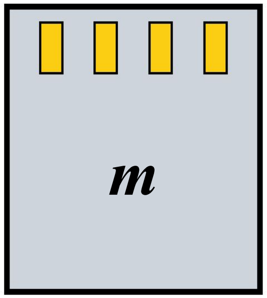
Unclonable Polymers and Their Cryptographic Applications

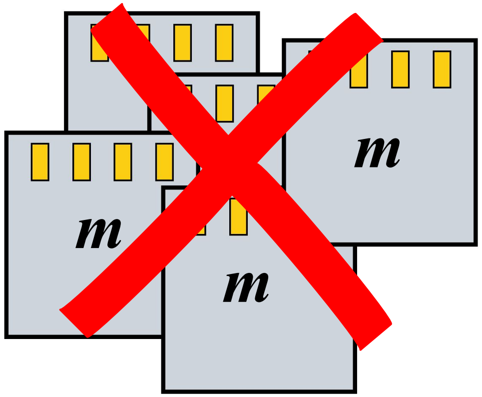
Ghada Almashaqbeh[1], Ran Canetti[2], Yaniv Erlich[3], Jonathan Gershoni[4], Tal Malkin[5], Itsik Pe'er[5], Anna Roitburd-Berman[4], and Eran Tromer[4,5]

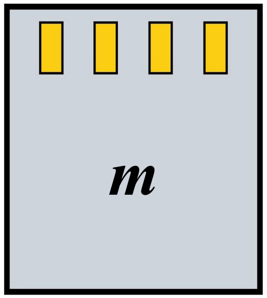
[1]University of Connecticut, [2]Boston University, [3]Eleven Therapeutics and IDC Herzliya, [4]Tel Aviv University, and [5]Columbia University

