Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA

Mathieu Renauld, François-Xavier Standaert, Nicolas Veyrat-Charvillon

CHES'09 – September 2009

Outline

Introduction

Algebraic Side-Channel Attack

Comparison with DPA

Advanced scenarios

Conclusion

Outline

Introduction

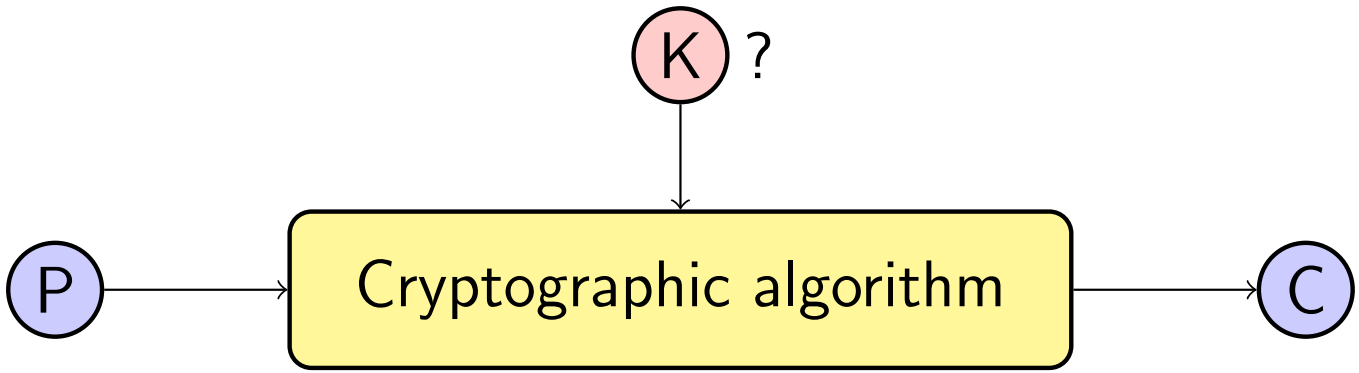
Algebraic Side-Channel Attack

Comparison with DPA

Advanced scenarios

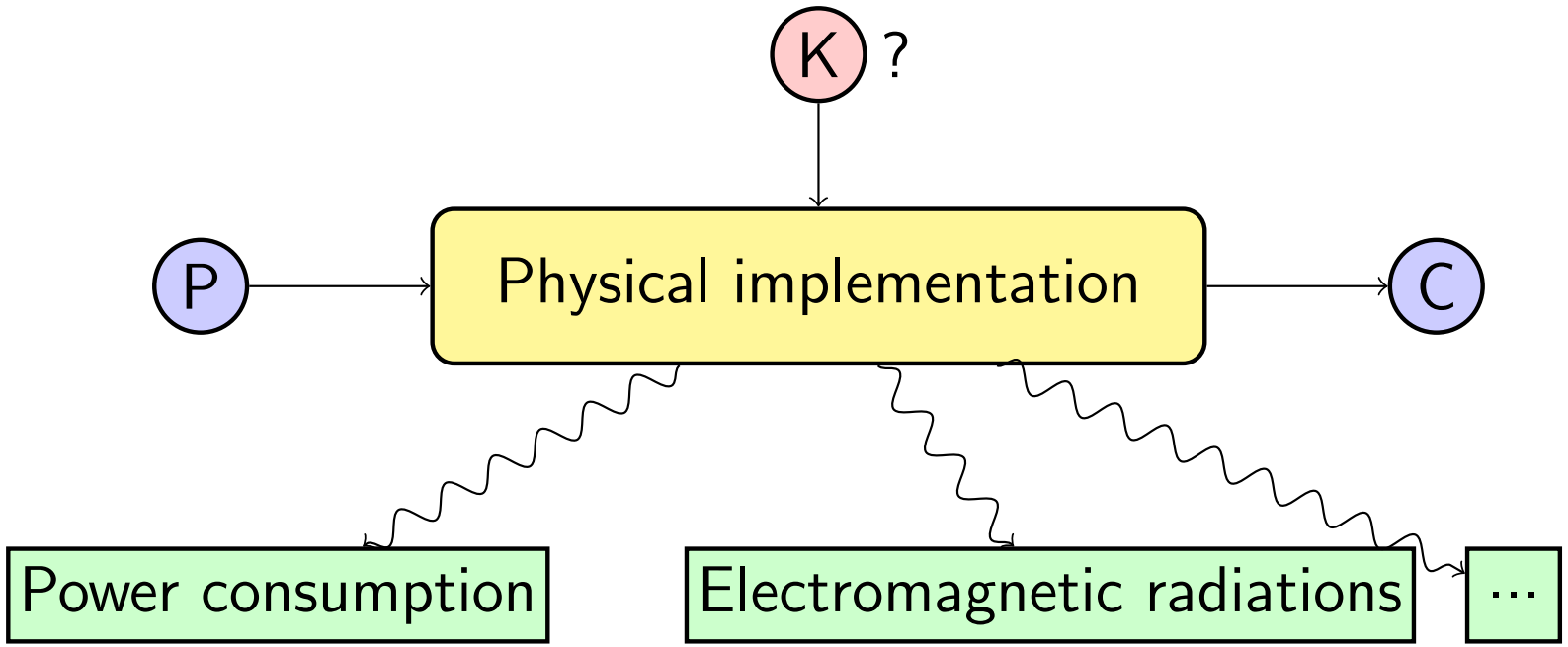
Conclusion

Classical cryptanalysis



Introduction

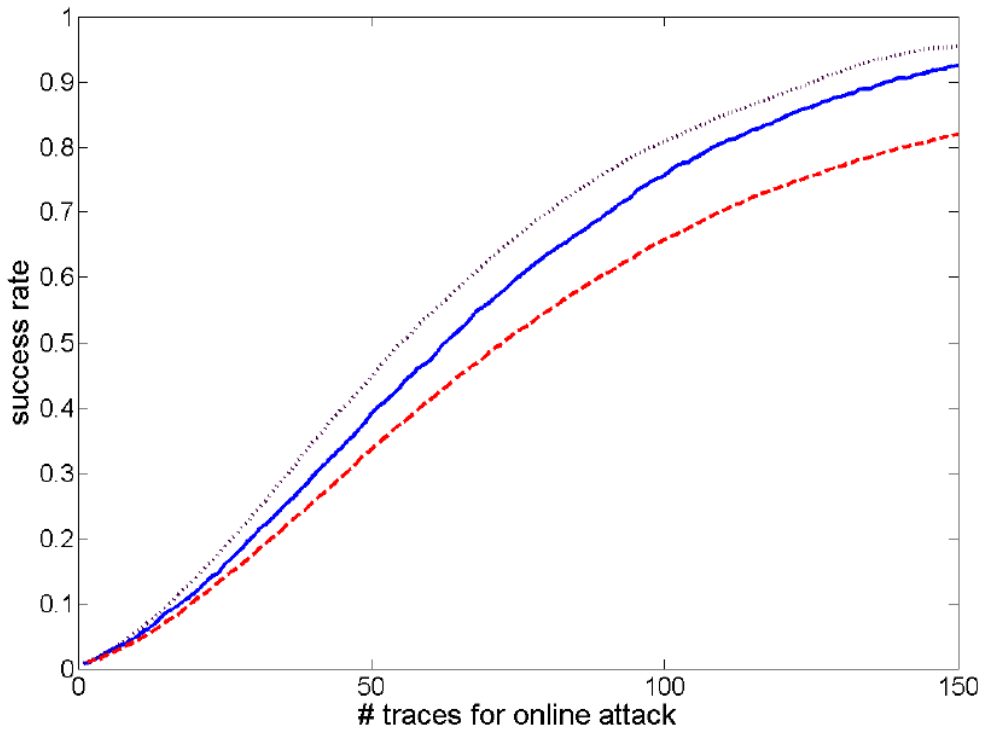
Side-Channel cryptanalysis



Introduction

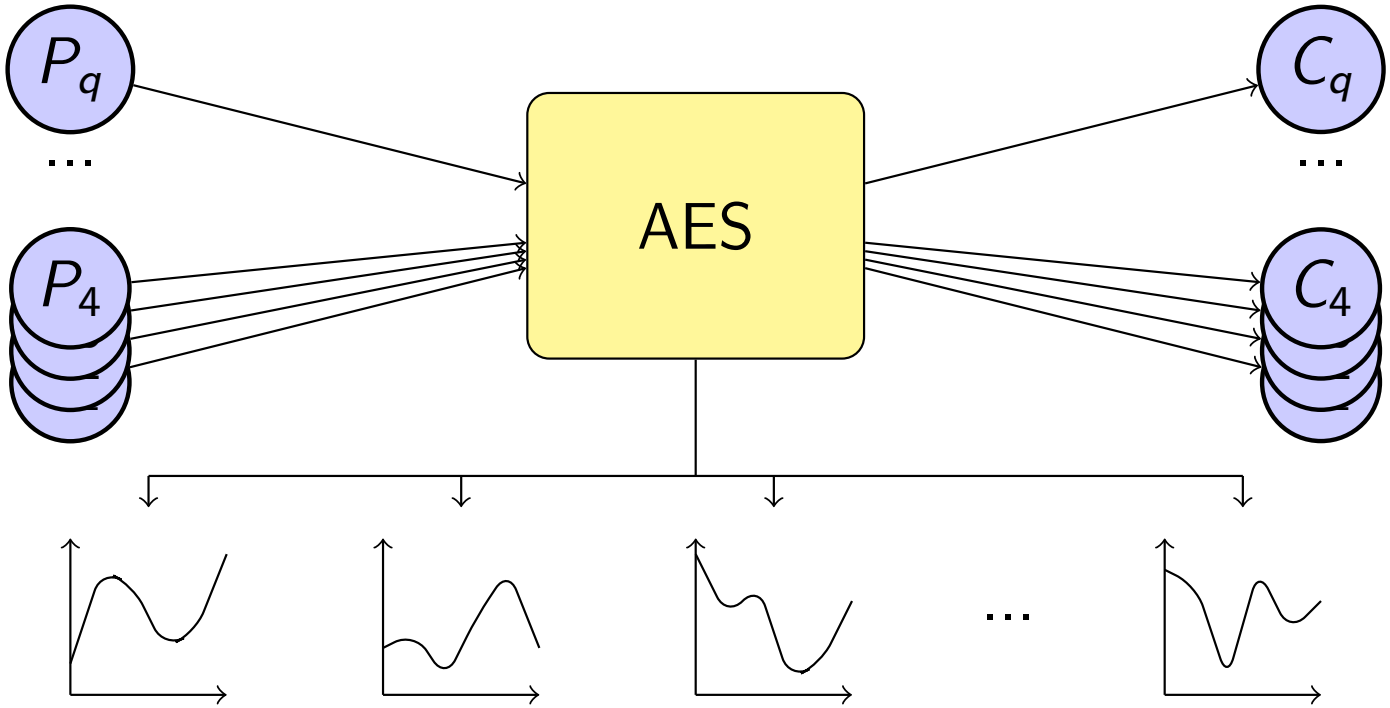
Open questions

What is the smallest possible data complexity?



