Clustering Approach for Higher-Order Deterministic Masking

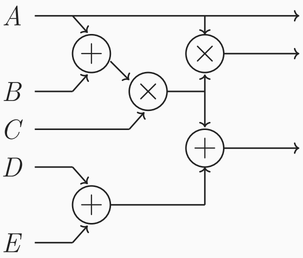
Vahid Jahandideh, Jan Schoone, Lejla Batina
Radboud University (The Netherlands)

GelreCrypt 2025
6 November, 2025

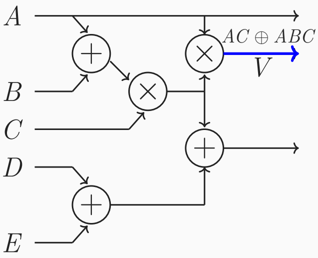
Side-Channel Attacks

The power trace of a device is correlated with the values processed inside it.

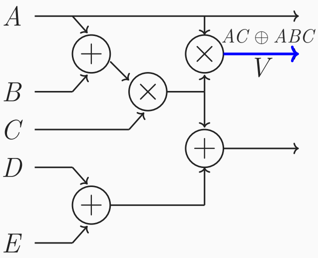
The power trace of a device is correlated with the values processed inside it.



The power trace of a device is correlated with the values processed inside it.



The power trace of a device is correlated with the values processed inside it.



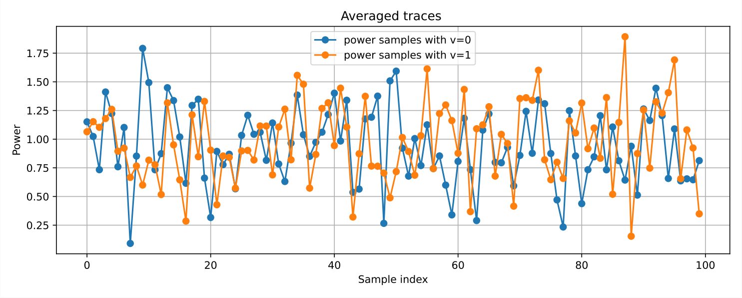
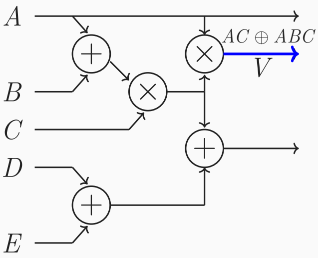


Figure: A single trace.

The power trace of a device is correlated with the values processed inside it.



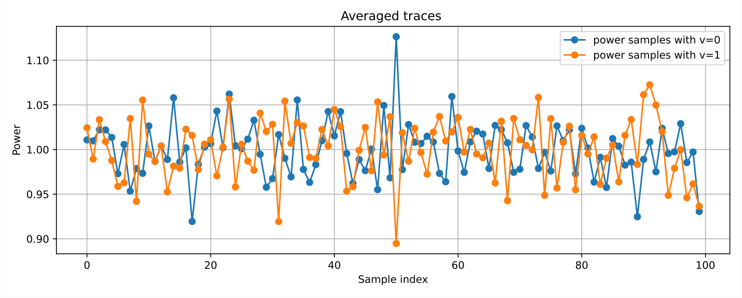
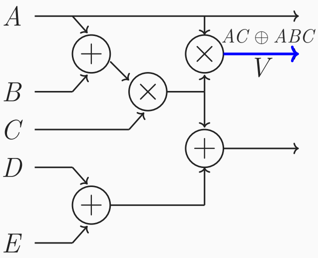


Figure: 100 traces aggregated.

The power trace of a device is correlated with the values processed inside it.



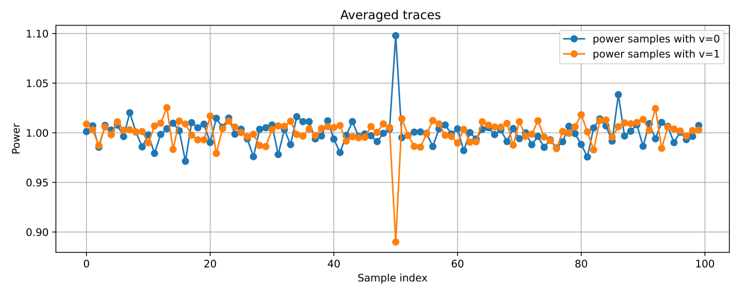
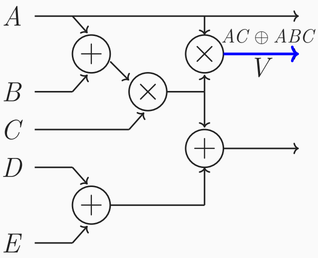


Figure: 1000 traces aggregated.

The power trace of a device is correlated with the values processed inside it.



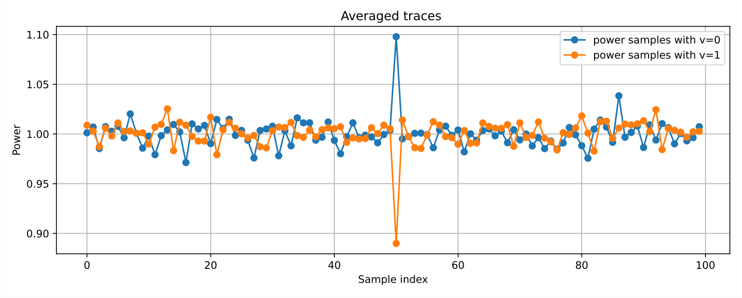


Figure: 1000 traces aggregated.

Take-away: These correlations let an adversary learn operands or even recover secret keys.

Masking Countermeasure

To protect a sensitive variable $X \in \mathbb{F}_{2^u}$ from side-channel leakage, masking is the most widely used countermeasure.

Masking Countermeasure

To protect a sensitive variable $X \in \mathbb{F}_{2^u}$ from side-channel leakage, masking is the most widely used countermeasure.

- Replace X with n random shares $\mathbf{X} = [X_0, \ldots, X_{n-1}]$ such that

$$\bigoplus_{i=0}^{n-1} X_i = X.$$

Masking Countermeasure

To protect a sensitive variable $X \in \mathbb{F}_{2^u}$ from side-channel leakage, masking is the most widely used countermeasure.

- Replace X with n random shares $\mathbf{X} = [X_0, \ldots, X_{n-1}]$ such that

$$\bigoplus_{i=0}^{n-1} X_i = X.$$

- Shares are (pseudo)random and independent subject to the XOR constraint. Any set of $t < n$ shares leaves X uniform (intuition: unless all shares are known, X is hidden).

Masking Countermeasure

To protect a sensitive variable $X \in \mathbb{F}_{2^u}$ from side-channel leakage, masking is the most widely used countermeasure.

- Replace X with n random shares $\mathbf{X} = [X_0, \ldots, X_{n-1}]$ such that

$$\bigoplus_{i=0}^{n-1} X_i = X.$$

- Shares are (pseudo)random and independent subject to the XOR constraint. Any set of $t < n$ shares leaves X uniform (intuition: unless all shares are known, X is hidden).
- All computations are performed on shares: linear ops are per-share; non-linear ops (e.g., multiplication) require dedicated gadgets (e.g., ISW/PINI/…).

Masking Countermeasure

To protect a sensitive variable $X \in \mathbb{F}_{2^u}$ from side-channel leakage, masking is the most widely used countermeasure.

- Replace X with n random shares $\mathbf{X} = [X_0, \ldots, X_{n-1}]$ such that
$$\bigoplus_{i=0}^{n-1} X_i = X.$$
- Shares are (pseudo)random and independent subject to the XOR constraint. Any set of $t < n$ shares leaves X uniform (intuition: unless all shares are known, X is hidden).
- All computations are performed on shares: linear ops are per-share; non-linear ops (e.g., multiplication) require dedicated gadgets (e.g., ISW/PINI/...).

Multiplication (goal)

Given shares $[X_0, \ldots, X_{n-1}]$ and $[Y_0, \ldots, Y_{n-1}]$, securely compute n shares of $Z = XY$ without leaking X or Y.

Probing Model and Glitch-Extended Probing Model

Side-channel leakage is often noisy and hard to model directly. Two idealized models capture what an attacker can observe without noise:

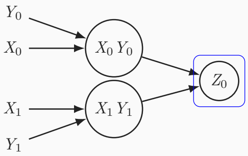
Probing Model and Glitch-Extended Probing Model

Side-channel leakage is often noisy and hard to model directly. Two idealized models capture what an attacker can observe without noise:

- **(Threshold) probing model.** The adversary can read the values on up to d internal wires (intermediate nodes) per execution.

Side-channel leakage is often noisy and hard to model directly. Two idealized models capture what an attacker can observe without noise:

- **(Threshold) probing model.** The adversary can read the values on up to d internal wires (intermediate nodes) per execution.
- **Glitch-extended probing model.** Probing a value V reveals the entire transitive fan-in used to compute V (to model glitches/hazards).

