Differential Power Analysis of the Picnic Signature Scheme

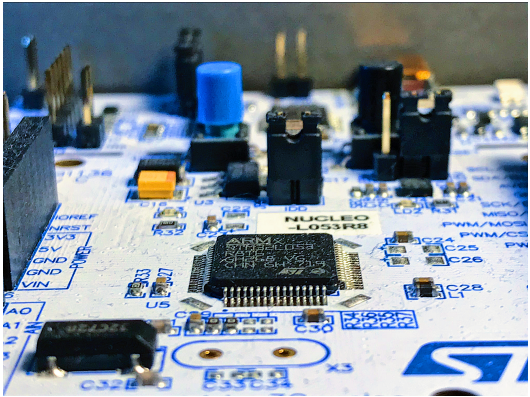
Tim Gellersen, **Okan Seker** and Thomas Eisenbarth

University of Lübeck, Germany

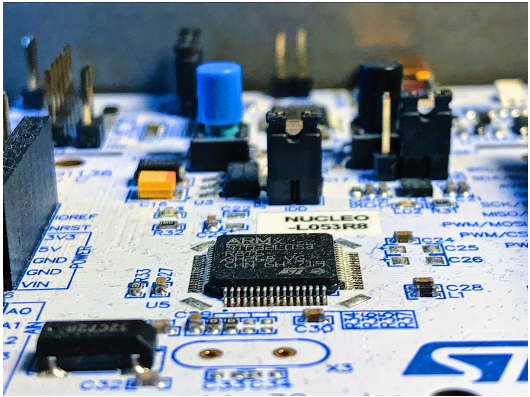
July 20, 2021
PQCrypto 2021

UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR IT SECURITY

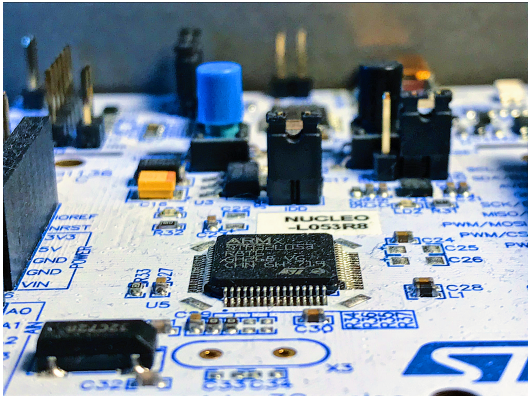
Physical Attacks on Embedded Devices



Physical Attacks on Embedded Devices

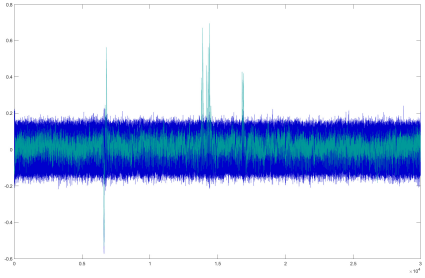


Physical Attacks on Embedded Devices



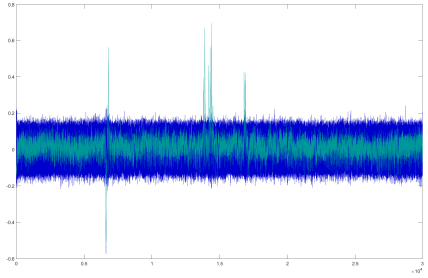
- Side Channel Attacks,
- Fault Injection,
- Timing,...

Physical Attacks on Embedded Devices



- Side Channel Attacks,
- Fault Injection,
- Timing,...

Physical Attacks on Embedded Devices



- Side Channel Attacks,
- Fault Injection,
- Timing,...

The results have been known since 1998!

Post-Quantum Cryptography Standardization: Round 3

Finalists

- CRYSTALS-DILITHIUM
- Falcon
- Rainbow

Alternates

- GeMSS
- **Picnic**
- SPHINCS+

Post-Quantum Cryptography Standardization: Round 3

Finalists

- CRYSTALS-DILITHIUM
- Falcon
- Rainbow

Alternates

- GeMSS
- **Picnic**
- SPHINCS+

Side-channel analysis on *protocol level* has a widespread attention.

