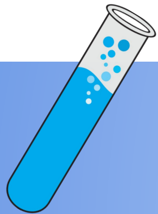
Unclonable Polymers and Their Cryptographic Applications

Ghada Almashaqbeh[1], Ran Canetti[2], Yaniv Erlich[3], Jonathan Gershoni[4], Tal Malkin[5], Itsik Pe'er[5], Anna Roitburd-Berman[4], and Eran Tromer[2]

[1]University of Connecticut, [2]Boston University, [3]Eleven Therapeutics and IDC Herzliya, [4]Tel Aviv University, and [5]Columbia University

QSig 2024

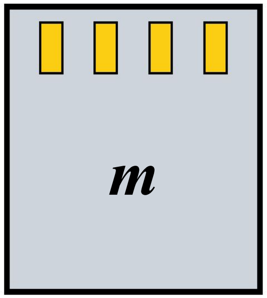


Unclonable Polymers and Their Cryptographic Applications

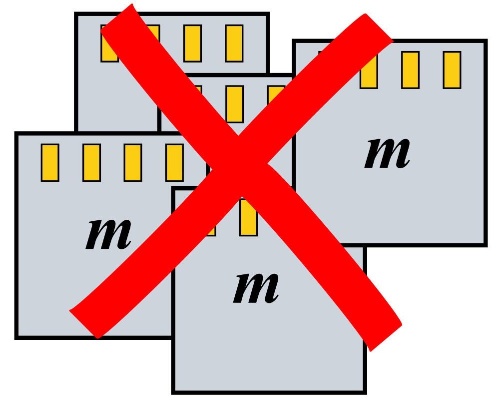
Ghada Almashaqbeh, Ran Canetti, Yaniv Erlich, Jonathan Gershoni,
Tal Malkin, Itsik Pe'er, Anna Roitburd-Berman, and Eran Tromer

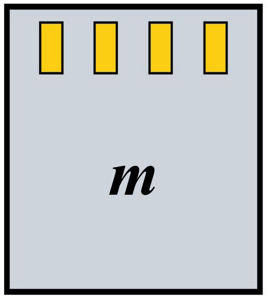
Legend:

