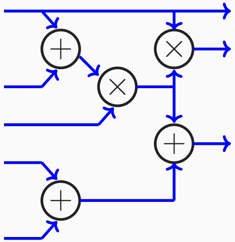
Radbound University

An Algebraic Approach for Evaluating Random Probing Security With Application to AES

Vahid Jahandideh, Bart Mennink, Lejla Batina
Radboud University (The Netherlands)

CHES 2024
September 4–7, 2024

- Typical side-channel attacks target a single sensitive variable.
- Advanced attacks combine leakages of multiple variables.
- The Random Probing Model (RPM) considers leakages of all variables.



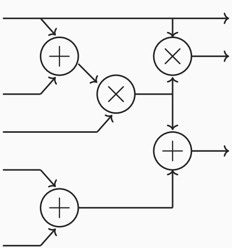
Random Probing Model

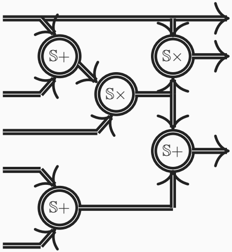
In this leakage model, each variable of the (protected) circuit leaks independently with a fixed probability p.

Boolean Masking

Masking circuit C includes the following three steps.

- Native inputs are n-shared, which is for a variable v to encode it with a random n-tuple as $V = (v_1, \ldots, v_n)$ such that $\bigoplus_{i=1}^{n} v_i = v$.
- Gates are replaced with gadgets. Gadgets work on n-sharings. For a gate G, we denote the corresponding gadget with $\mathbb{S}$G.
- To maintain security, a refresh gadget may be inserted at some gadget's input (or output) interface.





Security Definition

Maximum A posteriori Probability (MAP) decision for the value of native $v \in \mathbb{F}_q$ given RPM leakage $\mathcal{L}(n,p)$ is

$$\widetilde{v} = \operatorname*{argmax}_{\alpha \in \mathbb{F}_q} \Pr(v = \alpha \mid \mathcal{L}(n,p)).$$

We define the advantage of the adversary over random guessing as

$$\mathsf{Adv}_v(n,p) \triangleq \Pr(\widetilde{v} = v) - \frac{1}{q}.$$

RPM Security

A circuit family $\mathbb{S}\mathrm{C}$ that processes a native variable v is secure in the RPM framework if there exists a threshold p^o such that, given leakage $\mathcal{L}(n,p)$ with $p \leq p^o$, $\mathsf{Adv}_v(n,p)$ monotonically decreases to 0 as n increases.

We develop a framework to estimate $\mathrm{Adv}(\mathrm{n}, \mathrm{p})$ for various gadgets and circuits.

Open Challenges in the RPM:

- For typical masked circuits, security holds only if p decreases as n increases.
- In some works, derivation of security bound requires leak-free refresh gadget.
- Derived security bound usually depends on the complexity of $\mathbb{S}\mathsf{C}$.

Expansion Method (State-of-the-Art Approach):

- Works by iteratively masking the circuit:

$$\mathsf{C} \longrightarrow \mathbb{S}\mathsf{C} \longrightarrow \mathbb{S}(\mathbb{S}\mathsf{C}) \longrightarrow \mathbb{S}(\mathbb{S}(\mathbb{S}\mathsf{C})) \longrightarrow \ldots$$

- It can create a circuit secure at constant p (independent of n) leakage.
- It adds too much to the complexity of the final protected circuit.

Linear Circuits as Building Blocks

- Linear circuit $\mathbb{S}\mathsf{C}$ acts as an erasure channel with parameter $\mathsf{E}_{\mathbb{S}\mathsf{C}}(n, p)$.

$$\mathbb{S}\mathsf{C}, \mathcal{L}(n,p) \longrightarrow \boxed{\text{Adversary}} \longrightarrow \begin{cases} v & \text{with probability } \mathsf{E}_{\mathbb{S}\mathsf{C}}(n,p), \\ \perp & \text{otherwise.} \end{cases}$$

Figure: Erasure channel models leakage of linear circuit processing native v.

