

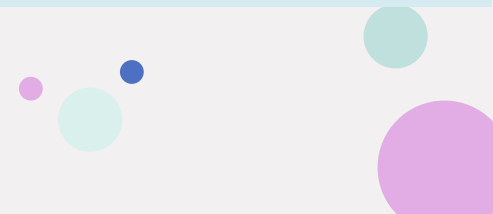


Lecture 22

Post Quantum (Lattice)-based Cryptography

CS409: Introduction to Cryptography

Sruthi Sekar



Big Picture so far

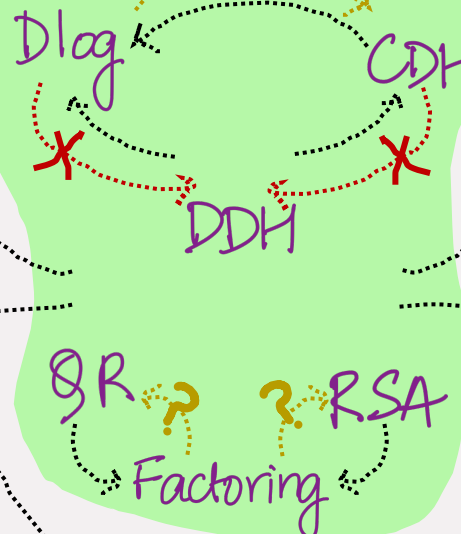
CRYPTOMANIA

KEY EXCHANGE

CCA-PKE $\longleftrightarrow$ CPA-PKE

TDP

HARDNESS ASSUMPTIONS



MINICRYPT

CCA-SKE

CPA-SKE

MAC

PRF

PRG

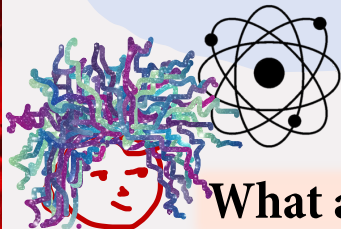
OWF

Digital Sig

CRHF

Commitment Schemes

Malicious Verifier Computational ZKP for NP



Evelyn

What about quantum attacks?

$\dots \rightarrow$ open $\dots \times$ doesn't imply $\dots \rightarrow$ implies

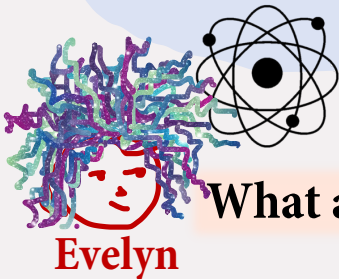
Big Picture so far

CRYPTOMANIA

KEY EXCHANGE

CCA-PKE $\leftrightarrow$ CPA-PKE

TDP



What about quantum attacks?

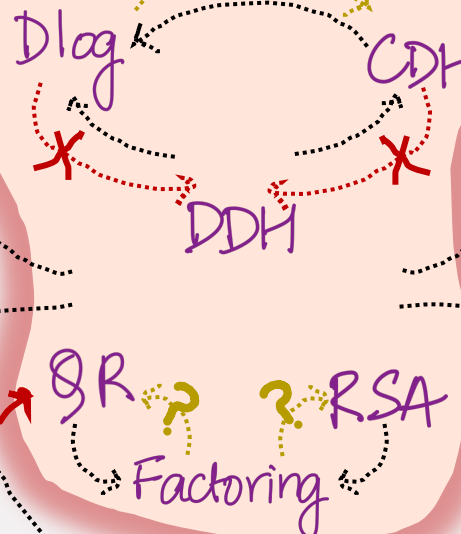
Evelyn



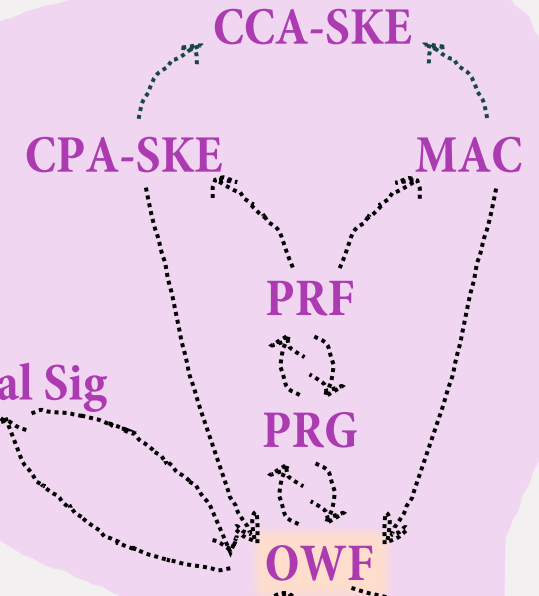
Very large-scale quantum computers will make them easy

~~HARDNESS ASSUMPTIONS~~

INSECURE



MINICRYPT



CRHF

Commitment Schemes

Malicious Verifier Computational ZKP for NP

...? open ...X doesn't imply implies

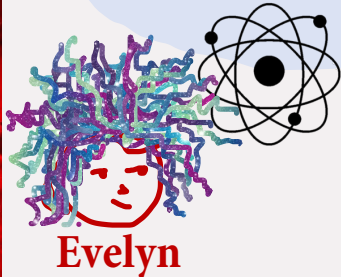
Today

CRYPTOMANIA

KEY EXCHANGE

CCA-PKE $\xleftrightarrow{?}$ CPA-PKE

TDP



Evelyn

In a World against Evelyn!

POST-QUANTUM
HARDNESS ASSUMPTION

LWE
(Learning With Errors)

MINICRYPT

CCA-SKE

CPA-SKE

MAC

PRF

PRG

OWF

Digital Sig

CRHF

Commitment Schemes

Malicious Verifier Computational ZKP for NP

$\xleftrightarrow{?}$ open $\nrightarrow$ doesn't imply $\implies$ implies

Why is Evelyn more powerful?



