MULTI-BIT CRYPTOSYSTEMS BASED ON LATTICE PROBLEMS

PKC 2007

Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa
(Tokyo Institute of Technology)

Agenda

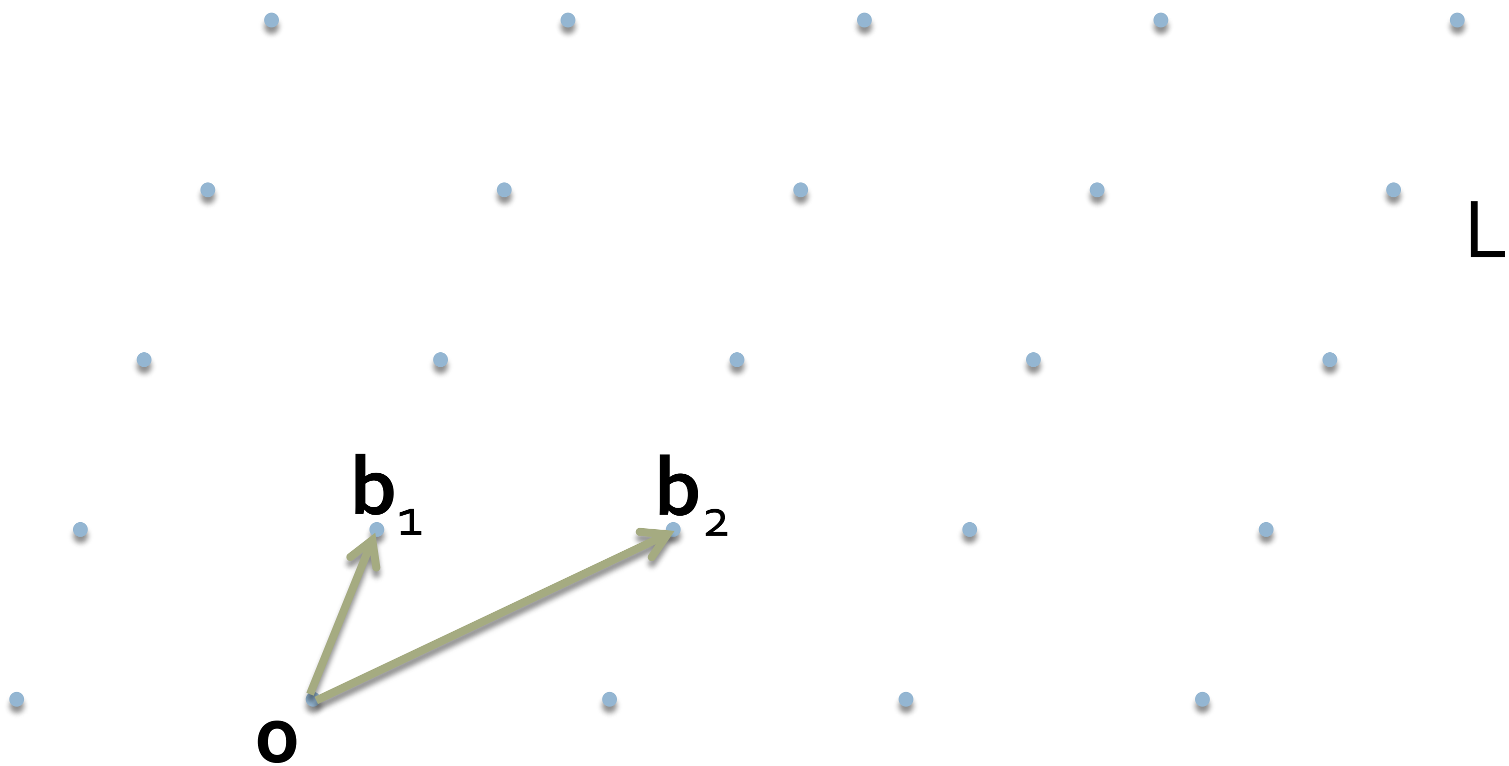
- Background
- Our Results
- Conclusion

Agenda

- Background
  - Lattices
  - Lattice problems
  - Lattice-based cryptosystems
  - Motivation
- Our Results
- Conclusion

Lattices

- Given: $\mathbf{B}=[\mathbf{b}_1,\ldots,\mathbf{b}_n]$
- $L(\mathbf{B}) := \{\Sigma_i \alpha_i \mathbf{b}_i \mid \alpha_i \in Z \text{ for all } i\}$

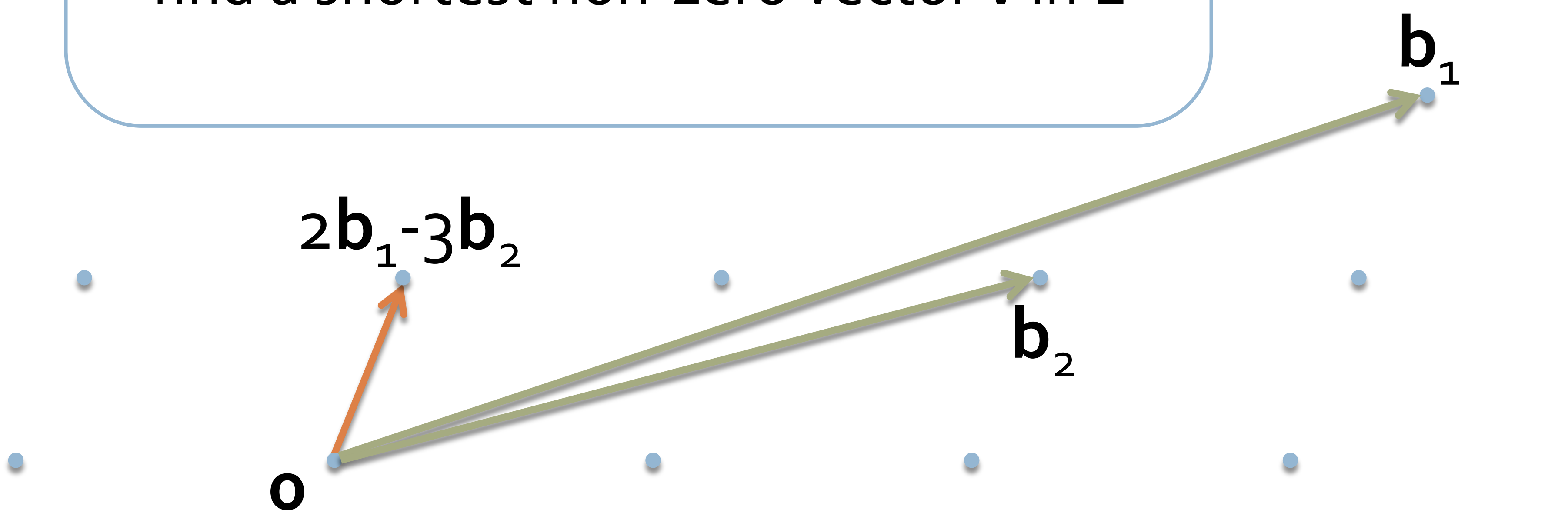


SVP (Shortest Vector Problem)

SVP:

Given a basis **B** of a lattice L,

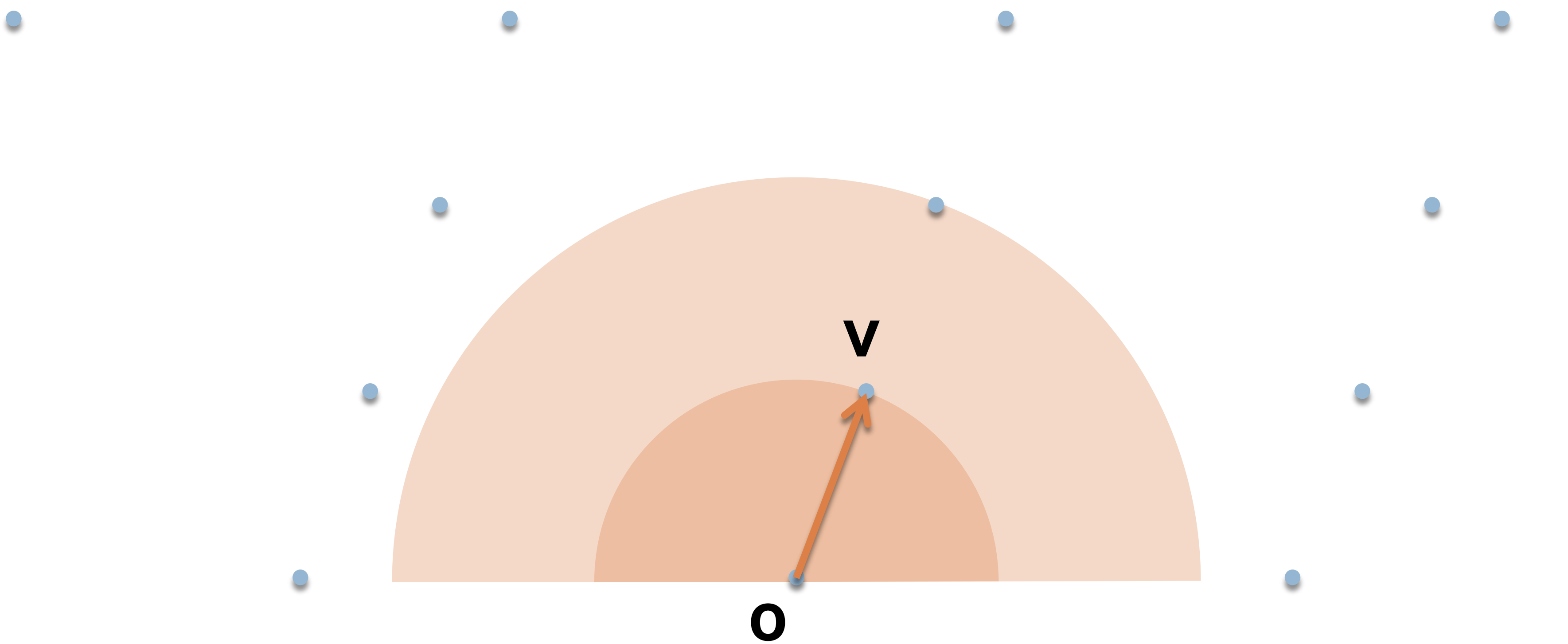
find a shortest non-zero vector **v** in L



uSVP (unique Shortest Vector Problem)

v: 2-unique

$\forall \mathbf{x} \in L,\ \text{if } \mathbf{x} \nparallel \mathbf{v} \text{ then } 2\|\mathbf{v}\| \le \|\mathbf{x}\|$



Hardness of uSVP

- If f < g, f-uSVP is not easier than g-uSVP
  - **v**:g-unique→**v**:f-unique
- f=1→NP-hard [Kumar and Sivakumar '01]
- $f=n^{1/4}$→coAM (seems not NP-hard) [Cai '98]
- f=poly(n)→?

