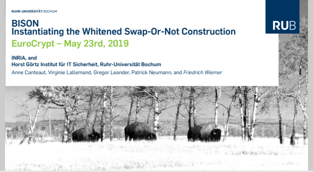
BISON
Instantiating the Whitened Swap-Or-Not Construction

EuroCrypt – May 23rd, 2019

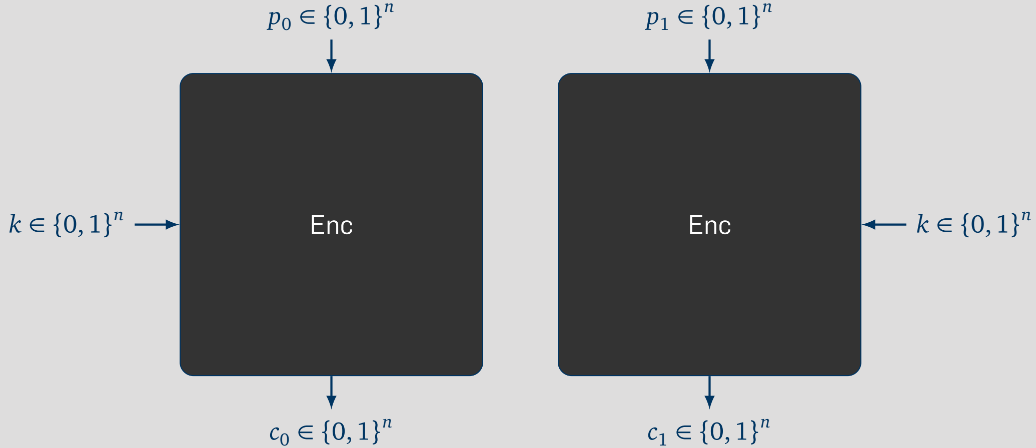
INRIA, and
Horst Görtz Institut für IT Sicherheit, Ruhr-Universität Bochum
Anne Canteaut, Virginie Lallemand, Gregor Leander, Patrick Neumann, and *Friedrich Wiemer*

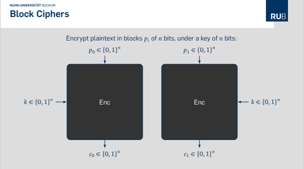


- Whitened Swap-Or-Not Construction developed by Hoang et al. and Tessaro
- Way of building block ciphers
- As this is one of the few talks here at EuroCrypt about block ciphers, lets start simple

Block Ciphers

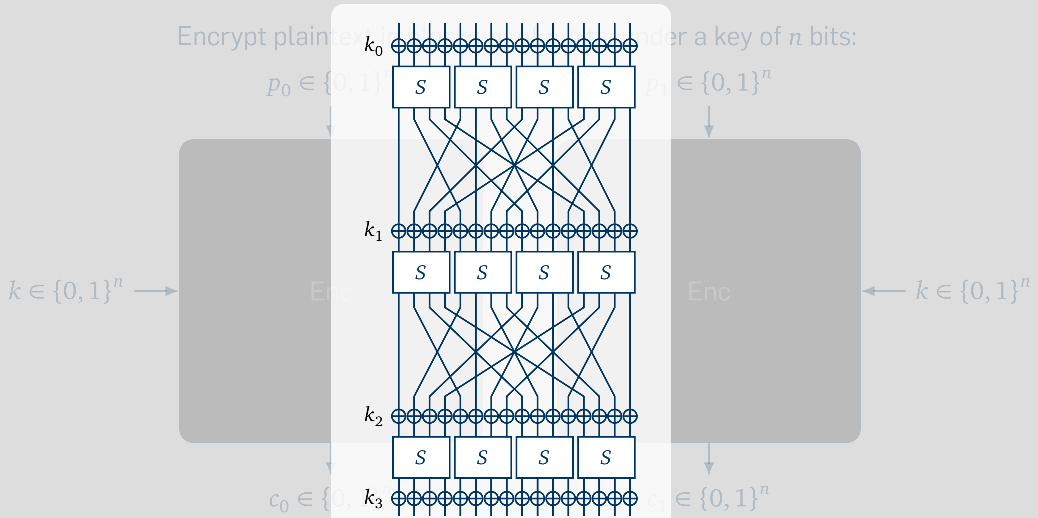
Encrypt plaintext in blocks p_i of n bits, under a key of n bits:

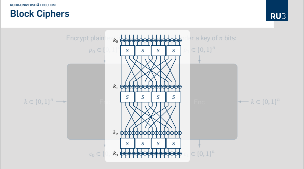




- Block ciphers encrypt *blocks* of n-bit inputs under an n-bit master key
- As a basic cryptographic primitive, we need special modes of operations, if the data to be encrypted is not of exactly n-bit length.
- This we do not consider here, instead we want to look at how to build this black box.

Block Ciphers





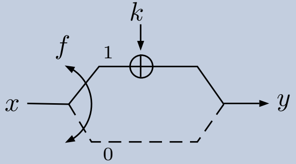
- Block ciphers encrypt *blocks* of n-bit inputs under an n-bit master key
- As a basic cryptographic primitive, we need special modes of operations, if the data to be encrypted is not of exactly n-bit length.
- This we do not consider here, instead we want to look at how to build this black box.

- Typicall approach is an SPN structure, where key-addition, S-box layer and a linear layer are iterated over several rounds.
- Relatively well understood
- Good security arguments against known attacks
- There are some problems: differentials and linear hull effects

The WSN construction

Published by Tessaro at AsiaCrypt 2015 [`ia.cr/2015/868`].

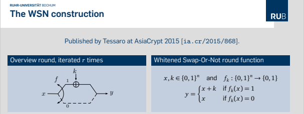
Overview round, iterated r times



Whitened Swap-Or-Not round function

$$x, k \in \{0,1\}^n \quad \text{and} \quad f_k : \{0,1\}^n \to \{0,1\}$$

$$y = \begin{cases} x + k & \text{if } f_k(x) = 1 \\ x & \text{if } f_k(x) = 0 \end{cases}$$

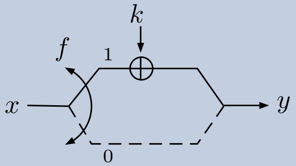


- Lets take a look at the WSN construction (simplified).
- Again, an iterated round function, where the input is fed into from the left.
- Next, a Boolean function decides if either the round key k is xored onto the input, or nothing happens.
- The result is the updated state, respective the output of the round.
- In other words, x, and k are both n-bit strings and f is an n-bit Boolean function.
- The round output y is either $x + k$ if $f_k(x) = 1$ or just x in the other case.
- So why is this nice?

The WSN construction

Published by Tessaro at AsiaCrypt 2015 [ia.cr/2015/868].

Overview round, iterated r times



Whitened Swap-Or-Not round function

$x, k \in \{0,1\}^n$ and $f_k : \{0,1\}^n \to \{0,1\}$

$$y = \begin{cases} x + k & \text{if } f_k(x) = 1 \\ x & \text{if } f_k(x) = 0 \end{cases}$$

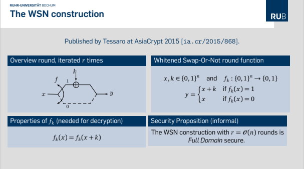
Properties of f_k (needed for decryption)

$$f_k(x) = f_k(x + k)$$

Security Proposition (informal)

The WSN construction with $r = \mathcal{O}(n)$ rounds is *Full Domain* secure.

└The WSN construction



- Lets take a look at the WSN construction (simplified).
- Again, an iterated round function, where the input is fed into from the left.
- Next, a Boolean function decides if either the round key k is xored onto the input, or nothing happens.
- The result is the updated state, respective the output of the round.
- In other words, x, and k are both n-bit strings and f is an n-bit Boolean function.
- The round output y is either $x + k$ if $f_k(x) = 1$ or just x in the other case.
- So why is this nice?

