

The mini-square propagation over block cipher and its application to AES and Camellia

Anwar Hasan, Christophe Negre

► **To cite this version:**

Anwar Hasan, Christophe Negre. The mini-square propagation over block cipher and its application to AES and Camellia. 2011. <hal-00556843>

HAL Id: hal-00556843

<https://hal.archives-ouvertes.fr/hal-00556843>

Submitted on 26 Aug 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The mini-square propagation over block cipher and its application to AES and Camellia

M. A. Hasan¹ and C. Negre^{1,2,3}

¹ECE Department and CACR, University of Waterloo, Ontario, Canada.

²Team DALI, Université de Perpignan, France.

³LIRMM, Université Montpellier 2, France.

Abstract. In this paper we introduce the mini-square propagation: four ciphertexts corresponding to four plaintexts with some specific differences summing to zero after several rounds. We then extend this propagation by appending a linear propagation to the mini-square propagation and by preceding it with differential propagations. We apply this approach to block ciphers AES and Camellia.

1 Introduction

Differential cryptanalysis [3] is based on the propagation of differences through an encryption function. Since its introduction by Biham and Shamir [3], many techniques based on it have been proposed [12, 16, 13]. Higher-order differential cryptanalysis [12] is a generalization of this technique, it ensures the ciphertexts corresponding to well chosen plaintexts sum to zero. Square cryptanalysis [6] or integral cryptanalysis can be seen as variants or special cases. Generally the number of the messages involved in the differential propagation approaches is quite large.

In this paper we introduce the mini-square propagation. This can be seen as a variant of higher-order differential cryptanalysis. In the mini-square propagation, four ciphertexts corresponding to four plaintexts with some specific differences sum to zero after several rounds. This mini-square propagation doesn't use any property of the S-boxes involved in the encryption function involved.

Since there is only four ciphertexts involved in the mini-square propagation, some extensions with certain classic approach are possible. We present here two possible extensions of this mini-square propagation. The first one is based on the same strategy used in differential-linear cryptanalysis: we append a linear propagation to the mini-square propagation which provides a linear expression of the four ciphertexts after several additional rounds. We apply this approach to block cipher AES [5].

The second extension of the mini-square propagation consists of preceding the propagation by several classical differential propagations. We apply it to block cipher Camellia [1] to design a differential-mini-square propagation over 6 rounds.

2 Mini-square propagation

The mini-square propagation is based on the property that the ciphertexts corresponding to four well chosen plaintexts sum to zero. The purpose of this section is to state this

property primarily for a single round of a block cipher with substitution-permutation network (SPN) structure and then for several rounds.

2.1 Mini-square property of one round of a SPN

The following lemma is the starting point of the mini-square propagation.

Lemma 1. *We consider a vectorial boolean function $S: \{0, 1\}^m \rightarrow \{0, 1\}^m$ and two constants $C, \Omega \in \{0, 1\}^m$. The following function*

$$S_{C,\Omega}: \{0, 1\}^m \rightarrow \{0, 1\}^m \\ z \mapsto S(C + z\Omega)$$

is affine: there exists $\alpha, \beta \in \{0, 1\}^m$ such that $S(C + z\Omega) = z\alpha + \beta$.

Proof. If S is a boolean function we reduce the polynomial expression of $S(C + z\Omega)$ to a degree one using the identity $z^2 = z$. We extend easily this property to a vectorial boolean function. \square

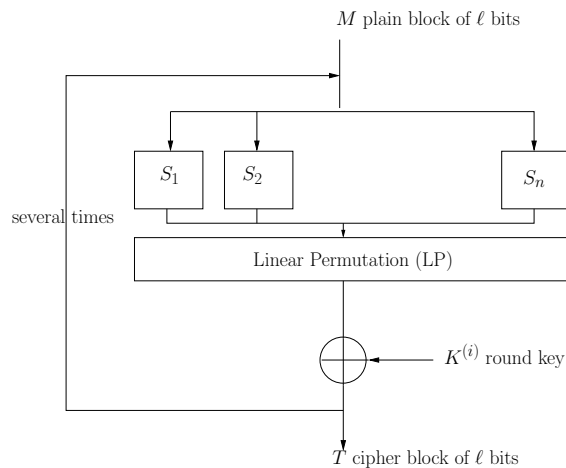
The following lemma states the mini-square property for an affine function which has two boolean variables. This result is a special case of the well known higher-order differential.

Lemma 2. *We consider a function*

$$f: \{0, 1\}^2 \rightarrow \{0, 1\}^m \\ (z, z') \mapsto z\alpha + z'\alpha' + \beta$$

Then we have $f(0, 0) + f(0, 1) + f(1, 0) + f(1, 1) = 0$.

The proof is straightforward and we omit it here. We now present the mini-square propagation on a single round of a block cipher with SPN structure. This propagation applies to SPNs such that each round consists of a layer of n parallel S-boxes (S_i for $i = 1, \dots, n$) followed by a linear permutation (LP) layer and a round key addition.



