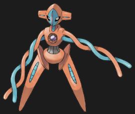


Deoxys

Jérémy Jean - Ivica Nikolić
Thomas Peyrin - Yannick Seurin

NTU (Singapore) and ANSSI (France)

DIAC 2016

Nagoya, Japan - September 27, 2016

http://www1.spms.ntu.edu.sg/~syllab/Deoxys

NANYANG
TECHNOLOGICAL
UNIVERSITY

Outline

Deoxys in third round

For 3rd round, two tweaks for Deoxys:

1. use of cheap LFSRs instead of multiplication in $GF(2^8)$ in the tweakable block cipher Deoxys-BC:
   - no change in security reasoning
   - faster and smaller implementation
2. changed the way the nonce is handled in Deoxys-II:
   - faster (removes two encryption calls)
   - more secure (we now obtain graceful security reduction for both authentication and confidentiality)

Parameters

We also changed the names:

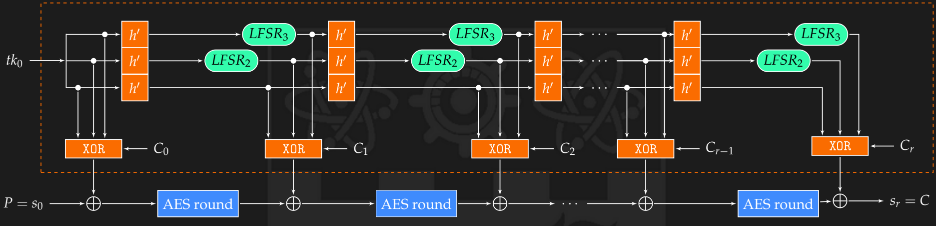
- Deoxys$\neq$ becomes Deoxys-I (nonce-respecting)
- Deoxys$=$ becomes Deoxys-II (nonce-misuse resistant)

	Mode		Internal primitive	
	TAE-like	SCT-2	Deoxys-BC-256	Deoxys-BC-384
Deoxys-I-128	✓		✓	
Deoxys-II-128		✓	✓	
Deoxys-I-256	✓			✓
Deoxys-II-256		✓		✓

Outline

Outline

The Deoxys-BC tweakey schedule



In details:

- TWEAKEY framework and STK construction [ASIACRYPT'14]
- round function is the AES round function
- h' will simply be a permutation of the nibbles positions
- each nibble of the k-th tweakey word is updated with $LFSR_k$
- very simple transformations: linear and lightweight

The Deoxys-BC tweakable block ciphers

Deoxys-BC-256 and Deoxys-BC-384

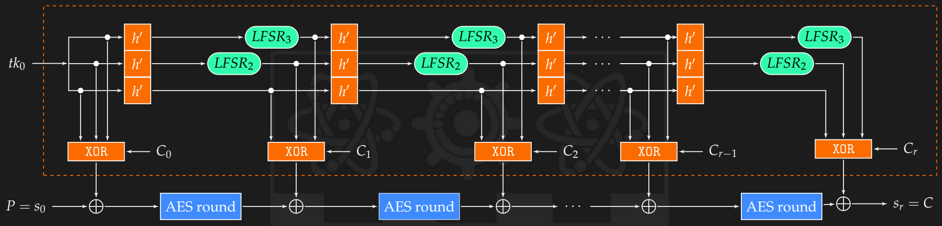
- 128-bit tweakable block ciphers
- The round function is **exactly** the AES round function
- Deoxys-BC-256:
  - **14 rounds**
  - 256-bit tweakey (2 tweakey words)
- Deoxys-BC-384:
  - **16 rounds**
  - 384-bit tweakey (3 tweakey words)

The TWEAKEY schedule:

- h' is a simple permutation of the 16 nibbles
- The LFSRs can be clocked with a single XOR
- Constant additions to break symmetries (RCON from AES KS)

Outline

The STK construction: rationale



Related-tweakey security analysis

A security analysis is now possible with STK:

- when considering one tweakey word, we ensure that function h' is itself a good tweakey schedule
- the LFSRs control the number of cancellations in g, when the subtweakeys are XORed to the internal state
- when considering several tweakey words, we can now reuse existing tools searching for good differential paths: for these tools it is easy to add the cancellation bound