Eurocrypt 2022

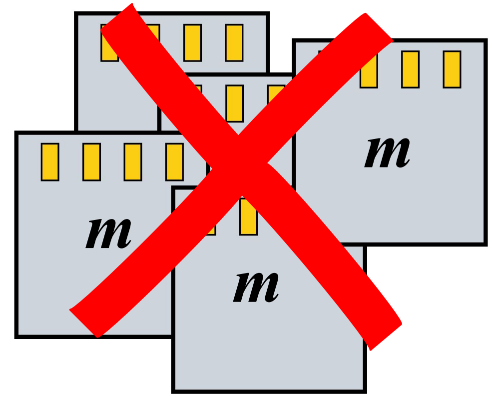


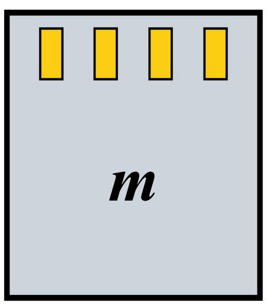
Unclonable





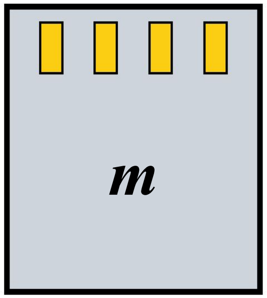
Unclonable



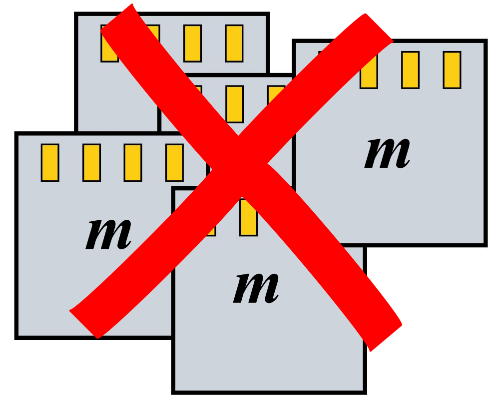


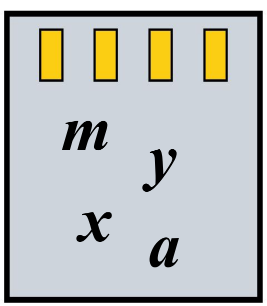
Retrieve m

Self-destructive



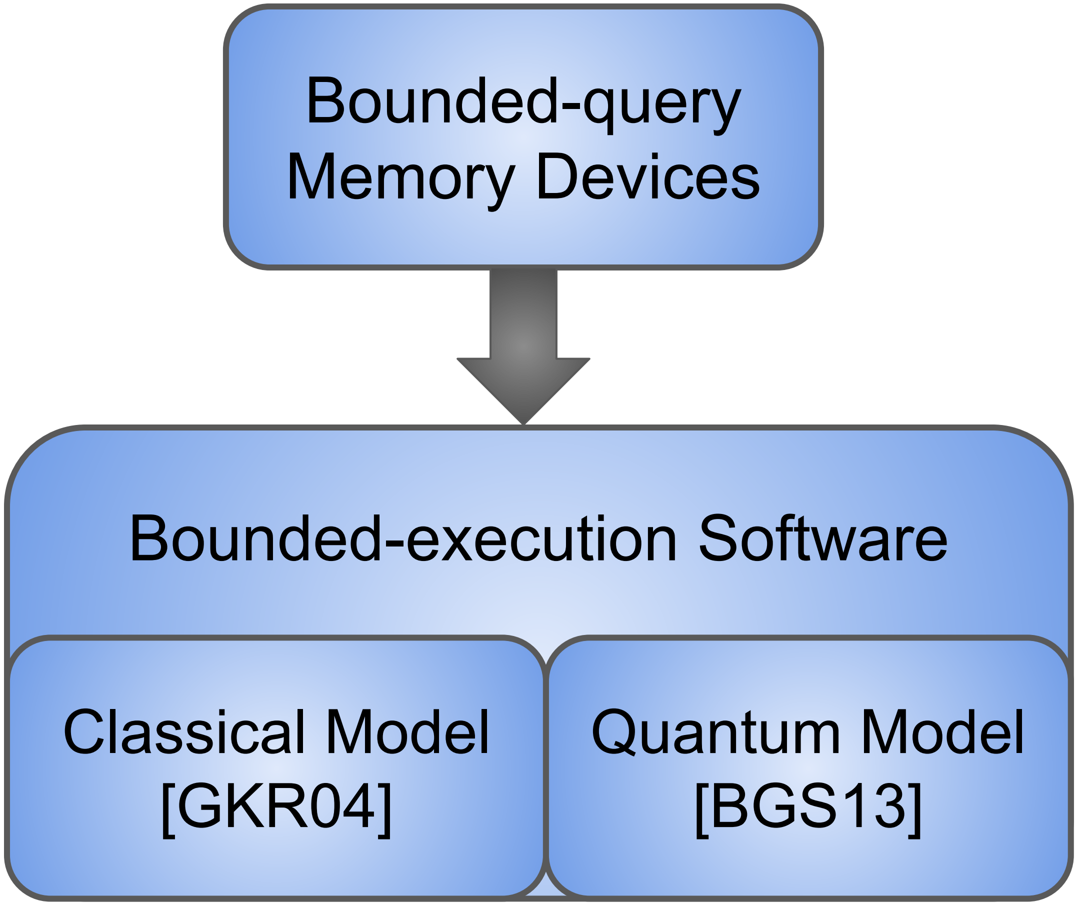
Unclonable





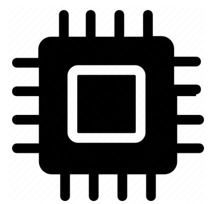
Retrieve m, x

Self-destructive


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

What we know:

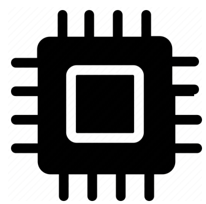
Hypothetical, one-time memory devices [GKR04]

$b \in \{0, 1\}$ ⇨  ⇨ m_b 

What we know:

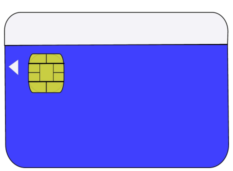
Hypothetical, one-time memory devices [GKR04]

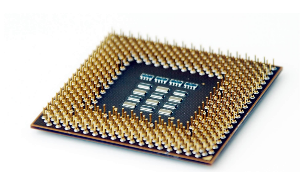
$b \in \{0, 1\}$



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

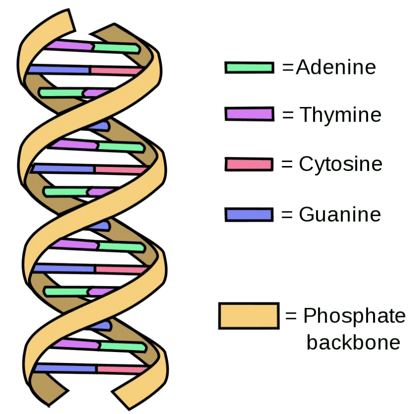
DNA-based Data Storage (Not Us)

10011100 …

message *m*

GTCACAT …

Nucleotides



DNA

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

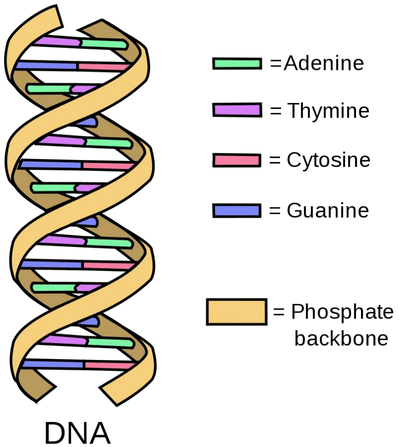
DNA-based Data Storage (Not Us)

10011100 …

message *m*

GTCACAT …

Nucleotides



Cloneable!

