Reexamining Current Beliefs about Post-quantum Hardness Assumptions

Paul S. Lou

Advisor & Committee Chair: Amit Sahai.
Committee: Raghu Meka, Todd Millstein, Alexander A. Sherstov.

UCLA

Arguably Happy Days

follow a similar nomenclature...

B-day

D-day — Normandy, 6 June 1944

V-Day — 14 February

Arguably Happy Days

follow a similar nomenclature…

But… have you heard of **Q-Day**?

Q-Day Is Not a Good Day

WIRED

1. Challenging our confidence in certain defenses against Q-Day, by introducing a quantum algorithm.
2. A new, plausibly more secure public-key encryption to mitigate damage on Q-Day.

Paul S. Lou

Advisor & Committee Chair: Amit Sahai.
Committee: Raghu Meka, Todd Millstein, Alexander A. Sherstov.

UCLA

Q-Day

the worst holiday maybe ever

From *Wikipedia*, the free encyclopedia:

- **Harvest now, decrypt later** is a surveillance strategy that relies on the acquisition and long-term storage of currently unreadable encrypted data awaiting possible breakthroughs in decryption technology that would render it readable in the future – a hypothetical date referred to as Y2Q (a reference to Y2K) or the worst holiday maybe ever.

Q-Day

the worst holiday maybe ever

From *Wikipedia*, the free encyclopedia:

- **Harvest now, decrypt later** is a surveillance strategy that relies on the acquisition and long-term storage of currently unreadable encrypted data awaiting possible breakthroughs in decryption technology that would render it readable in the future – a hypothetical date referred to as Y2Q (a reference to Y2K) or ~~the worst holiday maybe ever~~ **Q-Day**.

How Far Away is Quantum Computing?

four years ago, we were still poking fun at quantum computing:

How Far Away is Quantum Computing?

four years ago, we were still poking fun at quantum computing:

however… the state of affairs is changing…

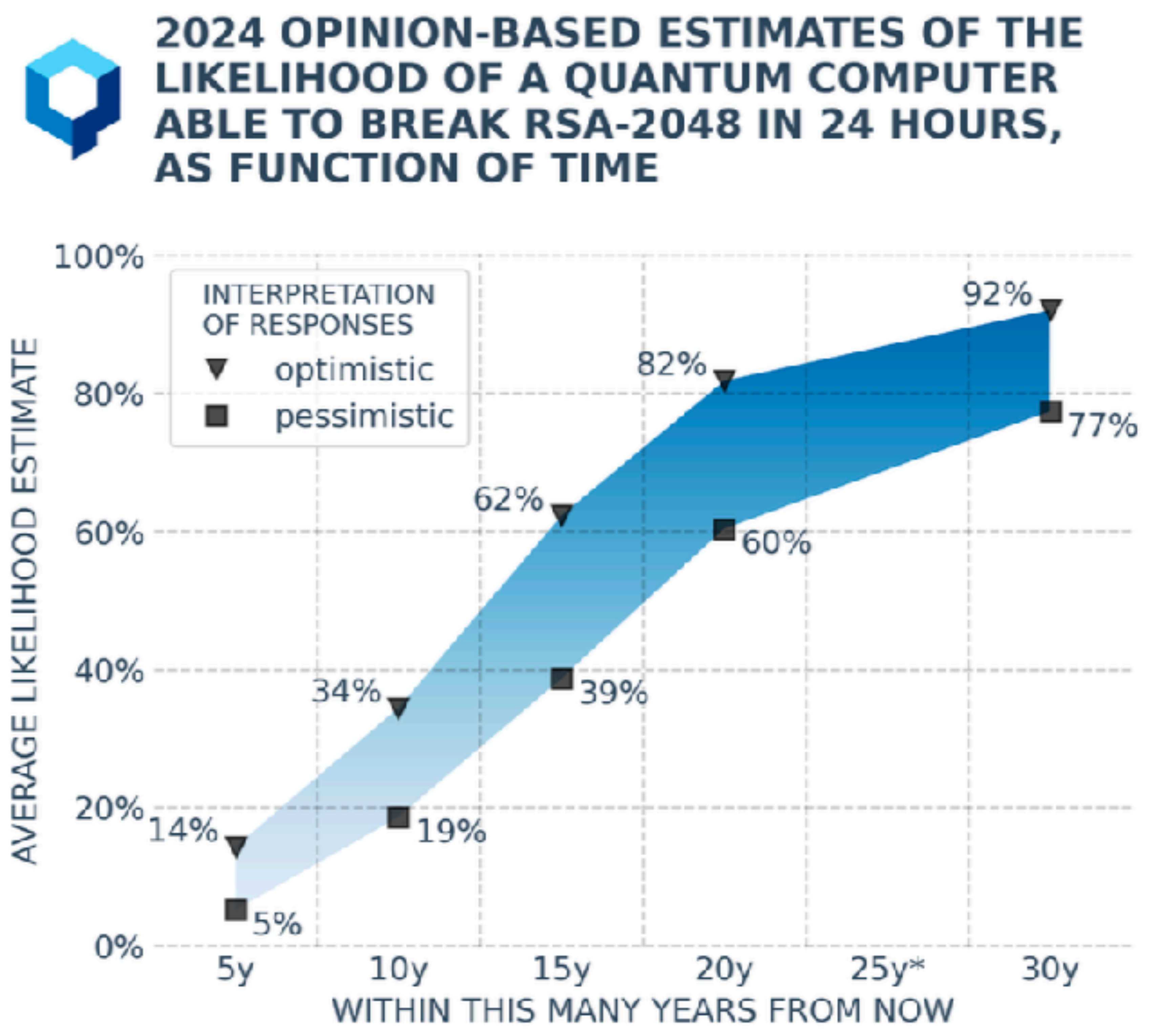
Quantum fault-tolerance milestones dropping like atoms

10 September 2024

Aaronson: *"Let me end by sticking my neck out.* ***If hardware progress continues at the rate we've seen for the past year or two, then I find it hard to understand why we won't have useful fault-tolerant QCs within the next decade.*** *(And now to retreat my neck a bit: the "if" clause in that sentence is important and non-removable!)."*

Authors: Dr. Michele Mosca, *Co-Founder & CEO, evolutionQ Inc.*
Dr. Marco Piani, *Senior Research Analyst, evolutionQ Inc.*
evolution GRI GLOBAL RISK INSTITUTE

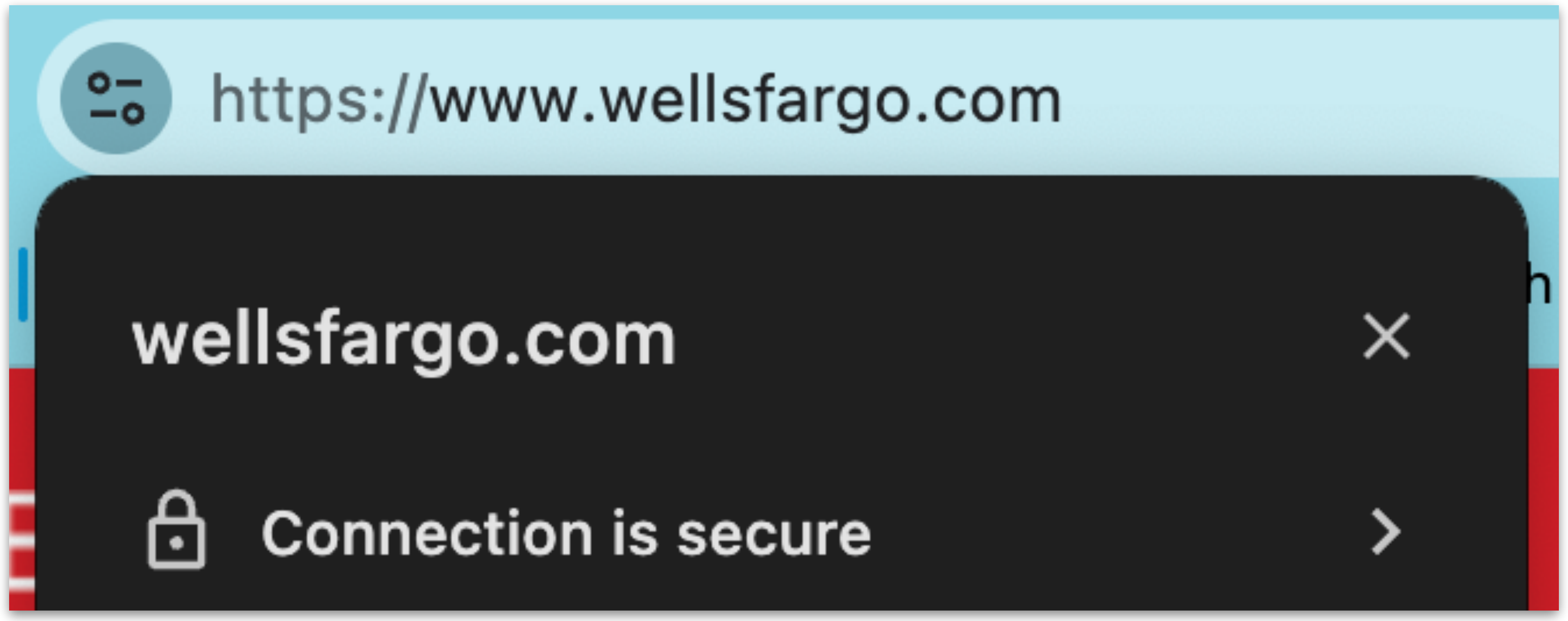
RSA-2048 is an encryption scheme widely used today that is theoretically *broken* by quantum computers.



Average likelihood estimates for the realization of a CRQC in the coming years, based on expert opinions Range between average of an optimistic (top value) or pessimistic (bottom value) of likelihood intervals indicated by the respondents.
*The 25 years timeframe was not considered explicitly.

Quantum computing experts: Q-day may occur in ~15 years.

At the time of 5 March 2024, **less than 2%** of all TLS 1.3 connections established with Cloudflare, a major internet security company, used cryptography that was secure against quantum computers.



Good News: Mitigations Against Q-Day

We are rapidly migrating to post-quantum cryptography

Post-quantum Cryptography: Cryptographic algorithms—usable today on normal everyday (i.e. *classical*) devices—that remain secure even against *quantum* computers.

Good News: Mitigations Against Q-Day

We are rapidly migrating to post-quantum cryptography

Post-quantum Cryptography: Cryptographic algorithms—usable today on normal everyday (i.e. *classical*) devices—that remain secure even against *quantum* computers.

What does "*secure*" mean?

secure—Latin sēcūrus.
From *sē-* (“without”) + *cūra* (“care”)
i.e., carefree or free from anxiety.

Is there cryptography secure against quantum computers?

Is there cryptography secure against quantum computers?

By the previous definition of *secure* as a feeling, perhaps **not**.

why?

Is there cryptography secure against quantum computers?

By the previous definition of *secure* as a feeling, perhaps **not**.

why?

(Are we not confident in our work as cryptographers?)

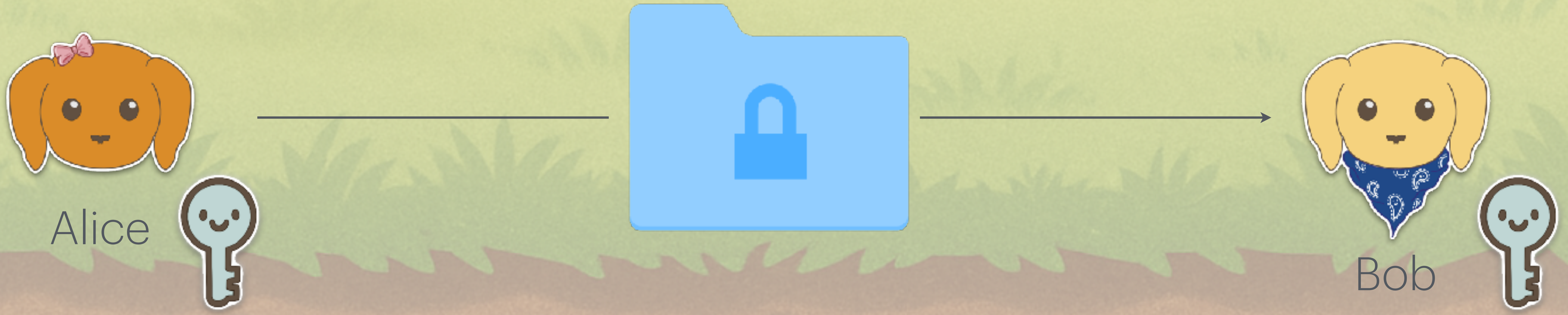
How does modern cryptography argue that the encryption algorithm is secure?

Cryptography and Computational Hardness

Symmetric-key Encryption

Alice and Bob share identical keys.

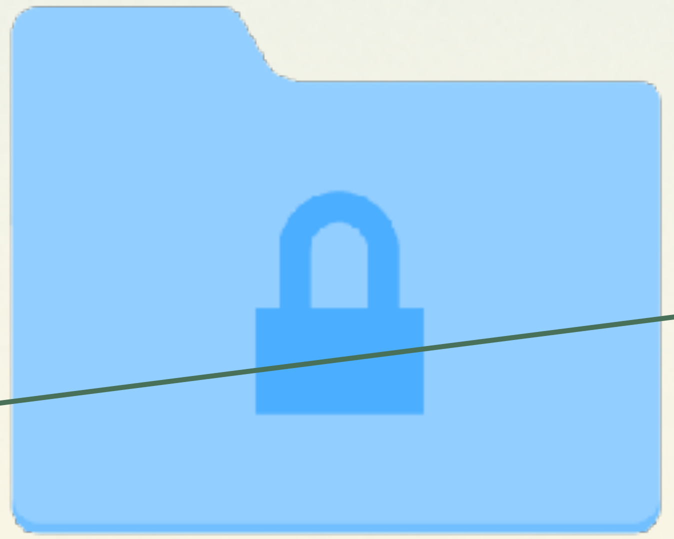
Cryptographic Primitive



Cryptography and Computational Hardness

Symmetric-key Encryption

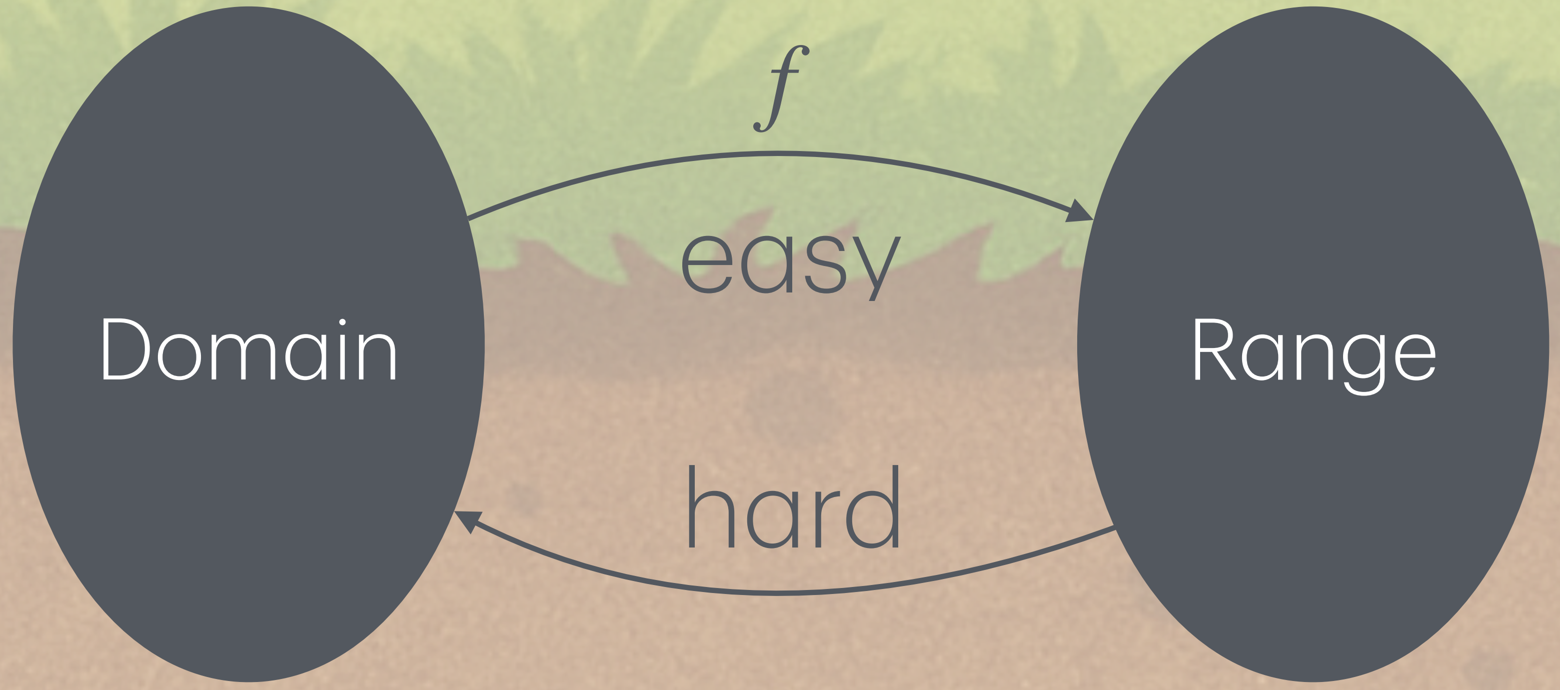
Alice and Bob share identical keys.



Cryptographic Primitive

Assume the existence of one-way functions.

One-way Functions

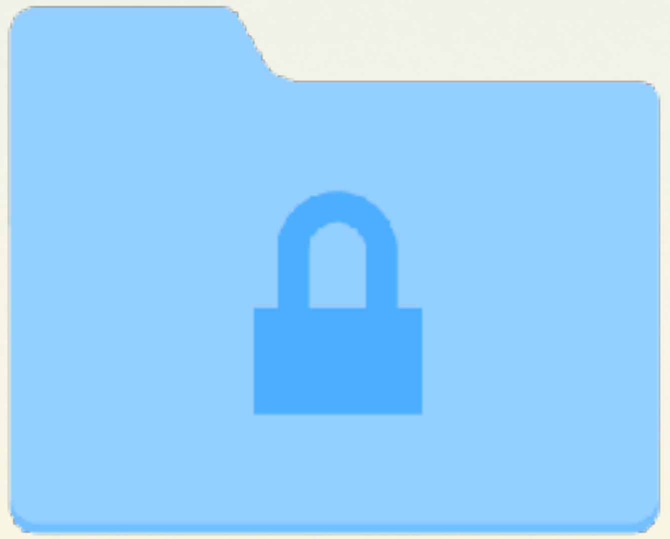


Hardness Assumption

Cryptography and Computational Hardness

Symmetric-key Encryption

Alice and Bob share identical keys.

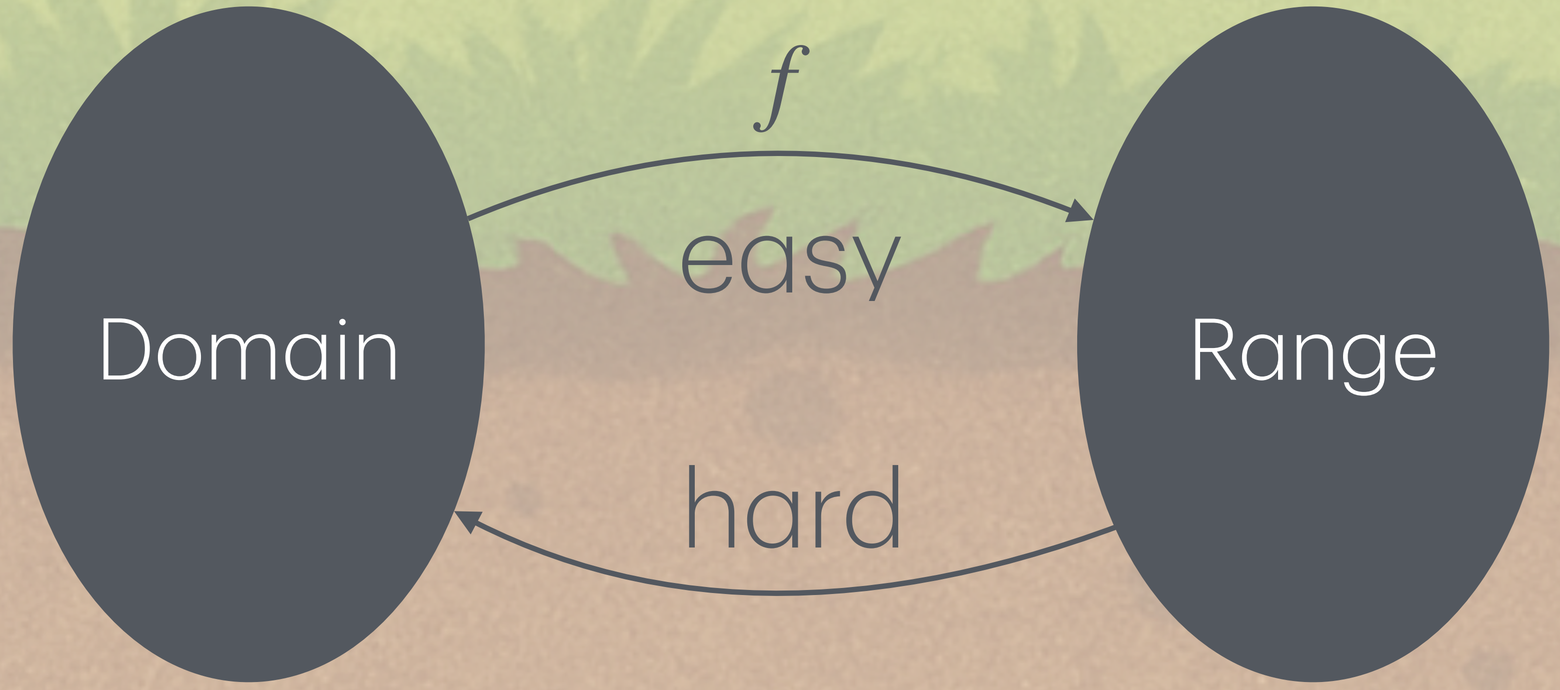


Cryptographic Primitive

Assume the existence of one-way functions.

Security Reduction: A mathematical proof that if any *efficient* adversary can break the scheme, it can also invert the one-way function. A contradiction to the one-wayness, so no such adversary can exist.

One-way Functions

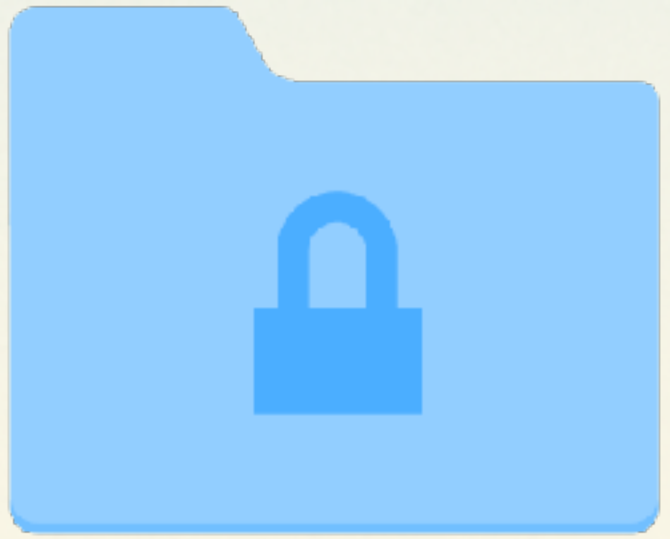


Hardness Assumption

Cryptography and Computational Hardness

Symmetric-key Encryption

Alice and Bob share identical keys.



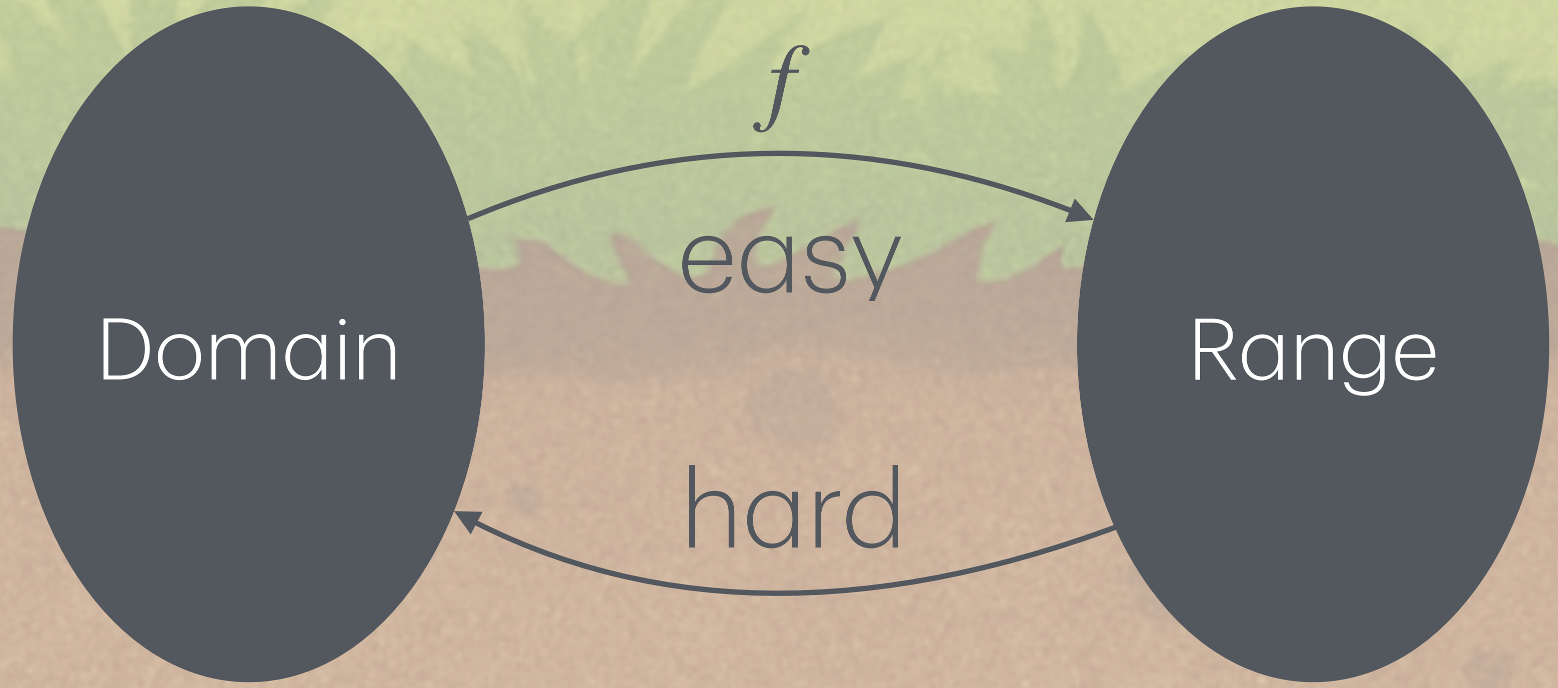
Cryptographic Primitive

Assume the existence of one-way functions.