- Assumption:
  - If f=poly(n), f-uSVP is intractable in the worst-case

Lattice-Based Cryptosystems

- Based on lattice problems
  - SVP, uSVP, CVP, and etc
- Advantages
  - Fast encryption and decryption
  - (Seemes) hard to attack with quantum power
- Two types
  - Type A: efficient, but no security proofs
  - Type B: security proofs, but inefficient

Related Works

Type A

GGH
[Goldreich, Goldwasser, and Halevi '98]

NTRU
[Hoffstein, Pipher, and Silverman '98]

Type B

AD
[Ajtai and Dwork '97]

AD_{GGH} (Errorless version of AD cryptosystem)
[Goldreich, Goldwasser, and Halevi '98]

Regev04
[Regev '04]

Regev05
[Regev '05]

Ajtai 05
[Ajtai '05]

Type B

- AD_{GGH}, Regev04, Regev05, and Ajtai05
- Advantage
  - Provable security
    - with average-case/worst-case connection (except Ajtai05)
- Disadvantages
  - |pk| is huge
  - |plaintext|=1

Motivation

- Towards practical lattice-based cryptosystems in Type B
  1. |pk|→small
  2. |plaintext|→large
     - w/o changing |cipher|

Agenda

- Background
- Our Results
  - Summary
  - Review of Regev04
  - Our technique
  - Analysis of trade-off
  - Pseudohomomorphism
- Conclusion

Our Results

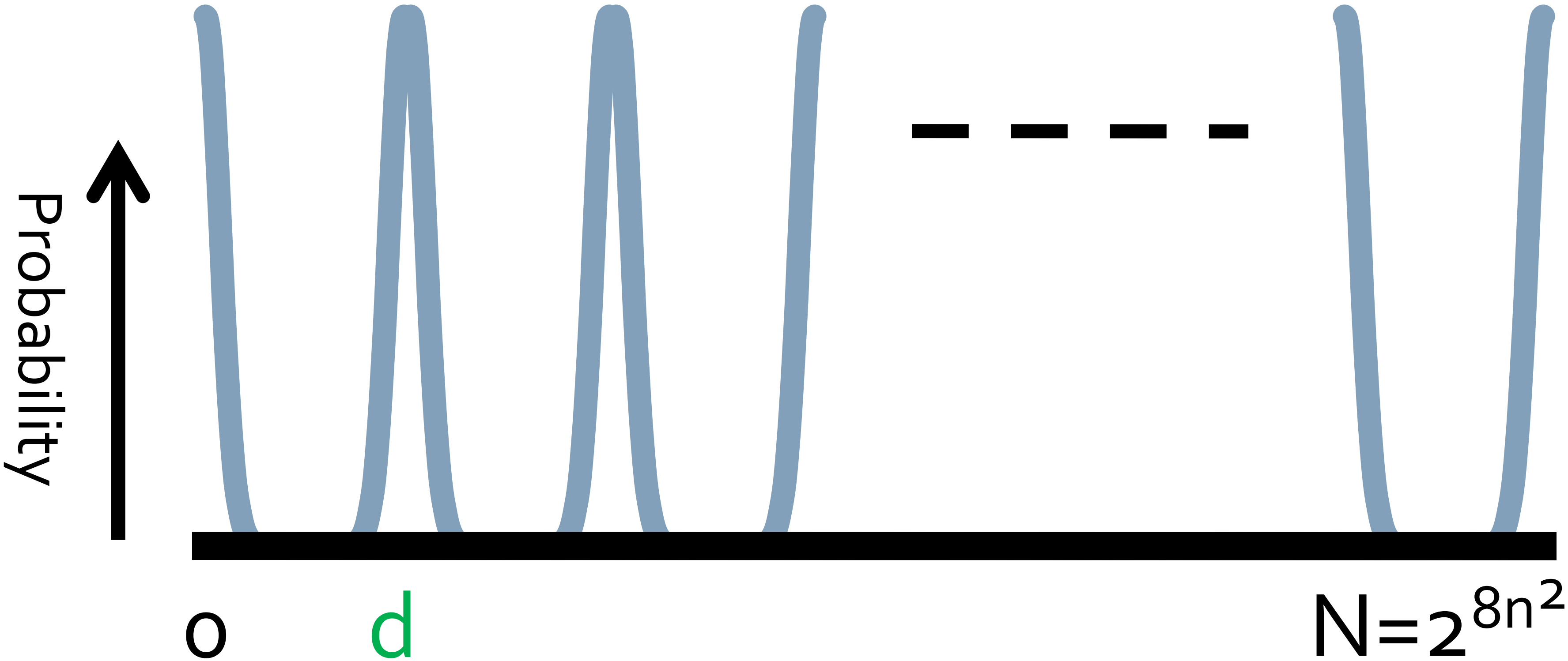
- Results
  - Proposal of multi-bit versions of Type B
    - AD_{GGH}, Regev04, Regev05, and Ajtai05
  - Analysis of the trade-off
    - between the size of plaintext and security levels
  - Pseudohomomorphism
    - AD_{GGH}, Regev04, Regev05, and Ajtai05

Eg: Regev04

- Security parameter: n
  - n is the dimension of lattices
- Key Generation
- Encryption
- Decryption
  - Decryption Errors
- Security Reduction

