A Block Cipher Based Pseudo Random Number Generator Secure against Side-Channel Key Recovery

Christophe Petit\textsuperscript{1}, François-Xavier Standaert\textsuperscript{1}, Olivier Pereira\textsuperscript{1}, Tal G. Malkin\textsuperscript{2}, Moti Yung\textsuperscript{2}

\textsuperscript{1}UCL Crypto Group, Université catholique de Louvain.
\textsuperscript{2}Dept. of Computer Science, Columbia University.
Physical Security

- Security is usually proved in an idealized model

While implemented, many secure cryptographic protocols are vulnerable to side-channel attacks (SC). Issue: partial information on the secret is leaked by physical media. By recovering many pieces of partial info, one can recover the whole secret key.
Physical Security

- Security is usually proved in an idealized model
- While implemented, many secure cryptographic protocols are vulnerable to side-channel attacks (SC)
Physical Security

- Security is usually proved in an idealized model
- While implemented, many secure cryptographic protocols are vulnerable to side-channel attacks (SC)
  - Issue: partial information on the SECRET is leaked by physical media
Physical Security

- Security is usually proved in an idealized model
- While implemented, many secure cryptographic protocols are vulnerable to side-channel attacks (SC)
  - Issue: partial information on the SECRET is leaked by physical media
  - By recovering many pieces of partial info, one can recover the whole secret key
Physical Security

- How to deal with leakages?
  - (Try to) remove them by electronic countermeasures (masking, noise addition, dual-rails,...)
Physical Security

- How to deal with leakages?
  - (Try to) remove them by electronic countermeasures (masking, noise addition, dual-rails,...)
  - Assume some perfect component (e.g. Katz’ non-tamperable device)
Physical Security

- How to deal with leakages?
  - (Try to) remove them by electronic countermeasures (masking, noise addition, dual-rails,...)
  - Assume some perfect component (e.g. Katz’ non-tamperable device)
  - Re-design algorithms
Re-design algorithms
- Do not only prevent leakages from occurring
- Make their combination hard
Physical Security

- Re-design algorithms
  - Do not only prevent leakages from occurring
  - Make their combination hard
  - Model the leakages
    - Micali-Reyzin model
Physical Security

- Re-design algorithms
  - Do not only prevent leakages from occurring
  - Make their combination hard
  - Model the leakages
    - Micali-Reyzin model
  - Case Study: Pseudo-Random Number Generator (PRNG)
Case Study: PRNG

- Black-Box security (BB): PRNG
- Grey-Box security (GB): prevent traditional SC cryptanalysis
Talk Overview

- Introduction
- PRNG
  - Construction
  - BB model & security
  - GB model & security
  - PRNG summary
- Conclusion and further work
Construction

(Public IV, secret keys)
Construction

- (Public IV, secret keys)
- First idea (in BB): if $E_1$ and $E_2$ are “good”, then the $y_i$’s should be PRNs.
Construction

- (Public IV, secret keys)
- First idea (in BB): if $E_1$ and $E_2$ are “good”, then the $y_i$’s should be PRNs.
- But (in GB) successive leakages allow recovering the whole secret.
The construction

So key update: \( k_{i+1} = k_i \oplus m_i \) and \( k_{i+1}^* = k_i^* \oplus m_i \)
The construction

- So key update: $k_{i+1} = k_i \oplus m_i$ and $k_{i+1}^* = k_i^* \oplus m_i$
- Each running key $k_i, k_i^*$ is used to encrypt only one message.
Black-Box Model

- Ideal cipher model $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}$
  - (Here $\mathcal{K} = \mathcal{M}$)
  - for each key $k \in \mathcal{K}$, the function $E_k(\cdot) = E(k, \cdot)$ is a random permutation on $\mathcal{M}$
Black-Box Model

- PRNG:
  - Deterministic algorithm $G: \mathcal{K} \rightarrow \hat{\mathcal{K}}$ (with $|\mathcal{K}| < |\hat{\mathcal{K}}|$)

$G$ is a PRNG if for any $A$, $\text{Adv}_{\text{prng}}(G, A) \approx 0$. 
Black-Box Model