Security Reduction: A mathematical proof that if any *efficient* adversary can break the scheme, it can also invert the one-way function. A contradiction to the one-wayness, so no such adversary can exist.

One-way Functions

Unstructured!

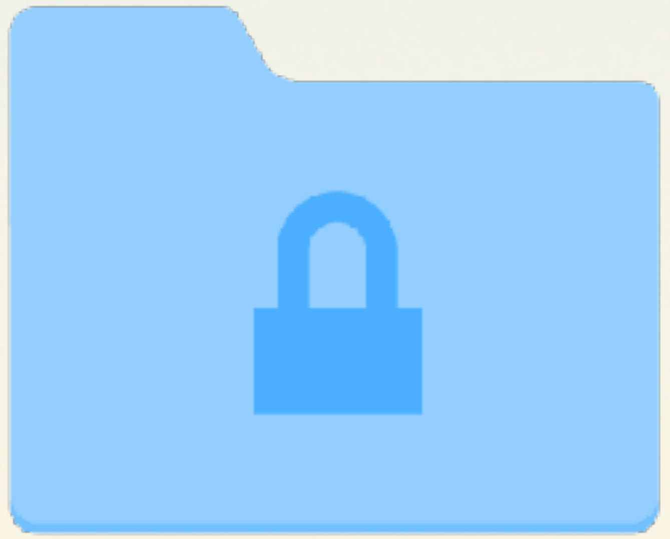


Hardness Assumption

Cryptography and Computational Hardness

Symmetric-key Encryption

Alice and Bob share identical keys.



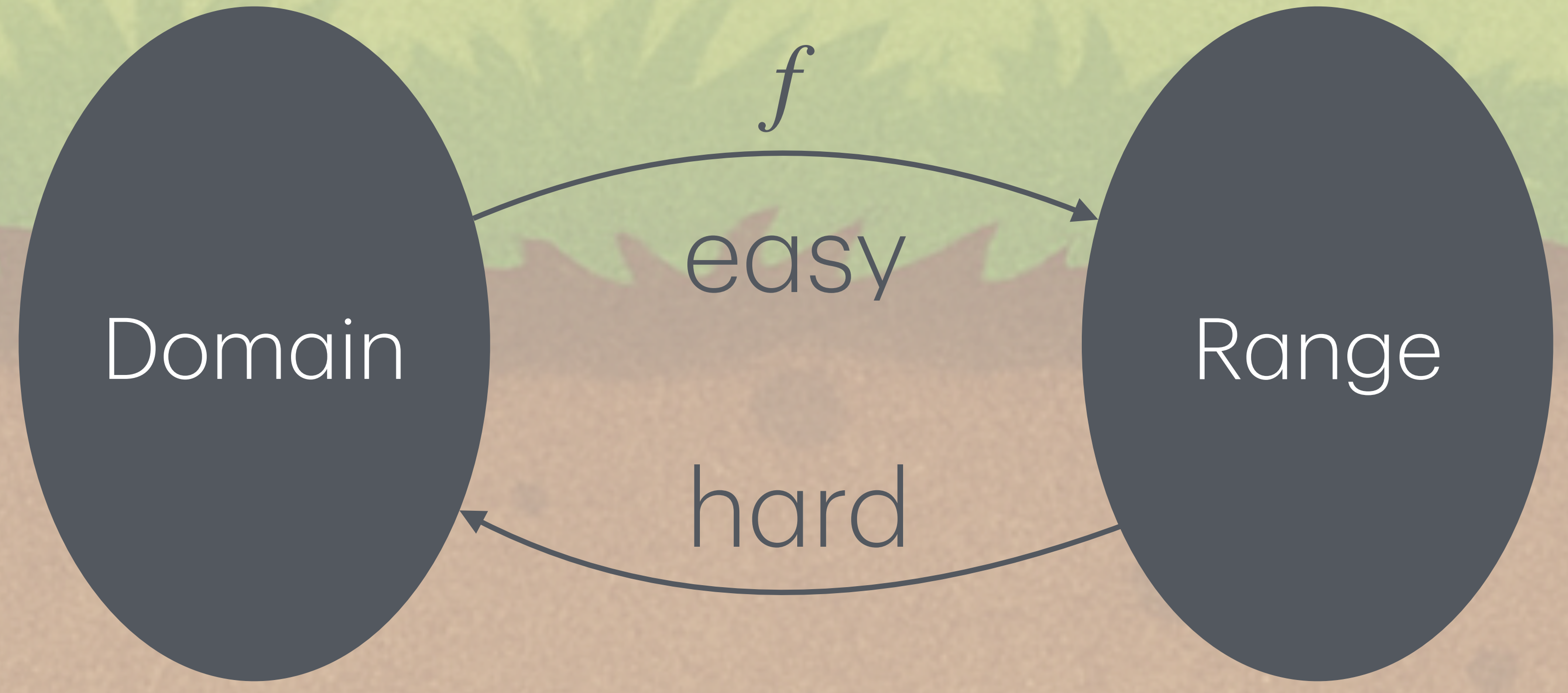
Cryptographic Primitive

Assume the existence of one-way functions.

Believable with little to no anxiety!

One-way Functions

Unstructured!

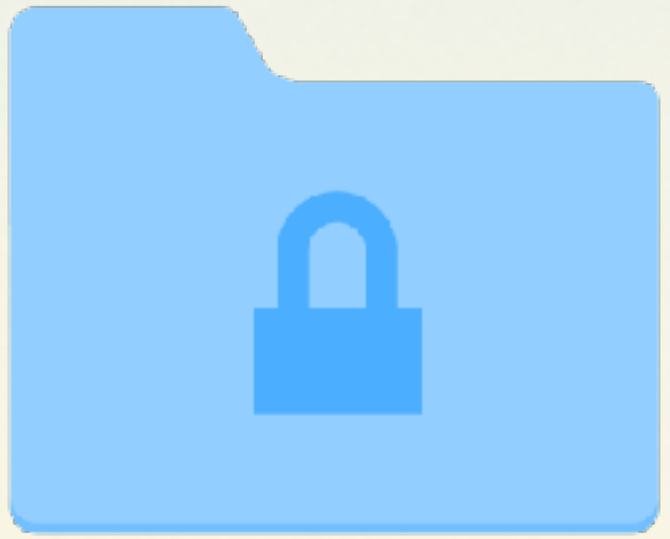


Hardness Assumption

Cryptography and Computational Hardness

Symmetric-key Encryption

Alice and Bob share identical keys.



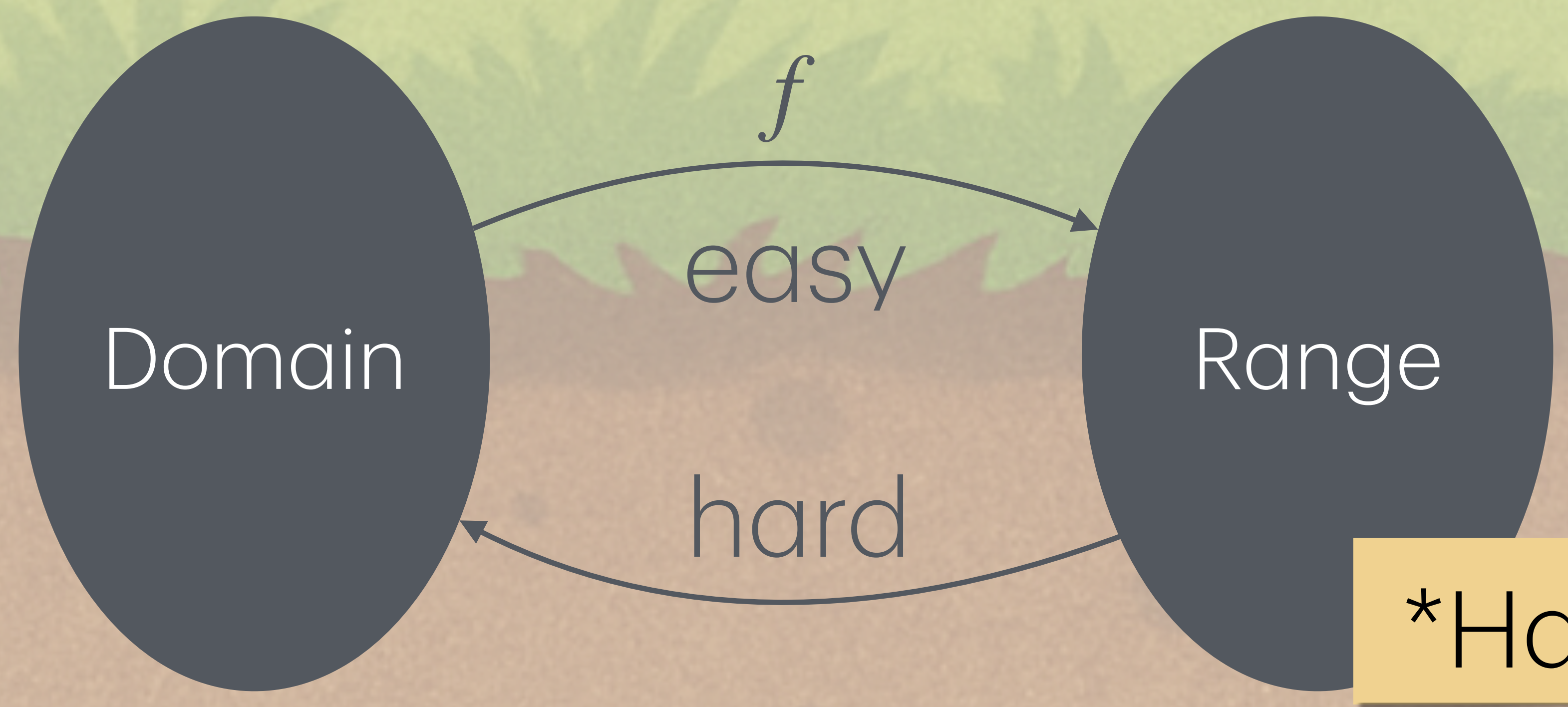
Cryptographic Primitive

Assume the existence of one-way functions.

Security Reduction: A mathematical proof that if any *efficient* adversary can break the scheme, it can also invert the one-way function. A contradiction to the one-wayness, so no such adversary can exist.

One-way Functions

Unstructured!



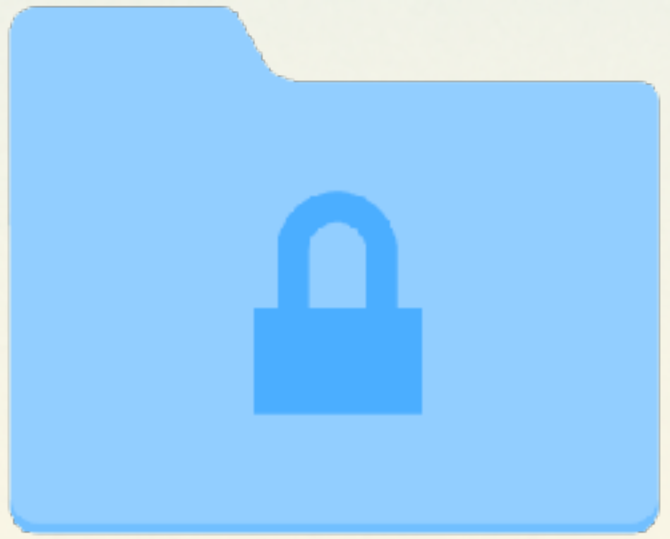
Hardness Assumption

*Hard for **classical** computers.

Cryptography and Computational Hardness

Symmetric-key Encryption

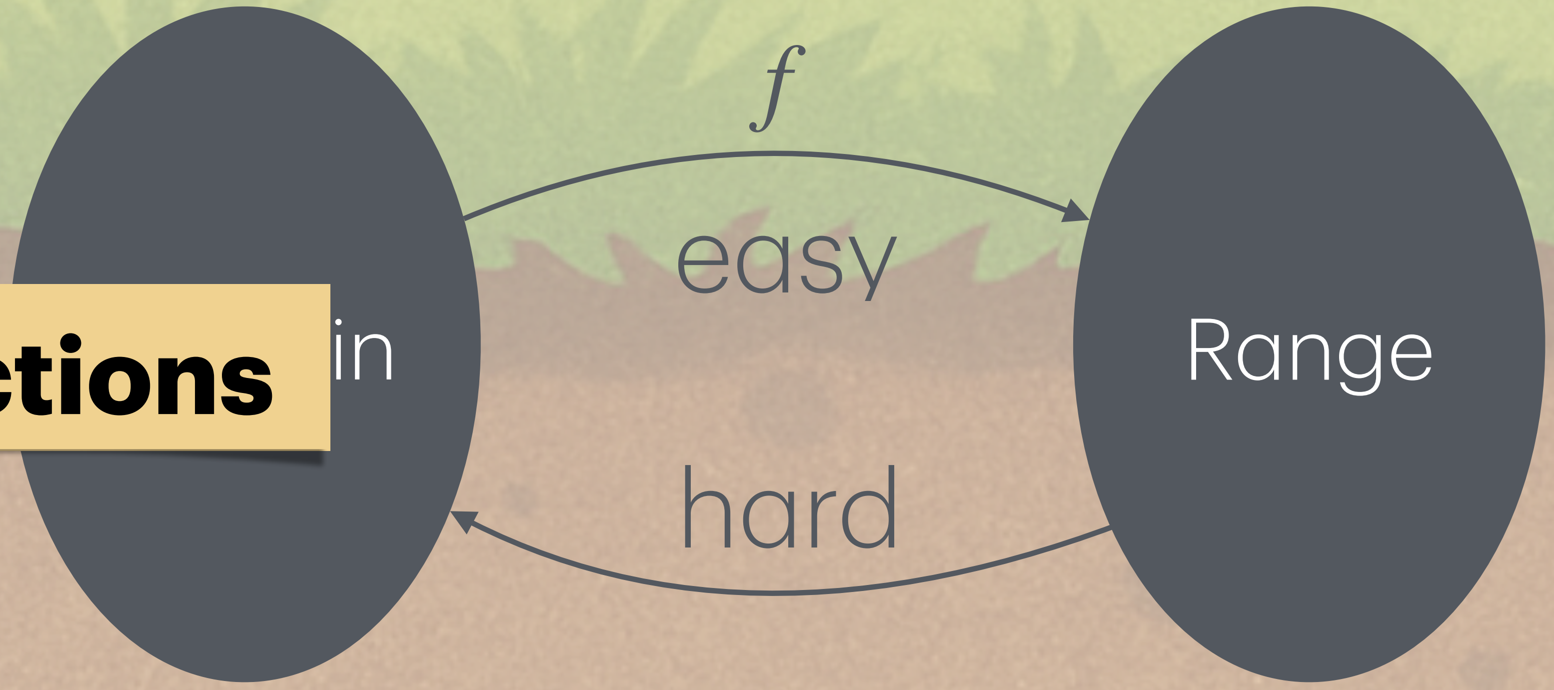
Alice and Bob share identical keys.



Cryptographic Primitive

Assume the existence of one-way functions.

Arguably believable with little to no anxiety!



Quantum-hard One-way Functions

Unstructured!

Hardness Assumption

Cryptography and Computational Hardness

Minicrypt [Impagliazzo '95]

Symmetric-key Encryption

Digital Signatures

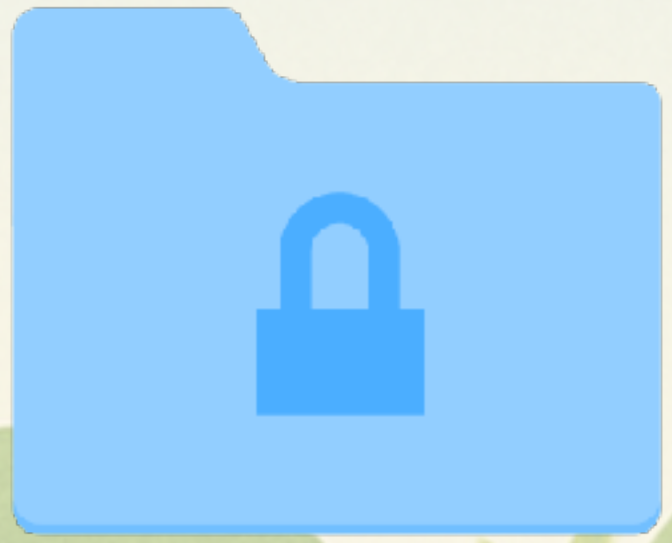
Commitment Schemes

Pseudorandom Number Generators

One-way Functions

Symmetric-key Encryption

Alice and Bob share identical keys.



Cryptography and Computational Hardness

Minicrypt [Impagliazzo '95]

Symmetric-key Encryption

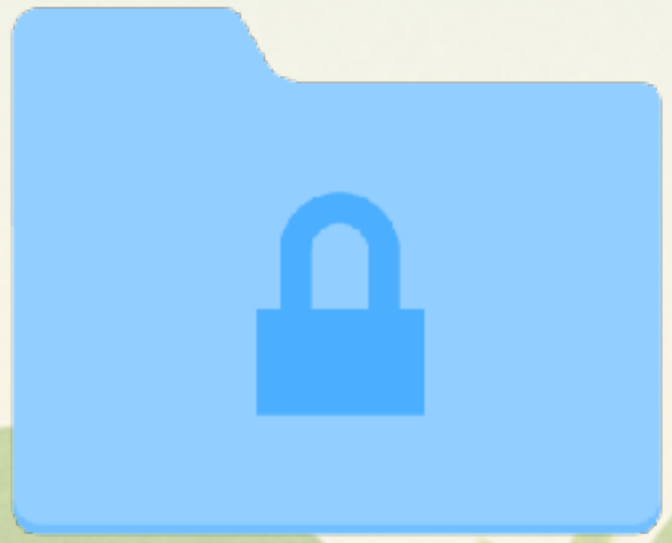
Digital Signatures

Commitment Schemes

Pseudorandom Number Generators

One-way Functions

Symmetric-key Encryption



Alice and Bob share identical keys.

How does Alice communicate an identical key to Bob?
Use symmetric-key encryption?

Cryptography and Computational Hardness

public key

Cryptomania [Impagliazzo '95]

Public-key Encryption

Alice

Alice encrypts a message under Bob's public key, and only Bob can decrypt the ciphertext with his private key.

Bob

private key

Cryptography and Computational Hardness

Cryptomania [Impagliazzo '95]

Public-key Encryption

Solves the key-exchange problem.
But... we need to assume **more** than just the existence of one-way functions!

Structured Hardness Assumptions

Cryptography and Computational Hardness

We assume these are **classically** hard to solve!

Integer Factoring, e.g. recover p, q from $N = p \cdot q$.

Discrete Logarithm, e.g. recover x from g^x for a group generator g.

Learning with errors, e.g. recover $\mathbf{s}$ from $(\mathbf{A}, \mathbf{A} \cdot \mathbf{s} + \mathbf{e})$.

Cryptomania [Impagliazzo '95]

Public-key Encryption

Solves the key-exchange problem.
But... we need to assume **more** than just the existence of one-way functions!

Structured Hardness Assumptions

Cryptography and Computational Hardness

Cryptomania [Impagliazzo '95]

Public-key Encryption

Oblivious Transfer

Structured Hardness Assumptions

Cryptography and Computational Hardness

Cryptomania [Impagliazzo '95]

Public-key Encryption

Oblivious Transfer

Fully Homomorphic Encryption

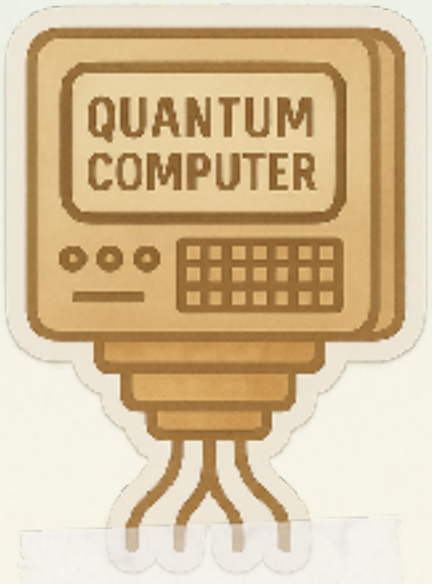
etc.

"Advanced cryptographic primitives"

More structure —> more useful & more vulnerable.

Structured Hardness Assumptions

A Post-quantum World



What about **quantum** computing?

Cryptomania [Impagliazzo '95]

Public-key Encryption

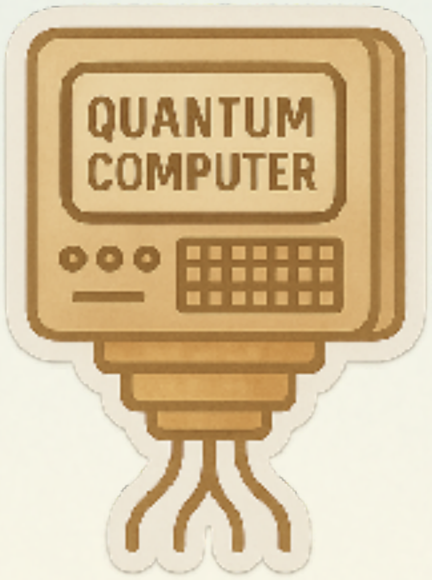
Oblivious Transfer

Fully Homomorphic Encryption

etc.

Structured Hardness Assumptions

A Post-quantum World



quantum algorithms

Integer Factoring, e.g. recover p, q from $N = p \cdot q$.

Discrete Logarithm, e.g. recover x from g^x for a group generator g.

Learning with errors, e.g. recover $\mathbf{s}$ from $(\mathbf{A}, \mathbf{A} \cdot \mathbf{s} + \mathbf{e})$.

Cryptomania [Impagliazzo '95]

Public-key Encryption

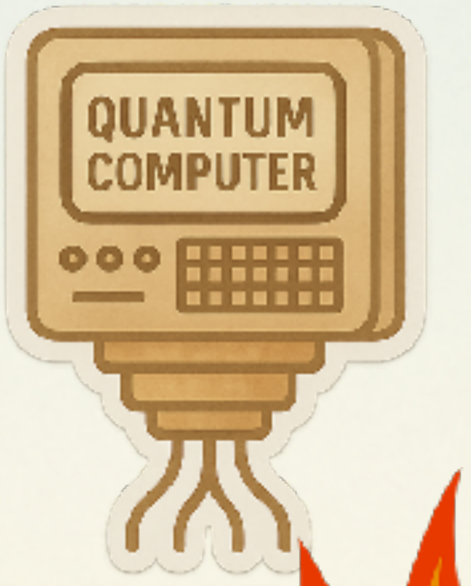
Oblivious Transfer

Fully Homomorphic Encryption

etc.

Structured Hardness Assumptions

A Post-quantum World



easy quantumly

Integer Factoring, e.g. recover p, q from $N = p \cdot q$.

easy quantumly

Discrete Logarithm, e.g. recover x from g^x for a group generator g.

Cryptomania [Impagliazzo '95]

Public-key Encryption

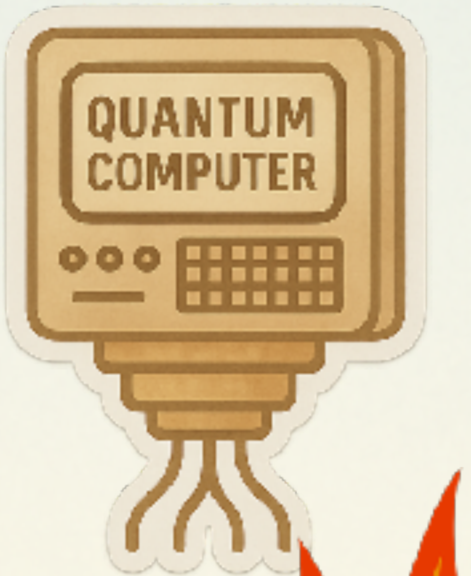
Oblivious Transfer

Fully Homomorphic Encryption

etc.

Structured Hardness Assumptions

A Post-quantum World



Integer Factoring, e.g. recover p, q from $N = p \cdot q$.

Discrete Logarithm, e.g. recover x from g^x for a group generator g.

Cryptomania [Impagliazzo '95]

Public-key Encryption

Oblivious Transfer

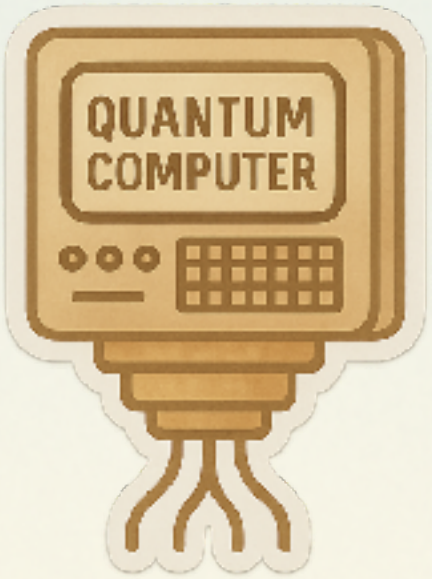
Fully Homomorphic Encryption

etc.