- Cryptographer
- Computational biologist
- Biochemist

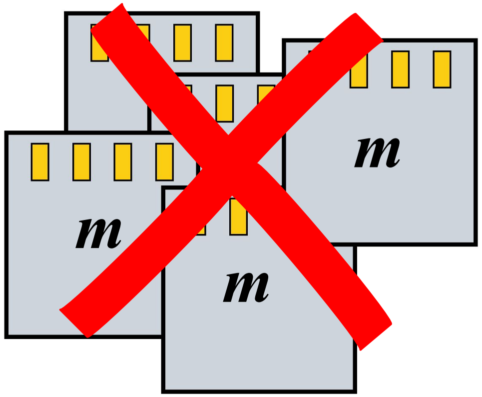


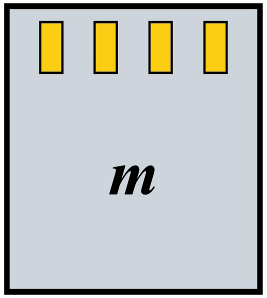
Unclonable





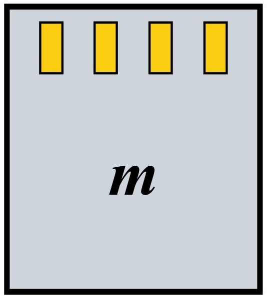
Unclonable



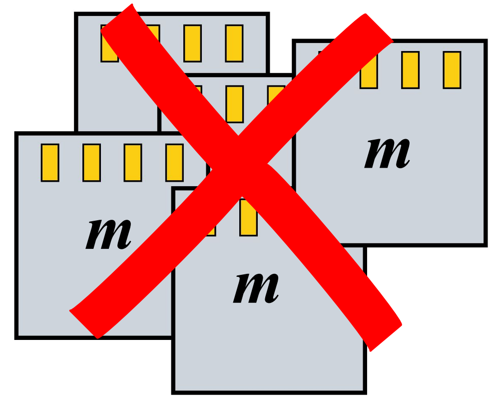


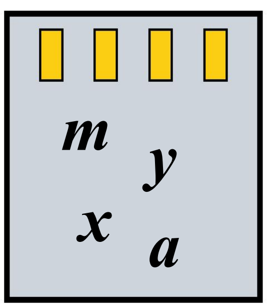
Self-destructive

Retrieve m



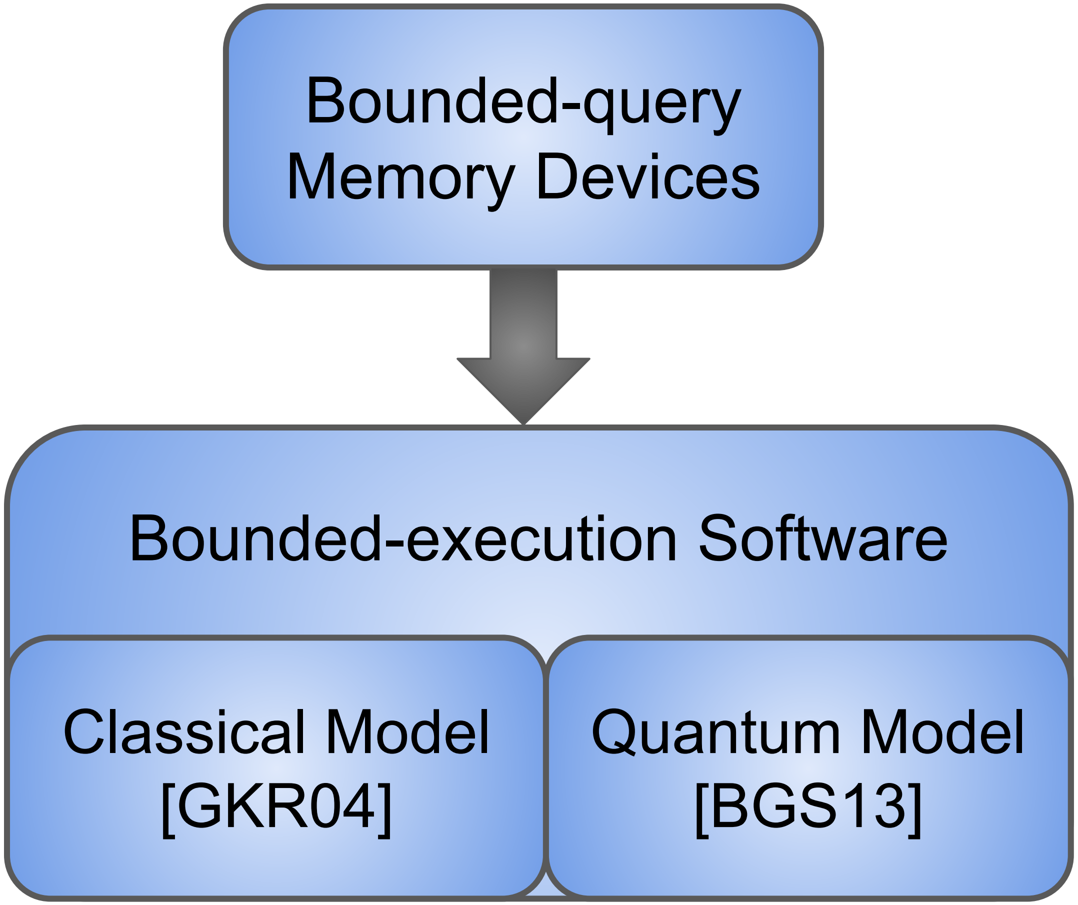
Unclonable





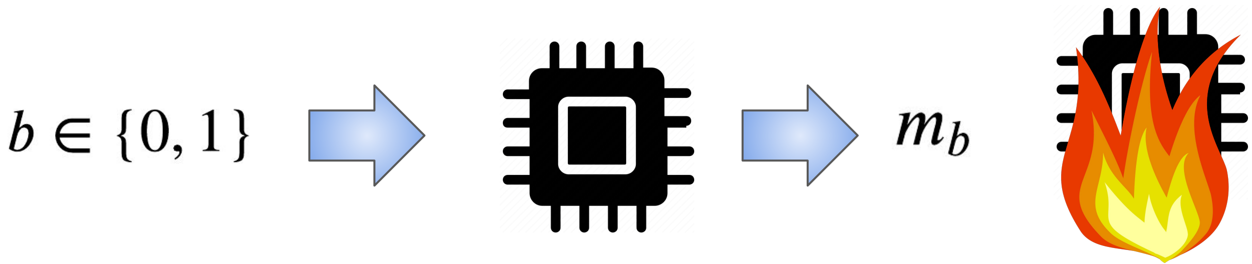
Retrieve m, x

Self-destructive


Bounded-query Memory Devices
Bounded-execution Software
Classical Model [GKR04]
Quantum Model [BGS13]

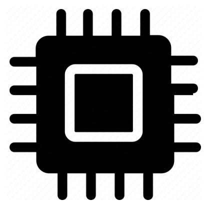
What we know:

Hypothetical, one-time memory devices [GKR04]

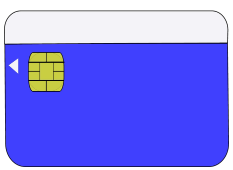


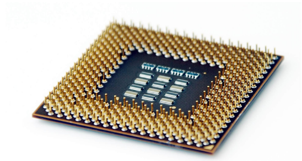
What we know:

Hypothetical, one-time memory devices [GKR04]

$b \in \{0, 1\}$ $\Rightarrow$  $\Rightarrow$ m_b 

Tamper-proof, trusted hardware





Side-channel attacks,
reverse engineering,...

??!

This Work: Alternative Technology!

Real-world unclonable and self-destructive memory devices

This Work: Alternative Technology!

Real-world unclonable and self-destructive memory devices

Formal modeling and analysis

This Work: Alternative Technology!

Real-world unclonable and self-destructive memory devices

Formal modeling and analysis

Amplification

This Work: Alternative Technology!

Real-world unclonable and self-destructive memory devices

Formal modeling and analysis

Amplification

Cryptographic applications

DNA-based Data Storage (Not Us)

10011100 …

message *m*

GTCACAT …

Nucleotides

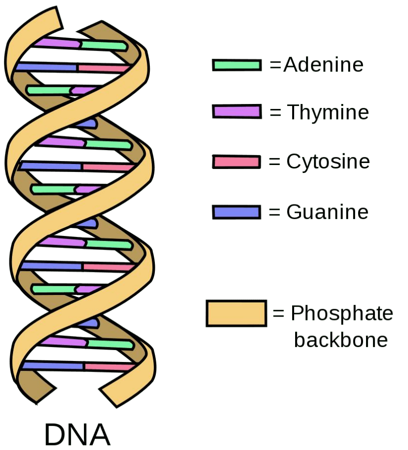


*Photo from https://www.ashg.org/discover-genetics/building-blocks/

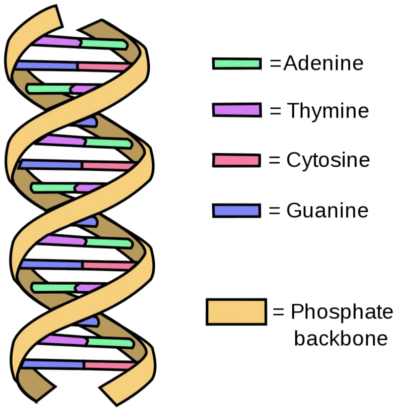
DNA-based Data Storage (Not Us)

10011100 …

message *m*

GTCACAT …

Nucleotides



DNA

Cloneable!

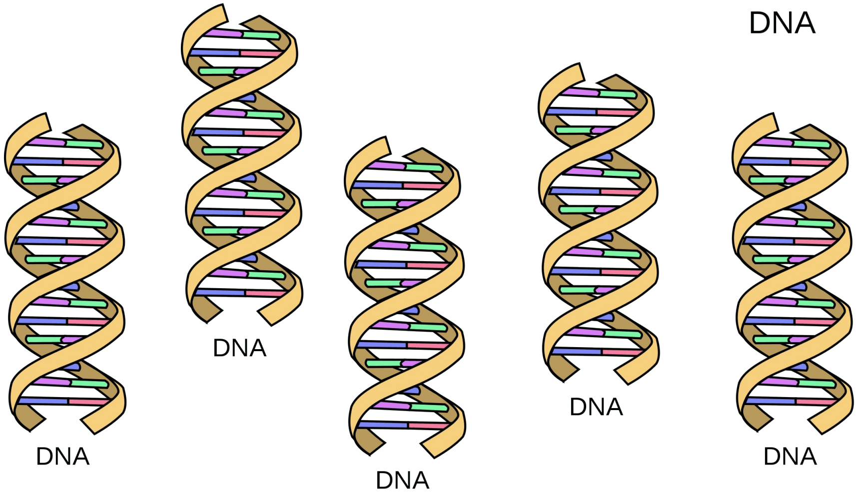


*Photo from https://www.ashg.org/discover-genetics/building-blocks/

Proteins (Us)

