Limits of Black-Box Constructions of Pseudorandom Codes

Mahesh Sreekumar Rajasree
Postdoctoral Researcher
CISPA Helmholtz Center for Information Security

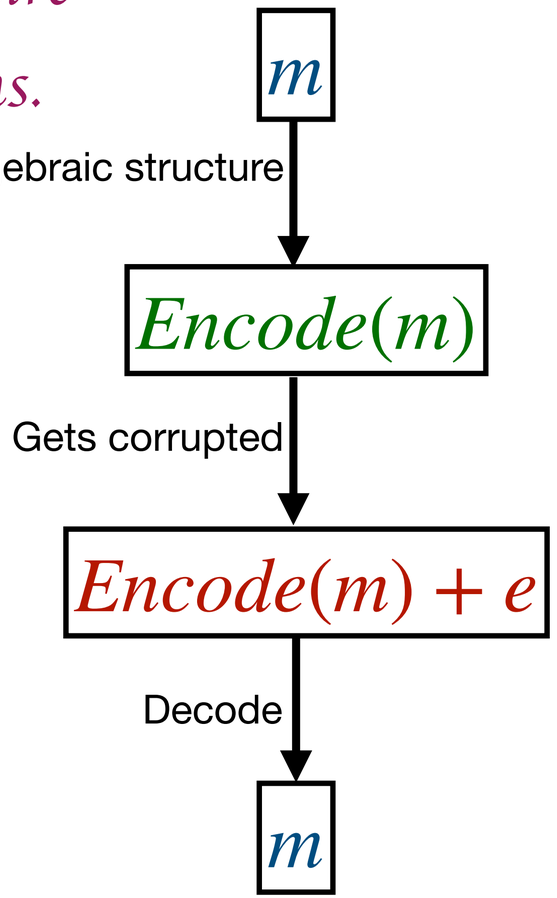
IMDEA Software Institute, Madrid
25 May 2026

Pseudorandom Codes

Pseudorandomness Meets Error-Correction

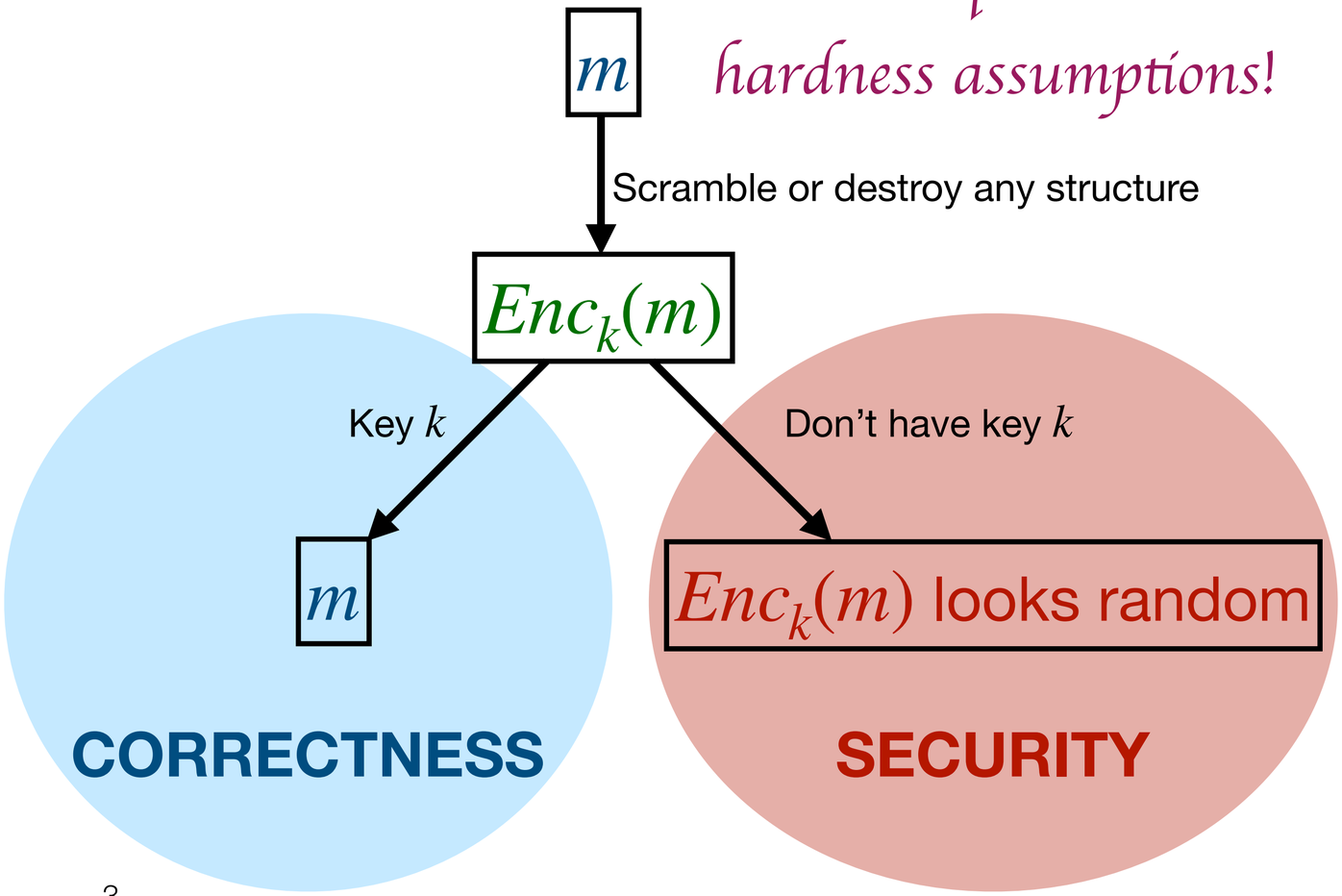
Coding Theory

Do not require assumptions.

