Forgery on Qameleon and SIV-TEM-PHOTON and SIV-Rijndael256

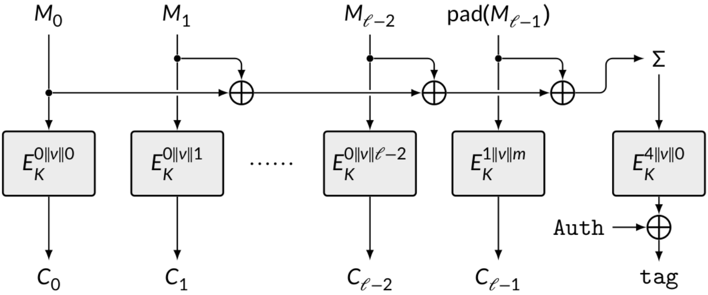
N.Datta, A.Jha, M.Nandi

Indian Statistical Institute, Kolkata, India

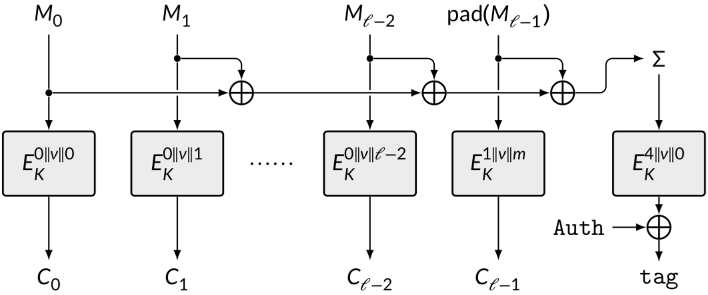
NIST Lightweight Workshop, 2019

Nov 05, 2019

Qameleon AE Mode



Qameleon AE Mode



- Observation: The message length is not used in the final tweakable block cipher.

Forgery on Qameleon

Forgery Description on Qameleon

- Query $(N,\ A,\ M_1 \| M_1)$ to the encryption oracle. Let $(C_1 \| C_2,\ T)$ be the ciphertext and tag pair.
- Forge with (N, A, ϵ, T), where ϵ denotes empty ciphertext.

Forgery on Qameleon

Forgery Description on Qameleon

- Query $(N,\ A,\ M_1\|M_1)$ to the encryption oracle. Let $(C_1\|C_2,\ T)$ be the ciphertext and tag pair.
- Forge with (N, A, ϵ, T), where ϵ denotes empty ciphertext.

Simple Extension

- Take any message $M = M_1\|\ldots\|M_m$ with $M_1 \oplus \cdots \oplus \mathrm{pad}(M_m) = 0$ and $m < 2^{28}$.
- Query $(N,\ A,\ M)$ to the encryption oracle. Let $(C,\ T)$ be the ciphertext and tag pair.
- Forge with (N, A, ϵ, T), where ϵ denotes empty ciphertext.

How the Forgery Works?

Exploiting improper tweak setting for tag generation

- The AD is same in both the cases.
- The checksum of M matches with the checksum for empty message, i.e. 0.
- The tweak value for tag generation block cipher call is same in both the cases, i.e. , $4\|v\|0$ (since nonce is same and $|M|/128 < 2^{28}$).

- Hence, the forgery succeeds with probability 1.

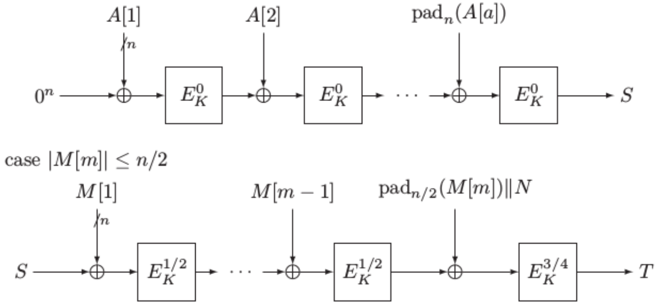
How to Resist the Forgery?