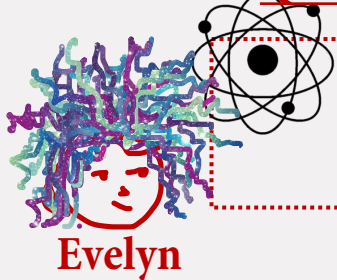
I: For unstructured search problems: classically NP-complete
(E.g. SAT: Find an assignment $a \in \{0,1\}^n$ s.t. $\phi(a) = 1$, for Boolean formula ϕ)

Classical: No sub-exponential time algorithms exist (*Exponential-time hypothesis*)

Quantum (Evelyn's world)

Grover's Algorithm

There exists a quantum algorithm that given ϕ (represented as a classical Boolean circuit) finds a satisfying assignment in time $2^{O(n/2)}$



Evelyn



Impact on cryptography: SKEs *broken* by Evelyn in (quantum) time $2^{O(n/2)}$

Solution: *double* the key-size (e.g. use 256-bit AES instead of 128-bit)

Why is Evelyn more powerful?



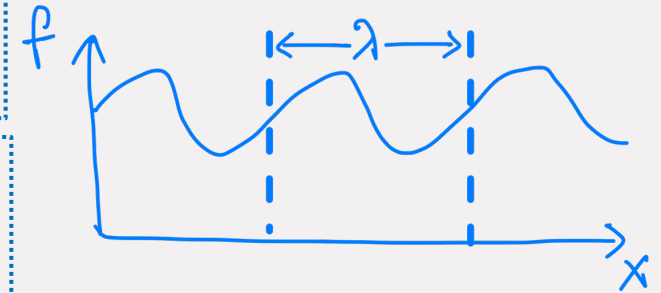
II: For structured “*period-finding*” problem (E.g. factoring, discrete log):
For *periodic* $f: (\mathbb{Z}_\ell, +) \rightarrow \mathbb{G}: \exists \lambda \in \mathbb{Z}_\ell$ s.t. $\forall x \in \mathbb{Z}_\ell f(x + \lambda) = f(x)$, **find smallest period λ**

Factoring: $f_{a,N}(x) := a^x \bmod N$, where $\mathbb{G} = (\mathbb{Z}_N^*, \cdot)$ and $a \in_R \mathbb{Z}_N^*$
period $\lambda(N) := (p-1)(q-1)$ (w.h.p.)
finding $\lambda(N)$ is equivalent to factoring N

Why?

Dlog: $f_{g,h}(x, y) := g^x h^{-y} \bmod p$, where $\mathbb{G} = (\mathbb{Z}_p^*, \cdot)$ and $g, h \in_R \mathbb{Z}_p^*$
period $\lambda(g, h) := (\text{dlog}_g(h), 1)$ (the discrete log)

Why?

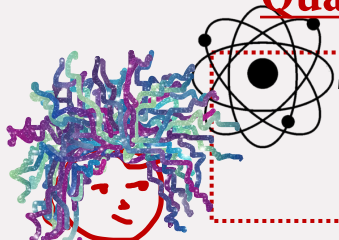


Classical: For certain periodic f , **PPT** algorithms are believed to not exist!

Quantum (Evelyn's world)

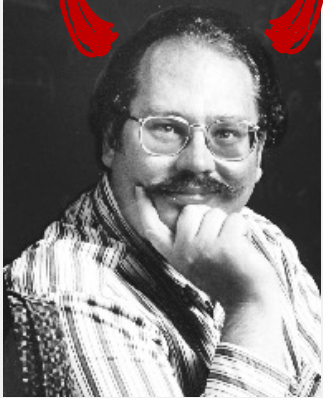
Shor's Algorithm

There exists a quantum algorithm that **finds the period λ** of a periodic function f as above (represented as a classical circuit) **in time $\text{polylog}(\ell)$** .

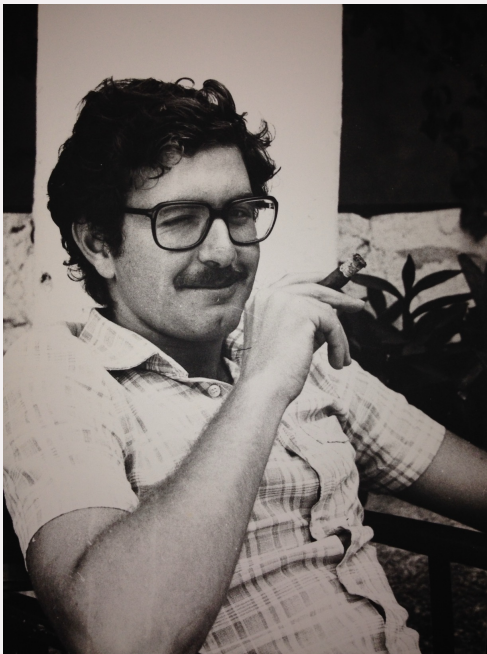


Evelyn

Factoring and Dlog are easy for Evelyn (quantum adversary)!



All the constructions we
learnt so far are broken in
the quantum world! ☹



“Cryptographers seldom sleep well”
-[Silvio Micali, 1988]

But life goes on.. Post-quantum life

NEWS

NIST Releases First 3 Finalized Post-Quantum Encryption Standards

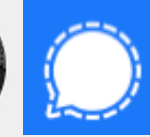
August 13, 2024

 Security Research

February 21, 2024

iMessage with PQ3: The new state of the art in quantum-secure messaging at scale

Posted by Apple Security Engineering and Architecture (SEAR)



Quantum Resistance and the Signal Protocol

ehrenkret on 19 Sep 2023



विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF
SCIENCE & TECHNOLOGY

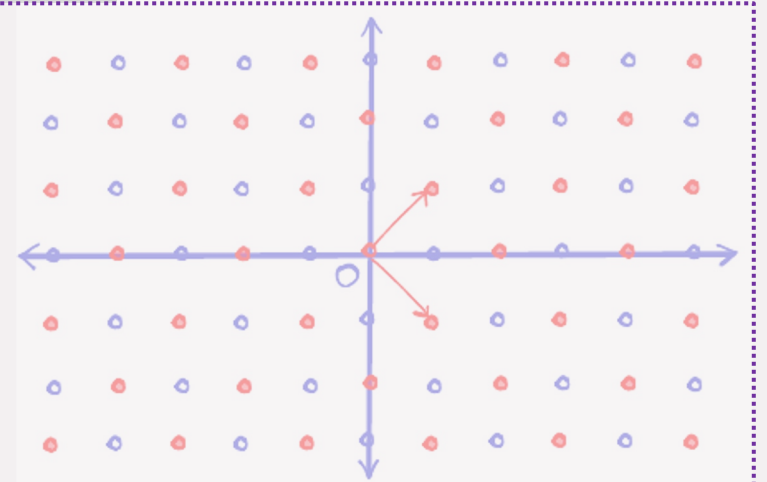
National Quantum Mission (NQM)

The Union Cabinet, approved the National Quantum Mission (NQM) on 19th April 2023 at a total cost of Rs.6003.65 crore from 2023-24 to 2030-31, aiming to seed, nurture and scale up scientific and industrial R&D and create a vibrant & innovative ecosystem in Quantum Technology (QT). This will accelerate QT

Enter: Lattice-based assumption

Why Lattice-based Crypto?

