Secrets, Quantum and AI

A JOURNEY THROUGH CRYPTOGRAPHY

Mahesh Sreekumar Rajasree

CISPA Helmholtz Center for Information Security

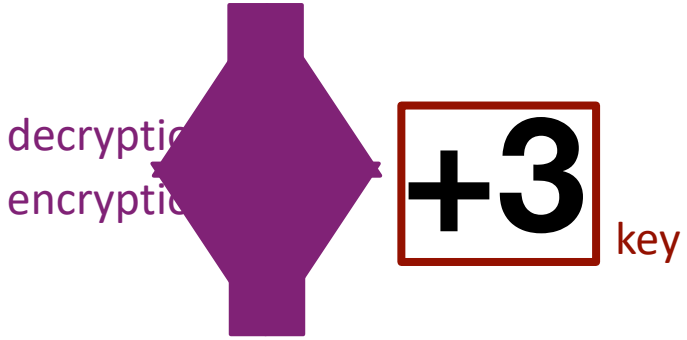
Indian Institute of Space Science and Technology (IIST)

18 August 2026

CAESAR CIPHER 60 BC

ciphertext

FDQ BRX UHDG WKLV?



CAN YOU READ THIS?

message

CAESAR CIPHER

HOW DO WE ATTACK IT?

TRY ALL 26 SHIFTS

ONE IS CORRECT

THIS IS A BRUTE-FORCE ATTACK.

The Imitation Game

Google Pictures

Enigma Machine

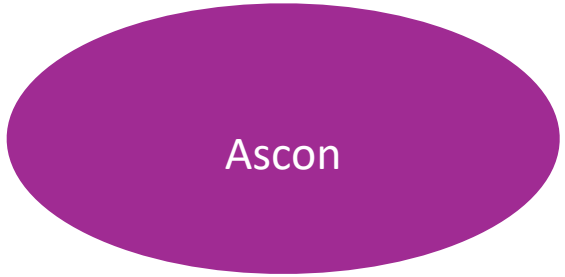
Wikipedia

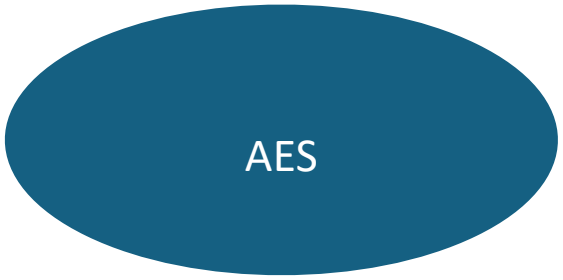
158 quintillion (1.58×10^{20})

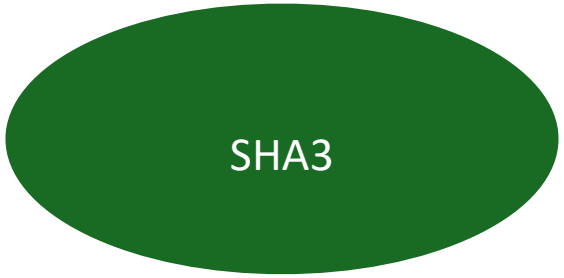
MODERN CIPHERS

Uses

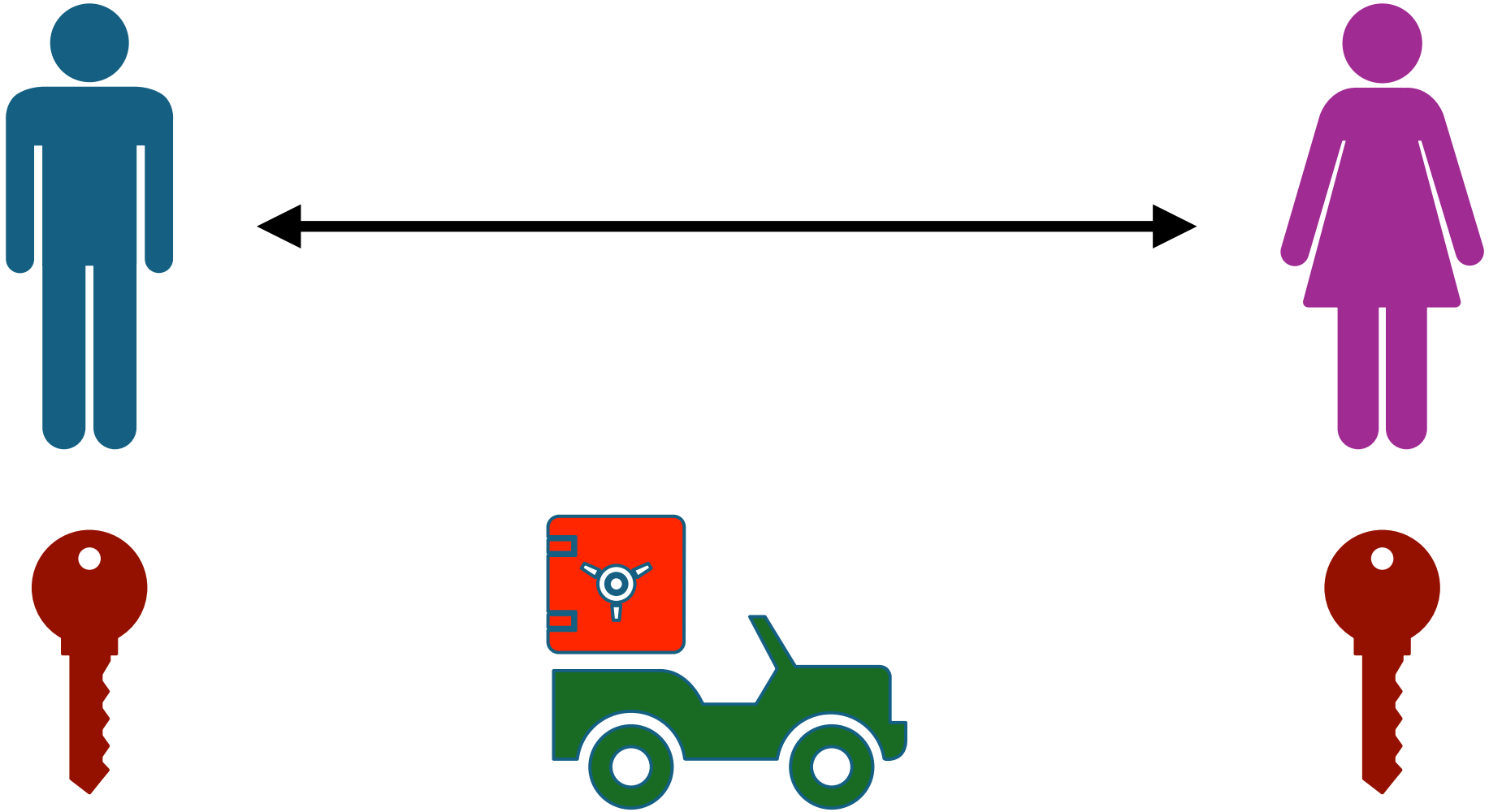
- Substitutions
- Permutations
- Non-linear operations



