Security in knowledge

Applying Remote Side-Channel Analysis Attacks on a Security-enabled NFC Tag

Thomas Korak

Thomas Plos

Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria.

RSACONFERENCE2013

Session ID: CRYP-R32

Session Classification: Advanced

Outline

- Near Field Communication (NFC)
- Side-Channel Analysis (SCA) Attacks
- Remote SCA Attacks
- Experimental Setup
- Achieved Results
- Discussion of Results
- Conclusion

Basics

Security in knowledge

Near Field Communication (NFC)

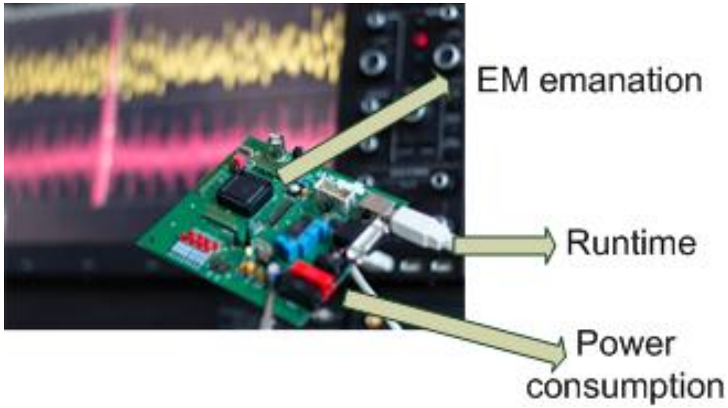
- Contactless (short range) communication technology
- NFC functionality in many smartphones
- (Active) reader communicates with (passive) tag
- Prerequisites for (passive) tags
  - Small chip size, low cost, low power consumption
  - Adequate level of security (using cryptographic primitives (e.g. AES))

http://www.businessinsider.com

http://www.nfcworld.com

Side-Channel Analysis (SCA) Attacks

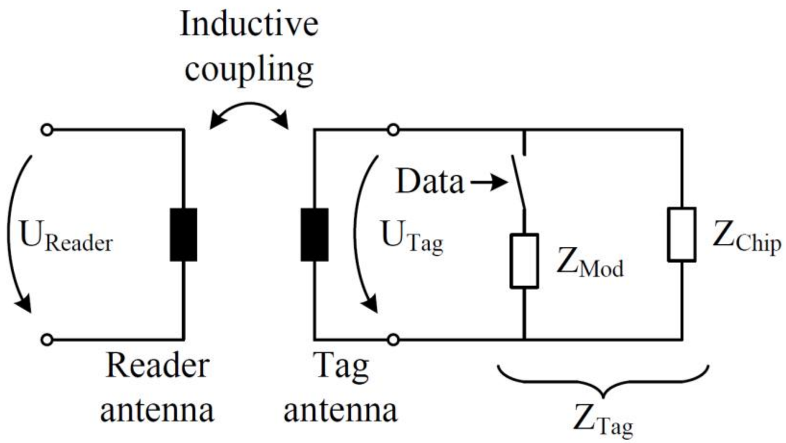
- Powerful attacks against cryptographic primitives
- Measure side-channel information in order to reveal (parts of) a secret
- What are popular side channels?



- Small number of attacks on contactless devices in literature
  - Most of them in close proximity
- Our work: Remote SCA attack on an NFC device

Remote SCA Attacks

- Measure EM emanation of the chip
  - Distance between chip and measurement probe
  - Reader signal is much stronger than side-channel signal
- Known solutions
  - Separate chip from antenna (Carluccio et al. [1])
  - Use analogue demodulation (Kasper et al. [2])
- Our approach
  - Strong reader field = carrier for data-dependent signal
  - *Parasitic load modulation*

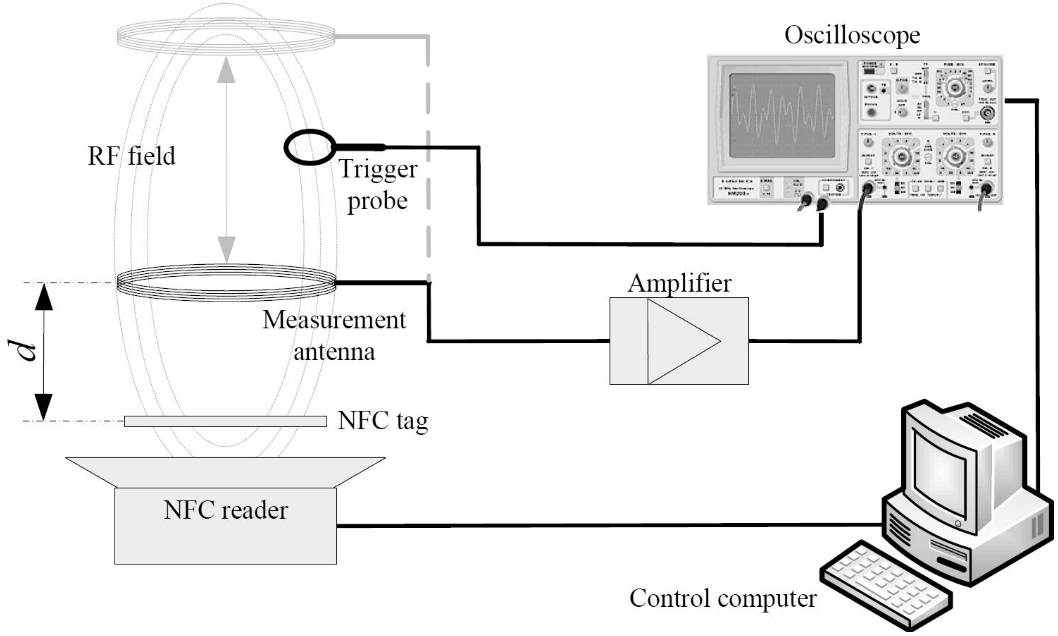


Experimental Setup

Security in knowledge

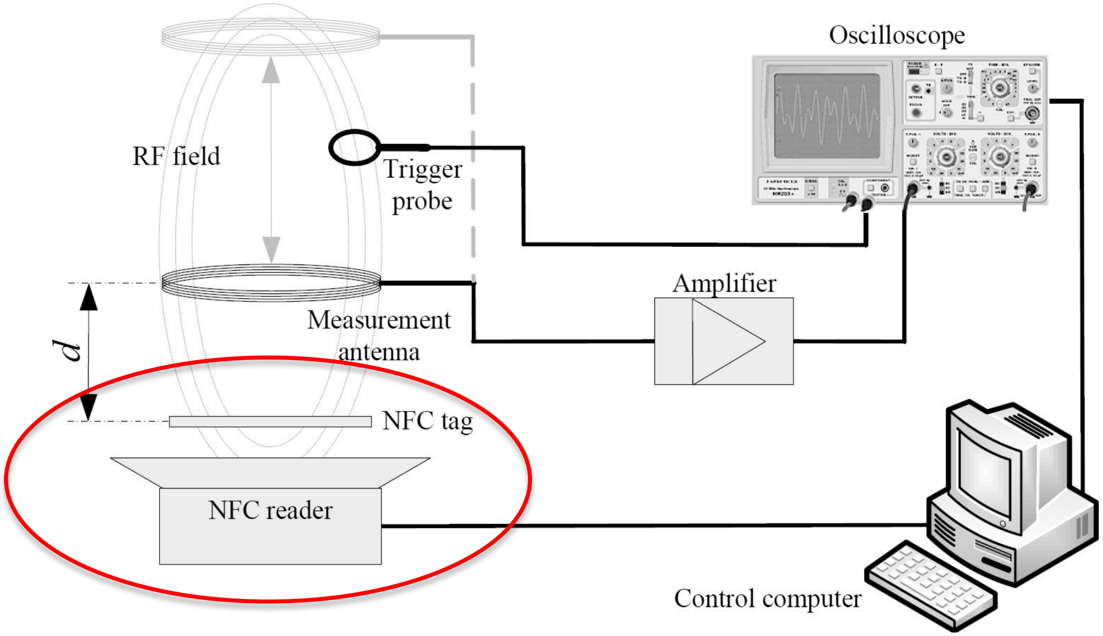
Experimental Setup

- Main parts



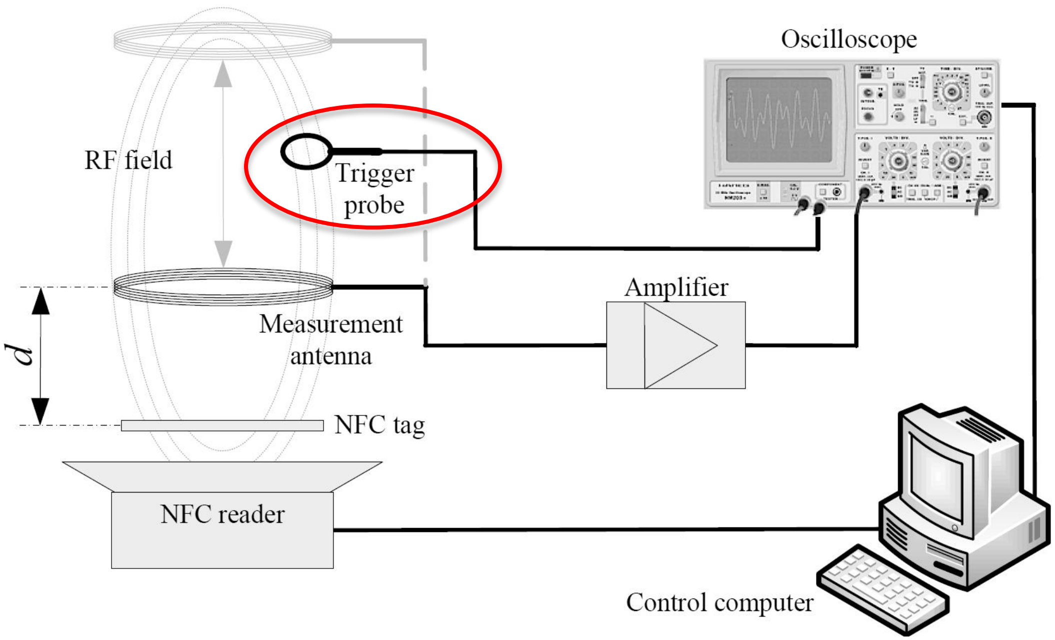
Experimental Setup

- Main parts
  - NFC reader, NFC tag (AES with secret key)



