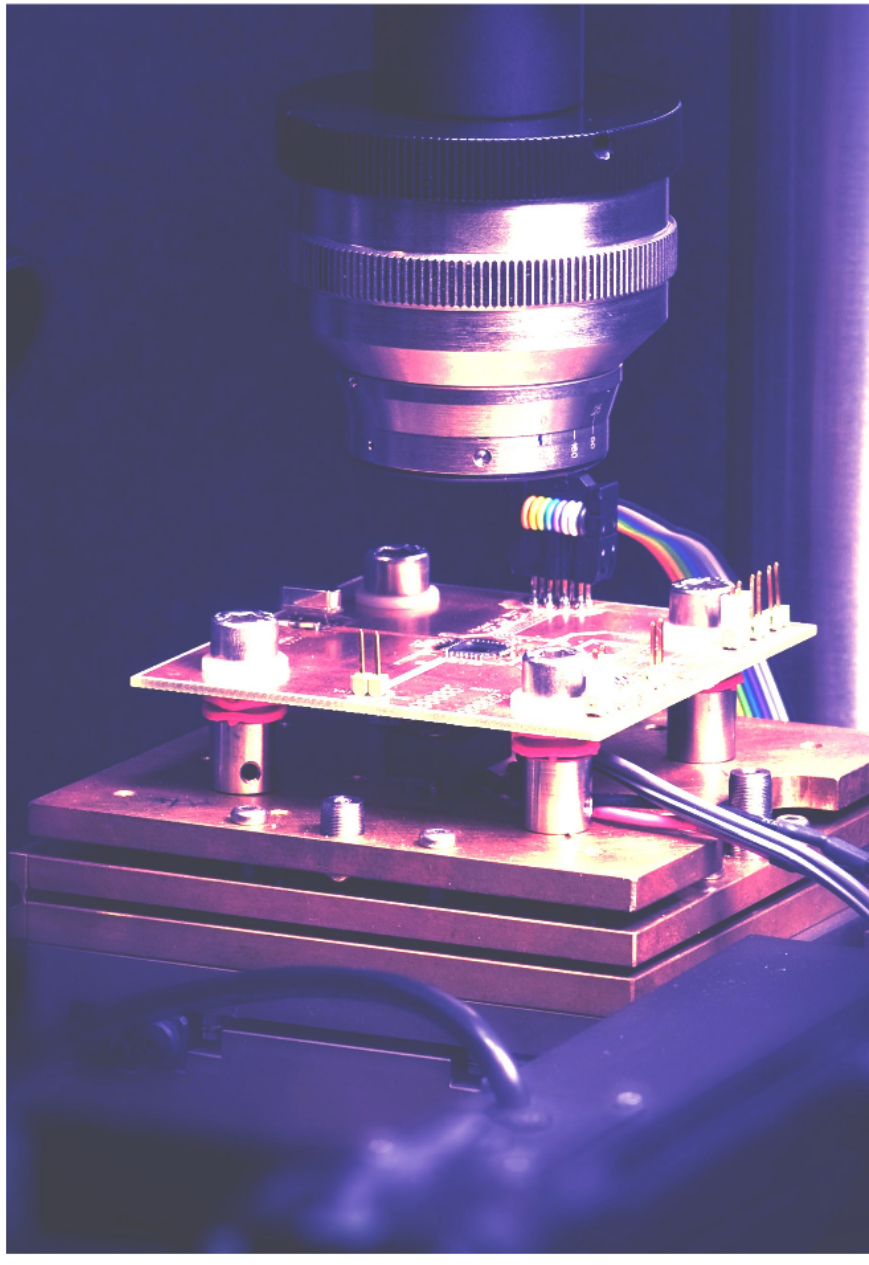
Differential Photonic Emission Analysis

Juliane Krämer

Security in Telecommunications
Technische Universität Berlin

COSADE 2013



The Photonic Side Channel

- analysis of photoemissions from switching transistors
- selective analysis of specific parts of the hardware
- utilizes both spatial and temporal information
- requires physical access to the chip
- requires access to the implementation

The Photonic Side Channel

- analysis of photoemissions from switching transistors
- selective analysis of specific parts of the hardware
- utilizes both spatial and temporal information
- requires physical access to the chip
- requires access to the implementation

The Photonic Side Channel

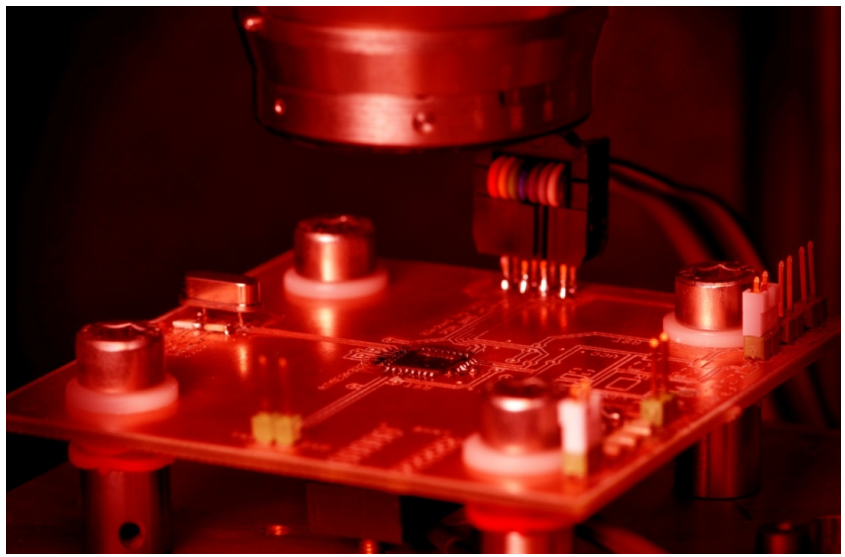
- analysis of photoemissions from switching transistors
- selective analysis of specific parts of the hardware
- utilizes both spatial and temporal information
- requires physical access to the chip
- requires access to the implementation

The Photonic Side Channel

- analysis of photoemissions from switching transistors
- selective analysis of specific parts of the hardware
- utilizes both spatial and temporal information
- requires physical access to the chip
- requires access to the implementation

The Photonic Side Channel

- analysis of photoemissions from switching transistors
- selective analysis of specific parts of the hardware
- utilizes both spatial and temporal information
- requires physical access to the chip
- requires access to the implementation



When AES blinks (2008)

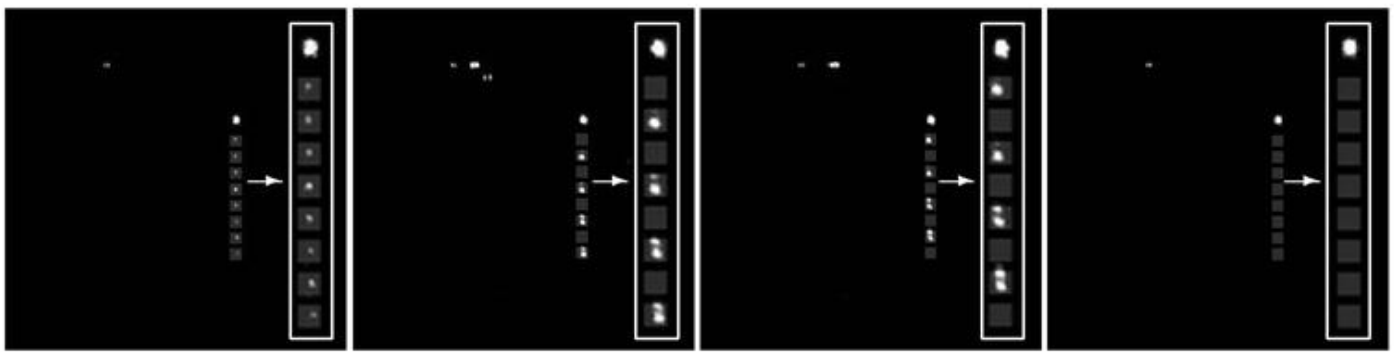
- attacking the initial AddRoundKey operation of AES ($\oplus$)
- measurement of emitted photons in SRAM

- Picosecond Imaging Circuit Analysis (PICA)

Ferrigno et al. 2008

When AES blinks (2008)