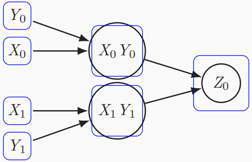


Probe Z_0 (probing).

Probing Model and Glitch-Extended Probing Model

Side-channel leakage is often noisy and hard to model directly. Two idealized models capture what an attacker can observe without noise:

- **(Threshold) probing model.** The adversary can read the values on up to d internal wires (intermediate nodes) per execution.
- **Glitch-extended probing model.** Probing a value V reveals the entire transitive fan-in used to compute V (to model glitches/hazards).



Probe Z_0 (glitch-extended): fan-in exposed.

Example

Let $X = X_0 \oplus X_1$ and $Y = Y_0 \oplus Y_1$. A 2-share "schoolbook" multiplication over $\mathbb{F}_2$:

$$\begin{cases} Z_0 &= X_0\,Y_0 \oplus X_1\,Y_1, \\ Z_1 &= X_0\,Y_1 \oplus X_1\,Y_0. \end{cases}$$

Implication. Probing Z_0 (or Z_1) reveals X and Y.

How to Multiply (ISW'03)

- In 2003, Ishai–Sahai–Wagner (ISW) introduced a multiplication gadget secure in the probing model.

How to Multiply (ISW'03)

- In 2003, Ishai–Sahai–Wagner (ISW) introduced a multiplication gadget secure in the probing model.
- For $d = 1$ (2 shares) over $\mathbb{F}_2$, one correct instantiation is:

$$\begin{cases} Z_0 = X_0\,Y_0 \oplus R, \\ Z_1 = X_1\,Y_1 \oplus (R \oplus X_0\,Y_1) \oplus X_1\,Y_0. \end{cases}$$

How to Multiply (ISW'03)

- In 2003, Ishai–Sahai–Wagner (ISW) introduced a multiplication gadget secure in the probing model.
- For $d = 1$ (2 shares) over $\mathbb{F}_2$, one correct instantiation is:

$$\begin{cases} Z_0 = X_0\,Y_0 \oplus R, \\ Z_1 = X_1\,Y_1 \oplus (R \oplus X_0\,Y_1) \oplus X_1\,Y_0. \end{cases}$$

- The gadget uses one fresh online random mask R per multiplication.

How to Multiply (ISW'03)

- In 2003, Ishai–Sahai–Wagner (ISW) introduced a multiplication gadget secure in the probing model.
- For $d = 1$ (2 shares) over $\mathbb{F}_2$, one correct instantiation is:

$$\begin{cases} Z_0 = X_0\,Y_0 \oplus R, \\ Z_1 = X_1\,Y_1 \oplus (R \oplus X_0\,Y_1) \oplus X_1\,Y_0. \end{cases}$$

- The gadget uses one fresh online random mask R per multiplication.
- For higher orders d, dedicated gadgets exist (cost and randomness grow with d^2).

How to Multiply (ISW'03)

- In 2003, Ishai–Sahai–Wagner (ISW) introduced a multiplication gadget secure in the probing model.
- For $d = 1$ (2 shares) over $\mathbb{F}_2$, one correct instantiation is:

$$\begin{cases} Z_0 = X_0 Y_0 \oplus R, \\ Z_1 = X_1 Y_1 \oplus (R \oplus X_0 Y_1) \oplus X_1 Y_0. \end{cases}$$

- The gadget uses one fresh online random mask R per multiplication.
- For higher orders d, dedicated gadgets exist (cost and randomness grow with d^2).
- ISW is not secure in the glitch-extended probing model.

How to Multiply (ISW'03)

- In 2003, Ishai–Sahai–Wagner (ISW) introduced a multiplication gadget secure in the probing model.
- For $d = 1$ (2 shares) over $\mathbb{F}_2$, one correct instantiation is:

$$\begin{cases} Z_0 = X_0 Y_0 \oplus R, \\ Z_1 = X_1 Y_1 \oplus (R \oplus X_0 Y_1) \oplus X_1 Y_0. \end{cases}$$

- The gadget uses one fresh online random mask R per multiplication.
- For higher orders d, dedicated gadgets exist (cost and randomness grow with d^2).
- ISW is not secure in the glitch-extended probing model.

Challenge

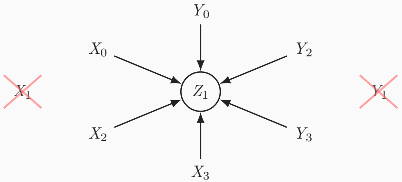
How can we perform secure multiplication under the glitch-extended probing model without relying on online randomness?

Nikova et al. $(n = 4)$ Deterministic Gadget

$$\begin{cases} Z_0 = (1 \oplus X_2 \oplus X_3)(1 \oplus Y_1 \oplus Y_2) \oplus Y_3 \oplus X_1, \\ Z_1 = (1 \oplus X_0 \oplus X_2)(1 \oplus Y_0 \oplus Y_3) \oplus Y_2 \oplus X_3, \\ Z_2 = (X_1 \oplus X_3)(Y_0 \oplus Y_3) \oplus Y_1 \oplus X_1, \\ Z_3 = (X_0 \oplus X_1)(Y_1 \oplus Y_2) \oplus Y_0 \oplus X_0. \end{cases}$$

Nikova et al. $(n = 4)$ Deterministic Gadget

$$\begin{cases} Z_0 = (1 \oplus X_2 \oplus X_3)(1 \oplus Y_1 \oplus Y_2) \oplus Y_3 \oplus X_1, \\ Z_1 = (1 \oplus X_0 \oplus X_2)(1 \oplus Y_0 \oplus Y_3) \oplus Y_2 \oplus X_3, \\ Z_2 = (X_1 \oplus X_3)(Y_0 \oplus Y_3) \oplus Y_1 \oplus X_1, \\ Z_3 = (X_0 \oplus X_1)(Y_1 \oplus Y_2) \oplus Y_0 \oplus X_0. \end{cases}$$

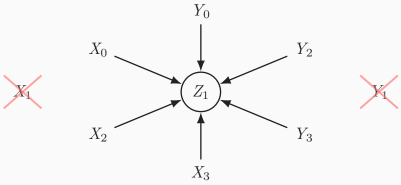


Probe Z_1 (glitch-extended):
fan-in excludes X_1, Y_1.

- **Glitch-extended safety example.** Probing Z_1 does not reveal X_1 or Y_1:
  $\mathrm{fanin}(Z_1) = \{X_0, X_2, X_3, Y_0, Y_2, Y_3\}$.

Nikova et al. ($n = 4$) Deterministic Gadget

$$
\begin{cases}
Z_0 = (1 \oplus X_2 \oplus X_3)(1 \oplus Y_1 \oplus Y_2) \oplus Y_3 \oplus X_1, \\
Z_1 = (1 \oplus X_0 \oplus X_2)(1 \oplus Y_0 \oplus Y_3) \oplus Y_2 \oplus X_3, \\
Z_2 = (X_1 \oplus X_3)(Y_0 \oplus Y_3) \oplus Y_1 \oplus X_1, \\
Z_3 = (X_0 \oplus X_1)(Y_1 \oplus Y_2) \oplus Y_0 \oplus X_0.
\end{cases}
$$

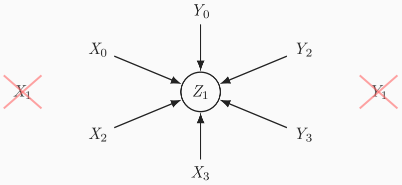


Probe Z_1 (glitch-extended): fan-in excludes X_1, Y_1.

- **Glitch-extended safety example.** Probing Z_1 does not reveal X_1 or Y_1: $\mathrm{fanin}(Z_1) = \{X_0, X_2, X_3, Y_0, Y_2, Y_3\}$.
- **Deterministic:** no online randomness is used.

Nikova et al. ($n = 4$) Deterministic Gadget

$$\begin{cases} Z_0 = (1 \oplus X_2 \oplus X_3)(1 \oplus Y_1 \oplus Y_2) \oplus Y_3 \oplus X_1, \\ Z_1 = (1 \oplus X_0 \oplus X_2)(1 \oplus Y_0 \oplus Y_3) \oplus Y_2 \oplus X_3, \\ Z_2 = (X_1 \oplus X_3)(Y_0 \oplus Y_3) \oplus Y_1 \oplus X_1, \\ Z_3 = (X_0 \oplus X_1)(Y_1 \oplus Y_2) \oplus Y_0 \oplus X_0. \end{cases}$$

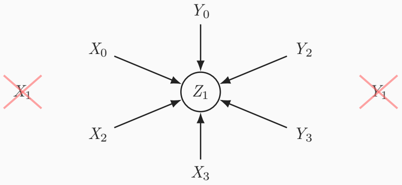


Probe Z_1 (glitch-extended): fan-in excludes X_1, Y_1.