- Tessaro was able to show that this construction, when iterated over $\mathcal{O}(n)$ rounds, achieves *Full Domain* security (what ever that means).
- One further property of f which we need for decryption is that x and $x + k$ maps to the same output.

The WSN construction

Encryption

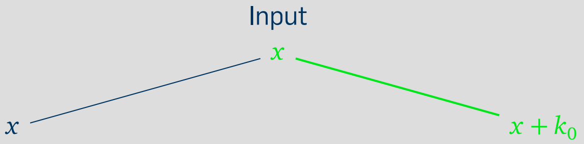
Input

x

- We can observe an interesting first property, when looking at the encryption procedure round by round
- Starting with the plaintext x...

The WSN construction

Encryption

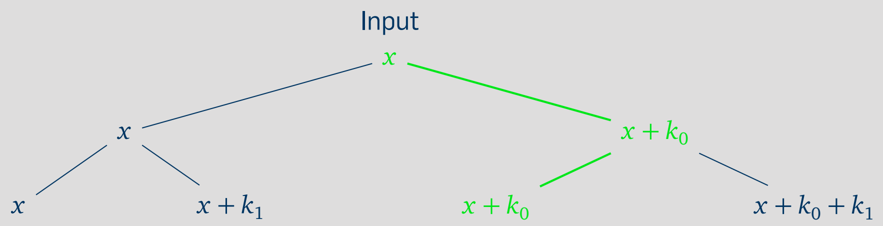


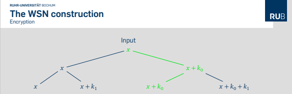
└The WSN construction

- We can observe an interesting first property, when looking at the encryption procedure round by round
- Starting with the plaintext x…
- …in each round, we either add the round key k_i, …

The WSN construction

Encryption



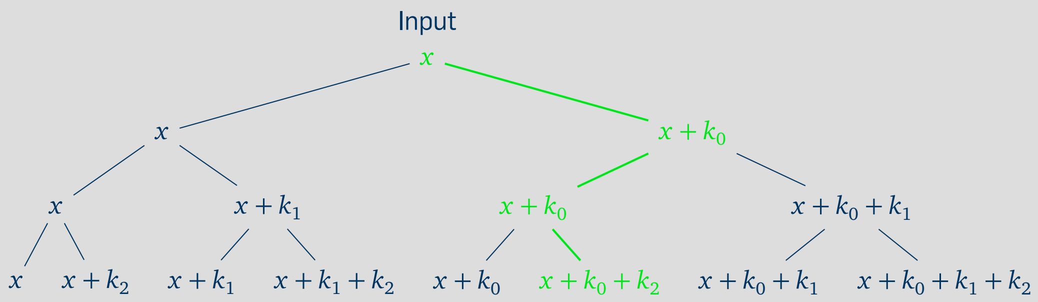


└The WSN construction

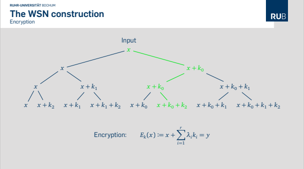
- We can observe an interesting first property, when looking at the encryption procedure round by round
- Starting with the plaintext x...
- ...in each round, we either add the round key k_i, ...
- ...or not.

The WSN construction

Encryption



Encryption: $E_k(x) := x + \sum_{i=1}^{r} \lambda_i k_i = y$



- We can observe an interesting first property, when looking at the encryption procedure round by round
- Starting with the plaintext x…
- …in each round, we either add the round key k_i, …
- …or not.
- Thus we end up with a binary tree of possible states.
- Furthermore, the encryption can also be written as the plaintext plus the sum of some round keys, chosen by the λ_i's here.

