Invariant subspaces in Simpira

Sondre Rønjom

Nasjonal sikkerhetsmyndighet, Oslo, Norway
sondrer@gmail.com

Abstract. In this short note we report on invariant subspaces in Simpira in the case of four registers. In particular, we show that the whole input space (respectively output space) can be partitioned into invariant cosets of dimension 56 over $\mathbb{F}_{2^8}^{64}$. These invariant subspaces are found by exploiting the *non-invariant* subspace properties of AES together with the particular choice of Feistel configuration. Though we give the invariant subspaces for $b = 4$ in this paper, we remark that there are invariant subspaces in several of the Simpira instances; these can be determined with only minor adjustments to the analysis in this paper.

1 Introduction

Invariant subspace cryptanalysis was introduced by Leander et. al. in [2] and has been further developed in for instance [3]. A coset of a vector space is called invariant relative to a function $f(x)$, if it is mapped to itself through it. Typically $f(x)$ is a block cipher permutation. Subspace cryptanalysis is typically of interest for block ciphers consisting of round functions with a high degree of symmetry. Several examples have shown that it can be quite easy to find these spaces if one cares to look for them. If it is difficult to identify such spaces by hand, an alternative approach is to go "fish for subspaces". For instance, for a byte-based block cipher, one simply encrypt all values for a particular byte (or fixed set of bit positions in bit-based designs) for several rounds and check whether the resulting ciphertexts span a coset of a subspace; the structure of the resulting subspace can then reveal the structure of more complicated invariant subspaces which could be hard to detect by inspection. An algorithm for finding invariant subspaces was also introduced in [3].

In Simpira we identify large invariant subspaces by exploiting the non-invariant subspace properties of AES. Concretely, when $b = 4$ we identify a large subspace U such that any coset of this space is invariant of the composition of two Simpira rounds. Thus, any coset of the plaintext is invariant over infinitely many even rounds. This is as far as we know the first time the plaintext space has been partitioned completely into cosets that are invariant of a block cipher permutation. Concretely, the invariant cosets of Simpira is spanned by $(x_1, MC \circ SR(z_1 \oplus y \oplus c_1), x_3, MC \circ SR(z_2 + y + c_2)$ where c_1 and c_2 are fixed 4×4 constant (random) matrices, z_i is a 4×4 matrix formed by setting the first two columns to all possible values, y is formed by setting the last two columns

to all possible values, and x_1 and x_3 are matrices set to all possible values. So each pair of constants c_1 and c_2 (there are 2^{64} unique combinations in total) results in an invariant coset of dimension 56. Thus, each of the 2^{64} cosets are invariant through any number of even rounds of Simpira, forming a partition of the plaintext space into invariant cosets.

For further details of Simpira, the reader is referred to [1].

2 Preliminaries

When $b = 4$ the state of Simpira consists of four 4×4 matrices over $\mathbb{F}_{2^8}$, $S = (x_1, x_2, x_3, x_4)$. We identify 4×4 matrices over $\mathbb{F}_{2^8}$ with vectors in $\mathbb{F}_{2^8}^{4\times4}$ as

$$\left\{ \begin{bmatrix} x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \\ x_4 & x_8 & x_{12} & x_{16} \end{bmatrix} \;\middle|\; \forall x_1, x_2, \ldots, x_{16} \in \mathbb{F}_{2^8} \right\}.$$

We identify the whole state S with the vector space $\mathbb{F}_{2^8}^{4\times4\times4} = \mathbb{F}_{2^8}^{64}$ simply by gluing together the columns of the matrices x_1, x_2, x_3 and x_4 into a vector $x = x_1 \times x_2 \times x_3 \times x_4$ of length 64 over $\mathbb{F}_{2^8}$.

For a vector space V and a function F on $\mathbb{F}_{2^8}^{4\times4}$ we write $F(V)$ to mean the set

$$F(V) = \{F(v) \,|\, v \in V\}.$$

For a subset $I \subset \{1, 2, \ldots, n\}$, and a subset of vector spaces $\{G_1, G_2, \ldots, G_n\}$, we use the notation G_I to mean the direct sum of a subset of those spaces determined by I,

$$G_I = \bigoplus_{i \in I} G_i.$$

In [4], three types of subspaces where defined for AES; the diagonal spaces $\mathcal{U}_I$, the column spaces $\mathcal{V}_I$ and the mixed spaces $\mathcal{W}_I$. Let $e_{i,j}$ be the 4×4 matrix with a single 1 in position i, j (or as a vector of length 16 with a single 1 in position $4 \cdot j + i$).