- **Glitch-extended safety example.** Probing Z_1 does not reveal X_1 or Y_1: $\mathrm{fanin}(Z_1) = \{X_0, X_2, X_3, Y_0, Y_2, Y_3\}$.
- **Deterministic:** no online randomness is used.
- **Uniformity:** verified by direct enumeration for the binary case ($u = 1$).

Nikova et al. ($n = 4$) Deterministic Gadget

$$\begin{cases} Z_0 = (1 \oplus X_2 \oplus X_3)(1 \oplus Y_1 \oplus Y_2) \oplus Y_3 \oplus X_1, \\ Z_1 = (1 \oplus X_0 \oplus X_2)(1 \oplus Y_0 \oplus Y_3) \oplus Y_2 \oplus X_3, \\ Z_2 = (X_1 \oplus X_3)(Y_0 \oplus Y_3) \oplus Y_1 \oplus X_1, \\ Z_3 = (X_0 \oplus X_1)(Y_1 \oplus Y_2) \oplus Y_0 \oplus X_0. \end{cases}$$



Probe Z_1 (glitch-extended):
fan-in excludes X_1, Y_1.

- **Glitch-extended safety example.** Probing Z_1 does not reveal X_1 or Y_1:
  $\mathrm{fanin}(Z_1) = \{X_0, X_2, X_3, Y_0, Y_2, Y_3\}$.
- **Deterministic:** no online randomness is used.
- **Uniformity:** verified by direct enumeration for the binary case ($u = 1$).

Computer-Aided Search

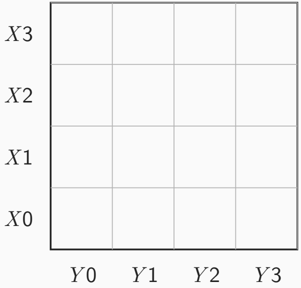
To date, no deterministic multiplication gadget secure against two or more glitch-extended probes is known.

Diving into the Problem (1/3)

Let shares of X be $(X_0, \ldots, X_{n-1})$ and shares of Y be $(Y_0, \ldots, Y_{n-1})$.

$$Z = XY$$

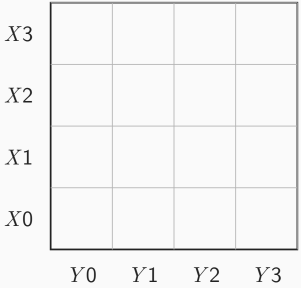
Probe Z_k (glitch-extended) reveals all $(i, j) \in \mathbf{L}_k$



Let shares of X be $(X_0, \ldots, X_{n-1})$ and shares of Y be $(Y_0, \ldots, Y_{n-1})$.

$$Z = \Big(\bigoplus_{i=0}^{n-1} X_i\Big)\Big(\bigoplus_{j=0}^{n-1} Y_j\Big)$$

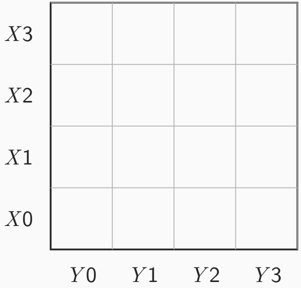
Probe Z_k (glitch-extended) reveals all $(i,j) \in \mathbf{L}_k$



Let shares of X be $(X_0, \ldots, X_{n-1})$ and shares of Y be $(Y_0, \ldots, Y_{n-1})$.

$$Z = \bigoplus_{i=0}^{n-1} \bigoplus_{j=0}^{n-1} X_i Y_j$$

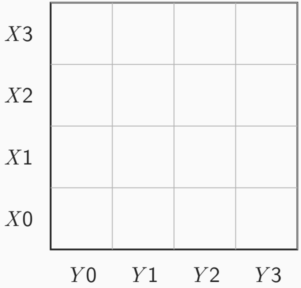
Probe Z_k (glitch-extended) reveals all $(i, j) \in \mathbf{L}_k$



Let shares of X be $(X_0, \ldots, X_{n-1})$ and shares of Y be $(Y_0, \ldots, Y_{n-1})$.

$$Z = \bigoplus_{i=0}^{n-1} \bigoplus_{j=0}^{n-1} X_i Y_j = \bigoplus_{k=0}^{n-1} Z_k$$

Probe Z_k (glitch-extended) reveals all $(i, j) \in \mathbf{L}_k$

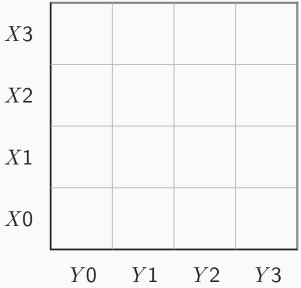


Let shares of X be $(X_0, \ldots, X_{n-1})$ and shares of Y be $(Y_0, \ldots, Y_{n-1})$.

$$Z = \bigoplus_{i=0}^{n-1} \bigoplus_{j=0}^{n-1} X_i Y_j = \bigoplus_{k=0}^{n-1} Z_k$$

$$Z_k = \bigoplus_{(i,j) \in \mathbf{L}_k} X_i Y_j,$$

Probe Z_k (glitch-extended) reveals all $(i,j) \in \mathbf{L}_k$



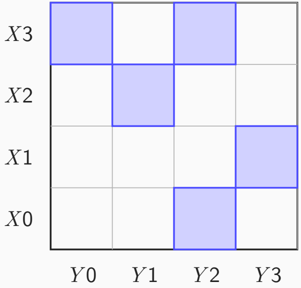
Let shares of X be $(X_0, \ldots, X_{n-1})$ and shares of Y be $(Y_0, \ldots, Y_{n-1})$.

$$Z = \bigoplus_{i=0}^{n-1} \bigoplus_{j=0}^{n-1} X_i Y_j = \bigoplus_{k=0}^{n-1} Z_k$$

$$Z_k = \bigoplus_{(i,j)\in \mathbf{L}_k} X_i Y_j,$$

A glitch-extended probe on Z_k reveals all pairs (X_i, Y_j) with $(i, j) \in \mathbf{L}_k$.

Probe Z_k (glitch-extended) reveals all $(i, j) \in \mathbf{L}_k$



Let shares of X be $(X_0, \ldots, X_{n-1})$ and shares of Y be $(Y_0, \ldots, Y_{n-1})$.

$$Z = \bigoplus_{i=0}^{n-1} \bigoplus_{j=0}^{n-1} X_i Y_j = \bigoplus_{k=0}^{n-1} Z_k$$

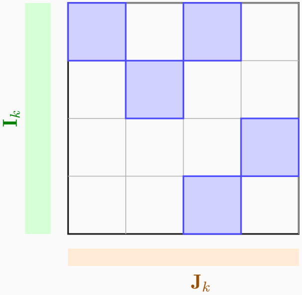
$$Z_k = \bigoplus_{(i,j)\in \mathbf{L}_k} X_i Y_j,$$

A glitch-extended probe on Z_k reveals all pairs (X_i, Y_j) with $(i, j) \in \mathbf{L}_k$.

$\mathbf{I}_k = \{ i \mid \exists j : (i, j) \in \mathbf{L}_k \}$, $\mathbf{J}_k = \{ j \mid \exists i : (i, j) \in \mathbf{L}_k \}$.

Equivalently, probing Z_k exposes all X_i for $i \in \mathbf{I}_k$ and all Y_j for $j \in \mathbf{J}_k$.

Probe Z_k (glitch-extended) reveals all $(i, j) \in \mathbf{L}_k$



Let shares of X be $(X_0, \ldots, X_{n-1})$ and shares of Y be $(Y_0, \ldots, Y_{n-1})$.

$$Z = \bigoplus_{i=0}^{n-1} \bigoplus_{j=0}^{n-1} X_i Y_j = \bigoplus_{k=0}^{n-1} Z_k$$

$$Z_k = \bigoplus_{(i,j)\in\mathbf{L}_k} X_i Y_j,$$

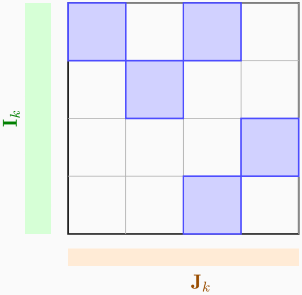
A glitch-extended probe on Z_k reveals all pairs (X_i, Y_j) with $(i,j) \in \mathbf{L}_k$.

$\mathbf{I}_k = \{ i \mid \exists j : (i,j) \in \mathbf{L}_k \}$, $\mathbf{J}_k = \{ j \mid \exists i : (i,j) \in \mathbf{L}_k \}$.

Equivalently, probing Z_k exposes all X_i for $i \in \mathbf{I}_k$ and all Y_j for $j \in \mathbf{J}_k$.

Goal: choose $\mathbf{L}_k$ so that each probe reveals as few shares as possible.