Cryptosystems based on these two hardness assumptions secure much of our digital world today.

Structured Hardness Assumptions

Post-quantum Hardness Assumptions



Cryptomania [Impagliazzo '95]

Public-key Encryption

Oblivious Transfer

Fully Homomorphic Encryption

etc.

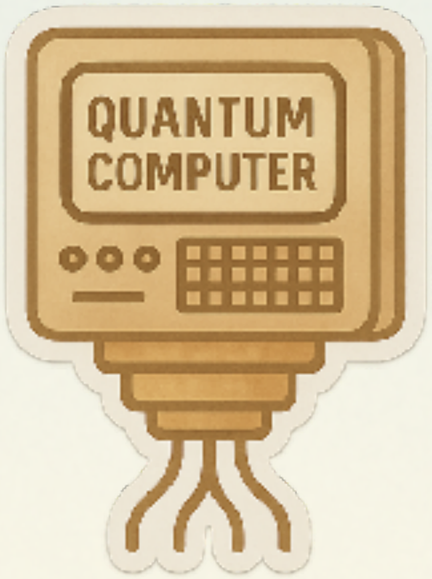
Noisy Linear Assumptions (NLAs),
e.g. LWE, LPN, McEliese

Isogenies

Multivariate Polynomial Systems

Structured Hardness Assumptions

Post-quantum Hardness Assumptions



Cryptomania [Impagliazzo '95]

Public-key Encryption

Oblivious Transfer

Fully Homomorphic Encryption

etc.

Noisy Linear Assumptions (NLAs),
e.g. LWE, LPN, McEliese

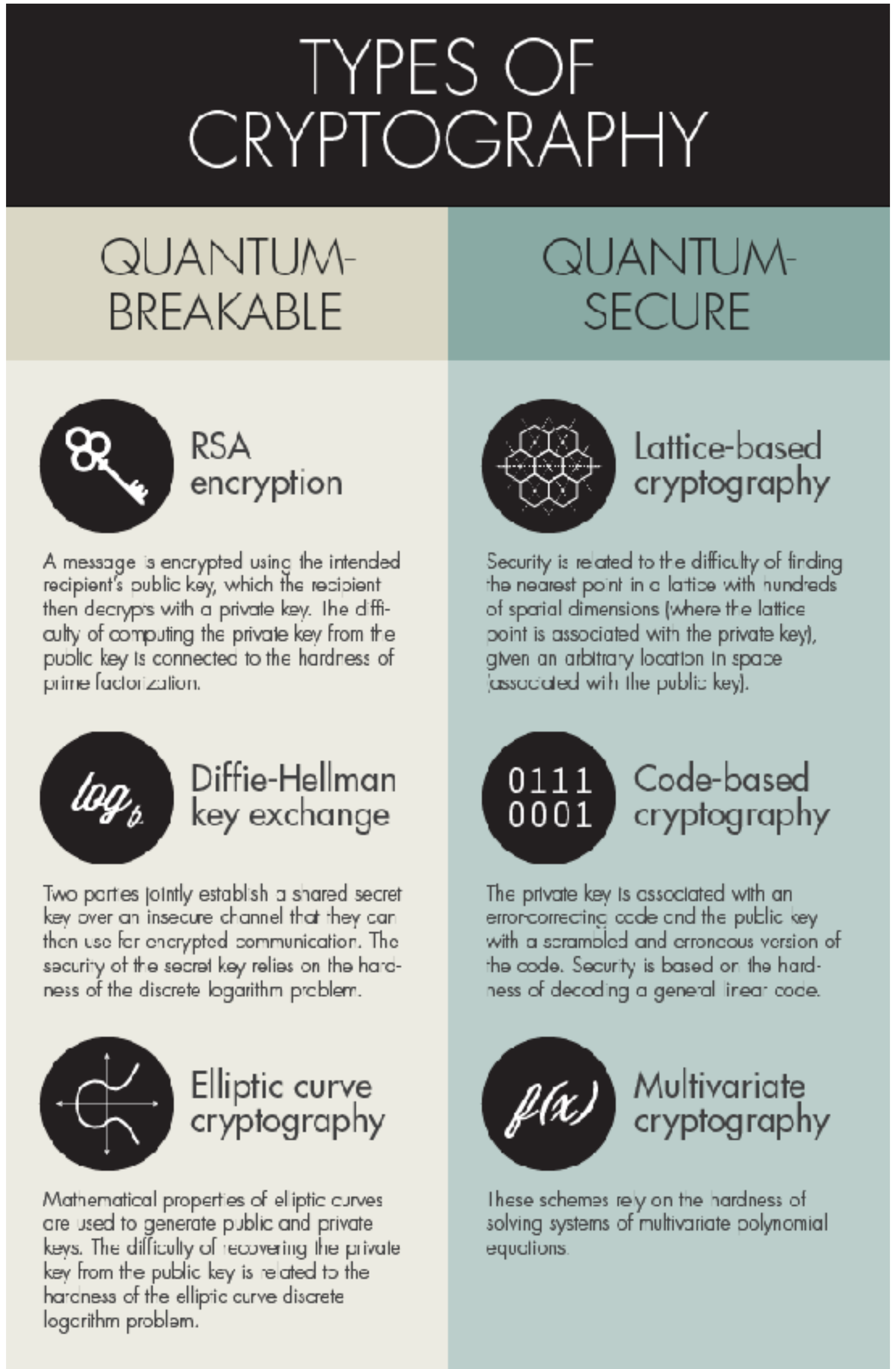
Isogenies

Multivariate Polynomial Systems

*How confident are we that these **structured** problems are hard for quantum computers to solve?*

Structured Hardness Assumptions

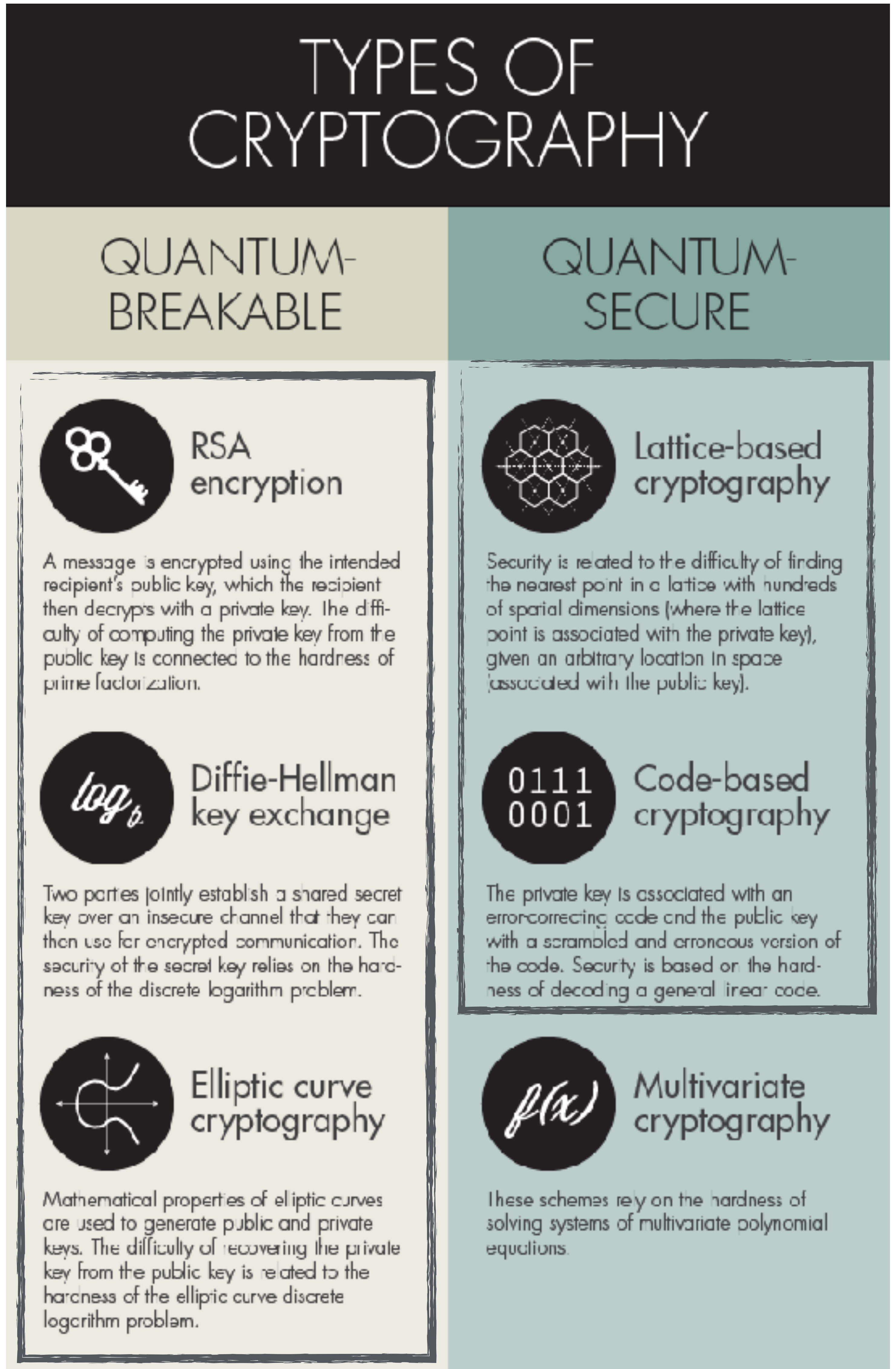
Common Beliefs about Post-quantum Cryptography



Olena Shmahalo/Quanta Magazine
September 8, 2015

Common Beliefs about Post-quantum Cryptography

Slain by Shor's algorithm.

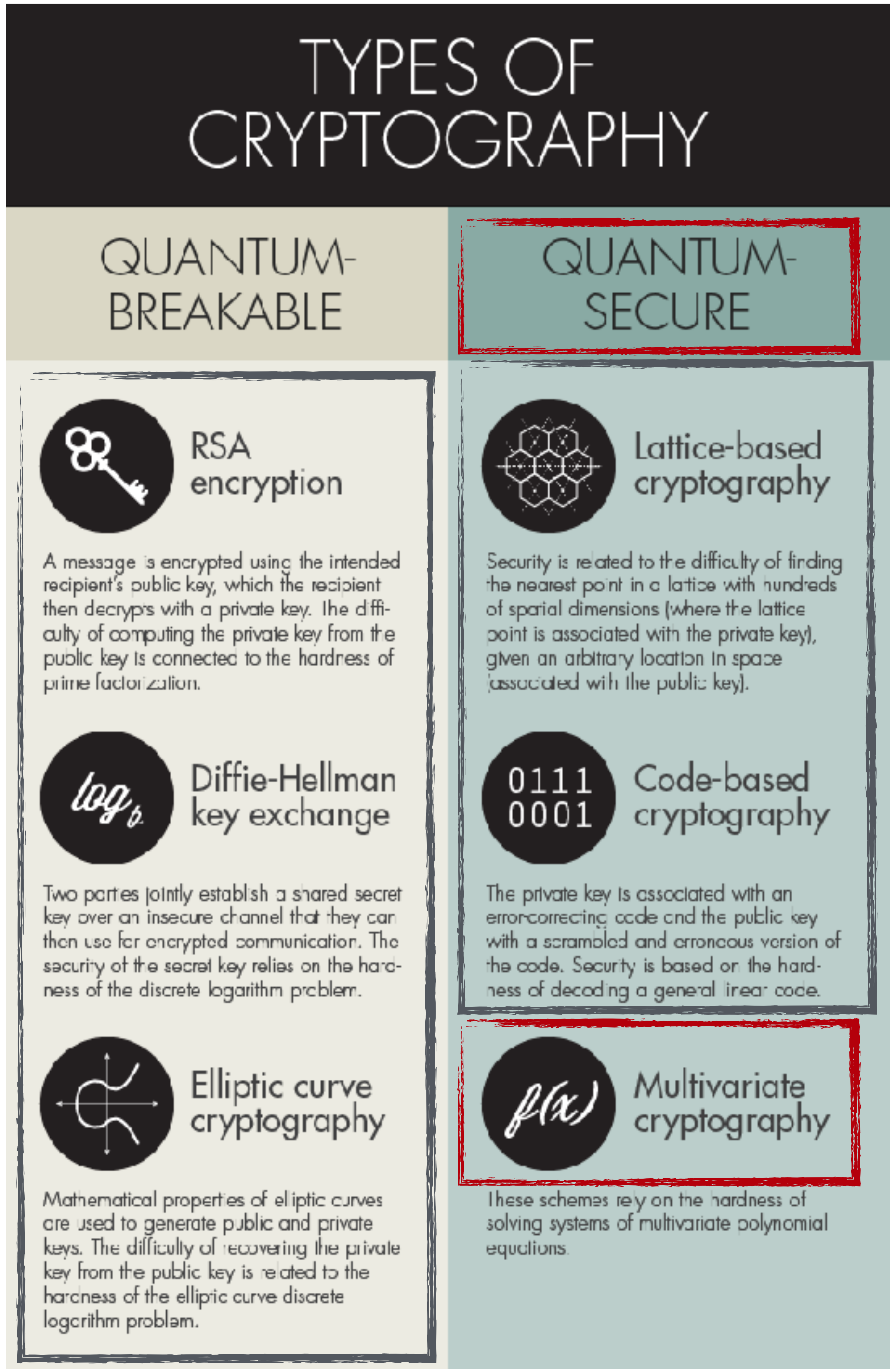


NLAs

Olena Shmahalo/Quanta Magazine
September 8, 2015

Common Beliefs about Post-quantum Cryptography

Slain by Shor's algorithm.

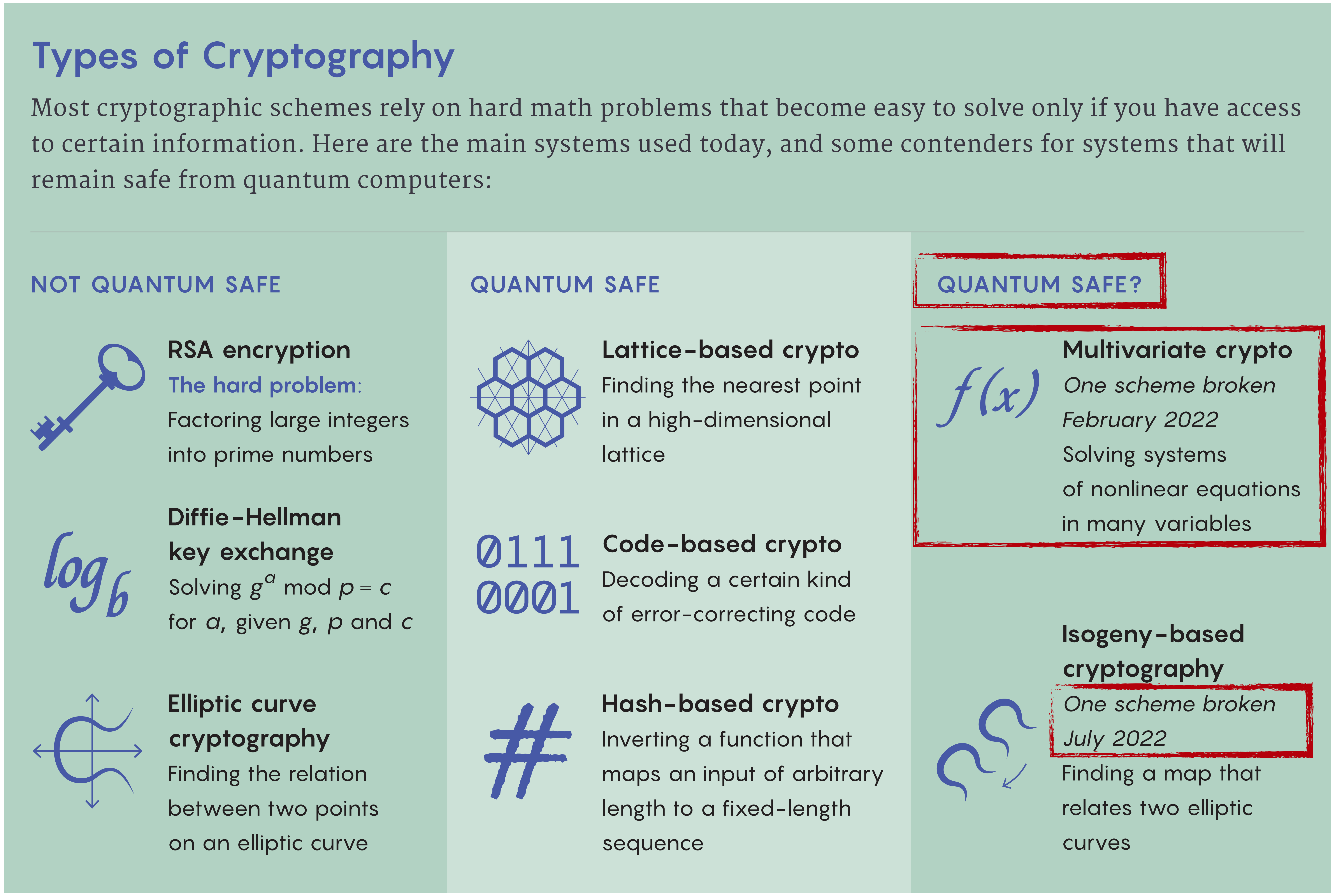


NLAs

Olena Shmahalo/Quanta Magazine

September 8, 2015

Common Beliefs about Post-quantum Cryptography



Merrill Sherman/Quanta Magazine
August 24, 2022

Common Beliefs about Post-quantum Cryptography


CRYPTOGRAPHY

'Post-Quantum' Cryptography Scheme Is Cracked on a Laptop

7

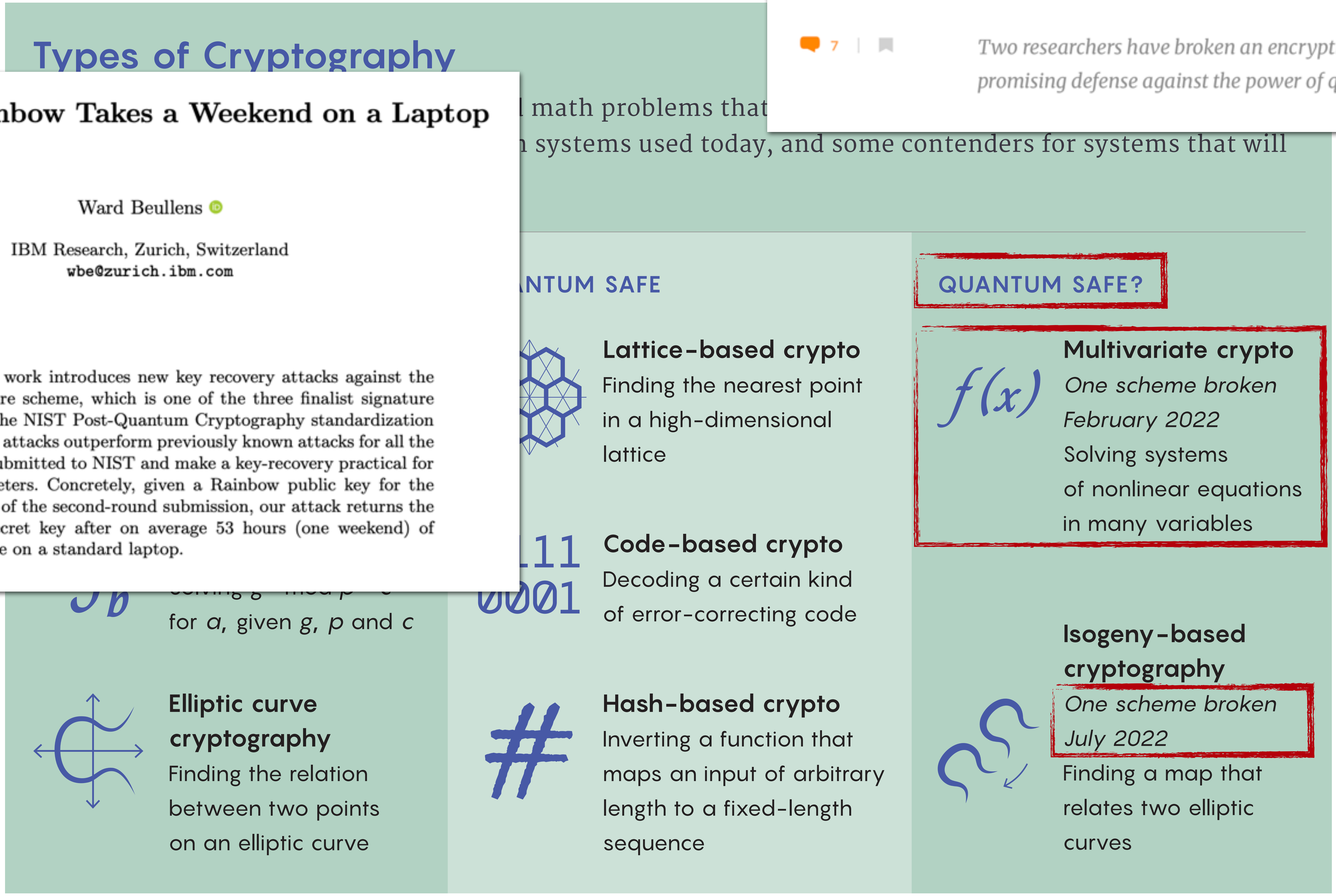
Two researchers have broken an encryption protocol that many saw as a promising defense against the power of quantum computing.

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

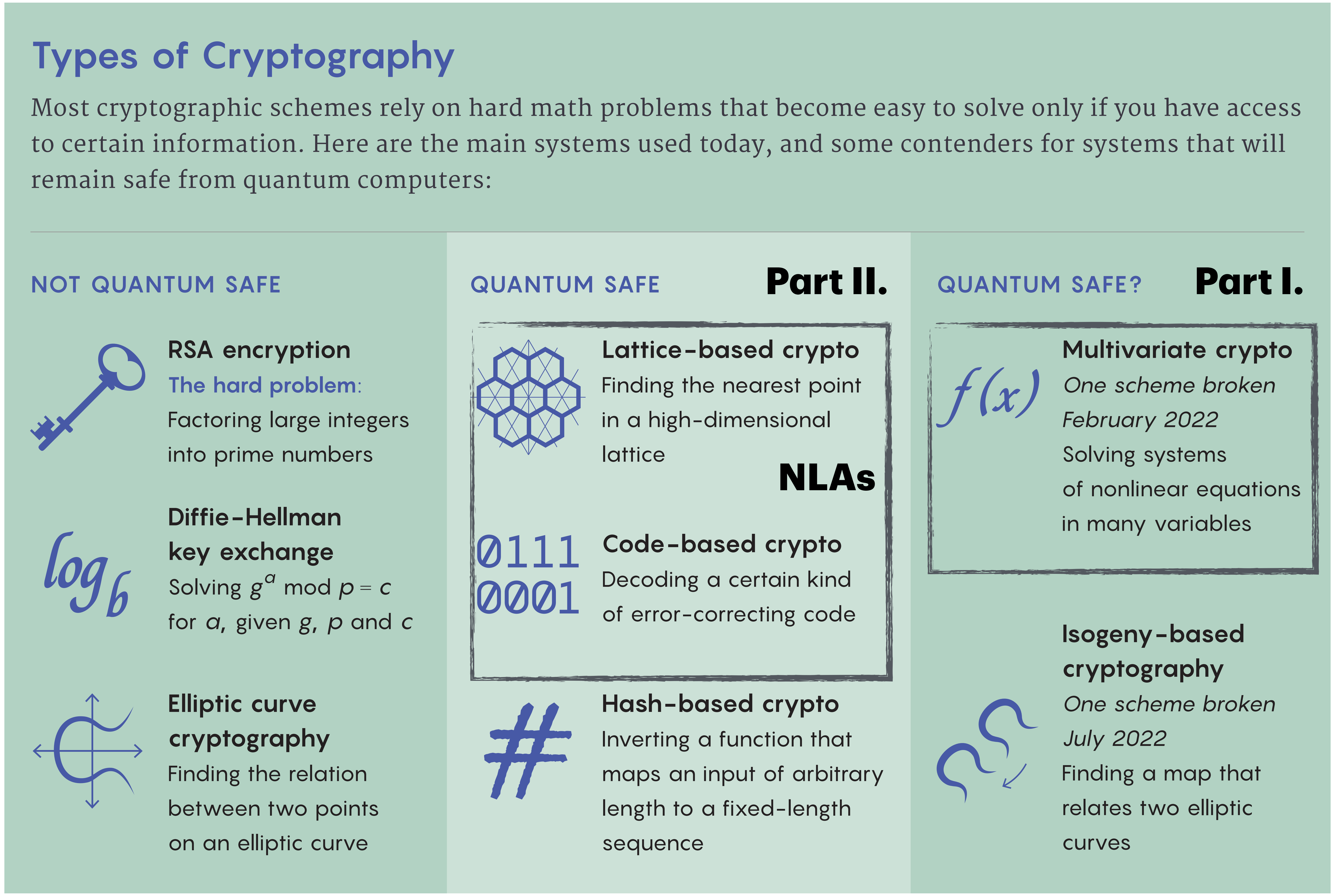
IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.



Merrill Sherman/Quanta Magazine
August 24, 2022

This Thesis:
Reexamining Current Beliefs about Post-quantum Cryptography



Merrill Sherman/Quanta Magazine
August 24, 2022

This Thesis

Challenging Two Beliefs about Post-quantum Hardness

1. Multivariate cryptography is currently believed post-quantum but nearly all cryptanalysis results are classical. Should we be more skeptical?

We give the first evidence for the existence of classically hard-to-solve, yet quantumly easy-to-solve multivariate polynomial systems.

NLAs

NLAs are the most reliable and widely studied assumptions believed to be quantum secure.

