SKINNY-AEAD and SKINNY-Hash: NIST LWC Second-round Candidate Status Update

Christof Beierle[1§], Jérémy Jean[2], Stefan Kölbl[3], Gregor Leander[1], Amir Moradi[1], Thomas Peyrin[4], Yu Sasaki[5], Pascal Sasdrich[1¶] and Siang Meng Sim[4]

[1] Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Bochum, Germany
[2] ANSSI, Paris, France
[3] Independent[‖]
[4] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
[5] NTT Secure Platform Laboratories, Japan

skinny@googlegroups.com

Introduction

This is a short update on our submission SKINNY-AEAD and SKINNY-Hash. Most of the new results are published in ToSC 2020 Special Issue [2].

1 New proofs/arguments supporting the security claims

No new updates for the moment.

2 New implementations

The hardware and two-share masking implementation results are presented in [2, §6].

3 New third-party analysis and its implications

A comprehensive list of third-party analysis on SKINNY-128-256 and SKINNY-128-384 is documented in [2, §5.3]. In short, both variants remain secure with at least 50% security margin. To the best of our knowledge, there are two new third-party analysis [5, 3] that is not included.

[5] presented a related-tweakey rectangle attack on 28-round SKINNY-128-384 (previous best was 27-round) under a specific setup on the tweakey and with time, data and memory complexity of $2^{315.25}$, 2^{122} and $2^{122.32}$ respectively. The authors also claimed a related-tweakey attack on SKINNY-AEAD-M1 with 24-round SKINNY-128-384. However, as discussed

[§] Part of the work of Christof Beierle was performed while he was affiliated with the University of Luxembourg

[¶] Part of the work of Pascal Sasdrich was performed while he was affiliated with Rambus Cryptoraphy, the Netherlands

[‖] Stefan Kölbl is now working at Google.

on the LWC forum [1], the attack on SKINNY-AEAD-M1 is invalid, and the authors had removed their attack on SKINNY-AEAD-M1 from their ePrint version [4].

Another work is [3]. They presented a collision path for 3-round (out of 56) SKINNY-tk3-Hash and a collision path for 7-round simplified SKINNY-tk3-Hash. This result clearly does not threaten SKINNY-Hash, but rather boosts confidence that our scheme is collision resistant with, again, a huge security margin.

There is no third-party analysis specifically on the mode. But this is not surprising since ΘCB3 has been proven secure. In addition, the same ΘCB3 framework has previously be adopted in one of the CAESAR candidates, Deoxys-I, and till date it remains secure.

4 Platforms and metrics in which the candidate performs better than current NIST standards

At mode level, ΘCB3 is highly parallelizable, and with the underlying lightweight tweakable block cipher SKINNY-128-384, our algorithms have the advantage over AES-GCM in both hardware and software performance.

Our algorithms are efficient for short messages. For authenticated encryption, the main reason is because the design is based on a tweakable block cipher, which allows to avoid any precomputation (like in OCB, AES-GCM, etc.). In particular, the first 128-bit message block is handled directly and by taking in account the tag generation, one needs only $m+1$ internal calls to the tweakable block cipher to process messages of m blocks of 128 bits each (if there is no associated data).

5 Target applications and use cases for which the candidate is optimized

Similar to OCB, which is one member of CAESAR's final portfolio, our submission is suited for high-performance applications, e.g., on a high-end server. In addition, the use of the lightweight block cipher SKINNY makes it suitable for low-end constrained devices as well. This makes our scheme suitable for scenarios like a network in which a main server needs to communicate with multiple IoT devices.

Our beyond-birthday-bound security allows significantly longer usage of our scheme under the same secret key as compared to schemes with birthday-bound security. This is impactful as rekeying may be costly and, if the usage of a device (over its entire lifespan) does not exceed (or come close to) the security bound, there is no need for rekeying. Our algorithms are also efficient for short messages as mentioned in the previous section.

6 Planned tweak proposals

If SKINNY-AEAD and SKINNY-Hash are selected for the final round, we are intending to make two changes to our submission:

6.1 Propose SKINNY-AEAD+ and SKINNY-Hash+

We observe that our submission guarantees a much larger security margin on its internal primitive than other candidates and this important aspect is not measured at all in performance benchmarks.

In order to provide more attractive security margin/efficiency trade-offs, we propose replacing all SKINNY-128-384 instances with SKINNY-128-384+, which is a reduced-round version from 56 rounds to 40 rounds, while everything else remains the same.

This change allows us to immediately gain up to a 1.4× performance gain, and it still gives 30% security margin in the worst-case related-key related-tweak scenario, without even excluding attacks with complexity much higher than 2^{128}.

The corresponding SKINNY-AEAD and SKINNY-Hash variants will also be denoted with a "+" sign, namely:

Current variants	New variants
SKINNY-AEAD-M1	SKINNY-AEAD-M1+
SKINNY-AEAD-M2	SKINNY-AEAD-M2+
SKINNY-AEAD-M3	SKINNY-AEAD-M3+
SKINNY-AEAD-M4	SKINNY-AEAD-M4+
SKINNY-tk3-Hash	SKINNY-tk3-Hash+

6.2 Drop SKINNY-128-256-based members

Unless the NIST LWC team prefers otherwise, we are planning to drop all variants that are based on SKINNY-128-256 in order to set the focus on those schemes that formally meet the NIST requirements. In particular, we plan to remove SKINNY-AEAD-M5, SKINNY-AEAD-M6 and SKINNY-tk2-Hash.

References

[1] (Feburary 7, 2020) New attacks on reduced Skinny. Official comments received on LWC forum., 2020. https://groups.google.com/a/list.nist.gov/g/lwc-forum/c/kCNjP0q64Bo.

[2] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. SKINNY-AEAD and SKINNY-Hash. *IACR Transactions on Symmetric Cryptology*, 2020(S1):88–131, Jun. 2020.

[3] X. Song, W. Jiang, Z. Li, L. Liu, and S. Wu. New collision paths for round-reduced SKINNY-Hash. *China Communications*, 17(6):145–152, 2020.

[4] Boxin Zhao, Xiaoyang Dong, Willi Meier, Keting Jia, and Gaoli Wang. Generalized related-key rectangle attacks on block ciphers with linear key schedule: Applications to skinny and gift. Cryptology ePrint Archive, Report 2019/714, 2019. https://eprint.iacr.org/2019/714.

[5] Boxin Zhao, Xiaoyang Dong, Willi Meier, Keting Jia, and Gaoli Wang. Generalized related-key rectangle attacks on block ciphers with linear key schedule: applications to SKINNY and GIFT. *Des. Codes Cryptogr.*, 88(6):1103–1126, 2020.