Recovering Keys from Secure EEPROM Memories

Josep Balasch, Lejla Batina, Benedikt Gierlichs,
Bart Jacobs, Ingrid Verbauwhede, and Roel Verdult

K.U. Leuven, Belgium & R.U. Nijmegen, The Netherlands

CHES 2011 Rump Session

Nara, Japan, 30 September 2011

The product: secure EEPROM

- Secure Memories with Authentication
  - EEPROM + Access Control Logic + Crypto Unit
- Mutual Authentication Protocol
  - Grants access to protected memory zones
  - Challenge-Response Protocol
  - Proprietary stream cipher and protocol (reverse engineered, analyzed and broken earlier)
- Authentication Attempts Counter
  - Lock chip after 4 invalid authentication attempts
- Applications (commercial, military)
  - Secure storage (e.g. cryptographic keys, biometric data)
  - Electronic payment systems

The product: security

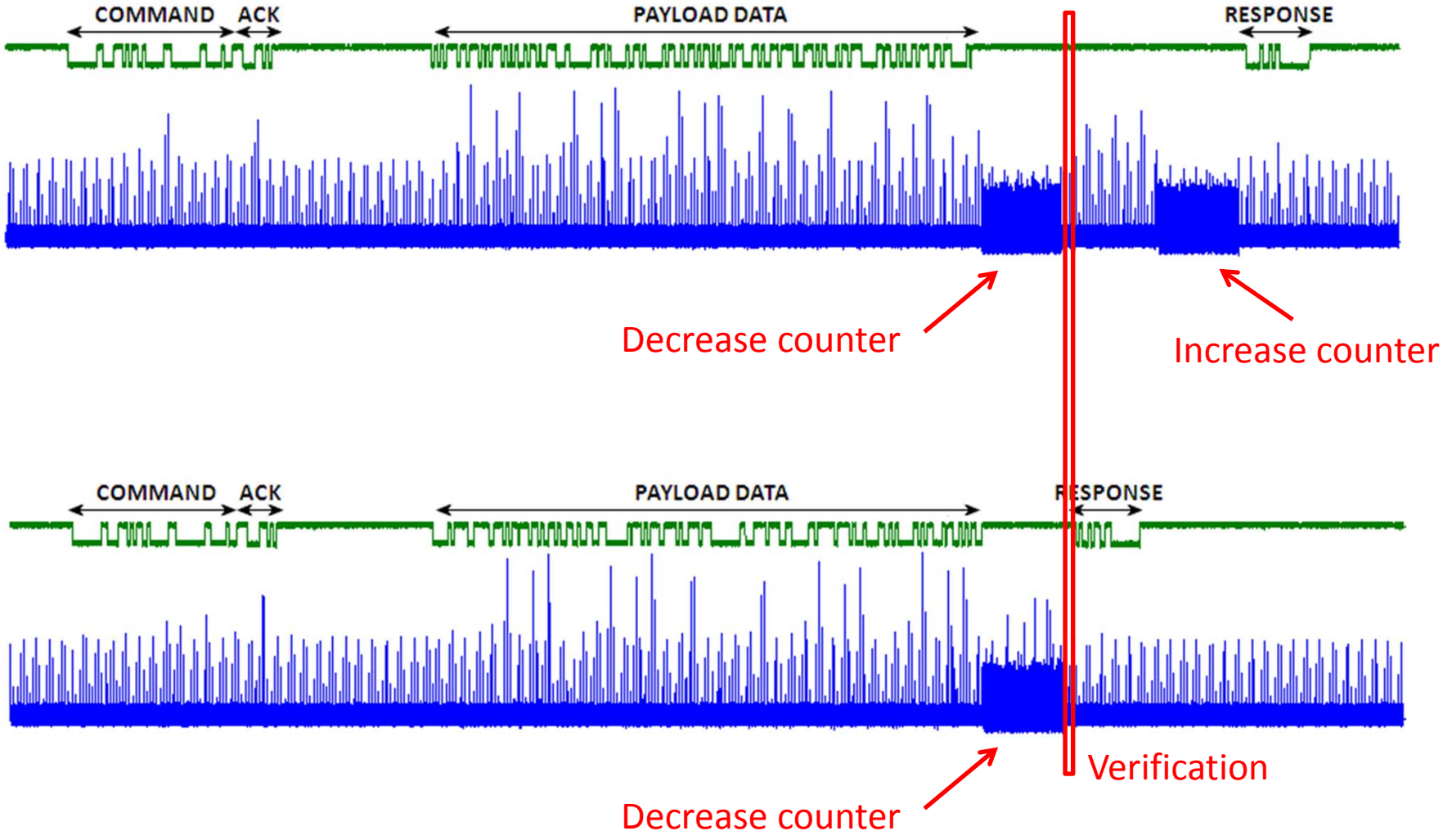
- *"* Tamper proof, metal shield layers, encrypted internal buses, defenses against timing and power supply attacks*"*