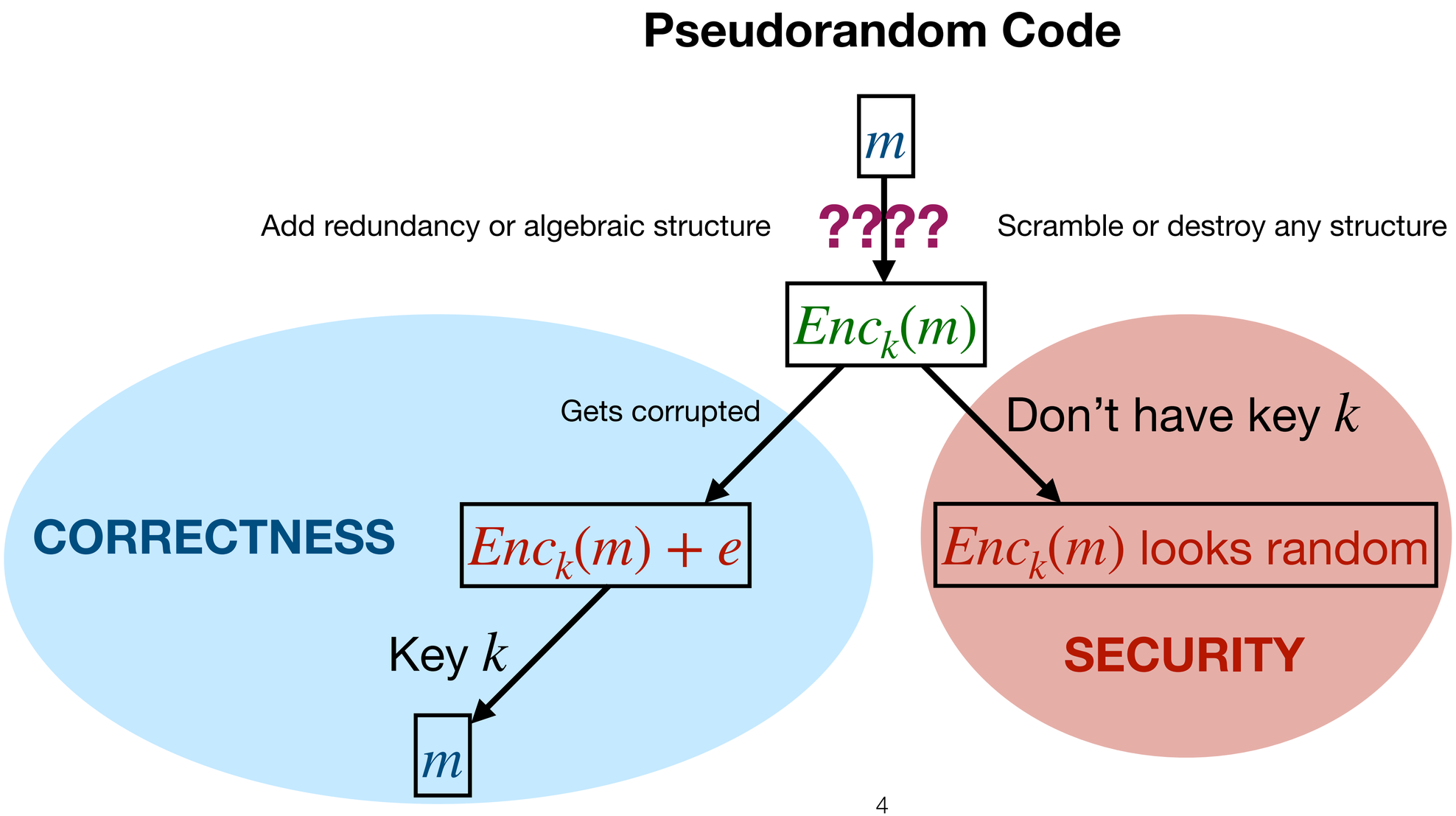


Cryptography

Requires hardness assumptions!



Pseudorandomness Meets Error-Correction



Initial 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 !!!

Constructions

Syntax of PK-PRC

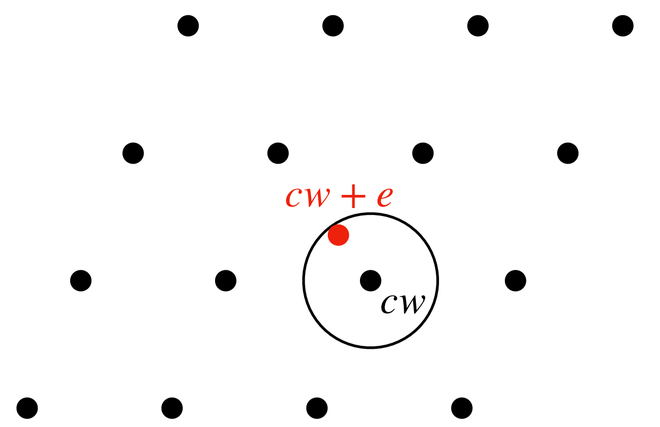
$$(pk, sk) \leftarrow Setup(1^\lambda)$$

$$cw \leftarrow Enc(pk, m)$$

$$cw \approx uniform$$

Psuedorandomness

$$m \leftarrow Dec(sk, cw + e)$$



Robustness

McEliece Assumption

McE'78,DDMN'12

- $(G, td) \leftarrow$ generator-matrix of binary linear code C (Binary Goppa codes)
- $P \leftarrow$ permutation matrix
- $T \leftarrow$ invertible matrix

Code-based cryptosytem

Post-quantum secure

$$PGT \approx \textit{uniform}$$

- $pk = PGT$, $sk = (P, T, td)$
- Encryption is $pk \cdot m + e$ where $Ham(e) = O(n/\log n)$.
- Decryption is $m' = Decode(td, P^{-1} \cdot ct)$ and output $T^{-1}m'$

McEliece Assumption

- Ciphertexts are not random.
- Can handle only $O(n/\log n)$ errors rather than constant fraction.
- Many natural replacements for Goppa codes are **insecure** due to algebraic distinguishers.
- Known attacks fail if PGT is masked with suitable amount of errors.

Noisy McEliece Assumption

DJK**R**W'26

- $G \leftarrow$ generator-matrix of binary linear code C (Algebraic-Geometric codes)
- $P \leftarrow$ permutation matrix
- $T \leftarrow$ invertible matrix
- $E \leftarrow Ber_{\rho}$

$$PGT + E \approx \textit{uniform}$$

- $pk = PGT + E$, $sk = (G, P, T)$
- Encryption is $pk \cdot m + e$ where $Ham(e) = O(n)$.

