Security Aspects of Authenticated Encryption
(in light of the CAESAR competition)

Elena Andreeva
COSIC, KU Leuven, Belgium

Cryptoday 2014
Technion, Haifa, Israel
30/12/2014
Outline

- Authenticated Encryption: AE
- Generic AE composition
- Dedicated AE schemes
  - nonce-based AE
  - nonce misuse resistant AE
- Further challenges
- CAESAR AE competition
AE Security Goal

Confidentiality + Authenticity
Confidentiality

Encryption Scheme

Alice  \[ M \rightarrow \text{Enc} \rightarrow \text{C} = 1001\ldots10 \rightarrow \text{Dec} \rightarrow M \]

Bob
Confidentiality

Encryption Scheme

Alice\[M \rightarrow Enc \rightarrow C' = 1011\ldots10 \rightarrow Dec \rightarrow M' \neq M\]

Bob

Confidentiality ≠ Authenticity
Authenticity

Message Authentication Code: MAC

Alice  \( K \)  \( \rightarrow \)  MAC  \( M \)  \( \rightarrow \)  T  \( \rightarrow \)  Bob

Bob  \( K \)  \( \rightarrow \)  MAC  \( M \)  \( \rightarrow \)  T' = T

\( T' = T \)
How to combine Encryption and MAC in a secure way?

Confidentiality + Authenticity
1. Encrypt and MAC

2. MAC then Encrypt

3. Encrypt then MAC

Caveat: Careful with interpretations!
Conventional Encryption

- **Enc = (Kg, Enc, Dec)**
  - Key generation: $K \leftarrow Kg$
  - Encryption: $(st, C) \leftarrow Enc^st_K(M)$ (randomized or stateful)
  - Decryption: $M \leftarrow Dec_K(st, C)$ (deterministic)
  - Correctness: $Dec_K(Enc_K(M)) = M$

- **Indistinguishability**
  - $IND-CPA$

![Diagram showing encryption and decryption processes]

- Each input $M$ is encrypted with $Enc_K$ to produce $Enc_K(M)$.
- The output $C$ is either randomized or stateful.
- The decrypted message $M$ is deterministic.
- The diagram illustrates a user trying to distinguish between random bits and randomized encryption.$^\dagger$
MAC

- **MAC** = (Kg, MAC, Verify)

  **Key generation**: \( K \leftarrow \$ \ Kg \)
  **Authentication**: \( T \leftarrow \text{MAC}_K(M) \) (any)
  **Verification**: \( 1/0 \leftarrow \text{Verify}_K(M, T) \) (deterministic)

  **Correctness**: \( \text{Verify}_K(M, \text{MAC}_K(M)) = 1 \)

- **Unforgeability** (weak \( M' \neq M \); strong \( M',T' \neq M,T \))

![Diagram showing MAC process]

Win if \(?\) is 1
Generic Composition [BN’00]

• IND-CPA $\text{Enc}$ + Unforgeable $\text{MAC}$

AE secure: Enc then MAC

• Off the shelf schemes

$\text{Enc}$ (CBC, CTR,...) + $\text{MAC}$ (CBC-MAC, HMAC, PMAC,...)

Caveat: Careful with interpretations!
A. $\text{Enc}$ often with badly or externally generated random $\text{st}$ or $\text{IV}$
B. $\text{st}$ or $\text{IV}$ is communicated out-of-band
A: Random IV Encryption

- **Enc** = (Kg, Enc, Dec)
  
  Key generation: $K \leftarrow$ Kg
  Encryption: IV, C $\leftarrow$ Enc$^{IV}_K$(M) (deterministic)
  Decryption: $M \leftarrow$ Dec$_K$ (IV, C) (deterministic)
  
  Correctness: Dec$_K$(Enc$^{IV}_K$(M)) = M
  
- **Indistinguishability**
  
  $\text{IND-CPA}$

  ![Diagram](image)
Nonce IV

• N: nonce IV
• Not required to be random
• Unique non-repeating value
• Can be communicated out of band
• Theoretically: a way to work with an IV (randomness/state) out of Enc algorithm
• Practically: ease of use
Nonce-based Encryption Scheme

