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

Nilanjan Datta, Ashwin Jha and Mridul Nandi

Indian Statistical Institute, Kolkata, India
nilanjan_isi_jrf@yahoo.com,ashwin.jha1991@gmail.com,mridul.nandi@gmail.com

Abstract. In this short note, we present simple forgeries against three NIST Round-1 candidates namely Qameleon, SIV-TEM-PHOTON and SIV-Rijndael256. In Qameleon, we observed that the checksum block processing doesn't use message length in the tweak, which can be exploited to mount forgery. For SIV-TEM-PHOTON and SIV-Rijndael256, we have observed that proper domain separation is not done during the final associated data block processing, which can be exploited to mount simple forgeries against them.

Keywords: Qameleon · SIV-TEM-PHOTON · SIV-Rijndael256 · Forgery

1 Forgery against Qameleon

We have found a trivial forgery against all the general purpose variants of Qameleon [1], namely qameleon12812864gpv1, qameleon12812896gpv1 (primary candidate), and qameleon128128128tcgpv1. The basic structure of Qameleon is depicted in 1.

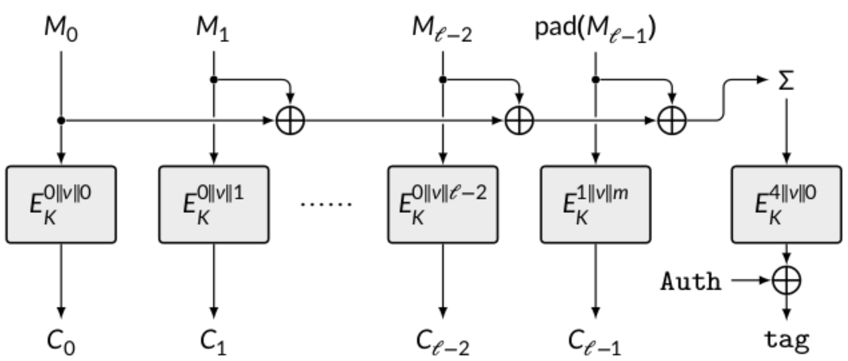

Figure 1: Qameleon Authenticated Encryption Mode

The attack (demonstrated below) exploits the improper tweak setting for tag generation block cipher call:

- 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.

First, the checksum of $M := M_1 \| M_1$ matches with the checksum for empty message, i.e. 0; second, 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 $|M|/128 < 2^{28}$); and lastly, AD is same in both the cases. Thus, the forgery succeeds with probability 1.

In fact, the attack can be extended for any message $M = M_1 \| \ldots \| M_m$ with $M_1 \oplus \cdots \oplus \text{pad}(M_m) = 0$ and $m < 2^{28}$.

Resisting the Forgery. Use of the message length in the tweak of the final tweakable block cipher can be a solution to this attack.

2 Forgery against SIV-TEM-PHOTON and SIV-Rijndael256

SIV-Rijndael256 [2] and SIV-TEM-PHOTON [3] are two SIV based constructions submitted in the NIST Lightweight Competition. For both the constructions, we have observed that if the message length is less than or equal to $n/2$ bits, two queries with same padded associated data (one with full block and the other with partial) generates same (ciphertext-tag) pair.

2.1 Forgery Attack on SIV-Rijndael256

The Forgery attack can be mounted as follows:

- 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).

2.2 Forgery Attack on SIV-TEM-PHOTON

The Forgery attack can be mounted as follows:

- 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).

Resisting the Forgeries. Use of different tweaks in the last associated data block can be a solution to this attack.

Acknowledgments

We communicated our findings with the designers of Qameleon, SIV-TEM-PHOTON, and SIV-Rijndael256, and they concur with our findings. We would like to thank them for giving their valuable time to go through our findings.

References

[1] Andrey Bogdanov Orr Dunkelman Senyang Huang Francesco Regazzoni Roberto Avanzi, Subhadeep Banik. Qameleon v.1.0: A Submission to the NIST Lightweight Cryptography Standardiza on Process. 2019. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/qameleon-spec.pdf.

