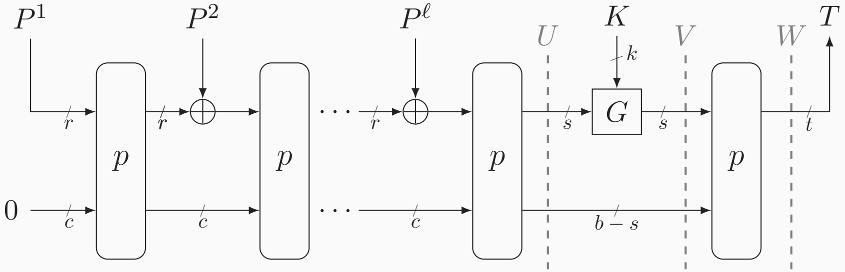
# Tightening Leakage Resilience of the Suffix Keyed Sponge

Henk Berendsen and Bart Mennink
Radboud University (The Netherlands)
FSE 2024
March 27, 2024

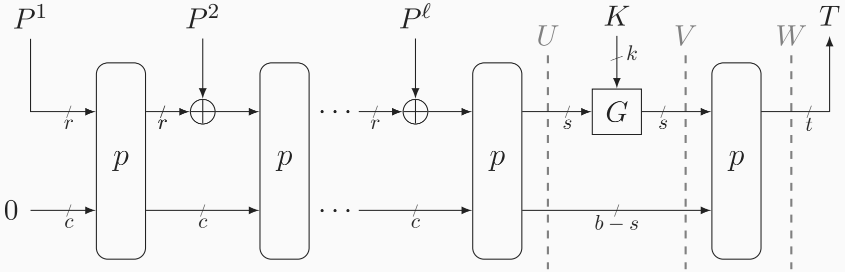
# Introduction

# The Suffix Keyed Sponge (SuKS)




- MAC function based on the sponge hash function [BDPV07]
- Used in NIST LWC finalist ISAP [DEM+21]
- Formal analysis by Dobraunig and Mennink [DM19]

# The Suffix Keyed Sponge (SuKS)




- MAC function based on the sponge hash function [BDPV07]
- Used in NIST LWC finalist ISAP [DEM⁺21]
- Formal analysis by Dobraunig and Mennink [DM19]
- Security proof involves *multicollisions*

# Multicollision Limit Function

## Idea

- Upper bound on size of the largest multicollision
- Formalised by Daemen et al. [DMV17] using a balls-and-bins experiment

## Idea

- Upper bound on size of the largest multicollision
- Formalised by Daemen et al. [DMV17] using a balls-and-bins experiment

## Definition

- $q$ balls, $2^r$ bins
- $\mu^q_{r,c}$ is smallest $x$ such that $\mathbf{Pr}\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

## Idea

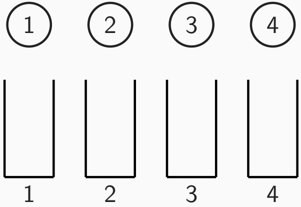
- Upper bound on size of the largest multicollision
- Formalised by Daemen et al. [DMV17] using a balls-and-bins experiment

## Definition

- $q$ balls, $2^r$ bins
- $\mu^q_{r,c}$ is smallest $x$ such that $\mathbf{Pr}\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

## Toy Example

- $q = 4$ balls
- $2^r = 4$ bins



# Multicollision Limit Function

## Idea

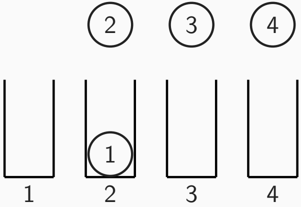
- Upper bound on size of the largest multicollision
- Formalised by Daemen et al. [DMV17] using a balls-and-bins experiment

## Definition

- $q$ balls, $2^r$ bins
- $\mu^q_{r,c}$ is smallest $x$ such that $\mathbf{Pr}\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

## Toy Example

- $q = 4$ balls
- $2^r = 4$ bins



## Idea

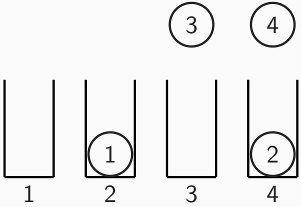
- Upper bound on size of the largest multicollision
- Formalised by Daemen et al. [DMV17] using a balls-and-bins experiment

## Definition

- $q$ balls, $2^r$ bins
- $\mu^q_{r,c}$ is smallest $x$ such that $\mathbf{Pr}\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

## Toy Example

- $q = 4$ balls
- $2^r = 4$ bins



# Multicollision Limit Function

## Idea

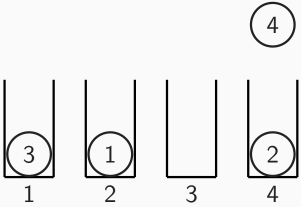
- Upper bound on size of the largest multicollision
- Formalised by Daemen et al. [DMV17] using a balls-and-bins experiment

## Definition

- $q$ balls, $2^r$ bins
- $\mu^q_{r,c}$ is smallest $x$ such that $\mathbf{Pr}\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

## Toy Example

- $q = 4$ balls
- $2^r = 4$ bins



## Idea

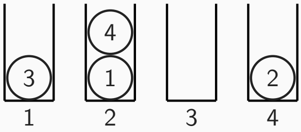
- Upper bound on size of the largest multicollision
- Formalised by Daemen et al. [DMV17] using a balls-and-bins experiment

## Definition

- $q$ balls, $2^r$ bins
- $\mu^q_{r,c}$ is smallest $x$ such that $\mathbf{Pr}\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

