

量子暗号

1. 情報理論的安全性
2. BB84量子鍵配布プロトコル
3. 量子暗号システム実現

究極の暗号：使い捨て鍵暗号

\oplus : 排他的和, mod2の加算
 $0\oplus 0=1\oplus 1=0, 1\oplus 0=0\oplus 1=1$

暗号化

0100001	送りたい7bit !
$\oplus 1101100$	使い捨て鍵
<hr/>	
1001101	送信7bit

復号化

1001101	受信7bit
$\oplus 1101100$	共有鍵
<hr/>	
0100001	復号7bit !

平文と同量以上の共有鍵があれば完全秘匿性達成!

7bit送るごとに使い捨ての鍵を使えば安全!!

⇒ 量子暗号通信で使い捨て鍵をどんどん生成
(量子鍵配送, QKD)

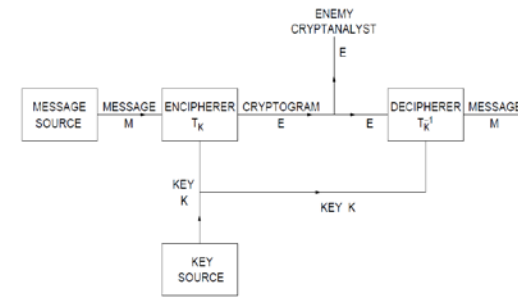
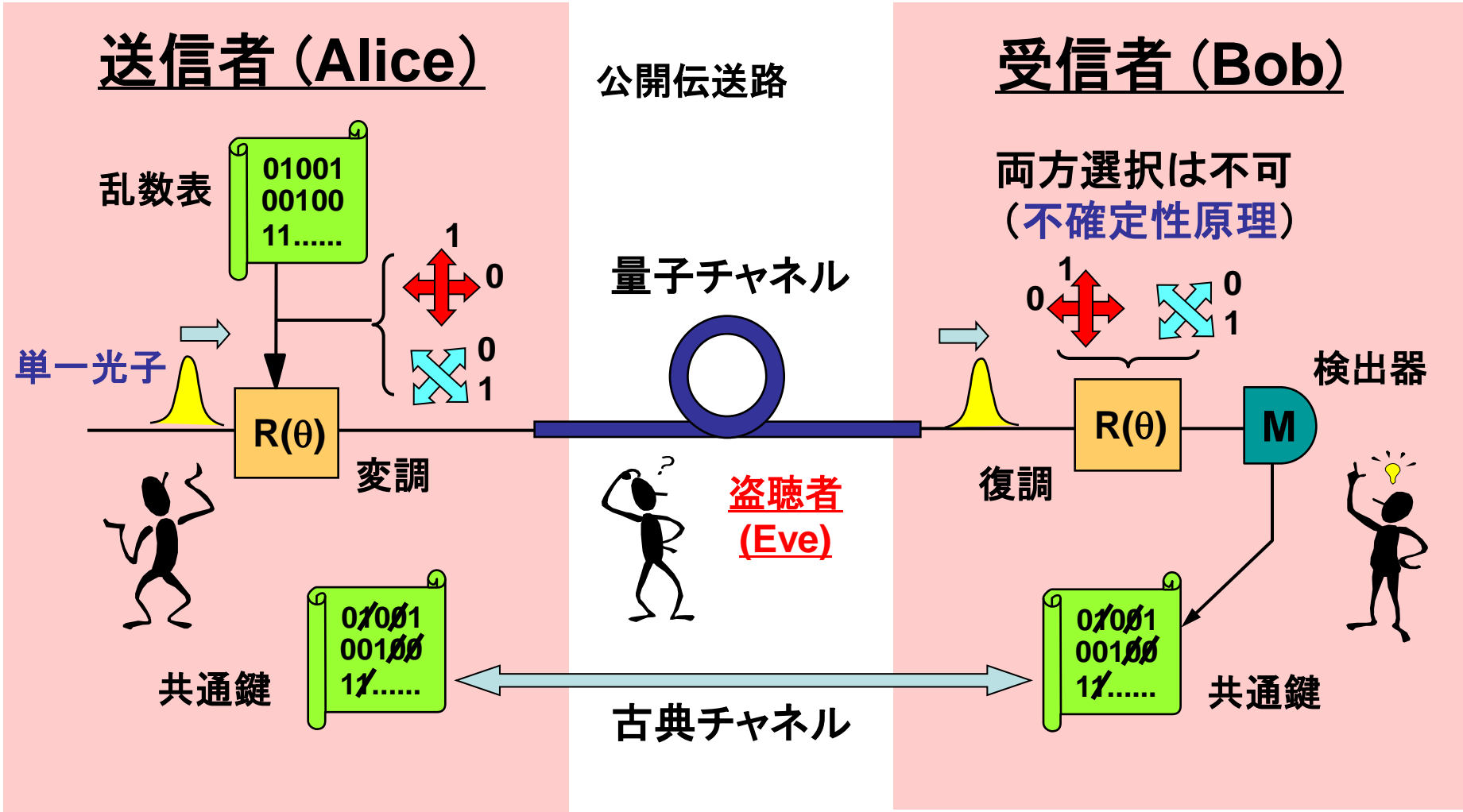


