CASA
Cyber Security in the Age of Large-Scale Adversaries

Decomposing Linear Layers

FSE 2023, (Kobe)

Christof Beierle, Patrick Felke, Gregor Leander, Sondre Ronjøm

Ruhr Universität Bochum RUB
University of Applied Sciences Hochschule Emden·Leer
NSM
Horst Görtz Institut

Ideal vs Real World

CASA
Cyber Security in the Age of Large-Scale Adversaries

Open Design

- public specification
- public design rational
- public security results

Closed design

- no public specification
- no public design rational
- no public security results

Examples for closed designs: GEA-1, SIMON/SPECK, STREEBOG

Ideal vs Real World

CASA
Cyber Security in the Age of Large-Scale Adversaries

Open Design

- public specification
- public design rational
- public security results

Closed design

- no public specification
- no public design rational
- no public security results

Examples for closed designs: GEA-1, SIMON/SPECK, STREEBOG

Ideal vs Real World

CASA
Cyber Security in the Age of Large-Scale Adversaries

Open Design	Closed design
▶ public specification	▶ no public specification
▶ public design rational	▶ no public design rational
▶ public security results	▶ no public security results

Examples for closed designs: GEA-1, SIMON/SPECK, STREEBOG

Example: Streebog [Russian standard]

- Russian hash function standard GOST R 34.11-2012
- SPN operating on a 64-byte state with
  - 8-bit permutation π (only given as a lookup-table)
  - permutation of bytes
  - 64×64 matrix with entries in $\mathbb{F}_2$, applied 8 times in parallel
- No design rationale or explanation how those were chosen

Reverse-engineering of building blocks

Research problem

Recover structure and/or design rationale

For S-boxes (well studied):

- very nice results for S-box π of Streebog [Perrin, ToSC 2019]

For linear layer: not well studied.

Our contribution

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Focus on the linear layer

Given a linear layer by a binary matrix, recover structure induced by constructions over extension fields.

- Problem 1: Given $M \in \mathrm{Mat}(\mathbb{F}_2, ms \times ms)$, decide whether $M \in \mathrm{Mat}(\mathbb{F}_{2^s}, m \times m)$
- Problem 2: Obfuscated case of Problem 1
- Problem 3: Decide whether M follows a well-known construction for MDS.

Our contribution

CASA
Cyber Security in the Age of Large-Scale Adversaries

Focus on the linear layer

Given a linear layer by a binary matrix, recover structure induced by constructions over extension fields.

- Problem 1: Given $M \in \mathrm{Mat}(\mathbb{F}_2, ms \times ms)$, decide whether $M \in \mathrm{Mat}(\mathbb{F}_{2^s}, m \times m)$
- Problem 2: Obfuscated case of Problem 1
- Problem 3: Decide whether M follows a well-known construction for MDS.

1. Field Structure

2. Obfuscation and More Structure

Example: A matrix $M \in \mathrm{Mat}(\mathbb{F}_2, 12 \times 12)$

CASA
Cyber Security in the Age of Large-Scale Adversaries

$$
\begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
$$

Example: A matrix $M \in \mathrm{Mat}(\mathbb{F}_2, 12 \times 12)$

Consider $s = 4$:

$$\left[\begin{array}{cccc|cccc|cccc}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
\hline
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
\hline
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right]$$

Example: A matrix $M \in \mathrm{Mat}(\mathbb{F}_2, 12 \times 12)$

CASA
Cyber Security in the Age of Large-Scale Adversaries

Consider $s = 4$:

$$\left[\begin{array}{cccc|cccc|cccc}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
\hline
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
\hline
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right] \stackrel{?}{=} \begin{bmatrix} M_{1,1} & M_{1,2} & M_{1,3} \\ M_{2,1} & M_{2,2} & M_{2,3} \\ M_{3,1} & M_{3,2} & M_{3,3} \end{bmatrix}$$

