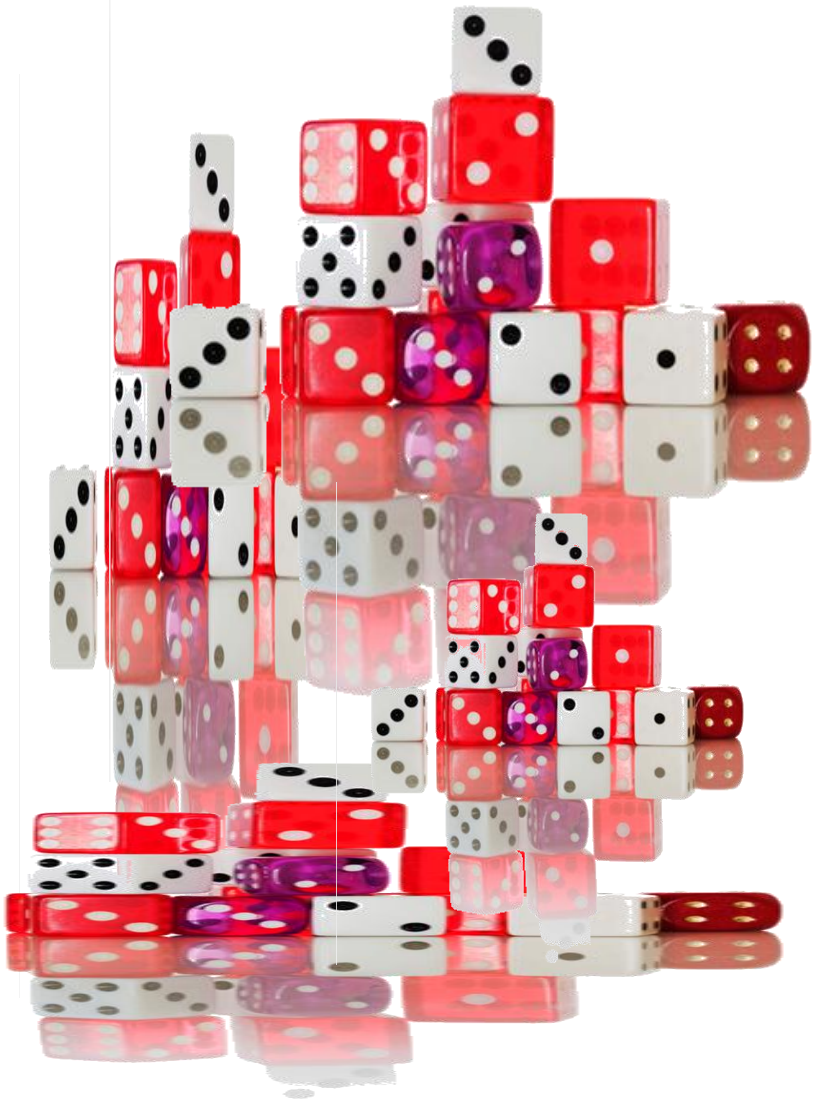
Extractors Against Side-Channel Attacks: Weak or Strong?

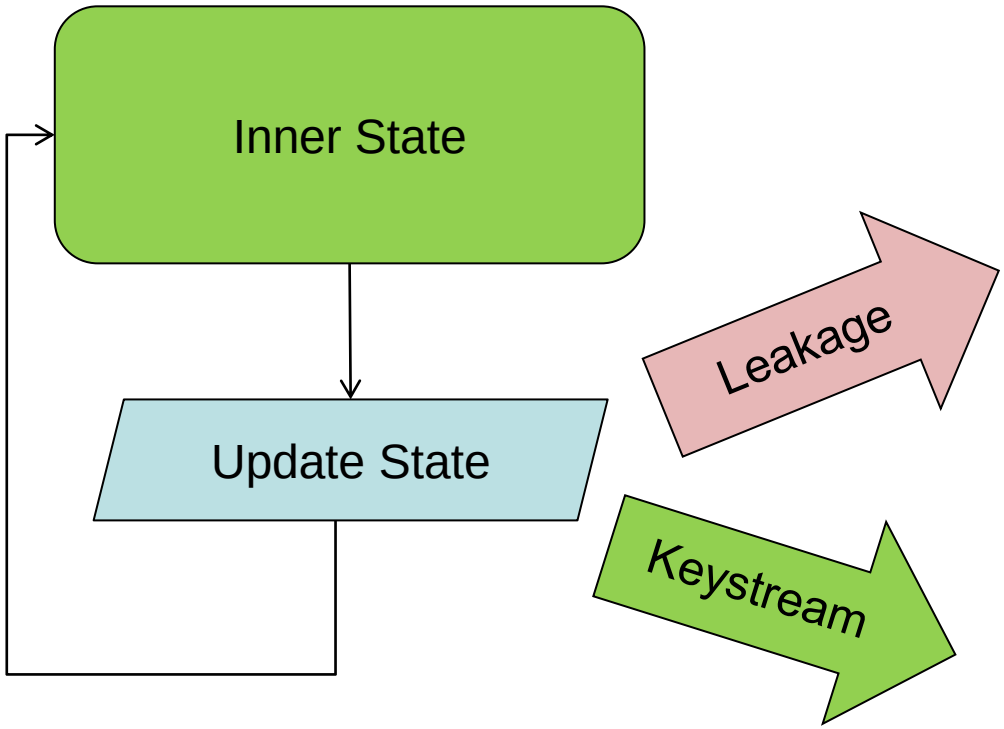
Marcel Medwed, Francois-Xavier Standaert