- ❑ Exponentially Hard (so far)
- ❑ Quantum-Resistant (so far)
- ❑ *Worst-case hardness (unique-feature of lattice-based crypto)**
- ❑ Simple and Efficient
- ❑ Surprising Power (only assumption under which *Fully Homomorphic Encryption (FHE)* known)



NEXT CLASS

*to understand this comment in depth, need to understand more about lattices, which I won't get into!

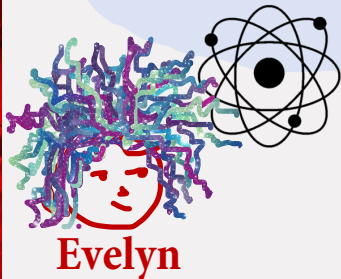
Today

CRYPTOMANIA

KEY EXCHANGE

CCA-PKE $\xleftrightarrow{?}$ CPA-PKE

TDP



Evelyn

In a World against Evelyn!

POST-QUANTUM
HARDNESS ASSUMPTION

LWE
(Learning With Errors)

MINICRYPT

CCA-SKE

CPA-SKE

MAC

PRF

PRG

Digital Sig

OWF

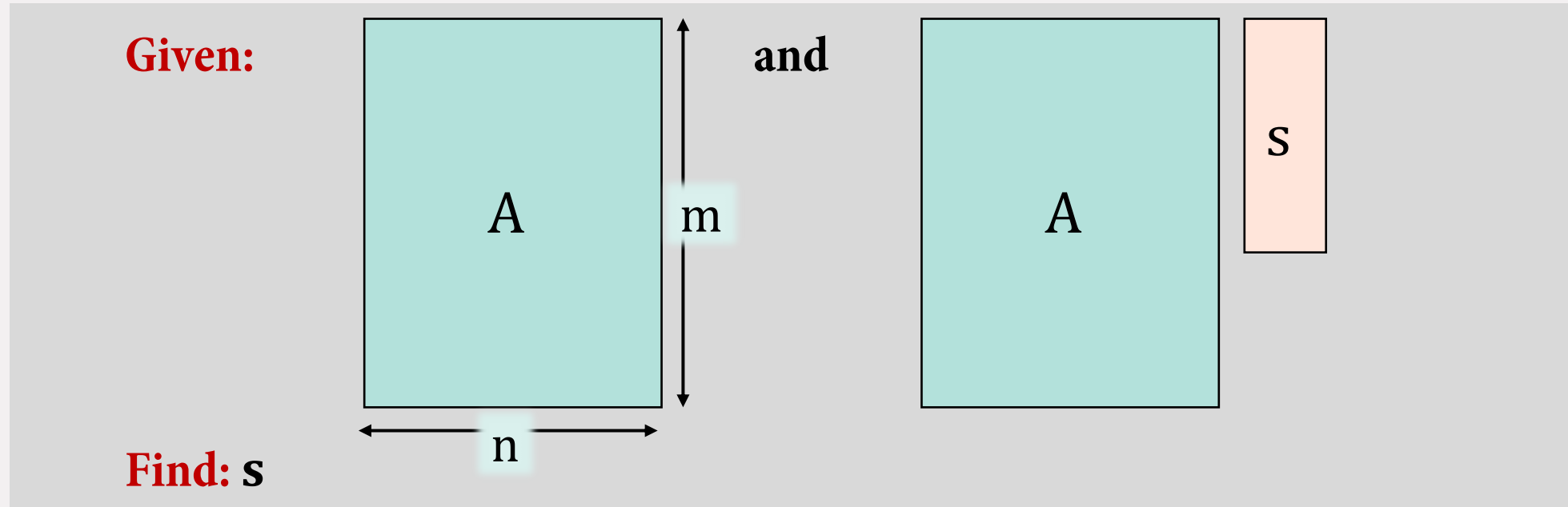
CRHF

Commitment Schemes

Malicious Verifier Computational ZKP for NP

$\xleftrightarrow{?}$ open $\nrightarrow$ doesn't imply $\implies$ implies

Solving Linear Equations



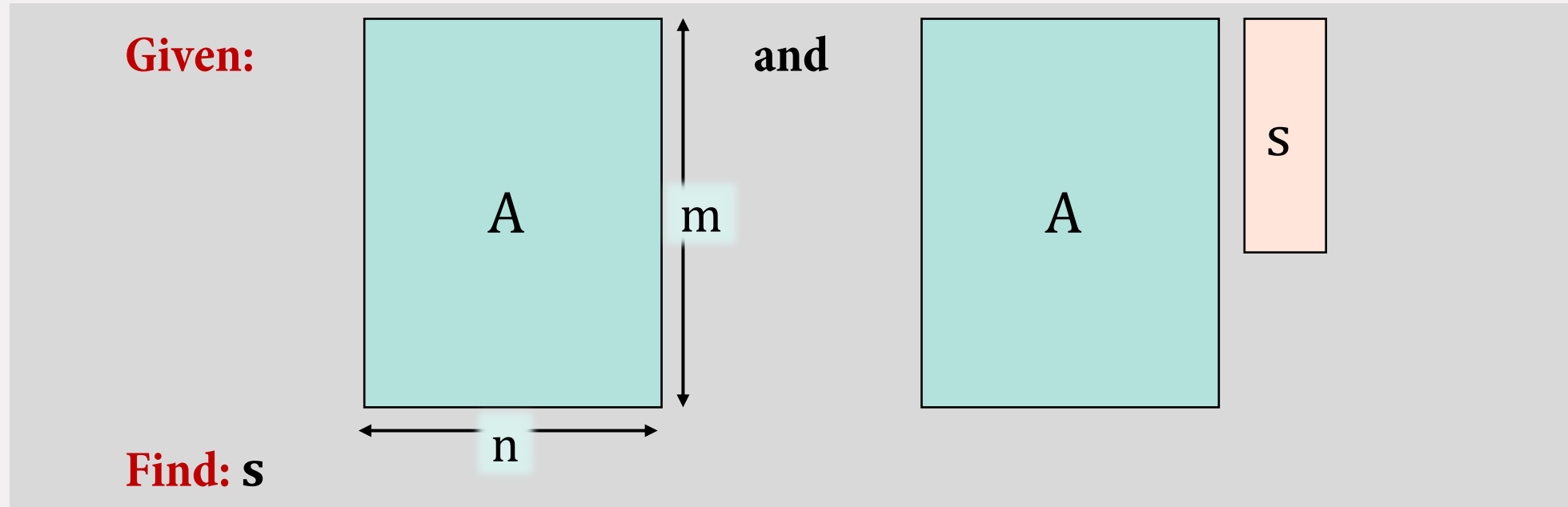
n variables and $m \gg n$ equations (over $\mathbb{Z}$)

