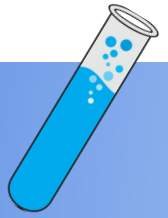
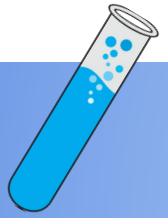


Unclonable Polymers and Their Cryptographic Applications

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[4,5]

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

July, 2022

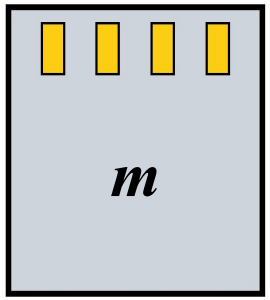


Unclonable Polymers and Their Cryptographic Applications

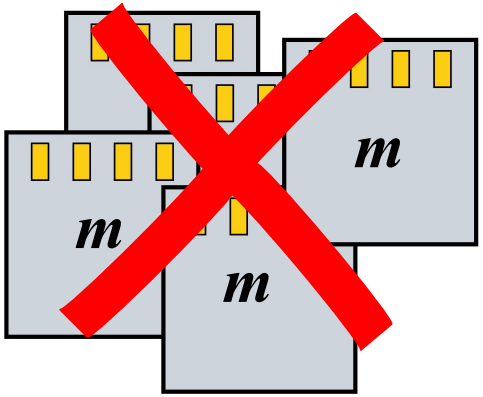
Ghada Almashaqbeh, Ran Canetti, Yaniv Erlich, Jonathan Gershoni, Tal Malkin, Itsik Pe'er, Anna Roitburd-Berman, and Eran Tromer

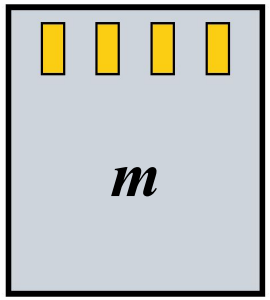
Legend:

- Cryptographer
- Computational biologist
- Biochemist

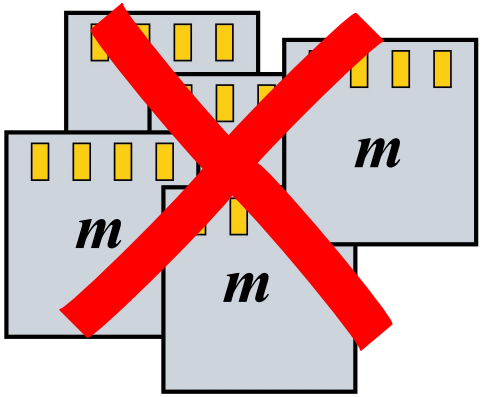


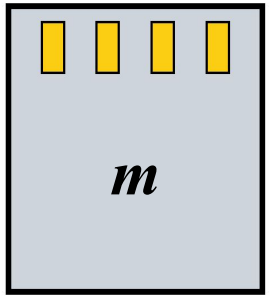
Unclonable





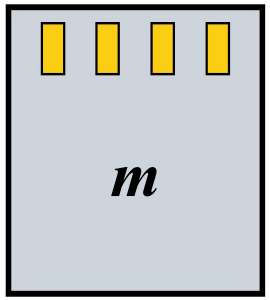
Unclonable



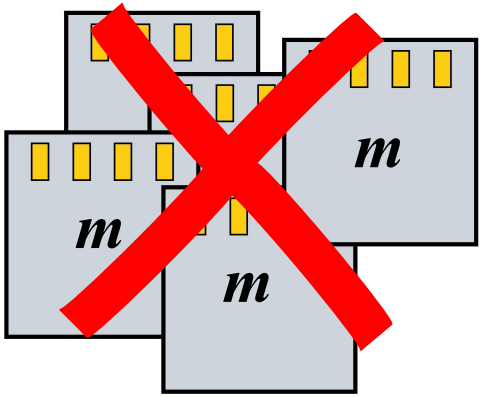


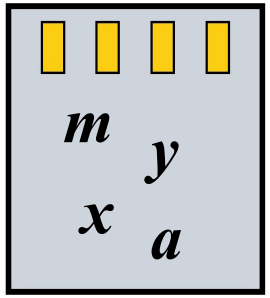
Self-destructive

Retrieve m



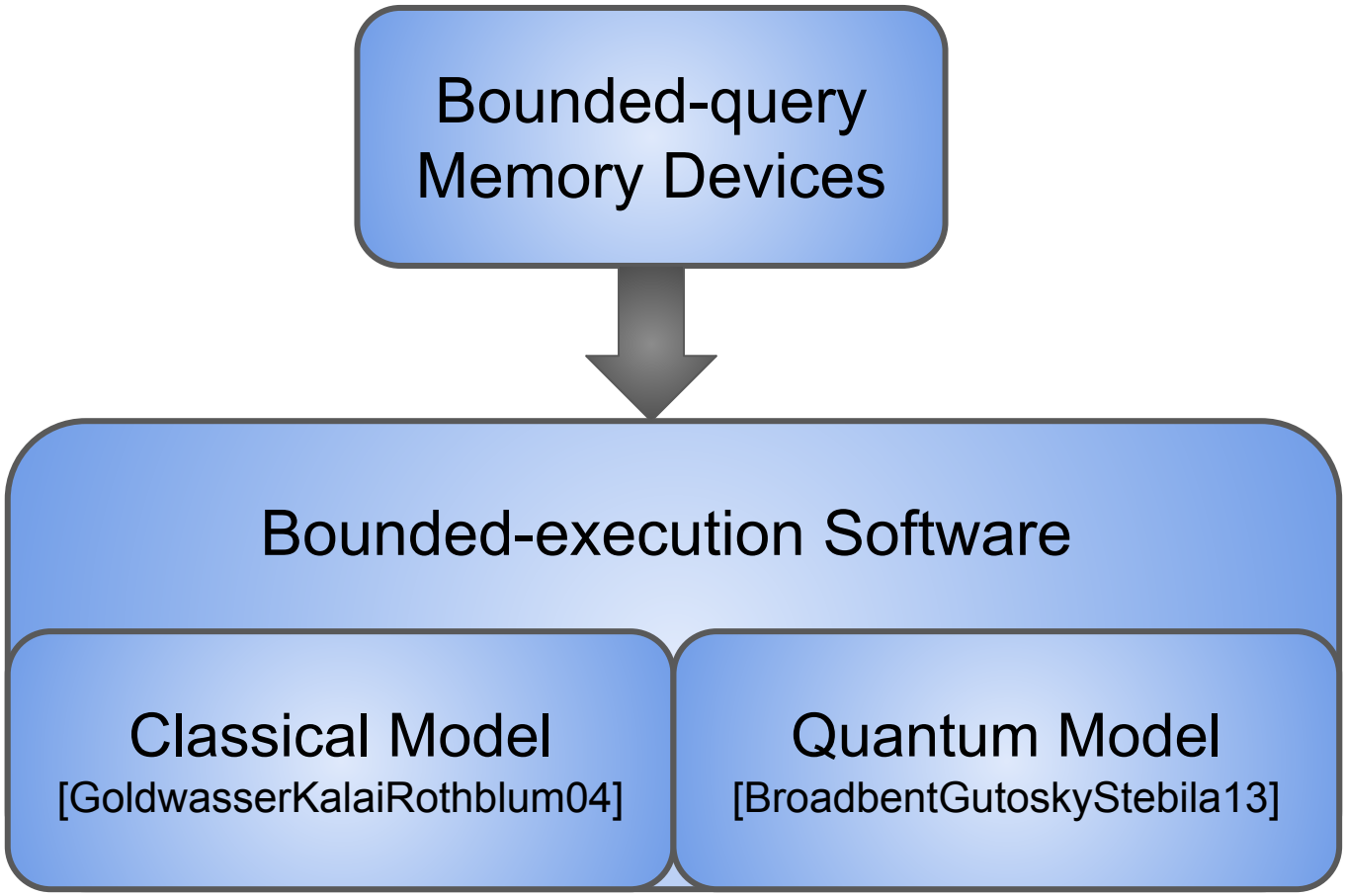
Unclonable





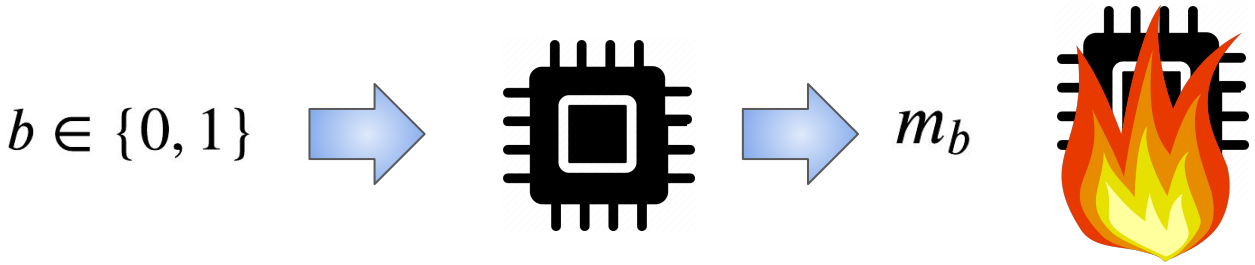
Self-destructive

Retrieve m, x


Bounded-query
Memory Devices
Bounded-execution Software
Classical Model
[GoldwasserKalaiRothblum04]
Quantum Model
[BroadbentGutoskyStebila13]

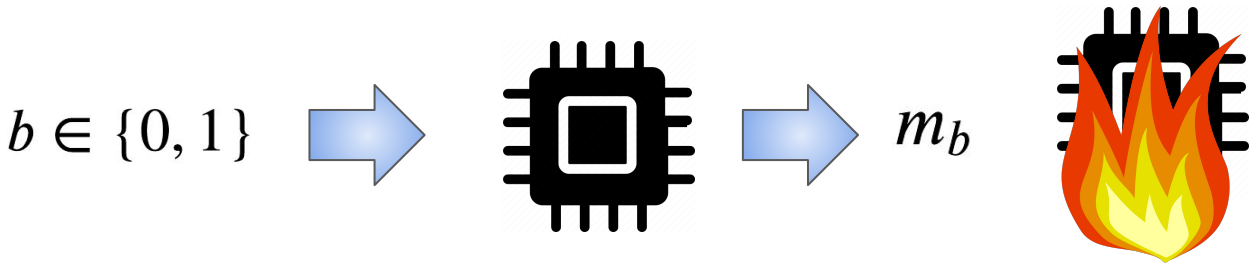
What we know:

Hypothetical, one-time memory devices [GKR04]

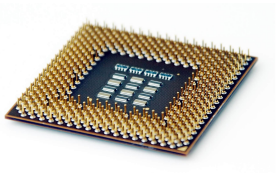


What we know:

Hypothetical, one-time memory devices [GKR04]



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

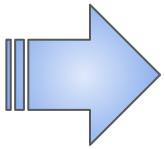
Amplification

Cryptographic applications

DNA-based Data Storage

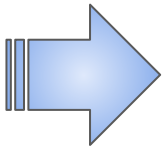
10011100 …

message *m*



GTCACAT …

Nucleotides



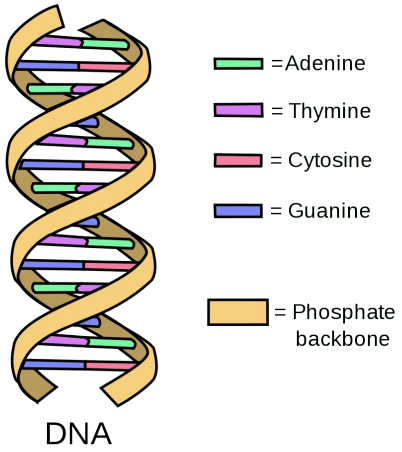


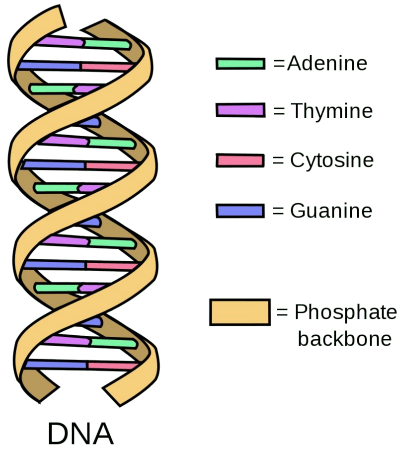
*Photo from https://www.ashg.org/discover-genetics/building-blocks/

DNA-based Data Storage

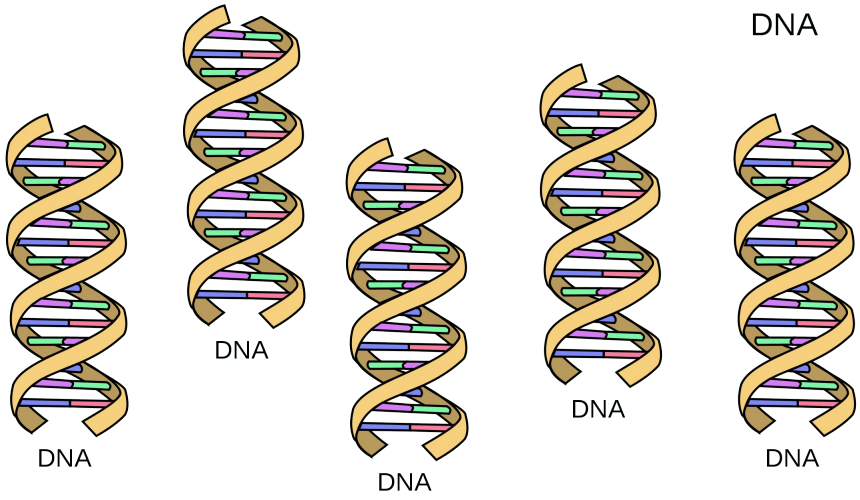
10011100 …
message *m*

GTCACAT …

Nucleotides

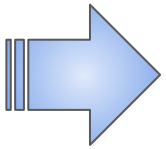


Cloneable!