We fix C a constant value and two differences $\Omega = (\Omega_1, \dots, \Omega_n)$ and $\Omega' = (\Omega'_1, \dots, \Omega'_n)$, where Ω_i and Ω'_i are the differences entering in the i -th S-box S_i .

Definition 1 (Support). We define the support $Supp(\Omega)$ of $\Omega = (\Omega_1, \dots, \Omega_n)$ as

$$Supp(\Omega) = \{i \in \{1, \dots, n\} \text{ such that } \Omega_i \neq 0\}.$$

We assume now that $Supp(\Omega) \cap Supp(\Omega') = \emptyset$. Under this assumption, considering the data entering the different S-boxes for $S(C + z\Omega + z'\Omega')$, there are three cases:

- for $i \in Supp(\Omega)$, the input data of S_i is equal to $C_i + z\Omega_i$ since $i \notin Supp(\Omega')$. Consequently, using Lemma 1 the output of S_i is equal to $z\alpha_i + \beta_i$ for some α_i, β_i depending on C_i, Ω_i and S_i .
- if $i \in Supp(\Omega')$, the input of S_i is equal to $C_i + z'\Omega'_i$ since in this case $i \notin Supp(\Omega)$. Then the output of S_i is equal to $z'\alpha'_i + \beta_i$ for some α'_i and β_i .
- For $i \notin Supp(\Omega)$ and $i \notin Supp(\Omega')$, the input of S_i is equal to C_i and thus the output of S_i is constant and equal to $\beta_i = S_i(C_i)$.

Consequently, if we put together these three cases we obtain the following expression of $S(C + z\Omega + z'\Omega')$

$$S(C + z\Omega + z'\Omega') = z\alpha + z'\alpha' + \beta.$$

where α_i, α'_i and β_i are defined above. Now if apply the linear permutation to this previous expression and then add the round key K we obtain

$$\begin{aligned} Round_K(C + z\Omega + z'\Omega') &= LP(S(C + z\Omega + z'\Omega')) + K \\ &= LP(z\alpha + z'\alpha' + \beta) + K \\ &= zLP(\alpha) + z'LP(\alpha') + LP(\beta) + K. \end{aligned}$$

It we set $\gamma = LP(\alpha)$ and $\gamma' = LP(\alpha')$ and $\rho = LP(\beta) + K$ we obtain that

$$Round_K(C + z\Omega + z'\Omega') = z\gamma + z'\gamma' + \rho.$$

Combining this expression of $Round_K(C + z\Omega + z'\Omega')$ and Lemma 2 we obtain the following mini-square propagation for one round of a SPN.

Proposition 1 (Mini-square propagation over one round of a SPN). Let $Round_K$ be a round function of a block cipher with a SPN structure consisting of a substitution layer through n parallel S-boxes, followed by a linear transformation and a round key addition. Let Ω and Ω' be two differences such that $Supp(\Omega) \cap Supp(\Omega') = \emptyset$ and let C be any constant block. Then there exist some constants γ, γ' and ρ such that

$$Round_K(C + z\Omega + z'\Omega') = z\gamma + z'\gamma' + \rho$$

and

$$Round_K(C) + Round_K(C + \Omega) + Round_K(C + \Omega') + Round_K(C + \Omega + \Omega') = 0.$$

2.2 Mini square propagation over several SPN rounds

Our purpose here is to extend the one round mini-square propagation of the previous subsection to several rounds. Actually we just need to apply the one round mini-square propagation iteratively. We will note $E_{i \rightarrow j}(M)$ the reduced encryption function which consists of ciphering from the i -th round to the j -th round.

1. We start in the first round with an arbitrary constant $C^{(0)}$ and with $\Omega^{(0)}$ with only one $\Omega_i^{(0)} \neq 0$ and $\Omega'^{(0)}$ with only one $\Omega'_j{}^{(0)} \neq 0$ where $i \neq j$.
2. Using Proposition 1 we know that the one round cipher of $C^{(0)} + z\Omega^{(0)} + z'\Omega'^{(0)}$ satisfies

$$\text{Round}_K(C^{(0)} + z\Omega^{(0)} + z'\Omega'^{(0)}) = C^{(1)} + z\Omega^{(1)} + z'\Omega'^{(1)}$$

for some $C^{(1)}$, $\Omega^{(1)}$ and $\Omega'^{(1)}$.

3. Then, if $\Omega^{(1)}$ and $\Omega'^{(1)}$ have disjoint support, we can again use Proposition 1 which gives that the cipher after the second round is

$$E_{1 \rightarrow 2}(C^{(0)} + z\Omega^{(0)} + z'\Omega'^{(0)}) = C^{(2)} + z\Omega^{(2)} + z'\Omega'^{(2)}$$

for some $C^{(2)}$, $\Omega^{(2)}$ and $\Omega'^{(2)}$.