Relation of the Metrics

When the adversary learns nothing, it still has the opportunity to guess the value of v. Therefore, we have:

$$\mathsf{Adv}_v(n,p) = \mathsf{E}_{\mathbb{S}\mathsf{C}}(n,p) + \frac{1}{q}[1 - \mathsf{E}_{\mathbb{S}\mathsf{C}}(n,p)] - \frac{1}{q} = \frac{q-1}{q}\mathsf{E}_{\mathbb{S}\mathsf{C}}(n,p).$$

Estimating $\mathrm{E}_{\mathbb{S}\mathsf{C}}(\mathrm{n}, \mathrm{p})$ (1/3)

We deploy a Monte Carlo approach to estimate $\mathsf{E}_{\mathbb{S}\mathsf{C}}(n, p)$.

- For each n, there is matrix $\mathbf{P}_n$ such that

  $$\mathbf{P}_n \cdot [v, \Sigma_{\mathbb{S}\mathsf{C}}]^\top = \mathbf{0},$$

  where $\Sigma_{\mathbb{S}\mathsf{C}}$ is the list of intermediates of $\mathbb{S}\mathsf{C}$.
- The rows of $\mathbf{P}_n$ are linearly independent.
- With substituting leakage L, this system of equations transforms into:

  $$\mathbf{P}_n^r \cdot [v, \Sigma_{\mathbb{S}\mathsf{C}}]^\top = \mathbf{b},$$

  with some known vector $\mathbf{b}$.
- By finding the set of solutions, the adversary can estimate the value of v.

Estimating $\mathrm{E}_{\mathbb{SC}}(\mathrm{n}, \mathrm{p})$ (2/3)

- The system

$$\mathbf{P}_n^r \cdot [v, \Sigma_{\mathbb{SC}}]^\top = \mathbf{b},$$

  by computing the row-echelon form, transforms into

$$\mathbf{G} \cdot [v, \Sigma_{\mathbb{SC}}]^\top = \mathbf{c}.$$

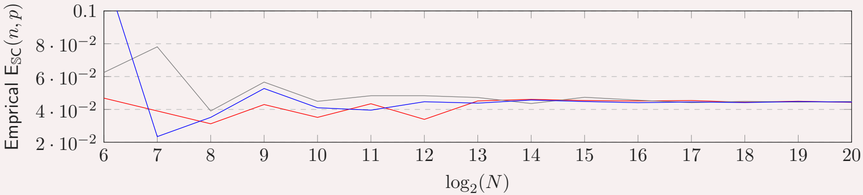
- Since it is in a finite field, it has bounded amount of solutions.
- v is always a pivot variable in $\mathbf{G}$.
- This system either uniquely determines v or gives no information about it.
- This behavior is determined by the structure of the row containing v.
- And is independent of $\mathbf{b}$. Hence, it is independent of leakage values.

Each instance of leakage L will result in a new matrix $\mathbf{G}$. By placing v in the first column if the first row of $\mathbf{G}$ has no free variables, v will be determined. Therefore, we have the following equality:

$$\mathsf{E}_{\mathbb{SC}}(n,p) = \Pr_{L \leftarrow \mathcal{L}(n,p)} [\mathbf{G}(1, 2 : \mathsf{end}) = \mathbf{0}].$$

Monte Carlo Method

To estimate the probability of an event e, the Monte Carlo method repeats the procedure N times, records the number of times e occurs, and returns N_e/N. As N increases, the error of estimation decreases.



Alternative Way of Reporting the Results

- We can derive a 2D table of estimations (one entry for each targeted (n, p)).
- This limits the applicability of the results in more sophisticated compositions.
- For typical gadgets, estimated $\mathsf{E}_{\mathbb{S}\mathsf{C}}(n, p)$ decays exponentially with n.

