RUB

RUHR-UNIVERSITÄT BOCHUM

Side-Channel Security Analysis of Ultra-Low-Power FRAM-based MCUs

14. April 2015

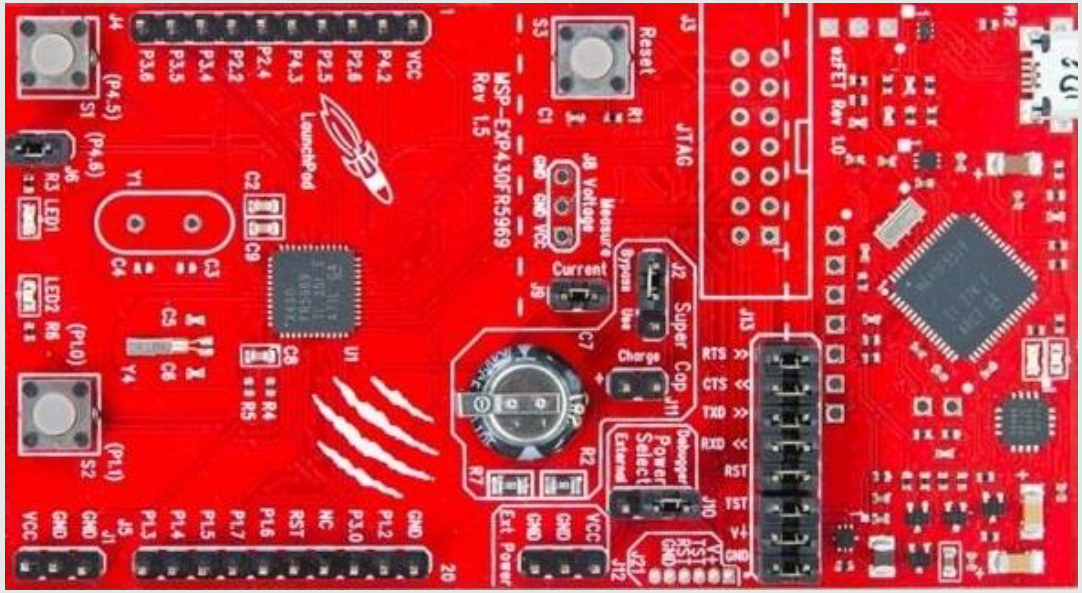
Amir Moradi and Gesine Hinterwälder

Ruhr-Universität Bochum

hgi Horst Görtz Institute for IT-Security

Story?

- MSP-EXP430FR5969 (kit)
- MSP430FR5969 (MCU)
  - FRAM
  - Ultra-Low Power
  - AES (hardware)



Story? (FRAM)

- non-volatile like flash
- much faster than flash (@ write) “125 ns”
- much less power than flash (@ write) “82 µA/MHz”
- super high write cycles “10^{15}”

- destructive (each read is followed by a write)
  - read speed limited to write speed
  - currently @ 8MHz
  - small cache for higher speeds (16MHzs)

Story? (Low-Power)

WHITE PAPER

Jacob Borgeson ,
MSP430 product marketing engineer
Texas Instruments

TEXAS INSTRUMENTS

Introducing advanced security to low-power applications with FRAM-based MCUs

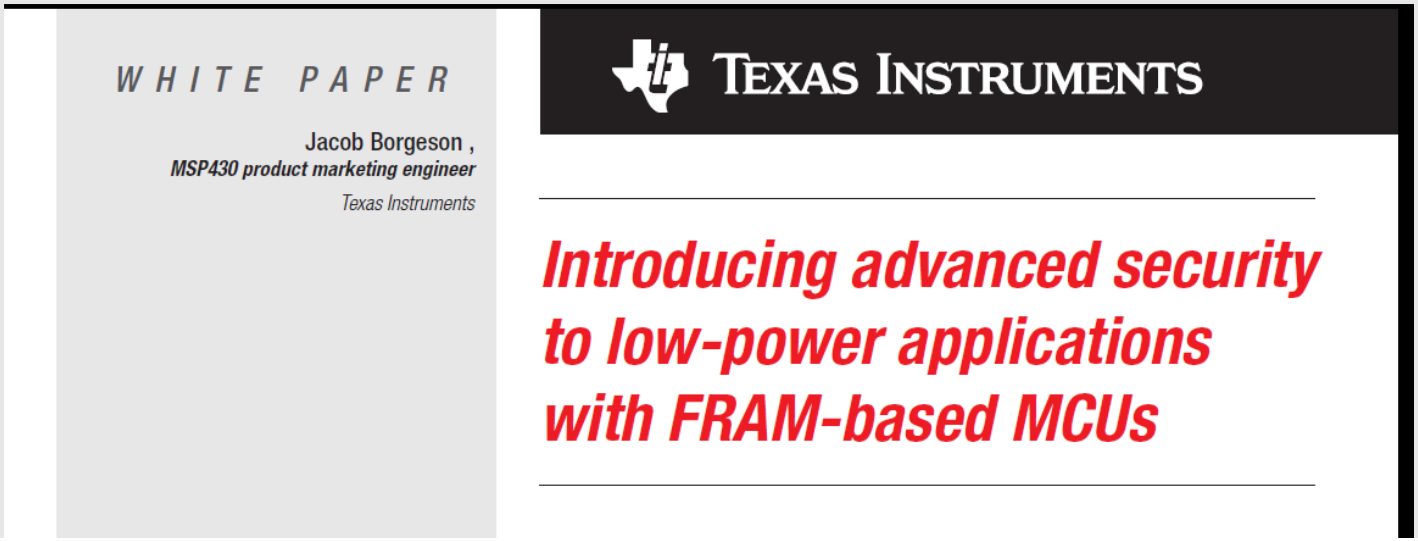
Introduction

Security is becoming increasingly important in a wide range of applications including smart phone accessories, smart metering, personal health monitoring, remote controls and access systems. According to a recent study conducted and published by ECN, the market for secure applications is expected to grow by 45% CAGR over the next five years[1].