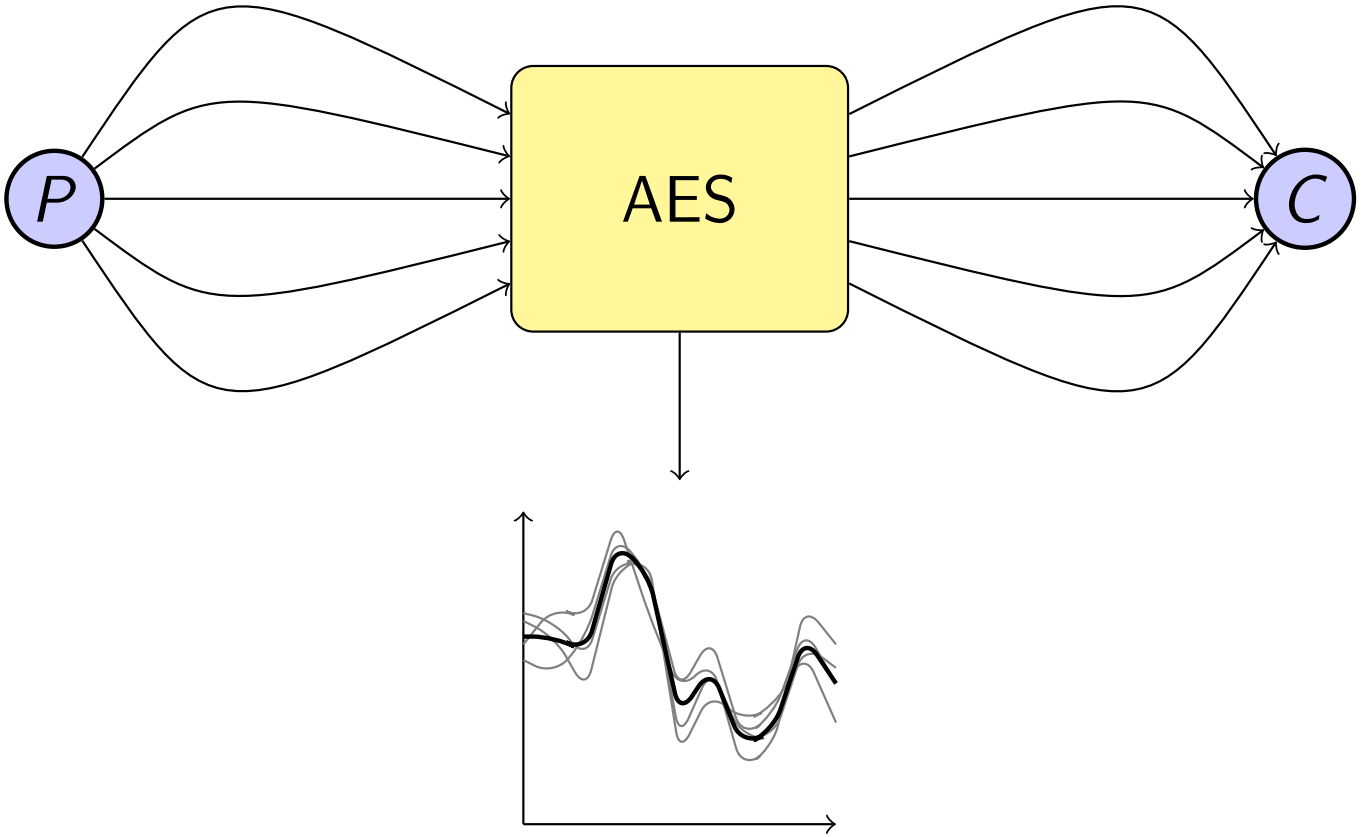
Introduction

Data complexity q

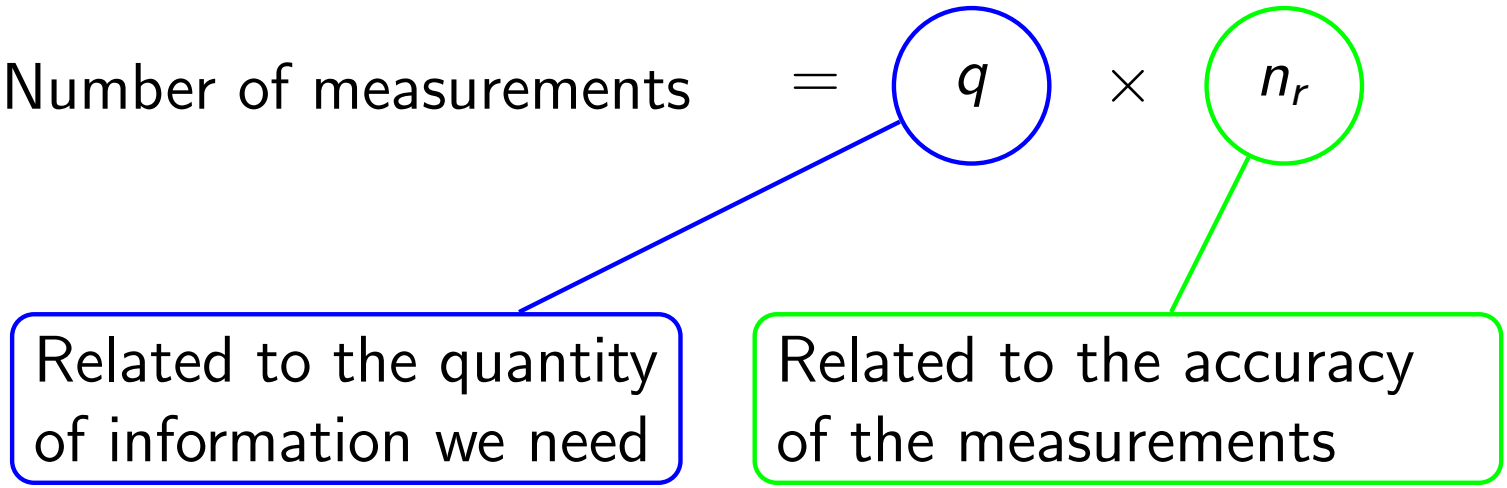


Introduction

Repetition number n_r

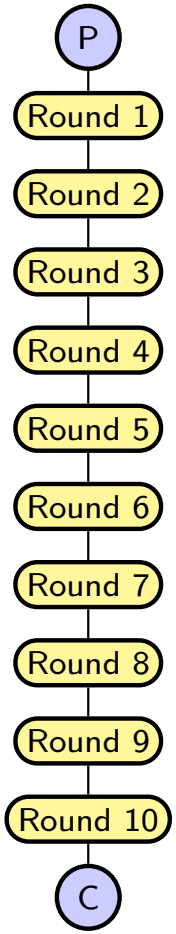


Introduction



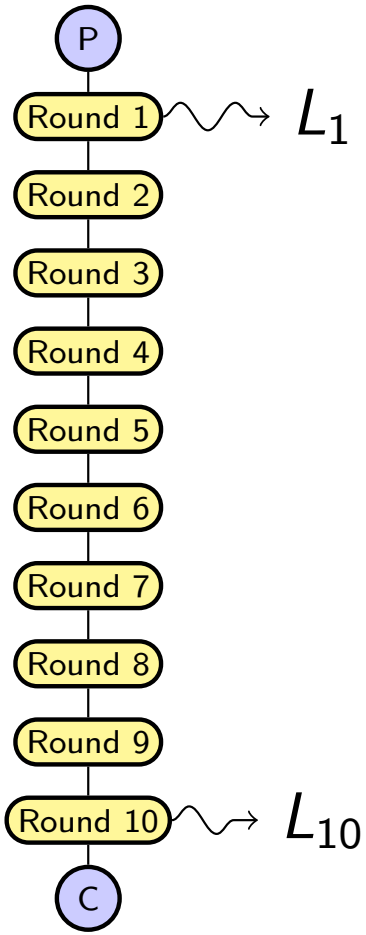
What is the minimum value for q?

Introduction



Which information can be used?

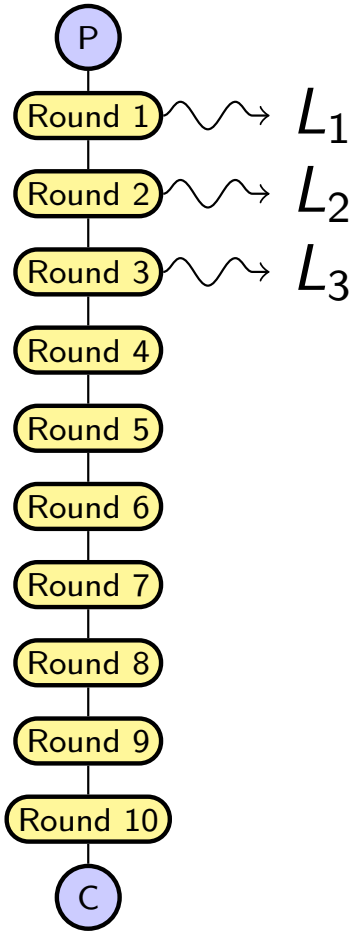
Introduction



DPA uses information from the first or last round (low diffusion)

Which information can be used?

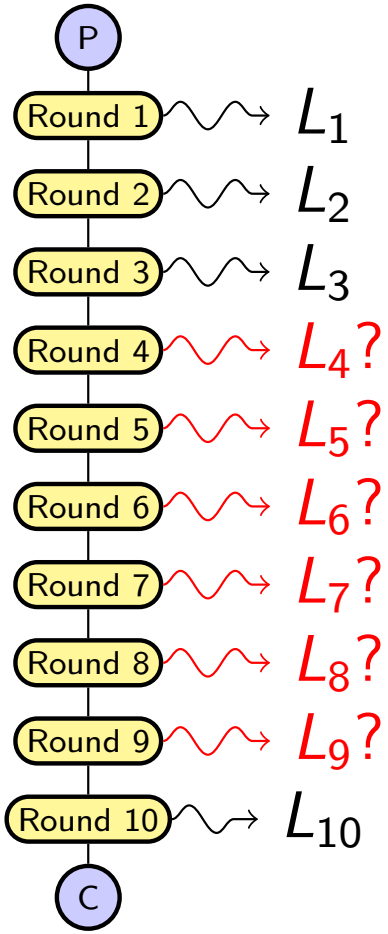
Introduction



Collision attacks can use leakages up to the third round

Which information can be used?

Introduction



What about the middle rounds?

Which information can be used?

Introduction

Most of the side-channel attacks aim to directly recover the key bits

Introduction

Most of the side-channel attacks aim to directly recover the key bits

Is it possible to use side-channel to recover less informative (easier) targets ...

... and combine this with a classic cryptanalysis phase to recover the key?

Introduction

Most of the side-channel attacks aim to directly recover the key bits

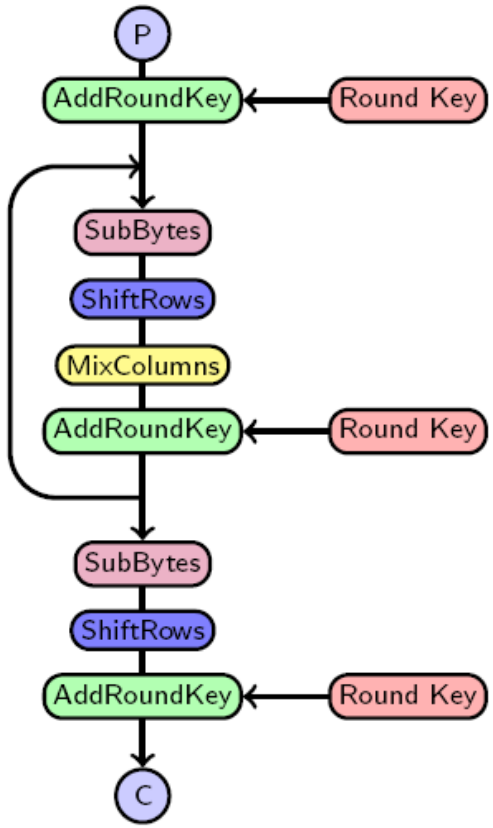
Is it possible to use side-channel to recover less informative (easier) targets ...

