Introduction

The Deoxys-BC tweakable BC
   - Deoxys-BC and the STK construction
   - Security of Deoxys-BC

The operating mode(s)
   - Nonce-respecting mode: Deoxys-I
   - Nonce-misuse resistant mode: Deoxys-II
   - Security claims and features

Performances

Conclusion
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)
We also changed the names:

- Deoxys≠ becomes Deoxys-I (nonce-respecting)
- Deoxys= becomes Deoxys-II (nonce-misuse resistant)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Internal primitive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TAE-like</td>
</tr>
<tr>
<td>Deoxys-I-128</td>
<td>✓</td>
</tr>
<tr>
<td>Deoxys-II-128</td>
<td></td>
</tr>
<tr>
<td>Deoxys-I-256</td>
<td>✓</td>
</tr>
<tr>
<td>Deoxys-II-256</td>
<td></td>
</tr>
</tbody>
</table>
Outline

1 Introduction

2 The Deoxys-BC tweakable BC
   - Deoxys-BC and the STK construction
   - Security of Deoxys-BC

3 The operating mode(s)
   - Nonce-respecting mode: Deoxys-I
   - Nonce-misuse resistant mode: Deoxys-II
   - Security claims and features

4 Performances

5 Conclusion
Introduction

2 The Deoxys-BC tweakable BC
   ▶ Deoxys-BC and the STK construction
   ▶ Security of Deoxys-BC

3 The operating mode(s)
   ▶ Nonce-respecting mode: Deoxys-I
   ▶ Nonce-misuse resistant mode: Deoxys-II
   ▶ Security claims and features

4 Performances

5 Conclusion
The Deoxys-BC tweakey schedule

\[tk_0 \rightarrow h' \rightarrow LFSR_3 \rightarrow h' \rightarrow LFSR_2 \rightarrow h' \rightarrow LFSR_3 \rightarrow \cdots \rightarrow h' \rightarrow LFSR_2 \rightarrow \cdots \rightarrow LFSR_3 \rightarrow C_r\]

\[P = s_0 \rightarrow + \rightarrow \text{AES round} \rightarrow + \rightarrow \text{AES round} \rightarrow \cdots \rightarrow + \rightarrow \text{AES round} \rightarrow s_r = C\]

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)
1. Introduction

2. The Deoxys-BC tweakable BC
   - Deoxys-BC and the STK construction
   - Security of Deoxys-BC

3. The operating mode(s)
   - Nonce-respecting mode: Deoxys-I
   - Nonce-misuse resistant mode: Deoxys-II
   - Security claims and features

4. Performances

5. Conclusion
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 \((4 \times 4 \text{ AES-like design})\)

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

<table>
<thead>
<tr>
<th>rounds</th>
<th>active SBoxes</th>
<th>upper bound on probability</th>
<th>method used</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>12</td>
<td>(2^{-72}/2^{-24})</td>
<td>Matsui’s</td>
</tr>
<tr>
<td>8</td>
<td>(\geq 17)</td>
<td>(2^{-108}/2^{-34})</td>
<td>ex. split ((4R+4R))</td>
</tr>
<tr>
<td>10</td>
<td>(\geq 22)</td>
<td>(2^{-132}/2^{-44})</td>
<td>ex. split ((5R+5R))</td>
</tr>
</tbody>
</table>

Meet-in-the-middle attacks

Using a computer-aided search tool, we checked that Demirci-Selçuk 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

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Model</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deoxys-BC-256 (14 rounds)</td>
<td>SK</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>25</td>
<td>26</td>
<td>30</td>
<td>34</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>RTK</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>12</td>
<td>$\geq$ 17</td>
<td>$\geq$ 22</td>
</tr>
<tr>
<td>AES-256 (14 rounds)</td>
<td>SK</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>25</td>
<td>26</td>
<td>30</td>
<td>34</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>RTK</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

Comparison of security claims

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

1 Introduction

2 The Deoxys-BC tweakable BC
   ▶ Deoxys-BC and the STK construction
   ▶ Security of Deoxys-BC

3 The operating mode(s)
   ▶ Nonce-respecting mode: Deoxys-I
   ▶ Nonce-misuse resistant mode: Deoxys-II
   ▶ Security claims and features

4 Performances

5 Conclusion
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

1. Introduction
2. The Deoxys-BC tweakable BC
   - Deoxys-BC and the STK construction
   - Security of Deoxys-BC
3. The operating mode(s)
   - Nonce-respecting mode: Deoxys-I
   - Nonce-misuse resistant mode: Deoxys-II
   - Security claims and features
4. Performances
5. Conclusion
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:

\[
\begin{align*}
A_1 & \rightarrow E_K^2 || 0 \\
A_2 & \rightarrow E_K^2 || 1 \\
& \cdots \\
A_{l_a} & \rightarrow E_K^2 || l_a - 1 \\
A_{*10^*} & \rightarrow E_K^6 || l_a \\
0 \oplus & \cdots \oplus \text{Auth}
\end{align*}
\]

For plaintext authentication:

\[
\begin{align*}
M_1 & \rightarrow E_K^0 || 0 \\
M_2 & \rightarrow E_K^0 || 1 \\
& \cdots \\
M_{l} & \rightarrow E_K^0 || l - 1 \\
M_{*10^*} & \rightarrow E_K^4 || l \\
\text{Auth} \oplus & \cdots \oplus \text{tag}
\end{align*}
\]
**Nonce-misuse resistant mode:** Deoxys-II

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

For plaintext encryption:

\[
\begin{align*}
0^8 || N &
\begin{array}{c}
E_K^1 || \text{tag} \\
M_1 \xrightarrow{\oplus} C_1
\end{array} \\
0^8 || N &
\begin{array}{c}
E_K^1 || \text{tag} + 1 \\
M_2 \xrightarrow{\oplus} C_2
\end{array} \\
\cdots &
\end{align*}
\]

\[
\begin{align*}
0^8 || N &
\begin{array}{c}
E_K^1 || \text{tag} + (l-1) \\
M_l \xrightarrow{\oplus} C_l
\end{array} \\
0^8 || N &
\begin{array}{c}
E_K^1 || \text{tag} + l \\
M_* \xrightarrow{\oplus} C_*
\end{array}
\end{align*}
\]
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

1 Introduction

2 The Deoxys-BC tweakable BC
   - Deoxys-BC and the STK construction
   - Security of Deoxys-BC

3 The operating mode(s)
   - Nonce-respecting mode: Deoxys-I
   - Nonce-misuse resistant mode: Deoxys-II
   - Security claims and features

4 Performances

5 Conclusion
Security claims - a comparison of the nonce-respecting case

The figure plots the advantage of an adversary as a function of the total number of queried blocks $\sigma$. The graph compares the security of different modes: Deoxys-I, Deoxys-II, COLM, OTR, OCB, and AEZ.
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

1. Introduction
   - Deoxys-BC and the STK construction
   - Security of Deoxys-BC

2. The Deoxys-BC tweakable BC
   - Deoxys-BC and the STK construction
   - Security of Deoxys-BC

3. The operating mode(s)
   - Nonce-respecting mode: Deoxys-I
   - Nonce-misuse resistant mode: Deoxys-II
   - Security claims and features

4. Performances

5. Conclusion
### 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
Introduction

The Deoxys-BC tweakable BC
- Deoxys-BC and the STK construction
- Security of Deoxys-BC

The operating mode(s)
- Nonce-respecting mode: Deoxys-I
- Nonce-misuse resistant mode: Deoxys-II
- Security claims and features

Performances

Conclusion
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!