While security of data and operations has always been a consideration for several of these applications, the rising financial risks

Consider a mobile credit card payment system that enables a merchant to process credit cards using a dongle connected to a mobile phone. Being able to compromise one of these devices would enable unscrupulous merchants to record confidential customer information for later use in fraudulent transactions. Alternatively, the ability to alter readings from electricity meters would allow consumers and businesses to substantially reduce their utility bills while shifting the costs to utilities and other customers. In fact, one reason why meters are moving from electromechanical systems to semiconductor-based "smart meters" is that the electromechanical portion can be easily tricked with a few magnets.

Story? (Low-Power)



WHITE PAPER

Jacob Borgeson ,
MSP430 product marketing engineer
Texas Instruments

TEXAS INSTRUMENTS

Introducing advanced security to low-power applications with FRAM-based MCUs

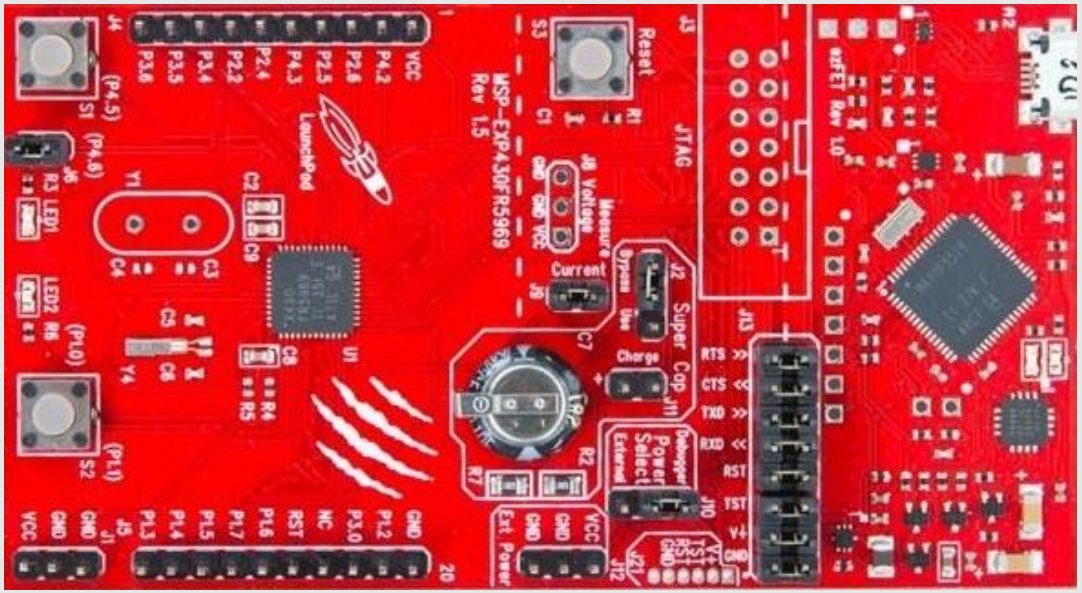
- **Power analysis:** Spectral Power Analysis (SPA) and Dynamic Power Analysis (DPA) are specialized techniques where the electromagnetic emissions or power usage of an MCU is measured to create a profile that can be used to determine what the MCU is doing internally. EEPROM and Flash require a charge pump operating at 10 to 14 V, which makes them relatively easy to detect. The extremely fast read and write speed of FRAM (less than 50 ns and 200 ns respectively), as well as its lower operating voltage (1.5 V) make it much more difficult to successfully mount an SPA- or DPA-based attack against.

Story? (AES)

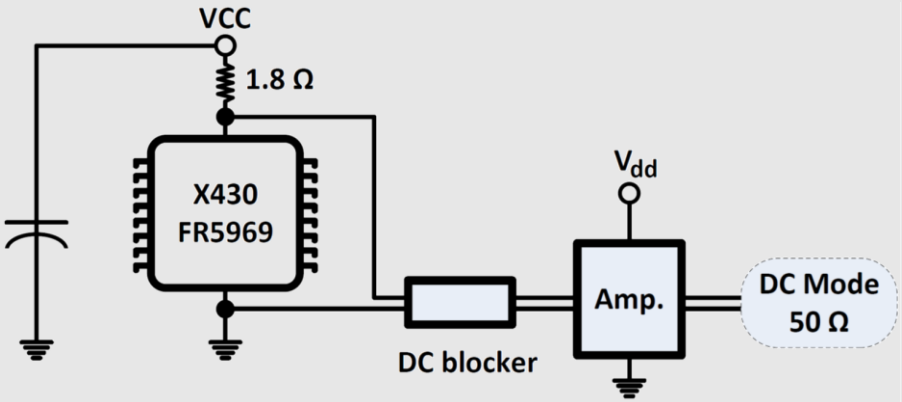
- Supporting 128, 192, 256 key sizes
- Supporting ECB, CBC, OFB, CFB
- Supporting pre-computed and on-the-fly KeySchedule
- not super fast