... and combine this with a classic cryptanalysis phase to recover the key?

We decided to use *algebraic cryptanalysis*.

Introduction

A block cipher ...

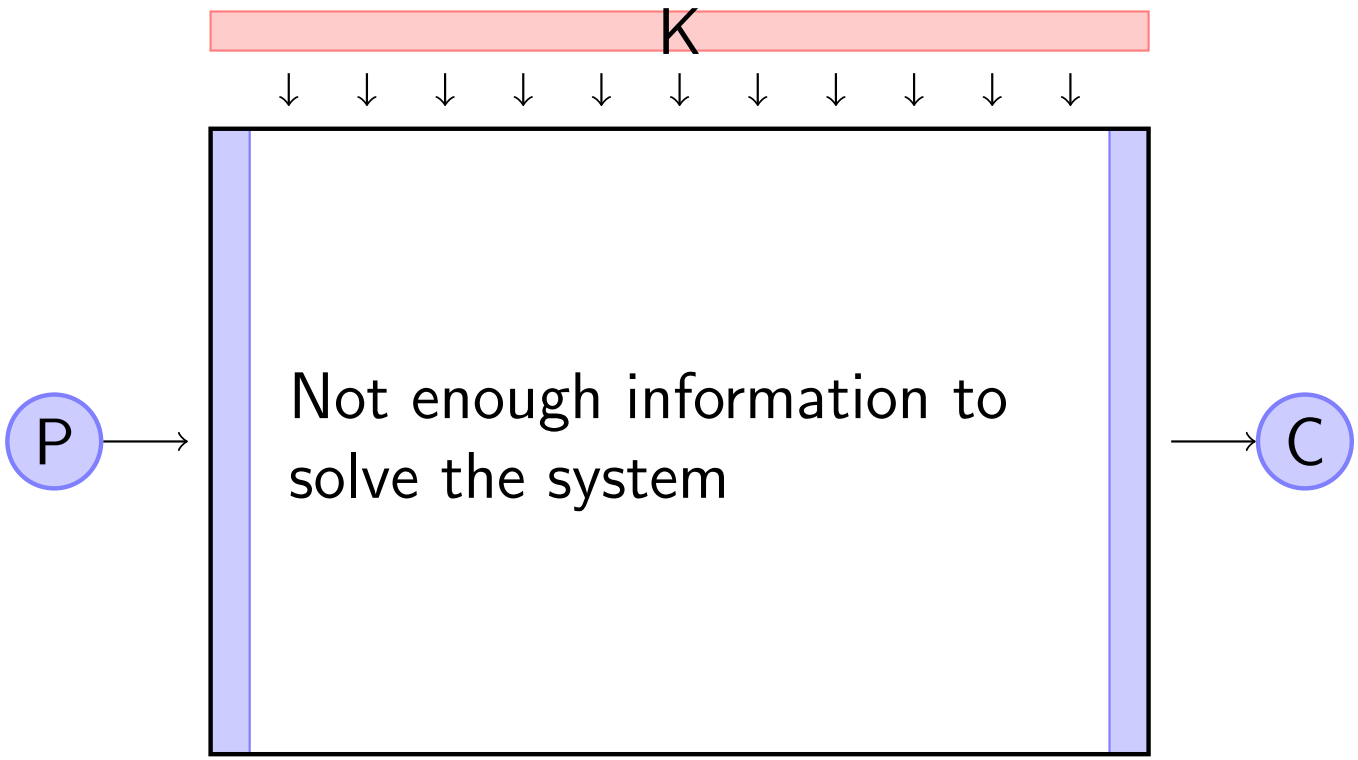


becomes a big set of low degree boolean equations

$$
\begin{aligned}
0 &= x_2 + x_{11} + x_{14} + x_2x_5 + x_4x_{10} \\
0 &= x_5 + x_9 + x_1x_6 + x_3x_{10}x_{13} + x_5x_7x_{16} \\
1 &= x_7 + x_{15} + x_{16} + x_3x_7 + x_9x_{11} \\
0 &= x_7 + x_1x_5 + x_6x_{11} + x_4x_5x_{12} \\
1 &= x_8 + x_{10} + x_{11} + x_{15} + x_2x_6 + x_6x_{10} \\
0 &= x_{10} + x_{15} + x_{16} + x_6x_{12} + x_9x_{16} + x_2x_9x_{14} \\
0 &= x_{13} + x_{14} + x_5x_{13} + x_8x_{12} + x_4x_7x_{12} + x_8x_9x_{11} \\
&\dots
\end{aligned}
$$

Introduction

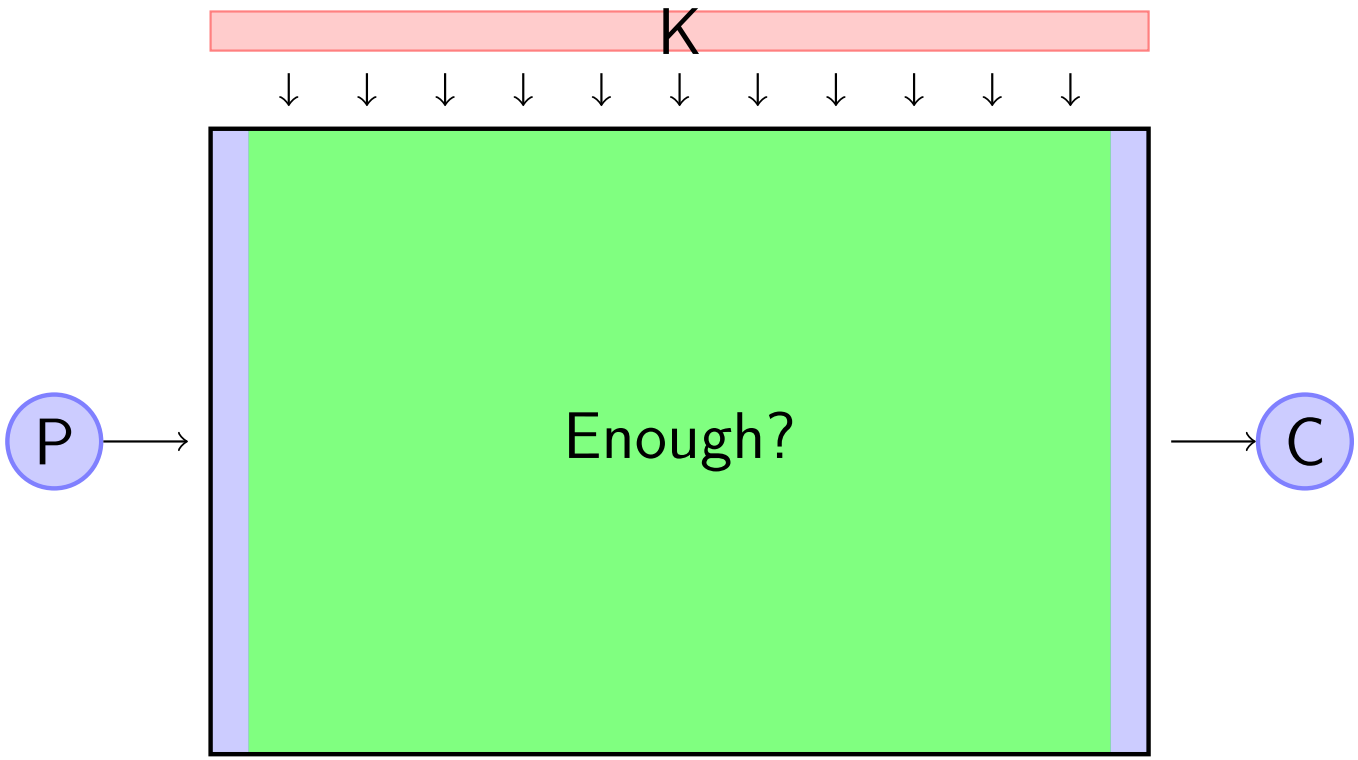
Classic algebraic attack



256 known bits

Introduction

Algebraic attack + side-channel information



256 known bits + side-channel information

Related work

Square attacks + side-channel

- V. Carlier, H. Chabanne, E. Dottax, H. Pelletier, 2005.

Differential cryptanalysis + side-channel

- H. Handschuh, B. Preneel, 2006.

Collision attacks

- A. Biryukov, D. Khovratovich, 2007.
- A. Bogdanov, 2007.
- A. Bogdanov, I. Kizhvatov, A. Pyshkin, 2008.