Fig. 1. Schematic of a general secrecy system

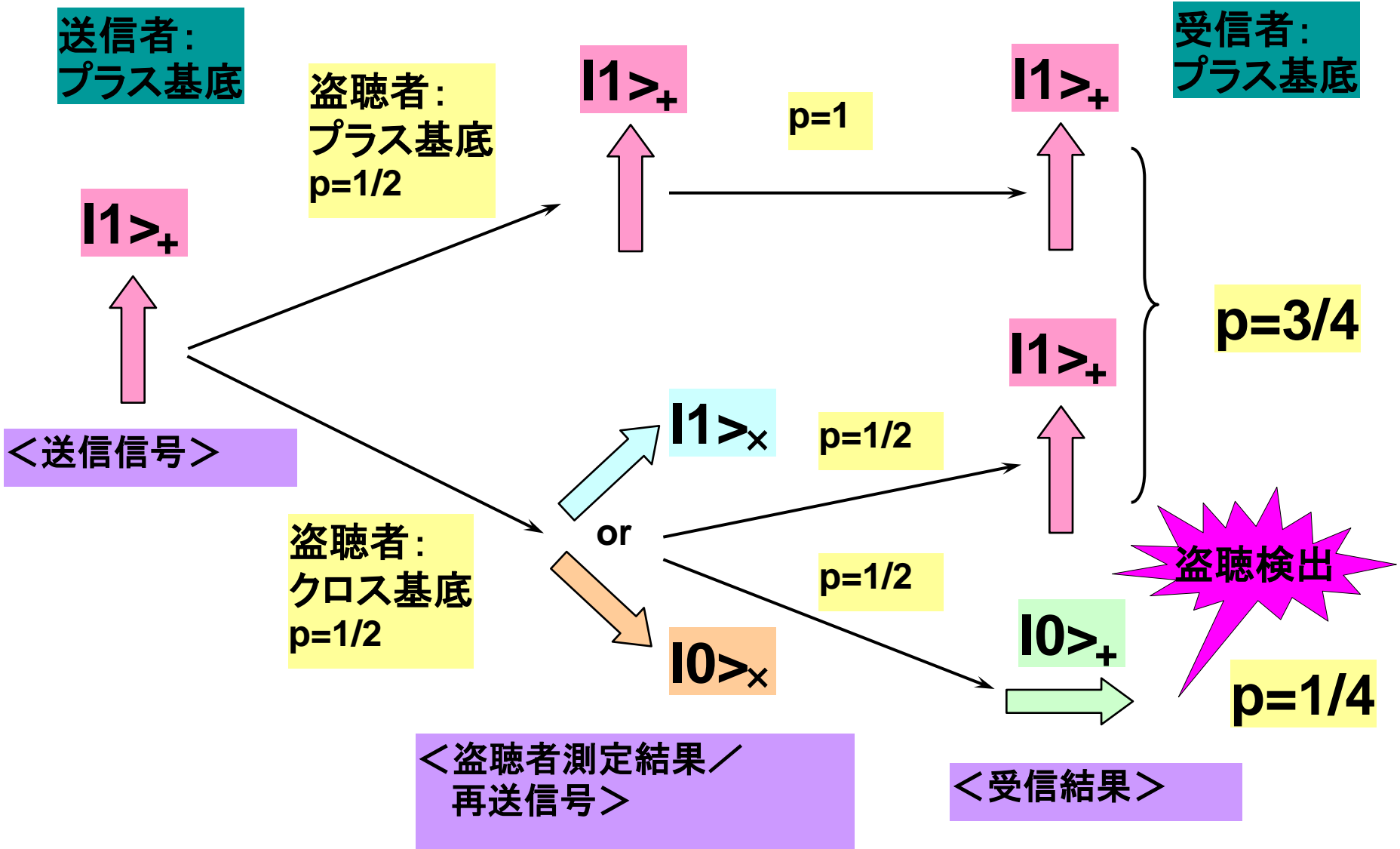
量子暗号鍵配布の一例BB84



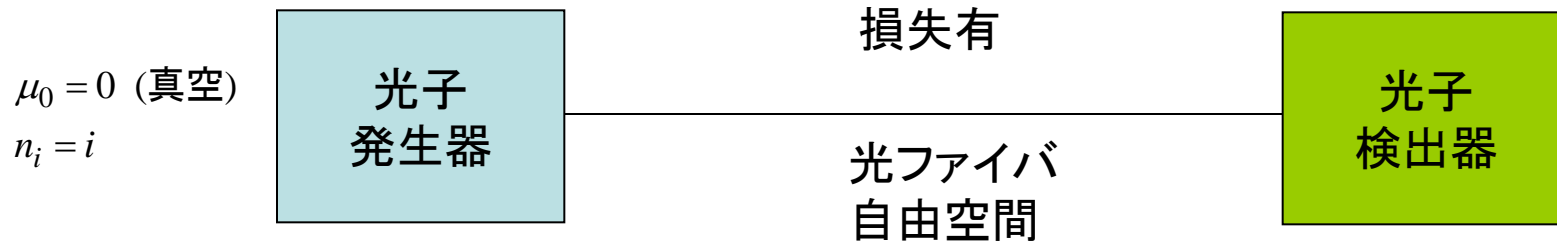
量子暗号プロトコルBB84

	元のbit列	1	0	1	1	0	0	1	1	0	0	1	1	1	0
送信者 Alice	変調法														
	送信偏光														
受信者 Bob	復調法														
	受信偏光		—	—				—				—		—	
	受信bit列	1	—	—	1	0	0	—	1	0	0	—	1	—	0