10011100 …

message *m*

SYRGAA …

Amino acids

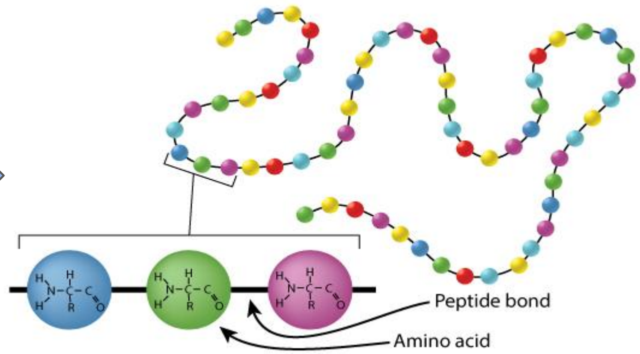
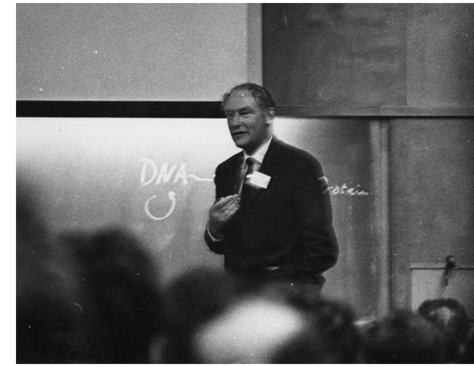
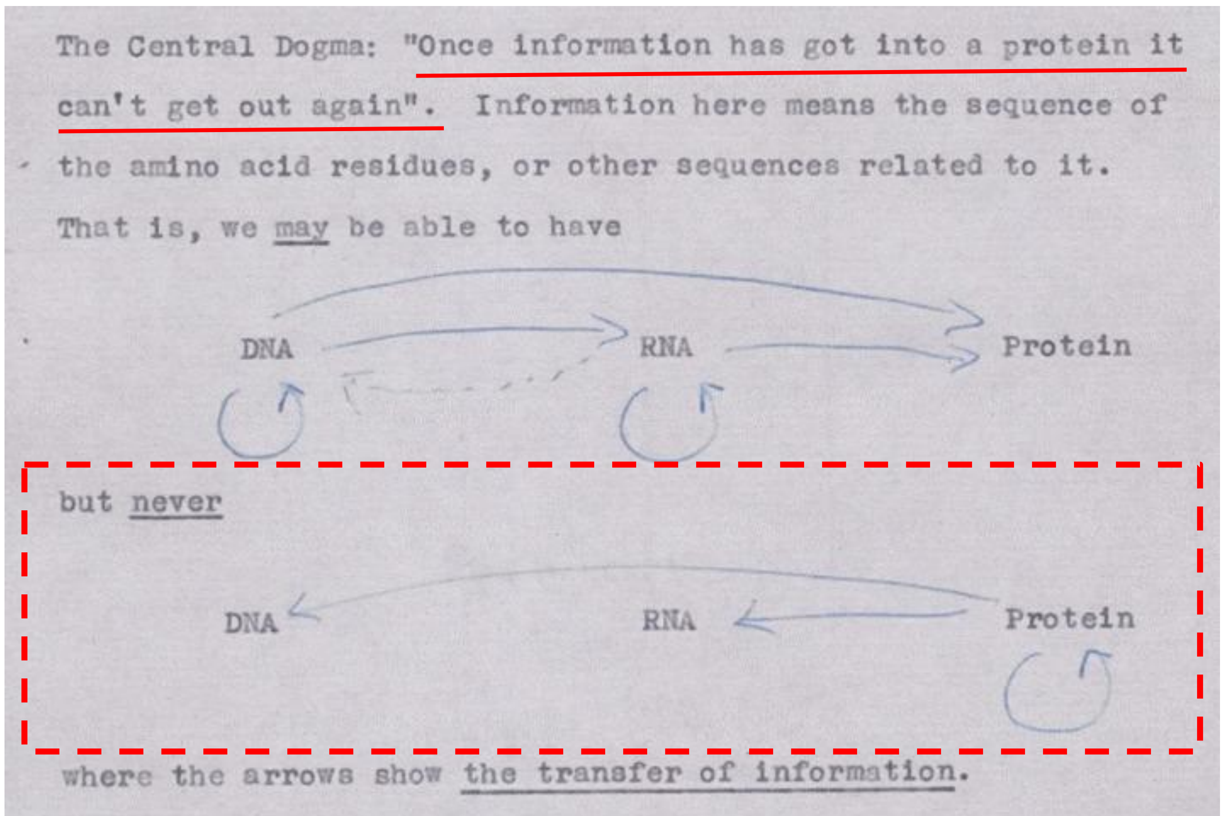


Image from: https://content.byui.edu/file/a236934c-3c60-4fe9-90aa-d343b3e3a640/1/module3/readings/proteins.html

Proteins are Unclonable



Central Dogma of Molecular Biology - Francis Crick, 1957:



The Central Dogma: "Once information has got into a protein it can't get out again". Information here means the sequence of the amino acid residues, or other sequences related to it.