Outline

Introduction

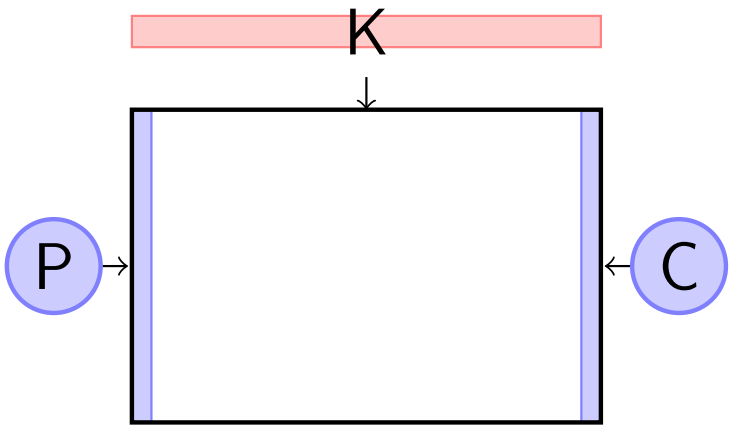
Algebraic Side-Channel Attack

Comparison with DPA

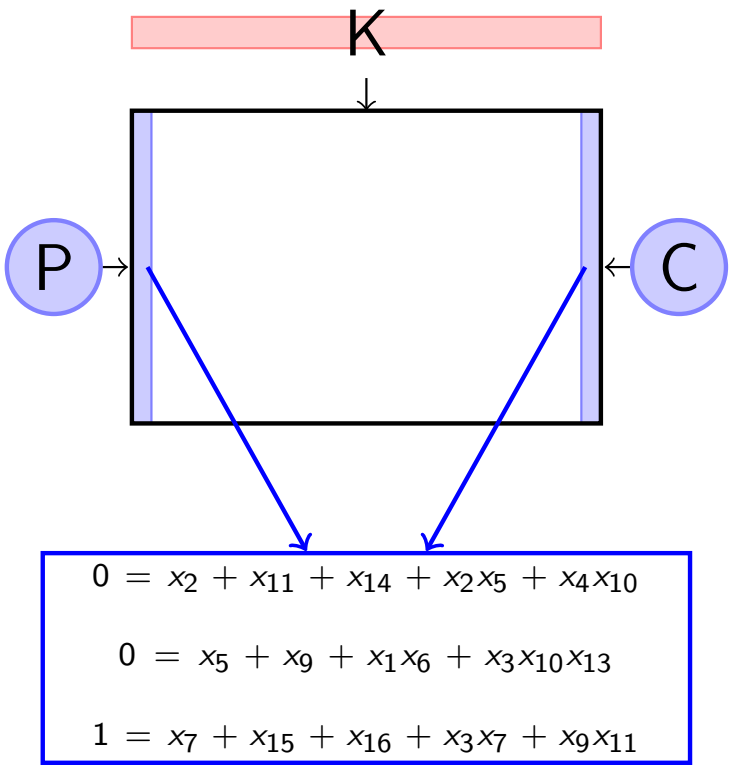
Advanced scenarios

Conclusion

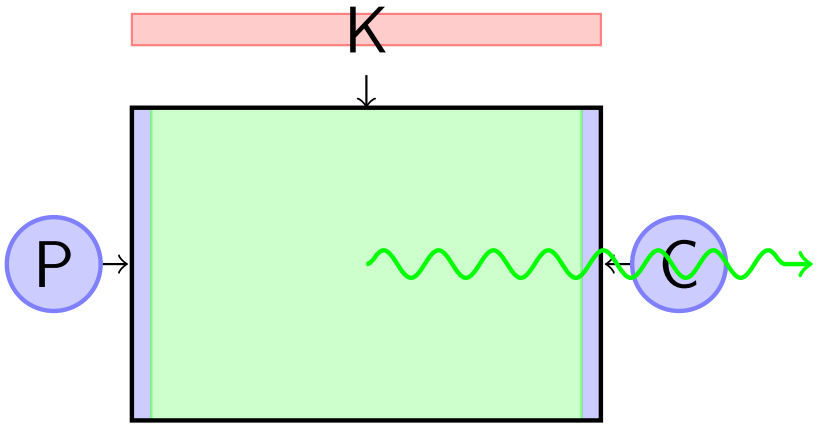
Algebraic Side-Channel Attack

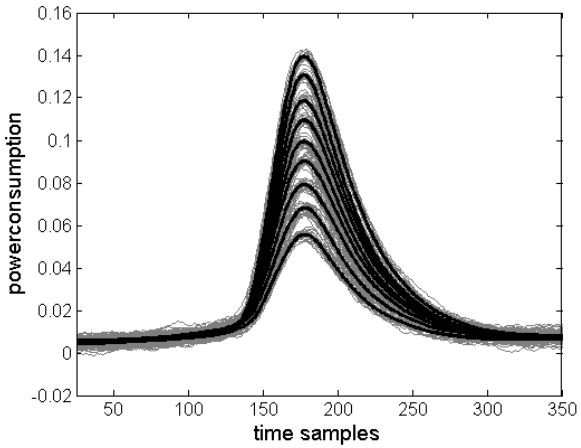


Algebraic Side-Channel Attack



Algebraic Side-Channel Attack



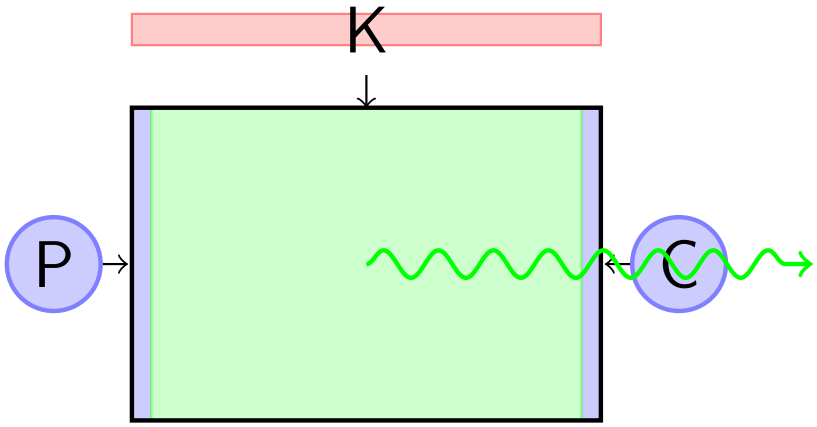


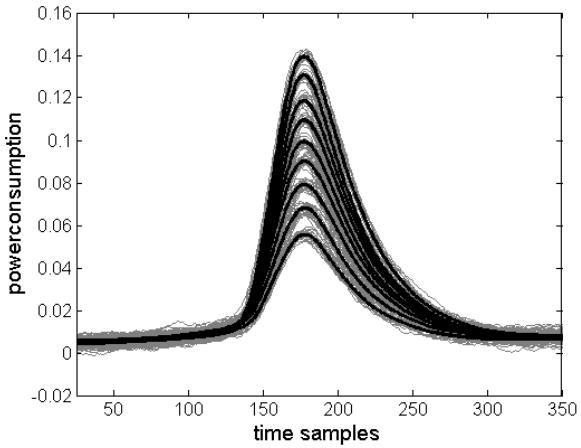
$$0 = x_2 + x_{11} + x_{14} + x_2x_5 + x_4x_{10}$$

$$0 = x_5 + x_9 + x_1x_6 + x_3x_{10}x_{13}$$

$$1 = x_7 + x_{15} + x_{16} + x_3x_7 + x_9x_{11}$$

Algebraic Side-Channel Attack

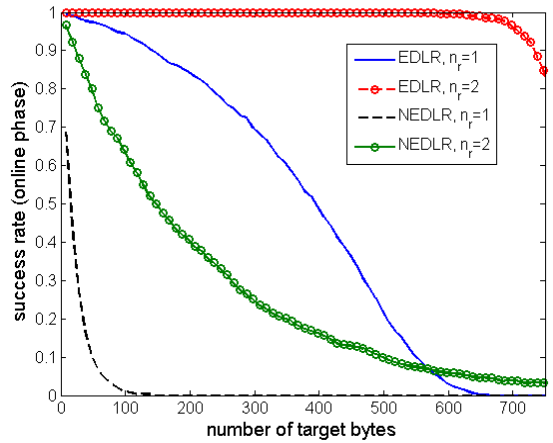




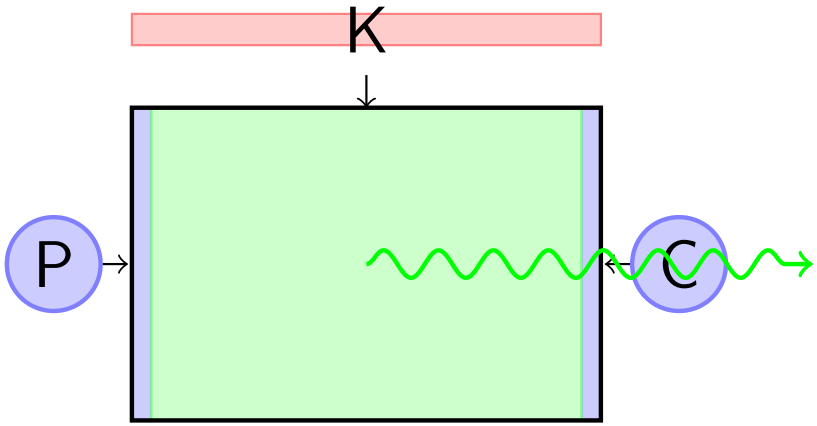
$$0 = x_2 + x_{11} + x_{14} + x_2x_5 + x_4x_{10}$$

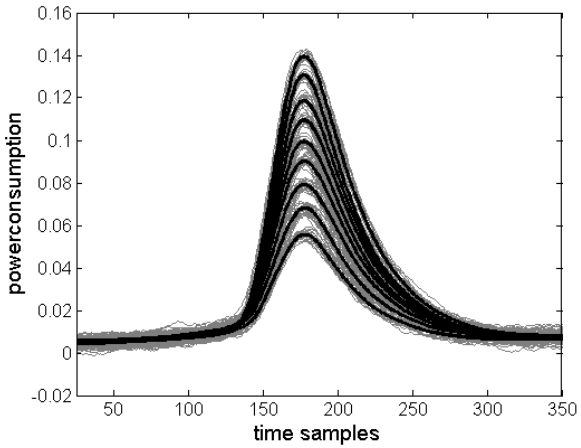
$$0 = x_5 + x_9 + x_1x_6 + x_3x_{10}x_{13}$$

$$1 = x_7 + x_{15} + x_{16} + x_3x_7 + x_9x_{11}$$



Algebraic Side-Channel Attack





$$0 = x_2 + x_{11} + x_{14} + x_2x_5 + x_4x_{10}$$

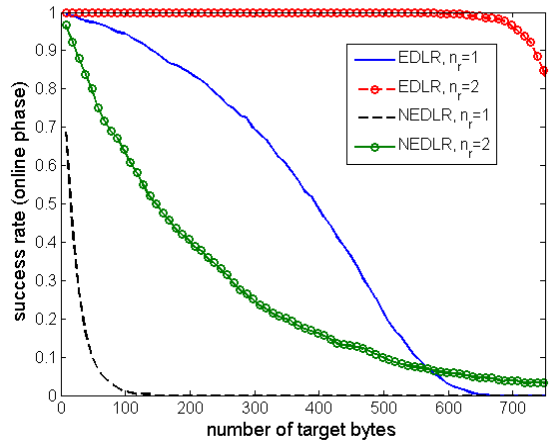
$$0 = x_5 + x_9 + x_1x_6 + x_3x_{10}x_{13}$$

$$1 = x_7 + x_{15} + x_{16} + x_3x_7 + x_9x_{11}$$

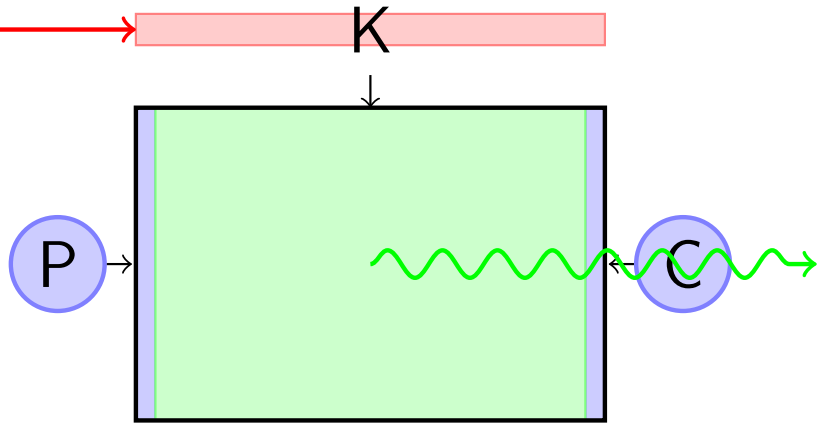
$$0 = x_7 + x_1x_5 + x_6x_{11} + x_4x_5x_{12}$$

$$1 = x_8 + x_{10} + x_{11} + x_{15} + x_2x_6 + x_6x_{10}$$

$$0 = x_{10} + x_{15} + x_{16} + x_6x_{12} + x_9x_{16}$$



Algebraic Side-Channel Attack



$$0 = x_2 + x_{11} + x_{14} + x_2x_5 + x_4x_{10}$$

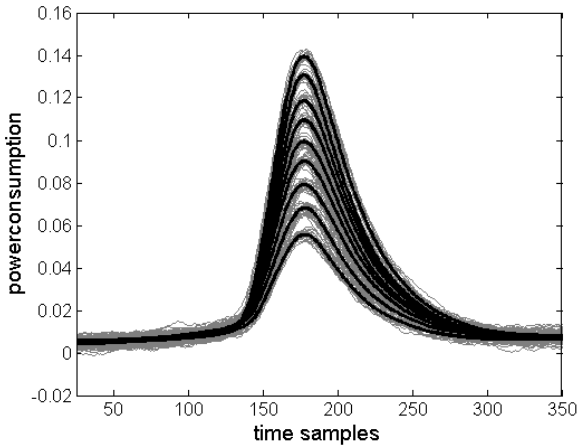
$$0 = x_5 + x_9 + x_1x_6 + x_3x_{10}x_{13}$$