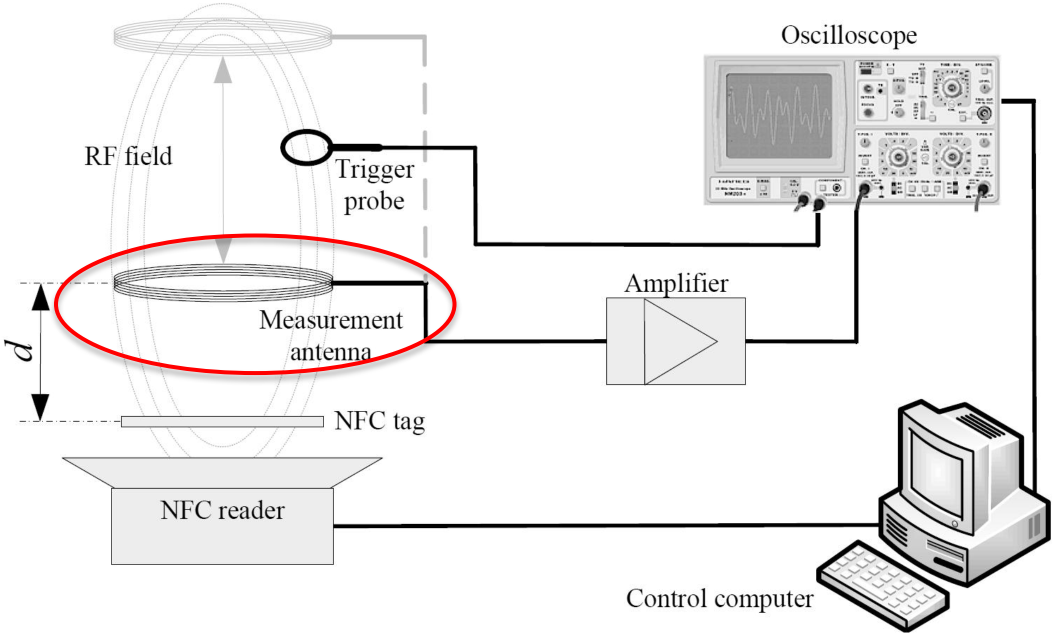
Experimental Setup

- Main parts
  - NFC reader, NFC tag (AES with secret key)
  - Trigger probe



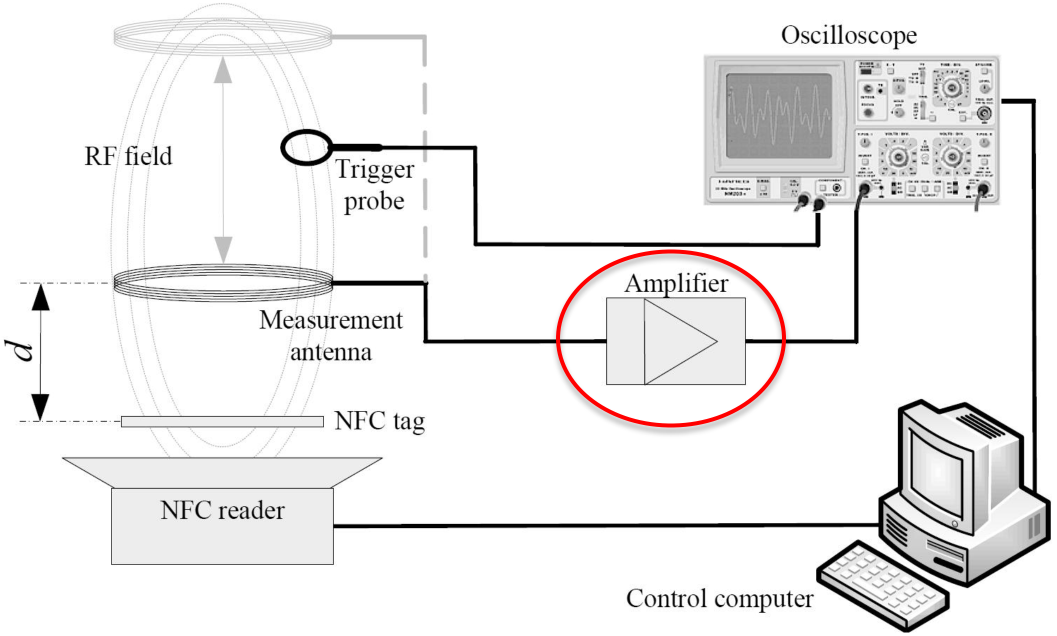
Experimental Setup

- Main parts
  - NFC reader, NFC tag (AES with secret key)
  - Trigger probe
  - Measurement antenna (self-made, 8cm diameter, 5 windings)



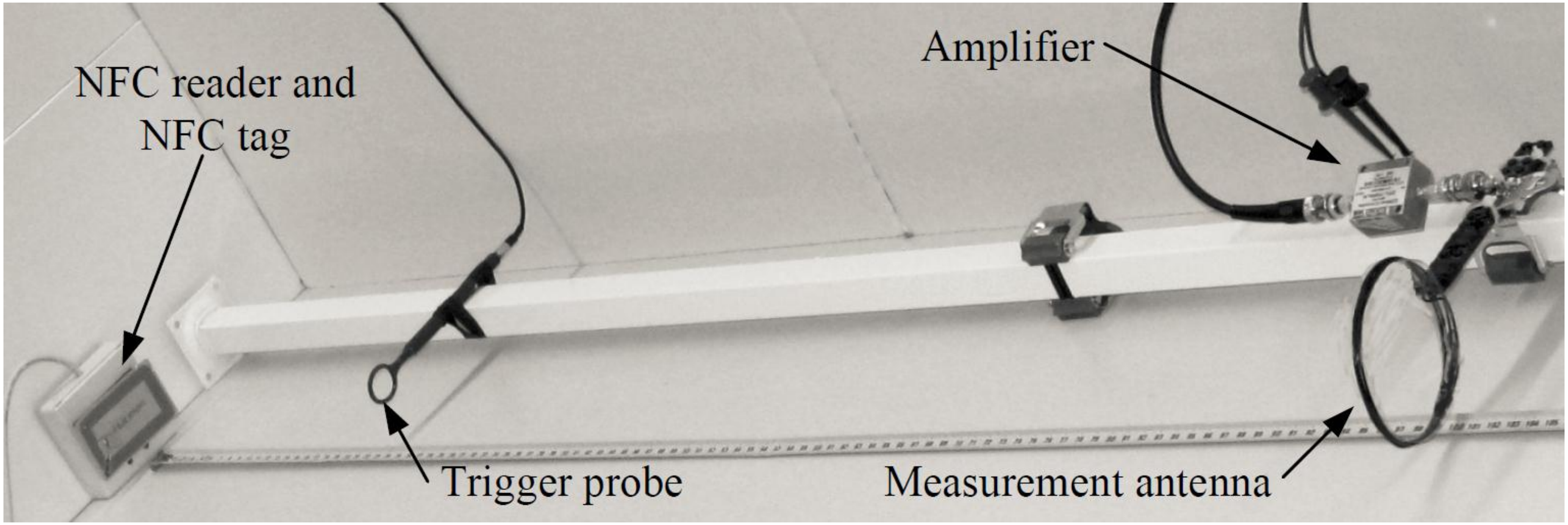
Experimental Setup

- Main parts
  - NFC reader, NFC tag (AES with secret key)
  - Trigger probe
  - Measurement antenna (self-made, 8cm diameter, 5 windings)
  - Amplifier



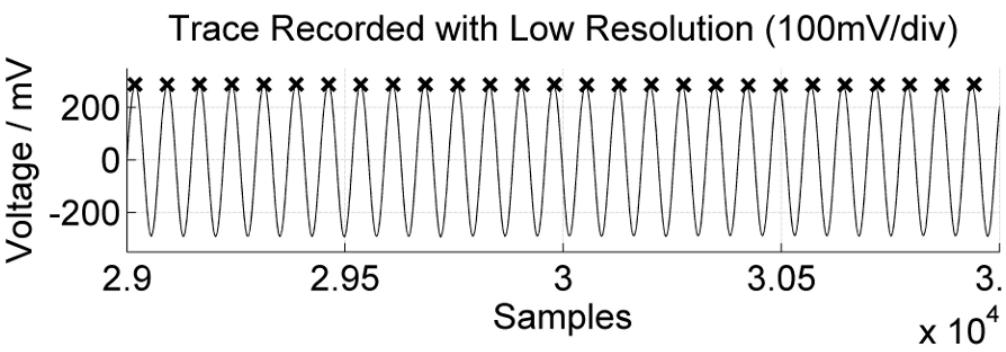
Experimental Setup

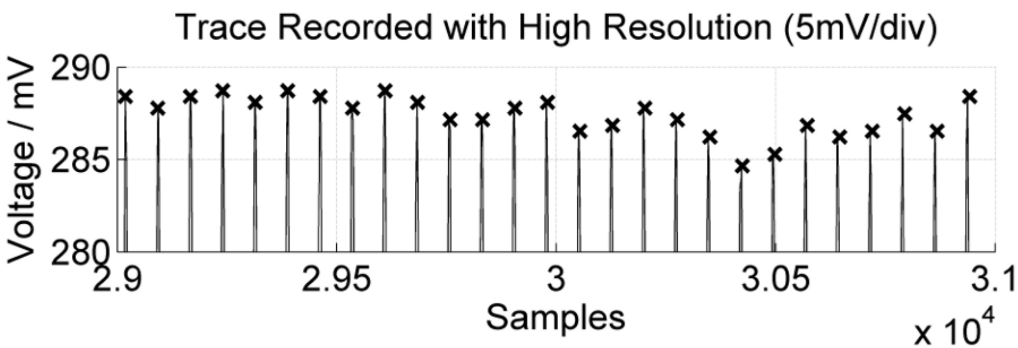
- Main parts
  - NFC reader, NFC tag (AES with secret key, key known by us)
  - Trigger probe
  - Measurement antenna (self-made, 8cm diameter, 5 windings)
  - Amplifier



Experimental Setup cont.