That is, we may be able to have

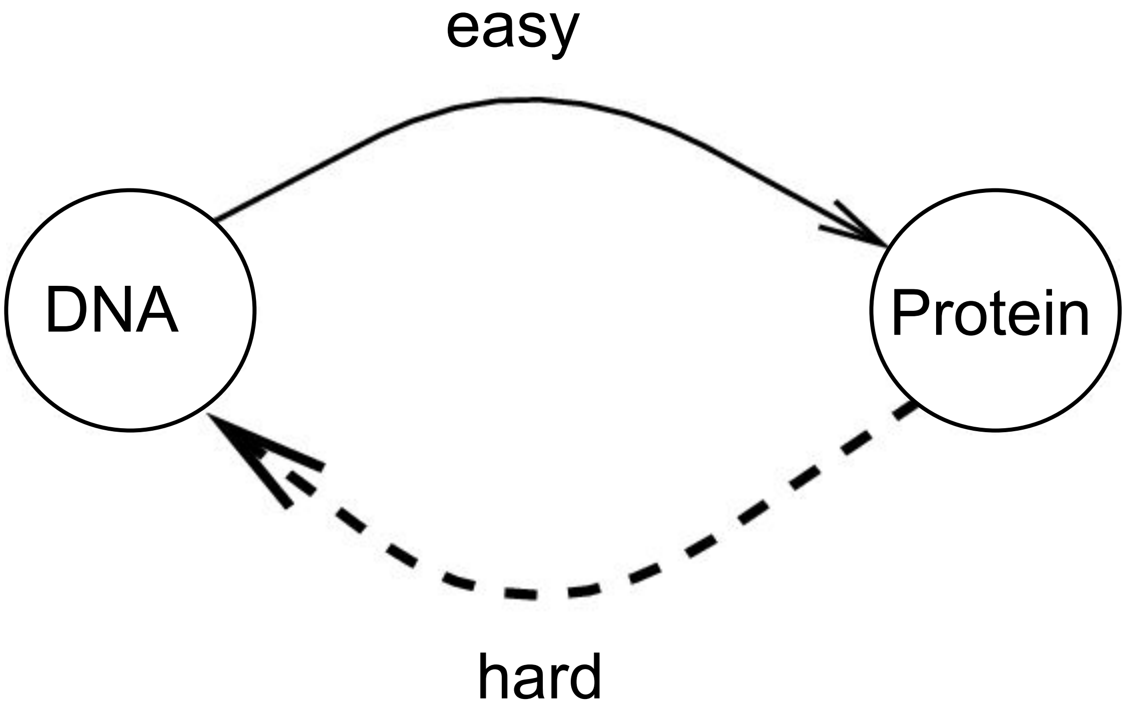
but never

where the arrows show the transfer of information.

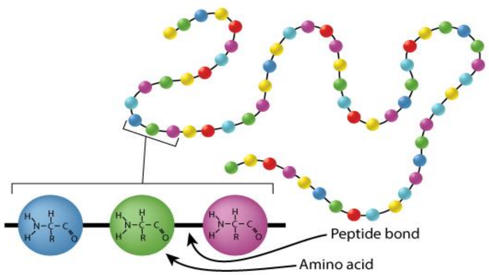
*images from https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.2003243

Proteins are Unclonable

A hypothesis (or a challenge) that is still standing for 65 years and a few billion years of evolution!



[Reading] Proteins is Destructive



Mass Spectrometry Instrument

10011100 …

message *m*

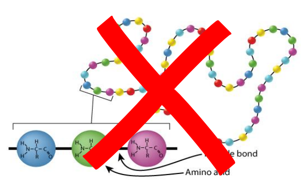
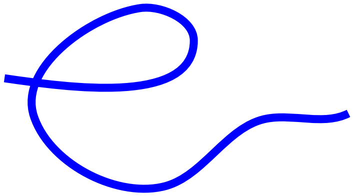


*Photo from https://www.creative-proteomics.com/support/mass-spectrometry-instruments.htm

Consumable Memory Tokens

A new protein-based construction for secure storage

Synthesize m

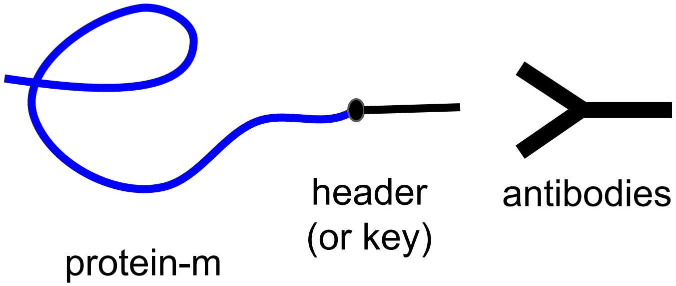


protein-m

Consumable Memory Tokens

A new protein-based construction for secure storage

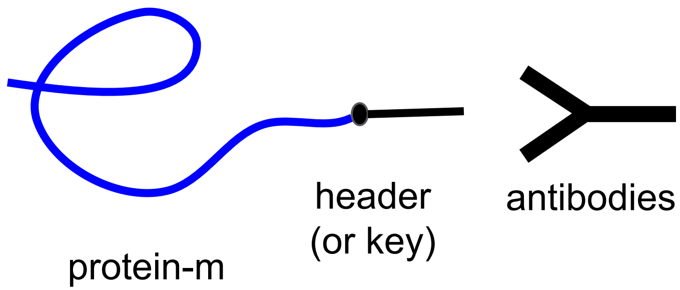
Synthesize m



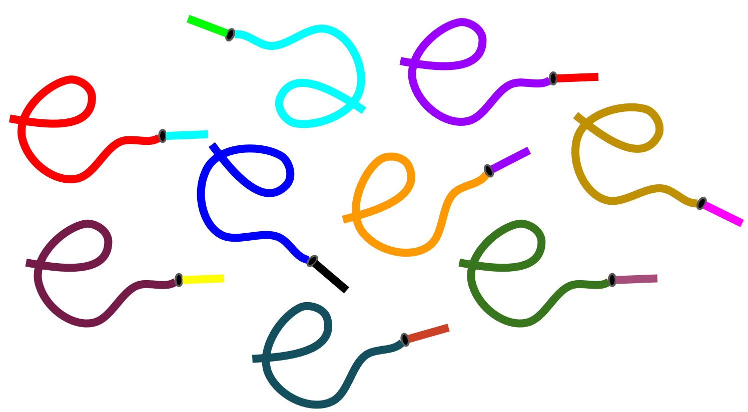
Consumable Memory Tokens

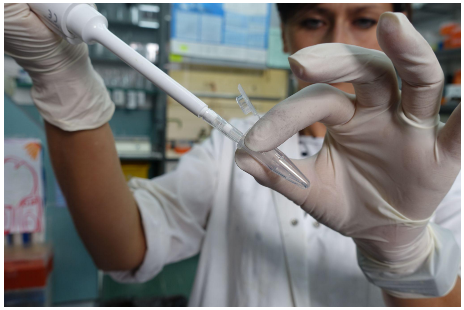
A new protein-based construction for secure storage