$M_{i,j} = \gamma^{N(i,j)}$ for $\gamma \in \mathbb{F}_{2^4}^*$

Usual field representation

$$
\left[\begin{array}{cccc|cccc|cccc}
1&1&0&1&0&0&1&0&0&0&1&1\\
0&1&0&1&1&0&0&1&1&0&1&0\\
0&0&0&1&0&1&1&1&1&1&0&1\\
1&1&1&0&1&0&1&0&0&1&1&0\\
\hline
1&0&1&1&0&0&1&0&0&1&1&1\\
1&1&1&0&1&0&0&1&1&0&0&0\\
1&1&1&1&0&1&1&1&0&1&0&0\\
0&1&1&1&1&0&1&0&0&1&0&1\\
\hline
1&0&1&1&0&1&0&0&0&1&0&1\\
1&1&1&0&0&0&1&0&0&0&0&1\\
1&1&1&1&1&0&0&1&0&0&1&1\\
0&1&1&1&0&0&1&1&1&1&1&1
\end{array}\right]
\stackrel{?}{=}
\begin{bmatrix}
\gamma^{N(1,1)} & \gamma^{N(1,2)} & \gamma^{N(1,3)}\\
\gamma^{N(2,1)} & \gamma^{N(2,2)} & \gamma^{N(2,3)}\\
\gamma^{N(3,1)} & \gamma^{N(3,2)} & \gamma^{N(3,3)}
\end{bmatrix}
$$

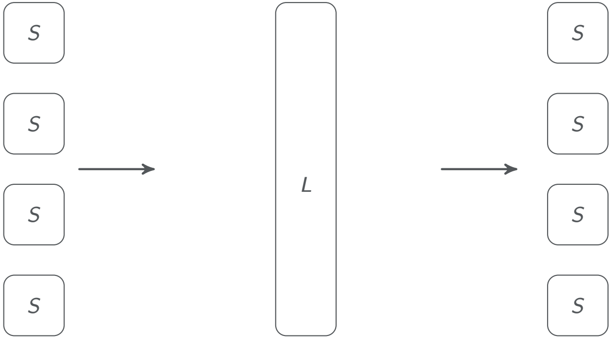
- Usually, $\mathbb{F}_{2^s} \sim \mathbb{F}_2[X]/(f)$, where f is an irred. polynomial in $\mathbb{F}_2[X]$ of deg. s
- More general: $\mathbb{F}_{2^s}$ as a subring of $\mathrm{Mat}(\mathbb{F}_2, s \times s)$ (e.g., [Lidl, Niederreiter,'94])

Usual field representation

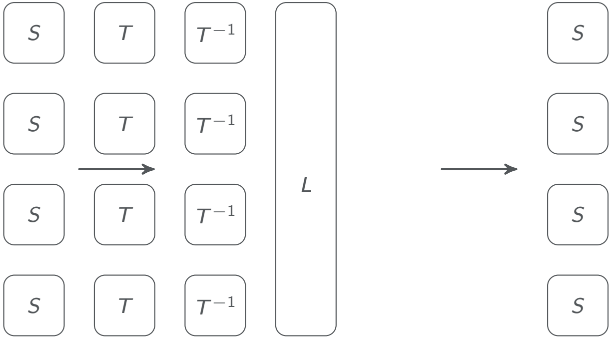
$$
\left[\begin{array}{cccc|cccc|cccc}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
\hline
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
\hline
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right]
\stackrel{?}{=}
\begin{bmatrix}
\gamma^{N(1,1)} & \gamma^{N(1,2)} & \gamma^{N(1,3)} \\
\gamma^{N(2,1)} & \gamma^{N(2,2)} & \gamma^{N(2,3)} \\
\gamma^{N(3,1)} & \gamma^{N(3,2)} & \gamma^{N(3,3)}
\end{bmatrix}
$$

- Usually, $\mathbb{F}_{2^s} \sim \mathbb{F}_2[X]/(f)$, where f is an irred. polynomial in $\mathbb{F}_2[X]$ of deg. s
- More general: $\mathbb{F}_{2^s}$ as a subring of $\mathrm{Mat}(\mathbb{F}_2, s \times s)$ (e.g., [Lidl, Niederreiter,'94])