LPN assumption

- Decryption is $m' = Decode(P^{-1} \cdot ct)$ and output $T^{-1}m'$

Syntax of SK-PRC

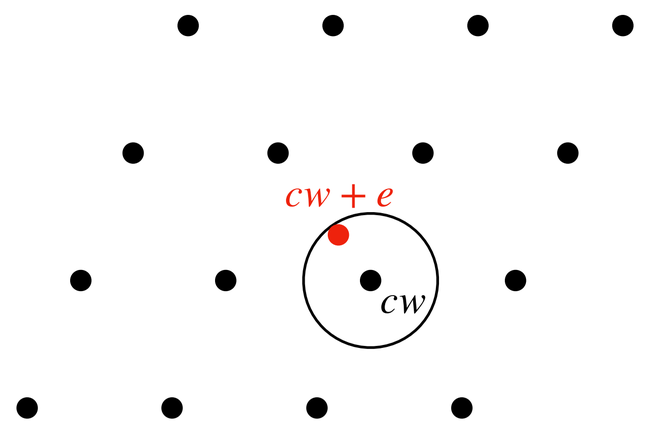
$$sk \leftarrow Setup(1^{\lambda})$$

$$cw \leftarrow Enc(sk, m)$$

$$cw \approx uniform$$

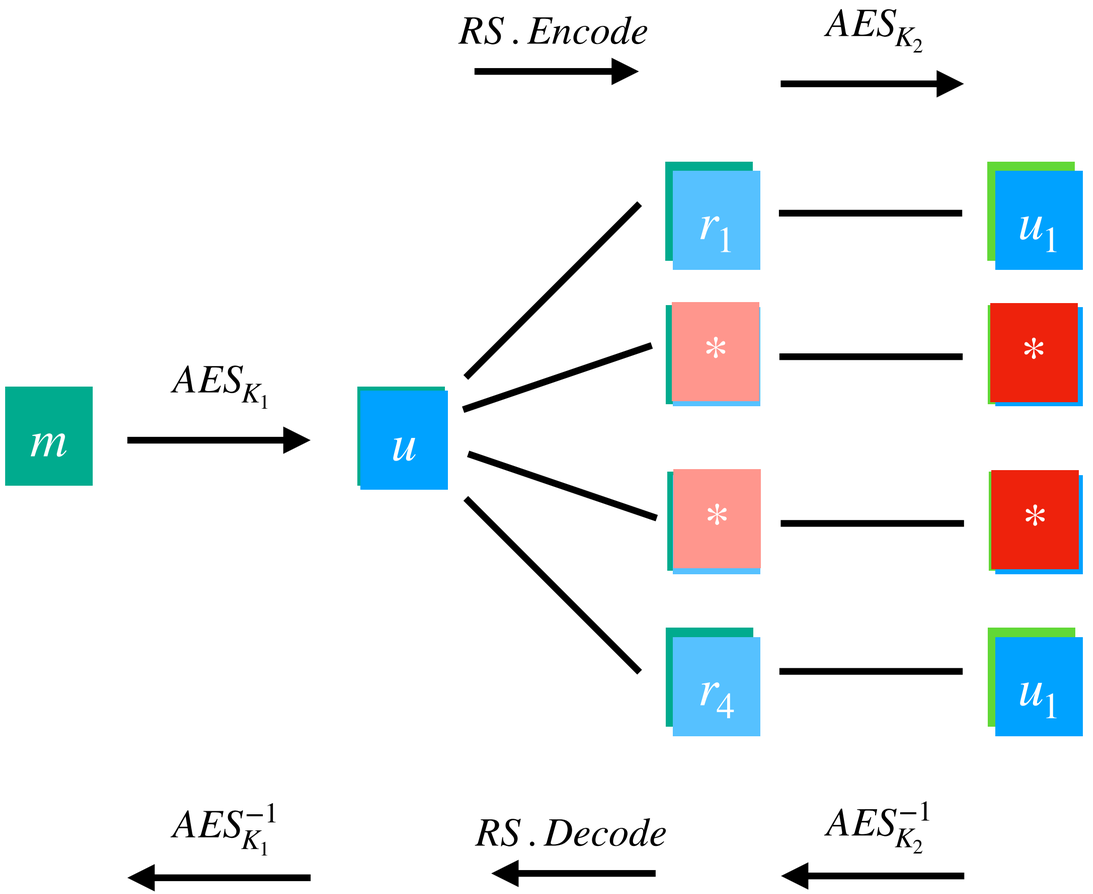
Psuedorandomness

$$m \leftarrow Dec(sk, cw + e)$$



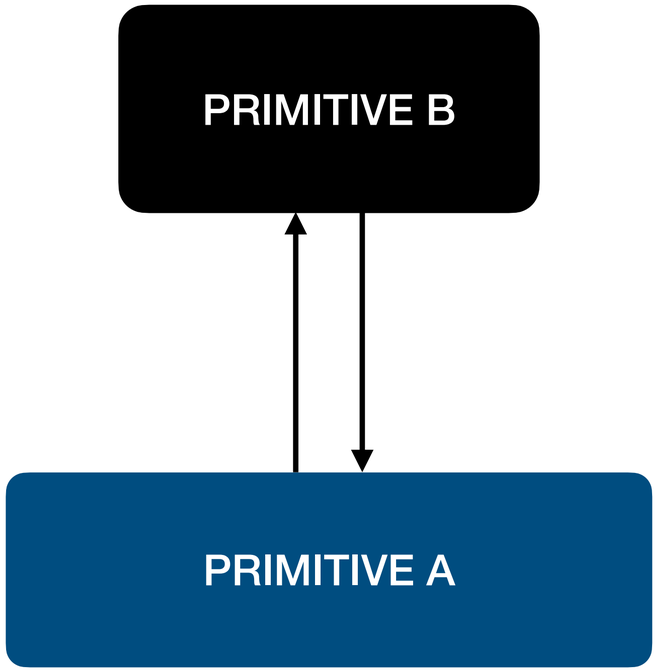
Robustness

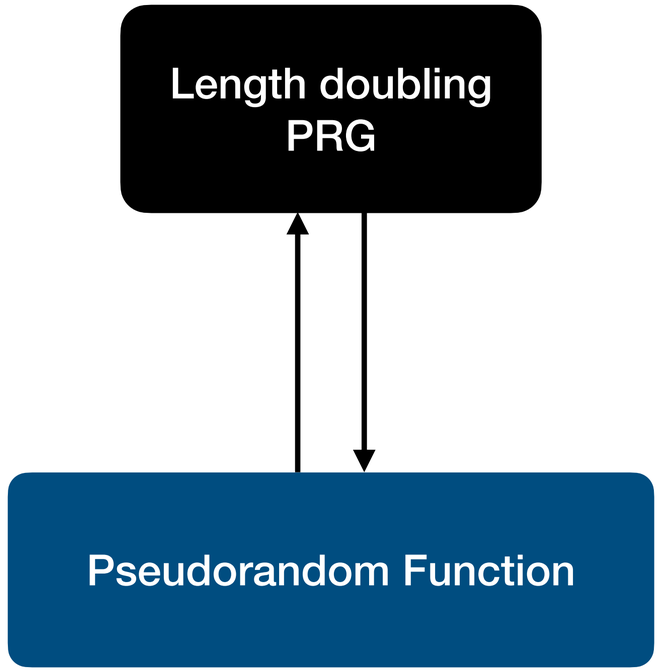
Blackbox Construction for Large Alphabets