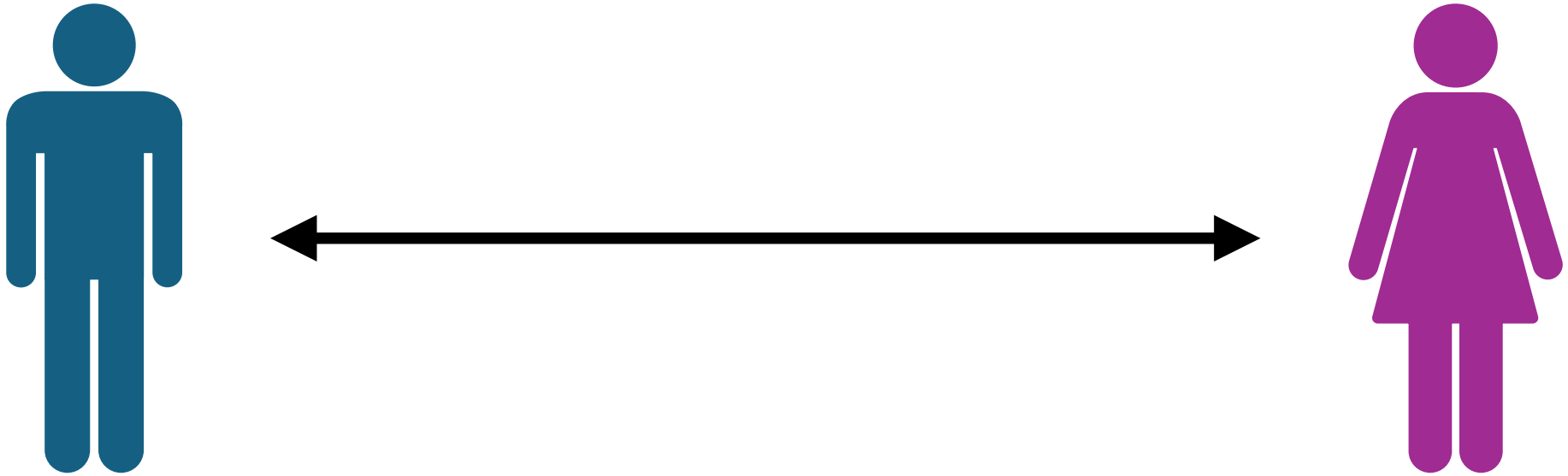




Symmetric Key Cryptosystems

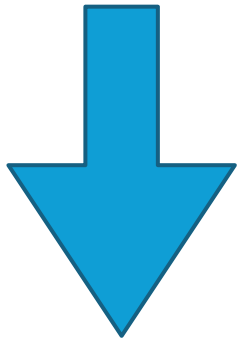


Public Key Cryptosystems [Diffie-Hellman’76, RSA’77]

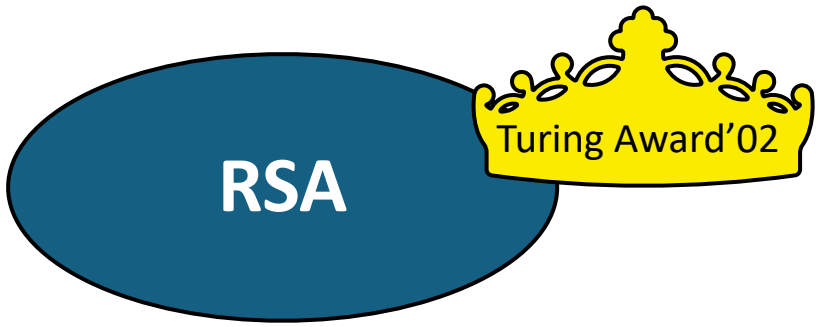


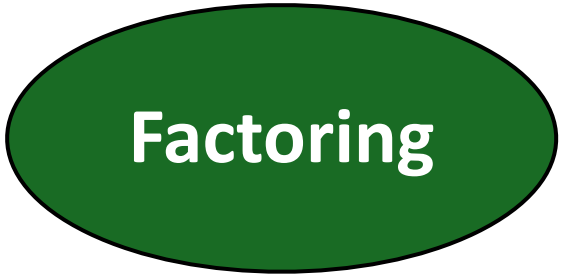
Security Proofs

Hacker is able to break security



Algorithm to solve a hard problem





Advanced Cryptosystems

Identity based encryption
Attribute based encryption
Functional encryption
Fully homomorphic encryption
Non-committing encryption
Incompressible encryption
Anamorphic encryption
Laconic encryption
Batch encryption
And more

