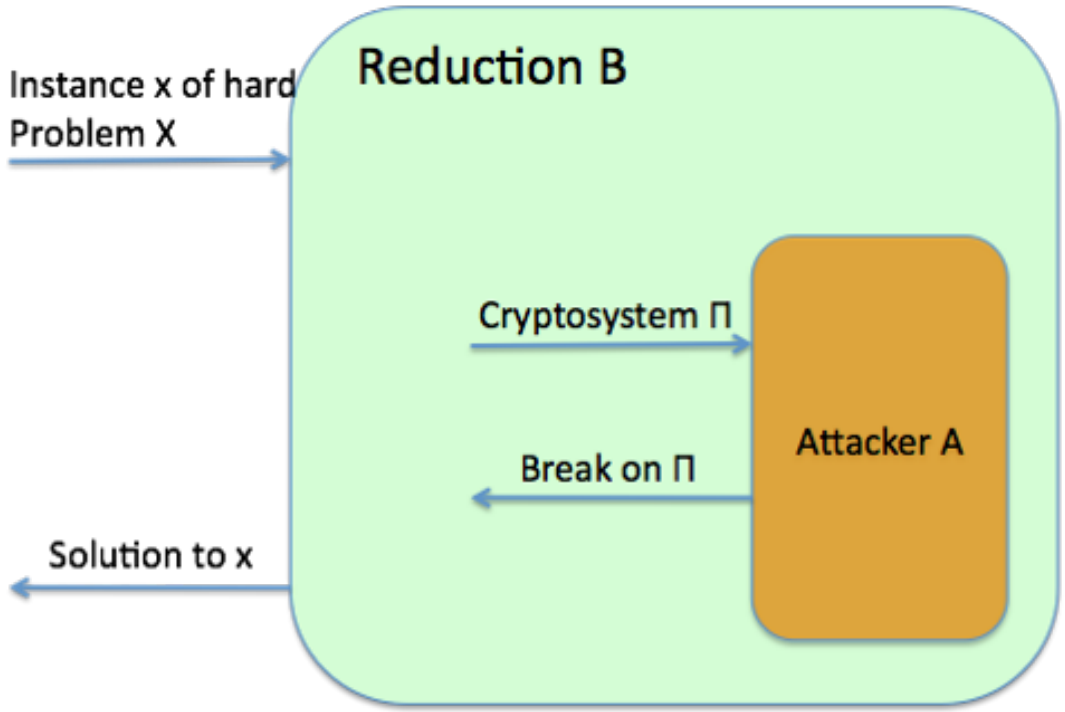
Cryptography: The Jugalbandi of Structure and Randomness