- attacking the initial AddRoundKey operation of AES ($\oplus$)
- measurement of emitted photons in SRAM

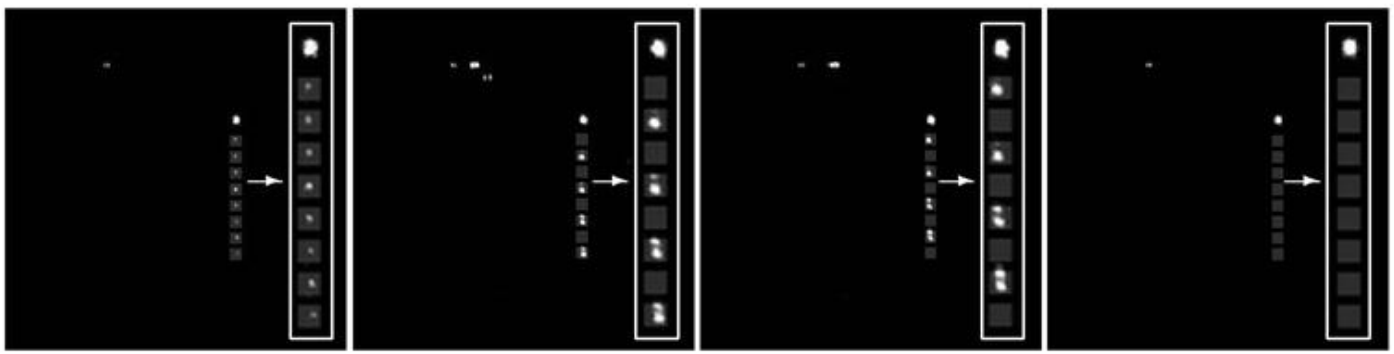


- Picosecond Imaging Circuit Analysis (PICA)

Ferrigno et al. 2008

When AES blinks (2008)

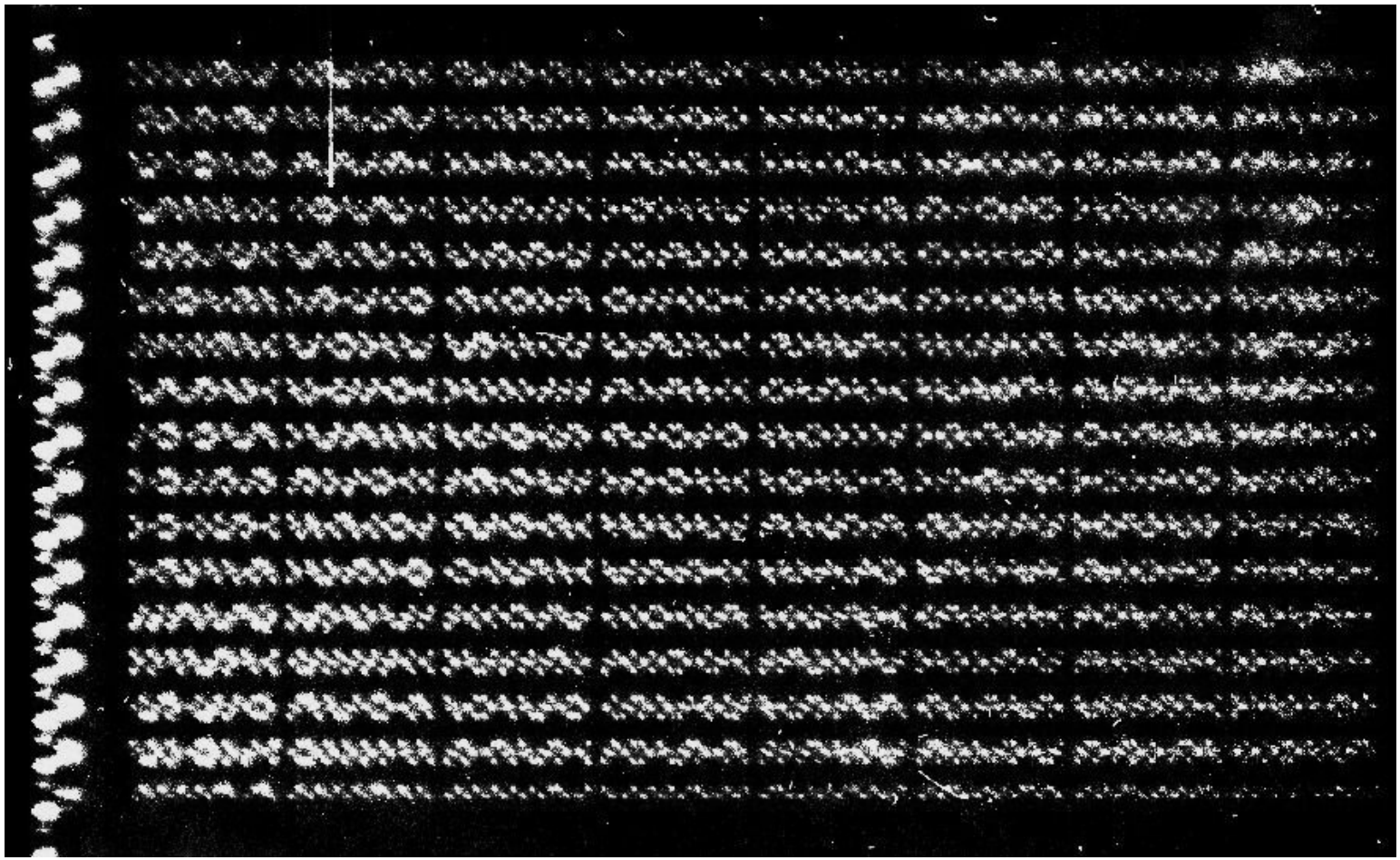
- attacking the initial AddRoundKey operation of AES ($\oplus$)
- measurement of emitted photons in SRAM



- Picosecond Imaging Circuit Analysis (PICA)

