダムに選ぶ。
    - $G(1^n) = ((N,e), (N,d))$
  - 長さ n のビット列 σ に対して、
    - $r \in \{1, \ldots, N-1\}$ をランダムに選ぶ。
    - $\mathrm{LSB}(r)$ は r の下位 n ビットを返すとする。
    - $E_{(N,e)}(\sigma) = (r^e \ \mathbf{mod}\ N, \sigma \oplus \mathrm{LSB}(r))$
  - $(y, \zeta) \in \{1, \ldots, N-1\} \times \{0,1\}^n$ に対して、
    - $D_{(N,e)}(y, \zeta) = \zeta \oplus \mathrm{LSB}(y^d \ \mathbf{mod}\ N)$

例

- P=11, Q=13 とする。n=4 と考える。
- N=PQ=143, (P–1)(Q–1)=120
- e=7, d=103 とする。
- ed=721=1 (**mod** 120)
  - ed=1 (**mod** 10) かつ ed=1 (**mod** 12)
- r=102 とする。
  - r^{ed}=r (**mod** 11) かつ r^{ed}=r (**mod** 11)
  - したがって、r^{ed}=r (**mod** 143)

例（つづき）

- σ=10 とする。
- LSB(r)=LSB(102)=6（102 の下位 4 ビット）
- $E_{(N,e)}(\sigma) = (r^e \bmod N, \sigma \oplus \mathrm{LSB}(r))$
  $= (102^7 \bmod 143, 10 \oplus 6)$
  $= (119, 12) = (y, \zeta)$
- $D_{(N,e)}(y, \zeta) = \zeta \oplus \mathrm{LSB}(y^d \bmod N)$
  $= 12 \oplus \mathrm{LSB}(119^{103} \bmod 143)$
  $= 12 \oplus \mathrm{LSB}(102) = 12 \oplus 6 = 10$

落し戸付き置換

- 置換の族 $\{p_\alpha\}$ と確率的多項式時間アルゴリズム I, S, F, B が落し戸付き置換であるとは、
  - 入力 1^n に対して、アルゴリズム I はランダムな n ビットのインデックス α と置換 p_α の落し戸 τ を返す。
  - 入力 α に対して、アルゴリズム S は p_α の定義域のランダムな要素をサンプルして返す。
  - p_α の定義域の要素 x に対して、$F(\alpha, x) = p_\alpha(x)$
  - p_α の値域の要素 y に対して、(α, τ) が $I(1^n)$ の返し得る出力ならば、$B(\tau, y) = p_\alpha^{-1}(y)$

ハードコア述語

- 落し戸付き置換に対して、ハードコア述語 b を構成することができる。
  - 多項式時間述語 $b : \{0,1\}^* \to \{0,1\}$ に対して、一様分布のもとで、いかなる多項式時間アルゴリズムも、$p_\alpha(x)$ から $b(x)$ を当てる確率は、1/2 よりも無視できないほど大きくはない。

落し戸付き置換から public-key を構成

- $\{p_\alpha\}, I, S, F, B, b$ を仮定。
- 1 ビットの public-key ブロック暗号 (G, E, D) を以下のように定義する
  - $G(1^n) = I(1^n) = (\alpha, \tau)$
  - ビット σ に対して、$E_\alpha(\sigma) = (F(\alpha, r), \sigma \oplus b(x))$ where $r \Leftarrow S(\alpha)$
  - $D_\tau(y, \zeta) = \zeta \oplus b(B(\tau, y))$

ElGamal

- 離散対数の困難性を利用。
- G を位数 q の巡回群、γ をその原始根とする。（q は n ビット）
- $\mathbf{Z}_q^* = \{1, \ldots, q-1\}$ とおく。
  - $x \in \mathbf{Z}_q^*$ をランダムに選ぶ。$\alpha = \gamma^x$ とおく。

    $G(1^n) = (\alpha, x)$
  - $y \in \mathbf{Z}_q^*$ をランダムに選ぶ。$\beta = \gamma^y$ とおく。

    $E_\alpha(m) = (\beta, \alpha^y \cdot m)$
  - $D_x(\beta, \zeta) = \zeta / \beta^x$

例

- $p=11$ とする（11 は素数）。
- **mod** 11 の剰余類は、0 を除くと乗法群を成す。
- $2^1=2$, $2^2=4$, $2^3=8$, $2^4=16=5$, $2^5=10$, $2^6=20=9$, $2^7=18=7$, $2^8=14=3$, $2^9=6$, $2^{10}=12=1$ (**mod** 11)
- したがって、この乗法群は位数 10 の巡回群。
- $\gamma=2$ はその原始根の一つ。
- $q=p-1=10$ とする。
- $\mathbf{Z}_{10}^{*} = \{1, \ldots, 9\}$

