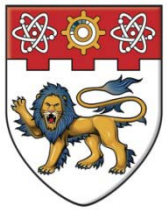


NANYANG TECHNOLOGICAL UNIVERSITY

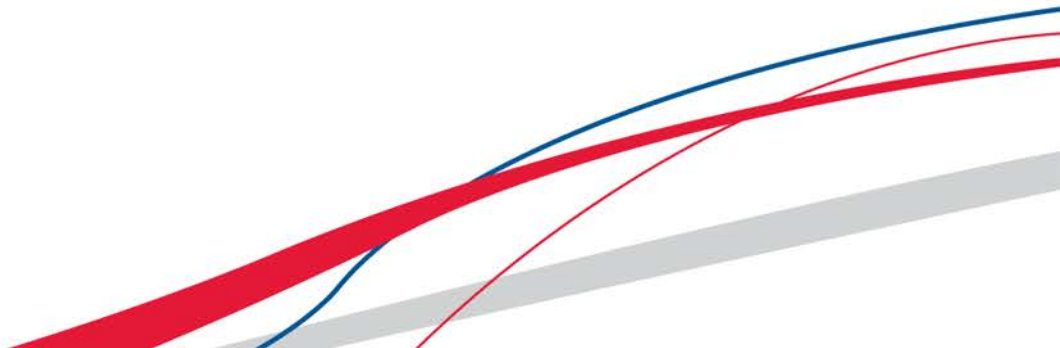
pace
Physical Analysis and Cryptographic Engineering

On the Security of RSM

Presenting 5 First- and Second Order Attacks

Sebastian Kutzner and Axel Y. Poschmann

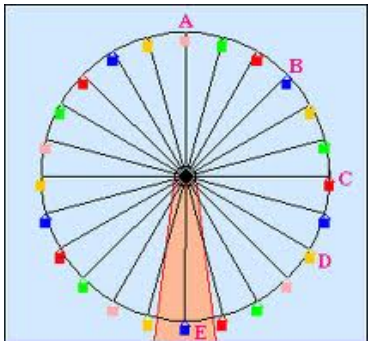
15 April, 2014



Agenda

- **Introduction to RSM**
- Index update Attack
- 1st order Correlation-Enhanced Collision Attack
- Univariate 2nd order CPA Attack
- Forced Collision Attack
- First-to-last-Round Collision Attack
- Conclusion

What is RSM?



- Introduced in 2012 by Nassar et al.
- Rotating Sboxes Masking
- Masking countermeasure for AES
- Efficient to implement in HW and SW
  - No time overhead
  - Reasonable size overhead
- Needs only 4 bit entropy/encryption
- Secure against 1st and 2nd order univariate attacks
- Implemented on a smart card for the DPA contest v4

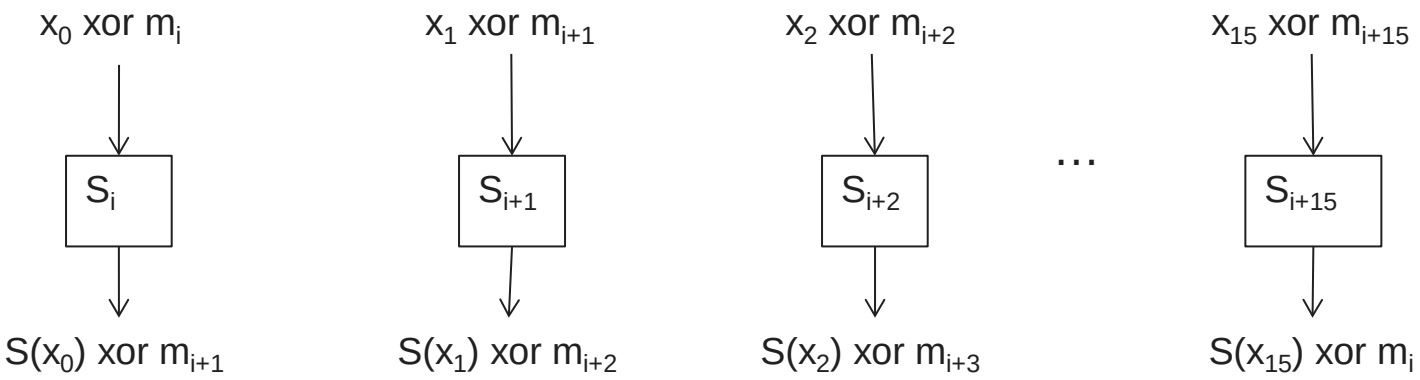
Theory

- 16 fixed and known masks with special properties:

[0x00, 0x0f, 0x36, 0x39, 0x53, 0x5c, 0x65, 0x6a, 0x95, 0x9a, 0xa3, 0xac, 0xc6, 0xc9, 0xf0, 0xff]

- 16 masked Sboxes $S_i(X)$ with the following property

$$S_i(X \text{ xor } m_i) = S(X) \text{ xor } m_{(i+1)\%16}$$

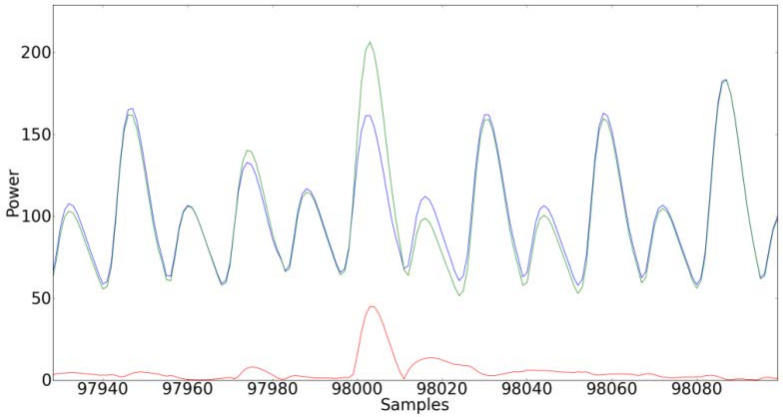


Agenda

- Introduction to RSM
- **Index update Attack**
- 1st order Correlation-Enhanced Collision Attack
- Univariate 2nd order CPA Attack
- Forced Collision Attack
- First-to-last-Round Collision Attack
- Conclusion

1st Attack – Exploit Index Update

- Attack index update
  - E.g. if (i+1)%16 = 0
  - → less power consumption while writing into register
  - → i = 15
  - → mask value = 0xff

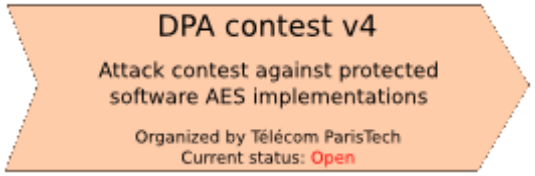


- All other masks are then uniquely determined

- → enables 1st order CPA with ~1,500 traces

DPA Contest v4

- Attack greatly improved by Zheng Kanghong
- → was first place in DPA contest v4 for non-profiled attacks until 10/03/14
- Only 78 traces needed to extract full key