Post-Quantum Cryptography Standardization: Round 3

Finalists

- CRYSTALS-DILITHIUM
- Falcon
- Rainbow

Alternates

- GeMSS
- **Picnic**
- SPHINCS+

Side-channel analysis on *protocol level* has a widespread attention.

Picnic signature scheme

- Fiat–Shamir-type signature from **MPC-in-the-head** ZKP.
- ☺ No number-theoretic assumptions
  - Block cipher
  - Hash function (modeled as RO)
- ☺ Various parameters

Our Contribution

The applicability of DPA attacks to protocols relying on the MPC-in-the-head paradigm.

Our Contribution

The applicability of DPA attacks to protocols relying on the MPC-in-the-head paradigm.

Two practical attacks to recover the secret key used in MPC-LowMC.

- An attack on the secret sharing process
- An attack on the Multiparty Computation of the `SboxLayer`

Our Contribution

The applicability of DPA attacks to protocols relying on the MPC-in-the-head paradigm.

Two practical attacks to recover the secret key used in MPC-LowMC.

- An attack on the secret sharing process
- An attack on the Multiparty Computation of the `SboxLayer`

A practical setup with a FRDM-K66F development board while monitoring electromagnetic emanation.

Our Contribution

The applicability of DPA attacks to protocols relying on the MPC-in-the-head paradigm.

Two practical attacks to recover the secret key used in MPC-LowMC.

- An attack on the secret sharing process
- An attack on the Multiparty Computation of the `SboxLayer`

A practical setup with a FRDM-K66F development board while monitoring electromagnetic emanation.

A novel algebraic key recovery part to reconstruct the key

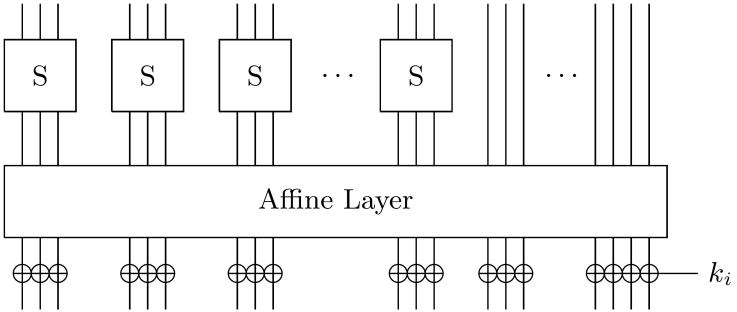
Table of Contents

LowMc Structure[1]

[1] Albrecht, M. R., Rechberger, C., Schneider, T., Tiessen, T., & Zohner, M. (2015, April). Ciphers for MPC and FHE. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 430-454).

LowMc Structure[1]

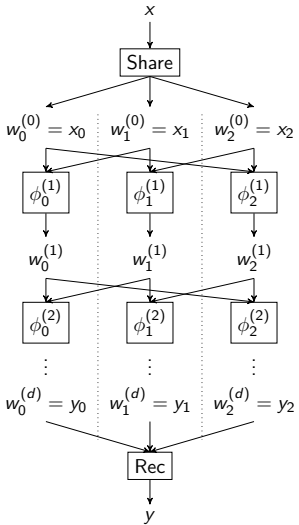
- 4 main layers: `KeyAddition`, `ConstantAddition`, `LinearLayer` and `SboxLayer`
- With low AND depth suitable for Multi-part computations.
- Only 30-bit go into the Sbox Layer



[1] Albrecht, M. R., Rechberger, C., Schneider, T., Tiessen, T., & Zohner, M. (2015, April). Ciphers for MPC and FHE. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 430-454).

