SCIENCE CHINA
Information Sciences

• LETTER •

September 2017, Vol. 60 099101:1–099101:3
doi: 10.1007/s11432-016-0417-7

Single key recovery attacks on reduced AES-192 and Kalyna-128/256

Gaoli WANG[1,2*] & Chunbo ZHU[1]

[1]*School of Computer Science and Technology, Donghua University, Shanghai* 201620*, China;*
[2]*School of Computer Science and Software Engineering, East China Normal University, Shanghai* 200062*, China*

Received June 21, 2016; accepted September 8, 2016; published online December 19, 2016

Citation Wang G L, Zhu C B. Single key recovery attacks on reduced AES-192 and Kalyna-128/256. Sci China Inf Sci, 2017, 60(9): 099101, doi: 10.1007/s11432-016-0417-7

Dear editor,

We re-evaluate the securities of reduced AES-192 and Kalyna-128/256 against key recovery attack in the single-key model. The meet-in-the-middle attack (MIMT) was first introduced into the analysis of AES by Demirci and Selçuk [1] at FSE 2008. The main idea was to set up a precomputation table for an ordered sequence of values. Later, ref. [2] showed that the storage of this table could be further reduced if one considered the ordered sequence of differences instead of values. At ASIACRYPT 2010, Dunkelman et al. [3] proposed the multiset tabulation and the differential enumeration techniques. The former replaced the ordered sequence of 256-byte values by a multiset of these values, while the latter allowed the adversary to efficiently enumerate the parameters that determine the multiset through a differential characteristic. Subsequently, Derbez et al. [4] reinforced the differential enumeration by incorporating the rebound concept with it. At FSE 2014, the key-dependent sieve technique, whose function was to filter wrong values of the sequence in the precomputation table, was developed by Li et al. [5]. Recently, ref. [6] further improved this kind of attack by combining the previous techniques with some MixColumns properties. Ref. [7, 8] also use the relation between subkey bytes to improve the distinguisher cryptanalysis. Moreover, due to the similarity between AES and Kalyna, these ideas and techniques for the MIMT attacks on AES can also apply to Kalyna. As a result, AlTawy et al. [9] mounted the first 7-round MIMT attacks on both Kalyna-128/256 and Kalyna-256/512. Afterwards, two single key recovery attacks on 9-round Kalyna-128/256 and Kalyna-256/512 were launched by Akshima et al. [10].

Our contribution. Inspired by the idea of [6], we first propose an observation for AES-192, upon which a new 5-round distinguisher is built. Then a 9-round MIMT attack, derived from this distinguisher, is mounted with 2^{113} chosen plaintexts, 2^{189} 9-round encryptions and 2^{177} 128-bit blocks. Compared to [5], where data/time/memory complexities are 2^{121}, $2^{187.5}$ and 2^{185}, respectively, our attack is more efficient in terms of data and memory complexities. Particularly, the new distinguisher can be constructed in time $2^{180.2}$ and memory 2^{177}, while the previous one in [5] requires $2^{194.8}$ encryptions and 2^{193} 128-bit blocks. In fact, the data and memory complexities of [5] are higher than those of the exhaustive search for AES-192. Consequently, ref. [5] has to utilize the data/time/memory tradeoff to optimize the result.

In the case of Kalyna-128/256, we first improve the previous best known 9-round key recovery at-

* Corresponding author (email: glwang@sei.ecnu.edu.cn)
The authors declare that they have no conflict of interest.

© Science China Press and Springer-Verlag Berlin Heidelberg 2016

Table 1 Summary of our results along with the previous known key recovery attacks on AES-192 and Kalyna-128/256

Algorithm	Rounds	Data	Time	Memory	Reference
AES-192	8	2^{107}	2^{172}	2^{96}	[4]
	9	2^{121}	$2^{187.5}$	2^{185}	[5]
	9	2^{113}	2^{189}	2^{177}	This article
Kalyna-128/256	7	2^{89}	$2^{230.2}$	$2^{202.64}$	[9]
	9	2^{105}	$2^{245.83}$	$2^{226.86}$	[10]
	9	2^{105}	$2^{238.8}$	$2^{226.7}$	This article
	10(2–11)[a)]	2^{115}	$2^{253.3}$	$2^{248.8}$	This article

a) The attack starts from the second round.