Key length	Encryption (clock cycles)	Decryption (clock cycles)
128 bits	168	168
192 bits	204	206
256 bits	234	234

Setup


MSP-EXP430FR5969
Rev 1.5
LaunchPad
Reset
JTAG
Super Cap
Charge
Current
Power Select
Ext Power
RTS
CTS
TXD
RXD
RST
TST

Setup

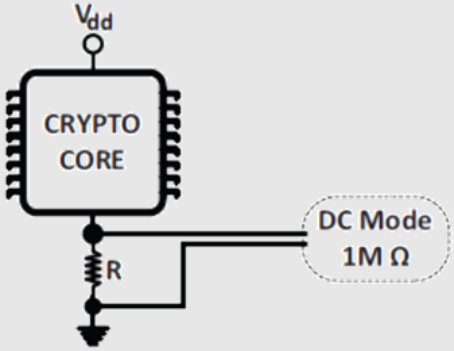

VCC
1.8 Ω
X430
FR5969
V_{dd}
Amp.
DC Mode
50 Ω
DC blocker

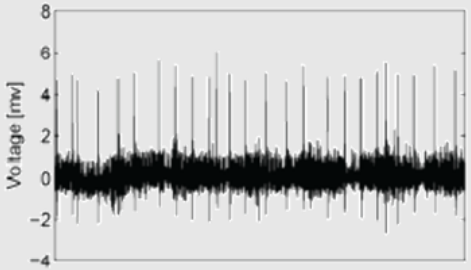

MCL
15542
BLK-89-S+


REMOVED
Mini-Circuits®
AMPLIFIER
ZFL-1000LN+
IN
0.1-1000 MHz
OUT
DATA: www.minicircuits.com/model
S F500701310
GND +15V

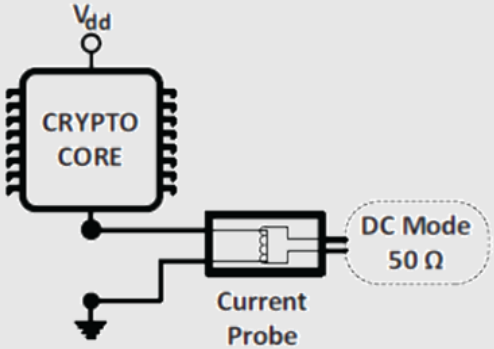

LeCroy

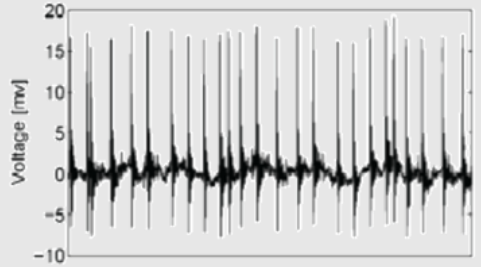
Setup matters?