Security of the STK construction

Related-key related-tweak attacks (4 × 4 AES-like design)

We prove that no good related-key related-tweak attacks differential path exist (even boomerang), with a computer-aided search tool.

rounds	active SBoxes	upper bound on probability	method used
6	12	$2^{-72}/2^{-24}$	Matsui's
8	≥ 17	$2^{-108}/2^{-34}$	ex. split (4R+4R)
10	≥ 22	$2^{-132}/2^{-44}$	ex. split (5R+5R)

Meet-in-the-middle attacks

Using a computer-aided search tool, we checked that Demirci-Selćuk MitM attack and its improvements cannot apply, even when using the tweak input as extra leverage.

Comparing Deoxys-BC and AES

Number of active Sboxes in single-key (SK) and related-key (RTK)

Cipher	Model	Rounds 1	2	3	4	5	6	7	8
Deoxys-BC-256	SK	1	5	9	25	26	30	34	50
(14 rounds)	RTK	0	0	1	5	9	12	≥ 17	≥ 22
AES-256	SK	1	5	9	25	26	30	34	50
(14 rounds)	RTK	0	0	1	3	5	5	5	10

Comparison of security claims

AES-256 claims 2^{256} security, while we only need to claim 2^{128} security for Deoxys-BC-256

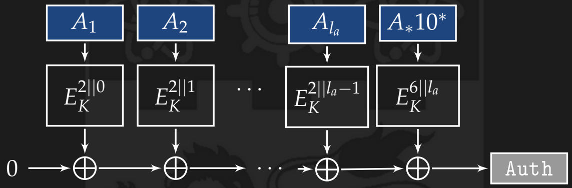
Outline

Outline

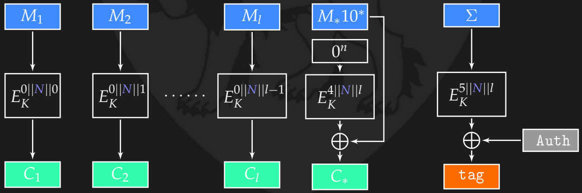
Nonce-respecting mode: Deoxys-I

Deoxys-I is similar to TAE or OCB3

For associated data authentication:



For plaintext:



Nonce-respecting mode: Deoxys-I

As the nonce is never reused, it is ensured that every call to the TBC during the encryption will have distinct tweak input values

We can directly reuse the TAE or OCB3 security proofs:

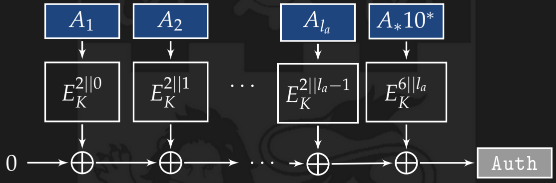
- but ensuring full security instead of birthday bound
- independent of the amount of data
- the proofs are simpler (see ΘCB3 and OCB3 proofs)
- no long initialization required: fast for short inputs

Outline

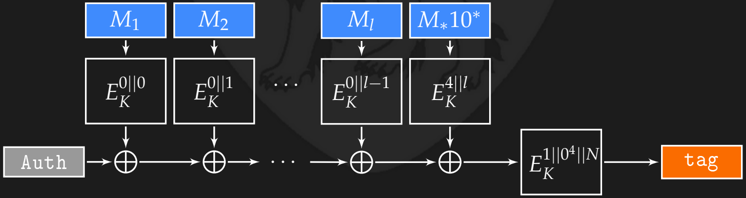
Nonce-misuse resistant mode: Deoxys-II

Deoxys-II is based on SCT-2:
an improved version of SCT mode [CRYPTO'16]

For associated data authentication:



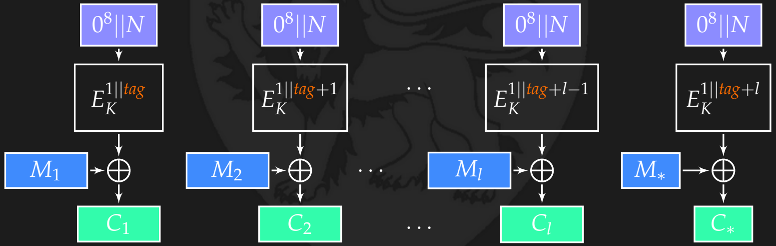
For plaintext authentication:



Nonce-misuse resistant mode: Deoxys-II

Deoxys-II is based on SCT-2:
an improved version of SCT mode [CRYPTO'16]

For plaintext encryption:



Nonce-misuse resistant mode: Deoxys-II

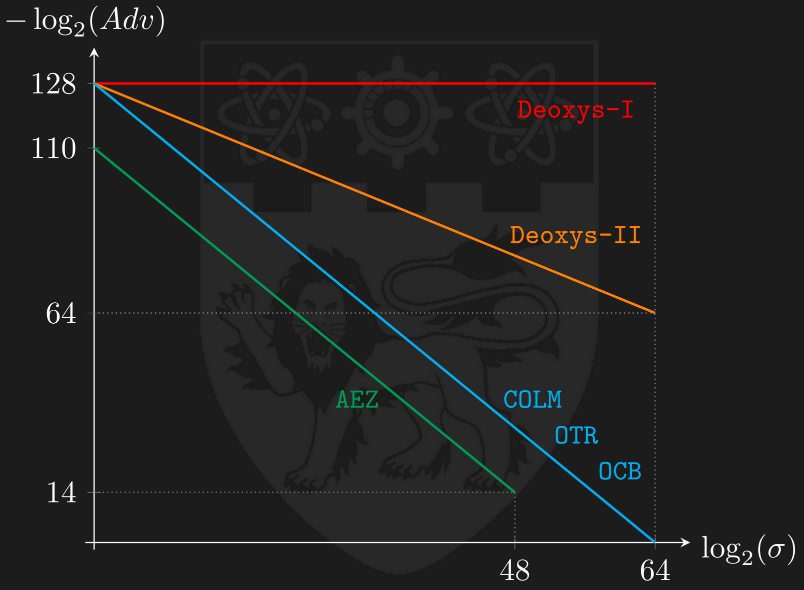
Nonce-misuse resistance in the **strong MRAE sense**
(not the weaker online misuse-resistance notion)

SCT-2 is the first AEAD mode that provides:

- full n-bit security when the nonce is not reused
- some ($n/2$-bit) security when the nonce is reused
- close to the full n-bit security when the nonce is reused only a few times
  (which is exactly what might happen in practice)

Outline

Security claims - a comparison of the nonce-respecting case



Features

Parallelization:

Both Deoxys-I and Deoxys-II are parallelizable

Small messages:

Both our modes are particularly efficient for small messages:

- almost no initialisation is required, unlike for sponge-based (long init process), AES-GCM-like or OCB3-like candidates (precomputation tables)
- for m message blocks:
  - only $m + 1$ encryption calls (optimal) for Deoxys-I
  - only $2m + 1$ encryption calls ($2m$ is optimal) for Deoxys-II
- small messages are important:
  - a typical use-case of hardware applications
  - a typical use-case of software applications (IMIX)

Memory overhead:

Both our modes have little memory overhead (no precomp. tables)

Outline

Performances of Deoxys

Software implementations

- less than a cycle per byte for Deoxys-I-128 on Haswell or Skylake (AES-NI)
- Deoxys-BC is basically 1.4/1.6 the speed of AES-128 (a bit faster on some platforms due to lighter key schedule)

Hardware implementations

- ASIC (Poschmann/Stöttinger implementation):
  - 2860 GE for Deoxys-BC-256 / 3575 GE for Deoxys-BC-384
- FPGA (GMU implementations):
  - Virtex 6/7: Deoxys-I-128 requires about 3250 LUTs for a throughput of 2.8 Gbit/s
  - these implementations contain encryption and decryption

Outline

Summary

- Deoxys-I and Deoxys-II both provide full n-bit security - **not birthday security !**
  - Deoxys-I: one-pass online mode attacker advantage does not depend on #data
  - Deoxys-II: two-pass mode MRAE security, linear security loss from #repeating nonces
- very fast in software: less than 1c/B on recent processors
- efficient in hardware: similar to AES, but operating modes require little area
- fast for short messages: no initialization and minimal number of encryption calls
- security proofs for the operating modes
- simple and clean
- to be continued: intermediate tags

Thank you !