SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

March 2017, Vol. 60 038102:1–038102:2
doi: 10.1007/s11432-016-0283-3

Cryptanalysis of round-reduced ASCON

Yanbin LI[1], Guoyan ZHANG[1], Wei WANG[1] & Meiqin WANG[1,2*]

[1]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan* 250100*, China;*
[2]*State Key Laboratory of Cryptology, State Cryptography Administration, Beijing* 100878*, China*

Received April 26, 2016; accepted August 12, 2016; published online December 20, 2016

Citation Li Y B, Zhang G Y, Wang W, et al. Cryptanalysis of round-reduced ASCON. Sci China Inf Sci, 2017, 60(3): 038102, doi: 10.1007/s11432-016-0283-3

ASCON[1)] is a candidate to the ongoing CAESAR competition[2)] which is launched to identify good authenticated encryption schemes from 2013. In CT-RSA 2015, the designers performed several detailed cryptanalysis on ASCON which retrieved the key for ASCON with at most 6-round initialization in a nonce-respecting scenario [1]. They also gave forgery attacks on 3/4-round finalization with $2^{33}/2^{101}$ messages in a nonce-misuse scenario. This article provides key recovery attacks on round-reduced version of ASCON with 7 rounds initialization and 5 rounds phase of plaintext processing, which works on round-reduced initialization comprising more than half number of original 12 rounds in the first time. In addition, we create forgery on 4/5/6 rounds finalization with $2^9/2^{17}/2^{33}$ messages, respectively, which is more practical compared to the previous ones. Our work is summarized in Table 1.

Brief description of ASCON. ASCON is designed by Dobraunig et al. The release of ASCON v1.1 passed into the second round of CAESAR competition, which comes in two favors, ASCON-128 and ASCON-128a.

State recovery attack on ASCON. Let X^i denote the input of the i-th round permutation. $X[i]$ denotes the i-th bit of state word X. $X^{i,j}$ denotes the j-th state word of input of the i-th round permutation. And $X_C^{i,j}$, $X_S^{i,j}$, $X_L^{i,j}$ denote the j-th state word of output of p_C, p_S, p_L in the i-th round permutation, respectively.

We focus on retrieving the key of the round-reduced version of ASCON where the initialization has 7 out of 12 rounds and the phase of plaintext processing has 5 out of 6 rounds. The attack consists of two main steps. The first step applies cube-like technique [2] to recover the intermediate state at the beginning of the phase of the plaintext processing. According to [1] and the ANF of S-box, we have the following property on which our attack is based.

Property 1. The cube sum $\sum X_L^5$ of each output bit after 5-round ASCON permutation in the phase of plaintext processing depends on the value of $X^{1,1}[i]$, $X^{1,3}[i]$ and $X^{1,4}[i]$, not depends on the value of $X^{1,2}[i]$.

Our attack is separated to preprocessing and online phases, where the preprocessing phase does not depend on the online values of the secret key. The preprocessing phase builds a table containing all cube-sum corresponding to each evaluation of the unknown bits $X^{1,1}$, $X^{1,3}$ and $X^{1,4}$ with the complexity 2^{66}. The online phase requires 2^{18} time

* Corresponding author (email: mqwang@sdu.edu.cn)

The authors declare that they have no conflict of interest.

1) http://ascon.iaik.tugraz.at.

2) http://competitions.cr.yp.to/caesar.html.