tack [10] by choosing a more optimal differential path. Furthermore, we present another 6-round distinguisher for Kalyna-128/256. Specially, the new distinguisher, covering round 2 to round 7, can handle three full active states in the middle of the differential trail by taking advantage of the linear relation between k_4 and k_5. When applying it to the attack of Kalyna-128/256, regrettably, we find it difficult to add one round at the beginning of the distinguisher. The main reason is the bit carry effect resulted from the pre-whitening key addition module 2^{64}. Instead, we are only able to add 4 rounds at the end of the distinguisher and start the attack from the 2nd round. To the best of our knowledge, our attacks is the first result on 10-round Kalyna-128/256. Table 1 summarizes our results along with the previous known key recovery attacks on AES-192 and Kalyna-128/256.

Definition 1 (δ-set)**.** Let a δ-set be an ordered set of 256 states that are different in one state byte (the active byte) and equal in the other state bytes (the inactive bytes).

Definition 2 (Multiset [3])**.** A multiset is a set of elements in which one element can appear more than once. For a multiset of 256 bytes, there are $\binom{2^8+2^8-1}{2^8} \approx 2^{506.17}$ different values.

9-round key recovery attack on AES-192. Looking into the MixColumns operation of the 6th round, we have $2 \cdot Z_6[8] \oplus 3 \cdot Z_6[10] \oplus Z_6[11] = W_6[10] \oplus W_6[11]$. Let $e_{\text{in}} = 2 \cdot Z_6[8] \oplus 3 \cdot Z_6[10] \oplus Z_6[11]$ and $e_{\text{out}} = X_7[10] \oplus X_7[11]$, then

$$e_{\text{in}} = e_{\text{out}} \oplus (k_6[10] \oplus k_6[11]). \tag{1}$$

Consider two pairs, say $(e^m_{\text{in}}, e^m_{\text{out}})$ and $(e^n_{\text{in}}, e^n_{\text{out}})$, according to (1), one has

$$e^m_{\text{out}} \oplus e^n_{\text{out}} = e^m_{\text{in}} \oplus e^n_{\text{in}}. \tag{2}$$

We now raise the following observation.

Observation 1. Let $\{w_1^0, w_1^1, \ldots, w_1^{255}\}$ be a δ-set which contains the right pair (w_1^i, w_1^j) satisfying the differential characteristic that covers the transition: $1 \xrightarrow{R_2} 4 \xrightarrow{R_3} 16 \xrightarrow{R_4} 12 \xrightarrow{R_5} 3 \xrightarrow{R_6} 2$. Consider the encryption of the first 32 states of the δ-set through 5-round AES-192, the 248-bit ordered sequence $(e^1_{\text{out}} \oplus e^0_{\text{out}}, e^2_{\text{out}} \oplus e^0_{\text{out}}, \ldots, e^{31}_{\text{out}} \oplus e^0_{\text{out}})$ can assume only 2^{176} of the 2^{248} theoretically possible values.

Based on this observation (the proof is in Appendix B.1), a 5-round distinguisher is constructed. Afterwards, we apply this distinguisher to the attack of 9-round AES-192 by adding one round at the beginning and three rounds at the end. The attack procedure splits into two phases: precomputation and online phases. In the precomputation phase, the adversary computes all the 2^{176} possible values of the sequence given in Observation 1, and stores them in a hash table. Then in the online phase, we first search for the right pair by guessing some subkeys, after which we check whether the deduced sequence exists in the hash table. If there is a match, we believe the guess is right since the probability for a wrong guess to pass this test is $2^{176-248} = 2^{-72}$. Finally, we exhaustively search the rest of the subkeys. Details are provided in Appendix B.2.