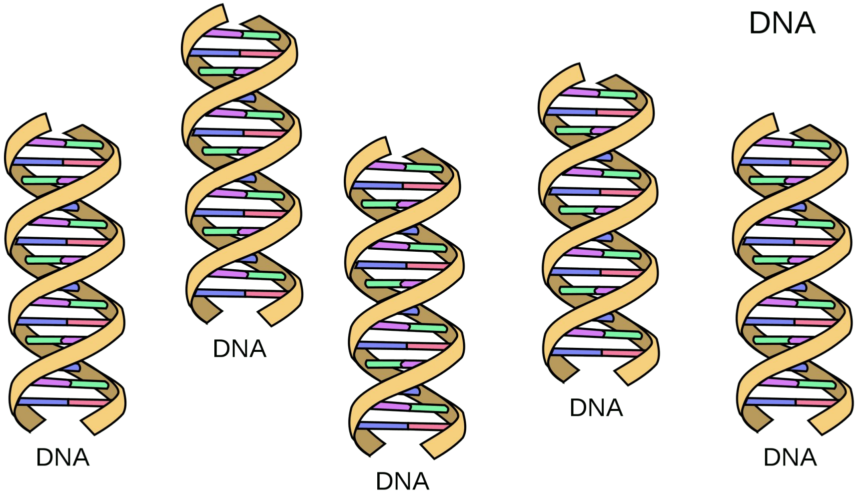


*Photo from https://www.ashg.org/discover-genetics/building-blocks/

Proteins (Us)

10011100 …

message *m*

SYRGAA …

Amino acids

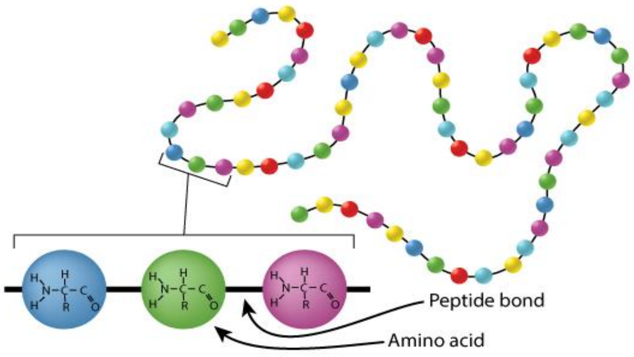
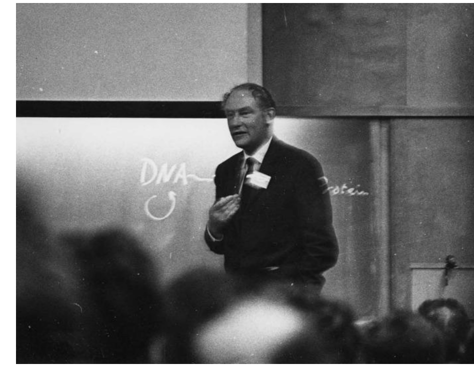
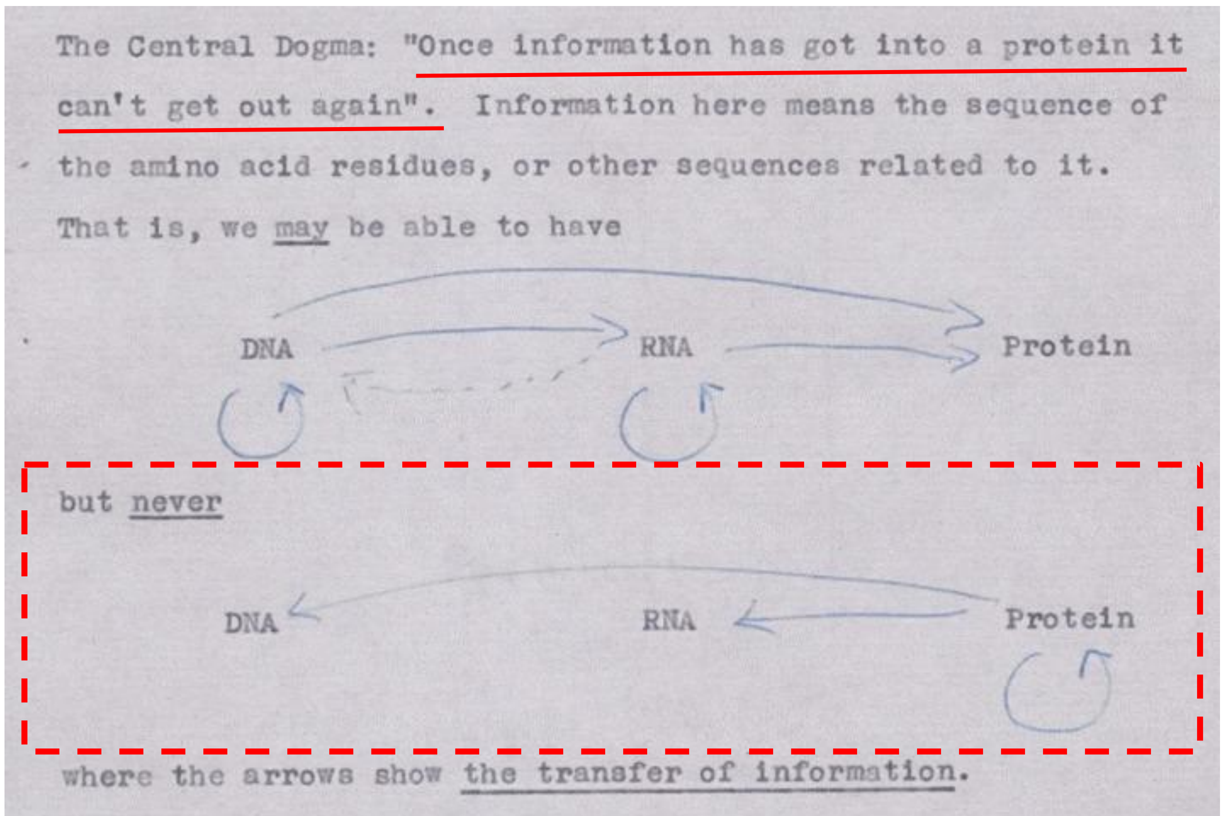