- Trace recording
  - Increase resolution
  - Only measure peaks of the signal
  - Decrease trace size using downsampling
  - Zoom factor (f_{zoom})





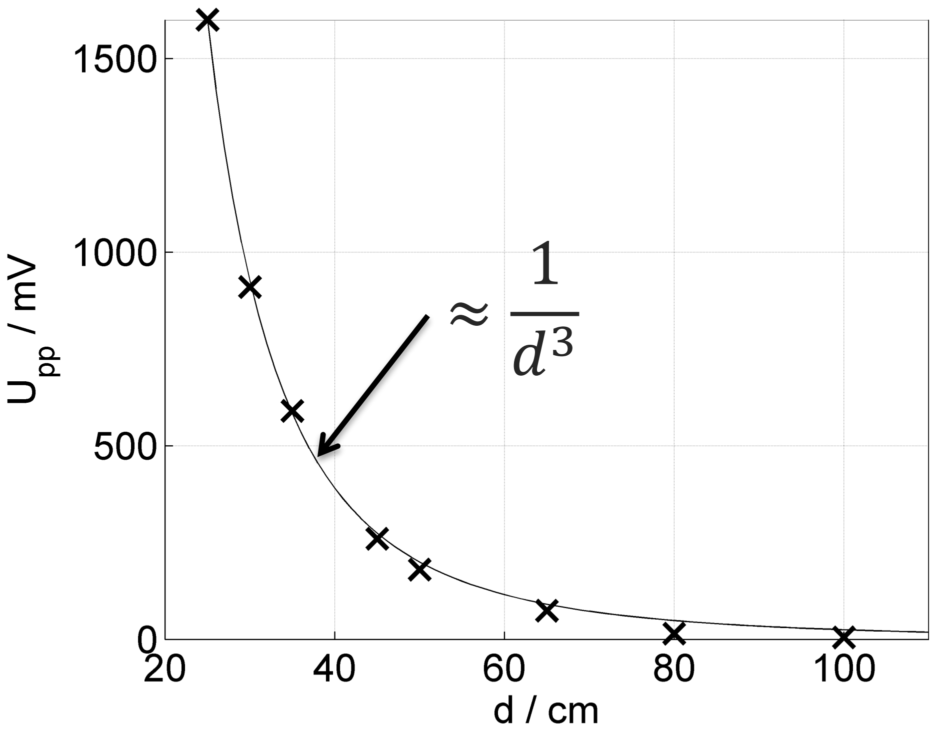
Achieved Results

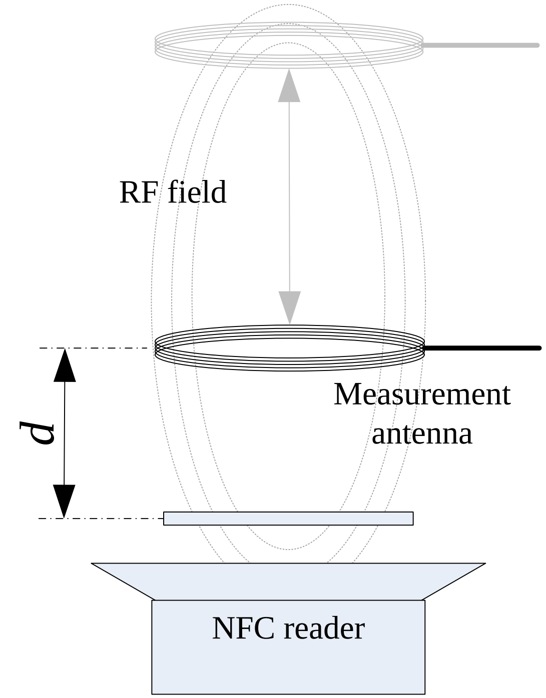
Security in knowledge

Achieved Results

- Influence of distance on peak-to-peak voltage (U_{pp})

$$U_{pp} = f(d)$$

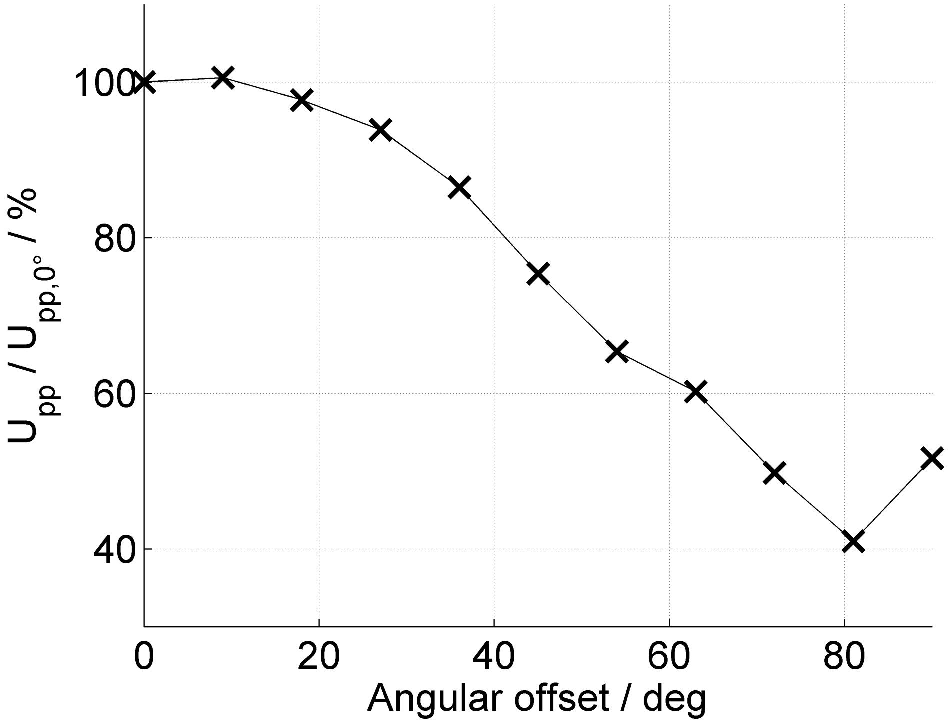


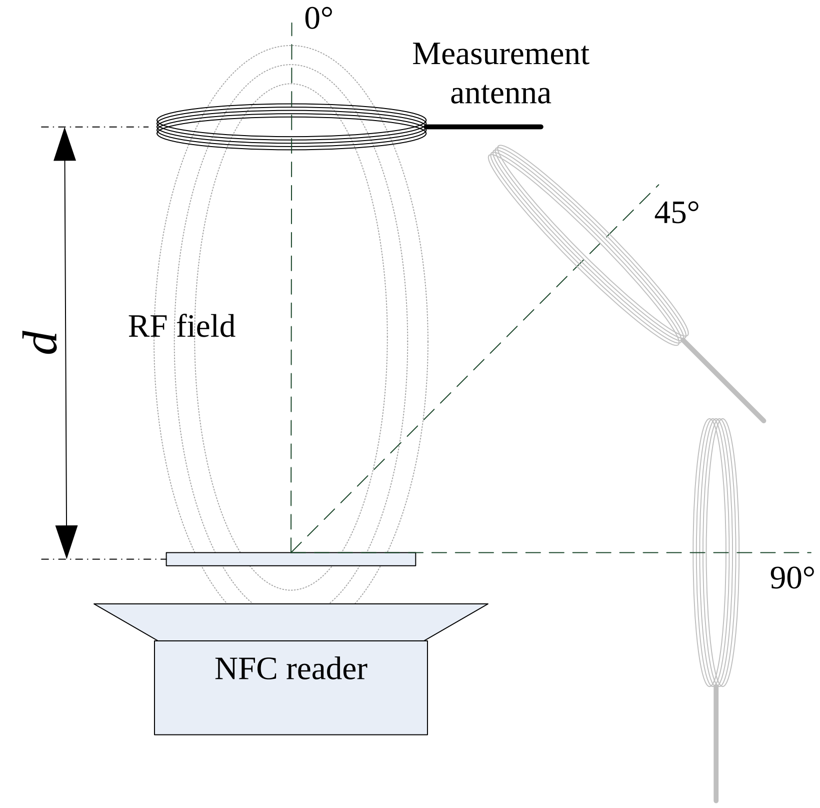


Achieved Results cont.