Impossibility Result

Blackbox Construction



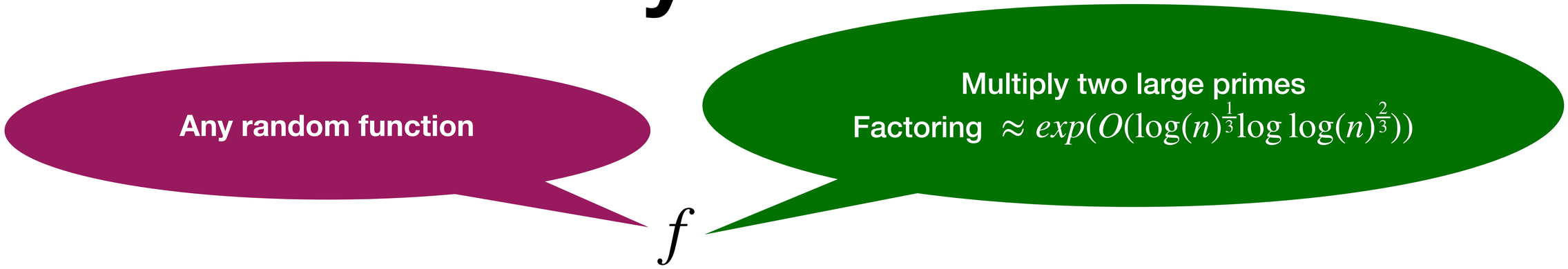


Goldreich,Goldwasser,Micali'86

Our Result

There is no blackbox construction of pseudorandom codes from

One-Way Function



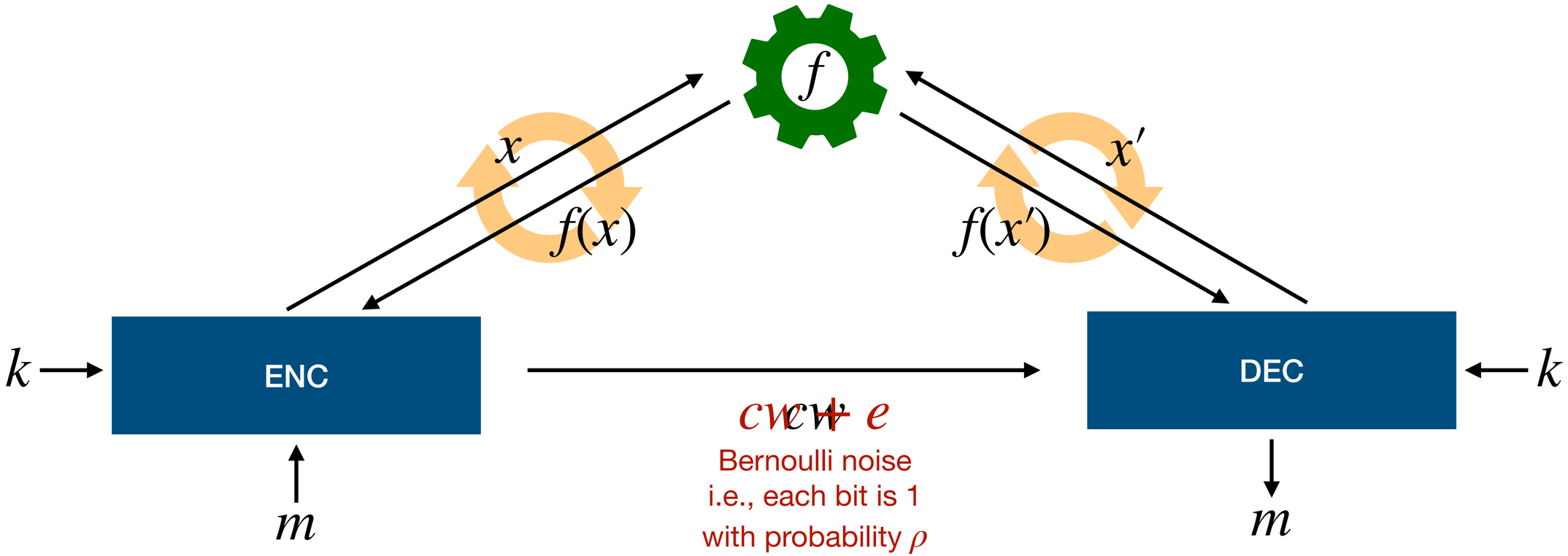
x —— **Efficient** ——▶ $f(x)$

r' ◀—— **Hard to invert in polynomial time** —— $f(r)$

s.t. $f(r') = f(r)$

where r is random

Blackbox Construction of PRC from f



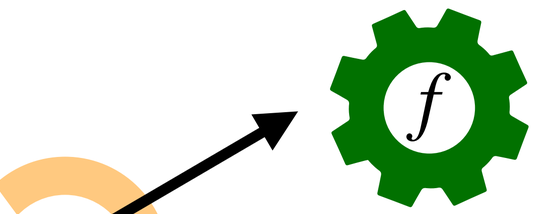
Security

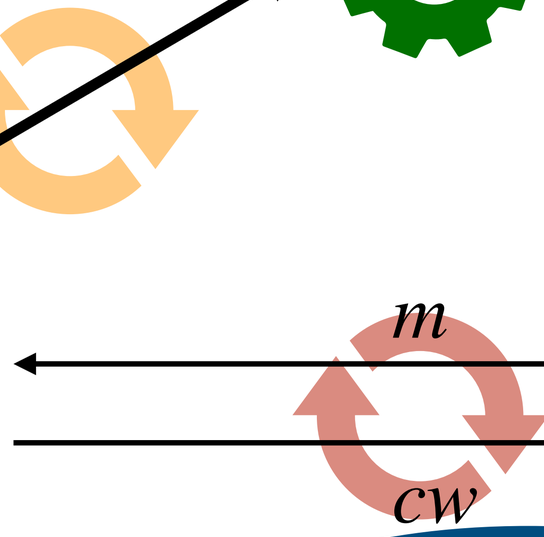
$b \leftarrow \{0,1\}$

$k \leftarrow Setup$

$if(b = 0) : cw \leftarrow Enc_k^f(m)$

$cw \leftarrow random$





But, only polynomially many queries allowed

Time and Space Unbounded

I can only use f as a source of hardness

Base Case

- $Dec^f_{(\cdot)}$ ~~does not make any~~ makes f queries that does not intersect with $Enc^f_{(\cdot)}$ queries !
  - Sends random m_i to challenger and obtain corresponding cw_i.
  - For each k, check whether $Dec_k(cw_i) = m_i$ for all i.
  - If there exists such a k, output “PRC”. Otherwise, “RANDOM”.

