情報・システム工学概論

情報を効率よく安全に伝送するための符号化技術

工学部計数工学科

新領域創成科学研究科複雑理工学専攻

山本博資（hirosuke@ieee.org）

通信と符号化

通信と符号化

使用者/通信会社 ➡ 通信コスト

雑音 ➡ 伝送誤り

公開通信路 ➡ 盗聴/改竄

通信と符号化

使用者/通信会社 ➡ 通信コスト ➡ データ圧縮
（情報源符号化）

雑音 ➡ 伝送誤り ➡ 誤り訂正
（通信路符号化）

公開通信路 ➡ 盗聴/改竄 ➡ 秘匿/認証
（暗号化）

記録と符号化

使用者/販売会社 ➡ コスト ➡ データ圧縮
（情報源符号化）

音楽

画像

光磁気ディスク

キズ，ホコリ ➡ 雑音/ノイズ ➡ 誤り訂正
（通信路符号化）

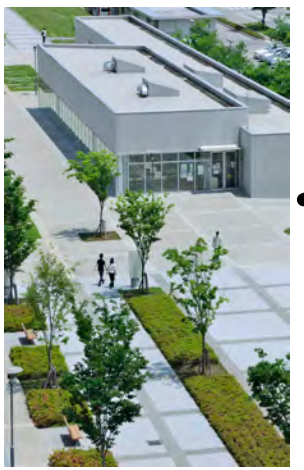
不正アクセス ➡ 漏洩/改竄 ➡ 秘匿/認証
（暗号化）

記録と符号化

使用者/販売会社 ➡ コスト ➡ データ圧縮
（情報源符号化）

音楽

画像



光磁気
ディスク

ハードディスク
フラッシュメモリ

キズ，ホコリ ➡ 雑音/ノイズ ➡ 誤り訂正
（通信路符号化）

不正アクセス ➡ 漏洩/改竄 ➡ 秘匿/認証
（暗号化）

通信，情報，符号化に関する数学的な基礎理論

⬇

情報理論
Information Theory

情報：　意味を排除し，確率を用いてモデル化

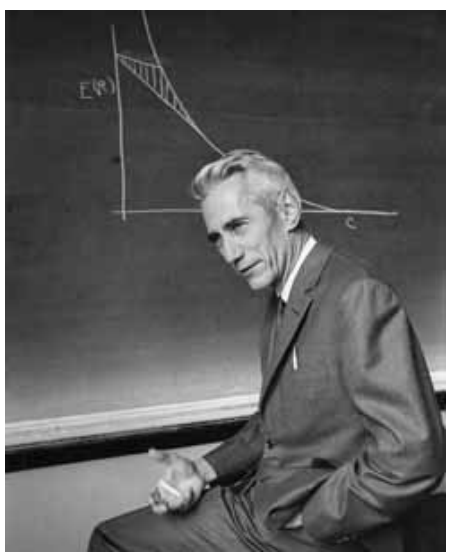
通信路：確率を用いてモデル化

情報理論の始まり

Claude E. Shannon (1916～2001)

A Mathematical Theory of Communication,
B.S.T.J, 1948

- 情報理論の創始
- 暗号理論の創始
- ブール代数を用いた論理回路設計
- 標本化定理
- 人工知能(コンピュータチェス，マイクロマウスなど)



第1回京都賞(1985)

