Distinguishers for Ciphers and Known Key Attack against Rijndael with Large Blocks

Marine Minier[1], Raphael C.-W. Phan[2,⋆], and Benjamin Pousse[3]

[1] CITI Laboratory – INSA de Lyon
21 Avenue Jean Capelle, 69621 Villeurbanne Cedex – France
marine.minier@insa-lyon.fr
[2] Electronic and Electrical Engineering, Loughborough University
LE11 3TU Leicestershire – UK
R.Phan@lboro.ac.uk
[3] XLIM (UMR CNRS 6172), Université de Limoges
23 avenue Albert Thomas, F-87060 Limoges Cedex – France
benjamin.pousse@unilim.fr

Abstract. Knudsen and Rijmen introduced the notion of known-key distinguishers in an effort to view block cipher security from an alternative perspective e.g. a block cipher viewed as a primitive underlying some other cryptographic construction such as a hash function; and applied this new concept to construct a 7-round distinguisher for the AES and a 7-round Feistel cipher. In this paper, we give a natural formalization to capture this notion, and present new distinguishers that we then use to construct known-key distinguishers for Rijndael with Large Blocks up to 7 and 8 rounds.

Keywords: Block ciphers, cryptanalysis, known-key distinguishers, Rijndael.

1 Introduction

Rijndael-b is an SPN block cipher designed by Joan Daemen and Vincent Rijmen [4]. It has been chosen as the new advanced encryption standard by the NIST [6] with a 128-bit block size and a variable key length, which can be set to 128, 192 or 256 bits. In its full version, the block lengths b and the key lengths Nk can range from 128 up to 256 bits in steps of 32 bits, as detailed in [4] and in [9]. There are 25 instances of Rijndael. The number of rounds Nr depends on the text size b and on the key size Nk and varies between 10 and 14 (see Table 1 for partial details). For all the versions, the current block at the input of the round r is represented by a $4 \times t$ with $t = (b/32)$ matrix of bytes $A^{(r)}$:

⋆ Part of this work done while the author was with the Laboratoire de sécurité et de cryptographie (LASEC), EPFL, Switzerland.

B. Preneel (Ed.): AFRICACRYPT 2009, LNCS 5580, pp. 60–76, 2009.

$$A^{(r)} = \begin{pmatrix} a_{0,0}^{(r)} & a_{0,1}^{(r)} & \cdots & a_{0,t}^{(r)} \\ a_{1,0}^{(r)} & a_{1,1}^{(r)} & \cdots & a_{1,t}^{(r)} \\ a_{2,0}^{(r)} & a_{2,1}^{(r)} & \cdots & a_{2,t}^{(r)} \\ a_{3,0}^{(r)} & a_{3,1}^{(r)} & \cdots & a_{3,t}^{(r)} \end{pmatrix}$$

The round function, repeated $Nr - 1$ times, involves four elementary mappings, all linear except the first one:

- SubBytes: a bytewise transformation that applies on each byte of the current block an 8-bit to 8-bit non linear S-box S.
- ShiftRows: a linear mapping that rotates on the left all the rows of the current matrix. the values of the shifts (given in Table 1) depend on b.
- MixColumns: a linear matrix multiplication; each column of the input matrix is multiplied by the matrix M that provides the corresponding column of the output matrix.
- AddRoundKey: an x-or between the current block and the subkey of the round r K_r.

Those $Nr - 1$ rounds are surrounded at the top by an initial key addition with the subkey K_0 and at the bottom by a final transformation composed by a call to the round function where the MixColumns operation is omitted. The key schedule derives $Nr + 1$ b-bits round keys K_0 to K_{Nr} from the master key K of variable length.

Table 1. Parameters of the Rijndael block cipher where the triplet (i, j, k) for the ShiftRows operation designated the required number of byte shifts for the second row, the third one and the fourth one

	AES	Rijndael-160	Rijndael-192	Rijndael-224	Rijndael-256
ShiftRows	(1,2,3)	(1,2,3)	(1,2,3)	(1,2,4)	(1,3,4)
Nb rounds (Nk=128)	10	11	12	13	14
Nb rounds (Nk=192)	12	12	12	13	14
Nb rounds (Nk=256)	14	14	14	14	14

The idea of exploiting distinguishers for cryptanalyzing block ciphers is well known: a key-recovery attack on block ciphers typically exploits a distinguisher [11]: a structural or statistical property exhibited by a block cipher for a randomly chosen secret key K that is not expected to occur for a randomly chosen permutation. Aside from being used subsequently in key-recovery attacks, so far it seems unclear if there are any other undesirable consequences due to distinguishers, although their existence tends to indicate some certificational weakness in ciphers.

Knudsen and Rijmen [12] recently considered block cipher distinguishers when the cipher key is known to the adversary, and suggested another exploitation of the existence of distinguishers: truncated differential distinguishers lead to

near collisions in some hash function compression functions built upon block ciphers, e.g. the Matyas-Meyer-Oseas (MMO) mode [15]. Generalizing, we can similarly say for a compression function constructed from a block cipher in any of the Preneel-Govaerts-Vandewalle (PGV) modes [16], that near collisions in the ciphertext of the underlying cipher translate to near collisions in the compression function's output chaining variable. Knudsen and Rijmen posed as an open problem if a security notion exists that can capture the kind of known-key distinguishers that they proposed, and yet which would rule out non-meaningful and contrived distinguishing attacks.

This paper takes a step to answering this question. We define a security notion to express the existence of known-key distinguishers for block ciphers in Section 2. Rather than settle for a notion that is meaningful solely when the key is known to the adversary, our notion intuitively also gives some indication on the cipher's security in the conventional unknown-key setting.

