Does Public Key Encryption Exist?

Oleg Izmerly, Tal Mor

Technion, Israel Institute of Technology,

2003

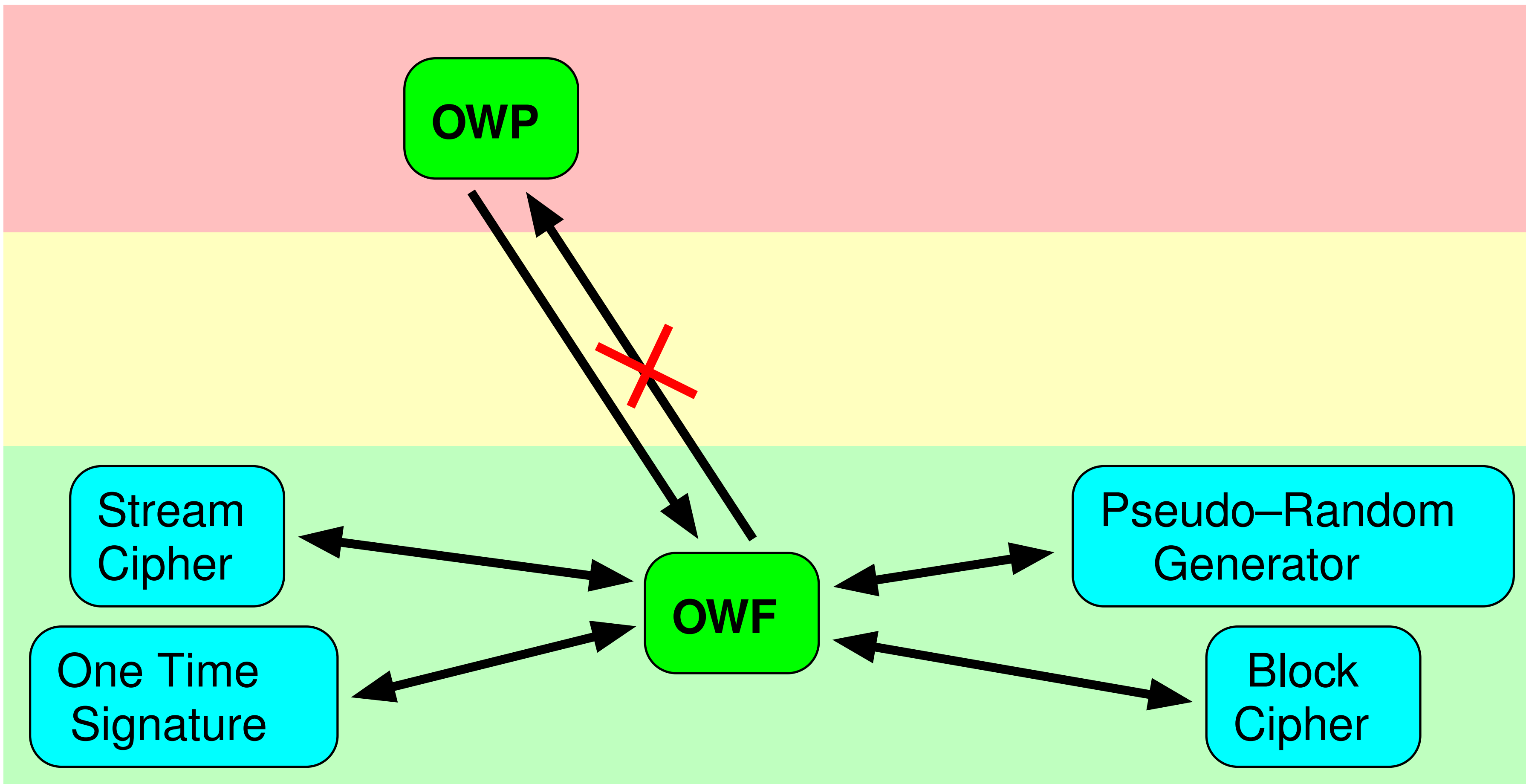
Cryptographic Primitives

- **One-Way Function (OWF)**
  - The description of f is publicly known and does not require any secret information for its operation.
  - Given x, it is easy to compute $f(x)$.
  - Given y, in the range of f, it is hard to find an x such that $f(x) = y$.

Cryptographic Primitives

- **One-Way Function (OWF)**
  - The description of f is publicly known and does not require any secret information for its operation.
  - Given x, it is easy to compute $f(x)$.
  - Given y, in the range of f, it is hard to find an x such that $f(x) = y$.
- **One-Way Permutation (OWP)** is similar to one-way function but it is a permutation.

The World of the OWF (Minicrypt)



Cryptographic Primitives

- **Trapdoor One-Way Function (TD-OWF)**
  - f is one-way function.
  - There is an efficient algorithm that inverts f, when some some *trapdoor key* is given.

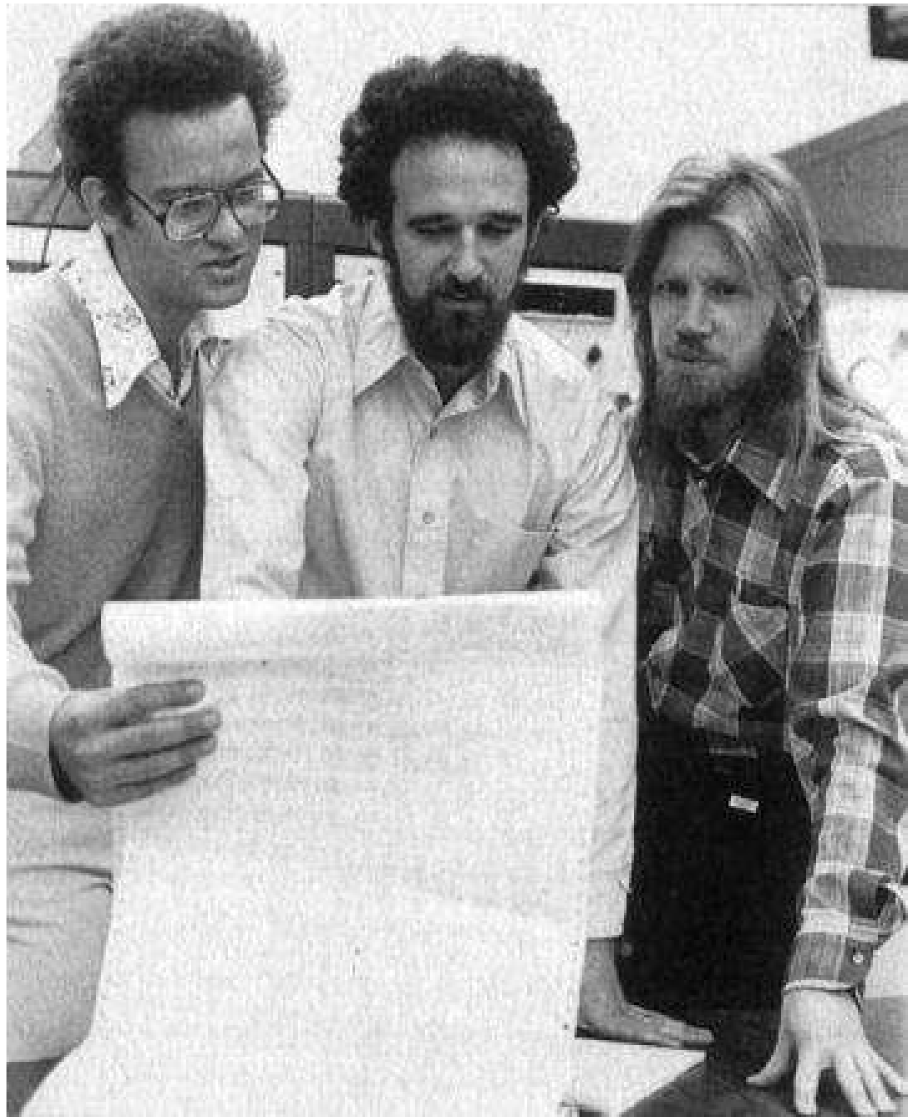
Cryptographic Primitives

- **Trapdoor One-Way Function (TD-OWF)**
  - f is one-way function.
  - There is an efficient algorithm that inverts f, when some some *trapdoor key* is given.
- **Trapdoor One-Way Permutation (TD-OWP)** is similar to trapdoor one-way function but it is a permutation.

