

A forgery attack on AES-OTR

Hassan Sadeghi, Javad Alizadeh

November 7, 2014

Abstract

AES-OTR is a submission to the CAESAR competition. In this note we present a forgery attack on AES-OTR

Keywords: AES-OTR, Forgery attack.

1 Introduction

OTR is a blockcipher mode of operation to authenticated encryption with associated data (AEAD), proposed by Minematsu [1][2]. AES-OTR is based on AES blockcipher .

2 Algorithms in AES-OTR

The encryption algorithm of AES-OTR using blockcipher (here AES) E , tag bit length τ . Both algorithms take the following byte sequences: a key K , a nonce N , an associated data A and a plaintext M . The output is a pair (C, T) where C is a ciphertext and T is a tag. For encryption, we first partition a plaintext M into n -bit blocks, i.e. $(M[1], \dots, M[m]) \leftarrow M$ where $|M[i]| = n, i = 1, \dots, m$ then $(M[2i-1], M[2i])$ is encrypted by a two-round Feistel permutation with masks as

$$C[2i-1] = E_K(2^{i-1}L \oplus M[2i-1]) \oplus M[2i], \quad (1)$$

$$C[2i] = E_K(2^{i-1}L \oplus \delta \oplus C[2i-1]) \oplus M[2i-1]. \quad (2)$$

where $\delta = E_K(\underline{N})$ and $L = 4\delta$.

The algorithms of encryption and decryption are described in Fig1

3 Forgery attack on AES-OTR

In this section we present an adversary that it can forge OTR by observations. First adversary outputs plaintext $M = M[1] || M[2] || \dots || M[m]$ where m is odd and

$$|M[i]| = n, \quad 1 \leq i \leq m$$

Algorithm OTR- $\mathcal{E}_{E,\tau,p}(N, A, M)$

1. $(C, TE) \leftarrow \text{EF}_E(N, M)$
2. **if** $A \neq \varepsilon$ **then** $TA \leftarrow \text{AF}_E(A)$
3. **else** $TA \leftarrow 0^n$
4. $T \leftarrow \text{msb}_\tau(TE \oplus TA)$
5. **return** (C, T)

Algorithm OTR- $\mathcal{D}_{E,\tau,p}(N, A, C, T)$

1. $(M, TE) \leftarrow \text{DF}_E(N, C)$
2. **if** $A \neq \varepsilon$ **then** $TA \leftarrow \text{AF}_E(A)$
3. **else** $TA \leftarrow 0^n$
4. $\hat{T} \leftarrow \text{msb}_\tau(TE \oplus TA)$
5. **if** $\hat{T} = T$ **return** M
6. **else return** \perp

Algorithm $\text{EF}_E(N, M)$

1. $\Sigma \leftarrow 0^n$
2. $\delta \leftarrow E(\underline{N}), L \leftarrow 4\delta$
3. $(M[1], \dots, M[m]) \stackrel{\leftarrow}{\leftarrow} M$
4. **for** $i = 1$ **to** $\lceil m/2 \rceil - 1$ **do**
5. $C[2i-1] \leftarrow E(L \oplus M[2i-1]) \oplus M[2i]$
6. $C[2i] \leftarrow E(L \oplus \delta \oplus C[2i-1]) \oplus M[2i-1]$
7. $\Sigma \leftarrow \Sigma \oplus M[2i]$
8. $L \leftarrow 2L$
9. **if** m **is even**
10. $L^* \leftarrow L \oplus \delta$
11. $Z \leftarrow E(L \oplus M[m-1])$
12. $C[m] \leftarrow \text{msb}_{|M[m]|}(Z) \oplus M[m]$
13. $C[m-1] \leftarrow E(L^* \oplus C[m]) \oplus M[m-1]$
14. $\Sigma \leftarrow \Sigma \oplus Z \oplus C[m]$
15. **if** m **is odd**
16. $L^* \leftarrow L$
17. $C[m] \leftarrow \text{msb}_{|M[m]|}(E(L^*)) \oplus M[m]$
18. $\Sigma \leftarrow \Sigma \oplus M[m]$
19. **if** $|M[m]| \neq n$ **then** $TE \leftarrow E(3L^* \oplus \Sigma)$
20. **else** $TE \leftarrow E(3L^* \oplus \delta \oplus \Sigma)$
21. $C \leftarrow (C[1], \dots, C[m])$
22. **return** (C, TE)

