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

Christophe Petit[1], François-Xavier Standaert[1],
Olivier Pereira[1], Tal G. Malkin[2], Moti Yung[2]

[1]UCL Crypto Group, Université catholique de Louvain.
[2] Dept. of Computer Science, Columbia University.

Physical Security

- Security is usually proved in an idealized model

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

Physical Security

- Re-design algorithms
  - Do not only prevent leakages from occuring
  - Make their combination hard

Physical Security

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

Physical Security

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

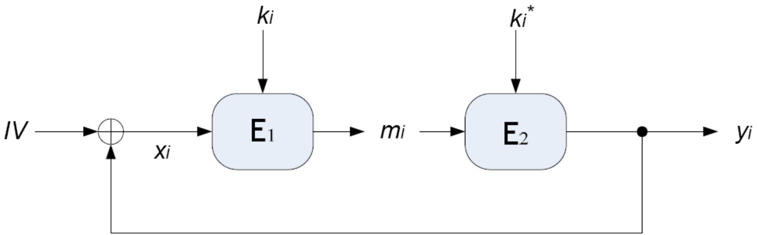
Case Study: PRNG

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

Talk Overview

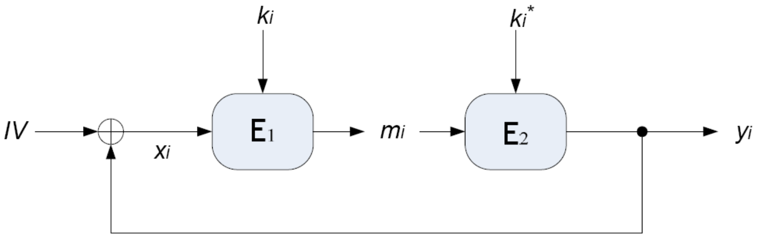
- Introduction
- PRNG
  - Construction
  - BB model & security
  - GB model & security
  - PRNG summary
- Conclusion and further work

Construction



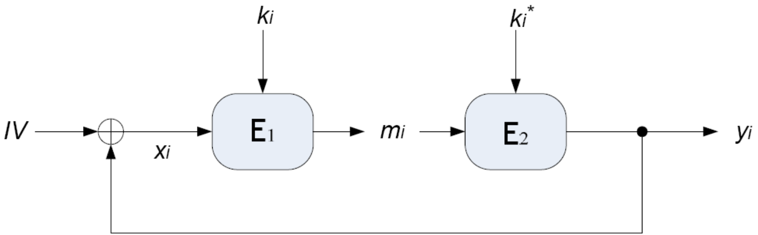
- (Public IV, secret keys)

Construction



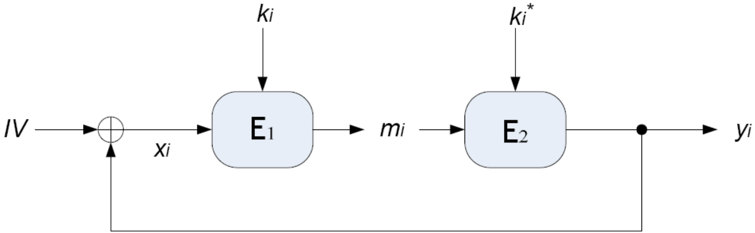
- (Public IV, secret keys)
- First idea (in BB): if E_1 and E_2 are "good", then the y_i's should be PRNs.

Construction



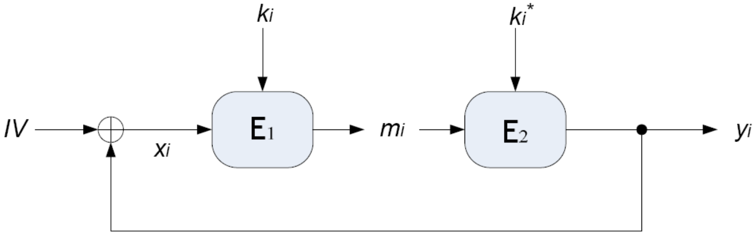
- (Public IV, secret keys)
- First idea (in BB): if E_1 and E_2 are "good", then the y_i's should be PRNs.
- But (in GB) successive leakages allow recovering the whole secret.