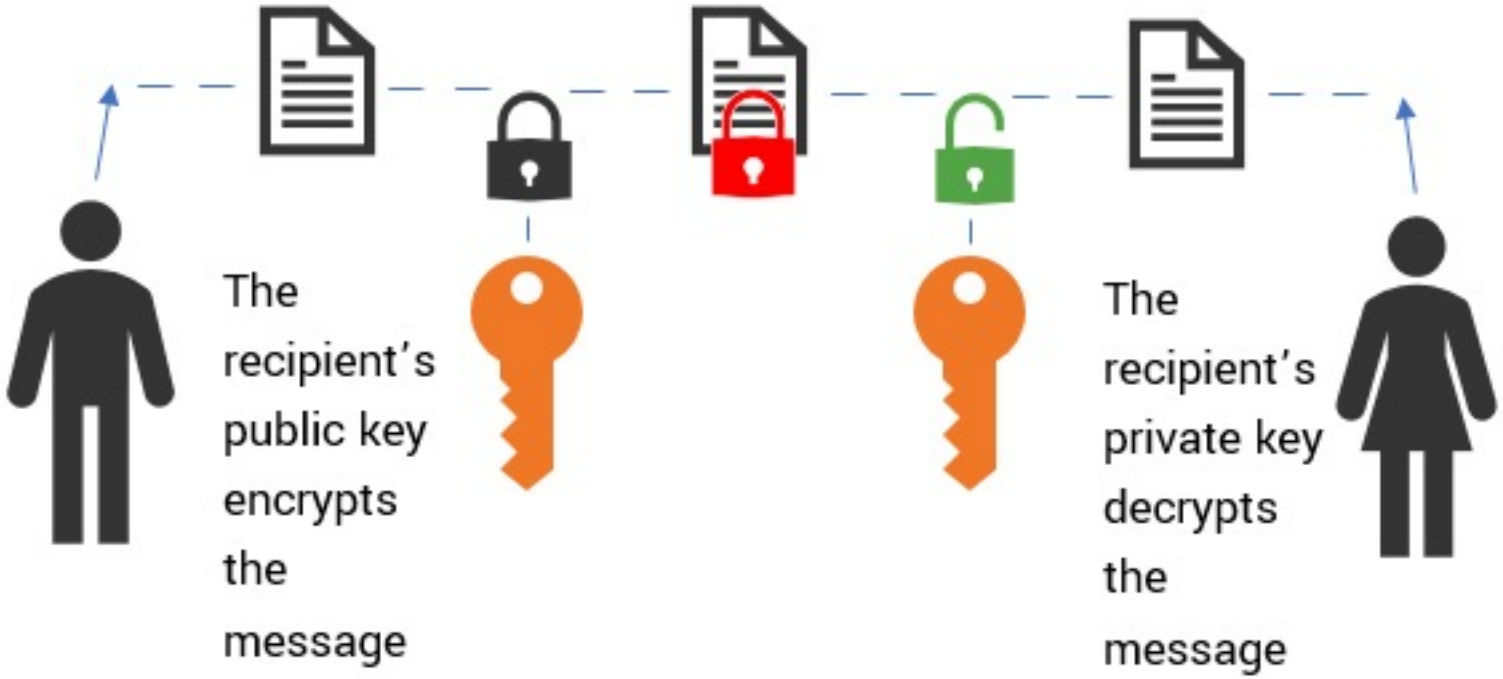
Shweta Agrawal
IIT Madras

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

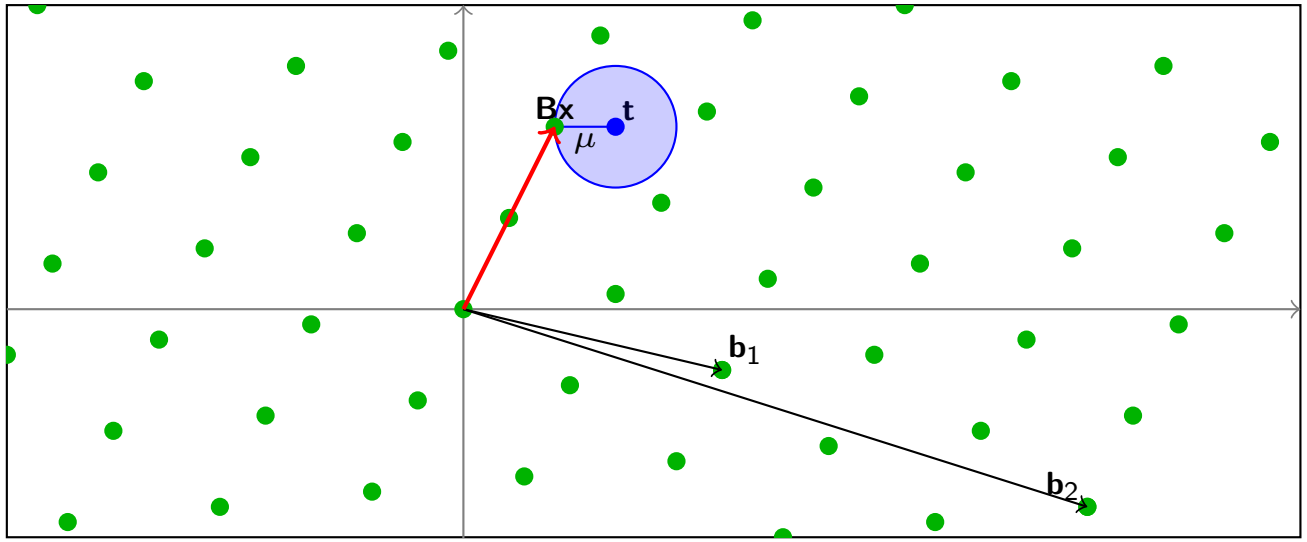
Walking the Fine Line

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

Functionality + Security

- Functionality requires structure
- Security requires randomness

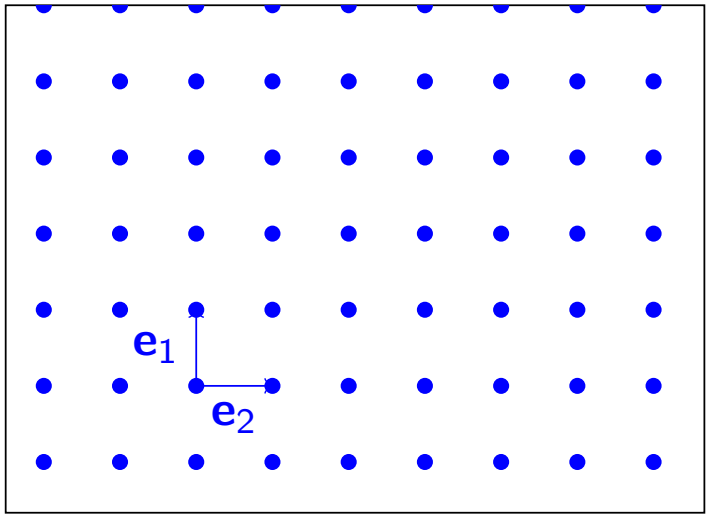
Closest Vector Problem on Lattices



Get both together from suitable hard problem in math

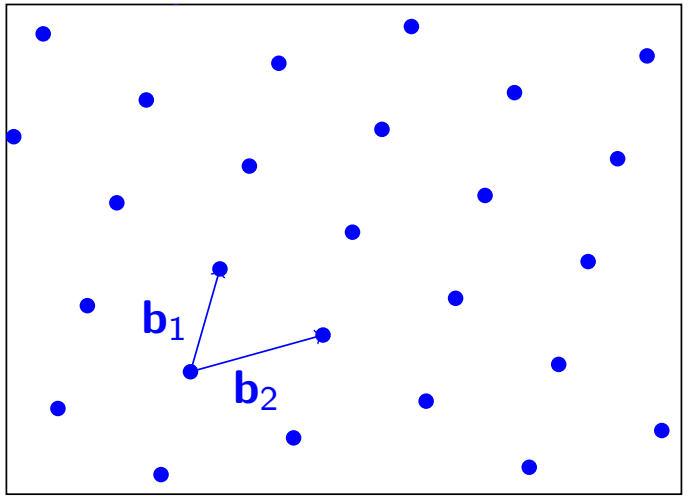
What is a lattice?

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

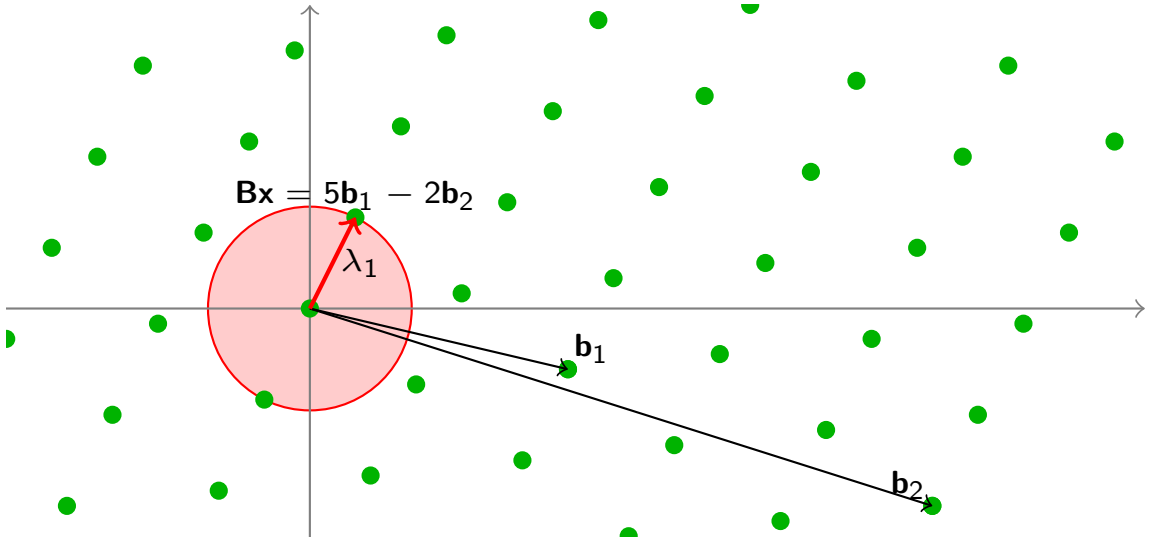
$$\Lambda = \mathbf{B}\mathbb{Z}^n \qquad (\mathbf{B} \in \mathbb{R}^{d \times n})$$

Discrete subgroup of R^n

Shortest Vector Problem

Definition (Shortest Vector Problem, SVP)

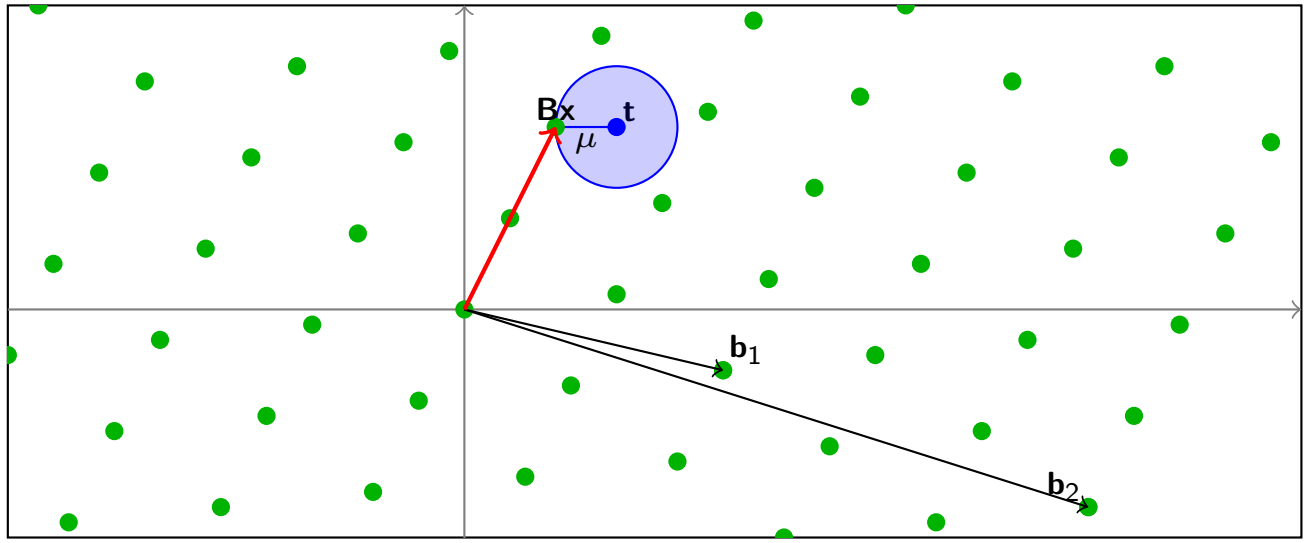
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \lambda_1$



Closest Vector Problem

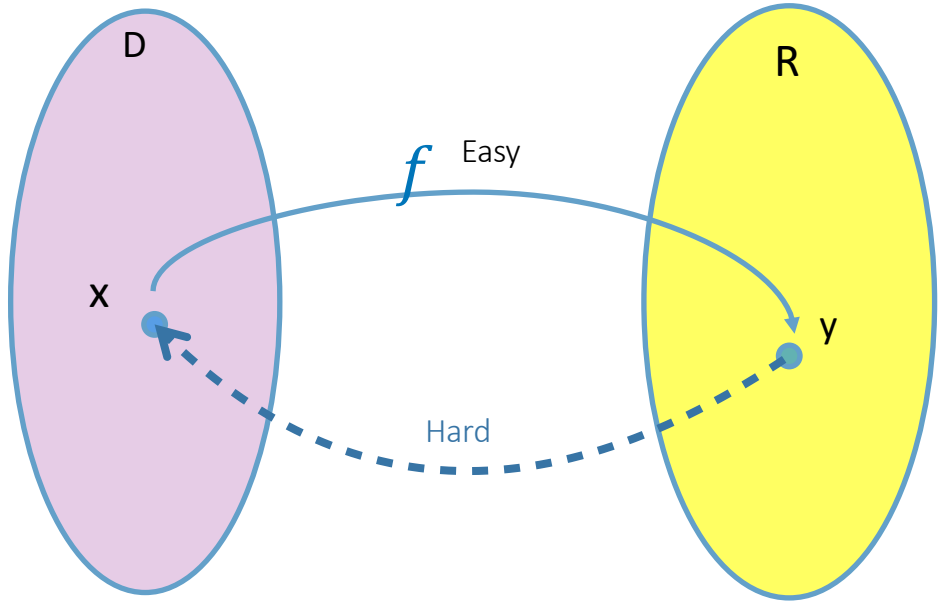
Definition (Closest Vector Problem, CVP)