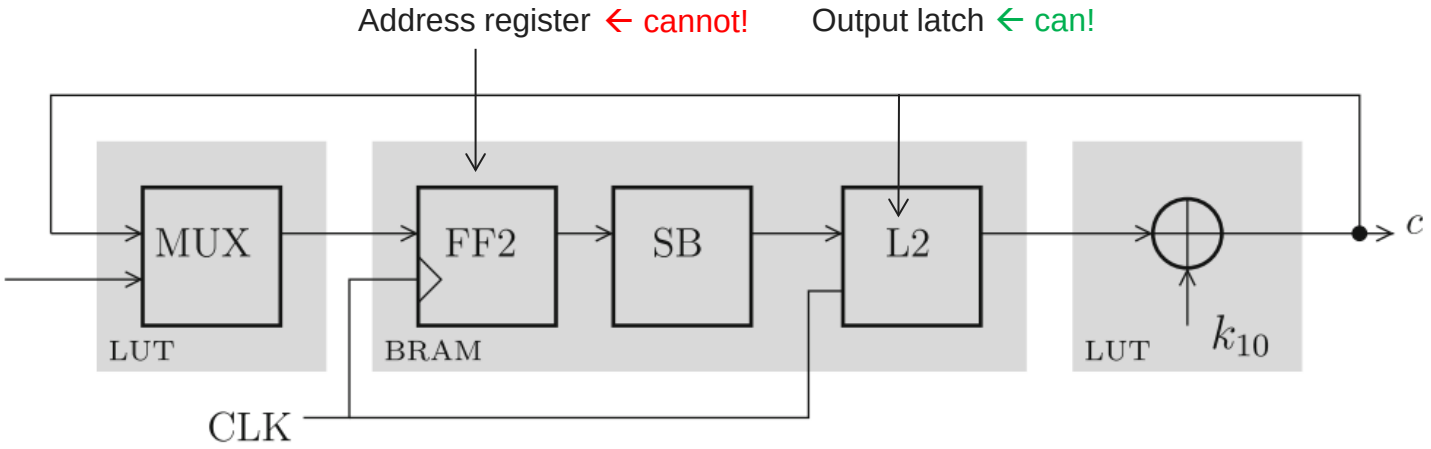


Agenda

- Introduction to RSM
- Index update Attack
- **1st order Correlation-Enhanced Collision Attack**
- Univariate 2nd order CPA Attack
- Forced Collision Attack
- First-to-last-Round Collision Attack
- Conclusion

Original Security Evaluation

- Only 150,000 measurements
- Verification of setup failed
- → Non-optimal attack model

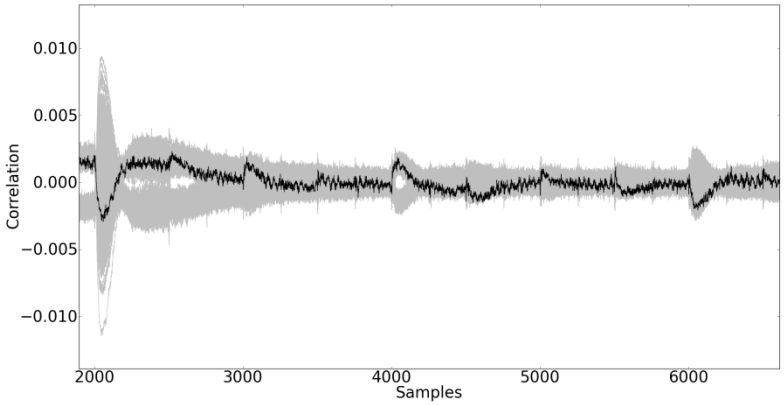


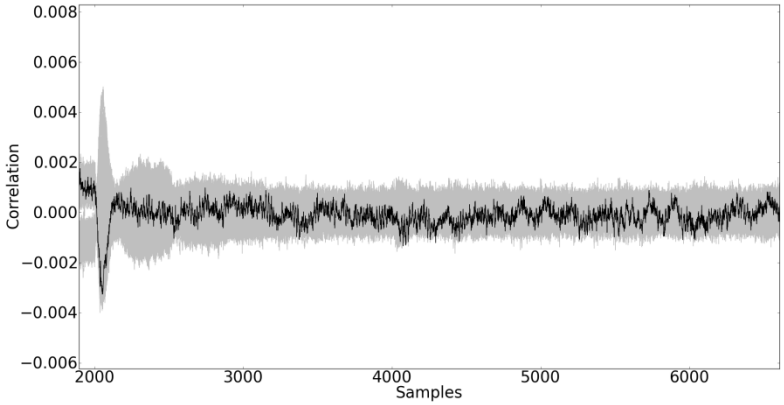
Implementation:
[Bhasin, S., He, W., Guilley, S., Danger, J.L.: Exploiting fpga block memories for protected cryptographic implementations]

Leakage model:
[Bhasin, S., Guilley, S., Heuser, A., Danger, J.L.: From cryptography to hardware: analyzing and protecting embedded Xilinx BRAM for cryptographic applications]

Refined Security Evaluation

- 10,000,000 measurements
- Corrected (verified) model
- Secure against 1st and 2nd order CPA (as expected)

