格子問題に基づく複数ビット公開鍵暗号

東京工業大学

草川恵太

河内亮周

田中圭介

東京工業大学

草川恵太

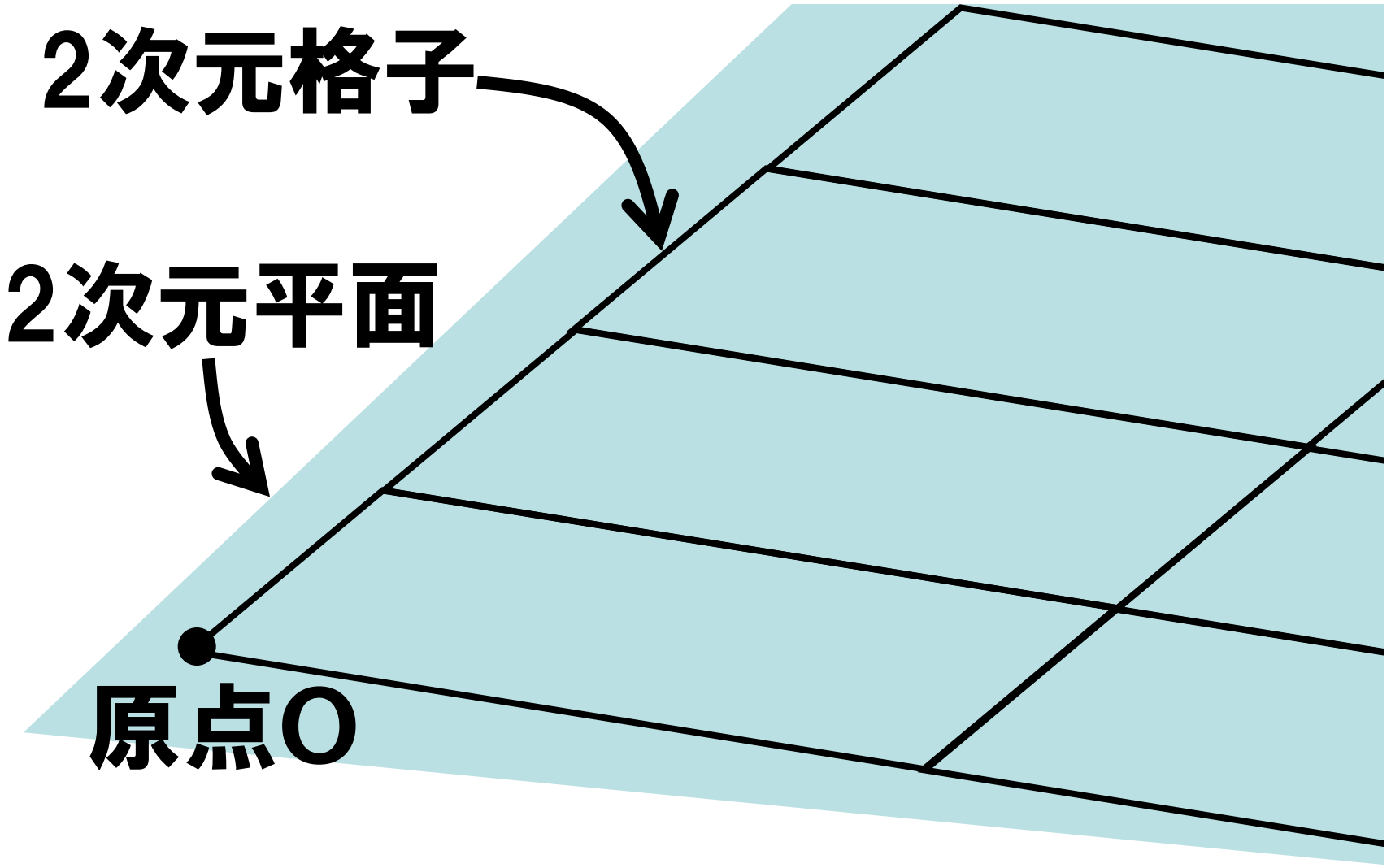
河内亮周

田中圭介

格子問題に基づく複数ビット公開鍵暗号

格子問題
に基づく
複数ビット
公開鍵暗号

R^n中のZ加群


2次元格子
2次元平面
原点O

格子問題
に基づく
複数ビット
公開鍵暗号

格子問題の例

SVP:最短ベクトル問題

uSVP:唯一最短ベクトル問題

CVP:最近ベクトル問題

SVPはRandomized Reductionの元でNP困難

量子計算機でも難しいと考えられている

格子問題に基づく複数ビット公開鍵暗号

現行のRSAや楕円曲線暗号は量子計算機に弱い

格子問題
に基づく
複数ビット
公開鍵暗号

組合せ系暗号の一つ

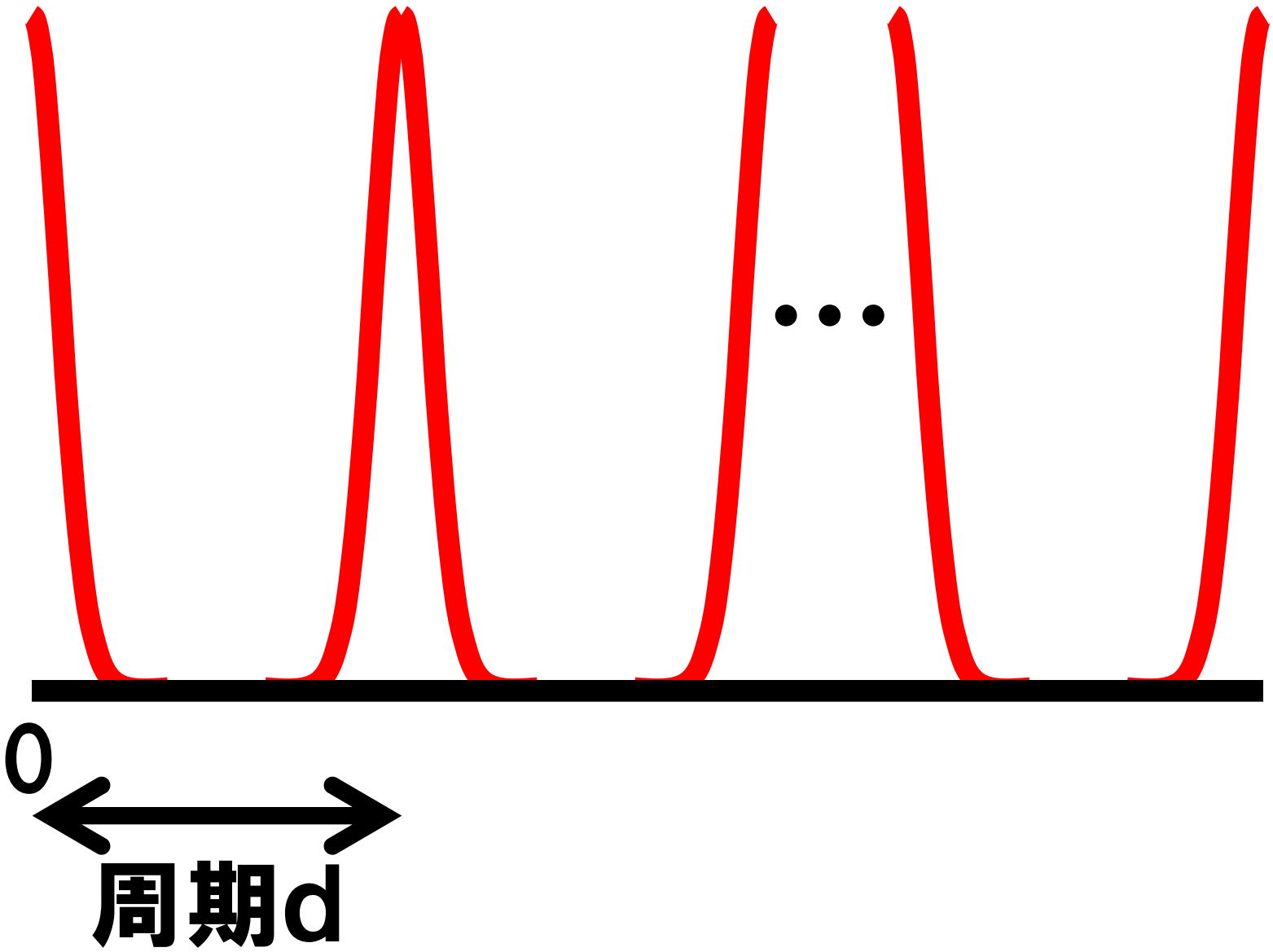
安全性の保証があり
量子計算機に(多分)
強いので(一部で)
注目の的

	ビット数	安全性
Ajtai-Dwork	1ビット	証明有
Regev03		
Regev05		
Ajtai05		証明微妙
GGH	複数ビット	証明無
NTRU		

