Insecurity on XLS and Forging Algorithm on the Mode COPA

Mridul Nandi

Indian Statistical Institute, Kolkata

mridul@isical.ac.in

August 23, 2014
DIAC, UCSB

Introduction and Overview.

1. Domain Extension and domain completion.
2. Briefly study XLS and COPA.
3. We have demonstrated a SPRP distinguisher for XLS which violates the claim in FSE 2007.
4. We extend this attack for the mode COPA.
5. We propose some alternative secure as well as efficient methods for domain completions.

Domain Extension and Completion

Domain Extension

- Using n-bit blockcipher constructing encryption over larger message sizes.
- Easy to define messages of size multiple of n (e.g., EME, HCBC, MHCBC etc.).
- Padding may be applied for AE but would not simply work for enciphering.

Domain Completion

- A generic method to make the domain complete (i.e., any message size).
- So far only two methods are known. (1) XLS (proposed by Ristenpart and Rogaway in FSE 2007) and (2) Nandi's construction in CyS 2009.
- Cook et. al proposed for domain completion for smaller sizes.

XLS

- Proposed by Ristenpart and Rogaway in FSE 2007.
- A Method of length-preserving encryption (or enciphering) for arbitrary message length.
- It requires an enciphering scheme $\mathcal{E}$ over $(\{0,1\}^n)^+$ and a blockcipher E.
- Replacing $\mathcal{E}$ by a blockcipher, XLS becomes an enciphering scheme over $\cup_{i=n}^{2n-1}\{0,1\}^i$.
- Used in Authenticated Encryption.

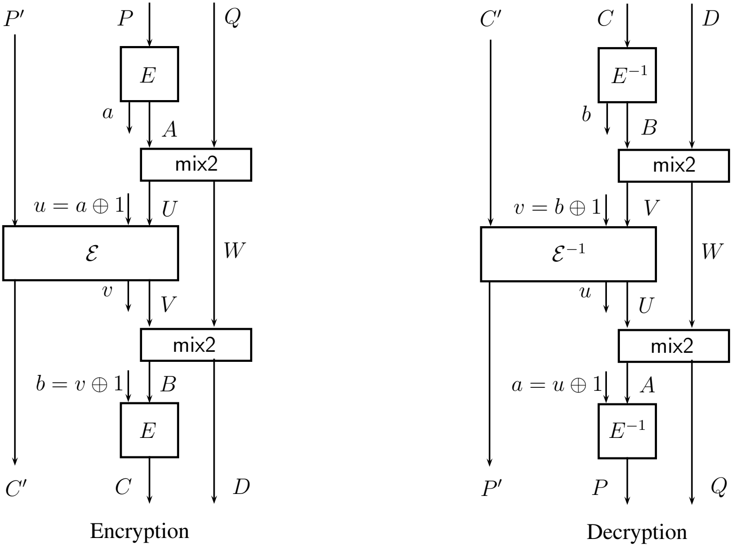
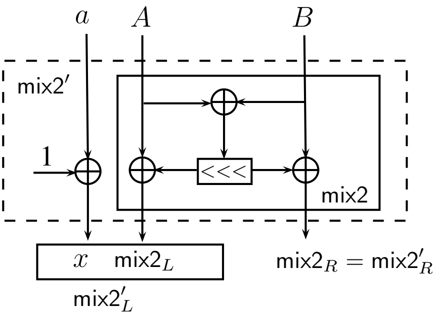

P'
P
Q
E
a
A
mix2
$u = a \oplus 1$
U
$\mathcal{E}$
W
v
V
mix2
$b = v \oplus 1$
B
E
C'
C
D
Encryption
C'
C
D
E^{-1}
b
B
mix2
$v = b \oplus 1$
V
$\mathcal{E}^{-1}$
W
u
U
mix2
$a = u \oplus 1$
A
E^{-1}
P'
P
Q
Decryption

Figure of mix2

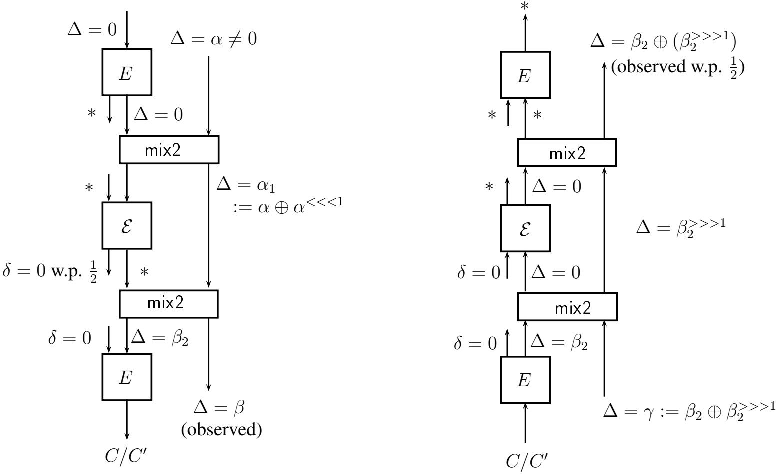


1. mix2 is defined as

$$\text{mix2}(A, B) = (A \oplus (A \oplus B)^{\lll}, B \oplus (A \oplus B)^{\lll}).$$

2. Note that mix2 is linear and hence difference propagate with probability one.
3. mix2 is inverse of itself.

CPCA Distinguisher of XLS for $2n - 1$ bit messages



Encryption Query 1 and 2

Decryption Query 1 and 2

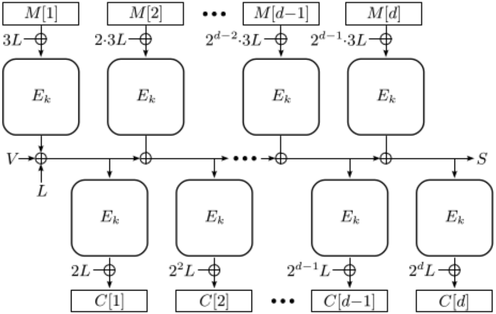
CPCA Distinguisher of XLS for $2n - 1$ bit messages

Distinguishing Algorithm $\mathcal{A}_0$ for XLS with message sizes $2n - 1$.