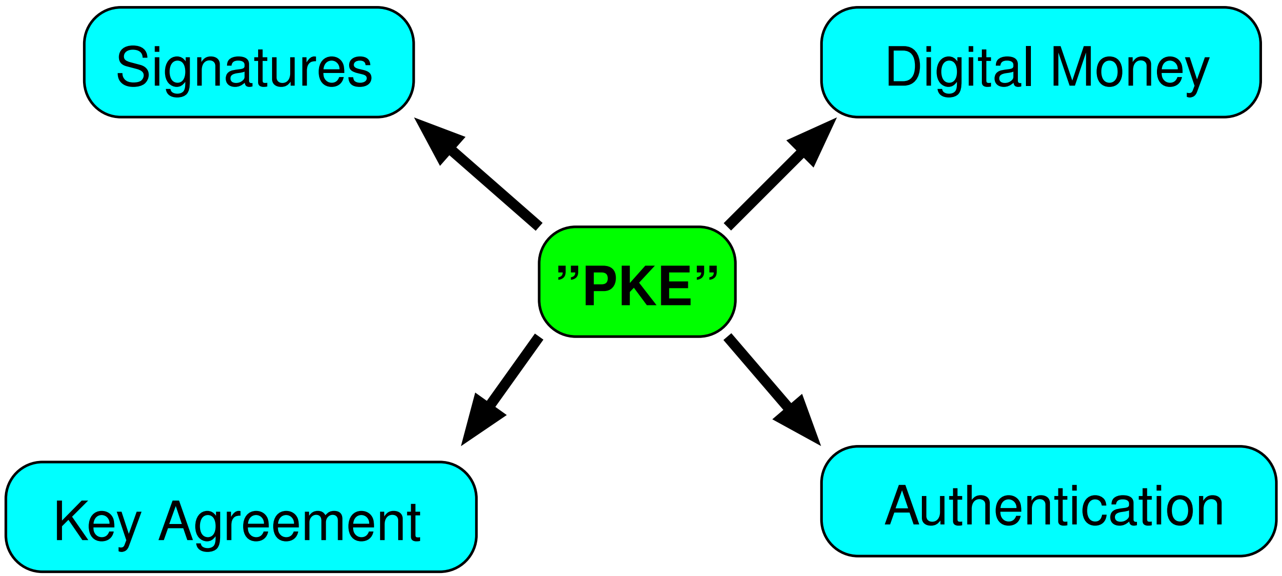
Cryptographic Primitives

- **Public Key Encryption (PKE)**
  - Encryption may be done by anyone with access to the “public key”.
  - Decryption may be done only by the holder of the “private key”.

Merkle-Hellman-Diffie



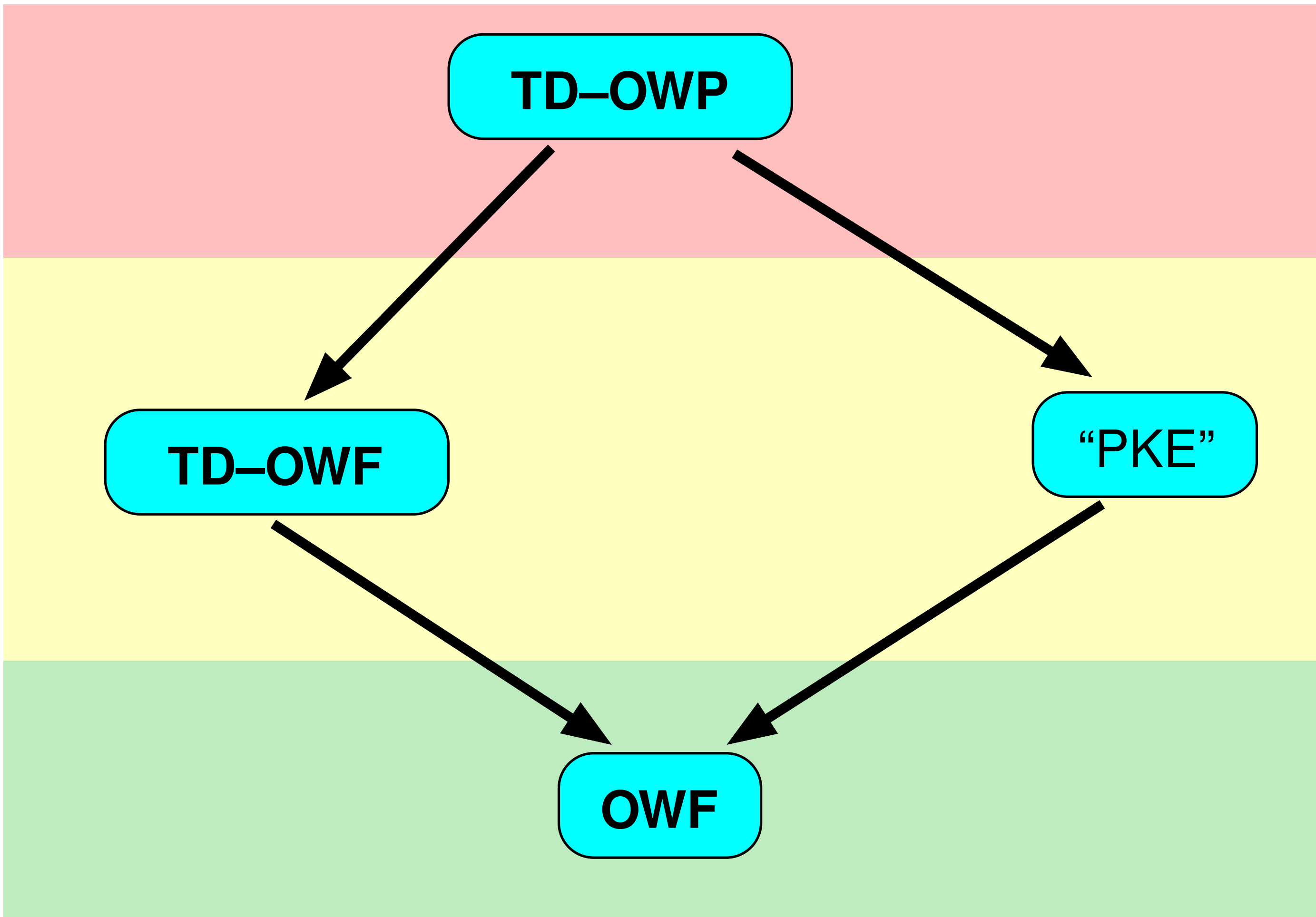
Cryptographic Primitives



Candidates for Public Key Encryption

cryptosystem	based on
RSA	factoring
Rabin	factoring
ElGamal	discrete logarithm
Knapsack	NP hard problem
Ajtai-Dwork	u-SVP problem
Regev	u-SVP problem
McEliece	error correcting codes problem