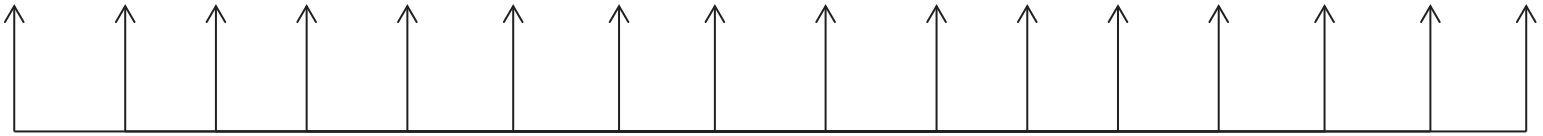




Mask Properties

- Found constant difference if the distance between two masks is 8

[0x00, 0x0f, 0x36, 0x39, 0x53, 0x5c, 0x65, 0x6a, 0x95, 0x9a, 0xa3, 0xac, 0xc6, 0xc9, 0xf0, 0xff]



$$\Delta = 0x95 - 0x95 - 0x95 - 0x95 - 0x95 - 0x95 - 0x95 - 0x95$$

$$m_i + m_{i+8} = 0x95$$

Mask Properties II

$$S_i(x_i \oplus k_i \oplus m_i) \oplus S_{i+8}(x_{i+8} \oplus k_{i+8} \oplus m_{i+8})$$

$$\Leftrightarrow S_{AES}(x_i \oplus k_i) \oplus m_{i+1} \oplus S_{AES}(x_{i+8} \oplus k_{i+8}) \oplus m_{i+8+1}$$

$$\Leftrightarrow S_{AES}(x_i \oplus k_i) \oplus S_{AES}(x_{i+8} \oplus k_{i+8}) \oplus 0x95$$

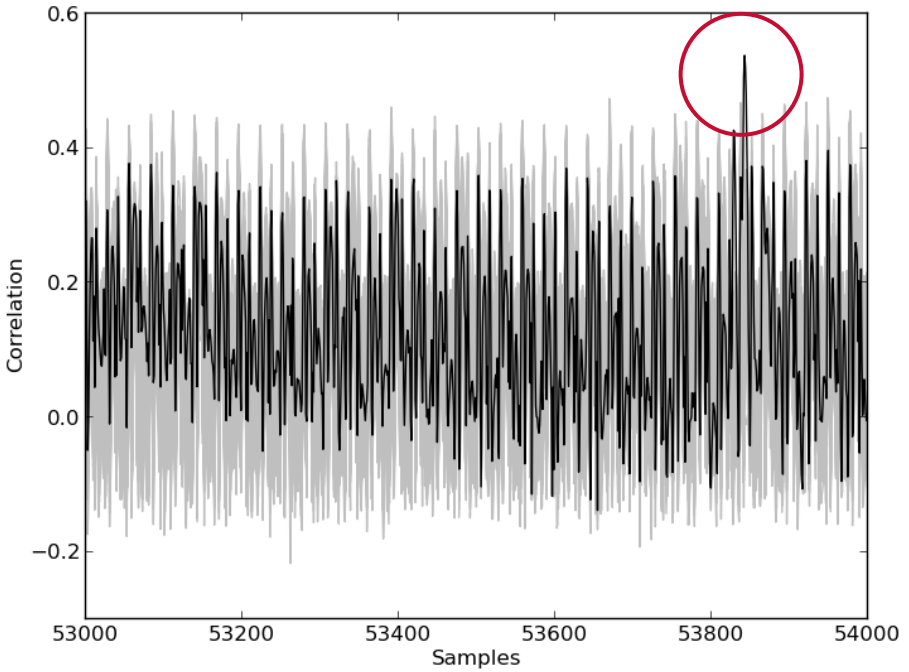
Collision

$$\Longrightarrow \quad S_i(x_i \oplus k_i \oplus m_i) = S_{i+8}(x_{i+8} \oplus k_{i+8} \oplus m_{i+8})$$

$$\Leftrightarrow \quad S_{AES}(x_i \oplus k_i) = S_{AES}(x_{i+8} \oplus k_{i+8}) \oplus 0x95$$

1st-order (Improved) Correlation-enhanced Collision Attack

- For every key hypothesis
  1. Find all traces where the two Sboxes “supposedly” collide
  2. Calculate the correlation between the two time instances S_i and S_{i+8}
  3. Highest correlation -> collision -> correct key



Agenda

- Introduction to RSM
- Index update Attack
- 1st order Correlation-Enhanced Collision Attack
- **Univariate 2nd order CPA Attack**
- Forced Collision Attack
- First-to-last-Round Collision Attack
- Conclusion