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 $\mathsf{E} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}$
  - (Here $\mathcal{K} = \mathcal{M}$)
  - for each key $k \in \mathcal{K}$, the function $\mathsf{E}_k(\cdot) = \mathsf{E}(k, \cdot)$ is a random permutation on $\mathcal{M}$

Black-Box Model

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

Black-Box Model

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

$$\begin{aligned}
\mathbf{Succ}_{\mathsf{G,A}}^{\mathrm{prng}-1} &= \Pr[\mathsf{A}(\hat{k}) = 1 : \hat{k} \stackrel{R}{\leftarrow} \hat{\mathcal{K}}], \\
\mathbf{Succ}_{\mathsf{G,A}}^{\mathrm{prng}-0} &= \Pr[\mathsf{A}(\hat{k}) = 1 : \hat{k} \leftarrow \mathsf{G}(k); k \stackrel{R}{\leftarrow} \mathcal{K}], \\
\mathbf{Adv}_{\mathsf{G,A}}^{\mathrm{prng}} &= |\mathbf{Succ}_{\mathsf{G,A}}^{\mathrm{prng}-1} - \mathbf{Succ}_{\mathsf{G,A}}^{\mathrm{prng}-0}|.
\end{aligned}$$

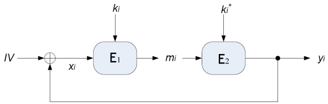
Black-Box Model

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

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

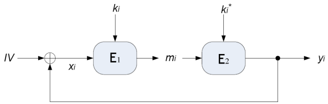
  - G is a PRNG if for any A, $\mathbf{Adv}^{\mathrm{prng}}_{\mathrm{G,A}} \approx 0$.

Black-Box Analysis

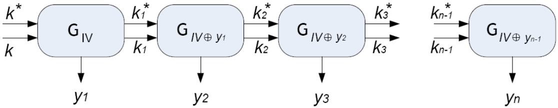


- Proof: study security of one round and extend it to multiple rounds by "hybrid argument"

Black-Box Analysis



- 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,

$$\mathbf{Succ}^{\mathrm{prng}-0}_{\mathsf{G}_X,\mathsf{A}} = \Pr[\mathsf{A}(\hat{k}) = 1 : (k, k^*) \xleftarrow{R} \mathcal{K} \times \mathcal{K}; \hat{k} \leftarrow \mathsf{G}_X(k, k^*)]$$

Black-Box Analysis

- Security of a single round

  By definition,

$$\mathbf{Succ}^{\mathrm{prng}-0}_{\mathsf{G}_X,\mathsf{A}} = \Pr[\mathsf{A}(\hat{k}) = 1 : (k, k^*) \stackrel{R}{\leftarrow} \mathcal{K} \times \mathcal{K}; \hat{k} \leftarrow \mathsf{G}_X(k, k^*)]$$

  Recalling what $\mathsf{G}_X(k, k^*)$ is,

Black-Box Analysis

- Security of a single round

  Recalling what $\mathsf{G}_X(k, k^*)$ is,

$$
\begin{aligned}
\mathbf{Succ}^{\mathrm{prng-0}}_{\mathsf{G}_X,\mathsf{A}} \quad = \quad & \Pr[\mathsf{A}(k_1, k_1^*, y) = 1 : \\
& k \xleftarrow{R} \mathcal{K}; k^* \xleftarrow{R} \mathcal{K}; \\
& m \leftarrow \mathsf{E}_k(X); \\
& k_1 \leftarrow m \oplus k; k_1^* \leftarrow m \oplus k^*; \\
& y \leftarrow \mathsf{E}_{k^*}(m)]
\end{aligned}
$$