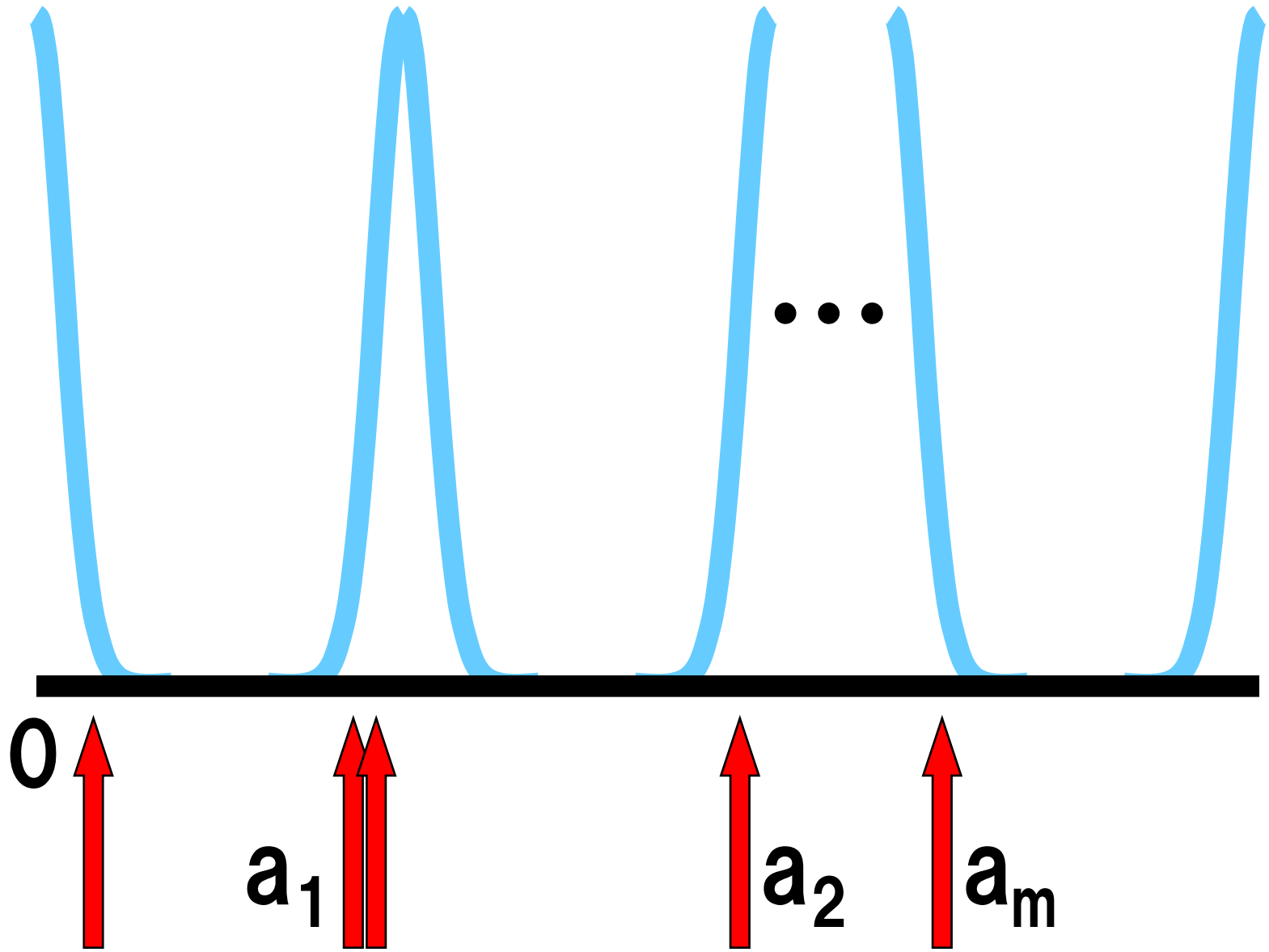
ここでは
Ajtai-Dwork
Regev03
を扱う

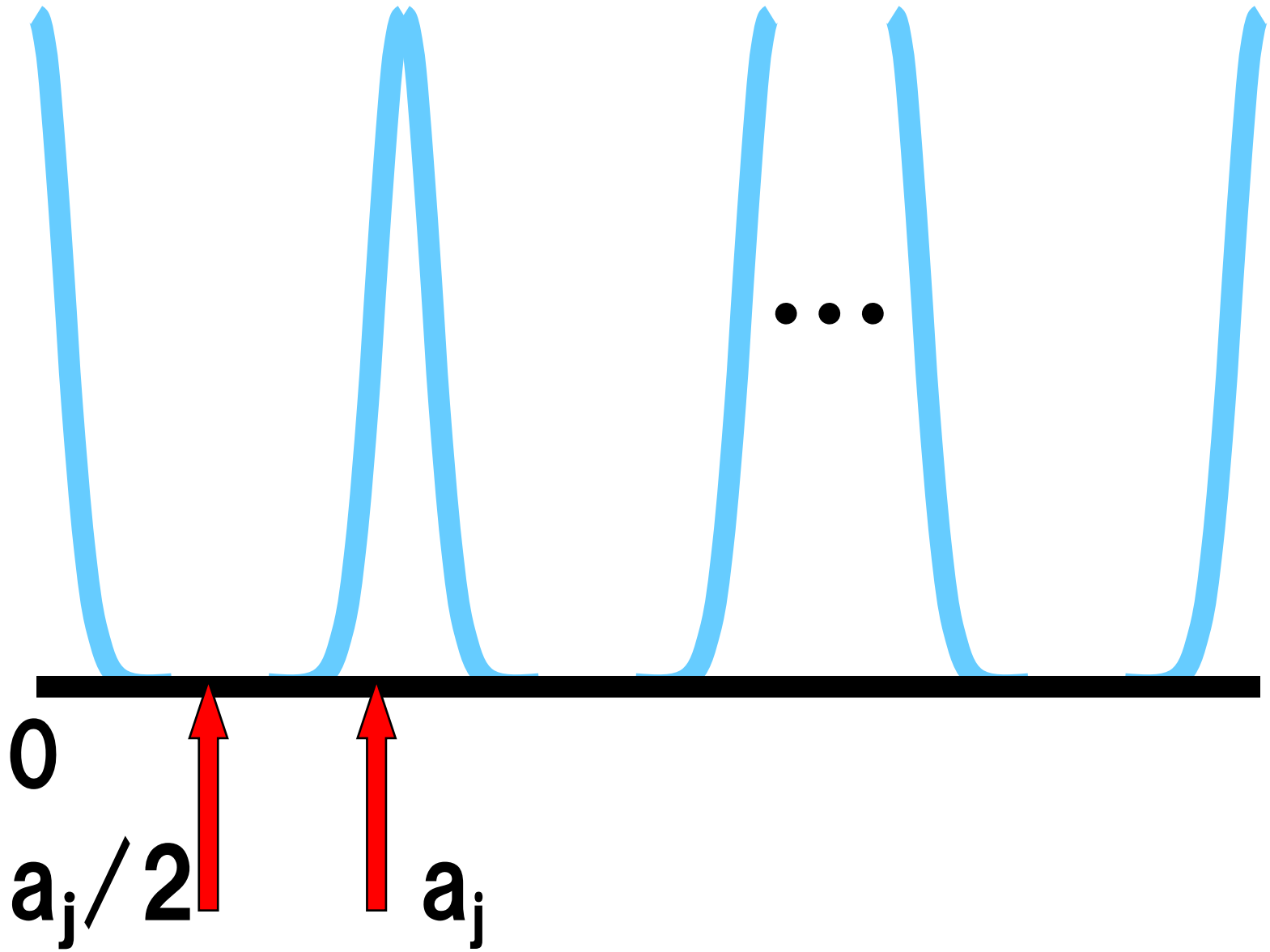
直観的な暗号の説明

周期的な分布を
生成し周期を
秘密鍵とする


0
周期d

分布に従って公開鍵$a_1,\ldots,a_m$を選ぶ


0
a_1
a_2
a_m


0
$a_j/2$
a_j

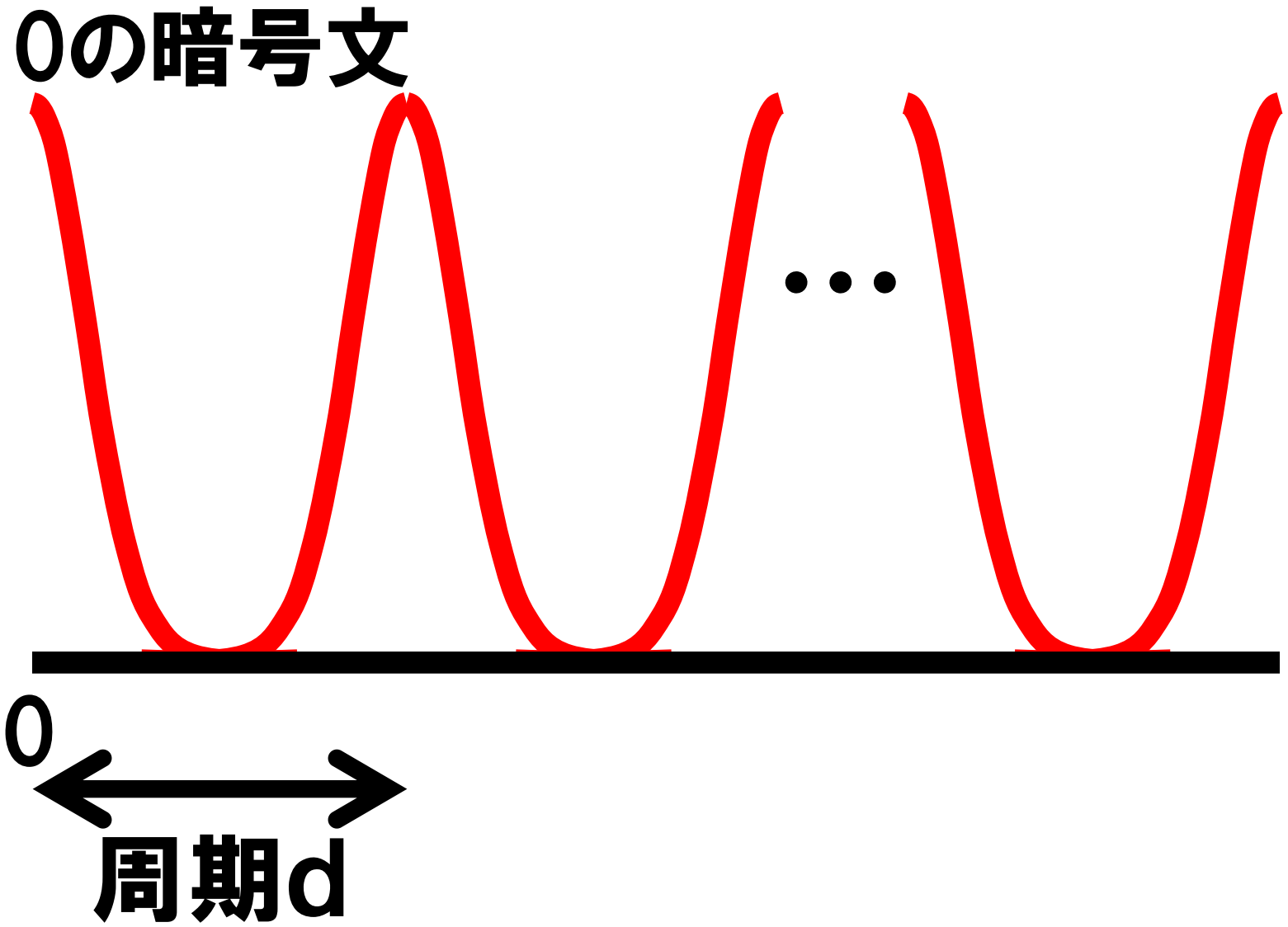
秘密鍵: d

公開鍵: $a_1,\ldots,a_m,j$

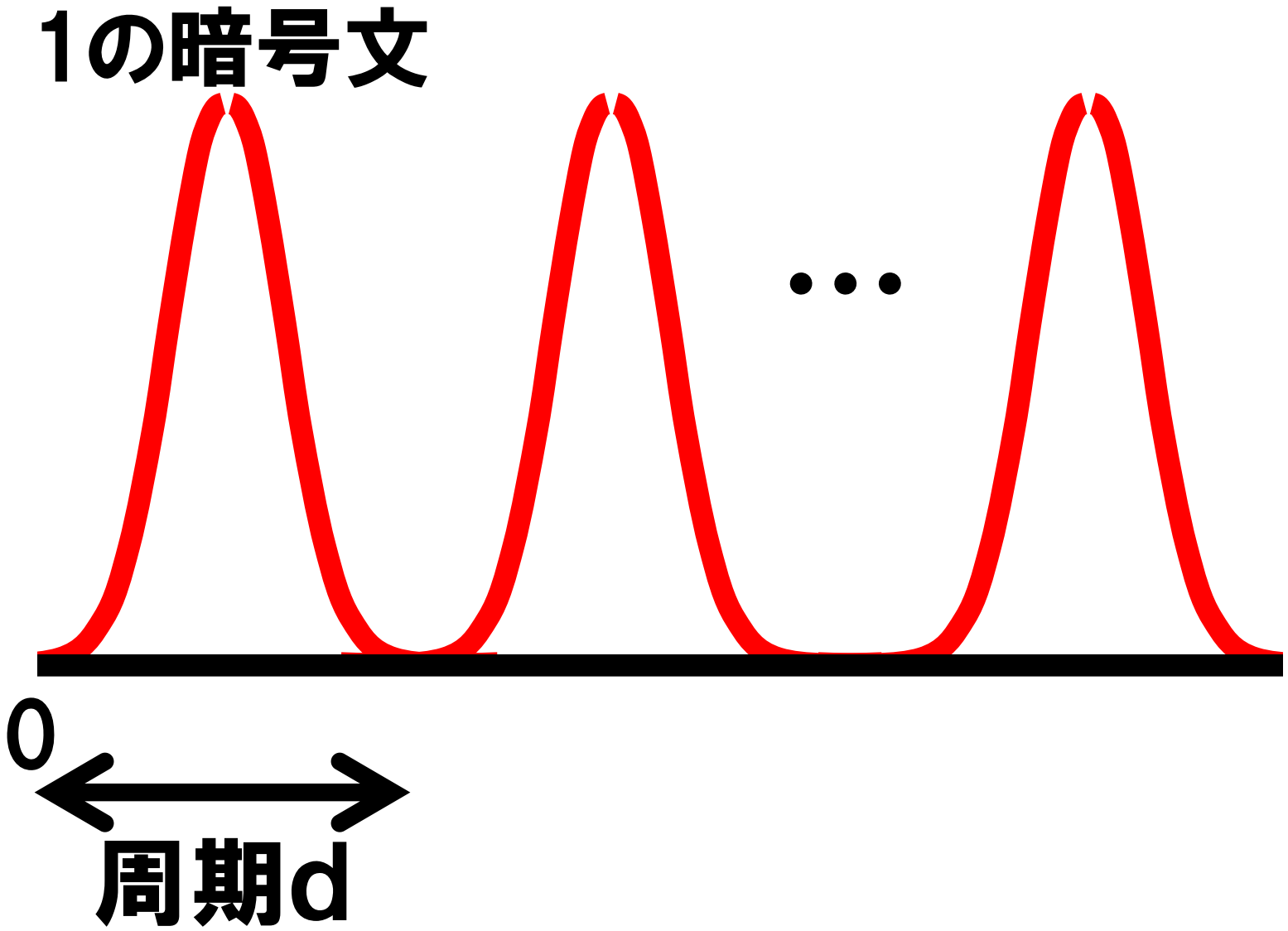