Remark

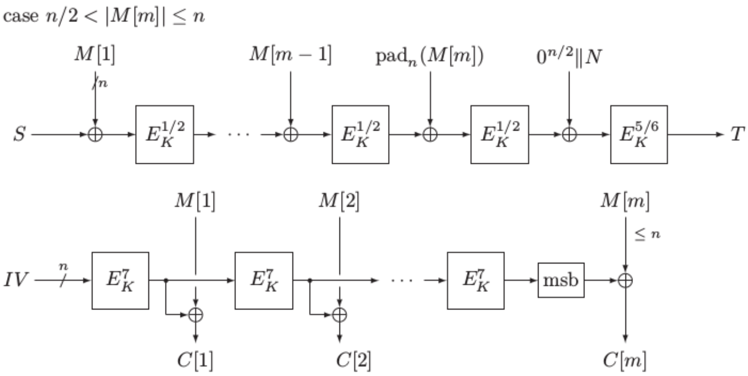
- Forging is possible only with empty message.
- Message length is used for non-empty messages, and hence forging with non-empty message is not possible.

- Use the message length in the tweak of the final tweakable block cipher is a solution to this attack.

SIV-Rijndael256 AE Mode



SIV-Rijndael256 AE Mode



SIV-Rijndael256 AE Mode

Algorithm $\mathcal{F}_K(N, A, M)$

$S \leftarrow 0^n$
$(A[1], \ldots, A[a]) \xleftarrow{n} A$
if $|A[a]| < n$ **then** $d \leftarrow 1$ **else** $d \leftarrow 2$
$A[a] \leftarrow \mathrm{pad}_n(A[a])$
for $i = 1$ **to** a **do**
    $S \leftarrow S \oplus A[i]$
    $S \leftarrow E_K^0(S)$
$(M[1], \ldots, M[m]) \xleftarrow{n} M$
for $i = 1$ **to** $m - 1$ **do**
    $S \leftarrow S \oplus M[i]$
    $S \leftarrow E_K^d(S)$
if $|M[m]| < n/2$ **then**
    $S \leftarrow S \oplus (\mathrm{pad}_{n/2}(M[m]) \| N)$
    $T \leftarrow E_K^3(S)$
if $|M[m]| = n/2$ **then**
    $S \leftarrow S \oplus (M[m] \| N)$
    $T \leftarrow E_K^4(S)$
if $n/2 < |M[m]| < n$ **then**
    $S \leftarrow S \oplus (\mathrm{pad}_n(M[m]))$
    $S \leftarrow E_K^d(S)$
    $S \leftarrow S \oplus (0^{n/2} \| N)$
    $T \leftarrow E_K^5(S)$
if $|M[m]| = n$ **then**
    $S \leftarrow S \oplus M[m]$
    $S \leftarrow E_K^d(S)$
    $S \leftarrow S \oplus (0^{n/2} \| N)$
    $T \leftarrow E_K^6(S)$
return T

- Observation: If $|M| \leq n/2$, d is not used in the algorithm, two queries with same padded AD generates same (ciphertext-tag) pair.

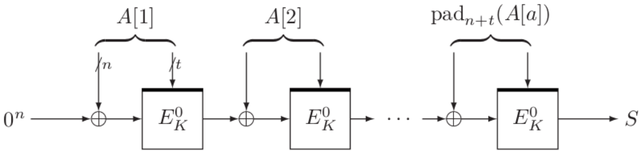
Forgery on SIV-Rijndael256

Forgery Description on SIV-Rijndael256

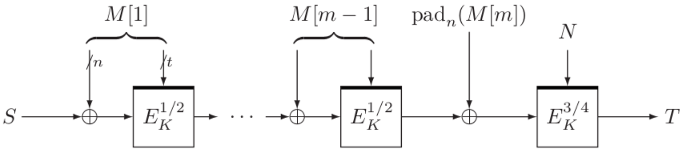
- Construct A ($|A| = 256$) and A' ($|A'| < 256$) such that $\text{pad}(A) = \text{pad}(A')$.
- Query (N, A, M), with $|M| \leq 128$. Let the ciphertext be (C, T).
- Forge with (N, A', C, T).

