Provable Security Evaluation of Structures against Impossible Differential and Zero Correlation Linear Cryptanalysis

Jian Guo

Nanyang Technological University, Singapore

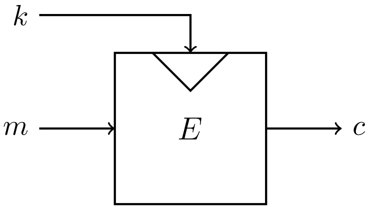
Joint work with Bing Sun, Meicheng Liu, Vincent Rijmen, and Ruilin Li

EUROCRYPT 2016
9 May 2016, Vienna, Austria

Outline

1. Introduction
2. Preliminaries
3. Impossible Differential Cryptanalysis of SPN Structures
4. Conclusion

Introduction - Block Ciphers



Differential cryptanalysis and *linear cryptanalysis* are among the most famous cryptanalytic tools, and most recent block ciphers are designed to be resistant to these two attacks.

Introduction - How to Ensure the Security

How to "prove" the security of a scheme E?

Introduction - How to Ensure the Security

How to "prove" the security of a scheme E?

- The security of many *public-key* crypto-systems can be reduced to hard mathematical problems;

Introduction - How to Ensure the Security

How to "prove" the security of a scheme E?

- The security of many *public-key* crypto-systems can be reduced to hard mathematical problems;
- If E is a provable operation mode of block ciphers, the security of E can be reduced to some other primitives, such as ideality of the underlying block ciphers or permutations;

Introduction - How to Ensure the Security

- However, for a dedicated block cipher, we cannot reduce the security to another problem;

Introduction - How to Ensure the Security

- However, for a dedicated block cipher, we cannot reduce the security to another problem;
- To show a dedicated block cipher is secure, a common way is to evaluate the security against all the known techniques, e.g., differential, linear (hull), impossible differential cryptanalysis.

Introduction - Basics of Impossible Differential

- For any un-keyed function $F : \mathbb{F}_{2^b} \rightarrow \mathbb{F}_{2^b}$, we can always find some α and β such that $\alpha \rightarrow \beta$ is an impossible differential of F.

Introduction - Basics of Impossible Differential

- For any un-keyed function $F : \mathbb{F}_{2^b} \to \mathbb{F}_{2^b}$, we can always find some α and β such that $\alpha \to \beta$ is an impossible differential of F.
- A block cipher $E(\cdot, k)$ may exhibit a differential $\alpha \to \beta$ that is a possible differential for some keys k's while it is impossible for the rest.

Introduction - Basics of Impossible Differential

- For any un-keyed function $F : \mathbb{F}_{2^b} \rightarrow \mathbb{F}_{2^b}$, we can always find some α and β such that $\alpha \rightarrow \beta$ is an impossible differential of F.
- A block cipher $E(\cdot, k)$ may exhibit a differential $\alpha \rightarrow \beta$ that is a possible differential for some keys k's while it is impossible for the rest.
- In practice, such differentials are difficult to determine in most of the cases. Generally, in a search for impossible differentials it is difficult to guarantee the completeness.

Introduction - Goals

- From the practical point of view, we are more interested in the impossible differentials that are independent of the secret keys.

Introduction - Goals

- From the practical point of view, we are more interested in the impossible differentials that are independent of the secret keys.

- Since in most cases the non-linear transformations applied to x can be written as $S(x \oplus k)$, we always employ impossible differentials that are independent of the S-boxes, which are called *truncated impossible differentials*, i.e., we only differentiate whether there are differences on some bytes and ignore the values of the differences.

- So, we will concentrate on linear layers.

Introduction

- We already know a lot about bonding the differential/linear probabilities, e.g., 25 active Sboxes in 4-round AES and at most 2^{-6} for each active Sbox, so maximum probability is 2^{-150}.

Introduction

- We already know a lot about bonding the differential/linear probabilities, e.g., 25 active Sboxes in 4-round AES and at most 2^{-6} for each active Sbox, so maximum probability is 2^{-150}.

- The security margin of the ciphers against impossible differential and zero correlation linear cryptanalysis may not yet be well studied and formulated. To some extend, the success of such attacks relies mainly on the attackers' intensive analysis of the structures used in each individual designs.

Introduction

- We already know a lot about bonding the differential/linear probabilities, e.g., 25 active Sboxes in 4-round AES and at most 2^{-6} for each active Sbox, so maximum probability is 2^{-150}.