Probe Z_k (glitch-extended) reveals all $(i,j) \in \mathbf{L}_k$



We can show that

$$\sqrt{n} \;\leq\; \max_{0 \leq k < n} \max\{\, |\mathbf{I}_k|,\ |\mathbf{J}_k| \,\}.$$

Diving into the Problem (2/3)

We can show that

$$\sqrt{n} \;\le\; \max_{0 \le k < n} \max\{\, |\mathbf{I}_k|,\; |\mathbf{J}_k| \,\}.$$

Best case (tight):

$$\sqrt{n} \;=\; \max_{0 \le k < n} \max\{\, |\mathbf{I}_k|,\; |\mathbf{J}_k| \,\}.$$

Diving into the Problem (2/3)

We can show that

$$\sqrt{n} \;\le\; \max_{0\le k<n} \max\{\,|\mathbf{I}_k|,\; |\mathbf{J}_k|\,\}.$$

Best case (tight):

$$\sqrt{n} \;=\; \max_{0\le k<n} \max\{\,|\mathbf{I}_k|,\; |\mathbf{J}_k|\,\}.$$

For $n = 4$, we can realize equality by pairing rows/columns as below.

$$\begin{bmatrix} X_0 & X_1 \\ X_2 & X_3 \end{bmatrix} \qquad \begin{bmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{bmatrix}$$

Diving into the Problem (2/3)

We can show that

$$\sqrt{n} \le \max_{0\le k<n} \max\{\, |\mathbf{I}_k|,\ |\mathbf{J}_k| \,\}.$$

Best case (tight):

$$\sqrt{n} = \max_{0\le k<n} \max\{\, |\mathbf{I}_k|,\ |\mathbf{J}_k| \,\}.$$

For $n = 4$, we can realize equality by pairing rows/columns as below.

$$\begin{bmatrix} X_0 & X_1 \\ X_2 & X_3 \end{bmatrix} \qquad \begin{bmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{bmatrix} \qquad \begin{cases} Z_0 = \mathbf{X}|_{\mathbf{I}_0} \otimes \mathbf{Y}|_{\mathbf{J}_0} = (X_0 \oplus X_1)\,(Y_0 \oplus Y_2), \\ Z_1 = \mathbf{X}|_{\mathbf{I}_1} \otimes \mathbf{Y}|_{\mathbf{J}_1} = (X_0 \oplus X_1)\,(Y_1 \oplus Y_3), \\ Z_2 = \mathbf{X}|_{\mathbf{I}_2} \otimes \mathbf{Y}|_{\mathbf{J}_2} = (X_2 \oplus X_3)\,(Y_0 \oplus Y_2), \\ Z_3 = \mathbf{X}|_{\mathbf{I}_3} \otimes \mathbf{Y}|_{\mathbf{J}_3} = (X_2 \oplus X_3)\,(Y_1 \oplus Y_3). \end{cases}$$

Diving into the Problem (2/3)

We can show that

$$\sqrt{n} \;\le\; \max_{0\le k<n} \max\{\, |\mathbf{I}_k|,\; |\mathbf{J}_k| \,\}.$$

Best case (tight):

$$\sqrt{n} \;=\; \max_{0\le k<n} \max\{\, |\mathbf{I}_k|,\; |\mathbf{J}_k| \,\}.$$

For $n = 4$, we can realize equality by pairing rows/columns as below.

$$\mathbf{X}|_{\mathbf{I}_0},\ \mathbf{X}|_{\mathbf{I}_1} \qquad \mathbf{Y}|_{\mathbf{J}_0},\ \mathbf{Y}|_{\mathbf{J}_2}$$

$$\begin{bmatrix} X_0 & X_1 \\ X_2 & X_3 \end{bmatrix} \qquad \begin{bmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{bmatrix}$$

$$\mathbf{X}|_{\mathbf{I}_2},\ \mathbf{X}|_{\mathbf{I}_3} \qquad \mathbf{Y}|_{\mathbf{J}_1},\ \mathbf{Y}|_{\mathbf{J}_3}$$

$$\begin{cases} Z_0 = \mathbf{X}|_{\mathbf{I}_0} \otimes \mathbf{Y}|_{\mathbf{J}_0} = (X_0 \oplus X_1)\,(Y_0 \oplus Y_2), \\ Z_1 = \mathbf{X}|_{\mathbf{I}_1} \otimes \mathbf{Y}|_{\mathbf{J}_1} = (X_0 \oplus X_1)\,(Y_1 \oplus Y_3), \\ Z_2 = \mathbf{X}|_{\mathbf{I}_2} \otimes \mathbf{Y}|_{\mathbf{J}_2} = (X_2 \oplus X_3)\,(Y_0 \oplus Y_2), \\ Z_3 = \mathbf{X}|_{\mathbf{I}_3} \otimes \mathbf{Y}|_{\mathbf{J}_3} = (X_2 \oplus X_3)\,(Y_1 \oplus Y_3). \end{cases}$$

Diving into the Problem (2/3)

We can show that

$$\sqrt{n} \;\leq\; \max_{0 \leq k < n} \max\{\, |\mathbf{I}_k|,\ |\mathbf{J}_k| \,\}.$$

Best case (tight):

$$\sqrt{n} \;=\; \max_{0 \leq k < n} \max\{\, |\mathbf{I}_k|,\ |\mathbf{J}_k| \,\}.$$

For $n = 4$, we can realize equality by pairing rows/columns as below.

$\mathbf{X}|_{\mathbf{I}_0}, \mathbf{X}|_{\mathbf{I}_1}$ $\quad$ $\mathbf{Y}|_{\mathbf{J}_0}, \mathbf{Y}|_{\mathbf{J}_2}$

$$\begin{bmatrix} X_0 & X_1 \\ X_2 & X_3 \end{bmatrix} \qquad \begin{bmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{bmatrix}$$

$\mathbf{X}|_{\mathbf{I}_2}, \mathbf{X}|_{\mathbf{I}_3}$ $\quad$ $\mathbf{Y}|_{\mathbf{J}_1}, \mathbf{Y}|_{\mathbf{J}_3}$

$$\begin{cases} Z_0 = \mathbf{X}|_{\mathbf{I}_0} \otimes \mathbf{Y}|_{\mathbf{J}_0} = (X_0 \oplus X_1)\,(Y_0 \oplus Y_2), \\ Z_1 = \mathbf{X}|_{\mathbf{I}_1} \otimes \mathbf{Y}|_{\mathbf{J}_1} = (X_0 \oplus X_1)\,(Y_1 \oplus Y_3), \\ Z_2 = \mathbf{X}|_{\mathbf{I}_2} \otimes \mathbf{Y}|_{\mathbf{J}_2} = (X_2 \oplus X_3)\,(Y_0 \oplus Y_2), \\ Z_3 = \mathbf{X}|_{\mathbf{I}_3} \otimes \mathbf{Y}|_{\mathbf{J}_3} = (X_2 \oplus X_3)\,(Y_1 \oplus Y_3). \end{cases}$$

This gadget is first-order probing secure, but not uniform.

If we had fresh masks R_k with $\bigoplus_k R_k = 0$, then $W_k = Z_k \oplus R_k$ would be a **uniform** sharing of Z.

Diving into the Problem (3/3)

If we had fresh masks R_k with $\bigoplus_k R_k = 0$, then $W_k = Z_k \oplus R_k$ would be a **uniform** sharing of Z.

We can synthesize such masks from the input shares: R_k is built from X_i's and Y_j's.

Diving into the Problem (3/3)

If we had fresh masks R_k with $\bigoplus_k R_k = 0$, then $W_k = Z_k \oplus R_k$ would be a **uniform** sharing of Z.

We can synthesize such masks from the input shares: R_k is built from X_i's and Y_j's.

To keep probing security, R_k must depend only on shares already in the fan-in of Z_k.

Diving into the Problem (3/3)

If we had fresh masks R_k with $\bigoplus_k R_k = 0$, then $W_k = Z_k \oplus R_k$ would be a **uniform** sharing of Z.

We can synthesize such masks from the input shares: R_k is built from X_i's and Y_j's.

To keep probing security, R_k must depend only on shares already in the fan-in of Z_k.

Simple efforts are not leading to uniformity.

Diving into the Problem (3/3)

If we had fresh masks R_k with $\bigoplus_k R_k = 0$, then $W_k = Z_k \oplus R_k$ would be a **uniform** sharing of Z.

We can synthesize such masks from the input shares: R_k is built from X_i's and Y_j's.

To keep probing security, R_k must depend only on shares already in the fan-in of Z_k.

Simple efforts are not leading to uniformity. Finally, a uniform multiplication gadget:

$$\begin{bmatrix} X_0 & X_1 \\ X_2 & X_3 \end{bmatrix} \begin{bmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{bmatrix}$$

Diving into the Problem (3/3)

If we had fresh masks R_k with $\bigoplus_k R_k = 0$, then $W_k = Z_k \oplus R_k$ would be a **uniform** sharing of Z.

