Leakage Resilient Symmetric Encryption via Re-keying

CHES 2013

Michel Abdalla[1] Sonia Belaïd[1,2] Pierre-Alain Fouque[1,3]

[1]École Normale Supérieure

[2]Thales Communications & Security

[3]Rennes University

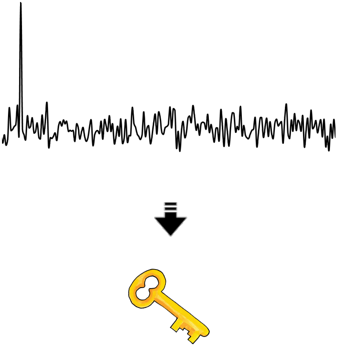
August, 23^{rd} 2013

Outline

Outline

Side-Channel Attacks

- physical leakage
  - timing
  - power consumption
  - electromagnetic radiations
  - ...
- statistical treatment
- key recovery



Countermeasures against Side-Channel Attacks

Masking

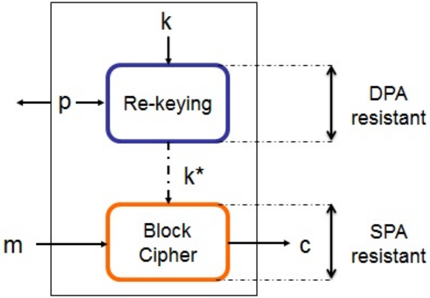
sensitive values randomized

x replaced by $x_m = x \star m$

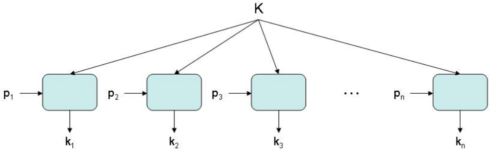
Drawbacks of Masking

- ✘ higher-order attacks
- ✘ glitches

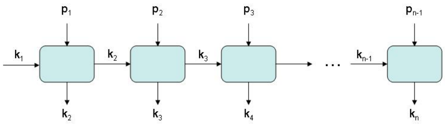
Re-keying



Two Main Re-keying Schemes

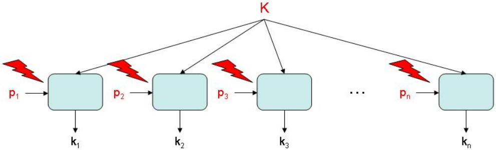


Parallel Scheme



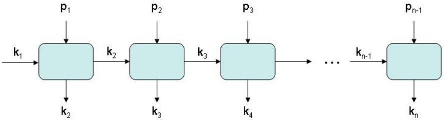
Sequential Scheme

Two Main Re-keying Schemes



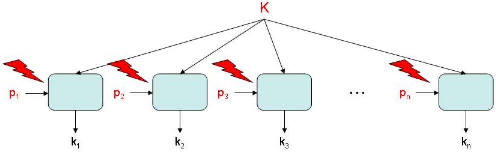
Parallel Scheme

vulnerable to *Differential Power Analysis*



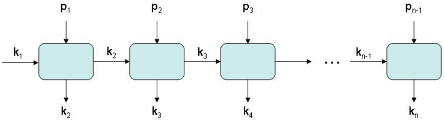
Sequential Scheme

Two Main Re-keying Schemes



Parallel Scheme

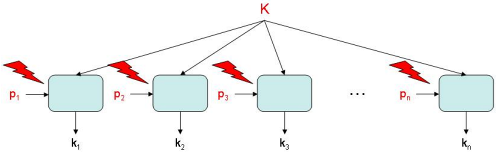
vulnerable to *Differential Power Analysis*



Sequential Scheme

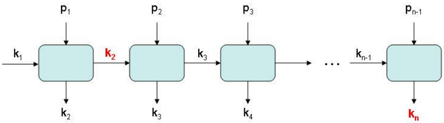
efficiency issue in case of *synchronization*

Two Main Re-keying Schemes



Parallel Scheme

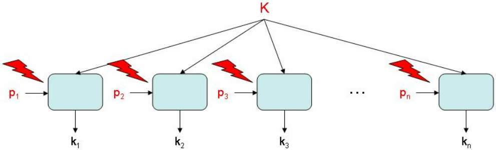
vulnerable to *Differential Power Analysis*



