Security evaluation of 128-bit block ciphers AES, CIPHERUNICORN-A, and Hierocrypt-3 against biclique attacks

Intermediate report prepared for the Cryptography Research and Evaluation Committees (CRYPTREC)

Christian Rechberger

In here we give an intermediate report on the security evaluation of the 128-bit block ciphers AES, Hierocrypt-3, and CIPHERUNICORN-A.

As part of their design, all these ciphers come with plausible arguments against large classes of differential and linear attacks, sometimes even with lower bounds against some smaller classes of those attacks. This is in contrast to another attack vector that in its basic form has the potential to be more practically relevant as it may need only a very small amount of known plaintext: meet-in-the-middle attacks. In this report we evaluate the aforementioned block ciphers against the meet-in-the-middle attack vector and in particular its most recent extension, the biclique attack. In addition, no related-key assumptions are needed.

Before we briefly describe intermediate experimental and cryptanalytic results, we discuss the individual designs through the lens of an attack planning to perform a meet-in-the-middle or biclique attack and answer the following question: How often is the key material used throughout the computation of a single encryption or decryption? With a brief review of meet-in-the-middle and biclique attacks, we motivate this question in the following.

1 Meet-in-the-middle and Biclique attacks on block ciphers

The basic idea of meet-in-the-middle attacks is to split an invertible transformation into two parts and separate parameters that are involved in only one part. Then these parameters can be searched independently with a match in the middle as a certificate of a right combination. One of the first applications is the cryptanalysis of DoubleDES $E_{K_2}(E_{K_1}(\cdot))$, which demonstrated that the total security level is not the sum of key lengths [16]. The reason is that given a plaintext/ciphertext pair, an adversary is able to compute the internal middle state of a cipher trying all possible values of K_1 and K_2 independently.

The same principle applies at the round level as well. If there is a sequence of rounds in a block cipher that does not depend on a particular key bit, the meet-in-the-middle attack might work. However, its application has been limited by the design of block ciphers, the majority of which use the full key in the very first rounds of a cipher. As a result, even as little as a half of a cipher is rarely attacked, with four attacked rounds in AES [8] and seven in DES [9, 18]. Compared to 7-round attacks on AES [25], and full 16-round attacks on DES [26], the meet-in-the-middle attacks were clearly inferior to other methods in spite of their impressively low data complexity. The widespread use of meet-in-the-middle attacks against the preimage resistance of hash functions follows this argument, as the message schedule of, e.g., SHA-1, admits as many as 15 rounds being independent of some message bits. The block ciphers KTANTAN [7] and GOST [21], recently attacked within the meet-in-the-middle framework, also do not use the full key for large fraction of their rounds.

In this context the recent meet-in-the-middle attacks on the full AES [5] might look as a counterexample. Nevertheless, they have not disclosed any new key schedule properties. However, they are able to cover up to 6 rounds with a new construction — a biclique, inherited from hash function cryptanalysis [22], which in turn is heavily based on so-called splice-and-cut and initial-structure techniques by Aoki and Sasaki [29]. In addition to the aforementioned length of the biclique, its dimension is another important property, and significantly contributes to the computational advantage compared to brute-force approaches. A biclique does not directly impose constraints on the key schedule decomposition and can be long enough to add a significant number of rounds to a meet-in-the-middle attack. The latter property is, however, difficult to achieve when aiming for a significant advantage over brute-force. Hence we start our study with the extent in which separation of key spaces as possible. And for this an important property of a cipher is the number of times parts or the master key material are used inside the cipher.

2 AES

AES comes in three key lengths. In its variant using a 128-bit key, the key material is re-used 11 times for the 10 rounds. In its variant using a 192-bit key, the key material is re-used less than 9 times. In its variant using a 256-bit key, the key material is re-used less than 8 times to generate the 15 rounds keys.

A survey of known cryptanalytic results in the single-secret-key key-recovery setting for more than 7 rounds of AES with all three key lengths is given in Table 1, Table 2, and Table 3.

Table 1. Summary of known results on AES-128 in the single-secret-key model for 7 or more rounds

rounds	data	workload	memory	method	reference
7	$2^{127.997}$	2^{120}	2^{64}	Square	[19], 2000
7	2^{32}	$2^{128-\epsilon}$	2^{100}	Square-multicoll.	[20], 2000
7	$2^{117.5}$	2^{123}	2^{109}	Impossible	[1], 2007
7	$2^{115.5}$	2^{119}	2^{45}	Impossible	[30], 2007
7	$2^{115.5}$	2^{119}	2^{109}	Impossible	[2], 2008
7	$2^{112.2}$	$2^{112} + 2^{117.2}$MA	2^{109}	Impossible	[23] 2008
7	2^{80}	2^{113}+2^{123} precomp.	2^{122}	MitM	[15], 2009
7	$2^{106.2}$	$2^{107.1} + 2^{117.2}$MA	$2^{94.2}$	Impossible	[25], 2010
7	2^{103}	2^{116}	2^{116}	Square-multiset	[17], 2010
8	2^{88}	$2^{125.34}$	2^{8}	Biclique	[6], 2011
10	2^{88}	$2^{126.18}$	2^{8}	Biclique	[6], 2011
10	2^{4}	$2^{126.89}$	2^{4}	Biclique	[4], 2012