We can synthesize such masks from the input shares: R_k is built from X_i's and Y_j's.

To keep probing security, R_k must depend only on shares already in the fan-in of Z_k.

Simple efforts are not leading to uniformity. Finally, a uniform multiplication gadget:

$$\begin{bmatrix} X_0 & X_1 \\ X_2 & X_3 \end{bmatrix} \begin{bmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{bmatrix} \qquad \begin{cases} Z_0 = (X_0 \oplus X_1)(Y_0 \oplus Y_2) \oplus (X_1 \oplus X_2) \oplus (Y_1 \oplus Y_2), \\ Z_1 = (X_2 \oplus X_3)(Y_1 \oplus Y_3) \oplus (X_1 \oplus X_2) \oplus (Y_1 \oplus Y_2), \\ Z_2 = (X_0 \oplus X_3)(Y_0 \oplus Y_2) \oplus (X_2 \oplus X_3) \oplus (Y_2 \oplus Y_3), \\ Z_3 = (X_1 \oplus X_2)(Y_1 \oplus Y_3) \oplus (X_2 \oplus X_3) \oplus (Y_2 \oplus Y_3). \end{cases}$$

Diving into the Problem (3/3)

If we had fresh masks R_k with $\bigoplus_k R_k = 0$, then $W_k = Z_k \oplus R_k$ would be a **uniform** sharing of Z.

We can synthesize such masks from the input shares: R_k is built from X_i's and Y_j's.

To keep probing security, R_k must depend only on shares already in the fan-in of Z_k.

Simple efforts are not leading to uniformity. Finally, a uniform multiplication gadget:

$$\begin{bmatrix} X_0 & X_1 \\ X_2 & X_3 \end{bmatrix} \begin{bmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{bmatrix} \qquad \begin{cases} Z_0 = (X_0 \oplus X_1)(Y_0 \oplus Y_2) \oplus (X_1 \oplus X_2) \oplus (Y_1 \oplus Y_2), \\ Z_1 = (X_2 \oplus X_3)(Y_1 \oplus Y_3) \oplus (X_1 \oplus X_2) \oplus (Y_1 \oplus Y_2), \\ Z_2 = (X_0 \oplus X_3)(Y_0 \oplus Y_2) \oplus (X_2 \oplus X_3) \oplus (Y_2 \oplus Y_3), \\ Z_3 = (X_1 \oplus X_2)(Y_1 \oplus Y_3) \oplus (X_2 \oplus X_3) \oplus (Y_2 \oplus Y_3). \end{cases}$$

There is a pattern!!!

Diving into the Problem (3/3)

If we had fresh masks R_k with $\bigoplus_k R_k = 0$, then $W_k = Z_k \oplus R_k$ would be a **uniform** sharing of Z.

We can synthesize such masks from the input shares: R_k is built from X_i's and Y_j's.

To keep probing security, R_k must depend only on shares already in the fan-in of Z_k.

Simple efforts are not leading to uniformity. Finally, a uniform multiplication gadget:

$$\begin{bmatrix} X_0 & X_1 \\ X_2 & X_3 \end{bmatrix} \begin{bmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{bmatrix} \quad \begin{cases} Z_0 = (X_0 \oplus X_1)(Y_0 \oplus Y_2) \oplus (X_1 \oplus X_2) \oplus (Y_1 \oplus Y_2), \\ Z_1 = (X_2 \oplus X_3)(Y_1 \oplus Y_3) \oplus (X_1 \oplus X_2) \oplus (Y_1 \oplus Y_2), \\ Z_2 = (X_0 \oplus X_3)(Y_0 \oplus Y_2) \oplus (X_2 \oplus X_3) \oplus (Y_2 \oplus Y_3), \\ Z_3 = (X_1 \oplus X_2)(Y_1 \oplus Y_3) \oplus (X_2 \oplus X_3) \oplus (Y_2 \oplus Y_3). \end{cases}$$

There is a pattern!!!

Can we generalize this pattern for square values of n?

Formalizing the pattern.

Formalizing the pattern.

- For $n = s^2$, index the n shares by a grid $\{0, \ldots, s-1\} \times \{0, \ldots, s-1\}$. A **cluster** $C = \{\mathbf{A}_0, \ldots, \mathbf{A}_{s-1}\}$ is a partition of the indices into s multi-shares (blocks) of size s:

$$\mathbf{A}_i \subseteq [n], \quad |\mathbf{A}_i| = s, \quad \mathbf{A}_i \cap \mathbf{A}_j = \varnothing \ (i \neq j), \quad \bigcup_i \mathbf{A}_i = [n].$$

Formalizing the pattern.

- For $n = s^2$, index the n shares by a grid $\{0, \dots, s-1\} \times \{0, \dots, s-1\}$. A **cluster** $C = \{\mathbf{A}_0, \dots, \mathbf{A}_{s-1}\}$ is a partition of the indices into s multi-shares (blocks) of size s:

$$\mathbf{A}_i \subseteq [n], \quad |\mathbf{A}_i| = s, \quad \mathbf{A}_i \cap \mathbf{A}_j = \varnothing \ (i \neq j), \quad \bigcup_i \mathbf{A}_i = [n].$$

- Two clusters $C^{(1)} = \{\mathbf{A}_i^{(1)}\}$ and $C^{(2)} = \{\mathbf{A}_j^{(2)}\}$ should be such that for all i, j,

$$\boxed{|\mathbf{A}_i^{(1)} \cap \mathbf{A}_j^{(2)}| = 1}$$

Formalizing the pattern.

- For $n = s^2$, index the n shares by a grid $\{0, \ldots, s-1\} \times \{0, \ldots, s-1\}$. A **cluster** $C = \{\mathbf{A}_0, \ldots, \mathbf{A}_{s-1}\}$ is a partition of the indices into s multi-shares (blocks) of size s:

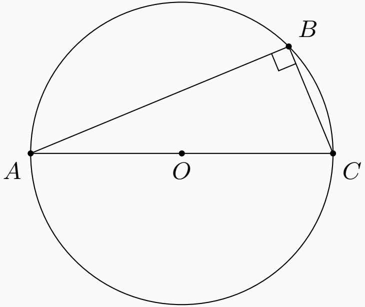
$$\mathbf{A}_i \subseteq [n], \quad |\mathbf{A}_i| = s, \quad \mathbf{A}_i \cap \mathbf{A}_j = \varnothing \ (i \neq j), \quad \bigcup_i \mathbf{A}_i = [n].$$

- Two clusters $C^{(1)} = \{\mathbf{A}_i^{(1)}\}$ and $C^{(2)} = \{\mathbf{A}_j^{(2)}\}$ should be such that for all i, j,

$$\boxed{|\mathbf{A}_i^{(1)} \cap \mathbf{A}_j^{(2)}| = 1}$$

Geometric view. Take $s \times s$ grid points ("shares") as the points of the affine plane. Two parallel classes of lines give exactly such cluster families: lines within a class are parallel (partition), and lines from different classes intersect in one point. This is why our search leads to finite affine geometry.

Euclidean Geometry example



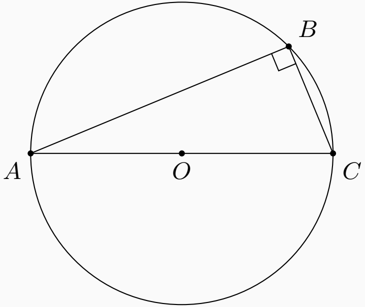


Figure: Thales' Theorem.

- (Mostly) planar geometry concerning points, lines and circles;

1

- (Mostly) planar geometry concerning points, lines and circles;
- Based on postulates:

1

- (Mostly) planar geometry concerning points, lines and circles;
- Based on postulates:

  (I): There is a line between any two points;

[1]

- (Mostly) planar geometry concerning points, lines and circles;
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): Any line can be extended infinitely long;

1

- (Mostly) planar geometry concerning points, lines and circles;
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): Any line can be extended infinitely long;
  - (III): There is a circle for each center and radius;

1

- (Mostly) planar geometry concerning points, lines and circles;
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): Any line can be extended infinitely long;
  - (III): There is a circle for each center and radius;
  - (IV): All right angles are equal;

1

- (Mostly) planar geometry concerning points, lines and circles;
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): Any line can be extended infinitely long;
  - (III): There is a circle for each center and radius;
  - (IV): All right angles are equal;
  - (V): (Parallel postulate) Given a line and a point not on the line, there is a line parallel to it through that point.[1]

[1] This is actually Playfair's axiom, which is equivalent.

- (Mostly) planar geometry concerning points, lines and circles;
- Based on postulates:

(I): There is a line between any two points;
(II): Any line can be extended infinitely long;
(III): There is a circle for each center and radius;
(IV): All right angles are equal;
(V): (Parallel postulate) Given a line and a point not on the line, there is a line parallel to it through that point.

