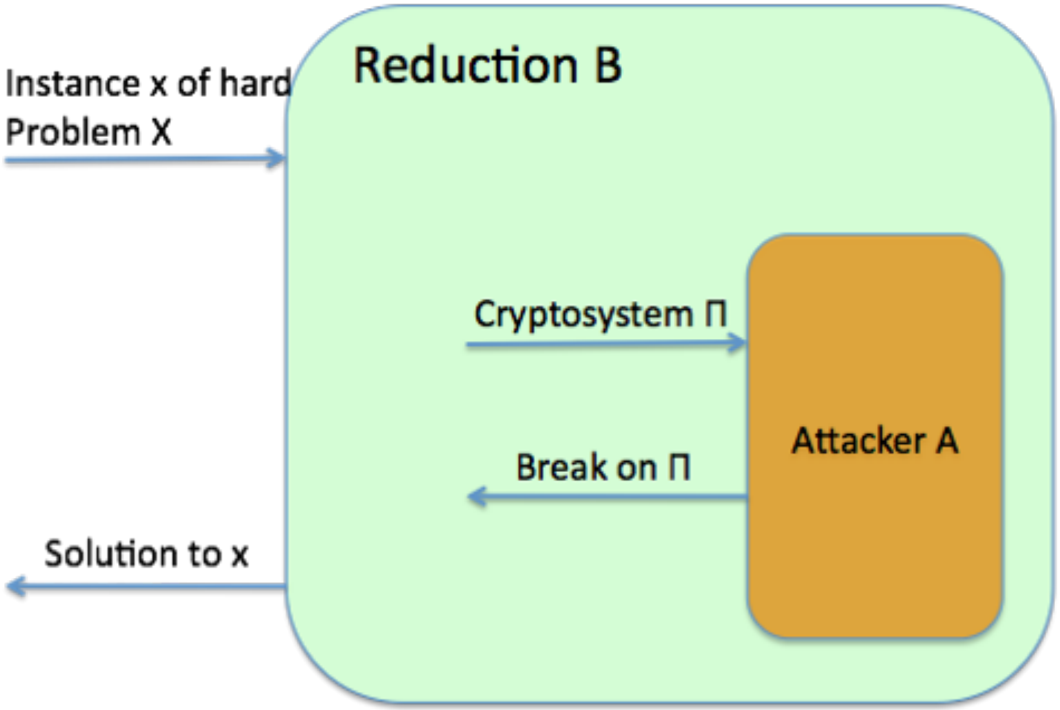
CS6115: Structure Vs Hardness in Cryptography

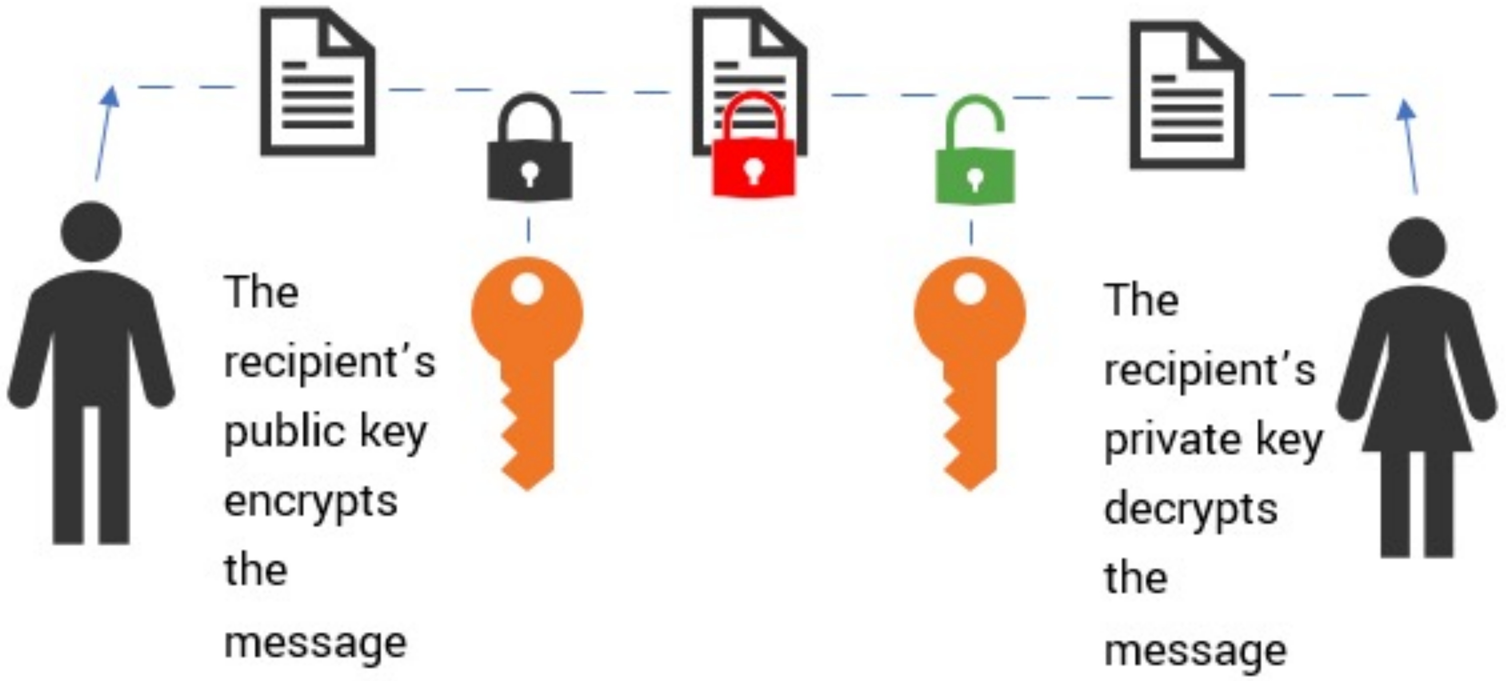
Shweta Agrawal
IIT Madras

Cryptography
The Art of Secret Keeping

Cryptography guarantees that breaking a cryptosystem is at least as hard as solving some difficult mathematical problem.



Case Study: Encryption



Functionality: Correctness of decryption
Security: Ciphertext looks uniformly random

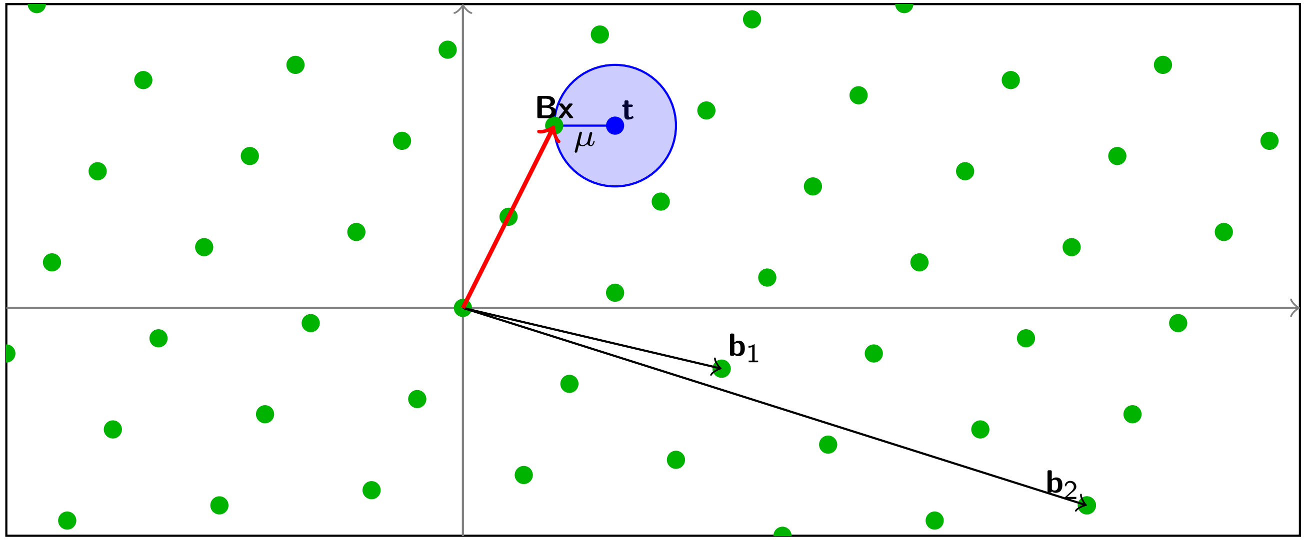
Walking the Fine Line

Want functionality together with security…
Any one without the other is easy – how?