## Toy Example

- $q = 4$ balls
- $2^r = 4$ bins



### Black Box Security Bound [DM19]

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

# Security of the SuKS

**Tight Black Box Security Bound [DM19, DM20]**

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

### Tight Black Box Security Bound [DM19, DM20]

$$\mathbf{Adv}_{F}^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

### Leakage Resilience Security Bound [DM19]

$$\mathbf{Adv}_{F,\mathcal{L}}^{\mathrm{nalr\text{-}prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}-\mu_{s,b-s}^{2(N-q)}\lambda}} + \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}} + \frac{\mu_{s,b-s}^{2(N-q)}}{2^{b-s}}$$

**Tight Black Box Security Bound [DM19, DM20]**

$$\mathbf{Adv}_{F}^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

**Leakage Resilience Security Bound [DM19]**

$$\mathbf{Adv}_{F,\mathcal{L}}^{\mathrm{nalr\text{-}prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}-\mu_{s,b-s}^{2(N-q)}\lambda}} + \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}} + \frac{\mu_{s,b-s}^{2(N-q)}}{2^{b-s}}$$

**This work: analyse tightness of leakage resilience security bound**

**Tight Black Box Security Bound [DM19, DM20]**

$$\mathbf{Adv}_{F}^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

**Leakage Resilience Security Bound [DM19]**

$$\mathbf{Adv}_{F,\mathcal{L}}^{\mathrm{nalr\text{-}prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}-\mu_{s,b-s}^{2(N-q)}\lambda}} + \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}} + \frac{\mu_{s,b-s}^{2(N-q)}}{2^{b-s}}$$

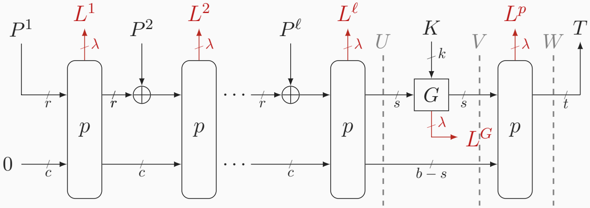
**This work: analyse tightness of leakage resilience security bound**

**This presentation: focus on third term in the bounds**

# Non-adaptive Leakage Resilience

- Leakage incurred by every *primitive* evaluation
  - Leakage modelled as function of primitive input and output
  - Non-adaptive: leakage function does not change
  - Bounded: at most $\lambda$ bits of leakage per primitive evaluation

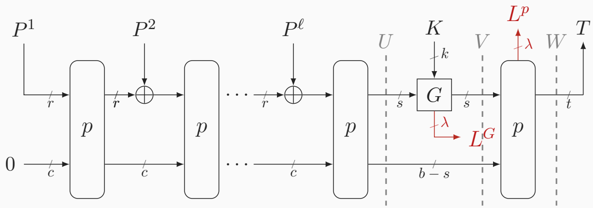
- Leakage incurred by every *primitive* evaluation
  - Leakage modelled as function of primitive input and output
  - Non-adaptive: leakage function does not change
  - Bounded: at most $\lambda$ bits of leakage per primitive evaluation




- Applying leakage model to SuKS:

# Non-adaptive Leakage Resilience

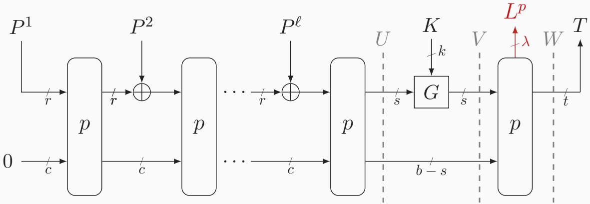
- Leakage incurred by every *primitive* evaluation
  - Leakage modelled as function of primitive input and output
  - Non-adaptive: leakage function does not change
  - Bounded: at most $\lambda$ bits of leakage per primitive evaluation




- Applying leakage model to SuKS:
  - Key blended into state *at the end*: no leakage in absorption phase

# Non-adaptive Leakage Resilience

- Leakage incurred by every *primitive* evaluation
  - Leakage modelled as function of primitive input and output
  - Non-adaptive: leakage function does not change
  - Bounded: at most $\lambda$ bits of leakage per primitive evaluation




- Applying leakage model to SuKS:
  - Key blended into state *at the end*: no leakage in absorption phase
  - Function $G$ assumed to be *strongly protected*

# Tightness Analysis

## Black Box Matching Attack

- Recall: black box and leakage resilience bounds are very similar

$$\frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}} \quad \text{versus} \quad \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}}$$

- Tightness: there exists an attack matching the leakage resilience bound
- Try creating such an attack based on the tight black box attack

## Black Box Matching Attack

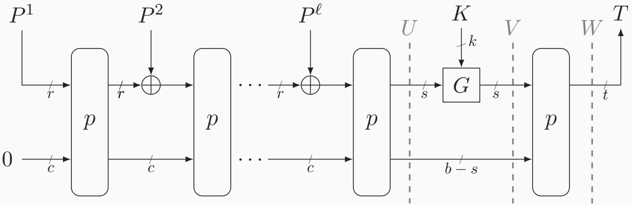
- Recall: black box and leakage resilience bounds are very similar

$$\frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}} \quad \text{versus} \quad \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}}$$

- Tightness: there exists an attack matching the leakage resilience bound
- Try creating such an attack based on the tight black box attack