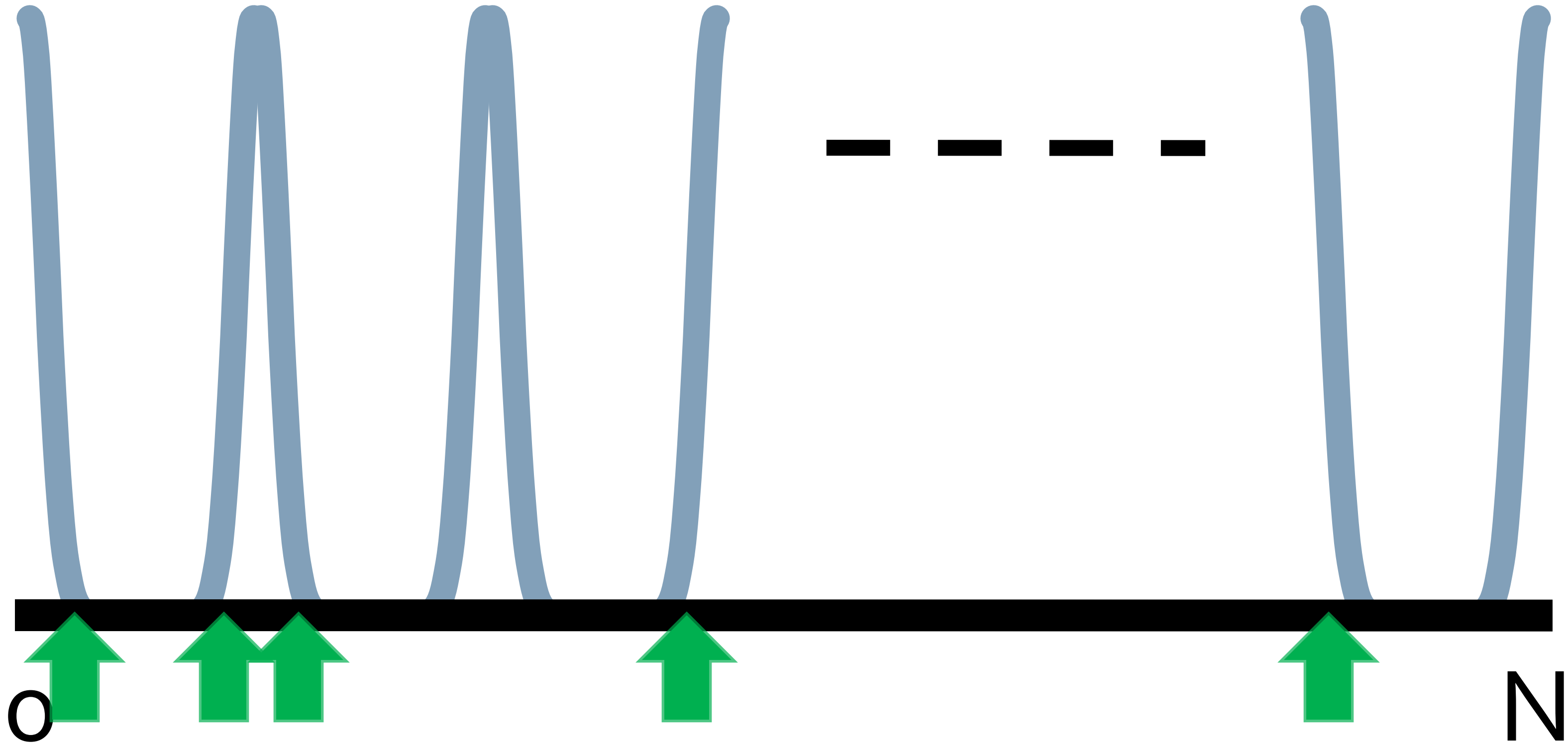
Regev04 - Key Generation 1

- Choose private priod d
- Consider periodic Gaussian distrib. with variance α^2



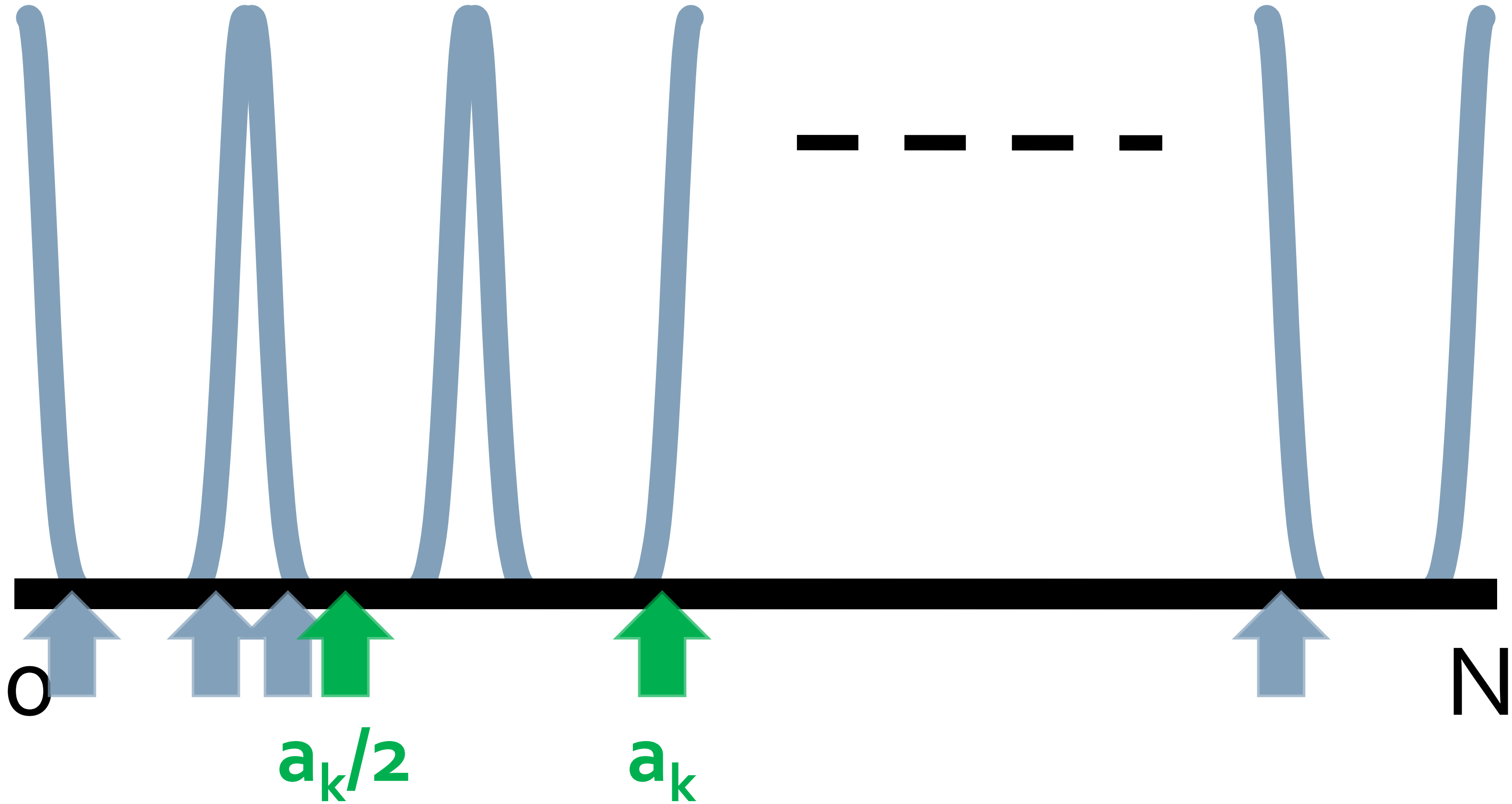
Regev04 - Key Generation 2

- Choose $a_1,\ldots,a_m$ according to the distribution



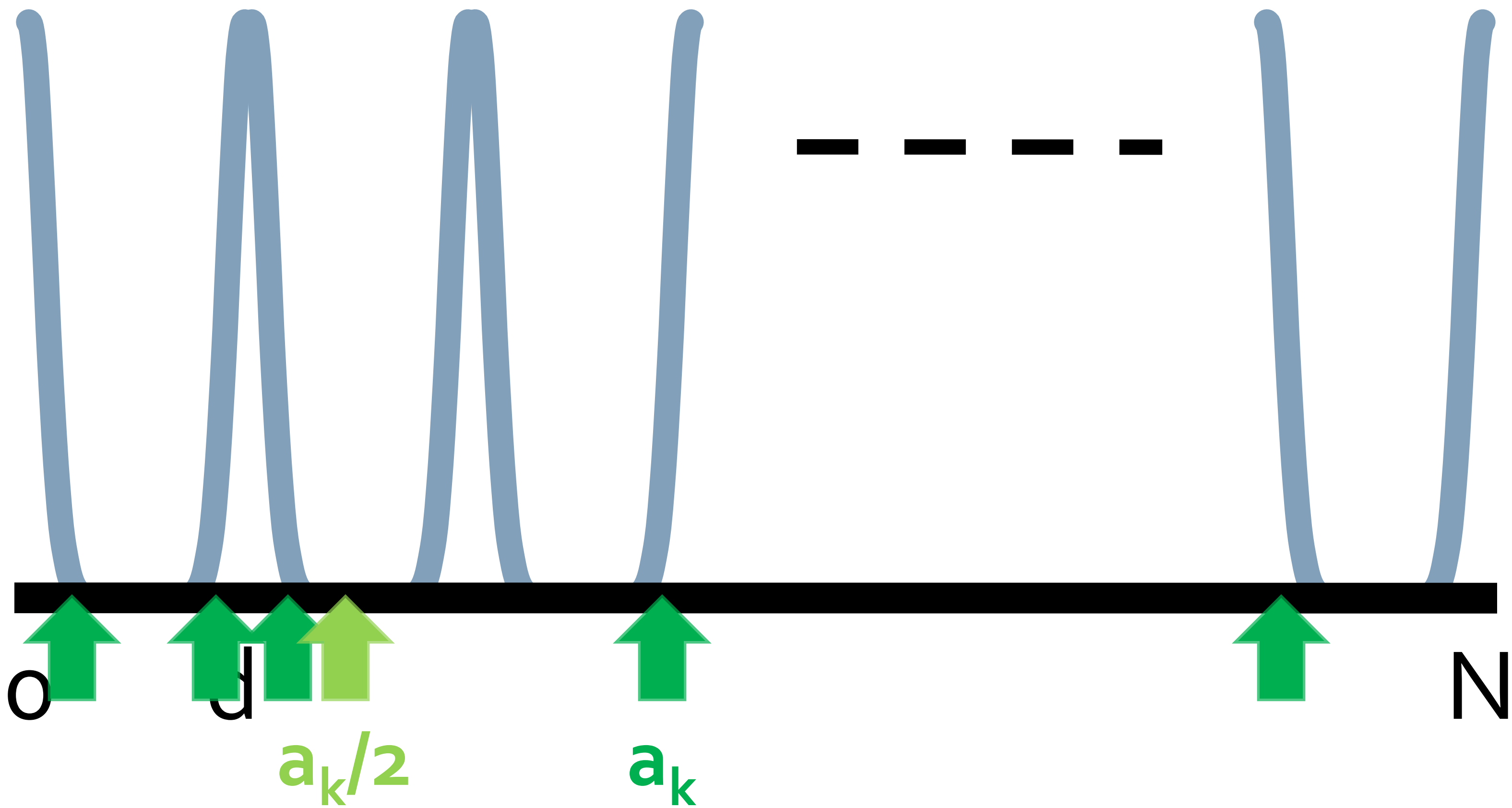
Regev04 - Key Generation 3

- Decide the index k
- $a_k/2$ must be in "bottom"