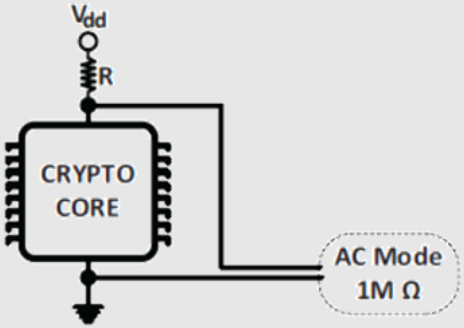


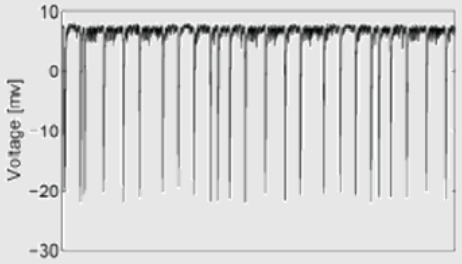
DC Mode



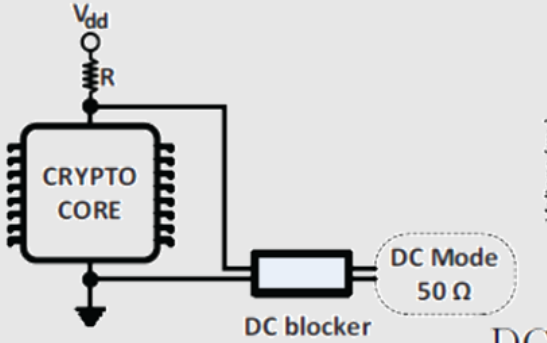


Current Probe

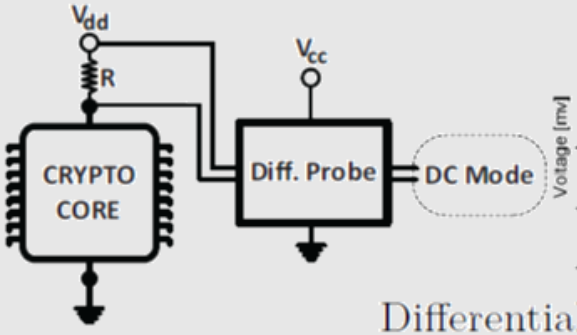


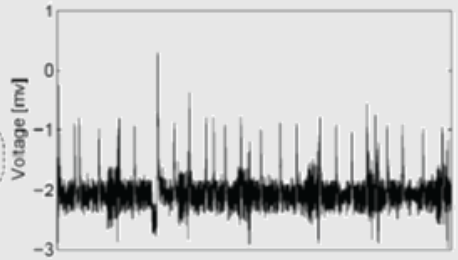


AC Mode

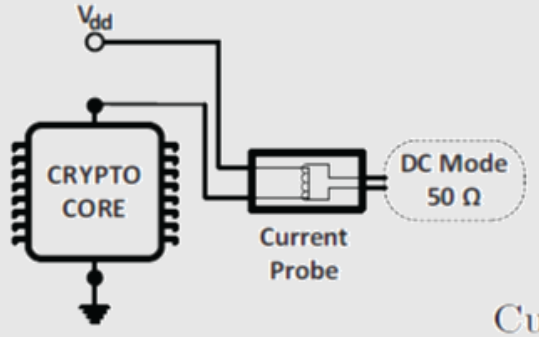


DC Mode with DC blocker





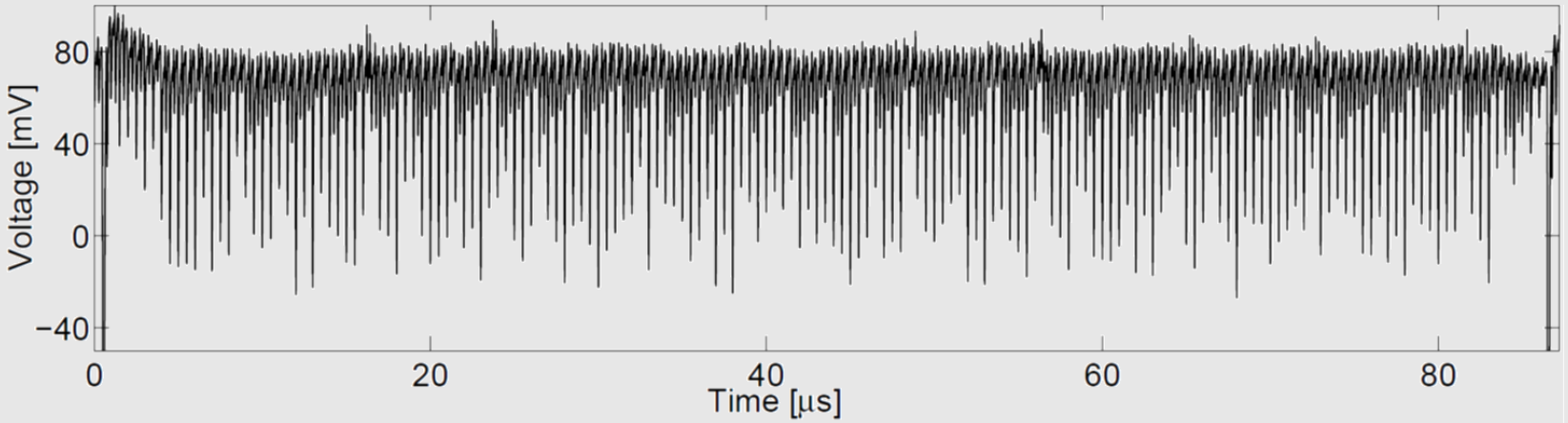
Differential Probe

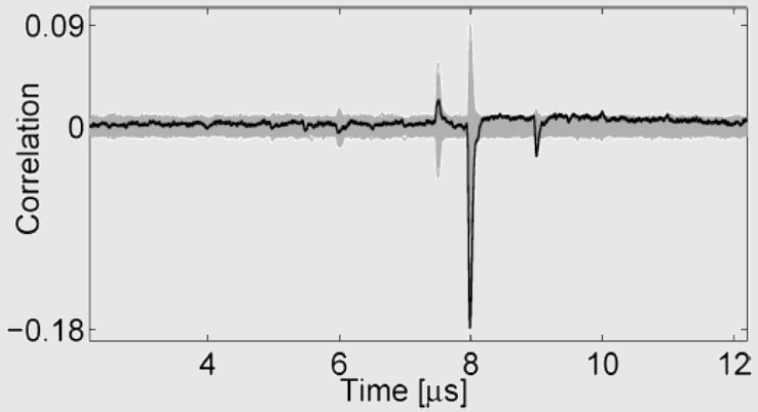


Current Probe

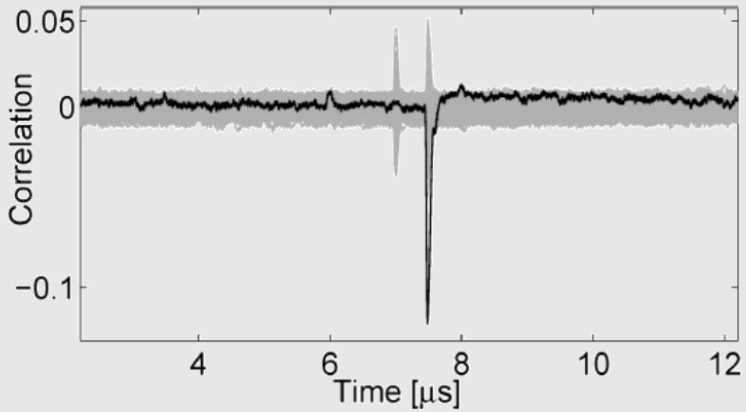
AES (hardware)