- PRNG:
  - Deterministic algorithm $G : \mathcal{K} \rightarrow \hat{\mathcal{K}}$ (with $|\mathcal{K}| < |\hat{\mathcal{K}}|$)
  - For any adversary $A : \hat{\mathcal{K}} \rightarrow \{0, 1\}$, let

$$\text{Succ}_{G,A}^{\text{prng}^{-1}} = \Pr[A(\hat{k}) = 1 : \hat{k} \leftarrow R \hat{\mathcal{K}}],$$

$$\text{Succ}_{G,A}^{\text{prng}^{-0}} = \Pr[A(\hat{k}) = 1 : \hat{k} \leftarrow G(k); k \leftarrow R \mathcal{K}],$$

$$\text{Adv}_{G,A}^{\text{prng}} = |\text{Succ}_{G,A}^{\text{prng}^{-1}} - \text{Succ}_{G,A}^{\text{prng}^{-0}}|.$$
Black-Box Model

- PRNG:
  - Deterministic algorithm $G : \mathcal{K} \rightarrow \hat{\mathcal{K}}$ (with $|\mathcal{K}| < |\hat{\mathcal{K}}|$)
  - For any adversary $A : \hat{\mathcal{K}} \rightarrow \{0, 1\}$, let

    $\begin{align*}
    \text{Succ}_{G,A}^{\text{prng,1}} &= \Pr[A(\hat{k}) = 1 : \hat{k} \xleftarrow{\text{R}} \hat{\mathcal{K}}], \\
    \text{Succ}_{G,A}^{\text{prng,0}} &= \Pr[A(\hat{k}) = 1 : \hat{k} \leftarrow G(k); k \xleftarrow{\text{R}} \mathcal{K}], \\
    \text{Adv}_{G,A}^{\text{prng}} &= |\text{Succ}_{G,A}^{\text{prng,1}} - \text{Succ}_{G,A}^{\text{prng,0}}|.
    \end{align*}$

- $G$ is a PRNG if for any $A$, $\text{Adv}_{G,A}^{\text{prng}} \approx 0$. 
Black-Box Analysis

- Proof: study security of one round and extend it to multiple rounds by “hybrid argument”
Proof: study security of one round and extend it to multiple rounds by “hybrid argument”

For each $X \in \mathcal{M} = \mathcal{K}$, let $G_X : \mathcal{K} \times \mathcal{K} \rightarrow \mathcal{K} \times \mathcal{K} \times \mathcal{K}$

$$G_X(K, K^*) = (E_K(X) \oplus K, E_K(X) \oplus K^*, E_{K^*}(E_K(X))).$$
Black-Box Analysis

- Security of a single round

By definition,

\[ \text{Succ}_{G_X,A}^{prng-0} = \Pr[A(\hat{k}) = 1 : (k, k^*) \xleftarrow{R} \mathcal{K} \times \mathcal{K}; \hat{k} \leftarrow G_X(k, k^*)] \]
Security of a single round

By definition,

\[ \text{Succ}_{G_X,A}^{\text{prng}^0} = \Pr[A(\hat{k}) = 1 : (k, k^*) \xleftarrow{\text{R}} \mathcal{K} \times \mathcal{K}; \hat{k} \leftarrow G_X(k, k^*)] \]

Recalling what \( G_X(k, k^*) \) is,
Black-Box Analysis

- Security of a single round

Recalling what \( G_X(k, k^*) \) is,

\[
\text{Succ}_{G_X,A}^{\text{prng-0}} = \Pr[A(k_1, k_1^*, y) = 1 : \]

\[
k \xleftarrow{\text{R}} \mathcal{K}; \quad k^* \xleftarrow{\text{R}} \mathcal{K};
\]

\[
m \leftarrow \text{E}_k(X);
\]

\[
k_1 \leftarrow m \oplus k; \quad k_1^* \leftarrow m \oplus k^*;
\]

\[
y \leftarrow \text{E}_{k^*}(m)
\]
Black-Box Analysis

- Security of a single round
  Recalling what $G_X(k, k^*)$ is,

\[
\text{Succ}^{\text{prng-0}}_{G_X,A} = \Pr[A(k_1, k_1^*, y) = 1 : \\
\quad k \overset{R}{\leftarrow} \mathcal{K}; \ k^* \overset{R}{\leftarrow} \mathcal{K}; \\
\quad m \leftarrow E_k(X); \\
\quad k_1 \leftarrow m \oplus k; \ k_1^* \leftarrow m \oplus k^*; \\
\quad y \leftarrow E_{k^*}(m)]
\]