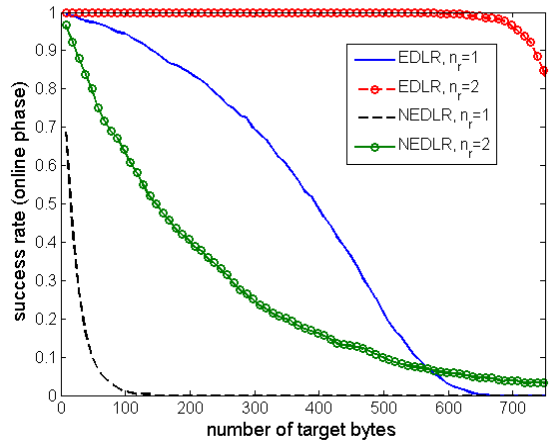
$$1 = x_7 + x_{15} + x_{16} + x_3x_7 + x_9x_{11}$$

$$0 = x_7 + x_1x_5 + x_6x_{11} + x_4x_5x_{12}$$

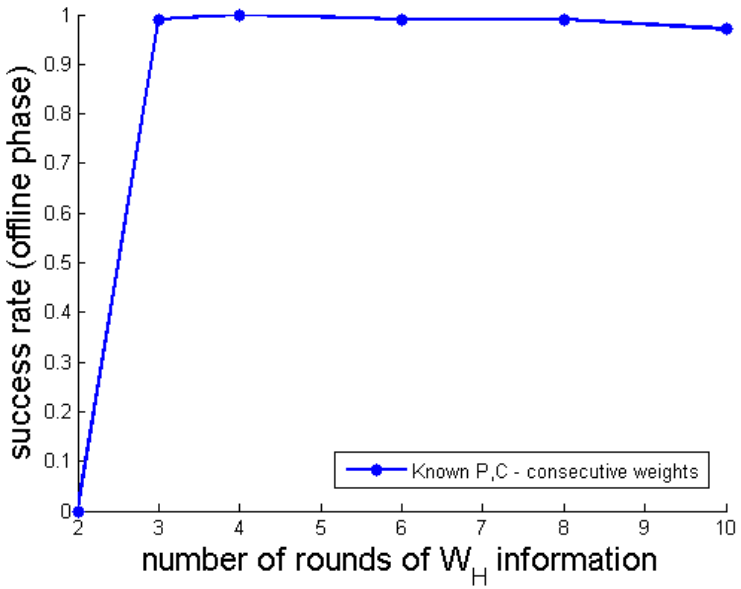
$$1 = x_8 + x_{10} + x_{11} + x_{15} + x_2x_6 + x_6x_{10}$$