Many cryptanalyses have been proposed against Rijndael-b, the first one against all the versions of Rijndael-b is due to the algorithm designers themselves and is based upon integral properties ([2], [3], [13]) that allows to efficiently distinguish 3 Rijndael inner rounds from a random permutation. This attack has been improved by Ferguson et al. in [5] allowing to cryptanalyse an 8 rounds version of Rijndael-b with a complexity equal to 2^{204} trial encryptions and $2^{128} - 2^{119}$ plaintexts.

Following the dedicated work of [7], this paper presents new four-round integral properties of Rijndael-b and the resulting 7 and 8 rounds known key distinguishers in Section 3.

2 Notions for Cipher Distinguishers

2.1 Definitions

Consider a family of functions $F : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{R}$ where $\mathcal{K} = \{0,1\}^k$ is the set of keys of F, $\mathcal{M} = \{0,1\}^l$ is the domain of F and $\mathcal{R} = \{0,1\}^L$ is the range of F, where k, l and L are the key, input and output lengths in bits. $F_K(\mathcal{M})$ is shorthand for $F(K, \mathcal{M})$. By $K \xleftarrow{\$} \mathcal{K}$, we denote randomly selecting a string K from $\mathcal{K}$. Similar notations apply for a family of permutations $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}$ where $\mathcal{K} = \{0,1\}^k$ is the set of keys of E and $\mathcal{M} = \{0,1\}^l$ is the domain and the range of E. Let $\mathrm{Func}(\mathcal{M})$ denotes the set of all functions on $\mathcal{M}$, and $\mathrm{Perm}(\mathcal{M})$ denotes the set of all permutations on $\mathcal{M}$. Let $G \xleftarrow{\$} \mathrm{Perm}(\mathcal{M})$ denotes selecting a random permutation.

The usual security notion one requires from a block cipher is to look like a pseudo-random permutation (PRP), for the keys uniformly drawn. This notion could be formalized as follows: a PRP adversary $\mathcal{A}$ gets access to an oracle, which, on input $P \in \mathcal{M}$, either returns $E_K(P)$ for a random key $k \in \mathcal{K}$ or returns $G(P)$ for a random permutation $G \in \mathrm{Perm}(\mathcal{M})$. The goal of $\mathcal{A}$ is to

guess the type of oracle it has - by convention, $\mathcal{A}$ returns 1 if it thinks that the oracle is computing $E_K(\cdot)$. The adversary's advantage is defined by:

$$Adv_E^{PRP}(\mathcal{A}) = |\Pr\left[K \xleftarrow{\$} \mathcal{K} : A^{E_K(\cdot)} = 1\right] - \Pr\left[G \xleftarrow{\$} \mathrm{Perm}(\mathcal{M}) : A^{G(\cdot)} = 1\right]|$$

E is said PRP-secure if for any $\mathcal{A}$ attacking E with resources, the advantage $Adv_E^{PRP}(\mathcal{A})$ is negligible (denoted by ε). The above notion does not take into account the decryption access. Hence, the stronger notion of Super Pseudo-Random Permutation (SPRP): as above, the adversary $\mathcal{A}$ gets access to an oracle, but in this case, the adversary not only accesses the permutations G and E_K but also their inverses G^{-1} and E_K^{-1}:

$$Adv_E^{SPRP}(\mathcal{A}) = |\Pr\left[K \xleftarrow{\$} \mathcal{K} : A^{E_K(\cdot),E_K^{-1}(\cdot)} = 1\right] - \Pr\left[G \xleftarrow{\$} \mathrm{Perm}(\mathcal{M}) : A^{G(\cdot),G^{-1}(\cdot)} = 1\right]|$$

As done by Luby and Rackoff in [14], formal results using those notions are stated with concrete bounds. However, in the "real life", we could only say that if a distinguisher exists for a given cipher E_K, it is not a PRP or a SPRP (according the distinguisher used). Note (as done in [17]) that a (adversarial) distinguisher is a (possibly computationally unbounded) Turing machine $\mathcal{A}$ which has access to an oracle $\mathcal{O}$; with the aim to distinguish a cipher E_K from the perfect cipher G by querying the oracle with a limited number n of inputs. The oracle $\mathcal{O}$ implements either E_K (for a key randomly chosen) or G. The attacker must finally answer 0 or 1. We measure the ability to distinguish E_K from G by the advantage $Adv_E(\mathcal{A}) = |p - p^*|$ (that must be true for a large part of the key space) where p (resp. $p*$) is the probability of answering 1 when $\mathcal{O}$ implements E_K (resp. G). Note also that three main classes of distinguishers exist: the non-adaptive distinguishers class (where the n plaintext queries are pre-computed), the adaptive distinguishers class (where the plaintext queries depend on the previous ones) and the super pseudo-random distinguishers one (where the queries are chosen according the previous ones and where the oracle also gets access to inverses of E_K and G).

2.2 Notions for Distinguishers

A generic definition of an n-limited non-adaptive distinguisher is given in [10] and described in Alg. 1. One gives an oracle $\mathcal{O}$ to Algorithm 1, which implements either E_K or G with probability $\frac{1}{2}$ each. The core of the distinguisher is the acceptance region $A^{(n)}$: it defines the set of input values $\mathbf{P} = (P_1, \cdots, P_n)$ which lead to output 0 (i.e. it decides that the oracle implements E_K) or 1 (i.e. it decides that the oracle implements G). The goal of the distinguisher is thus to decide whether $\mathcal{O}$ implements E_K or G. If a particular relation R that defines the acceptance region exists linking together inputs and outputs for a sufficient number of values (this efficiently-computable relation outputs 0 if the link exists

and 1 otherwise), the advantage of the non-adaptive distinguisher $Adv_E^{NA}(\mathcal{A})$ will be non-negligible. Note also that this distinguisher must work for a large part of the key space.