EASY

Gaussian Elimination!



Solving Linear Equations: Make it hard



n variables and $m \gg n$ equations (over $\mathbb{Z}_q$)

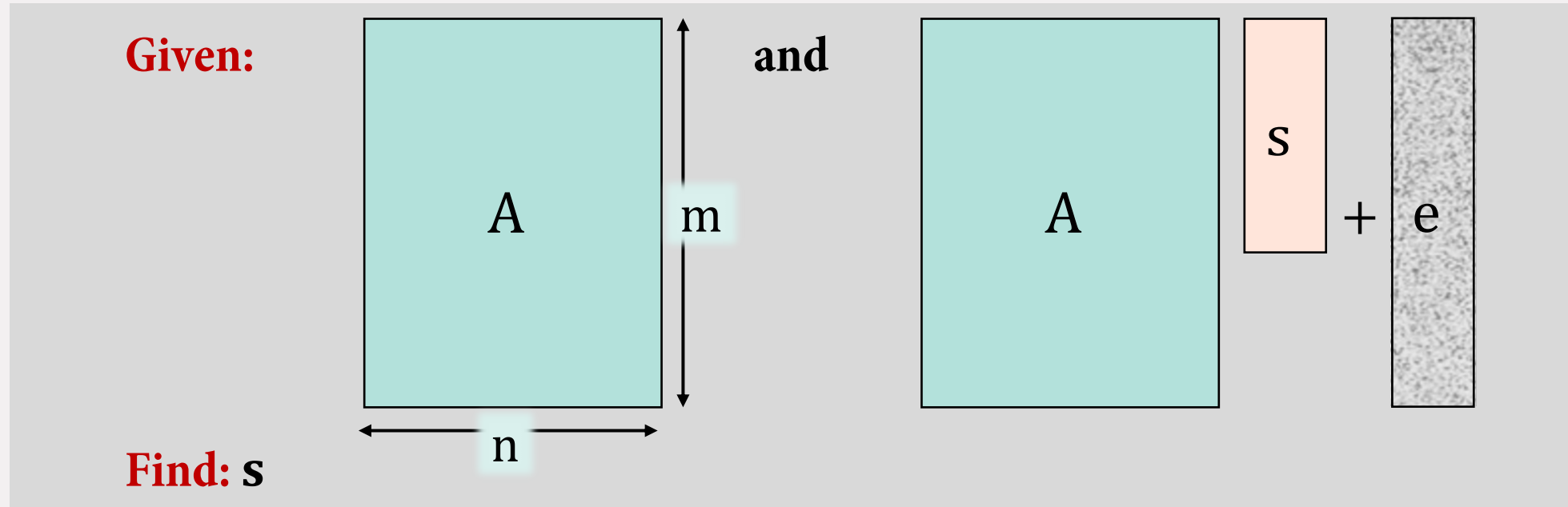
What if we “*chop the head*”, i.e. work with modulo some q ?

STILL EASY Gaussian Elimination mod q !



****Vinod's analogy:** chop the head as it's like cutting off the higher bits. E.g. $1121 \bmod 100 = 21$

Solving Linear Equations: Make it hard



n variables and $m \gg n$ equations (over $\mathbb{Z}$)

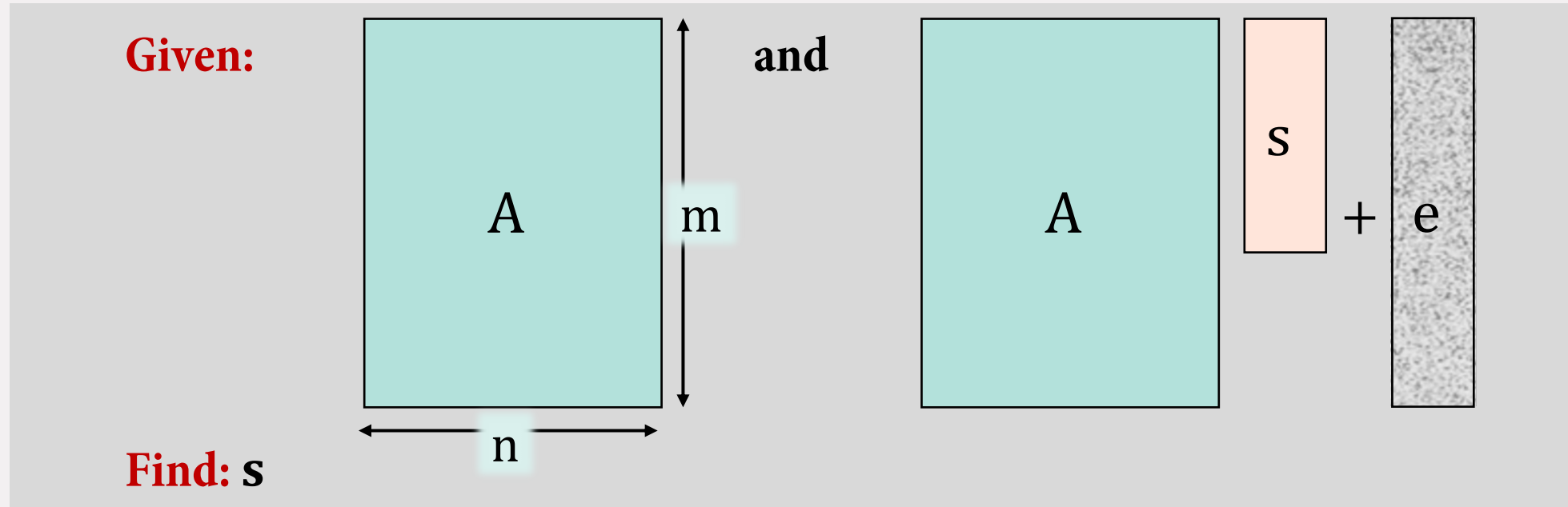
What if we “*chop the tail*”, i.e., add small error to each equation?