4. We repeat this process up to the round r which satisfies $\text{Supp}(\Omega^{(r)}) \cap \text{Supp}(\Omega'^{(r)}) \neq \emptyset$. At this step, we cannot extend further the mini-square propagation, since we cannot apply Proposition 1.
5. But we know that the ciphertext after the r -th round is

$$E_{1 \rightarrow r}(C^{(0)} + z\Omega^{(0)} + z'\Omega'^{(0)}) = C^{(r)} + z\Omega^{(r)} + z'\Omega'^{(r)}$$

and this implies following the mini-square formula for r rounds

$$E_{1 \rightarrow r}(C^{(0)}) \oplus E_{1 \rightarrow r}(C + \Omega^{(0)}) \oplus E_{1 \rightarrow r}(C + \Omega'^{(0)}) \oplus E_{1 \rightarrow r}(C + \Omega^{(0)} + \Omega'^{(0)}) = 0.$$

3 Extension at the bottom using linear propagation

We append a linear propagation to the mini-square propagation. This strategy is a straightforward application of the differential-linear method [13, 2]. In the sequel we will denote $T^{(i)}$ the partial ciphertext output by the i -th round.

We assume that there exists a mini square propagation over r rounds

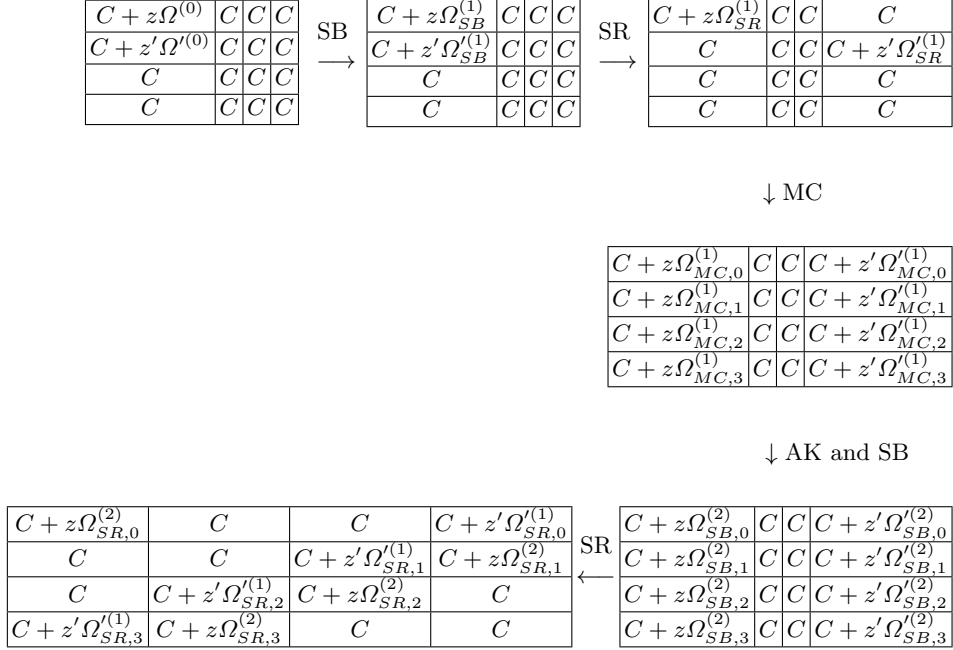
$$\left\{ \begin{array}{l} M_0 = M, \\ M_1 = M \oplus \Omega^{(0)}, \\ M_2 = M \oplus \Omega'^{(0)}, \\ M_3 = M \oplus \Omega^{(0)} \oplus \Omega'^{(0)} \end{array} \right\} \xrightarrow{r \text{ rounds}} T_0^{(r)} \oplus T_1^{(r)} \oplus T_2^{(r)} \oplus T_3^{(r)} = 0 \quad (1)$$

where $T_i^{(r)}$ is the cipher text after r rounds of the plain text M_i .

We further assume that there exists a linear propagation between the input of the $(r+1)$ -th round and the output of the s -th round of the considered SPN:

$$\lambda \cdot T^{(r)} \oplus \mu \cdot T^{(s)} = 0, \quad (2)$$

Fig. 1. Mini square propagation over two rounds of AES



and we assume that this propagation occurs with probability $p = 1/2 + \varepsilon$ with $|\varepsilon| \leq 1/2$. The piling-up lemma [14] tells us that the following cumulated propagations

$$\bigoplus_{i=0}^3 \left(\lambda \cdot T_i^{(r)} \oplus \mu \cdot T_i^{(s)} \right) = 0. \quad (3)$$

occurs with probability $1/2 + 2^3\varepsilon^4$. Now if we combine (3) with the mini-square propagation (1) we obtain that the identities $\mu \cdot \left(\bigoplus_{i=0}^3 T_i^{(s)} \right) = 0$ occurs with probability $1/2 + 2^3\varepsilon^4$.

3.1 Application to AES

AES is a block cipher which uses 128 bit block and consists of 10, 12 or 14 rounds (depending on the key size). Each round consists of SubByte (SB), ShiftRow (SR), MixColumn (MC) and AddKey (AK) operations. For a complete description the reader may refer to [5].

