Pipeline Implementation of ELmD, COPA and OTR

Cuauhtemoc Mancillas López and Lilian Bossuet

Hubert Curien Laboratory UMR CNRS 5516, Jean Monnet University, Saint-Etienne, France.

CAESAR Competition

Competition for Authenticated Encryption: Security, Applicability, and Robustness

- The CAESAR selection committee will select a portfolio of algorithms.
- Would be separate portfolios for software, hardware and lightweight.
- The process is like eStream competition for Stream Ciphers.

Submissions

- Based on Block Ciphers.
- Based on Stream Ciphers.
- Specific Constructions.
- Based on Sponge Functions.

Preliminaries

ELmD, COPA and OTR

Implementations

Results and Conclusions

Finite Fields

We shall often treat n bit binary strings as elements of $GF(2^n)$.

Elements in $\{0,1\}^n$ can be seen as polynomials of the form

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}.$$

Finite Fields

We shall often treat n bit binary strings as elements of $GF(2^n)$.

Elements in $\{0,1\}^n$ can be seen as polynomials of the form

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}.$$

For $X, Y \in \{0,1\}^n$,

- Addition in the field: $X \oplus Y$, realized by bitwise xor.
- Multiplication: XY, realized by ordinary polynomial multiplication followed by reduction using a fixed n degree irreducible polynomial.

Finite Fields

An important operation on finite fields is *xtimes*.

For $L \in GF(2^n)$, by xA or $2 \cdot L$, we mean the multiplication of the monomial x with the polynomial A followed by a reduction using the irreducible polynomial.

This does not amount to a multiplication, can be easily done using a shift and a conditional xor.

Block-Ciphers

Definition

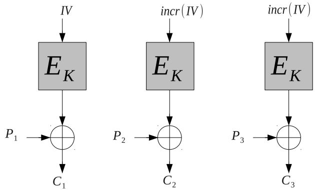
- Let n be the block length then the block cipher can be seen as a function
$$E : \{0,1\}^n \times \boldsymbol{K} \rightarrow \{0,1\}^n$$
- Denoted by $E(K, M) = E_K(M)$.
- For each K, E_K must be a permutation. So, each $E_K()$ has an inverse such that
$$D_K(E_K(M)) = M$$
- A secure block cipher is considered to be a **Strong Pseudo Random Permutation (SPRP).**

Block ciphers can encrypt only messages if n-bit size

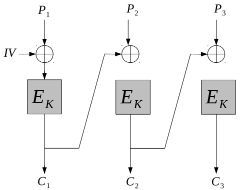
Modes of Operation

- Privacy Only.
- Message Authentication Codes (MAC).
- Authenticated Encryption (with Associated Data).
- Tweakable Enciphering Schemes
- On-line Ciphers.

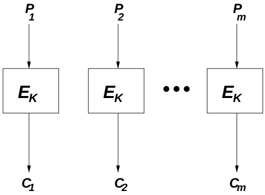
Classical Modes of Operation



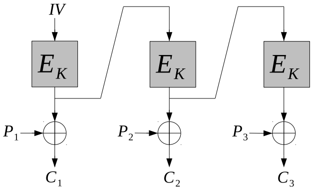
Counter ($IV = Nonce||counter$)



CBC



ECB



OFB

Authenticated Encryption with Associated Data

Definition

A AEAD is a function $\Psi = \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \rightarrow \mathcal{M} \times \mathcal{T}$

- $\mathcal{K}$ is key space, $\mathcal{N}$ nonce space, $\mathcal{T}$ tag space, $\mathcal{M}$ is message space and $\mathcal{H}$ is the associated data space.
- They provide authentication and privacy.
- Authentication is on message and associated data.
- They are not length preserving. Ciphertext is a pair C, τ where τ is a tag for authentication.