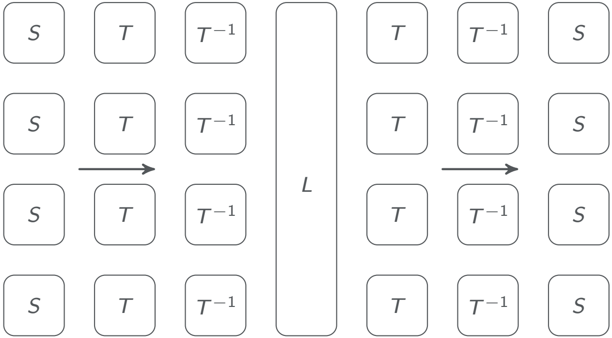
Choice



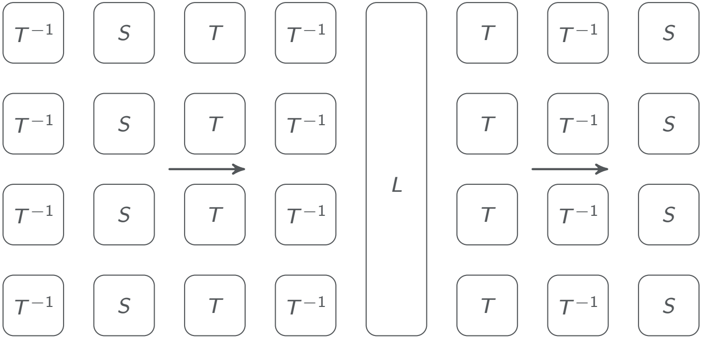
Choice



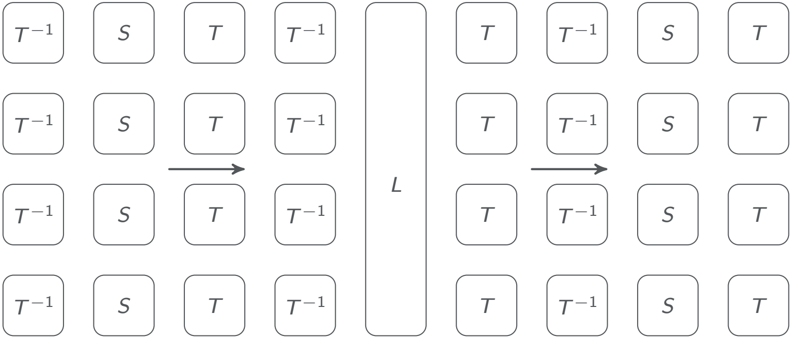
Choice



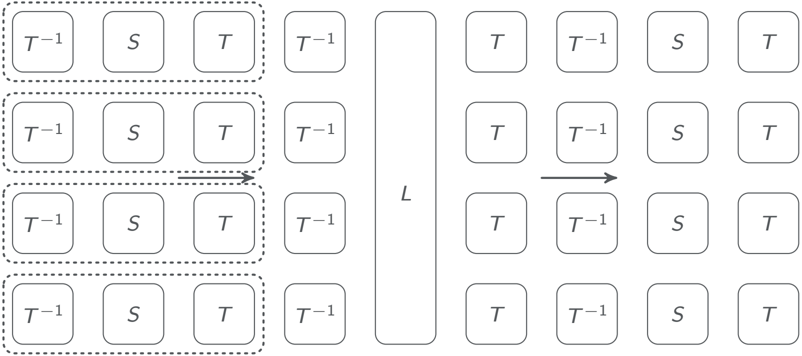
Choice



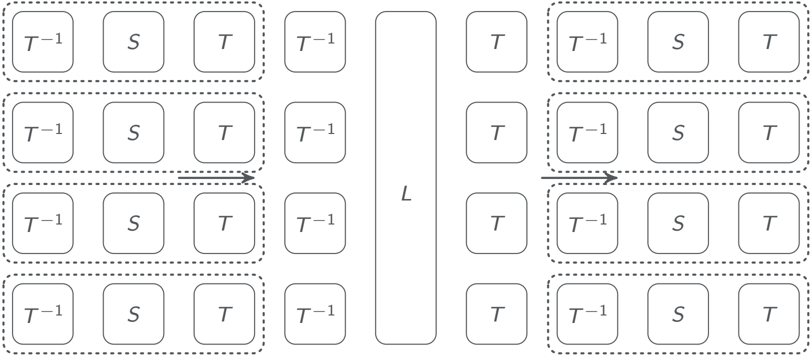
Choice



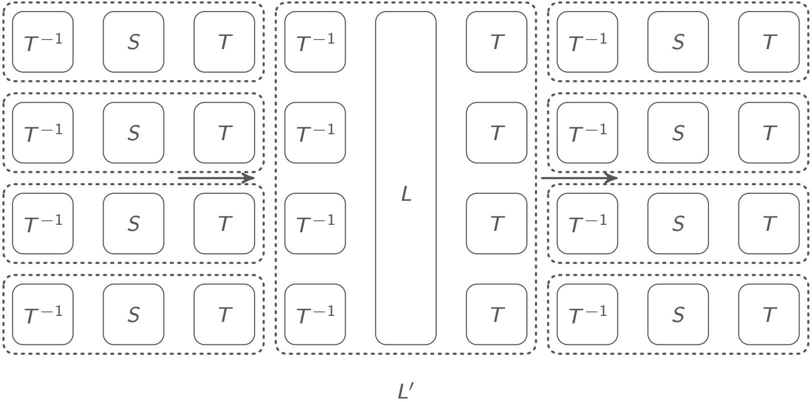
Choice



Choice



Choice



Matrix representations of $\mathbb{F}_{2^s}$

Starting with $L = (\gamma_{i,j})_{i,j}$

$$L' = \left(T\gamma_{i,j}T^{-1}\right)_{i,j}$$

The sub-matrices are still field elements, e.g.

$$\left(T\alpha T^{-1}\right)\left(T\beta T^{-1}\right) = \left(T\alpha\beta T^{-1}\right)$$

Problem (abstracted)

Let $\mathcal{S} = \{A_1, A_2, \ldots, A_n\} \subseteq \mathrm{GL}(s, \mathbb{F}_2)$. Decide whether the matrix ring $\mathbb{F}_2[\mathcal{S}]$ (i.e., the smallest subring of $\mathrm{Mat}(\mathbb{F}_2, s \times s)$ containing $\mathcal{S}$) is a field isomorphic to a (sub)field of $\mathbb{F}_{2^s}$.

$$\mathcal{S} = \{L'_{i,j}\}$$

When is $\mathbb{F}_2[\mathcal{S}]$ a field?

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Let's start easy: $\mathcal{S} = \{A\}$

Lemma (One Element in $\mathcal{S}$)