UCL Crypto Group

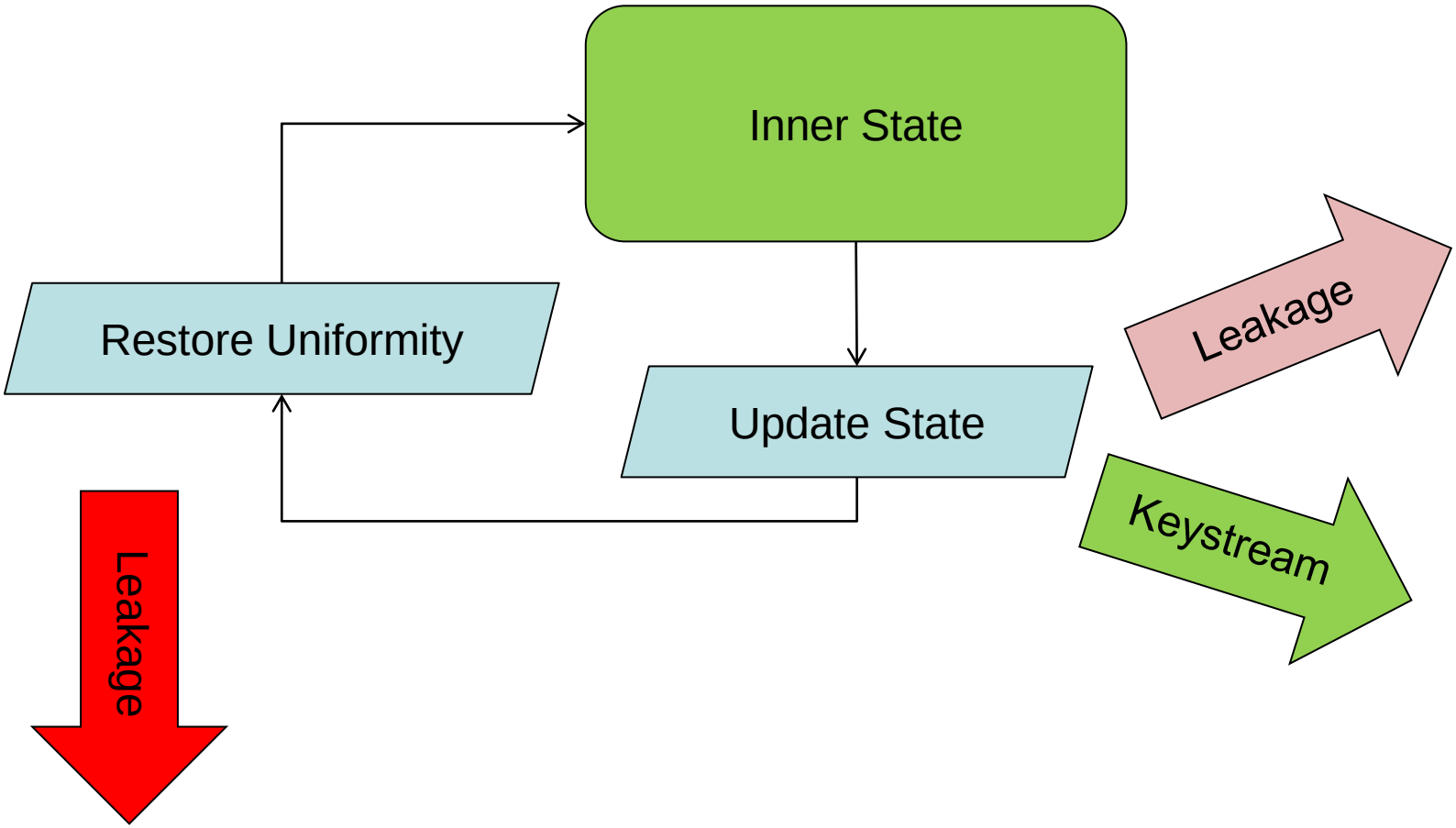
Extractors?



Stream Cipher



FOCS 2008:
Leakage Resilient Cryptography



Latincrypt 2010: How leaky are extractors?

- A 8-bit software implementation can easily undermine the security of the construction

Therefore...

...how does a hardware implementation perform?

- Throughput
- Parallelism

...what does it mean for the leakage?

...what about countermeasures?