Functionality + Security

- Functionality requires structure
- Security requires randomness

Closest Vector Problem on Lattices



Get both together from suitable hard problem in math

What is this course about?

- Study exciting recent progress in cryptography and mathematical assumptions that led to this progress.
- How do mathematical assumptions walk tightrope of structure and hardness?
- Are all assumptions "equal"? Yes and No!
- Study which assumption yields what cryptography
- In rare, fascinating examples, interplay/cooperation of assumptions
- Many open problems!

Pre-req: love for math and puzzles, working knowledge of algebra and probability. Prior experience in cryptography desirable but not necessary.

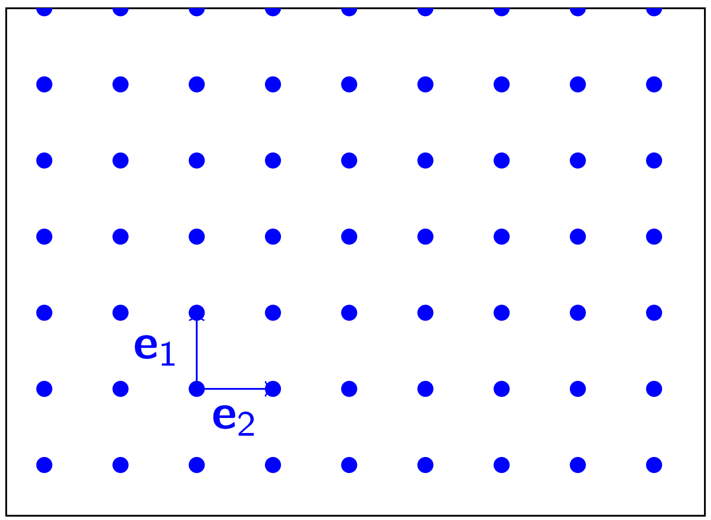
Course Requirements

- Assignments : 30%. Assignments will be open ended in nature and collaboration is encouraged.
- Two Scribes: 20%
- Class presentation : 20%
- Final Project: 30%

Highest ethical standards expected. Any dishonesty → F grade.

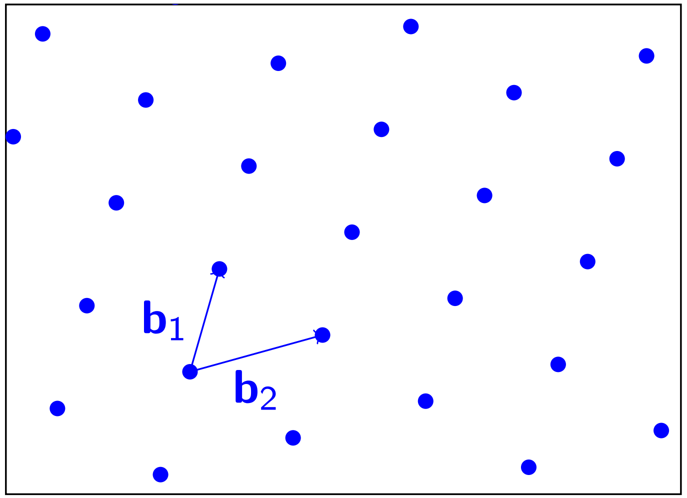
What is a lattice?

A set of points with periodic arrangement



The simplest lattice in n-dimensional space is the integer lattice

$$\Lambda = \mathbb{Z}^n$$



Other lattices are obtained by applying a linear transformation

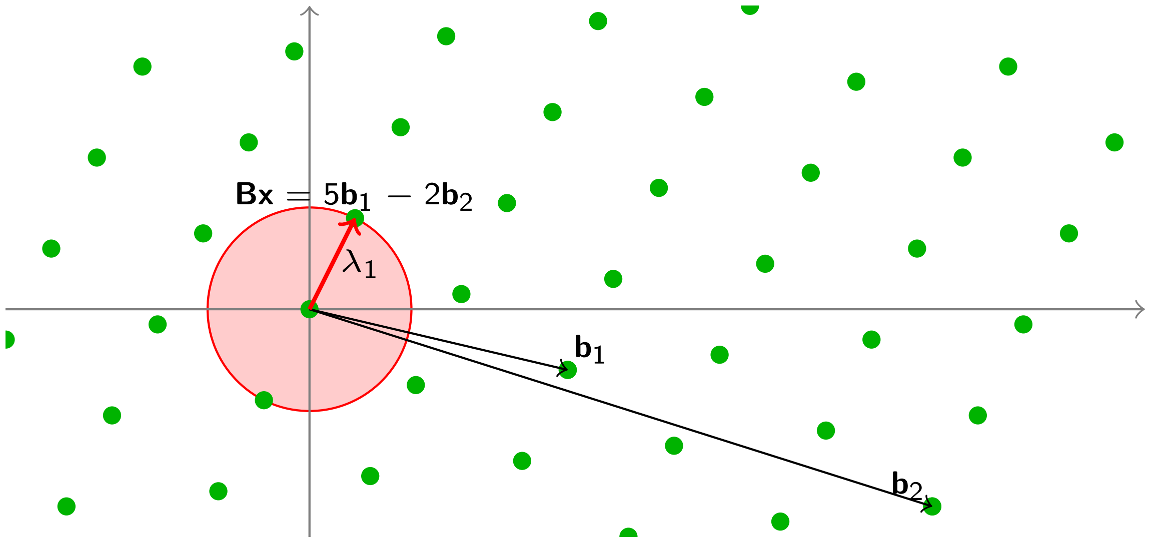
$$\Lambda = \mathbf{B}\mathbb{Z}^n \qquad (\mathbf{B} \in \mathbb{R}^{d \times n})$$

Discrete subgroup of R^n

Shortest Vector Problem

Definition (Shortest Vector Problem, SVP)

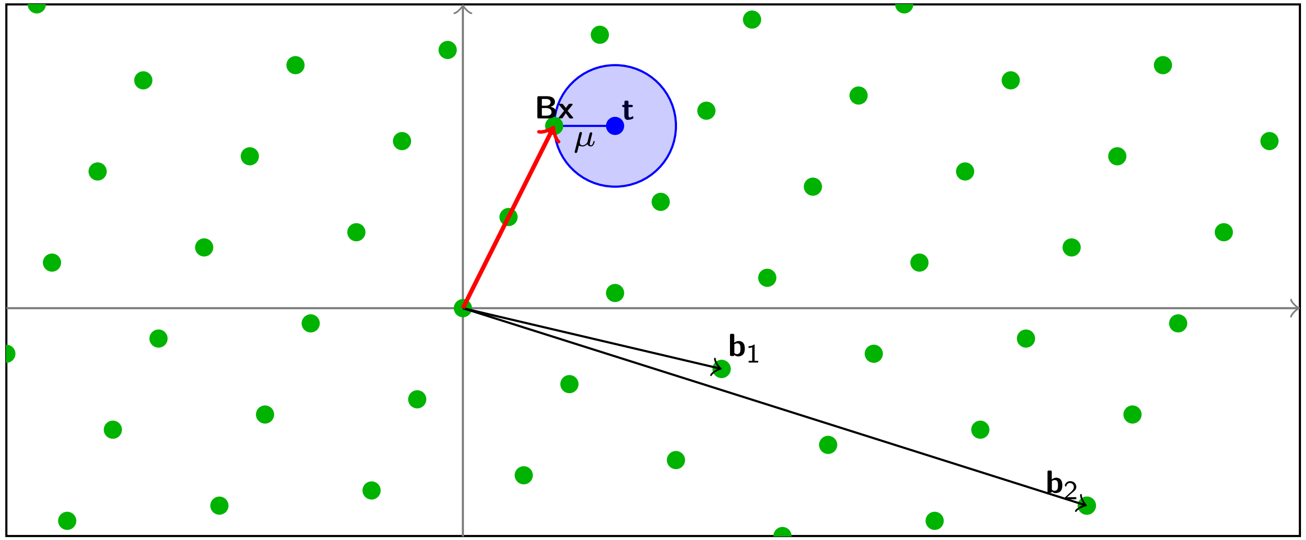
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \lambda_1$