- **Enc = (Kg, Enc, Dec)**

  - Key generation: $K \leftarrow \$ Kg$
  - Encryption: $C \leftarrow Enc_K(N, M)$ (deterministic)
  - Decryption: $M \leftarrow Dec_K(N, C)$ (deterministic)

  Correctness: $Dec_K(N, Enc_K(M)) = M$

- Indistinguishability (nonce respecting adversary) $\text{IND-CPA}$

  - Fix A: Adversary can select $N$
  - Fix B: out-of-band $|C|\$ Random bits
Build nonce-based AE from

1. IV-Enc + MAC
Generic Composition Reconsidered [NRS’14]

- Build nonce-based AE from
  2. N-Enc + MAC

- Generic composition disadvantages
  Efficiency issues: 2 passes over the data
  Use of 2 keys
  Prone to misuse with conventional Enc schemes
Other Ways to Build AE Schemes?

1. Generic **AE** composition
   + off the shelf primitives
   - 2 passes
   - 2 keys

2. Dedicated **AE** scheme (**AE** designs from scratch)

3. Something in between 😊 (state of the art)
## Dedicated AE

Prior to CAESAR

<table>
<thead>
<tr>
<th>Building Block</th>
<th>Nonce dependent AE security</th>
<th>Nonce independent AE security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Block cipher</strong></td>
<td>IAPM*’00, OCB*’01, XECB*’01, CCM’03, GCM’04, OTR*’14, CLOC’14</td>
<td>SIV’06, BTM’09, McOE-G’11, POET’14 COPA’13</td>
</tr>
<tr>
<td><strong>Permutation</strong></td>
<td>Sponge Wrap’11 Ketje&amp;Keyak’14 NORX’14</td>
<td>APE’14</td>
</tr>
</tbody>
</table>

* hold a patent
**AE Syntax**

- **AE** = (Kg, E, D)

  - **Key generation:** $K \leftarrow Kg$
  - **Encryption:** $C \leftarrow E_K(A, N, M)$ (deterministic)
  - **Decryption:** $M/\perp \leftarrow D_K(A, N, C)$ (deterministic)

  **Correctness:** $D_K(A, N, E_K(A, N, M)) = M$
AE Confidentiality

- $\text{IND-CPA}$

Adversary is nonce respecting
AE Integrity

- INT-CTX

Adversary maybe nonce respecting
Nonce-based AE Security

Adversary is nonce respecting
Example AE with Block Cipher

OCB [RBBK’01]

If BC (AES) is SPRP, OCB is AE secure up to $2^{n/2}$ queries for non repeating N
If $P$ is an ideal permutation, Sponge Wrap is AE secure up to $\min\{2^k, 2^{c/2}\}$ queries for non repeating $N$
- bound follows Sponge hash indifferentiability proof
- but possibly conservative for secret $K$ and $N$ not repeating
Authenticated Encryption AE
Generic AE composition
Dedicated AE schemes
  - nonce-based AE
    - nonce misuse resistant AE
Further challenges
CAESAR AE competition
Not all security should be lost if $N$ misused!
Distinct Nonces

\[ N_1 \rightarrow M_1 \rightarrow \text{OCB/Sponge Wrap} \rightarrow C_1 \]

\[ N_2 \rightarrow M_1 \rightarrow \text{OCB/Sponge Wrap} \rightarrow C_2 \]

\[ N_3 \rightarrow M_2 \rightarrow \text{OCB/Sponge Wrap} \rightarrow C_3 \]
**Nonce Misuse**

**Ciphertext Repetitions**

*What security can be lost?*

- Valid for **ALL** nonce respecting AE schemes

![Diagram](attachment:image.png)
What else can be lost?

\[ OCB-Enc \]

\[ M_1 \xrightarrow{\alpha_1} \text{AES}_K \xrightarrow{\alpha_1} C_1 \]
\[ M_2 \xrightarrow{\alpha_2} \text{AES}_K \xrightarrow{\alpha_2} C_2 \]
\[ \cdots \]
\[ M_d \xrightarrow{\alpha_d} \text{AES}_K \xrightarrow{\alpha_d} C_d \]
Nonce Misuse OCB
Ciphertext Block Repetitions