双方 チェック	テストbit	○				○					○				
	完成bit列				1	0			1	0			1		0

BB84での盗聴の検出過程



量子暗号通信の数理モデル



平均光子数 μ_j , 確率 q_j ($j = 0, \dots, k$)
 \Rightarrow 光子数 n_i^j , 生成確率 p_i^j ($i = 0, \dots$)

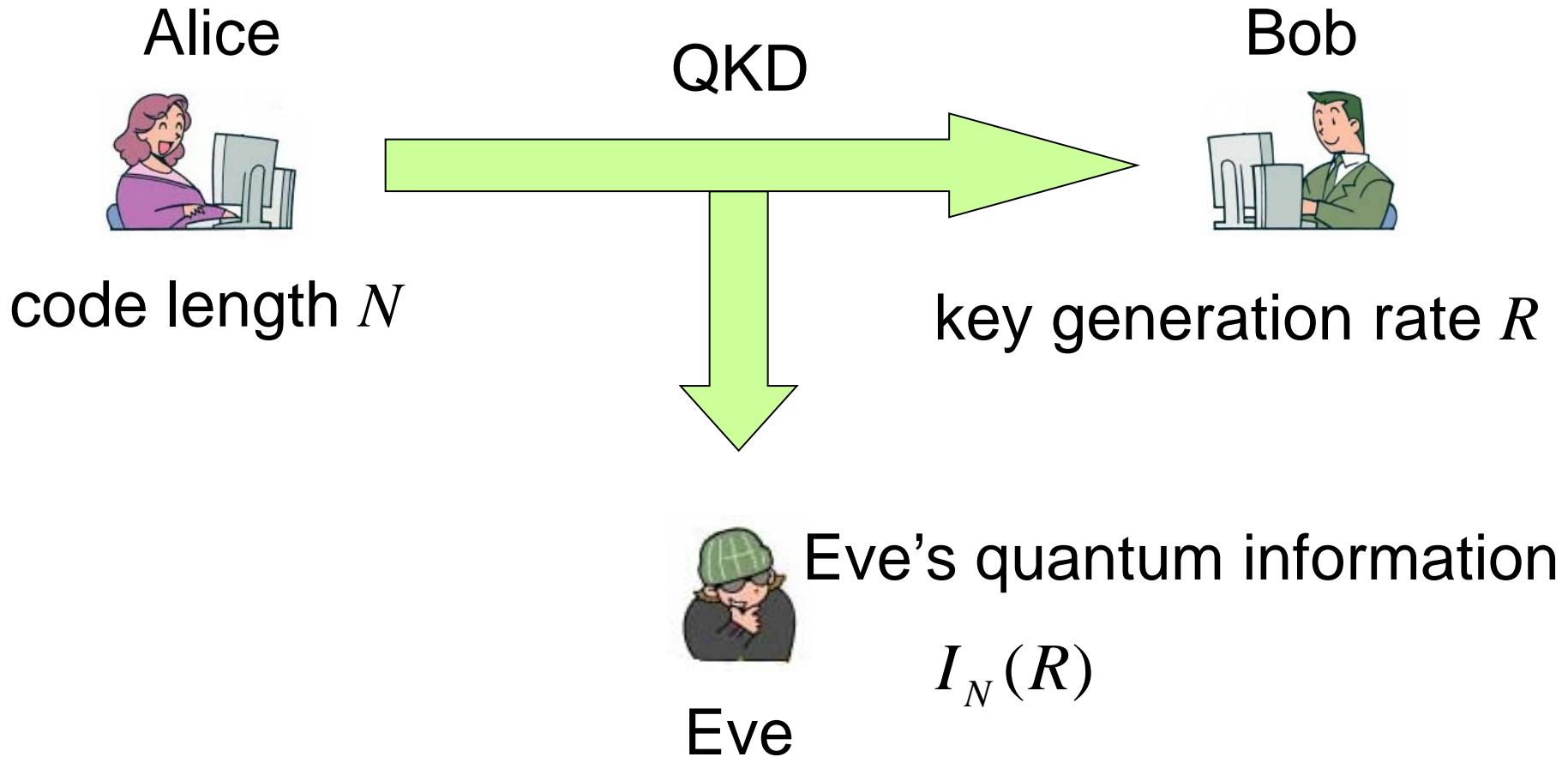
光子数 $n_i \rightarrow$ 検出確率 d_i
 n_0 : 真空 \rightarrow 検出確率 $d_0 (> 0)$
(d_0 : dark count rate)

