The Tweak to TinyJAMBU

Hongjun Wu and Tao Huang

Division of Mathematical Sciences
Nanyang Technological University
wuhongjun@gmail.com

17 May 2021

1 The Tweak

The permutation P_{384} in the original TinyJAMBU is used to process the nonce and associated data. In the new TinyJAMBU (version 2), the permutation P_{640} is used to replace P_{384} with more rounds. There is no change to the processing of plaintext blocks.

The tweak to TinyJAMBU is identical to the "Planned Tweak Proposals" specified in the "TinyJAMBU Update", which was submitted to NIST on September 18, 2020.

2 Reason for the Tweak

The reason for the tweak is to provide larger security margin for the protection of nonce and associated data against differential forgery attack.

In [1], Saha et al. analyzed the security margin of the nonce and associated data of TinyJAMBU against the differential forgery attack. In the original TinyJAMBU design, our analysis shows that the differential forgery attack against nonce and associated data succeeds with probability at most 2^{-73}. In [1], it is shown that some NAND gates in the differential trail are not independent, so the forgery attack against nonce and associated data succeeds with probability $2^{-70.64}$. The MILP code being used in the analysis is available online [2].

In TinyJAMBU v2, we increased the round number of the permutation being used to process nonce and associated data. It is shown in [1] that around 338 rounds are needed to resist the differential forgery attack on nonce and associated data. The permutation P_{640} in TinyJAMBU v2 has 302 more rounds than 338 rounds, so the security margin is large.

In our security analysis, we take into account the related NAND gates, as analysed in [1]. The differential analysis of TinyJAMBU v2 is much simpler than that of the original TinyJAMBU, because P_{640} itself is a strong permutation for protecting 32-bit data blocks against differential forgery attack.

References

[1] Dhiman Saha, Yu Sasaki, Danping Shi, Ferdinand Sibleyras, Siwei Sun, and Yingjie Zhang (2020). On the Security Margin of TinyJAMBU with Refined Differential and Linear Cryptanalysis. IACR Transactions on Symmetric Cryptology, 2020(3), 152-174. Available at `https://tosc.iacr.org/index.php/ToSC/article/view/8699/8291`.

[2] Dhiman Saha, Yu Sasaki, Danping Shi, Ferdinand Sibleyras, Siwei Sun, and Yingjie Zhang. The MILP code pertaining to the paper "On the Security Margin of TinyJAMBU with Refined Differential and Linear Cryptanalysis". Available at `https://github.com/c-i-p-h-e-r/refinedTrailsTinyJambu`