For $A \in \mathrm{GL}(s, \mathbb{F}_2)$, the ring $\mathbb{F}_2[A] = \{\sum_{i=0}^{m} c_i A^i \mid c_i \in \mathbb{F}_2, m \geq 0\}$ is a field isomorphic to a subfield of $\mathbb{F}_{2^s}$ if and only if the minimal polynomial of A, denoted m_A, is irreducible.

When is $\mathbb{F}_2[\mathcal{S}]$ a field? (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries

Lemma (Multiple Elements in $\mathcal{S}$)

Let $\mathcal{S} = \{A_1, A_2, \ldots, A_n\} \subseteq \mathrm{GL}(s, \mathbb{F}_2)$. Then, $\mathbb{F}_2[\mathcal{S}]$ is a field isomorphic to a subfield of $\mathbb{F}_{2^s}$ if and only if the multiplicative subgroup $\langle \mathcal{S} \rangle$ of $\mathrm{GL}(s, \mathbb{F}_2)$ is cyclic and generated by an element with irreducible minimal polynomial.

Proof:

- $\Leftarrow$ is clear from the previous lemma
- If $\mathbb{F}_2[\mathcal{S}]$ is a field, its multiplicative group is cyclic, hence $\langle \mathcal{S} \rangle$ is a cyclic subgroup. Let α be a generator of $\langle \mathcal{S} \rangle$. We have $\mathbb{F}_2[\alpha] = \mathbb{F}_2[\mathcal{S}]$. By the previous lemma, m_α is irreducible.