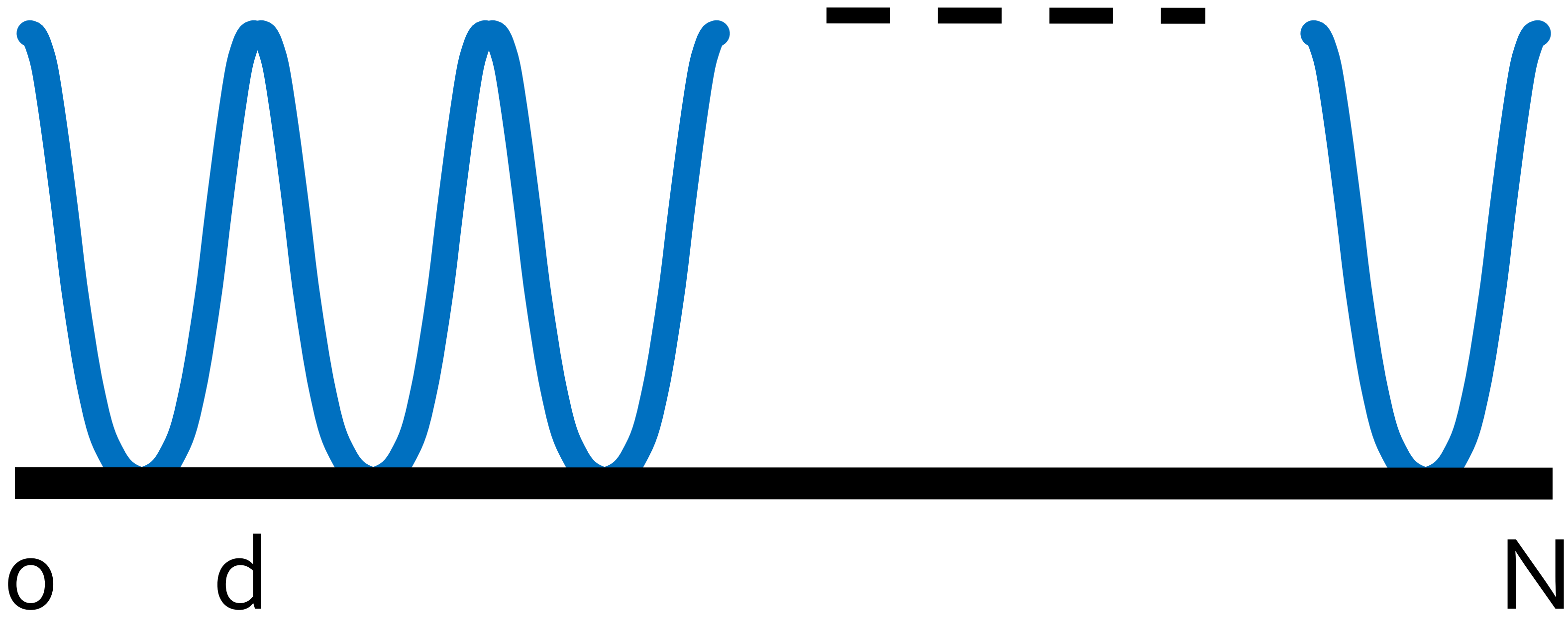
Regev04 - Key Generation 4

- Secret Key: d
- Public Key: $a_1, \ldots, a_m, k$



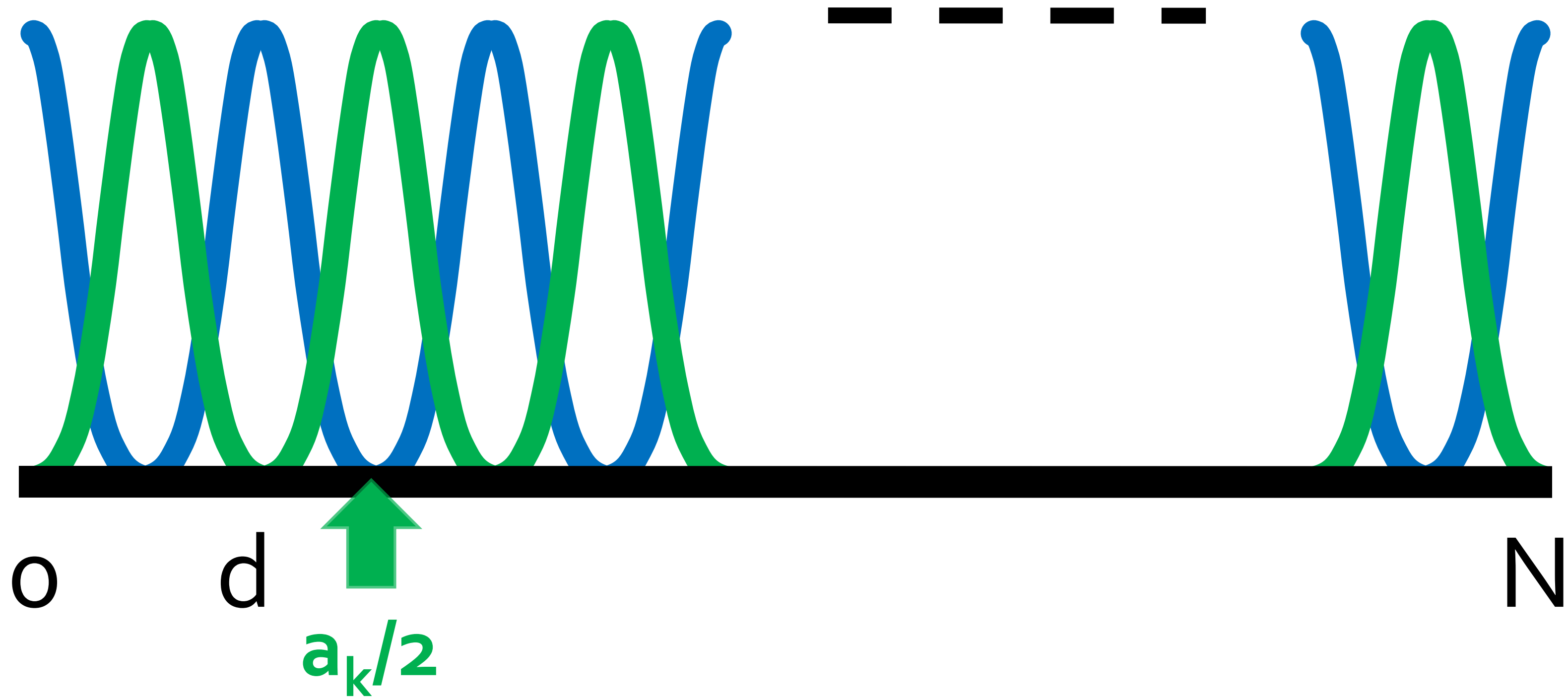
Regev04 - Encryption of "0"

- $r \in_R \{0,1\}^m$
- $E(0) = \Sigma_i \, r_i a_i \bmod N$



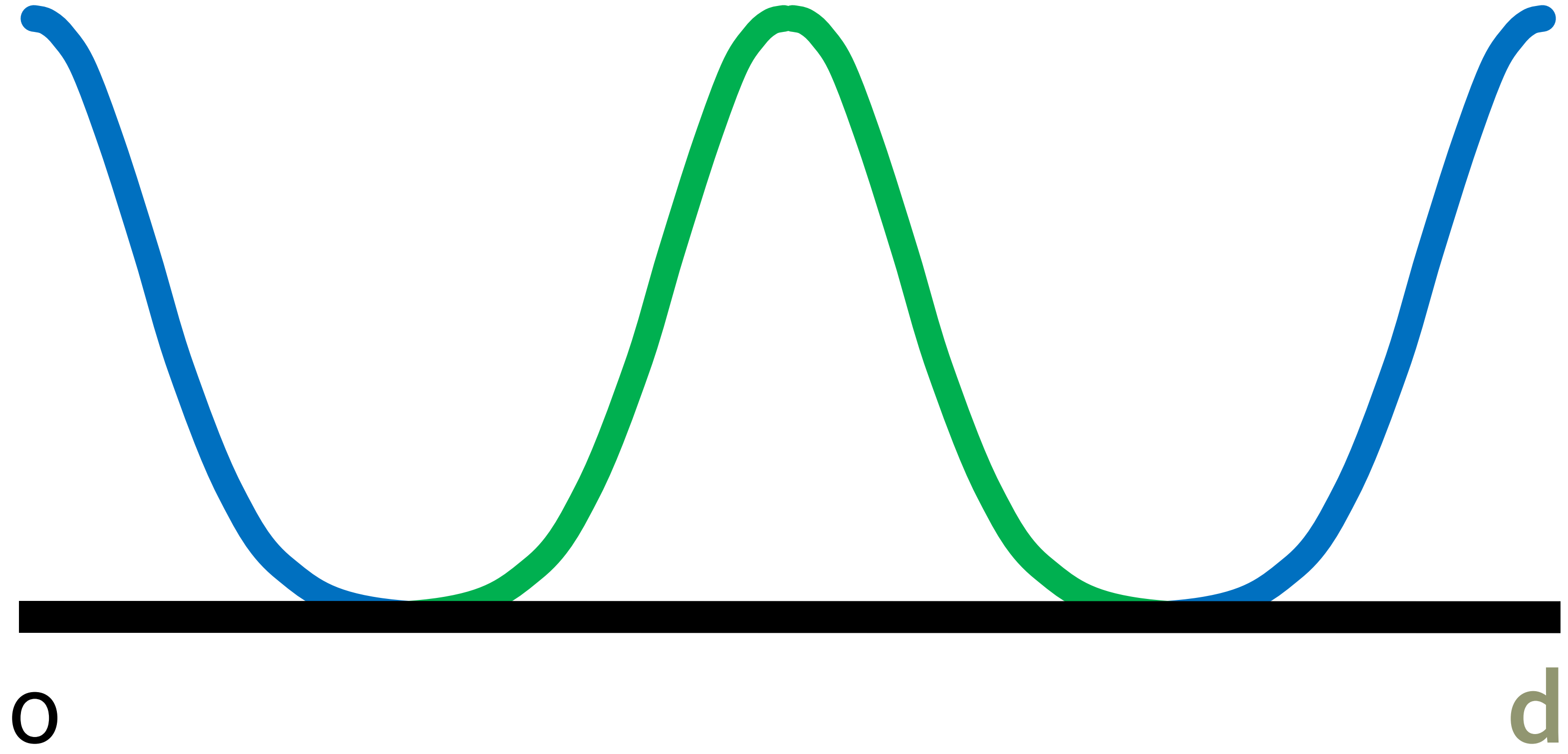
Regev04 - Encryption of "1"