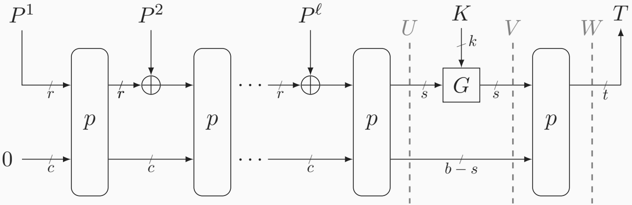
## Attacker Capabilities

- Attacker can make $q$ construction queries

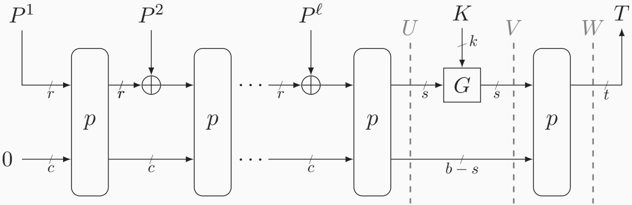



- Attacker wants to recover the state $W$ for one construction query
  - With $N$ guesses, success probability is $\frac{N}{2^{b-t}}$

# Black Box Attack Intuition

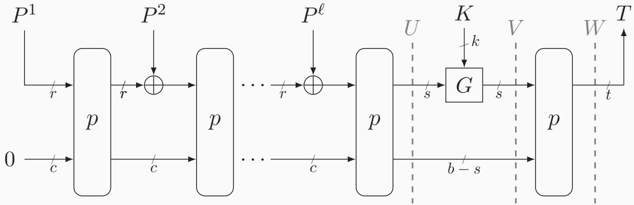



- Attacker wants to recover the state $W$ for one construction query
  - With $N$ guesses, success probability is $\frac{N}{2^{b-t}}$
  - With $\mu$ queries colliding in $T$, success probability is $\frac{\mu \cdot N}{2^{b-t}}$




$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \lesssim \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

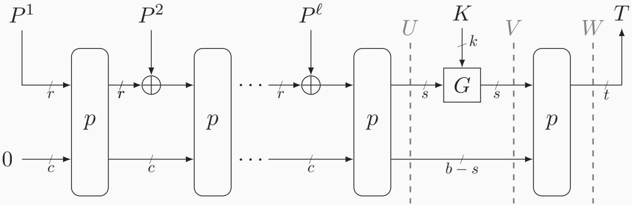
- Attacker wants to recover the state $W$ for one construction query
  - With $N$ guesses, success probability is $\frac{N}{2^{b-t}}$
  - With $\mu$ queries colliding in $T$, success probability is $\frac{\mu \cdot N}{2^{b-t}}$
- $\mu$ is bounded by multicollision limit function $\mu_{t,b-t}^{2q}$




$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \lesssim \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

- Attacker wants to recover the state $W$ for one construction query
  - With $N$ guesses, success probability is $\frac{N}{2^{b-t}}$
  - With $\mu$ queries colliding in $T$, success probability is $\frac{\mu \cdot N}{2^{b-t}}$
- $\mu$ is bounded by multicollision limit function $\mu_{t,b-t}^{2q}$
  - Each of the $2^t$ bins represents a tag value

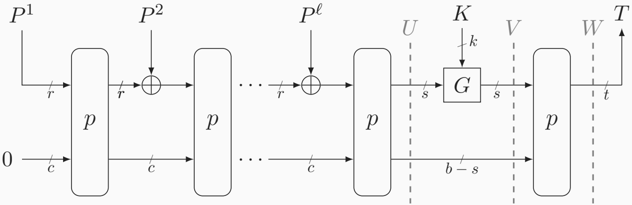
# Black Box Attack Intuition




$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \lesssim \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

- Attacker wants to recover the state $W$ for one construction query
  - With $N$ guesses, success probability is $\frac{N}{2^{b-t}}$
  - With $\mu$ queries colliding in $T$, success probability is $\frac{\mu \cdot N}{2^{b-t}}$
- $\mu$ is bounded by multicollision limit function $\mu_{t,b-t}^{2q}$
  - Each of the $2^t$ bins represents a tag value
  - The two subscript parameters sum to state size $b$

# Black Box Attack Intuition




$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \lesssim \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

- Attacker wants to recover the state $W$ for one construction query
  - With $N$ guesses, success probability is $\frac{N}{2^{b-t}}$
  - With $\mu$ queries colliding in $T$, success probability is $\frac{\mu \cdot N}{2^{b-t}}$
- $\mu$ is bounded by multicollision limit function $\mu_{t,b-t}^{2q}$
  - Each of the $2^t$ bins represents a tag value
  - The two subscript parameters sum to state size $b$
  - For 'close to uniform' distribution $D$, $\mu_{r,c}^{q,D} \leq \mu_{r,c}^{2q}$ [DMV17]

# Augmenting the Black Box Attack with Leakage

- Attacker needs to guess truncated part of state $W$
- Choose leakage function that leaks a part of this state

# Augmenting the Black Box Attack with Leakage

- Attacker needs to guess truncated part of state $W$
- Choose leakage function that leaks a part of this state
- Leakage function leaking the first $\lambda$ bits of $W$ after the tag $T$:

$$L_p^W : \{0,1\}^b \times \{0,1\}^b \to \{0,1\}^\lambda$$
$$L_p^W(V, W) = W_{t+1} \| W_{t+2} \| \cdots \| W_{t+\lambda}$$

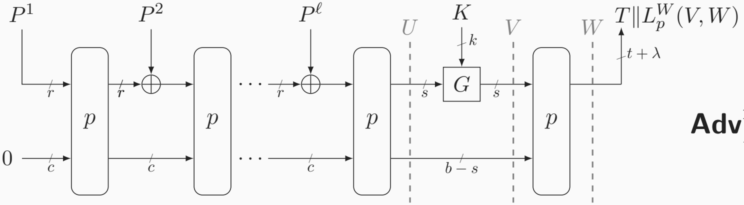
## Augmenting the Black Box Attack with Leakage