Image from: https://content.byui.edu/file/a236934c-3c60-4fe9-90aa-d343b3e3a640/1/module3/readings/proteins.html

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

DNA RNA Protein

but never

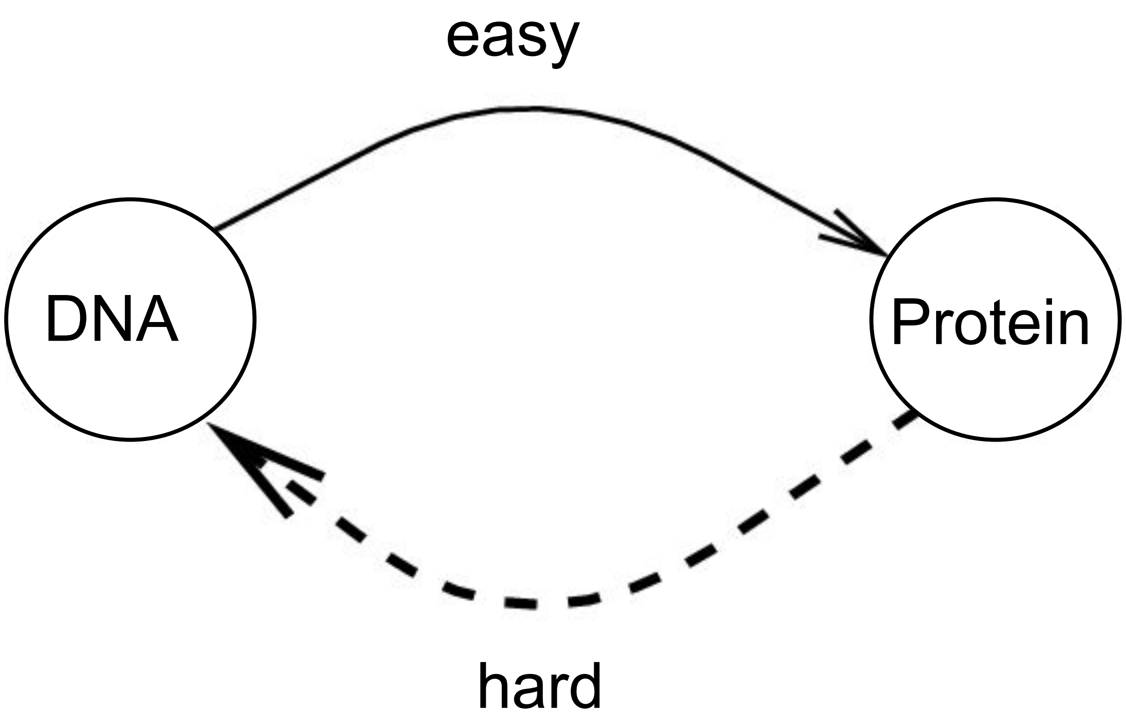
DNA RNA Protein

where the arrows show the transfer of information.

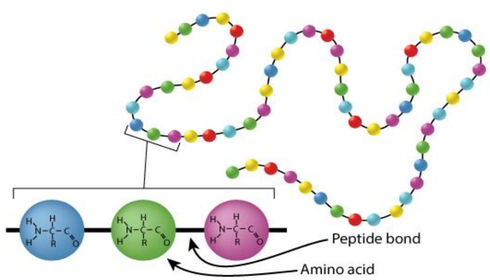
*images from https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.2003243

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



10011100 …

message *m*

Mass Spectrometry Instrument

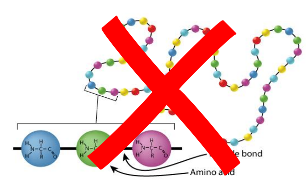
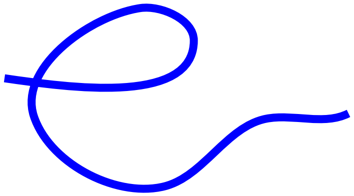


*Photo from https://www.creative-proteomics.com/support/mass-spectrometry-instruments.htm