Closest Vector Problem

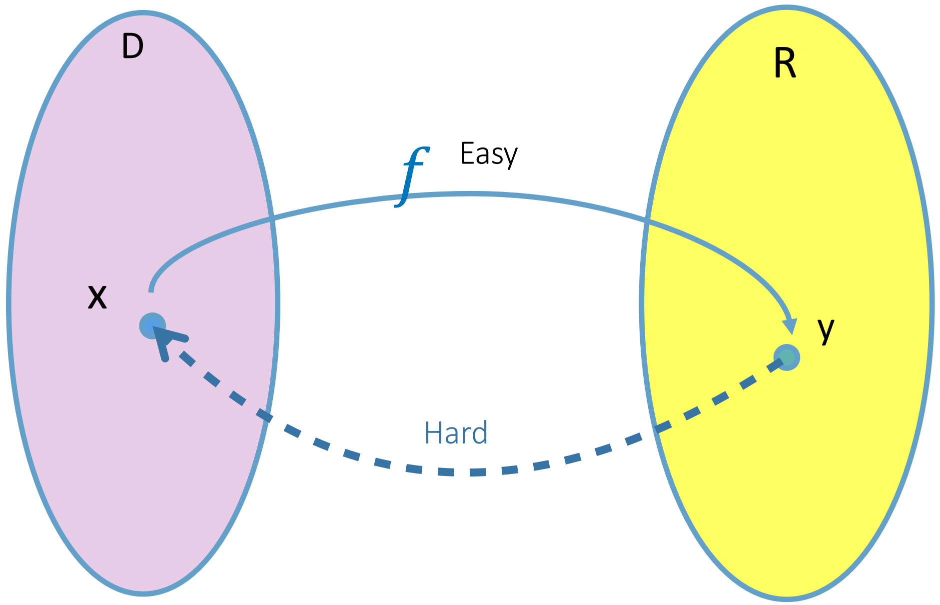
Definition (Closest Vector Problem, CVP)

Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \mu$ from the target



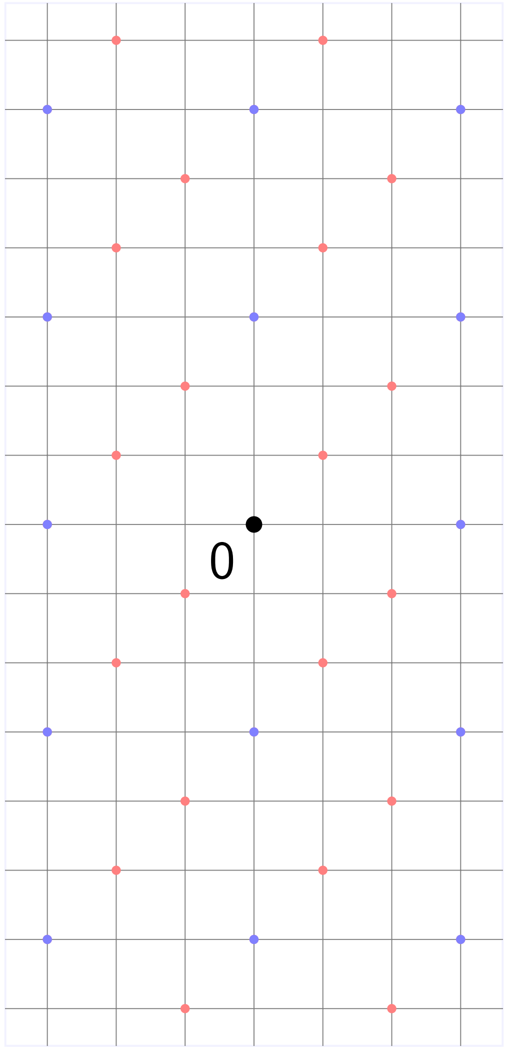
One Way Functions

$f: D \to R,$ One Way



Most basic "primitive" in cryptography!

Random Lattices in Cryptography



- Cryptography typically uses (random) lattices Λ such that
  - $\Lambda \subseteq \mathbb{Z}^d$ is an integer lattice
  - $q\mathbb{Z}^d \subseteq \Lambda$ is periodic modulo a small integer q.
- Cryptographic functions based on q-ary lattices involve only arithmetic modulo q.

Definition (q-ary lattice)

Λ is a q-ary lattice if $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$

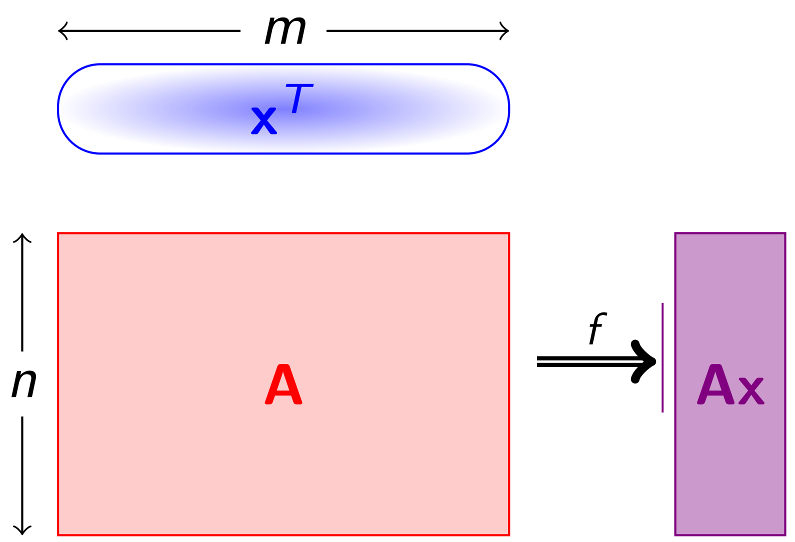
Examples (for any $\mathbf{A} \in \mathbb{Z}_q^{n\times d}$)

- $\Lambda_q(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{x} \bmod q \in \mathbf{A}^T\mathbb{Z}_q^n\} \subseteq \mathbb{Z}^d$
- $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\} \subseteq \mathbb{Z}^d$

Ajtai's One Way Function

- Parameters: $m, n, q \in \mathbb{Z}$
- Key: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$
- Input: $\mathbf{x} \in \{0,1\}^m$
- Output: $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$

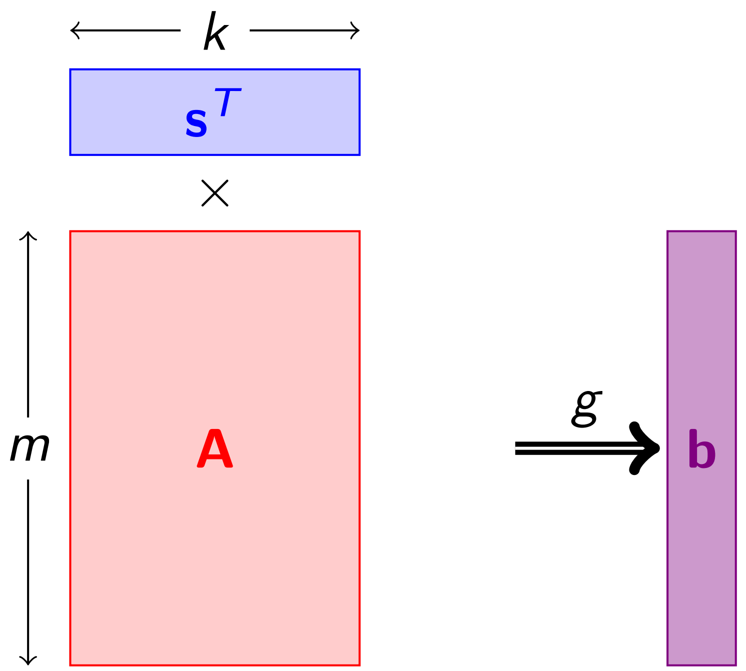
$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\}$$



Ajtai 96: For m > n log q, if lattice problems are hard to approximate in the worst case then $f_A(x)$ = A x mod q is a one way function.