Table 1 Results for ASCON-128

Attack type	Target	Scenario	Rounds	Time	Method	Source
Distinguisher	Permutation	–	12/12	2^{130}	Zero-sum	Ref. [1]
Key recovery	Initialization	Nonce-respecting	6/12	2^{66}	Cube-like	Ref. [1]
Key recovery	Initialization	Nonce-respecting	5/12	2^{35}	Cube-like	Ref. [1]
Key recovery	Initialization	Nonce-respecting	5/12	2^{36}	Differential-linear	Ref. [1]
Key recovery	Initialization	Nonce-respecting	4/12	2^{18}	Differential-linear	Ref. [1]
Key recovery	Initialization	Nonce-misuse	7/12	2^{97}	Cube-like	This article
Key recovery	Initialization	Nonce-misuse	7/12	2^{97}	Cube tester	This article
State recovery	Plaintext processing	Nonce-misuse	5/6	2^{66}	Cube-like	This article
Forgery	Finalization	Nonce-misuse	4/12	2^{101}	Differential	Ref. [1]
Forgery	Finalization	Nonce-misuse	3/12	2^{33}	Differential	Ref. [1]
Forgery	Finalization	Nonce-misuse	6/12	2^{33}	Cube tester	This article
Forgery	Finalization	Nonce-misuse	5/12	2^{17}	Cube tester	This article
Forgery	Finalization	Nonce-misuse	4/12	2^{9}	Cube tester	This article

to check with the cube sum obtained in the attack in the above table and obtains the specific value of the unknown words $X^{1,1}$, $X^{1,3}$ and $X^{1,4}$. Then we proceed to brute-force to recover $X^{1,2}$.

Key recovery attack on ASCON with cube-like technique. After the initialization, the rows 0, 1 and 2 of the state could be recovered if there are no associated data, while rows 3 and 4 are XORed with the key words K_1 and K_2, respectively. We introduce two definitions about equivalent key words $eK_1 = \Sigma_3^{-1}(K_1)$, $eK_2 = \Sigma_4^{-1}(K_2)$.

The careful selection of the cube variables leads to the following properties:

Property 2 ([1])**.** If we select the $N_2[0, \ldots, 31]$ as our cube variables, the cube sum of each output bit after 6-round ASCON permutation in the initialization depends on the value of $K_1[0, \ldots, 31]$, not depends on the value of $K_1[32, \ldots, 63]$ and $K_2[0, \ldots, 63]$.

Property 3. If we want to obtain $\sum X_L^{6,3}$ from X_S^7, it is much easier to directly compute the Xor of $X_L^{6,3}$ since the value of $\sum X_L^{6,3}$ depends on eK_2, but not depends on eK_1.

Our attack is still separated to preprocessing and online phases. The preprocessing phase costs the complexity 2^{65}, when the online phase requires the complexity 2^{97}. Finally, the remaining key bits need to be brute-forced with an additional complexity of 2^{64}.

Key recovery attack on ASCON with cube tester. We propose a cube tester [3] for 6-round ASCON permutation to retrieve the key of 7-round initialization as an alternative option to attacks using cube-like technique.

For 6 rounds ASCON permutation, we choose a set of 2^{33} nonces and introduce some new concepts of equivalent keys $eK_1 = \Sigma_3^{-1}(K_1)$, $eK_2 = \Sigma_4^{-1}(K_2)$. Then we can retrieve the key from a very obvious way with the complexity 2^{97}.

Forgery attack for ASCON. A cube tester for 5/6-round of ASCON permutation has a practical complexity of $2^{17}/2^{33}$. Such cube testers could be used to perform a forgery attack on the round-reduced version of ASCON with 5/6-round finalization with practical complexity $2^{17}/2^{33}$, which are reduced substantially from [1].

Acknowledgements This work was supported by National Basic Research Program of China (Grant No. 2013CB834205), National Natural Science Foundation of China (Grant Nos. 61133013, 61572293, 61602276), and Program for New Century Excellent Talents in University of China (Grant No. NCET-13-0350).

References

1 Dobraunig C, Eichlseder M, Mendel F, et al. Cryptanalysis of Ascon. In: Proceedings of the Cryptographer's Track at the RSA Conference, San Francisco, 2015. 371–387

2 Dinur I, Morawiecki P, Pieprzyk J, et al. Cube attacks and cube-attack-like cryptanalysis on the round-reduced keccak sponge function. In: Advances in Cryptology—EUROCRYPT 2015. Berlin: Springer, 2015. 733–761

3 Aumasson J-P, Dinur I, Meier W, et al. Cube testers and key recovery attacks on reduced-round MD6 and trivium. In: Fast Software Encryption. Berlin: Springer, 2009. 1–22