Consumable Memory Tokens

A new protein-based construction for secure storage

Synthesize m

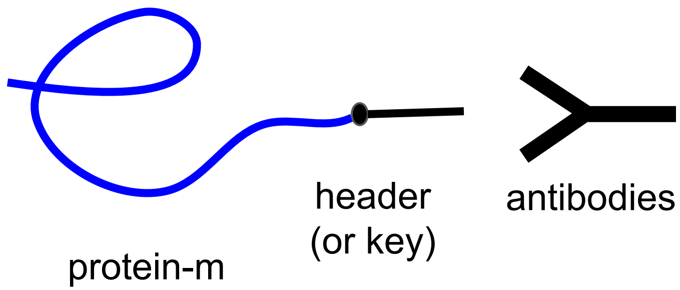


protein-m

Consumable Memory Tokens

A new protein-based construction for secure storage

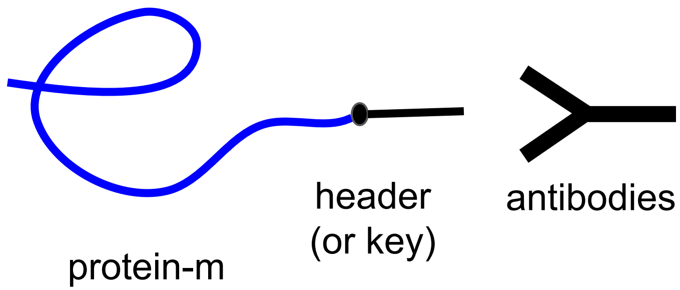
Synthesize m



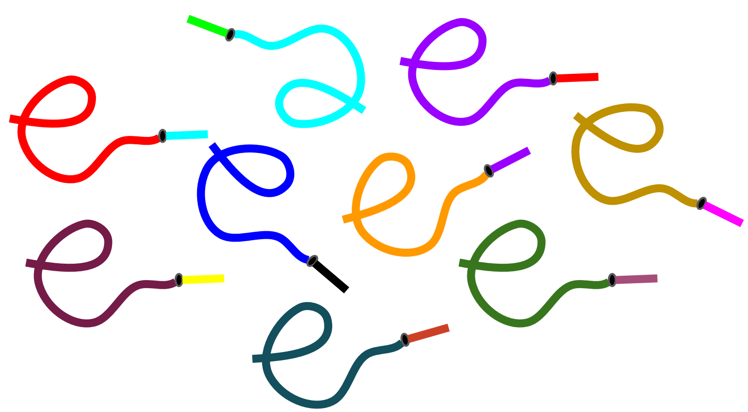
Consumable Memory Tokens

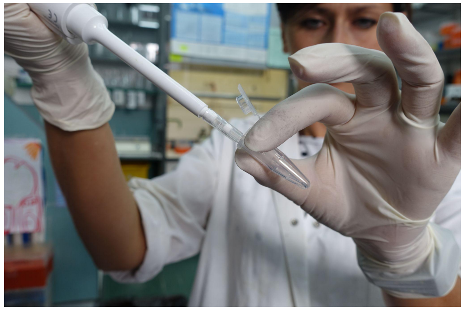
A new protein-based construction for secure storage