- (Mostly) planar geometry concerning points, lines ~~and circles~~
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): Any line can be extended infinitely long;
  - (III): There is a circle for each center and radius;
  - (IV): All right angles are equal;
  - (V): (Parallel postulate) Given a line and a point not on the line, there is a line parallel to it through that point.

- (Mostly) planar geometry concerning points and lines;
- Based on postulates:
  (I): There is a line between any two points;
  (II): Any line can be extended infinitely long;
  (III): There is a circle for each center and radius;
  (IV): All right angles are equal;
  (V): (Parallel postulate) Given a line and a point not on the line, there is a line parallel to it through that point.

- (Mostly) planar geometry concerning points and lines;
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): Any line can be extended infinitely long;
  - (III): ~~There is a circle for each center and radius;~~
  - (IV): All right angles are equal;
  - (V): (Parallel postulate) Given a line and a point not on the line, there is a line parallel to it through that point.

- (Mostly) planar geometry concerning points and lines;
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): ~~Any line can be extended infinitely long;~~
  - (III): ~~There is a circle for each center and radius;~~
  - (IV): All right angles are equal;
  - (V): (Parallel postulate) Given a line and a point not on the line, there is a line parallel to it through that point.

- (Mostly) planar geometry concerning points and lines;
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): ~~Any line can be extended infinitely long;~~
  - (III): ~~There is a circle for each center and radius;~~
  - (IV): ~~All right angles are equal;~~
  - (V): (Parallel postulate) Given a line and a point not on the line, there is a line parallel to it through that point.

- (Mostly) planar geometry concerning points and lines;
- Based on postulates:
  - (I): There is a line between any two points;
  - (II): ~~Any line can be extended infinitely long;~~
  - (III): ~~There is a circle for each center and radius;~~
  - (IV): ~~All right angles are equal;~~
  - (V): (Playfair's axiom) Given a line ℓ and a point p not on ℓ, there exists a line ℓ' such that $\ell \cap \ell' = \emptyset$ and $p \in \ell'$.

- (Mostly) planar geometry concerning points and lines;
- Based on postulates:

  (I): For any two distinct points, there is a line containing both;

  (II): ~~Any line can be extended infinitely long;~~

  (III): ~~There is a circle for each center and radius;~~

  (IV): ~~All right angles are equal;~~

  (V): (Playfair's axiom) Given a line ℓ and a point p not on ℓ, there exists a line ℓ' such that $\ell \cap \ell' = \emptyset$ and $p \in \ell'$.

Trivial examples

Definition (Finite Pre-Affine plane)

A finite pre-affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V).

Definition (Finite Pre-Affine plane)

A finite pre-affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V).

Example

Let $P = \emptyset$ and $L = \emptyset$.

Definition (Finite Pre-Affine plane)

A finite pre-affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V).

Example

Let $P = \emptyset$ and $L = \emptyset$. Then (P, L) satisfies (I) and (V) and thus is a finite pre-affine plane.

Definition (Finite Pre-Affine plane)

A finite pre-affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V).

Example

Let $P = \emptyset$ and $L = \emptyset$. Then (P, L) satisfies (I) and (V) and thus is a finite pre-affine plane.

Example

Let $P = \{x_1 \ldots, x_n\}$ and $L = \{P\}$ (the line contains all points in P).

Definition (Finite Pre-Affine plane)

A finite pre-affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V).

Example

Let $P = \emptyset$ and $L = \emptyset$. Then (P, L) satisfies (I) and (V) and thus is a finite pre-affine plane.

Example

Let $P = \{x_1 \ldots, x_n\}$ and $L = \{P\}$ (the line contains all points in P). Then (P, L) satisfies (I) and (V) and thus is a finite pre-affine plane.

Non-example and non-trivial example

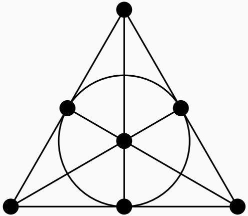


Figure: Fano plane.

Non-example and non-trivial example

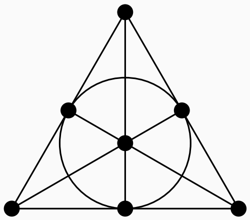


Figure: Fano plane.

The Fano plane has 7 points and 7 lines,

Non-example and non-trivial example

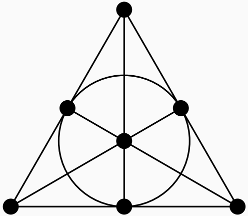


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points,

Non-example and non-trivial example

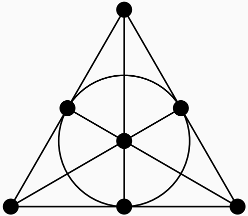


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points, each point lies on 3 lines

Non-example and non-trivial example

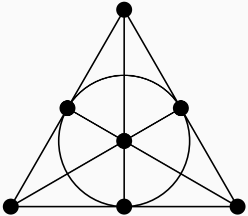


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points, each point lies on 3 lines and all lines intersect.

Non-example and non-trivial example

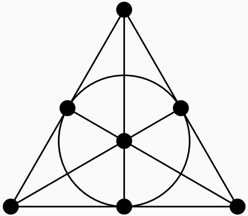


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points, each point lies on 3 lines and all lines intersect. It is actually an example of a projective plane.

Non-example and non-trivial example

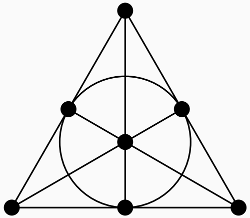
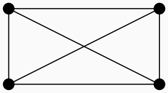


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points, each point lies on 3 lines and all lines intersect. It is actually an example of a projective plane.



Non-example and non-trivial example

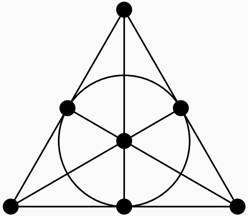
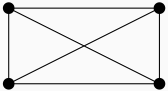


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points, each point lies on 3 lines and all lines intersect. It is actually an example of a projective plane.



This finite pre-affine plane has 4 points,

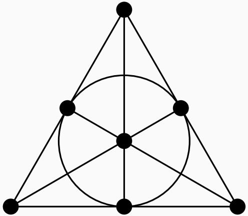
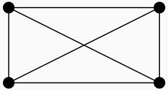


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points, each point lies on 3 lines and all lines intersect. It is actually an example of a projective plane.



This finite pre-affine plane has 4 points, 6 lines,

Non-example and non-trivial example

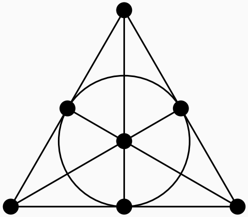
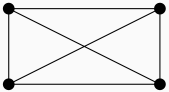


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points, each point lies on 3 lines and all lines intersect. It is actually an example of a projective plane.



This finite pre-affine plane has 4 points, 6 lines, and satisfies postulates (I) and (V).

Definition

A finite affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V)

Definition

A finite affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V) and additionally that there is a set of four points in P such that no three of them are on the same line.

Definition

A finite affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V) and additionally that there is a set of four points in P such that no three of them are on the same line.

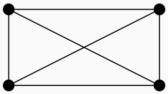


Figure: Affine plane of order 2.

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;
- The number of points per line in a finite affine plane is called the order of the affine plane.

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;
- The number of points per line in a finite affine plane is called the order of the affine plane.
- Let $A = (P, L)$ be an affine plane of order k.

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;
- The number of points per line in a finite affine plane is called the order of the affine plane.
- Let $A = (P, L)$ be an affine plane of order k.
  - Every point is on $k + 1$ lines.

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;
- The number of points per line in a finite affine plane is called the order of the affine plane.
- Let $A = (P, L)$ be an affine plane of order k.
  - Every point is on $k + 1$ lines.
  - A has k^2 points.

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;
- The number of points per line in a finite affine plane is called the order of the affine plane.
- Let $A = (P, L)$ be an affine plane of order k.
  - Every point is on $k + 1$ lines.
  - A has k^2 points.
  - For any line ℓ there are $k - 1$ lines that are parallel to ℓ.

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;
- The number of points per line in a finite affine plane is called the order of the affine plane.
- Let $A = (P, L)$ be an affine plane of order k.
  - Every point is on $k + 1$ lines.
  - A has k^2 points.
  - For any line ℓ there are $k - 1$ lines that are parallel to ℓ.
  - A has $k^2 + k$ lines.

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;
- The number of points per line in a finite affine plane is called the order of the affine plane.
- Let $A = (P, L)$ be an affine plane of order k.
  - Every point is on $k + 1$ lines.
  - A has k^2 points.
  - For any line ℓ there are $k - 1$ lines that are parallel to ℓ.
  - A has $k^2 + k$ lines.
  - A has $k + 1$ sets of parallel lines.