Black-Box Analysis

- Security of a single round

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

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

  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^*},

$$\mathbf{Succ}^{\mathrm{prng}-0}_{G_X,A} = \Pr[A(k_1, k_1^*, y) = 1 : k \xleftarrow{R} \mathcal{K}; k^* \xleftarrow{R} \mathcal{K}; P \xleftarrow{R} Perm(\mathcal{K}); P^* \xleftarrow{R} Perm(\mathcal{K}); m \leftarrow P(X); k_1 \leftarrow m \oplus k; k_1^* \leftarrow m \oplus k^*; y \leftarrow P^*(m)]$$

Black-Box Analysis

- Security of a single round

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

$$\mathbf{Succ}^{\mathrm{prng}-0}_{G_X,A} = \Pr[A(k_1, k_1^*, y) = 1 : \begin{array}{l} k \stackrel{R}{\leftarrow} \mathcal{K}; k^* \stackrel{R}{\leftarrow} \mathcal{K}; \\ P \stackrel{R}{\leftarrow} Perm(\mathcal{K}); P^* \stackrel{R}{\leftarrow} Perm(\mathcal{K}); \\ m \leftarrow P(X); \\ k_1 \leftarrow m \oplus k; k_1^* \leftarrow m \oplus k^*; \\ y \leftarrow P^*(m)] \end{array}$$

  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

$$
\begin{aligned}
\mathbf{Succ}^{\mathrm{prng}-0}_{\mathsf{G}_X,\mathsf{A}} \;=\; & \Pr[\mathsf{A}(k_1, k_1^*, y) = 1 : k \xleftarrow{R} \mathcal{K}; k^* \xleftarrow{R} \mathcal{K}; \\
& m \xleftarrow{R} \mathcal{K}; k_1 \leftarrow m \oplus k; \\
& k_1^* \leftarrow m \oplus k^*; y \xleftarrow{R} \mathcal{K}]
\end{aligned}
$$

Black-Box Analysis

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

$$
\begin{aligned}
\mathbf{Succ}^{\mathrm{prng}-0}_{\mathsf{G}_X,\mathsf{A}} \quad = \quad & \Pr[\mathsf{A}(k_1, k_1^*, y) = 1 : k \xleftarrow{R} \mathcal{K}; k^* \xleftarrow{R} \mathcal{K}; \\
& m \xleftarrow{R} \mathcal{K}; k_1 \leftarrow m \oplus k; \\
& k_1^* \leftarrow m \oplus k^*; y \xleftarrow{R} \mathcal{K}]
\end{aligned}
$$

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"

$$\mathbf{Succ}_{\mathsf{G}_X,\mathsf{A}}^{\mathrm{prng}-0} = \Pr[\mathsf{A}(k_1, k_1^*, y) = 1 : k_1 \overset{R}{\leftarrow} \mathcal{K}; k_1^* \overset{R}{\leftarrow} \mathcal{K}; y \overset{R}{\leftarrow} \mathcal{K}]$$

Black-Box Analysis

- Security of a single round

  So, each of the inputs of A "looks random"

$$\begin{aligned}\mathbf{Succ}^{\mathrm{prng}-0}_{\mathsf{G}_X,\mathsf{A}} &= \Pr[\mathsf{A}(k_1, k_1^*, y) = 1 : k_1 \stackrel{R}{\leftarrow} \mathcal{K}; k_1^* \stackrel{R}{\leftarrow} \mathcal{K}; \\ &\qquad y \stackrel{R}{\leftarrow} \mathcal{K}] \\ &= \mathbf{Succ}^{\mathrm{prng}-1}_{\mathsf{G}_X,\mathsf{A}}\end{aligned}$$

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 $\mathbf{Adv}^{\mathrm{prng}}_{\mathsf{G}^q,\mathsf{A}} > \epsilon$, then there is A′ such that $\mathbf{Adv}^{\mathrm{prng}}_{\mathsf{G},\mathsf{A}'} > \frac{\epsilon}{q}$ for one of the rounds

Grey-Box Model

Grey-Box Model

- Now recall that physical means leak information on the keys

Grey-Box Model

- Now recall that physical means leak information on the keys
- Implementation = algorithm + (probabilistic) leakage function of the keys
  $\mathsf{P}^q(K, K^*) = (\mathsf{G}^q(K, K^*), \mathsf{L}^q(K, K^*))$