NIST Post-quantum Cryptography Standardization Competition Round 3 Finalists for Key-Encapsulation Mechanism (KEM):

- NTRU [Lattice-based].
- SABER [Lattice-based].

Round 4 Submissions for KEM:

- BIKE [Code-based].
- Classic McEliece [Code-based].

Selected Algorithms for KEM

- CRYSTALS-Kyber (2022), FIPS 203. [Lattice-based].
- HQC (2025), FIPS coming soon. [Code-based].

ALL of these practical schemes are NLA-based.

Moreover, almost all *advanced* cryptographic primitives are based on two NLAs — **LWE and LPN.**

This Thesis

Challenging Two Beliefs about Post-quantum Hardness

1. Multivariate cryptography is currently believed post-quantum but nearly all cryptanalysis results are classical. Should we be more skeptical?

We give the first evidence for the existence of classically hard-to-solve, yet quantumly easy-to-solve multivariate polynomial systems.

2. In a world where both LWE and Alekhnovich LPN are (quantumly or classically) broken, can we still build public-key encryption (PKE) from NLAs?

We introduce two new NLAs, and show that in such a world, we can still obtain secure PKE.

Part I: A Quantum Algorithm for Multivariate Polynomial Systems

Based on joint work with Pierre Briaud, Itai Dinur, Riddhi Ghosal, Aayush Jain & Amit Sahai.

Multivariate Polynomial Systems

Example: $\begin{cases} x_1 + x_2 + x_3 + x_1x_3 + 1 = 0 \\ x_1 + x_3 + x_1x_2x_3 = 0 \end{cases}$ is a degree 3 polynomial system

that has $m = 2$ equations over $n = 3$ variables, and $\mathbb{F}_2$-solutions given by $\{(1,0,1), (0,1,0)\}$.

Multivariate Polynomial Systems

Example: $\left\{\begin{array}{r} x_1 + x_2 + x_3 + x_1x_3 + 1 = 0 \\ x_1 + x_3 + x_1x_2x_3 = 0 \end{array}\right\}$ is a degree 3 polynomial system

that has $m = 2$ equations over $n = 3$ variables, and $\mathbb{F}_2$-solutions given by $\{(1,0,1), (0,1,0)\}$.

Uniform Random Polynomial Systems:

For every monomial $\prod_{i \in S} x_i$, for $S \subseteq [n] = \{1,2,\ldots,n\}$, sample a random coefficient from $\mathbb{F}_2$.

Multivariate Polynomial Systems

Example: $\begin{cases} x_1 + x_2 + x_3 + x_1x_3 + 1 = 0 \\ x_1 + x_3 + x_1x_2x_3 = 0 \end{cases}$ is a degree 3 polynomial system

that has $m = 2$ equations over $n = 3$ variables, and $\mathbb{F}_2$-solutions given by $\{(1,0,1), (0,1,0)\}$.

Uniform Random Polynomial Systems:

For every monomial $\prod_{i \in S} x_i$, for $S \subseteq [n] = \{1,2,\ldots,n\}$, sample a random coefficient from $\mathbb{F}_2$.

However, existing cryptographic schemes use **structured** systems, i.e. less secure.

Cryptography Based on Multivariate Polynomials

An Example — Oil & Vinegar Signature Scheme [Patarin '97]

- We have $n = 2k$ variables, and $m = k$ degree-2 equations over $\mathbb{F}_q$ for $k, q \in \mathbb{N}$. These equations are structured, i.e. each quadratic equation has coefficient matrix of the form:

$$\mathbf{A} \triangleq \begin{pmatrix} \mathbf{0} & \mathbf{A}_1 \\ \mathbf{A}_2 & \mathbf{A}_3 \end{pmatrix} \in \mathbb{F}_q^{2k \times 2k}.$$

e.g. $\mathbf{x}^\top \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \mathbf{x} = 3x_1x_2 + 2x_2^2.$

Cryptography Based on Multivariate Polynomials

An Example — Oil & Vinegar Signature Scheme [Patarin '97]

- We have $n = 2k$ variables, and $m = k$ degree-2 equations over $\mathbb{F}_q$ for $k, q \in \mathbb{N}$. These equations are structured, i.e. each quadratic equation has coefficient matrix of the form:

$$\mathbf{A} \triangleq \begin{pmatrix} \mathbf{0} & \mathbf{A}_1 \\ \mathbf{A}_2 & \mathbf{A}_3 \end{pmatrix} \in \mathbb{F}_q^{2k \times 2k}.$$

e.g. $\mathbf{x}^\top \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \mathbf{x} = 3x_1x_2 + 2x_2^2.$

Observe if we assign a value to x_2, then the resulting polynomial is linear in x_1.

Cryptography Based on Multivariate Polynomials

An Example — Oil & Vinegar Signature Scheme [Patarin '97]

- We have $n = 2k$ variables, and $m = k$ degree-2 equations over $\mathbb{F}_q$ for $k, q \in \mathbb{N}$. These equations are structured, i.e. each quadratic equation has coefficient matrix of the form:

$$\mathbf{A} \triangleq \begin{pmatrix} \mathbf{0} & \mathbf{A}_1 \\ \mathbf{A}_2 & \mathbf{A}_3 \end{pmatrix} \in \mathbb{F}_q^{2k \times 2k}.$$

- Sample a random invertible linear transformation $\mathbf{T} : \mathbb{F}_q^{2k} \to \mathbb{F}_q^{2k}$ as the **private signing key.**

- Publish as **the public verification key**, all the transformed coefficient matrices:

$$\{\mathbf{T}^\top \mathbf{A} \mathbf{T}\}_{[k]}.$$

Cryptography Based on Multivariate Polynomials

An Example — Oil & Vinegar Signature Scheme [Patarin '97]

The system $\{\mathbf{x}^\top \mathbf{A}\mathbf{x}\}_{[k]}$ is easy to invert knowing $\{\mathbf{A}\}_{[k]}$: Randomly assign the last k variables, then solve a **linear** system of k equations in k variables.

This enables signing a message $\mathbf{m} \in \mathbb{F}_2^k$, the signature is $\mathbf{T}^{-1} \cdot \mathbf{x}$.

Cryptography Based on Multivariate Polynomials

An Example — Oil & Vinegar Signature Scheme [Patarin '97]

This system is **far from random**. Indeed, there is existing cryptanalysis that enables efficiently forging signatures [Kipnis, Shamir '99].

- Publish as **the public verification key**, all the transformed coefficient matrices:

$$\{\mathbf{T}^{\top}\mathbf{A}\mathbf{T}\}_{[k]}.$$

Cryptography Based on Multivariate Polynomials

An Example — Oil & Vinegar Signature Scheme [Patarin '97]

However, there are parameters for which the known classical attacks fail.
No known quantum attacks.

- Publish as **the public verification key**, all the transformed coefficient matrices:

$$\{\mathbf{T}^{\top}\mathbf{A}\mathbf{T}\}_{[k]}.$$

Cryptography Based on Multivariate Polynomials

An Example — Oil & Vinegar Signature Scheme [Patarin '97]

Our community assumes that this distribution of underdetermined polynomial systems is quantum secure. **Why?**

- Publish as **the public verification key**, all the transformed coefficient matrices:

$$\{\mathbf{T}^\top \mathbf{A} \mathbf{T}\}_{[k]}.$$

Cryptography Based on Multivariate Polynomials

An Example — Oil & Vinegar Signature Scheme [Patarin '97]

In October 2024, UOV was selected as one of the Round-2 candidates of the Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process.

Our Work: Challenging this Belief

We should be more skeptical!

- We construct a candidate distribution of underdetermined multivariate polynomial systems over $\mathbb{F}_2$ that is plausibly classically hard (for the same reasons our community uses to argue that other structured assumptions are hard), yet we give an efficient quantum algorithm solving it.

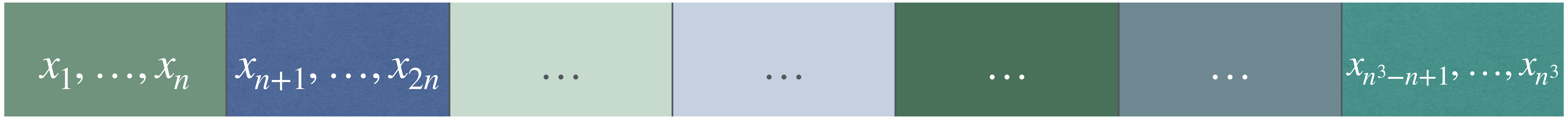
- **Algorithmically exciting!**

  - Existing quantum algorithms for algebraic problems largely exploit **periodicity**. However, *no obvious periodic structure* in multivariate polynomial systems, *nor do we find any*.

  - We use structural properties about the Fourier spectrum related to the distribution of roots.

Our Polynomial System

- Fix $d \geq 3$. Total of n^3 variables, organized into n^2 blocks of n variables.



1. **Degree d constraints**: Sample n^2 many **random** at most degree d polynomials, $\{p_i\}_{i \in [n^2]}$, each on a disjoint block of variables.

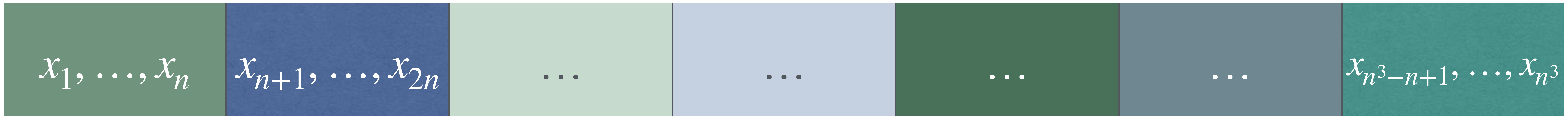
2. **Linear constraints**: a Generalized Reed-Solomon parity-check matrix over the field extension $\mathbb{F}_{2^n}$:

$$\mathbf{H} \in \mathbb{F}_{2^n}^{(1-\alpha)n^2 \times n^2} \leftrightarrow \overline{\mathbf{H}} \in \mathbb{F}_2^{(1-\alpha)n^3 \times n^3}.$$

$$\overline{\mathbf{H}} \cdot \mathbf{x} = \mathbf{0}.$$

Our Polynomial System

- Fix $d \geq 3$.Total of n^3 variables, organized into n^2 blocks of n variables.



1. **Degree d constraints**: Sample n^2 many **random** at most degree d polynomials, $\{p_i\}_{i \in [n^2]}$, each on a disjoint block of variables.

2. **Linear constraints**: a Generalized Reed-Solomon parity-check matrix over the field extension $\mathbb{F}_{2^n}$:

$$\mathbf{H} \in \mathbb{F}_{2^n}^{(1-\alpha)n^2 \times n^2} \leftrightarrow \overline{\mathbf{H}} \in \mathbb{F}_2^{(1-\alpha)n^3 \times n^3}.$$

$$\overline{\mathbf{H}} \cdot \mathbf{x} = \mathbf{0}.$$

Each linear constraint allows backsubstitution for 1 variable.

Post-substitution, the degree d constraints are in αn^3 variables.

Our Polynomial System

Known classical attacks fail.

Our Polynomial System

Known classical attacks fail.

Yet, we'll see that we can come up with a quantum attack.

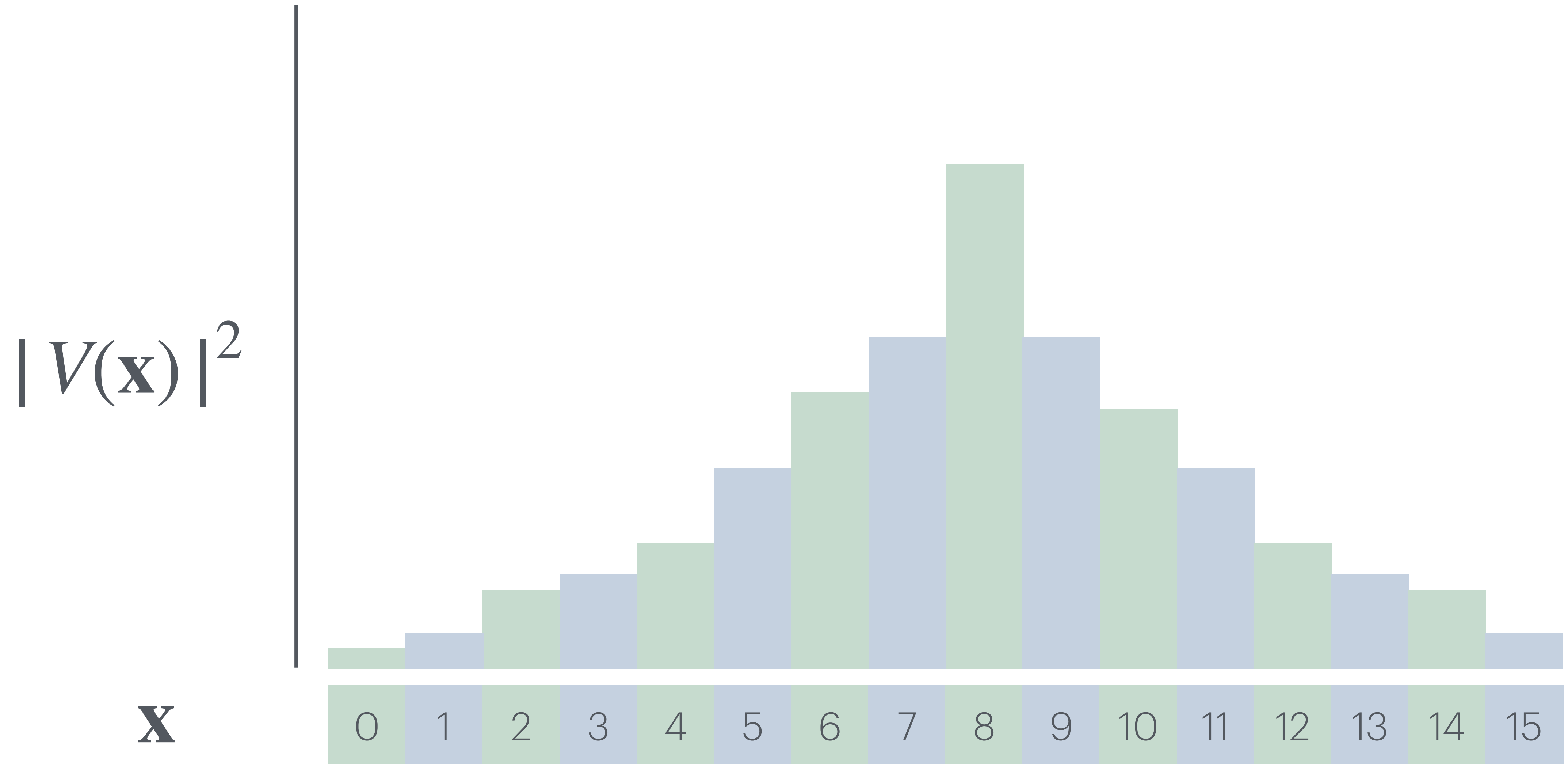
The Yamakawa-Zhandry Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- A standard measurement of a quantum state

$$|\phi\rangle = \sum_{\mathbf{x} \in \mathbb{F}^n} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$$

observes $\mathbf{x}$ with probability $|V(\mathbf{x})|^2$ where $V : \{0,1\}^n \to \mathbb{C}$.



The Yamakawa-Zhandry Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- A standard measurement of a quantum state

$$|\phi\rangle = \sum_{\mathbf{x} \in \mathbb{F}^n} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$$

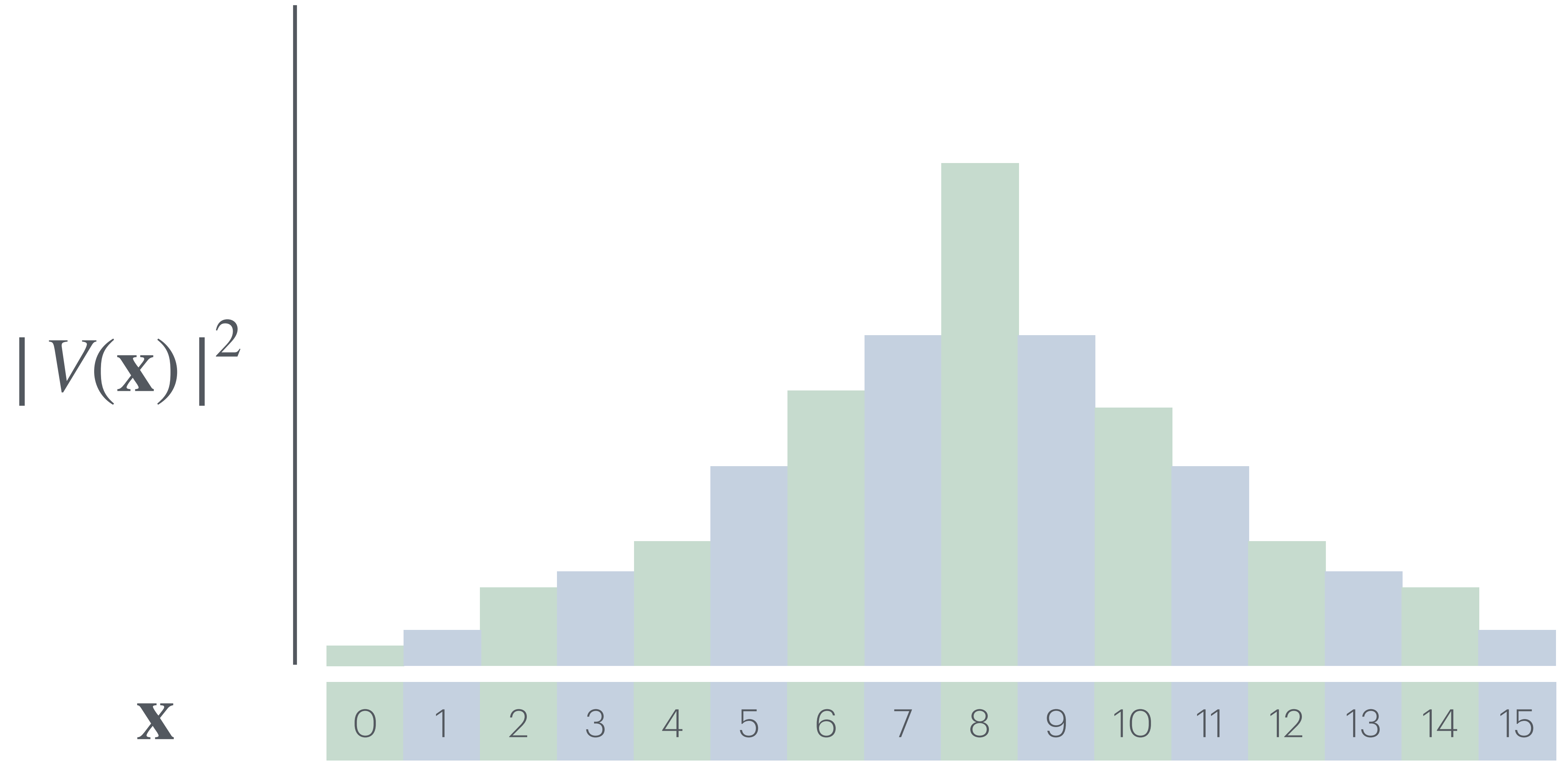
observes $\mathbf{x}$ with probability $|V(\mathbf{x})|^2$ where $V : \{0,1\}^n \to \mathbb{C}$.

- Define

$$|\psi\rangle = \sum_{\mathbf{y} \in \mathbb{F}^N} W(\mathbf{y}) \cdot |\mathbf{y}\rangle.$$

- **Using $|\phi\rangle, |\psi\rangle$, can we produce their coordinate-wise product? i.e.**

$$\sum_{\mathbf{x} \in \mathbb{F}^N} (V \cdot W)(\mathbf{x}) \cdot |\mathbf{x}\rangle.$$



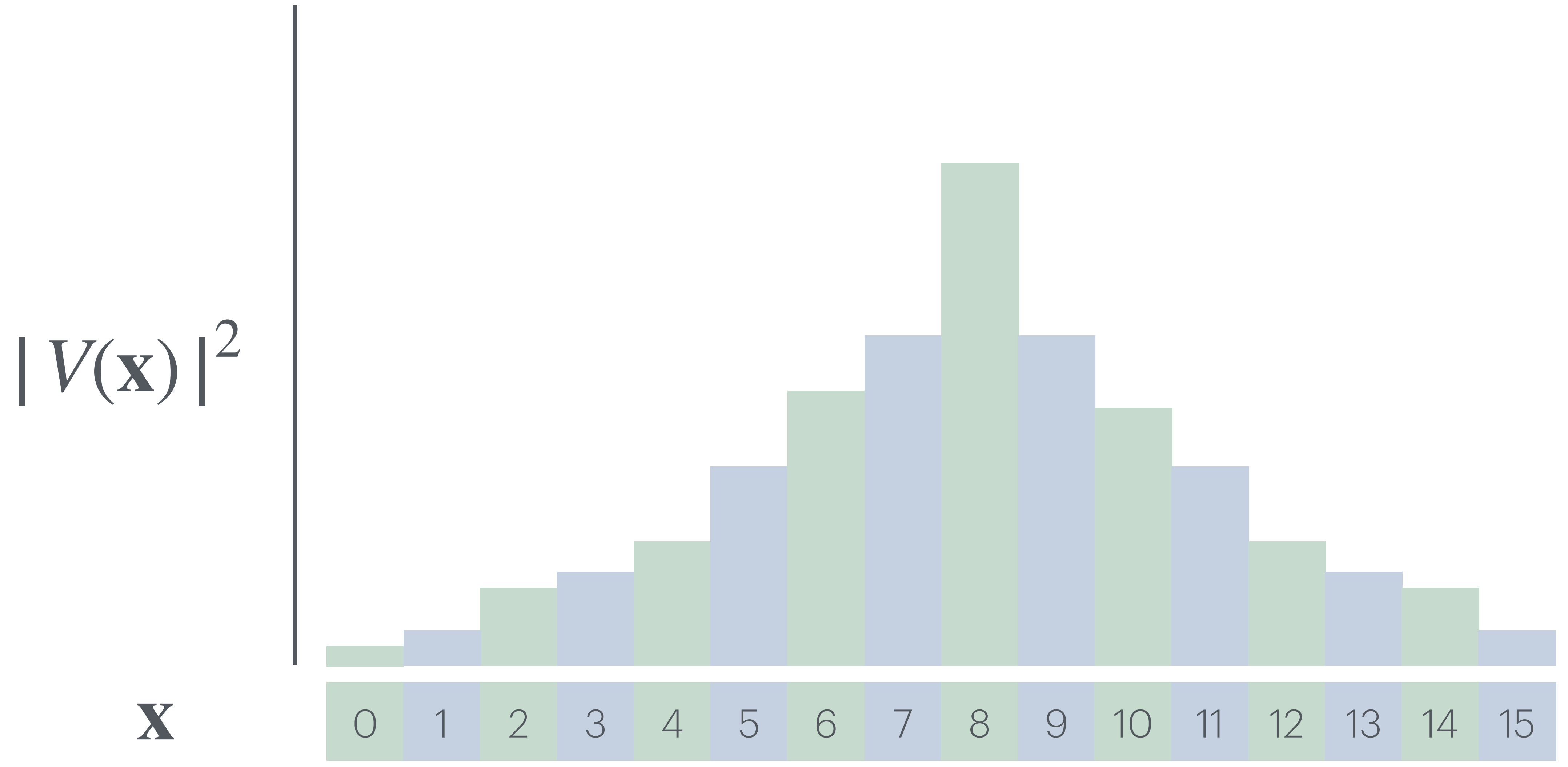
The Yamakawa-Zhandry Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- A standard measurement of a quantum state

$$|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{F}^n} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$$

observes $\mathbf{x}$ with probability $|V(\mathbf{x})|^2$ where $V : \{0,1\}^n \to \mathbb{C}$.



- Define

$$|\psi\rangle = \sum_{\mathbf{y}\in\mathbb{F}^N} W(\mathbf{y}) \cdot |\mathbf{y}\rangle.$$

- **Using $|\phi\rangle, |\psi\rangle$, can we produce their coordinate-wise product? i.e.**

$$\sum_{\mathbf{x}\in\mathbb{F}^N} (V \cdot W)(\mathbf{x}) \cdot |\mathbf{x}\rangle.$$

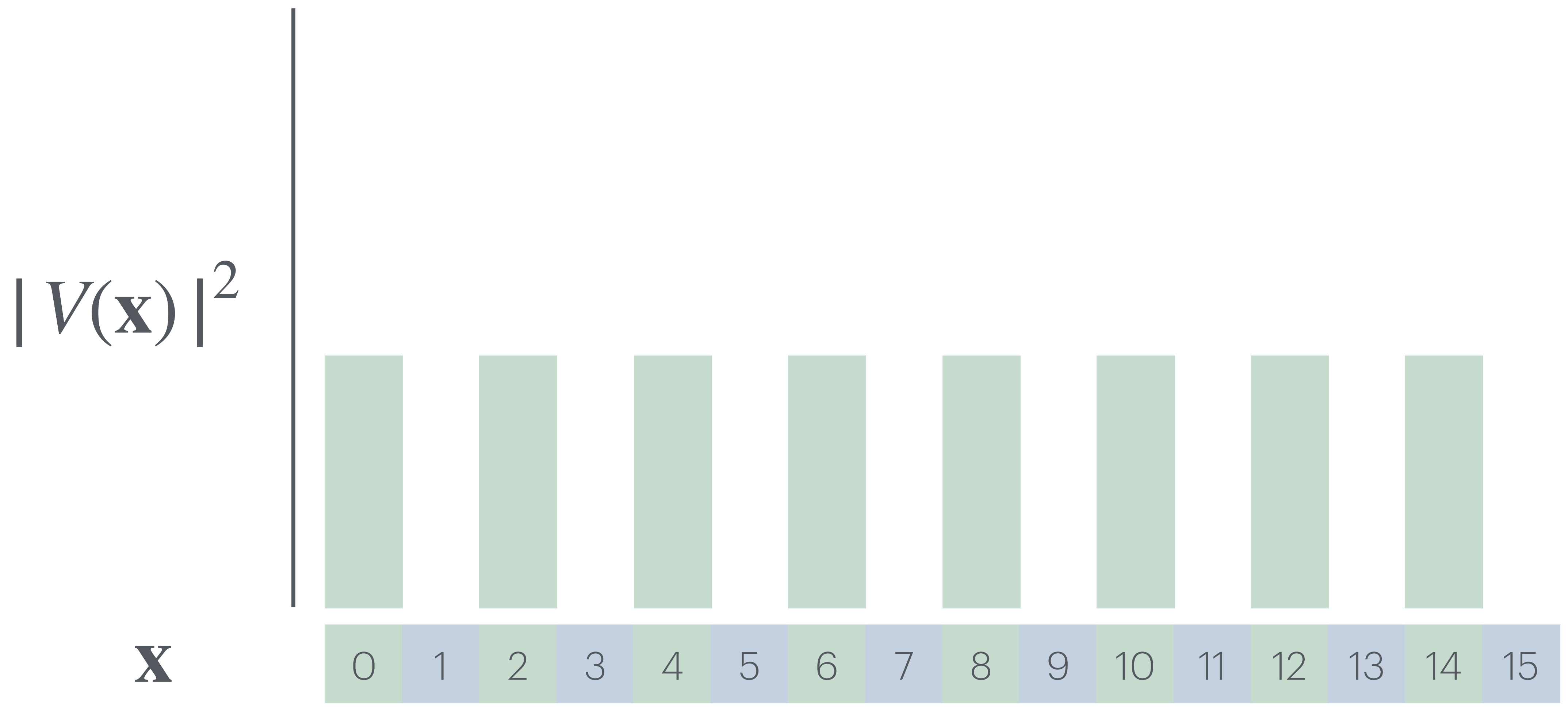
Their tensor contains undesired cross-terms:

$$|\phi\rangle|\psi\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} V(\mathbf{x})W(\mathbf{y}) \cdot |\mathbf{x}\rangle|\mathbf{y}\rangle.$$

The Coordinate-wise Product

- Let $|\phi\rangle$ be a uniform superposition over all codewords of the Generalized Reed-Solomon Code, so measuring this state results in a uniform random codeword, i.e.