Algorithm 1. An n-limited generic non-adaptive distinguisher (NA)

Parameters: a complexity n, an acceptance set $A^{(n)}$
Oracle: an oracle $\mathcal{O}$ implementing a permutation c
  Compute some messages $\mathbf{P} = (P_1, \cdots, P_n)$
  Query $\mathbf{C} = (C_1, \cdots, C_n) = c(P_1, \cdots, P_n)$ to $\mathcal{O}$
  if $\mathbf{C} \in A^{(n)}$ **then**
    Output 1
  else
    Output 0
  end if

This distinguisher is generic and includes the following cases: known plaintexts distinguisher and chosen plaintexts distinguisher. In the second case, the n inputs $\mathbf{P} = (P_1, \cdots, P_n)$ must be pre-defined according a particular filter h_1 (independent from the key). By misuse of language, we use the notation $h_1(\mathbf{P})$ to designate a plaintexts set "correctly" chosen, i.e. that verifies the requirements of h_1. The acceptance region $A^{(n)}$ could be seen as the necessary minimal number of outputs in $\mathbf{C}$ that verify a particular relation $R(h_1(\mathbf{P}), \mathbf{C})$. This relation must be independent from the key or have a high probability to happen for a large class of the keys. In this case, if a such relation R that happens with a certain probability exists between the inputs and outputs sets $h_1(\mathbf{P})$ and $\mathbf{C}$; then, the advantage of the distinguisher could be non-negligible.

To illustrate how this notion applies to the existence of distinguishers for block ciphers, consider E_K as 3-round AES. Let $h_1(\mathbf{P}) = \{P_i\}_{i=0}^{255}$ be a set of 2^8 plaintexts that in one byte each has one of 2^8 possible values, and equal in all other bytes (this defines h_1); and $\mathbf{C} = \{C_i\}_{i=0}^{255}$ denote the corresponding ciphertexts, i.e. $\mathbf{C} = E_K(\mathbf{P})$. Define C_i as a concatenation of 16 bytes i.e. $C_i = C_{i,0}||C_{i,1}||\ldots||C_{i,15}$. Define $R(h_1(\mathbf{P}), \mathbf{C})$ as $\bigoplus_{i=0}^{255} C_{i,j}$ for $j = 0 \ldots 15$ for the particular set $\mathbf{C} = E_K(h_1(\mathbf{P}))$ which outputs 1 (accept) if $\bigoplus_{i=0}^{255} C_{i,j} = 0$ for $j = 0 \ldots 15$ knowing that $\mathbf{P} = \{P_i\}_{i=0}^{255}$ and that $\bigoplus_{i=0}^{255} P_{i,j} = 0$; and outputs 0 otherwise. Thus, for the case of E_K, the probability that $R(h_1(\mathbf{P}), \mathbf{C})$ outputs 1 (accept) is 1, while for the case of a random permutation G, the probability is 2^{-l}. Hence $\mathbf{Adv}_{E_K,G}^{NA\text{-}CPA}(\mathcal{A}) = 1 - 2^{-l} >> \varepsilon$ where $NA\text{-}CPA$ means non-adaptive chosen plaintexts. And so, a distinguisher exists for 3-round AES. In fact, this is the well known 3-round integral distinguisher.

As defined in [17], the super pseudo-random distinguisher (described in Alg. 2) could be defined in a deterministic way because no upper bound on the computational capability of the distinguisher are supposed to be (the only limitation is on the number of queries to the oracle).

In answer to the question posed in [12], we now define a natural extension of the above described n-limited distinguishers, to capture the kind of distinguisher

Algorithm 2. An n-limited generic adaptive distinguisher with chosen input plaintexts or output ciphertexts

Parameters: functions $g_1, \cdots, g_n$, a set $A^{(n)}$
Oracle: an oracle $\mathcal{O}$ implementing permutations c and c^{-1}
Select a fixed direction and message $(B_1, Z_1^0) = g_1()$ and get $Z_1^1 = c(Z_1^0)$ if $B_1 = 0$ or $Z_1^1 = c^{-1}(Z_1^0)$ otherwise
Calculate a direction and a message $(B_2, Z_2^0) = g_2(Z_1^1)$ and get $Z_2^1 = c(Z_2^0)$ if $B_2 = 0$ or $Z_2^1 = c^{-1}(Z_2^0)$ otherwise
...
Calculate a direction and a message $(B_n, Z_n^0) = g_n(Z_1^1, \cdots, Z_{n-1}^1)$ and get $Z_n^1 = c(Z_n^0)$ if $B_n = 0$ or $Z_n^1 = c^{-1}(Z_n^0)$ otherwise
if $(Z_1^1, \cdots, Z_n^1) \in A^{(n)}$ **then**
Output 1
else
Output 0
end if

that interests us in this paper and in [12]: the non-adaptive chosen middletexts one. This is shown in Alg. 3. The oracle processes the middletexts supplied by the adversary moving in either/both directions towards plaintext and/or ciphertext ends. This notion also intuitively captures the setting of known-key attacks [12] since the oracle has the same kind of power to that of an adversary having knowledge of the key.

Algorithm 3. An n-limited generic non-adaptive chosen middletexts distinguisher ($NA\text{-}CMA$)

Parameters: a complexity n, an acceptance set $A^{(n)}$
Oracle: an oracle $\mathcal{O}$ implementing internal functions f_1 (resp. f_2) of permutation c that process input middletexts to the plaintext (resp. ciphertext) end
Compute some middletexts $\mathbf{M} = (M_1, \cdots, M_n)$
Query $\mathbf{P} = (P_1, \cdots, P_n) = (f_1(M_1), \cdots, f_1(M_n))$ and $\mathbf{C} = (C_1, \cdots, C_n) = (f_2(M_1), \cdots, f_2(M_n))$ to $\mathcal{O}$
if $(\mathbf{P}, \mathbf{C}) \in A^{(n)}$ **then**
Output 1
else
Output 0
end if