Sequential Scheme

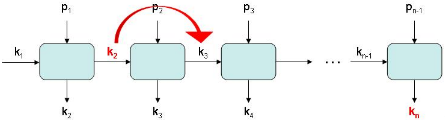
efficiency issue in case of *synchronization*

Two Main Re-keying Schemes



Parallel Scheme

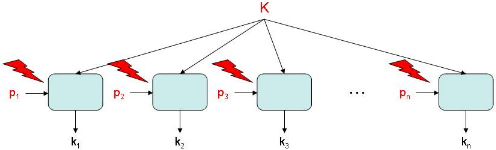
vulnerable to *Differential Power Analysis*



Sequential Scheme

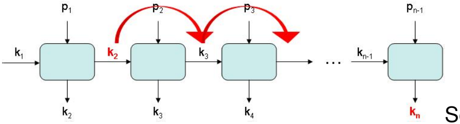
efficiency issue in case of *synchronization*

Two Main Re-keying Schemes



Parallel Scheme

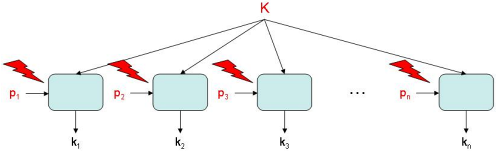
vulnerable to *Differential Power Analysis*



Sequential Scheme

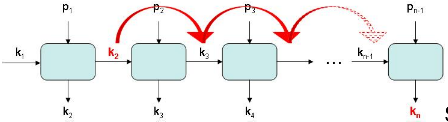
efficiency issue in case of *synchronization*

Two Main Re-keying Schemes



Parallel Scheme

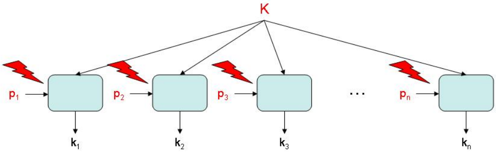
vulnerable to *Differential Power Analysis*



Sequential Scheme

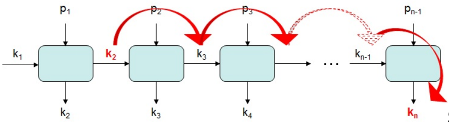
efficiency issue in case of *synchronization*

Two Main Re-keying Schemes



Parallel Scheme

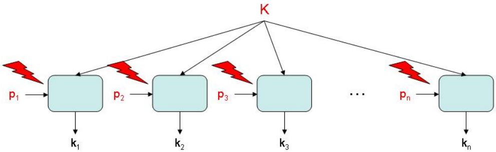
vulnerable to *Differential Power Analysis*



Sequential Scheme

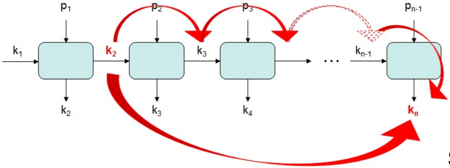
efficiency issue in case of *synchronization*

Two Main Re-keying Schemes



Parallel Scheme

vulnerable to *Differential Power Analysis*



Sequential Scheme

efficiency issue in case of *synchronization*

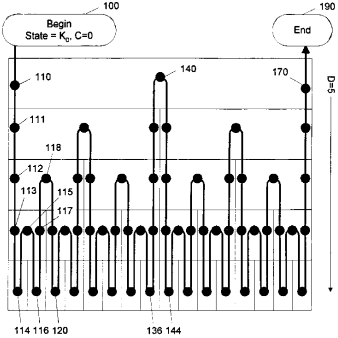
Existing Work

Kocher's Patent:
Leak-Resistant Cryptographic Indexed Key Update, 1999.