Univariate 2nd-order CPA

- Target Sbox output $S_i(x_i \oplus k_i \oplus m_i)$ ← cannot!
- Target $S_i(x_i \oplus k_i \oplus m_i) \oplus S_{i+8}(x_{i+8} \oplus k_{i+8} \oplus m_{i+8})$ ← can!
- Because:

$$\Leftrightarrow S_{AES}(x_i \oplus k_i) \oplus m_{i+1} \oplus S_{AES}(x_{i+8} \oplus k_{i+8}) \oplus m_{i+8+1}$$

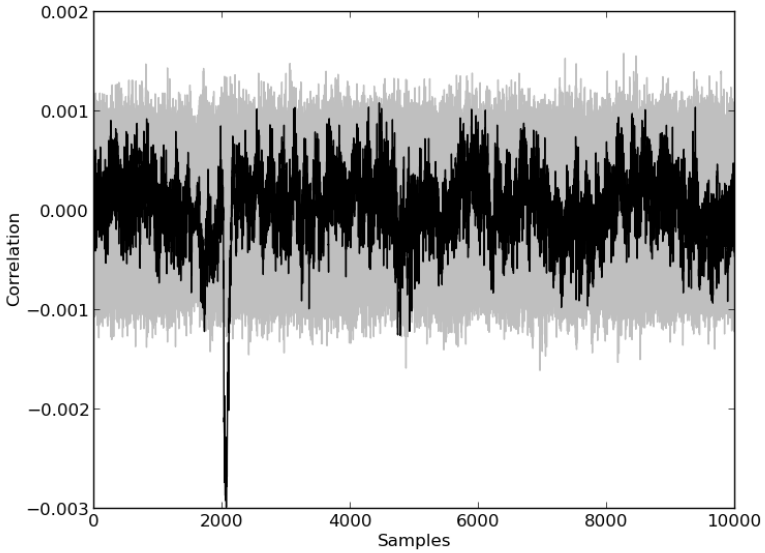
$$\Leftrightarrow S_{AES}(x_i \oplus k_i) \oplus S_{AES}(x_{i+8} \oplus k_{i+8}) \oplus 0x95$$

- But: power consumption follows

$$S_{AES}(x_i \oplus k_i) + S_{AES}(x_{i+8} \oplus k_{i+8}) \oplus 0x95$$

Univariate 2nd-order CPA

- Solution: use 2nd order moments, i.e., the variance
- 2^{16} key hypotheses
- ~1,500,000 traces required



Agenda

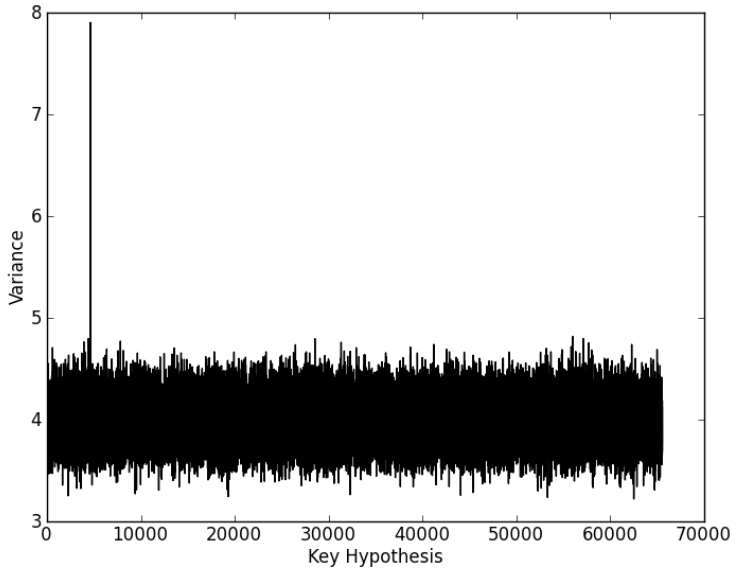
- Introduction to RSM
- Index update Attack
- 1st order Correlation-Enhanced Collision Attack
- Univariate 2nd order CPA Attack
- **Forced Collision Attack**
- First-to-last-Round Collision Attack
- Conclusion