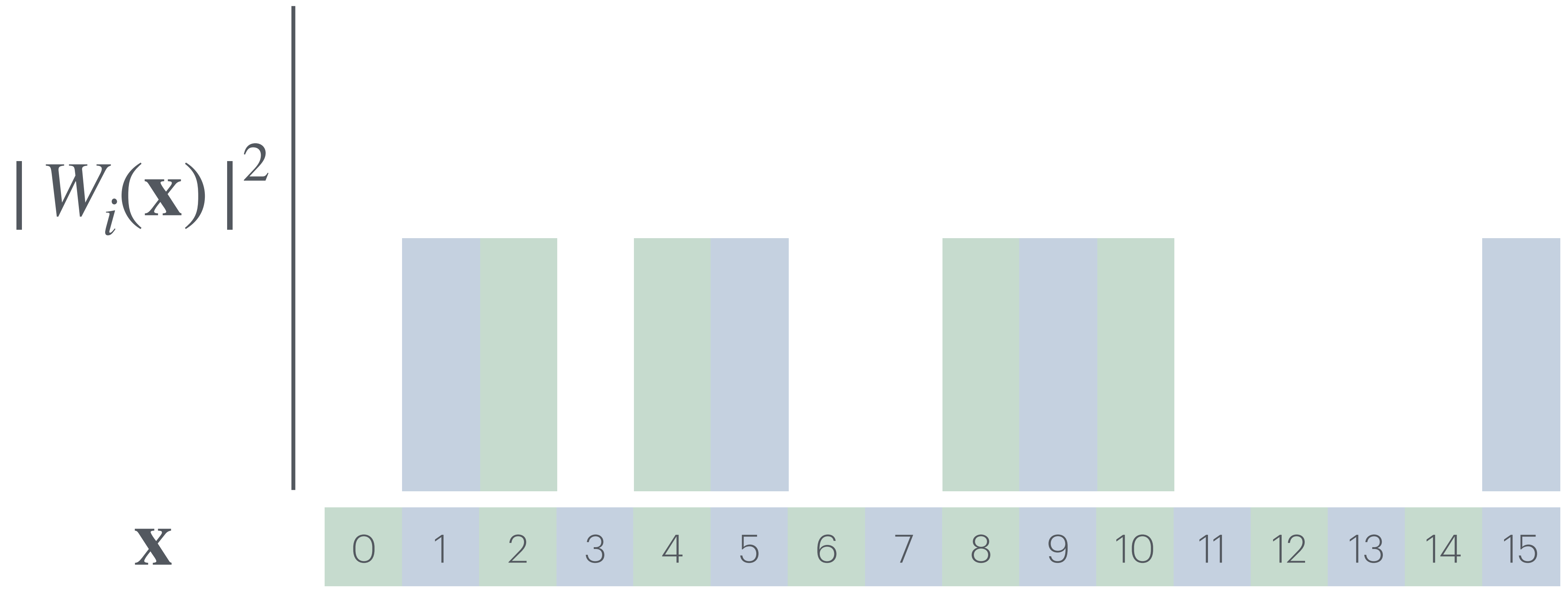
$$|\phi\rangle = \sum_{\mathbf{x} \in \mathbb{F}^N} V(\mathbf{x}) \cdot |\mathbf{x}\rangle, \text{ where } V(\mathbf{x}) = \begin{cases} 1/\sqrt{|C|} & \mathbf{x} \in C \\ 0 & \mathbf{x} \notin C \end{cases}.$$



The Coordinate-wise Product

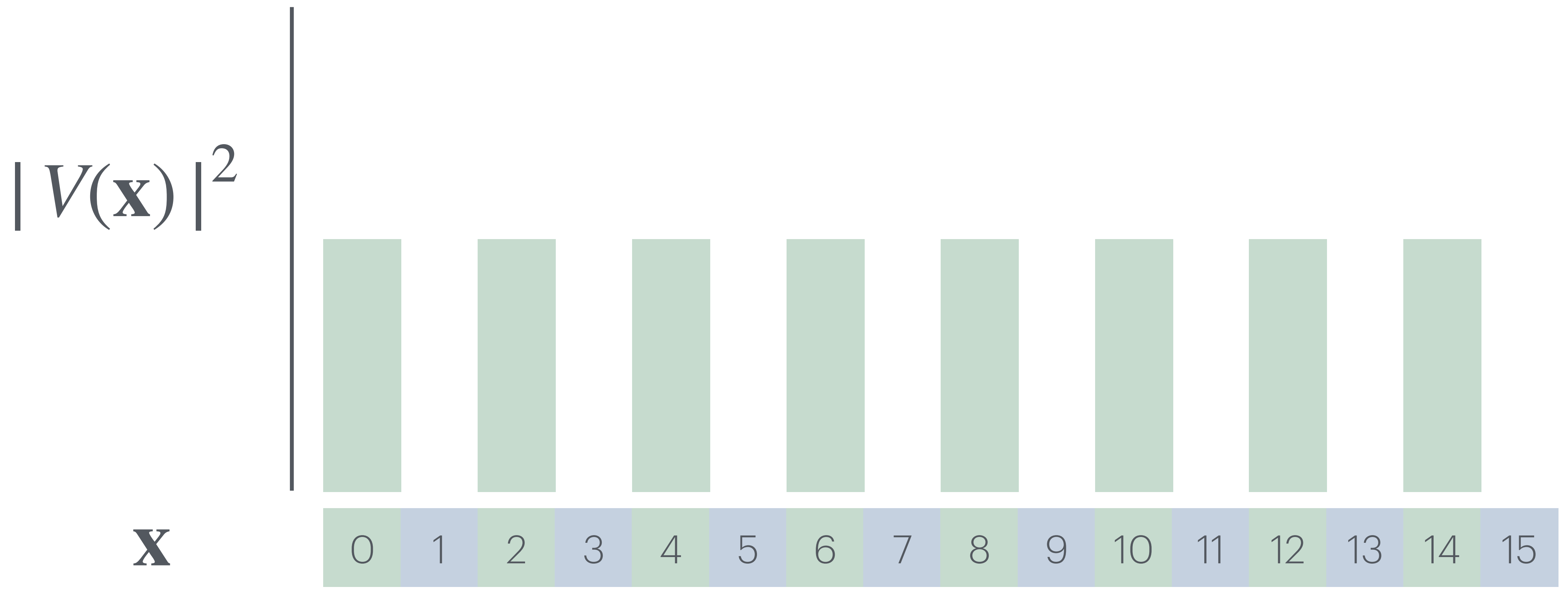
- Let $|\psi\rangle$ be a uniform superposition over all the roots of the degree d constraints, so measuring this state results in a uniform solution to the n^2 many polynomials p_i defined on disjoint variables. i.e. $|\psi\rangle = \bigotimes_{i=1}^{n^2} |\psi_i\rangle$ where for $i \in [n^2]$

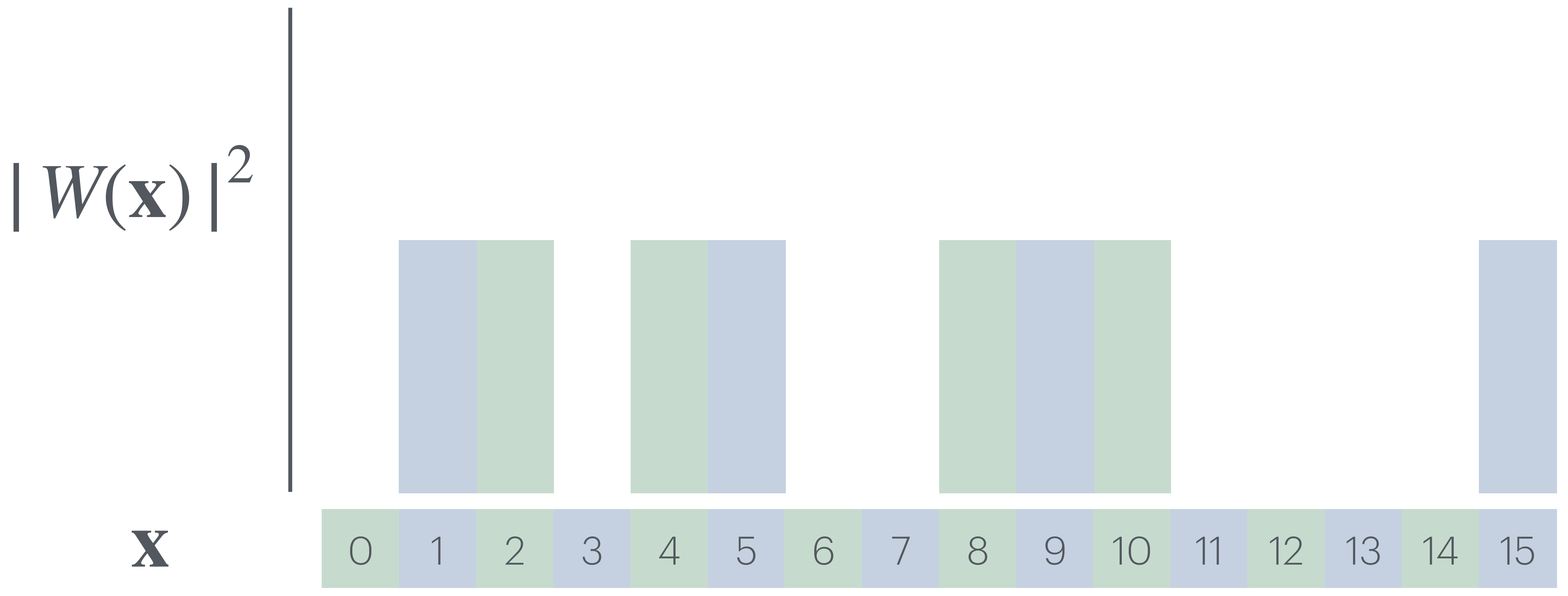
$$|\psi_i\rangle = \sum_{\mathbf{y} \in \mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$



The Coordinate-wise Product

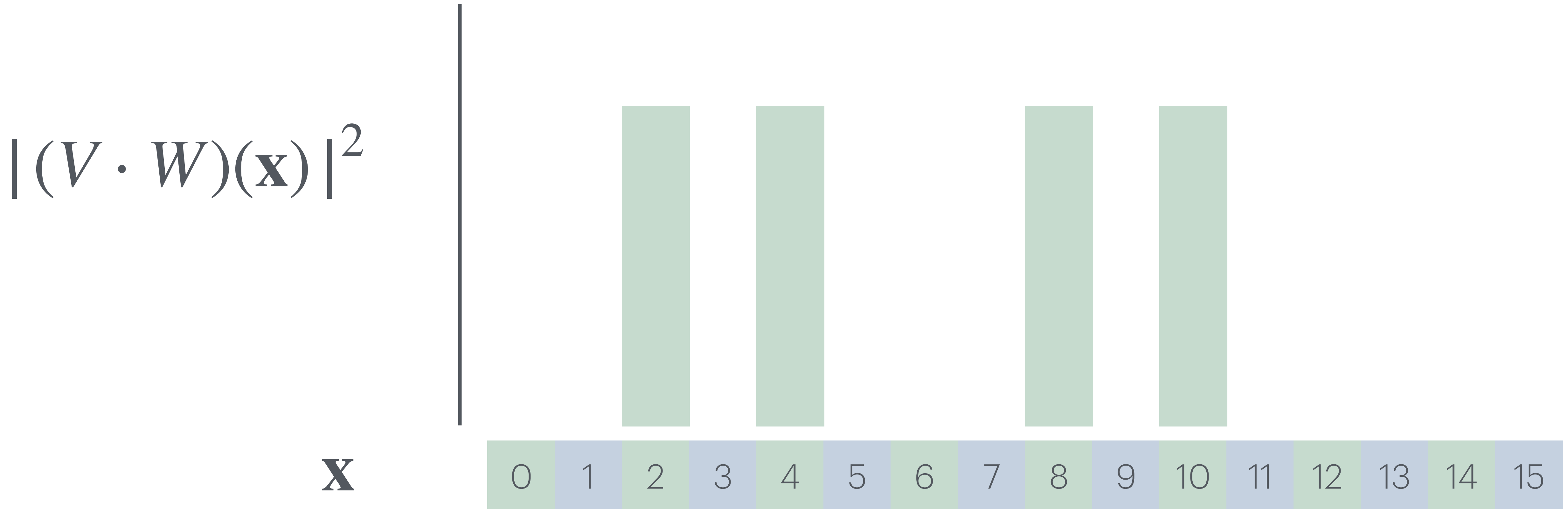
- Solving the polynomial system defined by the code constraint $\overline{\mathbf{H}} \cdot \mathbf{x} = \mathbf{0}$ and the random degree d polynomial system on disjoint variable blocks, $\{p_i\}_{i \in [n]}$, is exactly finding an $\mathbf{x}$ such that $V(\mathbf{x}) \neq 0$ AND $W(\mathbf{x}) \neq 0$.
- Therefore, **measuring the coordinate-wise product always gives us a solution to the polynomial system.**





The Coordinate-wise Product

- Solving the polynomial system defined by the code constraint $\overline{\mathbf{H}} \cdot \mathbf{x} = \mathbf{0}$ and the random degree d polynomial system on disjoint variable blocks, $\{p_i\}_{i \in [n]}$, is exactly finding an $\mathbf{x}$ such that $V(\mathbf{x}) \neq 0$ AND $W(\mathbf{x}) \neq 0$.
- Therefore, **measuring the coordinate-wise product always gives us a solution to the polynomial system.**



The Yamakawa-Zhandry Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- Define $|\hat{\phi}\rangle = \mathsf{QFT}\,|\phi\rangle, |\hat{\psi}\rangle = \mathsf{QFT}\,|\psi\rangle,$ so that

$$|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{y}\rangle.$$

- Apply a unitary addition to add the first register into the second register.

$$\mathbf{U}_{\mathsf{add}}|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{x}+\mathbf{y}\rangle$$

- **Wishful thinking:** If we could _uncompute_ the first register, the resulting state would be

$$\sum_{\mathbf{z}\in\mathbb{F}^N} (\hat{V} * \hat{W})(\mathbf{z})\,|\mathbf{z}\rangle = \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z})\,|\mathbf{z}\rangle$$

from which we could obtain our desired coordinate-wise product state by inverting the QFT.

The Yamakawa-Zhandry Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- Define $|\hat{\phi}\rangle = \mathrm{QFT}\,|\phi\rangle, |\hat{\psi}\rangle = \mathrm{QFT}\,|\psi\rangle,$ so that

$$|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{y}\rangle.$$

- Apply a unitary addition to add the first register into the second register.

$$\mathrm{U}_{\mathrm{add}}\,|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y})\ |\mathbf{x}\rangle\,|\mathbf{x}+\mathbf{y}\rangle$$

$|\mathbf{0}\rangle$

- **Wishful thinking:** If we could *uncompute* the first register, the resulting state would be

$$\sum_{\mathbf{z}\in\mathbb{F}^N} (\hat{V} * \hat{W})(\mathbf{z})\,|\mathbf{z}\rangle = \mathrm{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z})\,|\mathbf{z}\rangle$$

from which we could obtain our desired coordinate-wise product state by inverting the QFT.

Main Question:
How do you *uncompute* the first register?

The Yamakawa-Zhandry Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- Define $|\hat{\phi}\rangle = \text{QFT}\,|\phi\rangle, |\hat{\psi}\rangle = \text{QFT}\,|\psi\rangle,$ so that

$$|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{y}\rangle.$$

- Apply a unitary addition to add the first register into the second register.

$$\text{U}_{\text{add}}\,|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y})\;|\mathbf{x}\rangle\,|\mathbf{x}+\mathbf{y}\rangle \quad |\mathbf{0}\rangle$$

- **Wishful thinking:** If we could <u>*uncompute*</u> the first register, the resulting state would be

$$\sum_{\mathbf{z}\in\mathbb{F}^N} (\hat{V} * \hat{W})(\mathbf{z})\,|\mathbf{z}\rangle = \text{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z})\,|\mathbf{z}\rangle$$

from which we could obtain our desired coordinate-wise product state by inverting the QFT.

Main Question: How do you *uncompute* the first register?

YZ'22: Treat $\mathbf{y}$ as noise and decode a noisy codeword.

The Quantum Algorithm

1. Prepare uniform superposition over codewords $|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{F}^N} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$ and over roots of each polynomial $|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle$ for $i \in [n^2]$. Let $|\psi\rangle = \otimes_i |\psi_i\rangle$.

2. Compute $\left(\left(I \otimes \mathsf{QFT}^{-1}\right) \circ \mathbf{U}_{\mathsf{Decode}} \circ \mathbf{U}_{\mathsf{add}}\right)(\mathsf{QFT}|\phi\rangle \otimes \mathsf{QFT}|\psi\rangle)$.

3. Measure the second register and output the observation.

Two Technical Challenges

We have that

$$\left(\mathbf{U}_{\text{Decode}} \circ \mathbf{U}_{\text{add}}\right)(\text{QFT}\,|\,\phi\rangle \otimes \text{QFT}\,|\,\psi\rangle) = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{x} - \text{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle$$

The crux:

$$\text{RHS} \approx \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{0}\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle$$

$$\approx = |\,\mathbf{0}\rangle \otimes \text{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z})\,|\,\mathbf{z}\rangle$$

1. For what error distributions can we *uniquely* decode?
2. What error distribution is induced by a uniform distribution over the root set of multivariate polynomials over disjoint variables?

Two Technical Challenges

We have that

$$\left(\mathbf{U}_{\text{Decode}} \circ \mathbf{U}_{\text{add}}\right)(\text{QFT}\,|\,\phi\rangle \otimes \text{QFT}\,|\,\psi\rangle) = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{x} - \text{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle$$

The crux:

i.e. decoding almost always succeeds!

$$\text{RHS} \approx \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{0}\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle$$

$$\approx = |\,\mathbf{0}\rangle \otimes \text{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z})\,|\,\mathbf{z}\rangle$$

1. For what error distributions can we *uniquely* decode?

2. What error distribution is induced by a uniform distribution over the root set of multivariate polynomials over disjoint variables?

1. Uniquely Decodable Error Distributions

YZ'22: Burst error distributions with the following property are uniquely decodable:

$\mathbf{e}_1 \in \mathbb{F}_2^n$	$\mathbf{e}_2 \in \mathbb{F}_2^n$	$\dots$	$\dots$	$\dots$	$\dots$	$\mathbf{e}_{n^2} \in \mathbb{F}_2^n$

$$\text{for all } i \in [n^2],\ \mathbf{e}_i = \begin{cases} \mathbf{0} & \text{w.p. } 1/2 \\ \text{Unif}(\mathbf{F}_2^n \backslash \mathbf{0}) & \text{w.p. } 1/2 \end{cases}.$$

Our work: Extends to burst error distributions where blocks $\mathbf{0}$ are probability $1/2$, and have probability mass $2^{-\Omega(n)}$ on any point in $\mathbb{F}_2^n \backslash \{\mathbf{0}\}$.

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\psi_i\rangle = \sum_{\mathbf{y} \in \mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$

$$|\hat{\psi}_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} \hat{W}_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } \hat{W}_i(\mathbf{y}) = 2^{-n/2} \cdot \sum_{\mathbf{z}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot (-1)^{\mathbf{y}\cdot\mathbf{z}}.$$

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$

$$|\hat{\psi}_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} \hat{W}_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } \hat{W}_i(\mathbf{y}) = 2^{-n/2} \cdot \sum_{\mathbf{z}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot (-1)^{\mathbf{y}\cdot\mathbf{z}}.$$

What is the distribution over $\mathbb{F}_2^n$ defined by the probability mass function: $\mathbb{E}_{p_i}\left[\|\hat{W}_i(\,\cdot\,)\|^2\right]$?

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$

$$|\hat{\psi}_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} \hat{W}_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } \hat{W}_i(\mathbf{y}) = 2^{-n/2} \cdot \sum_{\mathbf{z}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot (-1)^{\mathbf{y}\cdot\mathbf{z}}.$$

Easy observation: $\mathbb{E}_{p_i}\left[\|\hat{W}_i(\mathbf{0})\|^2\right] = 2^{-n} \cdot \mathbb{E}_{p_i}\left[R_{p_i}\right] = \frac{1}{2}.$

Due to the 1-wise independence of random inhomogeneous degree d polynomials.

2. Distribution Induced by Root Sets are Uniquely Decodable

$$\mathbb{E}_p\left[\|\hat{W}_i(\mathbf{0})\|^2\right] = \frac{1}{2} \text{ (Property 1)}$$

2. Distribution Induced by Root Sets are Uniquely Decodable

$$\mathbb{E}_p\left[\|\hat{W}_i(\mathbf{0})\|^2\right] = \frac{1}{2}$$ (Property 1)

For all $\mathbf{y} \in \mathbb{F}_2^n \backslash \{\mathbf{0}\}, n \geq 10$, we can show that

$$\mathbb{E}_p\left[\|\hat{W}_i(\mathbf{y})\|^2\right] \leq 2^{-n/2}$$ (Property 2) .

2-wise independence of random inhomogeneous degree d polynomials => Property 2.

$\therefore$ **Any** 2-wise independent distribution on $\mathbf{F}_2[x_1, \ldots, x_n]$ gives the above distribution.

Part I Recap:

Classically Hard Systems Can be Quantumly Easy

- Prior to our work, no known polynomial-time quantum algorithms for conjectured classically hard multivariate polynomial systems.

- Our quantum algorithm applies generally to any structured polynomial system with

  1. Variable-disjoint constraints from shift-invariant, 2-wise independent distributions.

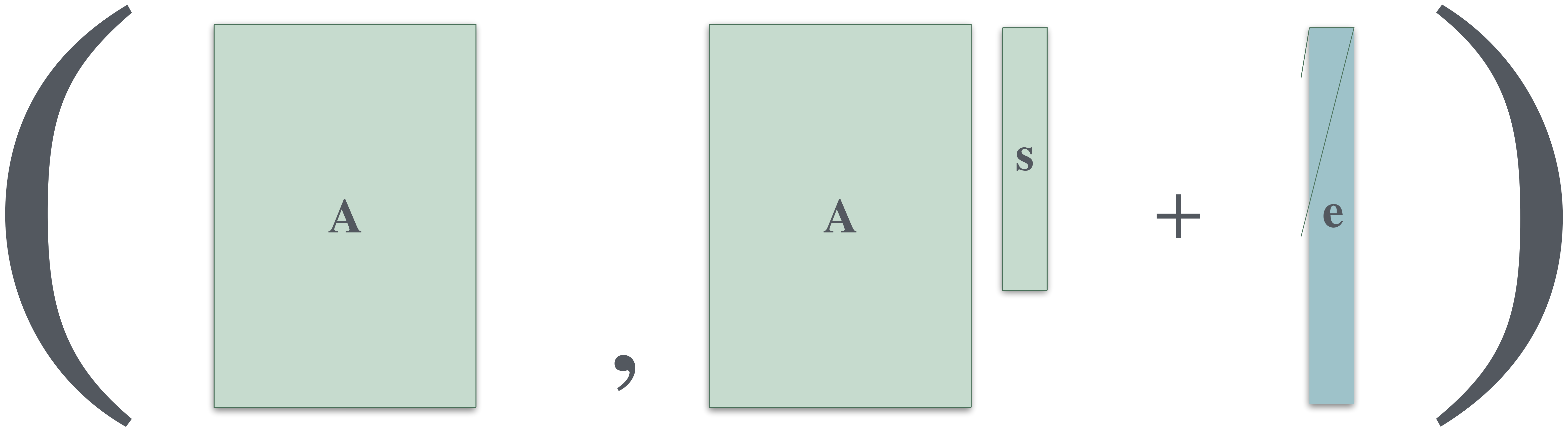
  2. Reed-Solomon code constraints.

Exciting Open Direction:
Alternative methods to uncompute the first register would extend algorithmic approach to other polynomial distributions.