- ✔ re-keying scheme
- ✔ solution to the synchronisation issue

but

- ✘ no proof given
- ✘ two keys used multiple times with different inputs



Our Contributions

- ✔ re-keying scheme (different from Kocher's)
- ✔ solution to the synchronisation issue

but also

- ✔ limited use of each secret key
- ✔ proof of leakage-resilience for the whole encryption scheme

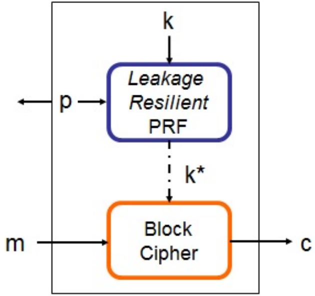
Outline

Leakage-Resilient Cryptography

- Leakage-Resilient Cryptography Model
  - only computation leaks
  - bounded amount of leakage per invocation
  - unlimited number of invocations
- Leakage-Resilient Encryption Scheme
  - challenge and leakage oracles
  - ciphertext indistinguishable from the encryption of a random string of the plaintext's size

Scheme 1: Symmetric Encryption from a LR PRF

- Re-keying Primitive
  - leakage-resilient PRF
  - non-adaptive leakage functions
  - non-adaptive inputs
- Block Cipher
  - as a PRF
  - not leakage-resilient



Theorem 1: This encryption scheme is a *non-adaptive leakage-resilient encryption scheme*.

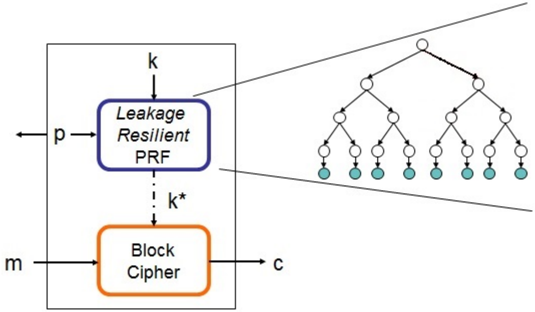
Scheme 1 instantiated with the CHES'12 PRF (1/2)

- instantiated with the Faust-Pietrzak-Schipper naLR naPRF

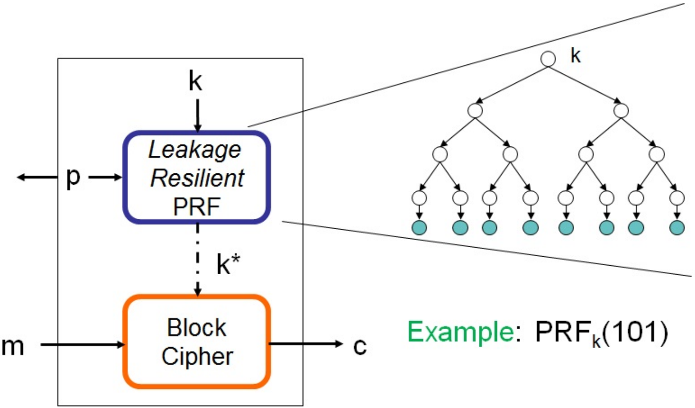
S. Faust, K. Pietrzak, J. Schipper: Practical Leakage-Resilient Symmetric Cryptography. CHES'12

- inspired by the Goldreich-Goldwasser-Micali tree

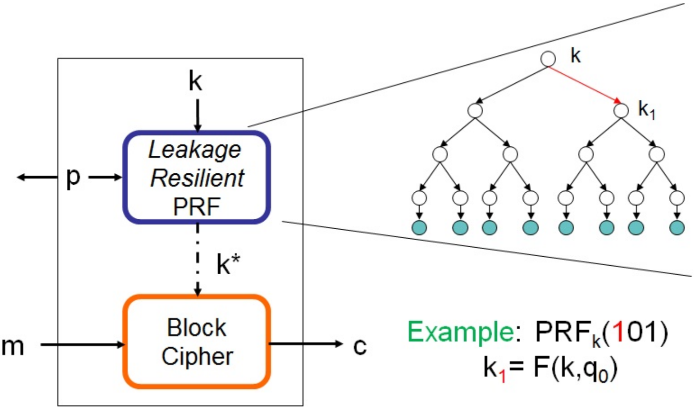
O. Goldreich, S. Goldwasser, S. Micali: How to construct random functions. J. ACM 33(4) (1986)



