Security Aspects of Authenticated Encryption

Elena Andreeva

COSIC, KU Leuven

Summer school on design and security of cryptographic algorithms and devices for real-world applications
Croatia, 05/06/2014
Authenticated Encryption AE
Generic AE composition
Dedicated AE schemes
  nonce-based AE
  nonce misuse resistant AE
Further challenges
Confidentiality
+
Authenticity
Ways to Build AE Schemes?

1. Generic **AE** composition off the shelf primitives
   - Symmetric **Authentication** (MAC)
   - +
   - Symmetric **Encryption**

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

3. Something in between 😊 (state of the art)
1. Ways of composing

- Enc then MAC: secure
- MAC then Enc: insecure
- Enc and MAC: insecure

_Caveat:_ Careful with interpretations!
Conventional Encryption

- **Enc** = (Kg, Enc, Dec)
  
  - **Key generation**: $K \leftarrow$ Kg
  - **Encryption**: $(st, C) \leftarrow$ $\text{Enc}^st_K(M)$ (randomized or stateful)
  - **Decryption**: $M \leftarrow \text{Dec}_K(st, C)$ (deterministic)

  **Correctness**: $\text{Dec}_K(\text{Enc}_K(M)) = M$

- **Indistinguishability**
  
  $\text{IND-CPA(CCA)}$

  ![Diagram](image)
MAC

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

  Key generation: K ← $\$ Kg
  Authentication: T ← MAC$_K$(M) (any)
  Verification: 1/0 ← Verify$_K$(M, T) (deterministic)

  Correctness: Verify$_K$(M, MAC$_K$(M)) = 1

- **Unforgeability** (weak M’ ≠ M; strong M’, T’ ≠ M, T)

```
M
\rightarrow T
\rightarrow MAC_K
\leftarrow M', T'
\rightarrow Verify_K
\leftarrow ?
Win if ? is 1
```
Generic Composition [BN’00]

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

AE secure: Enc then MAC

• Off the shelf schemes

Enc (CBC, CTR,...) + MAC (CBC-MAC, HMAC, PMAC,...)

Caveat: Careful with interpretations!

A. Enc often with badly or \textit{externally} generated random IV

B. IV should not be communicated out of band
### A: Random IV Encryption

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

  **Key generation:** \( K \leftarrow \$ \ Kg \)
  **Encryption:** \( IV, C \leftarrow Enc^P_K(M) \) (deterministic)
  **Decryption:** \( M \leftarrow Dec_K(IV, C) \) (deterministic)

  **Correctness:** \( Dec_K(Enc^P_K(M)) = M \)

- **Indistinguishability**

  **$IND$-CPA**

  ![Diagram]

  - **M**
  - **IV, C**
  - **M**
  - **Random bits**

  **Fix A:** Environment not Enc selects IV
  **B:** IV still in-band

  \( IV \leftarrow \$ IV, C \)
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: \( K \leftarrow \$ \text{Kg} \)
  - Encryption: \( C \leftarrow \text{Enc}_K(N, M) \) (deterministic)
  - Decryption: \( M \leftarrow \text{Dec}_K(N, C) \) (deterministic)
  - Correctness: \( \text{Dec}_K(N, \text{Enc}_K(M)) = M \)

- **Indistinguishability (nonce respecting adversary)**

  \( \text{IND-CPA} \)

  - Fix A: Adversary can select \( N \)
  - Fix B: out-of-band

  ![Diagram](image)
Build nonce-based AE from

1. IV-Enc + MAC

Efficiency issues: 2 passes over the data
Generic Composition Reconsidered [NRS’14]

• **Build nonce-based AE from**

2. N-Enc + MAC

• **Generic composition disadvantages**
  - Efficiency issues: 2 passes over the data
  - Prone to misuse with conventional Enc schemes
Outline

- Authenticated Encryption AE
- Generic AE composition
- Dedicated AE schemes
  - Nonce-based AE
  - Nonce misuse resistant AE
- Further challenges
# Dedicated AE: State of the Art

## 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>Block cipher</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>Permutation</td>
<td>SpongeWrap’11, Ketje&amp;Keyak’14, NORX’14</td>
<td>APE’14</td>
</tr>
</tbody>
</table>