The mini square propagation. In Fig. 1 we describe a two-rounds mini-square propagation for AES. We have used the following notation:

- the symbol C means the considered byte is constant, i.e., it does not depend on z or z' .
- z, z' are independent boolean variables,
- and $\Omega^{(i)}$ and $\Omega'^{(i)}$ are differences in the i -th round. We also specify the layer which outputs this difference with the subscripts SB, SR, MC or AK.

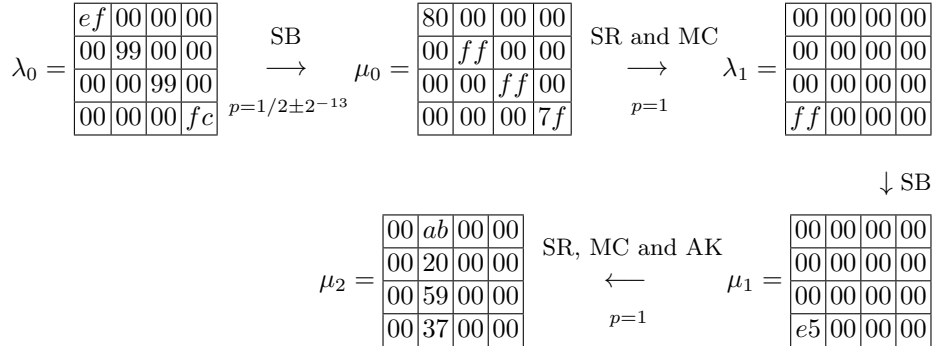
Afterwards, we apply the MixColumn and the AddKey to the block output by the ShiftRow of the second round. We obtain the following block

$$T_{z+2z'}^{(2)} = [C_{(i,j)} + z\Omega_{(i,j)}^{(2)} + z'\Omega'_{(i,j)}{}^{(2)}]_{i,j=0,\dots,3}.$$

We remark that the block $T_{z+2z'}^{(2)}$ has an affine expression in z and z' . Consequently, using Lemma 2 we have

$$T_0^{(2)} + T_1^{(2)} + T_2^{(2)} + T_3^{(2)} = 0.$$

The linear propagation. We have a mini-square propagation over two rounds of AES. We would like to extend this propagation by appending a linear propagation. We have analyzed the linear propagation of the S-box used in AES, to derive a linear propagation over two rounds. We have found a two-rounds linear propagation with 5 active S-boxes with a bias equal to $\pm 2^{-16}$. This two-rounds linear propagation is shown in the diagram below



The resulting attack over 6 rounds of AES. The mini-square-linear propagation over 4 rounds of AES uses is as follows

$$\left\{ \begin{array}{l} M_0 = M, \\ M_1 = M \oplus \Omega^{(0)}, \\ M_2 = M \oplus \Omega'^{(0)}, \\ M_3 = M \oplus \Omega^{(0)} \oplus \Omega'^{(0)} \end{array} \right\} \rightarrow \mu_2 \cdot (T_0^{(4)} \oplus T_1^{(4)} \oplus T_2^{(4)} \oplus T_3^{(4)}) = 0,$$

and this propagation occurs with probability $p = 1/2 + 2^{-61}$.

Using this propagation it is possible to design an attack over AES reduced to 5, 6 or 7 rounds. So far, the resulting attacks don't have a lower complexity with regard to

either data storage or computation compared to the best known attack of AES [7, 11, 8, 4, 18].

Consequently we only sketch the attack over 6 rounds in order to give an idea of the complexity involved in the mini-square-linear attacks. The attack over 6 rounds requires 2^{122} pairs of chosen plaintext-ciphertext. By guessing four bytes of the key in the first round and four bytes of the key in the 6-th round we can distinguish the right key bytes with a computational effort of $2^{122+64} = 2^{188}$ by peeling off partially the first round and the last round.

4 Extension at the top using differential propagation

In this section we present a strategy to extend a mini-square propagation by preceding it with two differential propagations. We will then illustrate this process in the case of block cipher Camellia. We consider a block cipher with a SPN structure and we assume that there exists a mini-square propagation between the r -th round and the s -th round of the considered SPN

$$(T_0^{(r)}, T_0^{(r)} \oplus \Omega^{(r)}, T_0^{(r)} \oplus \Omega'^{(r)}, T_0^{(r)} \oplus \Omega^{(r)} \oplus \Omega'^{(r)}) \longrightarrow \oplus_{i=0}^3 T_i^{(s)} = 0$$

We extend this propagation using two differential propagations $\Omega^{(0)} \rightarrow \Omega^{(r)}$ and $\Omega'^{(0)} \rightarrow \Omega'^{(r)}$ between the first and the r -th round. We use these propagations as follows

$$\begin{aligned} (T_0^{(0)}, T_0^{(0)} \oplus \Omega^{(0)}) &\rightarrow (T_0^{(r)}, T_0^{(r)} \oplus \Omega^{(r)}), \\ (T_0^{(0)}, T_0^{(0)} \oplus \Omega'^{(0)}) &\rightarrow (T_0^{(r)}, T_0^{(r)} \oplus \Omega'^{(r)}), \\ (T_0^{(0)} \oplus \Omega^{(0)}, T_0^{(0)} \oplus \Omega'^{(0)}) &\rightarrow (T_0^{(r)} \oplus \Omega^{(r)}, T_0^{(r)} \oplus \Omega'^{(r)}). \end{aligned}$$

This provides the three differences required in the mini-square propagation. A quick evaluation of the probability of the simultaneous occurrence of these propagations gives $pp' \max(p, p')$, where p and p' are the corresponding probabilities of the two individual differential propagations $\Omega^{(0)} \rightarrow \Omega^{(r)}$ and $\Omega'^{(0)} \rightarrow \Omega'^{(r)}$. In order to obtain a better probability, we consider here two differential propagations which have specific properties as stated in the following lemma.