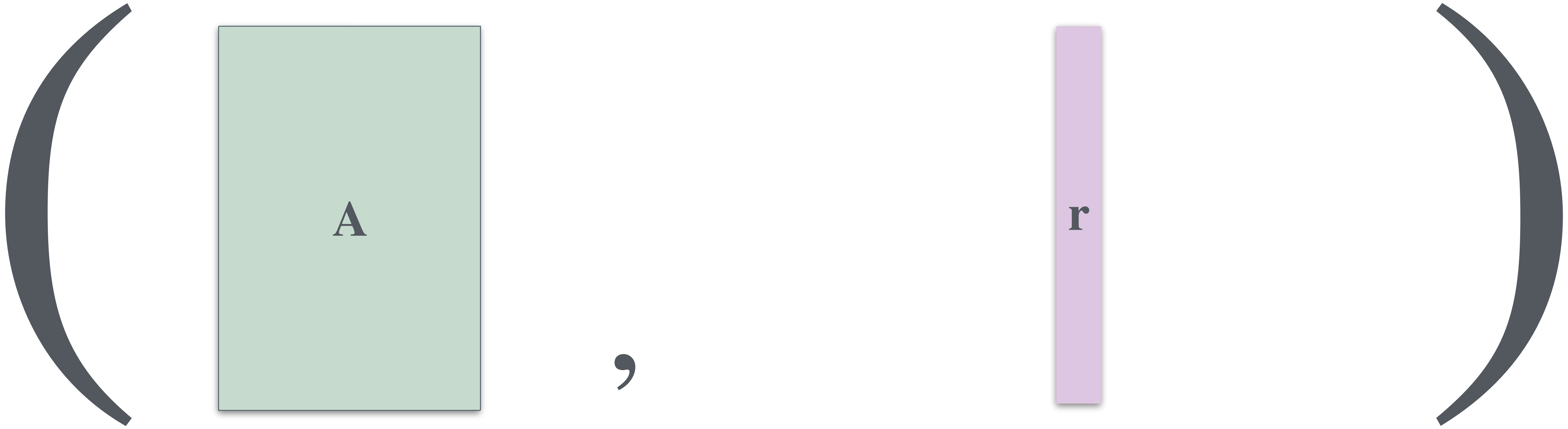
Part II: Public-key Encryption from New Noisy Linear Algebraic Assumptions

Based on joint work with Riddhi Ghosal, Aayush Jain, Amit Sahai & Neekon Vafa.

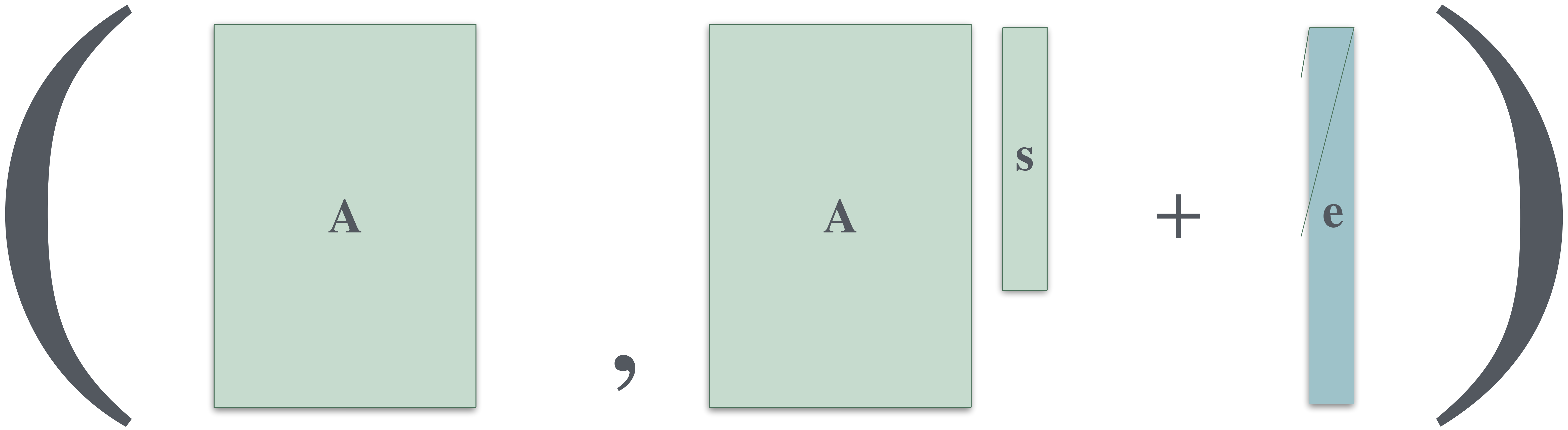
Noisy Linear Algebraic Assumptions



is computationally indistinguishable from

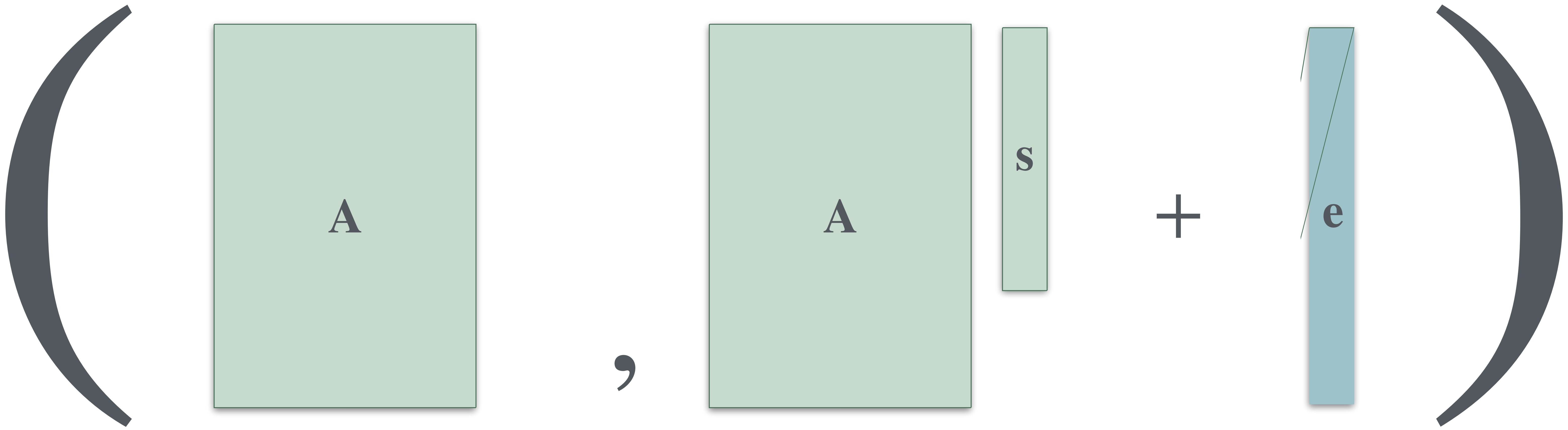


Noisy Linear Algebraic Assumptions



Learning with Errors (LWE):	Uniform over $\mathbb{F}_q^{m\times n}$	Uniform over $\mathbb{F}_q^{n}$	Small error (Discrete Gaussian)
Learning Parity with Noise (LPN):	_	_	Sparse, large error

Noisy Linear Algebraic Assumptions



Learning with Errors (LWE):	Uniform over $\mathbb{F}_q^{m \times n}$	Uniform over $\mathbb{F}_q^n$	Small error (Discrete Gaussian)
Learning Parity with Noise (LPN):	—	—	Sparse, large error

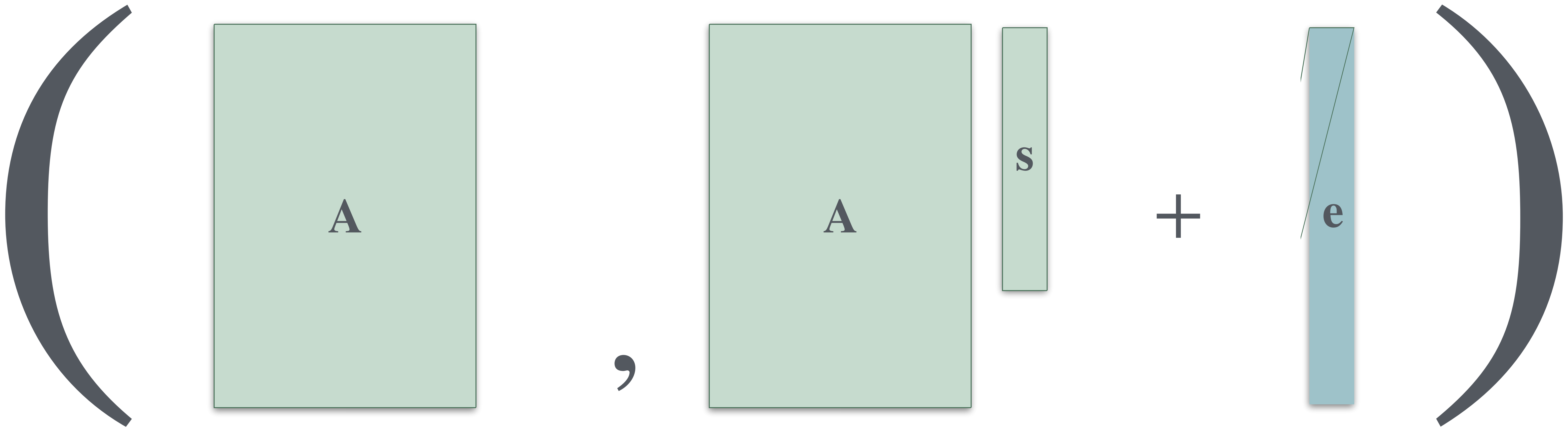
p-sparse means p probability of a non-zero entry. Sparsity is parameterized by the secret dimension. In the *primal*, this is n.

Noisy Linear Algebraic Assumptions

$$\left(\mathbf{A} \;,\; \mathbf{A}\mathbf{s} + \mathbf{e} \right)$$

	$\mathbf{A}$	$\mathbf{s}$	$\mathbf{e}$
Learning with Errors (LWE):	Uniform over $\mathbb{F}_q^{m \times n}$	Uniform over $\mathbb{F}_q^n$	Small error (Discrete Gaussian)
Learning Parity with Noise (LPN):	—	—	Sparse, large error
↳ (Special case of LPN) Alekhnovich LPN:	—	—	$n^{-0.5}$-sparse

Noisy Linear Algebraic Assumptions

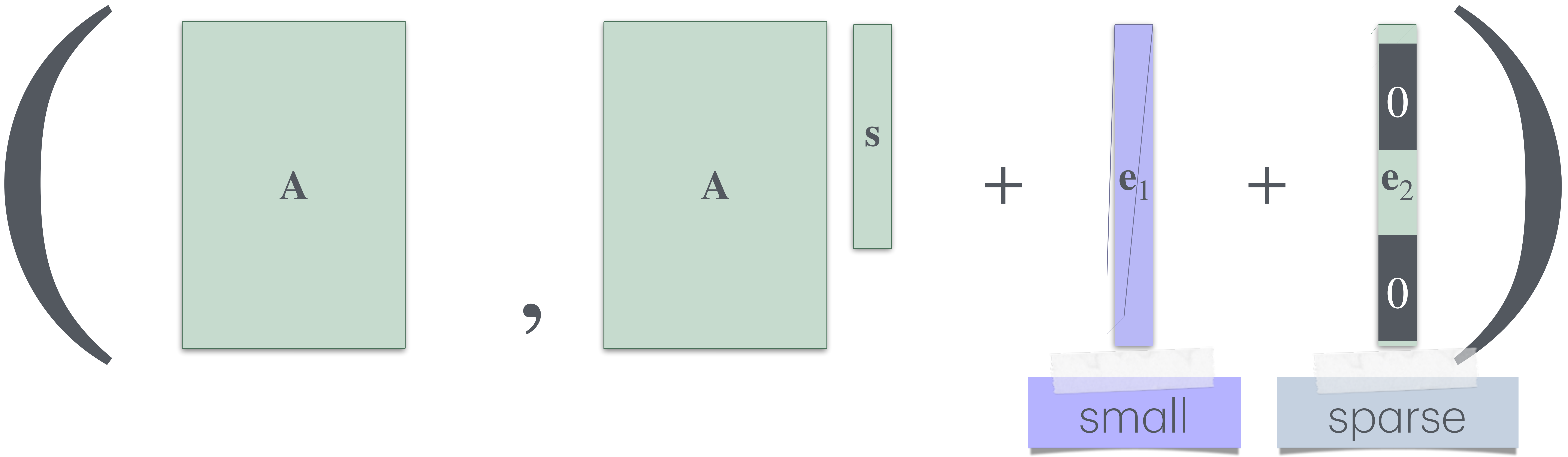


Learning with Errors (LWE): Implies PKE

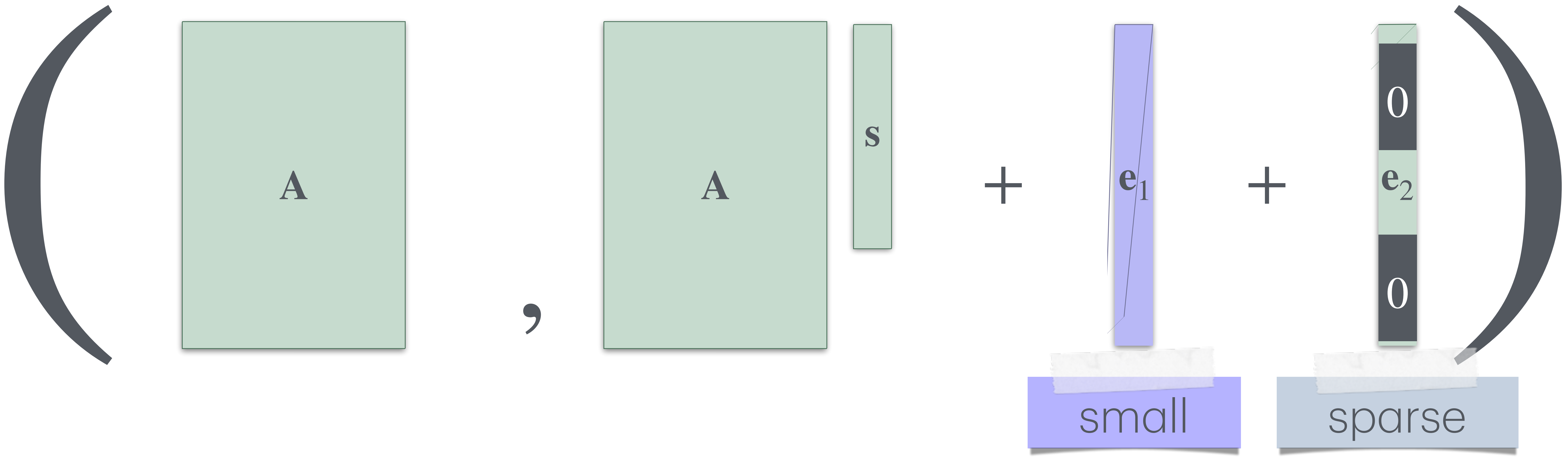
Learning Parity with Noise (LPN): **Alekhnovich Barrier**: LPN not known to imply PKE for $n^{-0.5+\varepsilon}$-sparsity for $\varepsilon > 0$.

(Special case of LPN) Alekhnovich LPN: Implies PKE

Our Work: Learning with Two Errors (LW2E): Beyond LWE and Alekhnovich LPN

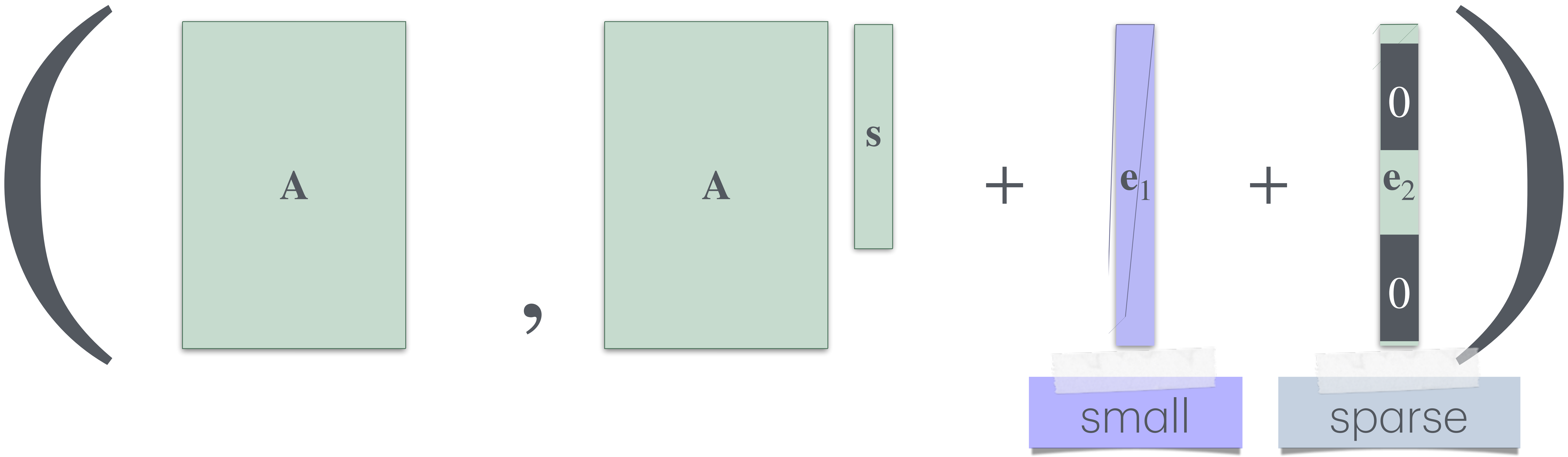


Our Work: Learning with Two Errors (LW2E): Beyond LWE and Alekhnovich LPN



- Provably at least as hard as LWE and LPN!
- Error is neither small nor sparse—intuitively harder!

Our Work: Learning with Two Errors (LW2E): Beyond LWE and Alekhnovich LPN



- Provably at least as hard as LWE and LPN!
- Error is neither small nor sparse—intuitively harder!

Is this useful for **public-key cryptography**?

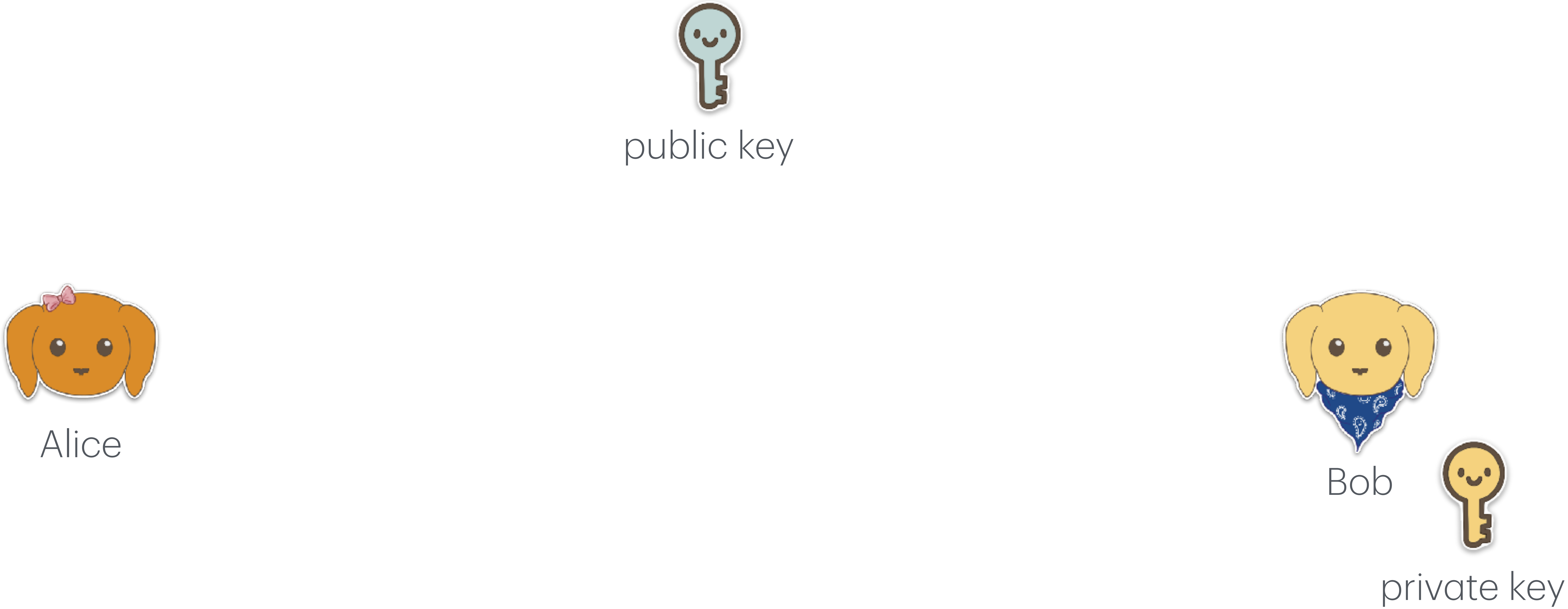
Our Work

We introduce the **Learning with Two Errors (LW2E)** assumption and the **Inhomogeneous Short and Sparse Integer Solution (ISSIS)** assumption.

Main result:

- We give evidence that LW2E and ISSIS—**in a range of parameters that imply public-key encryption (PKE)**—remain secure even if LWE and Alekhnovich LPN are broken.
- For these parameters conjecturably neither are lattice problems.

General Template for PKE from NLAs



General Template for PKE from NLAs

Let's assume $m = O(n)$. (For simplicity.)

public key

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) \in \mathbb{F}_q^{m \times n} \times \mathbb{F}_q^m$$

Alice

$x \in \{0,1\}$

Bob

private key

$\mathbf{s} \in \mathbb{F}_q^n$

General Template for PKE from NLAs

Let's assume $m = O(n)$. (For simplicity.)

public key

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) \in \mathbb{F}_q^{m \times n} \times \mathbb{F}_q^m$$

Alice

$x \in \{0,1\}$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

Bob

private key

$\mathbf{s} \in \mathbb{F}_q^n$

General Template for PKE from NLAs

Let's assume $m = O(n)$. (For simplicity.)

public key

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) \in \mathbb{F}_q^{m \times n} \times \mathbb{F}_q^m$$

Alice

$x \in \{0,1\}$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

if $x = 1$, ciphertext is $(\mathbf{r}^\top \cdot \mathbf{A},\ \mathbf{r}^\top \cdot \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q$
where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{error}}$.

Bob

private key

$\mathbf{s} \in \mathbb{F}_q^n$

General Template

Bob receives:

$$(\mathsf{ct}_1, \mathsf{ct}_2) \in \mathbb{F}_q^n \times \mathbb{F}_q$$

Alice

$x \in \{0,1\}$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

if $x = 1$, ciphertext is $(\mathbf{r}^\top \cdot \mathbf{A},\ \mathbf{r}^\top \cdot \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{error}}$.

Bob

private key

$\mathbf{s} \in \mathbb{F}_q^n$

General Template

Bob receives:

$$(\mathsf{ct}_1, \mathsf{ct}_2) \in \mathbb{F}_q^n \times \mathbb{F}_q$$

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

Alice

$x \in \{0,1\}$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

if $x = 1$, ciphertext is $(\mathbf{r}^\top \cdot \mathbf{A},\ \mathbf{r}^\top \cdot \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{error}}$.

Bob

private key

$\mathbf{s} \in \mathbb{F}_q^n$

General Template

Bob receives:

$$(\mathsf{ct}_1, \mathsf{ct}_2) \in \mathbb{F}_q^n \times \mathbb{F}_q$$

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (large)

Alice

$x \in \{0,1\}$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

if $x = 1$, ciphertext is $(\mathbf{r}^\top \cdot \mathbf{A},\ \mathbf{r}^\top \cdot \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{error}}$.

Bob

private key

$\mathbf{s} \in \mathbb{F}_q^n$

General Template

Bob receives:

$$(\mathsf{ct}_1, \mathsf{ct}_2) \in \mathbb{F}_q^n \times \mathbb{F}_q$$

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (large)

if $x = 1$, $\mathbf{r}^\top \cdot \mathbf{e}$ (small)

Alice

$x \in \{0,1\}$

if $x = 0$, ciphertext is $(\mathbf{u}_1, u_2) \leftarrow_\$ \mathbb{F}_q^n \times \mathbb{F}_q$

if $x = 1$, ciphertext is $(\mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{error}}$.