Quantum Computer

Shor’94

Factoring

RSA

Post Quantum Cryptography

Lattice based cryptography 

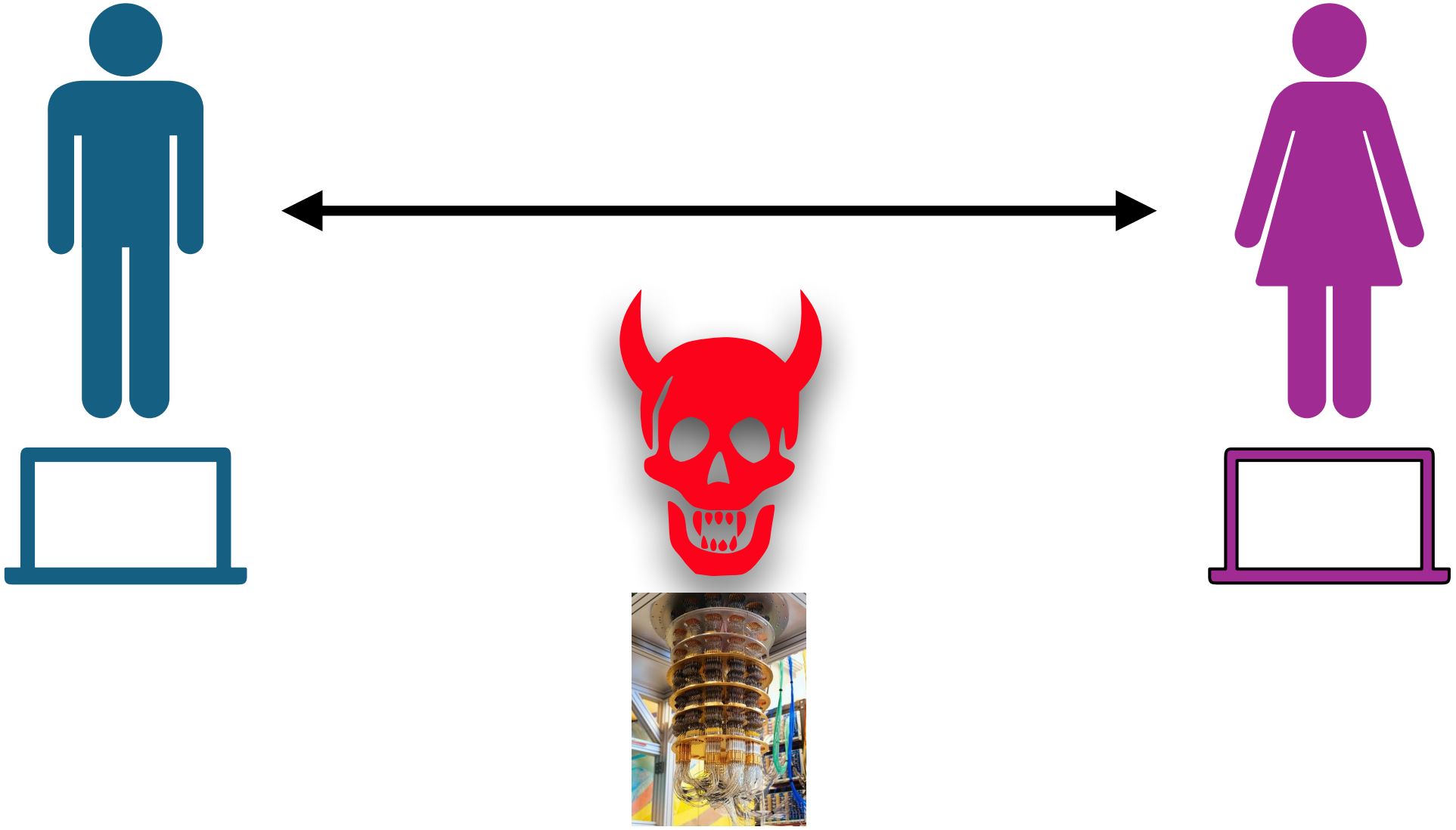
Isogeny based cryptography

Code based cryptography

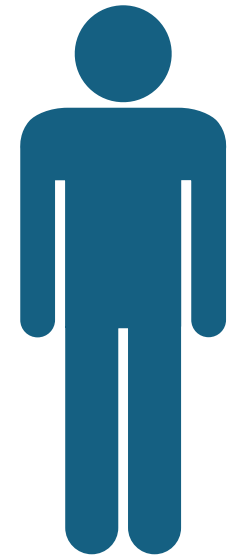
Multivariate polynomial based cryptography