- Influence of angular offset on peak-to-peak voltage (U_{pp})

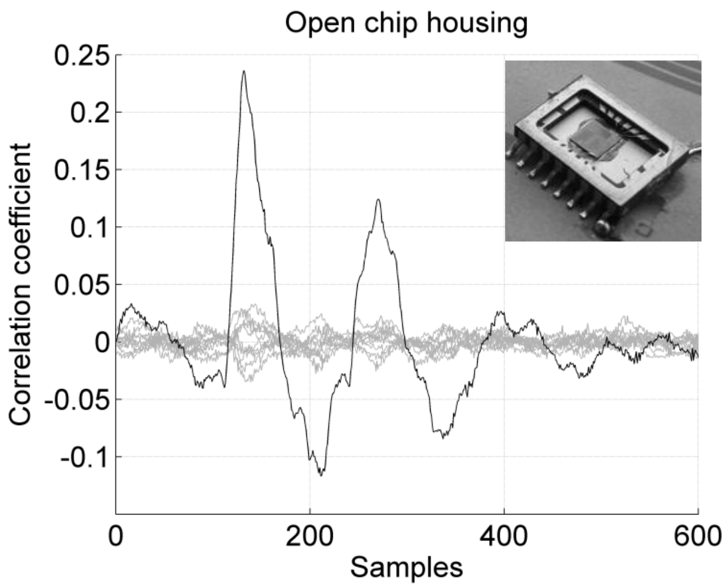
$$U_{pp} = f(angular\ offset)$$



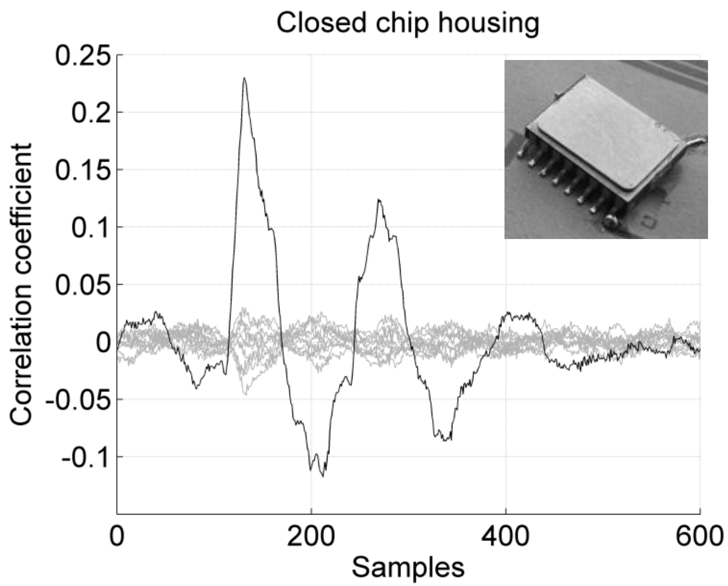


Achieved Results cont.

- Verification of the *parasitic load modulation*
  - Two scenarios: Opened and closed chip housing
  - 20 sets each containing 5000 traces at 7 cm distance
  - Calculate mean and standard deviation of correlation values



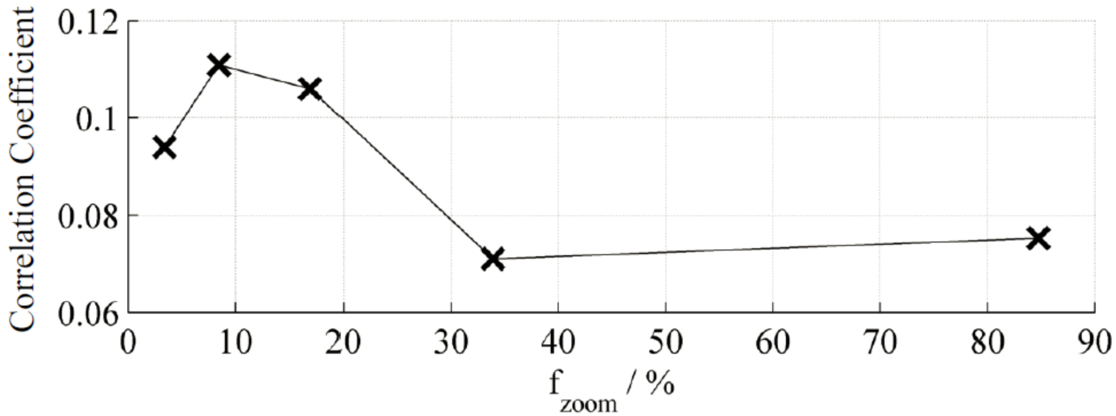
$$\bar{\rho}_{opened} = 0.244$$
$$\sigma_{opened} = 0.032$$



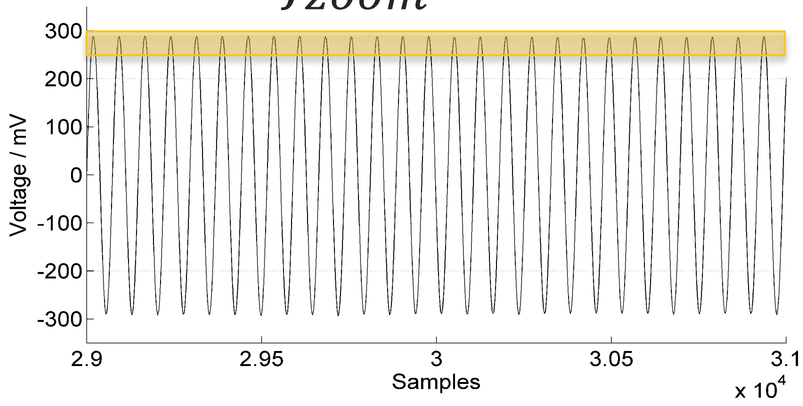
$$\bar{\rho}_{closed} = 0.246$$
$$\sigma_{closed} = 0.025$$

Achieved Results cont.

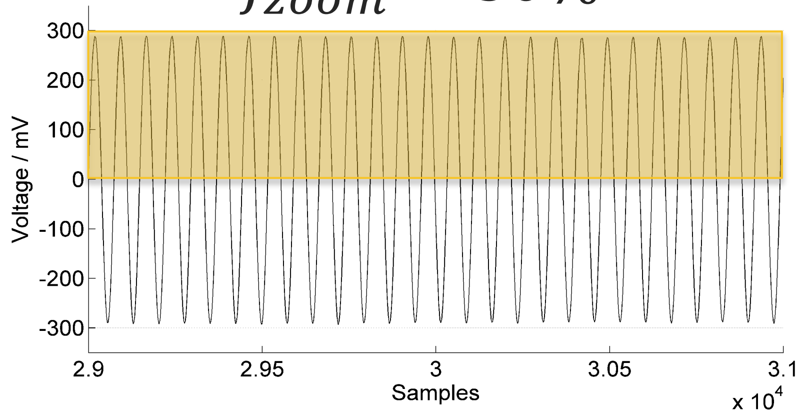
- Find best f_{zoom}



$f_{zoom} = 10\%$

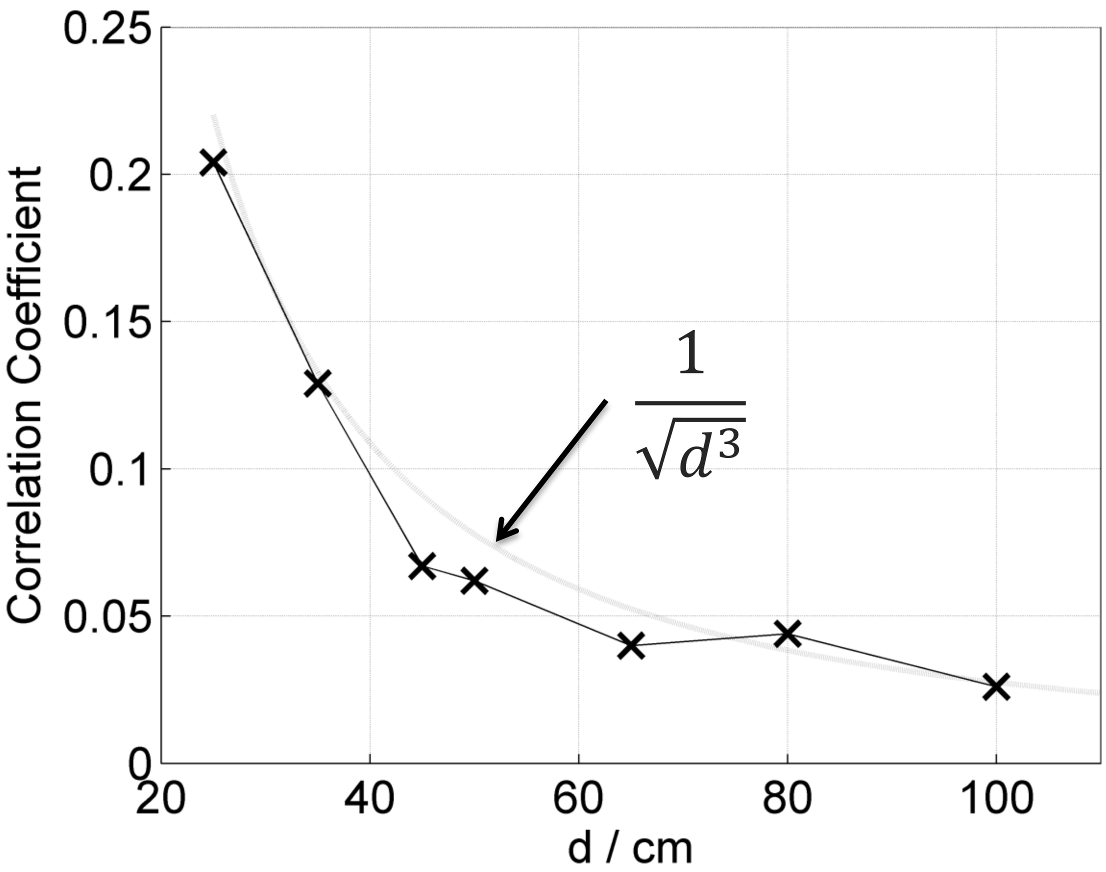


$f_{zoom} = 50\%$



Achieved Results cont.