情報理論の研究目的

データ圧縮：冗長性の除去する符号化
誤り訂正：冗長ビットを付加する符号化
情報セキュリティ：乱数を用いて撹拌する符号化

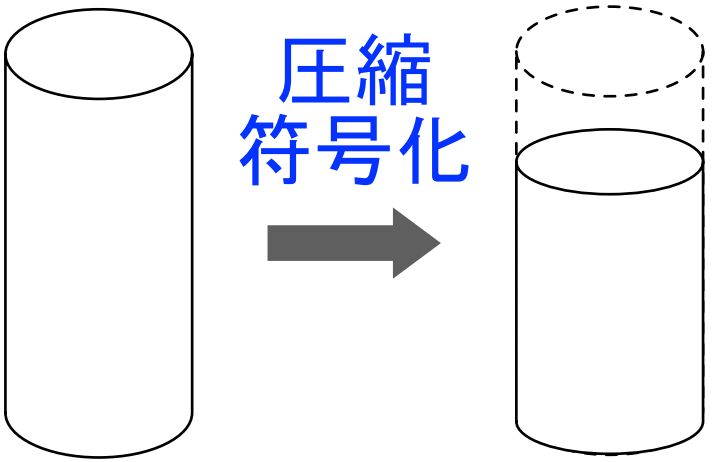
- 実用的な効率のよい符号を作る.
- 符号化効率の理論限界を明らかにする

シャノン理論
（Shannon Theory）

シャノン理論の研究意義

ファイル

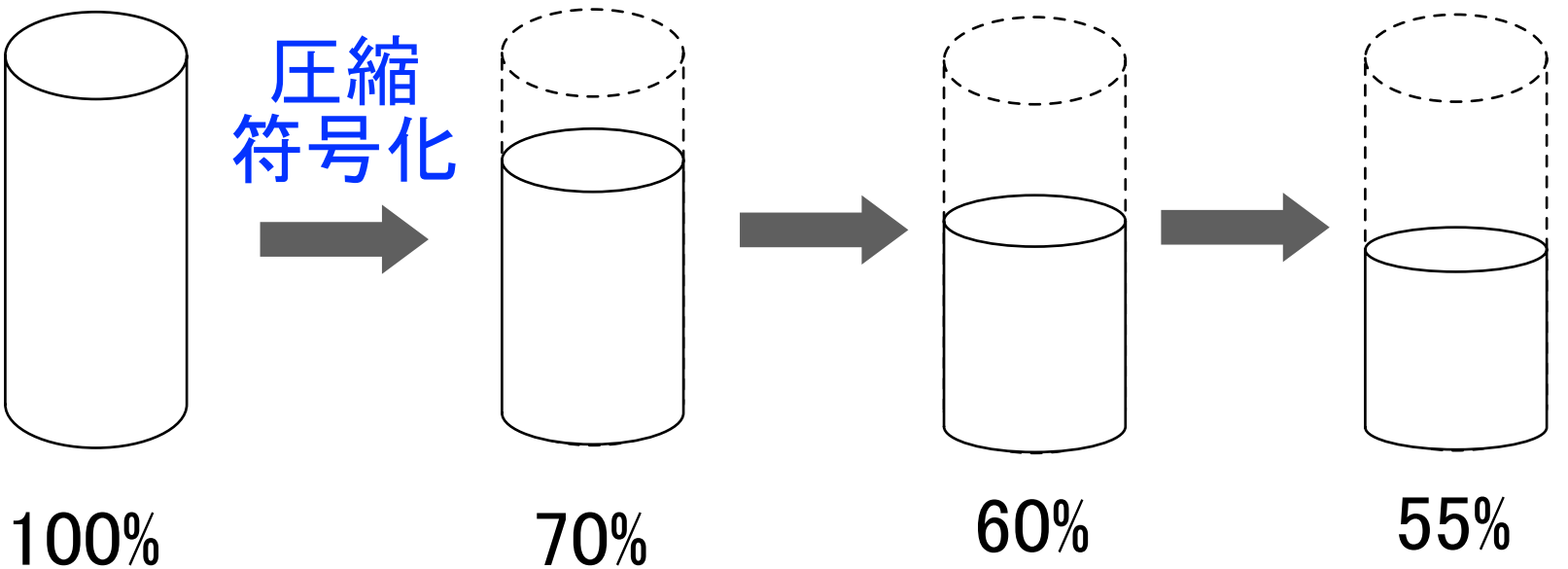
符号A



100%

70%

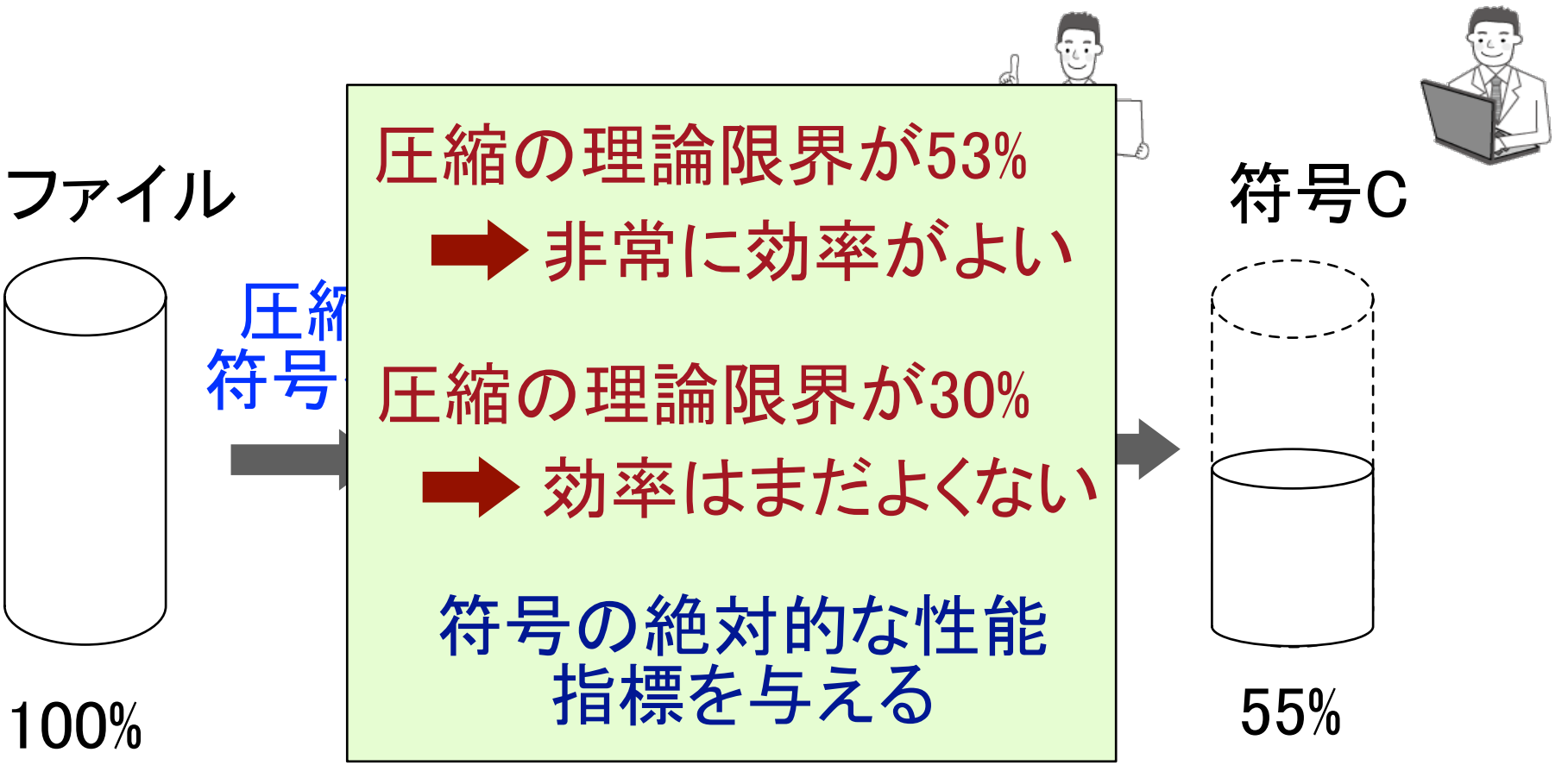
シャノン理論の研究意義



符号Cは性能がよいか？

もっと性能のよい符号は作れるか？

シャノン理論の研究意義



符号Cは性能がよいか？

もっと性能のよい符号は作れるか？

シャノン理論での仮定

無限の計算機パワー（無限大の計算速度，無限大のメモリ量）

例：　圧縮率の限界がR%で与えられることの証明

- 無限大の計算機パワーを用いても圧縮率がR以下にできない証明
- 無限大の計算機パワーを許して，Rを達成する符号化法を示す．

- 小手先の技術ではなく，本質を見抜く洞察力が必要
- 理論限界：コンピュータがどのように発達しても成り立つ

  コンピュータの発達とともに達成できる可能性がある

情報セキュリティ符号化

暗号理論

計算量的安全性に基づく暗号・情報セキュリティ符号化

コンピュータのモデル ➡ 多項式時間の計算：容易
指数時間の計算：困難

例： 公開鍵暗号など

情報理論

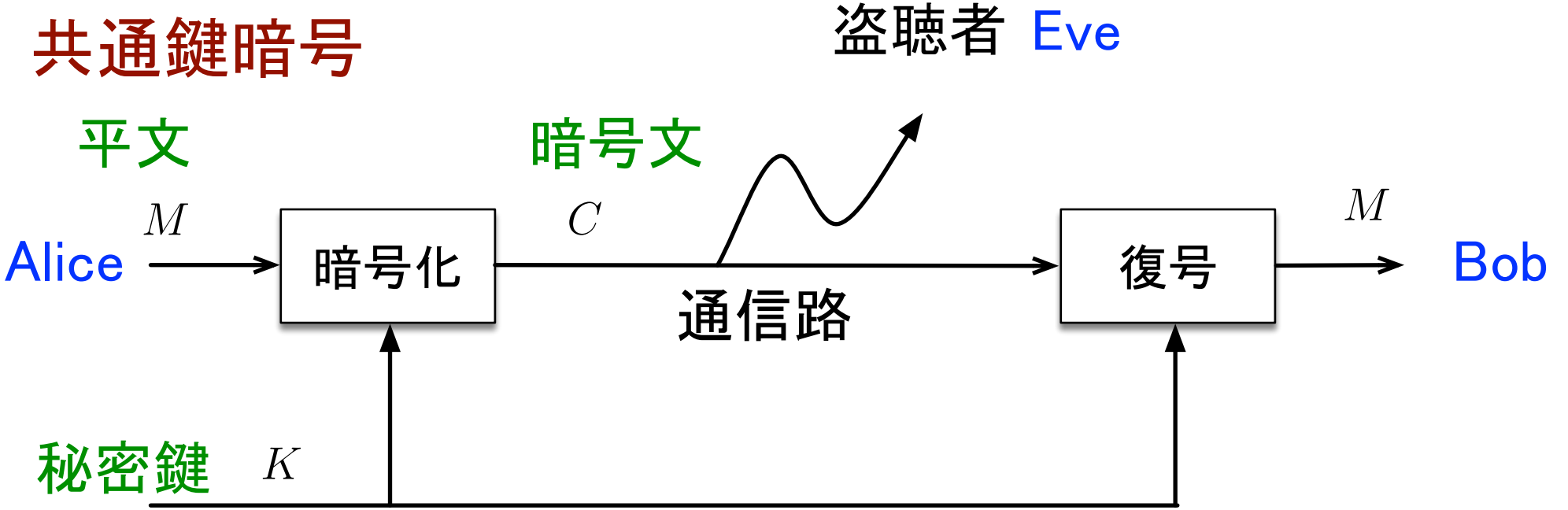
情報量的安全性に基づく暗号・情報セキュリティ符号化