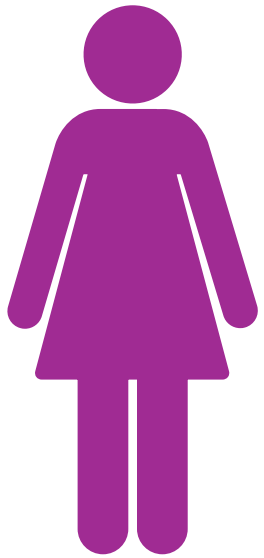
Hash based cryptography

Post-Quantum Cryptography

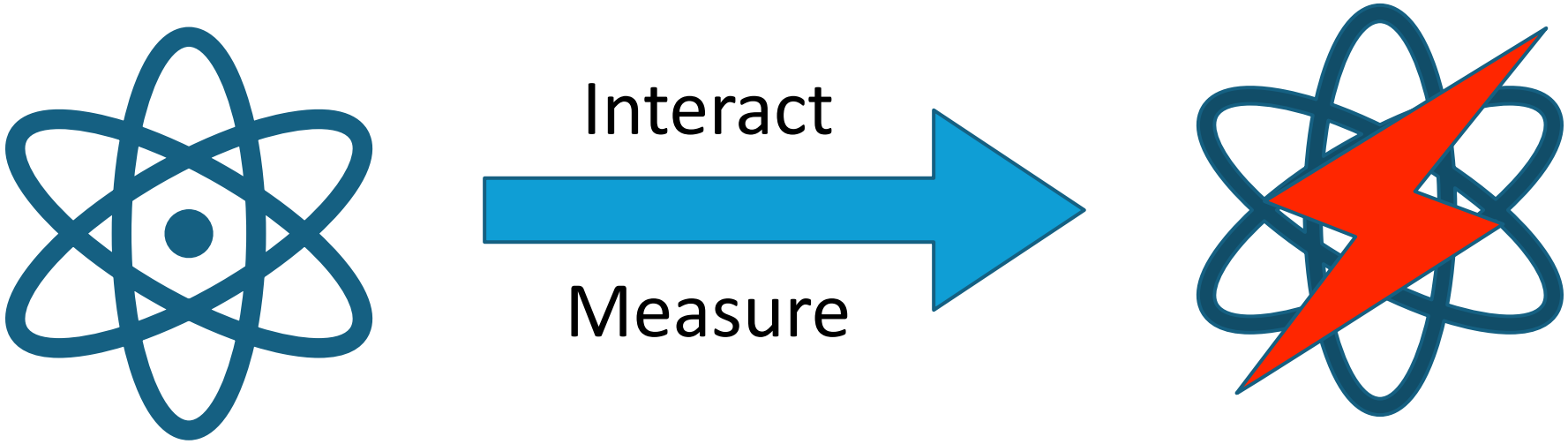


Quantum Cryptography

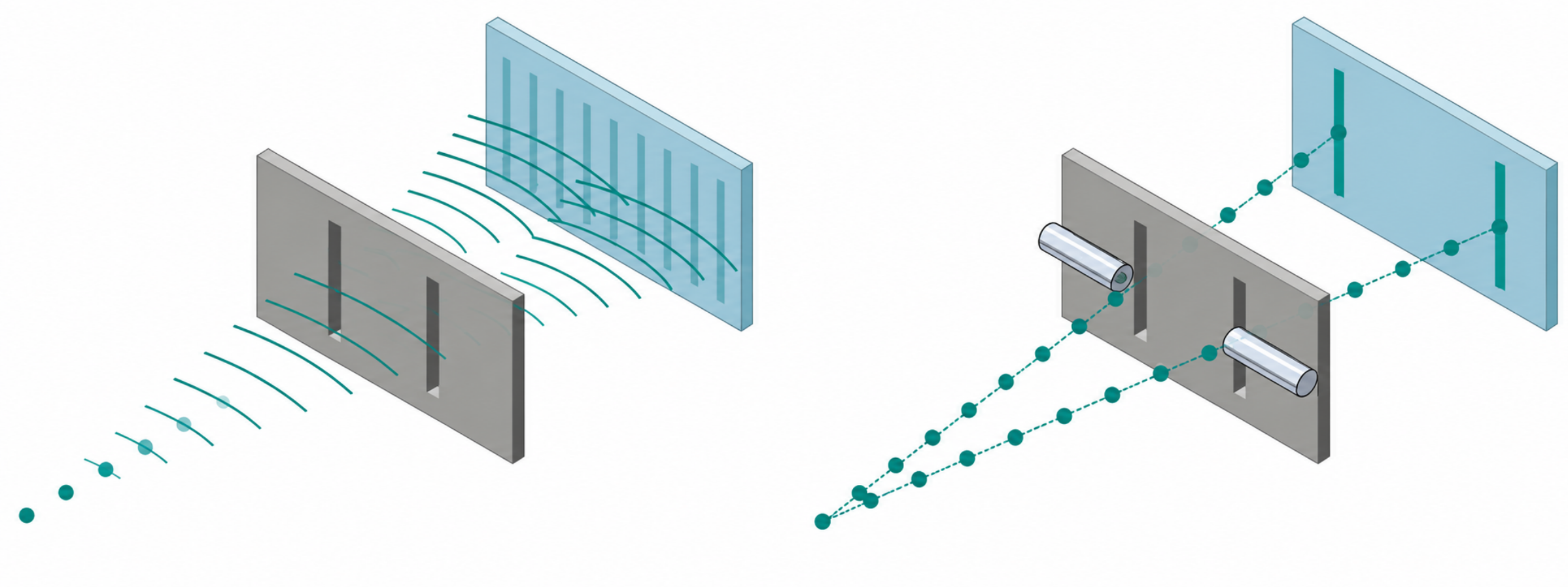




Quantum Mechanics

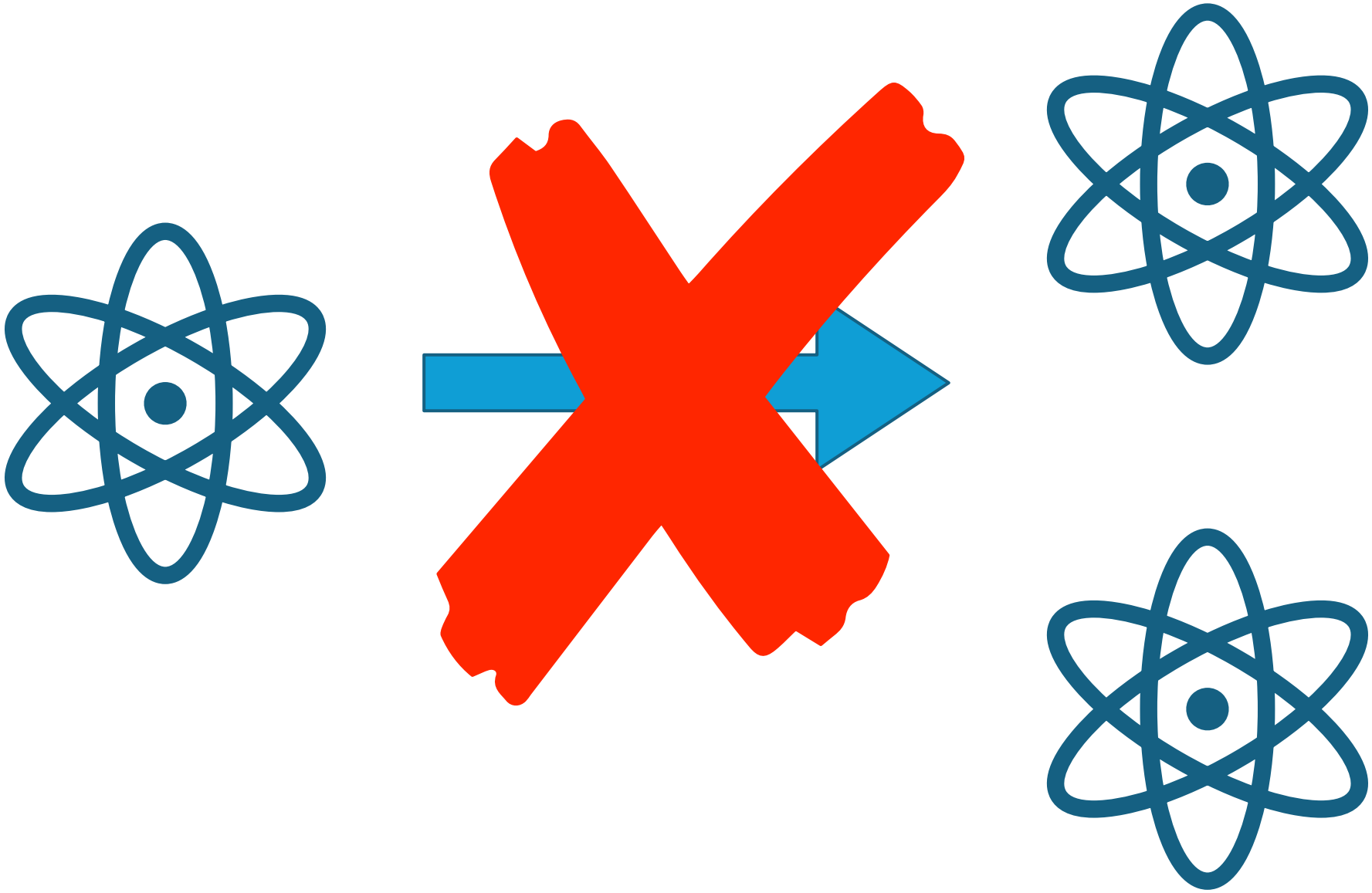


Double Slit Experiment

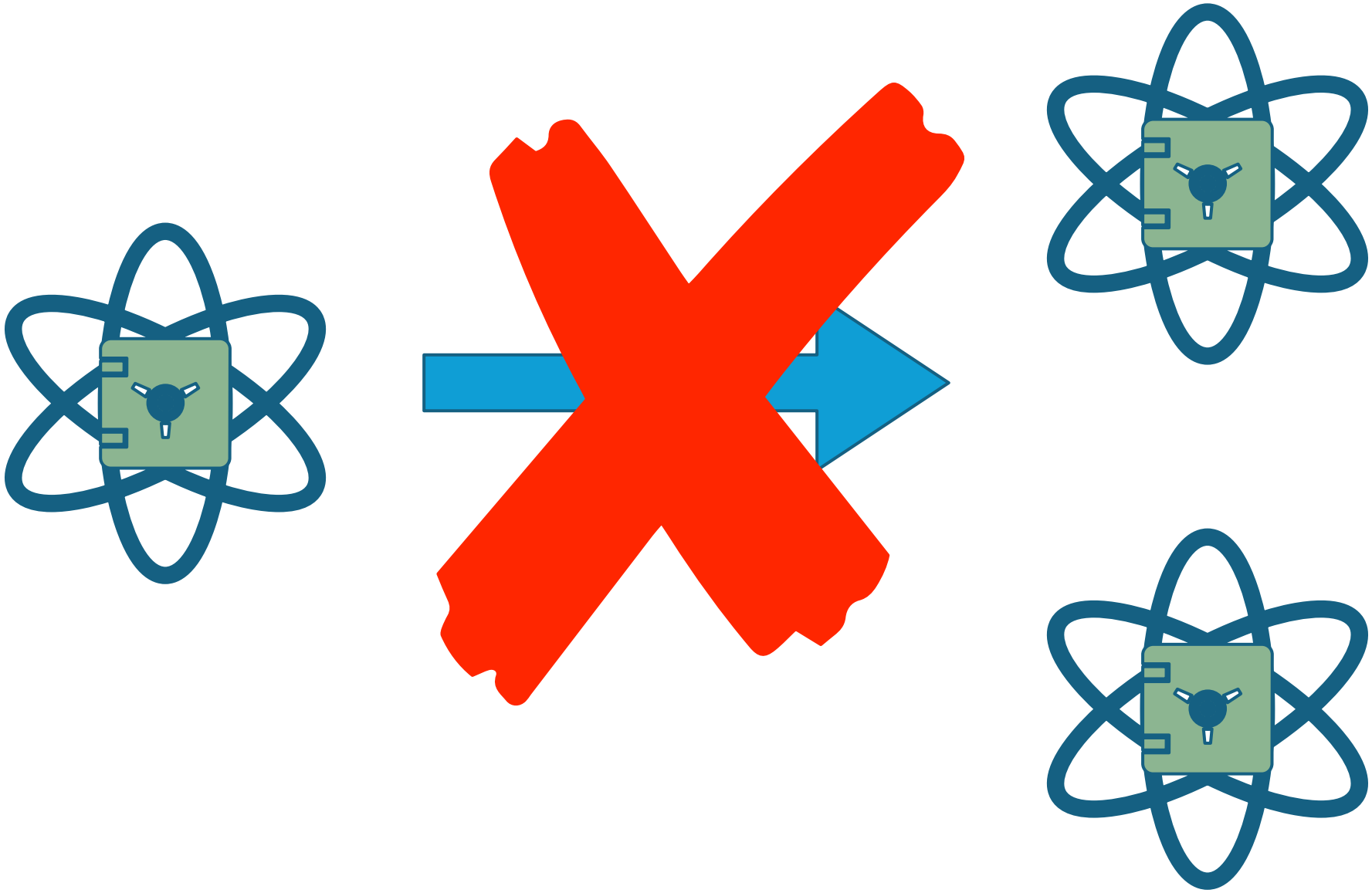


medium.com

Non-Cloning Theorem



Unclonable Encryption



Unclonable Encryption

Unconditional Unclonable Encryption

Prabhanjan Ananth*
UCSB

Amit Sahai†
UCLA

Abstract

We give an unconditional construction of information-theoretically secure one-time private-key unclonable encryption scheme for one-bit messages, with efficient encryption and decryption and exponentially small unclonable-indistinguishability advantage.

Statement on AI usage. The human authors take full responsibility for the claims and proofs contained in this paper, and have carefully refined and verified