3 Hierocrypt-3

Hierocrypt-3 is described in [13] and an overview of available cryptanalytic results is given in Table 4. In Hierocrypt-3, the 128-bit key variant with 6 rounds needs 13 round-keys of size 128 bits, the 192-bit key variant of Hierocrypt-3 with 7 rounds needs 15 rounds keys, and the 256-bit key variant needs 8 rounds with 17 round keys. Hence the key material is, in principle, used somewhat more often than in AES in all three variants: 13 times, 10 times, and more than 11 times.

4 CIPHERUNICORN-A

CIPHERUNICORN-A is specified in [11]. Its overall design features from a meet-in-the-middle attack point of view are as follows: There is a Feistel structure iterated for 16 rounds operating on a 128-bit block size, for all 3 key lengths of 128, 192, and 256 bits. In each round a 128-bit part of the output of the key schedule is used. Additionally two 128-bit parts are used for initial and final processing. Hence the 128-bit master key is re-used 18 times for CIPHERUNICORN-A with a 128-bit key,

Table 2. Summary of known results on AES-192 in the single-secret-key model for 7 or more rounds

rounds	data	workload	memory	method	reference
AES-192					
7	$2^{127.997}$	2^{120}	2^{64}	Square	[19], 2000
7	2^{36}	2^{155}	2^{32}	Square	[19], 2000
7	2^{32}	2^{182}	2^{32}	Square	[24], 2000
7	2^{32}	2^{140}	2^{84}	Square-multicoll.	[20], 2000
7	2^{92}	2^{186}	2^{153}	Impossible	[28], 2004
7	$2^{115.5}$	2^{119}	2^{45}	Impossible	[30], 2007
7	2^{92}	2^{162}	2^{153}	Impossible	[30], 2007
7	$2^{91.2}$	$2^{139.2}$	2^{61}	Impossible	[23] 2008
7	$2^{113.8}$	$2^{118.8}$MA	$2^{89.2}$	Impossible	[23] 2008
7	2^{34+n}	$2^{74+n}+2^{208-n}$ precomp.	2^{206-n}	MitM	[14], 2008
7	2^{80}	$2^{113}+2^{123}$ precomp.	2^{122}	MitM	[15], 2009
7	2^{103}	2^{116}	2^{116}	Square-multiset	[17], 2010
8	$2^{127.997}$	2^{188}	2^{64}	Square	[19], 2000
8	2^{113}	2^{172}	2^{129}	Square-multiset	[17], 2010
9	2^{80}	$2^{188.8}$	2^{8}	Biclique	[6], 2011
12	2^{80}	$2^{189.74}$	2^{8}	Biclique	[6], 2011

12 times for CIPHERUNICORN-A with a 192-bit key, and 9 times for CIPHERUNICORN-A with a 256-bit key.

5 Preliminary experiments

The key schedule properties discussed so far only relate to the length of two independent chunks, which may or may not be the largest contributor to the number of rounds that can be attacked with a biclique attack. The length of the biclique, and the matching part are also contributing to the total number of rounds attacks. For this, however, the diffusion properties of the round transformation are very influential. Preliminary experiments with implementations of the round transformation of both Hierocrypt-3 and CIPHERUNICORN-A suggest that the differences in the diffusion properties relevant for biclique attacks to vary, but are at a level that is comparable to the AES. Attacks with a non-negligible advantage over brute force for a higher number of rounds than done before in the single-secret-key model can be expected and will be detailed in the final report. At this point it seems however that the practical use of Hierocrypt-3 in any of the three key lengths is not threatened in any way.

Table 3. Summary of known results on AES-256 in the single-secret-key model for 7 or more rounds