The World of PKE



Regev's Cryptosystem

- **Encryption**

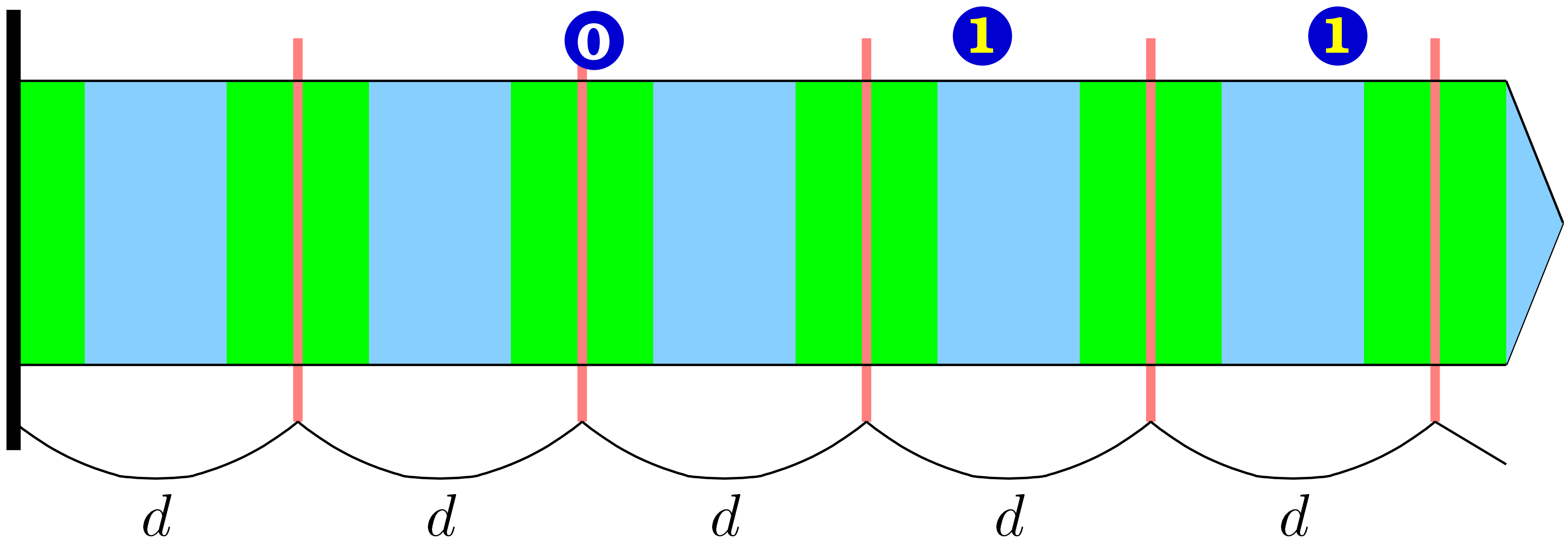
$$\boxed{\mathcal{E} : \{0,1\} \to [0,N) \subset \mathbb{Z}}$$

Encryption procedure must be probabilistic.

- **Decryption**

$$\boxed{\mathcal{D} : [0,N) \to \{0,1\}}$$

The Space Of Ciphertexts



Theorem *It is impossible to distinguish distributions of $\mathcal{E}(0)$ and $\mathcal{E}(1)$.*

Regev's PKE Security

Theorem *It is impossible to distinguish distributions of* $\mathcal{E}(0)$ *and* $\mathcal{E}(1)$.

Proof resulting from an assumption on the hardness of u-SVP.

u-SVP might be secure in a quantum environment.

Regev's Cryptosystem

- **Private Key**
  Private key is the real number $d, \sqrt{N}/2 < d < \sqrt{N}$. N is exponentially large.
- **Decryption Procedure**

$$\mathcal{D}(c) = \begin{cases} 0, & \mathrm{FRAC}(c/d) < 1/4 \\ 1, & otherwise \end{cases}$$

where $\mathrm{FRAC}(x)$ is the fractional part of x (the distance to the closest integer).

Proof of Security

Under the assumption that the private key is secure, it is infeasible to distinguish the encryption of 0 from the encryption of 1.

Private key is secure

$\mathcal{E}(0)$ **and** $\mathcal{E}(1)$ **are indistinguishable**

Chosen Plaintext Attacks

A form of attack in which the opponent can present arbitrary plaintext to be enciphered, and then capture the resulting ciphertext.

Not relevant for PKE, because anyone may encrypt.

Chosen Ciphertext Attack

A cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected or dictated by the analyst.

Chosen Ciphertext Attack

A cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected or dictated by the analyst.

Private key is secure

$\mathcal{E}(0)$ **and** $\mathcal{E}(1)$ **are indistinguishable**

Chosen Ciphertext Attack

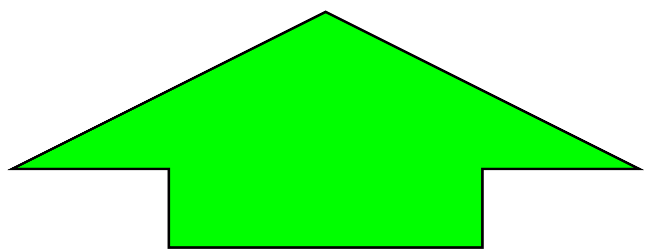
A cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected or dictated by the analyst.

$$\boxed{(A \Rightarrow B) \Longrightarrow (\neg B \Rightarrow \neg A)}$$

Chosen Ciphertext Attack

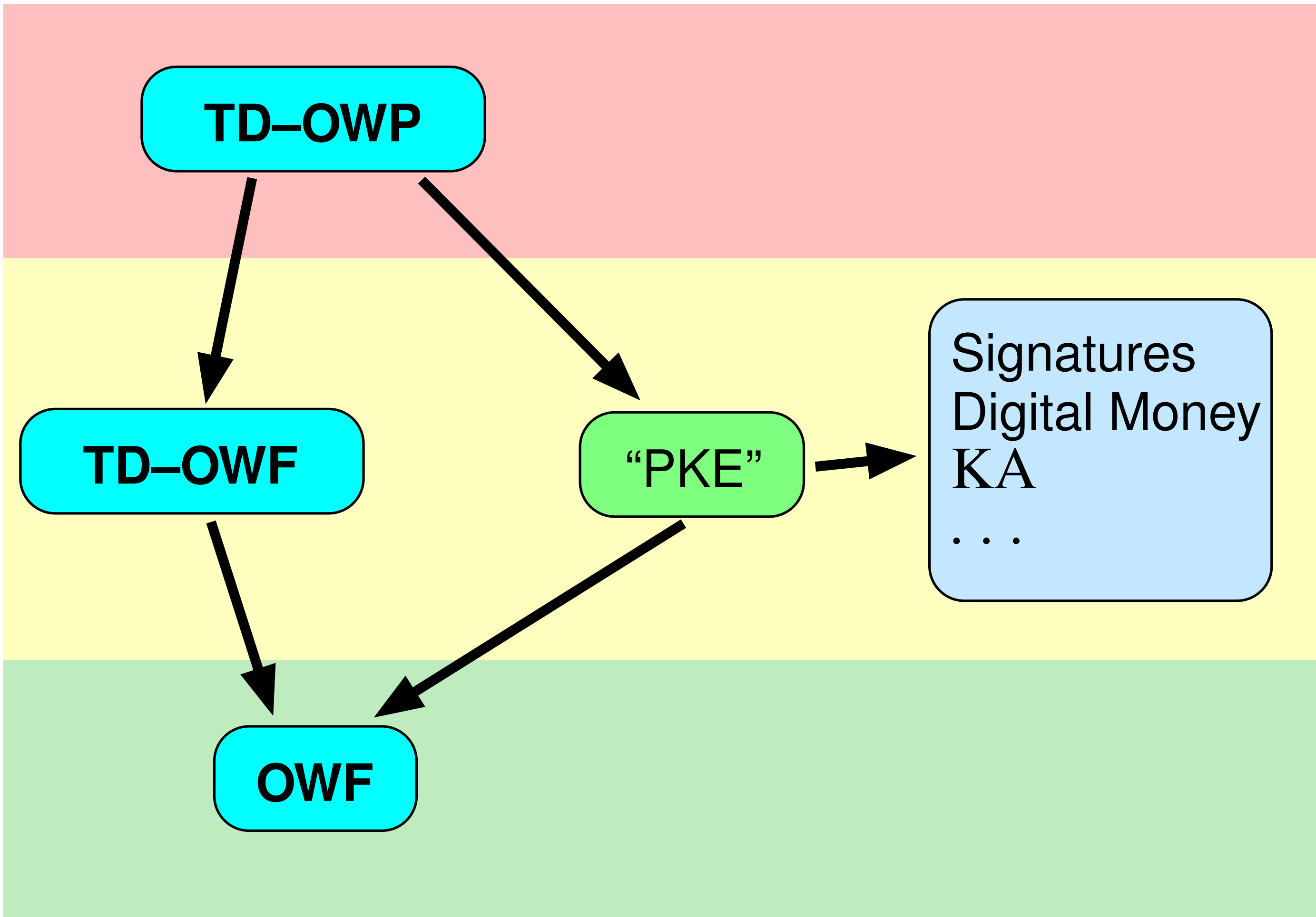
A cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected or dictated by the analyst.