- $r \in_R \{0,1\}^m$
- $E(1) = a_k/2 + \Sigma_i \, r_i a_i \bmod N$



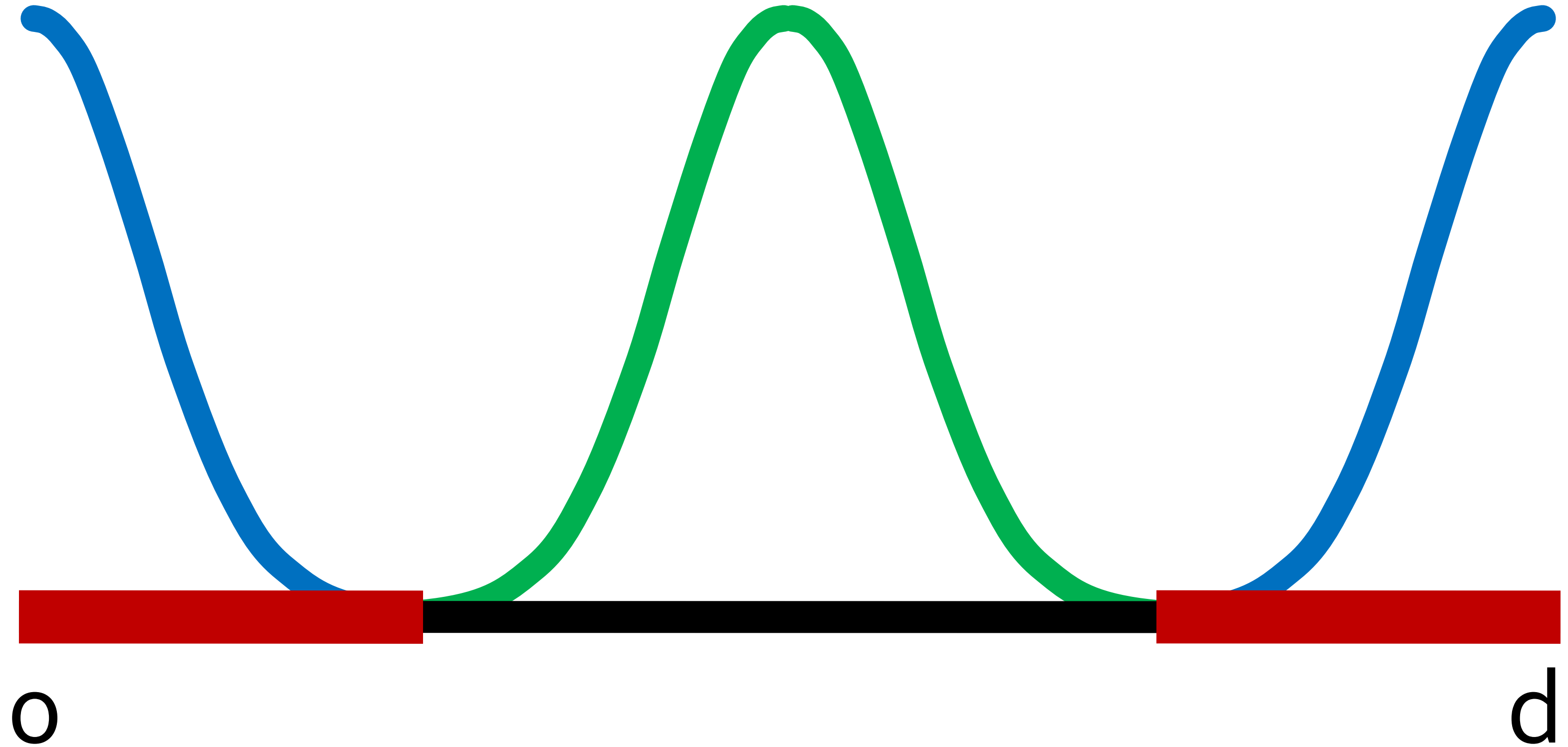
Regev04 - Decryption 1

- Received ciphertext is $c \in \{0,\ldots,N-1\}$
- Consider $c \bmod d$



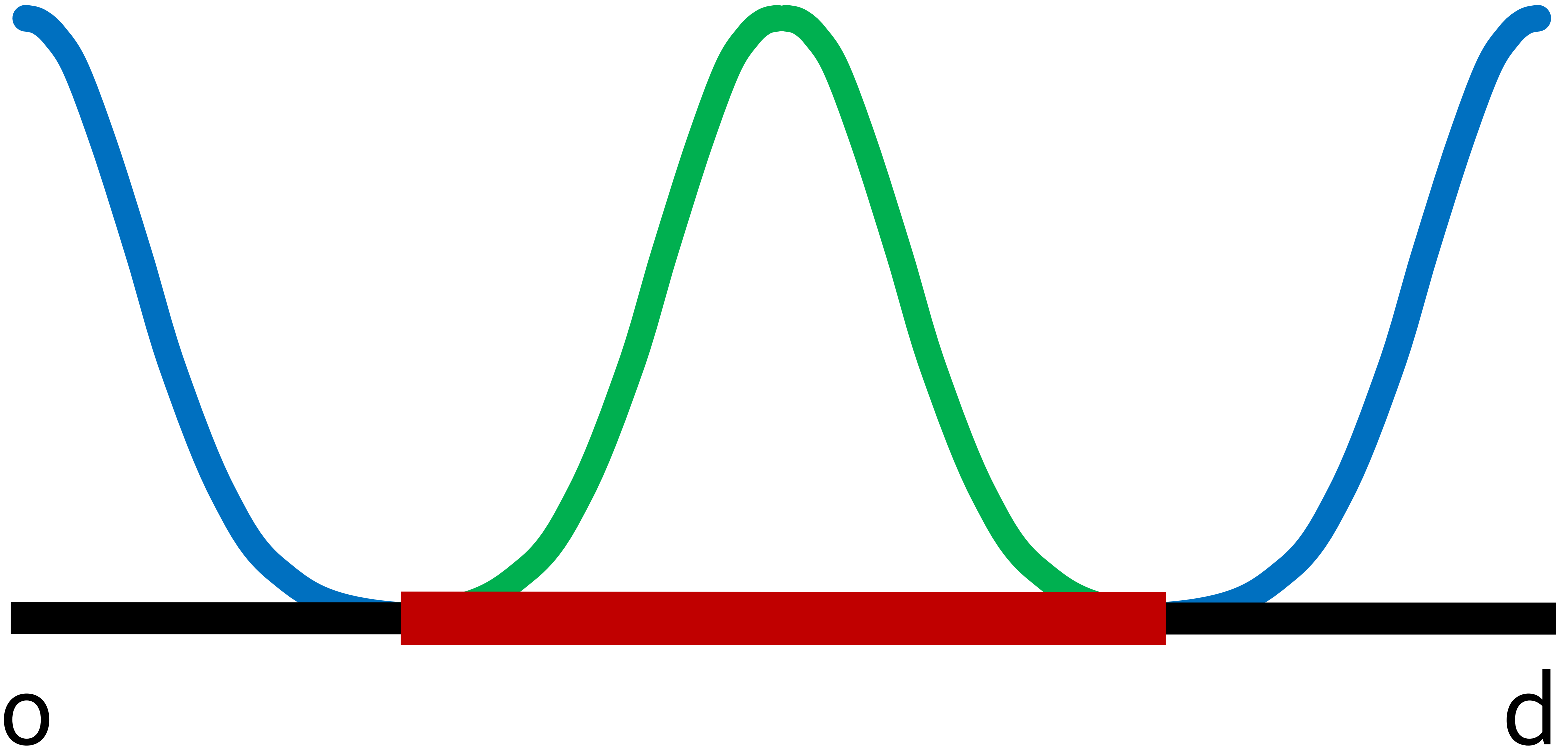
Regev04 - Decryption 2

- Decrypt to "o"



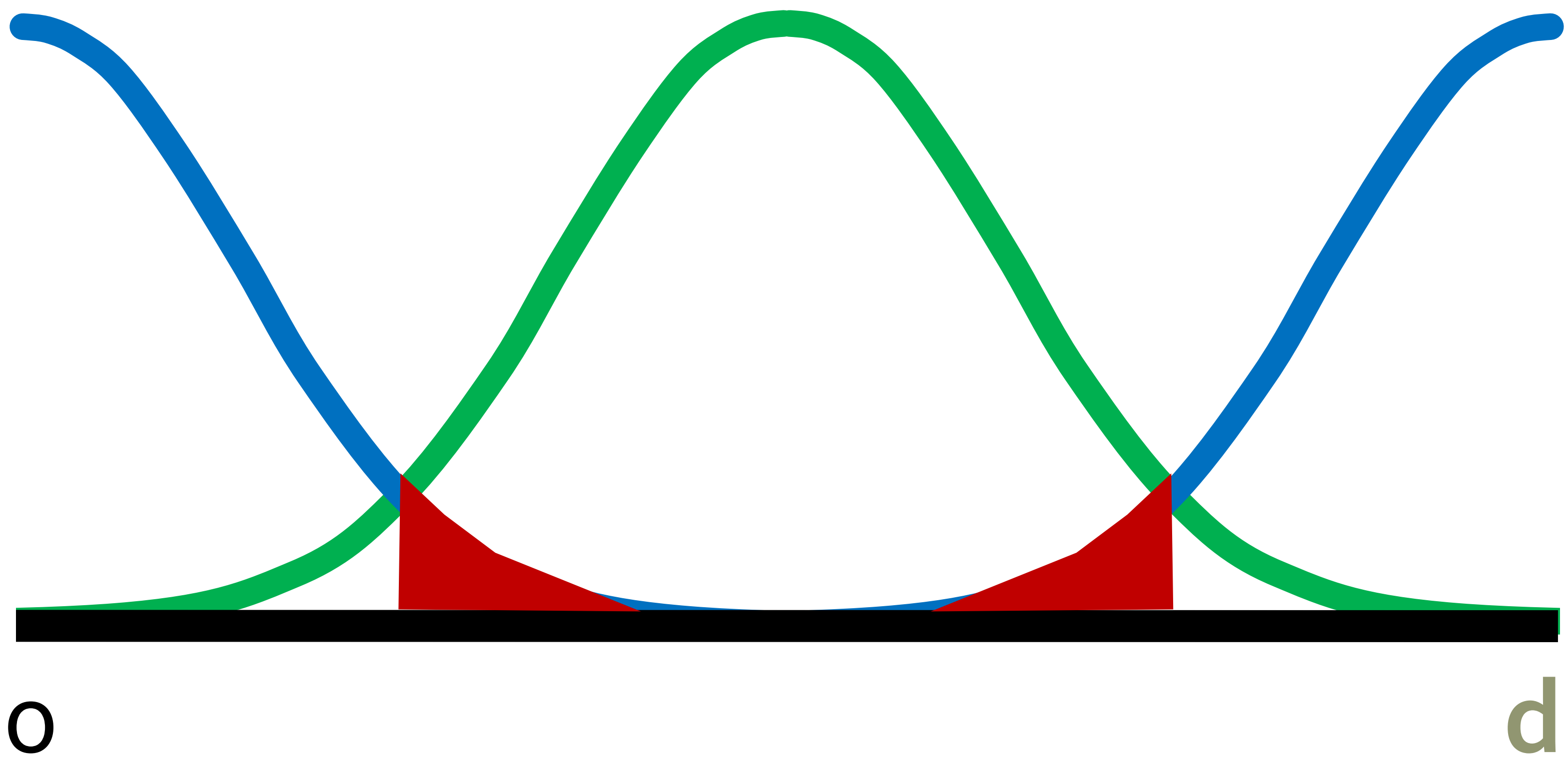
Regev04 - Decryption 3

- Decrypt to "1"