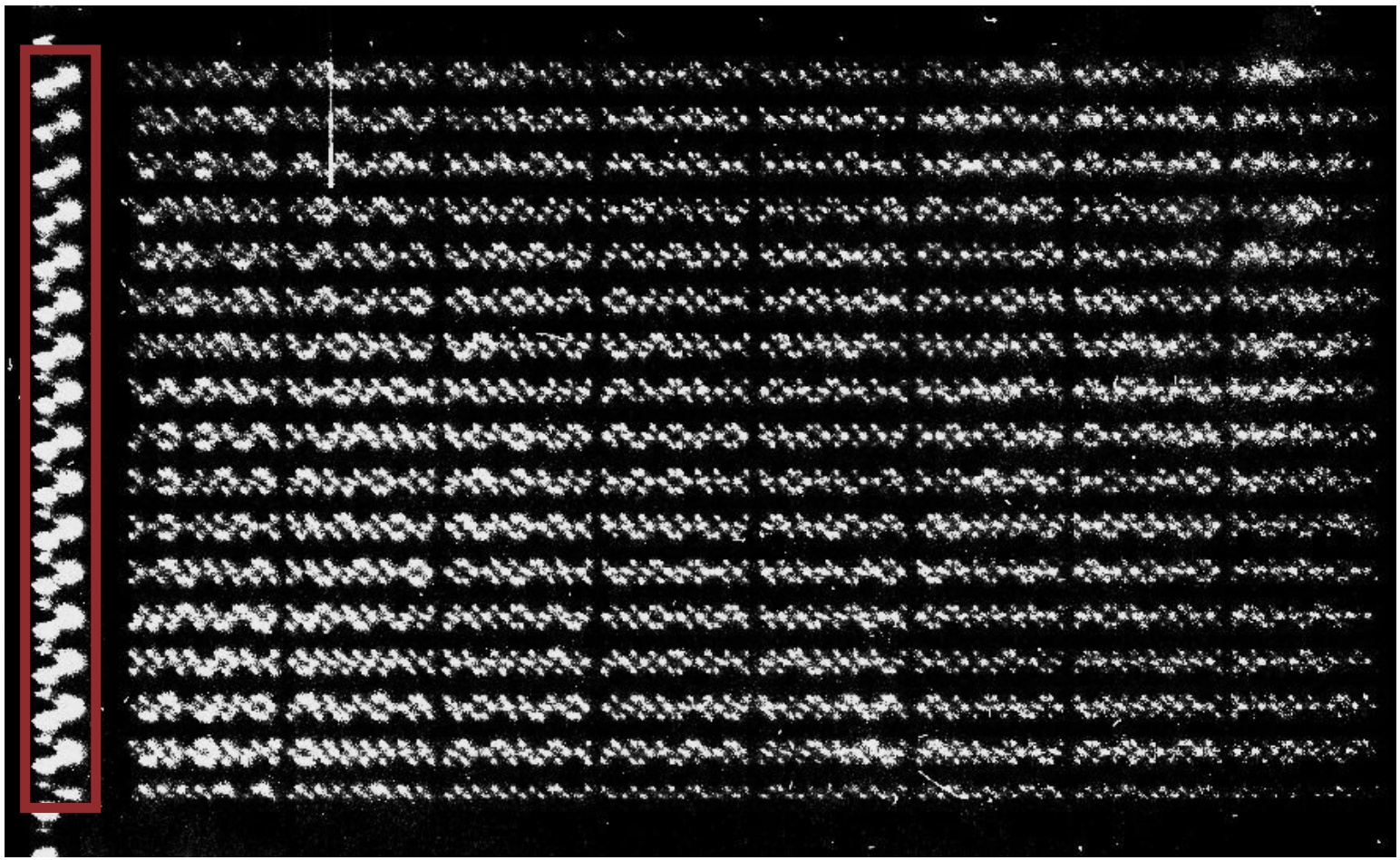
Ferrigno et al. 2008

Simple Photonic Emission Analysis (2012)



Schlösser et al. 2012

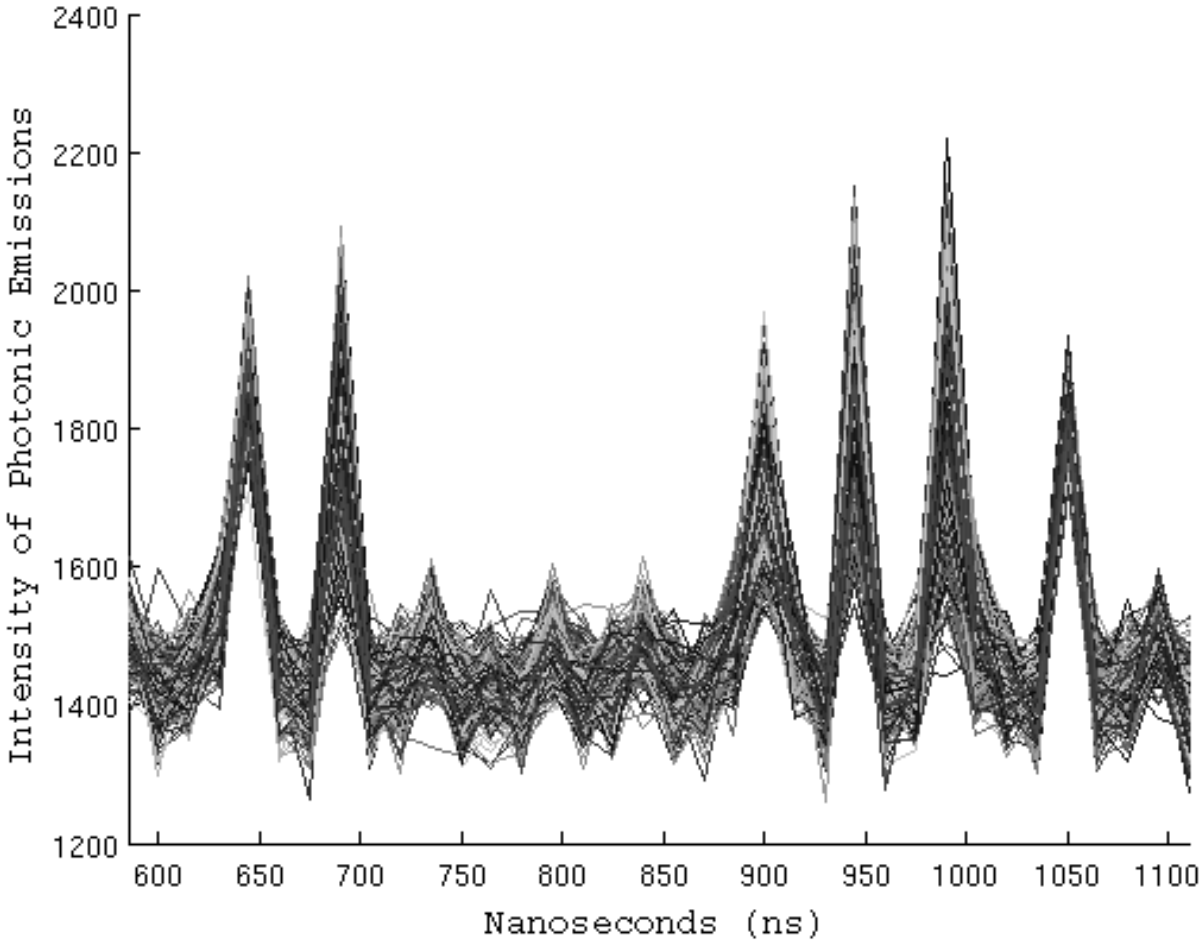
Simple Photonic Emission Analysis (2012)