STILL EASY Linear Regression



****Vinod's analogy:** chop the tail (of precision) as it's like making the system approximate instead of exact

Solving Linear Equations: Make it hard

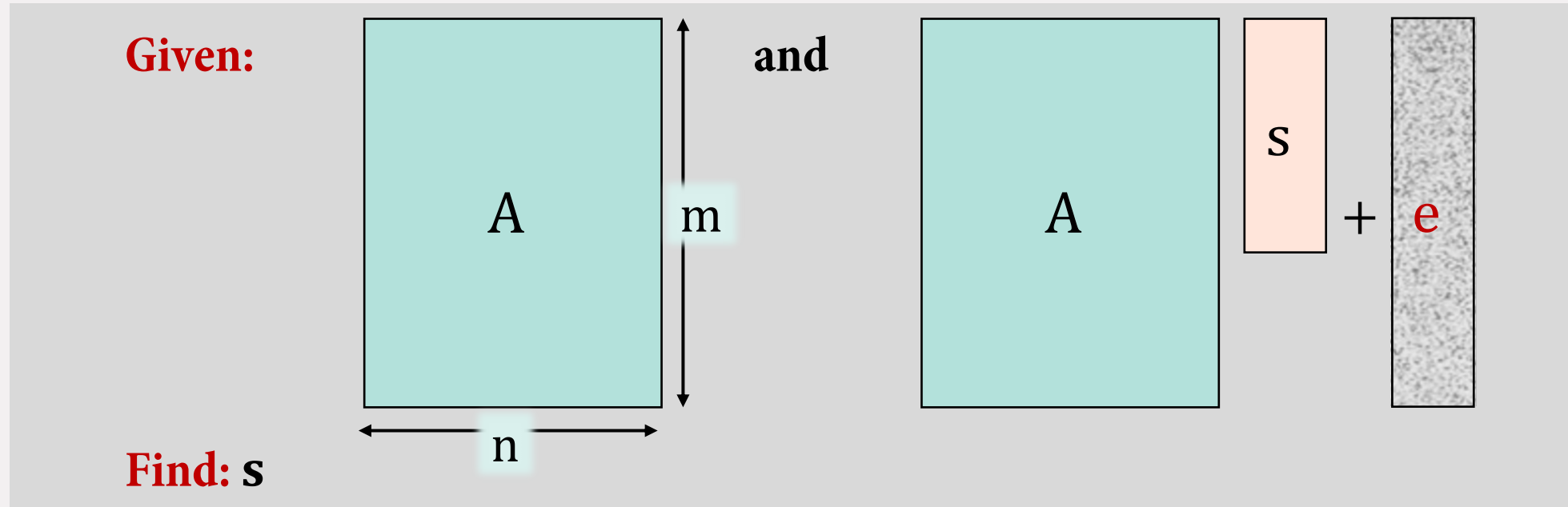


n variables and $m \gg n$ equations (over $\mathbb{Z}_q$)

What if we “*chop the head and tail*” both (**add small error and work mod q**)?

TURNS OUT TO BE VERY HARD

Solving Linear Equations: Make it hard



n variables and $m \gg n$ equations (over $\mathbb{Z}_q$)

Parameters*: **dimensions** n and m , **modulus** q , **error distribution** χ

$$A \in_R \mathbb{Z}_q^{m \times n}, s \in_R \mathbb{Z}_q^n, e \leftarrow \chi^m$$

What distribution χ ?: **1. (small) uniform in some interval $[-B, \dots, B]$**

Focus on 1. to understand

2. Interesting: χ_α is (discrete) Gaussian over $\mathbb{Z}$ with mean 0 and s.d. $\sigma := \alpha q$



*Decades of cryptanalysis says we are (quantum) safe with: (n = sec param, m = $\text{poly}(n)$, B = small-poly in n (e.g. $\sqrt{n}$), q = $\text{poly}(n) > B$)

Learning With Errors (LWE)

Definition 1: Search LWE

The (n, m', q, χ) -SLWE assumption holds if $\forall$ quantum polynomial Evelyn, following is negligible:

$$\Pr_{\substack{A \in_R \mathbb{Z}_q^{m' \times n} \\ s \in_R \mathbb{Z}_q^n, e \leftarrow \chi^{m'}}} [\text{Evelyn}(A, As + e) = s]$$

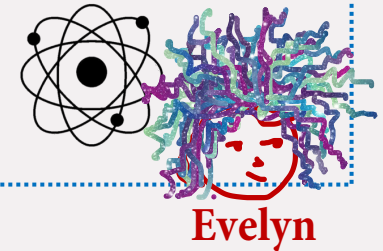
A

,

A

s
+

e



||| (equivalent)*

For sufficiently large m' $\Downarrow$ $\Uparrow$ (Obvious)

Definition 2: Decision LWE

The (n, m, q, χ) -DLWE assumption holds if $\forall$ quantum polynomial Evelyn, following is negligible:

$$\left| \Pr_{\substack{A \in_R \mathbb{Z}_q^{m \times n} \\ s \in_R \mathbb{Z}_q^n, e \leftarrow \chi^m}} [\text{Evelyn}(A, As + e) = 1] - \Pr_{\substack{A \in_R \mathbb{Z}_q^{m \times n} \\ r \in_R \mathbb{Z}_q^m}} [\text{Evelyn}(A, r) = 1] \right|$$