公開鍵を
足し合わせると
0の暗号文

$$S \subseteq_R \{1,2,\ldots m\}$$

$$E(0) = \sum_{i \in s} a_i$$


0の暗号文
…
0
周期d

$a_j/2$でずらすと
1の暗号文


1の暗号文
0
周期d

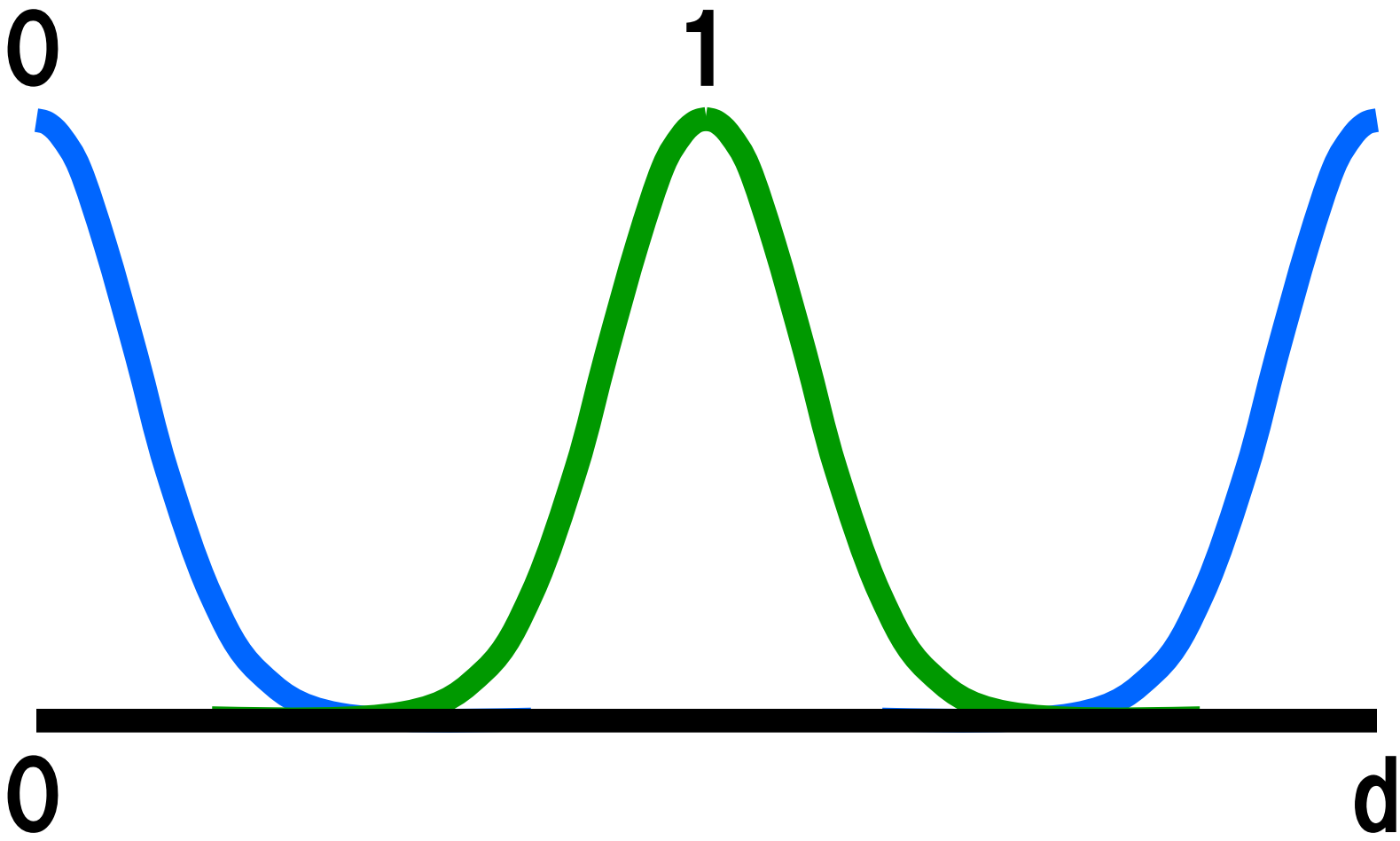
秘密鍵: d

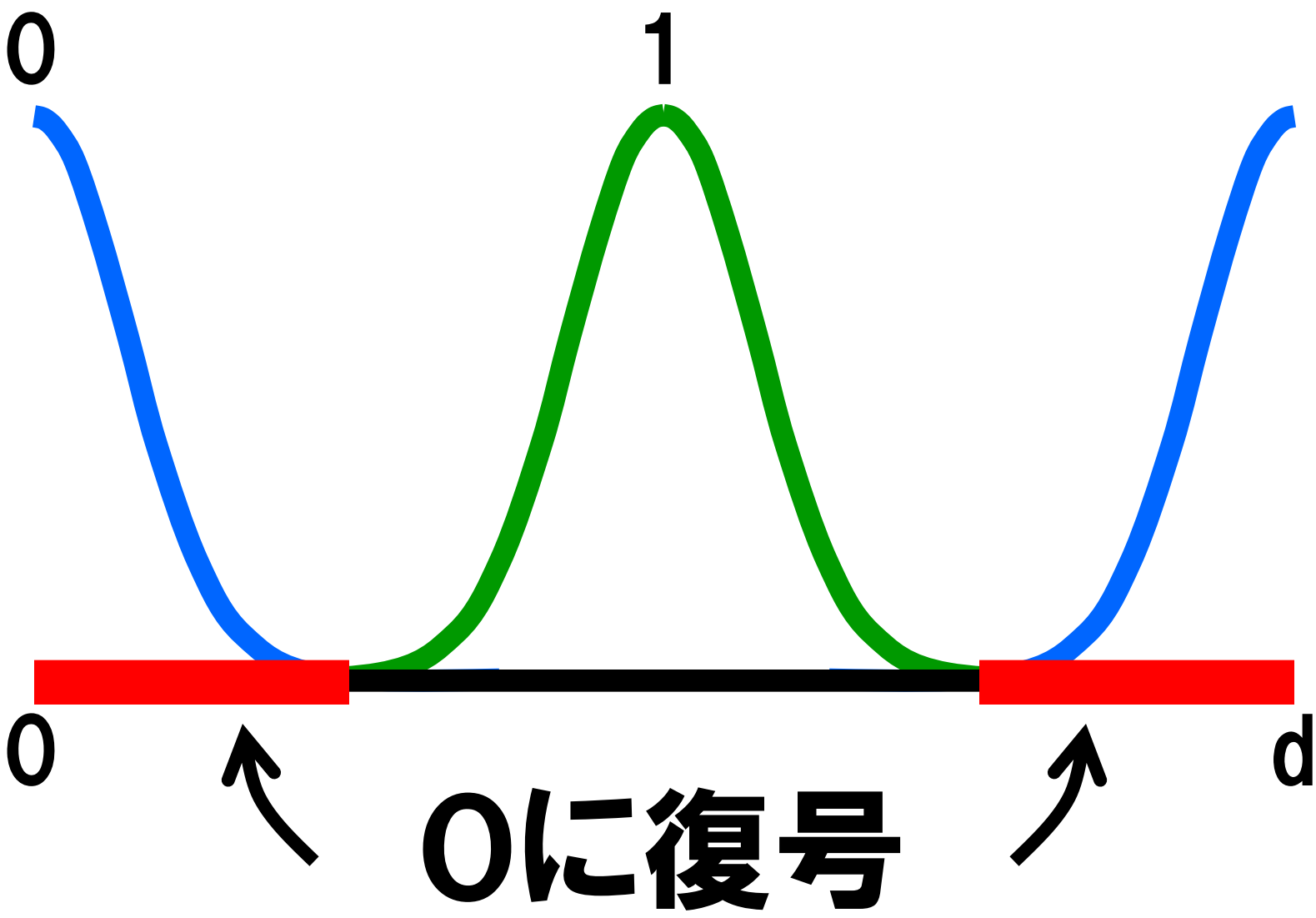
公開鍵: $a_1,\ldots,a_m,j$

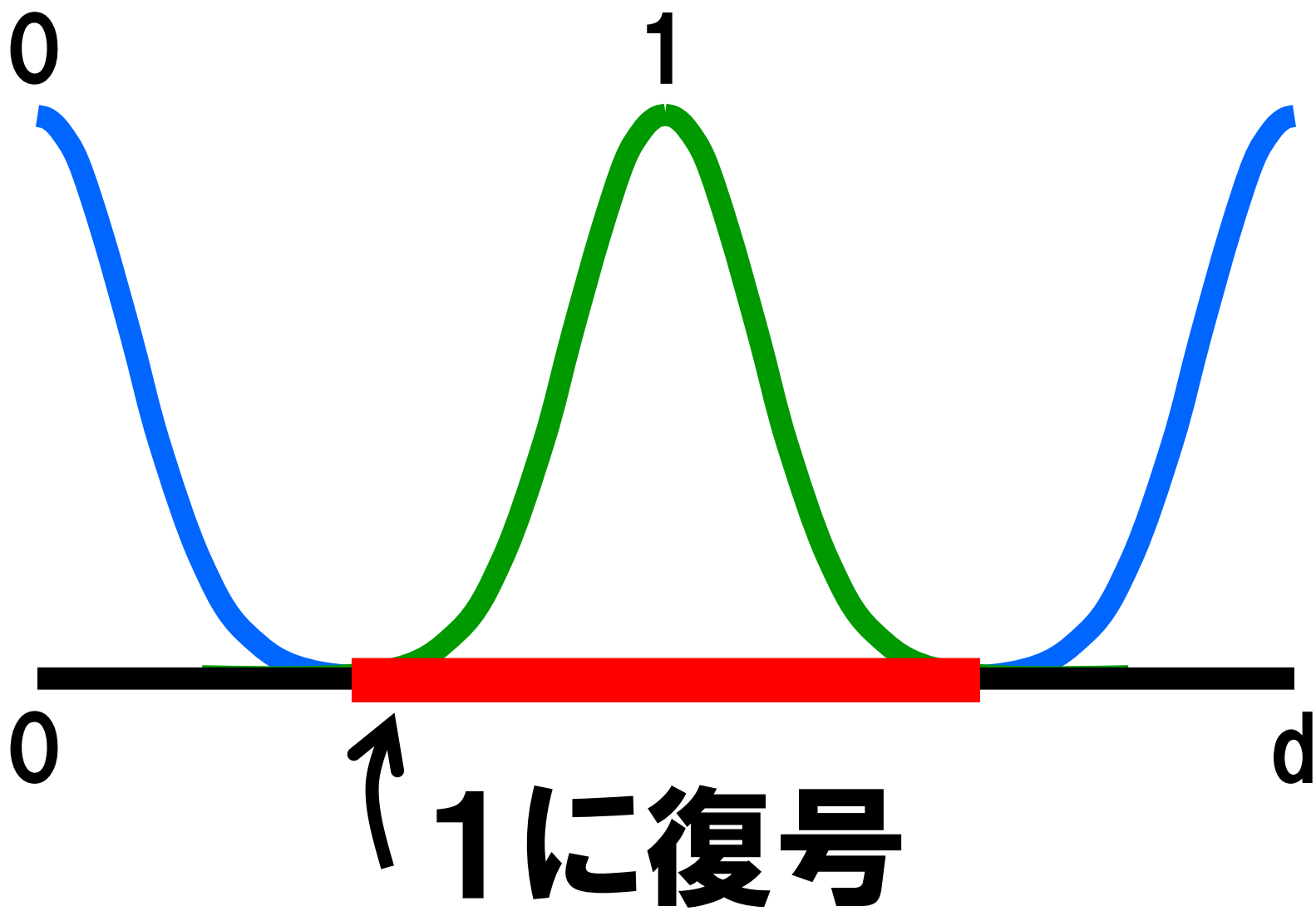
暗号化: $E(\sigma) =$