When is $\mathbb{F}_2[\mathcal{S}]$ a field? (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Lemma (Multiple Elements in $\mathcal{S}$)

Let $\mathcal{S} = \{A_1, A_2, \ldots, A_n\} \subseteq \mathrm{GL}(s, \mathbb{F}_2)$. Then, $\mathbb{F}_2[\mathcal{S}]$ is a field isomorphic to a subfield of $\mathbb{F}_{2^s}$ if and only if the multiplicative subgroup $\langle \mathcal{S} \rangle$ of $\mathrm{GL}(s, \mathbb{F}_2)$ is cyclic and generated by an element with irreducible minimal polynomial.

Proof:

- $\Leftarrow$ is clear from the previous lemma
- If $\mathbb{F}_2[\mathcal{S}]$ is a field, its multiplicative group is cyclic, hence $\langle \mathcal{S} \rangle$ is a cyclic subgroup. Let α be a generator of $\langle \mathcal{S} \rangle$. We have $\mathbb{F}_2[\alpha] = \mathbb{F}_2[\mathcal{S}]$. By the previous lemma, m_α is irreducible.

When is $\mathbb{F}_2[\mathcal{S}]$ a field? (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries

Lemma (Multiple Elements in $\mathcal{S}$)

Let $\mathcal{S} = \{A_1, A_2, \ldots, A_n\} \subseteq \mathrm{GL}(s, \mathbb{F}_2)$. Then, $\mathbb{F}_2[\mathcal{S}]$ is a field isomorphic to a subfield of $\mathbb{F}_{2^s}$ if and only if the multiplicative subgroup $\langle \mathcal{S} \rangle$ of $\mathrm{GL}(s, \mathbb{F}_2)$ is cyclic and generated by an element with irreducible minimal polynomial.

Proof:

- $\Leftarrow$ is clear from the previous lemma
- If $\mathbb{F}_2[\mathcal{S}]$ is a field, its multiplicative group is cyclic, hence $\langle \mathcal{S} \rangle$ is a cyclic subgroup. Let α be a generator of $\langle \mathcal{S} \rangle$. We have $\mathbb{F}_2[\alpha] = \mathbb{F}_2[\mathcal{S}]$. By the previous lemma, m_α is irreducible.

A group-theoretic question

Problem (further abstracted)

Decide whether a group $\langle A_1, A_2, \ldots, A_n \rangle \subseteq \mathrm{GL}(s, \mathbb{F}_2)$ is cyclic and generated by an element with irrreducible minimal polynomial.

Lemma (Folklore)

Let $G = \langle A_1, A_2 \rangle$ be a cyclic group

$$k_1 = \mathrm{ord}(A_1) \text{ and } k_2 = \mathrm{ord}(A_2).$$

Let h_1, h_2 be coprime positive integers such that $h_1 h_2 = \mathrm{lcm}(k_1, k_2)$ and, for $i \in \{1, 2\}$, $h_i \mid k_i$. Then, $G = \langle A_1^{k_1/h_1} \cdot A_2^{k_2/h_2} \rangle$.

- Applying this lemma iteratively allows to find a generator of a cyclic group $\langle A_1, \ldots, A_n \rangle$.

A group-theoretic question

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Problem (further abstracted)

Decide whether a group $\langle A_1, A_2, \ldots, A_n \rangle \subseteq \mathrm{GL}(s, \mathbb{F}_2)$ is cyclic and generated by an element with irrreducible minimal polynomial.

Lemma (Folklore)

Let $G = \langle A_1, A_2 \rangle$ be a cyclic group

$$k_1 = \mathrm{ord}(A_1) \text{ and } k_2 = \mathrm{ord}(A_2).$$

Let h_1, h_2 be coprime positive integers such that $h_1 h_2 = \mathrm{lcm}(k_1, k_2)$ and, for $i \in \{1, 2\}$, $h_i \mid k_i$. Then, $G = \langle A_1^{k_1/h_1} \cdot A_2^{k_2/h_2} \rangle$.

- Applying this lemma iteratively allows to find a generator of a cyclic group $\langle A_1, \ldots, A_n \rangle$.

A group-theoretic question

Problem (further abstracted)

Decide whether a group $\langle A_1, A_2, \ldots, A_n \rangle \subseteq \mathrm{GL}(s, \mathbb{F}_2)$ is cyclic and generated by an element with irrreducible minimal polynomial.