Grey-Box Model

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

Grey-Box Model

- Side-channel key recovery adversary

$$\mathbf{Succ}^{\mathrm{sc-kr-}\delta(K,K^*)}_{\mathsf{P}^q(K,K^*),\mathsf{A}} = \Pr[\mathsf{A}(\mathsf{P}^q(k,k^*)) = \delta(k,k^*) : k \xleftarrow{R} \mathcal{K}; k^* \xleftarrow{R} \mathcal{K}]$$

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

Grey-Box Model

- Side-channel key recovery adversary

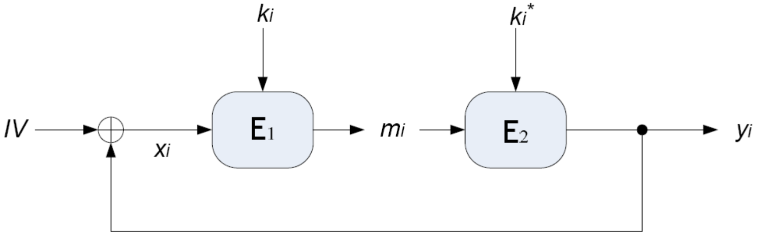
$$\mathbf{Succ}^{\mathrm{sc-kr}-\delta(K,K^*)}_{\mathsf{P}^q(K,K^*),\mathsf{A}} = \Pr[\mathsf{A}(\mathsf{P}^q(k,k^*)) = \delta(k,k^*) : k \xleftarrow{R} \mathcal{K}; k^* \xleftarrow{R} \mathcal{K}]$$

  $\delta(K, K^*)$ is part of the key (*e.g.*, 1 byte)
- If $\delta(K, K^*) = K_{[0\cdots7]}$

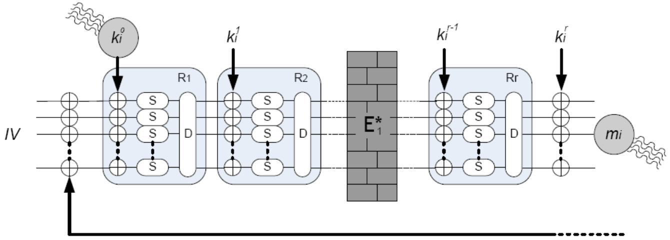
$$\mathbf{Succ}^{\mathrm{sc-kr}-K}_{\mathsf{P}^q(K,K^*),\mathsf{A}} = (\mathbf{Succ}^{\mathrm{sc-kr}-K_{[0\cdots7]}}_{\mathsf{P}^q(K,K^*),\mathsf{A}})^{n/8}$$

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

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

Grey-Box Analysis

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

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

- We derive formulae for the success rate

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

Grey-Box Analysis

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

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

- We derive formulae for the success rate

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

- Goal : show that SR remains small as q increases

Hamming Weight Leakages

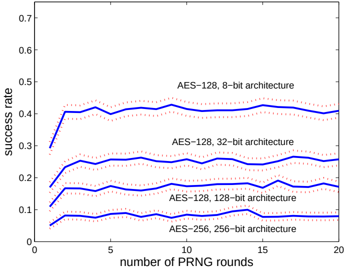
- Hamming weight leakages $\mathsf{L}(x) = W_H(x) = \sum_i x_i$
- (relevant in power consumption measures)

Hamming Weight Leakages

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

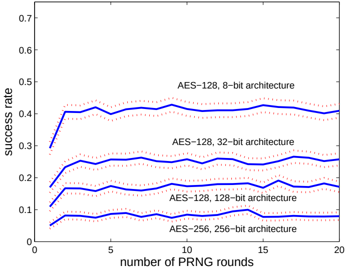
Noisy Identity Leakages

- Here the above formulae are hard to evaluate analytically $\longrightarrow$ Monte-Carlo simulations



Noisy Identity Leakages

- Here the above formulae are hard to evaluate analytically $\longrightarrow$ Monte-Carlo simulations