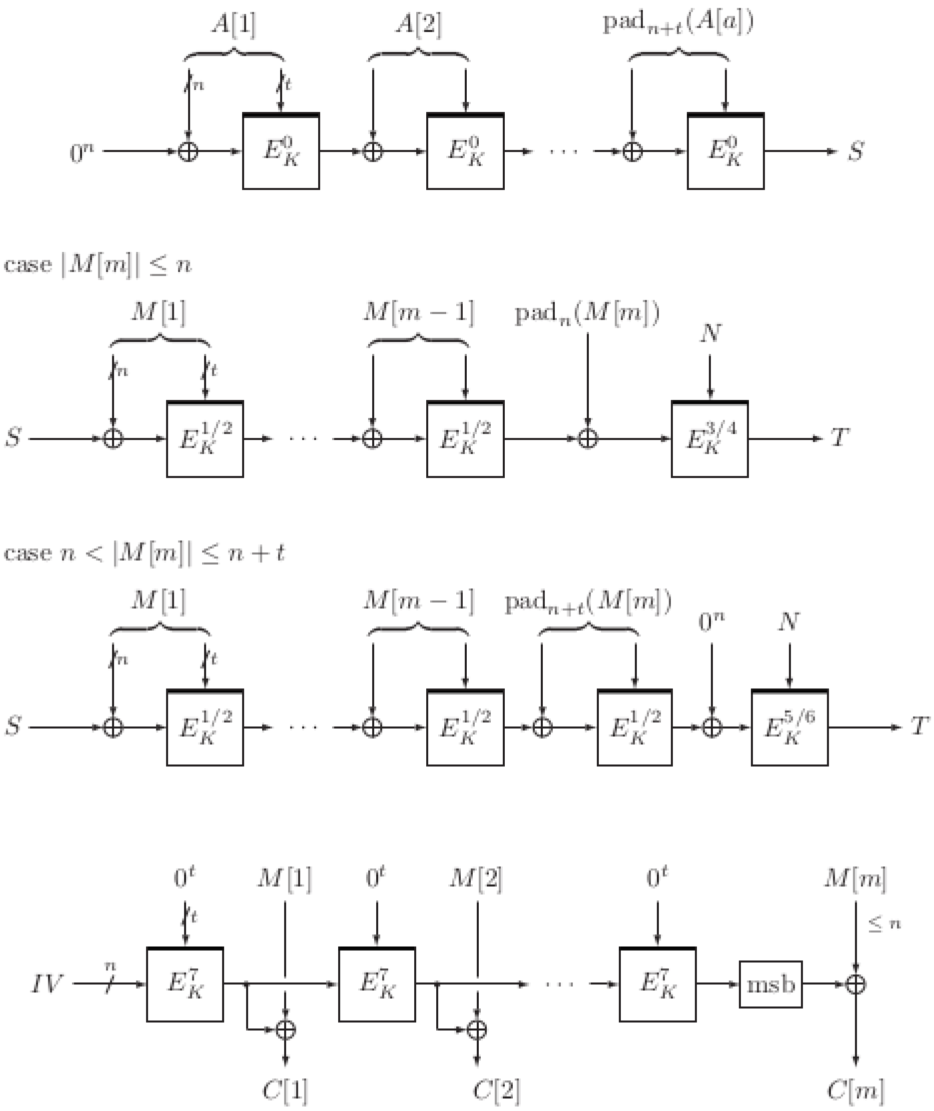

Figure 2: SIV-TEM-PHOTON

[2] Tetsu Iwata Ling Song Zhenzhen Bao, Jian Guo. SIV-Rijndael256 Authenticated Encryption and Hash Family. 2019. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/SIV-Rijndael256-Spec.pdf.

[3] Tetsu Iwata Ling Song Zhenzhen Bao, Jian Guo. SIV-TEM-PHOTON Authenticated Encryption and Hash Family. 2019. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/SIV-TEM-PHOTON-Spec.pdf.

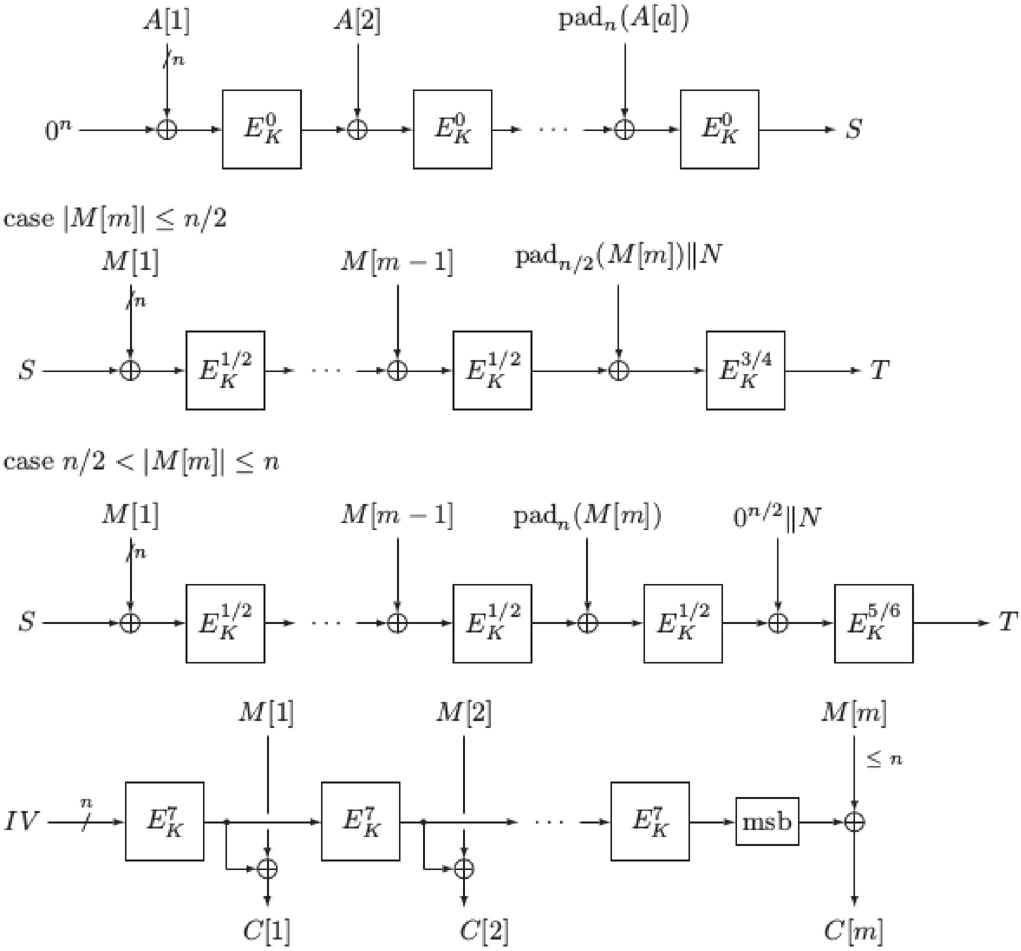

Figure 3: SIV-Rijndael256