Algorithm $\text{DF}_E(N, C)$

1. $\Sigma \leftarrow 0^n$
2. $\delta \leftarrow E(\underline{N}), L \leftarrow 4\delta$
3. $(C[1], \dots, C[m]) \stackrel{\leftarrow}{\leftarrow} C$
4. **for** $i = 1$ **to** $\lceil m/2 \rceil - 1$ **do**
5. $M[2i-1] \leftarrow E(L \oplus \delta \oplus C[2i-1]) \oplus C[2i]$
6. $M[2i] \leftarrow E(L \oplus M[2i-1]) \oplus C[2i-1]$
7. $\Sigma \leftarrow \Sigma \oplus M[2i]$
8. $L \leftarrow 2L$
9. **if** m **is even**
10. $L^* \leftarrow L \oplus \delta$
11. $M[m-1] \leftarrow E(L^* \oplus C[m]) \oplus C[m-1]$
12. $Z \leftarrow E(L \oplus M[m-1])$
13. $M[m] \leftarrow \text{msb}_{|C[m]|}(Z) \oplus C[m]$
14. $\Sigma \leftarrow \Sigma \oplus Z \oplus C[m]$
15. **if** m **is odd**
16. $L^* \leftarrow L$
17. $M[m] \leftarrow \text{msb}_{|C[m]|}(E(L^*)) \oplus C[m]$
18. $\Sigma \leftarrow \Sigma \oplus M[m]$
19. **if** $|C[m]| \neq n$ **then** $TE \leftarrow E(3L^* \oplus \Sigma)$
20. **else** $TE \leftarrow E(3L^* \oplus \delta \oplus \Sigma)$
21. $M \leftarrow (M[1], \dots, M[m])$
22. **return** (M, TE)

Algorithm $\text{AF}_E(A)$

1. $\Xi \leftarrow 0^n$
2. $\gamma \leftarrow E(0^n), Q \leftarrow 4\gamma$
3. $(A[1], \dots, A[a]) \stackrel{\leftarrow}{\leftarrow} A$
4. **for** $i = 1$ **to** $a-1$ **do**
5. $\Xi \leftarrow \Xi \oplus E(Q \oplus A[i])$
6. $Q \leftarrow 2Q$
7. $\Xi \leftarrow \Xi \oplus A[a]$
8. **if** $|A[a]| \neq n$ **then** $TA \leftarrow E(Q \oplus \gamma \oplus \Xi)$
9. **else** $TA \leftarrow E(Q \oplus 2\gamma \oplus \Xi)$
10. **return** TA

Fig. 1 Algorithms of AES-OTR with parallel ADP. Tag bit size is $0 < \tau \leq n$, and \underline{X} denotes the 10^* padding of X

We (privately) choose a key K and a nonce N then we give adversary a pair $(C[1] || C[2] || \dots || C[m], T)$ where

$$(C[1] || C[2] || \dots || C[m], T) = OTR - \xi_{E,\tau}(N, \varepsilon, M)$$

Adversary examines pair $(C[1] || C[2] || \dots || C[m], T)$ in five distinct cases:

Case1: There exists a number $i \in \{1, 2, \dots, \frac{m-1}{2}\}$ such that:

$$C[2i-1] \oplus M[2i] = C[2i] \oplus M[2i-1] \quad (3)$$

By (1) and (2) we conclude

$$\delta = M[2i-1] \oplus C[2i-1] \quad (4)$$

Adversary chooses M^* such that

$$\begin{aligned} |M^*| &< n, \\ \text{pad}(M^*) &= M[m] \oplus \delta = M[m] \oplus M[2i-1] \oplus C[2i-1] \end{aligned}$$

and puts $C^* := \text{msb}_{|M^*|}(C[m] \oplus M[m]) \oplus M^*$. Adversary claims that pair

$$(C[1] || C[2] || \dots || C[m-1] || C^*, T)$$

is a valid $(\text{Ciphertext}, \text{Tag})$ and it decrypted to

$$M[1] || M[2] || \dots || M[m-1] || M^*$$

Case2: There exist two number $i, j \in \{1, 2, \dots, \frac{m-1}{2}\}$ such that:

$$C[2i] \oplus M[2i-1] = C[2j] \oplus M[2j-1]$$

By (2) we conclude

$$2^{i-1}L \oplus C[2i-1] = 2^{j-1}L \oplus C[2j-1]$$

So we have

$$2^{i-1}L \oplus M[2i-1] = 2^{j-1}L \oplus C[2j-1] \oplus M[2i-1] \oplus C[2i-1] \quad (5)$$

By (1) and (5) we conclude

$$C[2i-1] \oplus M[2i] = E_K(2^{j-1}L \oplus C[2j-1] \oplus M[2i-1] \oplus C[2i-1]) \quad (6)$$

Adversary chooses $\{\tilde{M}[k] \mid 1 \leq k \leq m\}$ and $\{\tilde{C}[k] \mid 1 \leq k \leq m\}$ as follow:

$$\tilde{M}[k] = \begin{cases} C[2j-1] \oplus M[2i-1] \oplus C[2i-1] & \text{if } k = 2j-1 \\ C[2i-1] \oplus M[2i] \oplus C[2j-1] & \text{if } k = 2j \\ M[m] \oplus M[2j] \oplus C[2i-1] \oplus M[2i] \oplus C[2j-1] & \text{if } k = m \\ M[k] & \text{if } k \notin \{2j-1, 2j, m\} \end{cases}$$

$$\tilde{C}[k] = \begin{cases} C[2j] \oplus M[2j-1] \oplus C[2j-1] \oplus M[2i-1] \oplus C[2i-1] & \text{if } k = 2j \\ C[m] \oplus M[2j] \oplus C[2i-1] \oplus M[2i] \oplus C[2j-1] & \text{if } k = m \\ C[k] & \text{if } k \notin \{2j, m\} \end{cases}$$

By (6) adversary finds $(\tilde{C}[1] \parallel \tilde{C}[2] \parallel \dots \parallel \tilde{C}[m], T)$ is a valid $(Ciphertext, Tag)$ and it decrypted to

$$\tilde{M}[1] \parallel \tilde{M}[2] \parallel \dots \parallel \tilde{M}[m]$$

Case3: There exist two number $i, j \in \{1, 2, \dots, \frac{m-1}{2}\}$ such that:

$$M[2i] \oplus C[2i-1] = M[2j] \oplus C[2j-1]$$

By (1) we have

$$M[2i-1] \oplus M[2j-1] = 2^{i-1}L \oplus 2^{j-1}L \quad (7)$$

Adversary puts: $\tilde{M}[k] = \begin{cases} M[2i] \oplus M[2i-1] \oplus M[2j-1] & \text{if } k = 2j \\ M[2j] \oplus M[2i-1] \oplus M[2j-1] & \text{if } k = 2i \\ M[k] & \text{if } k \notin \{2j, 2i\} \end{cases}$

and $\tilde{C}[k] = \begin{cases} C[2i] \oplus M[2i-1] \oplus M[2j-1] & \text{if } k = 2j \\ C[2j] \oplus M[2i-1] \oplus M[2j-1] & \text{if } k = 2i \\ C[2j-1] \oplus M[2i-1] \oplus M[2j-1] & \text{if } k = 2i-1 \\ C[2i-1] \oplus M[2i-1] \oplus M[2j-1] & \text{if } k = 2j-1 \\ C[k] & \text{if } k \notin \{2j, 2i, 2i-1, 2j-1\} \end{cases}$