A

,

A

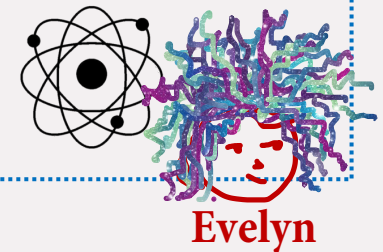
s
+

e

Real world

Random world

indistinguishable



*unlike what we saw for CDH (search variant) and DDH (decision variant)

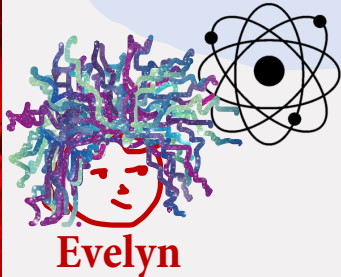
Today

CRYPTOMANIA

KEY EXCHANGE

CCA-PKE $\xleftrightarrow{?}$ CPA-PKE

TDP



Evelyn

In a World against Evelyn!

POST-QUANTUM
HARDNESS ASSUMPTION

LWE
(Learning With Errors)

MINICRYPT

CCA-SKE

CPA-SKE

MAC

PRF

PRG

OWF

Digital Sig

CRHF

Commitment Schemes

Malicious Verifier Computational ZKP for NP

$\xleftrightarrow{?}$ open $\nrightarrow$ doesn't imply $\implies$ implies

OWF and PRG from LWE

$$f_A(s, e) := As + e$$

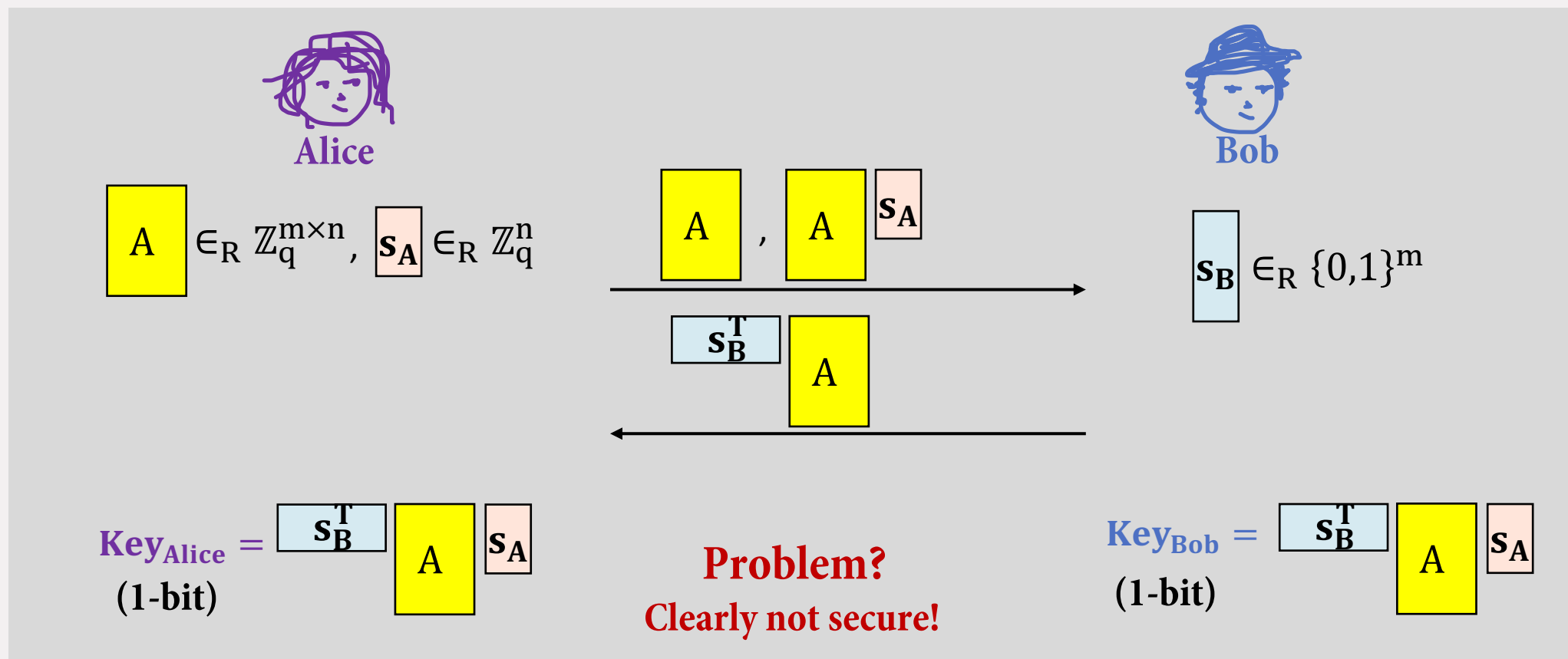
I: SLWE $\Rightarrow \{f_A\}_{A \in \mathbb{Z}_q^{m \times n}}$ is a one-way function family!

$$\left(\begin{array}{l} \because \Pr_{\substack{A \in_R \mathbb{Z}_q^{m' \times n} \\ s \in_R \mathbb{Z}_q^n, e \leftarrow \chi^{m'}}} [\text{Evelyn}(A, As + e) = s] \end{array} \right)$$

II: DLWE $\Rightarrow \{f_A\}_{A \in \mathbb{Z}_q^{m \times n}}$ is a pseudo-random function family!