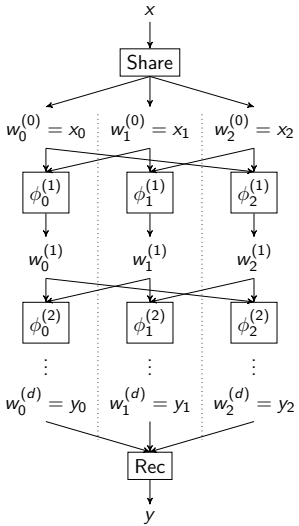
MPC-in-the-head: Zero-Knowledge for Boolean Circuits

MPC-in-the-head: Zero-Knowledge for Boolean Circuits



- Compute $y = \phi(x)$ in 3 branches.

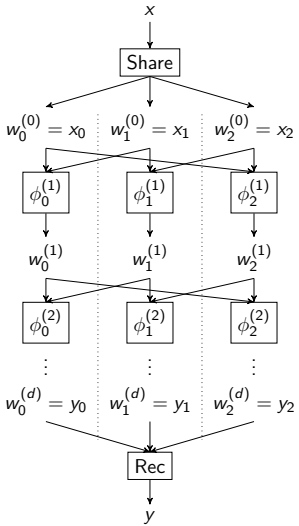
MPC-in-the-head: Zero-Knowledge for Boolean Circuits



- Compute $y = \phi(x)$ in 3 branches.
- Consider the set of functions:

$$\mathcal{D} = \{\mathsf{Share}, \mathsf{Rec}\} \cup \{\phi(x)_1, \ldots\}$$

MPC-in-the-head: Zero-Knowledge for Boolean Circuits

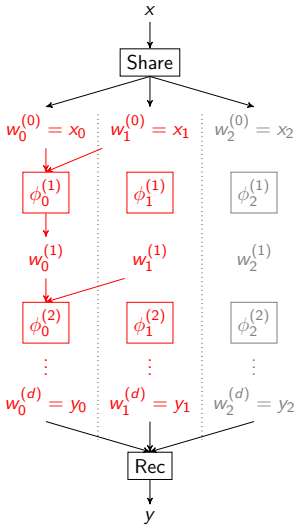


- Compute $y = \phi(x)$ in 3 branches.
- Consider the set of functions:

$$\mathcal{D} = \{\mathsf{Share}, \mathsf{Rec}\} \cup \{\phi(x)_1, \ldots\}$$

- Correctness: $y = \phi(x)$

MPC-in-the-head: Zero-Knowledge for Boolean Circuits



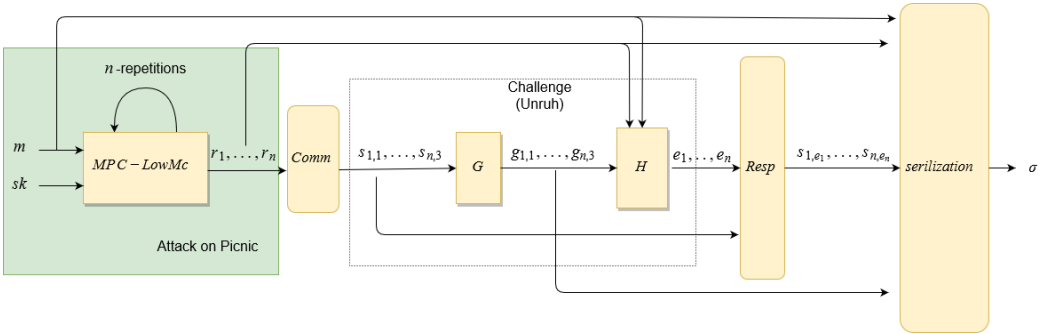
- Compute $y = \phi(x)$ in 3 branches.
- Consider the set of functions:

$$\mathcal{D} = \{\text{Share}, \text{Rec}\} \cup \{\phi(x)_1, \ldots\}$$

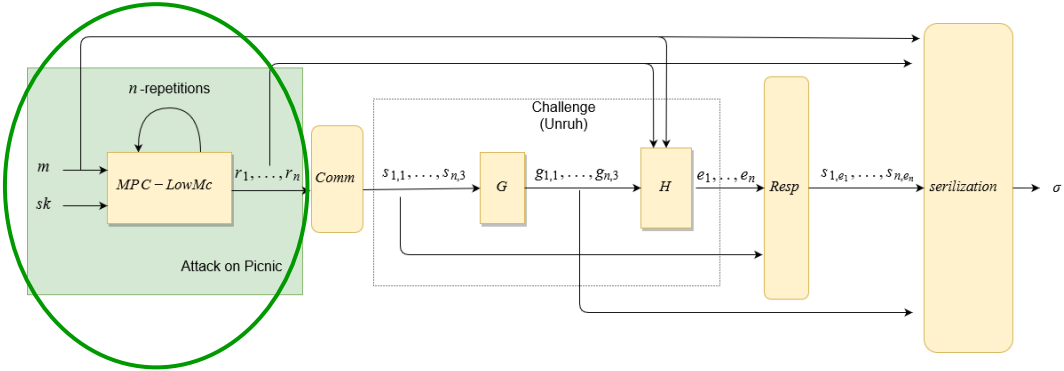
- Correctness: $y = \phi(x)$
- Revealing two branches will not leak any information.

An overview of Picnic Signature Scheme

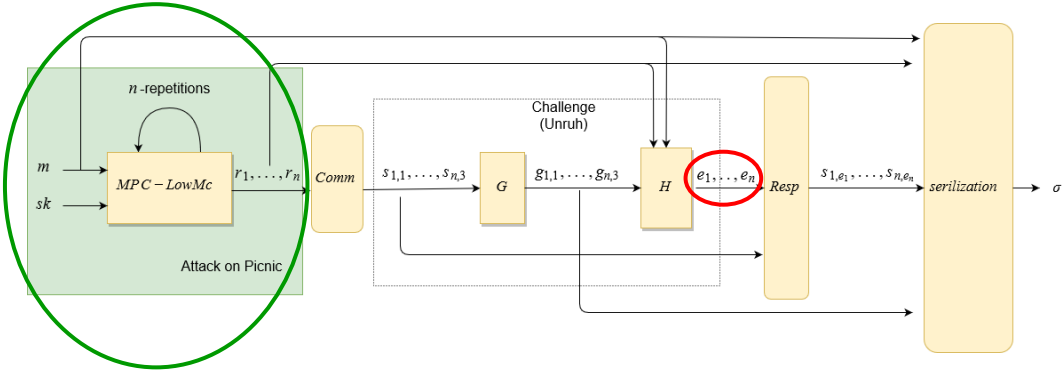
An overview of Picnic Signature Scheme



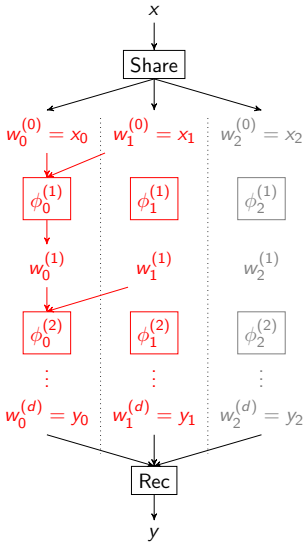
An overview of Picnic Signature Scheme



An overview of Picnic Signature Scheme

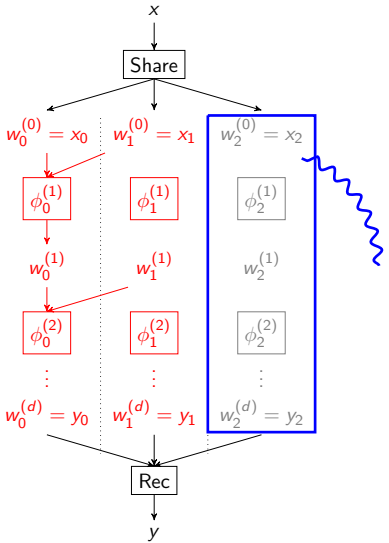


Probing MPC-in-the-head Protocol



Eve can access opened branches.