コンピュータのモデル ➡ 無限大の計算パワー

例： 秘密分散法など

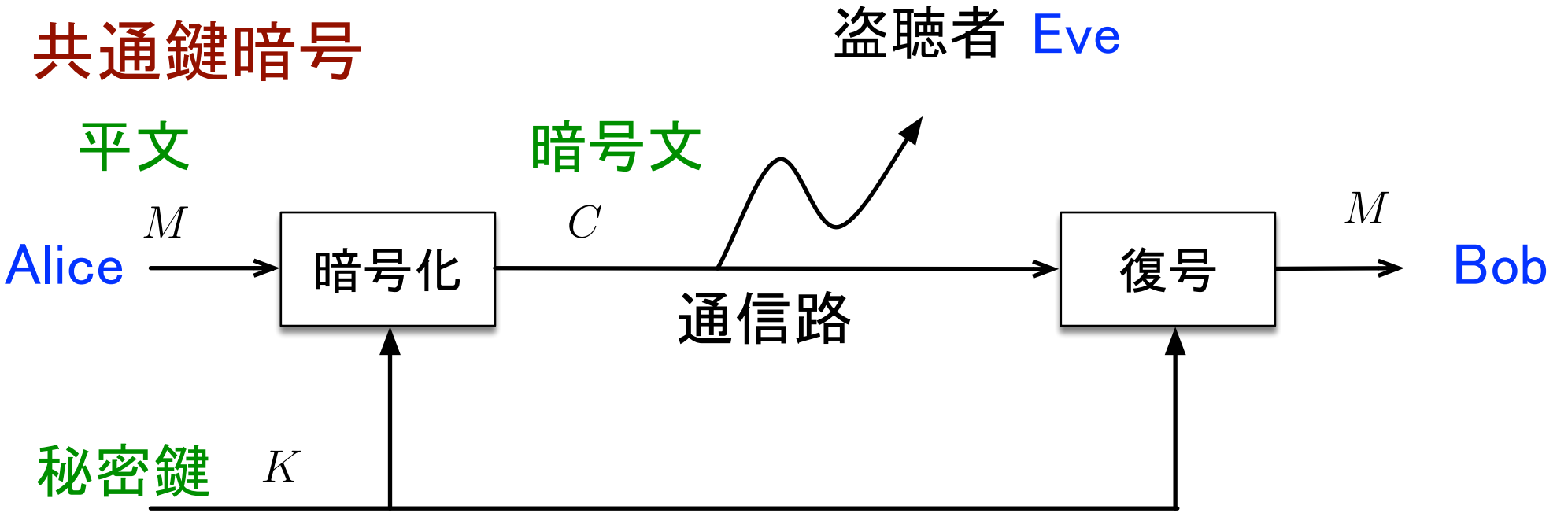
計算量的安全性に基づく暗号・情報セキュリティ符号化

共通鍵暗号



計算量的安全性に基づく暗号・情報セキュリティ符号化

共通鍵暗号



$M \in \{m_1, m_2, \cdots, m_L\}$ $P_M(m)$

$C \in \{c_1, c_2, \cdots, c_L\}$ $P_C(c)$

確率的に独立 ⟷ 完全秘匿

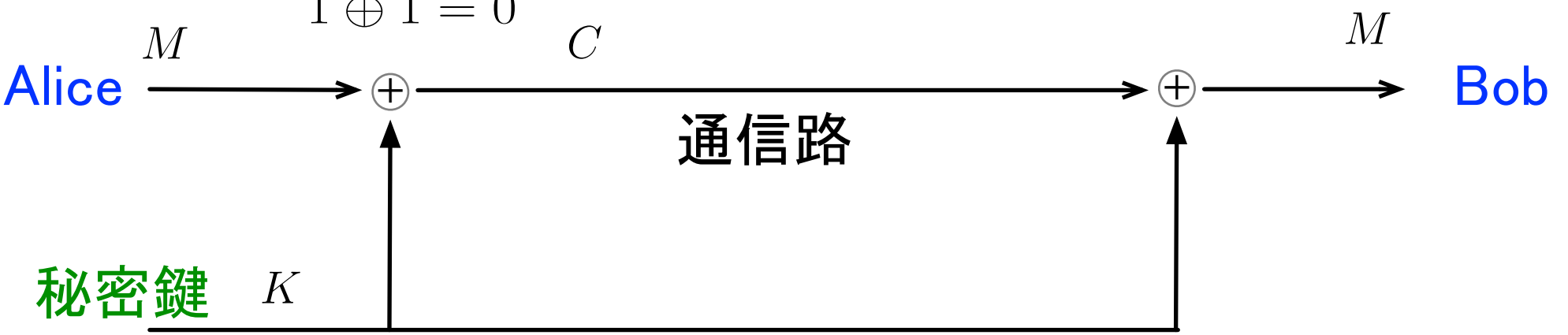
↕

鍵レート＝平文レート

バーナム暗号(Vernam Cipher)　One time pad

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

排他的論理和



$$M = \ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ \cdots$$
$$K = \ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ \cdots$$
$$C = \ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ \cdots$$

標準共通鍵暗号

DES (Data Encryption Standard) 1976, アメリカ連邦規格(FIPS)

平文64ビット, 鍵:54ビット

差分解読法　1990年 Biham-Shamir

線形解読法　1992年 Matsui

AES (Advanced Encryption Standard)

