From: Fukang Liu <liufukangs@gmail.com>
Sent: Thursday, August 1, 2019 3:46 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Subterranean 2.0
Attachments: Cryptanalysis of Subterranean-SAE.pdf

Dear Subterranean 2.0 team,
We have made a cryptanalysis of Subterranean-SAE, which is the authenticated encryption scheme based on Subterranean 2.0. In its official document, the designers introduce 8 blank rounds to separate the controllable input and output, and expect that 8 blank rounds can achieve a sufficient diffusion. Therefore, it is meaningful to investigate the security by reducing the number of blank rounds. Moreover, the designers make no security claim but expect a non-trivial effort to achieve full-state recovery in a nonce-misuse scenario. Thus, we are motivated to devise the following three types of attack.

1. The first practical full-state recovery attack with time complexity 2^16 and data complexity 1177 in a nonce-misuse scenario.

2. In a nonce-respecting scenario and when the number of blank rounds is reduced to 4 from 8, we can mount a key-recovery attack with time complexity 2^122 and data complexity 2^69.5, which is 2^6 times faster than brute force.

3. In a nonce-respecting scenario and when the number of blank rounds is reduced to 4 from 8, we can mount a practical distinguishing attack with data and time complexity 2^33.

Our paper has been uploaded to eprint https://eprint.iacr.org/2019/879. In addition, we have also discussed our results with the Subterranean 2.0 team and confirmed the validity of our attack.

The source code to help verify our practical attacks has been uploaded to github https://github.com/Crypt-CNS/Subterranean-SAE.git.

Our cryptanalysis does not threaten the security claim for Subterranean-SAE and we hope it can help further understand the security of Subterranean-SAE. In addition, we note that when increasing the number of blank rounds, the construction prevents us from using sufficient freedom of degree to achieve an attack. Therefore, the construction of Subterranean-SAE seems to be secure in a way.

Please find attached our paper.

Best regards,
Fukang Liu, Takanori Isobe and Willi Meier