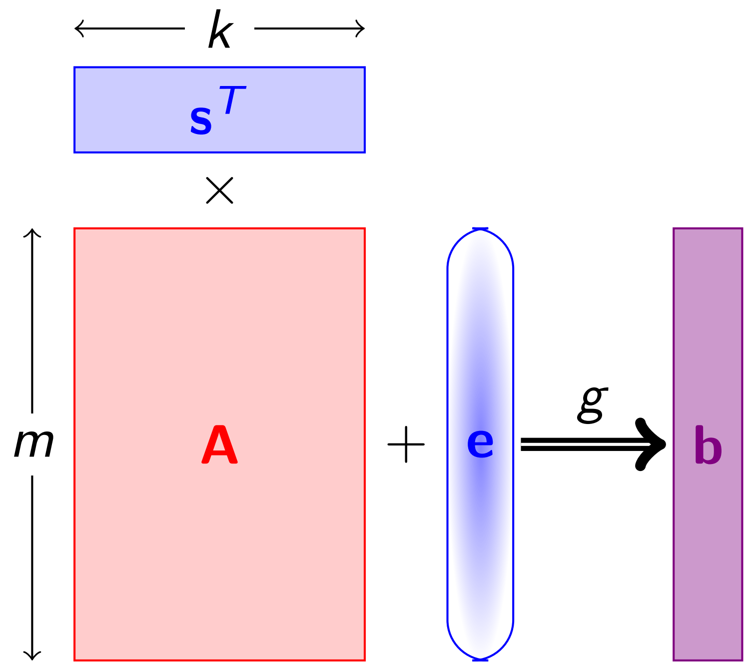
Regev's One Way Function

- $\mathbf{A} \in \mathbb{Z}_q^{m \times k}$, $\mathbf{s} \in \mathbb{Z}_q^k$, $\mathbf{e} \in \mathcal{E}^m$.
- $g_{\mathbf{A}}(\mathbf{s}) = \mathbf{A}\mathbf{s} \mod q$



Regev's One Way Function

- $\mathbf{A} \in \mathbb{Z}_q^{m \times k}$, $\mathbf{s} \in \mathbb{Z}_q^k$, $\mathbf{e} \in \mathcal{E}^m$.
- $g_{\mathbf{A}}(\mathbf{s}; \mathbf{e}) = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
- Learning with Errors: Given $\mathbf{A}$ and $g_{\mathbf{A}}(\mathbf{s}, \mathbf{e})$, recover $\mathbf{s}$.

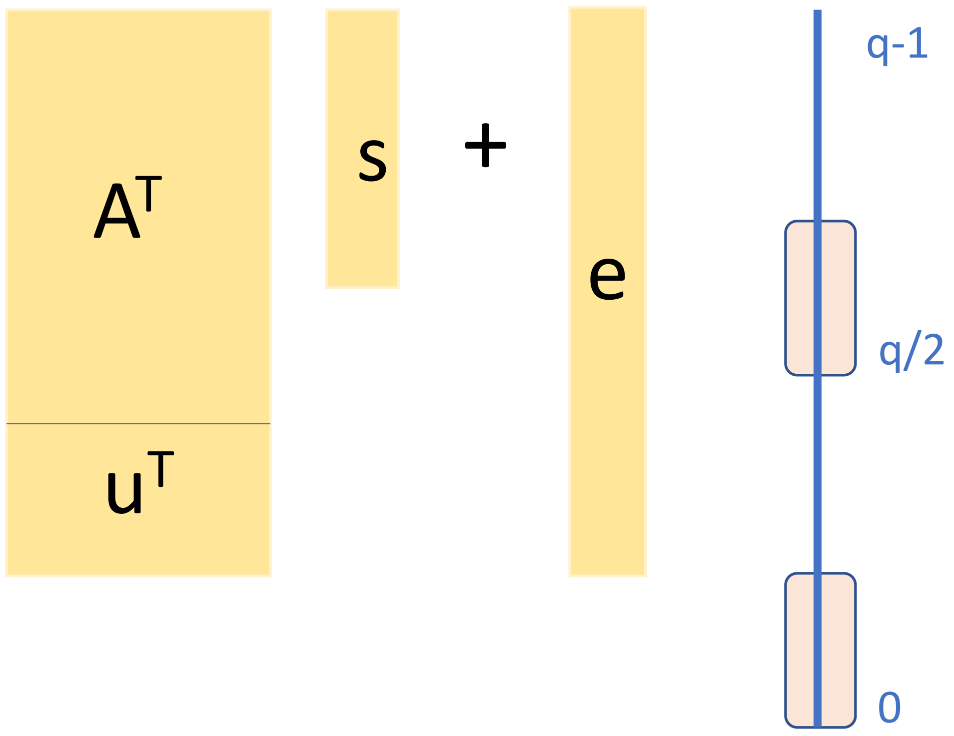


$$\Lambda_q(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{x} \bmod q \in \mathbf{A} * \mathbb{Z}_q^k\}$$

Regev 05: The function $g_A(s, e)$ is hard to invert on the average assuming lattice problems are hard to approximate in worst case

An Example Encryption Scheme

- Recall A (e) = u mod q hard to invert for short e
- Secret: e, Public : A, u
  - Encrypt (A, u) :
    - Pick random vector s
    - $c_0 = A^T s$ + noise
    - $c_1 = u^T s$ + noise' + q/2 msg
- Decrypt (e) :
    - $e^T c_0 - c_1$ = q/2 msg + noise