Lemma (Folklore)

Let $G = \langle A_1, A_2 \rangle$ be a cyclic group

$$k_1 = \mathrm{ord}(A_1) \text{ and } k_2 = \mathrm{ord}(A_2).$$

Let h_1, h_2 be coprime positive integers such that $h_1 h_2 = \mathrm{lcm}(k_1, k_2)$ and, for $i \in \{1, 2\}$, $h_i \mid k_i$. Then, $G = \langle A_1^{k_1/h_1} \cdot A_2^{k_2/h_2} \rangle$.

- Applying this lemma iteratively allows to find a generator of a cyclic group $\langle A_1, \ldots, A_n \rangle$.

Algorithm for deciding whether $\mathbb{F}_2[A_1, \dots, A_n]$ is a field

1. Apply iteratively to $G = \langle A_1, \dots, A_n \rangle$ to find a pseudo-generator α of G (α is indeed a generator if and only if G is cyclic)
2. We need to check whether $A_1, \dots, A_n$ are indeed elements of $\mathbb{F}_2[\alpha]$:
   For each A_i, check whether $A_i \in \mathrm{Span}(1, \alpha, \alpha^2, \dots, \alpha^{s-1})$.
   - If not, return "Not a field"
3. If m_α is not irreducible return "Not a field"
4. return α

Complexity

If we know the prime factorization of $2^s - 1$ running time is polynomial.

Algorithm for deciding whether $\mathbb{F}_2[A_1, \ldots, A_n]$ is a field

1. Apply iteratively to $G = \langle A_1, \ldots, A_n \rangle$ to find a pseudo-generator α of G (α is indeed a generator if and only if G is cyclic)
2. We need to check whether $A_1, \ldots, A_n$ are indeed elements of $\mathbb{F}_2[\alpha]$:
   For each A_i, check whether $A_i \in \mathrm{Span}(1, \alpha, \alpha^2, \ldots, \alpha^{s-1})$.
   - If not, return "Not a field"
3. If m_α is not irreducible return "Not a field"
4. return α

Complexity

If we know the prime factorization of $2^s - 1$ running time is polynomial.

Algorithm for deciding whether $\mathbb{F}_2[A_1, \ldots, A_n]$ is a field

CASA
Cyber Security in the Age of Large-Scale Adversaries

1. Apply iteratively to $G = \langle A_1, \ldots, A_n \rangle$ to find a pseudo-generator α of G (α is indeed a generator if and only if G is cyclic)
2. We need to check whether $A_1, \ldots, A_n$ are indeed elements of $\mathbb{F}_2[\alpha]$:
   For each A_i, check whether $A_i \in \mathrm{Span}(1, \alpha, \alpha^2, \ldots, \alpha^{s-1})$.
   - If not, return "Not a field"
3. If m_α is not irreducible return "Not a field"
4. return α

Complexity

If we know the prime factorization of $2^s - 1$ running time is polynomial.

Algorithm for deciding whether $\mathbb{F}_2[A_1, \dots, A_n]$ is a field

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

1. Apply iteratively to $G = \langle A_1, \dots, A_n \rangle$ to find a pseudo-generator α of G (α is indeed a generator if and only if G is cyclic)
2. We need to check whether $A_1, \dots, A_n$ are indeed elements of $\mathbb{F}_2[\alpha]$:
   For each A_i, check whether $A_i \in \mathrm{Span}(1, \alpha, \alpha^2, \dots, \alpha^{s-1})$.
   - If not, return "Not a field"
3. If m_α is not irreducible return "Not a field"
4. return α

Complexity

If we know the prime factorization of $2^s - 1$ running time is polynomial.