- $\mathbf{Succ}^{\text{sc-kr-K}}_{\text{AES256,A}} \simeq (0.08)^{32} = 2^{-116}$

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

Conclusion and Further Work

- 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

Thank you for attention

Thank you

Thank you for attention

Thank you

Thank you for attention

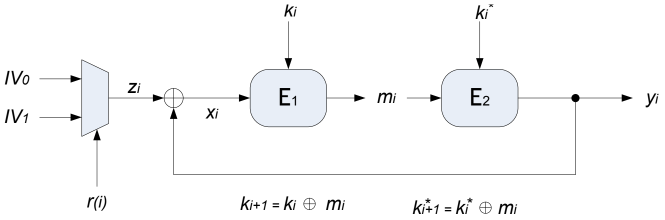
Thank you

Thank you for attention

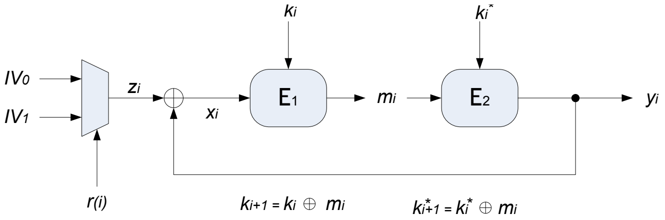
Thank you

Thank you for attention

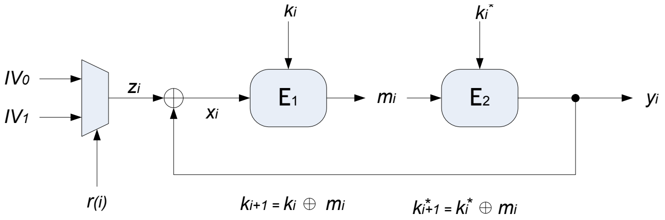
Secure initialization of the PRNG with a public seed



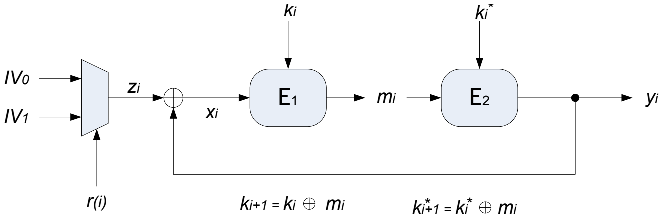
Secure initialization of the PRNG with a public seed



Secure initialization of the PRNG with a public seed

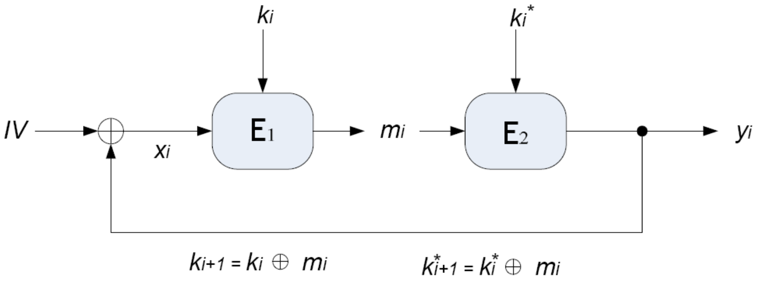


Secure initialization of the PRNG with a public seed

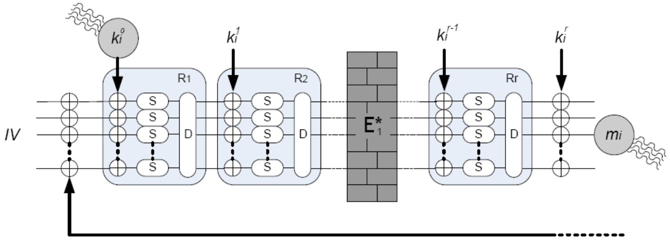


Grey-Box Model

- 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 $\longrightarrow$ same qualitative conclusions
  - key schedule $\longrightarrow$ adapt the leakage model $L(k_i)$
  - targeting not only the first iteration of the PRNG
    $\longrightarrow$ may increase SR, but qualitative results remains