Forced Collision Attack

- We have all the prerequisites to force collisions

$$S_{AES}(x_i \oplus k_i) = S_{AES}(x_{i+8} \oplus k_{i+8}) \oplus 0x95$$

- Is the power profile different if you force a collision in every measurement?
- → higher variance



Agenda

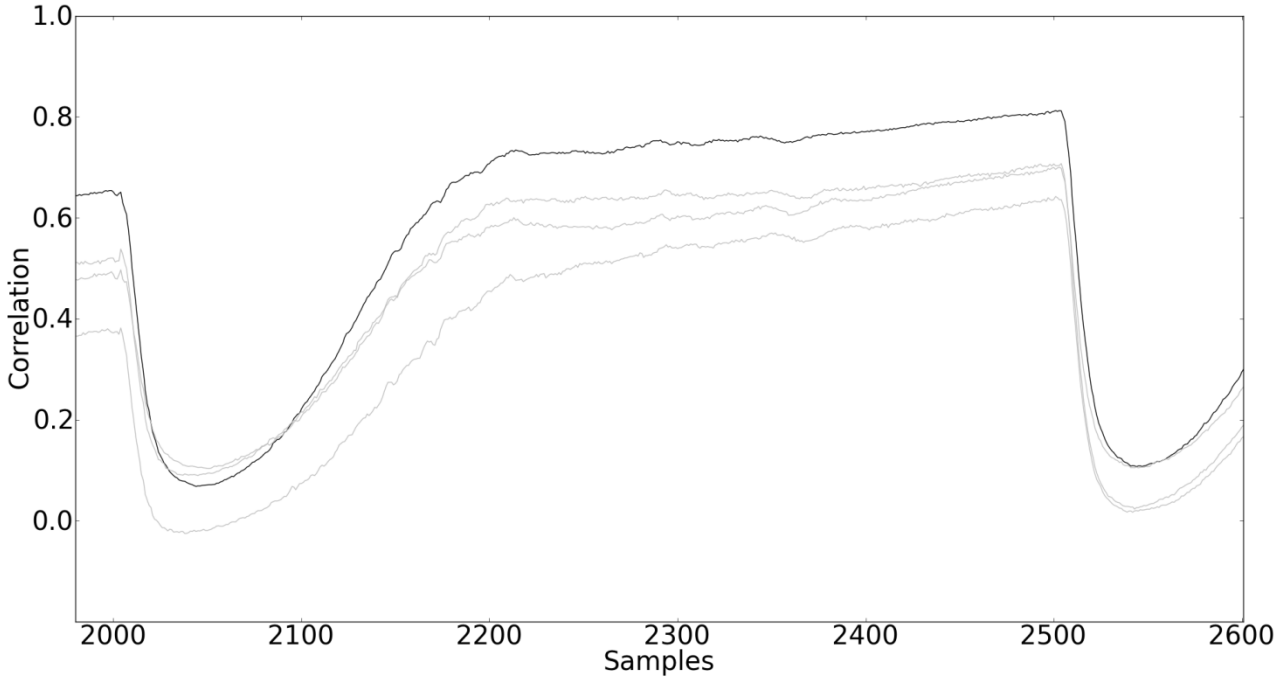
- Introduction to RSM
- Index update Attack
- 1st order Correlation-Enhanced Collision Attack
- Univariate 2nd order CPA Attack
- Forced Collision Attack
- **First-to-last-Round Collision Attack**
- Conclusion

First-to-last-round Collision

- Same masks are used in every round, but rotated
- Where will masks of first rounds be in the last round?
- → e.g. output mask for S_0 in 1st round is the same as for S_7 in the last round ((0 - 9) % 16 = 7)
- Check for collision:

$$S_{AES}(p_0 \oplus k_{0,0}) = SR^{-1}(c_7 \oplus k_{7,10})$$

First-to-last-round Collision



Agenda

- Introduction to RSM
- Index update Attack
- 1st order Correlation-Enhanced Collision Attack
- Univariate 2nd order CPA Attack
- Forced Collision Attack
- First-to-last-Round Collision Attack
- **Conclusion**

Conclusion

- Refined original security evaluation of RSM
- Found an exploitable structure in mask set
- Presented 5 new attacks on RSM, on software and hardware implementations
- Security analysis of RSM revised:
  - Second-order attacks possible
  - First-order attacks possible

Thank you!