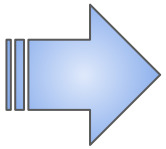
Proteins?

10011100 …
message *m*



SYRGAA …

Amino acids



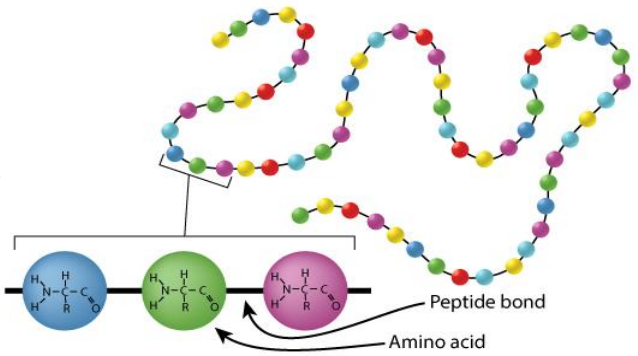
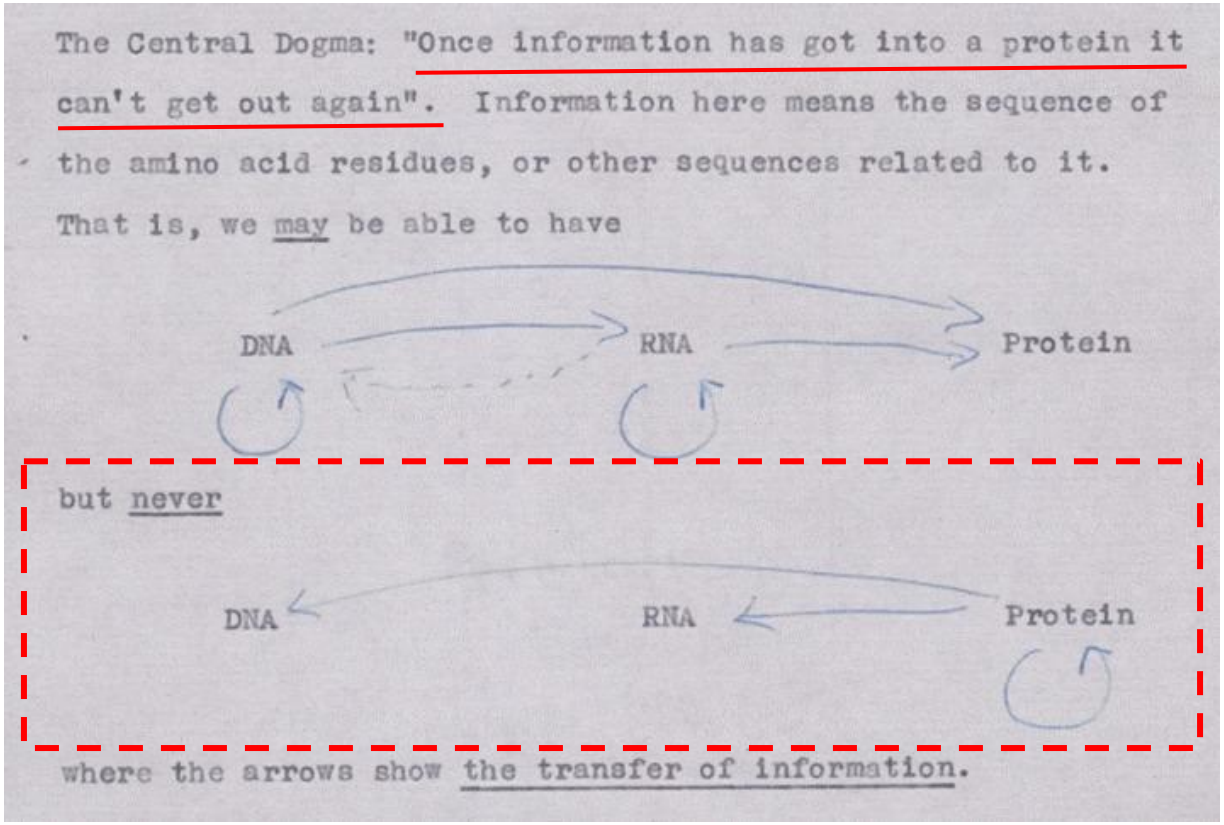


Image from: https://content.byui.edu/file/a236934c-3c60-4fe9-90aa-d343b3e3a640/1/module3/readings/proteins.html

Proteins are Unclonable

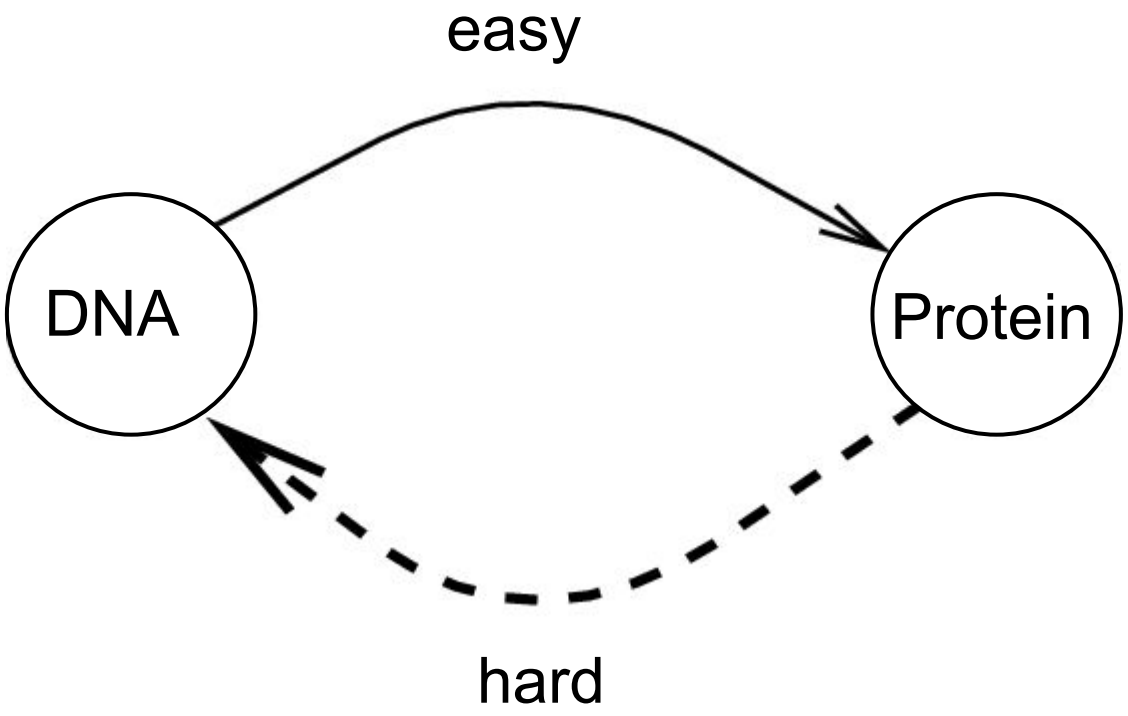
Central Dogma of Molecular Biology - Francis Crick, 1957:



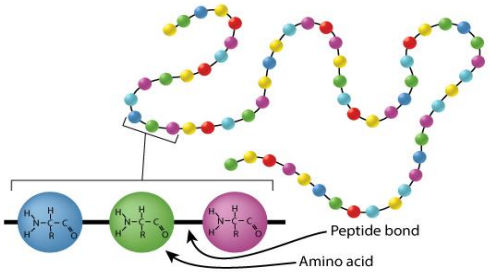
*https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.2003243

Proteins are Unclonable

A hypothesis (or a challenge) that is still standing for 65 years!



[Reading] Proteins is Destructive



Mass Spectrometry Instrument

SYRGAA …

Amino acids

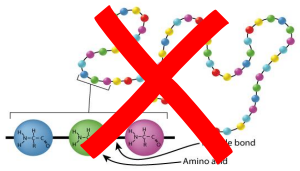
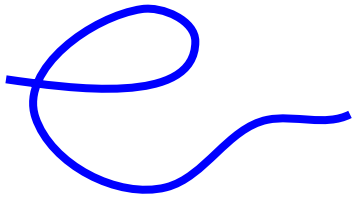


*Photo from https://www.creative-proteomics.com/support/mass-spectrometry-instruments.htm

Consumable Memory Tokens

A new protein-based construction for secure storage

Synthesize ***m***

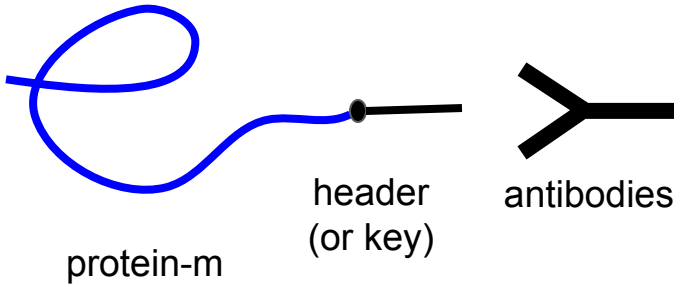


protein-m

Consumable Memory Tokens

A new protein-based construction for secure storage

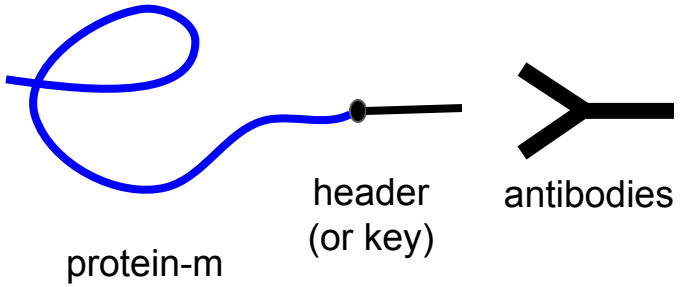
Synthesize ***m***



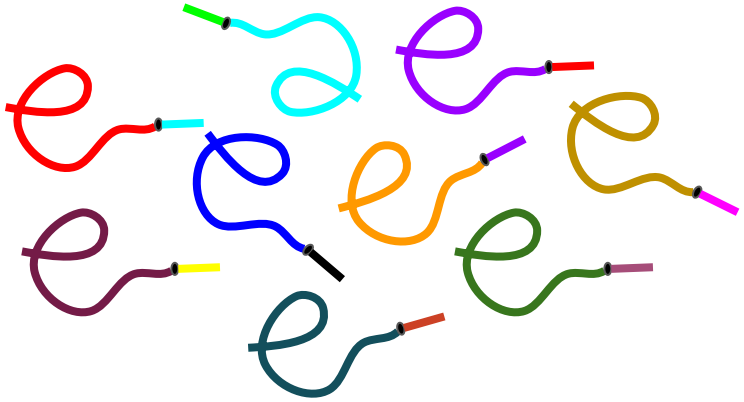
Consumable Memory Tokens

A new protein-based construction for secure storage

Synthesize ***m***