$\sigma\,(a_j/2) + \Sigma_{i\in S} a_i$

周期 d で
mod を取ると


0
1
0
d


0
1
0
d
0に復号


0
1
0
d
1に復号

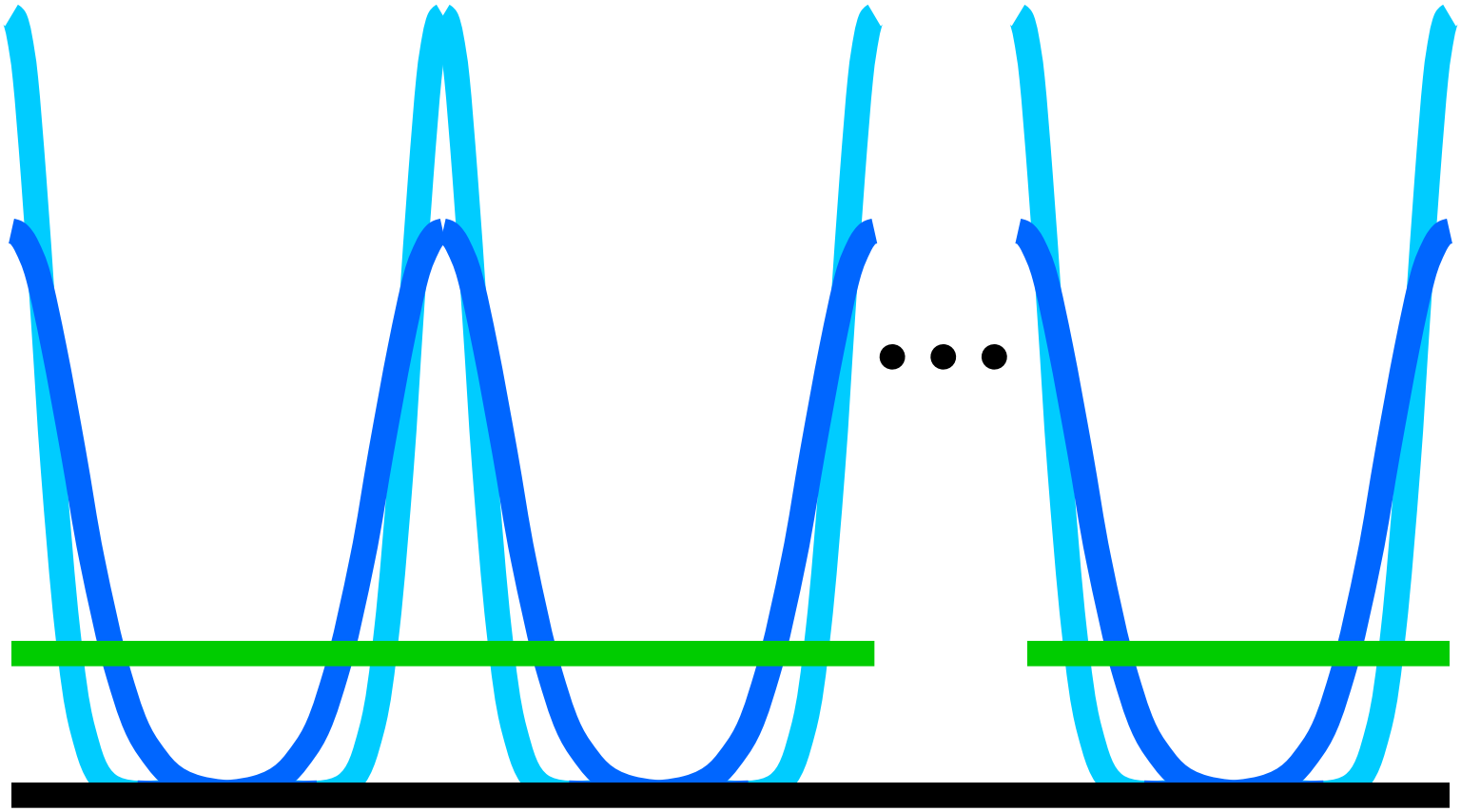
暗号の安全性

暗号文の分布を識別出来るなら任意の格子問題を解ける

Average-case Worst-case Connection

分布の分散と安全性が関係

分散が小さいと
安全性は低くなる



0

vs は vs より難しい

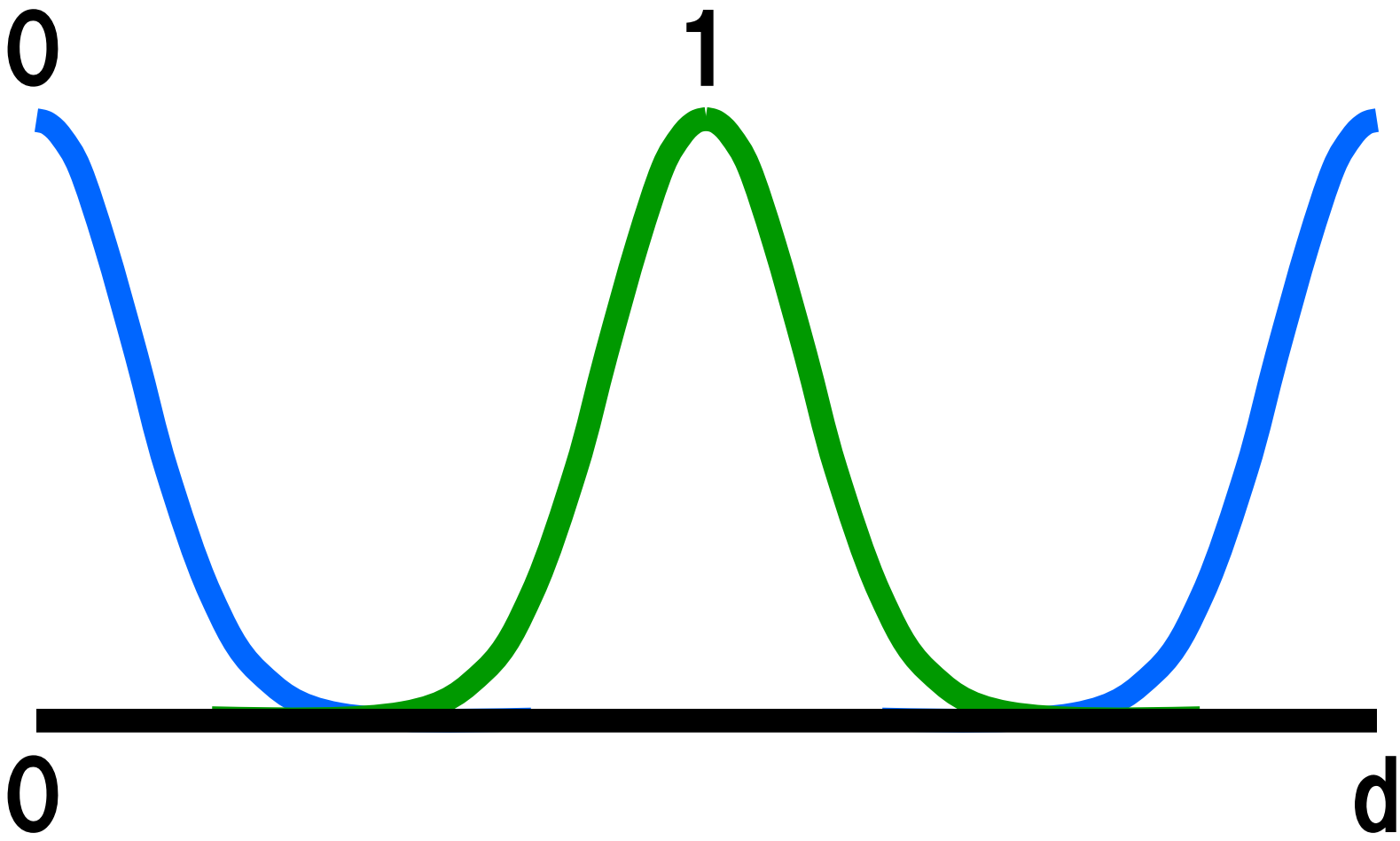
暗号の問題点

- 鍵サイズが大きい