Synthesize m



Mix with decoy proteins

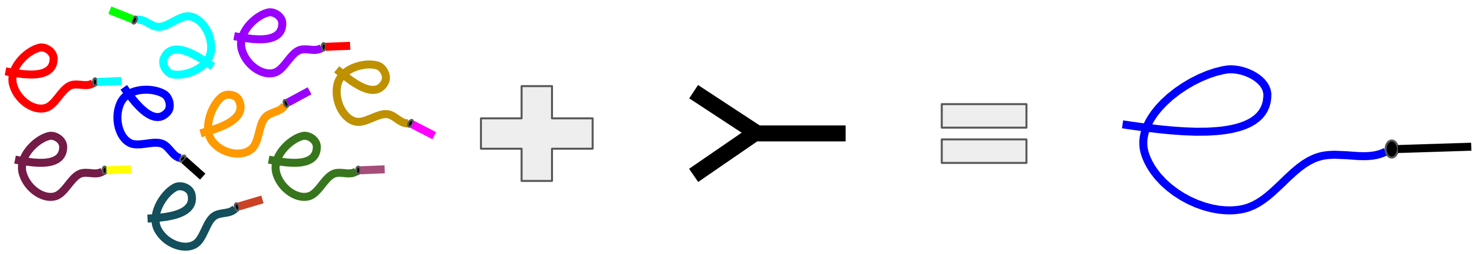




Consumable Memory Tokens

A new protein-based construction for secure storage

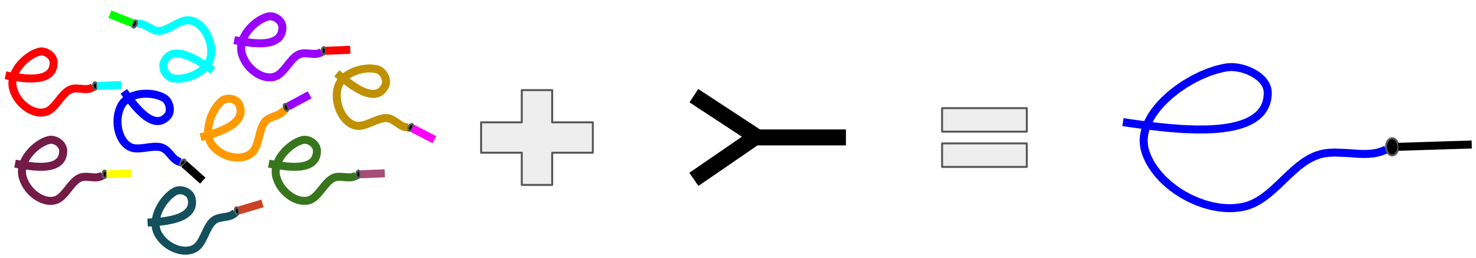
To retrieve m, first purify



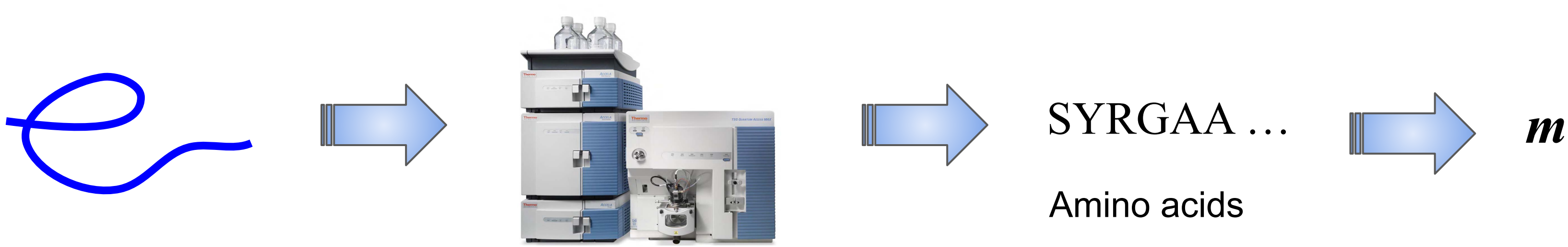
Consumable Memory Tokens

A new protein-based construction for secure storage

To retrieve m, first purify



then read the sequence



Model (Informal)

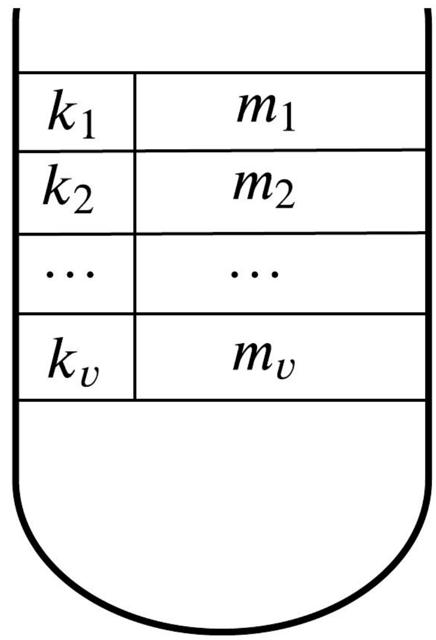
- Can store only a small number of short messages using short keys
- The only meaningful interaction is by applying antibodies (keys)
- Each retrieval attempt consumes part of the vial
- Account for powerful adversaries

n *key guesses ⇒ sample is destructed*

- Non-negligible soundness error γ

Extension: Partially Retrievable Memory

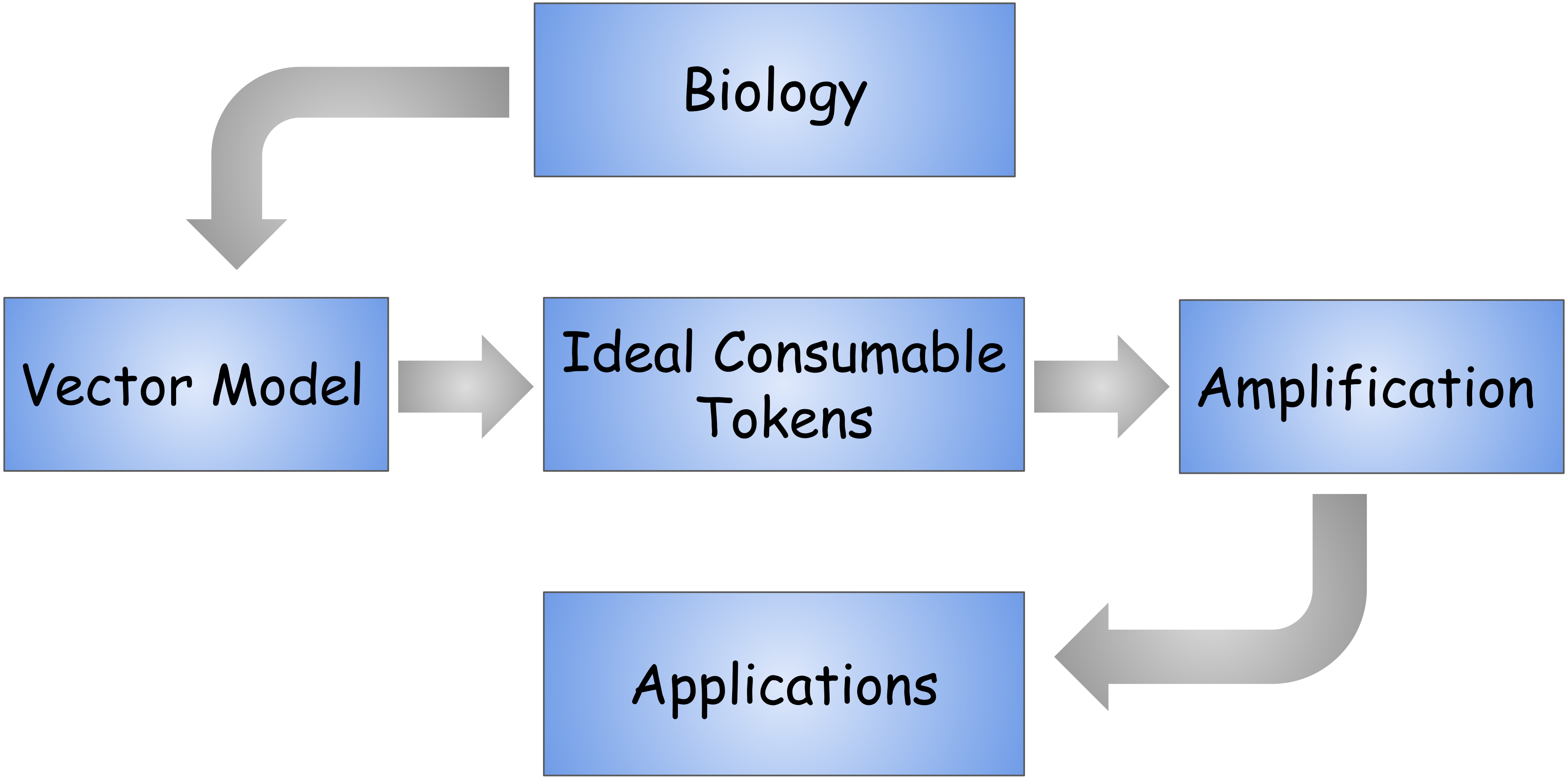
- Store $\boldsymbol{v}$ messages using $\boldsymbol{v}$ keys
- Only $\boldsymbol{n}$ out $\boldsymbol{v}$ messages can be retrieved ($\boldsymbol{n} < \boldsymbol{v}$)