完全単一光子源: $q_0 = 0; \mu_1 = 1, q_1 = 1, p_1^1 = 1$
不完全単一光子源例:
 $q_0 = 0; \mu_1 < 1, q_1 = 1, p_0^1 = 0.1, p_1^1 = 0.89, p_2^1 = 0.01$
弱コヒーレント光:
 μ_j : 小, p_i^j : ポアソン分布

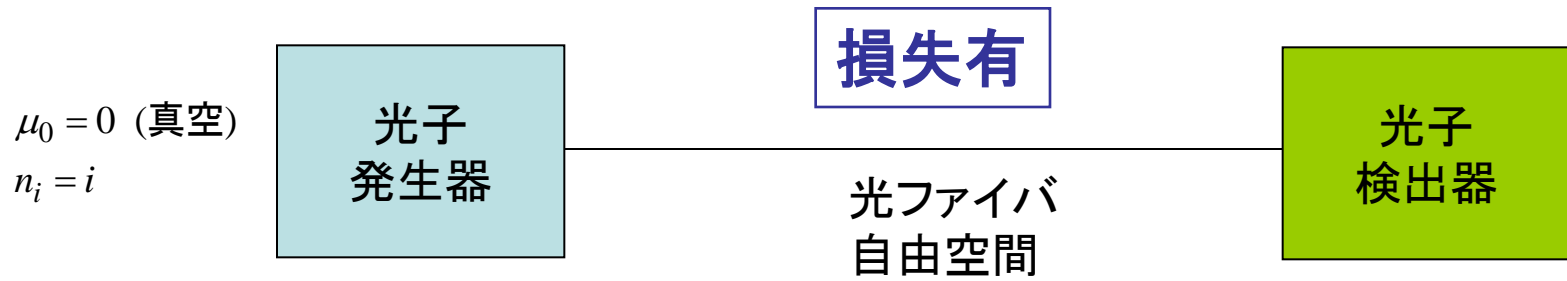
量子暗号プロトコル

量子(古典)ソフトウェア

Simple model of QKD



量子暗号通信モデル — 様々な不完全性



平均光子数 μ_j , 確率 q_j ($j = 0, \dots, k$)
 \Rightarrow 光子数 n_i^j , 生成確率 p_i^j ($i = 0, \dots$)

光子数 $n_i \rightarrow$ 検出確率 d_i
 n_0 : 真空 \rightarrow 検出確率 $d_0 (> 0)$
(d_0 : dark count rate)

完全単一光子源: $q_0 = 0; \mu_1 = 1, q_1 = 1, p_1^1 = 1$
不完全単一光子源例:
 $q_0 = 0; \mu_1 < 1, q_1 = 1, p_0^1 = 0.1, p_1^1 = 0.89, p_2^1 = 0.01$
弱コヒーレント光:
 μ_j : 小, p_i^j : ポアソン分布

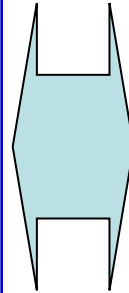
確率的挙動
量子暗号プロトコル
量子(古典)ソフトウェア

Security in a practical setting

ideal

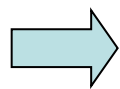
real

- single photon
= 1 random bit
- infinite length code
 - asymptotic estimation
- neglect estimation errors
 - no statistical fluctuation



- weak coherent light
 - 0,1,2,... photons
= 1 random bit
- finite length code
 - limited by memory and encode/decode time
- estimation errors
 - statistical fluctuation