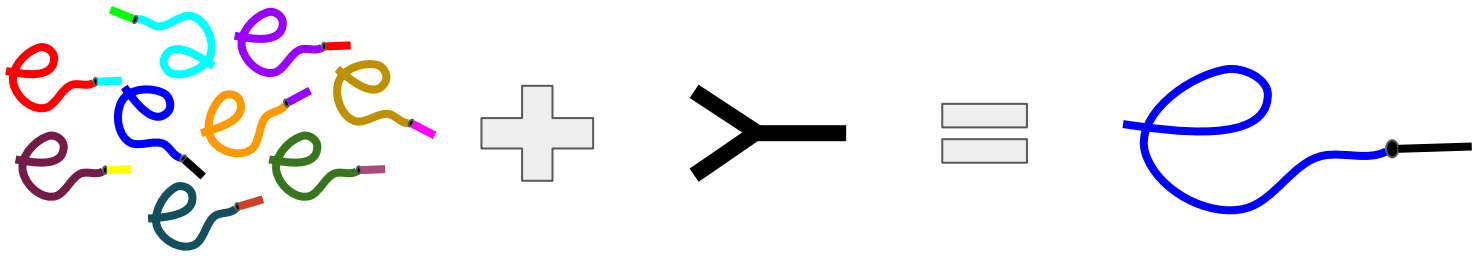
Mix with decoy proteins



Consumable Memory Tokens

A new protein-based construction for secure storage

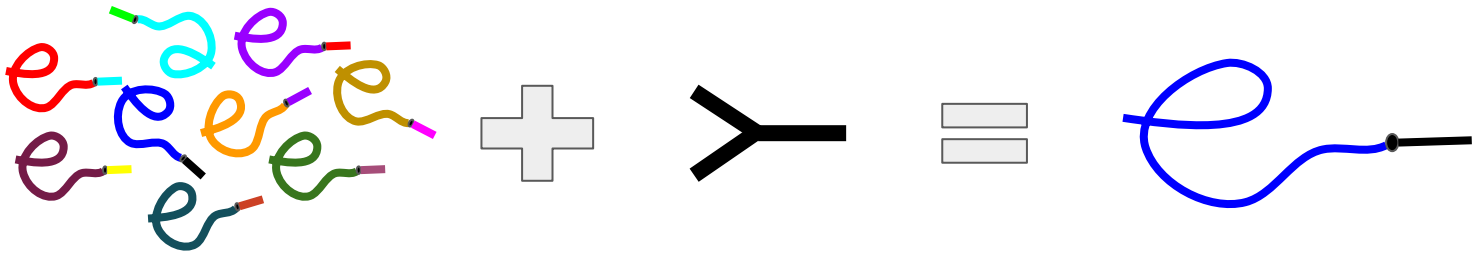
To retrieve ***m***, first purify



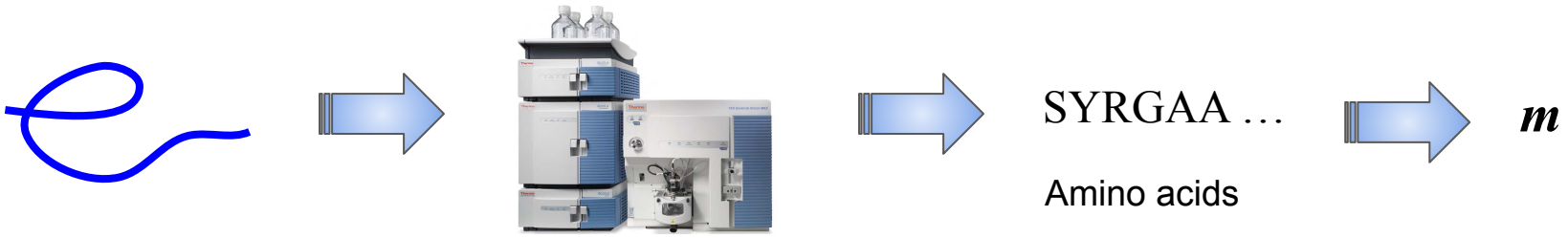
Consumable Memory Tokens

A new protein-based construction for secure storage

To retrieve ***m***, first purify

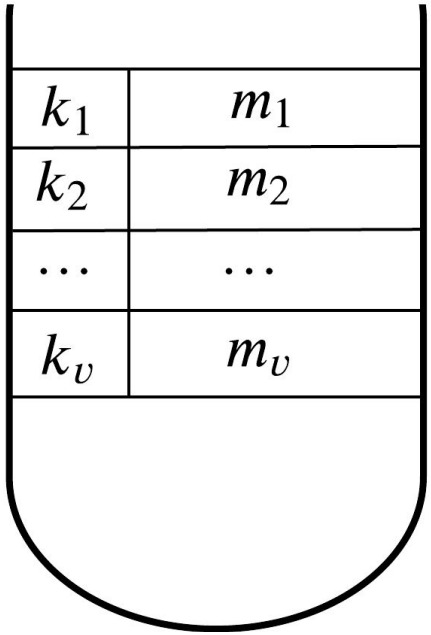


then read the sequence

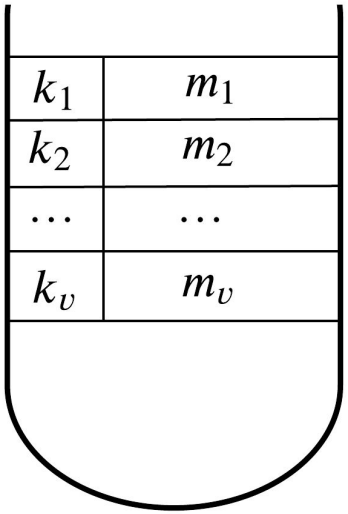


Extension: Partially Retrievable Memory

- Store v messages using v keys
- Only n out v messages can be retrieved



$(1, n, v)$-Consumable Tokens



One query

≤ n queries

$Encode(\mathbf{k}, \mathbf{m}, v)$

$Decode(k') = m_i \text{ if } k' = k_i \text{ else } \perp$

An adversary can try up to n key guesses ($n < v$),
The token self-destructs after that

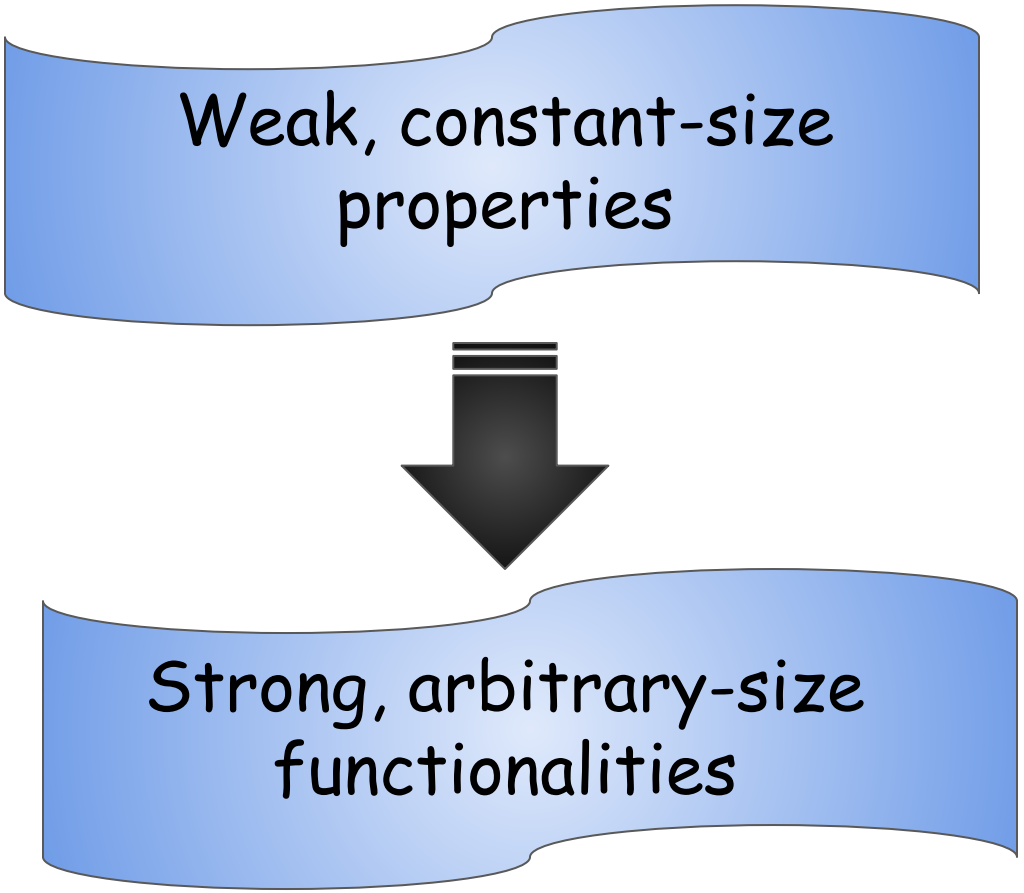
Model (Informal)