Lemma 3. *We consider two differential propagations over r rounds of a SPN*

$$\Omega^{(0)} \rightarrow \Omega^{(r)} \text{ and } \Omega'^{(0)} \rightarrow \Omega'^{(r)}$$

which occurs with probabilities p and p' respectively. We further assume that for each $i = 0, \dots, r-1$, $\text{Supp}(\Omega^{(i)}) \cap \text{Supp}(\Omega'^{(i)}) = \emptyset$ where $\Omega^{(i)}$ and $\Omega'^{(i)}$ are the intermediate differences of the considered differential propagation. Then if we fix M a plaintext, T its r -rounds ciphertext, and define

$$T_0^{(0)} = M, \quad T_1^{(0)} = M \oplus \Omega^{(0)}, \quad T_2^{(0)} = M \oplus \Omega'^{(0)}, \quad T_3^{(0)} = M \oplus \Omega^{(0)} \oplus \Omega'^{(0)},$$

then the following simultaneous differential propagations occurs with probability pp'

$$(T_0^{(0)}, T_1^{(0)}, T_2^{(0)}, T_3^{(0)}) \xrightarrow{r \text{ rounds}} (T, T \oplus \Omega^{(r)}, T \oplus \Omega'^{(r)}, T \oplus \Omega^{(r)} \oplus \Omega'^{(r)}).$$

Proof. We only prove it for one round, the extension to several rounds is straightforward. We first write $T_i^{(0)} = [t_{i,0}^{(0)}, t_{i,1}^{(0)}, \dots, t_{i,n-1}^{(0)}]$ where $t_{i,j}^{(0)}$ is the entry of the j -th S-box for $T_i^{(0)}$. We will also denote $\Lambda = LP^{-1}(\Omega^{(1)})$ and $\Lambda' = LP^{-1}(\Omega'^{(1)})$. Let $T_0^{(1)} = \text{Round}_K(T_0^{(0)})$, we assume that the two following propagations occurs simultaneously

$$\begin{aligned} T_1^{(0)} &= M \oplus \Omega^{(0)} \rightarrow T_0^{(1)} \oplus \Omega^{(1)}, \\ T_2^{(0)} &= M \oplus \Omega'^{(0)} \rightarrow T_0^{(1)} \oplus \Omega'^{(1)}. \end{aligned}$$

Now, we apply the S-box layer to $T_3^{(0)}$ and we have three situations

- if $j \in \text{Supp}(\Omega^{(0)})$, then $j \notin \text{Supp}(\Omega'^{(0)})$ which implies $t_{3,j}^{(0)} = t_{1,j}^{(0)}$ and thus $S_j(t_{3,j}^{(0)}) = S(t_{1,j}^{(0)}) = S_j(t_{0,j}^{(0)}) \oplus \lambda_j$,
- if $j \in \text{Supp}(\Omega'^{(0)})$, then $j \notin \text{Supp}(\Omega^{(0)})$ which implies $t_{3,j}^{(0)} = t_{2,j}^{(0)}$ and thus $S_j(t_{3,j}^{(0)}) = S_j(t_{2,j}^{(0)}) = S_j(t_{0,j}^{(0)}) \oplus \lambda'_j$,
- if $j \notin \text{Supp}(\Omega^{(0)})$ and $j \notin \text{Supp}(\Omega'^{(0)})$, then $t_{3,j}^{(0)} = t_{0,j}^{(0)}$ and thus $S_j(t_{3,j}^{(0)}) = S_j(t_{0,j}^{(0)})$.

Now if we put all these three cases together we obtain $S(T_3^{(0)}) = S(T_0^{(0)}) \oplus \Lambda \oplus \Lambda'$. If we then apply the linear transformation and add the round key we obtain $\text{Round}_K(T_3^{(0)}) = T_0^{(1)} \oplus \Omega^{(1)} \oplus \Omega'^{(1)}$ and this concludes the proof. \square

4.1 Application to Camellia

Camellia is a block cipher with a block size of 128 bits. There are three variants of Camellia: the first one uses 128 bit keys and 18 rounds, the second uses 192 bit keys and 24 rounds and the third one uses 256 bit keys and 24 rounds. Each variants consists of successive round function which has a Feistel structure. Each 6 rounds a specific key dependant affine function is applied: the (FL, FL^{-1}) layer. The function F used in the Feistel structure applies on the right half of the message block and consists of an addition of a round key followed by an S-box layer and a linear permutation. For a complete specification of Camellia we refer to [1].