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



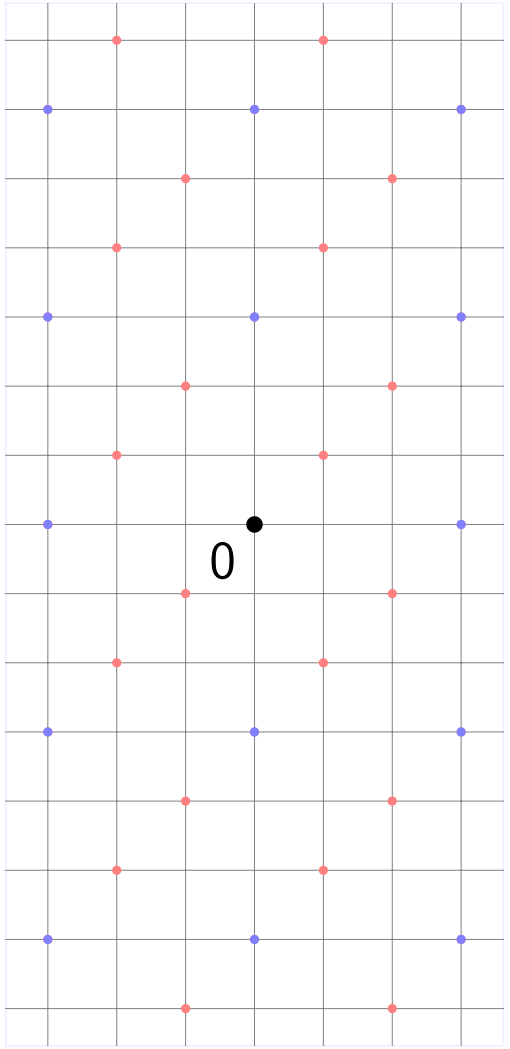
One Way Functions

$f: D \to R$, 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 $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$

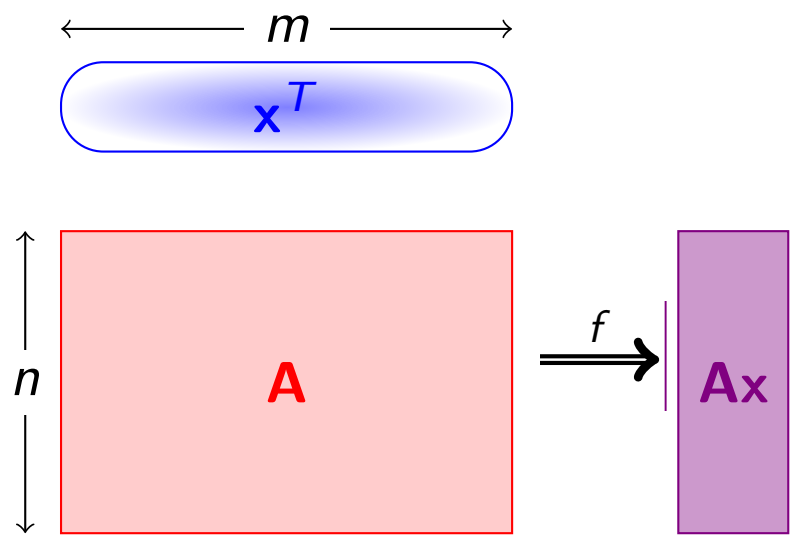
Examples (for any $\mathbf{A} \in \mathbb{Z}_q^{n \times d}$)

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

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: $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$

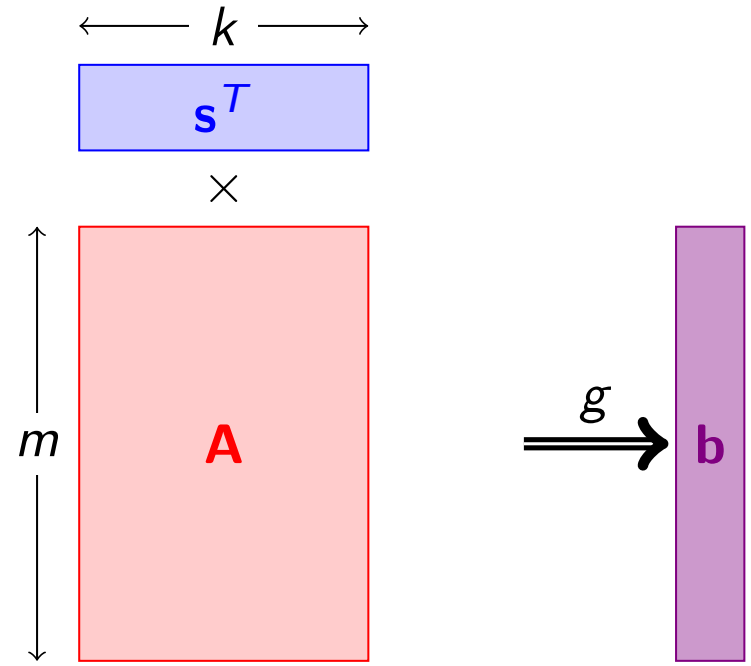
$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\}$$



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

Regev's One Way Function

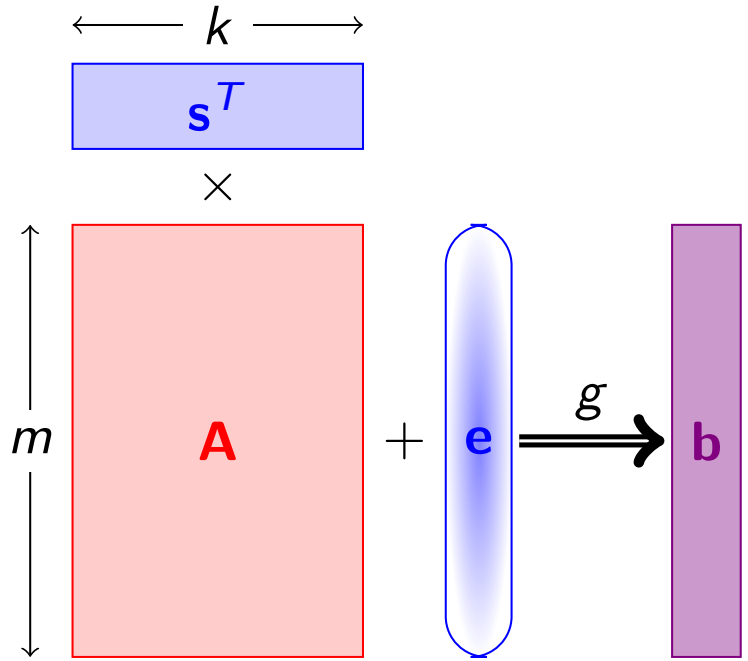
- $\mathbf{A} \in \mathbb{Z}_q^{m \times k}$, $\mathbf{s} \in \mathbb{Z}_q^k$, $\mathbf{e} \in \mathcal{E}^m$.
- $g_{\mathbf{A}}(\mathbf{s}\quad) = \mathbf{As}\qquad \bmod q$



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 $\mathbf{s}$.

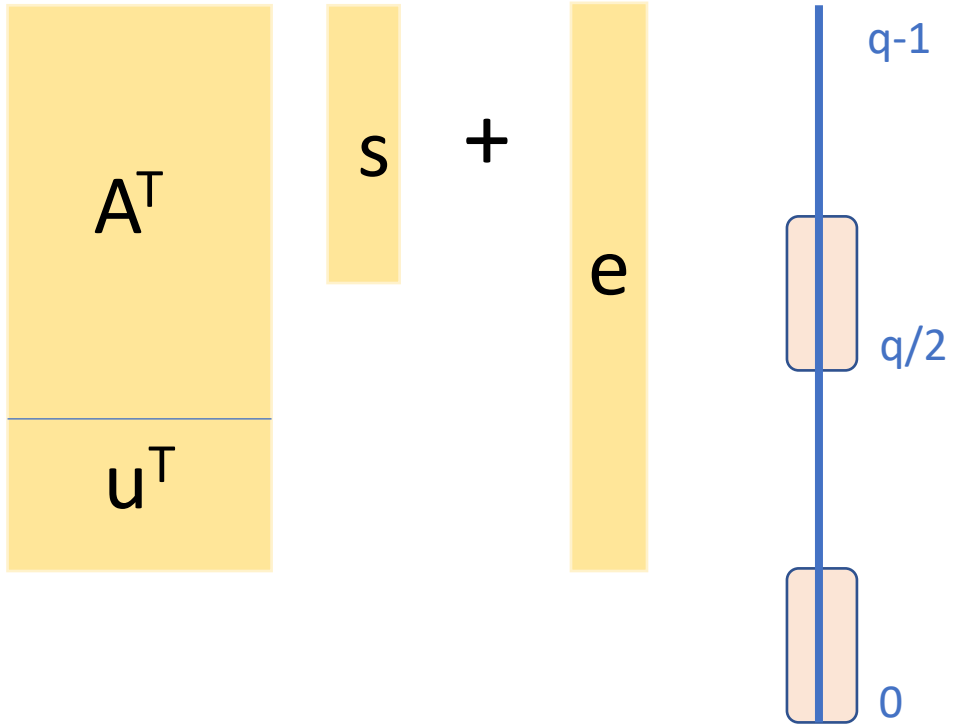
$$\Lambda_q(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{x} \bmod q \in \mathbf{A} * \mathbb{Z}_q^k\}$$