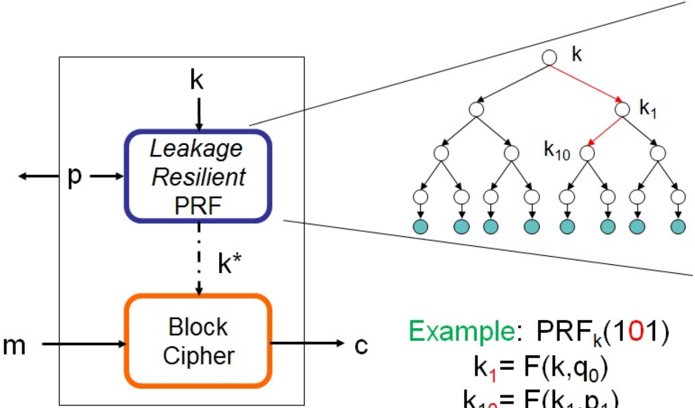
Scheme 1 instantiated with the CHES'12 PRF (1/2)



Scheme 1 instantiated with the CHES'12 PRF (1/2)



Scheme 1 instantiated with the CHES'12 PRF (1/2)

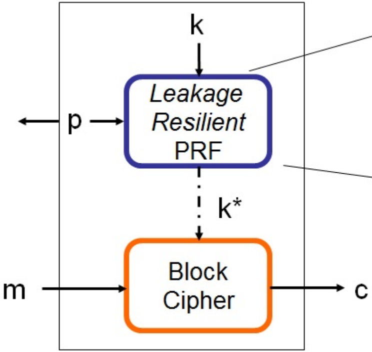


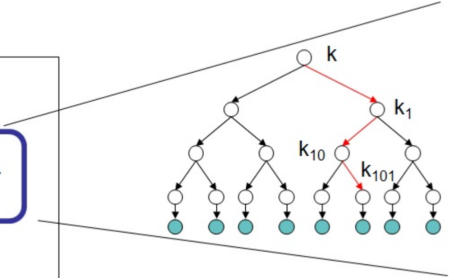
Example: $PRF_k(101)$

$k_1 = F(k, q_0)$

$k_{10} = F(k_1, p_1)$

Scheme 1 instantiated with the CHES'12 PRF (1/2)





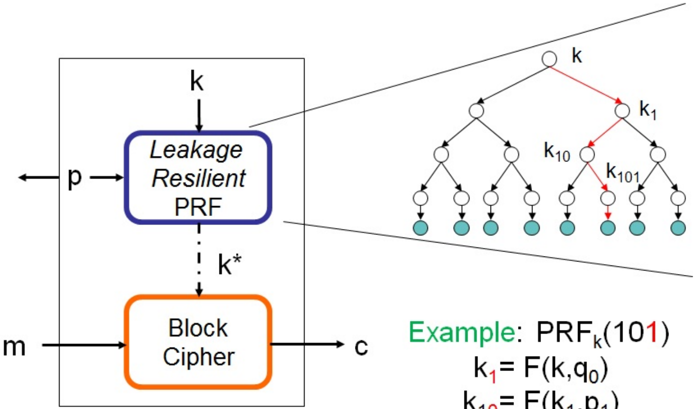
Example: $PRF_k(101)$

$k_1 = F(k, q_0)$

$k_{10} = F(k_1, p_1)$

$k_{101} = F(k_{10}, q_2)$

Scheme 1 instantiated with the CHES'12 PRF (1/2)



Example: $PRF_k(101)$

$k_1 = F(k, q_0)$

$k_{10} = F(k_1, p_1)$

$k_{101} = F(k_{10}, q_2)$

$k^* = F(k_{101}, p_3)$

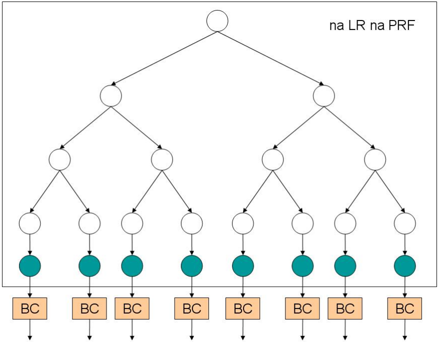
Scheme 1 instantiated with the CHES'12 PRF (2/2)

LR Encryption Scheme from

- ✔ naLR naPRF as re-keying scheme
- ✔ a SPA resistant block cipher

but

- ✘ not optimal
- ✘ no solution for the re-synchronization



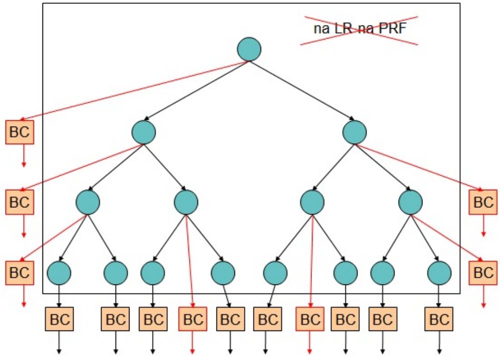
Scheme 2: Symmetric Encryption from a Weak PRF