- The forgery succeeds with probability 1.

SIV-TEM-PHOTON AE Mode



case $|M[m]| \leq n$



SIV-TEM-PHOTON AE Mode

Algorithm $\mathcal{F}_K(N, A, M)$

$S \leftarrow 0^n$

$(A[1], \ldots, A[a]) \xleftarrow{n+t} A$

if $|A[a]| < n + t$ **then** $d \leftarrow 1$ **else** $d \leftarrow 2$

$A[a] \leftarrow \mathrm{pad}_{n+t}(A[a])$

for $i = 1$ **to** a **do**

    $S \leftarrow S \oplus \mathrm{msb}_n(A[i])$

    $S \leftarrow E_K^{0,\mathrm{lsb}_t(A[i])}(S)$

$(M[1], \ldots, M[m]) \xleftarrow{n+t} M$

for $i = 1$ **to** $m - 1$ **do**

    $S \leftarrow S \oplus \mathrm{msb}_n(M[i])$

    $S \leftarrow E_K^{d,\mathrm{lsb}_t(M[i])}(S)$

if $|M[m]| < n$ **then**

    $S \leftarrow S \oplus \mathrm{pad}_n(M[m])$

    $T \leftarrow E_K^{3,N}(S)$

if $|M[m]| = n$ **then**

    $S \leftarrow S \oplus M[m]$

    $T \leftarrow E_K^{4,N}(S)$

if $n < |M[m]| < n + t$ **then**

    $M[m] \leftarrow \mathrm{pad}_{n+t}(M[m])$

    $S \leftarrow S \oplus \mathrm{msb}_n(M[m])$

    $S \leftarrow E_K^{d,\mathrm{lsb}_t(M[m])}(S)$

    $T \leftarrow E_K^{5,N}(S)$

if $|M[m]| = n + t$ **then**

    $S \leftarrow S \oplus \mathrm{msb}_n(M[m])$

    $S \leftarrow E_K^{d,\mathrm{lsb}_t(M[m])}(S)$

    $T \leftarrow E_K^{6,N}(S)$

return T

- Observation: If $|M| \leq n$, d is not used in the algorithm, two queries with same padded AD generates same (ciphertext-tag) pair.

Forgery on SIV-TEM-PHOTON

Forgery Description on SIV-TEM-PHOTON

- Construct A ($|A| = 384$) and A' ($|A'| < 384$) such that $\text{pad}(A) = \text{pad}(A')$.
- Query (N, A, M), with $|M| \leq 256$. Let the ciphertext be (C, T).
- Forge with (N, A', C, T).

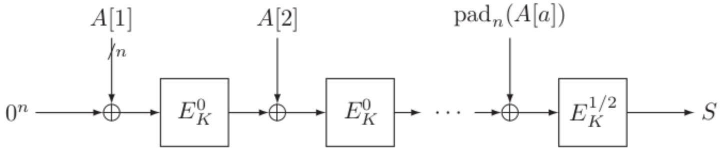
- The forgery succeeds with probability 1.

How to Resist the Forgery?

- Separate the domains for full and partial AD in the AD processing phase.
- Already suggested by the designers in their revised document.

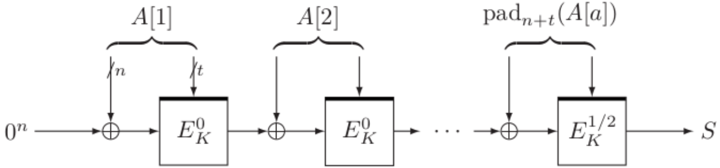
How to Resist the Forgery?

- Separate the domains for full and partial AD in the AD processing phase.
- Already suggested by the designers in their revised document.



How to Resist the Forgery?

- Separate the domains for full and partial AD in the AD processing phase.
- Already suggested by the designers in their revised document.



Thank You..!! Questions??