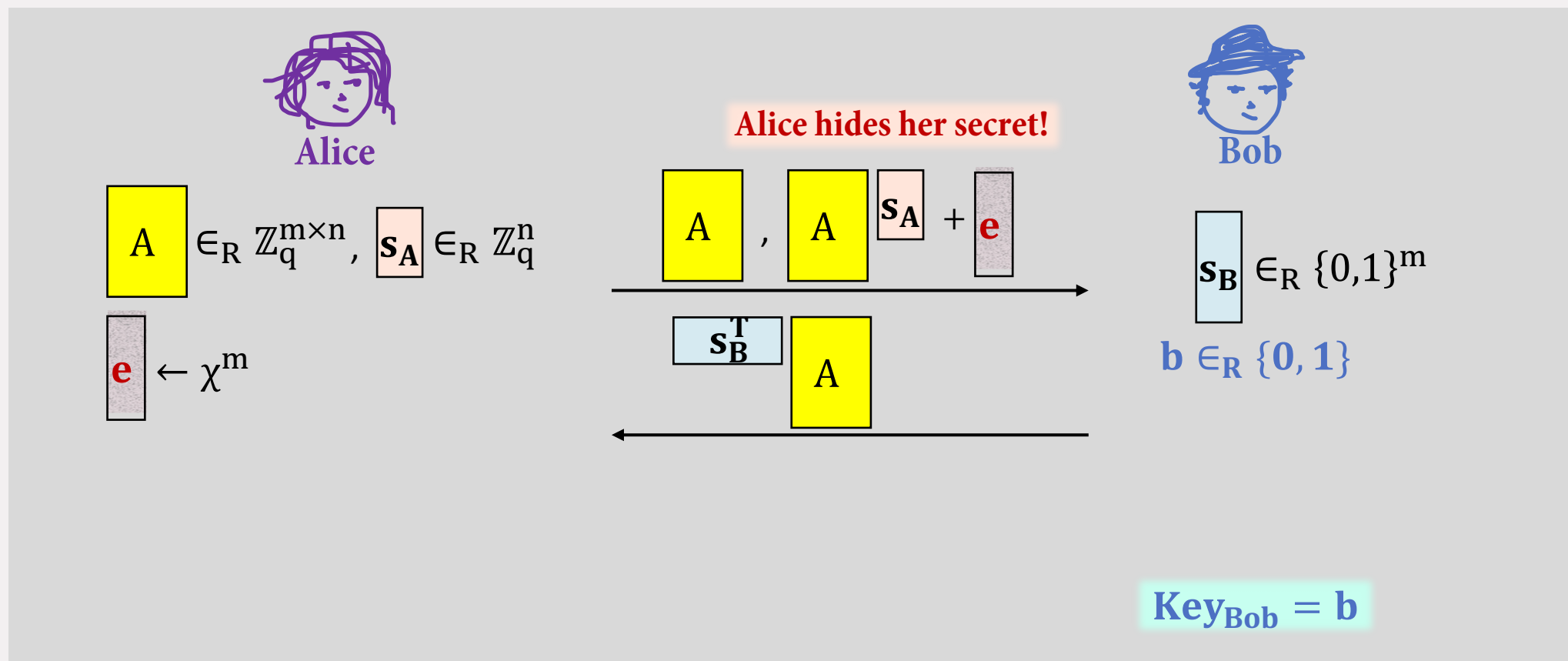
$$\left(\begin{array}{l} \because \begin{array}{c} \boxed{A}, \boxed{A} \boxed{s} + \boxed{e} \\ \text{Real world} \end{array} \approx \begin{array}{c} \boxed{A}, \boxed{r} \\ \text{Random world} \end{array} \end{array} \right)$$

1-Bit Key-Exchange [Regev05]



If we tried to mimic DH Key Exchange!

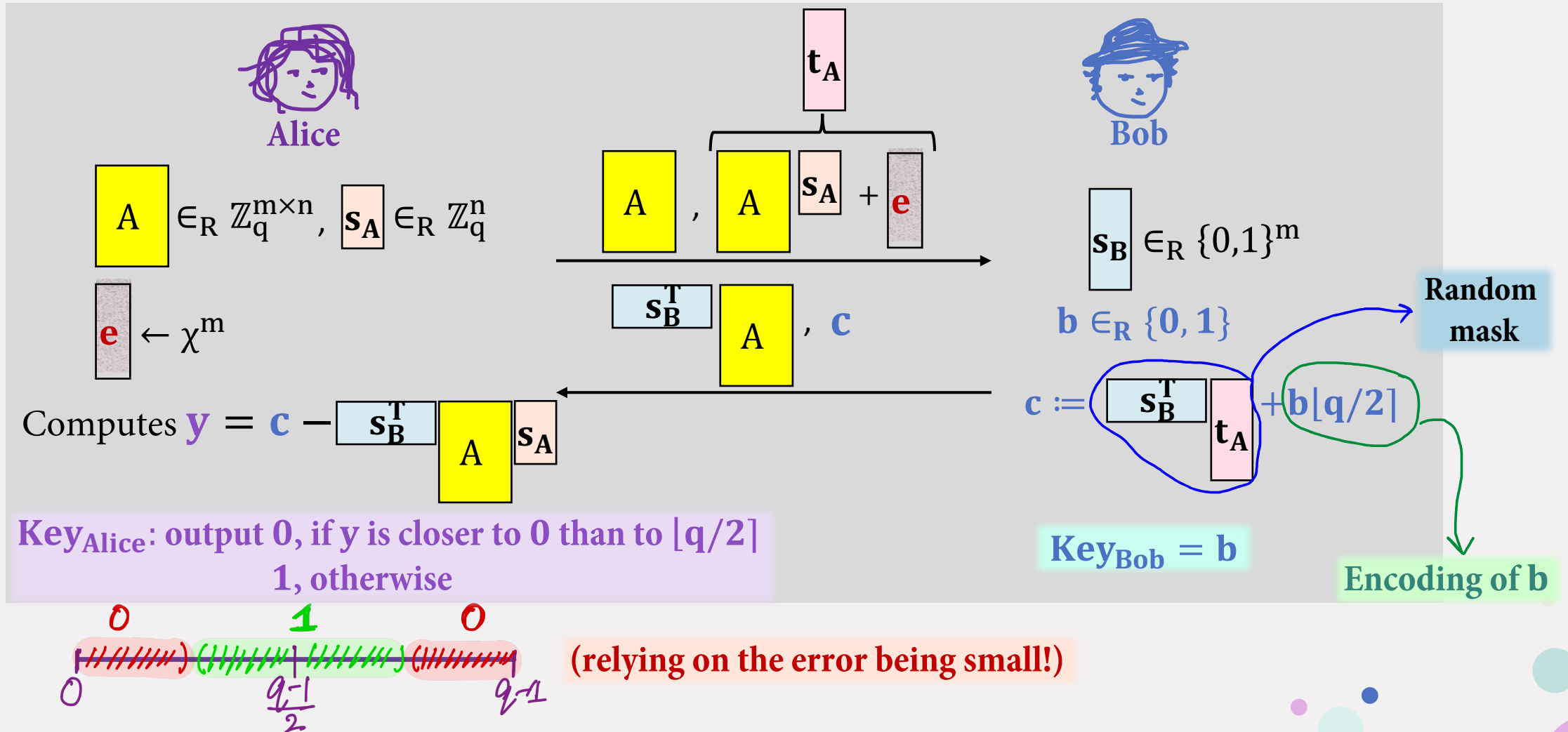
1-Bit Key-Exchange [Regev05]



Parameters: **dimensions** n and m , **modulus** q , **error distribution** χ

Bob picks a random bit and communicates it to Alice “secretly” using the random LWE-mask she sent! How?