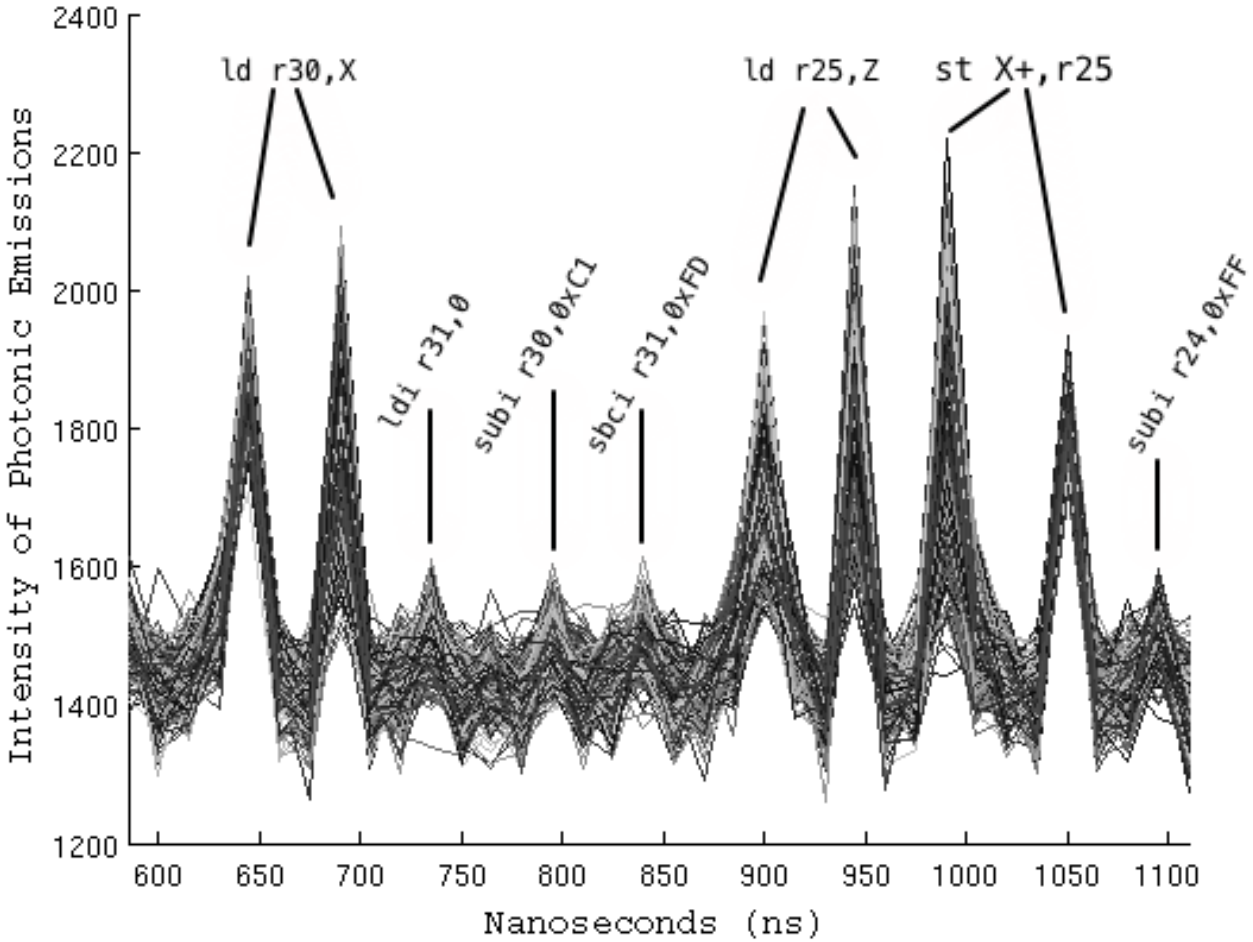
Schlösser et al. 2012

Differential Photonic Emission Analysis

Photonic Emissions during a SubBytes operation



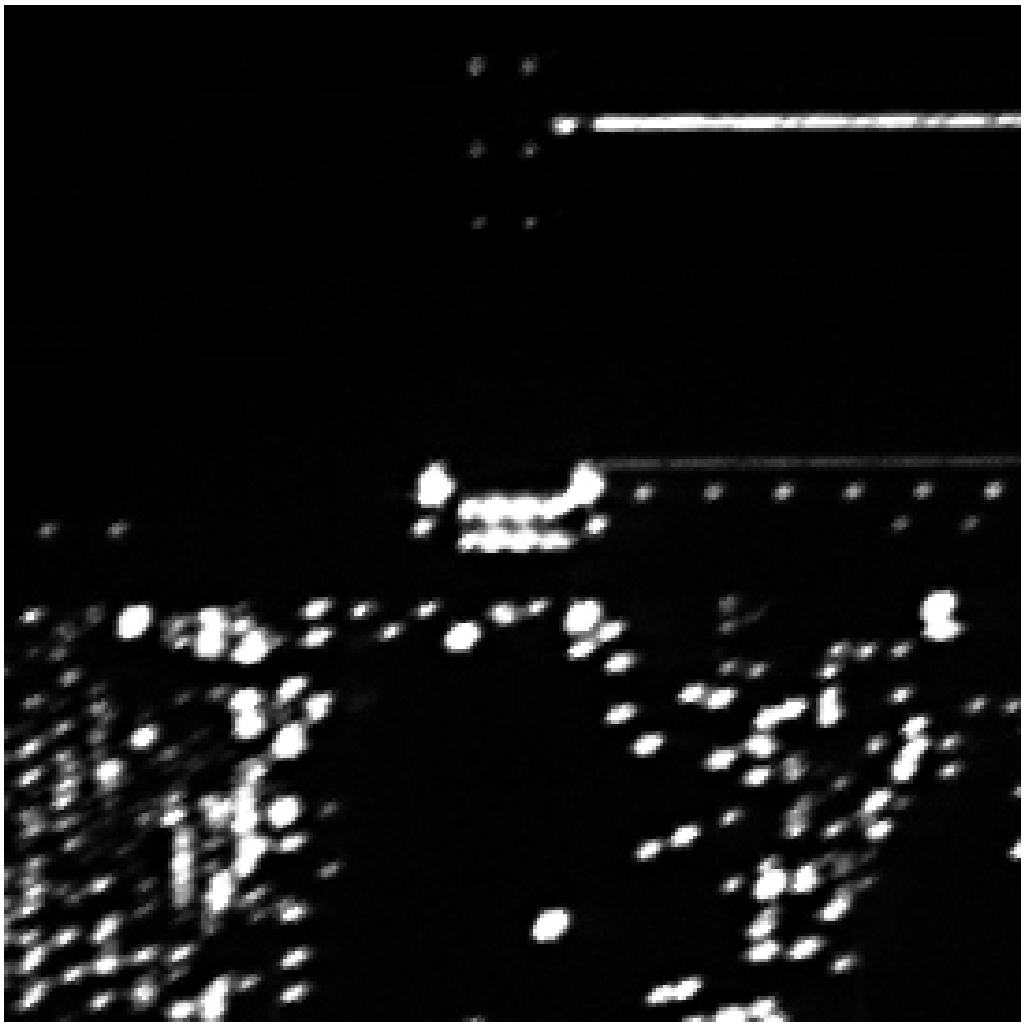
Photonic Emissions during a SubBytes operation