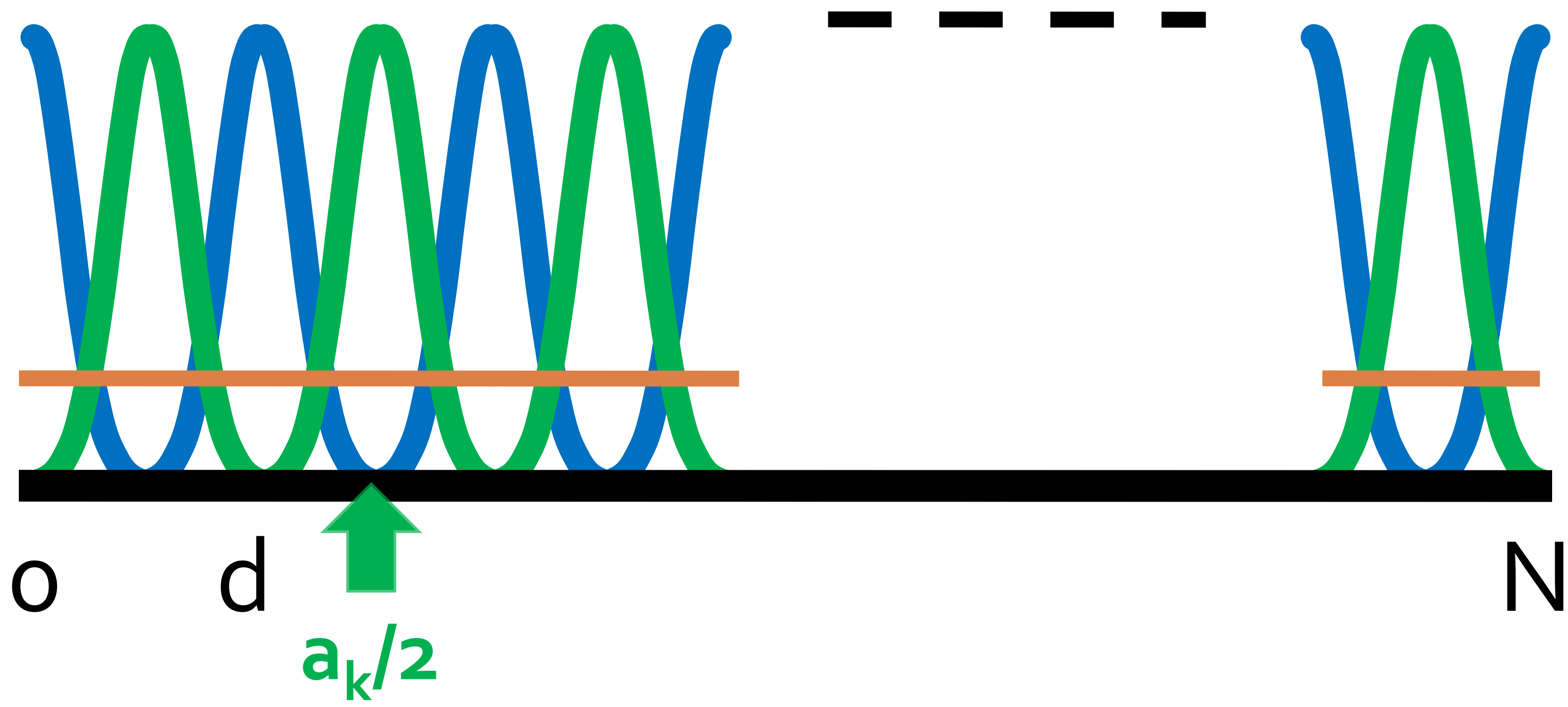
Regev04 - Decryption Errors

- Consider c mod d



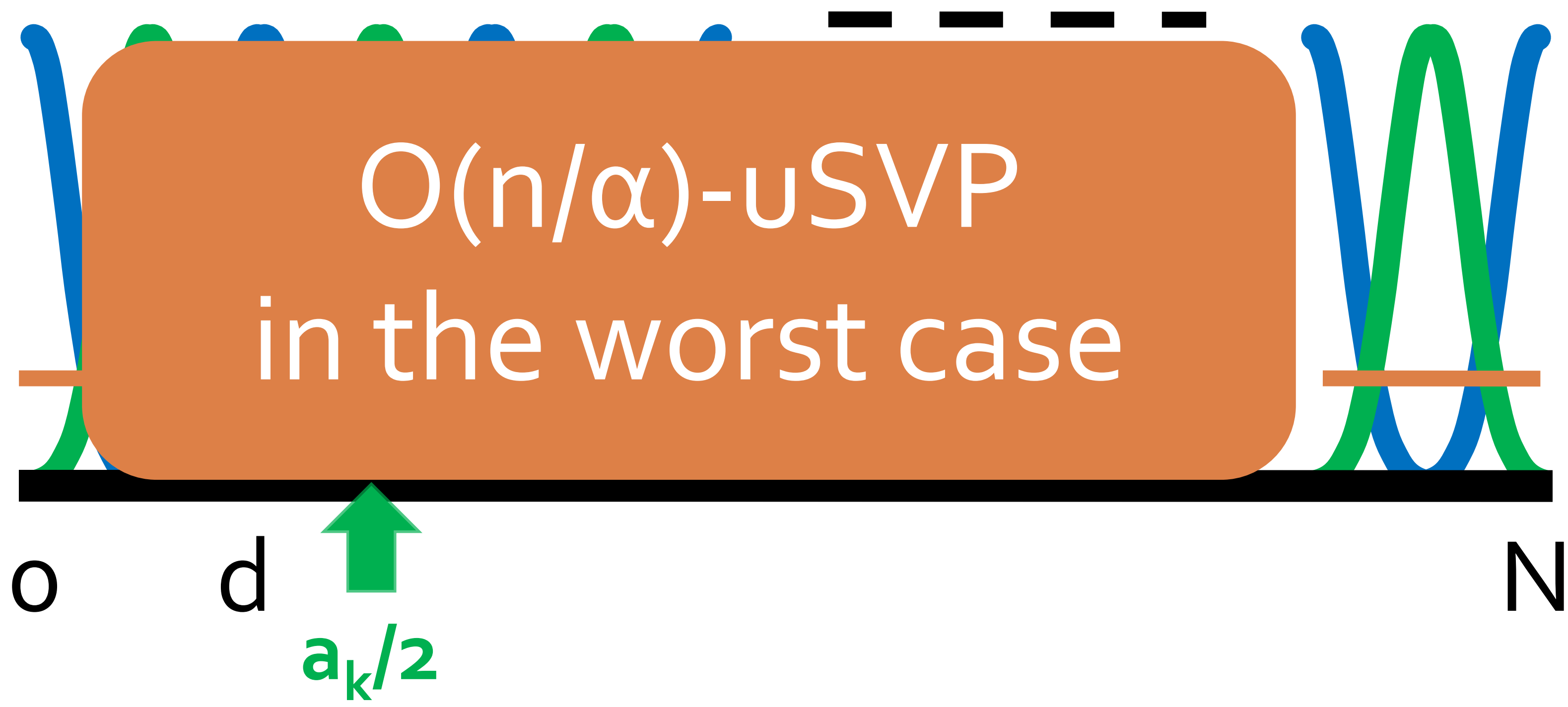
Regev04 - Security

- E(0) vs. E(1) with pk → E(0) vs. U with pk
- E(0) vs. U with pk → O(n/α)-uSVP in the worst case
  - α^2 is the variance of distrib. in key generation



Regev04 - Security

- E(0) vs. E(1) with pk → E(0) vs. U with pk
- E(0) vs. U with pk → O(n/α)-uSVP in the worst case
  - α^2 is the variance of distrib. in key generation