- Relationship between correlation coefficient and distance



$$\rho \approx \frac{1}{\sqrt{d^3}}$$

Discussion & Conclusion

Discussion

- Successful remote SCA attacks between 25 cm and 100 cm
  - 25 cm 3,000 traces required
  - 100 cm 30,000 traces required
- For distances exceeding 80 cm amplifier gain increased
  - In order to achieve desired f_{zoom} values
- Reader and tag in close proximity
  - Power tag from distance
  - Literature available (Kfir et al. [3])

Conclusion

- Performed remote SCA attacks on an NFC prototype tag
- No special equipment required
- Examined different distances up to 1 m
  - Reading range only a few centimeters
  - *Parasitic load modulation*
- Only record peaks of the signal and perform downsampling
  - Increase resolution
  - Decrease trace size
- Tackle attack
  - Introduce countermeasures (e.g., random delays)
  - Limit number of cryptographic operations

Thank you for your attention!

Questions?

References

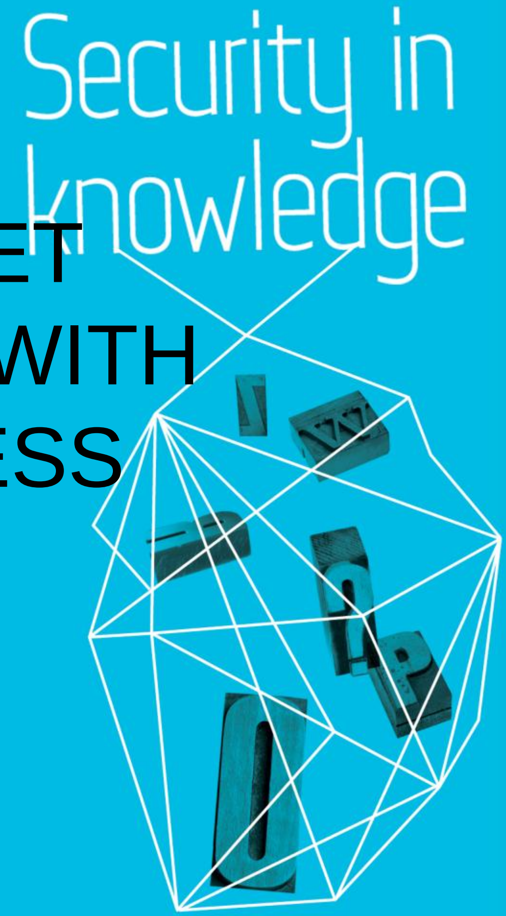
[1] Carluccio, D., Lemke, K., Paar, C.: *Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results.* In: Oswald, E. (ed.) RFIDSec 2005, Graz, Austria, July 13-15, pp. 44–51 (2005)

[2] Kasper, T., Oswald, D., Paar, C.: *EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment.* In: Youm, H.Y., Yung, M. (eds.) WISA 2009. LNCS, vol. 5932, pp. 79–93. Springer, Heidelberg (2009)

[3] Kfir, Z., Wool, A.: *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems.* In: Proceedings SecureComm 2005, Athens, Greece, September 5-9, pp. 47–58. IEEE Computer Society (2005)

RSA CONFERENCE 2013

PRACTICAL LEAKGE-RESILINET PSEUDO-RANDOM OBJECTS WITH MINIMUM PUBLIC RANDOMNESS



Yu Yu
Tsinghua University and East China Normal University

Francois-Xavier Standaert
UCL Crypto Group

Session ID: CRYP-R32

Session Classification: Advanced

Outline of the talk

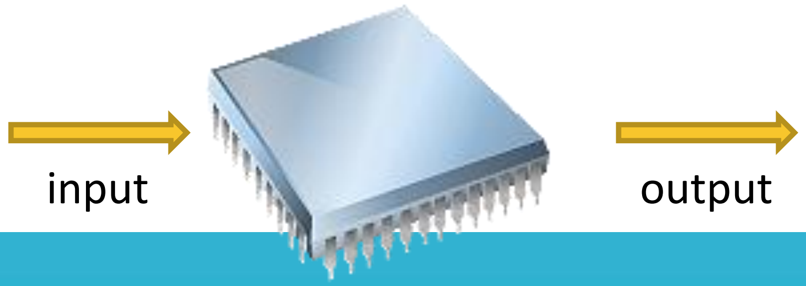
- Side-channel Attacks and Countermeasures
- Leakage-Resilient Stream Ciphers
  - FOCS 2008 / Eurocrypt 2009 Constructions
  - CCS 2010 / CHES 2012 Constructions
- Our Construction
  - Overview
  - Security Analysis

How cryptography works?

- Typical Assumptions:

  (1) A computational hard problem (RSA, DLP, AES).

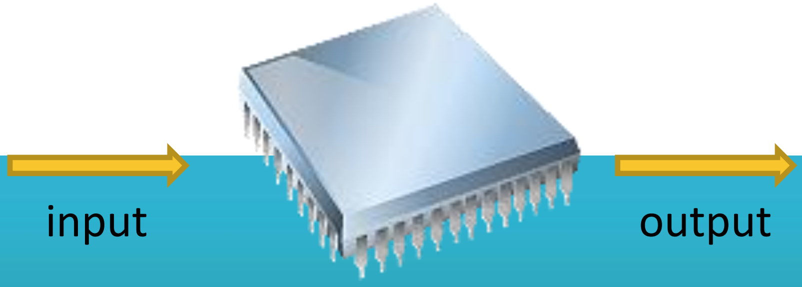
  (2) Black-box: attacker ONLY sees input-output and follows the protocol.
- Provable Security: Under assumptions #1 and #2, if one breaks the crypto-system (in polynomial-time), then it leads to efficient solution to the underlying hard problem, and hence acontradiction .
- Security guarantee voided if either assumption is not met.



Are these assumptions safe?

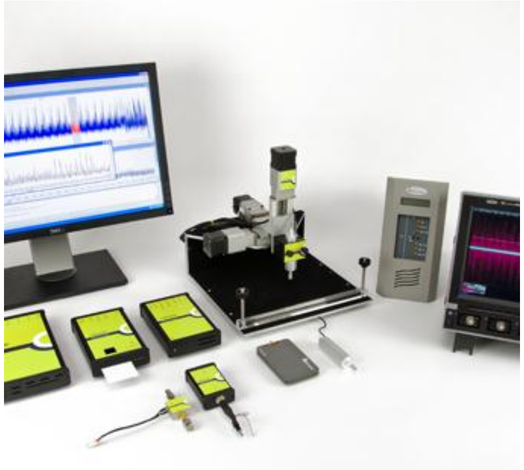
- Typical Assumptions:
  - A commonly believed computational hard problem (RSA, DLP, AES), where the secret key is randomly chosen from the key space.
  - Black-box: attacker ONLY sees its input-output behavior and follows the protocols.
- Assumption #1 is ok, or otherwise a breakthrough.
- Assumption #2 not always respected.

The implementation of a cryptographic algorithm (e.g. a security chip) might be leaking in many forms.



Side-channel attacks and beyond

- Definition: Any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms.
- It takes many forms:
  - Timing Attacks
  - Power Analysis (PA)
  - Electro-Magnetic Analysis (EM
  - Acoustic Analysis
  - etc.
- More invasive physical attacks: fault injections attacks.




Countermeasures against SCA

- Implementation level .
  - Software countermeasures: Masking, Hiding, etc.
  - Hardware countermeasures: dual-rail pre-charge logic styles (e.g. SABL ,WDDL).
- Design (algorithmic) level.
  - Leakage-Resilient Cryptography: design of cryptographic protocols that remain secure in the presence of arbitrary, yet bounded, leakage about the secret key.

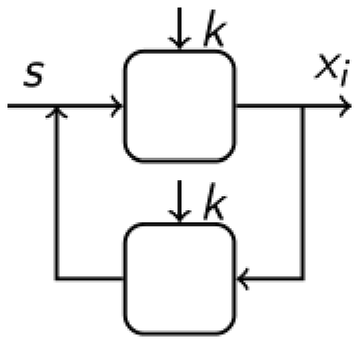
Leakage-Resilient Stream Ciphers

- What is a stream cipher?

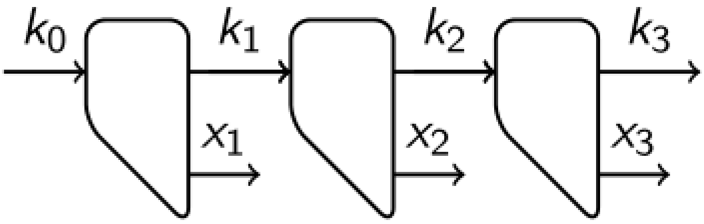
A symmetric key cipher where plaintext digits are combined with a pseudorandom key-stream.

- In practice, a stream cipher can be based on a block cipher (or PRG), and operate in iterations.

ANSI X9.17 PRG



Forward secure PRG
[BM82,Koc03]



How to model the leakages?

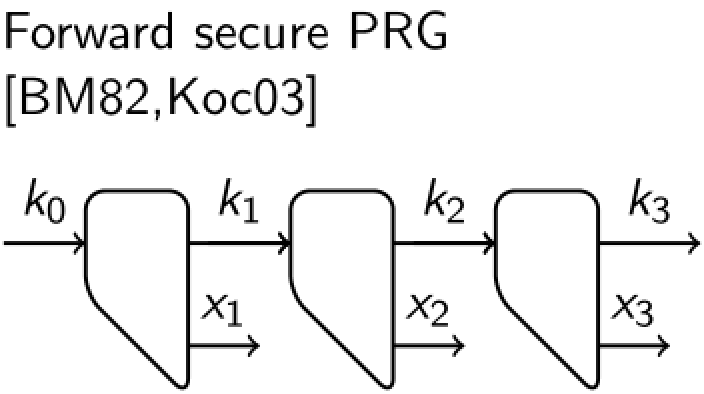
- We admit arbitrary but restricted leakages.
- Let L on n-bit input K be the leakage function.
- L is subject to the following restrictions.
  - Arbitrary.

    L is any efficiently computable function.
  - Bounded leakage [DP08,Pie09].

    For each i-th iteration, L_i has bounded range,

    i.e., $L_i : \{0,1\}^n \rightarrow \{0,1\}^{\lambda}$ for $\lambda < n$.