What else can be lost? (OCB loses confidentiality)

• If blocks in C repeat (over distinct OCB calls) then blocks in M repeat (OCB, IAPM, XCBC, ...)

\[
\begin{align*}
O CB-Enc & \\
M'_1 & \xrightarrow{\alpha_1} AES_K \xrightarrow{\alpha_1} C'_1 \\
M_2 & \xrightarrow{\alpha_2} AES_K \xrightarrow{\alpha_2} C_2 \\
\cdots & \cdots \cdots \\
M_d & \xrightarrow{\alpha_d} AES_K \xrightarrow{\alpha_d} C_d
\end{align*}
\]
Nonce Misuse Sponge Wrap

*What else can be lost? (Sponge Wrap looses confidentiality)*

\[c_1 \oplus c'_1 = m_1 \oplus m'_1\]
What to Do against Nonce Misuse?

Not all security should be lost if N misused!

1. Security up to repetitions
ciphertext leaks only presence of repeating Ms
**MAX:** SIV, BTM, HBS but **two passes over the data**

2. Security up to longest common prefix
ciphertext leaks only presence of common M prefixes
**LCP:** McOE-G, COPA, APE, POET
**LCP + X:** SpongeWrap
1. Online cipher + authentication [BBKN‘01, FFLW’12] [nmr AE scheme secure up to common prefix repetitions]
Regular vs Online Ciphers

- Normally in a cipher
  - $m_1$ $m_2$ $m_3$ $m_4$
  - $c_1$ $c_2$ $c_3$ $c_4$

- Online cipher
  - more efficient
  - different security (IND from random online permutation)

- $m_1$ $m_2$ $m_3$ $m_4$
- $c_1$ $c_2$ $c_3$ $c_4$
COPA [ABLMY’13]
Nonce Misuse Resistant AE

\[ \begin{align*}
L &= E_K(0) \\
\alpha_0 &= 3L \text{ and } \alpha_1 = 2L \\
\beta_1 &= 2^{d-1} \cdot 3^2L \text{ and } \beta_2 = 2^{d-1} \cdot 7L
\end{align*} \]
COPA
Security Proof

\[ M_1 \xrightarrow{XEX} C_1 \]
\[ M_2 \xrightarrow{XEX} C_2 \]
\[ \ldots \]
\[ M_d \xrightarrow{XEX} C_d \]
\[ \oplus_{i=1}^{d} M_i \xrightarrow{XEX} T \]

Implicit \( \oplus \) masks
\[ \alpha_i = 2^{i-1}.3L \]

If \( E \) is SPRP, COPA is AE secure up to \( 2^{n/2} \) queries
APE [ABLMNY’14]  
Nonce Misuse Resistant AE

If $P$ is ideal permutation, APE is AE secure up to $2^{c/2}$ queries
Authenticated Encryption AE
Generic AE composition
Dedicated AE schemes
  - nonce-based AE
  - nonce misuse resistant AE
Further challenges
CAESAR AE competition
Further Security Pitfalls in AE

What if attacker gets C decryptions before verification completed?

**RUP**: Release of unverified plaintext [ABLMNY’14]

- Scenarios
  - insecure memory
  - small buffer
  - real-time requirements

- Not in current AE security models!
AE Syntax under RUP

• Separate the AE Decryption D functionality into
  Dec and Verify (how we design AE schemes)

\[
C, T \leftarrow E_K(A, N, M) \\
M \leftarrow \text{Dec}_K(A, N, C, T) \\
1/0 \leftarrow \text{Verify}_K(A, N, C, T)
\]

Correctness: \( \text{Dec}_K(A, N, E_K(A, N, M)) = M \)
and \( \text{Verify}_K(A, N, E_K(A, N, M)) = 1 \)
RUP Confidentiality

- $\text{IND-CPA} + \text{PA1}$
- Plaintext awareness \(\text{PA1}\)