- AES-128 encryption (really low power)





model: an Sbox output bit



model: a bit of Sbox input XOR output

AES (software)

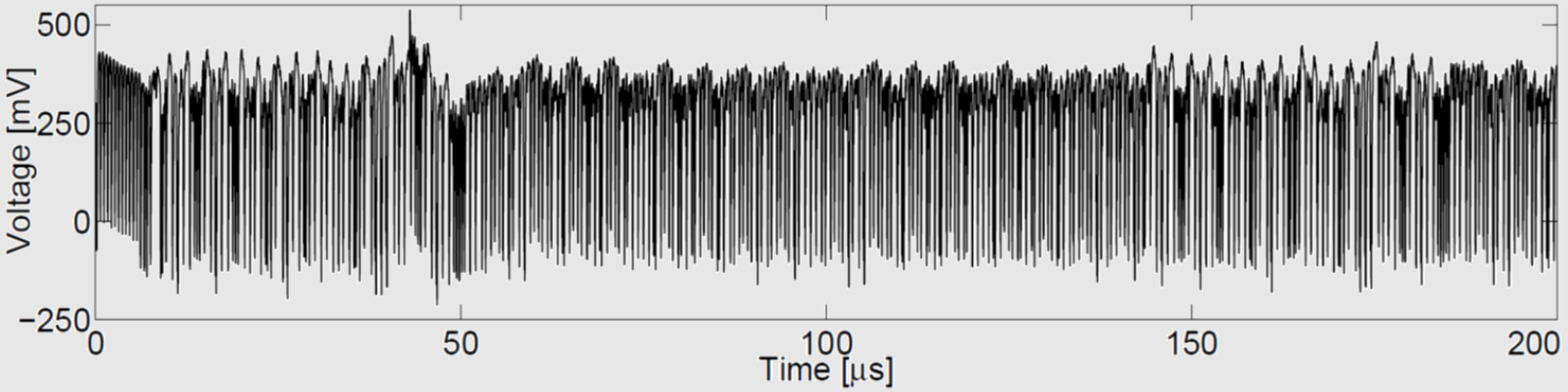
- taken from http://www.ti.com/tool/AES-128
- @ first glance, variable timing -> MixColumns

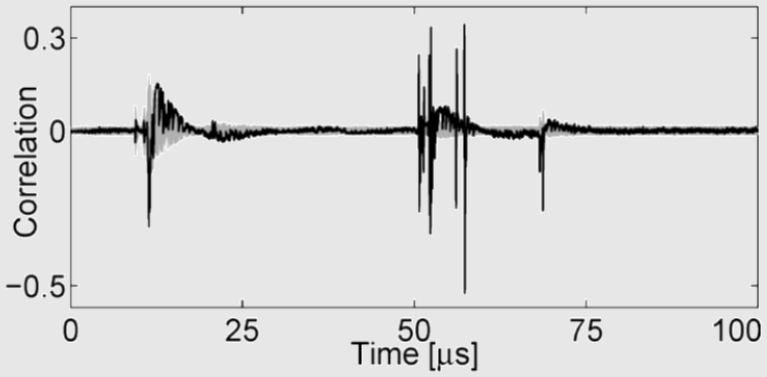
```
unsigned char galois_mul2 ( unsigned char value )
{       if (value > >7)   {
                return (( value << 1) ^ 0 x1b);  } else
                return ( value << 1) ;  }
```

- Conditional branch!
  - vulnerable to state-of-the-art timing attack
  - vulnerable to SPA