$$0 = x_{10} + x_{15} + x_{16} + x_6x_{12} + x_9x_{16}$$

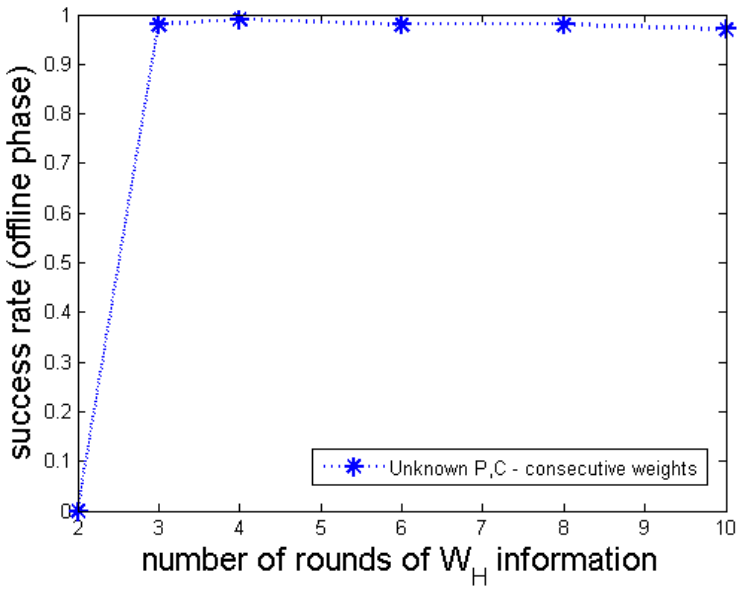




Algebraic Side-Channel Attack

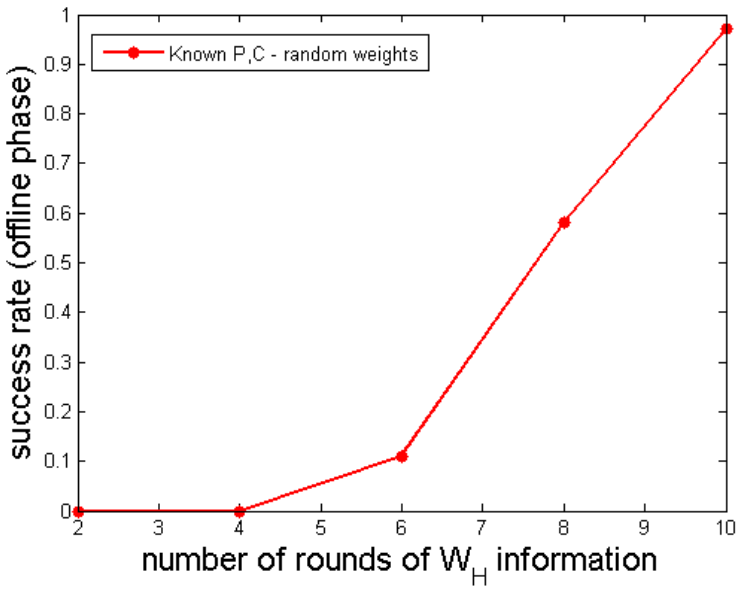


Known P, C, consecutive weights

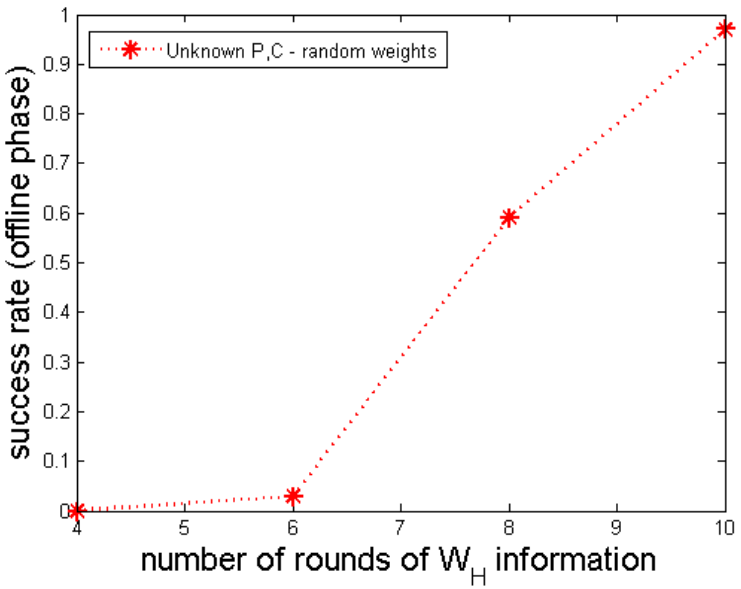


Unknown P, C, consecutive weights

Algebraic Side-Channel Attacks

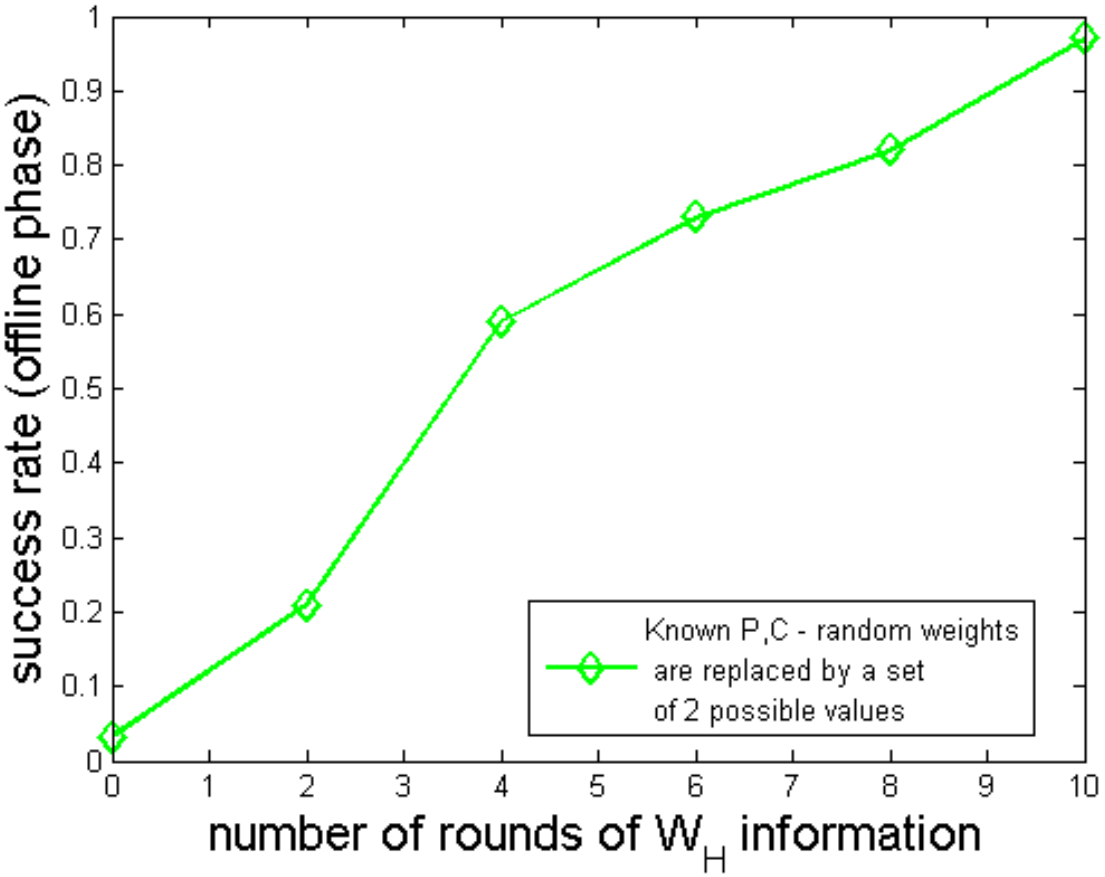


Known P, C, random weights

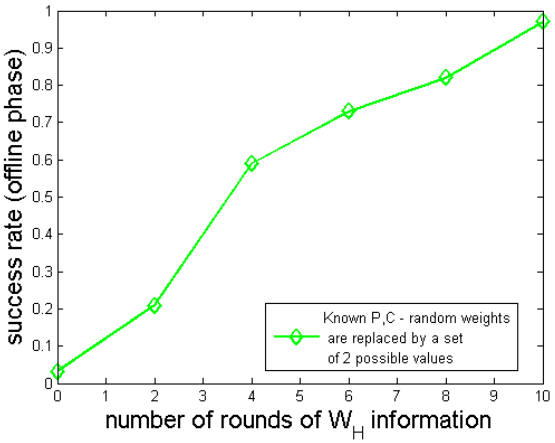


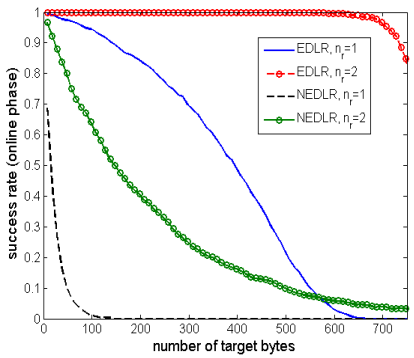
Unknown P, C, random weights

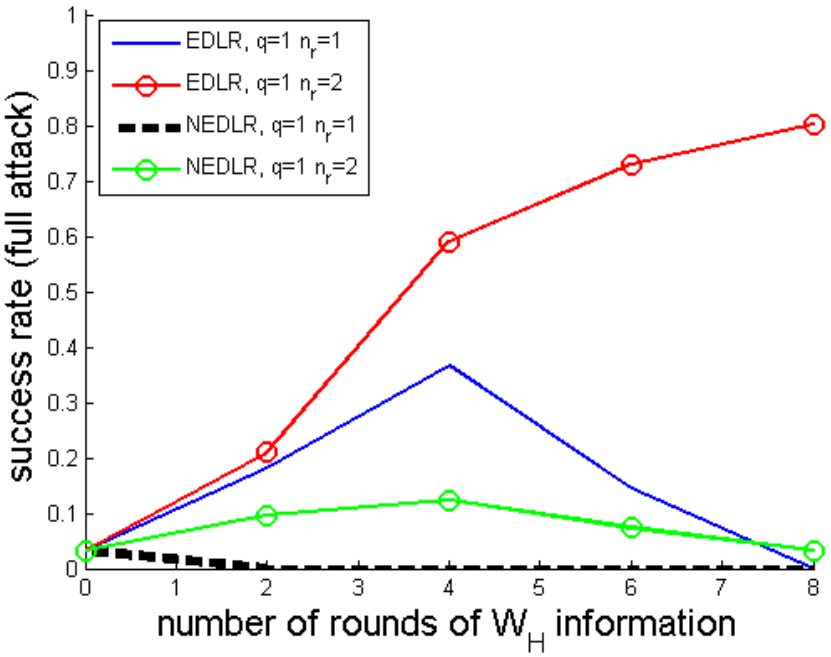
Algebraic Side-Channel Attacks



Algebraic Side-Channel Attacks







Outline

Introduction

Algebraic Side-Channel Attack

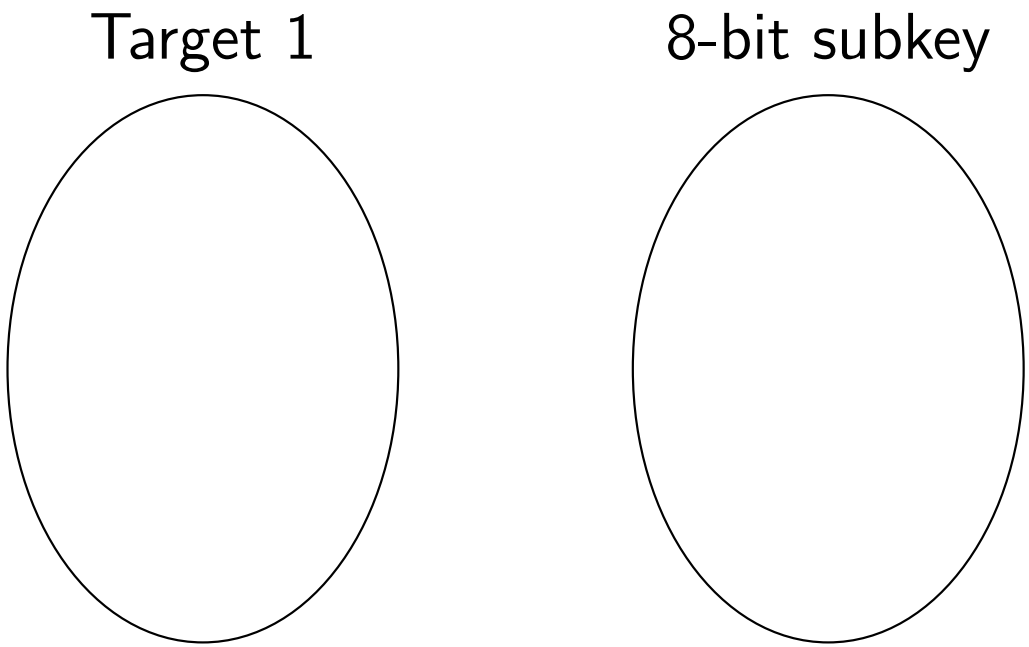
Comparison with DPA

Advanced scenarios

Conclusion

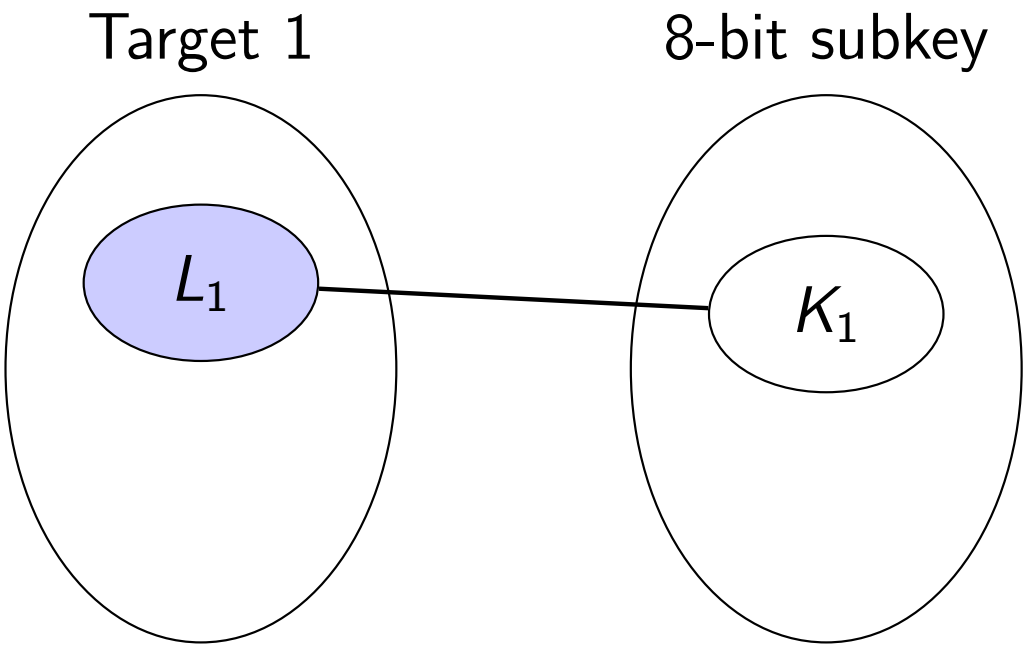
Comparison with DPA

Classical power analysis attack (DPA)



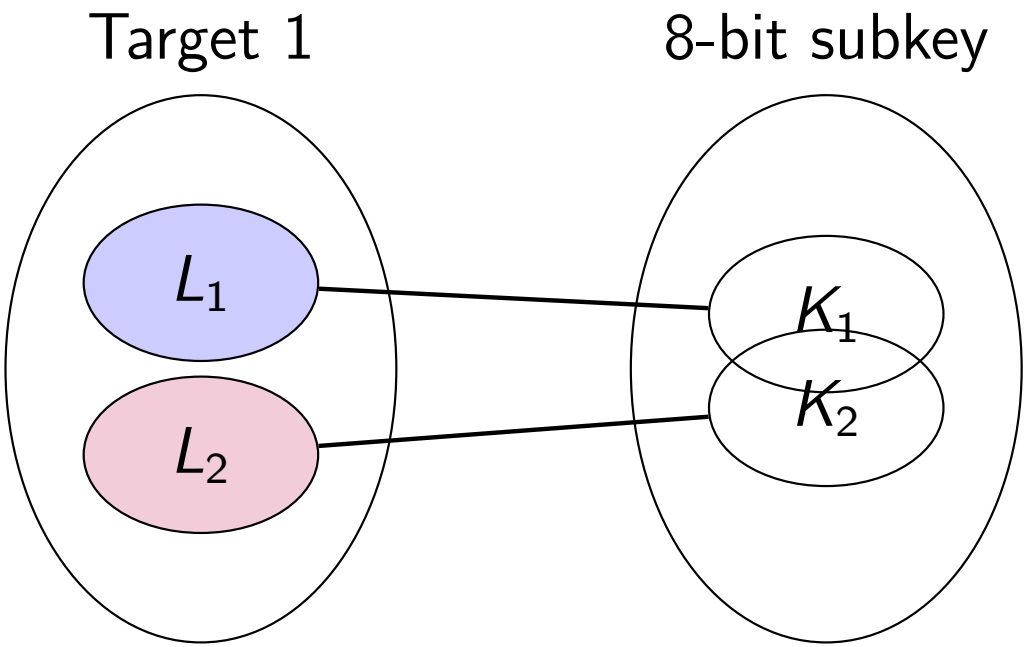
Comparison with DPA

Classical power analysis attack (DPA)



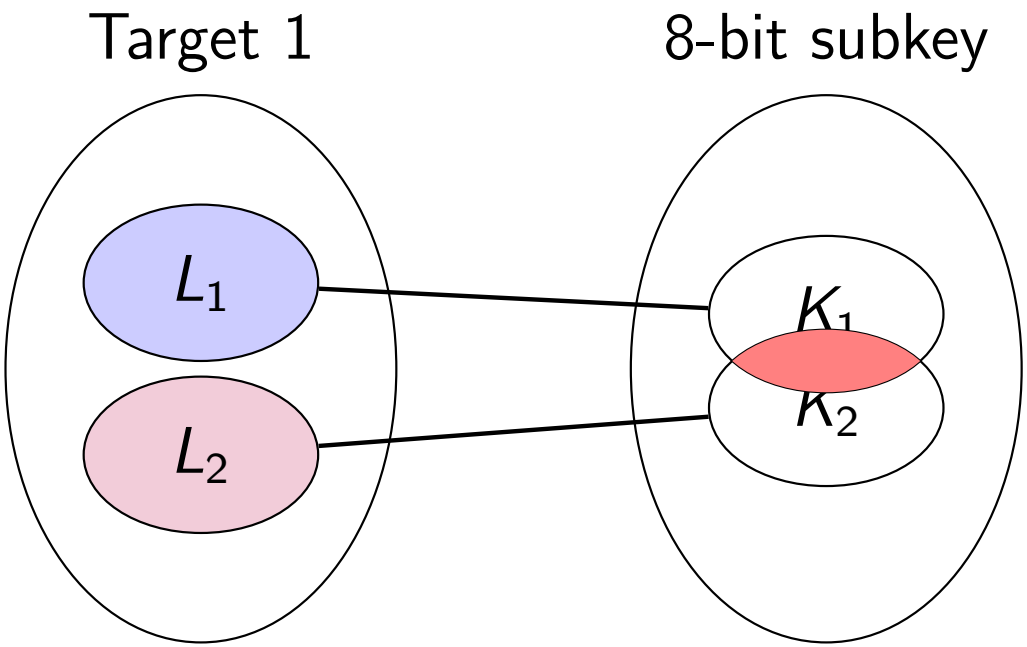
Comparison with DPA

Classical power analysis attack (DPA)



