1) Move the coins out of $\mathcal{E}$ — make it deterministic [RBBK01]

To improve resistance to random-number generation problems
To architect to existing abstraction boundaries

2) Add in “associated data” (AD) [R02]

To authenticate headers

**Syntax:** An AEAD scheme is a 3-tuple $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where
- $\mathcal{K}$ is a probabilistic algorithm that returns a string;
- $\mathcal{E}$ is a deterministic algorithm that maps a tuple $(K, N, A, M)$ to a ciphertext $C = \mathcal{E}(K, N, A, M)$ of length $|M| + \tau$; and
- $\mathcal{D}$ is a deterministic algorithm that maps a tuple $(K, N, A, C)$ to a plaintext $M$ or the symbol $\bot$

If $C = \mathcal{E}(K, N, A, M) \neq \bot$ then $\mathcal{D}(K, N, A, C) = M$
\[ \text{Adv}^{\text{aead}}_\mathcal{E}(\mathcal{A}) = \Pr[\mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K} \rightarrow 1] - \Pr[\mathcal{A}^{\$, \bot} \rightarrow 1] \]

\(\mathcal{A}\) may not:
- Repeat an \(N\) in an enc query
- Ask a dec query \((N, A, C)\) after \(C\) is returned by an \((N, A, \cdot)\) enc query
\( \text{Adv}^\text{priv}_\mathcal{E}(\mathcal{A}) = \Pr[\mathcal{A}^{\mathcal{E}_K} \rightarrow 1] - \Pr[\mathcal{A}^{\$} \rightarrow 1] \)

\( \mathcal{A} \) may not:

- Ask a dec query \((N, A, C)\) after \(C\) is returned by an \((N, A, \cdot)\) enc query
\[ \text{Adv}_\mathcal{E} (A) = \Pr[A \text{ forges}] \]

It outputs an \((N^*, A^*, C^*)\) where \(D(K, N^*, A^*, C^*) \neq \perp\) and no prior oracle query of \((N^*, A^*, M)\) returned \(C^*\)
All-in-one definition

\[ \text{Adv}^{\text{aead}}(A) = \Pr[A^{\mathcal{E}(K, \cdots), \mathcal{D}(K, \cdots)} \Rightarrow 1] - \Pr[A^{\mathcal{E}(\cdots), \bot} \Rightarrow 1] \]

A may not repeat any \( N \) query to its Enc oracle. It may not ask Dec\((N, A, C)\) after an Enc\((N, A, M)\) returned \( C \).

Two-part definition

\[ \text{Adv}^{\text{priv}}(A) = \Pr[A^{\mathcal{E}(K, \cdots)} \Rightarrow 1] - \Pr[A^{\mathcal{E}(\cdots)} \Rightarrow 1] \]

A may not repeat any \( N \) query.

\[ \text{Adv}^{\text{auth}}(A) = \Pr[A^{\mathcal{E}(K, \cdots)} \text{ forges}] \]

It outputs an \((N, A, C)\) where \( \mathcal{D}(K, N, A, C) \neq \bot \) and no prior oracle query of \((N, A, M)\) returned \( C \).
Generic composition

Encrypt-and-MAC

MAC-then-Encrypt

Encrypt-then-MAC

[Bellare, Namprempre 2000]
**SIV mode**
[Rogaway, Shrimpton 2006]

PRF operating on a vector of strings

ivE encryption scheme (eg, CTR), secure
AES-GCM-SIV

$K$ → DeriveKey → $K_1$ → POLYVAL Hash → $S$

$N$ → $R_{64}(AES_K(N \ 0))$ → $R_{64}(AES_K(N \ 1))$ → $K_1$

$R_{64}(AES_K(N \ 2))$ → $K_2$ → AES → $T$

$0$ → $R_{127}(S)$ → $\oplus$ → $0$ → $N$

Additions: no carry out of last 32 bits

Close to GHASH but adjusted to better match AES-NI: $\sum \alpha_i M_i K_1^i$
Thm [Jonsson 2002]  CCM is provably secure if $E$ is a good PRP.
**GCM**

[McGrew, Viega 2004]

(Follows CWC

[Kohno, Viega, Whiting 2004])

NIST SP 800-38D:2007

RFC 4106, 5084, 5116, 5288, 5647

ISO 19772:2009

---

**Thm** [Iwata, Ohashi, and Minematsu 2012] (correcting [McGrew, Viega 2004])

**GCM is provably secure (not great bounds) if** $E$ **is a good PRP.**
OCB (v3) [Krovetz Rogaway 2011], following [RBBK01,LRW02,R04] RFC 7253

Thm [Krovetz, Rogaway 2011]

OCB is provably secure (OK bounds) if $E$ is a strong PRP.
Tweakable Blockcipher (TBC)

\[ \tilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \rightarrow \{0,1\}^n \]

each \( \tilde{E}_K^T(\cdot) = \tilde{E}(K, T, \cdot) \) a permutation

\[ \text{Adv}^{\text{prp}}_{\tilde{E}}(A) = \Pr[A \tilde{E}_K \Rightarrow 1] - \Pr[A \pi \Rightarrow 1] \]

A \( \mathcal{T} \)-indexed family of random permutations on \( n \) bits
This is the official public announcement of the portfolio, bringing the CAESAR competition to a close. ... [H]ere is the final portfolio:

Use case 1: Ascon first choice, ACORN second choice.
Use case 2: AEGIS-128 and OCB, without a preference.
Use case 3: Deoxys-II first choice, COLM second choice.

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>57 round-1</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Mar 2014</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>29 round-2</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Mar 2014</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>16 round-3</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Aug 2016</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>7 finalists</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Mar 2018</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>6 winners</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Feb 209</strong></td>
</tr>
</tbody>
</table>
Deoxys-II
Jean, Nikolić, Peyrin, Seurin

Thm: Provably secure, with excellent bounds, if $E$ is a TBC.
The fastest CAESAR finalist on recent Intel processors

0.43 cpb (Skylake)
(0.25 cpb for AEGIS-128L on 16K messages)

AEGIS
AEGIS-128
[Wu, Preneel 2013]