- The security margin of the ciphers against impossible differential and zero correlation linear cryptanalysis may not yet be well studied and formulated. To some extend, the success of such attacks relies mainly on the attackers' intensive analysis of the structures used in each individual designs.

- Despite the known 4-/4-/8-round impossible differentials for the AES, ARIA and Camellia without FL/FL^{-1} layers, effort to find new impossible differentials of these ciphers that cover more rounds has never been stopped.

Introduction

- It is proved by Sun *et al.* in CRYPTO 2015 that the method proposed by Wu and Wang can find all impossible differentials if we do not investigate on the details of the nonlinear parts.

Introduction

- It is proved by Sun *et al.* in CRYPTO 2015 that the method proposed by Wu and Wang can find all impossible differentials if we do not investigate on the details of the nonlinear parts.
- For given input/output differences (α, β), we can use such method to determine whether $\alpha \rightarrow \beta$ is a possible or impossible differential.

Introduction

- It is proved by Sun *et al.* in CRYPTO 2015 that the method proposed by Wu and Wang can find all impossible differentials if we do not investigate on the details of the nonlinear parts.
- For given input/output differences (α, β), we can use such method to determine whether $\alpha \rightarrow \beta$ is a possible or impossible differential.
- We cannot find all the impossible differentials since the large amount of differentials to determine.

Preliminaries

Preliminaries

Assume $\alpha, \beta \in \mathbb{F}_{2^b}^m$, then $\alpha|\beta$ is defined as the bit-wise `OR` operation of α and β.

Preliminaries

Assume $\alpha, \beta \in \mathbb{F}_{2^b}^m$, then $\alpha|\beta$ is defined as the bit-wise `OR` operation of α and β. Let $\theta : \mathbb{F}_{2^b} \to \mathbb{F}_2$ be defined as

$$\theta(x) = \begin{cases} 0 & x = 0, \\ 1 & x \neq 0. \end{cases}$$

Preliminaries

Assume $\alpha, \beta \in \mathbb{F}_{2^b}^m$, then $\alpha|\beta$ is defined as the bit-wise `OR` operation of α and β. Let $\theta : \mathbb{F}_{2^b} \to \mathbb{F}_2$ be defined as

$$\theta(x) = \begin{cases} 0 & x = 0, \\ 1 & x \neq 0. \end{cases}$$

Then, for $X = (x_0, \ldots, x_{m-1}) \in \mathbb{F}_{2^b}^m$, the mode of X is defined as

$$\chi(X) \triangleq (\theta(x_0), \ldots, \theta(x_{m-1})) \in \mathbb{F}_2^m.$$

Preliminaries

The Hamming weight of X is defined as the number of non-zero elements of the vector, i.e.

$$H(X) = \#\{i|x_i \neq 0, i = 0, 1, \ldots, m-1\}.$$

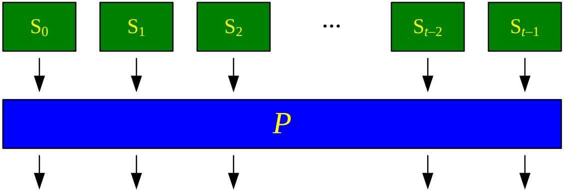
Preliminaries

- For $P = (p_{ij}) \in \mathbb{F}_{2^b}^{m \times m}$, denote by $\mathbb{Z}$ the integer ring, the characteristic matrix of P is defined as $P^* = (p_{ij}^*) \in \mathbb{Z}^{m \times m}$, where $p_{ij}^* = 0$ if $p_{ij} = 0$ and $p_{ij}^* = 1$ otherwise.

Preliminaries

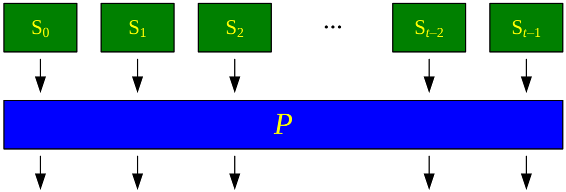
- For $P = (p_{ij}) \in \mathbb{F}_{2^b}^{m\times m}$, denote by $\mathbb{Z}$ the integer ring, the characteristic matrix of P is defined as $P^* = (p^*_{ij}) \in \mathbb{Z}^{m\times m}$, where $p^*_{ij} = 0$ if $p_{ij} = 0$ and $p^*_{ij} = 1$ otherwise.
- $p^*_{ij} = 0$ means the i-th output byte of the first round is independent of the j-th input byte.