Probing MPC-in-the-head Protocol



Eve can access opened branches.

A single probe on unopened branch will leak information!

Attack on the Secret Sharing Process

- Two n bit keys (or key shares) for two players k_0 and k_1 are generated randomly.
- The key share for the last player k_2 is calculated as:

$$k_2 = k_s \oplus k_0 \oplus k_1.$$

Attack on the Secret Sharing Process

- Two n bit keys (or key shares) for two players k_0 and k_1 are generated randomly.
- The key share for the last player k_2 is calculated as:

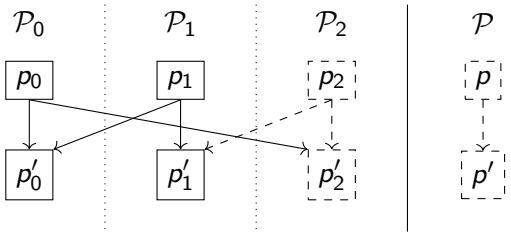
$$k_2 = k_s \oplus k_0 \oplus k_1.$$

For the challenge C_0:

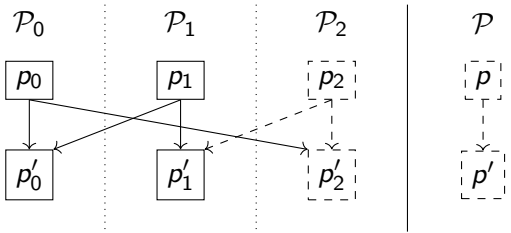
k_2 is the result of two chained xor-operations:

1. $R \leftarrow k_s \oplus k_0$ stored in a register R,
2. $k_2 \leftarrow R \oplus k_1$.

Attack on the Substitution Layer



Attack on the Substitution Layer



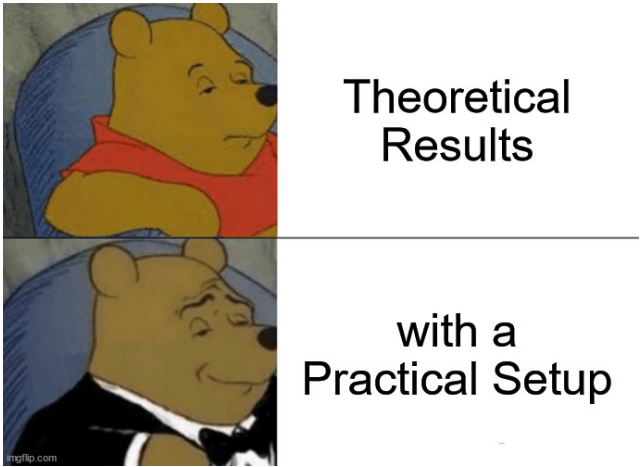
`SboxLayer` calculation for MPC-LowMC

Dashed boxes and arrows represent the values that are *not* opened during C_0

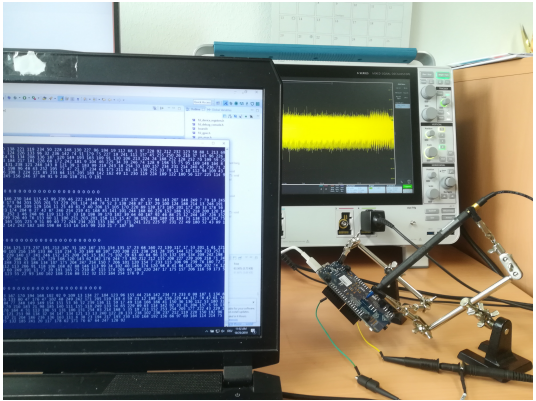
$$p = p_0 \oplus p_1 \oplus p_2 \text{ and } p' = p'_0 \oplus p'_1 \oplus p'_2$$