Outline

Motivation

The Extractor

IT Analysis

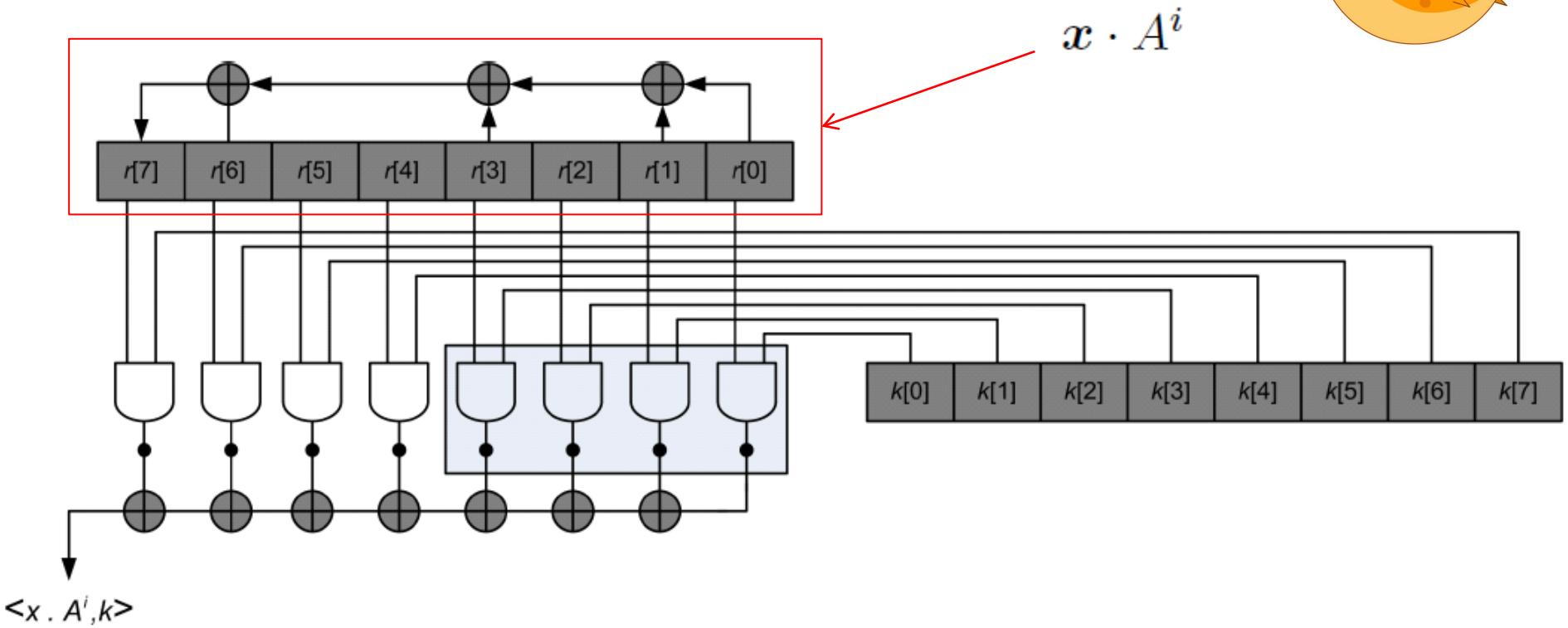
Security Analysis

Conclusions

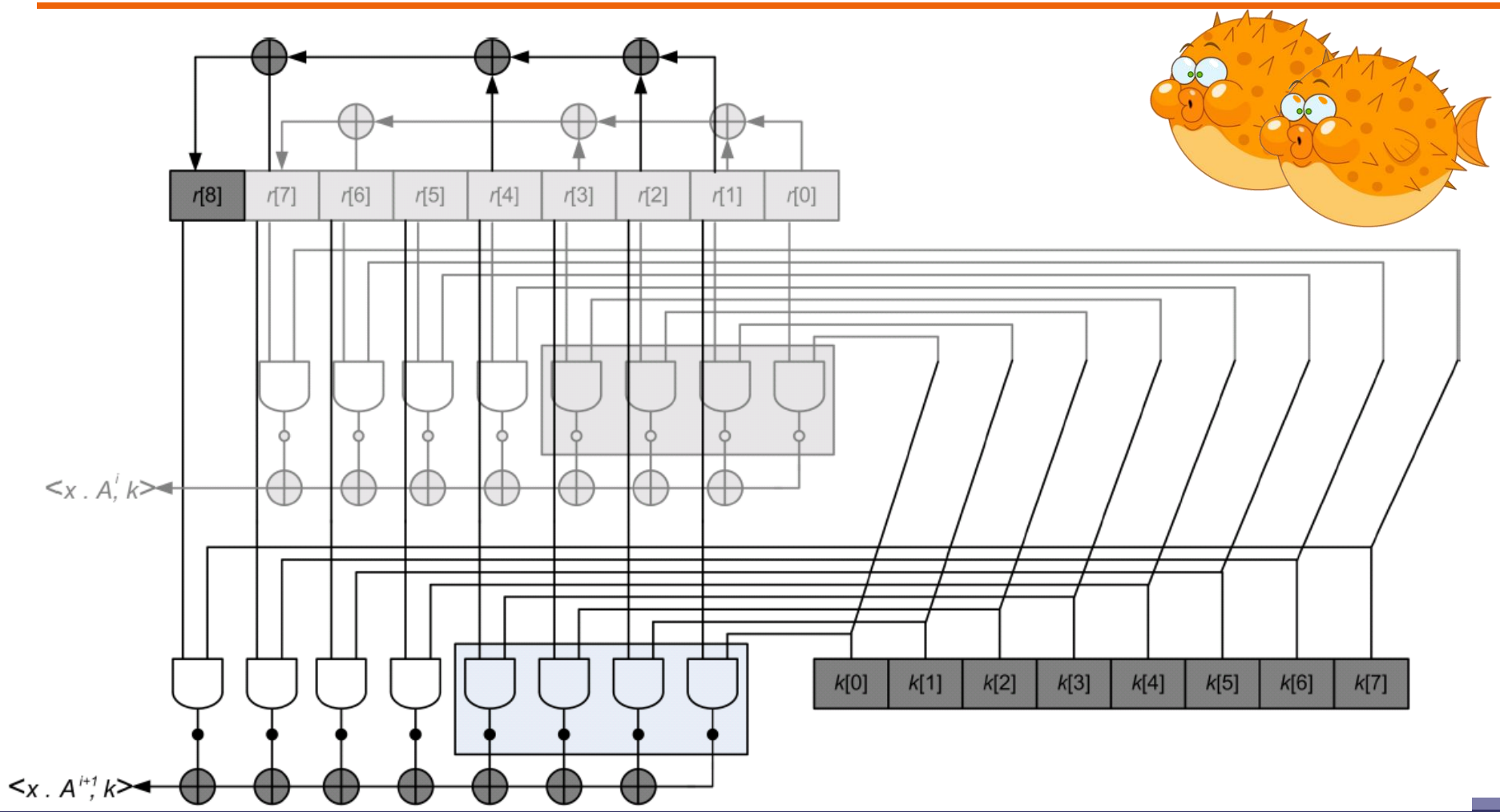
Low Complexity Extractor

$$\boxplus : \boldsymbol{k} \times \boldsymbol{x} \mapsto [\langle \boldsymbol{x} \cdot A^0, \boldsymbol{k} \rangle, \langle \boldsymbol{x} \cdot A^1, \boldsymbol{k} \rangle, \cdots, \langle \boldsymbol{x} \cdot A^{m-1}, \boldsymbol{k} \rangle]$$

Basic Architecture



Parallelism



Masking

$$\langle \boldsymbol{x} \cdot A^i, \boldsymbol{k} + \boldsymbol{m} \rangle + \langle \boldsymbol{x} \cdot A^i, \boldsymbol{m} \rangle = \langle \boldsymbol{x} \cdot A^i, \boldsymbol{k} \rangle$$

- Linear overhead
- No need to save masks

Post-Synthesis Results

Parallelization	1		4		8	
w/o masking	4.3 kGE	128 c	7.0 kGE	32 c	10.3 kGE	16 c
1st-order	7.3 kGE	576 c	10.1 kGE	144 c	13.6 kGE	72 c
2nd-order	7.3 kGE	1024 c	10.1 kGE	256 c	13.6 kGE	128 c
3rd-order	7.3 kGE	1472 c	10.1 kGE	368 c	13.6 kGE	184 c

Extractor Characteristics

- Extractor yields one sample per extracted bit
  - Many samples per plaintext
  - Masks are re-used
- But masking the extractor is much cheaper