1-Bit Key-Exchange [Regev05]



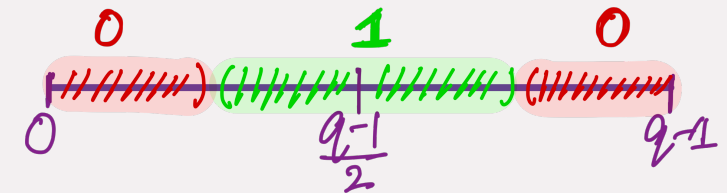
* $\lfloor q/2 \rfloor$: denotes rounding

1-Bit Key-Exchange [Regev05]

Correctness

$$\begin{aligned} y &= c - s_B^T A s_A = \cancel{s_B^T (A s_A + e)} + b \lfloor q/2 \rfloor - \cancel{s_B^T A s_A} \\ &= s_B^T e + b \lfloor q/2 \rfloor \end{aligned}$$

$$\therefore \text{Key}_{\text{Alice}} = \text{Key}_{\text{Bob}} \text{ if } |s_B^T e| < q/4$$



Error is chosen to be small enough to ensure negligible key-exchange error!

Security (assuming DLWE)

On the board (just intuitions are fine, skip the proof if you want)

1-Bit PKE from DLWE [Regev05]

$$\Pi = (\text{Gen}, \text{Enc}, \text{Dec}), \mathcal{M} = \{0,1\}$$

Gen(1^n): Pick $A \in_R \mathbb{Z}_q^{m \times n}$, $s_A \in_R \mathbb{Z}_q^n$, $e \leftarrow \chi^m$ (for $m, q = \text{poly}(n)$)

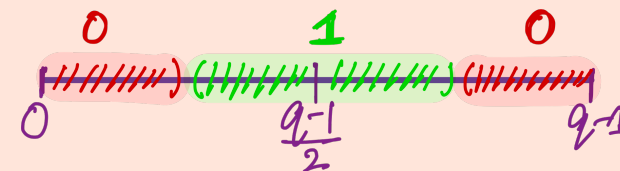
Output: $\text{pk} := (A, A s_A + e)$ and $\text{sk} := s_A$

Enc(pk, b): Sample $s_B \in_R \{0,1\}^m$, and encode $b \in \{0,1\}$ as $\tilde{b} = b \cdot \lfloor q/2 \rfloor$

Output: $c := s_B^T \text{pk} + (0^n, \tilde{b})$

Dec(sk, c): Compute $y = c \cdot (-s_A, 1)^T$

Output: 0, if y is closer to 0 than to $\lfloor q/2 \rfloor$
1, otherwise



Correctness? (similar to key exchange)

Security? (intuitions discuss on board (skip formal proof))

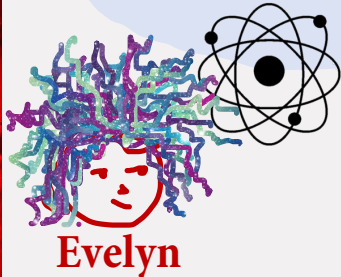
Summary

CRYPTOMANIA

KEY EXCHANGE

CCA-PKE $\leftrightarrow$ CPA-PKE

TDP



Evelyn

In a World against Evelyn!

POST-QUANTUM
HARDNESS ASSUMPTION

LWE
(Learning With Errors)

decisional $\equiv$ search

MINICRYPT

CCA-SKE

CPA-SKE

MAC

PRF

PRG

OWF

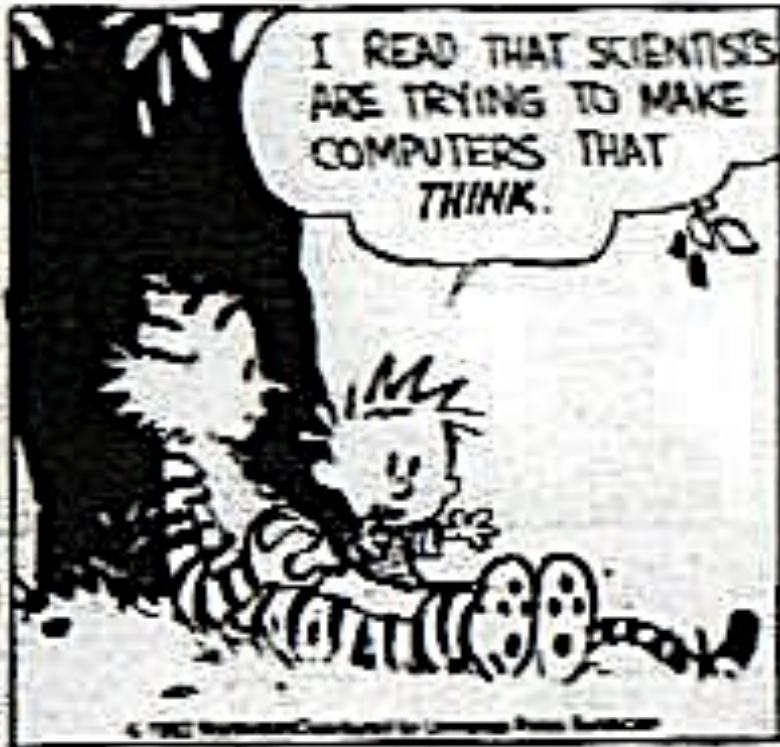
Digital Sig

CRHF

Commitment Schemes

Malicious Verifier Computational ZKP for NP

...? open ...X doesn't imply implies



Last lecture on Friday (31st Oct)