Construction (Coordinatization)

Let $\mathbb{F}$ *be a field and consider* $P := \mathbb{F} \times \mathbb{F}$.

Construction (Coordinatization)

Let $\mathbb{F}$ *be a field and consider* $P := \mathbb{F} \times \mathbb{F}$*. Furthermore, let* $a, b, s \in \mathbb{F}$ *and define* $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ *and* $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$*.*

Construction (Coordinatization)

Let $\mathbb{F}$ *be a field and consider* $P := \mathbb{F} \times \mathbb{F}$. *Furthermore, let* $a, b, s \in \mathbb{F}$ *and define* $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ *and* $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$. *Set* $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a \in \mathbb{F}}$. *Then* (P, L) *is an affine plane of order* $\#\mathbb{F}$.

Construction (Coordinatization)

Let $\mathbb{F}$ be a field and consider $P := \mathbb{F} \times \mathbb{F}$. Furthermore, let $a, b, s \in \mathbb{F}$ and define $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ and $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$. Set $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a \in \mathbb{F}}$. Then (P, L) is an affine plane of order $\#\mathbb{F}$.

Example (Affine plane of order 2)

Construction (Coordinatization)

Let $\mathbb{F}$ be a field and consider $P := \mathbb{F} \times \mathbb{F}$. Furthermore, let $a, b, s \in \mathbb{F}$ and define $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ and $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$. Set $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a \in \mathbb{F}}$. Then (P, L) is an affine plane of order $\#\mathbb{F}$.

Example (Affine plane of order 2)

Let $P := \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

Coordinatization of finite affine planes

Construction (Coordinatization)

Let $\mathbb{F}$ *be a field and consider* $P := \mathbb{F} \times \mathbb{F}$*. Furthermore, let* $a, b, s \in \mathbb{F}$ *and define* $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ *and* $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$*. Set* $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a \in \mathbb{F}}$*. Then* (P, L) *is an affine plane of order* $\#\mathbb{F}$*.*

Example (Affine plane of order 2)

Let $P := \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

Figure: P.

Construction (Coordinatization)

Let $\mathbb{F}$ be a field and consider $P := \mathbb{F} \times \mathbb{F}$. Furthermore, let $a, b, s \in \mathbb{F}$ and define $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ and $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$. Set $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a \in \mathbb{F}}$. Then (P, L) is an affine plane of order $\#\mathbb{F}$.

Example (Affine plane of order 2)

Let $P := \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

$\ell_0 \quad := \{(0, 0), (0, 1)\}; \quad \ell_1 \quad := \{(1, 0), (1, 1)\};$

Figure: P and first two lines.

Construction (Coordinatization)

Let $\mathbb{F}$ be a field and consider $P := \mathbb{F} \times \mathbb{F}$. Furthermore, let $a, b, s \in \mathbb{F}$ and define $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ and $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$. Set $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a \in \mathbb{F}}$. Then (P, L) is an affine plane of order $\#\mathbb{F}$.

Example (Affine plane of order 2)

Let $P := \{(0,0),(0,1),(1,0),(1,1)\}$.

$\ell_0 \quad := \{(0,0),(0,1)\}$; $\quad \ell_1 \quad := \{(1,0),(1,1)\}$;
$\ell_{0,0} := \{(0,0),(1,0)\}$; $\quad \ell_{0,1} := \{(0,1),(1,1)\}$;

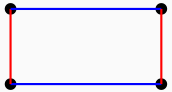


Figure: P and first four lines.

Construction (Coordinatization)

Let $\mathbb{F}$ be a field and consider $P := \mathbb{F} \times \mathbb{F}$. Furthermore, let $a, b, s \in \mathbb{F}$ and define $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ and $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$. Set $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a \in \mathbb{F}}$. Then (P, L) is an affine plane of order $\#\mathbb{F}$.

Example (Affine plane of order 2)

Let $P := \{(0,0), (0,1), (1,0), (1,1)\}$.

$\ell_0 \;\; := \{(0,0), (0,1)\}$; $\quad \ell_1 \;\; := \{(1,0), (1,1)\}$;
$\ell_{0,0} := \{(0,0), (1,0)\}$; $\quad \ell_{0,1} := \{(0,1), (1,1)\}$;
$\ell_{1,0} := \{(0,0), (1,1)\}$; $\quad \ell_{1,1} := \{(0,1), (1,0)\}$.

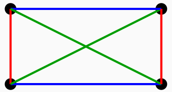


Figure: All points and lines.

Construction (Coordinatization)

Let $\mathbb{F}$ be a field and consider $P := \mathbb{F} \times \mathbb{F}$. Furthermore, let $a, b, s \in \mathbb{F}$ and define $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ and $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$. Set $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a\in\mathbb{F}}$. Then (P, L) is an affine plane of order $\#\mathbb{F}$.

Example (Affine plane of order 2)

Let $P := \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

$\ell_0 := \{(0, 0), (0, 1)\}$; $\ell_1 := \{(1, 0), (1, 1)\}$;
$\ell_{0,0} := \{(0, 0), (1, 0)\}$; $\ell_{0,1} := \{(0, 1), (1, 1)\}$;
$\ell_{1,0} := \{(0, 0), (1, 1)\}$; $\ell_{1,1} := \{(0, 1), (1, 0)\}$.

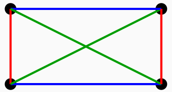


Figure: Affine plane of order 2.

Parallel lines

- Lines ℓ_a are parallel;

Parallel lines

- Lines ℓ_a are parallel;
- Lines in $\{\ell_{s,b} \mid b \in \mathbb{F}\}$ are parallel for each slope s.

Parallel lines

- Lines ℓ_a are parallel;
- Lines in $\{\ell_{s,b} \mid b \in \mathbb{F}\}$ are parallel for each slope s.
- We say that the lines ℓ_a have slope ∞.

Example

A finite affine plane of order 4. We take $\mathbb{F} := \mathbb{F}_2[X]/(X^2 + X + 1)$:

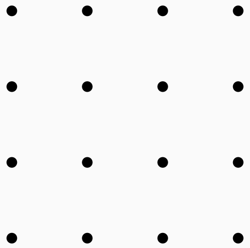


Figure: Points in $\mathbb{F}^2$

Example

A finite affine plane of order 4. We take $\mathbb{F} := \mathbb{F}_2[X]/(X^2 + X + 1)$:

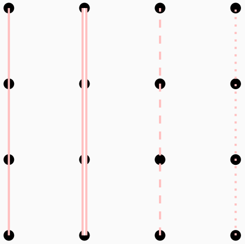


Figure: Lines of slope ∞.

Example

A finite affine plane of order 4. We take $\mathbb{F} := \mathbb{F}_2[X]/(X^2 + X + 1)$:

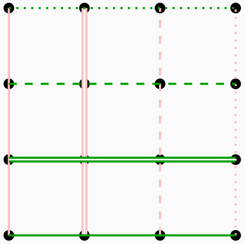


Figure: Lines of slope ∞ and 0.

Example

A finite affine plane of order 4. We take $\mathbb{F} := \mathbb{F}_2[X]/(X^2 + X + 1)$:

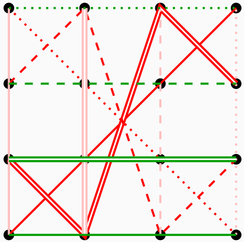


Figure: Lines of slope ∞, 0 and 1.

Example

A finite affine plane of order 4. We take $\mathbb{F} := \mathbb{F}_2[X]/(X^2 + X + 1)$:

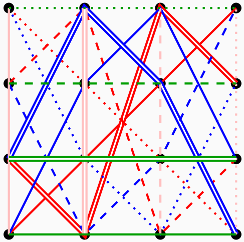


Figure: Lines of slope ∞, 0, 1 and x.

Example

A finite affine plane of order 4. We take $\mathbb{F} := \mathbb{F}_2[X]/(X^2 + X + 1)$:

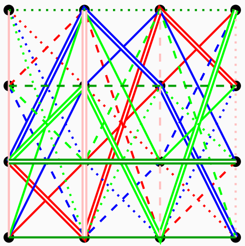


Figure: Lines of slope ∞, 0, 1, x and $x + 1$.

Example

A finite affine plane of order 4. We take $\mathbb{F} := \mathbb{F}_2[X]/(X^2 + X + 1)$:

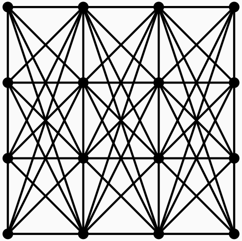


Figure: A finite affine plane of order 4.

Definition (Cluster)

Let X be a set of $n = s^2$ elements. A cluster C is a partition of X in s sets of equal size s.

Definition (Cluster)

Let X be a set of $n = s^2$ elements. A cluster C is a partition of X in s sets of equal size s.