- 平文⇔暗号文の効率が悪い

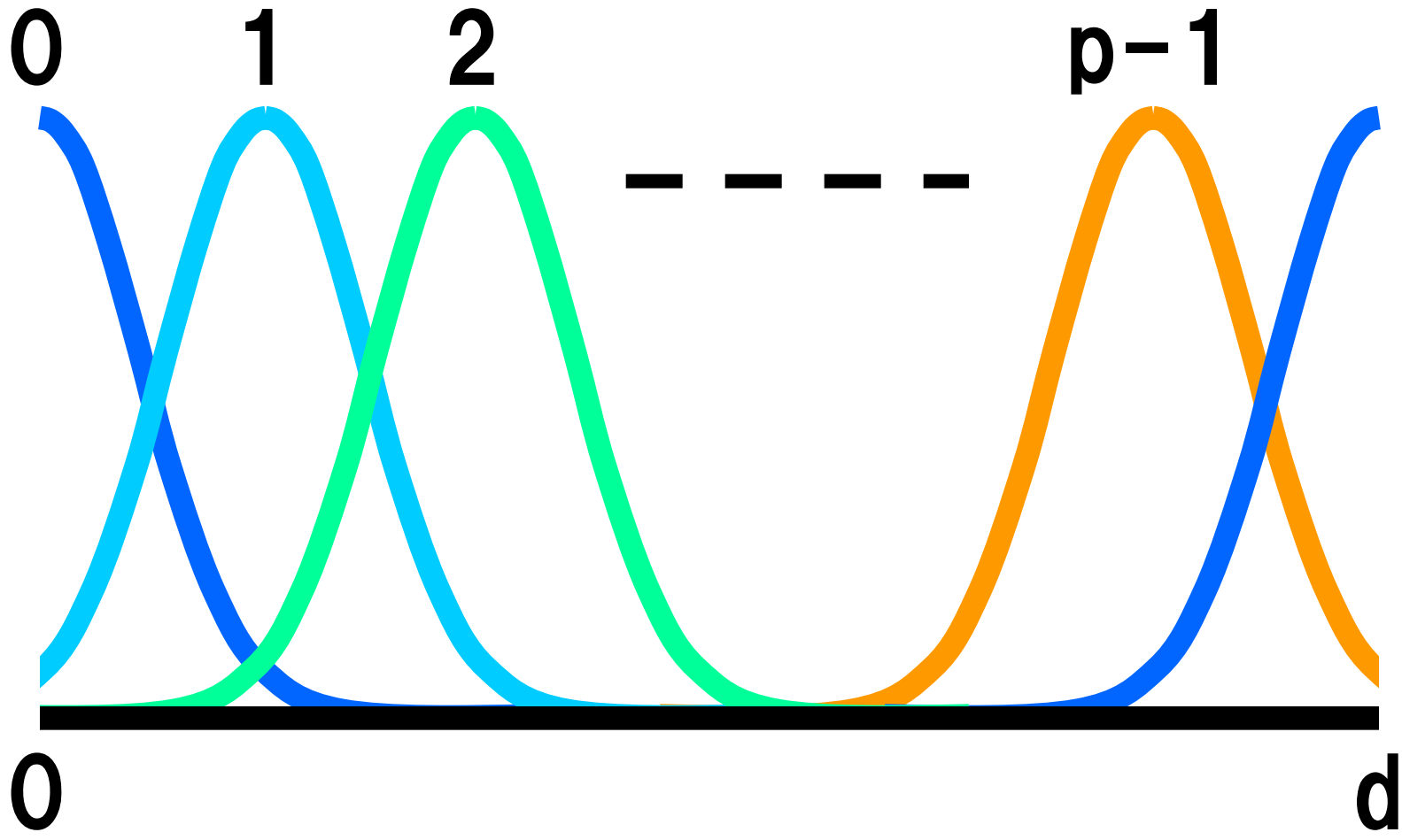
暗号文の
サイズを変えずに
平文空間を
大きくしたい

格子問題に基づく複数ビット公開鍵暗号

$p = O(n^{\varepsilon})$ 個の平文を埋め込む


0
1
0
d

スライドさせた
分布で埋める


0
1
2
p-1
0
d

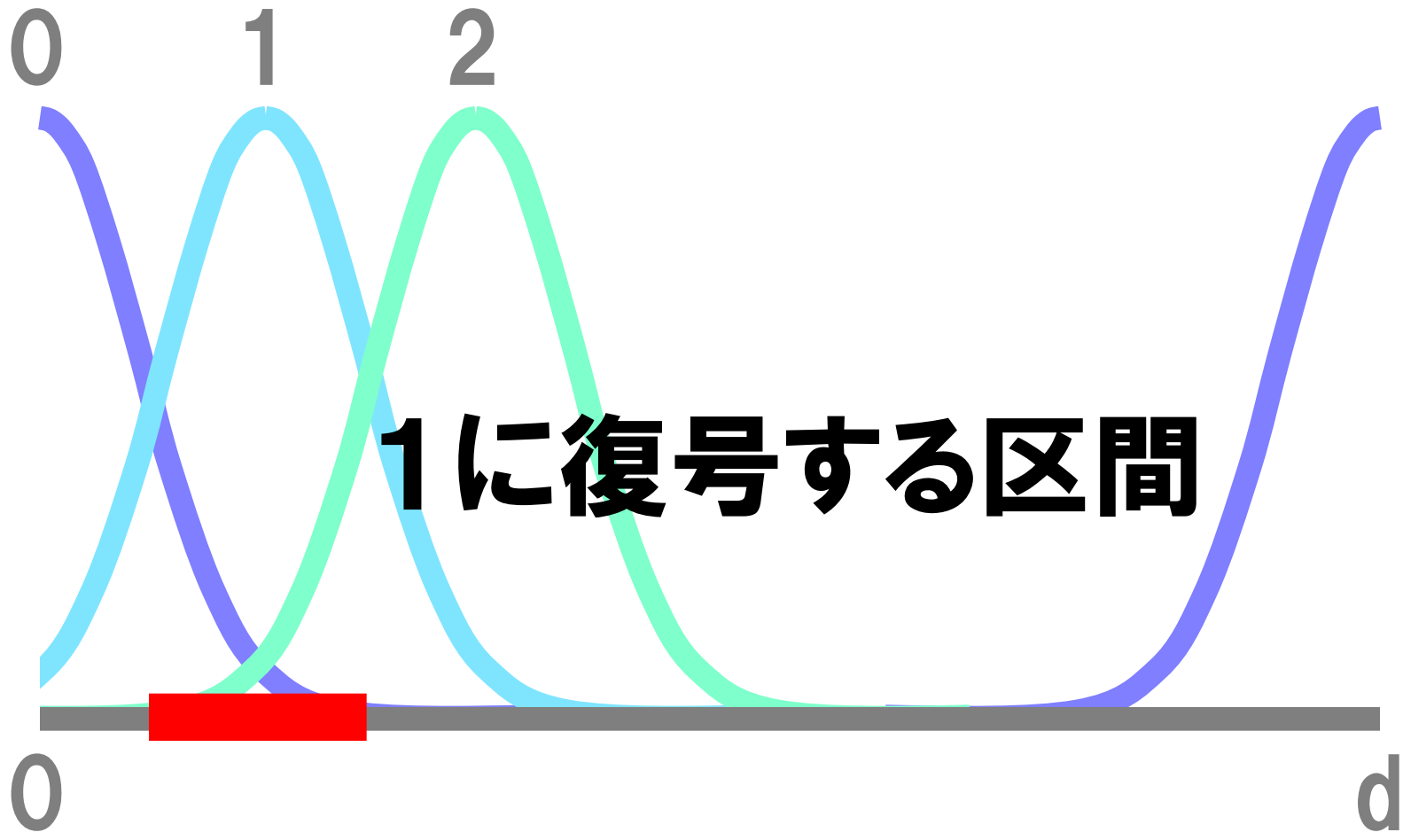
秘密鍵: d

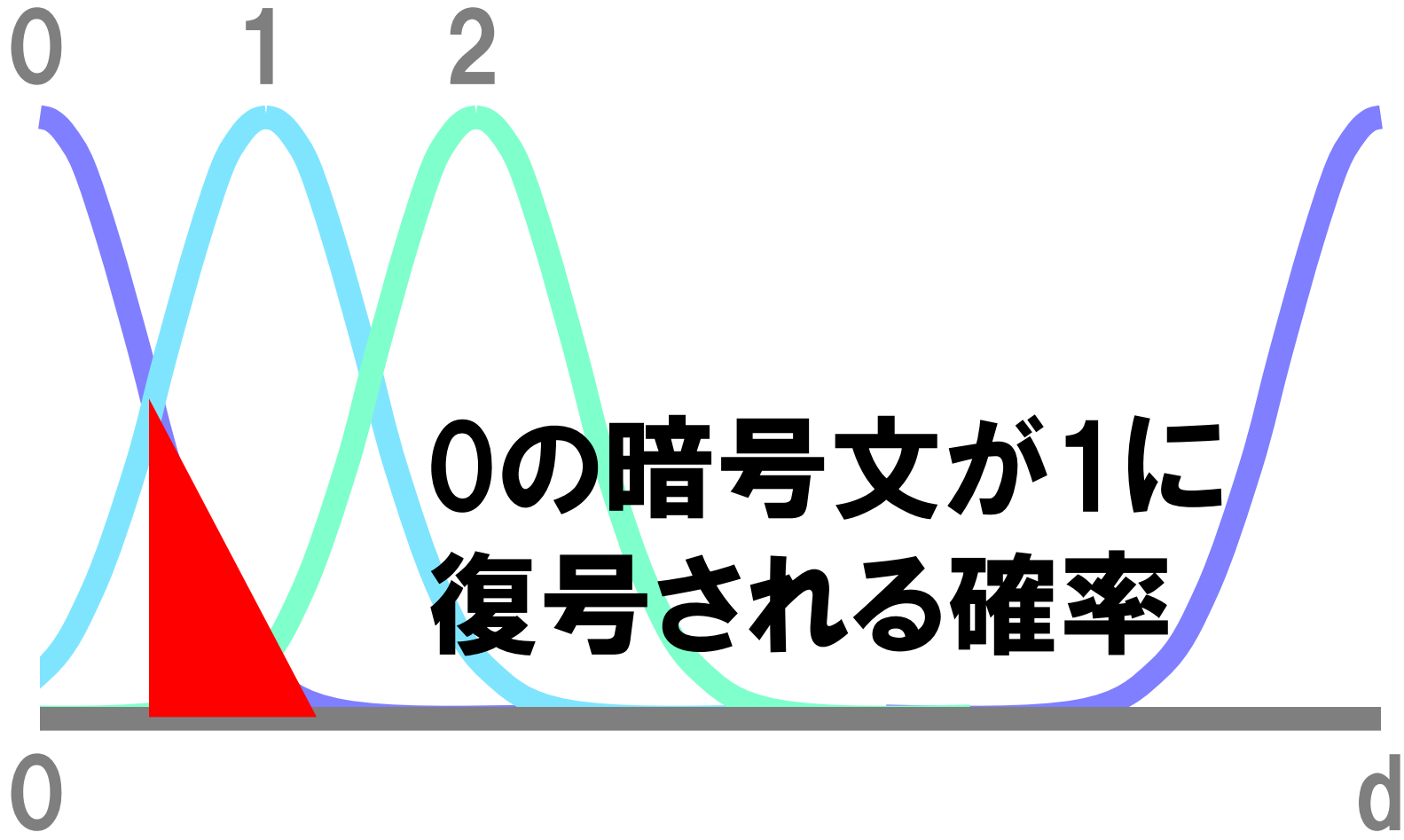
公開鍵: $a_1,\ldots,a_m,j$

暗号化: $E(\sigma) =$