- Attacker needs to guess truncated part of state $W$
- Choose leakage function that leaks a part of this state
- Leakage function leaking the first $\lambda$ bits of $W$ after the tag $T$:

$$L_p^W : \{0,1\}^b \times \{0,1\}^b \to \{0,1\}^\lambda$$
$$L_p^W(V,W) = W_{t+1} \| W_{t+2} \| \cdots \| W_{t+\lambda}$$

- Intuition: view leakage as longer tag

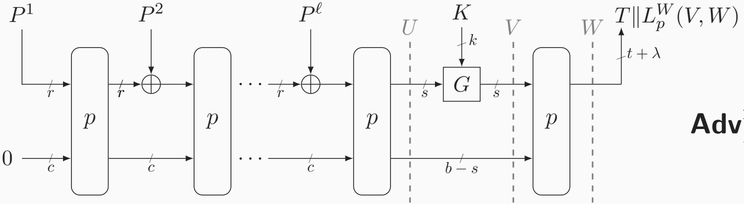
# Tightness of the Leakage Resilience Security Bound




$$\mathbf{Adv}_{F,\mathcal{L}}^{\text{nalr-prf}}(\mathcal{A}) \lesssim \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}}$$

- Attacker learns $t + \lambda$ bits of $W$, hence change in denominator

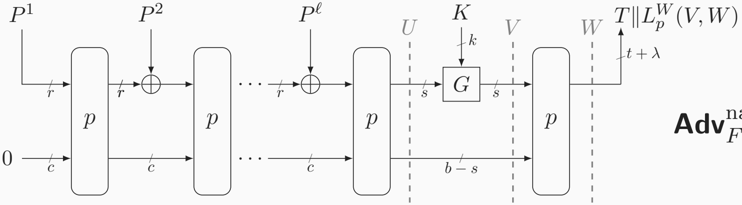
# Tightness of the Leakage Resilience Security Bound




$$\mathbf{Adv}_{F,\mathcal{L}}^{\text{nalr-prf}}(\mathcal{A}) \lesssim \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}}$$

- Attacker learns $t + \lambda$ bits of $W$, hence change in denominator
- Multicollision still only collides on $t$ bits
  - Therefore, leakage resilience security bound is not tight

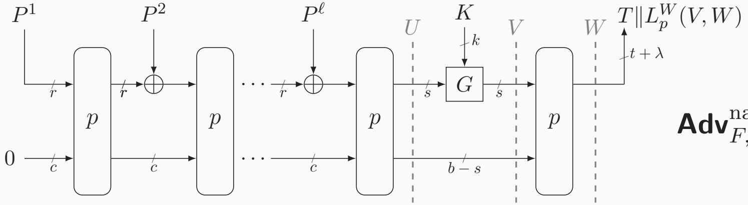
# Tightness of the Leakage Resilience Security Bound




$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{fixed}}}(\mathcal{A}) \lesssim \frac{\mu^{2q}_{t+\lambda,b-t-\lambda} \cdot N}{2^{b-t-\lambda}}$$

- Attacker learns $t+\lambda$ bits of $W$, hence change in denominator
- Multicollision still only collides on $t$ bits
  - Therefore, leakage resilience security bound is not tight
- Bound is easily tightened for leakage function $L_p^W$:
  - Replace $\mu^{2q}_{t,b-t}$ with $\mu^{2q}_{t+\lambda,b-t-\lambda}$
  - Holds for all 'fixed position' leakage functions

# Tightness of the Leakage Resilience Security Bound




$$\mathbf{Adv}_{F,\mathcal{L}_{\text{fixed}}}^{\text{nalr-prf}}(\mathcal{A}) \lesssim \frac{\mu_{t+\lambda,b-t-\lambda}^{2q} \cdot N}{2^{b-t-\lambda}}$$

- Attacker learns $t + \lambda$ bits of $W$, hence change in denominator
- Multicollision still only collides on $t$ bits
  - Therefore, leakage resilience security bound is not tight
- Bound is easily tightened for leakage function $L_p^W$:
  - Replace $\mu_{t,b-t}^{2q}$ with $\mu_{t+\lambda,b-t-\lambda}^{2q}$
  - Holds for all 'fixed position' leakage functions
- How can the bound be tightened for other types of leakage?

# Hamming Weight Leakage

**Hamming Weight (HW)**

The Hamming weight of a bitstring is the number of 1s, e.g. $\mathsf{HW}(101) = 2$

**Hamming Weight (HW)**

The Hamming weight of a bitstring is the number of 1s, e.g. $\mathrm{HW}(101) = 2$

## Why Hamming Weight Leakage?

- More realistic leakage model [May00, MOP07, DMMS21]
- Entropy loss depends on leakage value
- Non-uniform distribution

**Hamming Weight (HW)**

The Hamming weight of a bitstring is the number of 1s, e.g. $\mathsf{HW}(101) = 2$

## Why Hamming Weight Leakage?

- More realistic leakage model [May00, MOP07, DMMS21]
- Entropy loss depends on leakage value
- Non-uniform distribution

## Leakage and Multicollisions

- Due to non-uniformity, largest multicollision size depends on leakage value
- Multicollision limit function must take into account:
  - Non-uniform nature of Hamming weight leakage
  - The value of the Hamming weight leakage

# Multicollision Limit Function for HW Leakage

## Attacker's Goal

- To guess truncated part of $W$, attacker finds a multicollision in:
  - The first $t$ bits forming the tag $T$
  - The Hamming weight $w$ of $n$ *unknown* bits of $W$