LR Encryption Scheme from

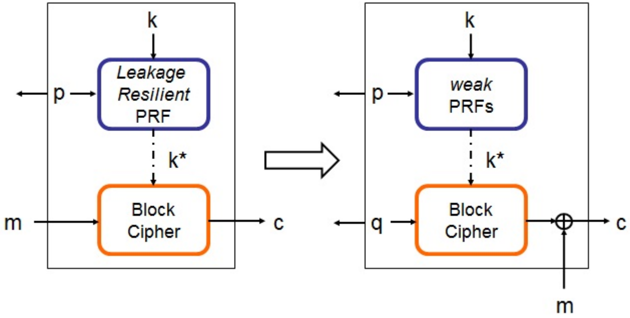
- ✔ only weak PRFs for the re-keying
- ✔ a SPA resistant block cipher
- ✔ more efficient
- ✔ with a solution for the re-synchronization

but

- ✘ additional constraint on the message



Security Aspects



- block cipher with **random inputs**
- **same primitive** for the block cipher and the weak PRFs
- plaintext **before** or **after** the block cipher

Synchronization Issue: Order?

Now we have a re-keying scheme,

how to determine the keys order for the synchronization?

Synchronization Issue: Order?

Now we have a re-keying scheme,

how to determine the keys order for the synchronization?

✔ short-cuts

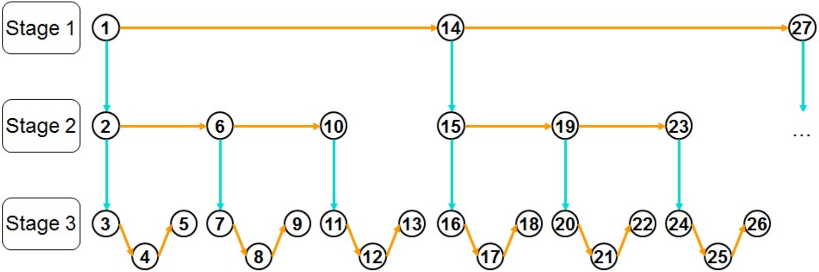
Synchronization Issue: Order?

Now we have a re-keying scheme,

how to determine the keys order for the synchronization?

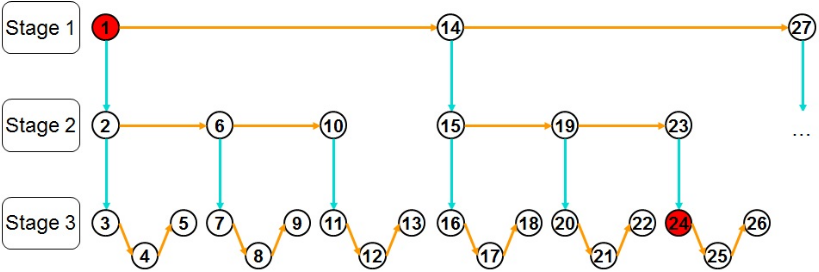
- ✔ short-cuts
- ✘ no additional relation between keys