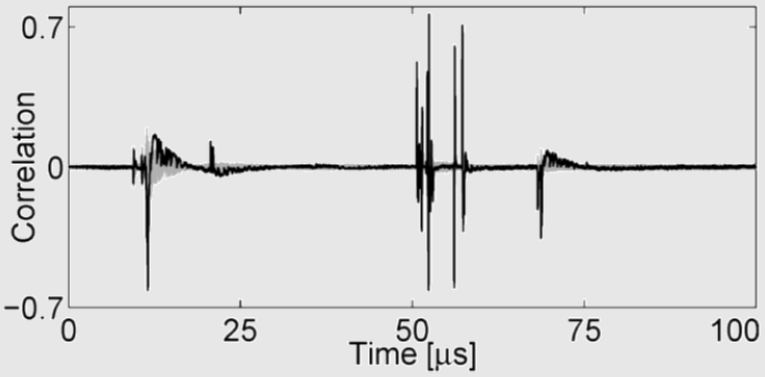
AES (software) @ 8MHz

- Much more power consuming than the hardware module





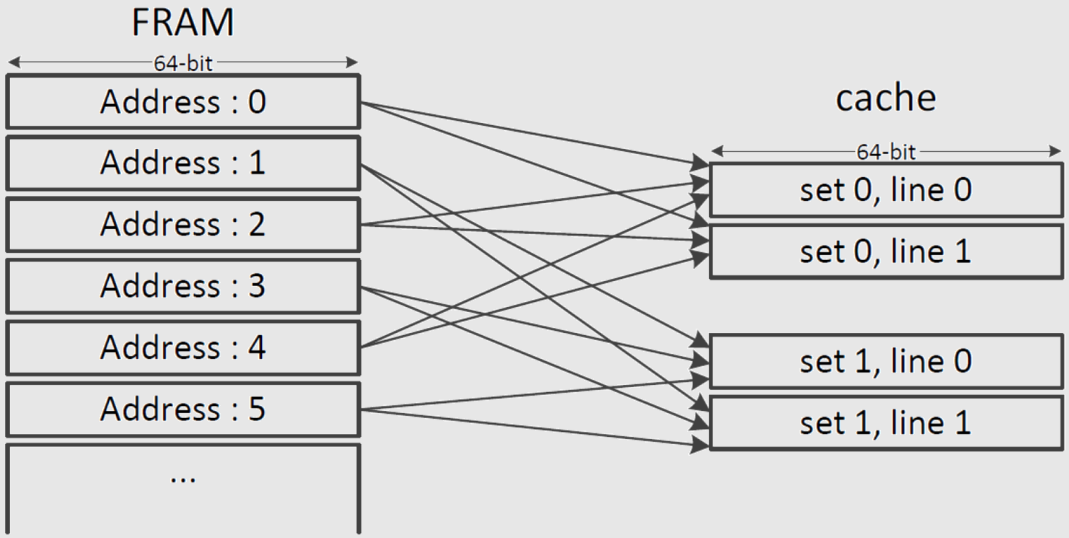
model: an Sbox output bit



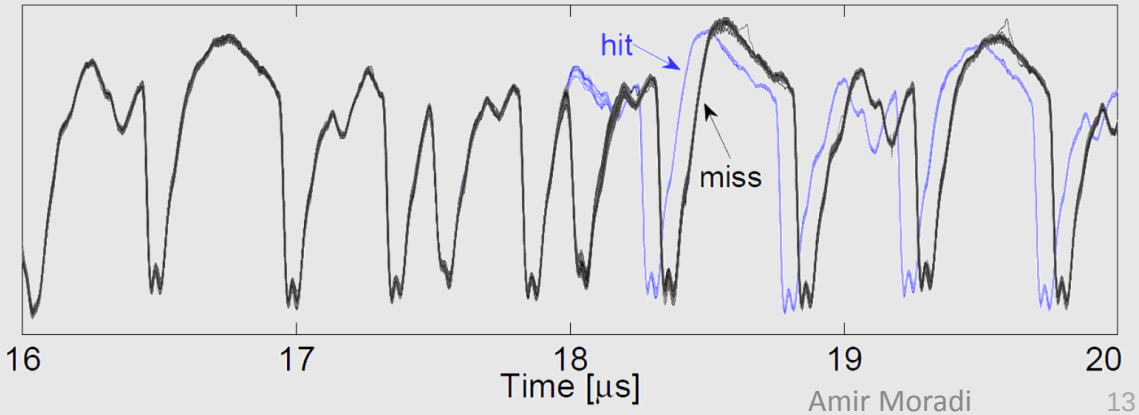
model: HW of an Sbox output

Cache / AES (software) @ 16MHz

- two-way set-associative
- pretty small
- shared
  - both program and data
- opens new doors for SCA
  - trace-driven cache attacks
  - may face many challenges due to its shared fashion