The above discrepancy is compensated by software



estimation of sacrifice bits with decoy method

Information Leakage

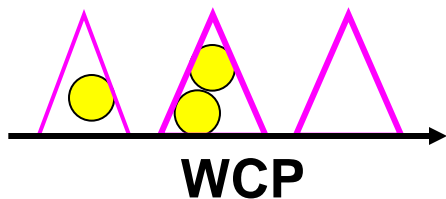
Alice

Eve

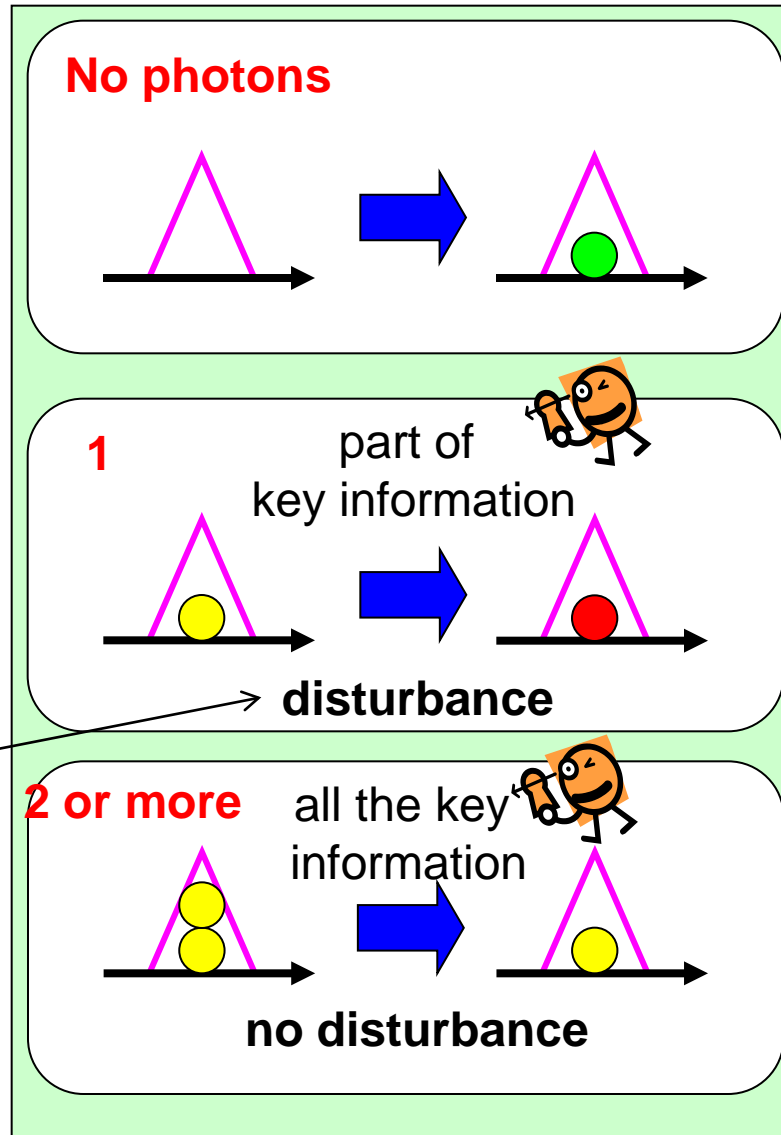
Bob

single intensity

probabilistic



Quantum Effect!!



