Fan Zhang, Zi-yuan Liang, Bo-lin Yang, Xin-jie Zhao, Shi-ze Guo, Kui Ren, 2018. Survey of design and security evaluation of authenticated encryption algorithms in the CAESAR competition *Frontiers of Information Technology & Electronic Engineering*, 19(12):1475-1499. https://doi.org/10.1631/FITEE.1800576

Survey of design and security evaluation of authenticated encryption algorithms in the CAESAR competition

Key words: CAESAR competition; Authenticated cipher; Block cipher; Stream cipher; Hash function; Security evaluation

Corresponding author: Fan Zhang
E-mail: fanzhang@zju.edu.cn
ORCID: http://orcid.org/0000-0001-6087-8243

Motivations

1. Authenticated ciphers provide both message confidentiality and integrity.

2. The Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) supported by the National Institute of Standards and Technology (NIST) is an ongoing project calling for submissions of authenticated encryption (AE) schemes.

3. The competition has a total of three rounds and the last round is approaching the end in 2018.

4. In this survey paper, we first introduce the requirements of the proposed design and the progress of candidate screening in the CAESAR competition.

Methods

1. We presented a brief introduction of the CAESAR competition and its requirements and development.

2. We classified 15 candidates, including 7 finalists and 8 third-round candidates, into 4 categories based on their structures.

3. We introduced the main design features of each candidate in detail.

4. We collected and discussed the research related to security analysis of the candidates in the last few years.

Major results

1. The candidates can be classified into 4 categories:

Table 3 Classification of the designed structure for third-round candidates

Class	Finalist(s)	Third-round candidate(s)	Characteristic
BC-AE	COLM/AES -COPA/ELmD, Deoxys, OCB	AES-JAMBU, AES-OTR, AEZ, CLOC/SILC	BC-AE adopts reversible round functions, permutations, and hash functions. It makes the block cipher a black box to accomplish the AE function.
SC-AE	ACORN	–	SC-AE is based on the stream cipher mode. It learns from the idea of the block cipher. SC-AE supplements and improves the block cipher function, and adds the corresponding authentication part.
SH-AE	Ascon	Ketje, Keyak, NORX	SH-AE uses a hash function, encryption scheme, and message authentication scheme to satisfy the confidentiality, integrity, and robustness requirements of the secret message. All candidates in the third round adopt sponge functions as their hash functions.
D-AE	AEGIS, MORUS	Tiaoxin	D-AE updates new state values by the relationship between adjacent states. Then it increases the correlation between adjacent states and accomplishes data integrity.

Major results (Cont'd)

2. The collected features show the design trends of the candidates.

Table 6 Some features of the third-round candidates

Candidate	Design construction	AE mode	Tag	AD	Parallel Enc/Dec	Block cipher mode	Design prototype	Mask design feature	Online	Original intension
ACORN	SC-AE	–	–	√	√/√	–	ACORN	–	√	Lightweight
AEGIS	D-AE	–	–	√	√/–	–	AES-round	–	√	Fast/AES-NI
Ascon	SH-AE	Ascon	–	√	–/–	–	Ascon	Duplex	√	Lightweight
COLM	BC-AE	PHASH &EME*	–	√	√/√	EME	AES	Doubling	√	Fast/AES-NI
AES-COPA	BC-AE	PMAC &XEX	–	√	√/√	XEX	AES	Doubling	√	Fast/AES-NI
ELmD	BC-AE	PHASH &EME*	√	√	√/√	EME	AES	Doubling	√	Fast/AES-NI
Deoxys	BC-AE	Deoxys	–	√	√/√	EME/TAE	Deoxys-BC	–	√	Lightweight
MORUS	D-AE	–	–	√	–/–	–	MORUS	–	√	Fast
OCB	BC-AE	OCB	–	√	√/√	XEX	AES	Doubling	√	Fast
AES-JAMBU	BC-AE	JAMBU	–	√	–/–	OFB	AES	–	√	Lightweight
AES-OTR	BC-AE	OTR	–	√	√/√	OTR	AES	Doubling	√	Fast
AEZ	BC-AE	AEZ	–	√	√/√	OTR	AES4/10	–	–	Fast/Low power
CLOC	BC-AE	CBCMAC &CFB	–	√	–/–	CFB	AES	–	√	Low-overhead
SILC	BC-AE	CBCMAC &CFB	–	√	–/√	CFB	AES	–	√	Lightweight
Ketje	SH-AE	Monkey-Wrap	√	√	–/–	–	Keccak-f	Duplex	√	Based on Keccak
Keyak	SH-AE	Motorist	√	√	√/√	–	Keccak-f	Duplex	√	Based on Keccak
NORX	SH-AE	–	–	√	√/√	–	Ng	Duplex	√	Lightweight
Tiaoxin	D-AE	Toxin-346	–	√	√/√	–	AES-round	–	√	Fast

*Ng: present modes are not used. √: the character is provided; –: not mentioned.

Conclusions

1. Most candidates adopt the structure of block cipher, and most of them work well.

2. A lot of candidates are designed for lightweight scenarios.

3. The candidates have lower costs, better confidentiality, and improved integrity, and most of them perform better than AES.