Weak, constant-size properties

Strong, arbitrary-size functionalities

Modeling and Applications



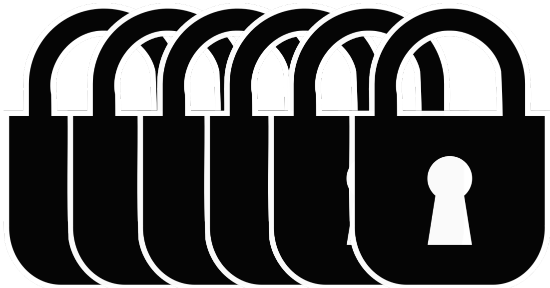
Applications of Consumable Tokens

Digital Lockers

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

$c = Enc_p(m)$

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



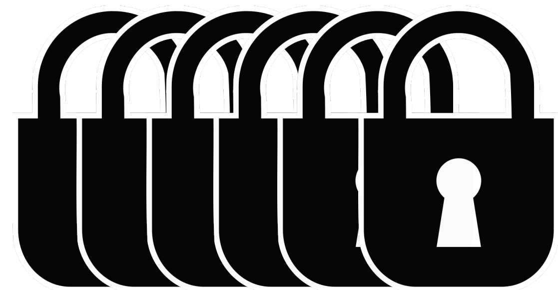
Resistant to brute search attacks

Digital Lockers

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

$c = Enc_p(m)$

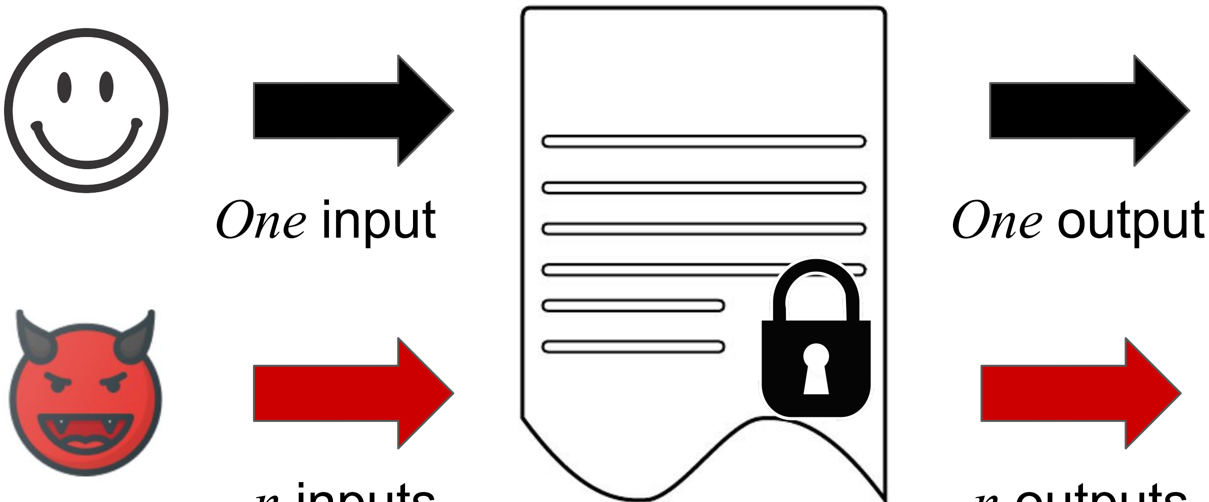
$i \in \{1, \dots, n\} : p_i \in \mathcal{P}, Dec_{p_i}(c)$