detection events: J^0

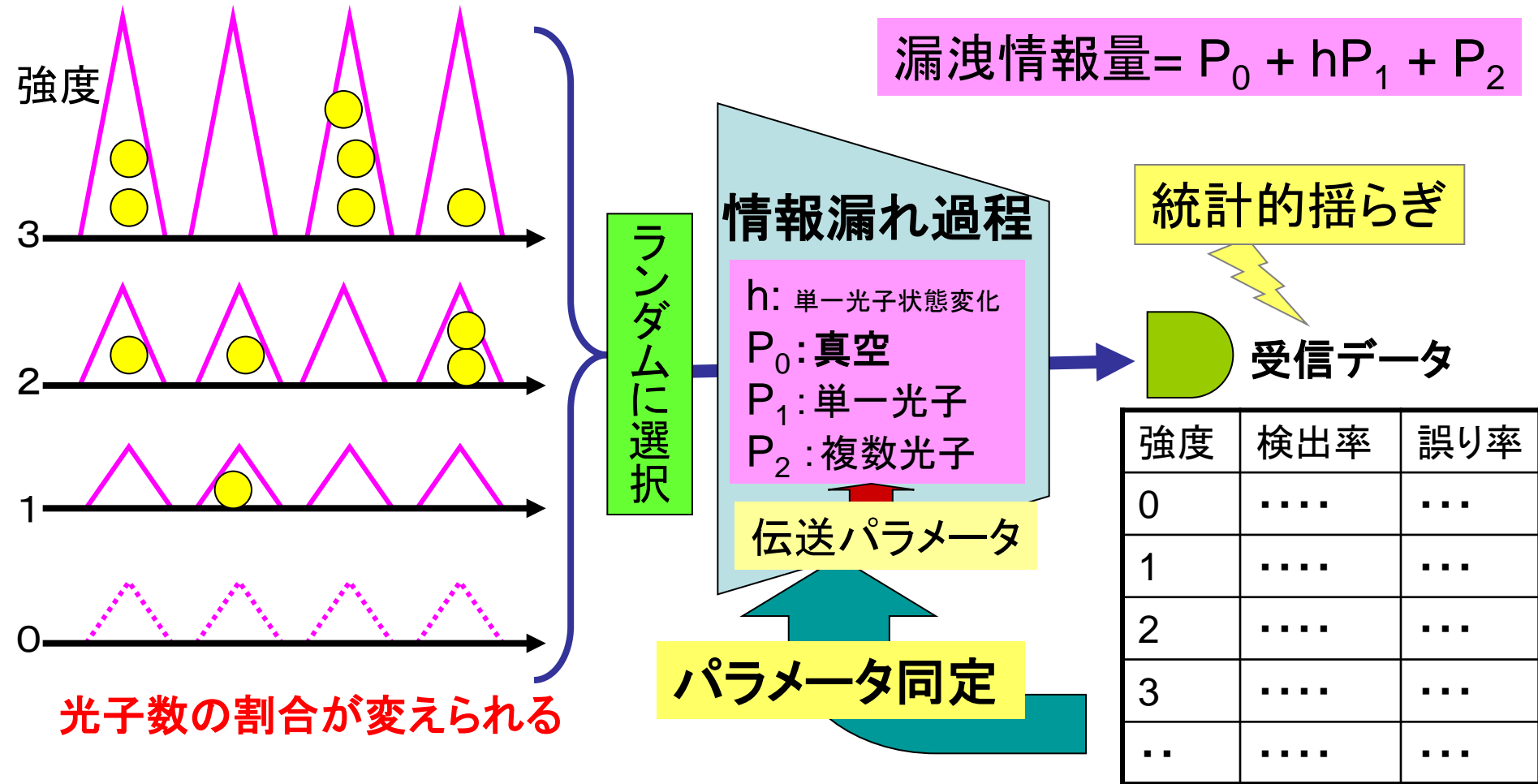
detection events: J^1
with phase error: r^1

detection events: J^2

Decoy+Quantum Information Theory

[Hwang 2003; Wang 2005, Ma et al. 2005; Hayashi 2007]

$$\text{漏洩情報量} = P_0 + hP_1 + P_2$$



送信強度 \Rightarrow 受信データの種類増加 \Rightarrow 推定精度向上 (4種で十分)

開発した量子暗号装置・実験環境



実験環境

量子通信装置

誤り訂正・秘密増幅装置

光ファイバ 20km
通常のオフィス環境
(ERATO-SORST
東京オフィス)

NEC製を改造
(送信強度: 4種類)
波長 $1.55\ \mu\text{m}$
システムクロック 62.5 MHz

PC (LINUX)
CPU:
Pentium(R)4(3GHz)
メモリ: 2GB

Setting of our decoy method QKD

decoy QKD (four intensities)

intensities : sending prob.

0 : 0.125

0.07 : 0.375

0.35 : 0.125

(signal) 0.50 : 0.375

code length $N = 10^5$

security parameter $\delta = 9$

$$I_E \leq 2^{-9}$$

One protocol:

7.5×10^8 pulses are sent

Alice

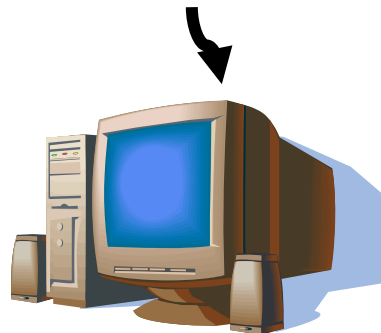


BB84 protocol

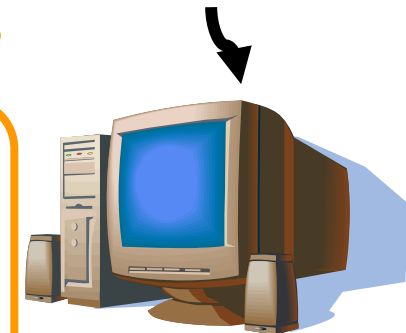
Bob



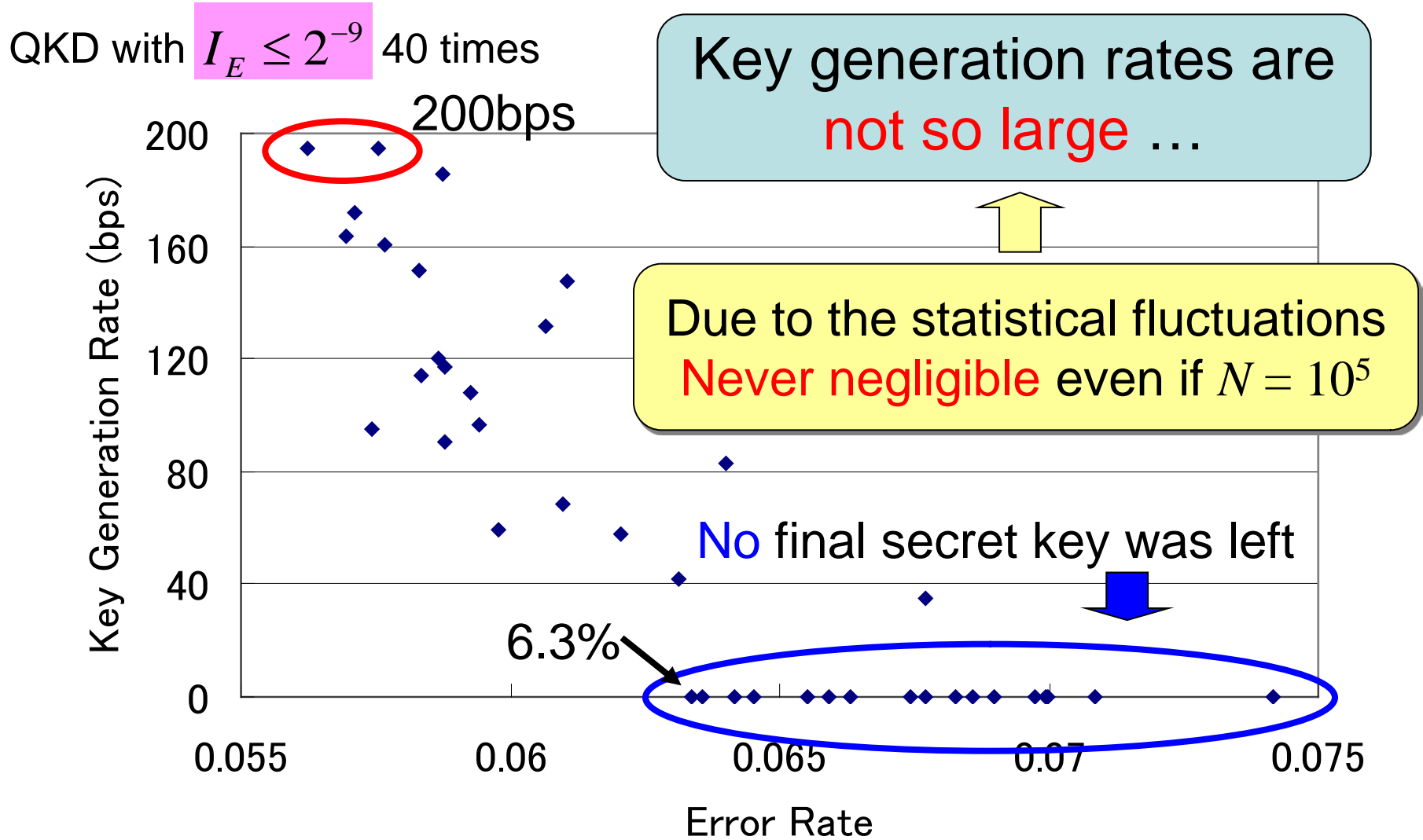
raw key + observed quantities



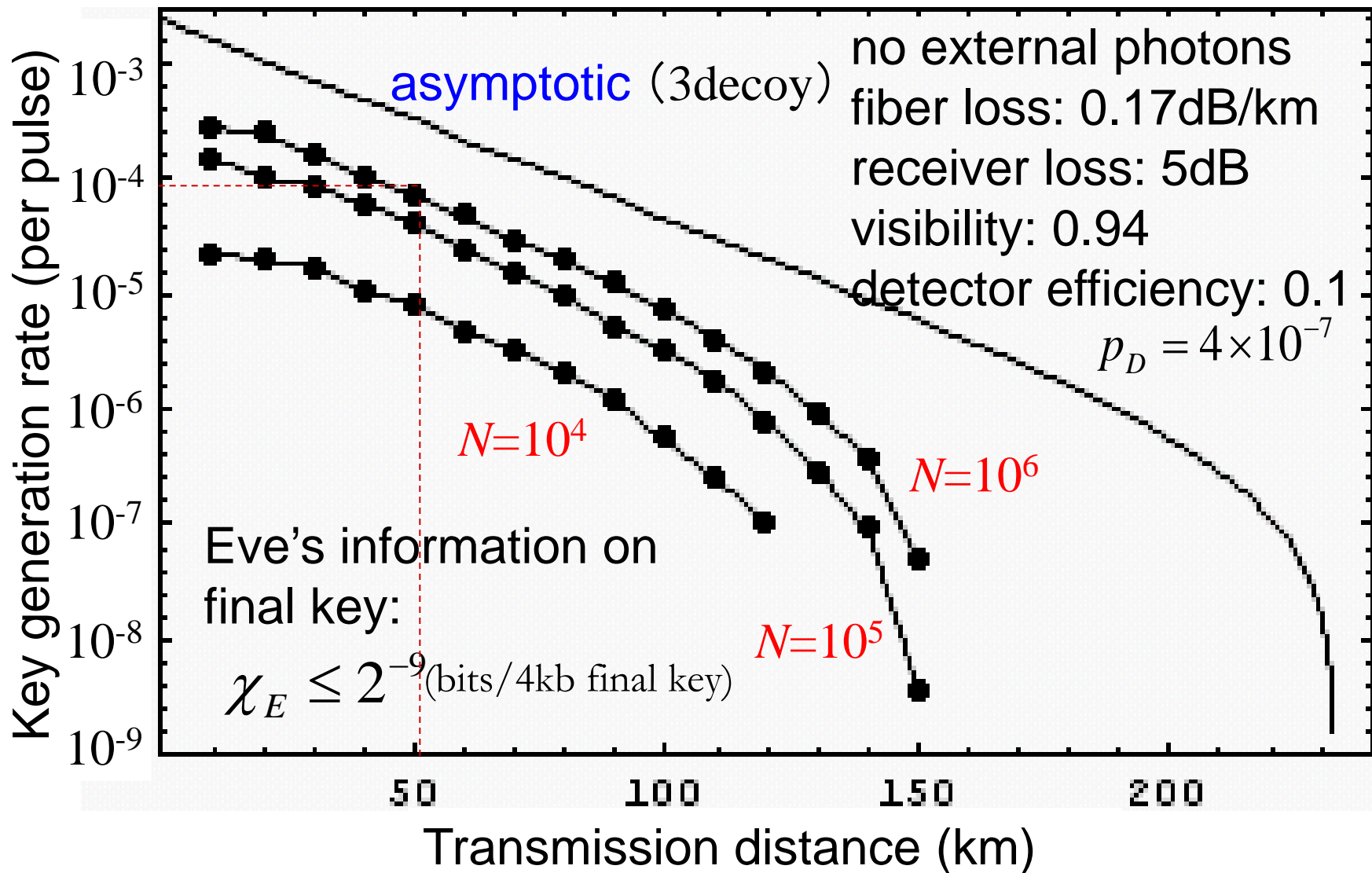
of pulses sent,
of pulses received,
of pulses with basis coincidence,
of error bits



Key generation rates with guaranteed quantitative security in the real world



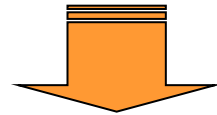
Performance Outlook



QKD System: Conclusion and requirements

Eve's information: $\leq 2^{-9}$
Key generation rate: 200 bps

Achievement of the **quantitative secure** QKD system
in the **real (finite) world** ($I_E \leq 2^{-\delta}$)



Performance criteria for QKD systems
in the real world !

Key generation rate
Transmission distance

Quantitative security

Quantum Cryptography: Future

- Single-photon Source
- Photon Detector