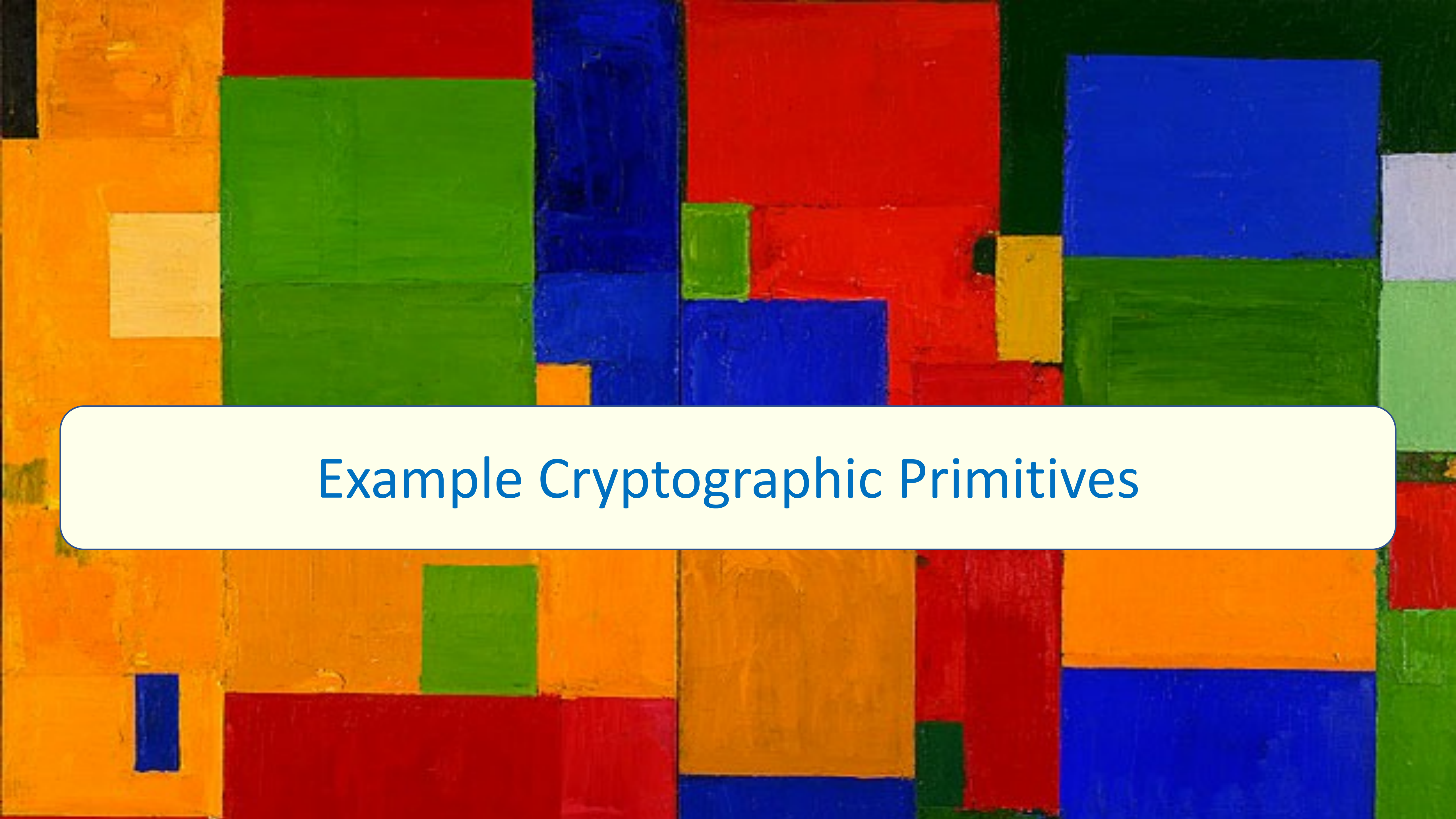


Indistinguishable from random!

Dancing the Dance

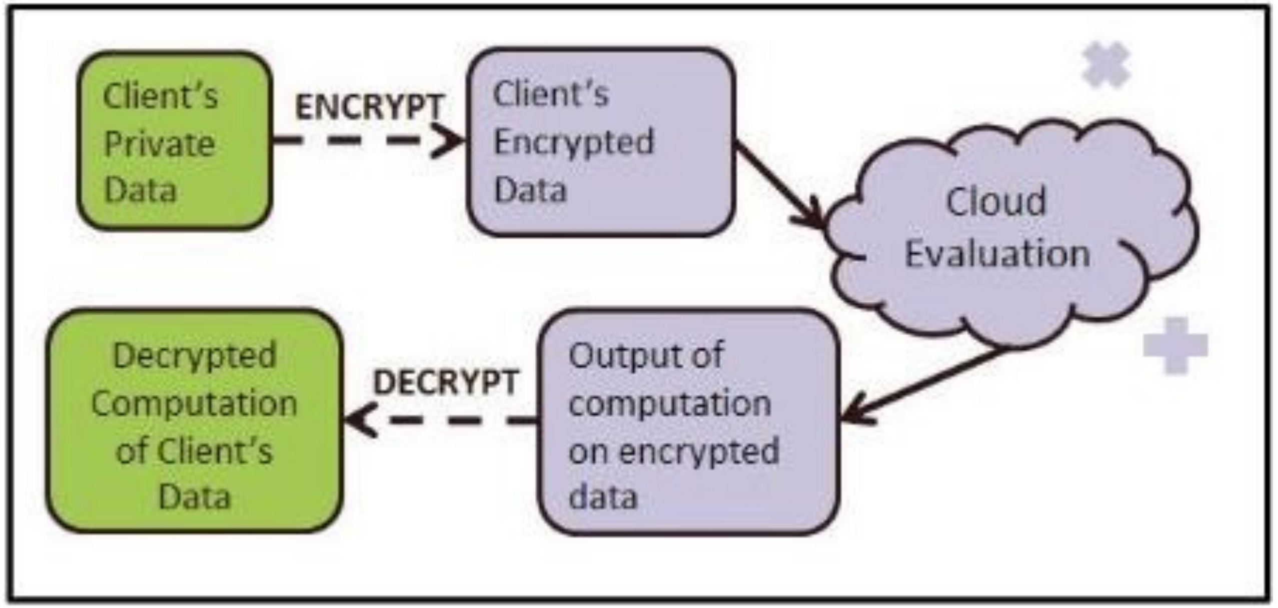
All of cryptography is a jugalbandi between

- correctness & security
- algorithms & complexity
- structure & randomness



Example Cryptographic Primitives

Fully Homomorphic Encryption
(G09, BV11, BGV12, GSW13···)

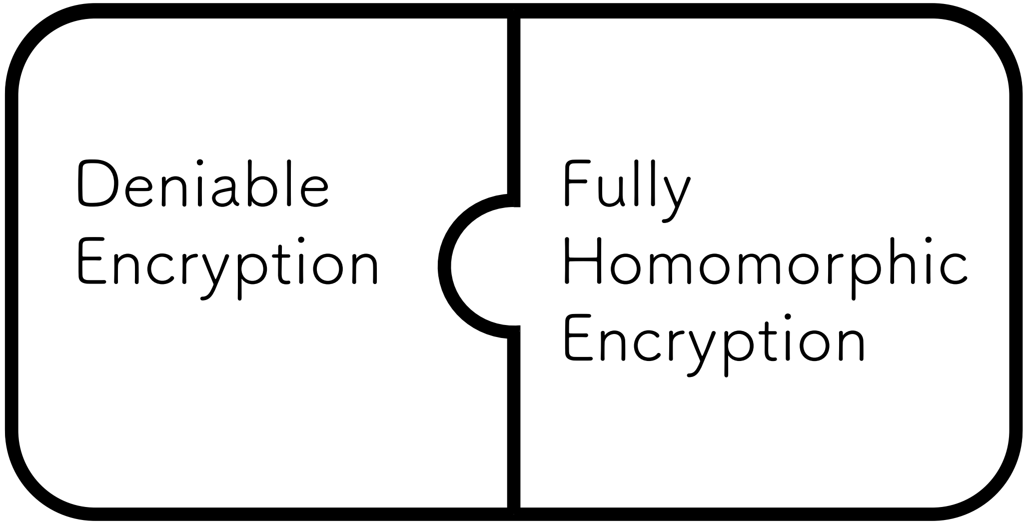


Expressive Functionality: Supports arbitrary circuits

Compact ciphertext, independent of circuit size

Encryption and function evaluation commute!
Enc(f(x)) =* f(Enc(x))