Synthesize m



Mix with decoy proteins

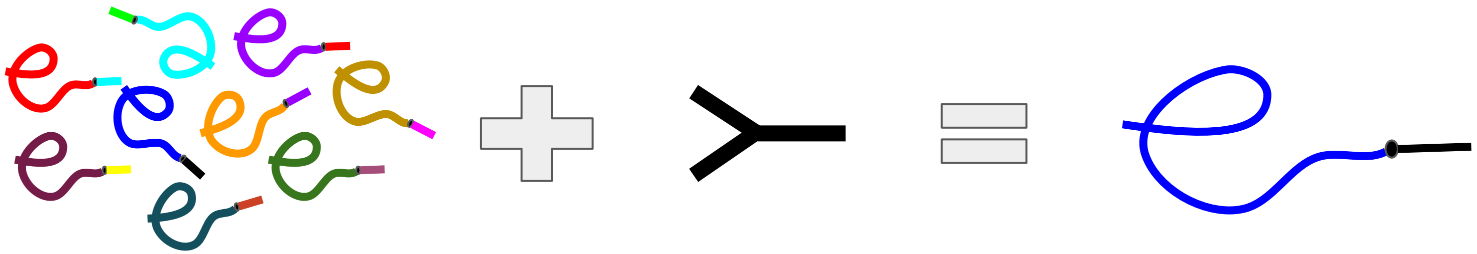




Consumable Memory Tokens

A new protein-based construction for secure storage

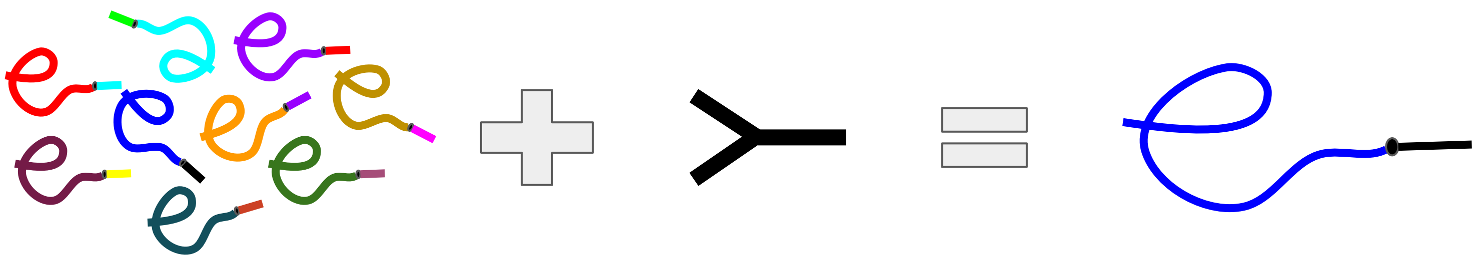
To retrieve m, first purify



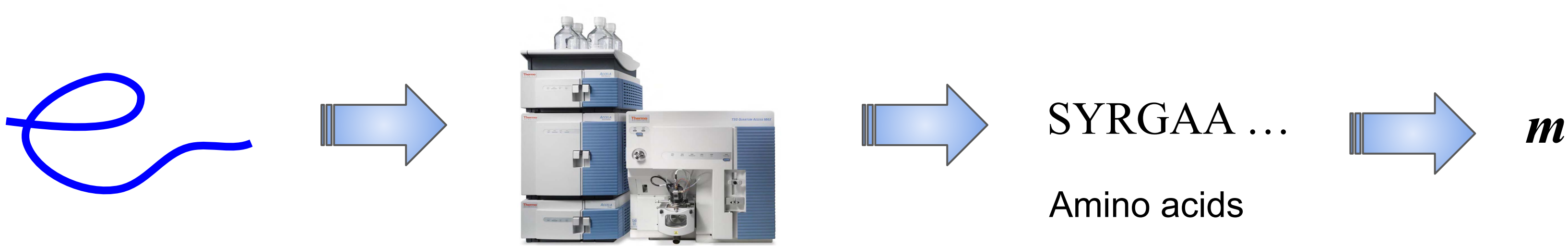
Consumable Memory Tokens

A new protein-based construction for secure storage

To retrieve m, first purify



then read the sequence



Model (Informal)

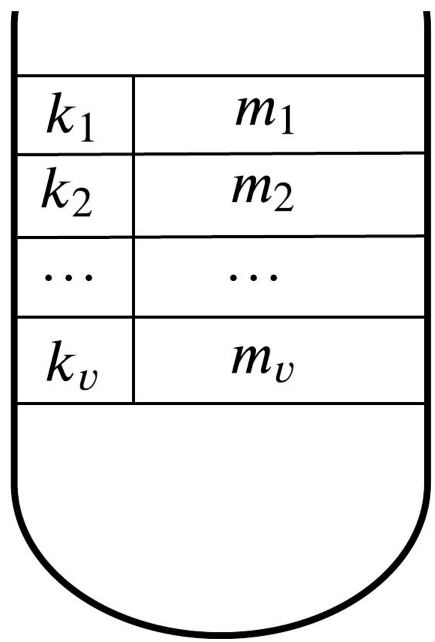
- Can store only a small number of short messages using short keys
- The only meaningful interaction is by applying antibodies (keys)
- Each retrieval attempt consumes part of the vial
- Account for powerful adversaries