Definition (MNO clusters)

Let C^1 and C^2 be two clusters of X, then they are maximally non-overlapping (MNO)

Definition (Cluster)

Let X be a set of $n = s^2$ elements. A cluster C is a partition of X in s sets of equal size s.

Definition (MNO clusters)

Let C^1 and C^2 be two clusters of X, then they are maximally non-overlapping (MNO) if given any set $c \in C^1$ and any set $d \in C^2$, we have $|c \cap d| = 1$.

Definition (Cluster)

Let X be a set of $n = s^2$ elements. A cluster C is a partition of X in s sets of equal size s.

Definition (MNO clusters)

Let C^1 and C^2 be two clusters of X, then they are maximally non-overlapping (MNO) if given any set $c \in C^1$ and any set $d \in C^2$, we have $|c \cap d| = 1$.

Definition (SMNO clusters)

Let $\mathfrak{C}$ be a collection of clusters. Then $\mathfrak{C}$ is called a collection of simultaneous MNO clusters

Definition (Cluster)

Let X be a set of $n = s^2$ elements. A cluster C is a partition of X in s sets of equal size s.

Definition (MNO clusters)

Let C^1 and C^2 be two clusters of X, then they are maximally non-overlapping (MNO) if given any set $c \in C^1$ and any set $d \in C^2$, we have $|c \cap d| = 1$.

Definition (SMNO clusters)

Let $\mathfrak{C}$ be a collection of clusters. Then $\mathfrak{C}$ is called a collection of simultaneous MNO clusters if each pair of clusters in $\mathfrak{C}$ is MNO.

Maximum number of SMNO clusters

- Assume we have a finite affine plane $A = (P, L)$ of order s;

Maximum number of SMNO clusters

- Assume we have a finite affine plane $A = (P, L)$ of order s;
- Any set s of parallel lines is a cluster of P;

- Assume we have a finite affine plane $A = (P, L)$ of order s;
- Any set s of parallel lines is a cluster of P;

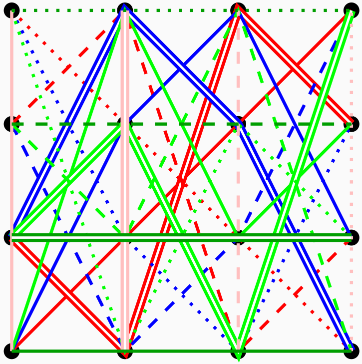


Figure: Example for $s = 4$.

Maximum number of SMNO clusters

- Assume we have a finite affine plane $A = (P, L)$ of order s;
- Any set s of parallel lines is a cluster of P;
- Then any two clusters so obtained are MNO;

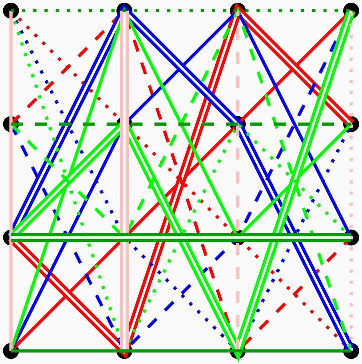


Figure: Example for $s = 4$.

Maximum number of SMNO clusters

- Assume we have a finite affine plane $A = (P, L)$ of order s;
- Any set s of parallel lines is a cluster of P;
- Then any two clusters so obtained are MNO;
- Then we obtain $s + 1$ SMNO clusters.

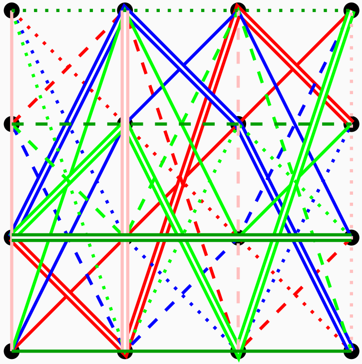


Figure: Example for $s = 4$.

Maximum number of SMNO clusters

- Assume we have a finite affine plane $A = (P, L)$ of order s;
- Any set s of parallel lines is a cluster of P;
- Then any two clusters so obtained are MNO;
- Then we obtain $s + 1$ SMNO clusters.
- Known to be possible for all prime powers ($s = p^k$).

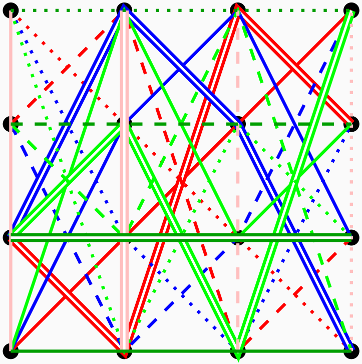


Figure: Example for $s = 4$.

- For $n = s^2$ where s is a prime power, there exist exactly $s + 1$ simultaneous MNO (SMNO) clusters over an n-sharing.

- For $n = s^2$ where s is a prime power, there exist exactly $s + 1$ simultaneous MNO (SMNO) clusters over an n-sharing.
- A cluster that has a missing multi-share can not be completed with less than $s - 1$ multi share from other clusters.

Properties of Clustering

- For $n = s^2$ where s is a prime power, there exist exactly $s+1$ simultaneous MNO (SMNO) clusters over an n-sharing.
- A cluster that has a missing multi-share can not be completed with less than $s-1$ multi share from other clusters.
- Let s be an odd prime power, and let $n = s^2$. Consider all sums:

$$\bigoplus \mathbf{A}_j^h \quad \text{for} \quad 0 \leq h \leq s, \quad 0 \leq j \leq s-1,$$

where $\mathbf{A}_j^h$ denotes the j-th multi-share from the h-th SMNO cluster of an n-sharing $\mathbf{X}$. Then, the rank of the resulting system of linear (parity) relations is n.

Our Multiplication Gadget

The gadget is deterministic and uniform, and it is secure against up to $d = s - 1$ glitch-extended probes.

Our Multiplication Gadget

The gadget is deterministic and uniform, and it is secure against up to $d = s - 1$ glitch-extended probes.

$$
\begin{aligned}
\alpha &= \lfloor k/s \rfloor, \\
\beta &= \mathrm{mod}(k, s), \\
R_k &= \bigoplus_{i=0}^{s-1} \Big({\mathbf{A}^{0}}_{\alpha}(\mathbf{X})[i] \oplus {\mathbf{A}^{\alpha+1}}_{\beta}(\mathbf{X})[i] \oplus {\mathbf{A}^{0}}_{\alpha}(\mathbf{Y})[i] \oplus {\mathbf{A}^{\alpha+1}}_{\beta}(\mathbf{Y})[i] \Big), \\
W_k &= {\mathbf{A}^{0}}_{\alpha}(\mathbf{X}) \otimes {\mathbf{A}^{\alpha+1}}_{\beta}(\mathbf{Y}), \\
Z_k &= R_k \oplus W_k.
\end{aligned}
$$

Here, $\mathbf{A}_j^h(\cdot)$ denotes the j-th multi-share from the h-th SMNO cluster applied to the input sharing.

Other Applications of Clustering

- For $d = 2$ security, our multiplication gadget requires $n = 9$ shares — which is not practically interesting.

Other Applications of Clustering

- For $d = 2$ security, our multiplication gadget requires $n = 9$ shares — which is not practically interesting.
- However, the clustering approach is also applicable to protecting the nonlinear layer χ_5.

Other Applications of Clustering

- For $d = 2$ security, our multiplication gadget requires $n = 9$ shares — which is not practically interesting.
- However, the clustering approach is also applicable to protecting the nonlinear layer χ_5.
- We constructed a uniform and deterministic χ_5 gadget using only $n = 4$ shares that achieves $d = 3$ probing security.

Other Applications of Clustering

- For $d = 2$ security, our multiplication gadget requires $n = 9$ shares — which is not practically interesting.
- However, the clustering approach is also applicable to protecting the nonlinear layer χ_5.
- We constructed a uniform and deterministic χ_5 gadget using only $n = 4$ shares that achieves $d = 3$ probing security.
- Previously, such gadgets were only known for $d = 1$ and $d = 2$.

Other Applications of Clustering

- For $d = 2$ security, our multiplication gadget requires $n = 9$ shares — which is not practically interesting.
- However, the clustering approach is also applicable to protecting the nonlinear layer χ_5.
- We constructed a uniform and deterministic χ_5 gadget using only $n = 4$ shares that achieves $d = 3$ probing security.
- Previously, such gadgets were only known for $d = 1$ and $d = 2$.
- This construction enables a fully deterministic masking of ASCON with $d = 3$ security — a new milestone.

Other Applications of Clustering

- For $d = 2$ security, our multiplication gadget requires $n = 9$ shares — which is not practically interesting.
- However, the clustering approach is also applicable to protecting the nonlinear layer χ_5.
- We constructed a uniform and deterministic χ_5 gadget using only $n = 4$ shares that achieves $d = 3$ probing security.
- Previously, such gadgets were only known for $d = 1$ and $d = 2$.
- This construction enables a fully deterministic masking of ASCON with $d = 3$ security — a new milestone.

Thank you for your attention!