Now using the ideal cipher model for $E_k$ and $E_{k^*}$,
Black-Box Analysis

- Security of a single round

Now using the ideal cipher model for $E_k$ and $E_{k^*}$,

$$\text{Succ}_{G_X,A}^{\text{prng}-0} = \Pr[A(k_1, k^*_1, y) = 1 :$$

$$k \overset{R}{\leftarrow} \mathcal{K}; k^* \overset{R}{\leftarrow} \mathcal{K};$$

$$P \overset{R}{\leftarrow} \text{Perm}(\mathcal{K}); P^* \overset{R}{\leftarrow} \text{Perm}(\mathcal{K});$$

$$m \leftarrow P(X);$$

$$k_1 \leftarrow m \oplus k; k^*_1 \leftarrow m \oplus k^*;$$

$$y \leftarrow P^*(m)]$$
Security of a single round

Now using the ideal cipher model for $E_k$ and $E_{k^*}$,

$\text{Succ}^{\text{prng}-0}_{G_X,A} = \Pr[A(k_1, k^*_1, y) = 1 :$

\begin{align*}
k &\leftarrow R \mathcal{K}; k^* &\leftarrow R \mathcal{K};  \\
P &\leftarrow R \text{Perm}(\mathcal{K}); P^* &\leftarrow R \text{Perm}(\mathcal{K});  \\
m &\leftarrow P(X);  \\
k_1 &\leftarrow m \oplus k; k^*_1 &\leftarrow m \oplus k^*;  \\
y &\leftarrow P^*(m)
\end{align*}

Choosing random permutation and then applying to $X$

is equivalent to choosing random element, so
Black-Box Analysis

- Security of a single round
  Choosing random permutation and then applying to $X$ is equivalent to choosing random element, so

$$\text{Succ}_{G_X, A}^{\text{prng-0}} = \Pr[A(k_1, k^*_1, y) = 1 : k \leftarrow R \mathcal{K}; k^* \leftarrow R \mathcal{K};
\quad m \leftarrow R \mathcal{K}; k_1 \leftarrow m \oplus k;
\quad k^*_1 \leftarrow m \oplus k^*; y \leftarrow R \mathcal{K}]$$
Black-Box Analysis

- Security of a single round
  Choosing random permutation and then applying to $X$ is equivalent to choosing random element, so

$$\text{Succ}_{G_X,A}^{\text{prng}-0} = \Pr[A(k_1, k_1^*, y) = 1 : k \overset{R}{\leftarrow} \mathcal{K}; k^* \overset{R}{\leftarrow} \mathcal{K};$$

$$m \overset{R}{\leftarrow} \mathcal{K}; k_1 \leftarrow m \oplus k;$$

$$k_1^* \leftarrow m \oplus k^*; y \overset{R}{\leftarrow} \mathcal{K}]$$

So, each of the inputs of $A$ “looks random”
Black-Box Analysis

- Security of a single round
  So, each of the inputs of A “looks random”

\[
\text{Succ}_{G_X,A}^{\text{prng}-0} = \Pr[A(k_1, k^*_1, y) = 1 : k_1 \xleftarrow{R} \mathcal{K}; k^*_1 \xleftarrow{R} \mathcal{K};
\]
\[
y \xleftarrow{R} \mathcal{K}
\]
Black-Box Analysis

- Security of a single round

  So, each of the inputs of $A$ “looks random”

\[
\text{Succ}^{\text{prng}-0}_{G_X,A} = \Pr[A(k_1, k^*_1, y) = 1 : k_1 \leftarrow \mathcal{K}; k^*_1 \leftarrow \mathcal{K}; y \leftarrow \mathcal{K}]
\]

\[= \text{Succ}^{\text{prng}-1}_{G_X,A}\]
Black-Box Analysis

- Security of $G^q$ ($q$ rounds of $G$): hybrid argument
  - Consider hybrid algorithms on $q$ rounds
Black-Box Analysis