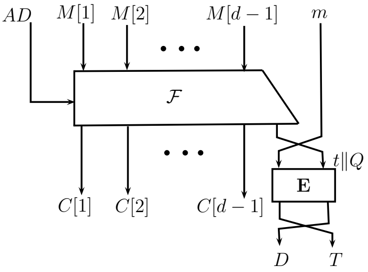
1. **query-1**. It makes an encryption query $(P, Q) \in \{0,1\}^n \times \{0,1\}^{n-1}$.
2. Let $(C, D) \in \{0,1\}^n \times \{0,1\}^{n-1}$ be its response.
3. Fix a non-zero bit string α of size $n - 1$.
4. **query-2**. It makes an encryption query $(P, Q' := Q \oplus \alpha)$ and obtains response (C', D').
5. Let $\beta = D \oplus D'$ and set $\gamma = \alpha \oplus \beta \oplus ((\alpha \oplus \beta) >> 2)$.
6. **query-3**. It makes a decryption query (C, D_1) and obtains response (P_1, Q_1) where
7. **query-4**. It makes a decryption query $(C', D_1' := D_1 \oplus \gamma)$ and obtains response (P_1', Q_1').
8. **if** $Q_1' = Q_1 \oplus \gamma$ **returns** 1, **else** 0.

Description of COPA for complete last block message

1. V is generated from associated data in a similar fashion.
2. $M[d] = \oplus_{i=1}^{d-1} M[i]$.



Description of COPA for other messages



- m is the partial block message.
- $\mathcal{F}$ represents COPA for complete block messages.
- **E** is the XLS when $\mathcal{E}$ is replaced by blockcipher.

Forging Algorithm on COPA

Forgery Algorithm $\mathcal{A}_1$.

1. Make queries $M_i \in \{0,1\}^n$ and obtains response $(C_i, t'_i \| Q_i)$ where $|t'_i| = 1$, $1 \leq i \leq q$.
2. Find b (assume $b = 0$), $|I| = |\{i : t'_i = b\}| \geq q/2$. $I = I_1 \sqcup I_2$, $|I_1| = |I_2|$.
3. Make queries (M_i, m), $i \in I$, $m \in \{0,1\}^{n-1}$ and obtains responses $((C_i, D_i), T_i)$.
4. Find $i \in I_1, j \in I_2, k \in I$ s.t.

$$Q_k = \left(\mathbf{R}^{-2}(D_i + Q_i)\right) + \left(D_j + (\mathbf{I} + \mathbf{R}^{-2})(Q_j + D_j)\right),$$

   otherwise abort.

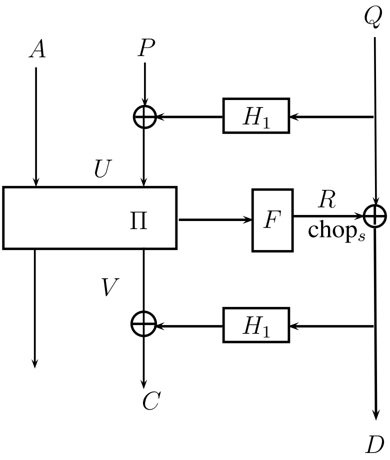
5. Return forgery query (C_k, D^*, T_j) where

$$D^* = D_j + (\mathbf{I} + \mathbf{R}^{-2})(D_i + Q_i + D_j + Q_j).$$

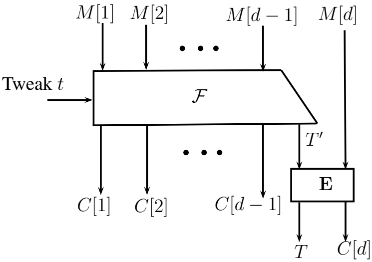
Forging Algorithm on COPA

- It requires about $2^{n/3}$ queries.
- The attacks is reduced to generalized birthday attack for $k = 3$. In other words, finding three elements $x \in l_1, y \in l_2$ and $z \in l$ from three lists such that $x \oplus y \oplus z = 0$.
- No known algorithm with time complexity less than $2^{n/2}$.
- Success probability is about $1/2$.
- It works for other COPA like constructions.

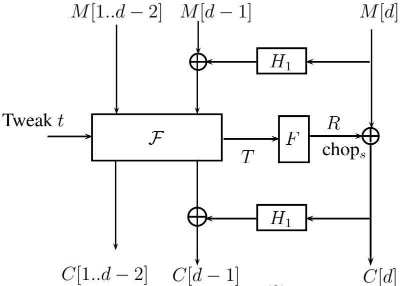
Nandi's CyS'09 Construction.



New Methods of domain completion of AE.



(1)



(2)

Conclusion.

1. We have demonstrated a SPRP distinguisher for XLS which violates the claim in FSE 2007.
2. We extend this attack for those AE which use it, e.g., COPA.
3. We propose some alternative secure as well as efficient methods for domain completions.

The End