## Attacker's Goal

- To guess truncated part of $W$, attacker finds a multicollision in:
  - The first $t$ bits forming the tag $T$
  - The Hamming weight $w$ of $n$ *unknown* bits of $W$

## Balls-and-bins Experiment

- One bin for each $(T, w)$-pair

$$2^t \text{ tags} \left\{ \begin{matrix} \overbrace{(0^t, 0) \quad \cdots \quad (0^t, n)}^{n+1 \text{ HW values}} \\ \vdots \qquad\qquad \vdots \\ (1^t, 0) \quad \cdots \quad (1^t, n) \end{matrix} \right.$$

# Multicollision Limit Function for HW Leakage

## Attacker's Goal

- To guess truncated part of $W$, attacker finds a multicollision in:
    - The first $t$ bits forming the tag $T$
    - The Hamming weight $w$ of $n$ *unknown* bits of $W$

## Balls-and-bins Experiment

- One bin for each $(T, w)$-pair
- Balls thrown according to $D_{\mathsf{HW}}(w)$:
    - Hamming weight distribution
    - Only counts specific bins

$$2^t \text{ tags} \left\{ \begin{array}{ccc} \multicolumn{3}{c}{\overbrace{\hspace{4cm}}^{n+1 \text{ HW values}}} \\ (0^t, 0) & \cdots & (0^t, n) \\ \vdots & & \vdots \\ (1^t, 0) & \cdots & (1^t, n) \end{array} \right.$$

## Attacker's Goal

- To guess truncated part of $W$, attacker finds a multicollision in:
  - The first $t$ bits forming the tag $T$
  - The Hamming weight $w$ of $n$ *unknown* bits of $W$

## Balls-and-bins Experiment

- One bin for each $(T, w)$-pair
- Balls thrown according to $D_{\mathsf{HW}}(w)$:
  - Hamming weight distribution
  - Only counts specific bins

Example: $D_{\mathsf{HW}}(0)$

$$2^t \text{ tags} \left\{ \begin{array}{ccc} \multicolumn{3}{c}{\overbrace{\hphantom{(0^t, 0) \quad \cdots \quad (0^t, n)}}^{n+1 \text{ HW values}}} \\ (0^t, 0) & \cdots & (0^t, n) \\ \vdots & & \vdots \\ (1^t, 0) & \cdots & (1^t, n) \end{array} \right.$$

# Multicollision Limit Function for HW Leakage

## Attacker's Goal

- To guess truncated part of $W$, attacker finds a multicollision in:
  - The first $t$ bits forming the tag $T$
  - The Hamming weight $w$ of $n$ *unknown* bits of $W$

## Balls-and-bins Experiment

- One bin for each $(T, w)$-pair
- Balls thrown according to $D_{\mathsf{HW}}(w)$:
  - Hamming weight distribution
  - Only counts specific bins

Example: $D_{\mathsf{HW}}(n)$

$$2^t \text{ tags} \left\{ \begin{array}{ccc} \multicolumn{3}{c}{\overbrace{\hspace{10em}}^{n+1 \text{ HW values}}} \\ (0^t, 0) & \cdots & (0^t, n) \\ \vdots & & \vdots \\ (1^t, 0) & \cdots & (1^t, n) \end{array} \right.$$

## Attacker's Goal

- To guess truncated part of $W$, attacker finds a multicollision in:
  - The first $t$ bits forming the tag $T$
  - The Hamming weight $w$ of $n$ *unknown* bits of $W$

## Balls-and-bins Experiment

- One bin for each $(T, w)$-pair
- Balls thrown according to $D_{\mathsf{HW}}(w)$:
  - Hamming weight distribution
  - Only counts specific bins
- Results in $\mu_{t',b-t'}^{q,D_{\mathsf{HW}}(w)}$:
  - $t' = t + \log_2(n+1)$
  - $2^{t'} = 2^t \cdot (n+1)$

Example: $D_{\mathsf{HW}}(n)$

$$2^t \text{ tags} \left\{ \overbrace{\begin{matrix} (0^t, 0) & \cdots & (0^t, n) \\ \vdots & & \vdots \\ (1^t, 0) & \cdots & (1^t, n) \end{matrix}}^{n+1 \text{ HW values}} \right.$$

# Bounding the Multicollision Limit Function

- Problem: $\mu_{r,c}^{q,D_{\mathsf{HW}}(w)}$ is hard to compute

# Bounding the Multicollision Limit Function

- Problem: $\mu_{r,c}^{q,D_{\mathsf{HW}}(w)}$ is hard to compute
- Solution: bound by uniform distribution with more than $q$ balls

- Problem: $\mu_{r,c}^{q,D_{\mathsf{HW}}(w)}$ is hard to compute
- Solution: bound by uniform distribution with more than $q$ balls
    - Recall result from [DMV17]:
        - For 'close to uniform' distribution $D$, $\mu_{r,c}^{q,D} \leq \mu_{r,c}^{2q}$

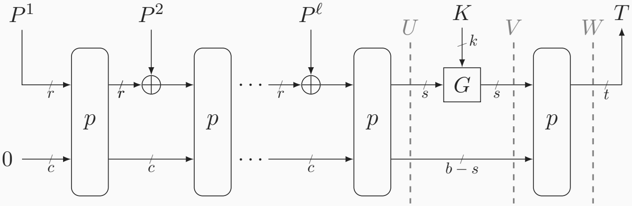
# Bounding the Multicollision Limit Function

- Problem: $\mu_{r,c}^{q,D_{\mathsf{HW}}(w)}$ is hard to compute
- Solution: bound by uniform distribution with more than $q$ balls
  - Recall result from [DMV17]:
    - For 'close to uniform' distribution $D$, $\mu_{r,c}^{q,D} \leq \mu_{r,c}^{2q}$
  - $D_{\mathsf{HW}}(w)$ is too far from uniform