rounds	data	workload	memory	method	reference
AES-256					
7	2^{36}	2^{172}	2^{32}	Square	[19], 2000
7	$2^{127.997}$	2^{120}	2^{64}	Square	[19], 2000
7	2^{32}	2^{200}	2^{32}	Square	[24], 2000
7	2^{32}	2^{184}	2^{140}	Square-multicoll.	[20], 2000
7	$2^{92.5}$	$2^{250.5}$	2^{153}	Impossible	[28], 2004
7	$2^{115.5}$	2^{119}	2^{45}	Impossible	[30], 2007
7	$2^{113.8}$	$2^{118.8}$MA	$2^{89.2}$	Impossible	[23] 2008
7	2^{92}	2^{163}MA	2^{61}	Impossible	[23] 2008
7	2^{34+n}	$2^{74+n}+2^{208-n}$ precomp.	2^{206-n}	MitM	[14], 2008
7	2^{80}	$2^{113}+2^{123}$ precomp.	2^{122}	MitM	[15], 2009
8	$2^{127.997}$	2^{204}	2^{1044}	Square	[19], 2000
8	$2^{116.5}$	$2^{247.5}$	2^{45}	Impossible	[30], 2007
8	$2^{89.1}$	$2^{229.7}$MA	2^{97}	Impossible	[23] 2008
8	$2^{111.1}$	$2^{227.8}$MA	$2^{112.1}$	Impossible	[23] 2008
8	2^{34+n}	$2^{202+n}+2^{208-n}$ precomp.	2^{206-n}	MitM	[14], 2008
8	2^{80}	2^{241}	2^{123}	MitM	[15], 2009
8	2^{113}	2^{196}	2^{129}	Square-multiset	[17], 2010
9	2^{120}	$2^{251.92}$	2^{8}	Biclique	[6], 2011
14	2^{40}	$2^{254.42}$	2^{8}	Biclique	[6], 2011

Table 4. Summary of known results on Hierocrypt-3 in the single-secret-key and known/chosen-key model

rounds	data	workload	memory	method	reference
2	2^{11}	2^{44}		key recovery, Square	[12], 2001
2.5	2^{13}	2^{174}		key recovery, Square	[12], 2001
2.5	2^{86}	2^{42}		key recovery, Impossible Differential	[10], 2002
3	$2^{34.6}$	2^{46}		key recovery, Square	[3], 2002
3	$2^{87.5}$	$2^{117.5}$		key recovery, Impossible Differential	[10], 2002
3.5	$2^{36.5}$	2^{176}		key recovery, Square	[3], 2002
3.5	–	2^{48}		known-key distinguisher, Rebound	[27], 2011
4.5	–	2^{48}		chosen-key distinguisher, Rebound	[27], 2011

For CIPHERUNICORN-A, there is no comparable earlier cryptanalysis. Also here the obtained results so far do not seem to threaten the practical use of CIPHERUNICORN-A in any of the three key lengths in any way and will be detailed in the final report.

6 Intermediate conclusions

Our preliminary conclusions are as follows. Among the versions of the three ciphers with a 128-bit key, AES re-uses the key 11 times, Hierocrypt-3 13 times, and CIPHERUNICORN-A 18 times, and hence CIPHERUNICORN-A can potentiall be more resistant against meet-in-the-middle and biclique attacks. Among the versions of the three ciphers with a 192-bit key, AES re-uses the key less than 9 times, Hierocrypt-3 10 times, and CIPHERUNICORN-A 12 times, and hence again CIPHERUNICORN-A can potentially be more resistant against meet-in-the-middle and biclique attacks while AES-192 the least. For the 256-kit-bit versions of the ciphers, the situation is different, however. AES re-uses the key less than 8 times, Hierocrypt-3 more than 11 times, and CIPHERUNICORN-A 9 times, and hence Hierocrypt-3 can potentially be more resistant against meet-in-the-middle and biclique attacks when only basic key scheduling properties are considered. In terms of concrete cryptanalysis, our preliminary cryptanalysis suggests that none of the three algorithms is practically threaten by the biclique attack vector as described in the literature or by new, yet unpublished, improvements to them.

References

1. Behran Bahrak and Mohammad Reza Aref. A novel impossible differential cryptanalysis of AES. In Proceedings of the Western European Workshop on Research in Cryptology 2007 (WEWoRC'07), pages 152–156, 2007.
2. Behran Bahrak and Mohammad Reza Aref. Impossible differential attack on seven-round AES-128. IET Inf. Secur., 2(2):28–32, June 2008.
3. Paulo S. L. M. Barreto, Vincent Rijmen, Jorge Nakahara Jr., Bart Preneel, Joos Vandewalle, and Hae Yong Kim. Improved SQUARE Attacks against Reduced-Round HIEROCRYPT. In Mitsuru Matsui, editor, FSE, volume 2355 of Lecture Notes in Computer Science, pages 165–173. Springer, 2001.
4. Andrey Bogdanov, Elif Bilge Kavun, Christof Paar, Christian Rechberger, , and Tolga Yalcin. Better than Brute-Force — Optimized Hardware Architecture for Efficient Biclique Attacks on AES-128. SHARCS 2012, 2012.
5. Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique Cryptanalysis of the Full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, ASIACRYPT, volume 7073 of Lecture Notes in Computer Science, pages 344–371. Springer, 2011.

6. Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique Cryptanalysis of the Full AES. ASIACRYPT 2011, 2011. http://eprint.iacr.org/2011/449.
7. Andrey Bogdanov and Christian Rechberger. A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN. In SAC'10, volume 6544 of Lecture Notes in Computer Science, pages 229–240. Springer, 2010.
8. Charles Bouillaguet, Patrick Derbez, and Pierre-Alain Fouque. Automatic Search of Attacks on Round-Reduced AES and Applications. In CRYPTO'11, volume 2442 of Lecture Notes in Computer Science, pages 169–187. Springer, 2011.
9. David Chaum and Jan-Hendrik Evertse. Crytanalysis of DES with a reduced number of rounds: Sequences of linear factors in block ciphers. In CRYPTO'85, volume 218 of Lecture Notes in Computer Science, pages 192–211. Springer, 1985.
10. Jung Hee Cheon, MunJu Kim, and Kwangjo Kim. Impossible Differential Cryptanalysis of Hierocrypt-3 Reduced to 3 Rounds. Nessie report, 2002.
11. NEC Corporation. Cryptographic Techniques Specification - CIPHERUNICORN-A.
12. Toshiba Corporation. Self-Evaluation: Hierocrypt-3, 2001.
13. Toshiba Corporation. Specification on a Block Cipher: Hierocrypt-3, 2002.
14. Hüseyin Demirci and Ali Aydin Selçuk. A meet-in-the-middle attack on 8-round AES. In FSE'08, volume 5086 of Lecture Notes in Computer Science, pages 116–126. Springer, 2008.
15. Hüseyin Demirci, Ihsan Taskin, Mustafa Çoban, and Adnan Baysal. Improved Meet-in-the-Middle Attacks on AES. In INDOCRYPT'09, volume 5922 of Lecture Notes in Computer Science, pages 144–156. Springer, 2009.
16. Whitfield Diffie and Martin Hellman. Special feature exhaustive cryptanalysis of the NBS Data Encryption Standard. Computer, 10:74–84, 1977.
17. Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved Single-Key Attacks on 8-Round AES-192 and AES-256. In ASIACRYPT'10, volume 6477 of Lecture Notes in Computer Science, pages 158–176. Springer, 2010.
18. Orr Dunkelman, Gautham Sekar, and Bart Preneel. Improved meet-in-the-middle attacks on reduced-round DES. In INDOCRYPT'07, volume 4859 of Lecture Notes in Computer Science, pages 86–100. Springer, 2007.
19. Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In FSE'00, volume 1978 of Lecture Notes in Computer Science, pages 213–230. Springer, 2000.
20. Henri Gilbert and Marine Minier. A Collision Attack on 7 Rounds of Rijndael. In AES Candidate Conference, pages 230–241, 2000.
21. Takanori Isobe. A single-key attack on the full GOST block cipher. In FSE'11, volume 6733 of Lecture Notes in Computer Science, pages 290–305. Springer, 2011.
22. Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva. Bicliques for preimages: attacks on Skein-512 and the SHA-2 family. Available at http://eprint.iacr.org/2011/286.pdf, 2011.
23. Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New impossible differential attacks on AES. In INDOCRYPT'08, volume 5365 of Lecture Notes in Computer Science, pages 279–293. Springer, 2008.
24. Stefan Lucks. Attacking seven rounds of Rijndael under 192-bit and 256-bit keys. In AES Candidate Conference, pages 215–229, 2000.
25. Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen, and Mahmoud Modarres-Hashemi. Improved Impossible Differential Cryptanalysis of 7-Round AES-128. In INDOCRYPT'10, volume 6498 of Lecture Notes in Computer Science, pages 282–291. Springer, 2010.

26. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In EUROCRYPT'93, volume 765 of Lecture Notes in Computer Science, pages 386–397. Springer, 1993.
27. Ivica Nikolic, Josef Pieprzyk, Przemyslaw Sokolowski, and Ron Steinfeld. Known and Chosen Key Differential Distinguishers for Block Ciphers. In Kyung Hyune Rhee and DaeHun Nyang, editors, ICISC, volume 6829 of Lecture Notes in Computer Science, pages 29–48. Springer, 2010.
28. Raphael Chung-Wei Phan. Impossible differential cryptanalysis of 7-round advanced encryption standard (AES). Inf. Process. Lett., 91(1):33–38, 2004.
29. Yu Sasaki and Kazumaro Aoki. Finding Preimages in Full MD5 Faster Than Exhaustive Search. In EUROCRYPT'09, volume 5479 of Lecture Notes in Computer Science, pages 134–152. Springer, 2009.
30. Wentao Zhang, Wenling Wu, and Dengguo Feng. New results on impossible differential cryptanalysis of reduced AES. In ICISC'07, volume 4817 of Lecture Notes in Computer Science, pages 239–250. Springer, 2007.