Private key is insecure

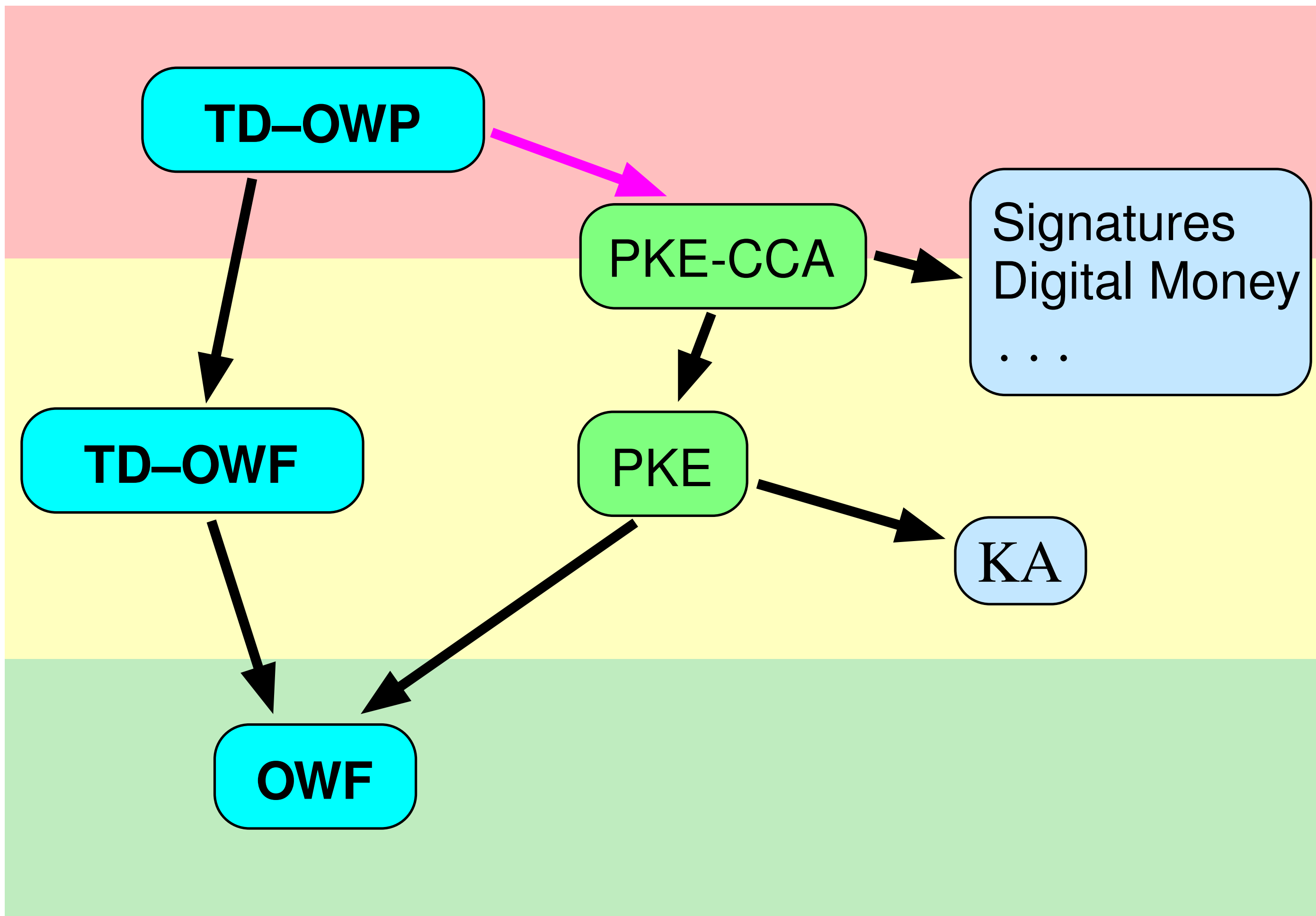


$\mathcal{E}(0)$ **and** $\mathcal{E}(1)$ **are distinguishable**

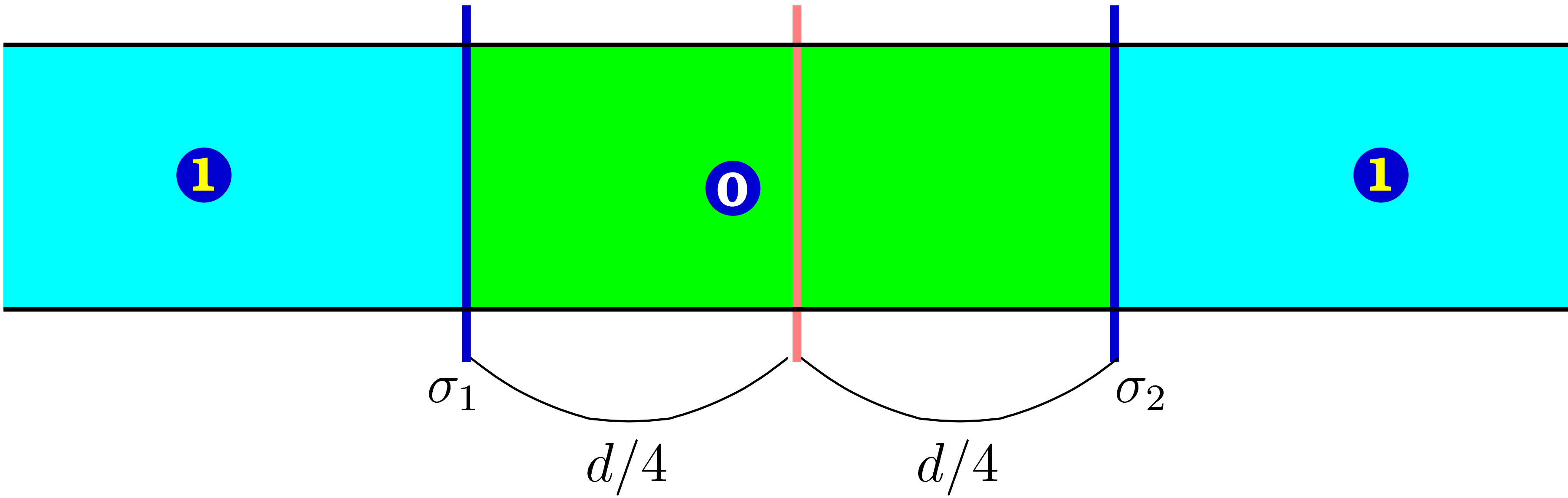
PKE in Context of CCA



PKE in Context of CCA



Regev's Cryptosystem. CCA



$$d = 2 \cdot (\sigma_2 - \sigma_1)$$

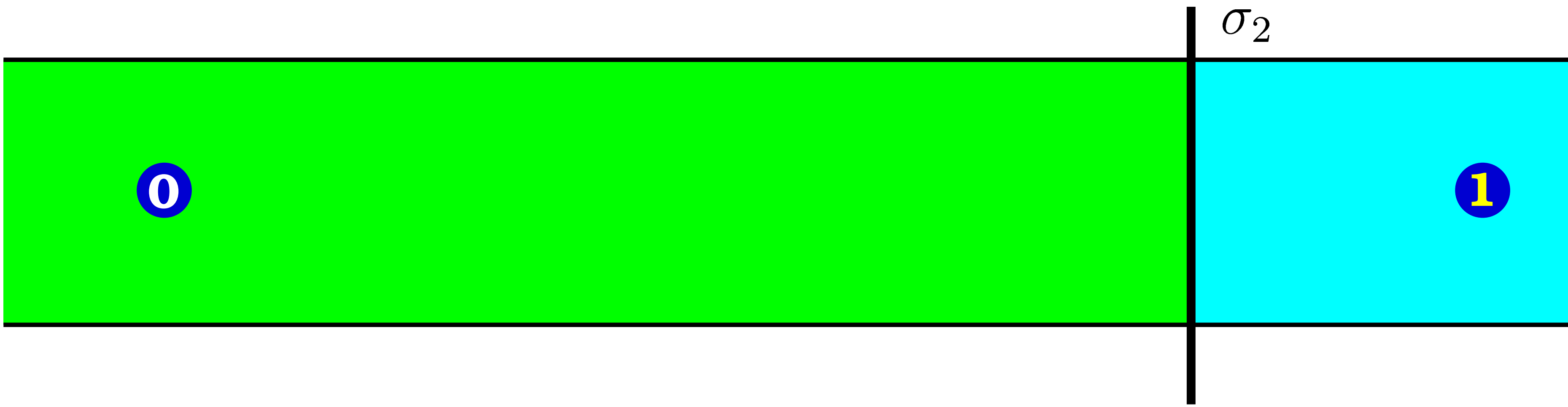
Regev's Cryptosystem. CCA

How to find σ's???