them. The construction and main ideas of the proof were generated entirely by Codex using GPT 5.6 Sol Ultra, using harness ideas generated by the authors based on the UCLA Moonshot Harness [ZHC+26] and [Ope26].

ChatGPT Astra

1. **High-dimensional sphere packing.** New upper bounds on sphere-packing density down to the Cohn–Elkies threshold.
2. **Binary and spherical codes.** Exponentially improved bounds on the maximum size of binary codes at any prescribed minimum distance, with analogous results for high-dimensional spherical codes.
3. **Non-sofic groups.** A construction establishing the existence of non-sofic groups, addressing a central open question in group theory.
4. **Connes's rigidity conjecture.** Disproof of a longstanding conjecture that certain groups are uniquely determined by their von Neumann algebras.
5. **Arithmetic circuit complexity.** New lower bounds for computing the permanent using arithmetic circuits and formulas, including an arithmetic-formula lower bound of order $n^4/\log n$.
6. **Quantum parallel repetition.** An exponential parallel repetition theorem for general two-player quantum games, extending a foundational principle from classical complexity theory.
7. **Closest vector problem.** Polynomial-factor hardness of approximation for the closest vector problem, a foundational lattice question related to post-quantum cryptography.
8. **Ehrhart's volume conjecture.** Determining, in every dimension, the maximum possible volume of a convex body whose centroid is its only interior lattice point.
9. **Multicolor Ramsey numbers.** A superexponential lower bound for multicolor triangle Ramsey numbers, resolving Erdős problem 183.
10. **Extremal number conjectures.** Results on the compactness and degeneracy conjectures in extremal graph theory, resolving Erdős problems 146 and 180.