An Implementation

RUHR-UNIVERSITÄT BOCHUM
An Implementation

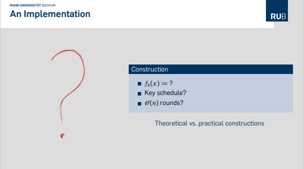
- Sounds all very great.
- So from a practitioners point of view the natural next point is: lets implement it.

An Implementation

Construction

- $f_k(x) := ?$
- Key schedule?
- $\mathcal{O}(n)$ rounds?

Theoretical vs. practical constructions



- Sounds all very great.
- So from a practitioners point of view the natural next point is: lets implement it.

- But uggh…
- How does this Boolean function f_k actually looks like?
- What about a key schedule? How do we derive the round keys?
- And how many are $\mathcal{O}(n)$ rounds?

- So, from a theoretical point of view we have a nice construction.
- But from a practical point of view it is basically useless.

- OK, let us fix this.

Generic Analysis

On the number of rounds

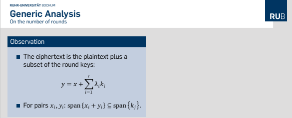
RUB

Observation

- The ciphertext is the plaintext plus a subset of the round keys:

$$y = x + \sum_{i=1}^{r} \lambda_i k_i$$

- For pairs x_i, y_i: $\operatorname{span}\{x_i + y_i\} \subseteq \operatorname{span}\left\{k_j\right\}$.



Generic Analysis
On the number of rounds

RUB

Observation

- The ciphertext is the plaintext plus a subset of the round keys:

$$y = x + \sum_{i=1}^{r} \lambda_i k_i$$

- For pairs x_i, y_i: $\operatorname{span}\{x_i + y_i\} \subseteq \operatorname{span}\{k_j\}$.

Distinguishing Attack for $r < n$ rounds

There is an $u \in \mathbb{F}_2^n \setminus \{0\}$, s. t. $\langle u, x \rangle = \langle u, y \rangle$ holds always:

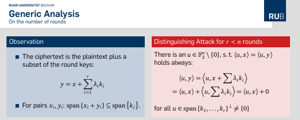
$$\langle u, y \rangle = \left\langle u, x + \sum \lambda_i k_i \right\rangle$$
$$= \langle u, x \rangle + \left\langle u, \sum \lambda_i k_i \right\rangle = \langle u, x \rangle + 0$$

for all $u \in \operatorname{span}\{k_1, \ldots, k_r\}^{\perp} \neq \{0\}$

2019-04-01

BISON Instantiating the Whitened Swap-Or-Not Construction
└─Generic Analysis

└─Generic Analysis



Generic Analysis

On the number of rounds

Observation

- The ciphertext is the plaintext plus a subset of the round keys:

$$y = x + \sum_{i=1}^{r} \lambda_i k_i$$

- For pairs x_i, y_i: $\mathrm{span}\,\{x_i + y_i\} \subseteq \mathrm{span}\,\{k_j\}$.

Distinguishing Attack for $r < n$ rounds

There is an $u \in \mathbb{F}_2^n \setminus \{0\}$, s. t. $\langle u, x\rangle = \langle u, y\rangle$ holds always:

$$\begin{aligned}\langle u, y\rangle &= \left\langle u, x + \sum \lambda_i k_i \right\rangle \\ &= \langle u, x\rangle + \left\langle u, \sum \lambda_i k_i \right\rangle = \langle u, x\rangle + 0\end{aligned}$$

for all $u \in \mathrm{span}\,\{k_1, \dots, k_r\}^{\perp} \neq \{0\}$

Rationale 1

Any instance must iterate at least n rounds; any set of n consecutive keys should be linearly indp.