Is bounded leakage sufficient?



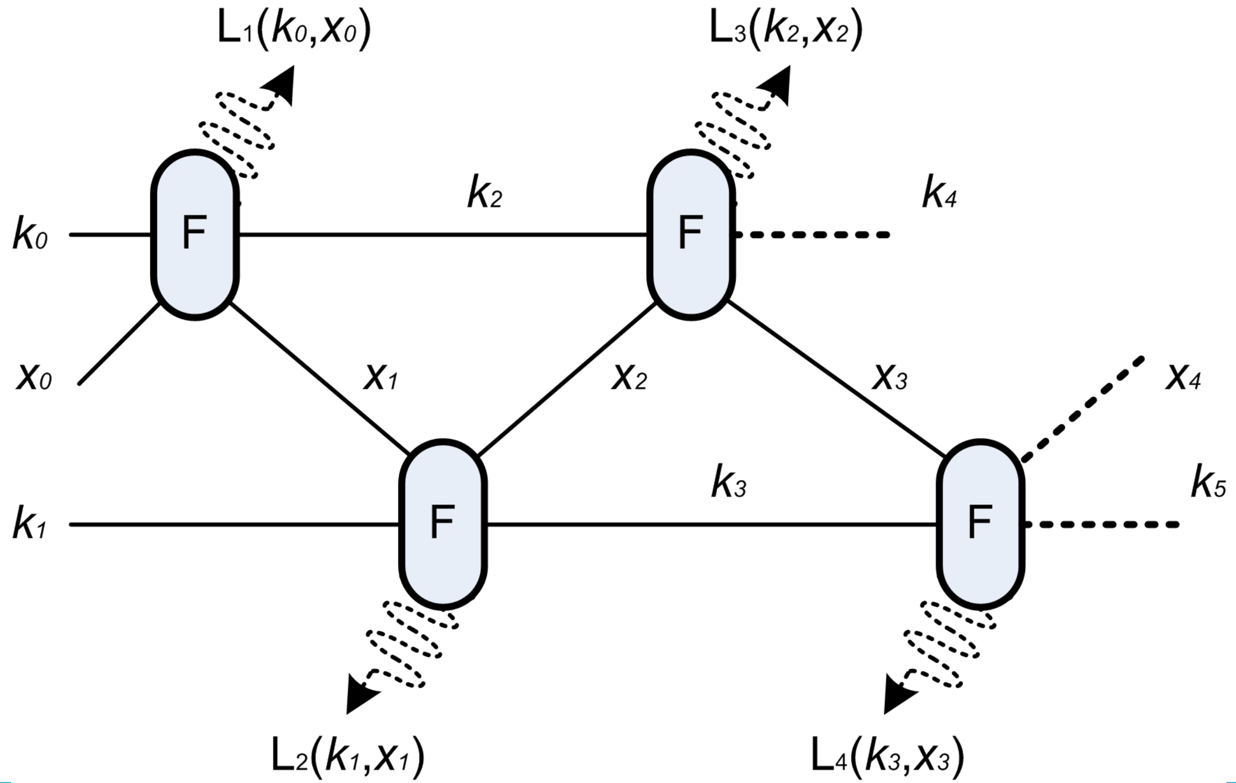
- Without side-channels, it is a secure stream cipher.
- Is it leakage-resilient in the bounded leakage model?
- No. Future computation attacks,

  let each $L_i(k_i)$ be the i-th bit of some future state, say k_{100}.

  Note a realistic attack, but sufficient to show the SC is not provably leakage-resilient.

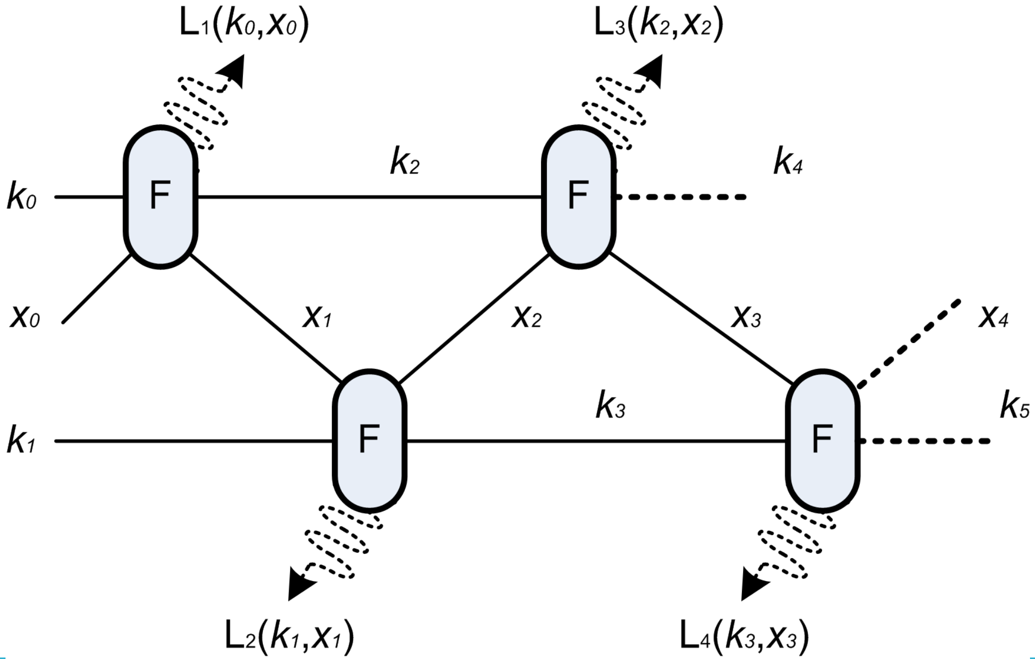
Leakage-Resilient Stream Ciphers in the Bounded Leakage Model

- In FOCS 2008, Dziembowski and Pietrzak presented a SC based on “alternating extraction”.



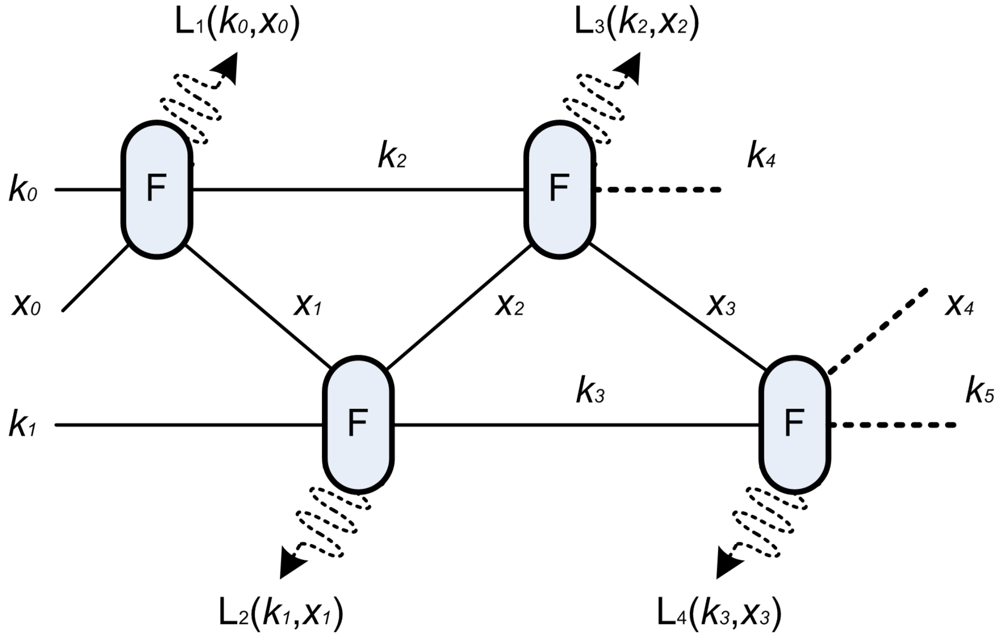
The FOCS 2008 Construction

- Key in two halves (k_0,k_1), public random value x_0.
- Function F is instantiated by a randomness extractor Ext and a pseudo-random generator G, i.e., $F(k_i,x_i)=G(Ext(k_i,x_i))$.
- Technical Ingredients: the output of an ε-secure PRG $G:\{0,1\}^n \rightarrow \{0,1\}^{2n}$, when leaking about any $\lambda \in O(\log(1/\varepsilon))$ bits, will be having $2n - \lambda$ bit of pseudo-entropy.