Security of Authenticated Encryption

Let's Ψ be a AE, it offers privacy:

$$\mathbf{Adv}_{\Psi}^{AE-priv}(\mathcal{A}) = \left| \Pr\left[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\Psi_K(\cdot,\cdot)} \Rightarrow 1 \right] - \Pr\left[\mathcal{A}^{\$(\cdot,\cdot)} \Rightarrow 1 \right] \right|$$

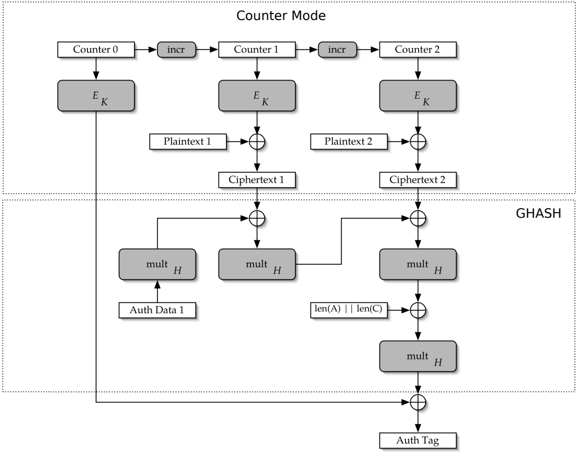
DAE is secure when $\mathbf{Adv}_{\Psi}^{DAE-priv}(\mathcal{A})$ is small for all efficient adversaries. It offers authentication:

$$\mathbf{Adv}_{\Psi}^{AE-auth}(\mathcal{A}) = \Pr[\mathcal{A}^{\Psi_K(\cdot,\cdot,\cdot)} \text{ forges }]$$

If $\mathbf{Adv}_{\Psi}^{DAE-auth}(\mathcal{A})$ is small, this signify that it must be hard for an adversary to create a valid ciphertext.

General Constructions

Combining an IV-based encryption scheme and a Message Authentication Code:



Galois Counter Mode

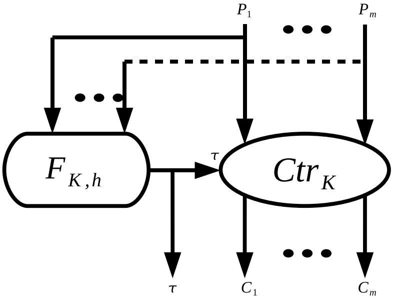
Parallelizable, Pipelineable.

IV misuse

- It must be different for each message.
- Unpredictable.
- Implementers and protocol designers often supply an incorrect IV: constant or counter.
- Privacy fails when IV is repeated.
- Maintain IV is a hard task.

IV misuse-resistant

Deterministic Authenticated Encryption (Rogaway and Srimpton 2006)



General structure

Two passes construction. For example *SIV*.

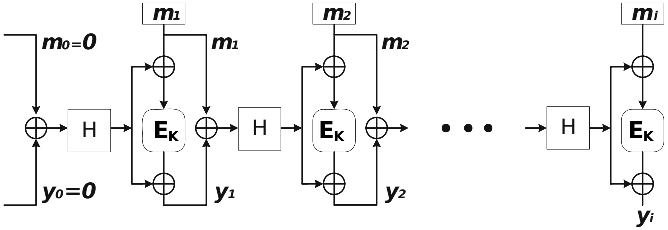
Something in Between

On-line cipher

$$\mathcal{E} : \mathcal{K} \times (\{0,1\}^n)^+ \to (\{0,1\}^n)^+$$

- It is a permutation on every block of n bits.
- Its output is same for a common prefix. The first $|M|$ bits of $\mathcal{E}_K(M \| N)$ and $\mathcal{E}_K(M \| N')$ are the same.

On-line Encryption



MHCBC (Nandi, 2008)

H is an AXU-Function

We implemented three constructions submitted to CAESAR.

- On-line
  - COPA (Andreeva, 2014)
  - ELmD (Datta and Nandi, 2014)
- IV-Based:
  - OTR (Minematsu, 2014)

Why

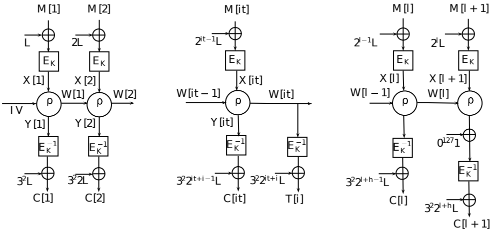
We implemented three constructions submitted to CAESAR.