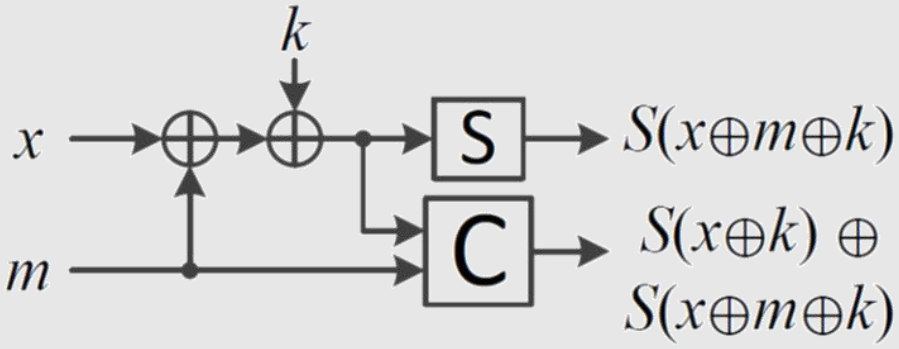
- SubBytes @ 16MHz

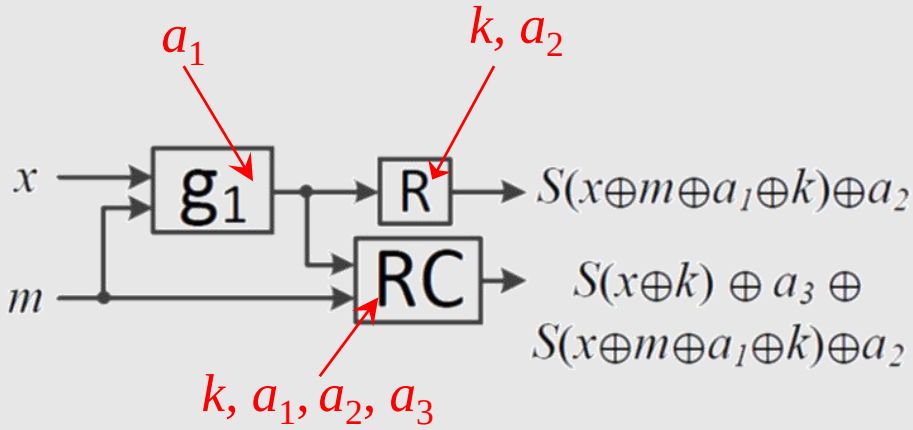


Internal Architecture

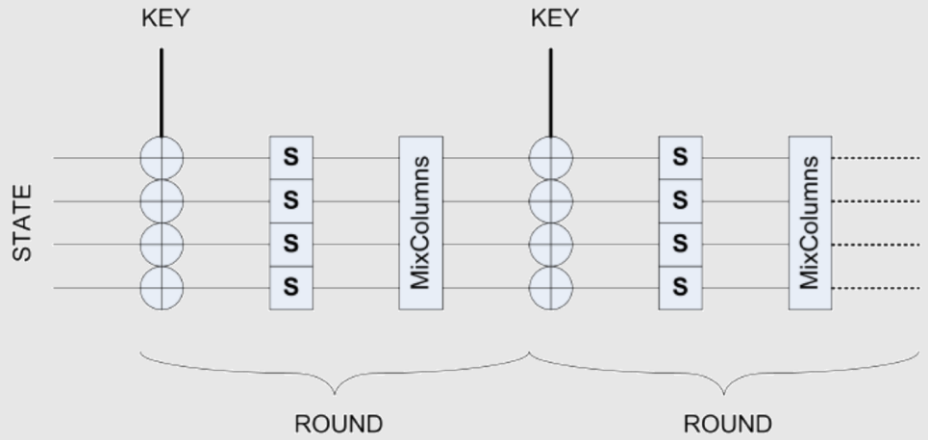
- mainly unknown to the end users
- pipelined CPU architecture with ??? stages
- usually such unknown architectures cause masked implementations to be still vulnerable

- Case study: S. Kerckhof, FX. Standaert, and E. Peeters @ CARDIS 2013 "From New Technologies to New Solutions - Exploiting FRAM Memories to Enhance Physical Security"