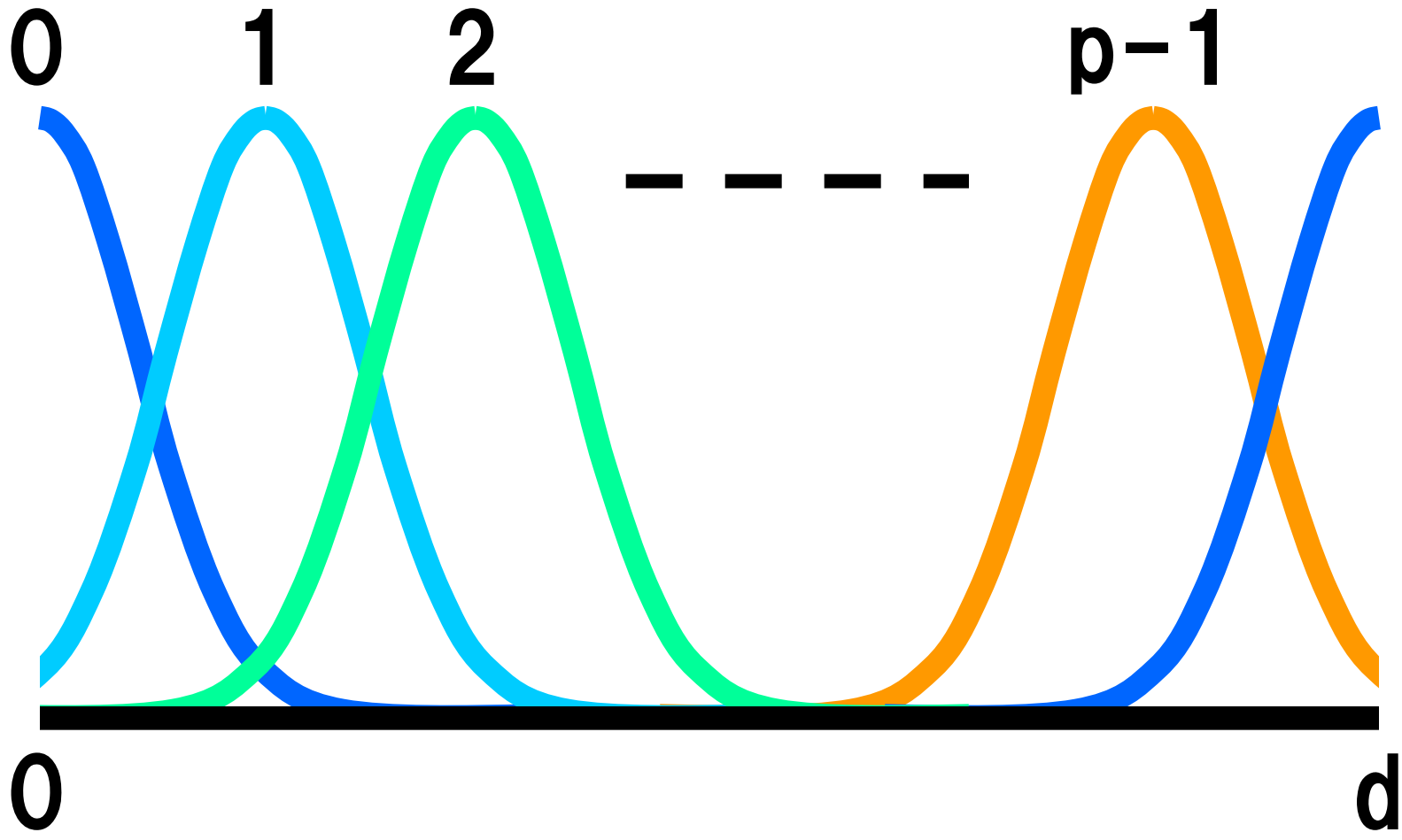
$\sigma\,(a_j/p) + \sum_{i\in S} a_i$

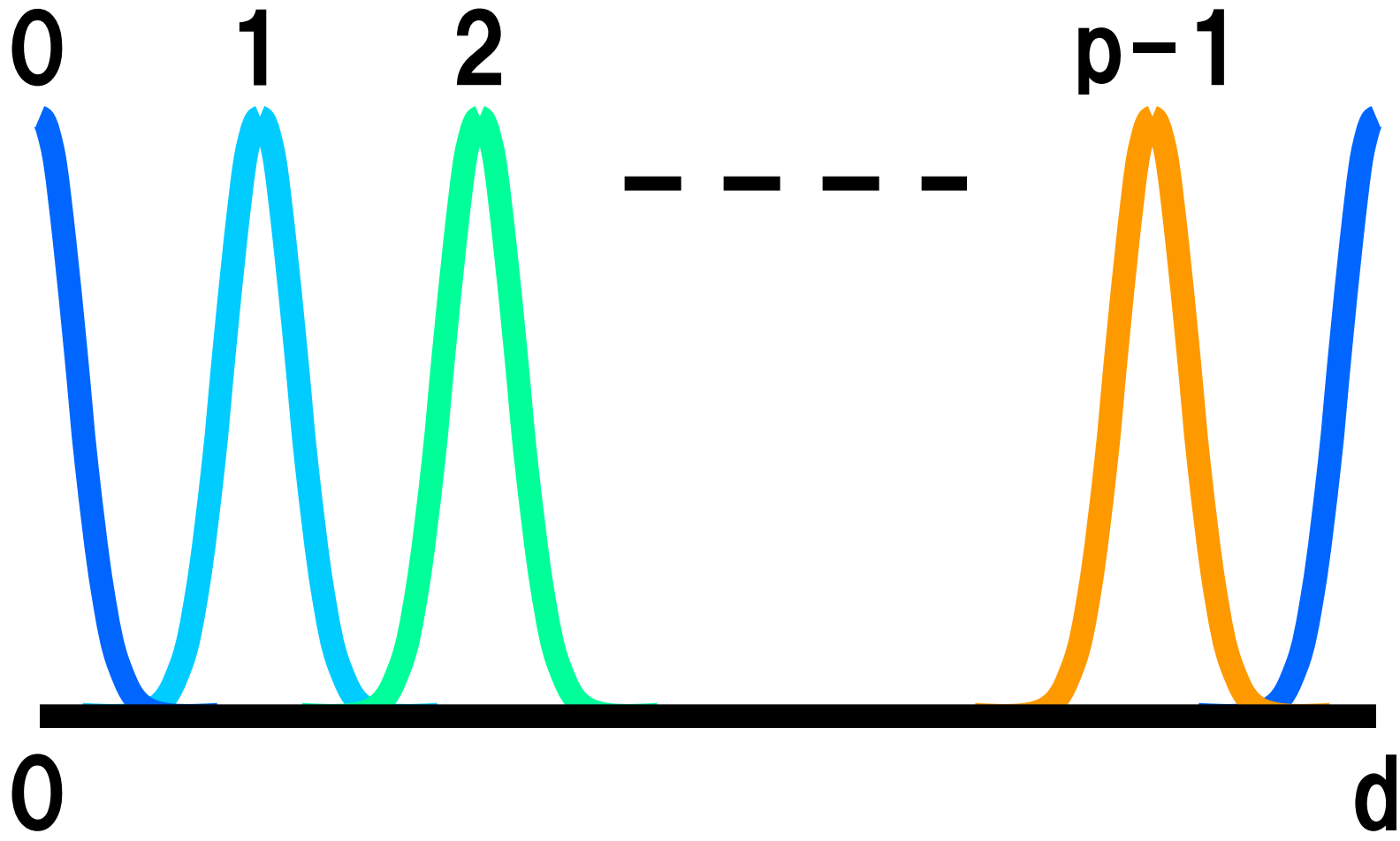
エラー確率が大きい


0
1
2
1に復号する区間
0
d


0
1
2
0の暗号文が1に
復号される確率
0
d

エラー確率を抑えるために分布の分散を小さくする


0
1
2
p-1
0
d


0
1
2
p-1
0
d

分散を小さくすると
安全性が低くなる

平文の個数と安全性のトレードオフ

	安全性	平文（ビット）	暗号文（ビット）
1ビット版	$n^{1.5}\log n$ uSVP	1	$8n^2$