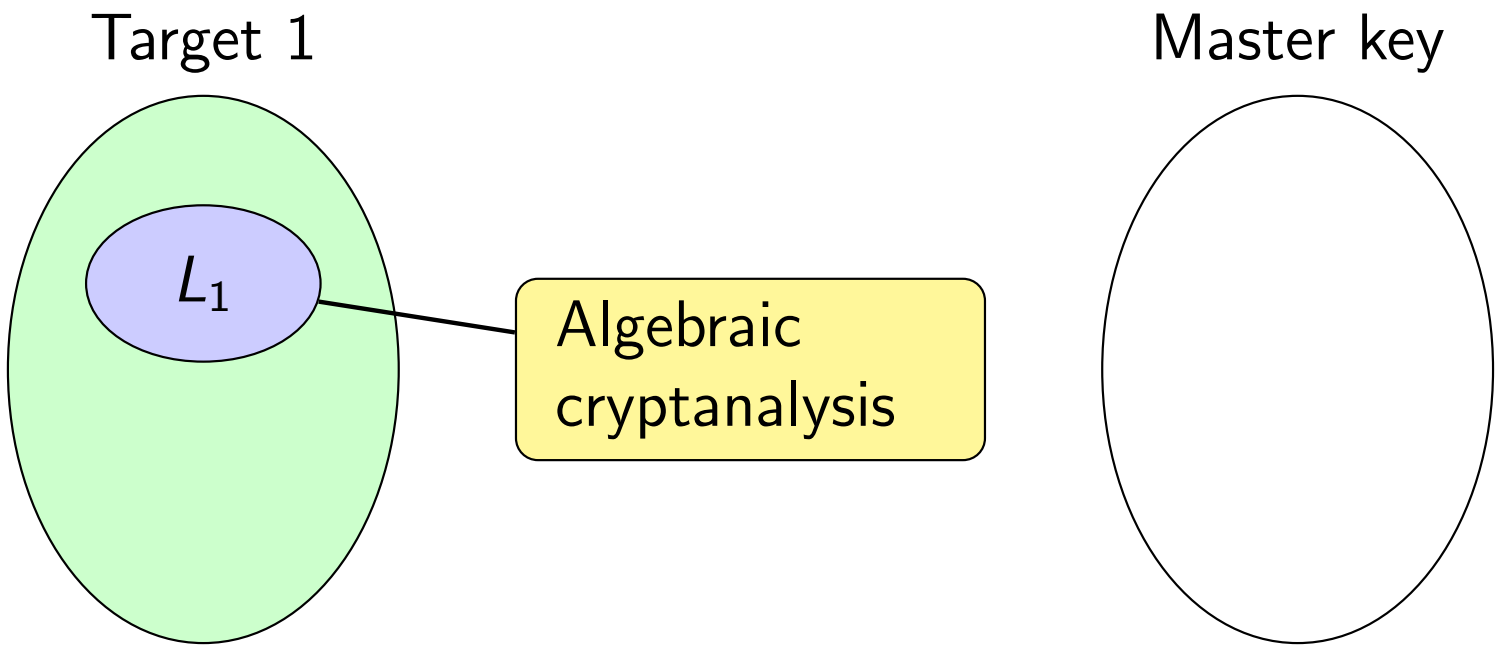
Comparison with DPA

Classical power analysis attack (DPA)



