SPAE: An authenticated encryption algorithms for low-cost embedded systems

Philippe Elbaz-Vincent[1], Cyril Hugounenq[1], and Sébastien Riou[2]

[1]Univ. Grenoble Alpes, CNRS, IF, 38000 Grenoble, France
[2]Tiempo, 38330 Montbonnot Saint Martin, France

March 1, 2019

Key Words: authenticated encryption with associated data (AEAD), nonce misuse resistance, low-cost hardware.

We propose a new block-cipher mode of operation, called SPAE, for authenticated encryption with associated data (AEAD). This mode is specifically designed toward embedded systems and industrial applications but is nevertheless patent-free. The algorithm has been developped to address the needs of a growing trend in IoT systems: storing an application processor's code and data on a low cost flash memory. Existing AEAD algorithms, such as OCB[1] [3], GCM [2], CCM [5], EAX [1], SIV [4], provide the required functionality however in practice each of them suffer from various drawbacks for this particular use case. We present in the table below a comparison of different AEAD schemes with respect to some importants criteria such as the number of calls to the encryption function and consequences of nonce (mis/re)use:

Name	Non trivial operations count	Consequence of Nonce reuse
OCB	(m+a+2)Ek + (m+a+1)Inc	• Forgeability • Equality of blocks revealed
GCM	(m+1)Ek + (m+a+1)GHASH	• Forgeability • Xor of plaintexts revealed
CCM	(2m+a+2)Ek	Xor of plaintexts revealed
EAX	(2m+a+4)Ek	Xor of plaintexts revealed
SIV	(2m+a)Ek	Equality of message revealed
SPAE	(m+a+2)Ek	Equality of first blocks revealed

SPAE is a generic construction around a block cipher providing both authentication and privacy in a single pass. We present also security statements that apply to this scheme responding to some industrial needs (in particular nonce misuse resistance). The cipher AES was used for concrete implementations and timings for several low-cost hardware platforms used in IoT industry show that AES-SPAE is over two times faster than AES-GCM.

This work is supported by SECURIOT-2-AAP FUI 23 and by ANR-15-IDEX-02.

[1]Part of the CAESAR final portfolio, `https://competitions.cr.yp.to/caesar.html`, announced February, 20, 2019.

References

[1] M. Bellare, P. Rogaway, and D. Wagner. The EAX Mode of Operation, 2004. `https://www.iacr.org/archive/fse2004/30170391/30170391.pdf`.

[2] D. McGrew and J. Viega. The Galois/counter mode of operation (GCM). *Submission to NIST Modes of Operation Process*, 20, 2004.

[3] P. Rogaway, M. Bellare, and J. Black. OCB: A Block-cipher Mode of Operation for Efficient Authenticated Encryption. *ACM Trans. Inf. Syst. Secur.*, 6(3):365–403, aug 2003.

[4] P. Rogaway and T. Shrimpton. The SIV Mode of Operation for Deterministic Authenticated-Encryption (Key Wrap) and Misuse-Resistant Nonce-Based Authenticated-Encryption, 2007.

[5] D. Whiting, R. Housley, and N. Ferguson. AES encryption & authentication using CTR mode & CBC-MAC. *IEEE P802*, 11, 2002.