Outline

Motivation

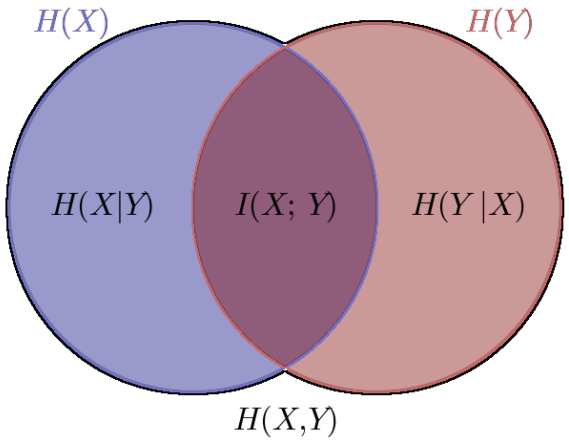
The Extractor

IT Analysis

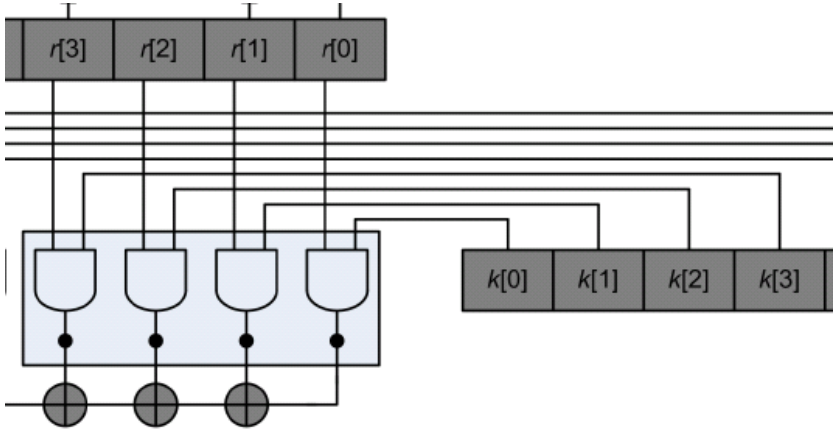
Security Analysis

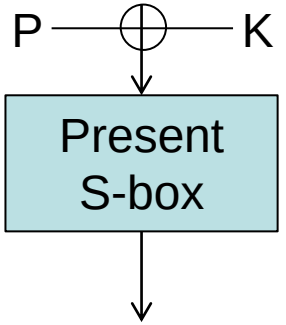
Conclusions

IT Analysis