- 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

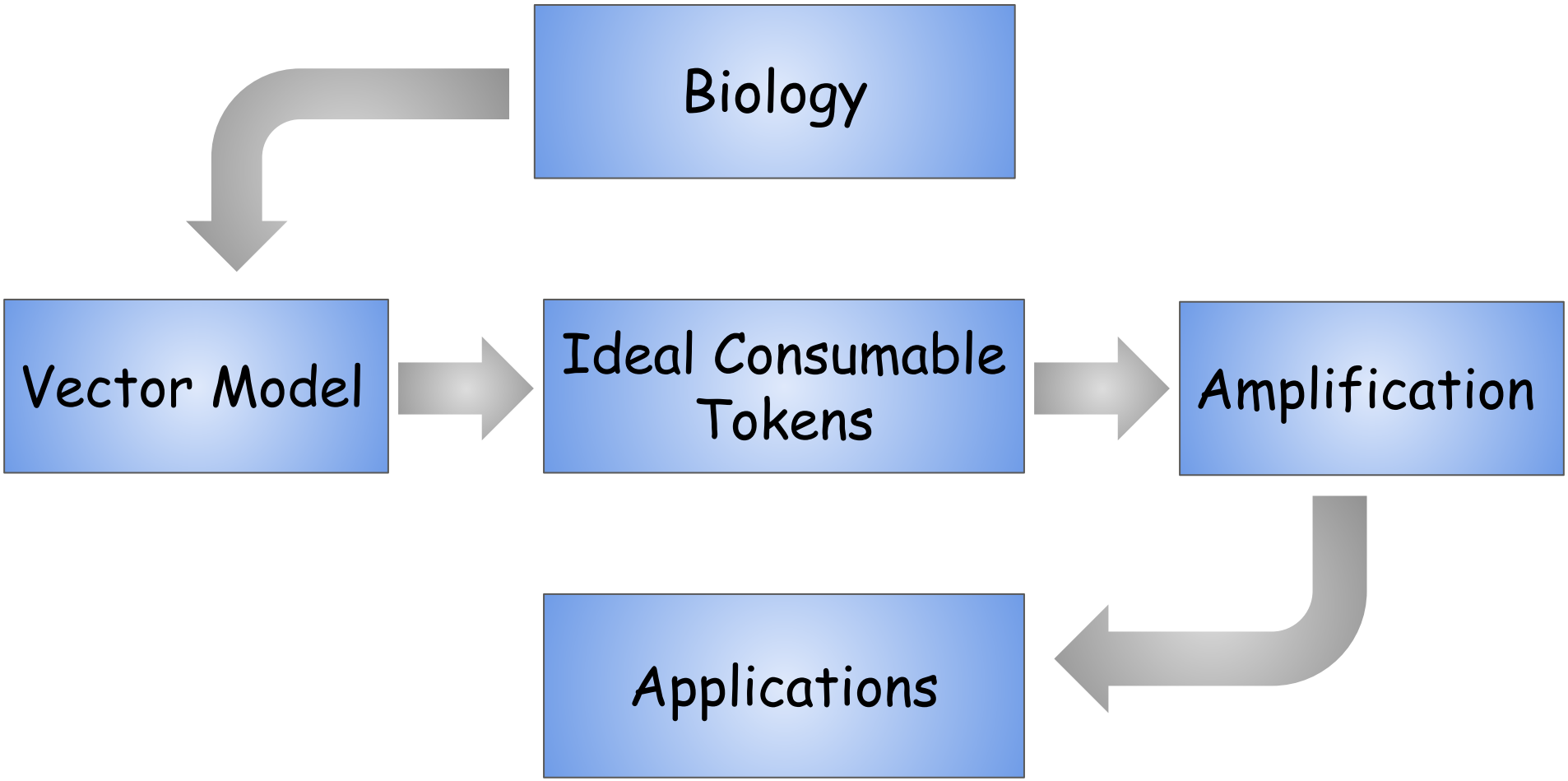
$$n \textit{ key guesses} \Rightarrow \textit{sample is destructed}$$

- Non-negligible soundness error γ

Challenge


Weak, constant-size properties
Strong, arbitrary-size functionalities

Our Work


Biology
Vector Model
Ideal Consumable Tokens
Amplification
Applications

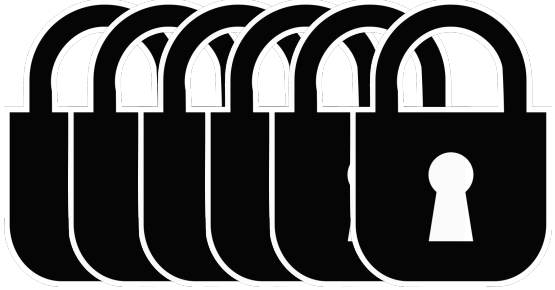
Applications of Consumable Tokens

Digital Lockers

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

$c = Enc_p(m)$

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



[CanettiDakdouk08] ⇒ Only brute search attacks are possible

Our work ⇒ Resistant to brute search attacks

In other words…
Bounded-query Point Function Obfuscation

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

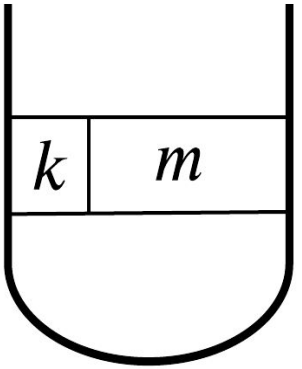
- $\mathcal{F}_{BPO}$ models obfuscation of this multi-output point function such that:

  Honest party: knows p, one query to obtain m
  Adversary: Can try up to n password guesses

Let's construct it from consumable tokens!

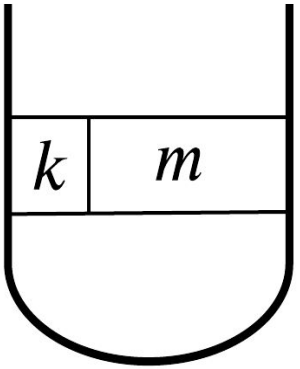
Is not this immediate?

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

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

No, it is not!

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

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

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

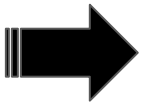
$$\Pr[\mathcal{A} \text{ retrieves } m] = \frac{n}{|\mathcal{P}|} + \gamma$$

BPO Construction–Attempt #2

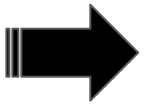
- Secret sharing of m

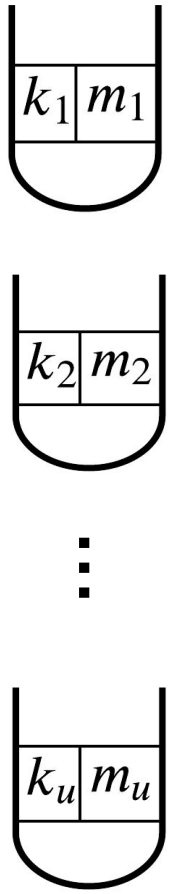
Share $m : m_1, m_2, \ldots, m_u$
such that $m = \oplus_{i=1}^{u} m_i$