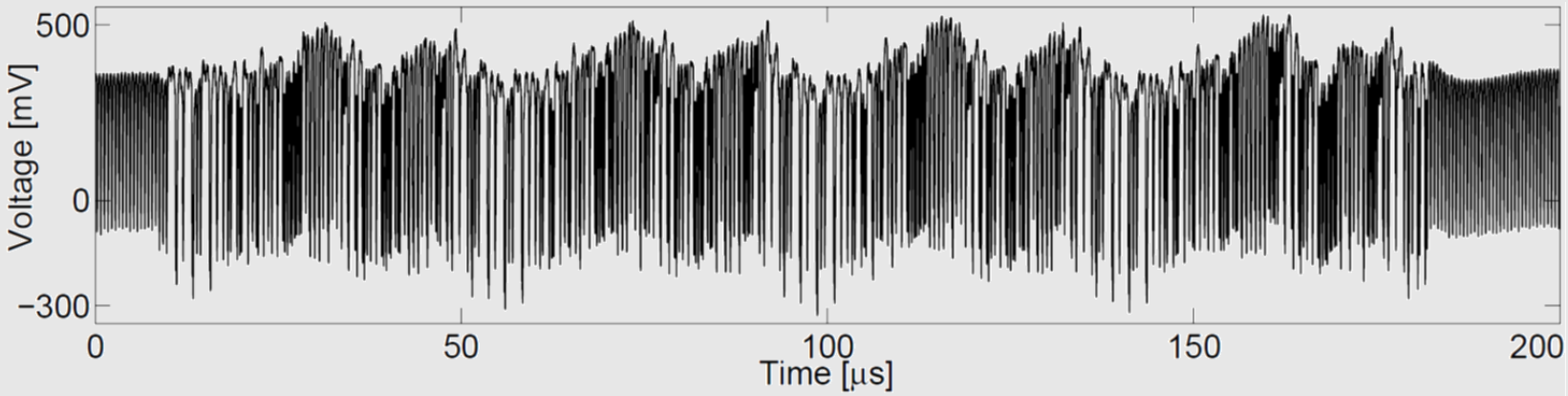




Masked Reduced LED @ 8MHz

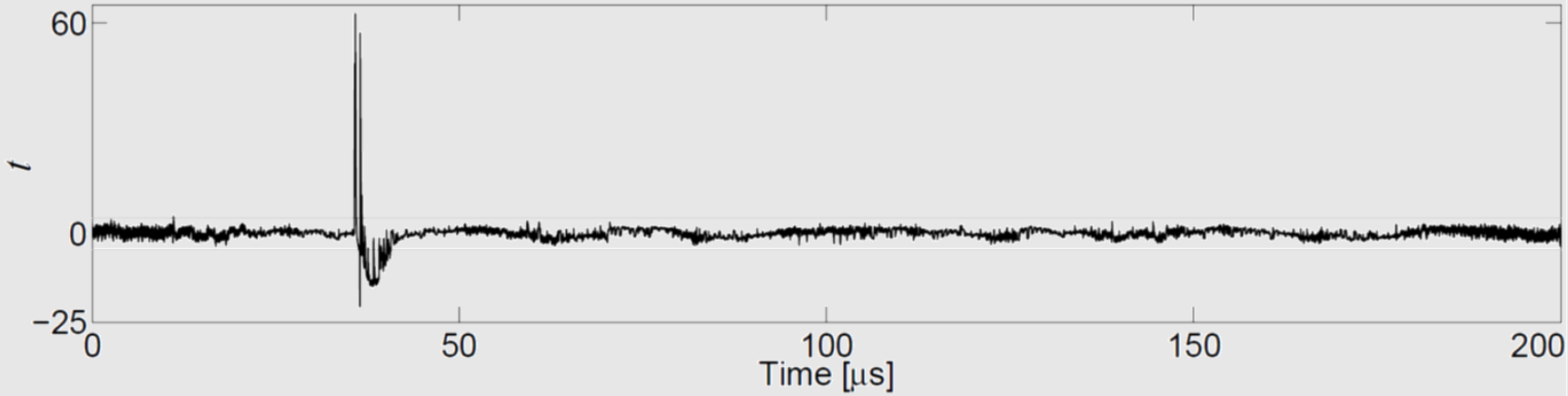


- 16-bit state and 4 rounds
- measurements excluding tables' pre-computation



Masked Reduced LED @ 8MHz

- non-specific (fixed vs. random) 1st-order *t*-test




```
mov     #STATE , pointer
rlam    #4, st0
add     st1 , st0
mov.b   st0 , 0( pointer )
rlam    #4, st2
add     st3 , st2
mov.b   st2 , 1( pointer )
```

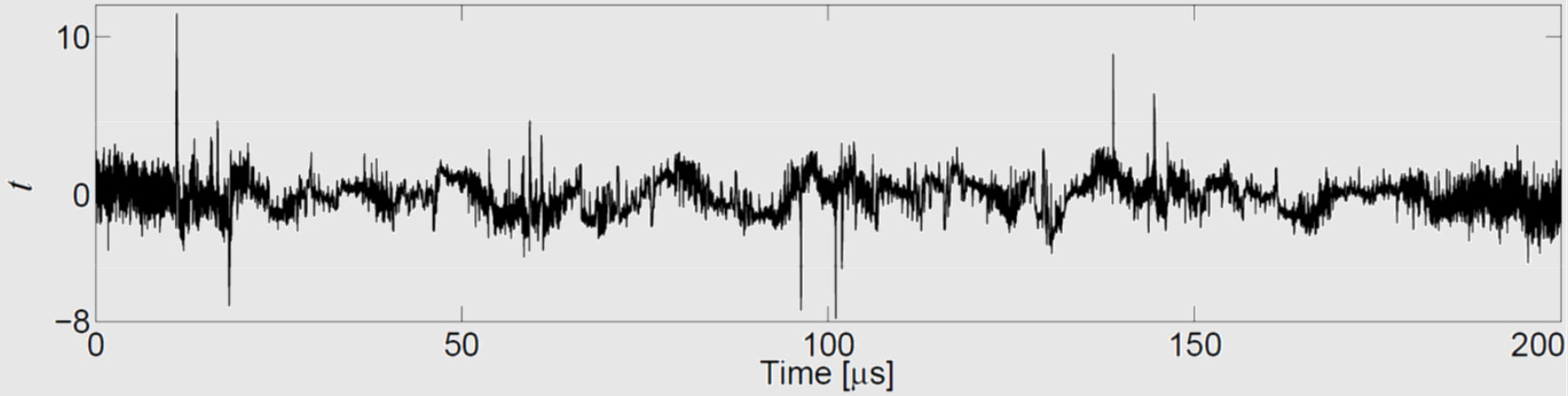
0(pointer) and 1(pointer) have been filled before by the unmasked plaintext

writing random data into a location leaks also about the previously stored value

Masked Reduced LED @ 8MHz

- These two memory locations cleared before being measured

```
mov     #STATE , pointer
mov.b   #0x00 ,0( pointer )
mov.b   #0x00 ,1( pointer )
```



- still 1st-order leakage

Masked Reduced LED @ 8MHz

- intensive investigations by inserting several nop instructions between probable leaky instructions
- finally, (masked) table look-ups
  - "reading from the tables stored in FRAM"

```
mov.b     @pointer , m0
```

- several attempts to avoid the leakage
  - e.g., by clearing the target register m0 beforehand
  - no success…

Sum up

- state-of-the-art attacks on unprotected device
  - expected results
- difficulties on measurements due to the low-power design
  - a suitable method to measure
- AES hardware accelerator, attackable but not easily
- software implementations highly vulnerable
- cache may become a leakage source
- unknown internal architecture may turn a masked implementation into a vulnerable design

- This work just gives an overview about the possible leakage sources when such a platform is being used in security-critical applications.

Thanks!
any questions?

amir.moradi@rub.de

Embedded Security Group, Ruhr-Universität Bochum, Germany