Application to Streebog

For the linear layer of Streebog (element $M \in \mathrm{Mat}(\mathbb{F}_2, 64 \times 64)$), the running time is less than a second and we directly obtain

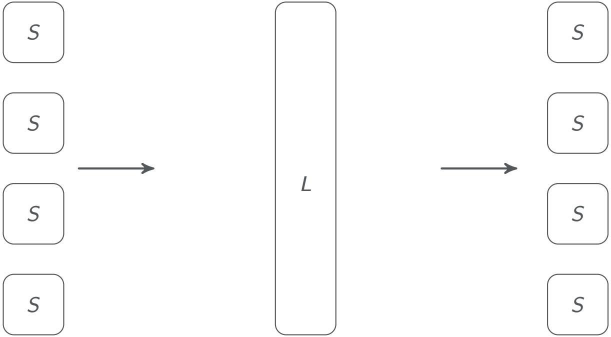
$$M = \begin{bmatrix} \gamma^{1} & \gamma^{64} & \gamma^{66} & \gamma^{39} & \gamma^{133} & \gamma^{249} & \gamma^{94} & \gamma^{135} \\ \gamma^{249} & \gamma^{84} & \gamma^{150} & \gamma^{0} & \gamma^{210} & \gamma^{1} & \gamma^{221} & \gamma^{32} \\ \gamma^{100} & \gamma^{16} & \gamma^{155} & \gamma^{15} & \gamma^{167} & \gamma^{36} & \gamma^{182} & \gamma^{57} \\ \gamma^{220} & \gamma^{174} & \gamma^{246} & \gamma^{217} & \gamma^{216} & \gamma^{17} & \gamma^{90} & \gamma^{198} \\ \gamma^{116} & \gamma^{188} & \gamma^{217} & \gamma^{246} & \gamma^{124} & \gamma^{127} & \gamma^{237} & \gamma^{206} \\ \gamma^{37} & \gamma^{129} & \gamma^{147} & \gamma^{243} & \gamma^{36} & \gamma^{167} & \gamma^{154} & \gamma^{89} \\ \gamma^{77} & \gamma^{66} & \gamma^{64} & \gamma^{238} & \gamma^{206} & \gamma^{3} & \gamma^{136} & \gamma^{124} \\ \gamma^{135} & \gamma^{230} & \gamma^{73} & \gamma^{137} & \gamma^{164} & \gamma^{32} & \gamma^{134} & \gamma^{1} \end{bmatrix}, \quad (1)$$

where

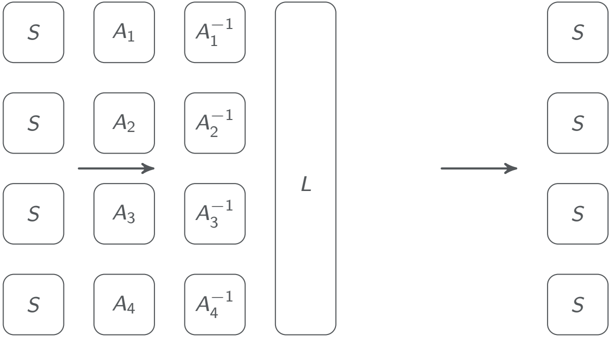
$$\gamma = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

1. Field Structure
2. Obfuscation and More Structure

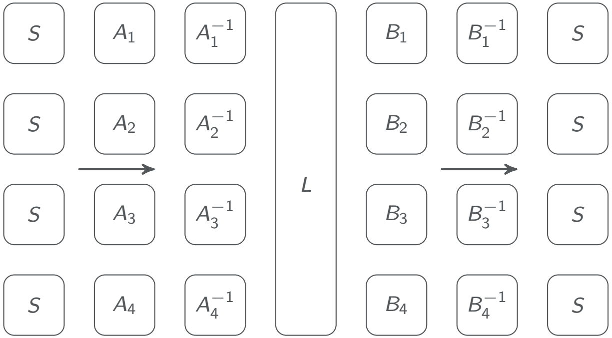
(Heavy) Obfuscated Case: Even More Choice



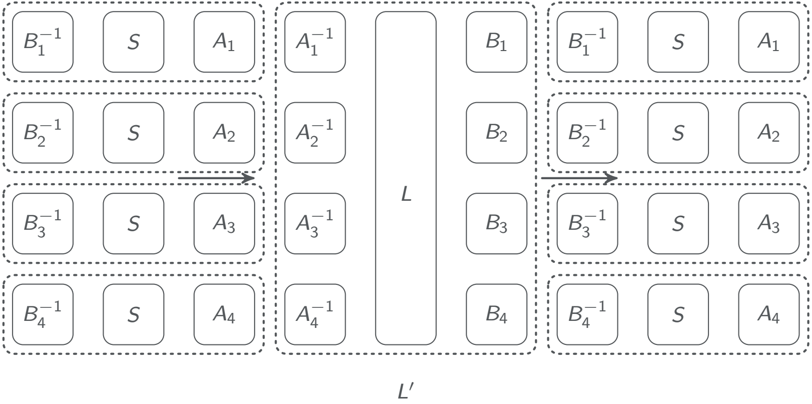
(Heavy) Obfuscated Case: Even More Choice