n *key guesses ⇒ sample is destructed*

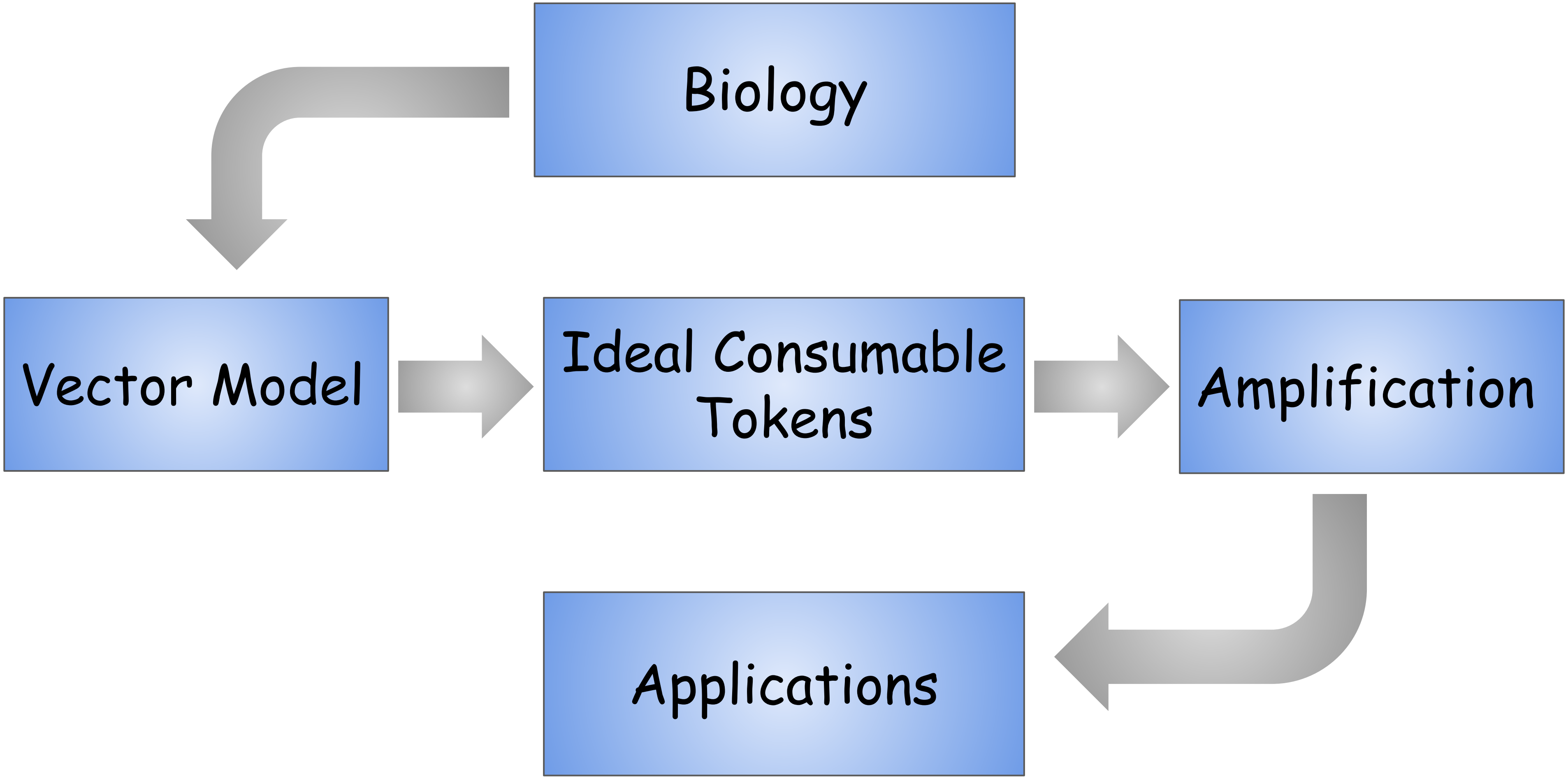
- Non-negligible soundness error γ

Extension: Partially Retrievable Memory

- Store v messages using v keys
- Only n out v messages can be retrieved ($n < v$)



Modeling and Applications



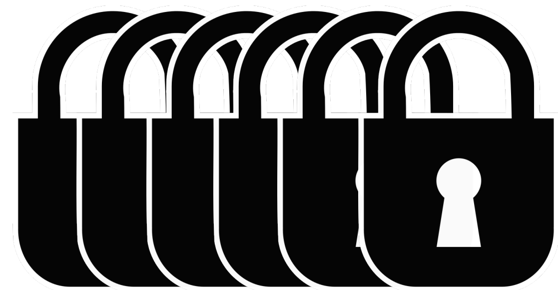
Applications of Consumable Tokens

Digital Lockers

Password $p \in \mathcal{P}$ and message m

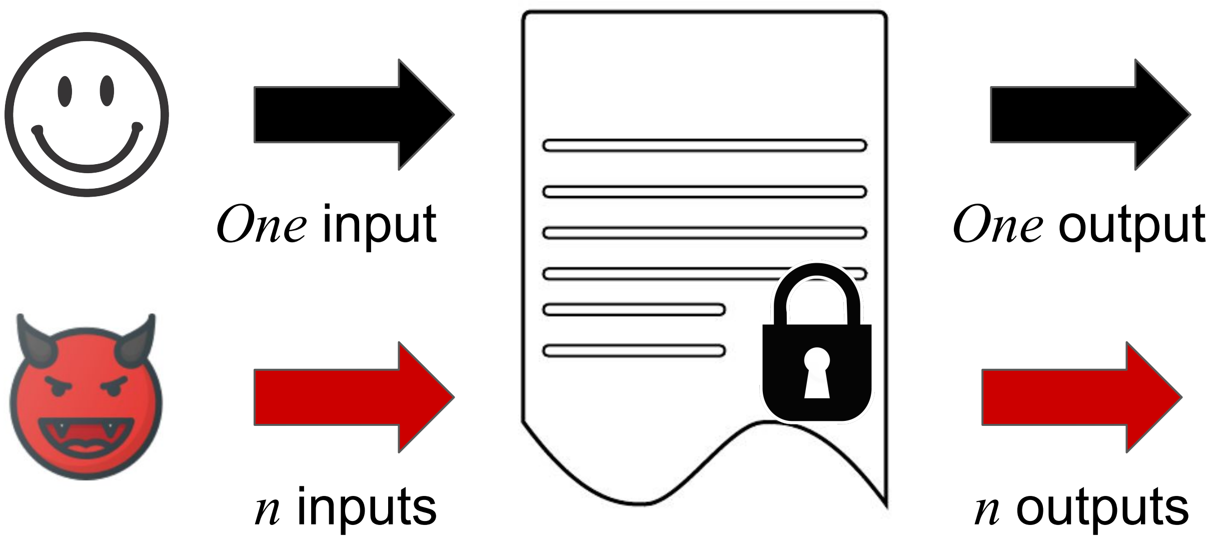
$c = Enc_p(m)$

$i \in \{1, \ldots, n\} : p_i \in \mathcal{P}, Dec_{p_i}(c)$



Resistant to brute search attacks

$(1, n)$-time Programs



$(1, n)$-time Programs Construction

$$f : \mathcal{X} \to \mathcal{Y}$$

Step 1: Create a consumable token

For each $x \in \mathcal{X}$ store a unique secret message m in the token

Step 2: Obfuscate a program for f

Obfuscate a program that outputs $f(x)$ only if the correct m corresponding to x is presented

Unclonable Cryptography

A Tale of No-cloning Paradigms—Polymer & Quantum*

*G. Almashaqbeh and R. Chatterjee. *Building Unclonable Cryptography: A Tale of Two No-cloning Paradigms.* Secrypt 2023

No-Cloning: Polymer vs. Quantum

- **Unclonable Polymers**
  - No superposition.
    - Either obtain the stored data or nothing.
  - No gentle measurement that do not disturb the polymer state.
    - Any data retrieval attempt irreversibly consumes the state.
  - Power gap between adversary and honest parties.
    - A powerful adversary can perform up to *n* data retrieval queries.

Polymer-based One-shot Signatures?

- **Cannot be achieved!**
  - The power gap allows an attacker to sign up to *n* messages instead of just one.
- **Potential Construction**
  - (1,n)-time programs.
  - Hash and sign paradigm using Chameleon hash functions [AGKZ20].
- **How can we achieve it in the polymer-based setting?**
  - Close the power gap by devising a stronger biology construction/model.
  - Or … some new direction?!