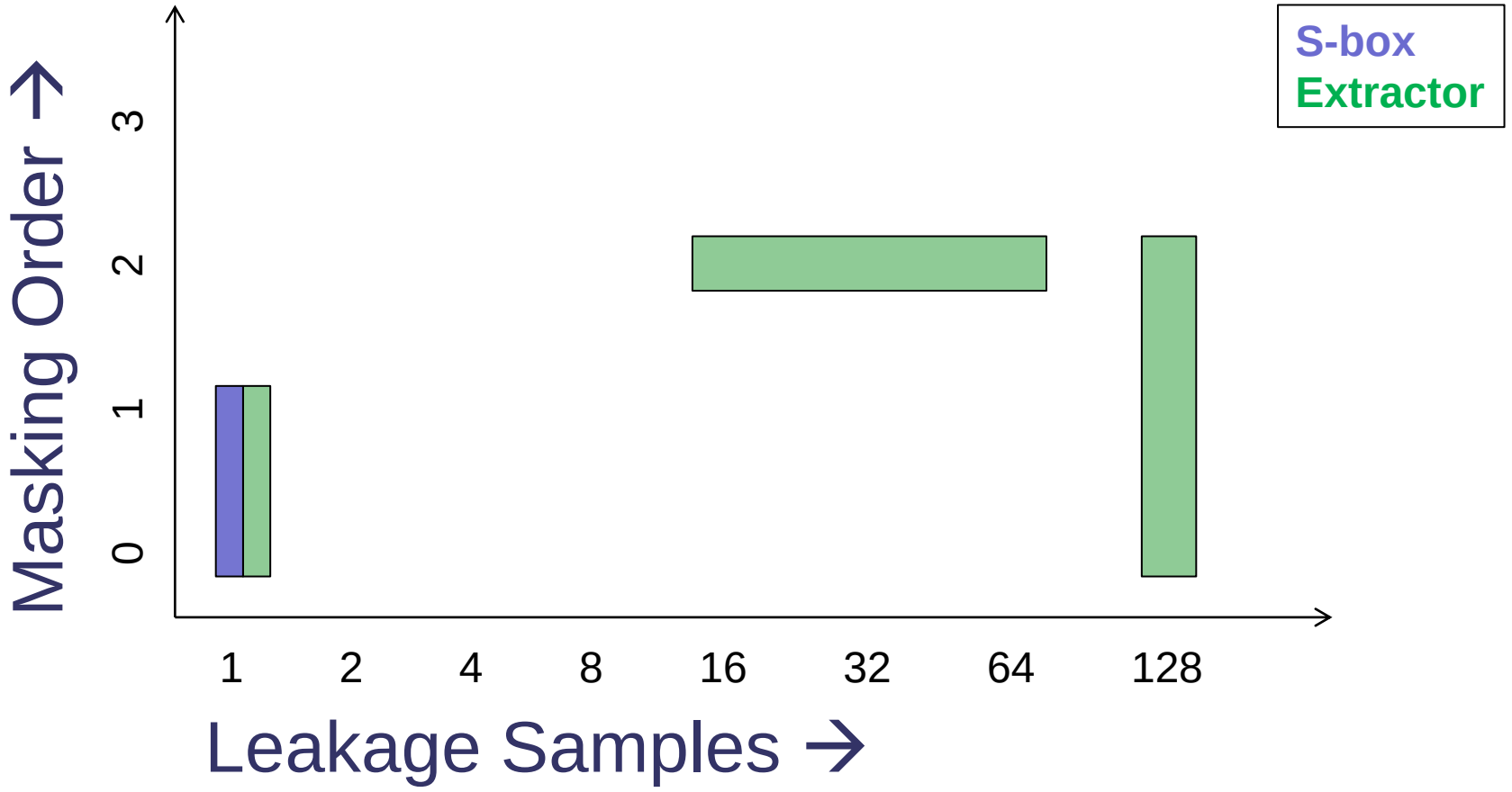
Leakage Simulation



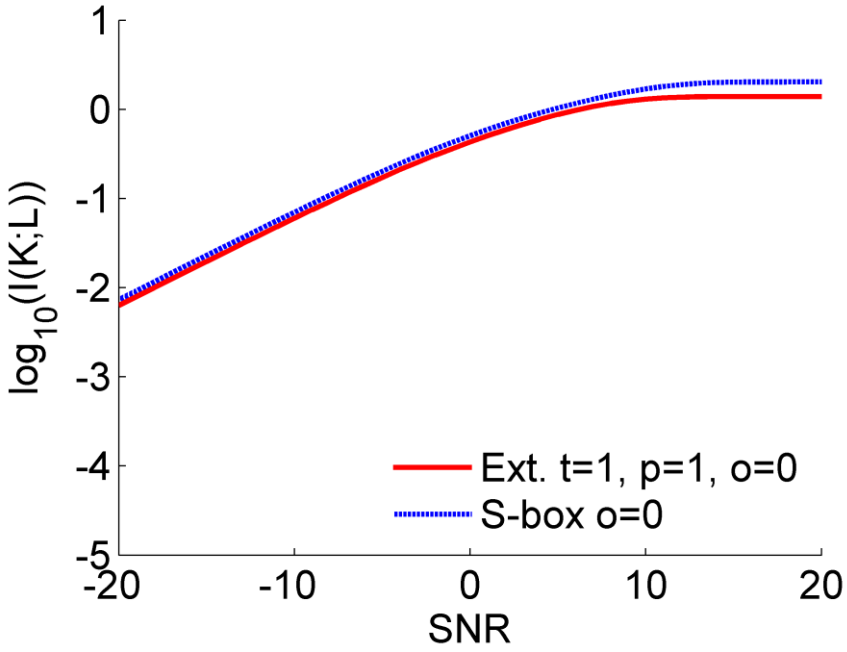


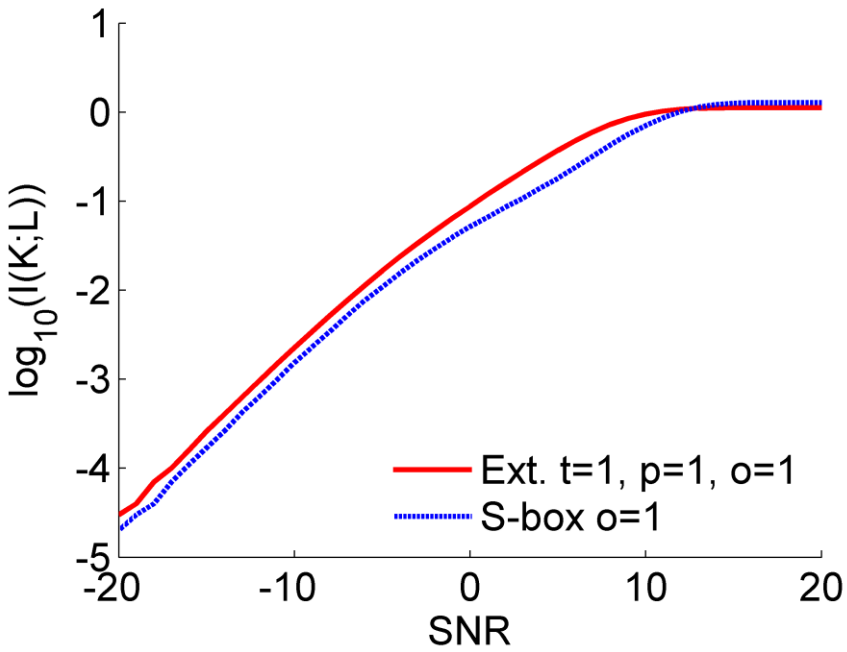
- 4-bit sub-keys
- Hamming weight
- No algorithmic noise
- Gaussian noise