# Bounding the Multicollision Limit Function

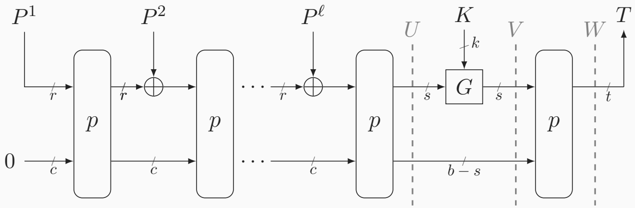
- Problem: $\mu_{r,c}^{q,D_{\mathsf{HW}}(w)}$ is hard to compute
- Solution: bound by uniform distribution with more than $q$ balls
  - Recall result from [DMV17]:
    - For 'close to uniform' distribution $D$, $\mu_{r,c}^{q,D} \leq \mu_{r,c}^{2q}$
  - $D_{\mathsf{HW}}(w)$ is too far from uniform
  - Our result (proof inspired by [DMV17]):
    - $\mu_{r,c}^{q,D_{\mathsf{HW}}(w)} \leq \mu_{r,c}^{\alpha(w)q}$
    - More frequent Hamming weight $w \implies$ larger $\alpha(w)$

# Tightening the Bound for Hamming Weight Leakage



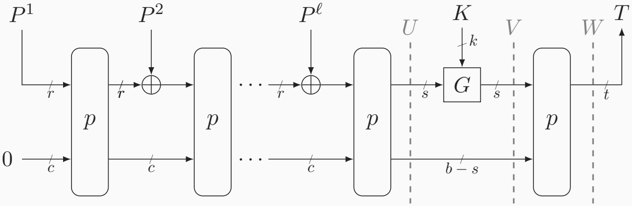

$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{HW}}}(\mathcal{A}) \lesssim \max_w \frac{\mu^{\alpha(w)q}_{t',b-t'} \cdot N}{\binom{n}{w} 2^{b-t-n}}$$

## Tightening the Bound for Hamming Weight Leakage




$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{HW}}}(\mathcal{A}) \lesssim \max_w \frac{\mu^{\alpha(w)q}_{t',b-t'} \cdot N}{\binom{n}{w} 2^{b-t-n}}$$

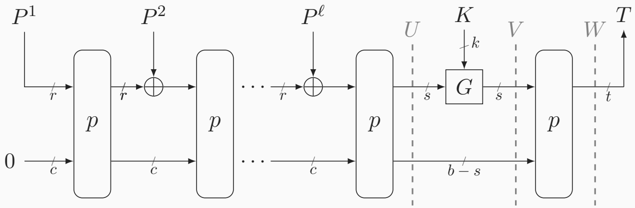
- Attacker knows tag $T$ and Hamming weight of $n$ truncated bits
  - The $n$ truncated bits have $\binom{n}{w}$ possible values
  - The $b-t-n$ unknown bits have $2^{b-t-n}$ possible values




$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{HW}}}(\mathcal{A}) \lesssim \max_w \frac{\mu^{\alpha(w)q}_{t',b-t'} \cdot N}{\binom{n}{w} 2^{b-t-n}}$$

- Attacker knows tag $T$ and Hamming weight of $n$ truncated bits
  - The $n$ truncated bits have $\binom{n}{w}$ possible values
  - The $b-t-n$ unknown bits have $2^{b-t-n}$ possible values
- Due to multicollision, attacker can match $\mu^{\alpha(w)q}_{t',b-t'}$ values with each guess

# Tightening the Bound for Hamming Weight Leakage




$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{HW}}}(\mathcal{A}) \lesssim \max_{w} \frac{\mu^{\alpha(w)q}_{t',b-t'} \cdot N}{\binom{n}{w} 2^{b-t-n}}$$

- Attacker knows tag $T$ and Hamming weight of $n$ truncated bits
  - The $n$ truncated bits have $\binom{n}{w}$ possible values
  - The $b-t-n$ unknown bits have $2^{b-t-n}$ possible values
- Due to multicollision, attacker can match $\mu^{\alpha(w)q}_{t',b-t'}$ values with each guess
- Attacker exploits 'worst-case' leakage value $w$

# Improvements in the Bound

# Comparing the Bounds with ISAP Parameters

- Ascon-p parameters: $(b, c, r, k) = (320, 256, 64, 128)$ with $s = t = k$
- $\lambda = 3$, $n = 7$
  - 7 bits $\implies$ 8 Hamming weight values
  - Can be encoded in 3 bits of leakage

- Ascon-p parameters: $(b, c, r, k) = (320, 256, 64, 128)$ with $s = t = k$
- $\lambda = 3$, $n = 7$
  - 7 bits $\implies$ 8 Hamming weight values
  - Can be encoded in 3 bits of leakage

**Order: original, fixed position leakage, HW leakage**

$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu^{2(N-q)}_{b-s,s} \cdot N}{2^{\min\{\delta,\varepsilon\}-\mu^{2(N-q)}_{s,b-s}\lambda}} + \frac{\mu^{2q}_{t,b-t} \cdot N}{2^{b-t-\lambda}} + \frac{\mu^{2(N-q)}_{s,b-s}}{2^{b-s}}$$

$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{fixed}}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu^{2(N-q)}_{b-s+\lambda,s-\lambda} \cdot N}{2^{\min\{\delta,\varepsilon\}-\lambda}} + \frac{\mu^{2q}_{t+\lambda,b-t-\lambda} \cdot N}{2^{b-t-\lambda}}$$