To see how this notion properly captures the 7-round known-key distinguisher for AES proposed by Knudsen and Rijmen [12], let E_K be 7-round AES, with no MixColumns in the last round. Let $\mathbf{M} = \{M_i\}_{i=0}^{2^{56}-1}$ denote the set of 2^{56} intermediate texts at the output of round 3 of E_K, that differ in seven bytes for $j = \{0, 1, 2, 3, 5, 10, 15\}$ and which have constant values in the remaining nine bytes. Let $\mathbf{P} = \{P_i\}_{i=0}^{2^{56}-1}$ be a set of 2^{56} plaintexts corresponding to the partial

decryption[1] of $\mathbf{M}$ by 3 rounds in reverse thus $\mathbf{P}$ is the plaintext subset input to E_K. Note that $\mathbf{P}$ defined in this way by Knudsen and Rijmen is only computable provided the round keys in rounds 1 to 3 are known to the adversary, or alternatively the key K is known, or one assumes the adversary can start in the middle by choosing the middletexts. This is not a problem since it is allowed by our notion. Let $\mathbf{C} = \{C_i\}_{i=0}^{2^{56}-1}$ denote the corresponding ciphertexts, i.e. $\mathbf{C} = E_K(\mathbf{P})$. Define C_i as a concatenation of 16 bytes i.e. $C_i = C_{i,0}||C_{i,1}||\ldots||C_{i,15}$. Define $R(\mathbf{P}, \mathbf{C}) = (\bigoplus_{i=0}^{2^{56}-1} P_{i,j}, \bigoplus_{i=0}^{2^{56}-1} C_{i,j})$ for $j = 0 \ldots 15$ and which outputs 1 if $\bigoplus_{i=0}^{2^{56}-1} C_{i,j} = 0$ for $j = 0 \ldots 15$ knowing that $\mathbf{P} = \{P_i\}_{i=0}^{2^{56}-1}$ and that $\bigoplus_{i=0}^{2^{56}-1} P_{i,j} = 0$; and outputs 0 otherwise. Thus, for the case of E_K, the probability that $R(\mathbf{P}, \mathbf{C})$ outputs 1 (accept) is 1, while for the case of a random permutation G, the probability is 2^{-l}.

Hence $\mathbf{Adv}_{E_K,G}^{NA\text{-}CMA}(\mathcal{A}) = 1 - 2^{-l} >> \varepsilon$. And so, a chosen middletext (a.k.a. known-key [12]) distinguisher exists for 7-round AES.

In the same way, the notion captures the 7-round distinguisher of [12] for a particular kind of Feistel cipher whose round function has the round key exclusive-ORed to the round function input, followed by an arbitrary key-independent transformation.

With this notion, we can also intuitively define security against the existence of distinguishers in the conventional setting where the key is unknown, which can be seen as a special case of $NA\text{-}CMA$.

Note here that it is apparent in the unknown-key setting that f_1 and f_2 are public functions, since it can in no way be dependent on the key, otherwise, the relation $R(\cdot, \cdot)$ becomes impossible to compute and thus verify. We defer the more detailed discussion to subsection 2.3.

2.3 Discussion

Observe that for the conventional setting where the adversary has no knowledge of the key K, it is intuitive that the distinguishing relation R operates on publicly computable functions f_1 and f_2 of the ciphertext set, otherwise if f_1 or f_2 is dependent on K, the relation cannot be verified since K is assumed to be unknown and must be uniformally distributed. Thus, the resultant notion becomes more meaningful and rules out trivial attacks where the adversary obtains a non-negligible advantage but for which is not meaningful.

Consider if the functions f_1 and f_2 in the $NA\text{-}CMA$ notion can be dependent on K, and indeed why not since K is known to A. Then take E_K to be infinitely many rounds of the AES, i.e. the number of rounds $r >> 7$. Then an adversary could still use the 7-round known-key distinguisher described in [12] as follows: peel off any number of rounds since it knows the cipher key and thus round keys to any round, and going backwards in reverse from the ciphertext end it peels off round by round until the output of round 7, and checks that the 7-round distinguisher covering the first 7 rounds is satisfied. Thus his advantage

[1] Note that this partial decryption is computable by the adversary since it knows the block cipher key K.

$\mathbf{Adv}^{NA\text{-}CMA}_{E_K,G}(\mathcal{A})$ is trivially non-negligible, although it is clear that we gain no insight into the ciphers security nor insecurity.

Thus, considering known-key distinguishers is a stronger notion than the conventional notion of unknown-key distinguishers, and so the inexistence of known-key distinguishers implies the inexistence of unknown-key distinguishers. Furthermore, it is hoped that this context might tell something about the security margin of a cipher, i.e. if an unknown-key distinguisher exists for the cipher up to s rounds, what is the most number of rounds t of the cipher for which is covered by a distinguisher if the key is known to the adversary. For instance, a distinguisher exists for the AES in the unknown-key setting up to 4 rounds [8], while Knudsen and Rijmen showed that a distinguisher exists for AES in the known-key context up to 7 rounds. This still allows some security margin considering AES has at least 10 rounds. From this perspective, (in)existence of known-key distinguishers can be viewed on the one hand as a certificational strength/weakness of a cipher; and on the other hand one still desires to gain some insight on the (in)security of a cipher from these known-key distinguishers. One obvious aim is what can be learned about unknown-key distinguishers from these known-key distinguishers.

Moreover, the only difference between the $NA\text{-}CPA/NA\text{-}CCA$ and $NA\text{-}CMA$ settings is in the extra control afforded to the latter adversary who effectively can choose his plaintext subset based on knowledge of the key what is really appreciable in the context of a meet in the middle attack. We can hence say that existence of known-key distinguishers exhibits some potentially undesirable structural property of the cipher, but which cannot be exploited in unknown-key distinguishers for key-recovery attacks only in the fact that the adversary is expected to not be able to choose the plaintext subset corresponding to the known-key distinguisher since he does not know the key. For the case of the AES, the adversary cannot turn the 7-round known-key distinguisher of Knudsen and Rijmen into an unknown-key distinguisher because he does not know the rounds keys for rounds 1 to 3.