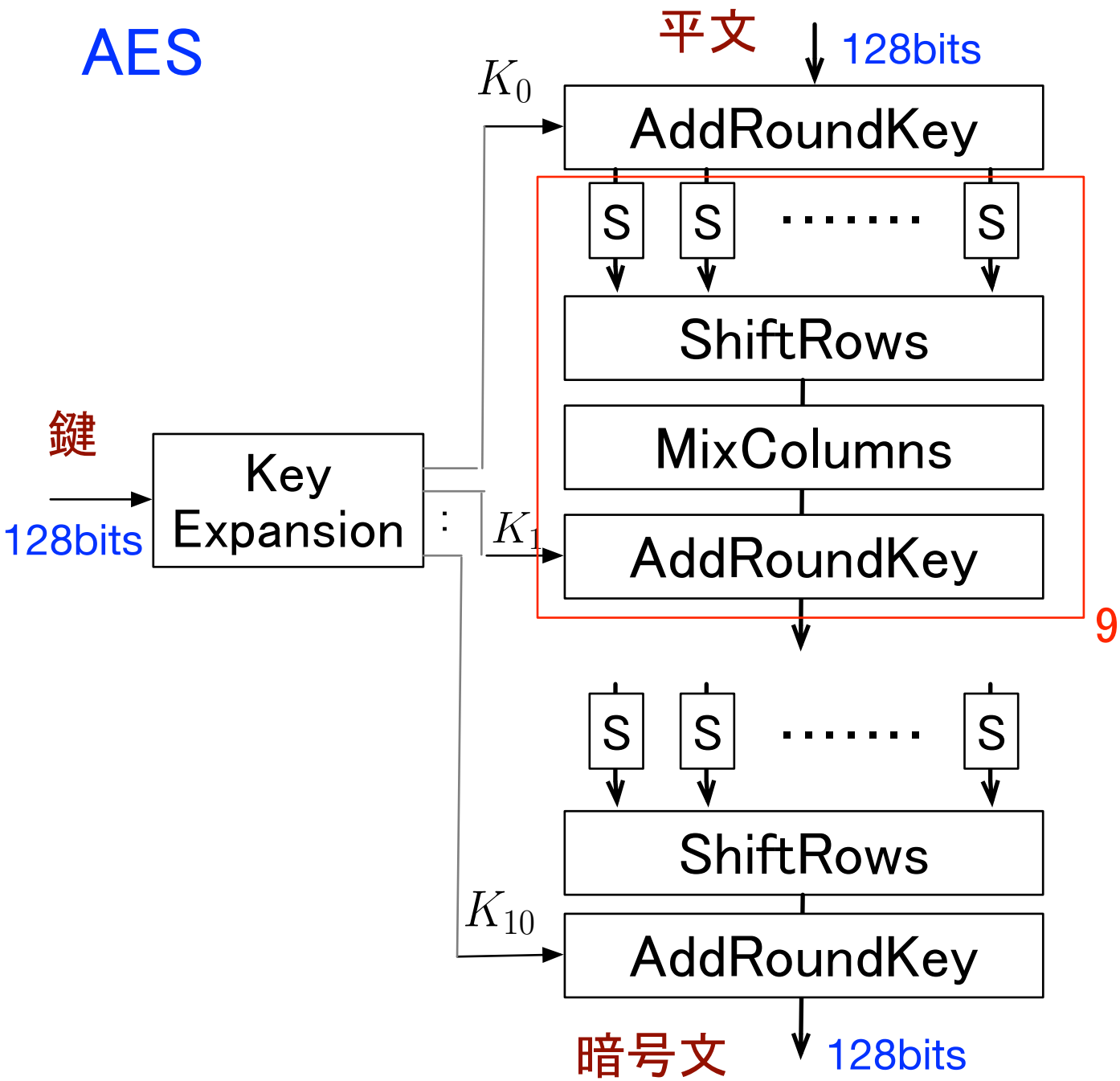
1997年NIST(アメリカ国立標準技術研究所)公募

2000年10月:21方式からRijndael (Daemen-Rijmen)が採用

2001年3月 アメリカ連邦規格

平文:128ビット, 鍵:128ビット, 192ビット, 256ビット

AES



排他的論理和

S-Box（1バイトの非線形変換）

バイト単位の転置

線形変換（4バイト単位の行列演算）

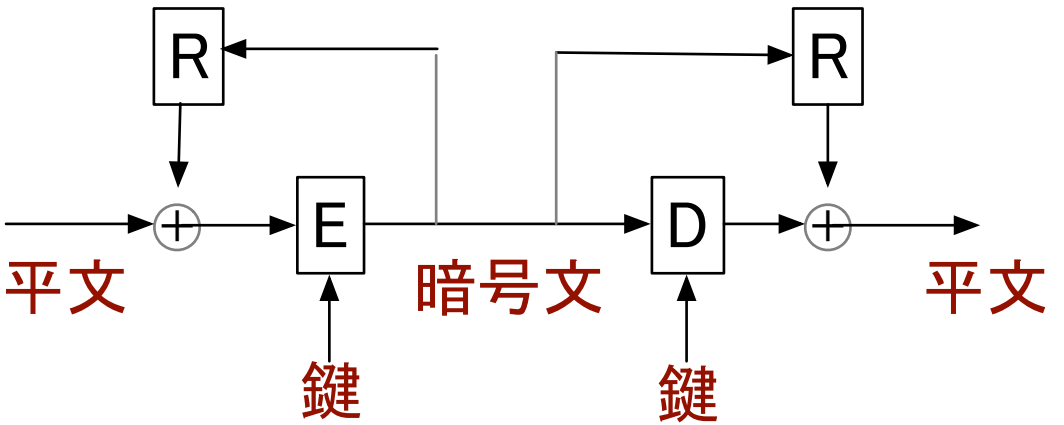
鍵192bits：11回
鍵256bits：13回

暗号利用モード

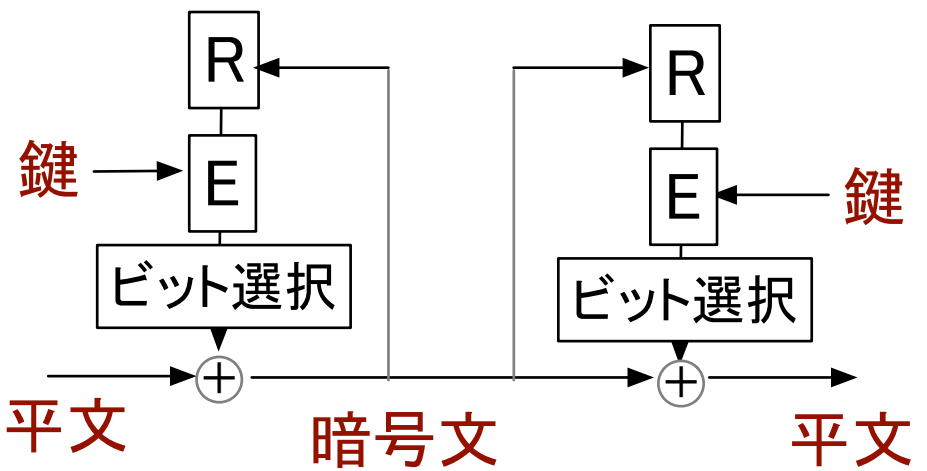
ECB(Electronic code book)モード

同じ平文が同じ暗号文になる

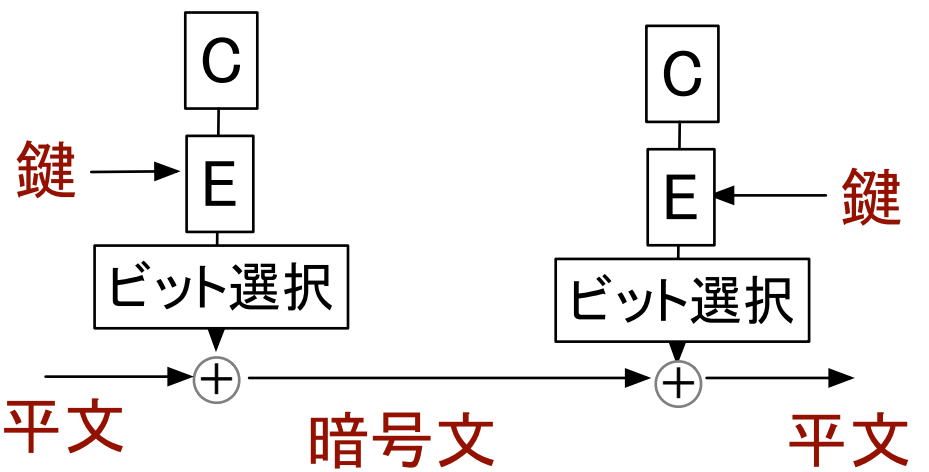
CBC(Cipher block chaining)モード



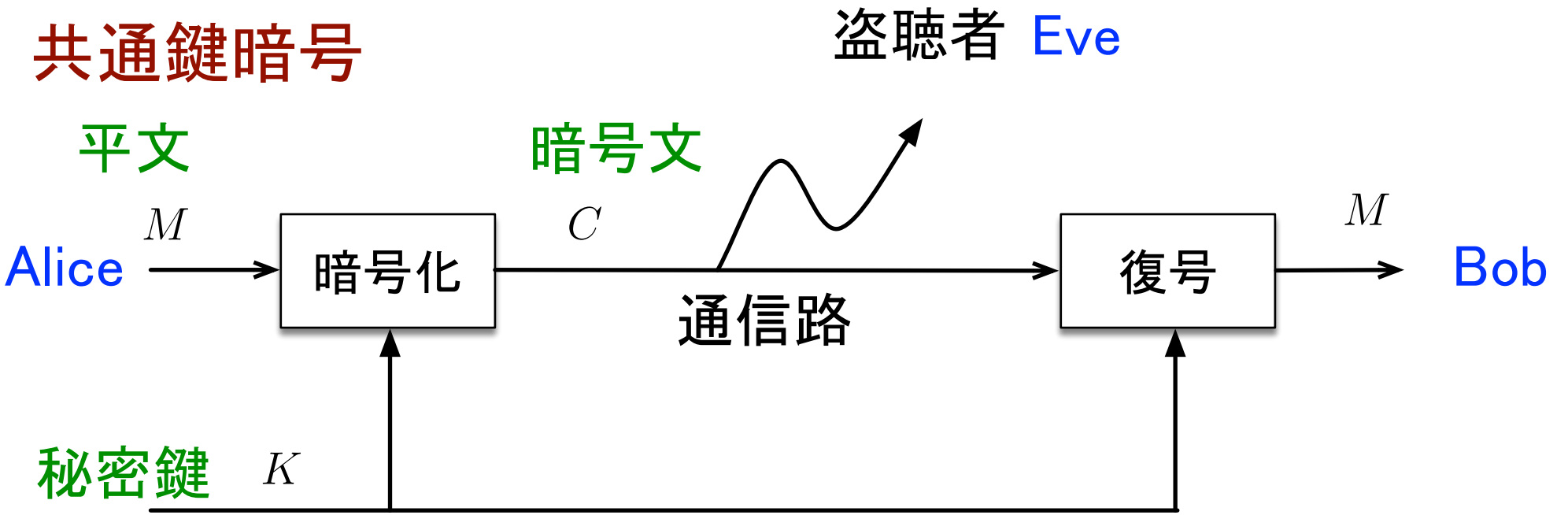
CFB(Cipher Feedbak)モード



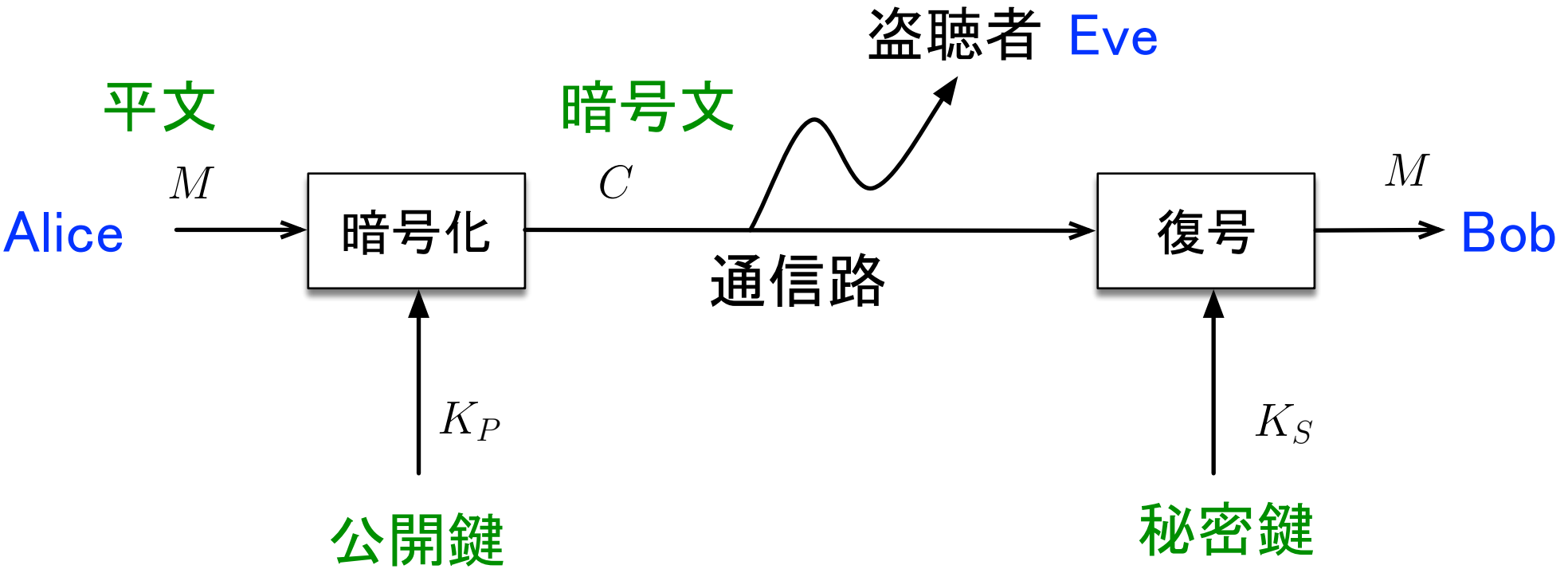
カウンターモード



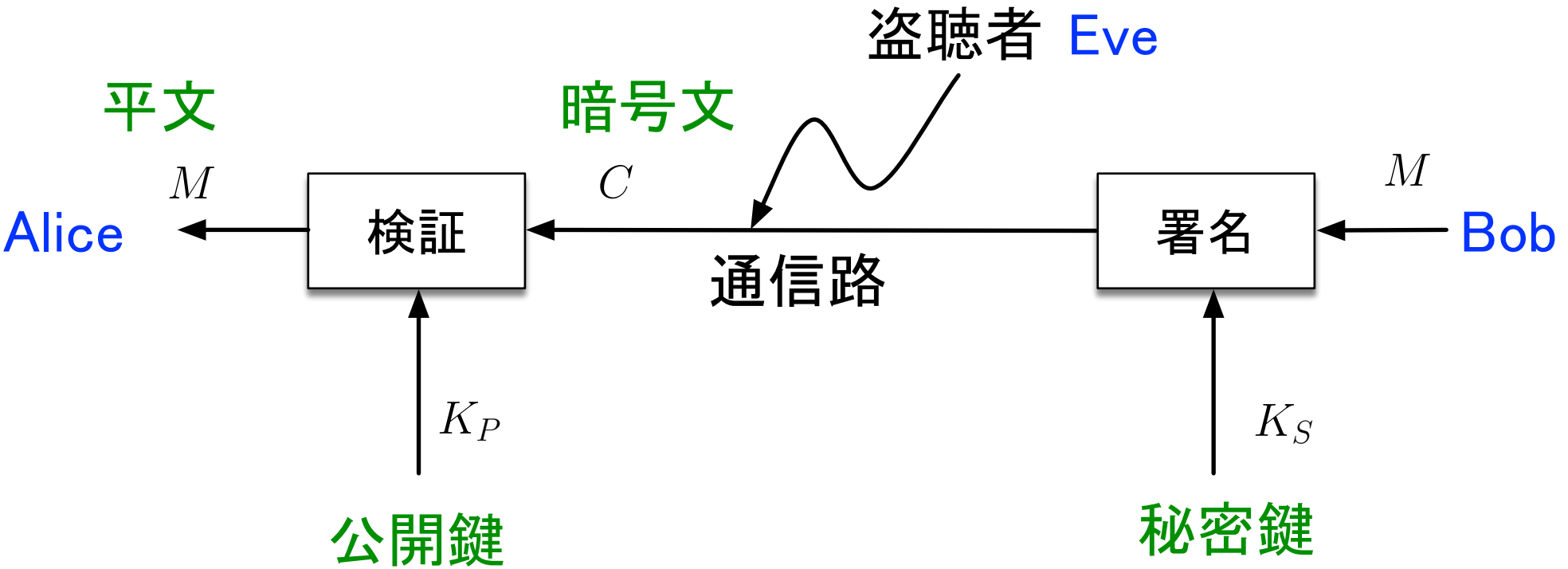
計算量的安全性に基づく暗号・情報セキュリティ符号化



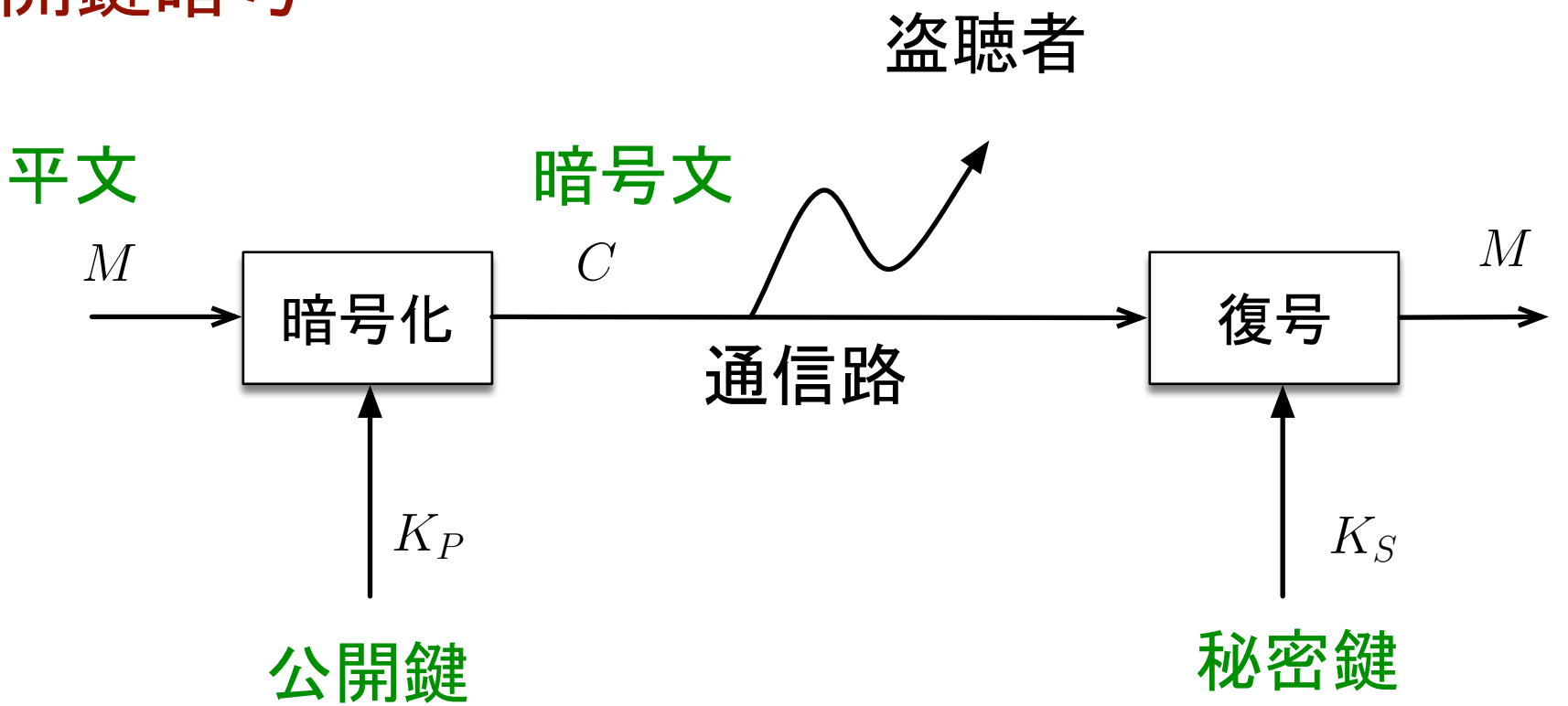
公開鍵暗号（秘匿通信）



公開鍵暗号（デジタル署名）



公開鍵暗号



公開鍵から秘密鍵を求めるのが困難となるように工夫

素因数分解の困難さ
離散対数問題の困難さ

← 整数論

フェルマーの小定理

p :素数, a : $1 \leq a \leq p-1$ の整数