$k_1 \leftarrow f_1(p)$
$k_2 \leftarrow f_2(p)$
$\ldots$
$k_u \leftarrow f_u(p)$



$Encode(k_1, m_1, 1)$
$Encode(k_2, m_2, 1)$
$\ldots$
$Encode(k_u, m_u, 1)$



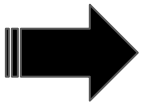


BPO Construction–Attempt #2

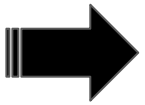
- Secret sharing of m

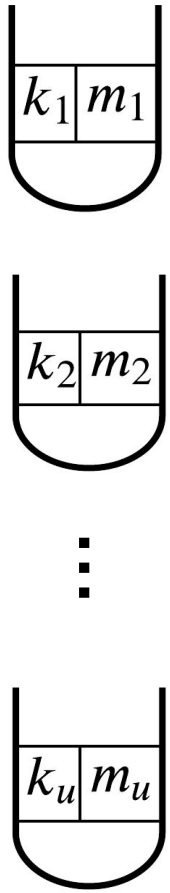
Share $m : m_1, m_2, \ldots, m_u$
such that $m = \oplus_{i=1}^{u} m_i$

$k_1 \leftarrow f_1(p)$
$k_2 \leftarrow f_2(p)$
$\ldots$
$k_u \leftarrow f_u(p)$



$Encode(k_1, m_1, 1)$
$Encode(k_2, m_2, 1)$
$\ldots$
$Encode(k_u, m_u, 1)$

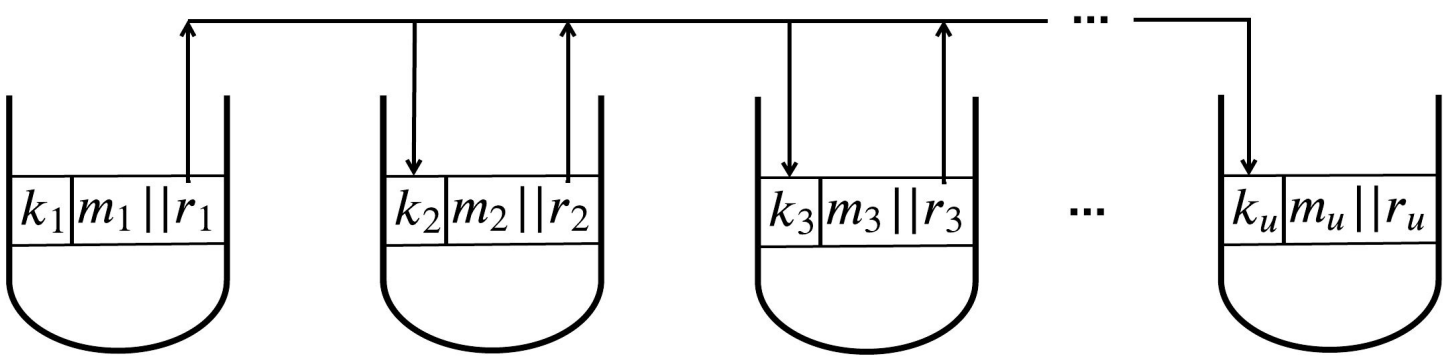




$$\Pr[\mathcal{A} \text{ retrieves } m] = \frac{un}{|\mathcal{P}|} + \left(1 - \frac{un}{|\mathcal{P}|}\right)\gamma^u$$

BPO Construction–Final Attempt

- Chaining of tokens



$k_1 \leftarrow f_1(p)$
$r_1 \leftarrow \{0,1\}^\kappa$

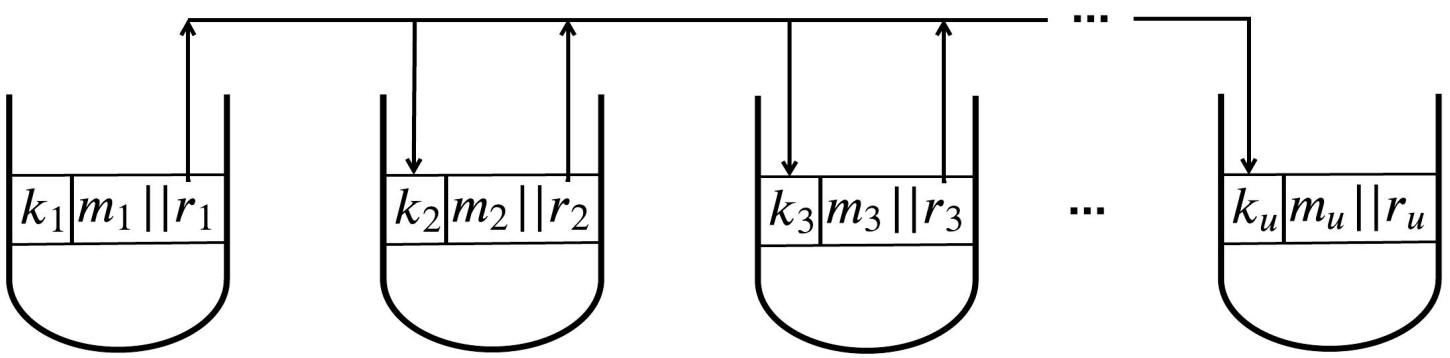
$r'_2 = r_1$
$k_2 \leftarrow f_2(p, r'_2)$
$r_2 \leftarrow \{0,1\}^\kappa$

$r'_3 = r_1 \oplus r_2$
$k_3 \leftarrow f_3(p, r'_3)$
$r_3 \leftarrow \{0,1\}^\kappa$

$r'_u = \oplus_{i=1}^{u-1} r_i$
$k_u \leftarrow f_u(p, r'_u)$
$r_u \leftarrow \{0,1\}^\kappa$