Interestingly, this in some way relates to the motivation behind the design of cipher key schedules that have known-roundkey security, i.e. knowledge of one or more round keys does not lead to the knowledge of other round keys. In this context, known-key distinguishers can potentially be exploited in actual key-recovery attacks. Taking the 7-round AES as an example but where its key schedule has known-roundkey security: if the adversary already knows the round keys for rounds 1 to 3, and by design he still cannot obtain the other round keys, nevertheless due to the existence of the 7-round known-key distinguisher, he can use his knowledge of round keys 1 to 3 to choose a plaintext subset that corresponds to the distinguisher, and with this distinguisher he can cover all the rounds through to round 7. This can be turned into a key-recovery attack on the round keys for rounds 4 to 7.

Relation to correlation intractability. In motivating the need for a notion for known-key distinguishers, Knudsen and Rijmen discuss the related work of Canetti et al. [1] that considered the notion of *correlation intractability*, that

when applied to the context of block ciphers where the key is known to the adversary, can be seen as follows: a correlation intractable cipher is one where there exists no binary relation R between the plaintext and ciphertext that is satisfied with non-negligible probability. Clearly, if the key is known, a relation can always be found and thus a cipher cannot be correlation intractable. Yet, this trivial case is ruled out from our $NA\text{-}CMA$ notion because of the restriction we put on R to be independent of the key. Indeed, Canetti et al.'s impossibility example cannot apply in our notion, since they directly input the key to the relation, while this is not allowed for our relation.

3 Known-Key Distinguishers for the Rijndael-*b* Block Cipher with Large Blocks

We present in this Section known key distinguishers against the Rijndael-b block cipher. Using particular new and old integral properties, the building distinguishers use really few middle-texts and have very low complexity.

In [13], L. Knudsen and D. Wagner analyze integral cryptanalysis as a dual to differential attacks particularly applicable to block ciphers with bijective components. A first-order integral cryptanalysis considers a particular collection of m words in the plaintexts and ciphertexts that differ on a particular component. The aim of this attack is thus to predict the values in the sums (i.e. the integral) of the chosen words after a certain number of rounds of encryption. The same authors also generalize this approach to higher-order integrals: the original set to consider becomes a set of m^d vectors which differ in d components and where the sum of this set is predictable after a certain number of rounds. The sum of this set is called a dth-order integral.

We first introduce and extend the consistent notations proposed in [13] for expressing word-oriented integral attacks. For a first order integral, we have:

- The symbol '$\mathcal{C}$' (for "Constant") in the ith entry, means that the values of all the ith words in the collection of texts are equal.
- The symbol '$\mathcal{A}$' (for "All") means that all words in the collection of texts are different.
- The symbol '?' means that the sum of words can not be predicted.

For a dth order integral cryptanalysis:

- The symbol '$\mathcal{A}^d$' corresponds with the components that participate in a dth-order integral, i.e. if a word can take m different values then $\mathcal{A}^d$ means that in the integral, the particular word takes all values exactly m^{d-1} times.
- The term 'A_i^d' means that in the integral the string concatenation of all words with subscript i take the m^d values exactly once.
- The symbol '$(\mathcal{A}_i^d)^k$' means that in the integral the string concatenation of all words with subscript i take the m^d values exactly k times.

3.1 Known Key Distinguisher for the AES

As mentioned in [12], we could build a 4-th order 4-round AES integral distinguisher considering that the last round does not contain a MixColumns operation. Then, and as shown in Fig. 1.a, all bytes of the ciphertexts are balanced in the 4 rounds integral. Moreover, a backward 3-round property could be built for three complete rounds as shown in Fig. 1.b.

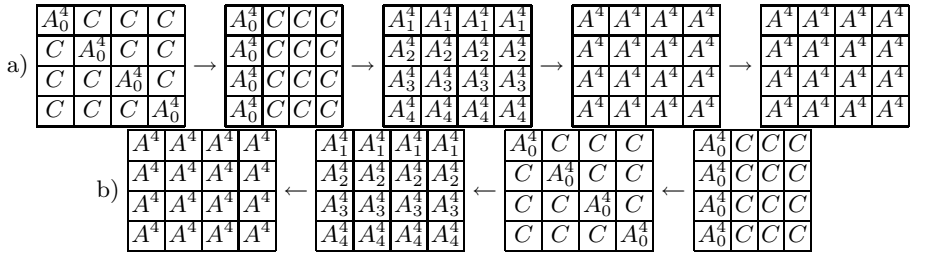

Fig. 1. a) The forward 4-round integral distinguisher with 2^{32} texts. b) A backward integral for three (full) rounds of AES with 2^{32} texts.

By applying the inside-out concatenation technique with the two previous properties, the authors of [12] could build a 7-round known key distinguisher (as shown on Fig. 2) against the AES. One chooses a structure of 2^{56} middle-texts: it has 7 active bytes whereas the other bytes are constant. We thus have 2^{24} sets of 2^{32} middletexts that represent first 2^{24} copies of the 4-round property (of Fig. 1.a) and also 2^{24} copies of the backward 3-round property (of Fig. 1.b). Then, when someone starts in the middle of the cipher, one can compute integral balanced property on both the reverse and forward directions.

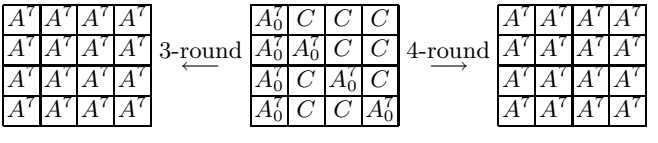

Fig. 2. The 7-round AES distinguisher with 2^{56} middle-texts. The 7th round is without MixColumns.

This known-key distinguisher simply records the frequencies in each byte of the plaintexts and ciphertexts, checks whether the values in each byte of the plaintexts and in each byte of the ciphertexts occur equally often. The time complexity is similar to the time it takes to do 2^{56} 7-round AES encryptions and the memory needed is small.