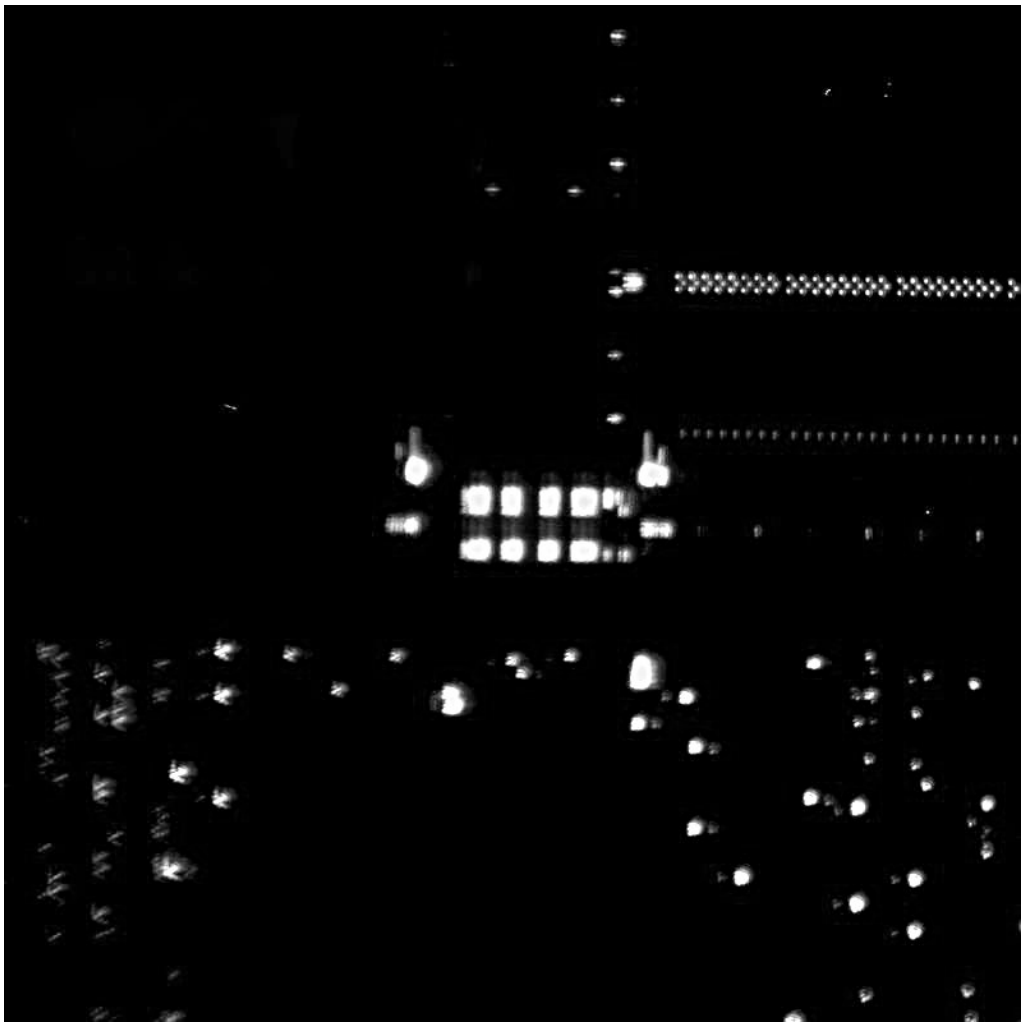
Spatial Analysis

Spatial Analysis

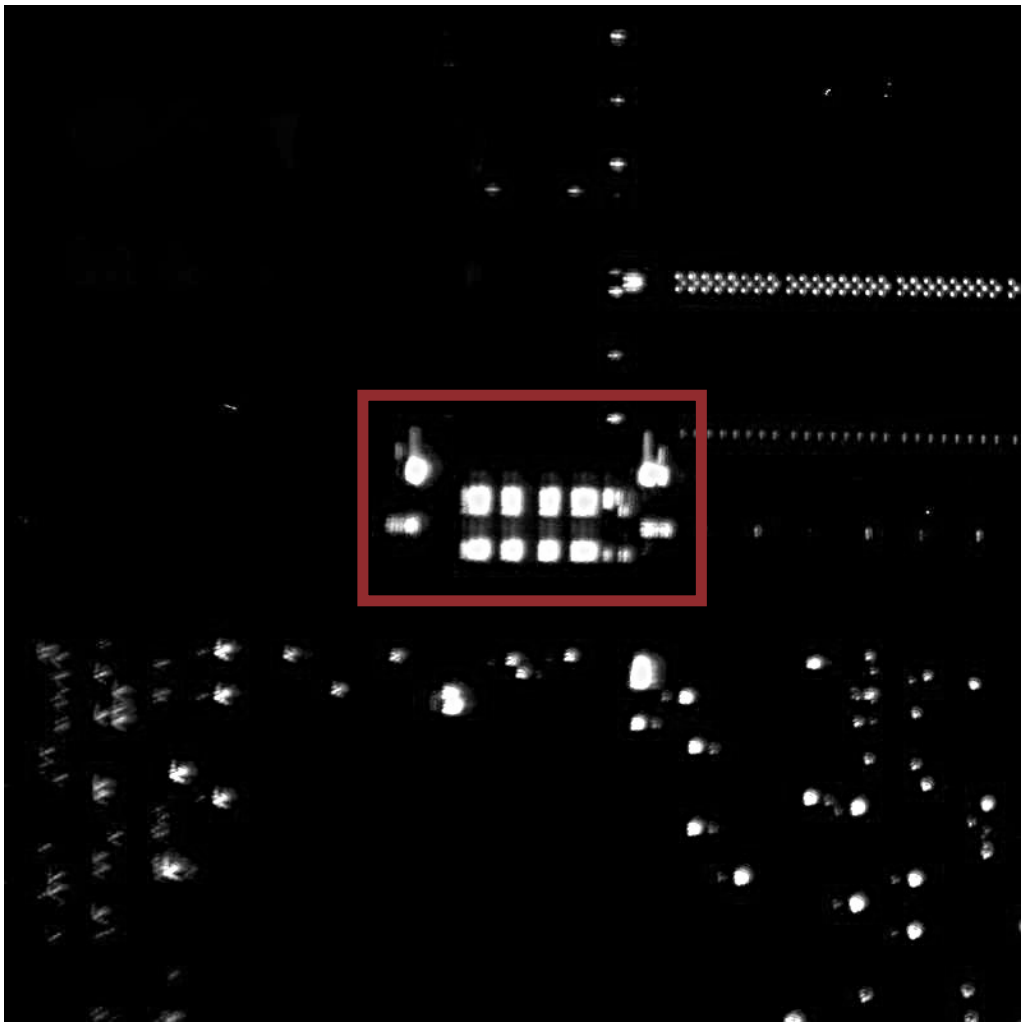
Spatial Analysis



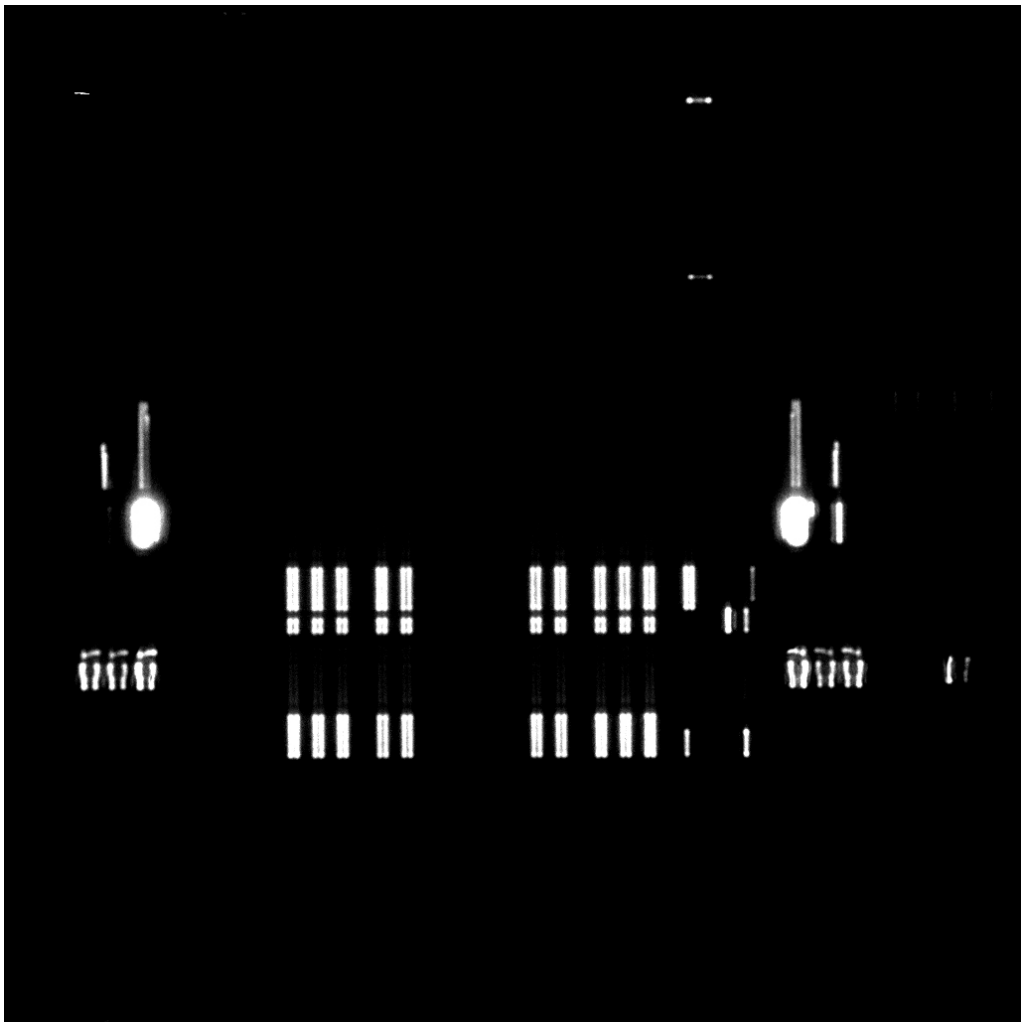