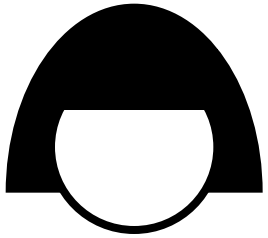
例（つづき）

- $\mathbf{Z}_{10}^{*} = \{1, \ldots, 9\}$
- $x=3 \in \mathbf{Z}_{10}^{*}$ をランダムに選んだとする。
- $\alpha=\gamma^{x}=2^{3}=8 \ (\mathbf{mod}\ 11)$
- $y=9 \in \mathbf{Z}_{10}^{*}$ をランダムに選んだとする。
- $\beta=\gamma^{y}=2^{9}=6 \ (\mathbf{mod}\ 11)$
- $m=5$ とする。
- $E_{\alpha}(m) = (\beta, \alpha^{y} \cdot m) = (6, 8^{9} \cdot 5) = (3, 2) \ (\mathbf{mod}\ 11)$
- $D_{x}(\beta, \zeta) = \zeta / \beta^{x} = 2/6^{3} = 5 \ (\mathbf{mod}\ 11)$

公開鍵暗号を使ったプロトコル

- Needham-Schroeder の公開鍵暗号による認証プロトコル（1978）の本質的部分（アリス・ボブ記法）

$$A \rightarrow B : \{A, N_A\}_{KB}$$
$$B \rightarrow A : \{N_A, N_B\}_{KA}$$
$$A \rightarrow B : \{N_B\}_{KB}$$