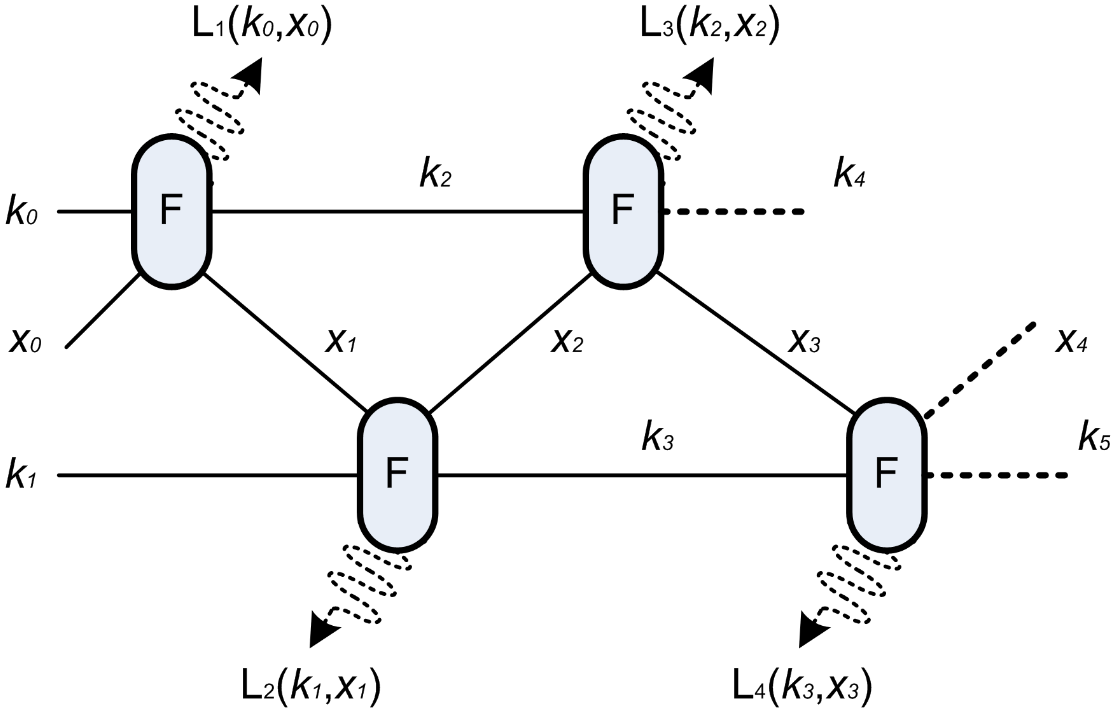
The FOCS 2008 Construction

- Security (informal): even if the SC continuously leak λ bits (per iteration) of adaptively chosen leakages, for as many as iterations, the final output (in absence of corresponding leakage) will be pseudo-random.



The Eurocrypt 2009 Construction

- Pietrzak simplified the FOCS 2008 construction: replacing the extractor+PRG with a weak PRF.
- Technical lemma: weak PRF is a computational extractor.



Pros and Cons of the FOCS 2008/ Eurocrypt 2009 Constructions

- Advantage: strong security.

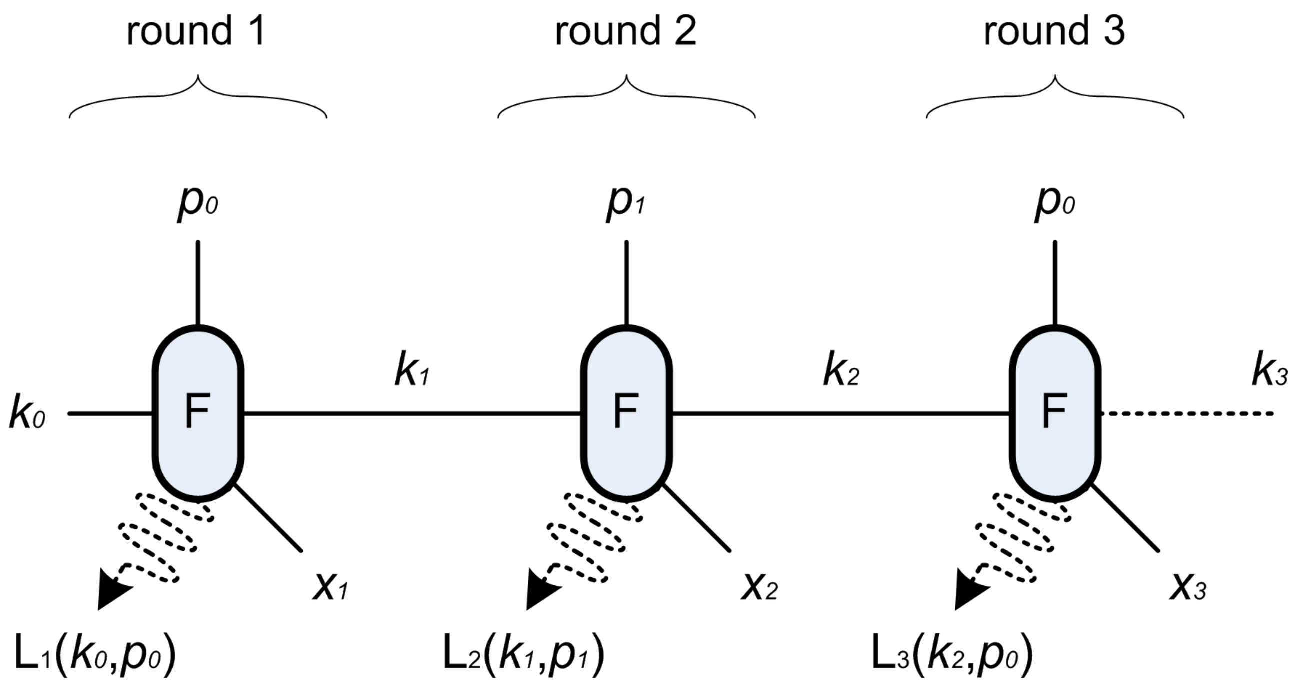
  I.e., prior to each iteration, the adversary can adaptively chosen the leakage function he wants to subscribe.

  Is this necessary ?
- Disadvantage:
  - a bit complicated (artificial ?) construction.
  - Efficiency issue: 2n bits of secret key only guarantees n bits of security.
- Question: can we construct something more practical?
  - Hint: use the tradeoff between the above advantage and disadvantage.

The CCS 2010 Construction

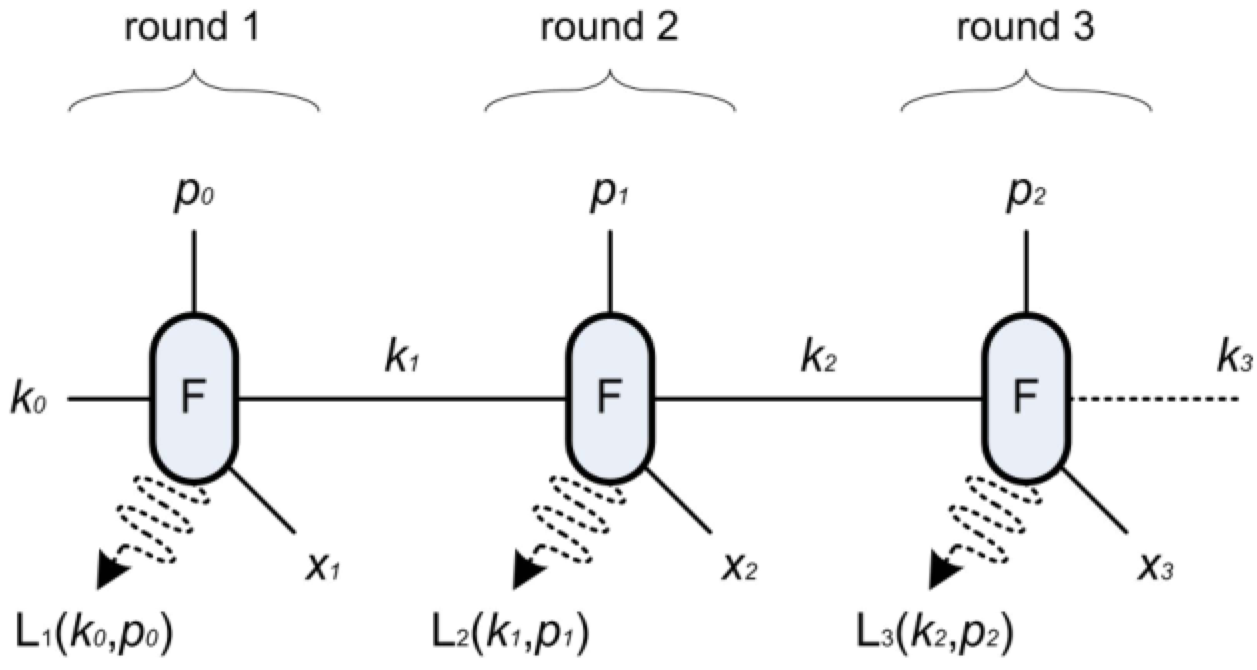
- Yu et al. proposed a more practical construction.

The idea: use alternating public values p_0 and p_1, and only allow non-adaptive (prefixed)) leakages.



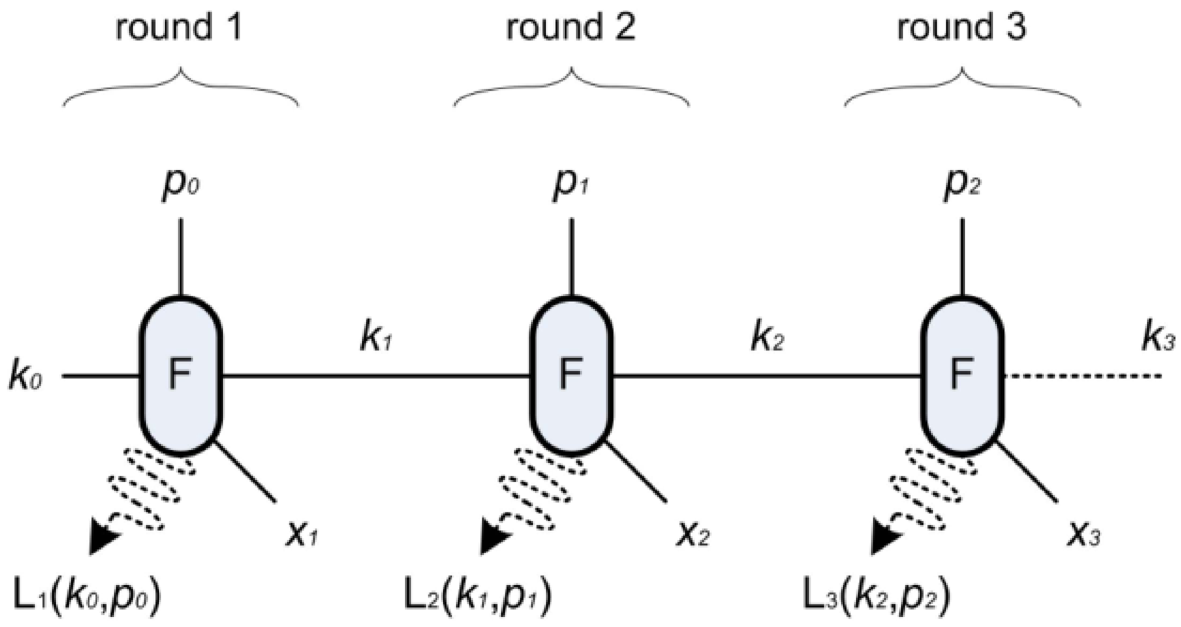
The CHES 2012 Construction

- Faust et al. pointed out that the CCS 2010 SC needs more public values than 2 in the standard model.
- Thus, not randomness efficient.