By (7) adversary finds $(\tilde{C}[1] \parallel \tilde{C}[2] \parallel \dots \parallel \tilde{C}[m], T)$ is a valid $(Ciphertext, Tag)$ and it decrypted to

$$\tilde{M}[1] \parallel \tilde{M}[2] \parallel \dots \parallel \tilde{M}[m]$$

Case4: (when $\tau = n$) There exists a number $i \in \{1, 2, \dots, \frac{m-1}{2}\}$ such that

$$T = C[2i-1] \oplus M[2i]$$

Since $A = \varepsilon$ we have $T = TE = E_K(3L^* \oplus \delta \oplus \Sigma)$ so by (1) we conclude

$$3L^* \oplus \delta \oplus \Sigma = 2^{i-1}L \oplus M[2i-1] \quad (8)$$

From (8) we obtain

$$3L^* \oplus \Sigma \oplus M[2i-1] \oplus C[2i-1] = 2^{i-1}L \oplus \delta \oplus C[2i-1] \quad (9)$$

By (2) and (9) we obtain

$$E_K \left(3L^* \oplus \Sigma \oplus M[2i-1] \oplus C[2i-1] \right) = C[2i] \oplus M[2i-1] \quad (10)$$

Adversary chooses \hat{M} such that

$$\begin{aligned} |\hat{M}| &< n, \\ \text{pad}(\hat{M}) &= M[m] \oplus M[2i-1] \oplus C[2i-1] \end{aligned}$$

and it puts $\hat{C} := \text{msb}_{|\hat{M}|} \left(C[m] \oplus M[2i-1] \oplus C[2i-1] \right)$. By (10) adversary finds

$$\left(C[1] \parallel C[2] \parallel \dots \parallel C[m-1] \parallel \hat{C}, C[2i] \oplus M[2i-1] \right)$$

is a valid (Ciphertext, Tag) and it decryped to

$$M[1] \parallel M[2] \parallel \dots \parallel M[m-1] \parallel \hat{M}$$

Case5: (when $\tau = n$) There exists a number $i \in \{1, 2, \dots, \frac{m-1}{2}\}$ such that

$$T = C[2i] \oplus M[2i-1]$$

Since $A = \varepsilon$ we have $T = TE = E_K(3L^* \oplus \delta \oplus \Sigma)$ so by (1) we conclude

$$3L^* \oplus \Sigma = 2^{i-1}L \oplus C[2i-1] \quad (11)$$

From (11) we obtain

$$3L^* \oplus \Sigma \oplus M[2i-1] \oplus C[2i-1] = 2^{i-1}L \oplus M[2i-1] \quad (12)$$

By (1) and (12) we obtain

$$E_K \left(3L^* \oplus \Sigma \oplus M[2i-1] \oplus C[2i-1] \right) = C[2i-1] \oplus M[2i] \quad (13)$$

Adversary chooses \hat{M} such that

$$\begin{aligned} |\hat{M}| &< n, \\ \text{pad}(\hat{M}) &= M[m] \oplus M[2i-1] \oplus C[2i-1] \end{aligned}$$

and it puts $\hat{C} := \text{msb}_{|\hat{M}|} \left(C[m] \oplus M[2i-1] \oplus C[2i-1] \right)$. By (13) adversary finds

$$\left(C[1] \parallel C[2] \parallel \dots \parallel C[m-1] \parallel \hat{C}, C[2i-1] \oplus M[2i] \right)$$

is a valid (Ciphertext, Tag) and it decryped to

$$M[1] \parallel M[2] \parallel \dots \parallel M[m-1] \parallel \hat{M}$$

4 Advantage of adversary

Advantage of our adversary is

$$Adv(A) = \left(\frac{3(m-1)}{2} + 2C\left(\frac{m-1}{2}, 2\right) \right) 2^{-128}$$

References

- [1] Minematsu, K.: Parallelizable Authenticated Encryption from Functions. IACR Cryptology ePrint Archive 2013, 628 (2013)
- [2] Minematsu, K.: Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. In: Eurocrypt (2014), to appear

Hassan Sadeghi
Department of Mathematics, Faculty of Science
University of Qom
Qom. Iran
Email: sadeghihassan64@gmail.com