We present now the differential-mini-square propagation over 6 rounds of Camellia with a (FL, FL^{-1}) layer between the 3rd and the 4th round. The propagation uses a combination of a three rounds differentials propagation and a three round mini-square propagation (which includes the (FL, FL^{-1}) layer).

Differential trails. The first differential propagation over three regular rounds is the following

$$\begin{aligned} (\Omega_L^{(0)}, \Omega_R^{(0)}) &= (0x1111001111110011, 0x0000000000001100) \rightarrow \\ (\Omega_L^{(1)}, \Omega_R^{(1)}) &= (0x0000000000001100, 0x0000000000000000) \rightarrow \\ (\Omega_L^{(2)}, \Omega_R^{(2)}) &= (0x0000000000000000, 0x0000000000001100) \rightarrow \\ (\Omega_L^{(3)}, \Omega_R^{(3)}) &= (0x0000000000001100, 0x1111001111110011) \end{aligned}$$

The second differential propagation is the following

$$\begin{aligned}
(\Omega'_L{}^{(0)}, \Omega'_R{}^{(0)}) &= (0x1111110000000000, 0x0000000000000011) \rightarrow \\
(\Omega'_L{}^{(1)}, \Omega'_R{}^{(1)}) &= (0x0000000000000011, 0x0000000011111100) \rightarrow \\
(\Omega'_L{}^{(2)}, \Omega'_R{}^{(2)}) &= (0x0000000011111100, 0x0000001100000000) \rightarrow \\
(\Omega'_L{}^{(3)}, \Omega'_R{}^{(3)}) &= (0x0000001100000000, 0x1111001111110011)
\end{aligned}$$

The support of the two intermediate differentials are disjoint, consequently Lemma 3 applies. The S-box differentials involved in the two differentials are all $0x11 \rightarrow 0x11$ which have for all S-boxes a probability of $1/2^7$. Consequently the simultaneous propagations of (4) over the three rounds have probability 2^{-49} .

$$\left\{ \begin{array}{l} M_0, \\ M_1 = M_0 \oplus \Omega^{(0)}, \\ M_2 = M_0 \oplus \Omega'^{(0)}, \\ M_3 = M_0 \oplus \Omega^{(0)} \oplus \Omega'^{(0)} \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} T_0^{(3)}, \\ T_0^{(3)} \oplus \Omega^{(3)}, \\ T_0^{(3)} \oplus \Omega'^{(3)}, \\ T_0^{(3)} \oplus \Omega^{(3)} \oplus \Omega'^{(3)}. \end{array} \right\} \quad (4)$$

Mini-square propagation. We assume now that the differential propagation (4) described in the previous subsection occurs. Consequently the messages entering the (FL, FL^{-1}) layer are $T_{z+2z'}^{(3)} = T_0^{(3)} \oplus z\Omega^{(3)} \oplus z'\Omega'^{(3)}$ for $z, z' \in \{0, 1\}$.

It can be proven (the proof is given in the appendix) that after one (FL, FL^{-1}) layer and three regular Feistel rounds the resulting ciphertexts $T_0^{(6)}, T_1^{(6)}, T_2^{(6)}, T_3^{(6)}$ satisfies

$$P^{-1}(T_{z+2z',L}^{(6)}) = (\mu'_0 + (z+z')\lambda'_0, \mu'_1 + (z+z')\lambda'_1, ?, \mu'_4 + (z+z')\lambda'_4, \mu'_5 + (z+z')\lambda'_5, ?, ?)$$

where P is the linear permutation in the function F of Camellia and μ_i, μ'_i, λ_i are some unknown constants. Then, using Lemma 2, we deduce that the sum of $P^{-1}(T_{i,L}^{(6)})$ for $i = 0, 1, 2, 3$ satisfies

$$\bigoplus_{i=0}^3 P^{-1}(T_{i,L}^{(6)}) = (0, 0, ?, ?, 0, 0, ?, ?). \quad (5)$$

Differential-mini-square attack on Camellia. We only discuss here a simple version of the attack using the differential-mini-square propagation over 7 rounds of Camellia. We use the formulas of [15] to establish the required number of plaintext-ciphertext for a probability of success $\cong 0.9$. This number is equal to 2^{68} quartets of plaintext-ciphertext which satisfies the differences $\Omega^{(0)}, \Omega'^{(0)}$ and $\Omega^{(0)} \oplus \Omega'^{(0)}$. Then we guess four bytes of the 7-th round key such that we can peel-off the last round and compute the four byte which sum to zero in (5). Then if the four byte sums if a considered quartet are equal to zero we increment a counter attached to the key. The total computational complexity of this attack is equal to 2^{102} round operations.

The best known attacks on reduced-round Camellia including the (FL, FL^{-1}) layer are square attack [10, 17] and higher order differential [17, 9]. If we compare mini-square attack to these attacks [9], we remark that the differential-mini-square attack is less efficient. In the higher order differential approach or the square attack, the probability of propagation is equal to 1, consequently the required number of plaintext-ciphertext is lower and the resulting computation complexity is also lower.