$$a^{p-1} = 1 \pmod{p}$$

例: $p = 5$ の場合

$$\begin{aligned} 1^4 &= 1 = 1 \pmod{5} \\ 2^4 &= 16 = 1 \pmod{5} \\ 3^4 &= 81 = 1 \pmod{5} \\ 4^4 &= 256 = 1 \pmod{5} \end{aligned}$$

フェルマーの小定理

p :素数, a : $1 \leq a \leq p-1$ の整数

$$a^{p-1} = 1 \pmod{p}$$

証明

$a_1 = b_1 \pmod{p}$

$a_2 = b_2 \pmod{p}$

$a_1 \neq a_2$ ➡ $b_1 \neq b_2$

$b_1 = b_2$ と仮定すると

$a_1 - a_2 = b_1 - b_2 = 0 \pmod{p}$

$$\begin{aligned} a\times 1 &= b_1 \pmod{p} \\ a\times 2 &= b_2 \pmod{p} \\ &\vdots \\ a\times p-1 &= b_{p-1} \pmod{p} \end{aligned}$$

$$a^{p-1}(1\times 2\times\cdots\times(p-1)) = 1\times 2\times\cdots\times(p-1) \pmod{p}$$

オイラーの定理

p, q : 素数, $n = pq$, $\phi(n) = (p-1)(q-1)$

a : n と互いに素な整数

$$a^{\phi(n)} = 1 \pmod{n}$$

例: $n = 15 = 3 \cdot 5$, $\phi(15) = 2 \cdot 4 = 8$ の場合

$$\begin{aligned}
1^8 &= 1 = 1 \pmod{15} \\