- *"Secure place for storage of sensitive information"*
- *"Truly secure means of preventing counterfeiting and piracy"*
- *"Can secure data against all the most sophisticated attacks […], including physical attacks"*
- *"[…] guarantee these values [authentication keys] can never be read"*
- *"is designed to keep contents secure, whether operating in a system or removed from the board and sitting in the hacker's lab"*

(all quotes from publicly available documents)

Analyzing power traces

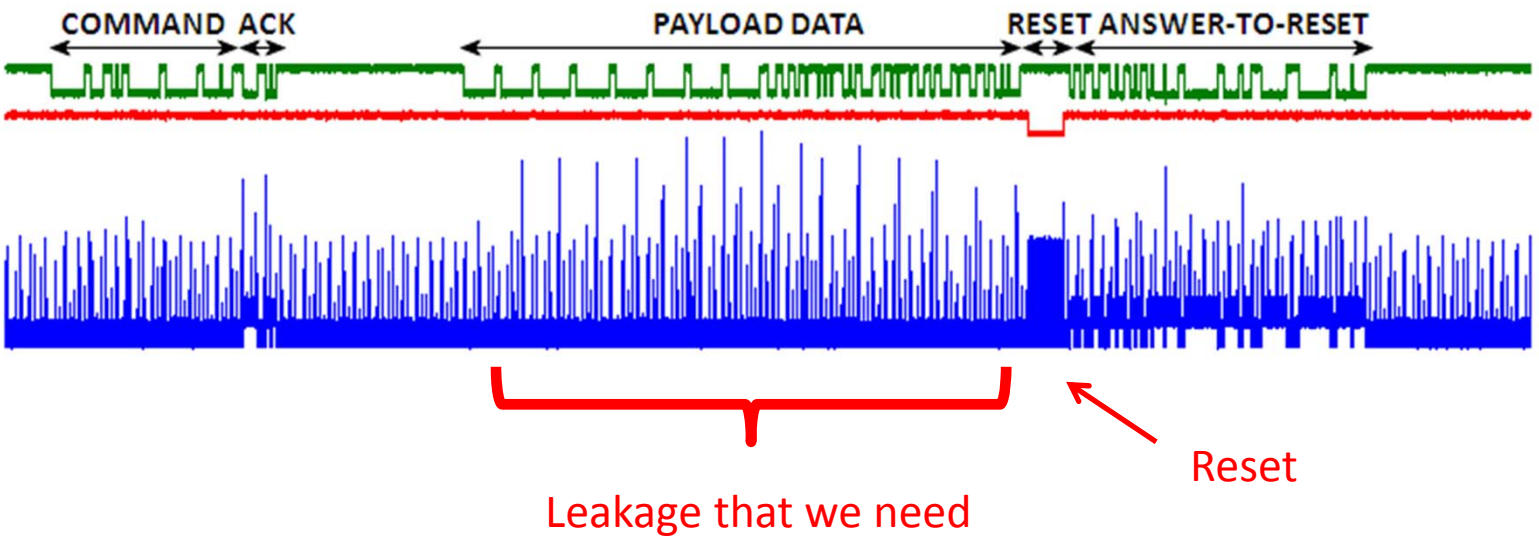
- Mutual Authentication Protocol



Power analysis?

- No countermeasures documented
- Perhaps not needed? Authentication Attempts Counters limit to 3 invalid attempts = 3 traces
- Templates or other fancy analysis
- What else?

Overcoming Authentication Attempt Counters



- Build custom reader and obtain unlimited number of traces
- Collection of 100 traces + full key extraction (64 bits) in 20 minutes on standard laptop