The authors of [12] introduce the k-sum problem (i.e. to find a collection of k texts $x_1, \cdots, x_k$ such as $\sum_{i=1}^{k} f(x_i) = 0$ for a given permutation f) with a

running time of $\mathcal{O}(k2^{n/(1+\log_2 k)})$ to conjecture that for a randomly chosen 128-bit permutation such a collection of texts with balanced properties could not be easily (i.e. in a reasonable computational time) found with a large probability. More precisely, the k-sum problem indicates with $n = 128$ and $k = 256$ a running time of 2^{58} operations ignoring small constants and memory. The k-sum problem is the best known approach in this case but does not give the particular balanced properties induced by the distinguisher. Thus, the authors conjecture that they have found a known-key distinguisher for AES reduced to 7 rounds using 2^{56} texts.

3.2 Rijndael-256

Thus, we have studied the same kind of properties for Rijndael-b. For the particular case of Rijndael-256, we have the two following forward and backward integral properties described in Fig. 3 and in Fig. 5. Note that the integral property of Fig. 3 could be extended by one round at the beginning using the method described in Fig. 4. This property is the one described in [7].

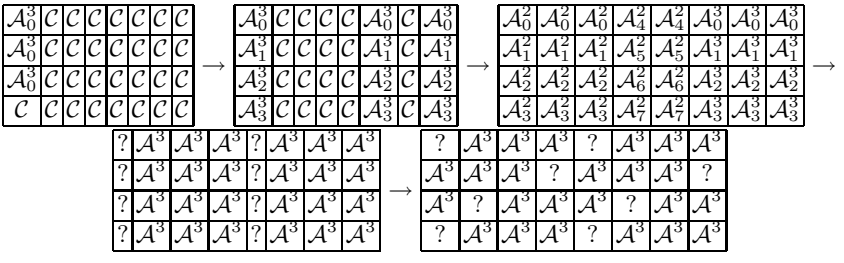

Fig. 3. 4-round 3th-order forward integral property of Rijndael-256 without the last MixColumns operation

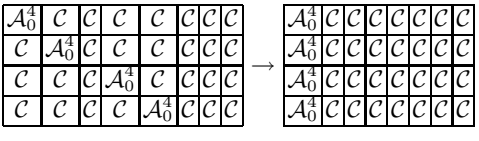

Fig. 4. Extension of a 4th order integral property by one round at the beginning for Rijndael-256

Using those two properties and the corresponding extension, we could build a 8-round known key distinguisher shown in Fig. 6. The process is exactly the same than the one described in 3.1 and the time complexity is similar to the time it takes to do 2^{40} 8-round Rijndael-256 encryptions and the memory needed is small. If we also use the k-sum problem to estimate the corresponding time to find a k-sum for a 256-bit permutation with $n = 256 - 64$ and $k = 2^{40}$, the

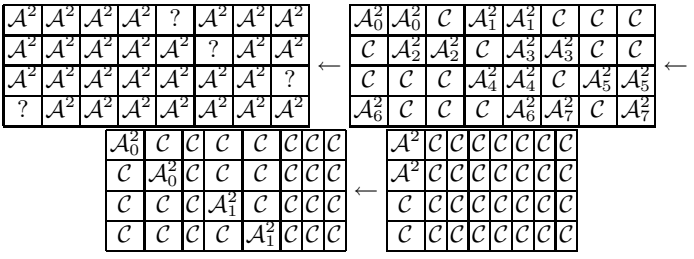

Fig. 5. The 2th-order backward 3-round integral property of Rijndael-256

corresponding complexity is around 2^{44} operations ignoring small constants and memory. Thus, we conjecture that we have found a known-key distinguisher for Rijndael-256 reduced to 8 rounds using 2^{40} middle-texts.

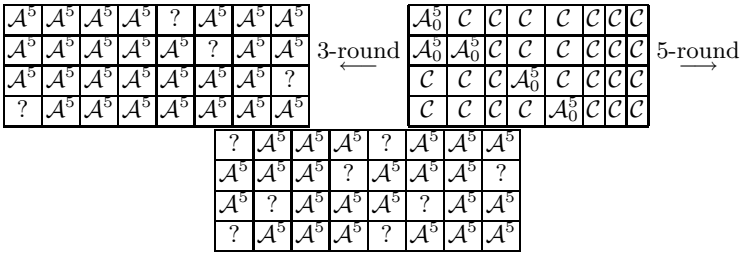

Fig. 6. The 8-round Rijndael-256 known-key distinguisher with 2^{40} middle-texts. The 8th round is without MixColumns.

3.3 Rijndael-224

Similarly, we found a 2th-order 4-round forward integral property for Rijndael-224 as shown in figure 7. We have found 42 2th-order integral properties (essentially the shifted ones). As previously done, this 2th-order four-round property could be extended by one round at the beginning using a 8th-order integral (considering that it represents 2^{48} copies of the 2th-order four-round integral). We also have found the backward 3-round 2-th order integral property for Rijndael-224 shown in Fig. 8.

Using those two properties and the corresponding extension, we could build a 8-round known key distinguisher shown in Fig. 9. The process is exactly the same than the one described in 3.1 and the time complexity is similar to the time it takes to do 2^{72} 8-round Rijndael-224 encryptions and the memory needed is small. If we also use the k-sum problem to estimate the corresponding time to find a k-sum for a 224-bit permutation with $n = 224 - 128$ and $k = 2^{72}$, the corresponding complexity is around $2^{73.8}$ operations ignoring small constants and memory. Thus, we conjecture that we have found a known-key distinguisher for Rijndael-224 reduced to 8 rounds using 2^{72} middle-texts.