- Get some encryption of "0".
- Learn another point in a nearby "1" area.
- Perform binary search.

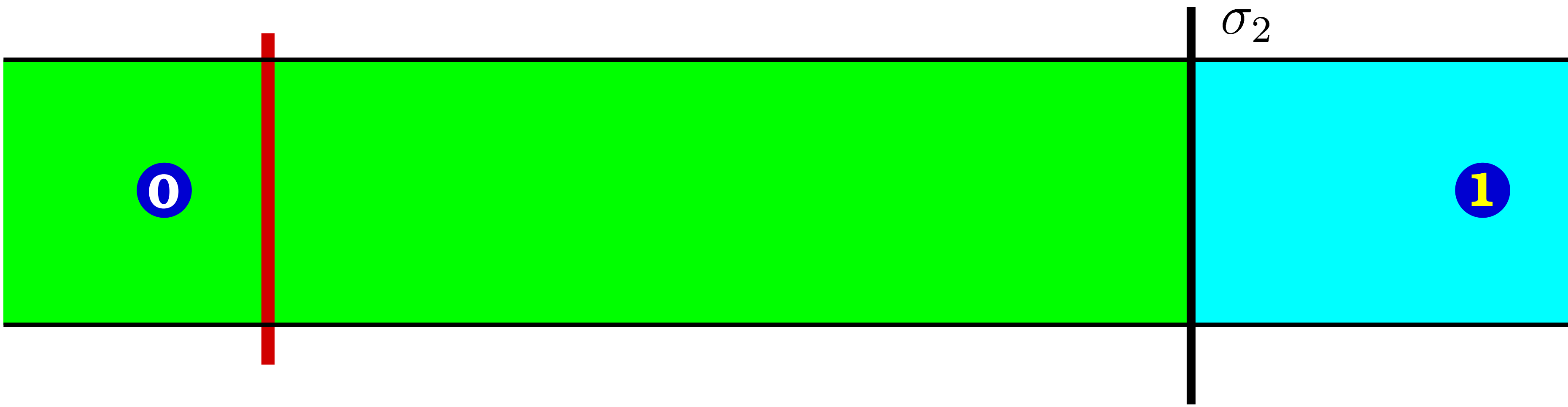
Regev's Cryptosystem. CCA

Binary Search



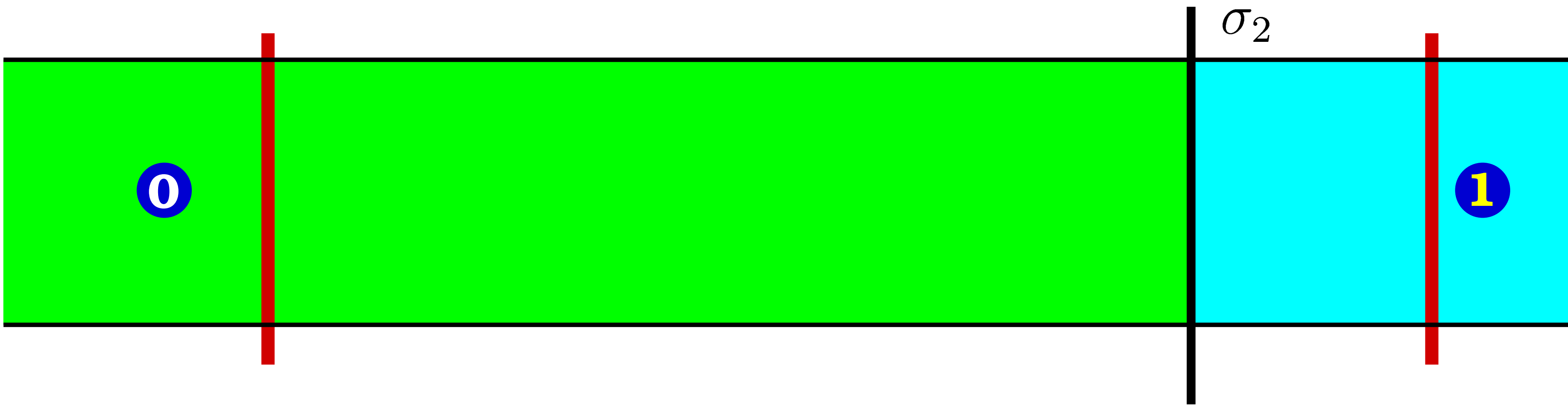
Regev's Cryptosystem. CCA

Binary Search



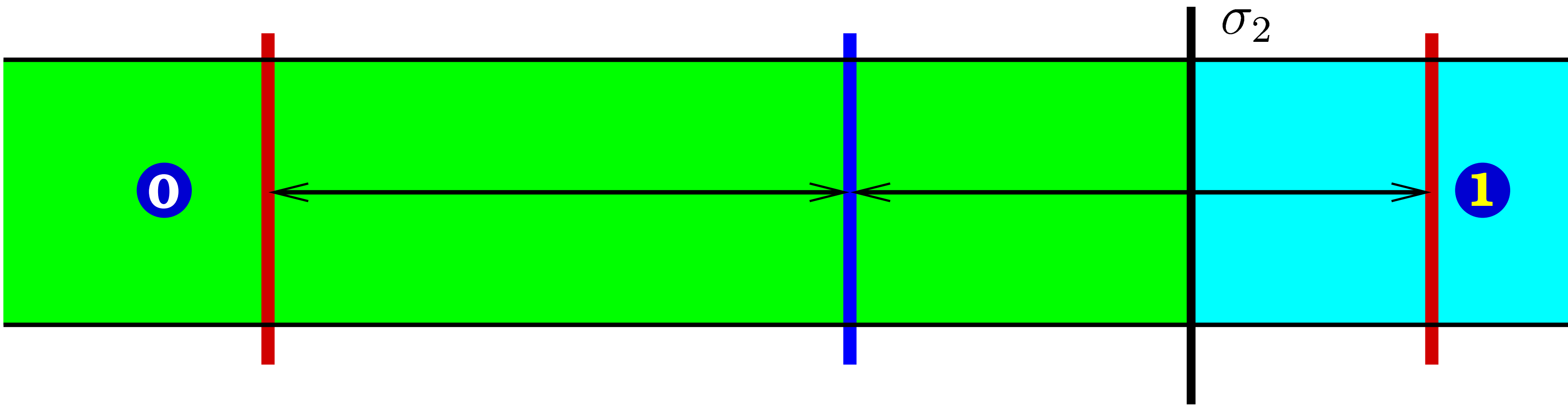
Regev's Cryptosystem. CCA

Binary Search



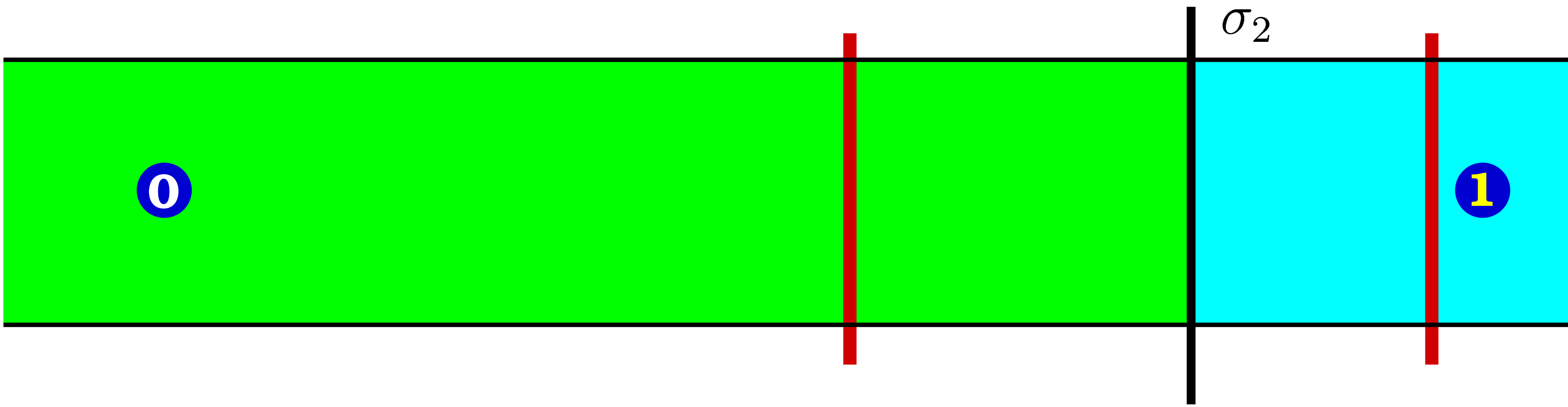