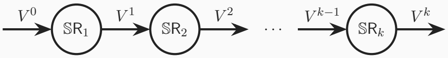
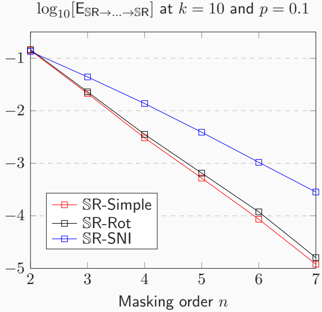


Figure: Multiple gadgets cascaded.



- Therefore, we try to express estimations as $\mathsf{E}_{\mathbb{S}\mathsf{C}}(n, p) < \alpha(\beta p)^{\gamma n}$ for some α, β, and $\gamma < 1$ constants. This expression might not hold out of the tested region.

Compositions (1/3)

- Refresh gadget $\mathbb{S}\mathsf{R}$ can help to decompose RPM security of a compound circuit to the RPM security of the composing gadgets.

$$\boxed{\mathbb{S}\mathsf{G}_1} \xrightarrow{V^0} \mathbb{S}\mathsf{R} \xrightarrow{V^1} \boxed{\mathbb{S}\mathsf{G}_2}$$

RPM Composition Theorem

For a bounded region of p values, the gadgets, and hence the composition, behave as an erasure channel for which

$$\mathsf{E}_{\mathbb{S}\mathsf{G}_1 \to \mathbb{S}\mathsf{R} \to \mathbb{S}\mathsf{G}_2}(n,p) \leq \mathsf{E}_{\mathbb{S}\mathsf{G}_1}(n,p') + \mathsf{E}_{\mathbb{S}\mathsf{R}}(n,p) + \mathsf{E}_{\mathbb{S}\mathsf{G}_2}(n,p')$$

holds, where $p' \geq p$ is a function of (n,p) and the structure of $\mathbb{S}\mathsf{R}$.

Compositions (2/3)

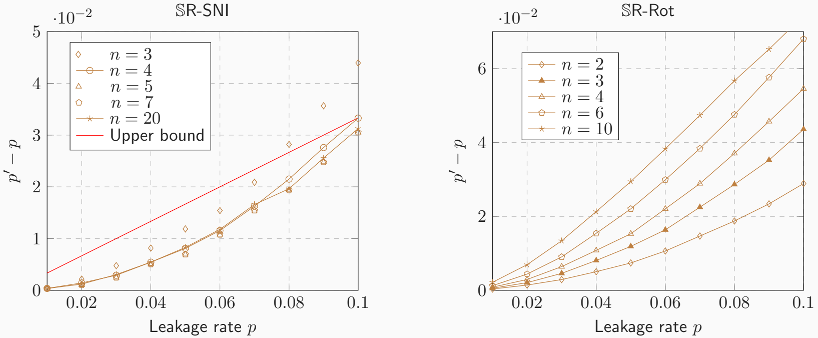
- Our main technique is to process parity relations inside $\mathbb{S}\mathsf{R}$ as follows:

$$\boxed{\mathbb{S}\mathsf{G}_1} \xrightarrow{V^0} \begin{cases} \mathrm{L}_1(\Sigma^r_{\mathbb{S}\mathsf{R}}) = \mathrm{L}_2(V^{0,r}, V^{1,r}, v) \oplus \mathbf{b}_1, \\ \mathrm{L}_3(V^{0,r}, V^{1,r}, v) = \mathbf{b}_2. \end{cases} \xrightarrow{V^1} \boxed{\mathbb{S}\mathsf{G}_2}$$

Figure: Processing parity relations inside the refresh gadget.

- L_1, L_2, and L_3 are linear relations. Superscript ^{r} denotes unknowns after substituting leakage, $\mathbf{b}_1$ and $\mathbf{b}_2$ are constant vectors.
- Equations in L_1 are independent.
- The upper subsystem has no impact on the posterior distribution of native v.
- We let the adversary learn the remaining boundary unknowns of the lower subsystem.
- This is equivalent to some extra leakage on the input/output shares.

