Statistical Fault Attacks Revisited Application to Authenticated Encryption

C. Dobraunig, M. Eichlseder, T. Korak, V. Lomné, F. Mendel

ASK 2016

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644052 (HECTOR).

Authenticated Encryption

- Encryption / Authentication
  - $\mathcal{E}(K, N, A, P) = (C, T)$
- Decryption / Verification
  - $\mathcal{D}(K, N, A, C, T) \in \{P, \bot\}$

Fault Attacks

- Differential Fault Analysis
- Collision Fault Analysis
- Safe Error Attack
- ...

⇒ Statistical Fault Attack

Statistical Fault Attack

- Fuhr et al. (FDTC 2013)
- Fault attack on AES with *faulty ciphertexts only*
- Succeeding with *random and unknown plaintexts*

- **Main Idea:** Fault injection introduces a *bias on a target variable*

Fault Models

- **Perfect control.** The attacker perfectly knows the statistical distribution of the faulty value
- **Partial control.** The attacker has some partial information on the distribution of the faulty value
- **No control.** The attacker has no information about the distribution of the faulty value, except that it is non uniform

Application to AES

- Attack on the 10th round

	Max. likelihood	Min. mean HW
a)	1	1
b)	10	14
c)	14	18

2^8 hypotheses per key byte

Application to AES

- Attack on the 9th round

	Square Euclidean Imbalance
a)	6
b)	14
c)	80

2^{32} hypotheses to retrieve 4 key bytes

Statistical Fault Attack

Requirements for the Attack

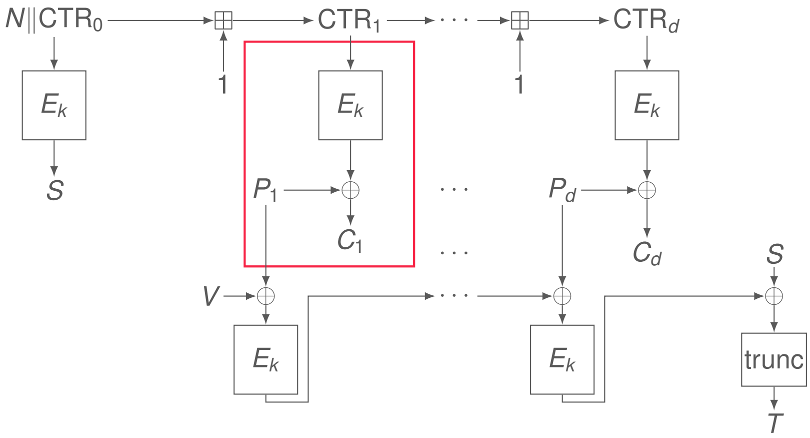
1. The inputs need to be different for each fault
2. The block cipher output needs to be known

Application

Authenticated encryption modes for block ciphers (ISO/IEC)

- CCM
- EAX
- GCM
- OCB
- SIV (Key Wrap)