複数ビット版	$n^{1.5+\varepsilon}\log n$ uSVP	$\varepsilon \log n$	$8n^2$

（例:Regev03）

	ビット数	安全性
mAjtai-Dwork	O(log n) ビット	証明有
mRegev03		
mRegev05		
mAjtai05		証明微妙
GGH	O(n) ビット	証明無
NTRU		

擬似準同型性

暗号の準同型性

$$E(m_1)+E(m_2)$$
$$=E(m_1+m_2)$$

擬似準同型性

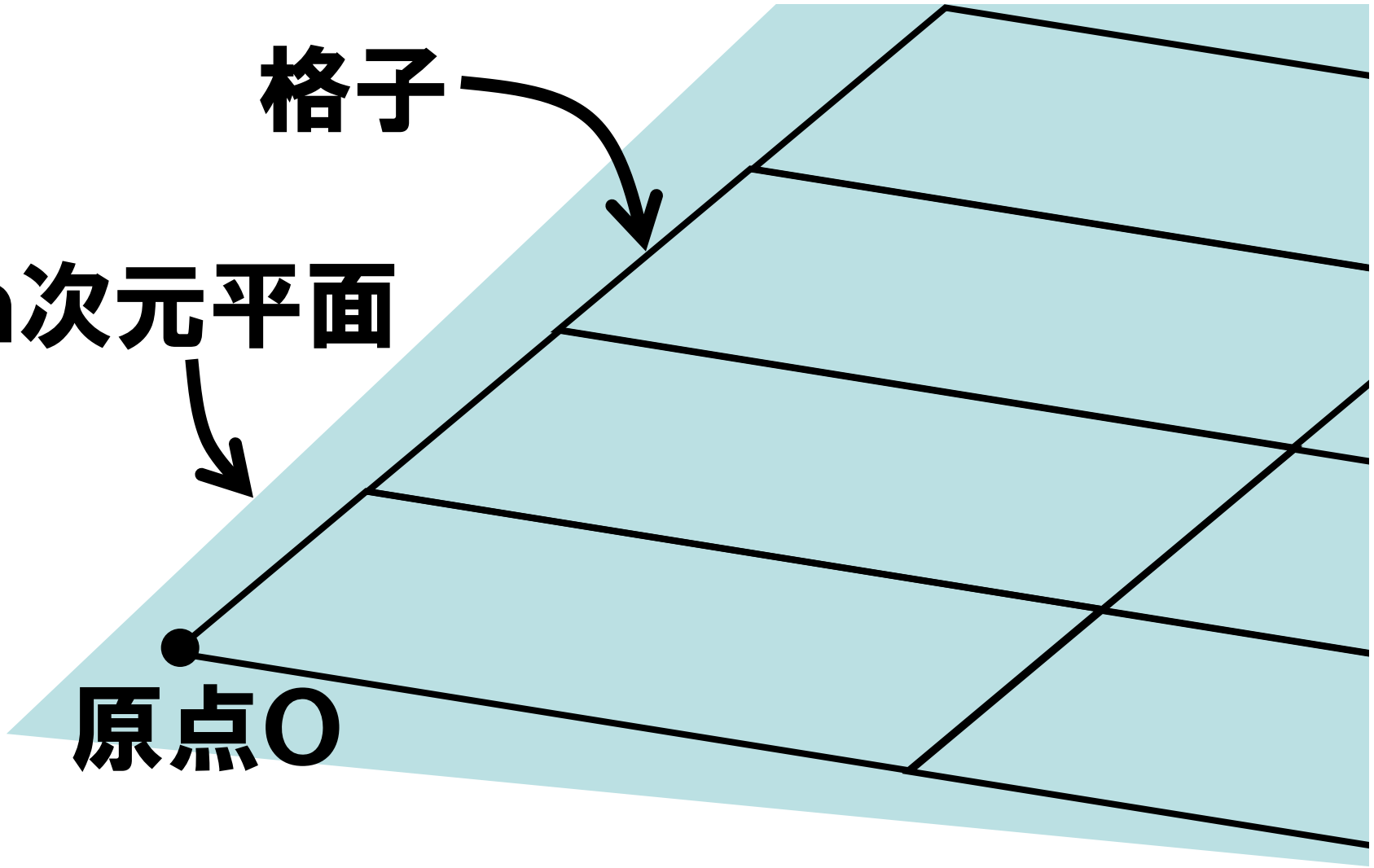
$$E_1(m_1) + E_1(m_2) = E_2(m_1 + m_2)$$