Synchronization Solution: Skip-lists



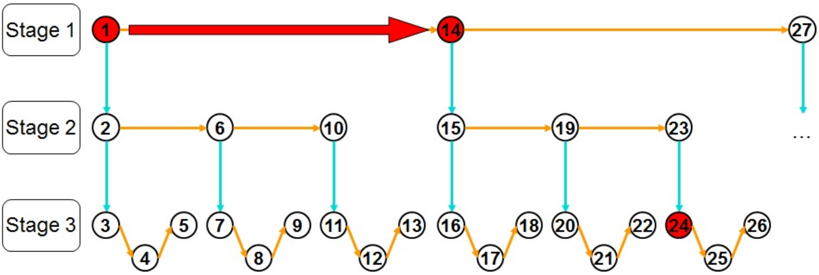
Solution: **Skip-lists**

Synchronization Solution: Skip-lists



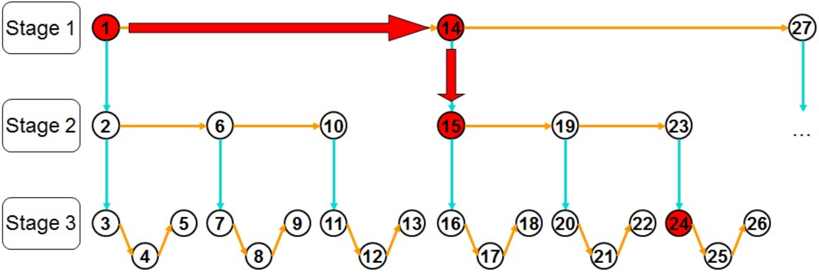
Example: Reach key K_{24} from K_1

Synchronization Solution: Skip-lists



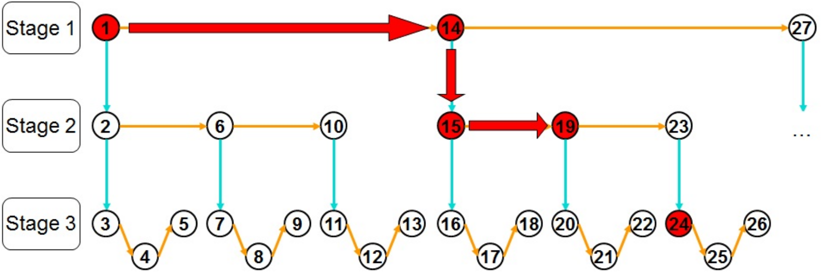
Example: Reach key K_{24} from K_1

Synchronization Solution: Skip-lists



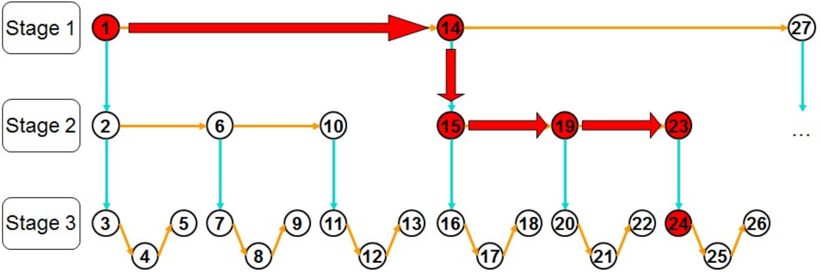
Example: Reach key K_{24} from K_1

Synchronization Solution: Skip-lists



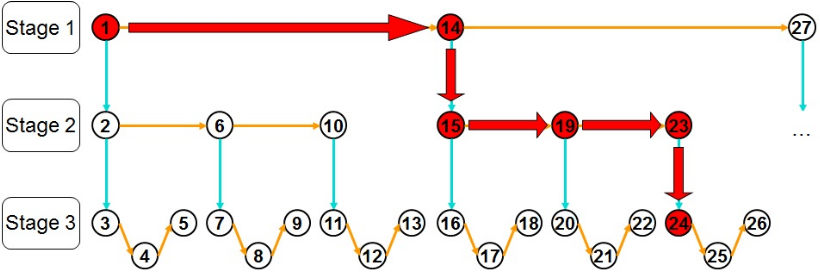
Example: Reach key K_{24} from K_1

Synchronization Solution: Skip-lists



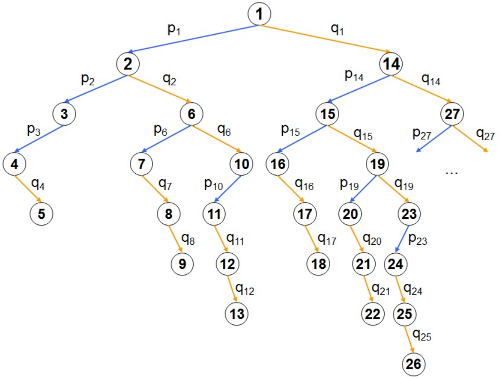
Example: Reach key K_{24} from K_1

Synchronization Solution: Skip-lists



Example: Reach key K_{24} from K_1 $\Rightarrow$ 5 derivations *instead of* 23 in the sequential scheme!