Bob

private key

$\mathbf{s} \in \mathbb{F}_q^n$

General Template for PKE from NLAs

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (large)

if $x = 1$, $\mathbf{r}^\top \cdot \mathbf{e}$ (small)

General Template for PKE from NLAs

To decrypt, Bob computes:

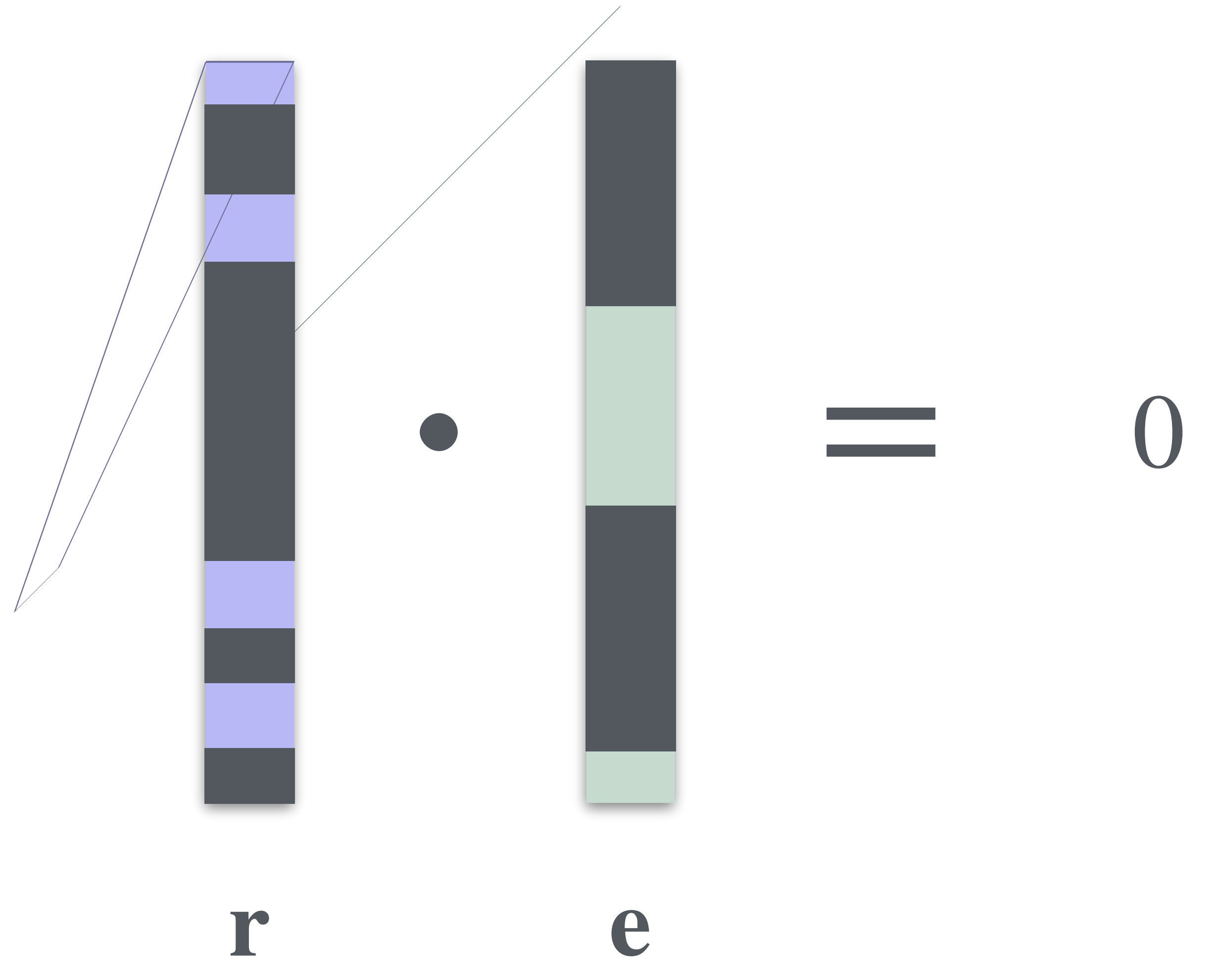
$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (large)

if $x = 1$, $\mathbf{r}^\top \cdot \mathbf{e}$ (small)

In the case of LWE, small.

In the case of LPN, when the sparsity of $\mathcal{D}_{\text{error}}$ is $n^{-0.5}$-sparse, then $\mathbf{0}$.



Can we get PKE from LW2E from the same construction template?

PKE from LW2E—Correctness?

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

PKE from LW2E—Correctness?

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (large)

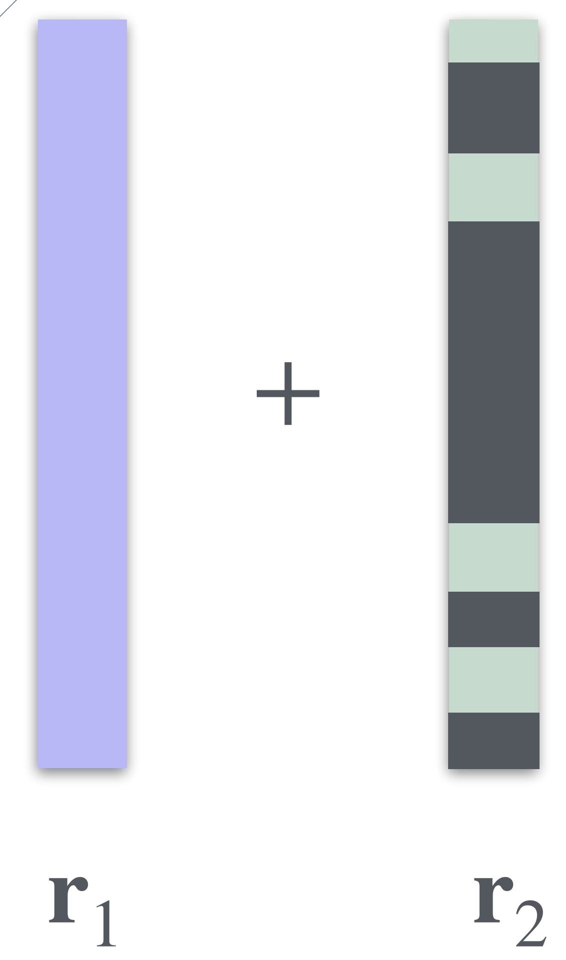
PKE from LW2E—Correctness?

To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (large)

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} = \mathbf{r}_1 + \mathbf{r}_2 \leftarrow_\$ \mathscr{D}_{\text{error}}$.



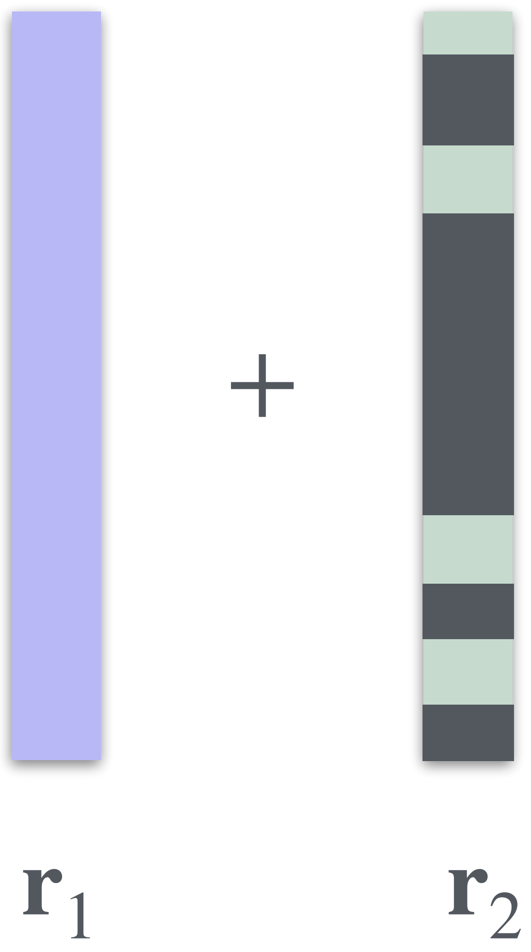
PKE from LW2E—Correctness?

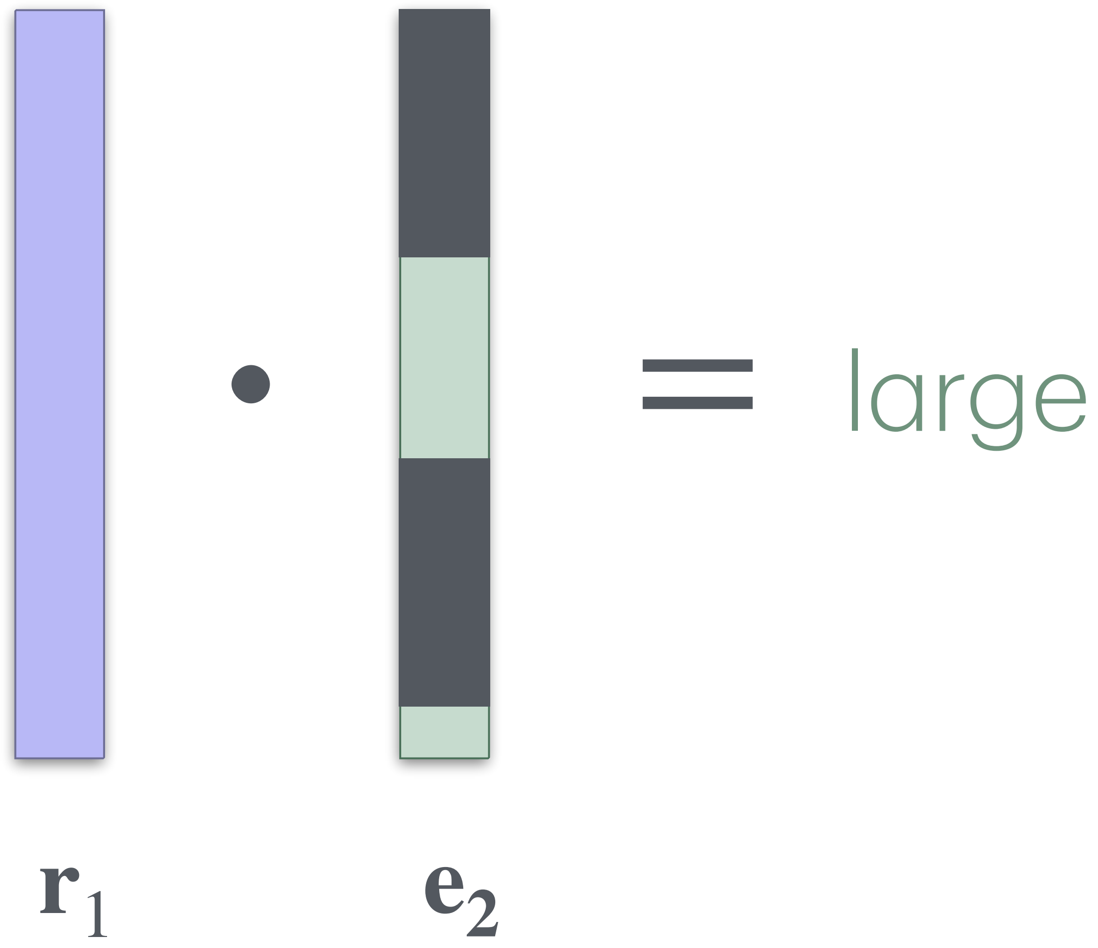
To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (large)

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} = \mathbf{r}_1 + \mathbf{r}_2 \leftarrow_\$ \mathscr{D}_{\text{error}}$.





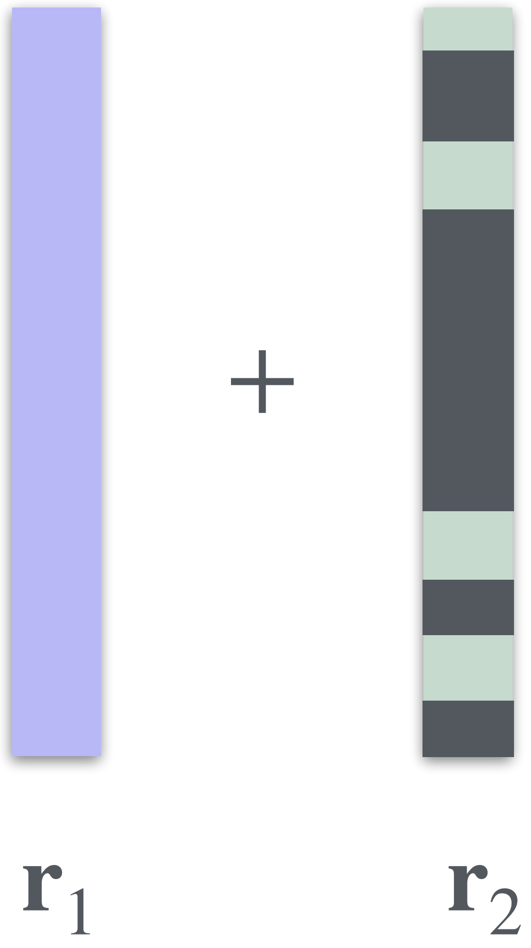
PKE from LW2E—Correctness?

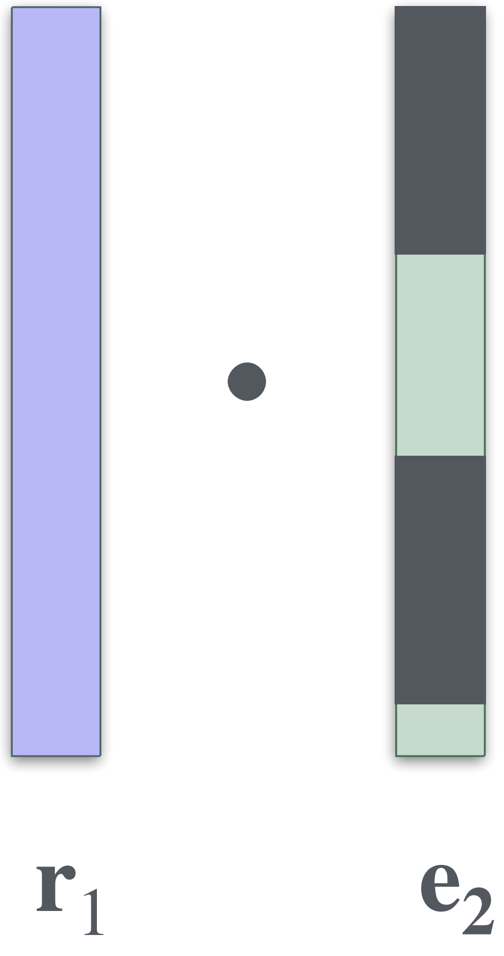
To decrypt, Bob computes:

$$\mathsf{ct}_2 - \mathsf{ct}_1^\top \cdot \mathbf{s} \in \mathbb{F}_q$$

if $x = 0$, uniform (large)

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} = \mathbf{r}_1 + \mathbf{r}_2 \leftarrow_\$ \mathscr{D}_{\text{error}}$.





= large

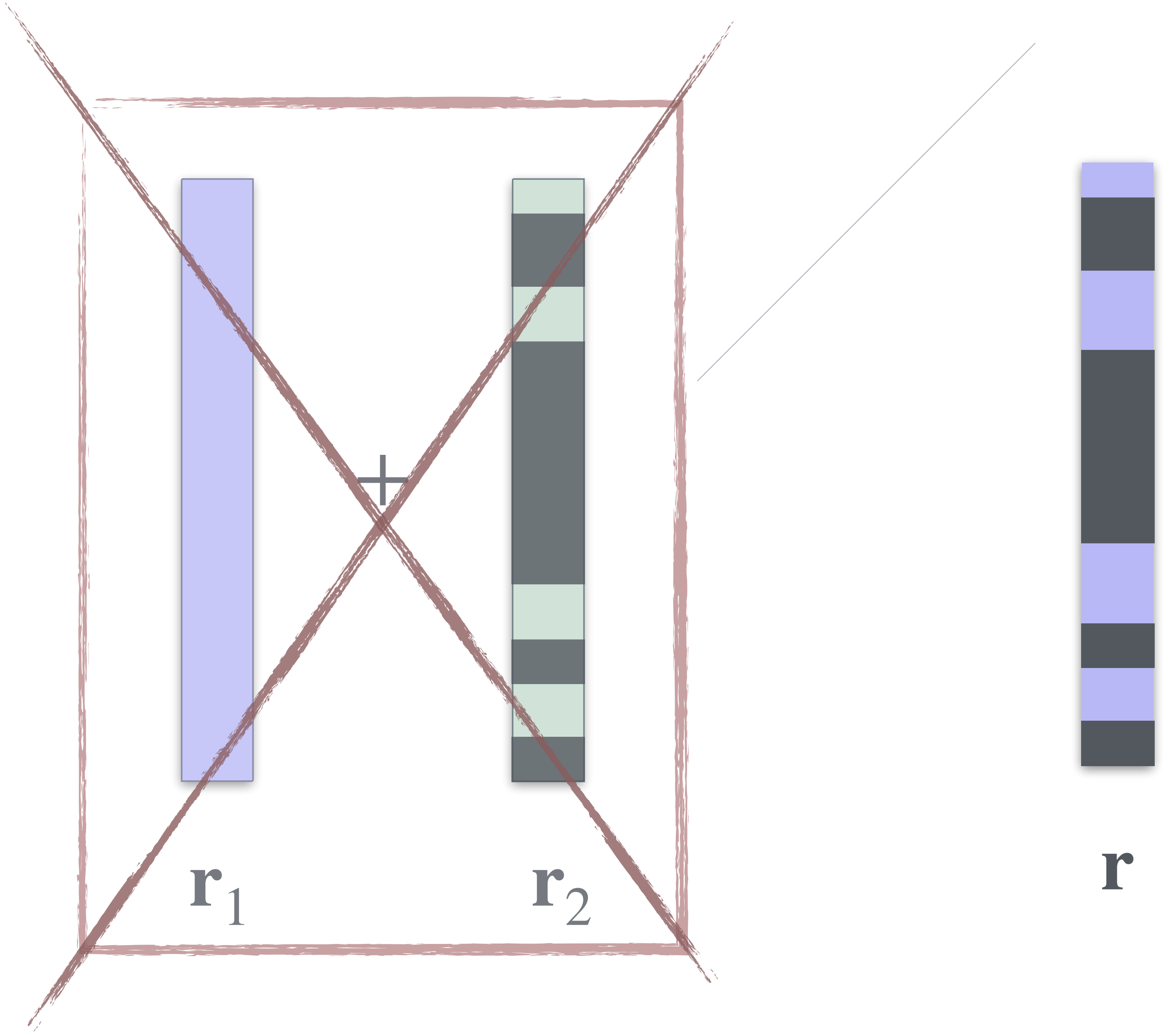
Not distinguishable from the case of $x = 0$

PKE from LW2E—A Fix

if $x = 0$, uniform (large)

Recall: $m = O(n)$.

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

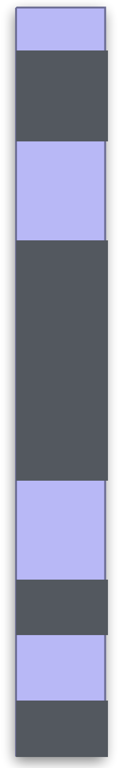


PKE from LW2E—A Fix

if $x = 0$, uniform (large)

Recall: $m = O(n)$.

if $x = 1$, $\mathbf{r}^{\top} \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_{\$} \mathscr{D}_{\text{small\&sparse}}$.



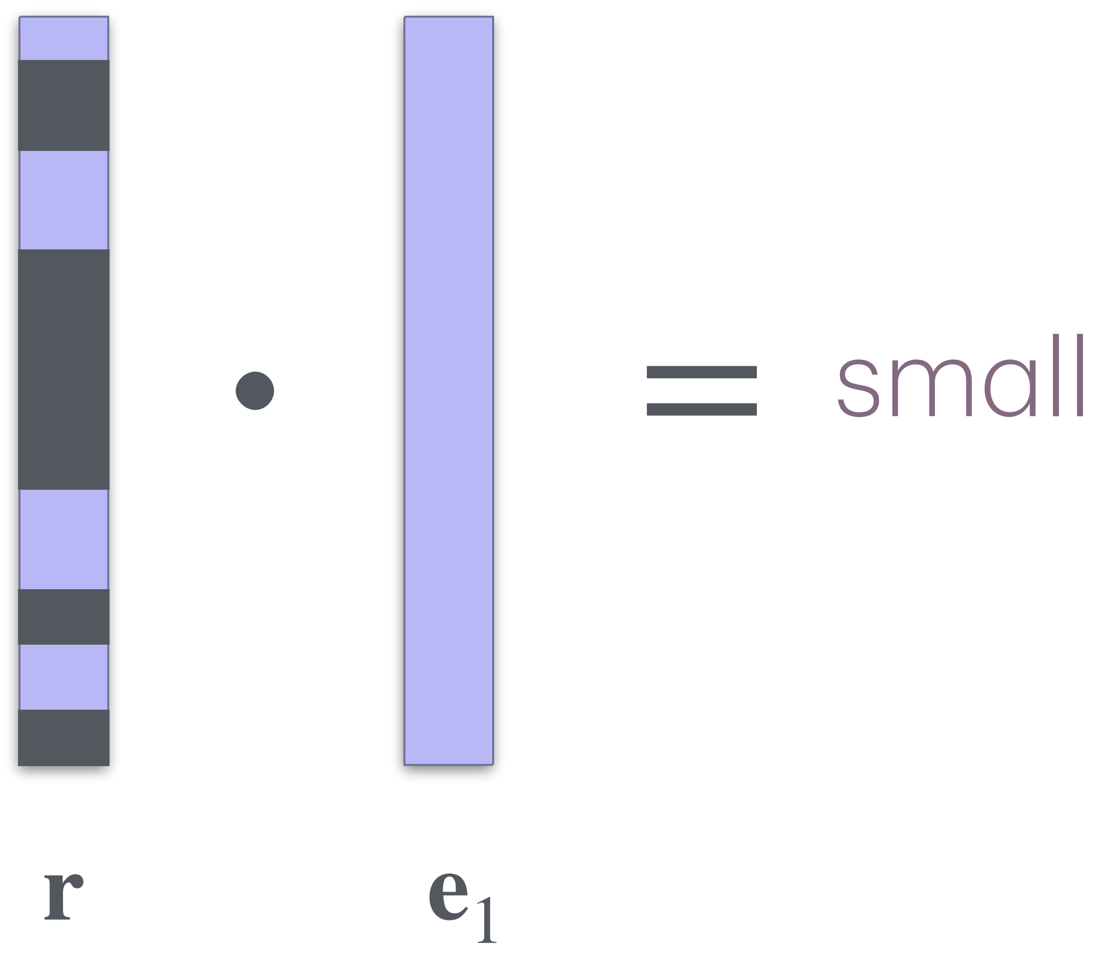
$\mathbf{r}$

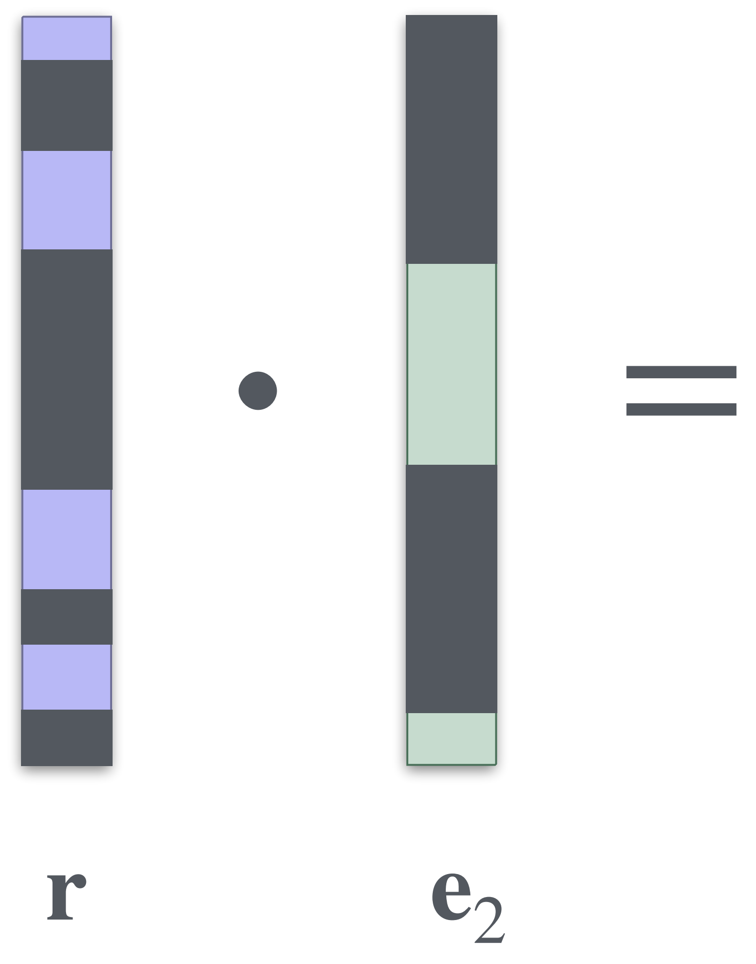
PKE from LW2E—Correctness

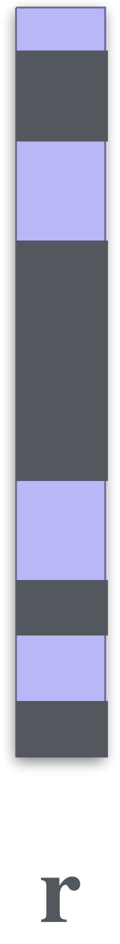
if $x = 0$, uniform (large)

Recall: $m = O(n)$.

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_\$ \mathcal{D}_{\text{small\&sparse}}$.