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

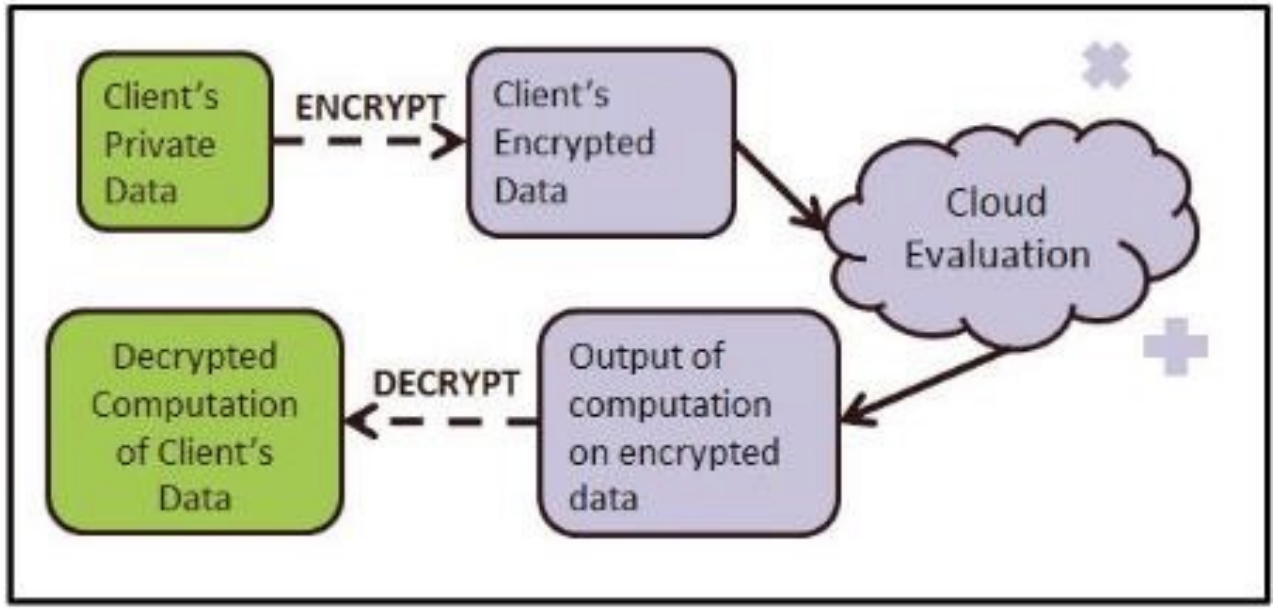
An Example Encryption Scheme

- Recall A (e) = u mod q hard to invert for short e
- Secret: e, Public : A, u
  - Encrypt (A, u) :
    - Pick random vector s
    - $c_0 = A^T s + \text{noise}$
    - $c_1 = u^T s + \text{noise} + q/2\ \text{msg}$
  - Decrypt (e) :
    - $e^T c_0 - c_1 = q/2\ \text{msg} + \text{noise}$



Indistinguishable from random!

Can be made Fully Homomorphic!
(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

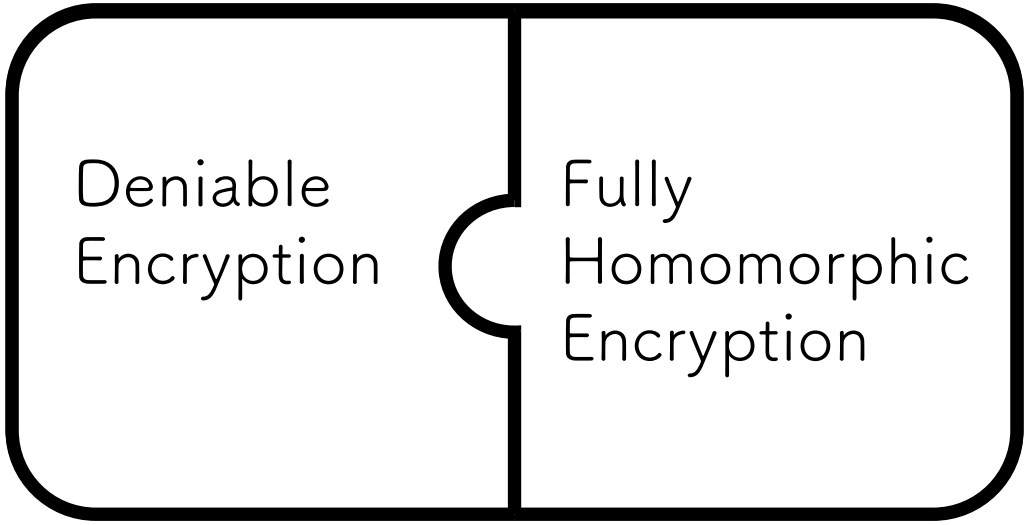
Dancing the Dance

All of cryptography is a jugalbandi between

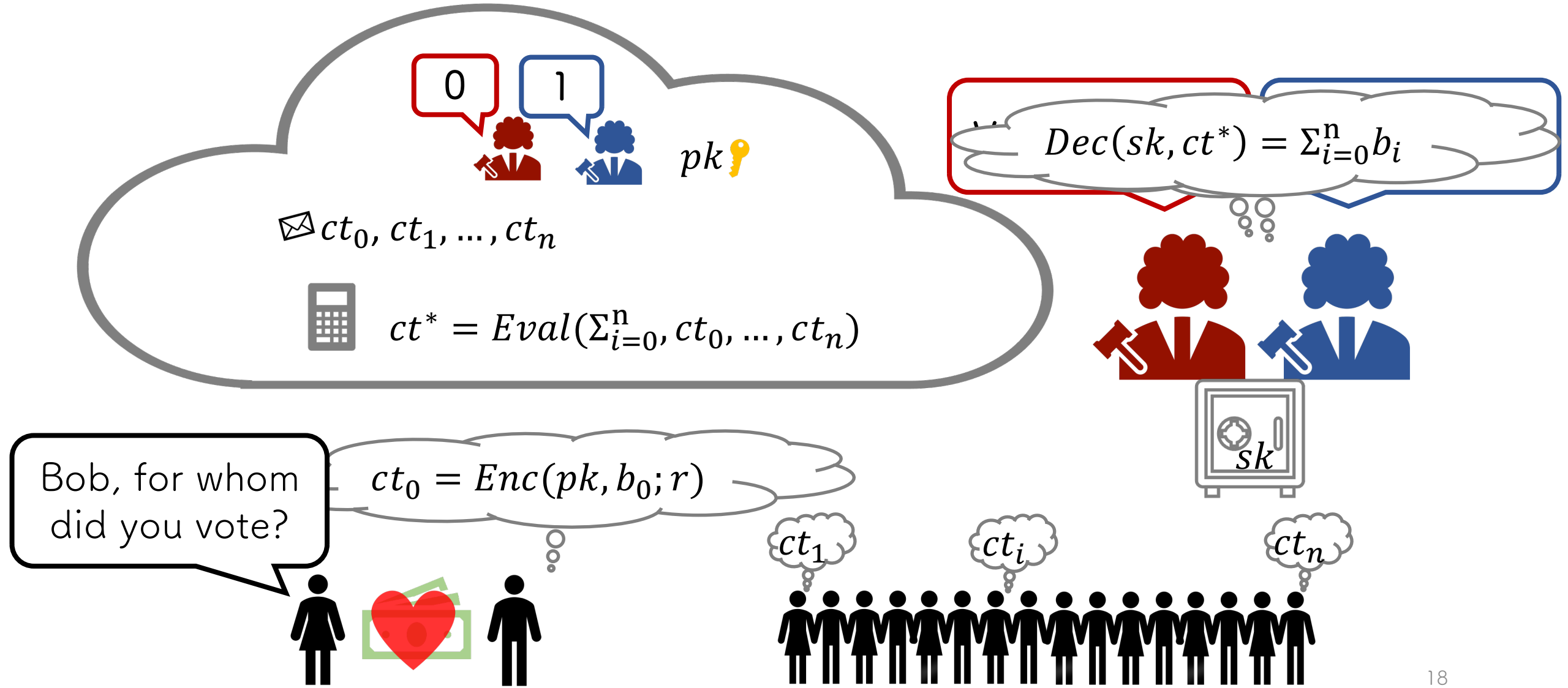
- correctness & security
- algorithms & complexity
- structure & randomness

Deniable FHE

The notion of Deniable FHE



Deniable FHE (AGM21)



Deniable FHE

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

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

"Fake" Distribution

"Honest" Distribution

$= \Sigma_{i=0}^{n} b_i$

sk

Bob, for whom did you vote?