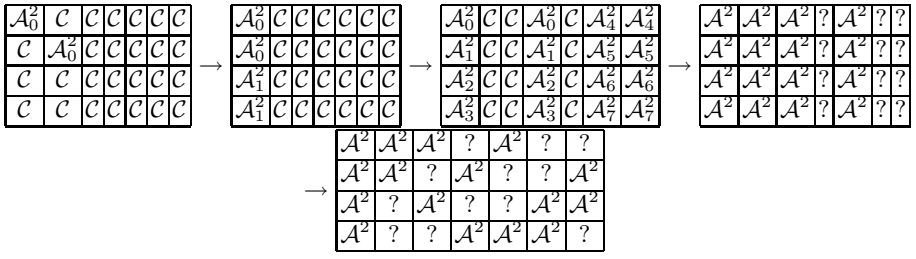

Fig. 7. Four-round 2th-order forward integral property of Rijndael-224. The last MixColumns is omitted.

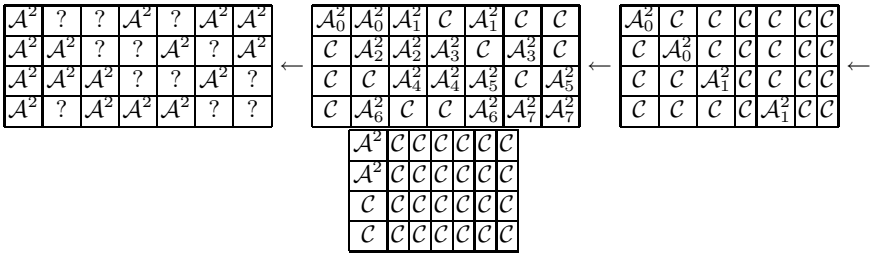

Fig. 8. The 2th-order 3-round backward integral property of Rijndael-224

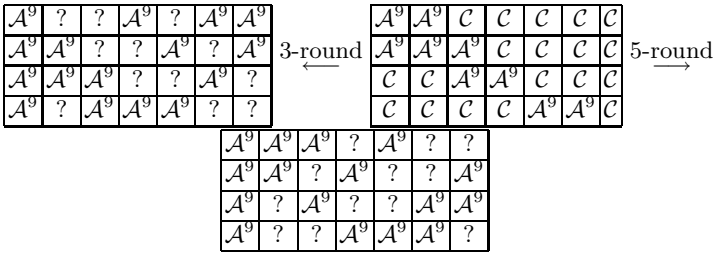

Fig. 9. The 8-round Rijndael-224 known-key distinguisher with 2^{72} middle-texts. The 8th round is without MixColumns.

3.4 Rijndael-192

In the same way, we have found a 3th-order forward 4-round integral property for Rijndael-192 as shown in Fig. 10. We have found 42 3th-order integral properties (essentially the shifted ones). We also have found the backward 2-th order integral property for Rijndael-224 shown in Fig. 11.

Using those two properties and the corresponding extension, we could build a 7-round known key distinguisher shown in Fig. 12. The process is exactly the same than the one described in 3.1 and the time complexity is similar to the time it takes to do 2^{32} 7-round Rijndael-192 encryptions and the memory needed is

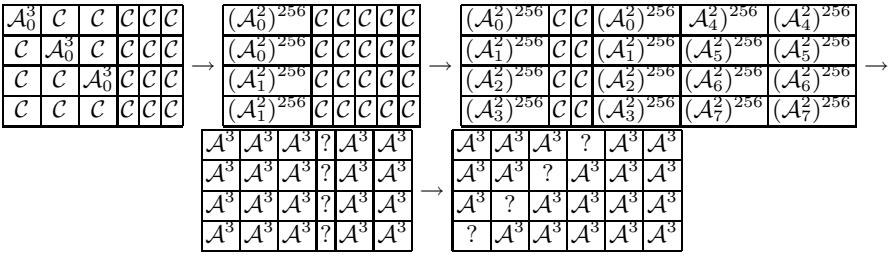

Fig. 10. The 3th-order 4-round forward integral property of Rijndael-192 (the last MixColumns is omitted)

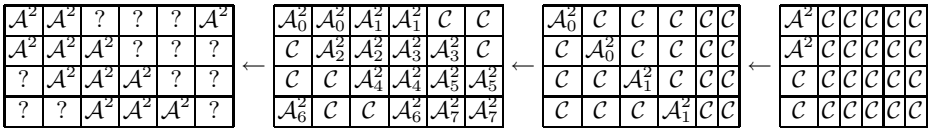

Fig. 11. 2th-order 3-round backward integral property of Rijndael-192

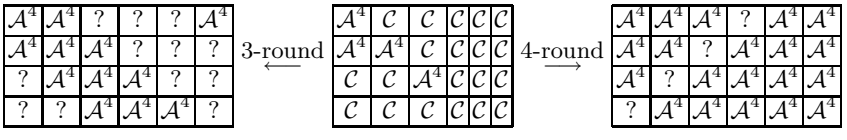

Fig. 12. The 7-round Rijndael-192 distinguisher with 2^{32} middle-texts. The 7th round is without MixColumns.

small. If we also use the k-sum problem to estimate the corresponding time to find a k-sum for a 192-bit permutation with $n = 192 - 96$ and $k = 2^{32}$, the corresponding complexity is around $2^{35.9}$ operations ignoring small constants and memory. Thus, we conjecture that we have found a known-key distinguisher for Rijndael-192 reduced to 7 rounds using 2^{32} middle-texts.

3.5 Rijndael-160

We also have found a 3th-order 4-round integral property for Rijndael-160 as shown in Fig. 13. We have found 42 3th-order integral properties (essentially the shifted ones). We also have found the backward 3-th order backward integral property for Rijndael-160 shown in Fig. 14.