Spatial Analysis



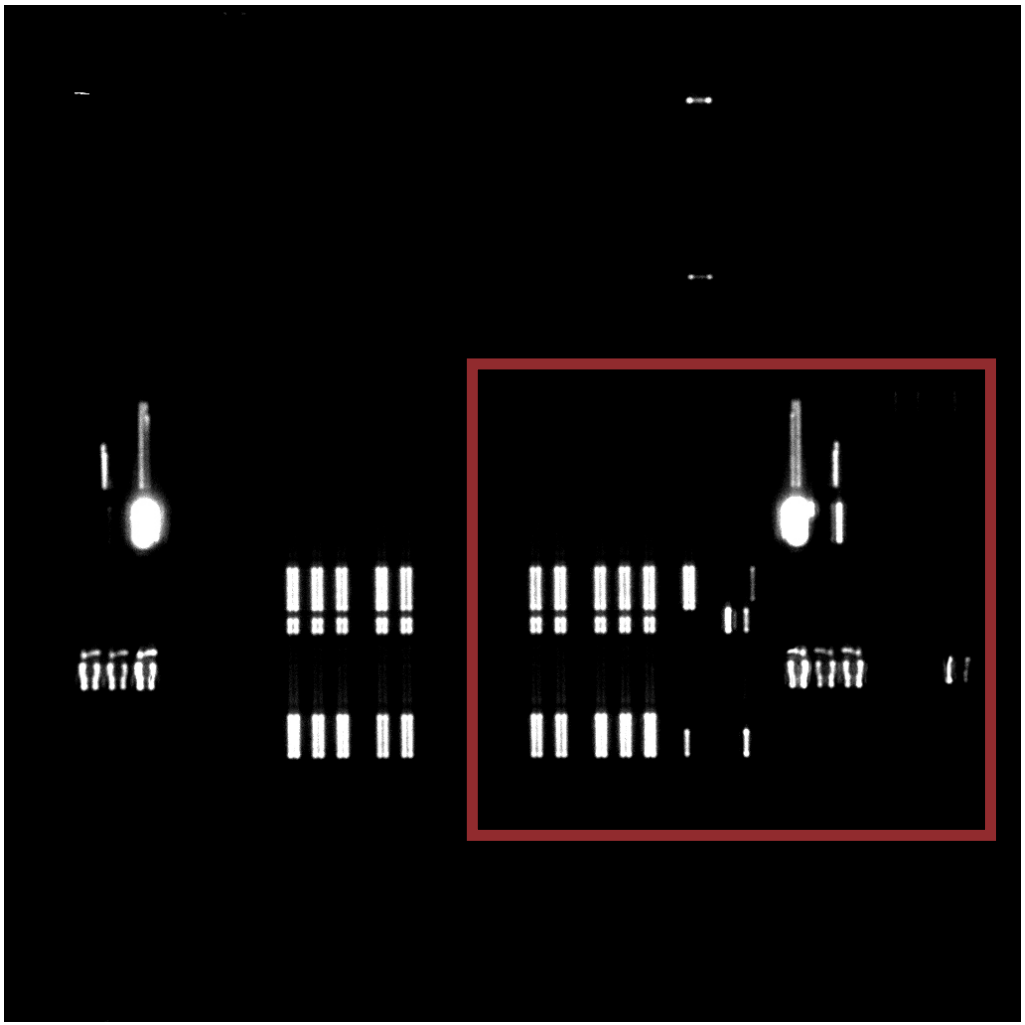
Spatial Analysis



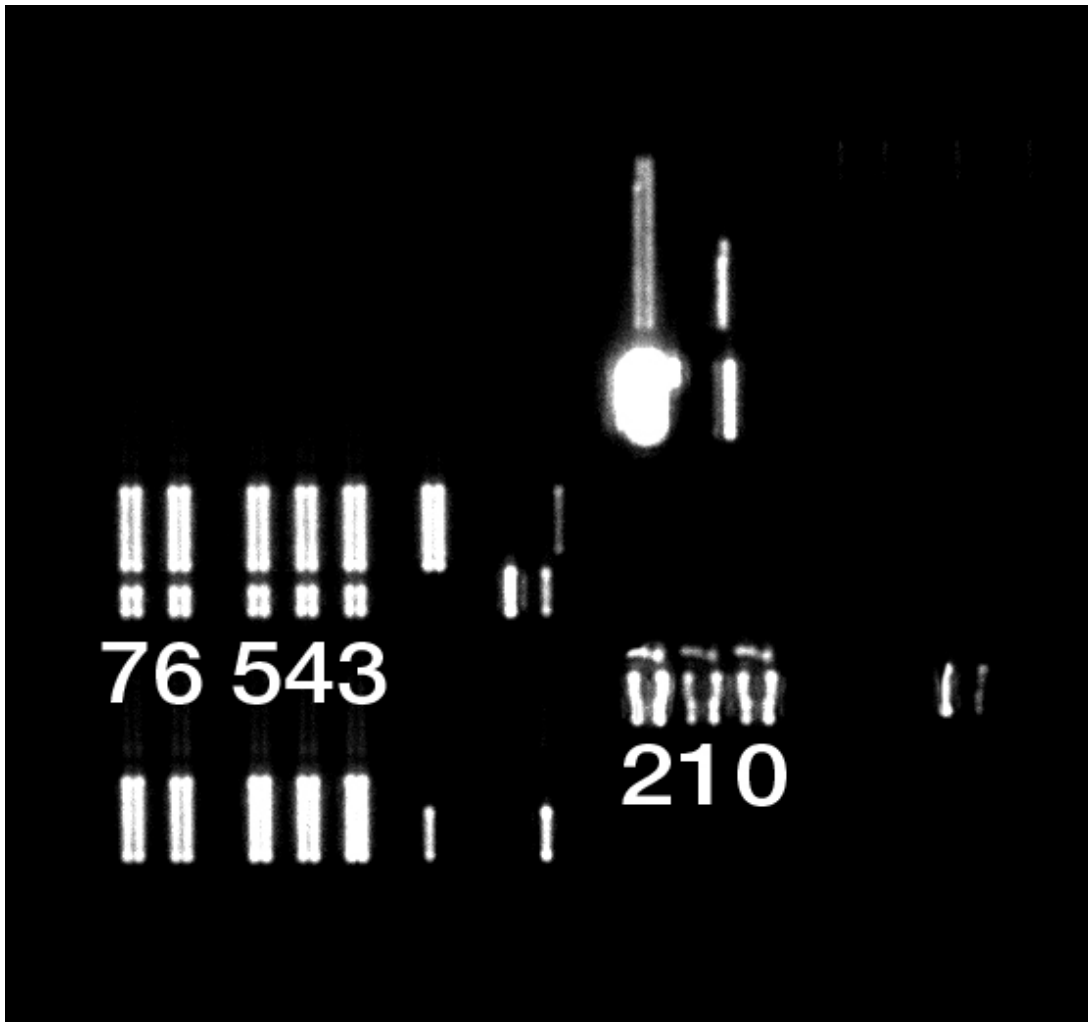
Spatial Analysis



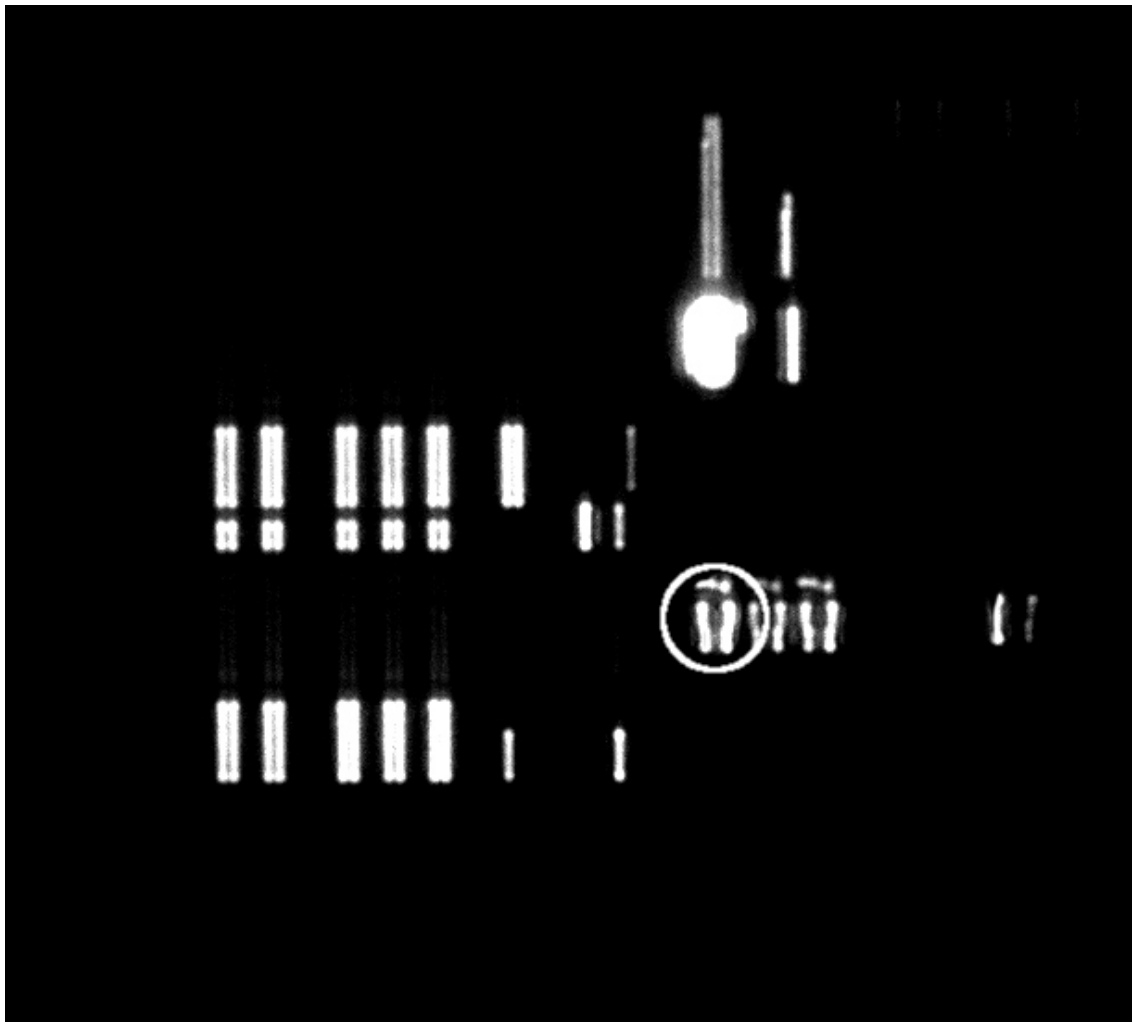
Spatial Analysis