$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{HW}}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \max_w \frac{\mu^{\alpha(w)(N-q)}_{b-s',s'} \cdot N}{\binom{n}{w} 2^{\min\{\delta,\varepsilon\}-n}} + \max_w \frac{\mu^{\alpha(w)q}_{t',b-t'} \cdot N}{\binom{n}{w} 2^{b-t-n}}$$

# Comparing the Bounds with ISAP Parameters

- Ascon-p parameters: $(b, c, r, k) = (320, 256, 64, 128)$ with $s = t = k$
- $\lambda = 3$, $n = 7$
  - 7 bits $\implies$ 8 Hamming weight values
  - Can be encoded in 3 bits of leakage

| Order: original, fixed position leakage, HW leakage | Security |
|---|---|
| $\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu^{2(N-q)}_{b-s,s} \cdot N}{2^{\min\{\delta,\varepsilon\}-\mu^{2(N-q)}_{s,b-s}\lambda}} + \frac{\mu^{2q}_{t,b-t} \cdot N}{2^{b-t-\lambda}} + \frac{\mu^{2(N-q)}_{s,b-s}}{2^{b-s}}$ | 110 bits |
| $\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{fixed}}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu^{2(N-q)}_{b-s+\lambda,s-\lambda} \cdot N}{2^{\min\{\delta,\varepsilon\}-\lambda}} + \frac{\mu^{2q}_{t+\lambda,b-t-\lambda} \cdot N}{2^{b-t-\lambda}}$ | 122 bits |
| $\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{HW}}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \max_w \frac{\mu^{\alpha(w)(N-q)}_{b-s',s'} \cdot N}{\binom{n}{w} 2^{\min\{\delta,\varepsilon\}-n}} + \max_w \frac{\mu^{\alpha(w)q}_{t',b-t'} \cdot N}{\binom{n}{w} 2^{b-t-n}}$ | 118 bits |

# Conclusion

# Conclusion

## Our Contribution

- SuKS leakage resilience security bound is not tight
- Tightened bounds improve security, but only for specific leakage types
- Multicollision limit function analysis carries over to other schemes

# Conclusion

## Our Contribution

- SuKS leakage resilience security bound is not tight
- Tightened bounds improve security, but only for specific leakage types
- Multicollision limit function analysis carries over to other schemes

## Future Work

- Adaptive leakage
- Leakage of bits in dynamic positions

## Our Contribution

- SuKS leakage resilience security bound is not tight
- Tightened bounds improve security, but only for specific leakage types
- Multicollision limit function analysis carries over to other schemes

## Future Work

- Adaptive leakage
- Leakage of bits in dynamic positions

**Thank you for your attention!**

# Supporting Slides

# Second Subscript Parameter of the Multicollision Limit Function

**Multicollision Limit Function Definition**

$\mu^{q}_{r,c}$ is smallest $x$ such that $\mathbf{Pr}\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

- Attacker knows $r$ bits of state, has to guess remaining $c$ bits
- Attacker has a multicollision for $r$ bits
- Attacker's success probability with $N$ guesses is at most $\frac{\mu^{2q}_{r,c} \cdot N}{2^c}$
- Exception: size of largest multicollision is greater than $\mu^{2q}_{r,c}$
- Probability of this is at most $\frac{\mu^{2q}_{r,c}}{2^c}$ by definition
- Accumulated probability bound of $\frac{\mu^{2q}_{r,c} \cdot (N+1)}{2^c}$

# Strongly Protected Function $G$

**Definition $2^{-\delta}$-uniformity**

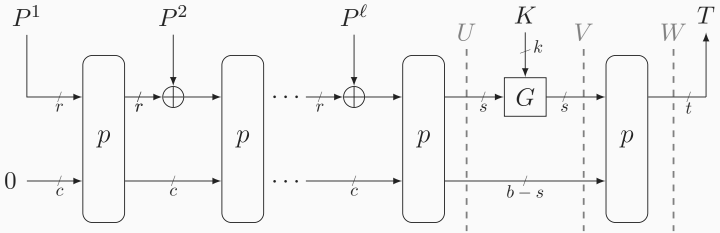
$G$ is $2^{-\delta}$-uniform if, for a randomly drawn $K$ and any $X, Y$, $\delta$ is the largest real number such that $\mathbf{Pr}\left(G(K, X) = Y\right) \leq 2^{-\delta}$

**Definition $2^{-\varepsilon}$-universality**

$G$ is $2^{-\varepsilon}$-universal if, for a randomly drawn $K$ and any distinct $X, X'$, $\varepsilon$ is the largest real number such that $\mathbf{Pr}\left(G(K, X) = G(K, X')\right) \leq 2^{-\varepsilon}$

- We assume that $G$ is 'strongly protected':
  - $G$ is $2^{-\delta}$-uniform and $2^{-\varepsilon}$-universal *even under internal leakage*

# Black Box Matching Attack




$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \lesssim \frac{\mu_{t,b-t}^{2q} \cdot N}{2^{b-t}}$$

(1) $q$ construction queries on distinct plaintexts $P_i$ give tags $T_i$

(2) Primitive queries on these $P_i$ give the corresponding $U_i$

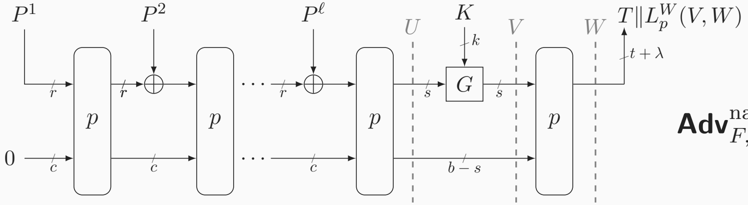
(3) Find a $\mu$-fold collision $T$ in the tags $T_i$