The Road Ahead

- **A hybrid no-cloning model**
  - Combine quantum- and polymer-based models to obtain the best of both worlds.
    - The two models seem to be incomparable and complementary rather than alternatives.
    - Potentially obtain both bounded-execution and no-power-gap measurements/data retrieval.

Thank you!

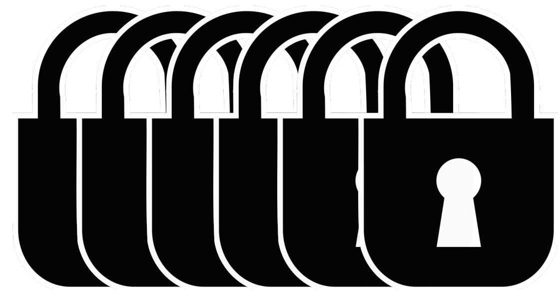
Questions?

Digital Lockers

Password $p \in \mathcal{P}$ and message m

$c = Enc_p(m)$

$i \in \{1, \dots, n\} : p_i \in \mathcal{P}, Dec_{p_i}(c)$



Resistant to brute search attacks

- Create u tokens to store u shares of m
- Map p into u token keys
- Chain the tokens together so A can try only n password guesses

In other words…
Bounded-query Point Function Obfuscation

$$I_{p,m}(p') = \begin{cases} m & \text{if } p' = p \\ \perp & \text{otherwise} \end{cases}$$

- $\mathcal{F}_{BPO}$ models obfuscation of this multi-output point function such that:

Honest party: knows p, one query to obtain m

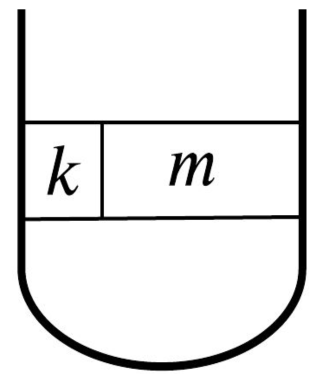
Adversary: Can try up to n password guesses

Let's construct it from consumable tokens!

Is not this immediate?

- Map p to a token key k
- Use a (1, n, 1)-consumable token to encode m under k

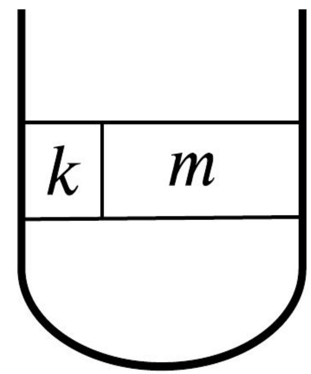
$$k \leftarrow f(p) \quad \Rightarrow \quad Encode(k, m, 1) \quad \Rightarrow$$



No, it is not!

- Map p to a token key k
- Use a (1, n, 1)-consumable token to encode m under k

$$k \leftarrow f(p) \quad \Rightarrow \quad Encode(k, m, 1) \quad \Rightarrow$$



$\mathcal{F}_{CT}$ **has non-negligible γ, which violates $\mathcal{F}_{BPO}$!**

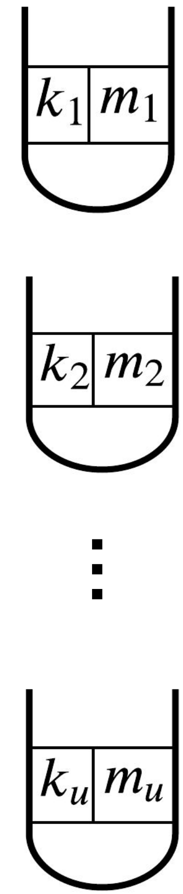
$$\Pr[\mathcal{A} \text{ retrieves } m] = \frac{n}{|\mathcal{P}|} + \gamma$$

BPO Construction–Attempt #2

- Secret sharing of m

Share $m : m_1, m_2, \ldots, m_u$
such that $m = \bigoplus_{i=1}^{u} m_i$

$$
\begin{aligned}
k_1 &\leftarrow f_1(p) \\
k_2 &\leftarrow f_2(p) \\
&\ldots \\
k_u &\leftarrow f_u(p)
\end{aligned}
\quad\Longrightarrow\quad
\begin{aligned}
&Encode(k_1, m_1, 1) \\
&Encode(k_2, m_2, 1) \\
&\ldots \\
&Encode(k_u, m_u, 1)
\end{aligned}
\quad\Longrightarrow
$$

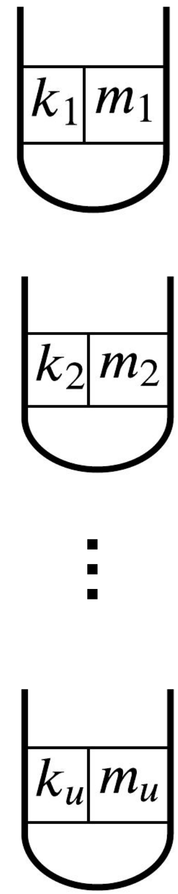


BPO Construction–Attempt #2

- Secret sharing of m

Share $m : m_1, m_2, \ldots, m_u$
such that $m = \bigoplus_{i=1}^{u} m_i$

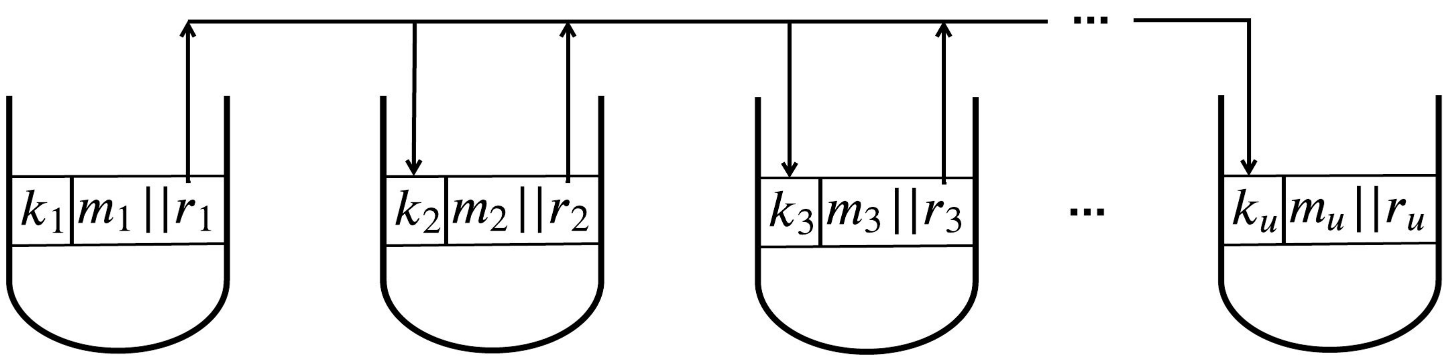
$$
\begin{aligned}
k_1 &\leftarrow f_1(p)\\
k_2 &\leftarrow f_2(p)\\
&\ldots\\
k_u &\leftarrow f_u(p)
\end{aligned}
\quad \Rightarrow \quad
\begin{aligned}
&Encode(k_1, m_1, 1)\\
&Encode(k_2, m_2, 1)\\
&\ldots\\
&Encode(k_u, m_u, 1)
\end{aligned}
\quad \Rightarrow
$$