Regev's Cryptosystem. CCA

Binary Search



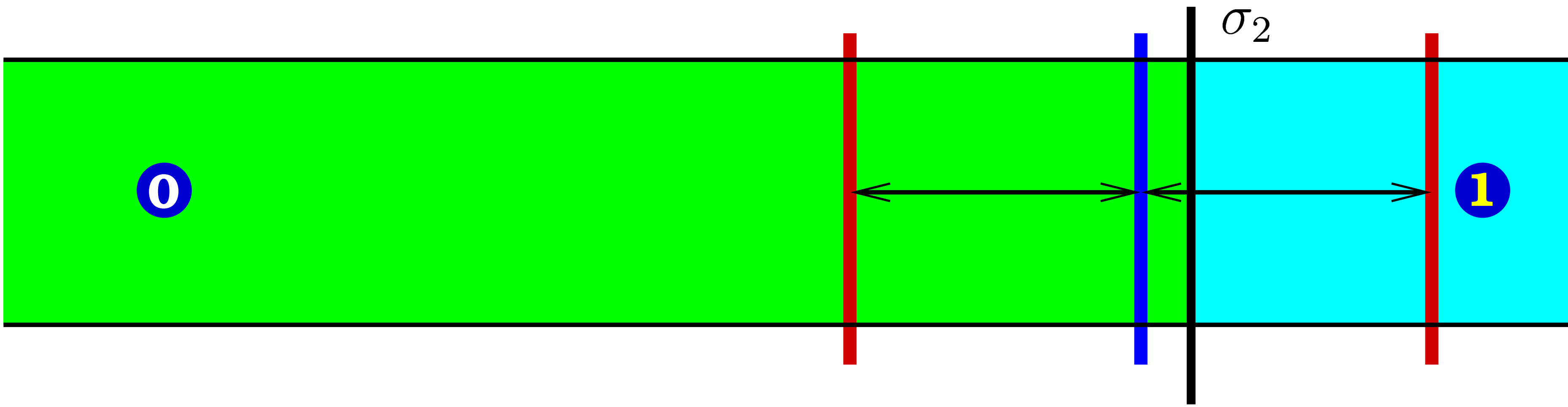
Regev's Cryptosystem. CCA

Binary Search



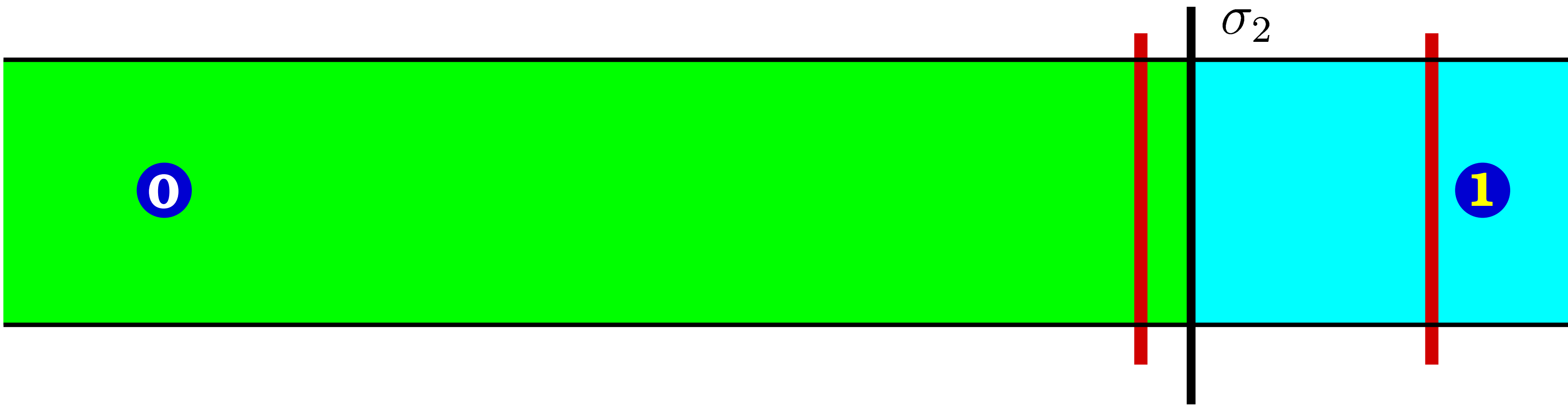
Regev's Cryptosystem. CCA

Binary Search



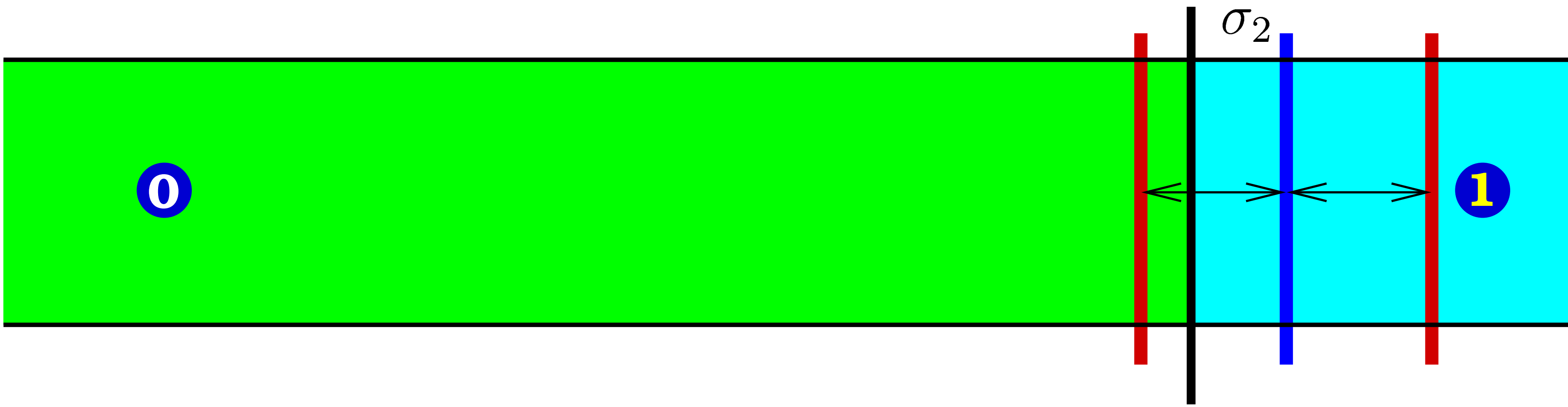
Regev's Cryptosystem. CCA

Binary Search



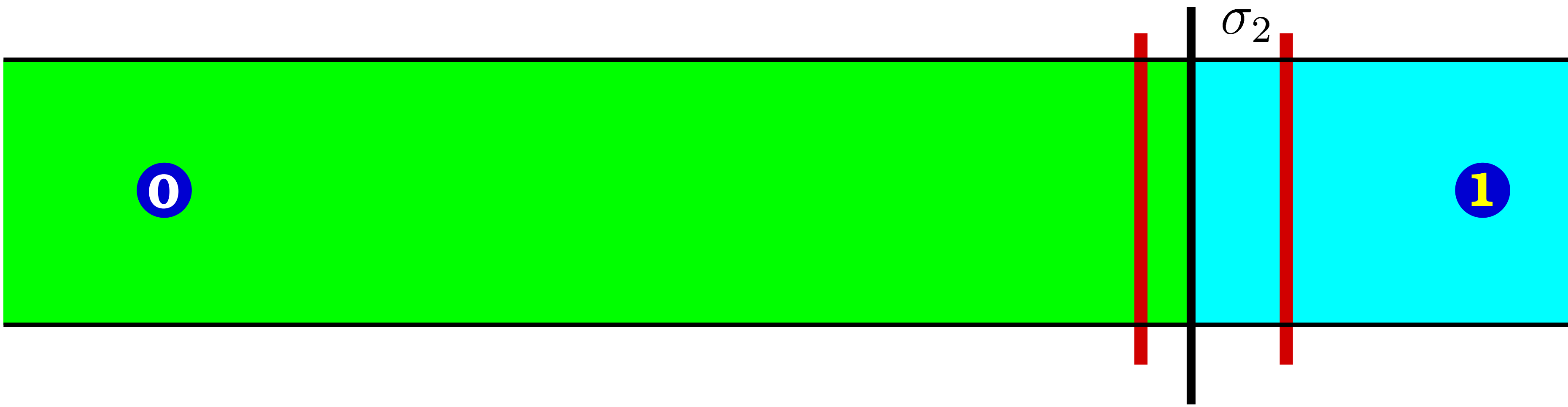
Regev's Cryptosystem. CCA

Binary Search