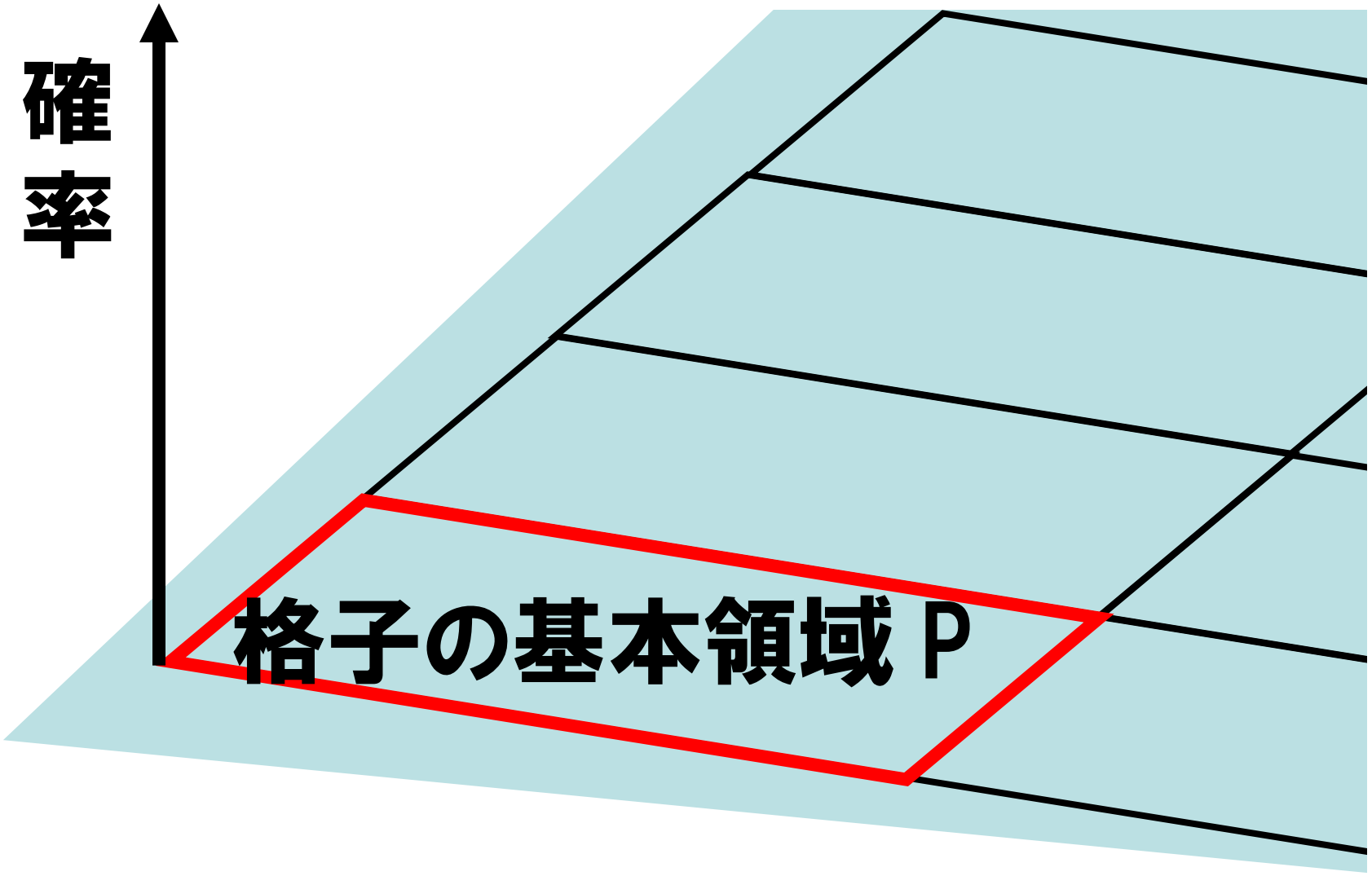
Ajtai05を
複数ビット化すると
実現可能

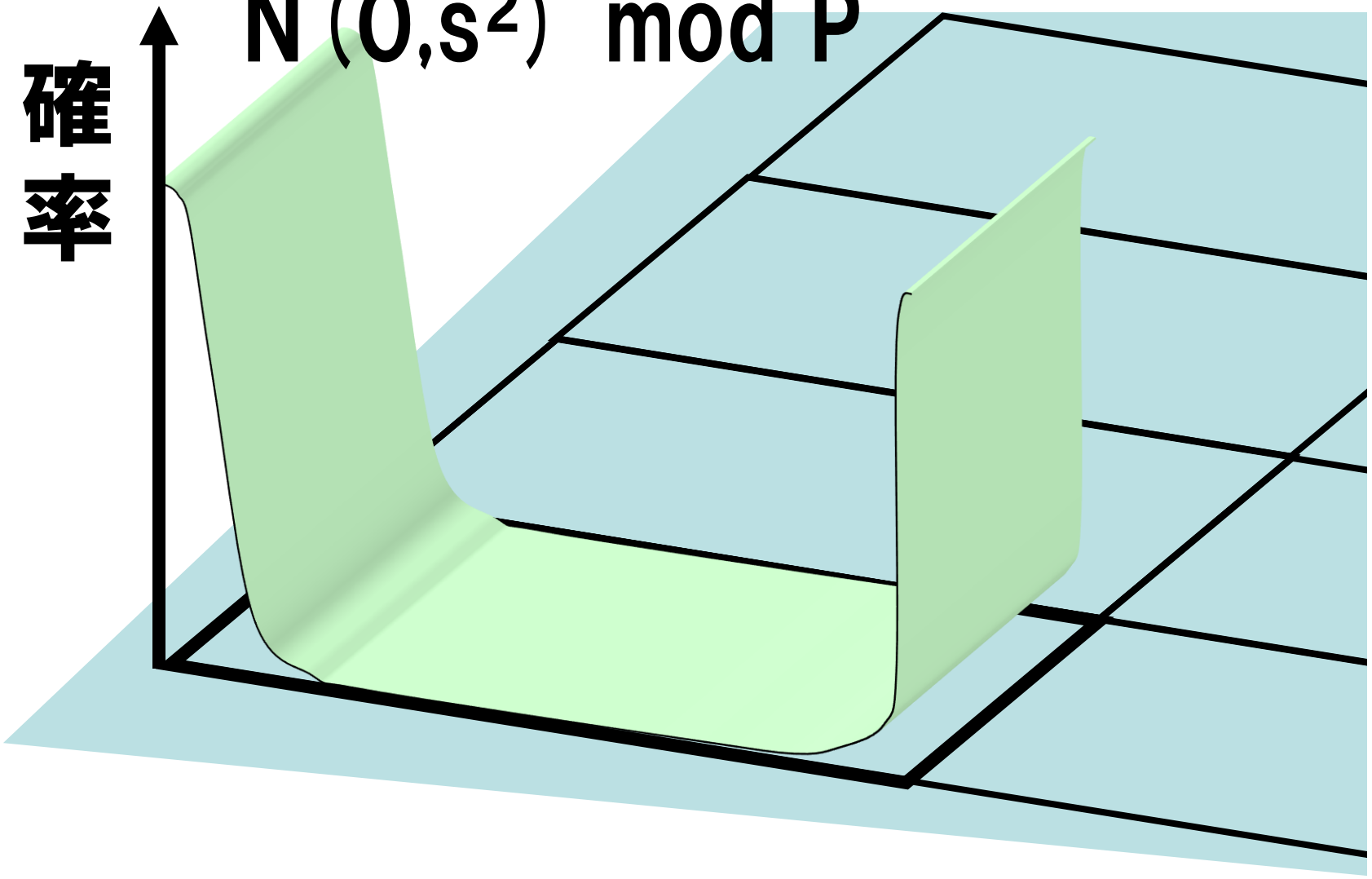
Ajtai05の説明

暗号化に
ガウス分布を
用いる

$N(m,s^2)$ を格子の基本領域で mod する


格子
n次元平面
原点O


確率
格子の基本領域 P


N (0,s²) mod P
確率

Ajtai05の
擬似準同型性

ガウス分布の再生性

$$N(m_1, s_1^2) + N(m_2, s_2^2) = N(m_1 + m_2, s_1^2 + s_2^2)$$

基本領域で
modを取っても
再生性がある

$$E_{s_1^2}(m_1) + E_{s_2^2}(m_2) = E_{s_1^2+s_2^2}(m_1+m_2)$$

が成立

同じ公開鍵・秘密鍵で暗号化・復号可能

組合せ系では見られなかった性質

まとめ

■複数ビット化

- ●1ビット暗号を暗号文のサイズを変えずに複数ビット化
- ●平文の個数と安全性のトレードオフ

■擬似準同型性

- ●Ajtai05を複数ビット化することで実現可能
- ●組合せ系では今までにない性質

■今後の課題

- ●nビット暗号かつ安全性証明がある暗号を作る
  - ロGGHやNTRUはnビット暗号だが安全性証明が無い
- ●擬似準同型性の応用

参考文献

- Ajtai, Dwork（STOC ‘97）
- Goldreich, Goldwasser, Halevi（CRYPTO ‘97）
- Regev（STOC 2003）
- Regev（STOC 2005）
- Ajtai（STOC 2005）
- 高橋征義（高橋メソッド）