アリス

乱数・ノンス
（作った人しか知り得ない）

$\{A, N_A\}_{KB}$

{アリス, アリスの秘密}ボブの公開鍵

このとき、アリスの秘密は、
アリスとボブしか知り得ない。

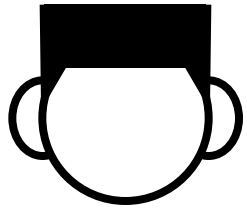
$\{N_A, N_B\}_{KA}$

{アリスの秘密, ボブの秘密}アリスの公開鍵

アリスの秘密が帰って来たということは、
ボブが最初のメッセージを受信したはず。

$\{N_B\}_{KB}$

ボブ



$\{A, N_A\}_{KB}$

{アリス, アリスの秘密}ボブの公開鍵

$\{N_A, N_B\}_{KA}$

{アリスの秘密, ボブの秘密}アリスの公開鍵

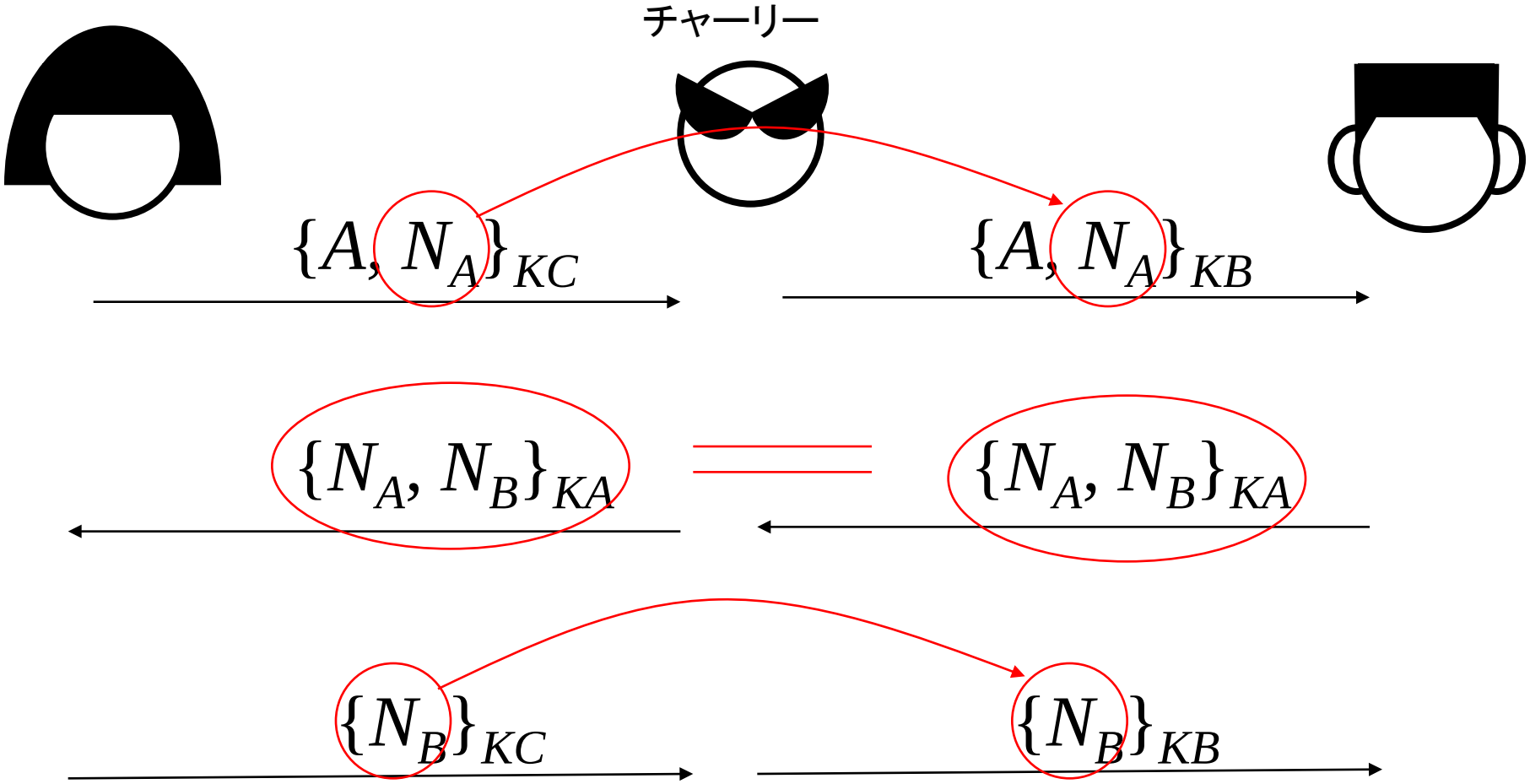
このとき、ボブの秘密は、
アリスとボブしか知り得ない？

$\{N_B\}_{KB}$

同様

Man-in-the-Middle攻撃

- Lowe が20年近くたってから発見（1995）
  - プロトコルの厳格なモデル化が一つの理由



修正されたプロトコル

- Needham-Schroeder-Lowe

$$A \rightarrow B : \{A, N_A\}_{KB}$$
$$B \rightarrow A : \{B, N_A, N_B\}_{KA}$$
$$A \rightarrow B : \{N_B\}_{KB}$$

署名スキーム

- 署名スキームとは、確率的多項式時間アルゴリズムの三つ組 (G, S, V) で、以下の二つの条件を満たすもののことである。
  - 1^n が入力されたとき、鍵生成アルゴリズム G は、ビット列の対を返す。
  - G が返した任意の対 (s, v) と任意の $\alpha \in \{0,1\}^*$ に対して、署名アルゴリズム S と、検証アルゴリズム V は、以下の等式を満たす。

    $$\Pr[V(v, S(s, \alpha))=1] = 1$$

    ただし、確率はアルゴリズム S の内部的なコイン投げに従う。

ElGamal

- G を位数 q の巡回群、γ をその原始根とする。
- $\mathbf{Z}_q^* = \{1, \ldots, q-1\}$ とおく。
  - $x \in \mathbf{Z}_q^*$ をランダムに選ぶ。$\alpha = \gamma^x$ とおく。

    $G(1^n) = (x, \alpha)$
  - q と素な $y \in \mathbf{Z}_q^*$ をランダムに選ぶ。$\beta = \gamma^y$ とおく。m を署名したい文書、$h(m)$ をそのハッシュ値とする。$\zeta = y^{-1}(h(m) - x\beta) \bmod q$ とおく。

    $S(x, m) = (m, \beta, \zeta)$

    ただし、$yy^{-1} \equiv 1 \bmod q$
  - $V(\alpha, (m, \beta, \zeta)) = (\alpha^\beta \beta^\zeta = \gamma^{h(m)})$

例

- $p=11$
- $\gamma=2$
- $q=p-1=10$
- $\mathbf{Z}_{10}^{*} = \{1, \ldots, 9\}$
- $x=3 \in \mathbf{Z}_{10}^{*}$ をランダムに選んだとする。
- $\alpha=\gamma^{x}=2^{3}=8$ (**mod** 11)

例（つづき）

- $y=9 \in \mathbf{Z}_{10}^{*}$ は 10 と素。$y^{-1}=9$ (**mod** 10)
- $\beta=\gamma^{y}=2^{9}=6$ (**mod** 11)
- $h(m)=5$ とする。
- $\zeta = y^{-1}(h(m) - x\beta) = 9\cdot(5 - 3\cdot 6) = -117$
  $= 3$ (**mod** 10)
- $\alpha^{\beta}\beta^{\zeta} = 8^{6}\cdot 6^{3} = 10$ (**mod** 11)
- $\gamma^{h(m)} = 2^{5} = 10$ (**mod** 11)

ハッシュ関数

- $\ell : \mathbf{N} \to \mathbf{N}$ とする。
- 関数族 $\{h_s : \{0,1\}^* \to \{0,1\}^{\ell(|s|)}\}_{s \in \{0,1\}^*}$ が無衝突ハッシュであるとは、確率的多項式時間アルゴリズム I が存在して、
  - s と x に対して $h_s(x)$ を返す多項式時間アルゴリズムが存在する。
  - $s = I(1^n)$ から、h_s の衝突を無視できない確率で返す確率的多項式時間アルゴリズムは存在しない。
- 関数 h の衝突とは、$h(x)=h(x')$ かつ $x \neq x'$ を満たす対 (x, x')

SHA-1

- Digital Signature Standard
- 初期段階
  - ビット列に対して 1 を一つ付加。
  - k*512 – 64 の長さになるように 0 を付加。
  - 最後に、もとの長さを 64 ビット 2 進数で付加。
- 32 ビット語 H_0, H_1, H_2, H_3, H_4 を初期化。
- 各 512 ビット・ブロックに対して、
  - 16 個の 32 ビット語に分割。
  - H_0, H_1, H_2, H_3, H_4 を更新
- 最終的な $H_0H_1H_2H_3H_4$ を返す。