5 Conclusion

We have presented in this paper the concept of the mini-square propagation over a block cipher: for a well chosen quartet of plaintexts, the corresponding ciphertexts, after several rounds of a block cipher with SPN structure, are equal to zero when added together. One particularity of the mini-square propagation is that it only requires four plaintext-ciphertext pairs. This small number of messages involved in the propagation make the extension of the propagation possible by a regular differential propagation and/or a linear propagation. We have presented a mini-square propagation over two rounds of AES and its extension to a four rounds mini-square-linear propagation. For the best of our knowledge this type of propagation was unknown. We have also presented a mini-square propagation over three rounds of Camellia and its extension to a six rounds as a differential-mini-square propagation.

References

1. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In *Proceedings of the 7th Annual International Workshop on Selected Areas in Cryptography, SAC '00*, pages 39–56, London, UK, 2001. Springer-Verlag.
2. E. Biham, O. Dunkelman, and N. Keller. Enhancing Differential-Linear Cryptanalysis. In *Advances in Cryptology - ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 254–266. Springer, 2002.
3. E. Biham and A. Shamir. *Differential cryptanalysis of the data encryption standard*. Springer-Verlag, London, UK, 1993.
4. A. Biryukov. The boomerang attack on 5 and 6-round reduced aes. In *AES Conference 2004*, volume 3373 of *LNCS*, pages 11–15. Springer, 2005.
5. J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.
6. Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The Block Cipher Square. In *Fast Software Encryption (FSE'97)*, volume 1267 of *LNCS*, pages 149–165, London, UK, 1997. Springer-Verlag.
7. H. Demirci and A.A. Selçuk. A meet-in-the-middle attack on 8-round aes. In *Fast Software Encryption (FSE 2008)*, volume 5086 of *LNCS*, pages 116–126, 2008.
8. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting. Improved cryptanalysis of rijndael. In *Fast Software Encryption (FSE 2000)*, volume 1978 of *LNCS*, pages 213–230, 2000.
9. Y. Hatano, H. Sekine, and T. Kaneko. Higher Order Differential Attack of Camellia (II). In *Selected Areas in Cryptography, SAC'2002*, volume 2595 of *LNCS*, pages 129–146, 2003.
10. Y. He and S. Qing. Square Attack on Reduced Camellia Cipher. In *Proceedings of the Third International Conference on Information and Communications Security (ICICS 2001)*, *LNCS*, pages 238–245, London, UK, UK, 2001. Springer.
11. G. Henri and M. Minier. A Collision Attack on 7 Rounds of Rijndael. In *AES Candidate Conference*, pages 230–241, 2000.
12. L. R. Knudsen. Truncated and higher order differentials. In *Fast Software Encryption (FSE'94)*, volume 1008 of *LNCS*, pages 196–211. Springer, 1995.
13. S. K. Langford and M. E. Hellman. Differential-Linear Cryptanalysis. In *Advances in Cryptology - CRYPTO '94*, volume 839 of *LNCS*, pages 17–25, 1994.

14. M. Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '93, pages 386–397. Springer-Verlag New York, Inc., 1994.
15. Ali Aydin Selçuk. On Probability of Success in Linear and Differential Cryptanalysis. *J. Cryptology*, 21(1):131–147, 2008.
16. David Wagner. The Boomerang Attack. In *Fast Software Encryption (FSE'99)*, volume 1636 of *LNCS*, pages 156–170. Springer, 1999.
17. Y. Yeom. Integral Cryptanalysis and Higher Order Differential Attack. *Trends in Mathematics (ICMS)*, 8(1):101–118, june 2005.
18. W. Zhang, W. Wu, and D. Feng. New results on impossible differential cryptanalysis of reduced aes. In *Information Security and Cryptology (ICISC) 2007*, volume 4817 of *LNCS*, pages 239–250. Springer, 2007.

A Proof of the mini-square propagation of Camellia

Before proceeding in the proof concerning the expression of $P^{-1}(T_{z+2z',L}^{(6)})$ we need to rewrite the expression of the function FL . This function operates on a 64 bit block X which is split in two 32 bit blocks $X = (X_L, X_R)$. The FL function is then defined in [1] as follows

$$FL(X_L, X_R) = (Y_L, Y_R) \text{ where } \begin{cases} Y_R = ((X_L \& K_L) \lll 1) \wedge X_R, \\ Y_L = ((Y_R \mid K_L) \lll 1) \wedge X_R. \end{cases}$$

This former expression can be rewritten in an affine form

$$FL(X_L, X_R) = (((X_L \cdot K') \lll 1) + X_R \cdot (K_R + 1) + K_R, \quad (6) \\ ((X_L \cdot K_L) \lll 1) + X_R)$$

where $K' = ((K_L \cdot ((K_R + 1) \ggg 1)) + K_L)$. The inverse function FL^{-1} of FL has a similar affine expression, but we don't need this expression here: knowing that FL^{-1} is affine is sufficient to obtain the 3-round mini-square propagation.