Different Scenarios



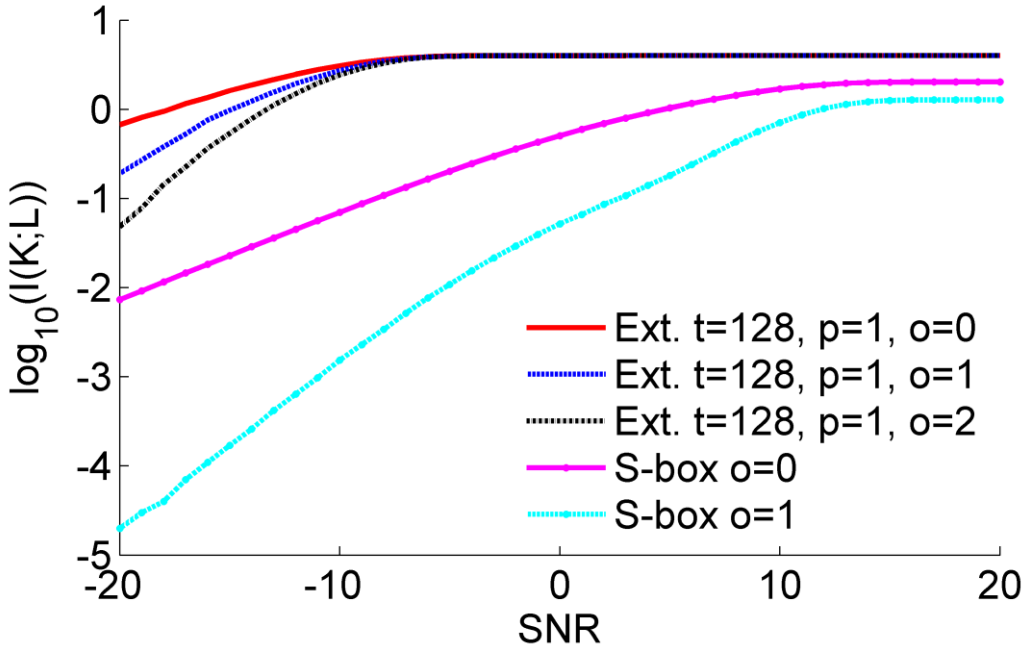
Comparison: Single Sample





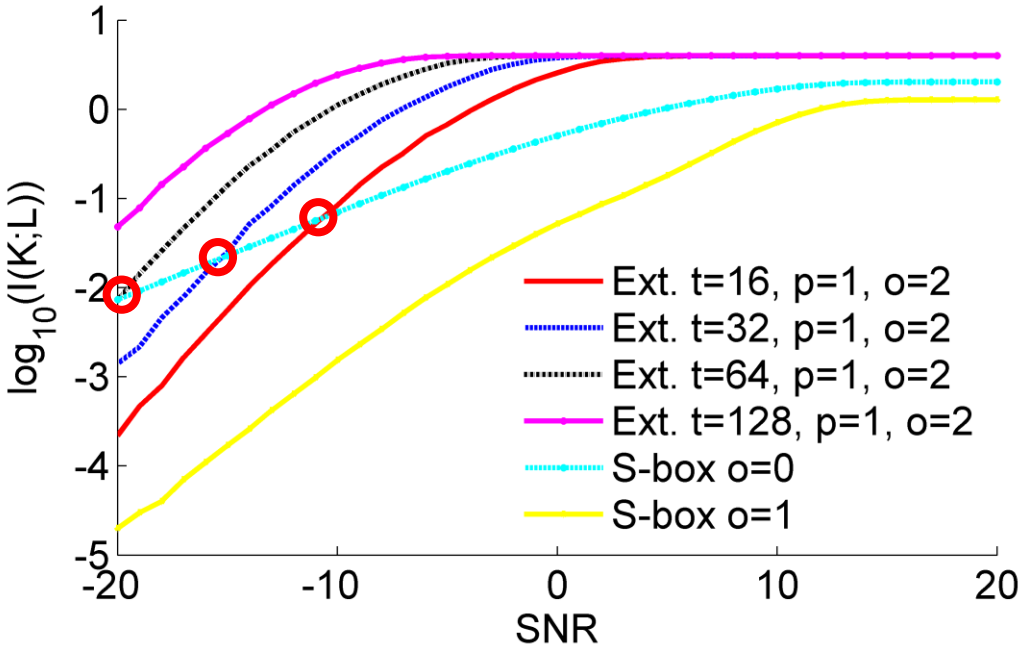
- Single sample leaks like S-box
- Masking is effective → $O(n^{order})$

Comparison: Multi Sample



- Masking is still there
- But a large amount of noise is needed

Reducing the Exploitable Samples



- Information depends linearly on num. Samples
- Curves intersect earlier

IT Analysis Results

- Masking works
- Steep slopes are easily achievable
- Without reducing the samples sufficiently, the noise will not be enough

Outline

Motivation

The Extractor

IT Analysis

Security Analysis

Conclusions

Using Multiple Samples?

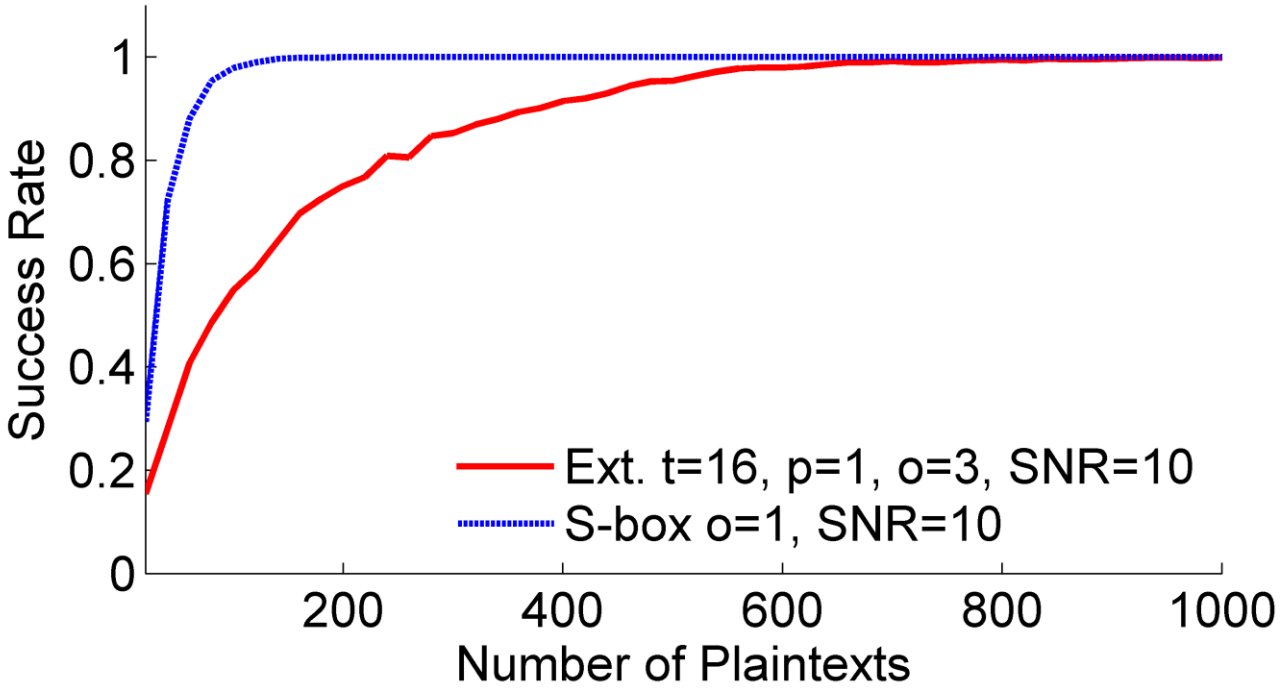
- Are multiple samples relevant?