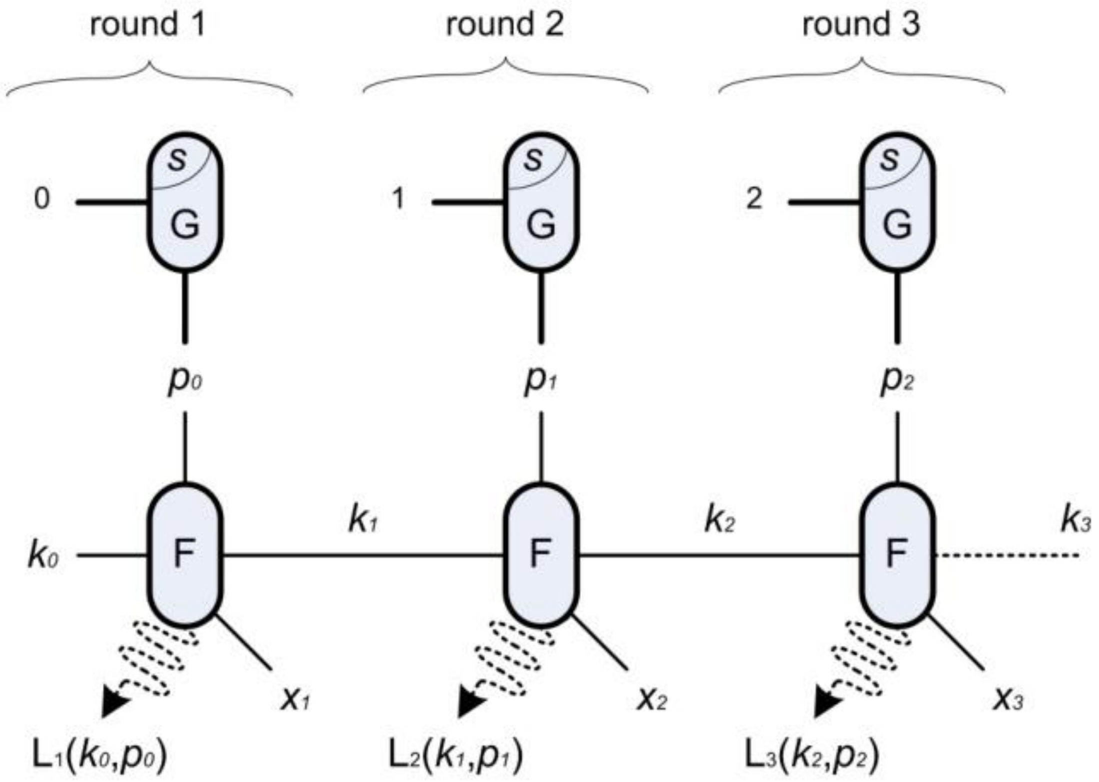


Our motivation

- Can we reprove the CHES 2012 construction with much less public randomness (ideally one string)?
- The main contribution of our paper.



Overview of our construction

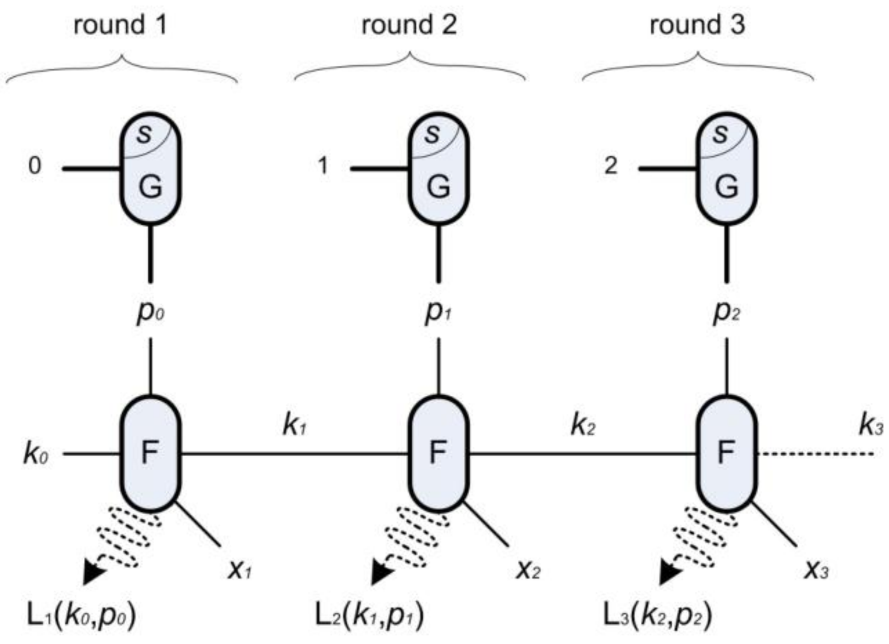


Use a public seed s to generate all public random strings p_0, p_1, p_2,…., where G is a pseudo-random function, e.g. , p_i=G(s, i) = AES_s(i).

The upper part is running in public.
The lower part follows bounded leakage, i.e., each L_i leaks λ bits.

How can we prove this?

- Trivial (due to CHES 2012) if s is kept secret and only $p_0, p_1, \ldots,$ are given to the adversary.
- The goal: showing that the security holds even if the adversary sees seed s.

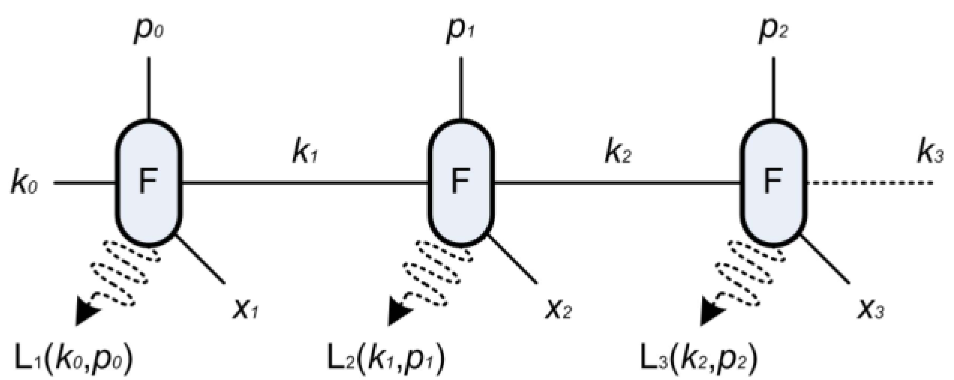


CHES 2012 Construction

- Theorem (CHES 2012,informal). For any l ∈ poly(n), every adversary predicts b_B with probability ½+negl(n).

Alice	Eve	Bob
$s \leftarrow U_n$	$\xrightarrow{p_0, \cdots, p_{\ell-1}}$	$k_0 \leftarrow U_n$
$p_0, \cdots, p_{\ell-1} \leftarrow \mathsf{G}(s,0), \cdots, \mathsf{G}(s, \ell-1)$		Evaluate SC on $k_0, p_0, \cdots, p_{\ell-1}$
		to get $\mathsf{view}_\ell \setminus s$ and x_ℓ
		$b_\mathsf{B} \leftarrow U_1$
	$\xleftarrow{r, \mathsf{view}_\ell \setminus s}$	if $b_\mathsf{B} = 0$ then $r := x_\ell$
		else if $b_\mathsf{B} = 1$ then $r \leftarrow U_n$

$$\mathsf{view}_\ell \stackrel{\text{def}}{=} (S, X_1, \cdots, X_{\ell-1}, \mathsf{L}_1(K_0, P_0), \cdots, \mathsf{L}_{\ell-1}(K_{\ell-2}, P_{\ell-2}))$$



Proof sketch.

- If by contradiction that when additionally given S, there exists efficient D and constant c such that Pr[D(R,view$_l$)=b$_B$] >=½+n^{-c}. Then, it implies the following 2-pass key agreement protocol.
- The protocol extends to public key encryption by parallel repetition, which is a contradiction to the known separation that no black-box construction of PKE from PRG [Impagliazzo and Rudich, STOC 89].
- The contradiction also implies an OT protocol.

Alice	Eve	Bob
$s \leftarrow U_n$	$\xrightarrow{p_0, \cdots, p_{\ell-1}}$	$k_0 \leftarrow U_n$
$p_0, \cdots, p_{\ell-1} \leftarrow \mathsf{G}(s, 0), \cdots, \mathsf{G}(s, \ell-1)$		Evaluate SC on $k_0, p_0, \cdots, p_{\ell-1}$
		to get $\mathsf{view}_\ell \setminus s$ and x_ℓ
		$b_\mathsf{B} \leftarrow U_1$
	$\xleftarrow{r, \mathsf{view}_\ell \setminus s}$	if $b_\mathsf{B} = 0$ then $r := x_\ell$
$b_\mathsf{A} \leftarrow \mathsf{D}(r, \mathsf{view}_\ell)$		else if $b_\mathsf{B} = 1$ then $r \leftarrow U_n$

Conclusion

- Practical leakage-resilient stream ciphers in the standard model with simple construction and minimal public randomness.
- One can also use the technique to construct leakage-resilient (GGM based) pseudo-random function (against non-adaptive inputs and leakages).

Questions.

Thanks!