Assumptions

$Dec^f_{(\cdot)}$ is deterministic.

$Dec^f_{(\cdot)}$ makes a single f query.

High-Level Idea

I know DEC and also $Quer_{(\cdot)}$

Learn frequent **GLOBAL** queries and store those queries and responses in $\mathscr{L}_k$

$Quer_k(cw)$

k → DEC

cw ↑ m ↓

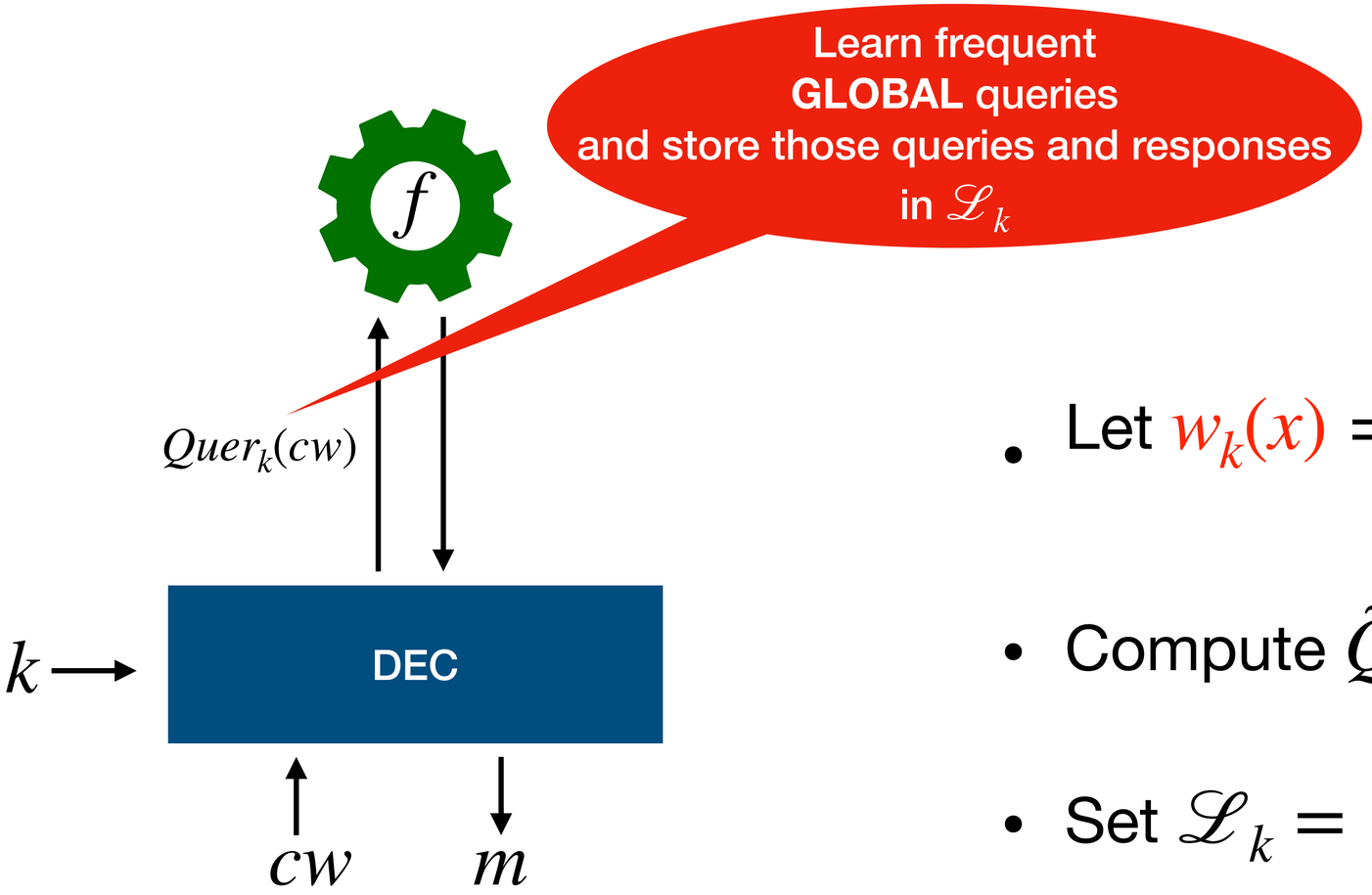
Trivial case

DEC* ← $k, \mathscr{L}_k$

cw ↑ m ↓

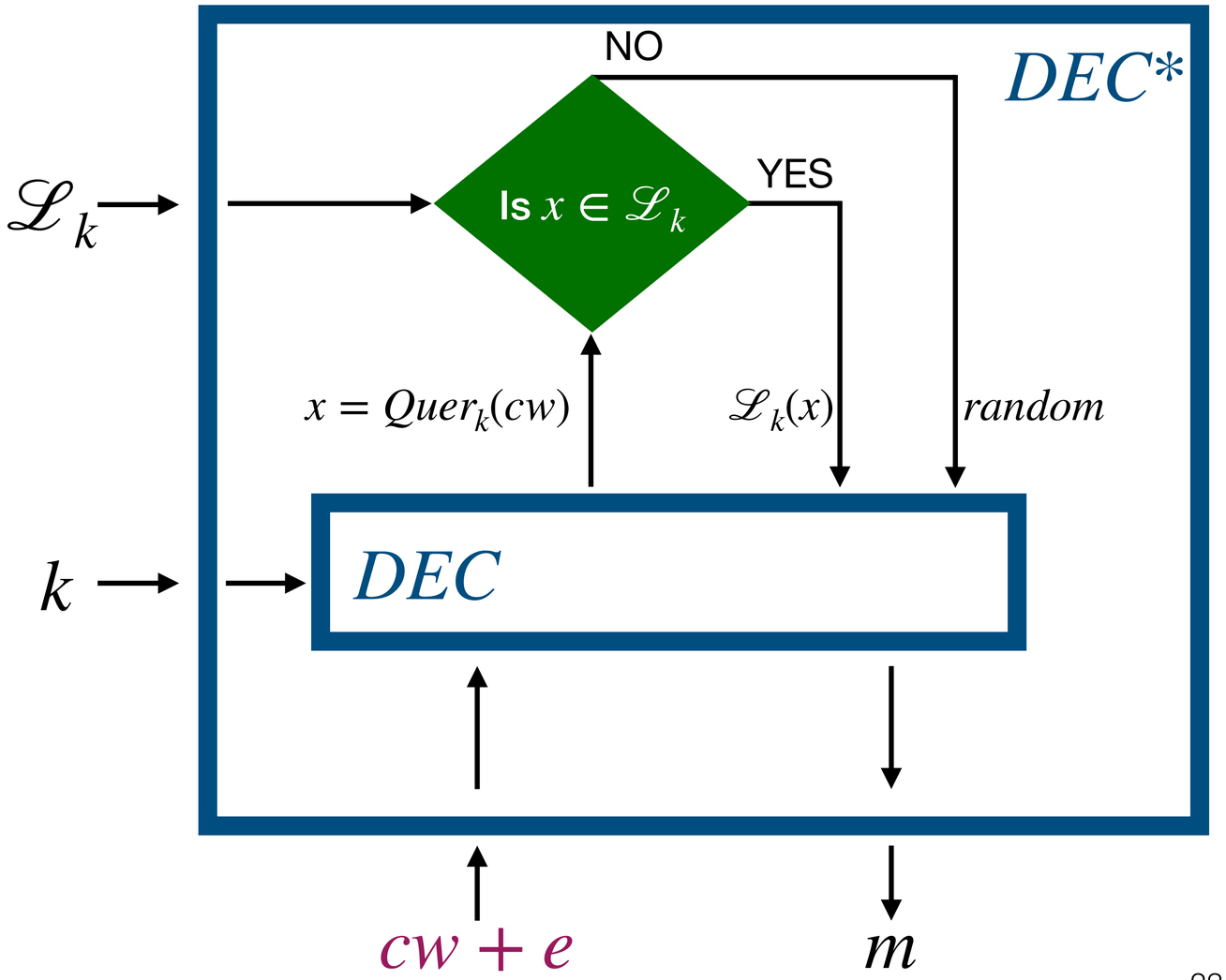