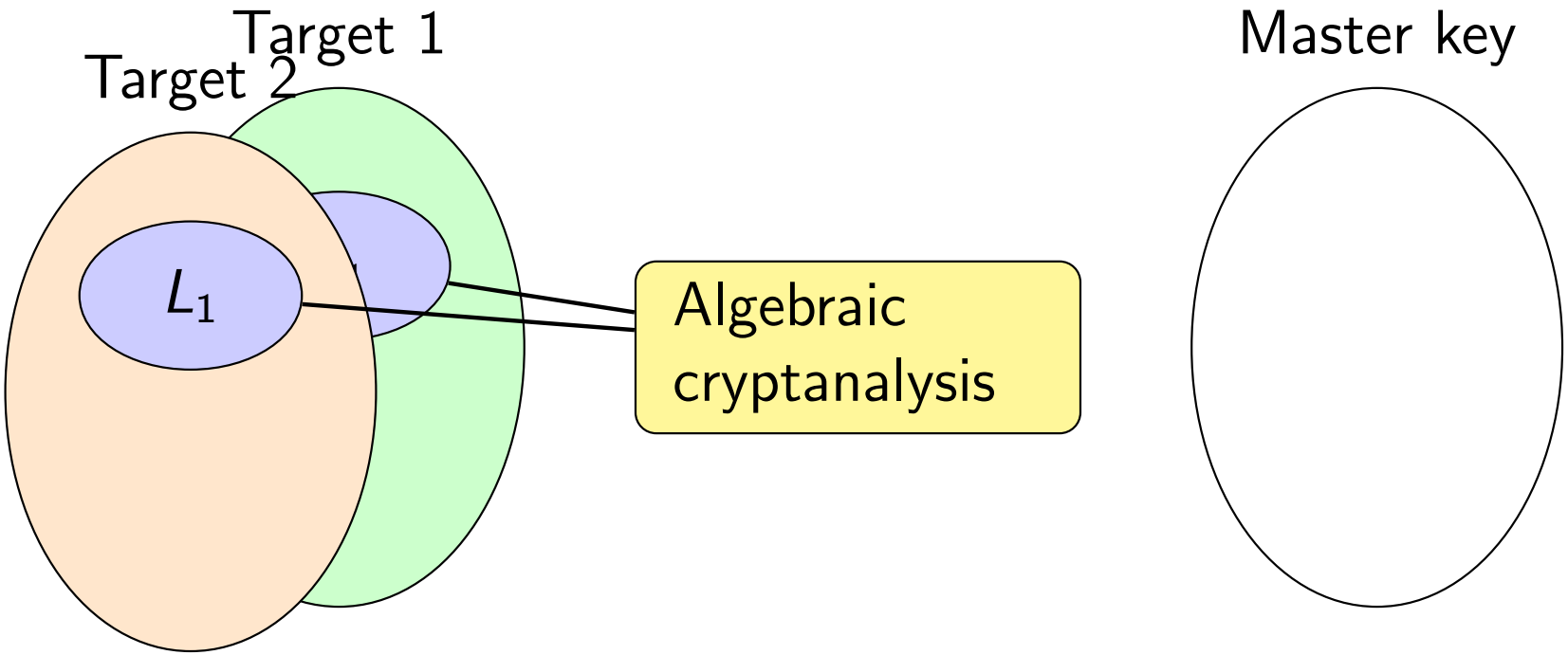
Comparison with DPA

Algebraic side-channel attack



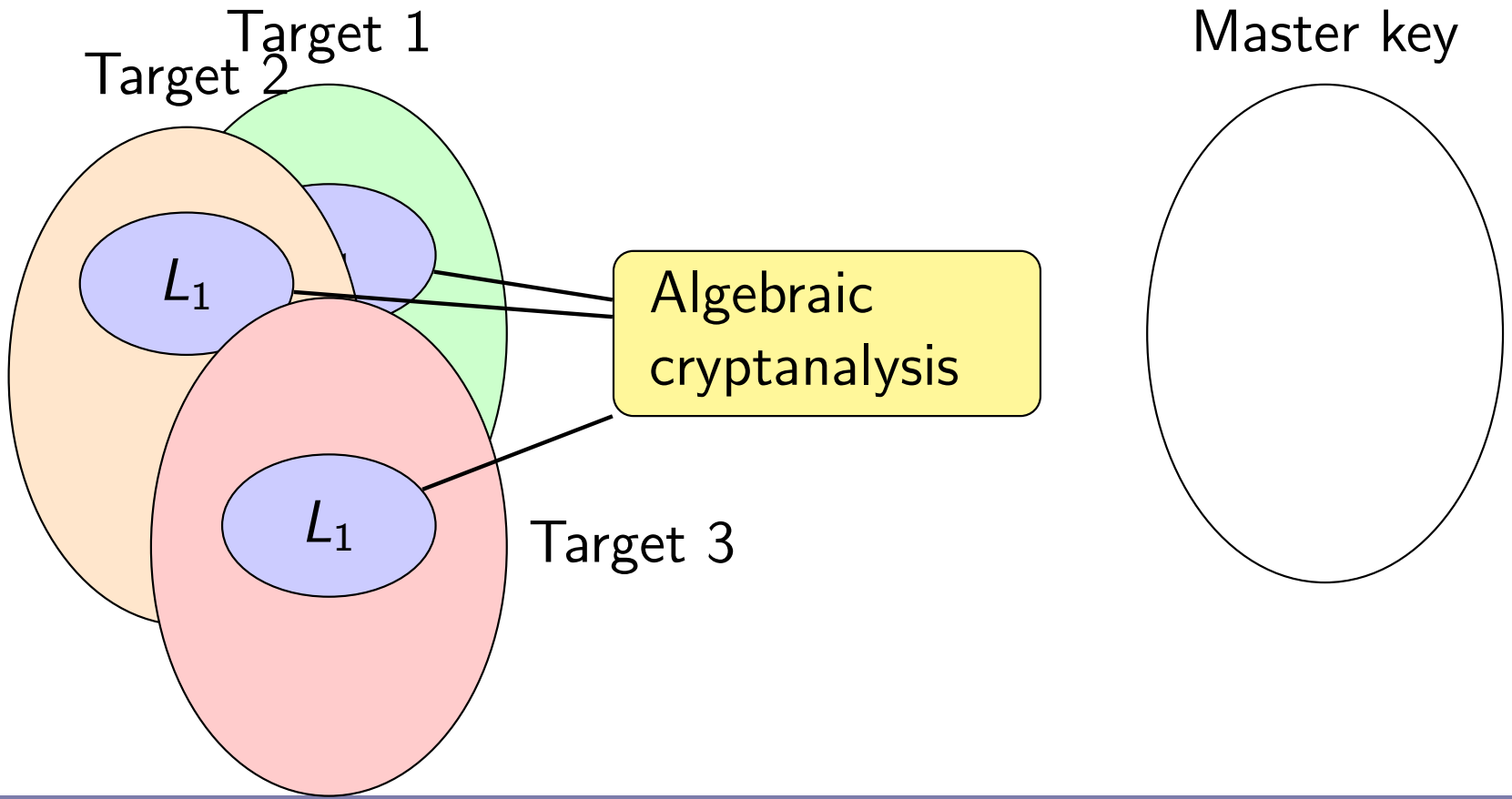
Comparison with DPA

Algebraic side-channel attack



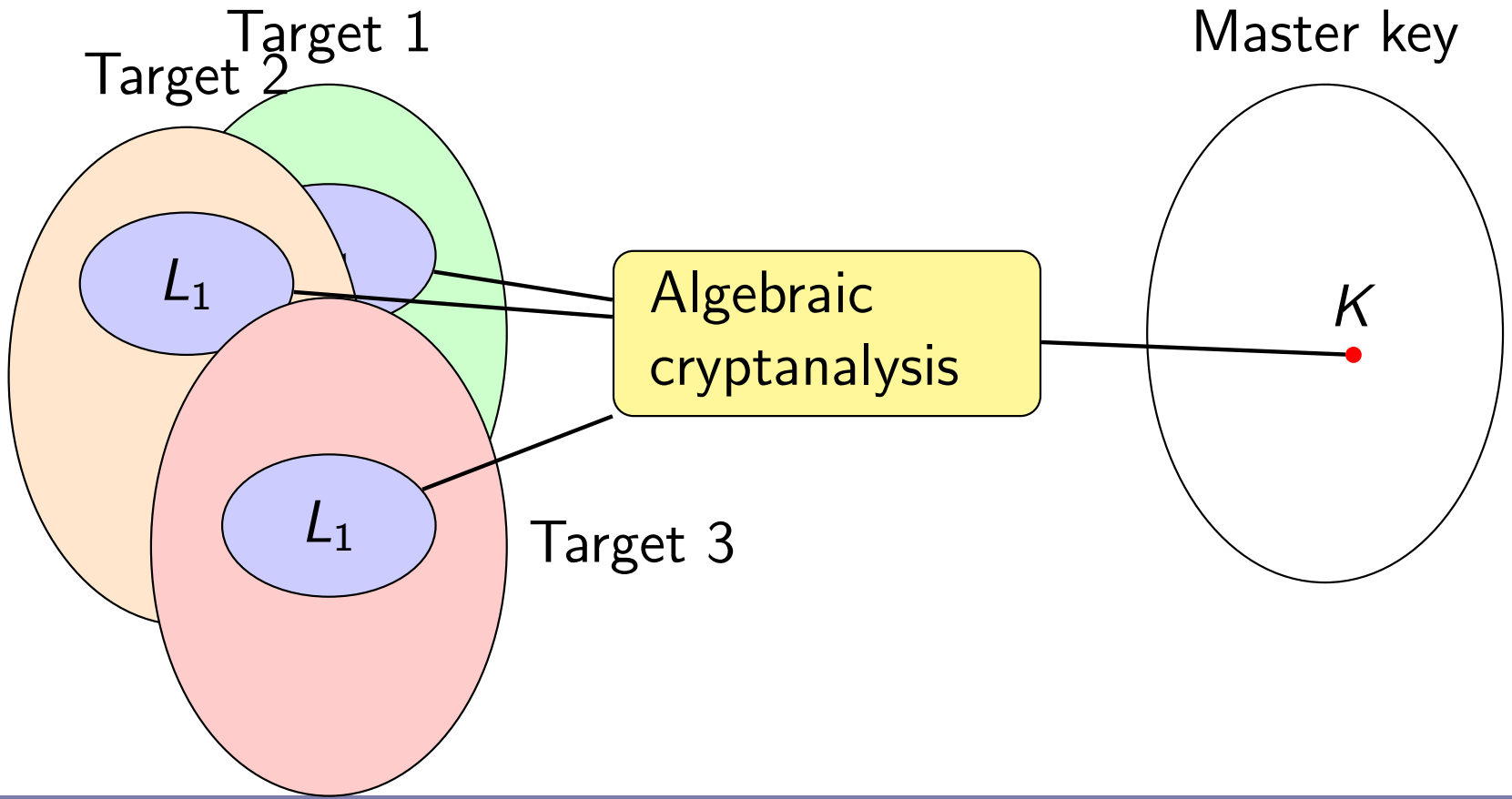
Comparison with DPA

Algebraic side-channel attack



Comparison with DPA

Algebraic side-channel attack



Outline

Introduction

Algebraic Side-Channel Attack

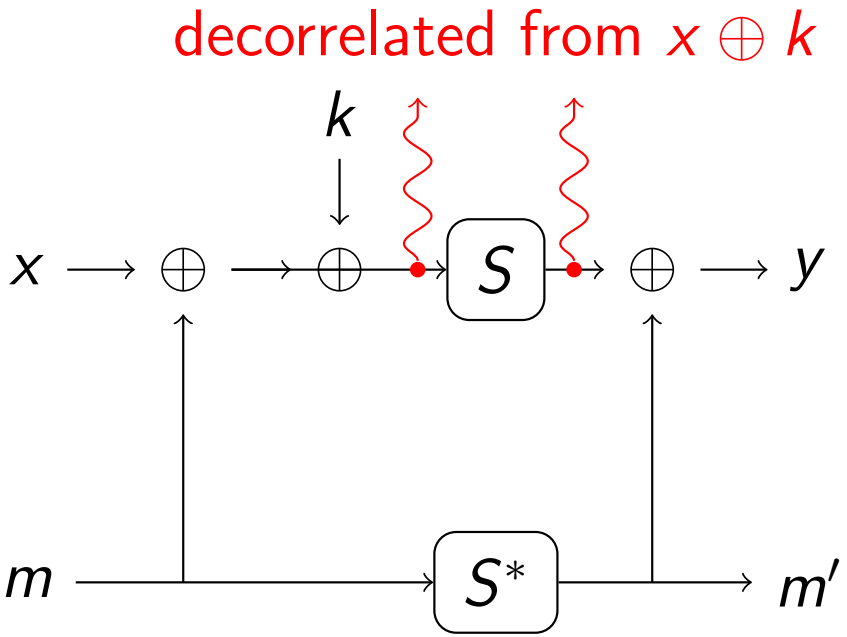
Comparison with DPA

Advanced scenarios

Conclusion

Advanced scenarios

Masked implementation

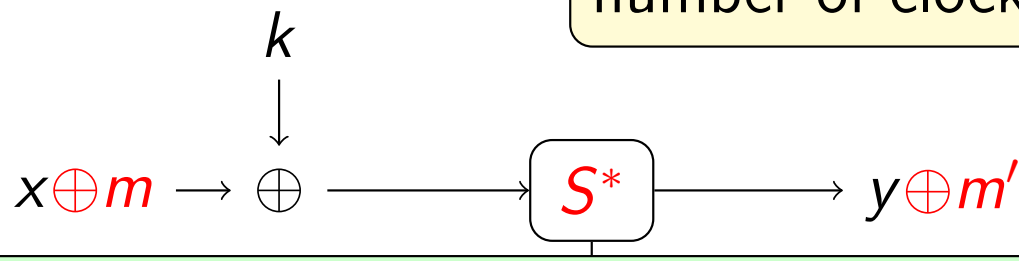


Advanced scenarios

Masking with S-box pre-computation (Herbst et al., 2006).

Mask size = 48 bits

Little impact on the number of clock cycles



New table look-up S^*; S^* is pre-computed on the fly for m and m'.

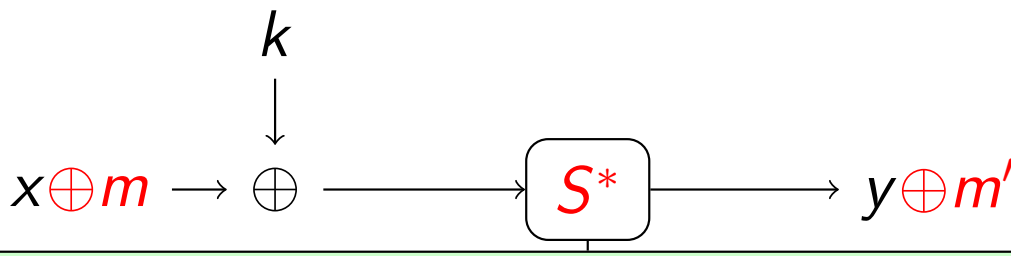
Some additional targets, but increased algebraic complexity $\Rightarrow$ **harder** to attack.

Advanced scenarios

Masking in $GF(2^4)^2$ (Oswald and Schramm, 2005).

Each S-box can have a different mask

Bigger impact on the number of clock cycles

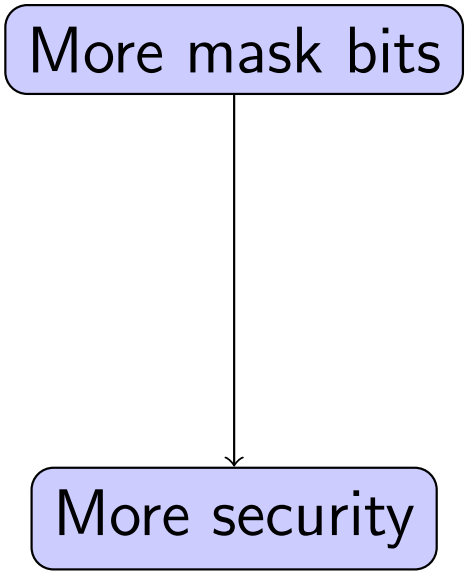


Masked inversion in $GF(2^4)^2$ via 14 table look-ups and 15 XOR operations.

A lot more targets $\Rightarrow$ **easier** to attack.

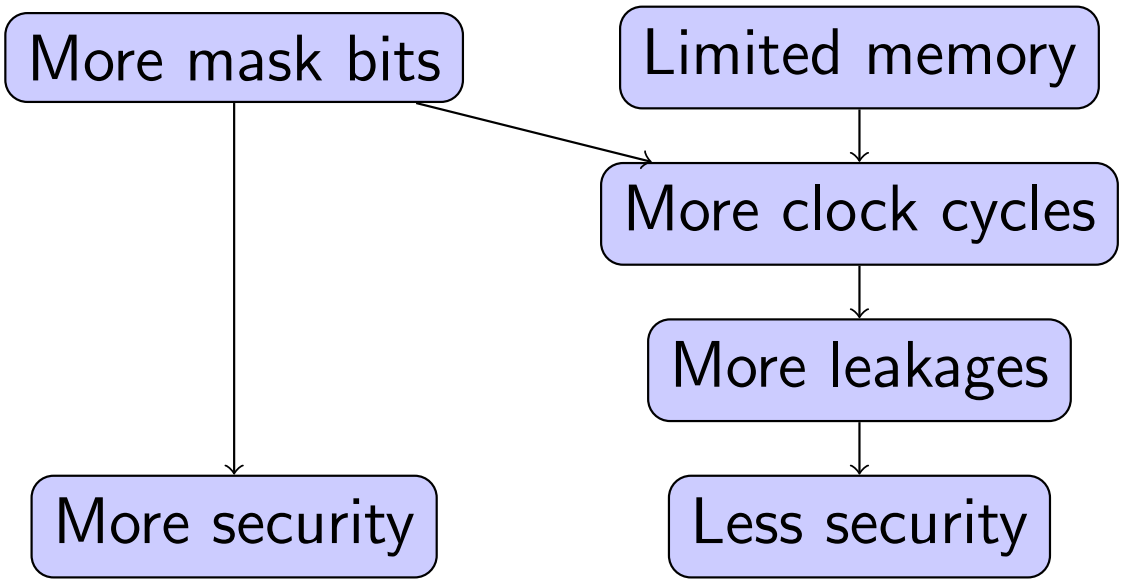
Advanced scenarios

Classical assumption



Advanced scenarios

Algebraic side-channel attack



Time also matters.

Outline

Introduction

Algebraic Side-Channel Attack

Comparison with DPA

Advanced scenarios

Conclusion

Conclusion

Advantages

- data complexity $q = 1$
- side-channel information from everywhere in the cryptosystem
- efficient in an unknown plaintext/ciphertext context
- efficient against some masked implementations

Disadvantages

- require a strong profiling phase
- not error-tolerant

Conclusion

Between theoretical and practical

require a strong profiling phase

data complexity = 1

What about the rekeying strategies?

Thank you for your attention.