$ct_0 = Enc(pk, b_0; r)$

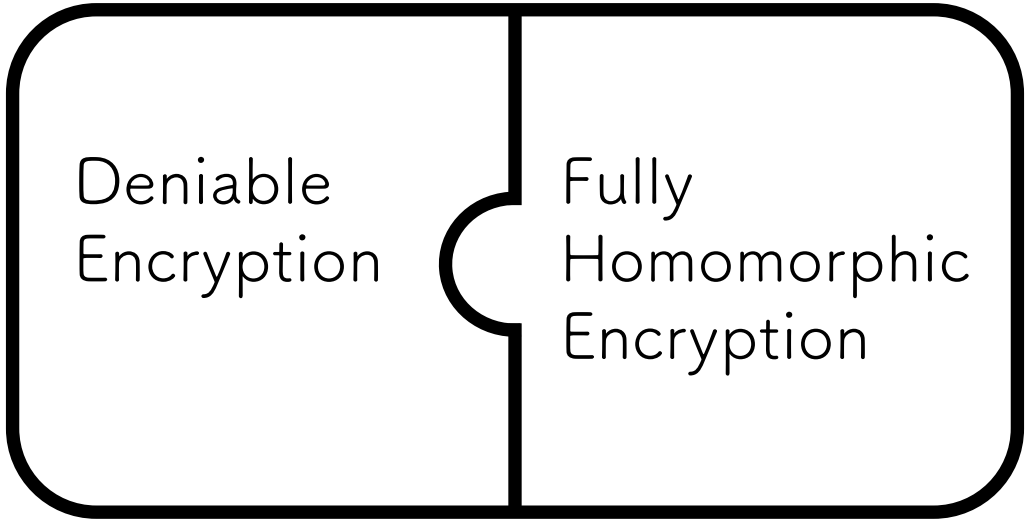
$r' \leftarrow Fake(pk, b_0, r, \overline{b_0})$

ct_n

$\overline{b_0}, r'$

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



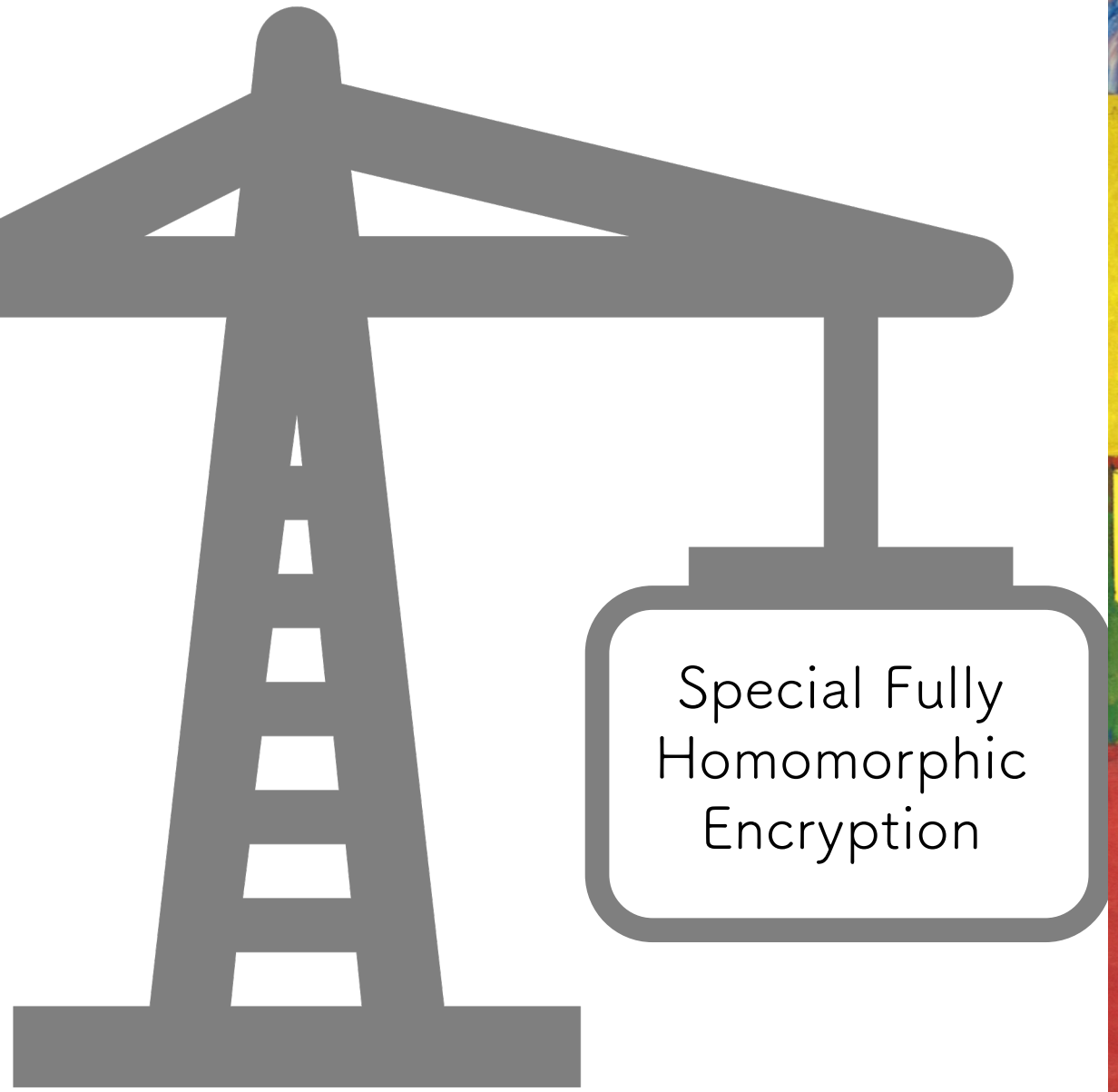
Deniable FHE

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

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

Deniable FHE

Our Construction of Deniable FHE



FHE: A Very Brief Recap

- All known FHE schemes add noise in CT for security.
- Homomorphic evaluation of CTs (eval(f, $ct_1 \cdots ct_n$)) cause noise to grow
- Kills correctness after noise grows too much
- Limits number of homomorphic operations

How to keep going: Gentry's bootstrapping [Gen09]!

The Magic of Bootstrapping

- Assume that an encryption scheme is powerful enough to support evaluation of its own decryption circuit Dec.

- By correctness of decryption, $\mathrm{Dec}(\mathrm{ct}_x, \mathrm{sk}) = x$

$$\mathrm{Dec}\left(x \;, \mathrm{sk} \right) = x$$

- Define circuit $\mathrm{Dec}_{\mathrm{ct}}(\mathrm{sk}) = \mathrm{Dec}(\mathrm{sk}, \mathrm{ct})$
- By correctness of homomorphic evaluation, $\mathrm{Eval}(F, \mathrm{ct}_x) = \mathrm{ct}(F(x))$

$$\mathrm{Eval}\left(\mathrm{Dec}_{\mathrm{ct}} , \mathrm{sk} \right) = \mathrm{Dec}_{\mathrm{ct}}(\mathrm{sk}) = x$$

The Magic of Bootstrapping

- Originally introduced to reduce noise in evaluated ciphertext

- Homomorphic evaluation of decryption
  - removes large old noise
  - adds small new noise (size small since decryption shallow)

AGM21: Oblivious Sampling of FHE ciphertexts!

The Magic of Bootstrapping

- Assume that decryption always outputs 0 or 1
  - even if input ct is not well formed

- Then, bootstrapping always outputs proper encryption of 0 or 1!

$$\mathsf{Eval}\left(\mathsf{Dec}_{ct}, \boxed{sk}\right) = \boxed{\mathsf{Dec}_{ct}(sk)} = \boxed{x}$$

Even if input "ct" is a random element in ciphertext space!

