Elena Andreeva\textsuperscript{1}, Andrey Bogdanov\textsuperscript{2}, Nilanjan Datta\textsuperscript{3}, Atul Luykx\textsuperscript{1}, Bart Mennink\textsuperscript{1}, \textbf{Mridul Nandi}\textsuperscript{3}, Elmar Tischhauser\textsuperscript{2}, Kan Yasuda\textsuperscript{4}

\textsuperscript{1}KU Leuven and iMinds, Belgium

\textsuperscript{2}DTU Compute, Denmark

\textsuperscript{3}Indian Statistical Institute, India

\textsuperscript{4}NTT Secure Platform Laboratories, Japan

September 27, 2016
CAESAR Overview

Table: CAESAR Round 3 Candidates. *Deoxys uses tweakable block cipher modes and creates a new tweakable block cipher.

<table>
<thead>
<tr>
<th>Dedicated</th>
<th>Block Cipher Mode</th>
<th>Permutation-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORN</td>
<td>AES-OTR</td>
<td>Ascon</td>
</tr>
<tr>
<td>AEGIS</td>
<td>CLOC and SILC</td>
<td>Ketje</td>
</tr>
<tr>
<td>AEZ</td>
<td>COLM</td>
<td>Keyak</td>
</tr>
<tr>
<td>MORUS</td>
<td>JAMBU</td>
<td>NORX</td>
</tr>
<tr>
<td>Tiaoxin</td>
<td>OCB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deoxys*</td>
<td></td>
</tr>
</tbody>
</table>
Block Cipher Mode Disadvantages

1. Usually birthday bound security

2. Efficiency cannot improve beyond block cipher (see e.g. AEGIS vs. CTR)
1. Block ciphers are ubiquitous

2. Can be used with any block cipher

3. A safe bet: security reduction to underlying block cipher

Block size $\geq 128$ bits $\Rightarrow$ Can process petabytes of data with success probability well below $2^{-30}$
Table: CAESAR Round 3 Candidates. *Deoxys uses tweakable block cipher modes and creates a new tweakable block cipher.

<table>
<thead>
<tr>
<th>Dedicated</th>
<th>Block Cipher Mode</th>
<th>Permutation-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORN</td>
<td>AES-OTR</td>
<td>Ascon</td>
</tr>
<tr>
<td>AEGIS</td>
<td>CLOC and SILC</td>
<td>Ketje</td>
</tr>
<tr>
<td>AEZ</td>
<td>COLM</td>
<td>Keyak</td>
</tr>
<tr>
<td>MORUS</td>
<td>JAMBU</td>
<td>NORX</td>
</tr>
<tr>
<td>Tiaoxin</td>
<td>OCB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deoxys*</td>
<td></td>
</tr>
</tbody>
</table>
Table: CAESAR Round 3 Candidates. *Deoxys uses tweakable block cipher modes and creates a new tweakable block cipher.

<table>
<thead>
<tr>
<th>Dedicated</th>
<th>Block Cipher Mode</th>
<th>Permutation-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORN</td>
<td>AES-OTR</td>
<td>Ascon</td>
</tr>
<tr>
<td>AEGIS</td>
<td>CLOC and SILC</td>
<td>Ketje</td>
</tr>
<tr>
<td>AEZ</td>
<td>COLM</td>
<td>Keyak</td>
</tr>
<tr>
<td>MORUS</td>
<td>JAMBU</td>
<td>NORX</td>
</tr>
<tr>
<td>Tiaoxin</td>
<td>OCB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deoxys*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ΘCB and SCT)</td>
<td></td>
</tr>
</tbody>
</table>
Robustness

**Table:** Levels of resistance to nonce misuse.

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-OTR</td>
<td>COLM</td>
<td>Deoxys-II (SCT)</td>
</tr>
<tr>
<td>CLOC and SILC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JAMBU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deoxys-I</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Background: Online Nonce Misuse Resistance

\[
\begin{array}{c|c}
M & M_1 \\
\hline
& N_1, K \rightarrow C_1, C_1^* \rightarrow T_1 \\
M & M_2 \\
\hline
& N_2, K \rightarrow C_2, C_2^* \rightarrow T_2 \\
M' & \\
\hline
& N_3, K \rightarrow C_3 \rightarrow T_3
\end{array}
\]
Background: Online Nonce Misuse Resistance

Equality of prefixes of messages determined

No relationship past common prefix

Hoang et al. CRYPTO 2015 attack. . .

but still much more robust than GCM, OCB, OTR, . . .
Background: Online Nonce Misuse Resistance

Equality of prefixes of messages determined

No relationship past common prefix

Hoang et al. CRYPTO 2015 attack. . .

but still much more robust than GCM, OCB, OTR, . . .
Background: Online Nonce Misuse Resistance

Equality of prefixes of messages determined
Background: Online Nonce Misuse Resistance

1. Equality of prefixes of messages determined
2. No relationship past common prefix
Equality of prefixes of messages determined

No relationship past common prefix

Hoang et al. CRYPTO 2015 attack...
Background: Online Nonce Misuse Resistance

1. Equality of prefixes of messages determined
2. No relationship past common prefix
3. Hoang et al. CRYPTO 2015 attack...
4. but still much more robust than GCM, OCB, OTR, ...
Advantage over SCT: *Online* Scheme

1. High latency (receive full message before first output)
2. Storage issues (large internal state)

\[
\begin{align*}
\end{align*}
\]

Dependency in SCT.
Advantage over SCT: *Online* Scheme

1. High latency (receive full message before first output)
2. Storage issues (large internal state)

\[
\begin{align*}
\downarrow & & & \\
\end{align*}
\]

Dependency in SCT.

\[
\begin{align*}
\downarrow & & \downarrow & \\
\end{align*}
\]

Dependency in COLM.
## COLM Comparison with ELmD and COPA

<table>
<thead>
<tr>
<th>Feature</th>
<th>COPA</th>
<th>ELmD</th>
<th>COLM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplified masking</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Fully parallelizable authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>XOR mixing for authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$\rho$ mixing for encryption</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bottom layer encryption</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Intermediate tags</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
COLM Description
Summary

COLM: strengths of COPA + ELmD

1. security reduction to block cipher
2. online misuse resistance: most robust AES-mode in the competition
3. highly parallelizable

Thank you for your attention.
1. Andreeva et al. “How to securely release unverified plaintext in authenticated encryption” ASIACRYPT 2014
4. Nandi “XLS is Not a Strong Pseudorandom Permutation” ASIACRYPT 2014
5. Nandi “Revisiting Security Claims of XLS and COPA” eprint