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

$(1, n)$-time Programs



$(1, n)$-time Programs Construction

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

Step 1: Create a consumable token

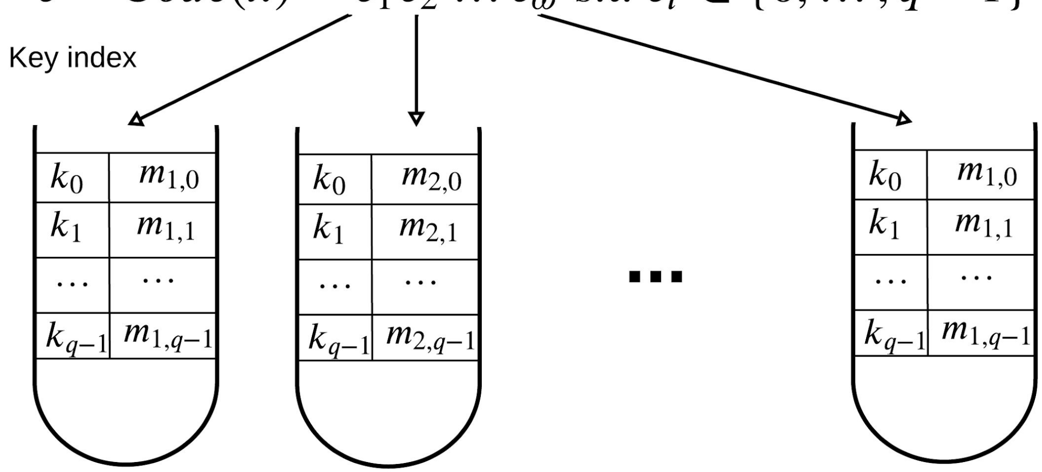
For each $x \in \mathcal{X}$ store a unique secret message m in the token

Step 2: Obfuscate a program for f

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

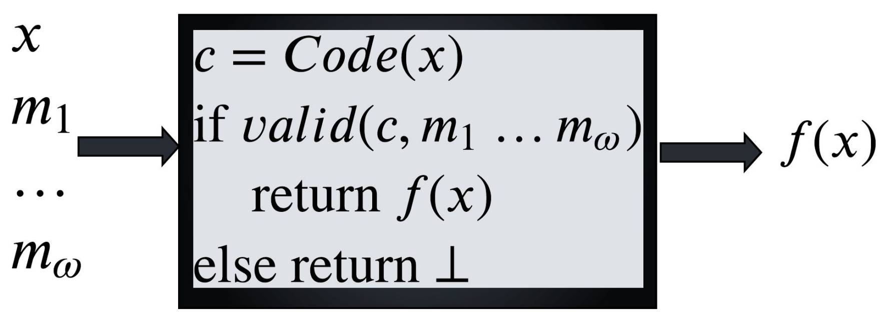
$(1, n)$-time Programs Construction

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



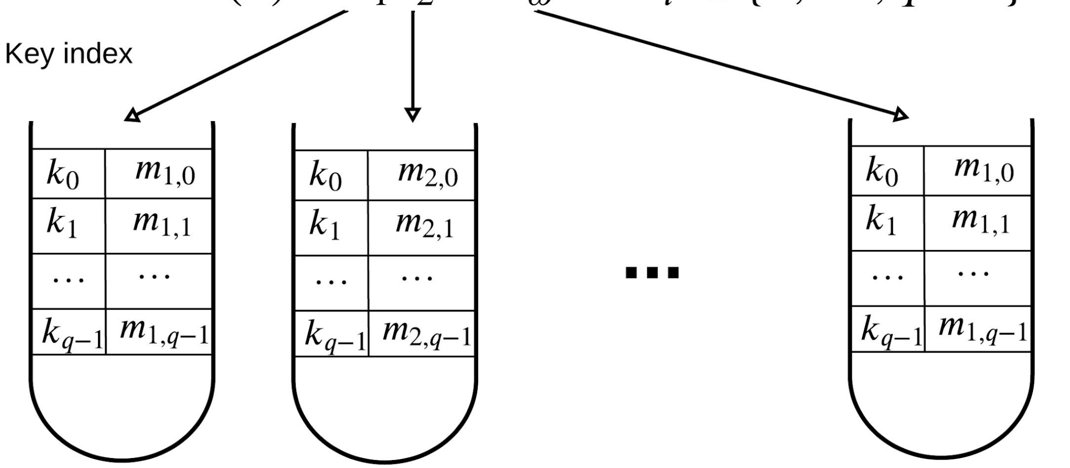
$|\mathcal{X}| = q^{d+1}$

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



$(1, n)$-time Programs Construction

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



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

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

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?