The Magic of Bootstrapping

- Assume that decryption outputs 0 w.o.p for random input

- Then, bootstrapping outputs encryption of 0 w.o.p for random input

$$\mathsf{Eval}\left[\mathsf{Dec}_{\mathsf{rand}}, \mathsf{sk}\right] = \mathsf{Dec}_{\mathsf{rand}}(\mathsf{sk}) = 0$$

Given enc(sk), run dec homomorphically on random to generate encryption of 0 w.o.p!

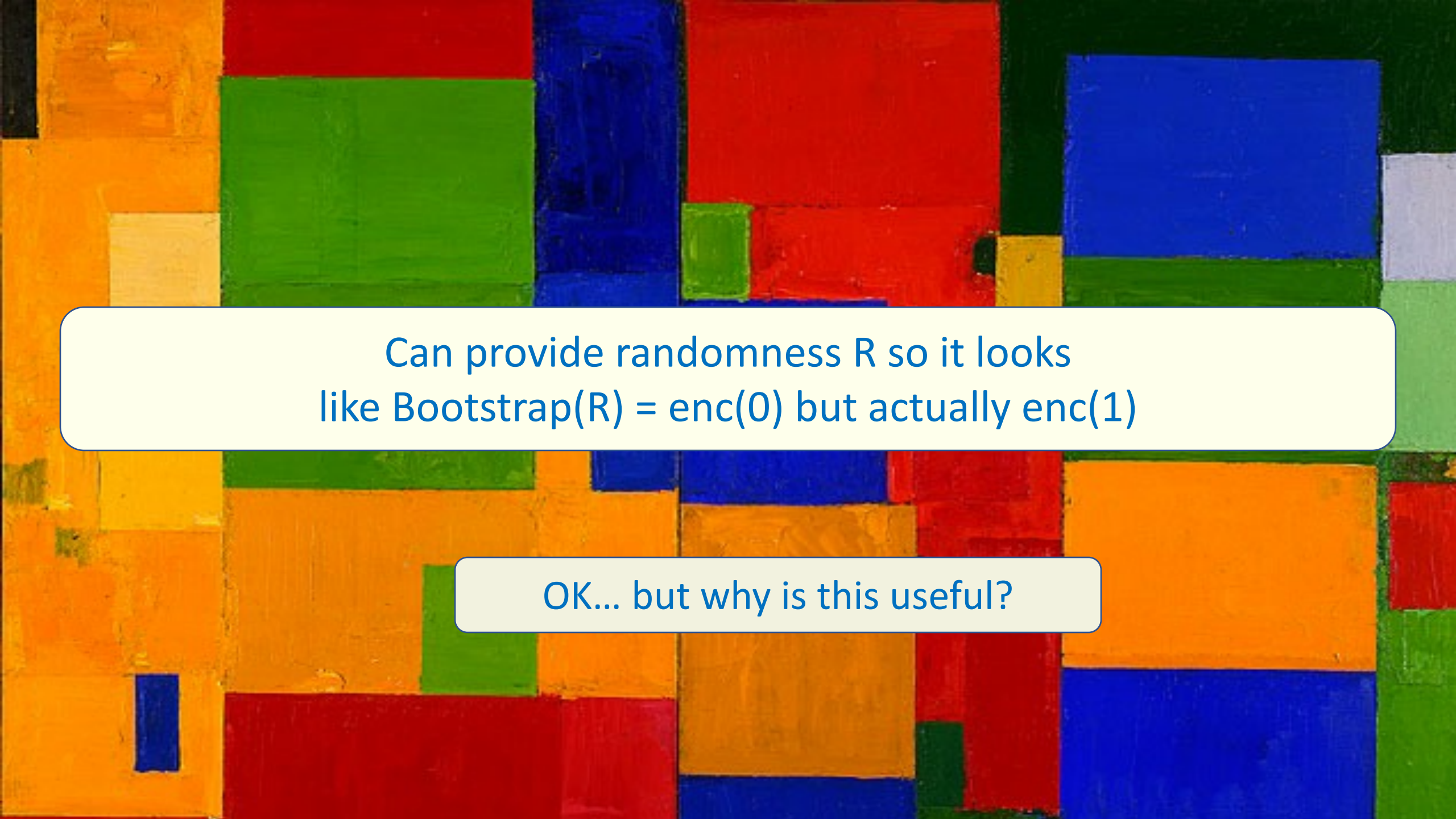
But, wait a minute…

- Given encryption of 1, decryption outputs 1 w.o.p
- Encryption of 1 is indistinguishable from random!

$$\text{Eval}\left[\text{Dec}_{ct1}, \boxed{sk}\right] = \boxed{\text{Dec}_{ct1}(sk)} = \boxed{1}$$

- Can pretend as if ct1 = enc(1) is a random string

Pretend bootstrapping outputs enc(0) but actually enc(1)!


Can provide randomness R so it looks
like Bootstrap(R) = enc(0) but actually enc(1)
OK… but why is this useful?

Leveraging our trick (binary msg space)

- Let $B(x) = Eval(pk, Dec_x, ct_{sk})$ the bootstrapping procedure
  - recall $Dec_x(sk) = Dec(sk, x)$

- Denote homomorphic addition (mod 2) as
$$Eval(pk, +, ct_a, ct_b) = ct_a \oplus ct_b$$

$$B(R_1) \oplus \cdots \oplus B(R_n) = \text{Enc}\,(\text{Parity}\,(x_1, \ldots, x_n))$$

Construction

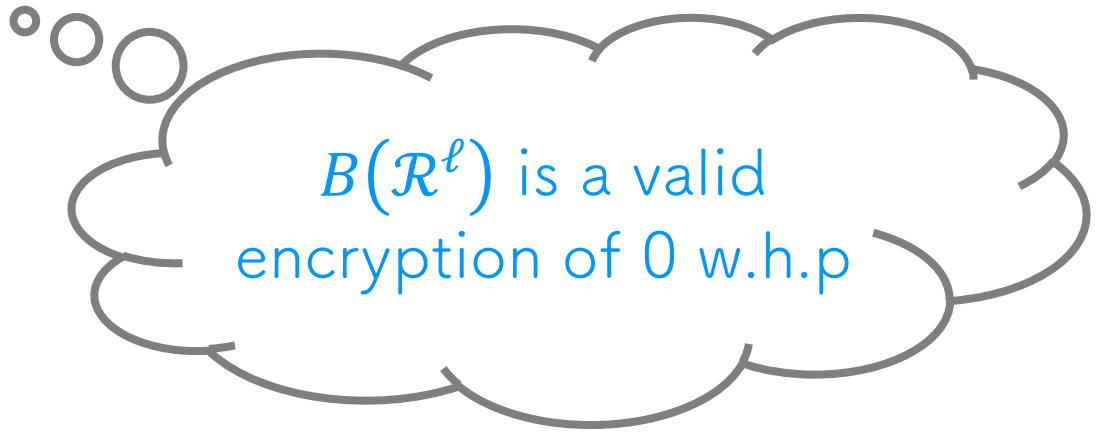
Gen:

1. $(pk, sk) \leftarrow Gen$
2. $ct_{sk} \leftarrow Enc(pk, sk)$
3. Output $pk = (pk, ct_{sk}), sk = sk$

Construction

$Enc(pk, b)$:

1. Sample $x_1, \ldots, x_n \leftarrow \{0,1\}$ s.t. $\sum_i x_i = b \ (mod\ 2)$
2. For $x_i = 0$, sample $R_i \leftarrow \mathcal{R}^\ell$
3. For $x_i = 1$, sample $r_i \leftarrow \{0,1\}^{\ell'}$ and set $R_i = Enc(pk, 1; r_i)$
4. Compute $ct = B(R_1) \oplus \cdots \oplus B(R_n)$
5. Output ct



Construction

$Fake(pk, b, rand, \bar{b})$:

1. If $b = \bar{b}$, output $rand$
2. Sample $k \leftarrow [n]$ s.t. $x_k = 1$
3. Set $x'_k = 0$ and $R'_k = Enc(pk, 1; r_k)$
4. For $i \neq k$, set $R'_i = R_i$ and $r'_i = r_i$
5. Output $rand' = (x'_1, \ldots, x'_n, \{R'_i\}_{x'_i=0}, \{r'_i\}_{x'_i=1})$

By pretending one ciphertext enc(1) is random, parity flipped!