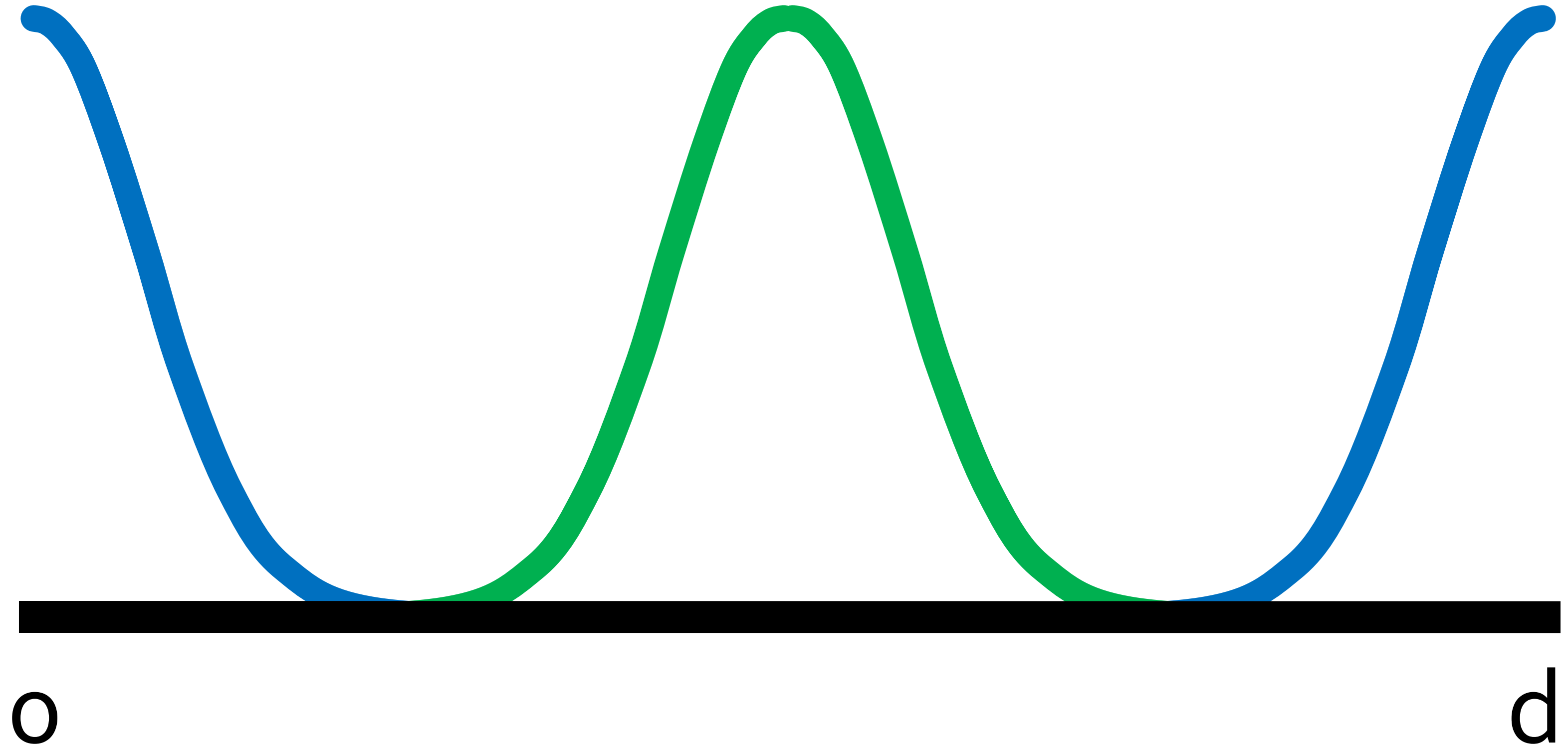


Our Technique

- #plaintext : 2 $\rightarrow$ p
- Increase # of "waves"
  - Same |ciphertext| and |pk|