(4) For each $P_i$ in the $\mu$-fold collision, find a collision in the $\mathrm{left}_s(U_i)$

(5) Make $N$ primitive queries $p^{-1}(T\|Z_j)$ for varying $Z_j$

(6) For outcome $Y\|\mathrm{right}_{b-s}(U_i)$, use collision of step (4) to mount a forgery

# Matching Attack Fixed Position Leakage




$$\mathbf{Adv}^{\text{nalr-prf}}_{F,\mathcal{L}_{\text{fixed}}}(\mathcal{A}) \lesssim \frac{\mu^{2q}_{t+\lambda,b-t-\lambda} \cdot N}{2^{b-t-\lambda}}$$

(1) $q$ construction queries on distinct plaintexts $P_i$ give tags and leakages $T_i \| L_i$

(2) Primitive queries on these $P_i$ give the corresponding $U_i$

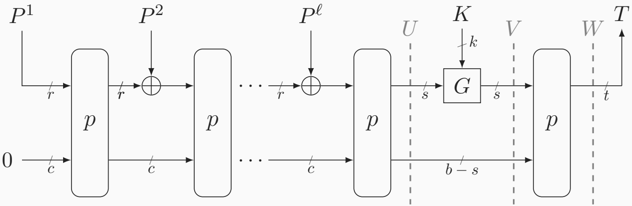
(3) Find a $\mu$-fold collision $T \| L$ in the tag-leakage pairs

(4) For each $P_i$ in the $\mu$-fold collision, find a collision in the $\text{left}_r(U_i)$

(5) Make $N$ primitive queries $p^{-1}(T \| L \| Z_j)$ for varying $Z_j$

(6) For outcome $Y \| \text{right}_{b-s}(U_i)$, use collision of step (4) to mount a forgery

# Matching Attack Hamming Weight Leakage




$$\mathbf{Adv}_{F,\mathcal{L}_{\mathrm{HW}}}^{\mathrm{nalr\text{-}prf}}(\mathcal{A}) \lesssim \max_{w} \frac{\mu_{t',b-t'}^{\alpha(w)q} \cdot N}{\binom{n}{w} 2^{b-t-n}}$$

(1) $q$ construction queries on distinct plaintexts $P_i$ give tag-leakage pairs $T_i, w_i$

(2) Primitive queries on these $P_i$ give the corresponding $U_i$

(3) For the optimal $w$, find a $\mu$-fold collision $T, w$ in the tag-leakage pairs

(4) For each $P_i$ in the $\mu$-fold collision, find a collision in the $\mathrm{left}_r(U_i)$

(5) Make $N$ primitive queries $p^{-1}(T \| Z_j)$ for varying $Z_j$, taking into account the leaked Hamming weight $w$ of $n$ bits

(6) For outcome $Y \| \mathrm{right}_{b-s}(U_i)$, use collision of step (4) to mount a forgery

## Proof Strategy for Bounding the Multicollision Limit Function

(1) Consider two balls-and-bins experiments:

exp1. $\alpha(w)q$ balls, $2^r$ bins (corresponds to $\mu_{r,c}^{q,D_{\mathsf{HW}}(w)}$)

exp2. $q$ balls thrown according to $D_{\mathsf{HW}}$, $2^r$ bins (corresponds to $\mu_{r,c}^{\alpha(w)q}$)

(2) Find a lower bound $t$ for $\mu_{r,c}^{\alpha(w)q}$

(3) Show that for all $y \geq t$ and every bin $i$,

$$\mathbf{Pr}\left(|i\text{th bin in exp1}| = y\right) \geq \mathbf{Pr}\left(|i\text{th bin in exp2}| = y\right)$$

(4) From step (3) it follows that for all $y \geq t$,

$$\mathbf{Pr}\left(|\text{fullest bin in exp1}| > y\right) \geq \mathbf{Pr}\left(|\text{fullest bin in exp2}| > y\right)$$

(5) From step (4) it follows that $\mu_{r,c}^{q,D_{\mathsf{HW}}(w)} \leq \mu_{r,c}^{\alpha(w)q}$ $\square$

[BDPV07] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
**Sponge functions.**
Ecrypt Hash Workshop 2007, May 2007.

[DEM+21] Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink, Robert Primas, and Thomas Unterluggauer.
**ISAP v2.**
Final Round Submission to NIST Lightweight Cryptography, 2021.

[DM19] Christoph Dobraunig and Bart Mennink.
**Security of the Suffix Keyed Sponge.**
*IACR Trans. Symmetric Cryptol.*, 2019(4):223–248, 2019.

[DM20] Christoph Dobraunig and Bart Mennink.
**Tightness of the Suffix Keyed Sponge Bound.**
*IACR Trans. Symmetric Cryptol.*, 2020(4):195–212, 2020.

[DMMS21] Sébastien Duval, Pierrick Méaux, Charles Momin, and François-Xavier Standaert.
**Exploring Crypto-Physical Dark Matter and Learning with Physical Rounding Towards Secure and Efficient Fresh Re-Keying.**
*IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(1):373–401, 2021.

[DMV17] Joan Daemen, Bart Mennink, and Gilles Van Assche.
**Full-State Keyed Duplex with Built-In Multi-user Support.**
In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017*, volume 10625 of *LNCS*, pages 606–637. Springer, 2017.

[May00] Rita Mayer-Sommer.
**Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards.**
In Çetin Kaya Koç and Christof Paar, editors, *CHES 2000*, volume 1965 of *LNCS*, pages 78–92. Springer, 2000.

[MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp.
**Power analysis attacks - revealing the secrets of smart cards.**
Springer, 2007.