- On-line
  - COPA (Andreeva, 2014)
  - ELmD (Datta and Nandi, 2014)
- IV-Based:
  - OTR (Minematsu, 2014)

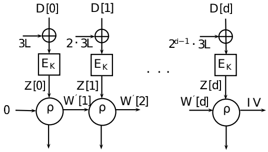
Why

- Pipelineable
- High speed applications

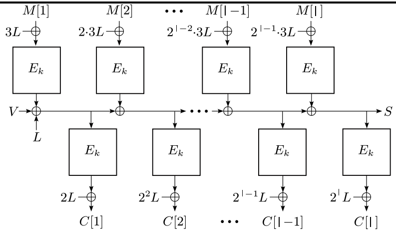
ELmD and COPA



ELmD

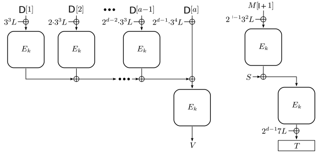


Associated Data



1101

COPA

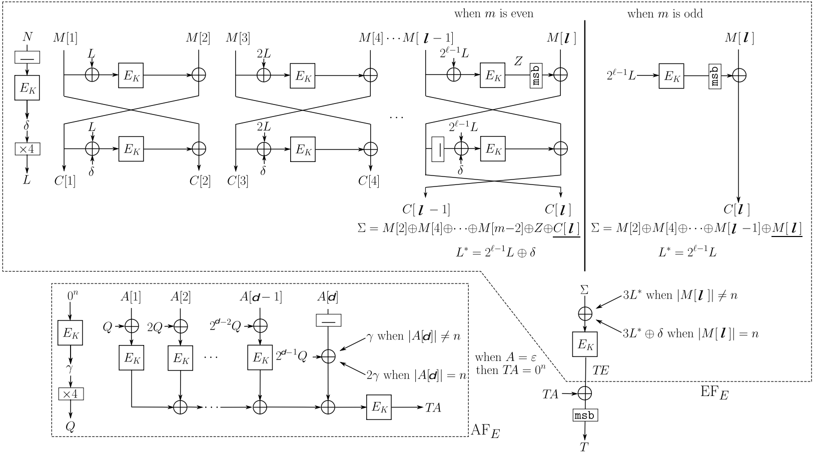


Associated Data

Where $L = E_K(0)$ and $M[l+1] = M[1] \oplus M[2] \oplus ... \oplus M[l]$.

ρ is defined as: $Y[i], W[i] \leftarrow X[i] \oplus 3 \cdot W[i-1], x \oplus 2 \cdot W[i-1]$

OTR

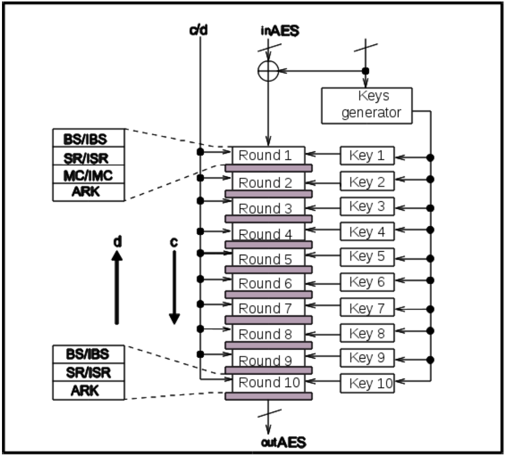


when m is even
when m is odd
N
$M[1]$
$M[2]$
$M[3]$
$M[4] \cdots M[\ell - 1]$
$M[\ell]$
L
$2L$
$2^{\ell-1}L$
Z
E_K
msb
δ
$\times 4$
$C[1]$
$C[2]$
$C[3]$
$C[4]$
$C[\ell - 1]$
$C[\ell]$
$\Sigma = M[2] \oplus M[4] \oplus \cdots \oplus M[m-2] \oplus Z \oplus C[\ell]$
$L^* = 2^{\ell-1}L \oplus \delta$
$\Sigma = M[2] \oplus M[4] \oplus \cdots \oplus M[\ell - 1] \oplus M[\ell]$
$L^* = 2^{\ell-1}L$
0^n
$A[1]$
$A[2]$
$A[d-1]$
$A[d]$
Q
$2Q$
$2^{d-2}Q$
$2^{d-1}Q$
γ when $|A[d]| \neq n$
2γ when $|A[d]| = n$
TA
AF_E
when $A = \varepsilon$
then $TA = 0^n$
Σ
$3L^*$ when $|M[\ell]| \neq n$
$3L^* \oplus \delta$ when $|M[\ell]| = n$
TE
EF_E
T