2^8 &= 256 = 15 \times 17 + 1 = 1 \pmod{15} \\
4^8 &= 65536 = 15 \times 4369 + 1 \times 1 = 1 \pmod{15} \\
7^8 &= 5764801 = 15 \times 384320 + 1 = 1 \pmod{15} \\
&\vdots
\end{aligned}$$

オイラーの定理

p, q : 素数, $n = pq$, $\phi(n) = (p-1)(q-1)$

a : n と互いに素な整数

$$a^{\phi(n)} = 1 \pmod{n}$$

証明

$\mathcal{B} = \{b_1, b_2, \cdots, b_{\phi(n)}\}$ $C = b_1 \times b_2 \times \cdots \times b_{\phi(n)}$

n と互いに素な n 未満の整数の集合

$\mathcal{A} = \{ab_1, ab_2, \cdots, ab_{\phi(n)}\}$

$$a^{\phi(n)} C = C \pmod{n}$$

RSA暗号 (Rivest-Shamir-Adelman, 1977)

p, q : 素数, $n = pq$, $\phi(n) = (p-1)(q-1)$

e , d : $e \times d = 1 \pmod{\phi(n)}$ を満たす整数

秘密鍵: p, q, d

公開鍵: n, e

暗号化

平文: M

暗号文: $C = M^e \pmod{n}$

復号

暗号文: C

平文: $M = C^d \pmod{n}$

$$C^d = (M^e)^d = M^{ed} = M^{k\phi(n)+1} = M \pmod{n}$$

RSA暗号 (Rivest-Shamir-Adelman, 1977)