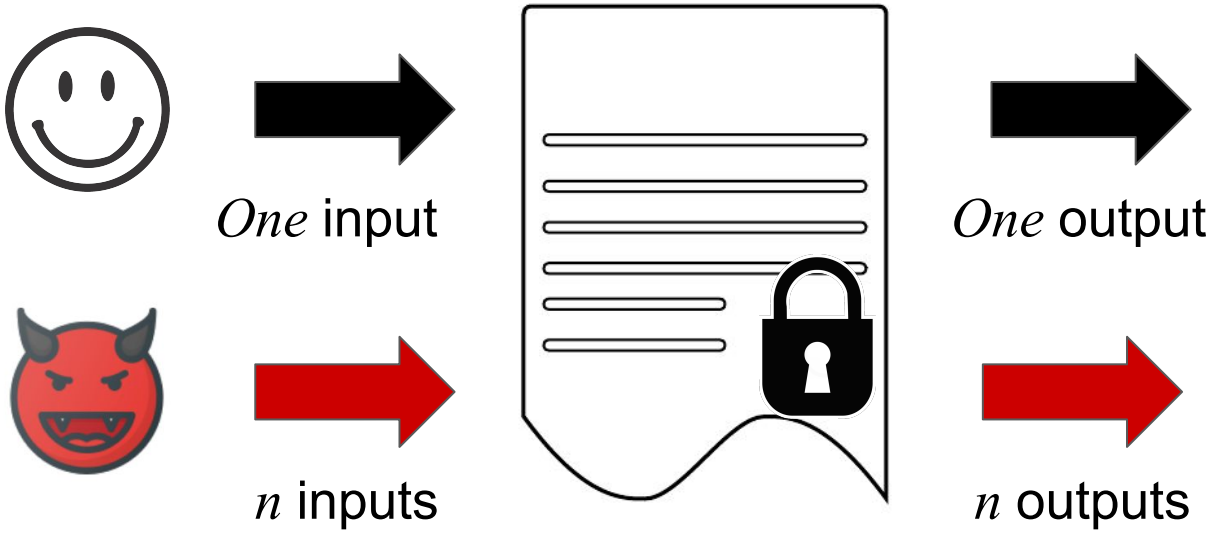
BPO Construction–Final Attempt

- 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



- (1,1)-time programs = [GKR]'s one-time programs
- (k,k)-time programs = [GKR]'s k-time programs

Let's construct (1,n)-time programs from consumable tokens!

$(1, n)$-time Programs Construction

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

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

$(1, n)$-time Programs Construction

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

Step 1: Create a consumable token

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

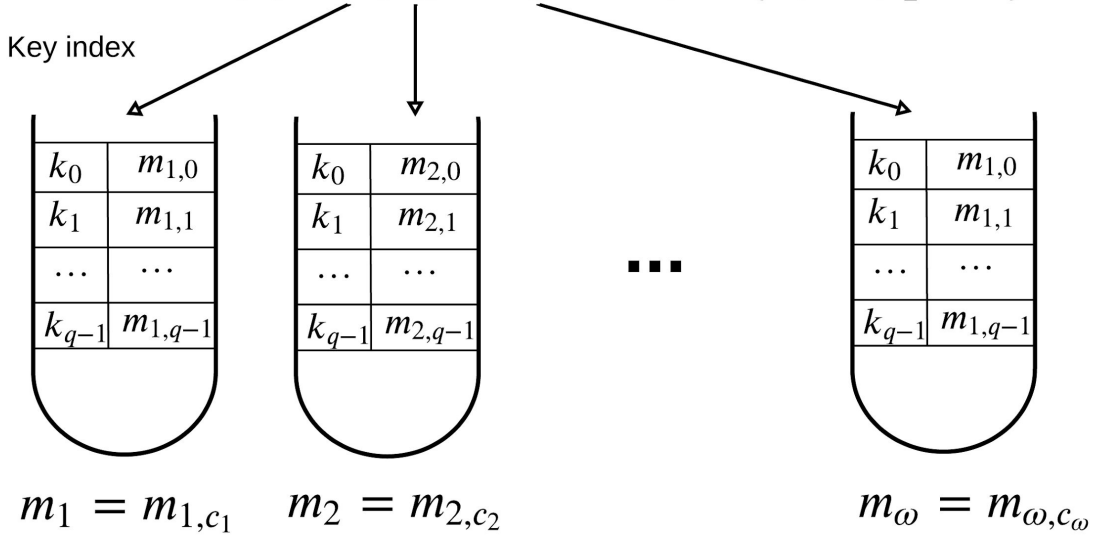
Step 2: Obfuscate a program for f

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

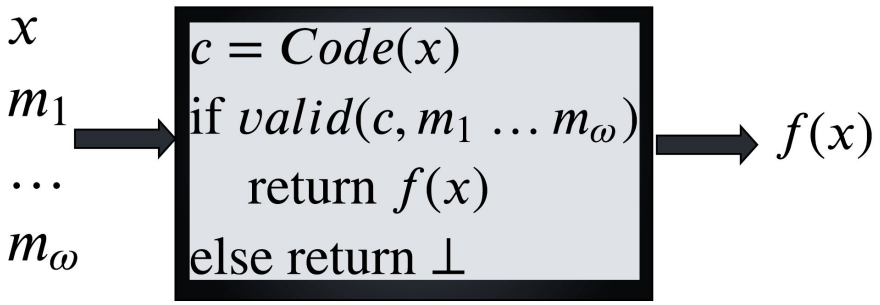
f with large domain?

$(1, n)$-time Programs Construction

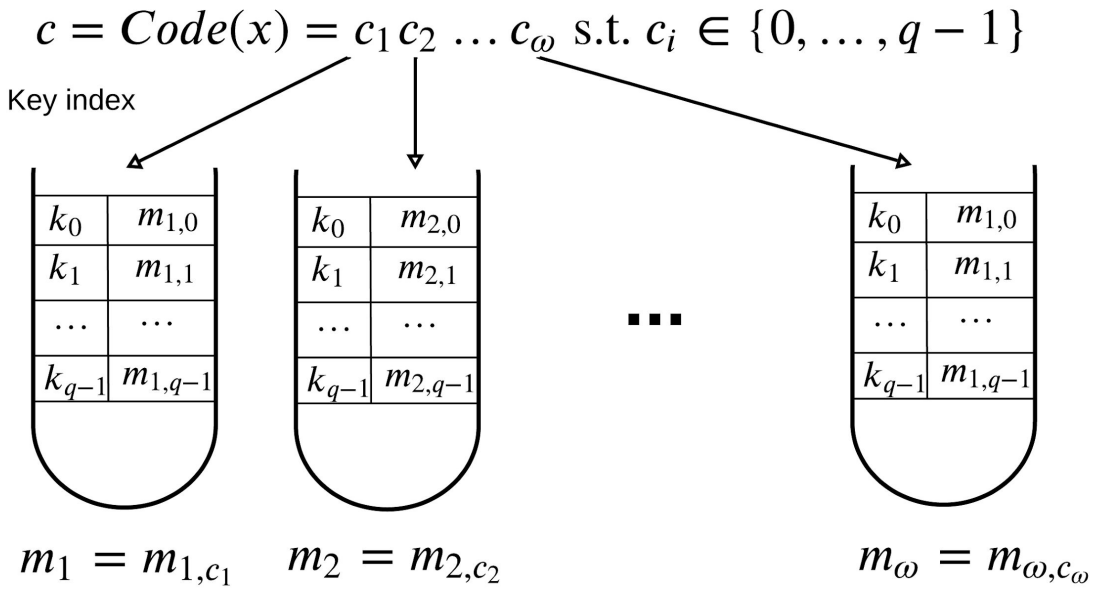
$c = Code(x) = c_1 c_2 \ldots c_\omega$ s.t. $c_i \in \{0, \ldots, q-1\}$



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



$(1, n)$-time Programs Construction



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

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

Conclusion and Future Work

- **This work**
  - An innovative, real-world construction of unclonable and self-destructive memory devices
  - Formal treatment and provably-secure cryptographic applications

- **Future work**
  - *Biology:* full biological construction and empirical results
  - *Cryptography:* refine our model and more applications

Thank you!

Questions?