Adversary can choose any nonce
RUP Integrity

• Int-RUP

Adversary can choose any nonce
<table>
<thead>
<tr>
<th>IV Type</th>
<th>Scheme</th>
<th>PA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random</td>
<td>CTR, CBC encryption</td>
<td>Yes</td>
</tr>
<tr>
<td>Nonce</td>
<td>OCB</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>GCM, Sponge Wrap</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>CCM</td>
<td>No</td>
</tr>
<tr>
<td>Arbitrary</td>
<td>COPA</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>McOE-G</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>APE</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SIV, BTM, HBS</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Encode-then-Encipher</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Further Challenges

• AE security
  - handling failure events?
  - further generic results?
  - identify relevant AE security risks?

• Security of present solutions?
Authenticated Encryption AE

Generic AE composition

Dedicated AE schemes
  - nonce-based AE
  - nonce misuse resistant AE

Further challenges

CAESAR AE competition
CAESAR Competition

Competition for Authenticated Encryption: Security, Applicability, and Robustness

• Follows NIST AES, EU NESSIE, EU eStream, and NIST SHA-3 and is co-funded by NIST
• Need for secure and efficient authenticated encryption
• Winner should offer advantages over AES-GCM and be suitable for widespread adoption
• 57 submissions in march 2014
• 7 withdrawals
CAESAR Timeline

• Jan 2015 – announcement 2\textsuperscript{nd} round candidates
• Dec 2015 – announcement 3\textsuperscript{rd} round candidates
• Dec 2016 – announcement of finalists
• Dec 2017 – announcement of final portfolio
CAESAR Candidate Characteristics