- Time complexity of multiple sample attack is the same as for single sample attack

Exploiting the Information?

- Case study: CPA
- We need preprocessing for masking
  - Normalized product combining
- We cannot exploit mask re-use

CPA Attacks



- Extractor looks suddenly very strong

Outline

Motivation

The Extractor

IT Analysis

Security Analysis

Conclusions

Conclusions I

Extractors can be implemented efficiently in hardware

Efficient masking up to arbitrary orders

Many samples are the main issue

Reducing samples allows higher security than in software (e.g. Parallelism)

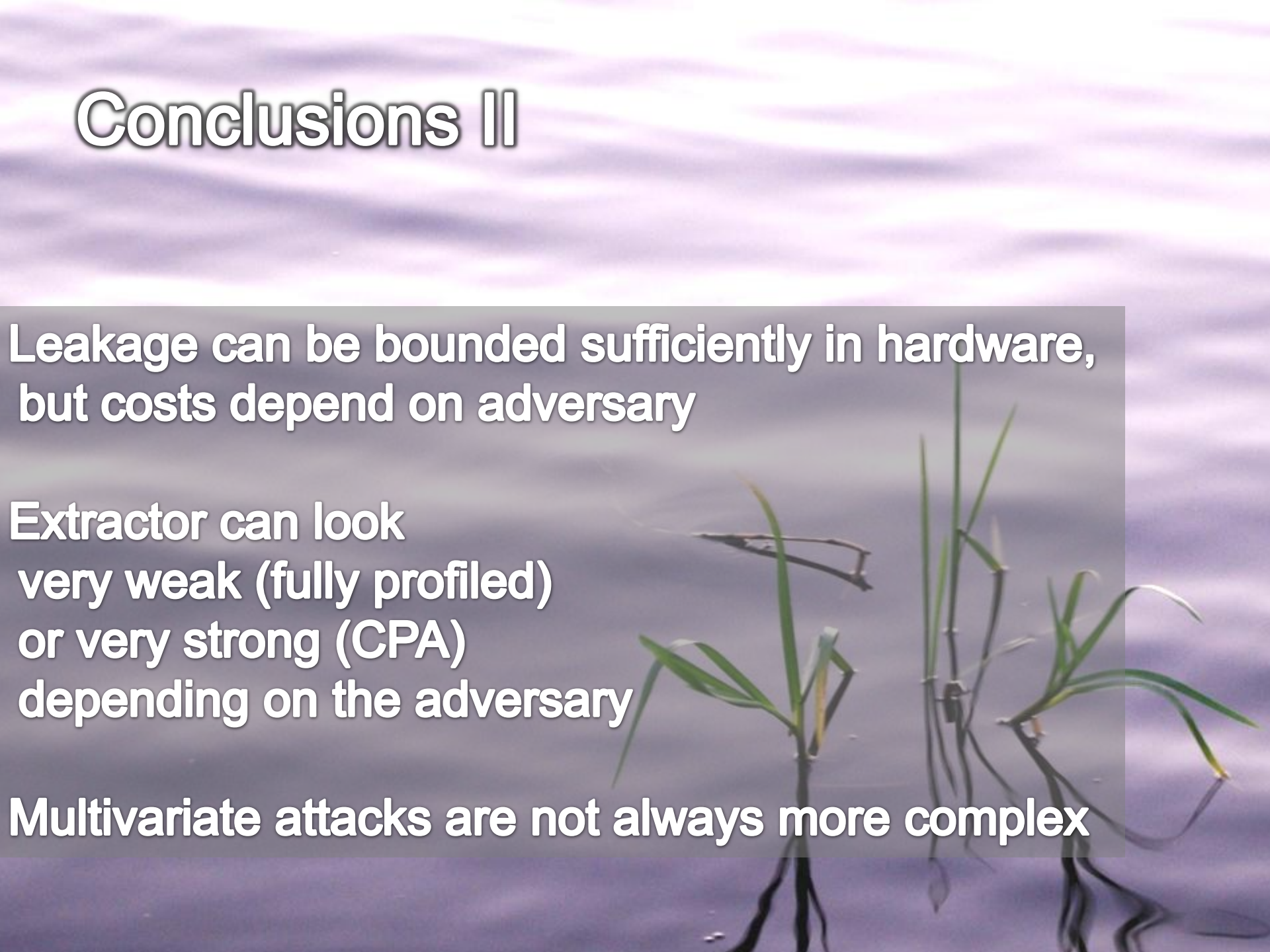
Future work: Key schedule

Conclusions II

Leakage can be bounded sufficiently in hardware,
but costs depend on adversary

Extractor can look
very weak (fully profiled)
or very strong (CPA)
depending on the adversary

Multivariate attacks are not always more complex



Extractors Against Side-Channel Attacks: Weak or Strong?

Marcel Medwed, Francois-Xavier Standaert

UCL Crypto Group