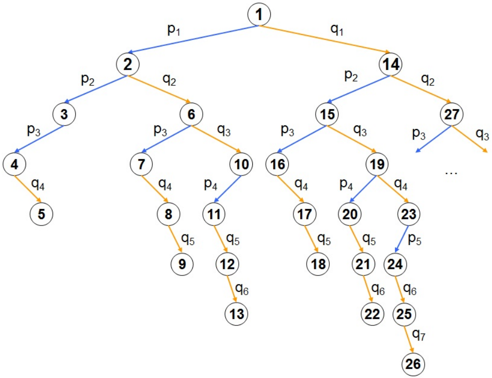
First Proposition



First possibility: one fresh random value per derivation

- # fresh random values ≈ # nodes

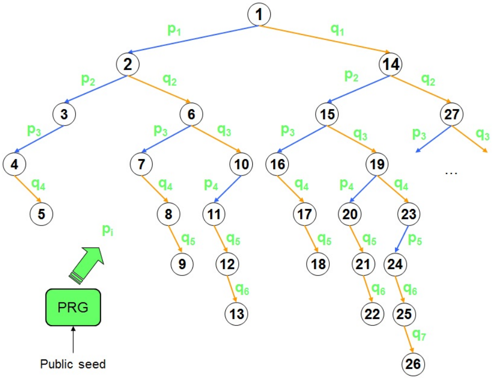
Second Proposition from [FPS12]



Second possibility [FPS12]: one fresh random value per tree layer

- # fresh random values $\approx$ tree depth

Third Proposition from [YS13]



Third possibility [YS13] random values generated by a PRG

- # fresh random values = 1 (seed)

Outline

Instantiation

- weak PRF for the derivation:

Instantiation

- weak PRF for the derivation: AES ✔

Instantiation

- weak PRF for the derivation: AES ✔
- block cipher:

Instantiation

- weak PRF for the derivation: AES ✔
- block cipher: AES ✔

Instantiation

weak PRF for the derivation:	AES	✔
block cipher:	AES	✔
PRG:		

Instantiation

- weak PRF for the derivation: AES ✔
- block cipher: AES ✔
- PRG: AES ✔

Instantiation

- weak PRF for the derivation: AES ✔
- block cipher: AES ✔
- PRG: AES ✔

Only one primitive for the whole encryption scheme:

SPA-resistant AES ✔

Complexity Evaluation

Table: Number of key derivations N

	K_{10}	K_{10^2}	K_{10^3}	K_{10^4}
$\#$stages $= 2, \#$children $= 2$	4	34	$3.3 \cdot 10^2$	$3.3 \cdot 10^3$
$\#$stages $= 5, \#$children $= 5$	5	10	15	20
sequential scheme	10	10^2	10^3	10^4

Complexity Evaluation

Table: Number of key derivations N

	K_{10}	K_{10^2}	K_{10^3}	K_{10^4}
$\#$stages $= 2, \#$children $= 2$	4	34	$3.3 \cdot 10^2$	$3.3 \cdot 10^3$
$\#$stages $= 5, \#$children $= 5$	5	10	15	20
sequential scheme	10	10^2	10^3	10^4

Complexity Evaluation

Table: Number of key derivations N

	K_{10}	K_{10^2}	K_{10^3}	K_{10^4}
$\#$stages $= 2, \#$children $= 2$	4	34	$3.3 \cdot 10^2$	$3.3 \cdot 10^3$
$\#$stages $= 5, \#$children $= 5$	5	10	15	20
sequential scheme	10	10^2	10^3	10^4

$$\begin{aligned} \mathcal{C} &= (\,\#derivations + \#block\ encryptions + \#random\ values)\,\tau_{AES} \\ &= \left(N_k + N_m - 1 + N_m + \frac{N_k + 2N_m - 1}{\lfloor n/\log(1/\epsilon)\rfloor}\right)\tau_{AES} \end{aligned}$$

Outline

Conclusion

- Summary
  - ⋆ **leakage-resilient** symmetric encryption
  - ⋆ **efficient** symmetric encryption
  - ⋆ re-keying scheme **without** PRF
- Further Work
  - ⋆ **more efficient** encryption schemes
  - ⋆ leakage-resilient encryption using **modes of operation**

Thank you