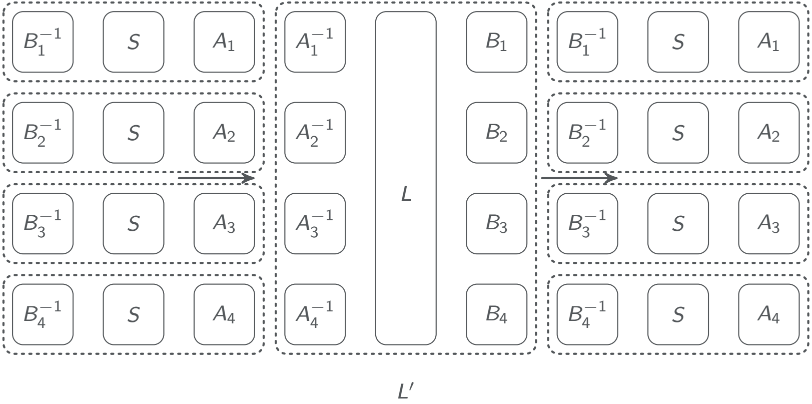
(Heavy) Obfuscated Case: Even More Choice



(Heavy) Obfuscated Case: Even More Choice



(Heavy) Obfuscated Case: Even More Choice



In the paper: Algorithm to efficiently recover L for L' also in this case

Cauchy MDS

CASA
Cyber Security in the Age of Large-Scale Adversaries

After we identified the field strucure: What more can be said?

Cauchy construction

We give a way to test if a (heavily obfuscated) matrix corresponds to a Cauchy-MDS Matrix.

Details in the paper.

Application to Streebog

Cyber Security in the Age of Large-Scale Adversaries

$$M = \begin{bmatrix} \gamma^{1} & \gamma^{64} & \gamma^{66} & \gamma^{39} & \gamma^{133} & \gamma^{249} & \gamma^{94} & \gamma^{135} \\ \gamma^{249} & \gamma^{84} & \gamma^{150} & \gamma^{0} & \gamma^{210} & \gamma^{1} & \gamma^{221} & \gamma^{32} \\ \gamma^{100} & \gamma^{16} & \gamma^{155} & \gamma^{15} & \gamma^{167} & \gamma^{36} & \gamma^{182} & \gamma^{57} \\ \gamma^{220} & \gamma^{174} & \gamma^{246} & \gamma^{217} & \gamma^{216} & \gamma^{17} & \gamma^{90} & \gamma^{198} \\ \gamma^{116} & \gamma^{188} & \gamma^{217} & \gamma^{246} & \gamma^{124} & \gamma^{127} & \gamma^{237} & \gamma^{206} \\ \gamma^{37} & \gamma^{129} & \gamma^{147} & \gamma^{243} & \gamma^{36} & \gamma^{167} & \gamma^{154} & \gamma^{89} \\ \gamma^{77} & \gamma^{66} & \gamma^{64} & \gamma^{238} & \gamma^{206} & \gamma^{3} & \gamma^{136} & \gamma^{124} \\ \gamma^{135} & \gamma^{230} & \gamma^{73} & \gamma^{137} & \gamma^{164} & \gamma^{32} & \gamma^{134} & \gamma^{1} \end{bmatrix},$$

$$\gamma = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

is a Cauchy matrix with

$$(u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8) = (\gamma^{120}, \gamma^{223}, \gamma^{198}, \gamma^{57}, \gamma^{49}, \gamma^{166}, \gamma^{131}, \gamma^{254})$$

$$(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8) = (\gamma^{77}, \gamma^{82}, \gamma^{59}, \gamma^{220}, \gamma^{72}, \gamma^{209}, \gamma^{4}, 0).$$

The End

Thank you very much for your attention!
Questions?