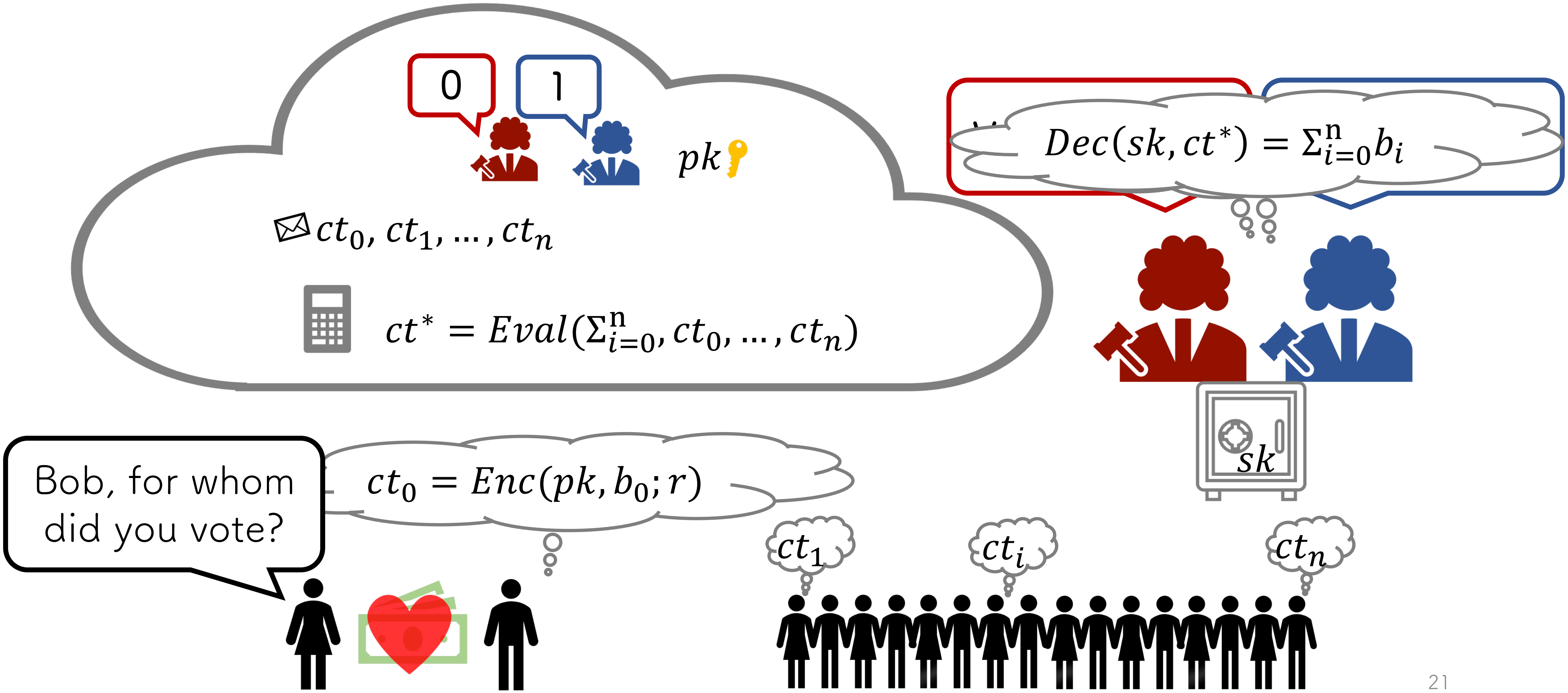
* : roughly



Deniable FHE

The notion of Deniable FHE

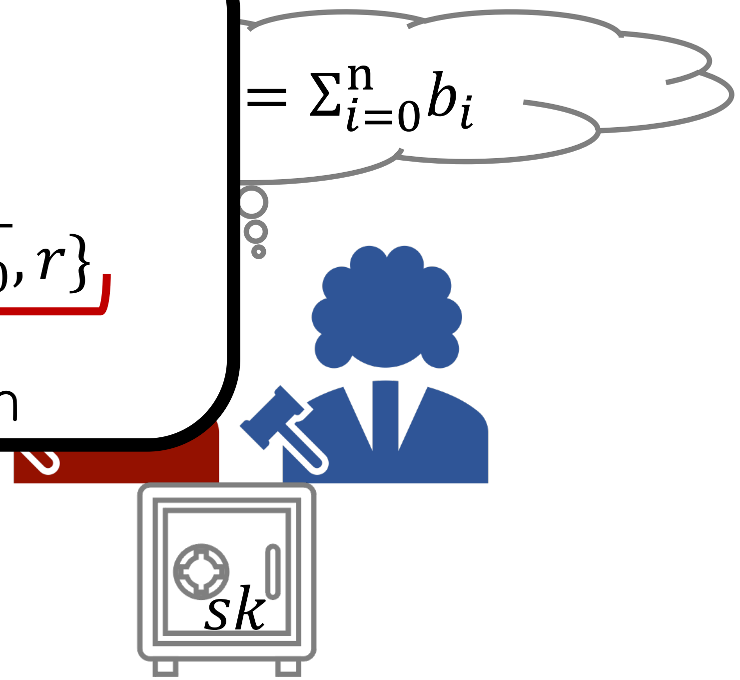
Deniable FHE (AGM21)

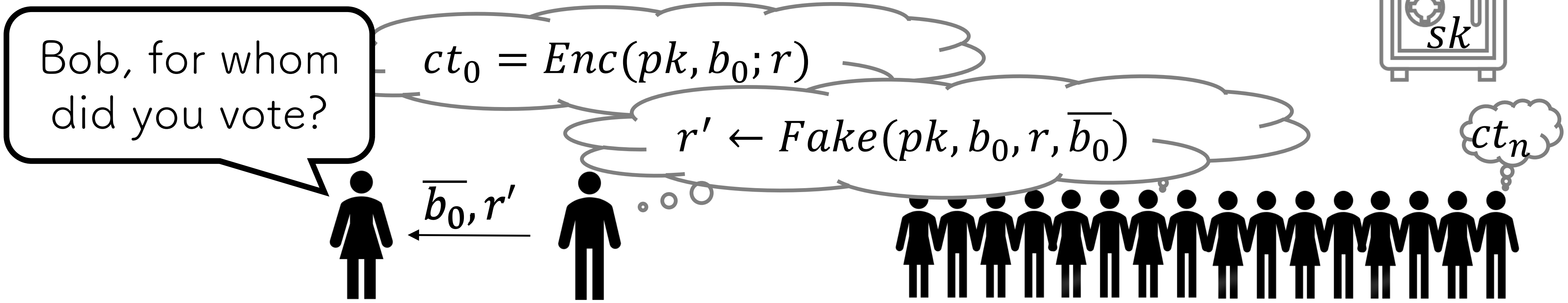


Deniable FHE

$$ct_0 = Enc(pk, b_0; r) = Enc(pk, \overline{b_0}; r')$$

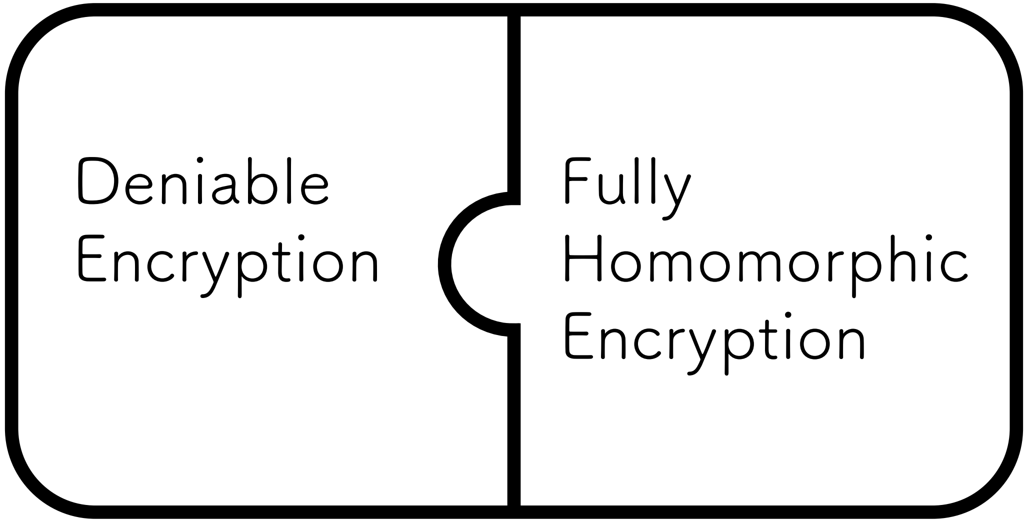
$$\underbrace{\{pk, Enc(pk, b_0; r), \overline{b_0}, r'\}}_{\text{“Fake” Distribution}} \approx_c \underbrace{\{pk, Enc\left(pk, \overline{b_0}; r\right), \overline{b_0}, r\}}_{\text{“Honest” Distribution}}$$





Deniable FHE

- A Deniable FHE scheme $(Gen, Enc, Eval, Dec, Fake)$
  - $(Gen, Enc, Eval, Dec)$ is an FHE scheme
  - $(Gen, Enc, Dec, Fake)$ is a Deniable Encryption scheme