Definition 1. *(**Diagonal spaces**) The diagonal spaces $\mathcal{U}_i$ are defined as*

$$\mathcal{U}_i = < e_{0,i}, e_{1,i+1}, e_{2,i+2}, e_{3,i+3} >$$

where $i + j$ is computed modulo 4. For instance, the diagonal space $\mathcal{U}_0$ corresponds to the symbolic matrix

$$\mathcal{U}_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix} \;\middle|\; \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\}.$$

Definition 2. *(**Column spaces**) The column spaces $\mathcal{V}_i$ are defined as*

$$\mathcal{V}_i =< e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i} > .$$

For instance, the columns space $\mathcal{V}_0$ corresponds to the symbolic matrix

$$\mathcal{U}_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix} \;\middle|\; \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\}.$$

The last type of subspaces we define are called mixed subspaces.

Definition 3. *(**Mixed spaces**) The ith mixed subspace $\mathcal{W}_i$ is defined as*

$$\mathcal{W}_i = MC \circ SR((\mathcal{V}_i))).$$

For instance, $\mathcal{W}_0$ corresponds to symbolic matrix

$$\mathcal{W}_0 = \left\{ \begin{bmatrix} \alpha \cdot x_1 & x_4 & x_3 & (\alpha+1) \cdot x_2 \\ x_1 & x_4 & (\alpha+1) \cdot x_3 & \alpha \cdot x_2 \\ x_1 & (\alpha+1) \cdot x_4 & \alpha \cdot x_3 & x_2 \\ (\alpha+1) \cdot x_1 & \alpha \cdot x_4 & x_3 & x_2 \end{bmatrix} \;\middle|\; \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\}$$

where α is the generator of the AES field.

Let $I \subseteq \{0, 1, 2, 3\}$. Then, we define:

$$\mathcal{V}_I = \bigoplus_{i \in I} \mathcal{V}_i, \qquad \mathcal{U}_I = \bigoplus_{i \in I} \mathcal{U}_i, \qquad \mathcal{W}_I = \bigoplus_{i \in I} \mathcal{W}_i.$$

The dimension of any of the spaces $\mathcal{U}_I, \mathcal{V}_I$ and $\mathcal{W}_I$ is $4 \cdot |I|$. In [4] the authors proved the following lemmas related to these subspaces. Assume $f_k(x)$ is one AES round with a fixed key k.

Lemma 1. *[4] For $I \subseteq \{0, 1, 2, 3\}$ where $0 < |I| \leq 3$ and $a \in \mathbb{F}_{2^8}^{4\times 4}$. Then there exist a unique $b \in \mathbb{F}_{2^8}^{4\times 4}$ such that*

$$f_k(\mathcal{U}_I \oplus a) = \mathcal{V}_I \oplus b.$$

Lemma 2. *[4] For $I \subseteq \{0, 1, 2, 3\}$ where $0 < |I| \leq 3$ and $a \in \mathbb{F}_{2^8}^{4\times 4}$. Then there exist a unique $b \in \mathbb{F}_{2^8}^{4\times 4}$ such that*

$$f_k(\mathcal{V}_I \oplus a) = \mathcal{W}_I \oplus b.$$

We will consider subspaces in $\mathbb{F}_{2^8}^{4\times 4\times k}$ formed by concatenating the columns of k AES states (4×4 matrices). When we write $U \times V$ for two subspaces U and V of $\mathbb{F}_{2^8}^{4\times 4}$ we mean the subspace

$$\left\{ x \times y \;\middle|\; \forall x \in U, \forall y \in V \right\}$$

of dimension $\dim(U) + \dim(V)$. When we write (U, U), we mean the subspace

$$\left\{ x \times x \;\middle|\; \forall x \in U \right\}$$

of dimension $\dim((U, U)) = \dim(U)$ in $\mathbb{F}_{2^8}^{4\times 4\times 2}$.

3 Invariant subspaces in Simpira

Let $f(x) = f_0(x)$ denote one AES round without the key addition and let $F(x) = f(x) \times f(x)$ denote the concatenation of two AES rounds forming a map from $\mathbb{F}_{2^8}^{4\times4}$ to $\mathbb{F}_{2^8}^{4\times4} \times \mathbb{F}_{2^8}^{4\times4} = \mathbb{F}_{2^8}^{32}$. The main reason for invariant subspaces in Simpira is characterized in the following.

Lemma 3. *For $I \subset \{0,1,2,3\}$ with $0 < |I| \leq 4$ and fixed a_1 and a_2 in $\mathcal{U}_I^\perp$, there exist b_1 and $b_2 \in \mathcal{V}_I^\perp$ such that*

$$\left\{ f(x \oplus a_1) \times f(x \oplus a_2) \,\middle|\, \forall x \in \mathcal{U}_I \right\} = (\mathcal{V}_I \oplus b_1, \mathcal{V}_I \oplus b_2).$$

Proof. This follows directly from Lemma 1.