AI + Cryptography

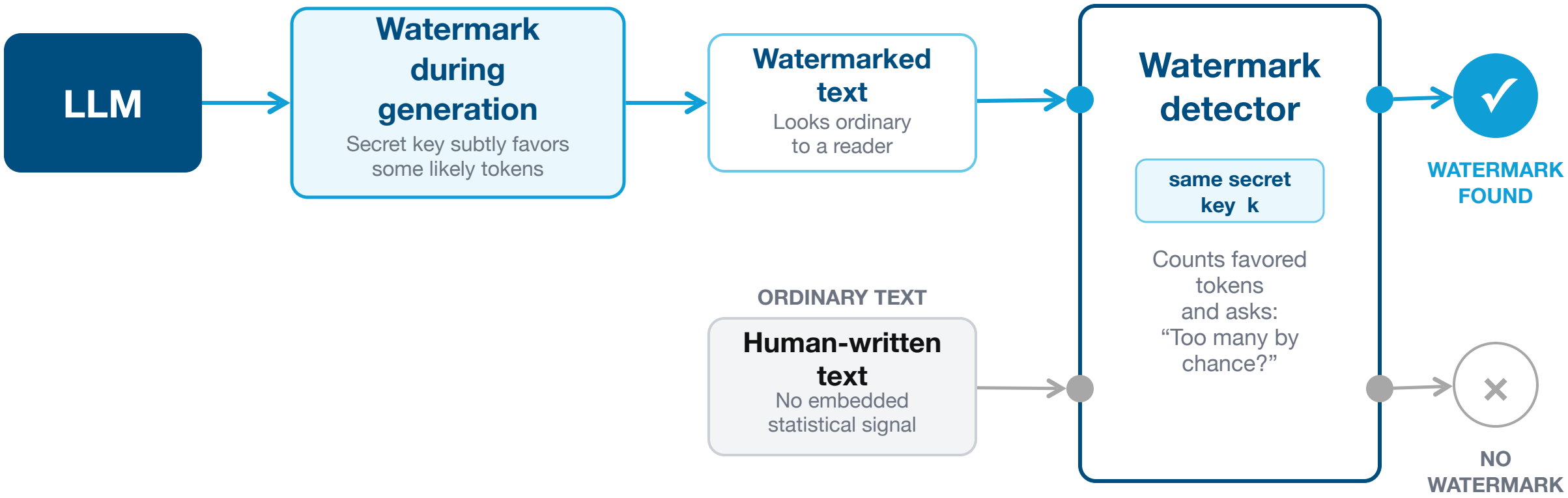
Watermarking LLMs

Verifiable and private machine learning

Embedding backdoors in a model

And more …

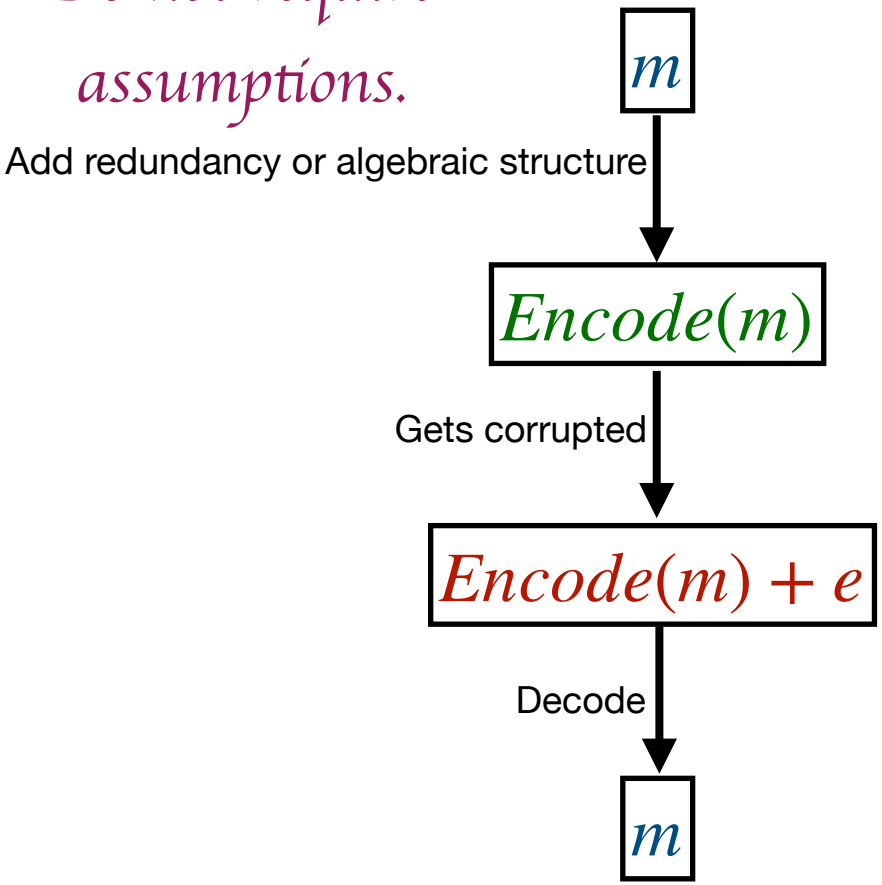
Watermarking LLMs



Pseudorandomness Meets Error-Correction

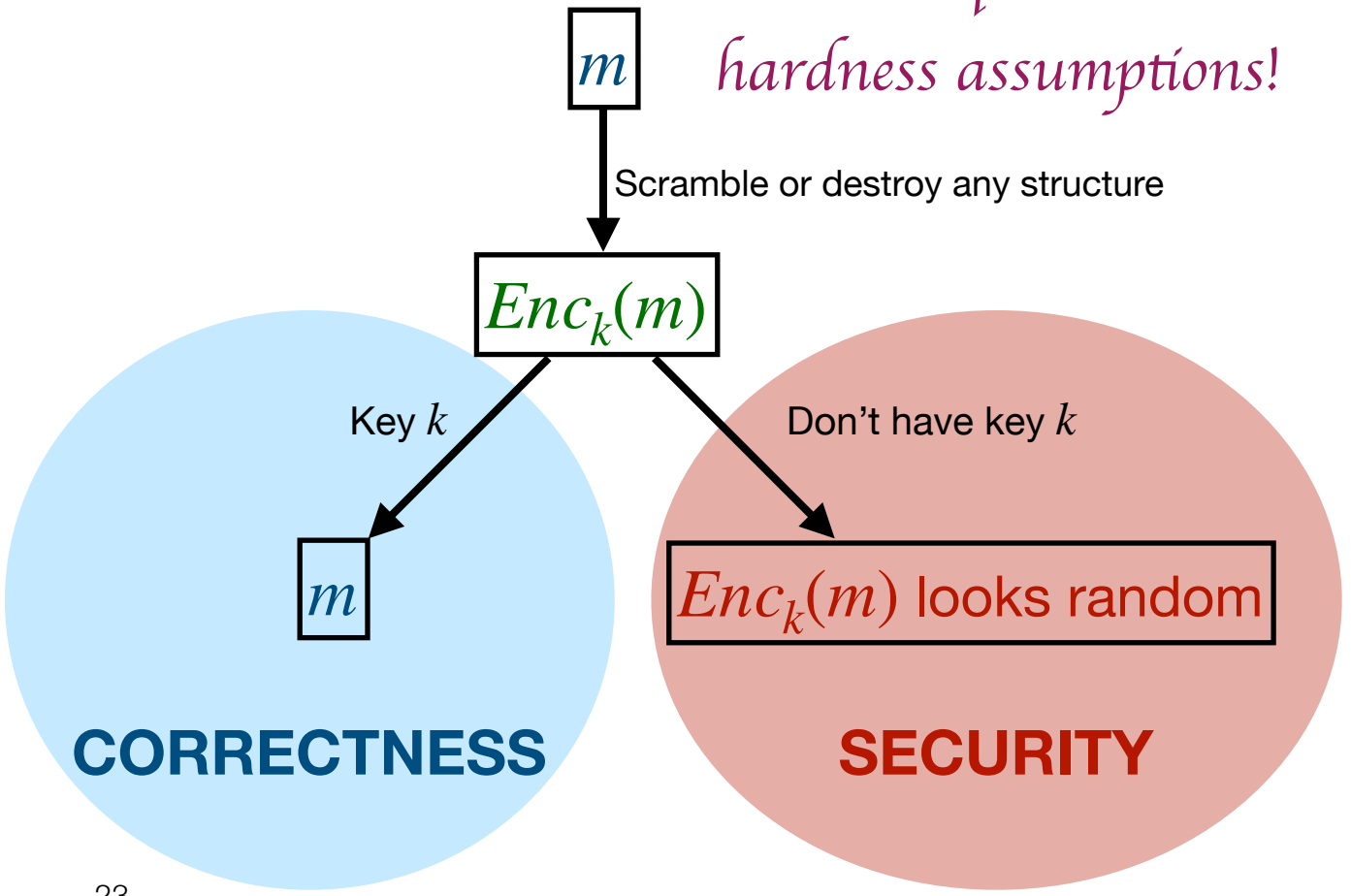
Coding Theory

Do not require assumptions.

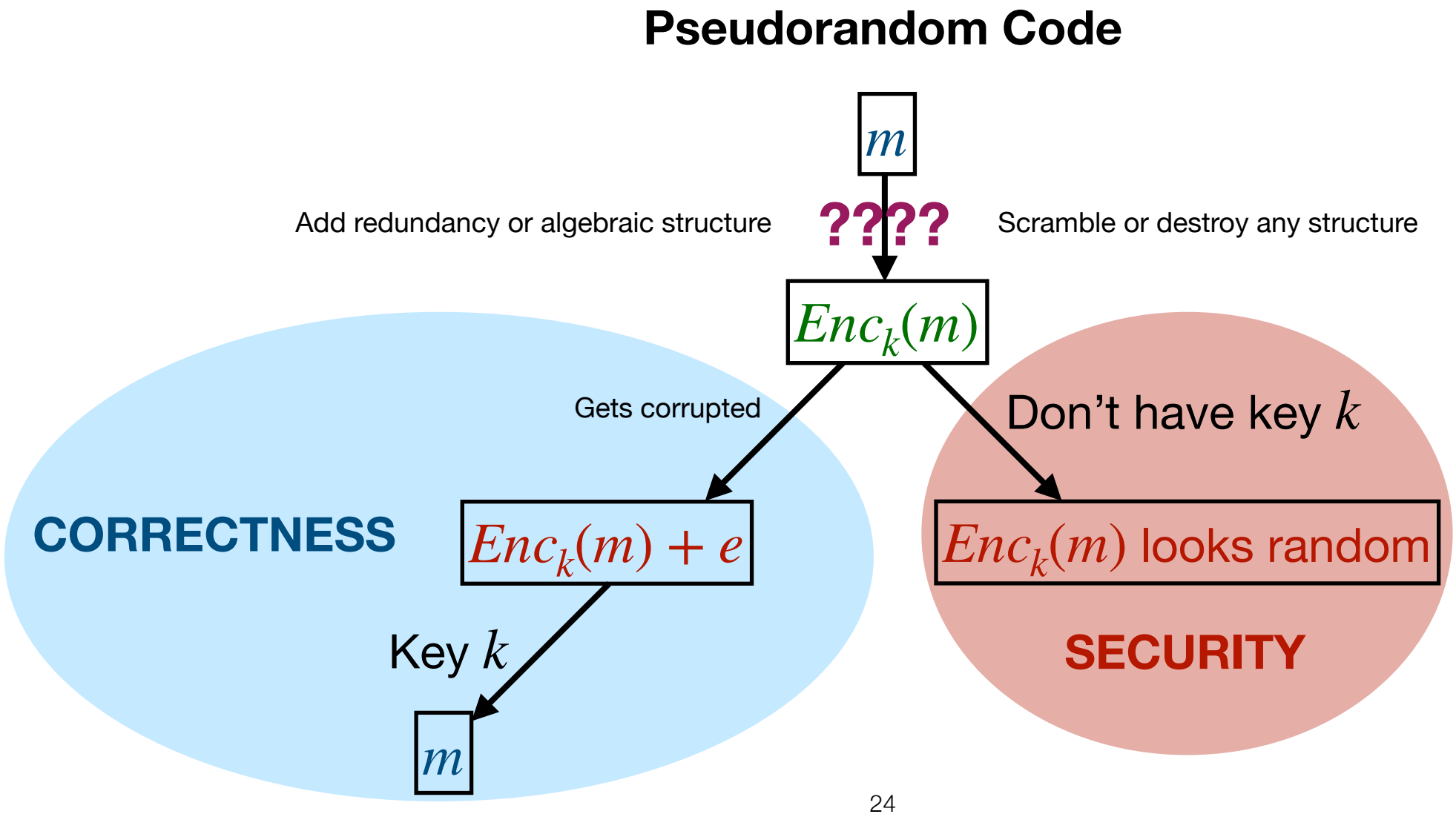


Cryptography

Requires hardness assumptions!



Pseudorandomness Meets Error-Correction



Works on PRCs

Subexponential LPN

Planted Hyperloop and Planted XOR

- Introduced by Christ and Gunn at **CRYPTO'24** for watermarking LLM/AI models.
- More works on constructions appeared in **NeurIPS'25, RANDOM'25**.
- In **FOCS'25** and **STOC'26**, extended to stronger settings.

Permuted Codes

- In **TCC'25**, two independent works showed strong barriers in building these !!!

Conclusion

- Symmetric key cryptosystems
- Public key cryptosystems
- Advanced cryptosystem (other areas of cryptography)
- Post-quantum cryptography
- Quantum cryptography
- AI + cryptography

Thank You!!!

https://mahe94.github.io/