- QKD Protocol
- System Security

- Quantum Cryptographic Protocols

- Quantum Repeater

量子計算

量子アルゴリズム

1. Shorの素因数分解アルゴリズム
2. 隠れ部分群問題

Shorの素因数分解アルゴリズム

15=3×5 と素因数したい

$\mathbf{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, 乗法群 $(\mathbf{Z}_{15}^*, \times)$

$7^1 = 7, 7^2 = 4, 7^3 = 13, 7^4 = 1$ 7の位数4

$\gcd(7^{4/2} - 1, 15) = 3, \gcd(7^{4/2} + 1, 15) = 5$

Shorのアルゴリズムと隠れ部分群問題

整数 \mathbf{Z} の部分群 $4\mathbf{Z}$, 剰余類 $0+4\mathbf{Z}, 1+4\mathbf{Z}, 2+4\mathbf{Z}, 3+4\mathbf{Z}$

$$f(x)=7^x \pmod{15} \Rightarrow f(0)=1, f(1)=7, f(2)=4, f(3)=13$$

- 剰余類上で定数値
- 異なる剰余類上では異なる値

⇒隠れ部分群問題：部分群の生成元を求める

Shorのアルゴリズム

\mathbf{Z} の部分群 \mathbf{Z}_4 を求める問題と等価($\mathbf{Z}_{\phi(15)} = \mathbf{Z}_8$ でよい)

$\text{GF}(2^l)$ 乗法群上で近似, Fourier変換, 連分数展開

Buchmann-Williams暗号

ElGamal暗号

Diffie-Hellman鍵交換

実2次体

ゼロ知識対話証明

代数曲線(楕円曲線)

離散対数

グラフ同型

現代暗号理論

素因数分解

最短格子点

RSA公開鍵暗号

NTRU, etc.

古典計算の世界