Preliminaries - SPN Ciphers



r-round SPN cipher: $(SP)^{r-1}S$, the structure $\mathcal{E}^{(r)}$ refers to exactly the same, except the Sboxes can take all possible permutations.

Preliminaries - SPN Ciphers



r-round SPN cipher: $(SP)^{r-1}S$, the structure $\mathcal{E}^{(r)}$ refers to exactly the same, except the Sboxes can take all possible permutations.

Impossible differential now refers to that regardless of the choices of Sboxes.

Preliminaries

Let $\mathcal{E}^{(r)}$ be an r-round iterated structure. If $\alpha \to \beta$ is a possible differential of $\mathcal{E}^{(r_1)}$ and $\beta \to \gamma$ is a possible differential of $\mathcal{E}^{(r_2)}$. Then $\alpha \to \gamma$ is a possible differential of $\mathcal{E}^{(r_1+r_2)}$.

$$
E: \quad \begin{array}{ccccc}
x & \xrightarrow{E_1} & y & \xrightarrow{E_2} & z \\
| & & | & & | \\
x \oplus \alpha & \xrightarrow{E_1} & y \oplus \beta & \xrightarrow{E_2} & z \oplus \gamma
\end{array}
$$

Preliminaries

Let $\mathcal{E}^{(r)}$ be an r-round iterated structure. If $\alpha \rightarrow \beta$ is a possible differential of $\mathcal{E}^{(r_1)}$ and $\beta \rightarrow \gamma$ is a possible differential of $\mathcal{E}^{(r_2)}$. Then $\alpha \rightarrow \gamma$ is a possible differential of $\mathcal{E}^{(r_1+r_2)}$.

$$
E: \quad \begin{array}{ccccc}
x & \xrightarrow{E_1} & y & \xrightarrow{E_2} & z \\
| & & | & & | \\
x \oplus \alpha & \xrightarrow{E_1} & y \oplus \beta & \xrightarrow{E_2} & z \oplus \gamma
\end{array}
$$

Note. For dedicated cipher with *fixed choice of Sboxes*, this statement may not hold.

Preliminaries

Fact 1. For a structure $\mathcal{E}$, if there do not exist r-round impossible differentials, there do not exist R-round impossible differentials for any $R \geq r$.

Preliminaries

Fact 1. For a structure $\mathcal{E}$, if there do not exist r-round impossible differentials, there do not exist R-round impossible differentials for any $R \geq r$.

Fact 2. $\alpha \to \beta$ is a possible differential of a single S layer $\mathcal{E}^S$ if and only if $\chi(\alpha) = \chi(\beta)$.

Impossible Differential Cryptanalysis of SPN Structures

Lemma 1

If $\alpha_1 \to \beta_1$ and $\alpha_2 \to \beta_2$ are possible differentials of $\mathcal{E}^{SP}$, then there always exist possible differential $\alpha \to \beta$ such that

$$\begin{cases} \chi(\alpha) = \chi(\alpha_1)|\chi(\alpha_2), \\ \chi(\beta) = \chi(\beta_1)|\chi(\beta_2), \end{cases}$$

Impossible Differential Cryptanalysis of SPN Structures

Proof.

Find $\lambda \in \mathbb{F}_{2^b}^*$ such that

$$\chi\left(\begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix} \middle| \begin{pmatrix} 0 \\ y_1 \\ y_2 \end{pmatrix}\right) = \chi\left(\begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ \lambda y_1 \\ \lambda y_2 \end{pmatrix}\right).$$

□

Impossible Differential Cryptanalysis of SPN Structures

Corollary 1 (Propagation from 1-round to r-round SPN)

If $\alpha_1 \to \beta_1$ and $\alpha_2 \to \beta_2$ are possible differentials of $\mathcal{E}_{SP}^{(r)}$, $\alpha_1|\alpha_2 \to \beta_1|\beta_2$ is also a possible differential of $\mathcal{E}_{SP}^{(r)}$.

Impossible Differential Cryptanalysis of SPN Structures

- A specific form: $(x_0, 0) \rightarrow (y_0, 0)$ and $(0, x_1,) \rightarrow (0, y_1)$ are possible differentials of $\mathcal{E}_{SP}$, where x_0, x_1, y_0, y_1 are non-zero, then $(x_0, x_1) \rightarrow (y_0, y_1)$ is a possible differential.