- Security of $G^q$ ($q$ rounds of $G$): hybrid argument
  - Consider hybrid algorithms on $q$ rounds
  - The $i^{th}$ hybrid has $i$ single $G$ rounds, followed by $q - i$ rounds of truly random generators
Black-Box Analysis

- Security of $G^q$ ($q$ rounds of $G$): hybrid argument
  - Consider hybrid algorithms on $q$ rounds
  - The $i^{th}$ hybrid has $i$ single $G$ rounds, followed by $q - i$ rounds of truly random generators
  - The $i + 1^{th}$ hybrid differs from the $i^{th}$ hybrid only by one round
Black-Box Analysis

- Security of $G^q$ ($q$ rounds of $G$): hybrid argument
  - Consider hybrid algorithms on $q$ rounds
  - The $i^{th}$ hybrid has $i$ single $G$ rounds, followed by $q - i$ rounds of truly random generators
  - The $i + 1^{th}$ hybrid differs from the $i^{th}$ hybrid only by one round
  - If there is $A$ such that $\text{Adv}_{G^q,A}^{\text{prng}} > \epsilon$, then there is $A'$ such that $\text{Adv}_{G,A'}^{\text{prng}} > \frac{\epsilon}{q}$ for one of the rounds
Grey-Box Model

Now recall that physical means leak information on the keys.

Implementation = algorithm + (probabilistic) leakage

\[ P_{\text{q}}(K, K^\ast) = (G_{\text{q}}(K, K^\ast), L_{\text{q}}(K, K^\ast)) \]

We show the available information does not permit recovering the secret.
Grey-Box Model

- Now recall that physical means leak information on the keys
Now recall that physical means leak information on the keys.

Implementation = algorithm + (probabilistic) leakage function of the keys

\[ P^q(K, K^*) = (G^q(K, K^*), L^q(K, K^*)) \]
Grey-Box Model

- Now recall that physical means leak information on the keys
- Implementation = algorithm + (probabilistic) leakage function of the keys
  \[ P^q(K, K^*) = (G^q(K, K^*), L^q(K, K^*)) \]
- We show the available information does not permit recovering the secret
Grey-Box Model

- Side-channel key recovery adversary

\[
\text{Succ}^{\text{sc-kr-}\delta(K,K^*)}_{P^q(K,K^*),A} = \Pr[A(P^q(k, k^*)) = \delta(k, k^*):]
\]

\[
k \leftarrow R \mathcal{K}; k^* \leftarrow R \mathcal{K}
\]

\(\delta(K, K^*)\) is part of the key (e.g., 1 byte)
Grey-Box Model

- Side-channel key recovery adversary

\[
\text{Succ}_{P^q(K,K^*)}^{\text{sc-kr-}\delta(K,K^*)} = \Pr[A(P^q(k, k^*)) = \delta(k, k^*) : k \leftarrow_R K; k^* \leftarrow_R K]
\]

\(\delta(K, K^*)\) is part of the key (e.g., 1 byte)

- If \(\delta(K, K^*) = K_{[0\ldots7]}\)

\[
\text{Succ}_{P^q(K,K^*)}^{\text{sc-kr-K}} = (\text{Succ}_{P^q(K,K^*)}^{\text{sc-kr-K}_{[0\ldots7]}})^{n/8}
\]
Grey-Box Model

Assumptions:
- Fixed IV
- Leakages on the $m_i$’s, $k_i$’s (and $k_i^{*}$’s)
- Cannot be related but by the rekeying relations

$$k_{i+1}^j = k_i^j \oplus m_i$$
Grey-Box Model

- Additional assumptions
  - Iterative BC, no key schedule
  - The adversary targets first round key $L(k_i) = L(k_i^0)$
  - Form of leakage functions: HW, GHW, NI
Grey-Box Analysis

