Differential Photonic Emission Analysis

Juliane Krämer

Security in Telecommunications Technische Universität Berlin

COSADE 2013





- 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

- 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

- 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

- 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

- 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)

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)

Simple Photonic Emission Analysis (2012)

alter at state water a state of a to be a state of the second at the second at the state of the second at the s a state have been a state and a state of a state of a state of the state of the state of the state of the state the state in the standard of the state and the state in the state of the state of the state of the state of the මන්තරාවක් මෙන්තරාවක් ස්කර්ත්රයක් අතරවන් මත්තර කරන කරන්නේ දිදුවන්න දින්තරාවක් මාන්තරාවක් මහතාවක් මෙන්තරාවක් මත්ත くくざい うちょうかん しょうかい かくしょう しょうしょう かくしょうしょう しょうしょう ම කියටමින් කිරීමෙකින් මැදීමේ මාර්ගම මාර්ගම මාර්ගමයක් මාර්ගමයක් මාර්ගමයක් මාර්ගමයක් මාර්ගමයක් මාර්ගමයක් මාර්ගමයක ලංකාරකක්ෂේ මැමිණීමෙක් මෙන්තිමෙක් මැතිවෙන්නේ කිරීමෙන්නේ කිරීමෙන්ත් මාන්තිමේ මාන්තිමේ මාන්තිමේ මෙන්ත් මාන්තිමේ ම ーン・レント・ いくつうがい ちゅうろうちょ しんりょうろう ろうしゅうしょ ちょうしんせい むくひはし いちんせいさく star a star bestar star a s and the second secon a saturation and the state the present of the present state the state of the and the second and the second of the second second and where the advantage of the second

Simple Photonic Emission Analysis (2012)

in a start a second to be a start and a start and a second to be a start a second a start a start and a start a a the state in the second state in a final second state of a state state state of the state state and state att ***** and the second and the second seco the state in the standard of the state and the state in the state of the state of the state of the state of the ක්ෂාවන්ත්රී නියේතිවාදීම කියන් මොල මෙන්න කරන වෙන වෙන්න සිංහින විටාදීම වැඩි කියනීම ද くくざく うちょうしょう しょうかい しょうしょう しょうしょう しょうしょう しょうしょう しょうしょう しょうしょう しょうしょう ひょうしょう and the standard of the second second and the standard and the second second second second second second second ろうかんごうそう うかんかんかん うちゅうかんかん ひろうちょう うちゃくよう かく べんかいかんかい ひかかくかんがい いくしょうしょう しょうりょう しょうしょう しょうしょう いんしょう しょうしょう しょうしょう a star والمراجعة والمراجع والمراجع والمتعاد والمراجع و <u>ar a the second and the second states of the second states that second states the constants of the constants and the constants and the constants are c</u> and the second and the second of the second second rectander to a consider the and the constant



Differential Photonic Emission Analysis

Photonic Emissions during a SubBytes operation



Photonic Emissions during a SubBytes operation





















Result of the Difference of Means Analysis



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 14/14

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 Krämer², Susanna Orlic¹, Jean-Pierre Seifert²

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

COSADE 2013: Differential Photonic Emission Analysis

Differential Photonic Emission Analysis

Juliane Krämer¹, Dmitry Nedospasov¹, Alexander Schlösser², Jean-Pierre Seifert¹

¹Security in Telecommunications, Technische Universität Berlin, Germany {juliane,dmitry,jpseifert}@sec.t-labs.tu-berlin.de ²Optical 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. <u>Timing Attacks on Implementations of Diffie-Hellman</u>, <u>RSA</u>, <u>DSS</u>, and <u>Other Systems</u>, Proc Int Cryptol Conf, Volume 1109 of Lecture Notes in Computer Science, Springer 1996
 - J. Krämer, D. Nedospasov, A. Schlösser, J.-P. Seifert. <u>Differential</u> <u>Photonic Emission Analysis</u>. 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. <u>Simple Photonic Emission Analysis of AES.</u> Workshop on Cryptographic Hardware and Embedded Systems (CHES 2012), Leuven, Belgium, 2012