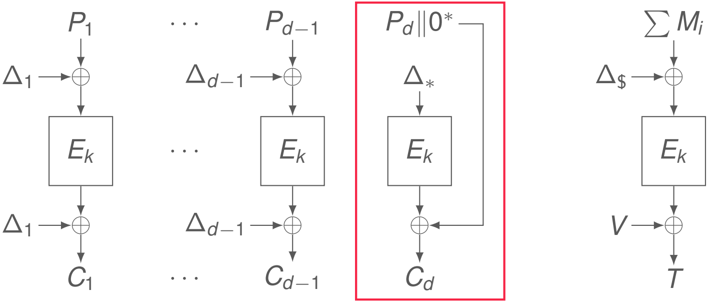
Attack on CCM



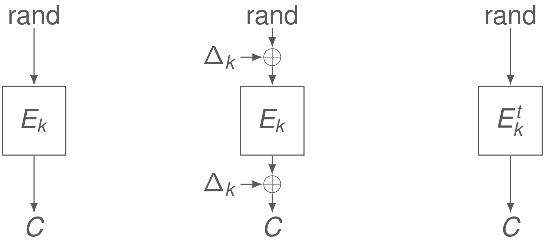
Attack on EAX and GCM

- EAX
  - CTR + CMAC
  - cleaned-up CCM
- GCM
  - CTR + CW MAC

Attack on OCB

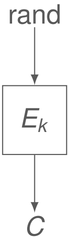


Application to other schemes



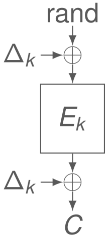
Basic Construction

- Cloc/Silc
  - CFB + CBC MAC
- OTR
  - XE + 2r-Feistel



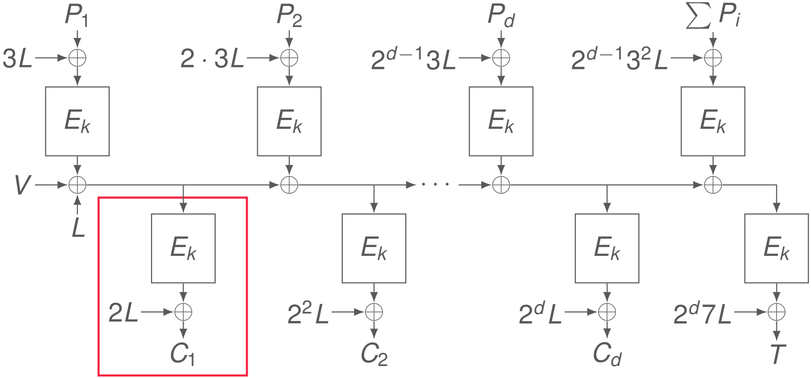
XEX-like Construction

- Output is mask by Δ_k
  - $\Delta_k := \delta_k$
  - $\Delta_k := \delta_k + \delta_n$
  - $\Delta_k := \delta_{k,n}$



- Example: COPA

Attack on COPA



- $L = E_k(0)$

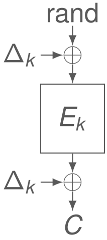
Attack on COPA

- Idea: Consider $2L$ as part of the last subkey
    - $SK'_{10} := SK_{10} \oplus 2L$
- Apply SFA to recover SK'_{10}
- Repeat attack to either recover
    - SK_9 (in round 9) or
    - $SK'_{10} := SK_{10} \oplus 2^2L$ of the next block the get SK_{10}

⇒ Attack complexity (number of needed faults) is doubled

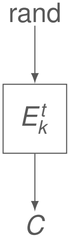
XEX-like Construction

- Output is mask by Δ_k
  - $\Delta_k := \delta_k$
  - $\Delta_k := \delta_k + \delta_n$
  - $\Delta_k := \delta_{k,n}$

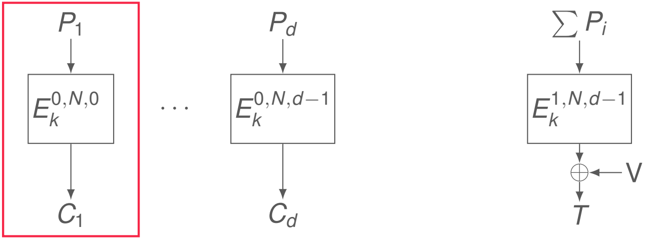


Tweakable Block Cipher

- TWEAKEY framework
  - Deoxys
  - KIASU
  - . . .



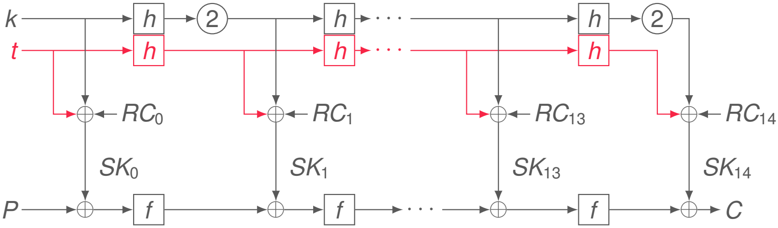
Attack on Deoxys$^{\neq}$



- Similar to OCB

Attack on Deoxys$^{\neq}$

- Deoxys-BC-256



Summary of Results

Primitive	Classification	Comments
CCM	basic	CTR
GCM	basic	CTR
EAX	basic	CTR
OCB	basic	XE
Cloc/Silc*	basic	CFB
OTR*	basic	XE
COPA*	XEX	
ELmD*	XEX	
SHELL*	XEX	
KIASU*	TBC	TWEAKEY
Deoxys*	TBC	TWEAKEY

* CAESAR candidates

Practical Verification/Implementation

- Clock glitches
  - General-purpose microcontroller (ATxmega 256A3)
  - AES software implementation
  - AES hardware co-processor
- Laser fault injection
  - Smartcard microcontroller
  - AES hardware co-processor

⇒ Key-recovery with a small number of faulty ciphertexts

Summary

- SFA is a powerful tool
- Attacks are not limited to AES-based modes
  - e.g. Prøst, Joltik, Scream,. . .
- Applicable to some Sponge modes
  - APE construction
  - e.g. PRIMATEs, Ascon

Thank you

http://eprint.iacr.org/2016/616

References

E. Biham and A. Shamir
Differential Fault Analysis of Secret Key Cryptosystems
CRYPTO 1997

D. Boneh, R. A. DeMillo, and R. J. Lipton
On the Importance of Checking Cryptographic Protocols for Faults
EUROCRYPT 1997

J. Blömer and V. Krummel
Fault Based Collision Attacks on AES
FDTC 2006

T. Fuhr, É. Jaulmes, V. Lomné, and A. Thillard
Fault Attacks on AES with Faulty Ciphertexts Only
FDTC 2013

C. Dobraunig, M. Eichlseder, T. Korak, V. Lomné, and F. Mendel
Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes
ASIACRYPT 2016