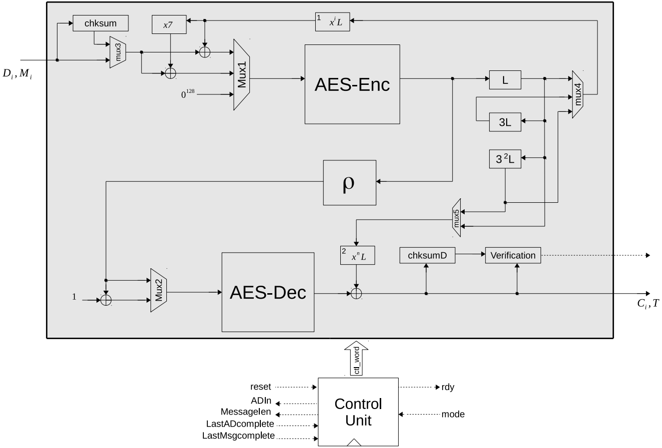
Design Decisions

- Design optimized for FPGAs with 6 input LUTS (Virtex 5, Spartan 6, etc).
- Use separated AES-Encryption and AES-Decryption cores.
- Optimize for speed.

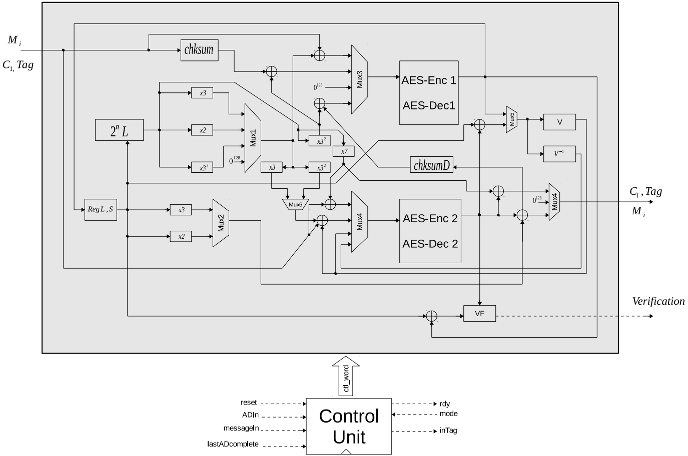
AES architecture



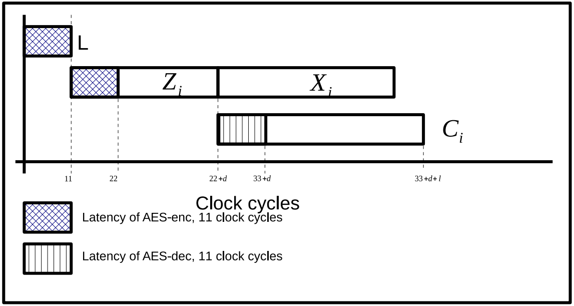
Hardware Architecture for ELmD



Hardware Architecture for COPA



Operations in the time for ELmD



Results

Mode	**Area Slices**	**Frequency (MHz)**	**Latency clock cycles**	Throughput
ELmD	5225	234.64	$35 + \#D$	30.03
COPA	10391	230.87	$61 + \#D$	29.55
OTR	4925	296.28	$25 + \#D$	37.92
AES-GCM* Virtex 5	4770	311	-	36.92
AES pipelined encryption	2190	315.56	10	40.39
AES pipelined decryption	2360	239.34	10	30.63

*Abdellatif et al. 2014.

Conclusions

- ELmD saves almost 50% of logic resources used in comparison with COPA.
- OTR is competitive with GCM.
- ELmD and COPA use more resources than GCM, but the security that they offer is stronger.
- There are more possibilities to exploit the parallel and pipeline properties of these algorithms.

Thanks for your attention

Questions?