Learning Global Queries

Time and Space Unbounded



- Let $w_k(x) = \Pr_{u \leftarrow \{0,1\}^{|cw|}}[Quer_k(u) = x]$.
- Compute $\tilde{Q}_k = \{x \mid w_k(x) \geq 1/poly(\lambda)\}$.
- Set $\mathscr{L}_k = \{(x, f(x)) \mid \forall x \in \tilde{Q}\}$

How does DEC^* work ?

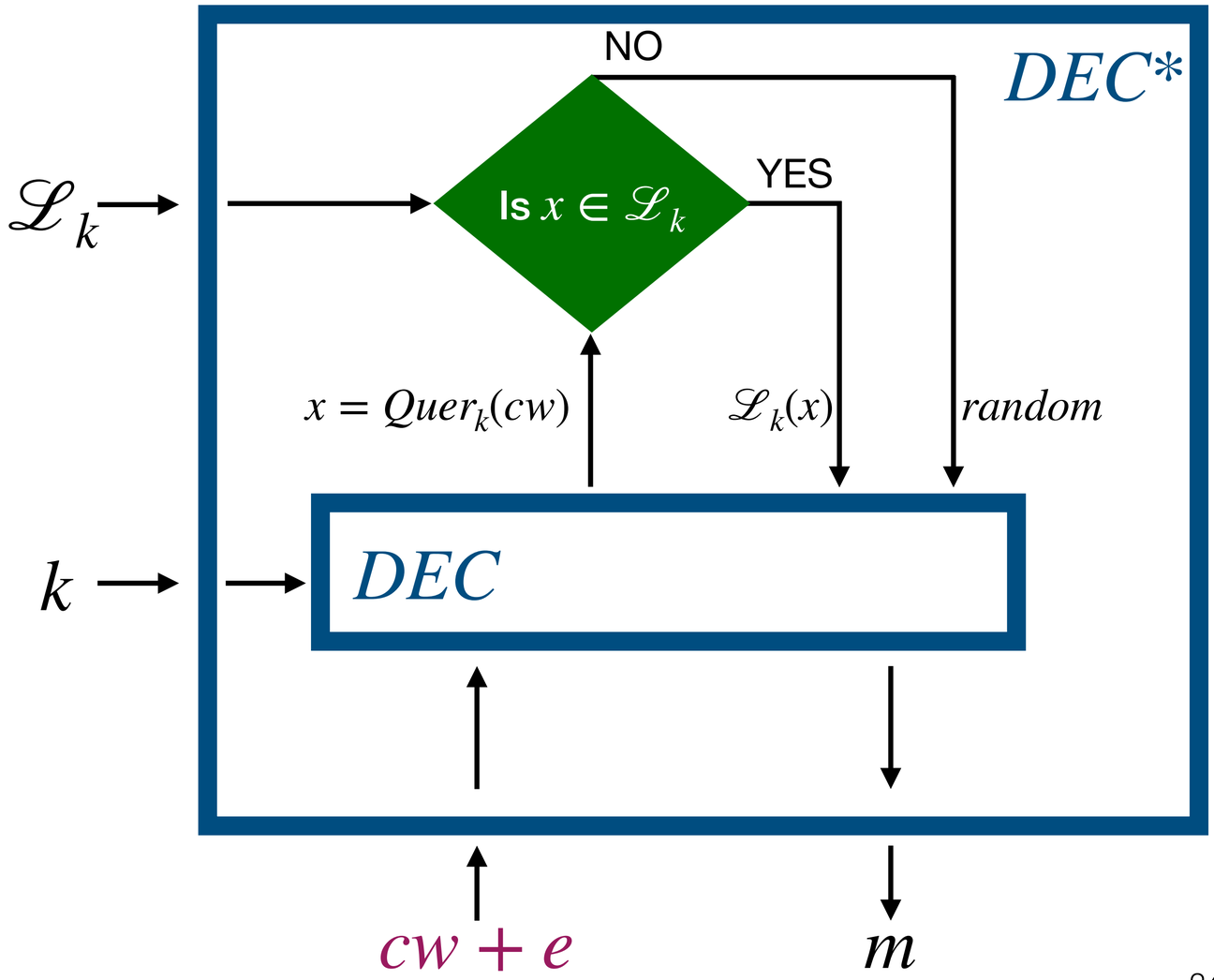


- If “YES”, perfect simulation because $\mathscr{L}_k = \{(x, f(x))\}$.

- If “NO”, simulation might fail.