- Online +
- Parallelizable +
- Nonce misuse resistant +
- Release of unverified plaintext RUP +
- Underlying primitive
- Inverse free +
- Efficient +
<table>
<thead>
<tr>
<th>#</th>
<th>AE Scheme</th>
<th>Type (BC or P)</th>
<th>Parallelizable (E/D)</th>
<th>Online (E/D)</th>
<th>NMR Nonce misuse resistance</th>
<th>Inverse free</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ACORN</td>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>++AE</td>
<td>BC</td>
<td>Partly/Partly</td>
<td></td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>AEGIS</td>
<td>BC</td>
<td></td>
<td></td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>AES-CMCC</td>
<td>BC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>AES-COBRA</td>
<td>BC</td>
<td>Partly/Partly</td>
<td>Fully/Fully</td>
<td></td>
<td>Yes</td>
<td>Withdrawn</td>
</tr>
<tr>
<td>6</td>
<td>AES-COPA</td>
<td>BC</td>
<td>Partly/Partly</td>
<td>Fully/Fully</td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>AES-CPFB</td>
<td>BC</td>
<td>Fully/No</td>
<td>Fully/Fully</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>AES-JAMBU</td>
<td>BC</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>AES-OTR</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td>A+N</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>AEZ</td>
<td>BC</td>
<td>Fully/Fully</td>
<td></td>
<td></td>
<td>MAX</td>
<td>No</td>
</tr>
<tr>
<td>11</td>
<td>Artemia</td>
<td>P/Sponge</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Ascon</td>
<td>P/Sponge</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>AVALANCHE</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Calico</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>CBA</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>CBEAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Withdrawn</td>
</tr>
<tr>
<td>17</td>
<td>CLOC</td>
<td>BC</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>AE Scheme</td>
<td>Type (BC or P)</td>
<td>Parallelizable (E/D)</td>
<td>Online (E/D)</td>
<td>NMR Nonce misuse resistance</td>
<td>Inverse free</td>
<td>Status</td>
</tr>
<tr>
<td>----</td>
<td>-------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>--------------</td>
<td>-----------------------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>18</td>
<td>Deoxys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>ELmD</td>
<td>BC</td>
<td>Partly/Partly</td>
<td>Fully/Fully</td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Enchilada</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td>None</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>FAKER</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td></td>
<td></td>
<td>Withdrawn</td>
</tr>
<tr>
<td>22</td>
<td>HKC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Withdrawn</td>
</tr>
<tr>
<td>23</td>
<td>HS1-SIV</td>
<td>Other</td>
<td>Fully/Fully</td>
<td>No/No</td>
<td>MAX</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>ICEPOLE</td>
<td>P/Sponge</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td>LCP+X</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>iFeed[AES]</td>
<td>BC</td>
<td>Fully/No</td>
<td>Fully/Fully</td>
<td>LCP+X</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Joltik</td>
<td>BC</td>
<td>Fully/Fully, Partly/Partly</td>
<td>Fully/Fully, Fully/Fully</td>
<td>None, LCP</td>
<td>No, No</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Julius</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>No/No</td>
<td>MAX</td>
<td>Yes, No</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Ketje</td>
<td>P/Sponge</td>
<td>No/No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Keyak</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>KIASU</td>
<td>BC</td>
<td>Fully/Fully, Partly/Partly</td>
<td>Fully/Fully, Fully/Fully</td>
<td>None, LCP</td>
<td>No, No</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>LAC</td>
<td>BC</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td>None</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Marble</td>
<td>BC</td>
<td>Partly/Partly</td>
<td>Fully/Fully</td>
<td>A+N/MAX, online</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>AE Scheme</td>
<td>Type (BC or P)</td>
<td>Parallelizable (E/D)</td>
<td>Online (E/D)</td>
<td>NMR Nonce misuse resistance</td>
<td>Inverse free</td>
<td>Status</td>
</tr>
<tr>
<td>----</td>
<td>-------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>--------------</td>
<td>-----------------------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>33</td>
<td>McMambo</td>
<td>LRX</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td></td>
<td>No</td>
<td>Withdrawn</td>
</tr>
<tr>
<td>34</td>
<td>Minalpher</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>MORUS</td>
<td>Other</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td>A+N/LCP+X</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>NORX</td>
<td>P/Sponge</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td>A+N/LCP+X</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>OCB</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td>None</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>OMD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>PAEQ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>PAES</td>
<td>AES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Withdrawn</td>
</tr>
<tr>
<td>41</td>
<td>PANDA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Withdrawn</td>
</tr>
<tr>
<td>42</td>
<td>$\pi$-Cipher</td>
<td>P/Sponge</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td>None</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>POET</td>
<td>BC/AES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>POET-G withdrawn</td>
</tr>
<tr>
<td>44</td>
<td>POLAWIS</td>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>PRIMATEs</td>
<td>P/Sponge</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Prøst</td>
<td>P</td>
<td>Partly/Partly, Fully/Fully, No/No</td>
<td>Fully/Fully</td>
<td>Yes, No, Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Raviyoyla</td>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# CAESAR Classification

[https://aezoo.compute.dtu.dk](https://aezoo.compute.dtu.dk)

<table>
<thead>
<tr>
<th>#</th>
<th>AE Scheme</th>
<th>Type (BC or P)</th>
<th>Parallelizable (E/D)</th>
<th>Online (E/D)</th>
<th>NMR Nonce misuse resistance</th>
<th>Inverse free</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>Sablier</td>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Scream</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td>None</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>SHELL</td>
<td>BC</td>
<td>Partly/Partly</td>
<td>Fully/Fully</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Silc</td>
<td>BC</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td>A+N</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Silver</td>
<td>BC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>STRIBOB</td>
<td>P/Sponge</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td>A+N</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Tiaoxin</td>
<td>BC</td>
<td>No/No</td>
<td>Fully/Fully</td>
<td>None</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>TriviA-ck</td>
<td>Other</td>
<td>No/No</td>
<td>No/No</td>
<td>A+N</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Wheesht</td>
<td>Other</td>
<td></td>
<td>None</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>YAES</td>
<td>BC</td>
<td>Fully/Fully</td>
<td>Fully/Fully</td>
<td>None</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Software comparison:

More Features ...

• Further features:
  - Incrementality, tag truncation, ciphertext expansion, secret msg number, etc.
  - Side channel resistance
  - Distinctive security properties
  - ...

• AE design categories
  (nonce-based vs nonce misuse resistant, software, hardware, etc.)
Thank you!

Elena.Andreeeva@esat.kuleuven.be