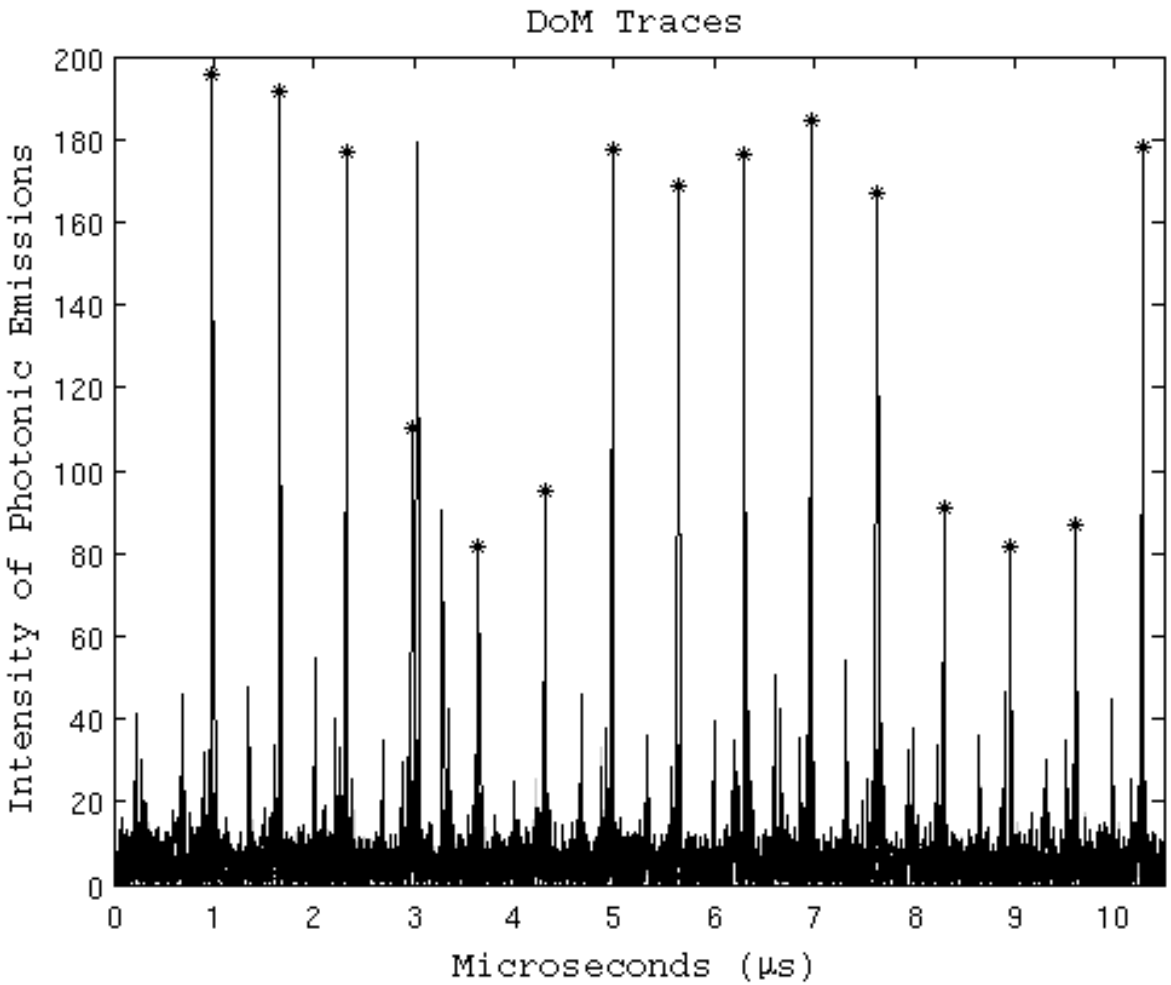
Spatial Analysis



Spatial Analysis



Result of the Difference of Means Analysis



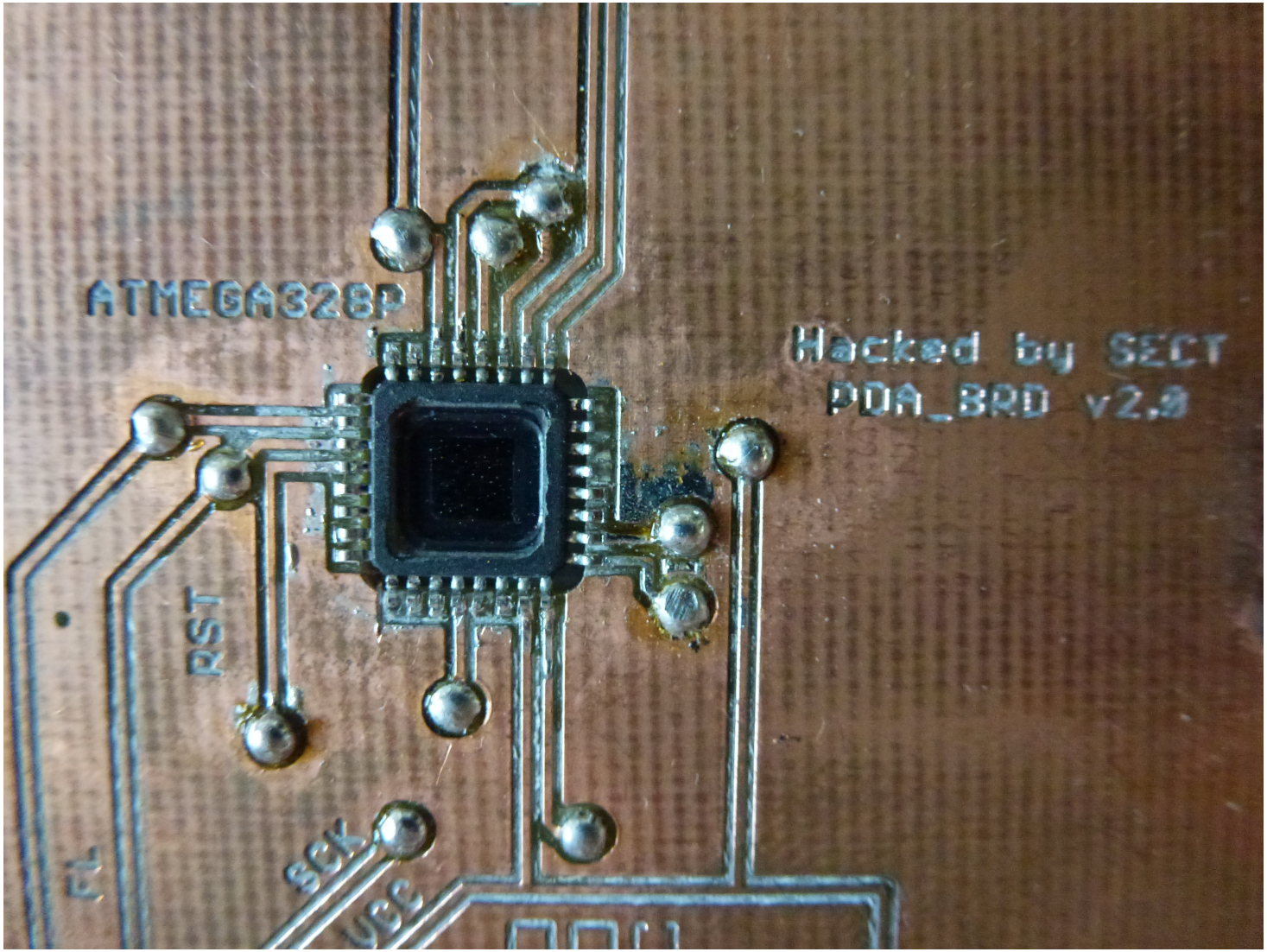
Thank you!