暗号化

平文: M

暗号文: $C = M^e \pmod{n}$

復号

暗号文: C

平文: $M = C^d \pmod{n}$

例: $n = 15 = 3 \cdot 5$, $\phi(15) = 2 \cdot 4 = 8$ の場合

$e = 3$, $d = 3$, $e \times d = 9 = 8 + 1 = 1 \pmod{8}$

$M = 8$ $C = M^3 = 512 = 34 \times 15 + 2 = 2 \pmod{15}$

$M = C^3 = 8 \pmod{15}$

$M = 6$ $C = M^3 = 216 = 14 \times 15 + 6 = 6 \pmod{15}$

$M = C^3 = 216 = 14 \times 15 + 6 = 6 \pmod{15}$

RSA暗号 (Rivest-Shamir-Adelman, 1977)

p, q : 素数, $n = pq$, $\phi(n) = (p-1)(q-1)$

e , d : $e \times d = 1 \pmod{\phi(n)}$ を満たす整数

秘密鍵: p, q, d

公開鍵: n, e

$p, q \Rightarrow n$: 容易

$n \Rightarrow p, q$: 困難

暗号化

平文: M

暗号文: $C = M^e \pmod{n}$

解読

暗号文: C

$n \Rightarrow p, q \Rightarrow \phi(n) \Rightarrow d$

素因数分解 e

$M = C^d \pmod{n}$

RSA暗号を用いたデジタル署名

p, q : 素数, $n = pq$, $\phi(n) = (p-1)(q-1)$

e , d : $e \times d = 1 \pmod{\phi(n)}$ を満たす整数

秘密鍵: p, q, d

公開鍵: n, e

$p, q \Rightarrow n$: 容易

$n \Rightarrow p, q$: 困難

暗号化

平文: M

暗号文: $C = M^d \pmod{n}$

復号

暗号文: C

平文: $M = C^e \pmod{n}$

$$C^e = (M^d)^e = M^{ed} = M^{k\phi(n)+1} = M \pmod{n}$$

素因数分解の困難さ

離散対数問題の困難さ

p :素数, g :原始元

$y = g^x \pmod p$: $1 \leq x, y \leq p-1$

$x \Rightarrow y$:容易

$y \Rightarrow x$:困難

実数なら

$x = \log_g y$

例: $p = 13$, $g = 2$ の場合

$2^1 = 2 = 2 \pmod{13}$

$2^2 = 4 = 4 \pmod{13}$

$2^3 = 8 = 8 \pmod{13}$

$2^4 = 16 = 3 \pmod{13}$

$2^5 = 32 = 6 \pmod{13}$

$2^6 = 64 = 12 \pmod{13}$

$2^7 = 128 = 11 \pmod{13}$

$2^8 = 256 = 9 \pmod{13}$

$2^9 = 512 = 5 \pmod{13}$

$2^{10} = 1024 = 10 \pmod{13}$

$2^{11} = 2048 = 7 \pmod{13}$

$2^{12} = 4096 = 1 \pmod{13}$

ElGamal暗号 (1984)

離散対数問題

p :素数, g :原始元

$y = g^x \pmod p$: $1 \le x, y \le p-1$

$x \Rightarrow y$:容易

$y \Rightarrow x$:困難

秘密鍵: x

公開鍵: p, g, y

暗号化

平文: M 乱数: r

暗号文: $C_1 = g^r \pmod p$

$C_2 = My^r \pmod p$

復号

暗号文: $C_1 = g^r \pmod p$

$C_2 = My^r \pmod p$

$C_1^x = g^{rx} = g^{xr} = y^r \pmod p$

$M = C_2 / C_1^x \pmod p$

ElGamal暗号 (1984)

秘密鍵: x

公開鍵: p, g, y

暗号化

平文: M　乱数: r

暗号文: $C_1 = g^r \pmod p$

$C_2 = My^r \pmod p$

復号

暗号文: $C_1 = g^r \pmod p$

$C_2 = My^r \pmod p$

$C_1^x = g^{rx} = g^{xr} = y^r \pmod p$

$M = C_2/C_1^x \pmod p$

例: $p = 13$, $g = 2$, $x = 9$, $y = 2^9 = 512 = 5 \pmod{13}$

$M = 9$, $r = 5$ **の場合**

$C_1 = 2^5 = 32 = 6 \pmod{13}$

$C_2 = 9 \times 5^5 = 9 \times 3125 = 28125 = 6 \pmod{13}$

$C_1^x = 6^9 = 10077696 = 5 \pmod{13}$

$M = 6 \times 5^{-1} = 6 \times 8 = 48 = 13 \times 3 + 9 = 9 \pmod{13}$

$(5 \times 8 = 40 = 3 \times 13 + 1 = 1 \pmod{13})$

ElGamal暗号 (1984)

秘密鍵: x

公開鍵: p, g, y

暗号化

平文: M　乱数: r

暗号文: $C_1 = g^r \pmod p$

$C_2 = My^r \pmod p$

復号

暗号文: $C_1 = g^r \pmod p$

$C_2 = My^r \pmod p$

$C_1^x = g^{rx} = g^{xr} = y^r \pmod p$

$M = C_2/C_1^x \pmod p$

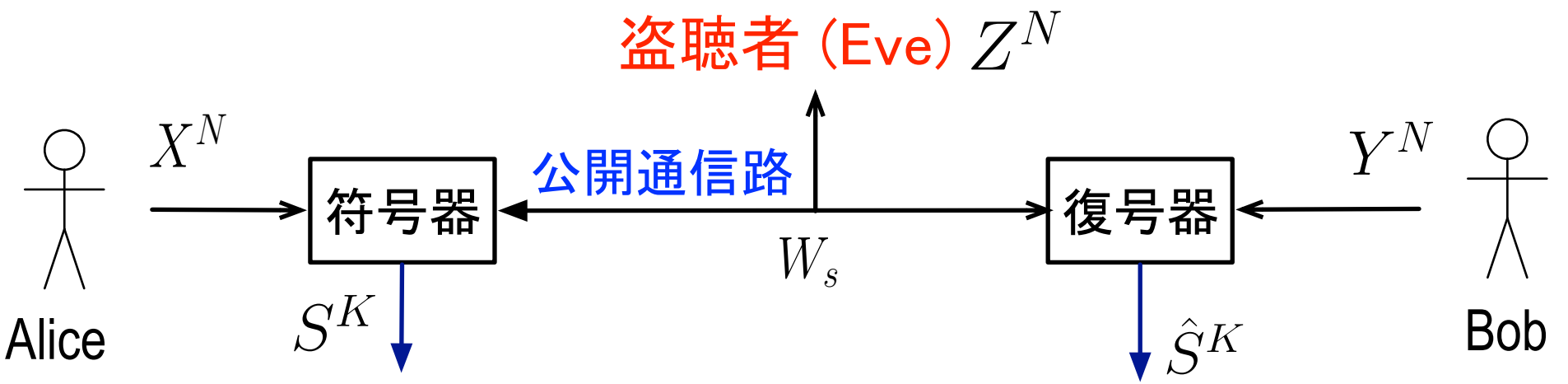
特長

M が同じでも (C_1, C_2) が毎回異なる.