Using those two backward and forward properties, we could build a 7-round known key distinguisher shown in Fig. 15. The process is exactly the same than the one described in 3.1 and the time complexity is similar to the time it takes to do 2^{40} 7-round Rijndael-160 encryptions and the memory needed is small. If we also use the k-sum problem to estimate the corresponding time to find a k-sum

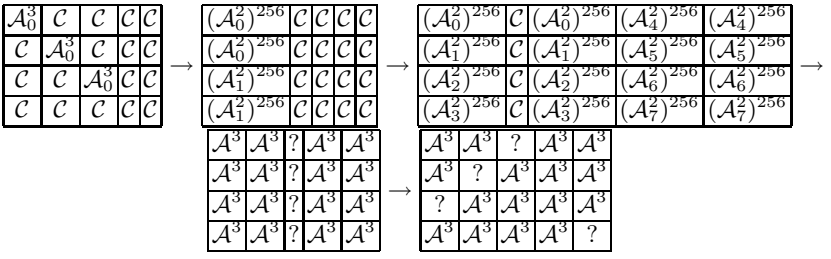

Fig. 13. 3th order 4-round forward integral property of Rijndael-160 (the last round is without MixColumns)

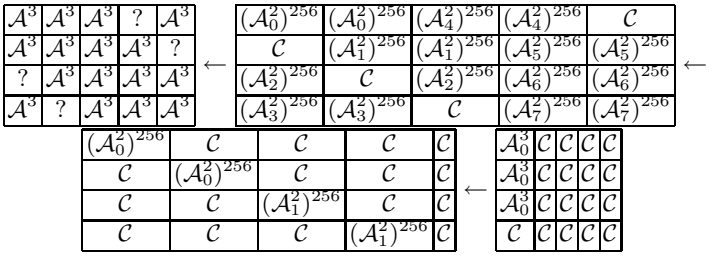

Fig. 14. 3th order integral backward property for Rijndael-160

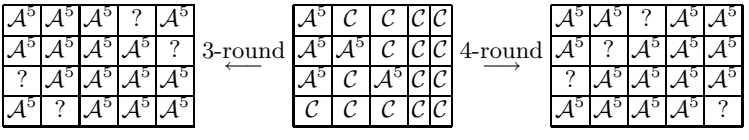

Fig. 15. The 7-round Rijndael-160 distinguisher with 2^{40} middle-texts. The 7th round is without MixColumns.

Table 2. Summary of known-key distinguishers on Rijndael-b. CM means Chosen Middle-texts.

Cipher	nb rounds	Key sizes	Data Complexity	Time Complexity	Memory	Source
AES	7	(all)	2^{56} CM	2^{56}	small	[12]
Rijndael-256	8	(all)	2^{40} CM	2^{40}	small	this paper
Rijndael-224	8	(all)	2^{72} CM	2^{72}	small	this paper
Rijndael-192	7	(all)	2^{32} CM	2^{32}	small	this paper
Rijndael-160	7	(all)	2^{40} CM	2^{40}	small	this paper

for a 160-bit permutation with $n = 160 - 32$ and $k = 2^{40}$, the corresponding complexity is around 2^{43} operations ignoring small constants and memory. Thus, we conjecture that we have found a known-key distinguisher for Rijndael-192 reduced to 7 rounds using 2^{40} middle-texts.

4 Conclusion

In this paper, we have shown how to build known-key distinguisher against the various versions of Rijndael-b using essentially particular new dth-order integral properties in forward and backward sense. Table 2 sums up the results presented in this paper.

Note that we have used as done in [12] the k-sum problem to estimate the corresponding complexity to build such distinguishers for random permutations. This model is less pertinent in our case because we need to estimate such a problem for random functions and no more for random permutations. Thus, we however think that the corresponding complexity is around to be the same even if this stays as an open problem.

References

1. Canetti, R., Goldreich, O., Halevi, S.: On the random oracle methodology, revisited. Journal of the ACM 51(4), 557–594 (2004)
2. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher Square. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997)
3. Daemen, J., Rijmen, V.: AES proposal: Rijndael. In: The First Advanced Encryption Standard Candidate Conference. N.I.S.T. (1998)
4. Daemen, J., Rijmen, V.: The Design of Rijndael. Springer, Heidelberg (2002)
5. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.: Improved cryptanalysis of rijndael. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 213–230. Springer, Heidelberg (2001)
6. FIPS 197. Advanced Encryption Standard. Federal Information Processing Standards Publication 197, U.S. Department of Commerce/N.I.S.T (2001)
7. Galice, S., Minier, M.: Improving integral attacks against Rijndael-256 up to 9 rounds. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 1–15. Springer, Heidelberg (2008)
8. Gilbert, H., Minier, M.: A collision attack on 7 rounds of Rijndael. In: AES Candidate Conference, pp. 230–241 (2000)
9. Nakahara Jr., J., de Freitas, D.S., Phan, R.C.-W.: New multiset attacks on Rijndael with large blocks. In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS, vol. 3715, pp. 277–295. Springer, Heidelberg (2005)
10. Junod, P.: On the optimality of linear, differential, and sequential distinguishers. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 17–32. Springer, Heidelberg (2003)
11. Knudsen, L.R.: Contemporary block ciphers. In: Damgård, I. (ed.) Lectures on Data Security. LNCS, vol. 1561, pp. 105–126. Springer, Heidelberg (1999)
12. Knudsen, L.R., Rijmen, V.: Known-key distinguishers for some block ciphers. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 315–324. Springer, Heidelberg (2007)

13. Knudsen, L.R., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
14. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing 17(2), 373–386 (1988)
15. Matyas, S.M., Meyer, C.H., Oseas, J.: Generating strong one-way functions with cryptographic algorithm. IBM Technical Disclosure Buletin 27, 5658–5659 (1985)
16. Preneel, B., Govaerts, R., Vandewalle, J.: Hash functions based on block ciphers: A synthetic approach. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 368–378. Springer, Heidelberg (1994)
17. Vaudenay, S.: Decorrelation: A theory for block cipher security. J. Cryptology 16(4), 249–286 (2003)