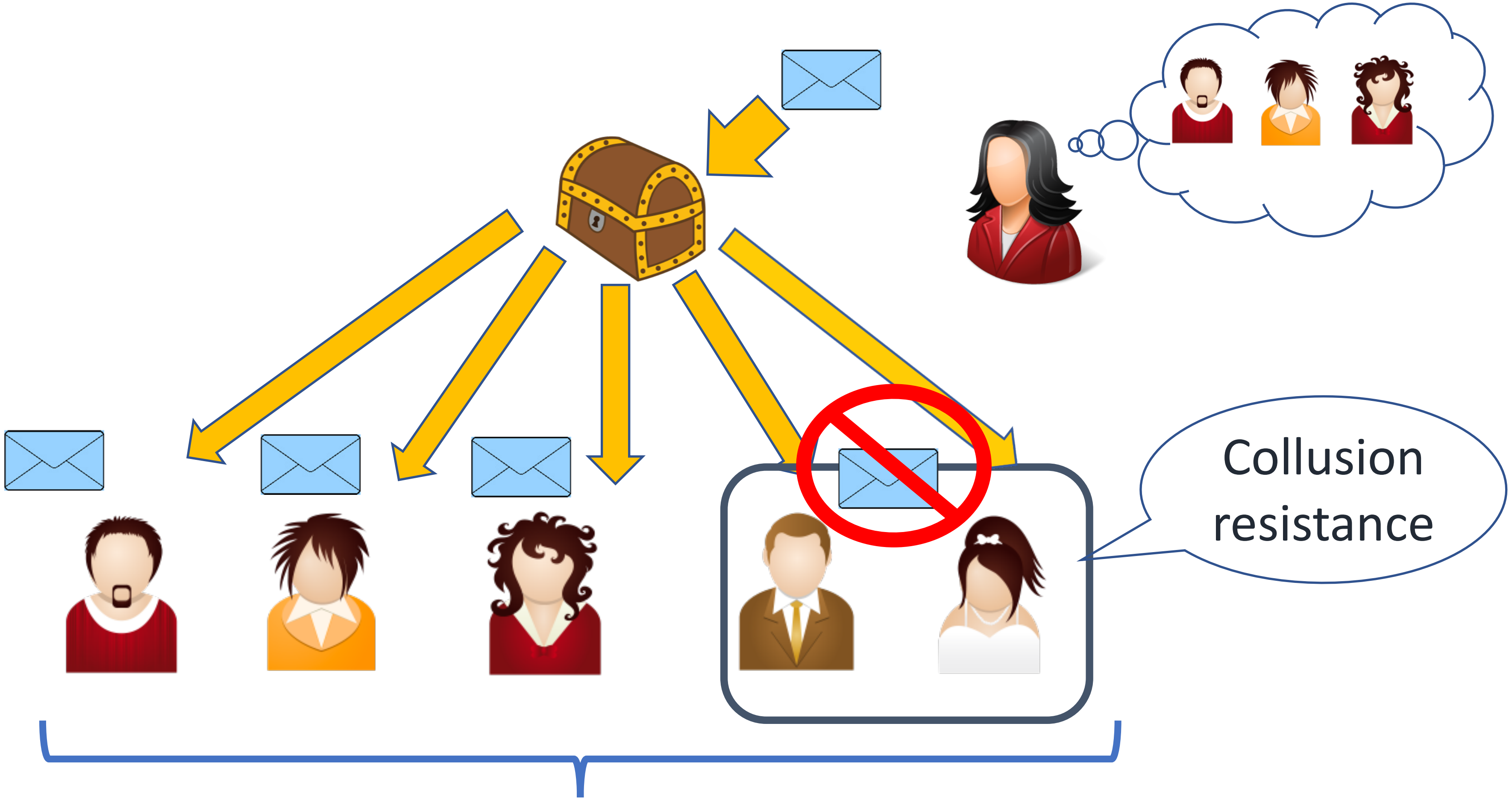


Deniable FHE

A Deniable FHE scheme $(Gen, Enc, Eval, Dec, Fake)$ syntax

- $Gen \rightarrow (pk, sk)$
- $Enc(pk, m; r) = ct$
- $Dec(sk, ct) = b$
- $Eval(pk, f, ct_1, \ldots, ct_k) = ct^*$
- $Fake(pk, b, r, \bar{b}) \rightarrow r'$

Broadcast Encryption



All users in the system
(# of users = N)

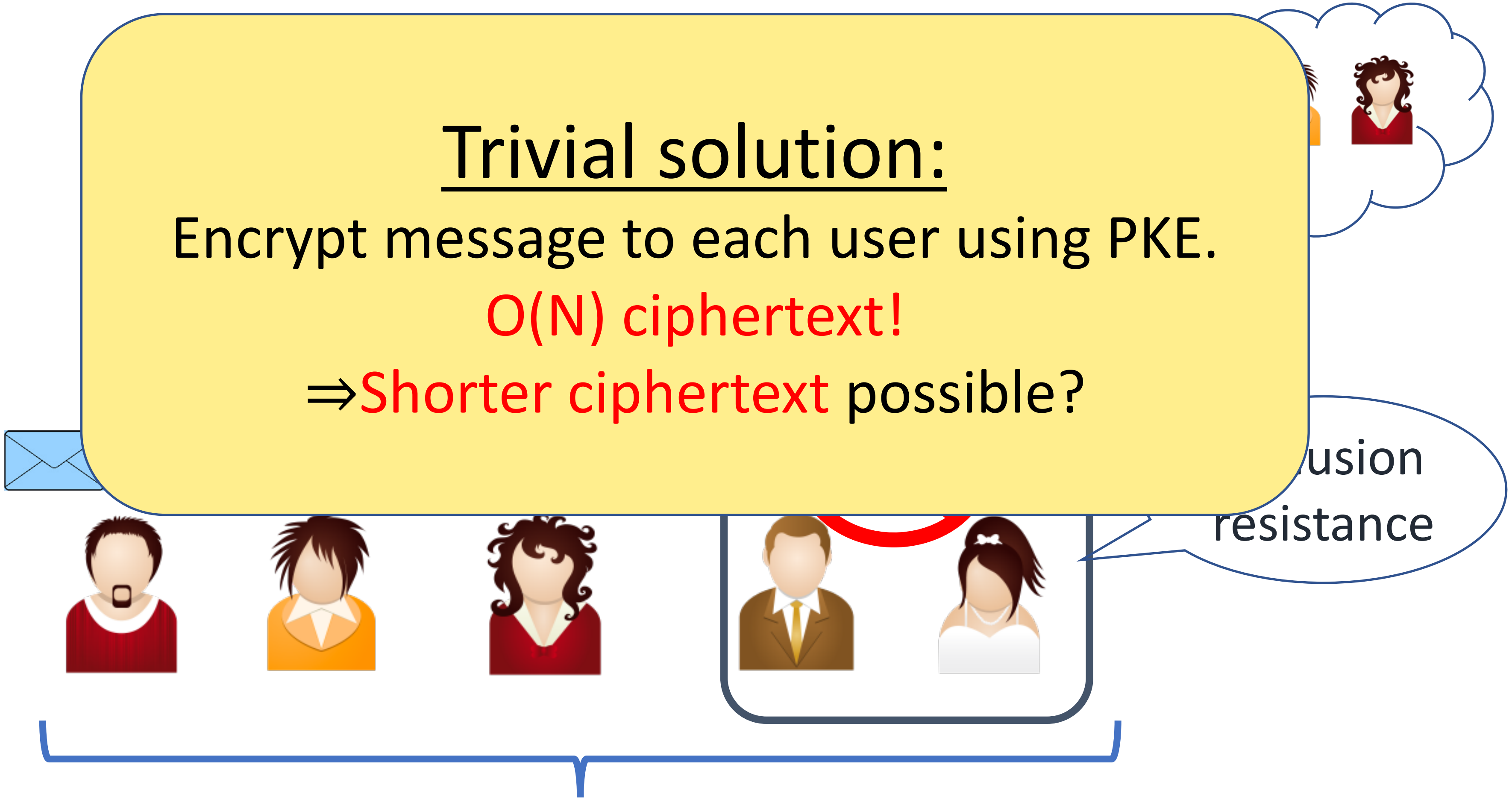
Broadcast Encryption

<u>Trivial solution:</u>

Encrypt message to each user using PKE.