$$\boxed{\Pr[\mathcal{A} \text{ retrieves } m] = \frac{un}{|\mathcal{P}|} + \left(1 - \frac{un}{|\mathcal{P}|}\right)\gamma^u}$$

BPO Construction–Final Attempt

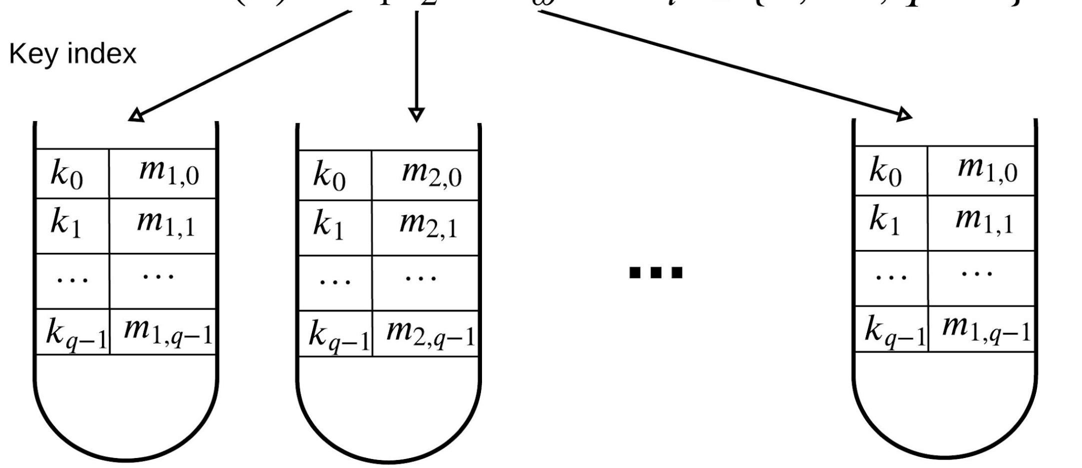
- Chaining of tokens



$$\Pr[\mathcal{A} \text{ retrieves } m] \approx \frac{n}{|\mathcal{P}|} + \left(1 - \frac{n}{|\mathcal{P}|}\right)\gamma^u$$ 🙂

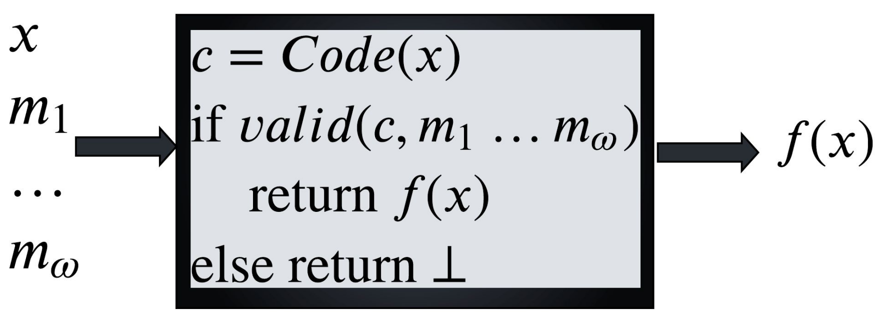
$(1, n)$-time Programs Construction

$c = Code(x) = c_1 c_2 \dots c_\omega$ s.t. $c_i \in \{0, \dots, q-1\}$



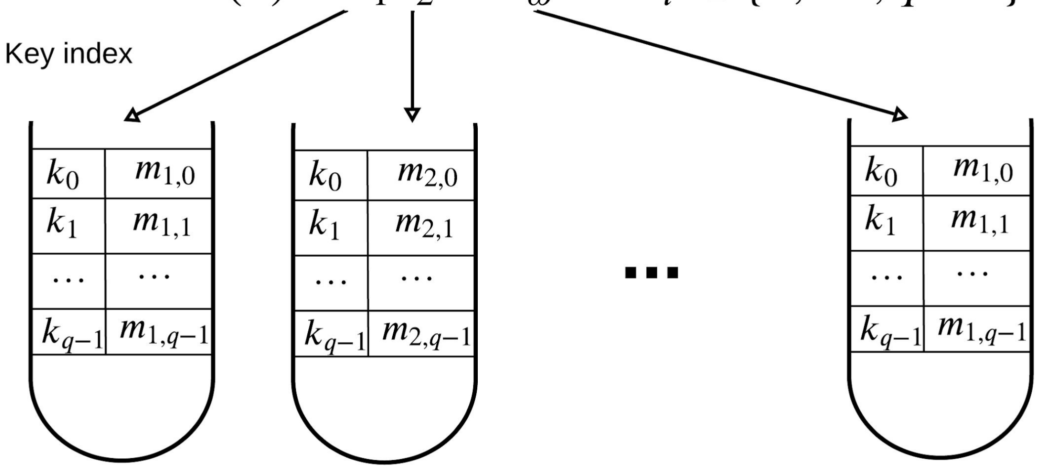
$m_1 = m_{1,c_1}$ $m_2 = m_{2,c_2}$ $m_\omega = m_{\omega,c_\omega}$

$|\mathcal{X}| = q^{d+1}$



$(1, n)$-time Programs Construction

$$c = Code(x) = c_1 c_2 \ldots c_\omega \text{ s.t. } c_i \in \{0, \ldots, q-1\}$$



$m_1 = m_{1,c_1}$ $\quad$ $m_2 = m_{2,c_2}$ $\quad$ $m_\omega = m_{\omega,c_\omega}$

$$|\mathcal{X}| = q^{d+1}$$

Set the code distance such that only n valid codewords can be retrieved!