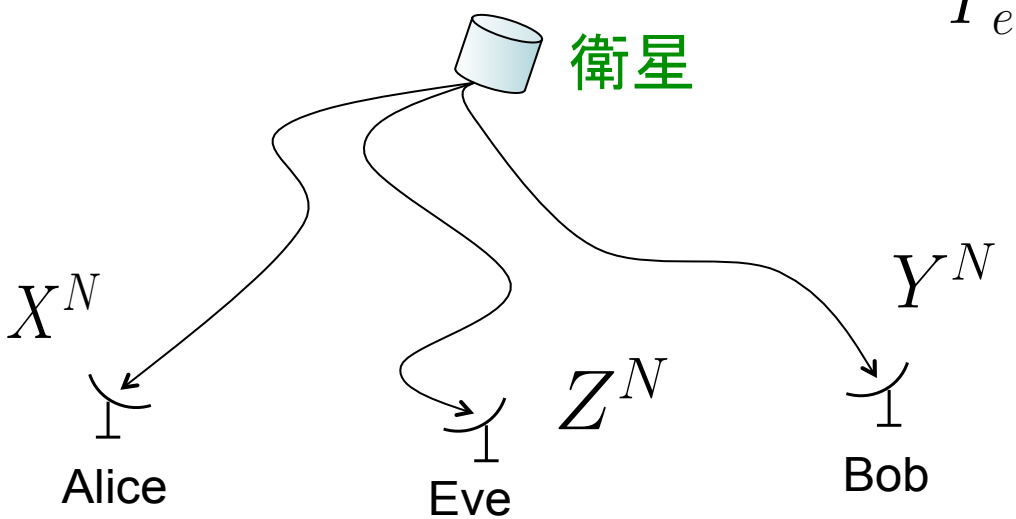
離散対数問題が解ける

$C_1 = g^r \pmod p$ ➡ r ➡ $M = C_2/y^r$

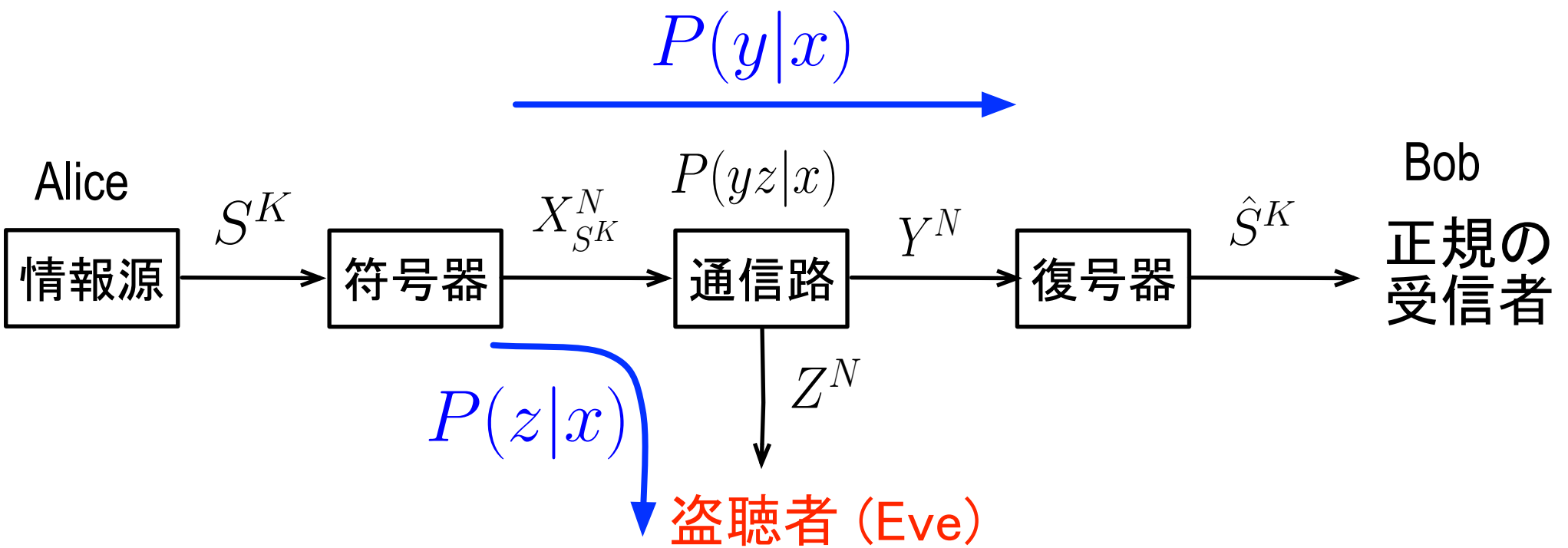
情報量的安全性に基づく乱数共有システム



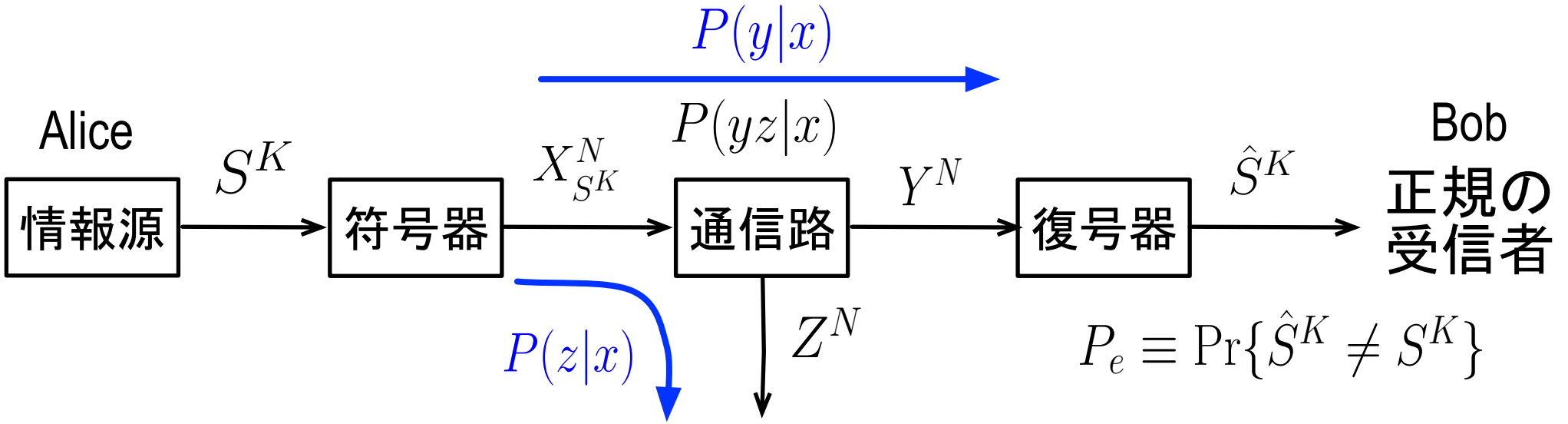
$$P_e \equiv \Pr\{\hat{S}^K \neq S^K\}$$



雑音のある通信路


$P(y|x)$
Alice
S^K
情報源
符号器
$X_{S^K}^N$
$P(yz|x)$
通信路
Y^N
復号器
$\hat{S}^K$
Bob
正規の
受信者
Z^N
$P(z|x)$
盗聴者 (Eve)

通信路符号化符号化定理



盗聴者の通信路の方が
雑音が大きい場合

$C_Y > C_Z$

符号化レート: $R = K/N$

情報源エントロピー: $H(S)$

通信路容量: $C_Y \equiv \max_X I(X;Y)$

$C_Z \equiv \max_X I(X;Z)$

$$R < \frac{C_Y}{H(S)} \Longleftrightarrow P_e < \varepsilon$$

$$R > \frac{C_Z}{H(S)} \Longleftrightarrow P_e^{(Z)} > 1-\varepsilon$$