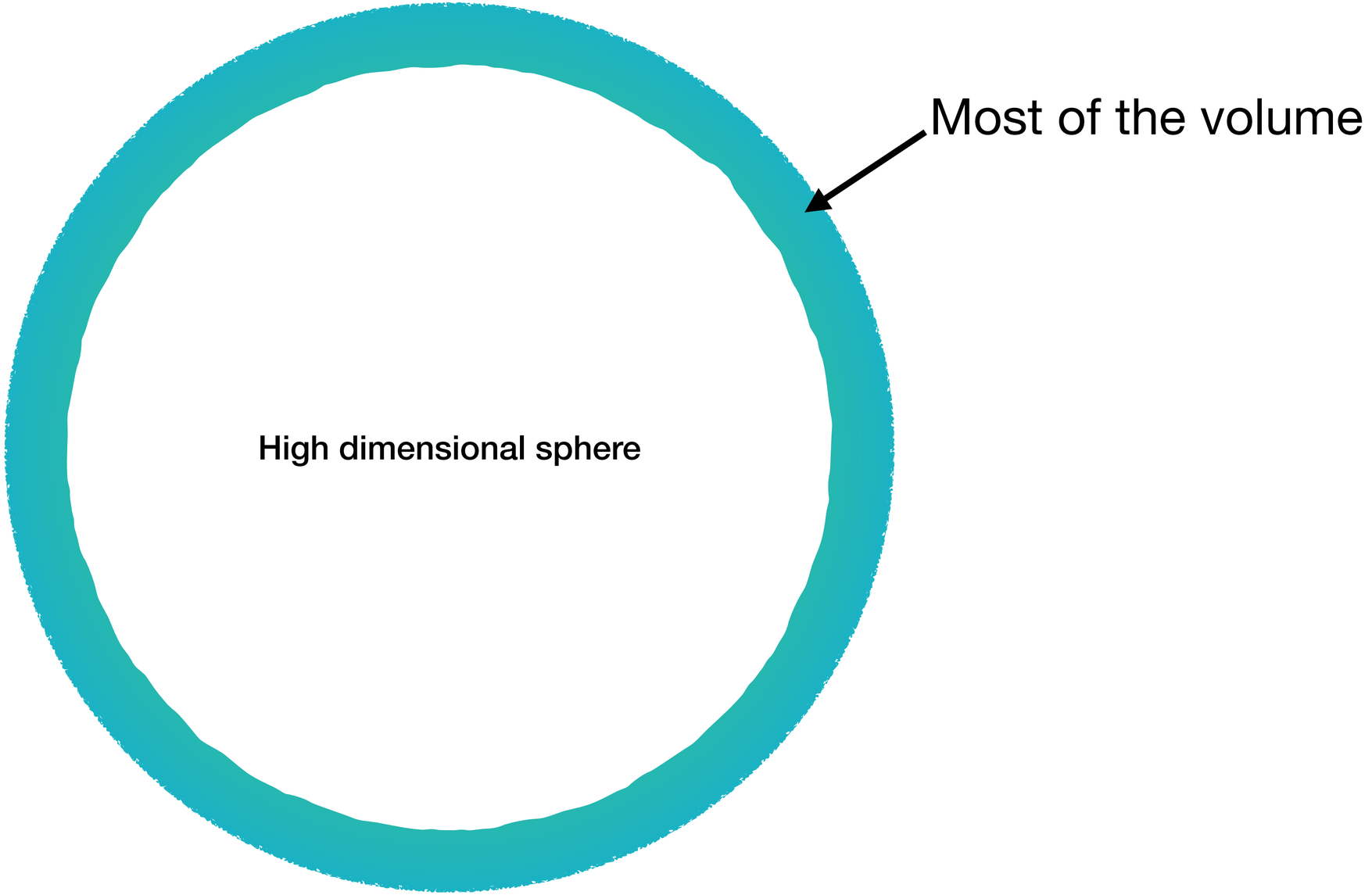
Are **NON-GLOBAL** but **LOCAL** queries frequent?

Worst-Case Dec

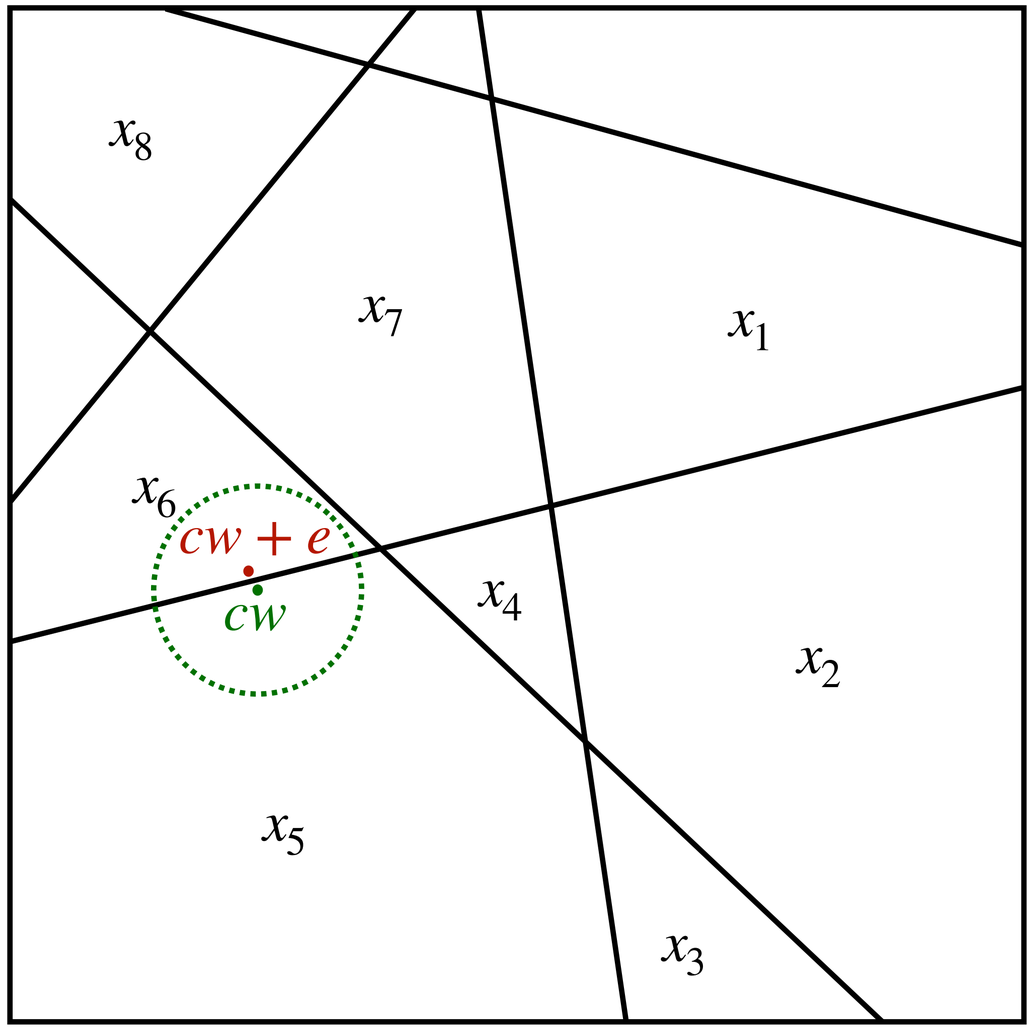


- For every codeword cw_i, $x_i = Quer_k(cw_i + e)$ is **unique**.
- Maybe possible that $w_k(x_i) = negl(\lambda)$
- In this case, “NO” is always executed!