Construction

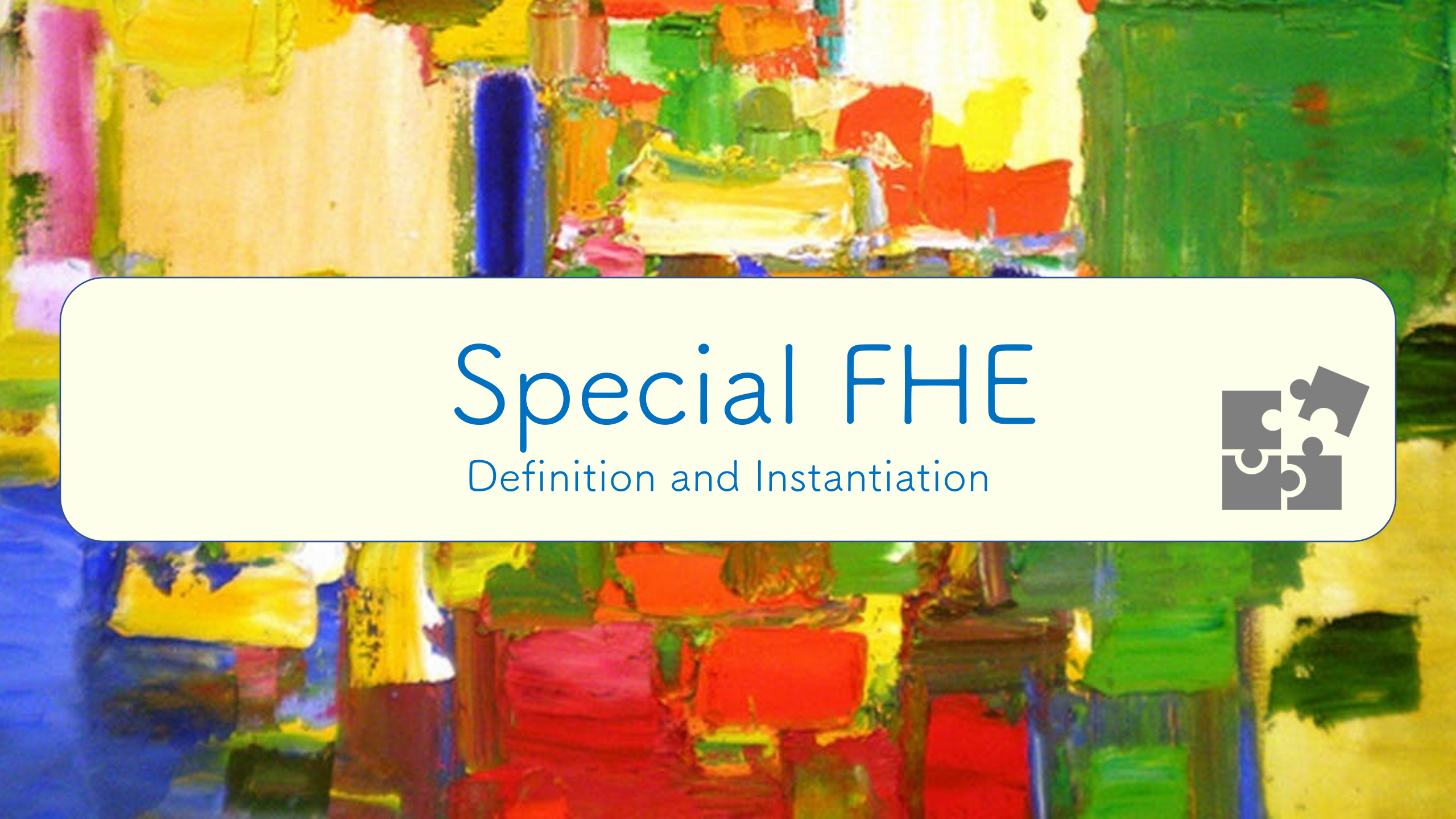
$Eval(pk, f, ct_1, \ldots, ct_k)$:

1. Interpret ct_i as special FHE ciphertext ct_i
2. Output $Eval(pk, f, ct_1, \ldots, ct_k)$

$Dec(dsk, ct)$:

1. Interpret ct as special FHE ciphertext ct
2. Output $Dec(sk, ct)$

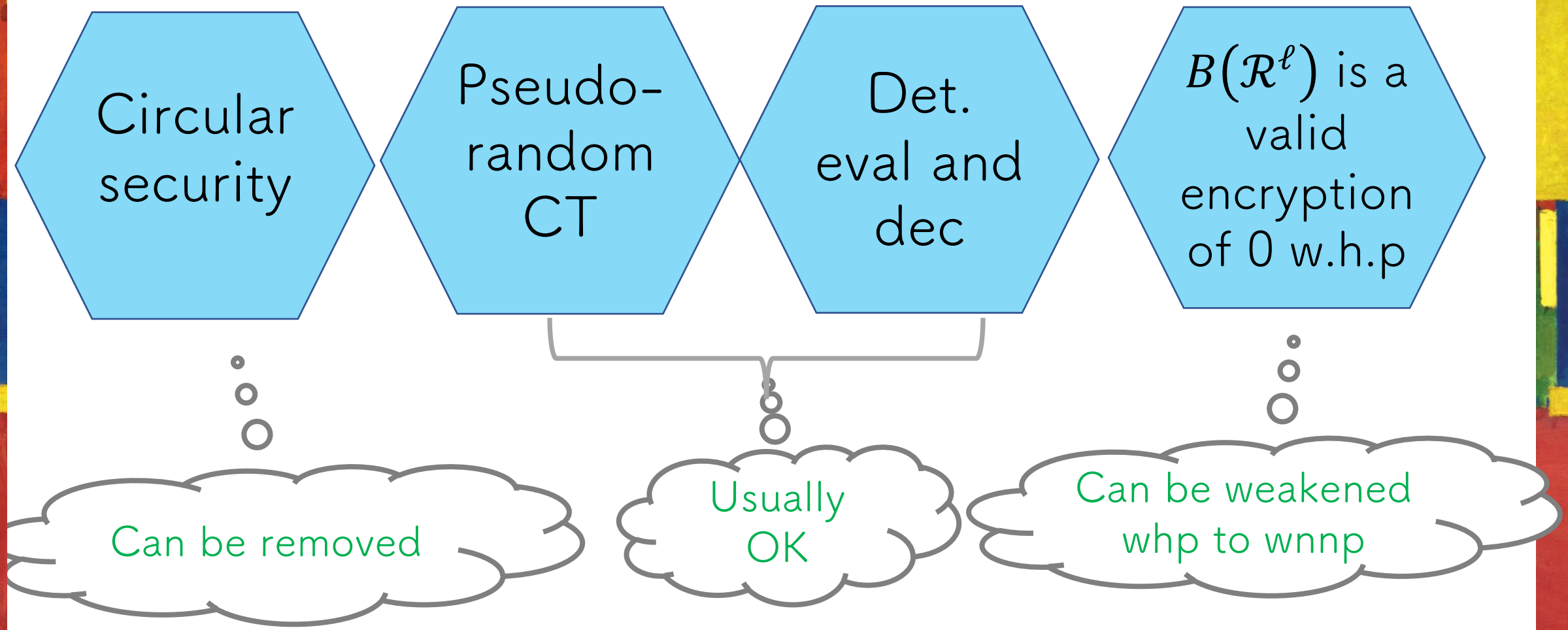
As before!