Impossible Differential Cryptanalysis of SPN Structures

- A specific form: $(x_0, 0) \to (y_0, 0)$ and $(0, x_1,) \to (0, y_1)$ are possible differentials of $\mathcal{E}_{SP}$, where x_0, x_1, y_0, y_1 are non-zero, then $(x_0, x_1) \to (y_0, y_1)$ is a possible differential.
- The contrapositive: if $(x_0, x_1) \to (y_0, y_1)$ is an impossible differential of $\mathcal{E}_{SP}$, either $(x_0, 0) \to (y_0, 0)$ or $(0, x_1) \to (0, y_1)$ is an impossible differential.

Impossible Differential Cryptanalysis of SPN Structures

Theorem 1

There exists an impossible differential of $\mathcal{E}_{SP}^{(r)}$ if and only if there exists an impossible differential $\alpha \not\rightarrow \beta$ of $\mathcal{E}_{SP}^{(r)}$ where $H(\alpha) = H(\beta) = 1$.

Impossible Differential Cryptanalysis of SPN Structures

With the help of Theorem 1, we are able to reduce the complexities of checking whether there exists an impossible differential of an SPN structure with m input/output words from $\mathcal{O}(2^{2m})$ to $\mathcal{O}(m^2)$.

Finding the Upper Bound

Theorem 2

Let t_1 and t_2 be the smallest integers such that $(P^*)^{t_1}$ and $(P^*)^{-t_2}$ are all-one matrices. Then there does not exist any impossible differential $\mathcal{E}_{SP}^{(r)}$ for $r \geq t_1 + t_2 + 1$.

Finding the Upper Bound

Diffusion Layer of the AES:

$$P = \begin{pmatrix}
2&0&0&0&0&3&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&2&0&0&0&0&3&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&2&0&0&0&0&3\\
3&0&0&0&0&1&0&0&0&0&1&0&0&0&0&2\\
0&0&0&1&2&0&0&0&0&3&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&2&0&0&0&0&3&0\\
0&0&0&3&1&0&0&0&0&1&0&0&0&0&2&0\\
0&0&0&2&3&0&0&0&0&1&0&0&0&0&1&0\\
0&0&1&0&0&0&0&1&2&0&0&0&0&3&0&0\\
0&0&3&0&0&0&0&1&1&0&0&0&0&2&0&0\\
0&0&2&0&0&0&0&3&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&2&3&0&0&0&0&1&0&0\\
0&3&0&0&0&0&1&0&0&0&0&1&2&0&0&0\\
0&2&0&0&0&0&3&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&2&0&0&0&0&3&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&2&3&0&0&0
\end{pmatrix}.$$

Finding the Upper Bound

Characteristic matrix of Diffusion Layer of the AES:

$$P^* = \begin{pmatrix}
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0
\end{pmatrix}.$$

Finding the Upper Bound

Square of the characteristic matrix:

$$
(P^*)^2 = \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix},
$$

so $t_1 = 2$, similarly we can find $t_2 = 2$, hence there does not exist any impossible differential of $\mathcal{E}^{\text{AES}}$ which covers $r \geq 5$ rounds

Finding the Upper Bound

Since we already have 4-round impossible differential of $\mathcal{E}^{AES}$, unless we investigate on the details of the S-boxes, with respect to the number of rounds, we cannot find better impossible differentials for the AES.

Links Between Impossible Differential and Zero-Correlation Linear Cryptanalysis

Due to the duality of impossible differential and zero-correlation linear cryptanalysis, all the results on impossible differential here apply to zero-correlation linear cryptanalysis as well.

Conclusion

We mainly investigated the security of *structures* against impossible differential and zero correlation linear cryptanalysis.

Conclusion

We mainly investigated the security of *structures* against impossible differential and zero correlation linear cryptanalysis.

(1) Reduced the problem whether there exists an r-round impossible differential to that with the Hamming weights of the input and output differences being 1;

Conclusion

We mainly investigated the security of *structures* against impossible differential and zero correlation linear cryptanalysis.

(1) Reduced the problem whether there exists an r-round impossible differential to that with the Hamming weights of the input and output differences being 1;

(2) Given a method to upper bound the rounds of impossible differentials and zero correlation linear hulls.

Future Work

These results are obtained when the details of Sboxes are NOT taken into account, what happens if we do ?

Future Work

These results are obtained when the details of Sboxes are NOT taken into account, what happens if we do ?

Stay tuned for

"New Insights on AES-Like SPN Ciphers" in CRYPTO 2016.

Thanks for Your Attention!