Let us now proceed in the proof of the affine expression of $P^{-1}(T_{z+2z',L}^{(6)})$. We assume that the 3rd round ciphertexts satisfy $T_{z+2z'}^3 = C^{(3)} + z\Omega^{(3)} + z'\Omega'^{(3)}$ with

$$\Omega^{(3)} = (0, 0, 0, 0, 0, 0, \delta^{(3)}, 0 \mid \Omega_{3,R}), \\ \Omega'^{(3)} = (0, 0, 0, \delta'^{(3)}, 0, 0, 0, 0 \mid \Omega_{3,R}).$$

This is the case when the two differential propagations of (4) occurs. We now successively apply the (FL, FL^{-1}) layer and rounds 4, 5 and 6 in order to obtain the required expression of $P^{-1}(T_{z+2z',L}^{(6)})$.

- *Layer* (FL, FL^{-1}) . We apply (FL, FL^{-1}) to $T_{z+2z'}^{(3)}$. We will denote $T_{z+2z'}^{(FL)}$ the resulting block. Using the expression of FL of (6) we obtain for the left half of $T_{z+2z'}^{(FL)}$

$$T_{z+2z',L}^{(FL)} = C_L^{(FL)} + (0, 0, z\delta_1^{(FL)} + z'\delta_1'^{(FL)}, z'\delta_2'^{(FL)}, 0, 0, z\delta_2^{(FL)} + z'\delta_3'^{(FL)}, z'\delta_4'^{(FL)}).$$

Now, since FL^{-1} is an affine function, we have

$$T_{z+2z',R}^{(FL)} = C_R^{(FL)} + (z + z')\Omega_R^{(FL)}.$$

- *Round 4.* Let us push the mini-square propagation through the 4-th round. The left half is just a copy of the right part $T_{z+2z',L}^{(4)} = T_{z+2z',R}^{(FL)}$. For the right half we first need to apply the F function to $T_{z+2z',R}^{(FL)}$. The expression of $T_{z+2z',R}^{(FL)}$ is affine in the indeterminate $z + z'$. Consequently using Lemma 1 we have

$$S(T_{z+2z',R}^{(3)} + K^{(4)}) = \alpha + (z + z')\beta,$$

and then applying the linear permutation P we get $F(T_{z+2z',R}^{(3)}) = P(\alpha) + (z + z')P(\beta) = \alpha' + (z + z')\beta'$. Finally, we add $T_{z+2z',L}^{(FL)}$ to this expression of $F(T_{z+2z',R}^{(FL)})$ which gives

$$\begin{aligned} T_{z+2z',R}^{(4)} &= C_L^{(FL)} + (0, 0, z\delta_1^{(FL)} + z'\delta_1^{(FL)}, z'\delta_2^{(FL)}, 0, 0, z\delta_2^{(FL)} + z'\delta_3^{(FL)}, z'\delta_4^{(FL)}) \\ &\quad + \alpha' + (z + z')\beta' \\ &= C_R^{(4)} + (0, 0, z\delta_1^{(4)} + z'\delta_1^{(4)}, z\delta_2^{(4)} + z'\delta_2^{(4)}, 0, 0, z\delta_3^{(4)} + z'\delta_3^{(4)}, z\delta_4^{(4)} + z'\delta_4^{(3)}) \\ &\quad + (z + z')(\beta'_0, \beta'_1, 0, 0, \beta'_4, \beta'_5, 0, 0) \end{aligned}$$

- *Round 5.* We apply the 5-th round to $T_{z+2z',L}^{(4)}$. We don't need the left half, so we proceed only on the right half. For the right half, we add the round key and apply the S-boxes: with Lemma 1 we have

$$S(T_{z+2z',R}^{(4)} + K^{(5)}) = (\mu_0 + (z + z')\lambda_0, \mu_1 + \lambda_1, ?, ?, \mu_4 + \lambda_4, \mu_5 + \lambda_5, ?, ?) \quad (7)$$

Then symbol “?” means that the expression is quadratic in z, z' and the resulting sum over z and z' is unknown. Now we have

$$P^{-1}(T_{z+2z',R}^{(5)}) = P^{-1}(T_{z+2z',L}^{(4)}) + S(T_{z+2z',R}^{(4)} + K^{(5)}).$$

Using (7) and the fact that $T_{z+2z',L}^{(4)}$ is affine in $(z + z')$ we obtain

$$P^{-1}(T_{z+2z',R}^{(5)}) = (\mu'_0 + (z + z')\lambda'_0, \mu'_1 + (z + z')\lambda'_1, ?, ?, \mu'_4 + (z + z')\lambda'_4, \mu'_5 + (z + z')\lambda'_5, ?, ?)$$

- *Round 6.* We only consider the left half of the block output by the 6-th round. We have $T_{z+2z',L}^{(6)} = T_{z+2z',R}^{(5)}$ and thus $P^{-1}(T_{z+2z',L}^{(6)}) = P^{-1}(T_{z+2z',R}^{(5)})$ which is given above. This ends the proof.