A Practical Measurement Setup

A Practical Measurement Setup



A Practical Measurement Setup

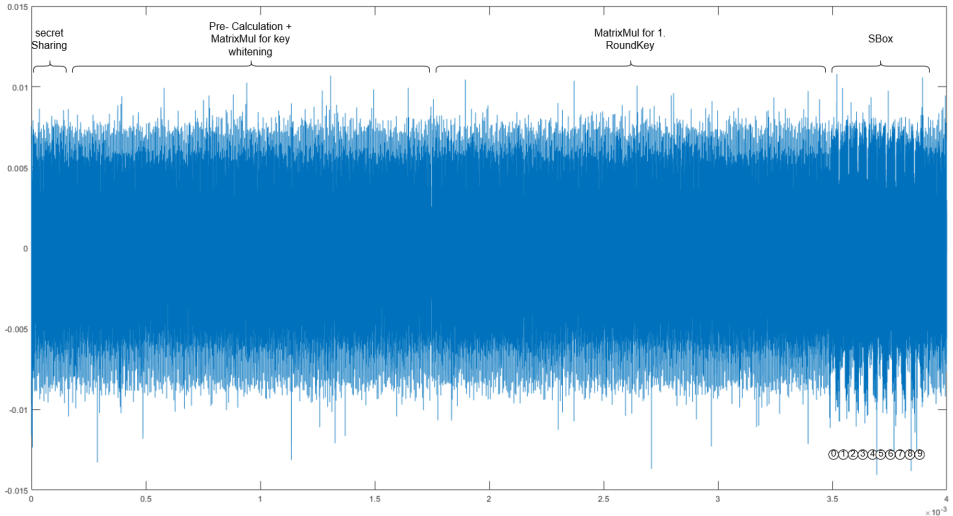


- Capture: Tektronix MSO 6 with 312.5 MHz sampling rate

A Practical Measurement Setup

- Capture: Tektronix MSO 6 with 312.5 MHz sampling rate
- Target device: SNXP Cortex-M4F MCU, operated at 120 MHz
- Source: EM emanations on a blocking cap (C37)

An Example Trace



First Step: Verifying the leakage

Test Vector Leakage Assessment (TVLA)

A pass-fail test to decide if an implementation has exploitable leakage

- fixed-vs-random (FvR): to detect all possible first-order leakage
- random-vs-random (RvR): to identify a specific exploitable leakage

```
---------------- Encryption -----------------------------
00000 00000000000000000000000000000000 -> 7DF76B0C1AB899B33E42F047B91B546F
00001 00000000000000000000000000000000 -> 7DF76B0C1AB899B33E42F047B91B546F
00002 94C3076F0433989CF3651E1C323E3F58 -> 6C76202524A3A9BD14524BC8A7749F5D
00003 00000000000000000000000000000000 -> 7DF76B0C1AB899B33E42F047B91B546F
00004 00000000000000000000000000000000 -> 7DF76B0C1AB899B33E42F047B91B546F
00005 3A3A3757CC71598FC3D6F38BCB16766A -> FB01C070BA4957A56A2DF6A0BFBBFD06
00006 65DDC4DB94B991A249EB219CC5946891 -> CF837BE15C720FEBFDA1754D0A9C9D2F
00007 94DC1372D1BC5DFBA43D08FF65863DFF -> 8E93841327CA4DF8045248E11DC71919
00008 D5286B83BACFFC763B1C0863564A9827 -> C26C0EA9C3576FEE2168CCD344CA3FFC
00009 00000000000000000000000000000000 -> 7DF76B0C1AB899B33E42F047B91B546F
00010 00000000000000000000000000000000 -> 7DF76B0C1AB899B33E42F047B91B546F
```

First Step: Verifying the leakage

Probing the opened share

$$a_2 = a \oplus a_0 \oplus a_1$$

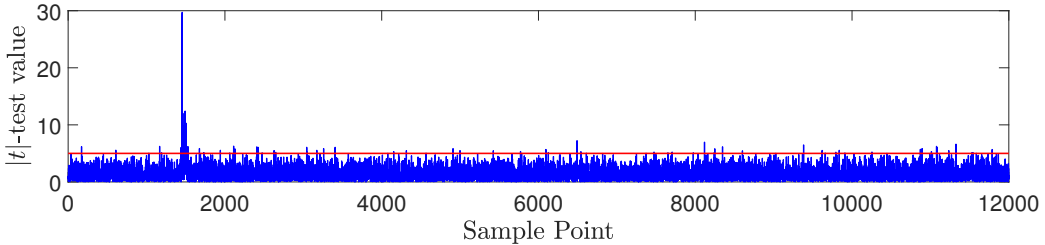
- Measurements from 10th Sbox calculation with 6000 traces.