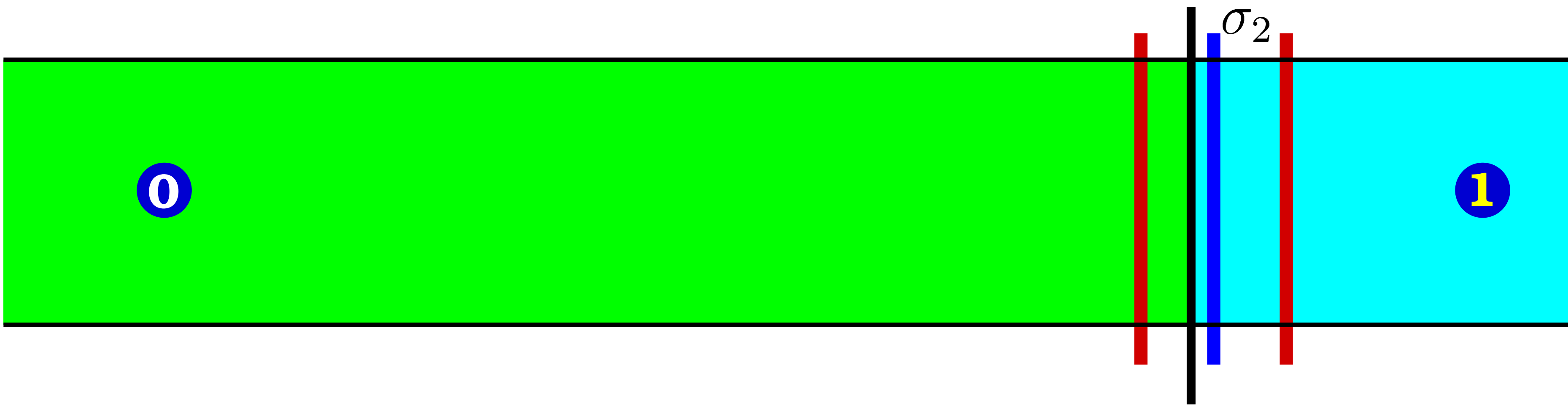
Regev's Cryptosystem. CCA

Binary Search



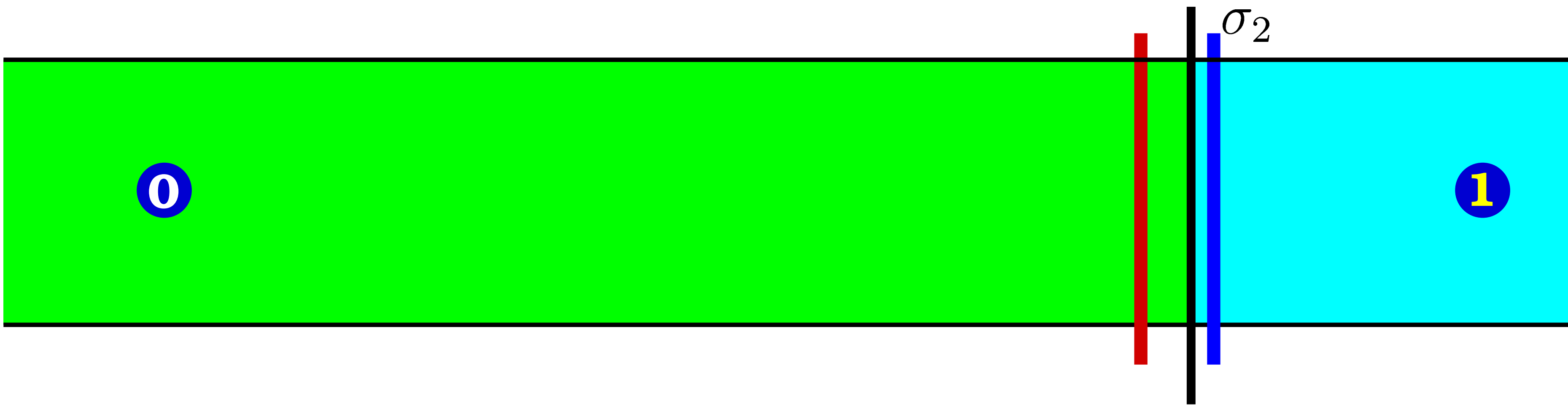
Regev's Cryptosystem. CCA

Binary Search



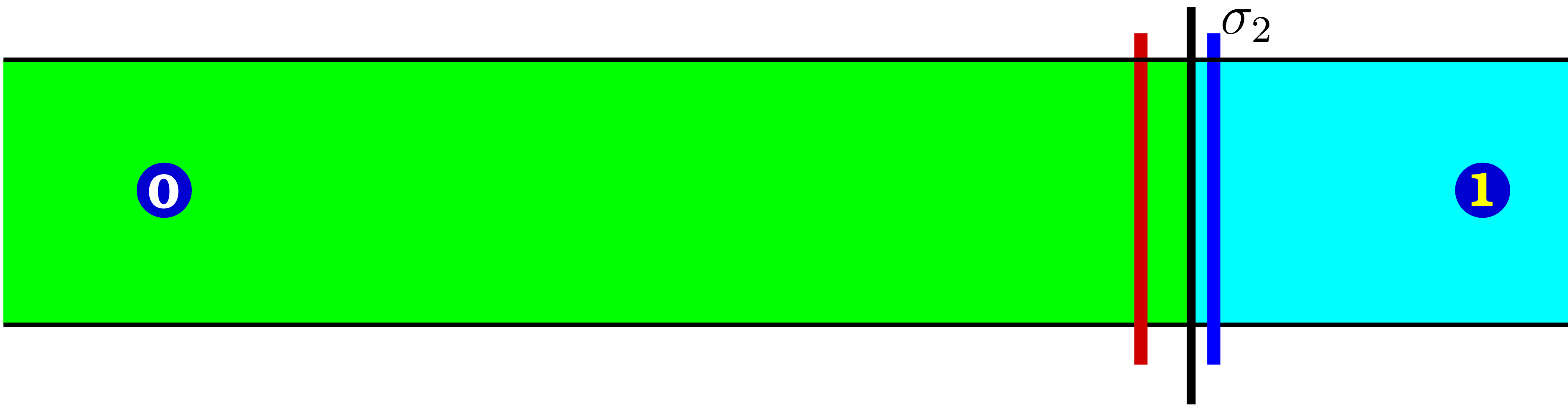
Regev's Cryptosystem. CCA

Binary Search



Regev's Cryptosystem. CCA

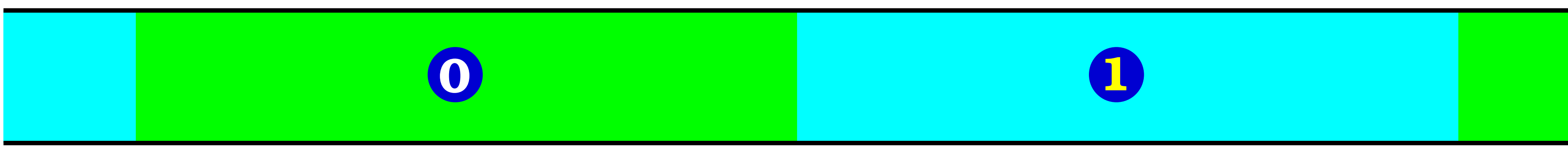
Binary Search



σ_2 may be found effectively with arbitrary accuracy.