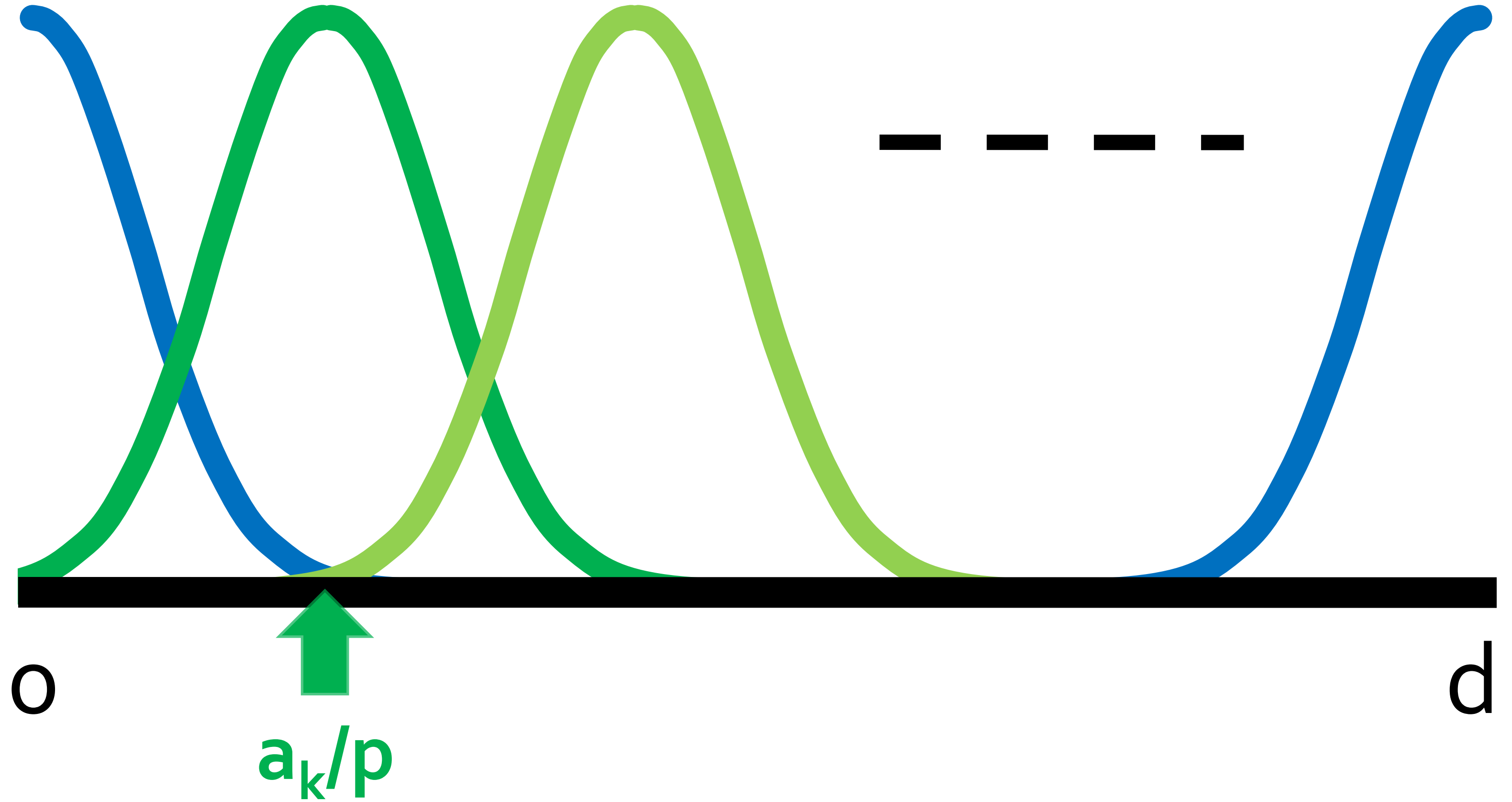
Multi Bit - Illustration

- E(0): Blue
- E(1): Green



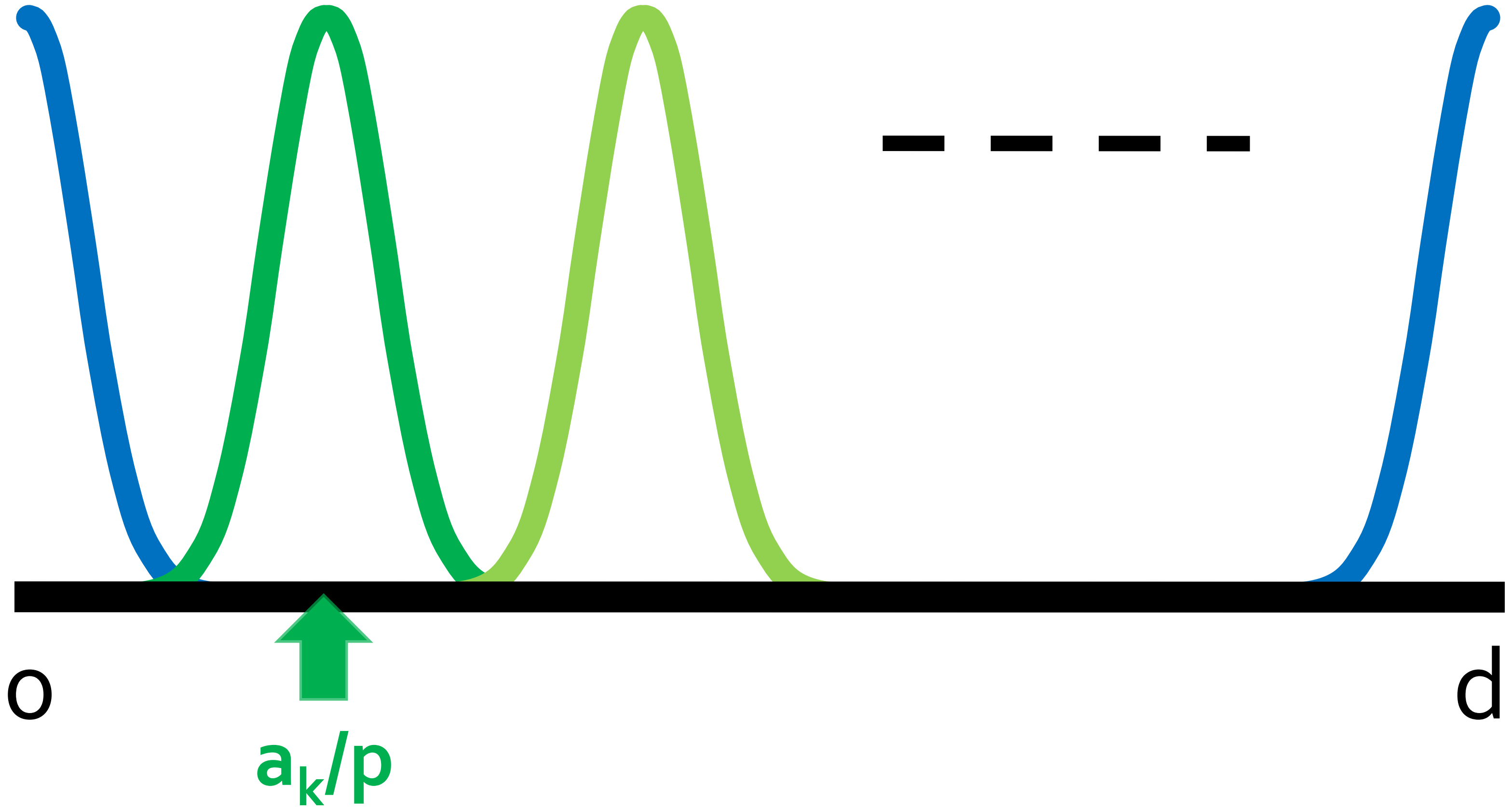
Multi Bit - Illustration

- Increase # of "waves"
- with a_k=(p+1)d+e



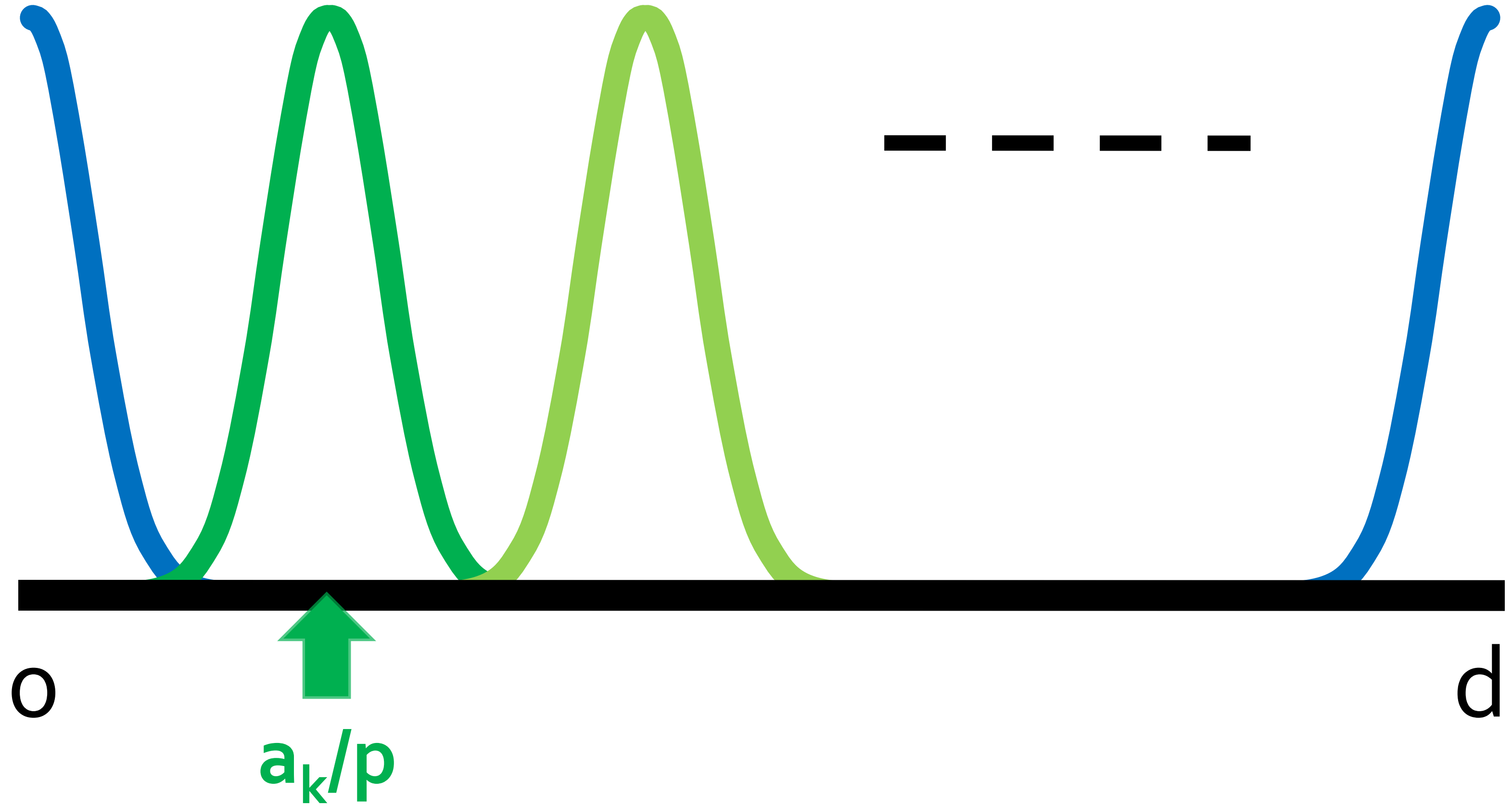
Multi Bit - Illustration

- make “waves” thin to decrease decrytpion errors
- Variance: $\alpha^2 \rightarrow (\alpha/p)^2$ in key generation



Multi Bit - Illustration

- Variance: $\alpha^2 \rightarrow (\alpha/p)^2$
- Underlying Problem: $O(n/\alpha)$-uSVP $\rightarrow$ $O(pn/\alpha)$-uSVP



Comparison

	Regev04	Ours
plaintext	1	**log p**
ciphertext	$8n^2$	←
public key	$\tilde{O}(n^4)$	←
secret key	$\tilde{O}(n^2)$	←
security	$\tilde{O}(n^{1.5})$-uSVP	$\tilde{O}(\mathbf{p}n^{1.5})$-uSVP

Comparison - 2

	AD_{GGH}	Ours	Regev04	Ours
plaintext	1	**log p**	1	**log p**
security	$O(n^{11})$-uSVP	$O(\mathbf{p}n^{11})$-uSVP	$\tilde{O}(n^{1.5})$-uSVP	$\tilde{O}(\mathbf{p}n^{1.5})$-uSVP

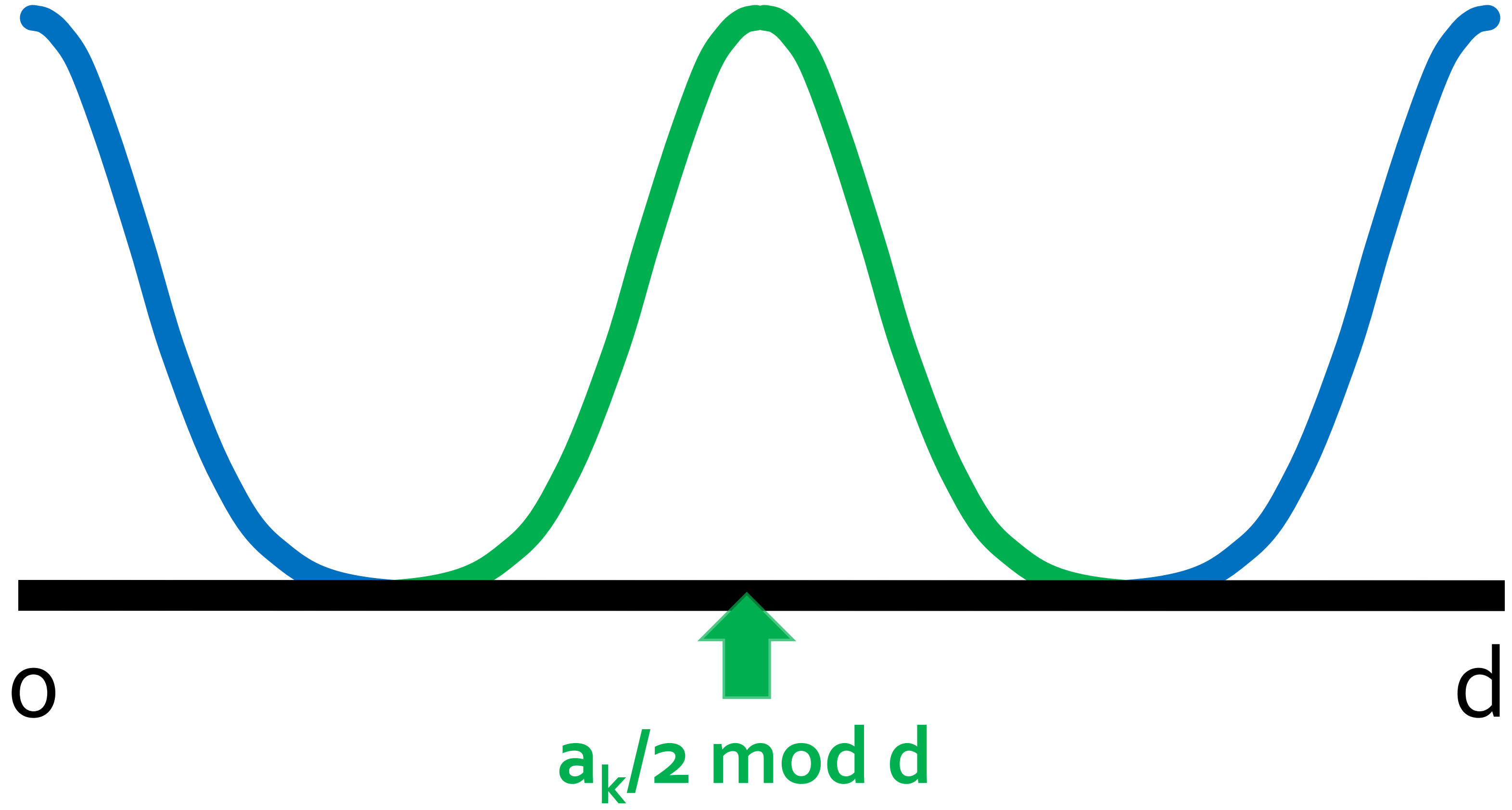
	Regev05	Ours	Ajtai05	Ours
plaintext	1	**log p**	1	**log p**
security	$SVP_{\tilde{O}(n^{1.5})}$	$SVP_{\tilde{O}(\mathbf{p}n^{1.5})}$	DA	DA'

Homomorphism of PKE

- E(m)+E(m')=E(m+m')
  - cf. RSA, Goldwasser-Micali,...
- Do R04 and ours have homomorphism?
  - No
  - Pseudo-homomorphism

Pseudo-homomorphism

- D(blue)=0, D(green)=1
- D(blue+green)=1 , D(green+green)=0



Conclusions

- Results
  - Proposal of multi-bit versions of Type B
    - AD_{GGH}, Regev04, Regev05, and Ajtai05
  - Analysis of the trade-off
    - between the size of plaintext and security levels
  - Pseudo-homomorphism
    - AD_{GGH}, Regev04, Regev05, and Ajtai05
- Open Problem
  - $\Theta(n)$-bit cryptosystems with a/w connection
    - We develop $O(\log n)$-bit cryptosystems with a/w
    - It may require new idea