First Step: Verifying the leakage

Probing the opened share

$$a_2 = a \oplus a_0 \oplus a_1$$

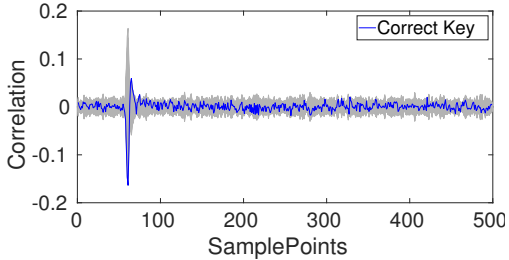
- Measurements from 10th Sbox calculation with 6000 traces.
- the $|t|$-value clearly exceeds 4.5.



Attack on the Secret Sharing Process

- DPA results shows a peak with 20,000 traces.

$$H_{k^*} = \mathrm{HW}(k_1 \oplus (k^* \oplus k_0)) \; \forall k^* \in \mathbb{F}_2^8$$

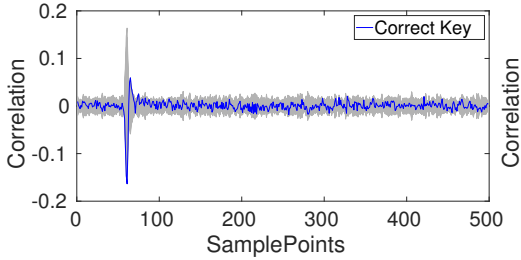


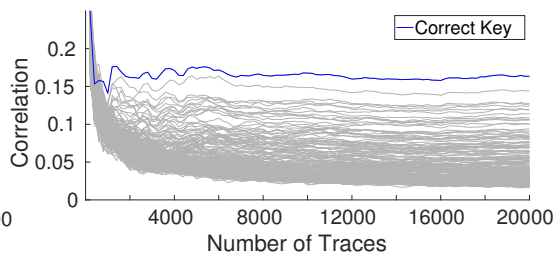
Attack on the Secret Sharing Process

- DPA results shows a peak with 20,000 traces.

$$H_{k^*} = \mathrm{HW}(k_1 \oplus (k^* \oplus k_0)) \; \forall k^* \in \mathbb{F}_2^8$$

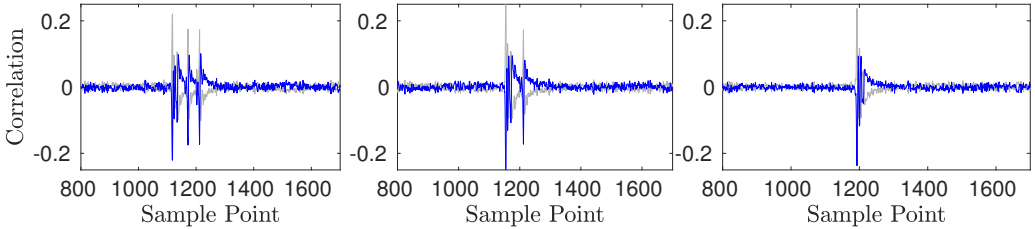
- The second figure shows that the correct key is distinguishable with 2000 traces.
- Every signature contains 219 repetitions $\rightarrow$ 30 signature