We have in particular that

$$\left\{ f(x) \times f(x) \,|\, \forall x \in \mathbb{F}_{2^8}^{4\times4} \right\} = \left\{ x \times x \,\middle|\, \forall x \in \mathbb{F}_{2^8}^{4\times4} \right\}.$$

Lemma 4. *For $I \subset \{0,1,2,3\}$ with $0 < |I| \leq 4$ and fixed a and b in V_I we have that*

$$\left\{ f(x \oplus a) \times f(x \oplus b) \,\middle|\, \forall x \in \mathbb{F}_{2^8}^{4\times4} \right\} \subset \mathcal{W}_I^\perp \times \mathcal{W}_I^\perp \oplus (\mathcal{W}_I, \mathcal{W}_I).$$

Proof. The constants a and b affects the same $|I|$ columns in x such that the output becomes linearly independent of each other in these positions after the s-box layer. The values are identical in the rest of the columns, such that the set of values belongs to $\mathcal{V}_I^\perp \times \mathcal{V}_I^\perp \oplus (\mathcal{V}_I, \mathcal{V}_I)$, by definition $SR \circ MC$ maps the resulting values to the space $W_I^\perp \times \mathcal{W}_I^\perp \oplus (\mathcal{W}_I, \mathcal{W}_I)$.

Theorem 1. *For a fixed random $a \times b \in \mathcal{V}_{\{0,1\}} \times \mathcal{V}_{\{0,1\}}$, we have that*

$$\left\{ F(F(x) \oplus a) \,\middle|\, \forall x \in \mathbb{F}_{2^8}^{4\times4} \right\} \subset H$$

where

$$H = \mathcal{W}_{\{0,1\}} \times \mathcal{W}_{\{0,1\}} \oplus (\mathcal{W}_{\{2,3\}}, \mathcal{W}_{\{2,3\}}).$$

Proof. This follows by combining the two previous Lemmas.

Notice that H is equal to

$$\left\{ (MC \circ SR(z_1 \oplus x) \times MC \circ SR(z_2 \oplus x) \right\}$$

where $z_i \in \mathcal{V}_0 \oplus \mathcal{V}_1$are 4×4 matrices formed by setting the first two columns to all possible values, while x is formed by setting the last two columns to all possible values.

We proceed by investigating the structure of the Simpira Feistel over two rounds. For $b = 4$, the input to Simpira in round t is $(x_1^t, x_2^t, x_3^t, x_4^t)$ where each x_i^t is drawn from $\mathbb{F}_{2^8}^{4\times 4}$. In the following we simplify the notation a bit by writing $F_i^t(x) = f(f(x) + k_{t,i})$ where $k_{t,i}$ is the constant to the ith function in the t'th round. The output after one round of Simpira is then

$$(x_1^{t+1}, x_2^{t+1}, x_3^{t+1}, x_4^{t+1}) = (F_1^t(x_1^t) \oplus x_2^t, F_2^t(x_4^t) + x_3^t, x_4^t, x_1^t).$$

where the constants $k_{i,j}$ belong to $\mathcal{V}_0 \oplus \mathcal{V}_1$. If we continue the recursion for one more round we get a new state

$$(x_1^{t+2}, x_2^{t+2}, x_3^{t+2}, x_4^{t+2}) = (F_1^{t+1}(x_1^{t+1}) \oplus x_2^{t+1}, F_2^{t+1}(x_4^{t+1}) + x_3^{t+1}, x_4^{t+1}, x_1^{t+1}) \tag{1}$$

If we substitute the variables in (1) with the variables x_i^t from two rounds before, we get

$$(x_1^{t+2}, \mathbf{F_2^{t+1}(x_1^t)} \oplus \mathbf{x_4^t}, x_1^t, \mathbf{F_1^t(x_1^t)} \oplus \mathbf{x_2^t})) \tag{2}$$

where $x_1^{t+2} = F_1^{t+1}(F_1^t(x_1^t) \oplus x_2^t) \oplus F_2^t(x_4^t) + x_3^t$. We have marked the output values relevant to subspace cryptanalysis in bold. In particular, from Theorem 1 it follows that the invariant subspaces in Simpira are spanned by

$$\left\{ x_1, MC \circ SR(z_1 \oplus x \oplus c_1), x_3, MC \circ SR(z_2 + x + c_2) \right| \}$$

where c_1 and c_2 are fixed random constants, $z_i \in \mathcal{V}_{\{0,1\}}$ are 4×4 matrices formed by setting the first two columns to all possible values, x is formed by setting the last two columns to all possible values, and x_1 and x_3 are matrices set to all possible values. Thus each pair of constants c_1 and c_2 (there are 2^{64} unique combinations in total) results in an invariant coset of dimension 56 for any even number of rounds.

Note that it is straight-forward to extend this to an odd number of rounds. The adversary can either prepare plaintexts by first encrypting a coset one round (for instance with zero-constants), or asking for a double-encryption of ciphertexts.

References

1. Shay Gueron and Nicky Mouha. Simpira: A family of efficient permutations using the aes round function. Cryptology ePrint Archive, Report 2016/122, 2016. http://eprint.iacr.org/.
2. Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 206–221. Springer, 2011.

3. Gregor Leander, Brice Minaud, and Sondre Rønjom. A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, pages 254–283, 2015.
4. Christian Rechberger and Sondre Rønjom. Subspace cryptanalysis. to be published, 2016.