Improved key recovery attack on 9-round Kalyna-128/256. Because of the pre-whitening key addition module 2^{64}, the differences can propagate to the next bytes in the same column. To bypass this effect, our distinguisher will be located in the first 6 rounds and the most significant byte of x_1 is specifically chosen as the active byte. Moreover, in order to save 2^8 time of guessing the pre-whitening key, the sequences will be encoded in the form of multiset.

As before, the first step is to form an equation by exploiting the MixColumns and AddRoundkey of round 6. More detailed, the adversary has

$$\begin{aligned} e_{\text{in}} = e_{\text{out}} \oplus (&\text{0x7D} \cdot k_6[8] \oplus \text{0xF9} \cdot k_6[9] \oplus \text{0x25} \cdot \\ &k_6[10] \oplus \text{0x84} \cdot k_6[11] \oplus \text{0xE6} \cdot k_6[12] \oplus \text{0x64} \cdot \\ &k_6[13] \oplus \text{0xB8} \cdot k_6[14] \oplus \text{0x11} \cdot k_6[15]), \end{aligned} \tag{3}$$

where $e_{\text{in}} = Z_6[12] \oplus Z_6[13] \oplus Z_6[14] \oplus Z_6[15]$, $e_{\text{out}} = \text{0x7D} \cdot X_7[8] \oplus \text{0xF9} \cdot X_7[9] \oplus \text{0x25} \cdot X_7[10] \oplus \text{0x84} \cdot X_7[11] \oplus \text{0xE6} \cdot X_7[12] \oplus \text{0x64} \cdot X_7[13] \oplus \text{0xB8} \cdot$

$X_7[14] \oplus 0\text{x}11 \cdot X_7[15]$. As regards two pairs, say $(e^m_{\text{in}}, e^m_{\text{out}})$ and $(e^n_{\text{in}}, e^n_{\text{out}})$, we deduce

$$e^m_{\text{out}} \oplus e^n_{\text{out}} = e^m_{\text{in}} \oplus e^n_{\text{in}}. \tag{4}$$

Here is the new observation.

Observation 2. Let $\{x^0_1, x^1_1, \ldots, x^{255}_1\}$ be a δ-set which contains the right pair (x^i_1, x^j_1) conforming to the differential characteristic that covers the transition: $1 \xrightarrow{R_1} 8 \xrightarrow{R_2} 16 \xrightarrow{R_3} 16 \xrightarrow{R_4} 6 \xrightarrow{R_5} 4 \xrightarrow{R_6} 8$. Consider the encryption of this δ-set through 6-round Kalyna-128/256, the multiset $(e^0_{\text{out}} \oplus e^i_{\text{out}}, e^1_{\text{out}} \oplus e^i_{\text{out}}, \ldots, e^{255}_{\text{out}} \oplus e^i_{\text{out}})$ assumes only 2^{224} of the $2^{506.17}$ theoretically possible values.

With this observation (the proof is in Appendix C.1), we propose a new 6-round distinguisher for Kalyna-128/256. Later, the distinguisher is extended by three rounds at the end such that a 9-round key recovery attack could be launched. Appendix C.2 gives an account of the attack procedure.

10-round key recovery attack on Kalyna-128/256 from the second round. In order to make full use of the key relation between consecutive odd and even indexed subkeys, the new 6-round distinguisher is specifically located in round 2 to round 7. As a result, we can obtain all the 16 bytes of k_5 for free once k_4 is known.

For the MixColumns and AddRoundkey operations of the 7th round, we establish an equation as follows:

$$\begin{aligned} e_{\text{in}} = e_{\text{out}} &\oplus 0\text{x}21 \cdot k_7[4] \oplus 0\text{x}5\text{F} \cdot k_7[5] \oplus \\ &0\text{x}9\text{B} \cdot k_7[6] \oplus 0\text{x}\text{D}3 \cdot k_7[7], \end{aligned} \tag{5}$$

