Authenticated Encryption and the CAESAR Competition

Elena Andreeva
COSIC, KU Leuven, Belgium

ESC Workshop 2015
Clervaux, Luxembourg
12/01/2015
Main Question

How to achieve secure AE?

1. Combine Enc + MAC
   
   Generic composition:
   
   Bellare, Namprempre (2000), Namprempre et al. (2014)

2. Dedicated AE schemes ≈ Inbetweeners 😊
   
   State of the art
Towards Dedicated Schemes

1. **Generic AE composition**
   - + combines off the shelf primitives
   - - prone to implementation errors
   - - 2 data passes
   - - 2 keys

2. **Dedicated AE schemes**
   - nonce-based (randomness is not required)
Nonce-based AE

Alice

\[ E : C \leftarrow E_K(A, N, M) \]
\[ D : M/\bot \leftarrow D_K(A, N, C) \]
Correctness: \( D_K(A, N, E_K(A, N, M)) = M \)

Bob


Nonce dependent AE: Security fails when \( N \) repeats
Nonce MR AE: Provide security when \( N \) repeats
## Dedicated AE (Prior to CAESAR)

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Nonce dependent</th>
<th>Nonce MR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Block cipher</strong></td>
<td>IAPM*, OCB*, XECB*, CCM, GCM, OTR*, CLOC</td>
<td><strong>SIV</strong>, BTM, McOE-G, POET, COPA</td>
</tr>
<tr>
<td><strong>Permutation</strong></td>
<td>Sponge Wrap, Ketje&amp;Keyak, NORX</td>
<td><strong>APE</strong></td>
</tr>
</tbody>
</table>

*Green ISO/IEC 19772:2009 (NIST recommended: CCM, GCM)*  
*Blue part of the CAESAR competition (+OCB)*  
*hold a patent*
# AE Characteristics

<table>
<thead>
<tr>
<th>Security</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Nonce misuse resistant <strong>NMR</strong></td>
<td>+ Online</td>
</tr>
<tr>
<td>+ Secure against release of unverified plaintext <strong>RUP</strong></td>
<td>+ Parallelizable</td>
</tr>
<tr>
<td>+ Side-channel resistant</td>
<td>+ Inverse free</td>
</tr>
<tr>
<td></td>
<td>+ Low # data passes</td>
</tr>
<tr>
<td></td>
<td>+ Incrementality</td>
</tr>
<tr>
<td></td>
<td>+ Static AD</td>
</tr>
</tbody>
</table>

| **Underlying primitive?**                     |                                      |
| **Target security levels?**                   |                                      |
| **Target platform?**                          |                                      |
Nonce Misuse

- Flawed implementations
- Bad user management
- Backup reset of virtual machine clones

Not all security should be lost if N is misused!
1. MAX security up to $M$ repetitions
   SIV, BTM, HBS but **two passes over the data**

2. LCP security up to longest common prefix
   McOE-G, COPA, APE, POET
Release of Unverified Plaintext RUP
Andreeva et al. (2014)

- Insecure memory
- Small buffer
- Real-time requirements

Attacker gets ciphertext decryptions before verification completed!

(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)

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

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

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

Adversary can choose any nonce
RUP Integrity

- Int-RUP

Adversary can choose any nonce
# Release of Unverified Plaintext

**Andreeva et al. (2014)**

<table>
<thead>
<tr>
<th>Nonce</th>
<th>AE scheme</th>
<th>RUP confidentiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonce dependent</td>
<td>OCB, CCM, GCM, SpongeWrap</td>
<td>No</td>
</tr>
<tr>
<td>Nonce MR</td>
<td>COPA, McOE-G, APE, BTM, HBS</td>
<td>Yes</td>
</tr>
</tbody>
</table>
In Summary …

Multiple AE security and efficiency objectives
More analysis and trust in AE before deployment

Cryptographic competition
CAESAR

Competition for Authenticated Encryption: Security, Applicability, and Robustness

- Easy to use, secure and efficient AE
- Advantageous over AES-GCM and suitable for widespread adoption
CAESAR Comparison

- Properties dataviz by Xavier Dutoit

CAESAR Comparison

- Properties dataviz by Xavier Dutoit
  
CAESAR
Comparison and Categories

- Properties dataviz by Xavier Dutoit
  - Type (BC, Permutation, stream cipher, …)
  - Subtype (AES, AES-4, dedicated BC/permutation, …)
  - Parallelizable
  - Online
  - Inverse free
  - NMR
  - RUP
  - Analysis

Accurate comparison?
1. Designers/community validation of the basic properties
Properties dataviz by Xavier Dutoit ➔

https://mjos.fi/aead_feedback/

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

Categories (speculate 😊 …)

Target platforms and applications
hardware/software/low latency/lightweight/…

Security
high margin/NMR/RUP/side-channel/…
http://competitions.cr yp.to/caesar.html
Thank you!

Elena.Andreeeva@esat.kuleuven.be