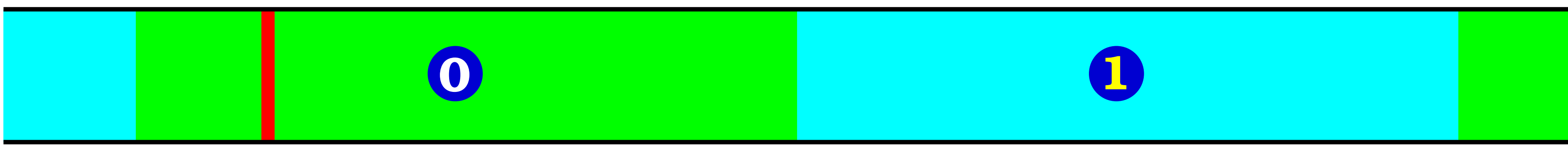
Regev's Cryptosystem. CCA

We need two neighboring ciphertexts separated by a threshold (the point where the decryption oracle changes its value).



Regev's Cryptosystem. CCA

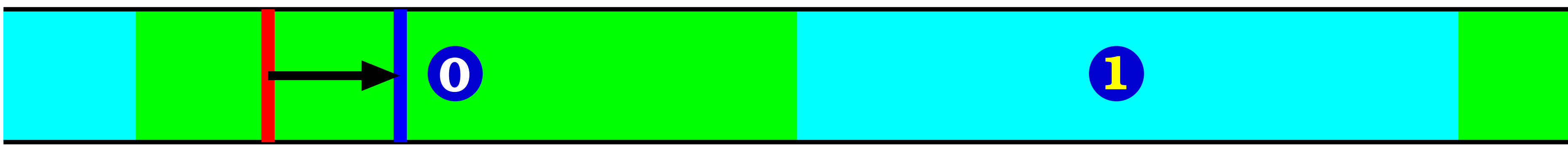
We need two neighboring ciphertexts separated by a threshold (the point where the decryption oracle changes its value).



Get some arbitrary encryption of 0.

Regev's Cryptosystem. CCA

We need two neighboring ciphertexts separated by a threshold (the point where the decryption oracle changes its value).

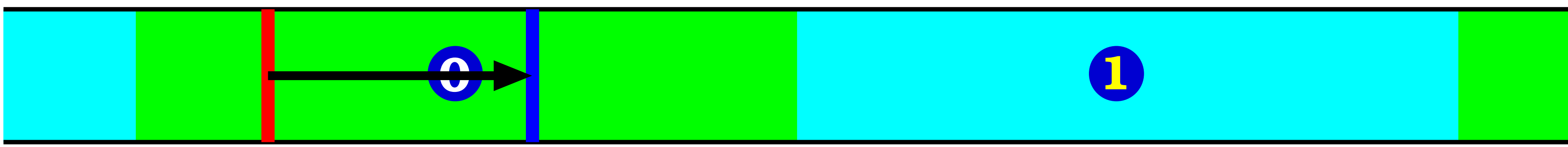


Jump to some "safe" distance.

$\frac{d}{2} > \frac{\sqrt{N}}{4}$, so we either stay on the "0" or move to the "1", but not to the next "0".

Regev's Cryptosystem. CCA

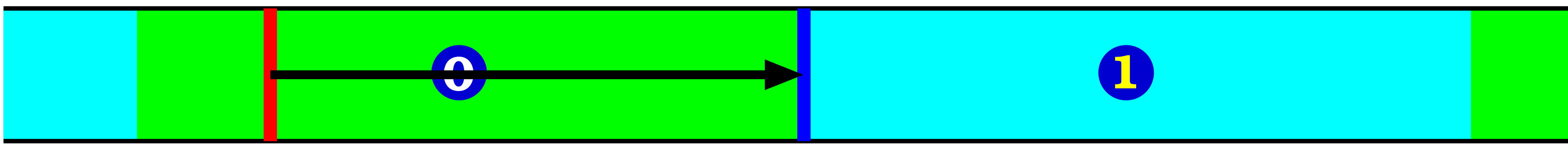
We need two neighboring ciphertexts separated by a threshold (the point where the decryption oracle changes its value).



Double the distance from the original point.

Regev's Cryptosystem. CCA

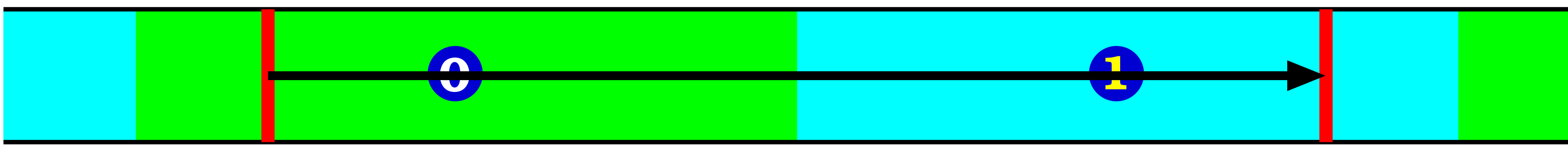
We need two neighboring ciphertexts separated by a threshold (the point where the decryption oracle changes its value).



Double it again . . .

Regev's Cryptosystem. CCA

We need two neighboring ciphertexts separated by a threshold (the point where the decryption oracle changes its value).



And again . . .

Regev's Cryptosystem. CCA

Practical Results

$\lfloor \log N \rfloor$	# of ciphertexts
100	197
200	397
300	603
400	798
500	996
600	1203

Regev's Cryptosystem. CCA

Corollary: Regev's cryptosystem is weak against chosen ciphertext attacks. Ajtai-Dwork cryptosystem has the same weakness.

Regev's Cryptosystem. CCA

Corollary: Regev's cryptosystem is weak against chosen ciphertext attacks. Ajtai-Dwork cryptosystem has the same weakness.

Is it possible to make a PKE resistant against chosen ciphertext attacks?

PKE Secure Against CCA (PKE-CCA)

$$\boxed{\mathrm{PKE} \Longrightarrow \mathrm{PKE-CCA}}$$

Some known constructions providing security against chosen ciphertext attacks *require* trapdoor one-way permutation (TD-OWP).

1. M. Naor, M. Yung, 1996.
2. D. Dolev, C. Dwork, M. Naor, 2000.
3. Y. Lindell, 2002.

PKE Secure Against CCA (PKE-CCA)

$$\boxed{\mathrm{PKE} \Longrightarrow \mathrm{PKE-CCA}}$$

Some known constructions providing security against chosen ciphertext attacks *require* trapdoor one-way permutation (TD-OWP).
The only known candidate for TD-OWP is RSA.

PKE Secure Against CCA (PKE-CCA)

$$\boxed{\mathrm{PKE} \Longrightarrow \mathrm{PKE} - \mathrm{CCA}}$$

Some known constructions providing security against chosen ciphertext attacks *require* trapdoor one-way permutation (TD-OWP).
The only known candidate for TD-OWP is RSA.
Other constructions are based on the random oracle model.
D. Pointcheval, 2000.

PKE Secure Against CCA (PKE-CCA)

$$\boxed{\mathrm{PKE} \Longrightarrow \mathrm{PKE-CCA}}$$

Some known constructions providing security against chosen ciphertext attacks *require* trapdoor one-way permutation (TD-OWP).
The only known candidate for TD-OWP is RSA.
Other constructions are based on the random oracle model.

But there is no theoretical justification for this model.

The World of PKE