where $e_{\text{in}} = 0\text{x}8\text{A} \cdot Z_7[0] \oplus 0\text{x}14 \cdot Z_7[4] \oplus 0\text{x}\text{C}7 \cdot Z_7[5] \oplus 0\text{x}29 \cdot Z_7[6] \oplus 0\text{x}6\text{E} \cdot Z_7[7]$, $e_{\text{out}} = 0\text{x}21 \cdot X_8[4] \oplus 0\text{x}5\text{F} \cdot X_8[5] \oplus 0\text{x}9\text{B} \cdot X_8[6] \oplus 0\text{x}\text{D}3 \cdot X_8[7]$. Hence, given $(e^m_{\text{in}}, e^m_{\text{out}})$ and $(e^n_{\text{in}}, e^n_{\text{out}})$, the following equation is tenable:

$$e^m_{\text{out}} \oplus e^n_{\text{out}} = e^m_{\text{in}} \oplus e^n_{\text{in}}. \tag{6}$$

Observation 3. Let $\{x^0_2, x^1_2, \ldots, x^{255}_2\}$ be a δ-set which contains the right pair (x^i_2, x^j_2) conforming to the differential characteristic that covers the transition: $1 \xrightarrow{R_2} 8 \xrightarrow{R_3} 16 \xrightarrow{R_4} 16 \xrightarrow{R_5} 16 \xrightarrow{R_6} 5 \xrightarrow{R_7} 4$. Consider the encryption of this δ-set through 6-round Kalyna-128/256 starting from round 2, the multiset $(e^0_{\text{out}} \oplus e^i_{\text{out}}, e^1_{\text{out}} \oplus e^i_{\text{out}}, \ldots, e^{255}_{\text{out}} \oplus e^i_{\text{out}})$ assumes only 2^{248} of the $2^{506.17}$ theoretically possible values.

Again, we exploit the observation to construct the new 6-round distinguisher. It is then extended by adding 4 rounds in the backward direction. However, the pre-whitening key addition module 2^{64} prevent us from adding one round at the beginning. Therefore, the attack has to start from the second round. In this manner, we mount a single key recovery attack on Kalyna-128/256 reduced to 10 rounds. Details are available in Appendix D.2.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61572125, 61373142), High Technology Field of "Action Plan for Scientific and Technological Innovation" in Shanghai (Grant No. 16511101400).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Demirci H, Selçuk A A. A meet-in-the-middle attack on 8-round AES. In: Fast Software Encyption. Berlin: Springer-Verlag, 2008. 116–126
2 Demirci H, Taşkin I, Çoban M, et al. Improved meet-in-the-middle attacks on AES. In: Proceedings of International Conference on Cryptology in India. Berlin: Springer-Verlag, 2009. 144–156
3 Dunkelman O, Keller N, Shamir A. Improved single-key attacks on 8-round AES-192 and AES-256. In: Advances in Cryptology—ASIACRYPT 2010. Berlin: Springer-Verlag, 2010. 158–176
4 Derbez P, Fouque P A, Jean J. Improved key recovery attacks on reduced round AES in the single-key setting. In: Advances in Cryptology—EUROCRYPT 2013. Berlin: Springer-Verlag, 2013. 371–187
5 Li L B, Jia K T, Wang X Y. Improved single-key attacks on 9-round AES-192/256. In: Fast Software Encyption. Berlin: Springer-Verlag, 2015. 127–146
6 Li R J, Jin C H. Meet-in-the-middle attacks on 10-round AES-256. Designs Codes Cryptogr, 2015, 80: 459–471
7 Huang J L, Lai X J. Revisiting key schedule's diffusion in relation with round function's diffusion. Designs Codes Cryptogr, 2014, 73: 85–103
8 Li L, Wu W L, Zheng Y F. Automatic search for key-bridging technique: applications to LBlock and TWINE. In: Fast Software Encryption. Berlin: Springer-Verlag, 2016. 247–267
9 AlTawy R, Abdelkhalek A, Youssef A M. A meet-in-the-middle attack on reduced-round Kalyna-b/2b. Ieice Trans Inf Syst, 2016, E99.D: 1246–1250
10 Akshima, Chang D H, Ghosh M, et al. Single key recovery attacks on 9-round Kalyna-128/256 and Kalyna-256/512. In: Information Security and Cryptology—ICISC 2015. Berlin: Springer-Verlag, 2015. 119–135