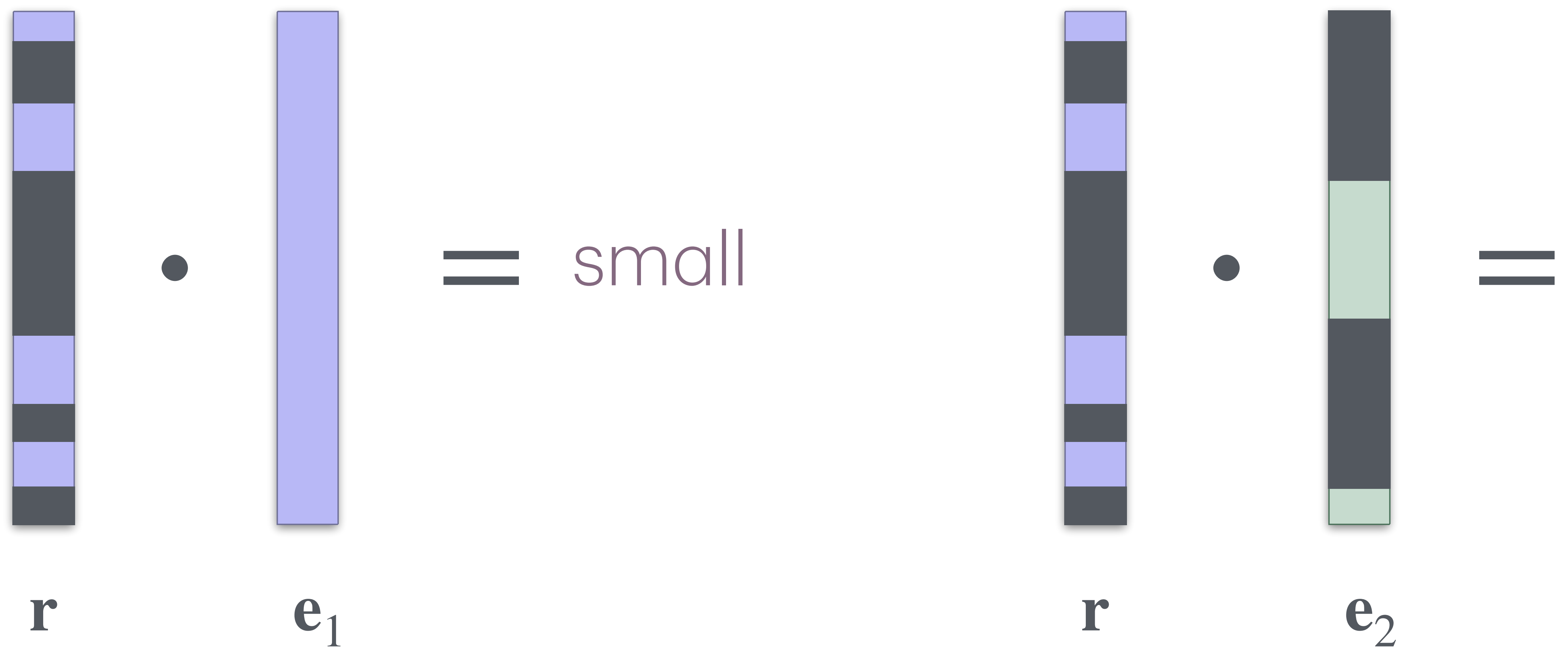


PKE from LW2E—Correctness Exploits Asymmetry

if $x = 0$, uniform (large)

Recall: $m = O(n)$.

if $x = 1$, $\mathbf{r}^{\top} \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_{\$} \mathscr{D}_{\text{small\&sparse}}$.



$n^{-\delta}$ sparse

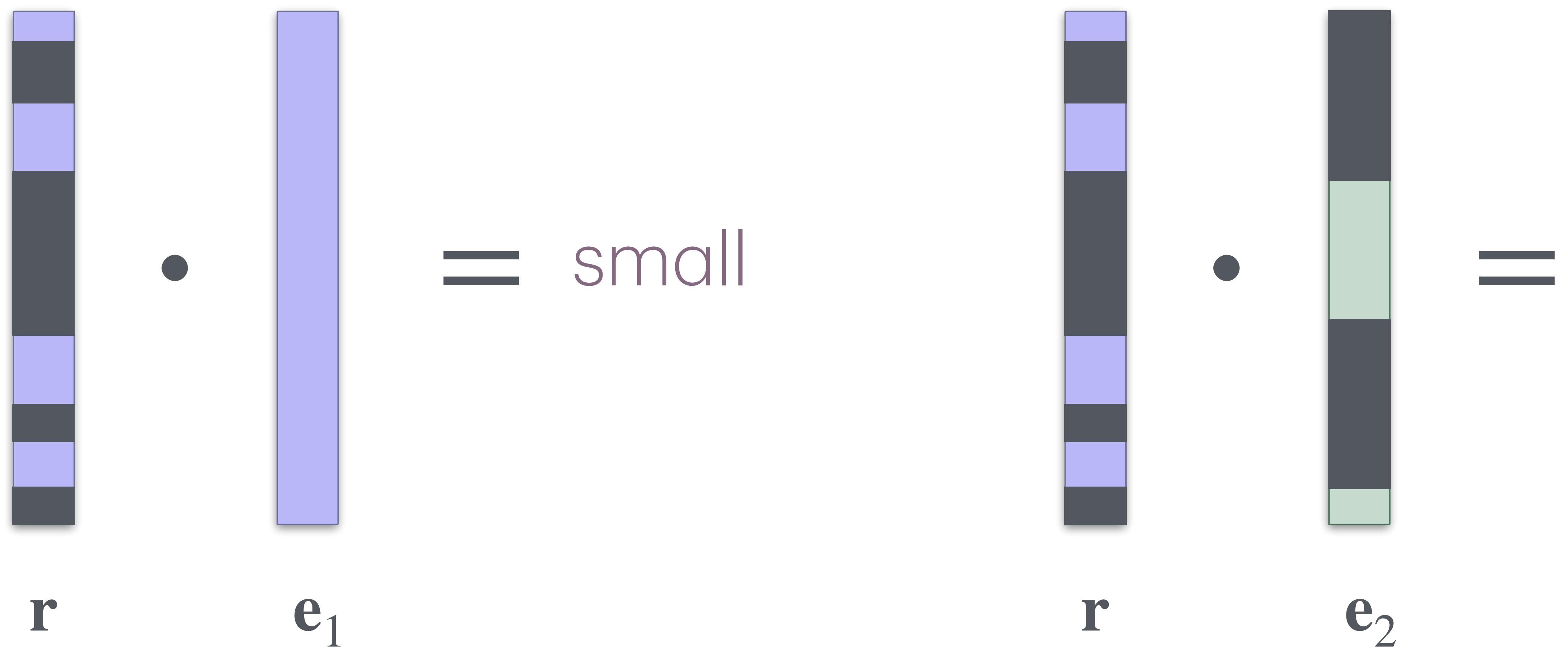
$n^{-\gamma}$ sparse

PKE from LW2E—Correctness Exploits Asymmetry

if $x = 0$, uniform (large)

Recall: $m = O(n)$.

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.



$n^{-\delta}$ sparse

$n^{-\gamma}$ sparse

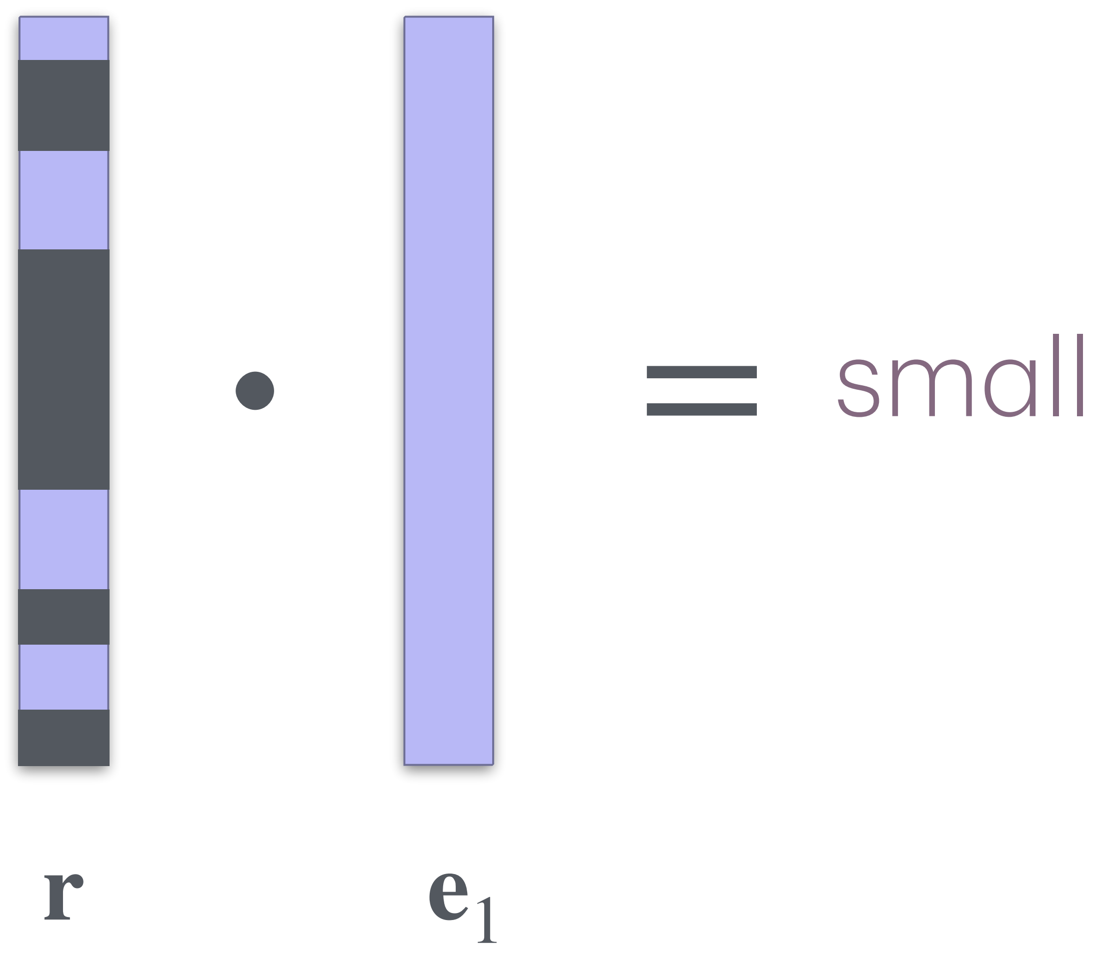
Can assume that $\delta, \gamma \leq 1$.

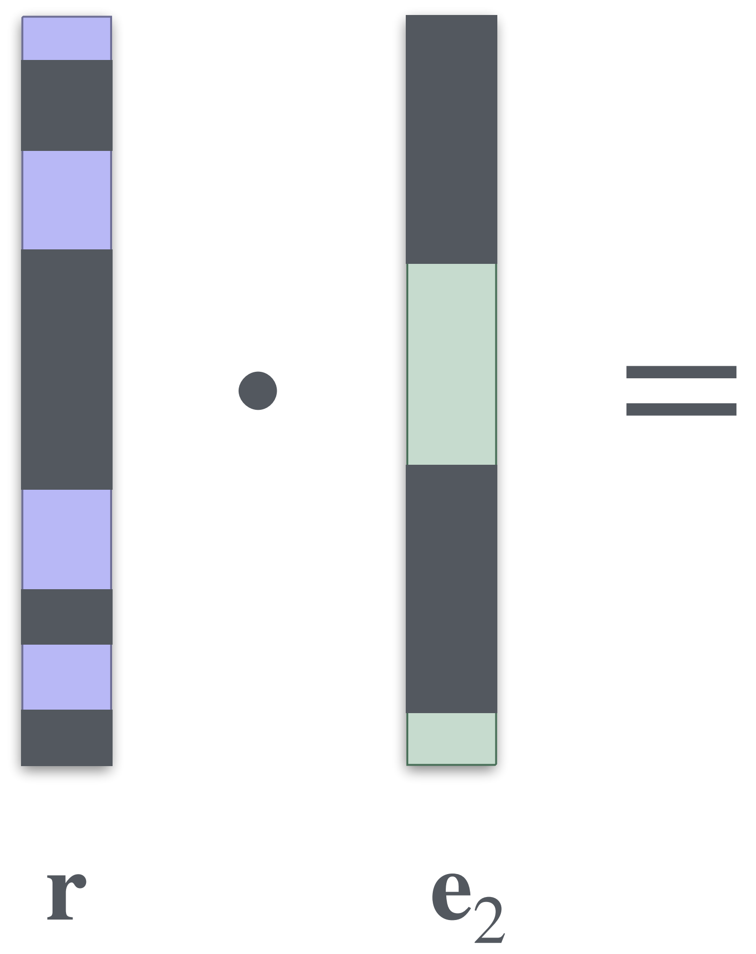
PKE from LW2E—Correctness Exploits Asymmetry

if $x = 0$, uniform (large)

Recall: $m = O(n)$.

if $x = 1$, $\mathbf{r}^\top \cdot (\mathbf{e}_1 + \mathbf{e}_2)$ where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.





Probability of being 0 is roughly $(1 - n^{-\delta})^{n^{1-\gamma}} \approx e^{-n^{1-\gamma-\delta}}$.

For correctness, want this to be non-negligible, i.e. $\gamma + \delta \geq 1$.

$n^{-\delta}$ sparse

$n^{-\gamma}$ sparse

Can assume that $\delta, \gamma \leq 1$.

PKE from LW2E

What about security?

PKE from LW2E—Security?

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

Adversary's view when $x = 1$

PKE from LW2E—Security?

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

Adversary's view when $x = 1$

PKE from LW2E—Security?

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

Adversary's view when $x = 1$

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

Can we apply the Leftover Hash Lemma?

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

PKE from LW2E—Security?

Recall: $m = O(n)$.

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$

Can we apply the Leftover Hash Lemma (LHL)?

PKE from LW2E—Security?

where $\mathbf{r} \leftarrow_{\$} \mathscr{D}_{\text{small\&sparse}}$.

Amount of entropy in $\mathbf{r}$: $\log \left(\binom{m}{mn^{-\delta}} B^{mn^{-\delta}} \right)$ bits.

LHL needs the entropy to be greater than $n \log q$.

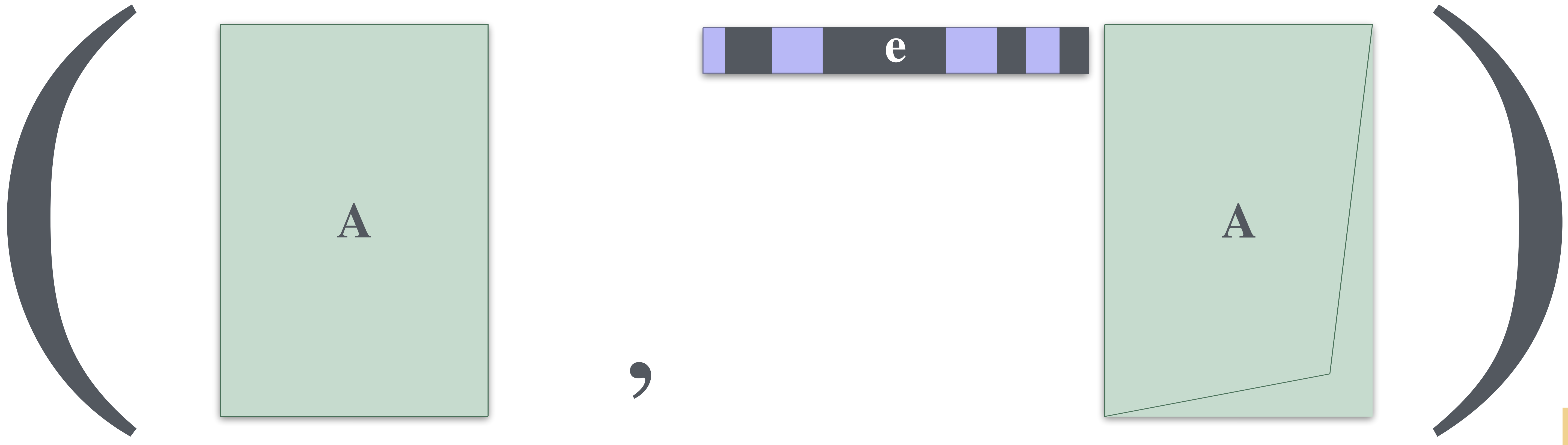
However, this is not possible when $m = O(n)$.

No known setting of m, δ, γ beyond the Alekhnovich barrier such that correctness holds and security holds via LW2E alone.

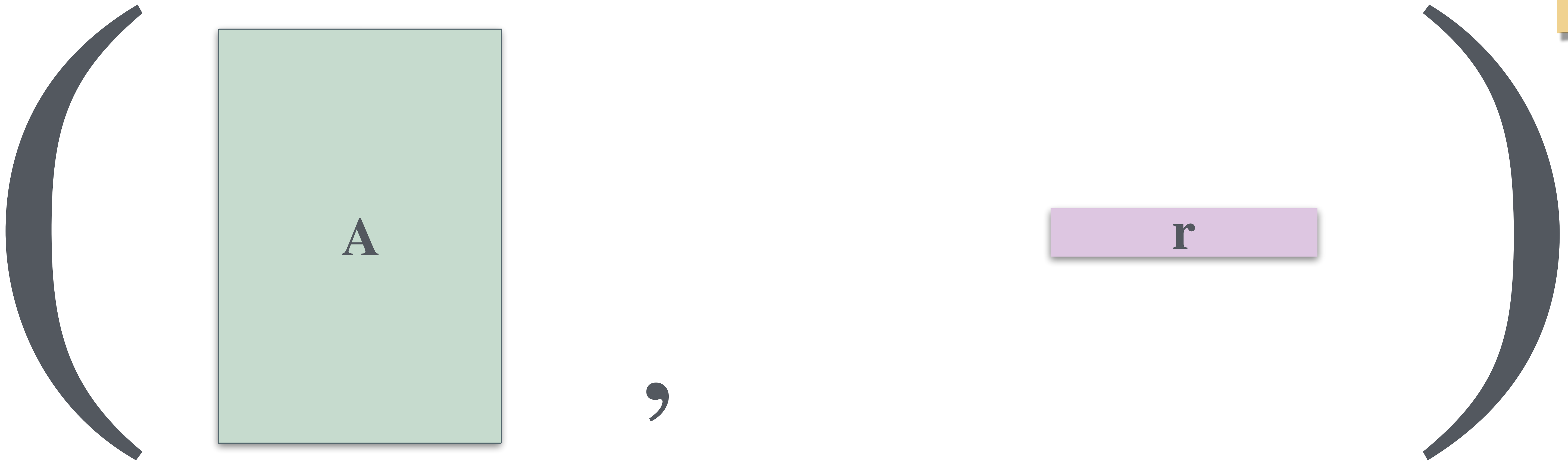
PKE from LW2E?

How do we get security?

Inhomogeneous Short and Sparse Integer Solution (ISSIS) Problem



is computationally indistinguishable from



A computational version of LHL.

PKE from LW2E & ISSIS—Security

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

Adversary's view when $x = 1$

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

PKE from LW2E & ISSIS—Security

$$(\mathbf{A}, \mathbf{b} \triangleq \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1 + \mathbf{e}_2, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{b})$$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

Adversary's view when $x = 1$

by LW2E

Hybrid 1: $(\mathbf{A}, \mathbf{u}, \mathbf{r}^\top \cdot \mathbf{A}, \mathbf{r}^\top \cdot \mathbf{u})$

where $\mathbf{r} \leftarrow_\$ \mathscr{D}_{\text{small\&sparse}}$.

by ISSIS

Hybrid 2: $(\mathbf{A}, \mathbf{u}, \tilde{\mathbf{u}}, u')$, i.e. uniform random field elements.

PKE from LW2E & ISSIS—Security

by LW2E

Intuitively harder than both LWE and LPN.

by ISSIS

PKE from LW2E & ISSIS—Security

by LW2E

Intuitively harder than both LWE and LPN.

by ISSIS

How does its hardness relate to LWE and LPN?

ISSIS & LWE and Lattice Assumptions

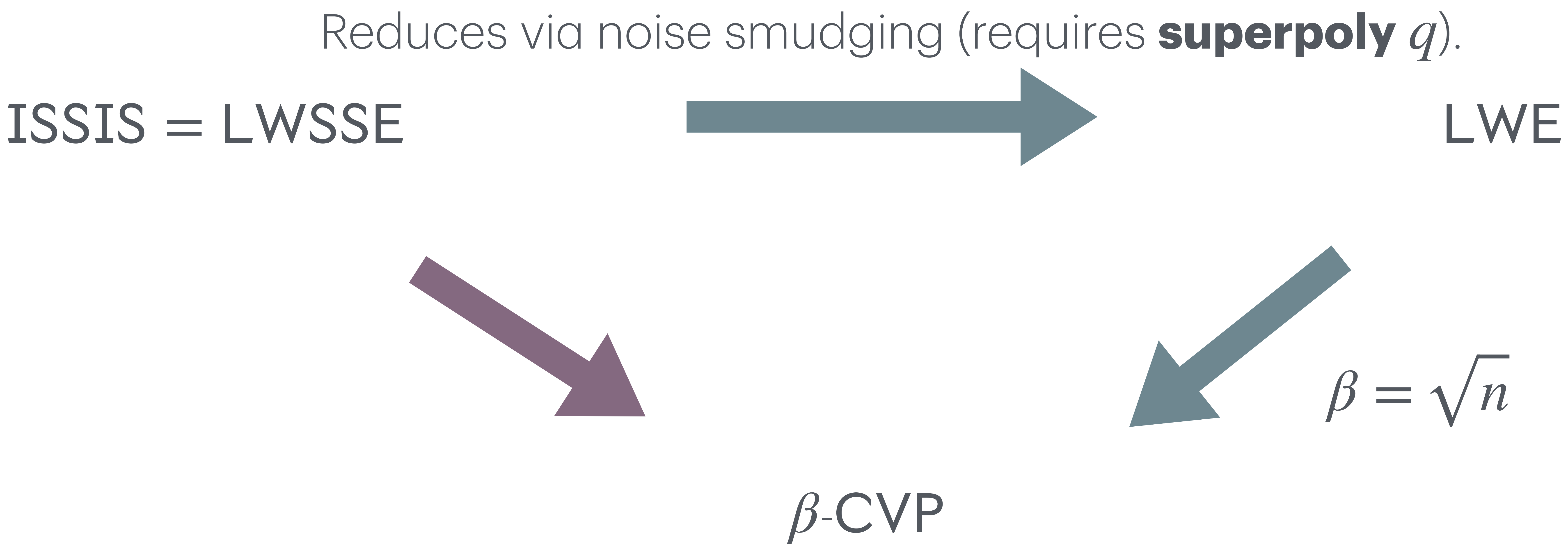
Can we separate ISSIS from LWE and lattice assumptions?

No.

In general, it is not known how to obtain formal separations between assumptions without proving $P \neq NP$.

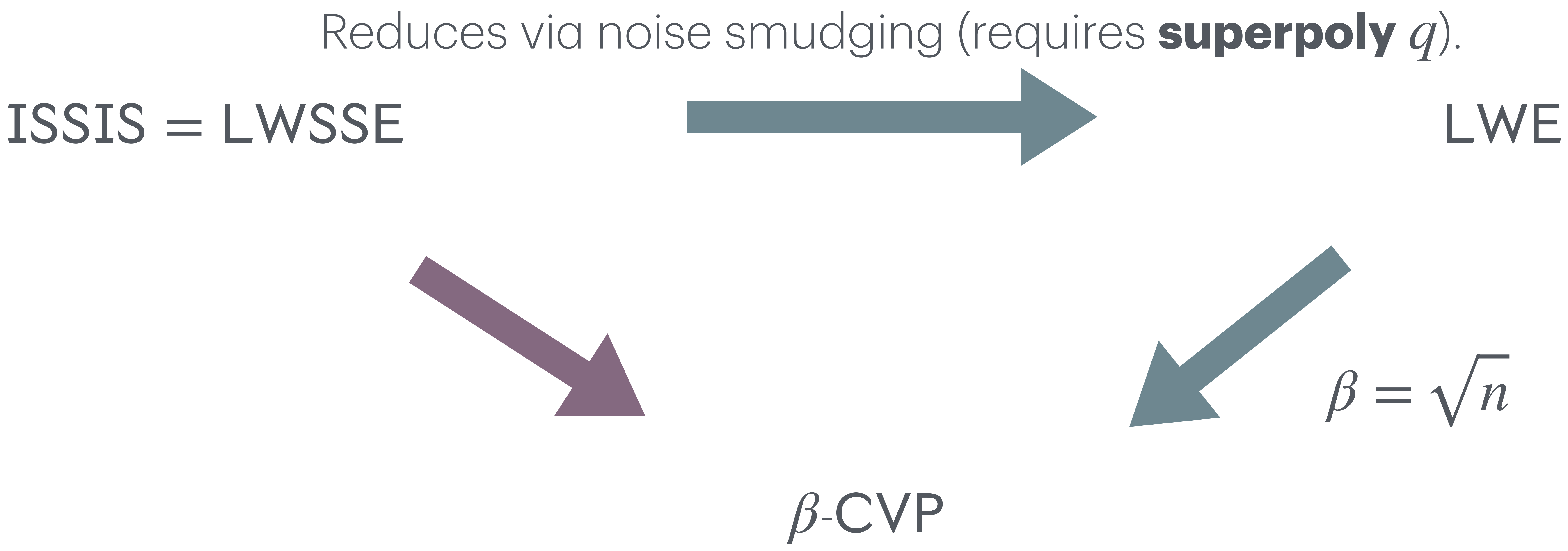
What can we show?

ISSIS & LWE and Lattice Assumptions



ISSIS & LWE and Lattice Assumptions

Parameter Setting: Secret dim. n, #samples $m = 20n$, modulus $q = n^{12}$, smallness bound $\xi = n^{0.6}$, sparsity $n^{-0.1}$.



ISSIS & LWE and Lattice Assumptions

Parameter Setting: Secret dim. n, #samples $m = 20n$, modulus $q = n^{12}$, smallness bound $\xi = n^{0.6}$, sparsity $n^{-0.1}$.

ISSIS = LWSSE

Standard reduction idea fails in this parameter setting.

β-CVP

ISSIS & LWE and Lattice Assumptions

Parameter Setting: Secret dim. n, #samples $m = 20n$, modulus $q = n^{12}$, smallness bound $\xi = n^{0.6}$, sparsity $n^{-0.1}$.

ISSIS = LWSSE

Standard reduction idea fails in this parameter setting.

β-CVP

Intuitively: In the total SIS regime, i.e. there are many short vectors which are not sparse. The β-CVP oracle is blind to sparseness.

Recap:

Reexamining Our Defenses Against the Worst Holiday Maybe Ever

Part I. We challenge the belief that classically secure underdetermined multivariate polynomial systems should be believed to be quantum secure.

We give the first evidence of a classically hard, quantumly easy multivariate system & show new applications of the YZ'22 framework.

Recap:

Reexamining Our Defenses Against the Worst Holiday Maybe Ever

Part I. We challenge the belief that classically secure underdetermined multivariate polynomial systems should be believed to be quantum secure.

We give the first evidence of a classically hard, quantumly easy multivariate system & show new applications of the YZ'22 framework.

Part II. We give a plan-B for NLAs in the case of a catastrophic break of LWE and Alekhnovich LPN.

We give new NLAs that imply PKE and remain plausibly secure in a world where two of the principal lattice-based and random-code based assumptions are broken.