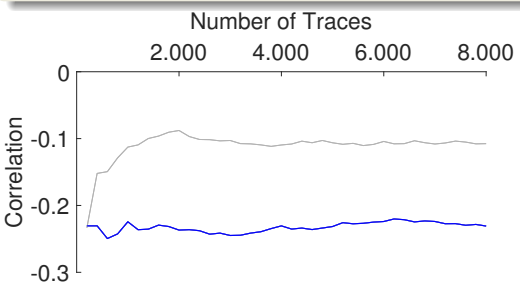
Attack on the Substitution Layer

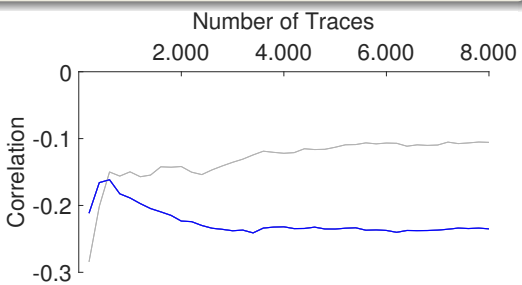
- DPA results shows a peak with 20,000 traces.
- The correct key (which has the highest-negative value) is distinguishable with 2,000 traces
- Every signature contains 219 repetitions $\rightarrow$ 30 signature



Attack on the Substitution Layer

- DPA results shows a peak with 20,000 traces.
- The correct key (which has the highest-negative value) is distinguishable with 2,000 traces
- Every signature contains 219 repetitions $\rightarrow$ 30 signature



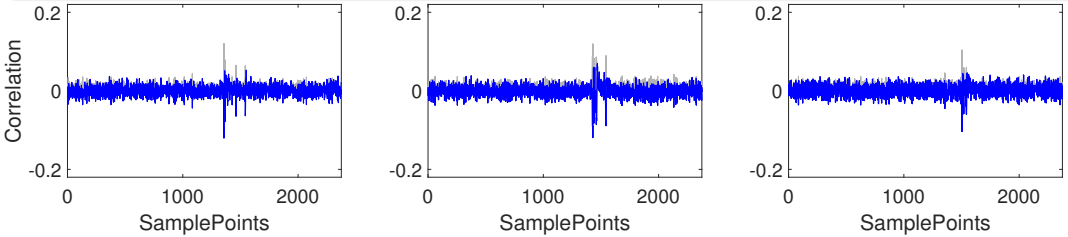


Attack on Deeper Rounds

- Due to the MPC-in-the-Head structure the values are opened for each round.

Attack on Deeper Rounds

- Due to the MPC-in-the-Head structure the values are opened for each round.
- This lead us to attacks on deeper rounds.



Attack on Deeper Rounds

- Due to the MPC-in-the-Head structure the values are opened for each round.
- This lead us to attacks on deeper rounds.
- Combine the key related information to solve the following system:

$$\mathcal{U}k_s = \mathcal{V}$$

  - $\mathcal{U}$ is the coefficient deduced from LowMC structure: $30r \times 128$ matrix
  - k_s is the secret key: 128×1 bit vector
  - $\mathcal{V}$ bits derived from DPA: $30r \times 1$ bit vector

Conclusion

Conclusion

Side-channel analysis on protocol level is a real threat.

Conclusion

Side-channel analysis on protocol level is a real threat.

MPC-in-the-Head paradigm does not necessarily provide probing security.

Conclusion

Side-channel analysis on protocol level is a real threat.

MPC-in-the-Head paradigm does not necessarily provide probing security.

Attacks on different stages of Picnic signature scheme leads to full key recovery.

Conclusion

Side-channel analysis on protocol level is a real threat.

MPC-in-the-Head paradigm does not necessarily provide probing security.

Attacks on different stages of Picnic signature scheme leads to full key recovery.

A novel algebraic key recovery to combine the attacks on different rounds.

Conclusion

Side-channel analysis on protocol level is a real threat.

MPC-in-the-Head paradigm does not necessarily provide probing security.

Attacks on different stages of Picnic signature scheme leads to full key recovery.

A novel algebraic key recovery to combine the attacks on different rounds.

Thank you! & Questions?
More details at `https://ia.cr/2020/267`