Concentration of Measure



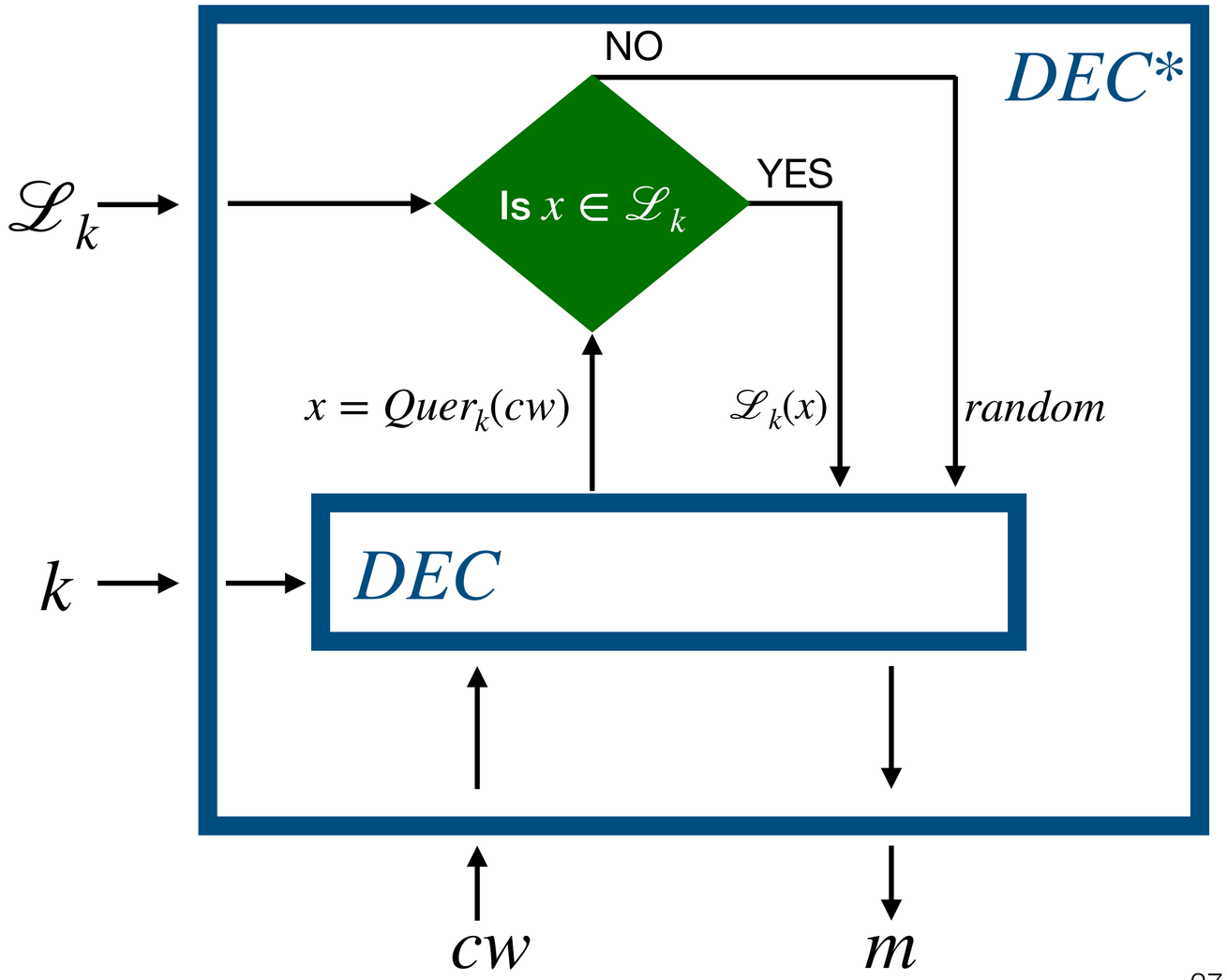
Hypercontractivity Theorem [Bon70][Bec75]



$Quer_k : \{cw_i\} \to \{x_j\}$

- Note that Dec_k must properly decode $cw + e$.
- If a Boolean function (including $Quer_k$) is not almost constant, then some input variable must have non-negligible influence on the output.
- **The theorem is for uniformly random strings.**
- Rely on pseudorandomness of the codewords.

How does DEC^* work ?



- If “YES”, perfect simulation because $\mathscr{L} = \{(x, f(x))\}$.

- If “NO”, simulation might fail.

NON-GLOBAL but LOCAL queries are not frequent !!!

Lifting to Multiple Queries

- Suppose $Dec^{f}_{(\cdot)}$ makes ℓ many queries.
- Perform the previous transformation with $Quer$ being the **first query** made by $Dec^{f}_{(\cdot)}$.
- This will give $Dec^{*f}_{(\cdot)}$ that makes at most $\ell - 1$ many queries!

My Results

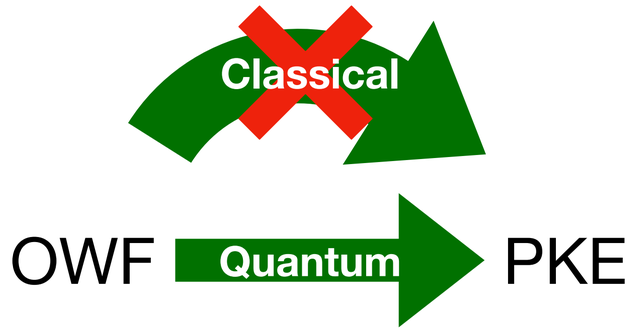
- Proved that PRCs cannot be constructed via black-box techniques from a broad class of standard cryptographic primitives — including obfuscation. [DM**R**-TCC'25, **Outstanding paper award**].

- Extended the **impossibility** result to the **quantum setting** also! [Under submission]

- Constructed PRCs secure against **stronger adversaries** (CCA security) using non black-box techniques [Accepted in CRYPTO 2026!].

Future Work on PRCs

- Develop **quantum** PRCs, where **codewords** are **quantum states**.
  - Study decryption under different quantum error models
  - Allow classical or quantum messages
  - Identify minimal computational assumptions
- Explore more constructions/impossibilities for **plain** PRCs.



Thank You!

https://mahe94.github.io