The photonic side channel poses a real threat nowadays.

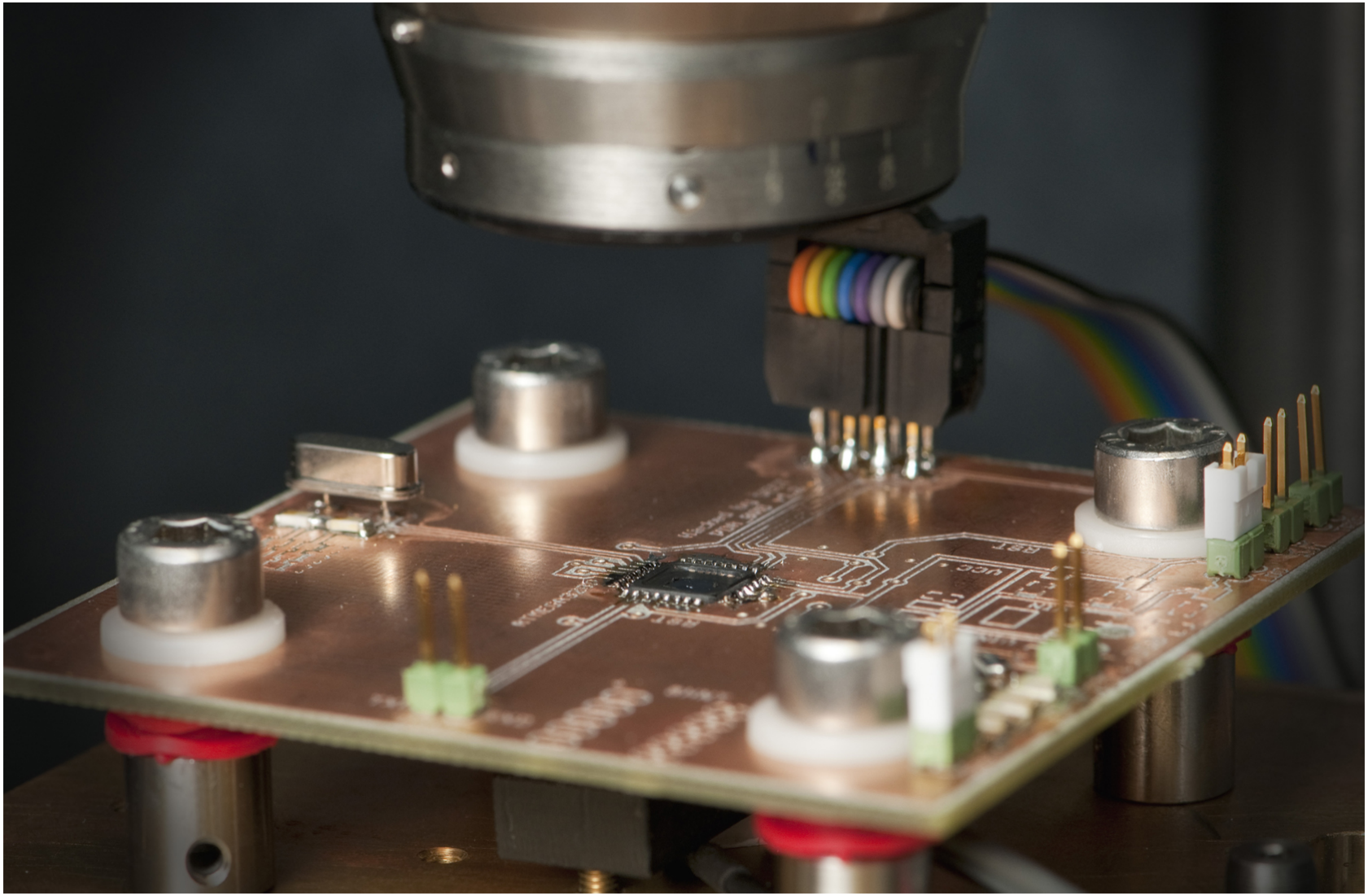
- The equipment necessary for the measurements is affordable.
- As well simple as differential successfull attacks have been shown.
- No efficient countermeasures! $\rightarrow$ Future work.

Questions?

Freigelegter Chip auf einer Leiterplatte



Test-Mikrocontroller unter dem Mikroskop



Schlösser et al. 2012

CHES 2012: Simple Photonic Emission Analysis

Simple Photonic Emission Analysis of AES

Photonic side channel analysis for the rest of us

Alexander Schlösser*,[1], Dmitry Nedospasov*,[2], Juliane Krämer[2],
Susanna Orlic[1], Jean-Pierre Seifert[2]

[1]Optical Technologies, Technische Universität Berlin, Germany
{schloesser,orlic}@opttech.tu-berlin.de
[2]Security in Telecommunications, Technische Universität Berlin, Germany
{dmitry,juliane,jpseifert}@sec.t-labs.tu-berlin.de
* Equal contribution

Abstract. This work presents a novel low-cost optoelectronic setup for time- and spatially resolved analysis of photonic emissions and a corresponding methodology, Simple Photonic Emission Analysis (SPEA). Observing the backside of ICs, the system captures extremly weak photoemissions from switching transistors and relates them to program running in the chip. SPEA utilizes both spatial and temporal information about these emissions to perform side channel analysis of ICs. We successfully performed SPEA of a proof-of-concept AES implementation and were able to recover the full AES secret key by monitoring accesses to the S-Box. This attack directly exploits the side channel leakage of a single transistor and requires no additional data processing. The system costs and the necessary time for an attack are comparable to power analysis techniques. The presented approach significantly reduces the amount of effort required to perform attacks based on photonic emission analysis and allows AES key recovery in a relevant amount of time.

Differential Photonic Emission Analysis

Juliane Krämer[1], Dmitry Nedospasov[1],
Alexander Schlösser[2], Jean-Pierre Seifert[1]

[1]Security in Telecommunications, Technische Universität Berlin, Germany
{juliane,dmitry,jpseifert}@sec.t-labs.tu-berlin.de
[2]Optical Technologies, Technische Universität Berlin, Germany
{schloesser}@opttech.tu-berlin.de

Abstract. This work presents the first differential side channel analysis to exploit photonic emissions. We call this form of analysis Differential Photonic Emission Analysis (DPEA). After identifying a suitable area for the analysis, our system captures photonic emissions from switching transistors and relates them to the program running in the chip. The subsequent differential analysis reveals the secret key. We recovered leakage from the datapath's driving inverters of a proof of concept AES-128 implementation. We successfully performed DPEA and were able to recover the full AES secret key from the photonic emissions. The system costs for an attack are comparable to power analysis techniques and the presented approach allows for AES key recovery in a relevant amount of time. Thus, this work extends the research on the photonic side channel and emphasizes that the photonic side channel poses a serious threat to modern secure ICs.

AES - Advanced Encryption Standard

- DES-Nachfolger
- 'Rijndael'
- vom NIST im Jahr 2000 standardisiert
- 128-bit Blockchiffre
- variable Schlüsselgröße: 128, 192 oder 256 bits
- 10, 12 oder 14 Runden (abhängig von der Schlüssellänge)
- byte-weise Operationen

AES - 128

- initial: AddRoundKey ($\oplus$)
- 9 Runden
  - SubBytes - die einzige nicht-lineare Operation
  - ShiftRows
  - MixColumns
  - AddRoundKey
- 10. Runde
  - SubBytes
  - ShiftRows
  - AddRoundKey

Literatur

- J. Ferrigno, M. Hlaváč. When AES blinks: introducing optical side channel. Information Security, IET, vol.2, no.3, pp.94-98, September 2008
- P. C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Proc Int Cryptol Conf, Volume 1109 of Lecture Notes in Computer Science, Springer 1996
- J. Krämer, D. Nedospasov, A. Schlösser, J.-P. Seifert. Differential Photonic Emission Analysis. International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2013), Paris, Frnace, 2013
- A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, J.-P. Seifert. Simple Photonic Emission Analysis of AES. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2012), Leuven, Belgium, 2012