O(N) ciphertext!

⇒Shorter ciphertext possible?



All users in the system
(# of users = N)

Hardness Assumptions

Sources of Hardness

- Algebra: eg SVP, CVP etc
- Number Theory: eg factoring, DDH etc
- Algebraic Geometry: Elliptic curve groups with pairings
- Complexity theoretic: one-way functions … Indistinguishability Obfuscation
- Quantum computation: entanglement!
- Statistical Physics etc…

Will study <u>some</u> assumptions from perspective of how they yield crypto

What about NP Hardness?

The Many Worlds of Impagliazzo

The Many Worlds of Hardness

- World 1: Algorithmica P=NP or NP$\subseteq$BPP
- World 2: Heuristica P$\neq$NP, but finding hard problems is hard. Average-case easy
- World 3: Pessiland P$\neq$NP AND average-case hard.

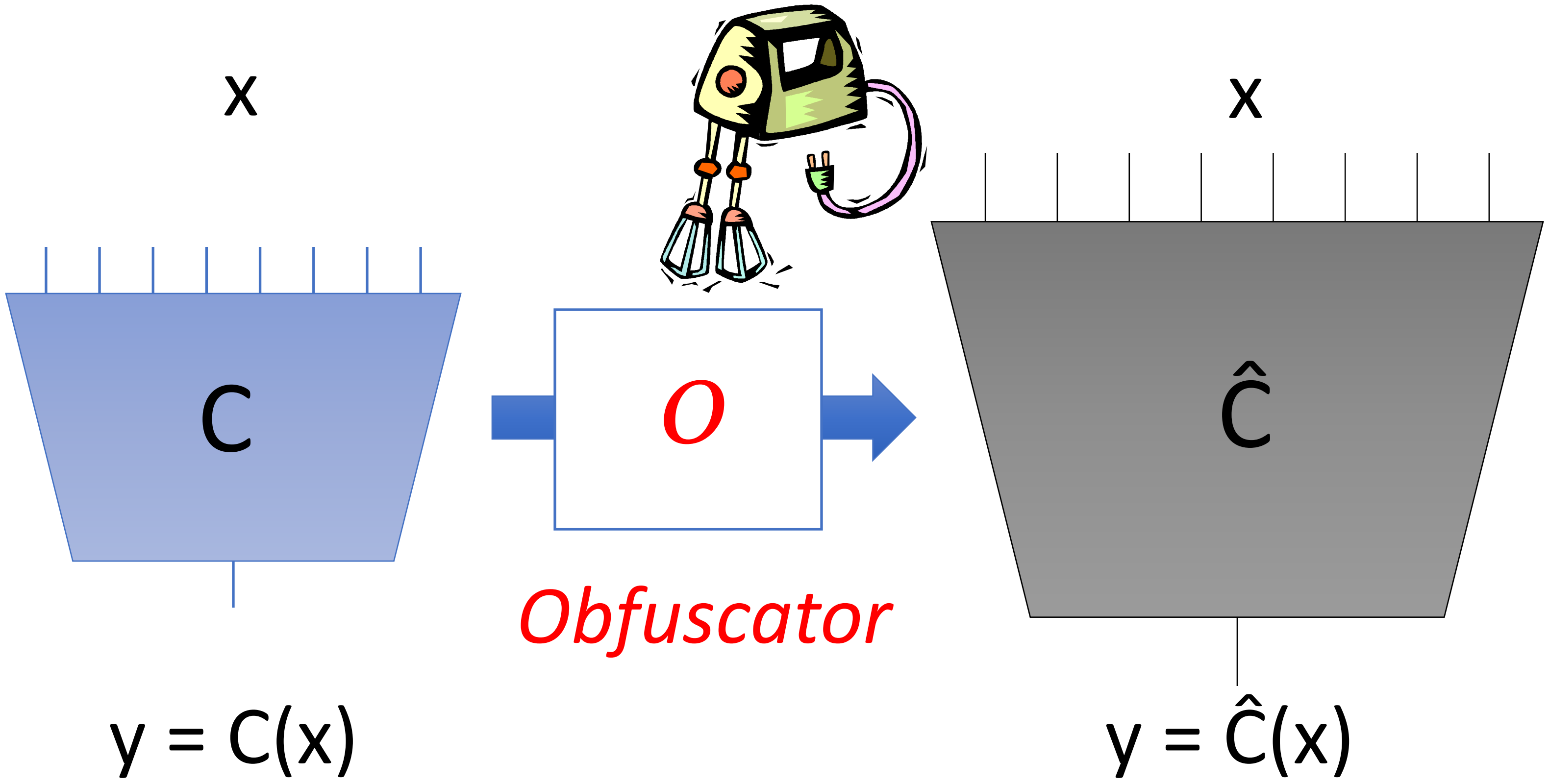
  But, no one way functions (OWF)
- World 4: Minicrypt, OWF exist. SKE implied
- World 5: Cryptomania, PKE exists
- World 6: Obfustopia, iO exists

Which world do we live in? We have no idea! ☺

We conjecture: Obfustopia

Indistinguishability Obfuscator *iO* [BGI+01]

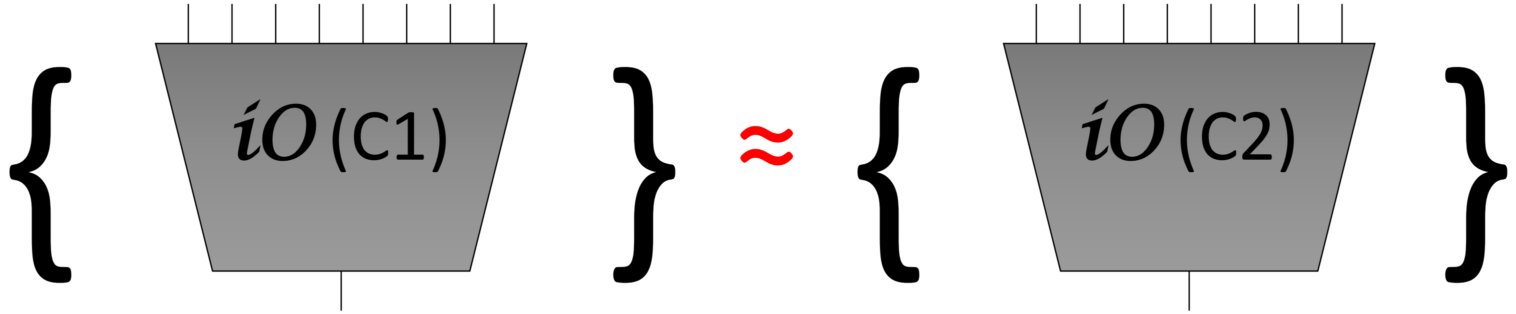
Compile a circuit/TM C into one Ĉ that *preserves functionality,*
and is unintelligible (resistant to reverse engineering)



Indistinguishability Obfuscator *iO* [BGI+01]

Hard: *"Which one of two equivalent circuits $C_1 \equiv C_2$ is obfuscated?"*

$C_1 \equiv C_2$, meaning
- Same size $|C_1|=|C_2|$
- Same truth table $TB(C_1) = TB(C_2)$



Trivial, if efficiency is not an issue

Nontrivial, if efficiency is desired

Indistinguishability Obfuscator $i\mathcal{O}$ [BGI+01]

Hard: *"Which one of two equivalent circuits $C_1 \equiv C_2$ is obfuscated?"*

$C_1 \equiv C_2$, meaning

- Same size $|C_1|=|C_2|$
- Same truth table $TB(C_1) = TB(C_2)$

$$\{\, i\mathcal{O}(C1) \,\} \approx \{\, i\mathcal{O}(C2) \,\}$$

Quest: Finding an efficient compiler $i\mathcal{O}$

We'll take scenic route!

- Ask interesting questions
  - Different assumptions?
  - Post-Quantum?
  - More efficient?

- Explore relationships between assumptions
  - New ways to co-operate

- Always open to topics/ideas/detours