* hold a patent
Nonce-based AE

- \( \text{AE} = (K_g, E, D) \)

Key generation: \( K \leftarrow \$ K_g \)
Encryption: \( C \leftarrow E_K(A, N, M) \) (deterministic)
Decryption: \( M/\bot \leftarrow D_K(A, N, C) \) (deterministic)

Correctness: \( D_K(A, N, E_K(A, N, M)) = M \)

- AE confidentiality + AE integrity = AE security
AE Confidentiality

- $\text{IND-CPA}$

Adversary is nonce respecting
AE Integrity

- **INT-CTX**

```
N, A, M

E_K

C

D_K

C' ≠ C

? ≠ ⊥

Win if ? is M ≠ ⊥
```

Adversary maybe nonce respecting
Nonce-based AE Security

Adversary is nonce respecting
Example: OCB [RBBK’01]

\[ \alpha_i = f_i(K,N) \]
\[ \beta_i = g_i(K,N) \]
Outline

- Authenticated Encryption AE
- Generic AE composition
- Dedicated AE schemes
  - Nonce-based AE
    - Nonce misuse resistant AE
- Further challenges
Not all security should be lost if N misused!
Distinct Nonces

$N_1 \quad M_1 \quad \text{OCB} \quad C_1$

$N_2 \quad M_1 \quad \text{OCB} \quad C_2$

$N_3 \quad M_2 \quad \text{OCB} \quad C_3$
What security can be lost?

- Valid for all nonce respecting AE schemes
What else can be lost?

**Nonce Misuse OCB**

**Ciphertext Block Repetitions**

\[ \begin{align*}
\alpha_1 & \rightarrow \text{AES}_K \rightarrow C_1 \\
\alpha_2 & \rightarrow \text{AES}_K \rightarrow C_2 \\
\cdots & \rightarrow \cdots \\
\alpha_d & \rightarrow \text{AES}_K \rightarrow C_d
\end{align*} \]
What else can be lost? (OCB looses confidentiality)

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

\[
\begin{align*}
&\text{OCB-Enc} \\
&\quad M'_1 \quad M_2 \quad \ldots \quad M_d \\
&\quad \alpha_1 \quad \alpha_2 \quad \ldots \quad \alpha_d \\
&\quad \text{AES}_K \quad \text{AES}_K \quad \text{AES}_K \\
&\quad C'_1 \quad C_2 \quad \ldots \quad C_d
\end{align*}
\]
What to Do against Nonce Misuse?

Not all security should be lost if N misused!

1. Security up to common prefixes
   ciphertext leaks only presence of common M prefixes
   McOE-G, COPA, APE, COBRA, POET

2. Security up to repetitions
   ciphertext leaks only presence of repeating Ms
   SIV, BTM, HBS but two passes over the data
Nonce Misuse Resistance via Online Ciphers

- Online cipher + authentication [BBKN‘01, FFLW’12]

nonce misuse resistant $nmr$ AE scheme secure up to common prefix repetitions
Regular vs Online Ciphers

• Normally in a cipher

\[ m_1 \rightarrow c_1 \quad m_2 \rightarrow c_2 \quad m_3 \rightarrow c_3 \quad m_4 \rightarrow c_4 \]

• Online cipher

- more efficient
- different security (IND from random online permutation)
L = \( E_K(0) \)

\( \alpha_0 = 3L \) and \( \alpha_1 = 2L \)

\( \beta_1 = 2^{d-1} \cdot 3^2L \) and \( \beta_2 = 2^{d-1} \cdot 7L \)
If $E$ is SPRP, COPA is AE secure up to $2^{n/2}$ queries.
Outline

- Authenticated Encryption AE
- Generic AE composition
- Dedicated AE schemes
  - Nonce-based AE
  - Nonce misuse resistant AE
- Further challenges
Further Security Pitfalls in AE

What if attacker gets C decryptions before verification completed?

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

- **Scenarios**
  - Insufficient memory
  - 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

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

Adversary can choose any nonce
RUP Integrity

• Int-RUP

Adversary can choose any nonce
## Security of AE Schemes under RUP

<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, SpongeWrap</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?
Thank you!