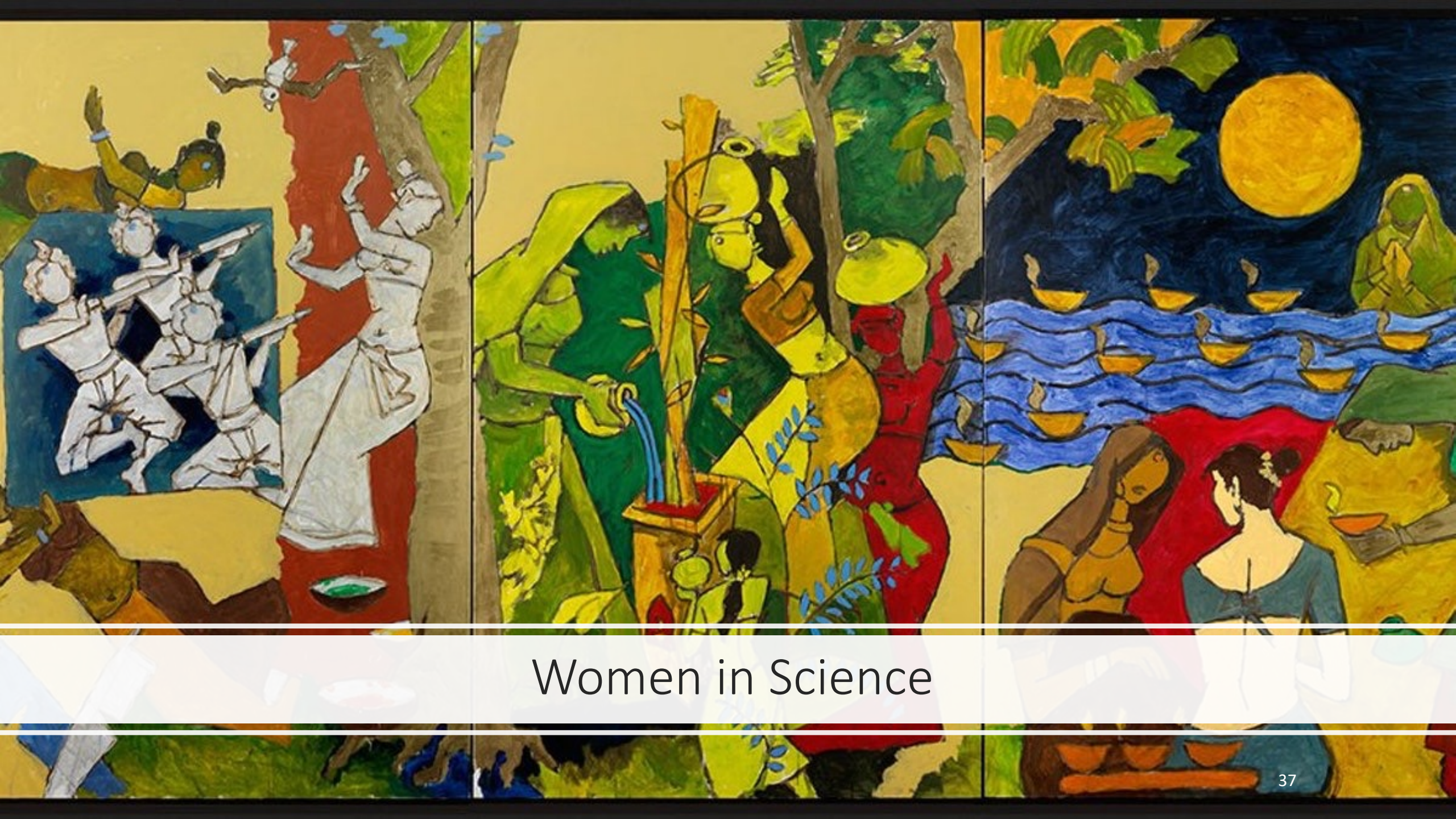
Special FHE

Definition and Instantiation

Special FHE



[BGV14] FHE satisfies all properties!



Women in Science

Is Science Objective?

"Whenever the subject of women in science comes up, there are people fiercely committed to the idea that sexism does not exist. They will point to everything and anything else to explain differences while becoming angry and condescending if you even suggest that discrimination could be a factor. But these people are wrong. This data shows they are wrong."

[Scientific American 2012]

Can we be open to this idea?

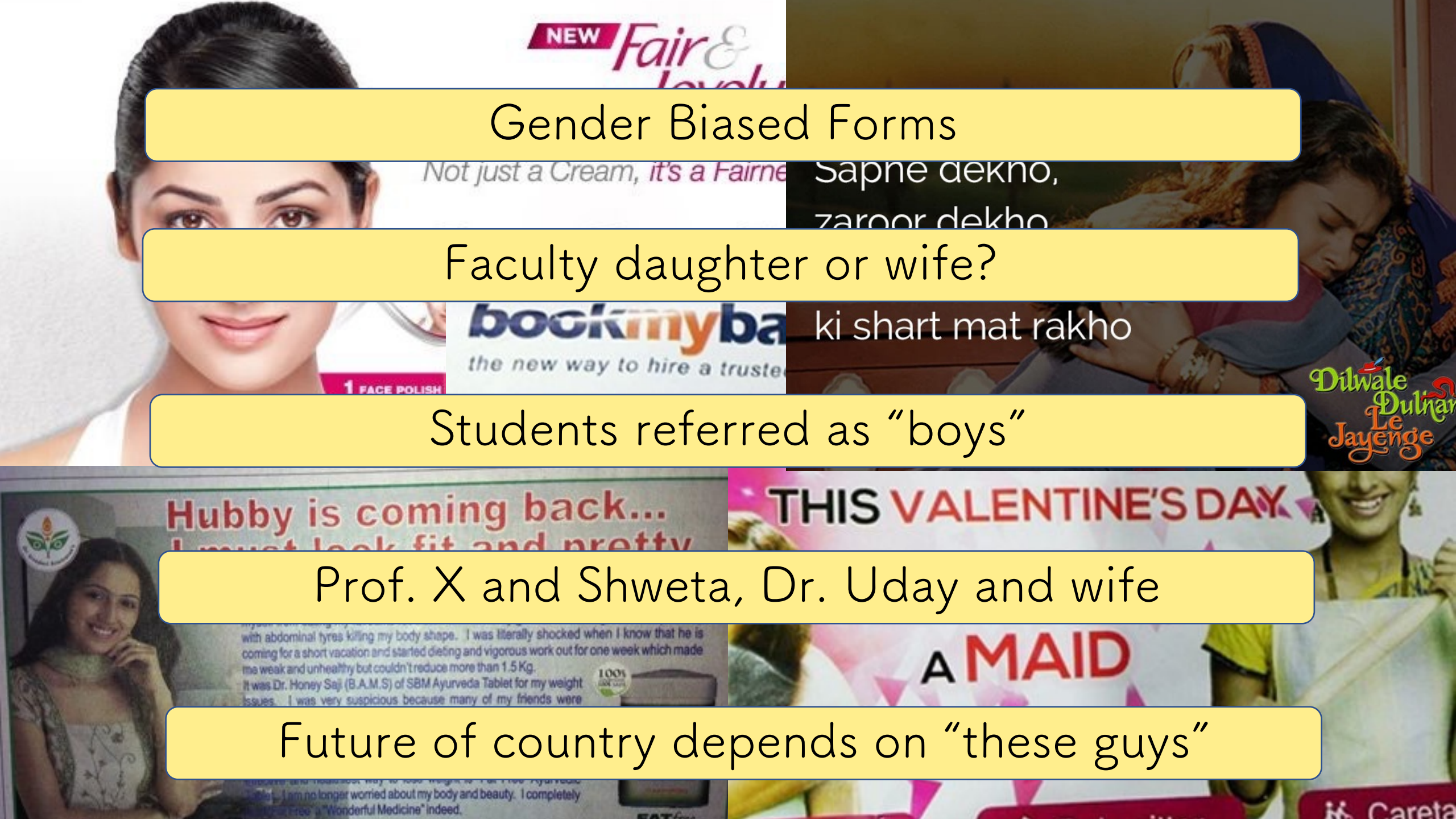
Society has biases!

A girl receives literally thousands of suggestions over time that tell her what her place/role is…

- My earliest memory: Blessings received when touching feet of elders
- Today's experience: Prepared for women who (seem to) need, not for women who (seem to) lead
- Enormous pressure felt by (esp.) MS/PhD students about "own desires" versus family/expectations. Seen many bright young girls giving up or compromising heavily on career

Sometimes, discards/rebels.

Often internalizes/compromises.



Gender Biased Forms

Faculty daughter or wife?

Students referred as "boys"

Prof. X and Shweta, Dr. Uday and wife

Future of country depends on "these guys"

Society has biases! And Science?

Scientists are supposed to be objective, able to evaluate data and results without being swayed by emotions or biases. This is a fundamental tenet of science. What this extensive literature shows is, in fact, scientists are people, subject to the same cultural norms and beliefs as the rest of society.

[Prof. Alison Coil, UCSD]

Things I've heard

∞ times

- Women can't do math
- Women are good at rote learning not reasoning
- It is not feminine to argue
- Why would Google pay so much to hire a woman whose just going to go on maternity leave
- I saw a very beautiful woman on our floor today and I wondered, what she is doing on the science floor?
- Your paper has better chances since it will get sympathy, being an all woman paper
- You left your parents to follow your desires? Our daughters would never do that
- If you study so much, who will marry you?
- Women need to put family first

So… what next?

- Is this daunting/depressing? Seeing it is overcoming it!

It only matters if you let it!

- Reject these suggestions and they cannot touch you.
- Calling it out? Take a call.
- Preserve creative energy: results talk loudest!
- Cultivate support system
- Personally: Follow(ed) gut even when no support. Willing to accept consequences.

No Looking Back!

Life is not easy for any of us. But what of that? We must have perseverance and above all confidence in ourselves. We must believe that we are gifted for something and that this thing must be attained.

-Marie Curie (first scientist to be awarded a Nobel Prize in two different categories)

Thank You

Images Credit: MF Hussain, Hans Hoffman
Slides Credit: Daniele Micciancio, Chris Peikert, Saleet Mossel