- With observed leakages $l^q = \{L(k_i), L(m_i)\}$ and relations $k_{i+1} = k_i \oplus m_i$, the best guess is

$$k_{\text{guess}} := \arg \max_k \Pr[K = k | L^q = l^q]$$
Grey-Box Analysis

- With observed leakages $l^q = \{L(k_i), L(m_i)\}$ and relations $k_{i+1} = k_i \oplus m_i$, the best guess is

$$k_{\text{guess}} := \arg \max_k \Pr[K = k | L^q = l^q]$$

- We derive formulae for the success rate

$$\text{Succ}_{p^q(K, K')}^{\text{sc-kr}-K_0} = f(q, \{L(k_i), L(m_i)\})$$
Grey-Box Analysis

- With observed leakages $l^q = \{L(k_i), L(m_i)\}$ and relations $k_{i+1} = k_i \oplus m_i$, the best guess is

$$k_{\text{guess}} := \arg \max_k \Pr[K = k | L^q = l^q]$$

- We derive formulae for the success rate

$$\text{Succ}_{P^q(K, K^*)}^{sc-kr-K_0} = f(q, \{L(k_i), L(m_i)\})$$

- Goal: show that SR remains small as $q$ increases
Hamming Weight Leakages

- Hamming weight leakages $L(x) = W_H(x) = \sum_i x_i$
- (relevant in power consumption measures)
Hamming Weight Leakages

- Hamming weight leakages $L(x) = W_H(x) = \sum_i x_i$
- (relevant in power consumption measures)
- In this case we compute: $\text{Succ}_{\text{sc}}^{\text{sc} - kr - K_0} P^q(K, K^*), A = \frac{n+1}{2^n}$
- High security, independently of $q$
Noisy Identity Leakages

- Here the above formulae are hard to evaluate analytically → Monte-Carlo simulations
Noisy Identity Leakages

- Here the above formulae are hard to evaluate analytically → Monte-Carlo simulations

\[ \text{Succ}_{\text{AES256, A}} \approx (0.08)^{32} = 2^{-116} \]
PRNG Summarized

- BB : secure in the ideal cipher model
PRNG Summarized

- BB: secure in the ideal cipher model
- GB: SC Key Recovery prevented by the rekeying process
  Some practically relevant leakages are investigated and
  $SR \ll 1$ even if $q$ increases
PRNG Summarized

- BB: secure in the ideal cipher model
- GB: SC Key Recovery prevented by the rekeying process
  Some practically relevant leakages are investigated and $SR \ll 1$ even if $q$ increases
  With other countermeasures, leakages on more rounds means better attack
Conclusion and Further Work

- Re-design strategy to be used with other countermeasures
Re-design strategy
to be used with other countermeasures

Need of theoretical framework for SC
  unify BB and GB...
  define physical primitives
  compose primitives
Thank you

Thank you for attention
Thank you for attention
Thank you

Thank you for attention
Thank you

Thank you for attention
Thank you

Thank you for attention
Thank you

Thank you for attention
Secure initialization of the PRNG with a public seed

\[ k_{i+1} = k_i \oplus m_i \]

\[ k_{i+1}^* = k_i^* \oplus m_i \]
Secure initialization of the PRNG with a public seed

\[ k_{i+1} = k_i \oplus m_i \]
\[ k_{i+1}^* = k_i^* \oplus m_i \]
Secure initialization of the PRNG with a public seed

\[ k_{i+1} = k_i \oplus m_i \]

\[ k_{i+1}^* = k_i^* \oplus m_i \]
Secure initialization of the PRNG with a public seed
**Grey-Box Model**

- **Assumptions**:
  - Fixed IV (removed further)
  - Leakages on the $m_i$’s, $k_i$’s (and $k_i^*$’s)
  - Cannot be related but by the rekeying relations
    \[ k_{i+1}^j = k_i^j \oplus m_i \]
Grey-Box Model

- Additional assumptions
  - Iterative BC, no key schedule
  - The adversary targets first round key $L(k_i) = L(k_i^0)$
  - Form of leakage functions: HW, GHW, NI
  - We suppose Bayesian adversary
Discussion about Grey-Box assumptions

- Many assumptions
  - make the proofs cleaner...
  - ...but are not essential.
- Relaxations $\rightarrow$ same qualitative conclusions
  - key schedule $\rightarrow$ adapt the leakage model $L(k_i)$
  - targeting not only the first iteration of the PRNG
    $\rightarrow$ may increase SR, but qualitative results remains