- For a $\mathbb{S}$R-SNI refresh gadget, our numerical computations give an estimation as $p' \approx p + \frac{1}{3}p$ for $n \geq 3$ and $p \leq 0.1$.



- For the other tested $\mathbb{S}$R gadget, p' is increasing with n for any p.

Multiplication Gadgets (1/2)

- For $\mathbb{S}$AND gadgets, we deploy linearization to derive a lower bound and upper bound on the adversary's post-leakage information.

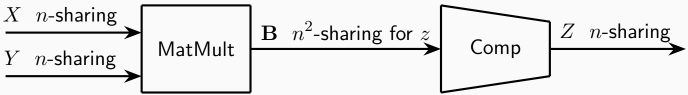


Figure: Typical multiplication gadget.

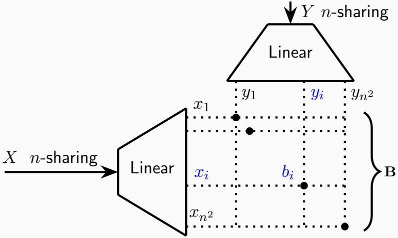
- If the compression block Comp behaves as a refresh gadget, we can use the composition theorem as:

$$\mathsf{E}_{\mathsf{MatMult} \to \mathsf{Comp}}(n, p) \leq \mathsf{E}_{\mathsf{MatMult}}(n, p') + \mathsf{E}_{\mathsf{Comp}}(n, p).$$

Here, p' exceeds p and depends on the structure of Comp.

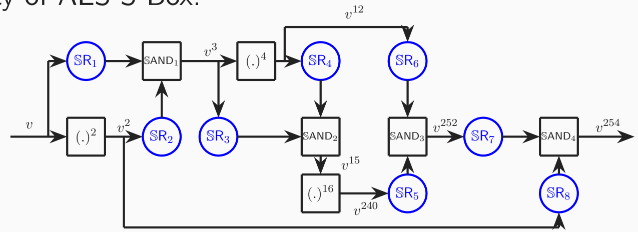
Multiplication Gadgets (2/2)

- MatMult is non-linear. The operations inside it can be arranged as follows.



- $b_i - x_i y_i = 0$ is the only non-linear relation. b_i is not involved in any parity equation other than this relation.
- If we ignore leakage of b_i, non-linear relations will disappear. This will reduce the advantage of the adversary. Hence, the derived bound, denoted $\mathsf{E}^{-}_{\mathsf{MatMult}}(n, p)$, will be a lower bound.
- If we force both x_i and y_i to leak on the leakage of b_i, we derive $\mathsf{E}^{+}_{\mathsf{MatMult}}(n, p)$.
- For $\mathbb{S}$AND-Rec, E^{+} and E^{-} are exponentially decaying with n for $p \leq 0.07$.

The RPM security of AES S-Box.



Security Bound

Using the composition theorem, we can derive the following bound:

$$\mathsf{E}_{\mathbb{S}\text{S-box}}(n,p) \leq 8\mathsf{E}_{\mathbb{S}\mathsf{R}}(n,p) + 3\mathsf{E}_{\mathbb{S}\mathsf{AND}}(n,p') + \mathsf{E}_{\mathbb{S}\mathsf{AND}}(n,p'').$$

This bound directly depends on the complexity of the S-box.

- Unlike the bound for protected S-box, our security bound for the whole protected AES does not depend on the number of gates in AES.

Conclusion

- We defined a metric for RPM security and established a framework for evaluating it.
- We demonstrated how to handle leakage of refresh gadgets. This gives a composition theorem, which is inherent to RPM.
- Our work provides a clearer relationship between circuit complexity and RPM security.
- However, the final numerical relations are derived with Monte Carlo estimations.
- An interesting follow-up work would be to analytically sketch these probabilities and verify the estimations.

Thank you for your attention!