2019-04-01

BISON Instantiating the Whitened Swap-Or-Not Construction
└─Generic Analysis

└─Generic Analysis

Generic Analysis

On the Boolean functions f

A bit out of the blue sky, but:

Rationale 2

For any instance, f_k has to depend on all bits, and for any $\delta \in \mathbb{F}_2^n : \Pr[f_k(x) = f_k(x + \delta)] \approx \frac{1}{2}$.

Generic Analysis
On the Boolean functions f

A bit out of the blue sky, but:

Rationale 2

For any instance, f_k has to depend on all bits, and for any $\delta \in \mathbb{F}_2^n : \Pr[f_k(x) = f_k(x + \delta)] \approx \frac{1}{2}$.

A genus of the WSN family: BISON

RUB

Rationale 1

Any instance must iterate at least n rounds; any set of n consecutive keys should be linearly indp.

Rationale 2

For any instance, f_k has to depend on all bits, and for any $\delta \in \mathbb{F}_2^n : \Pr[f_k(x) = f_k(x+\delta)] \approx \frac{1}{2}$.

Generic properties of **B**ent wh**I**tened **S**wap **O**r **N**ot

- At least n iterations of the round function
- Consecutive round keys linearly independent
- The round function depends on all bits
- $\forall \delta : \Pr[f_k(x) = f_k(x+\delta)] = \frac{1}{2}$ (*bent*)

A genus of the WSN family: BISON

RUB

Rationale 1

Any instance must iterate at least n rounds; any set of n consecutive keys should be linearly indp.

Rationale 2

For any instance, f_k has to depend on all bits, and for any $\delta \in \mathbb{F}_2^n : \Pr[f_k(x) = f_k(x+\delta)] \approx \frac{1}{2}$.

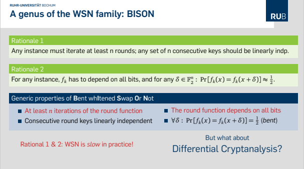
Generic properties of Bent whItened Swap Or Not

- At least n iterations of the round function
- Consecutive round keys linearly independent
- The round function depends on all bits
- $\forall \delta : \Pr[f_k(x) = f_k(x+\delta)] = \frac{1}{2}$ (*bent*)

Rational 1 & 2: WSN is *slow* in practice!

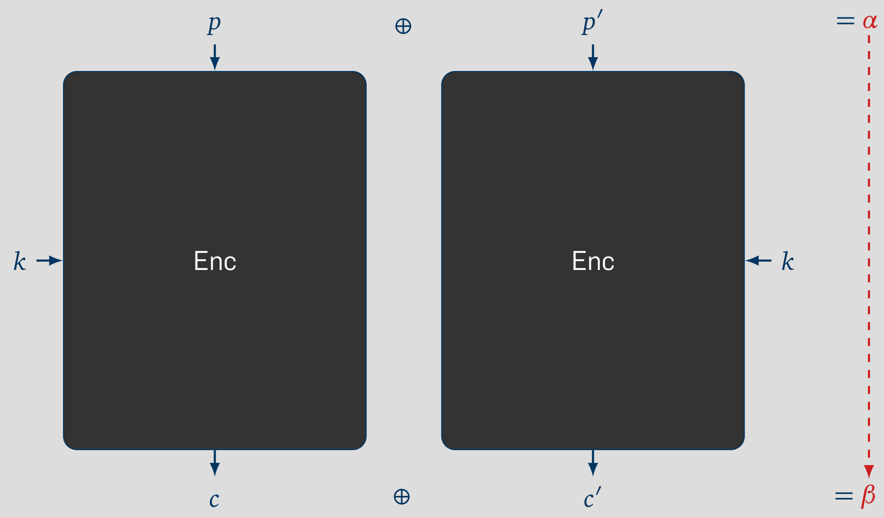
But what about

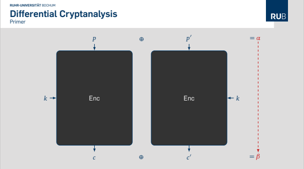
Differential Cryptanalysis?



Differential Cryptanalysis

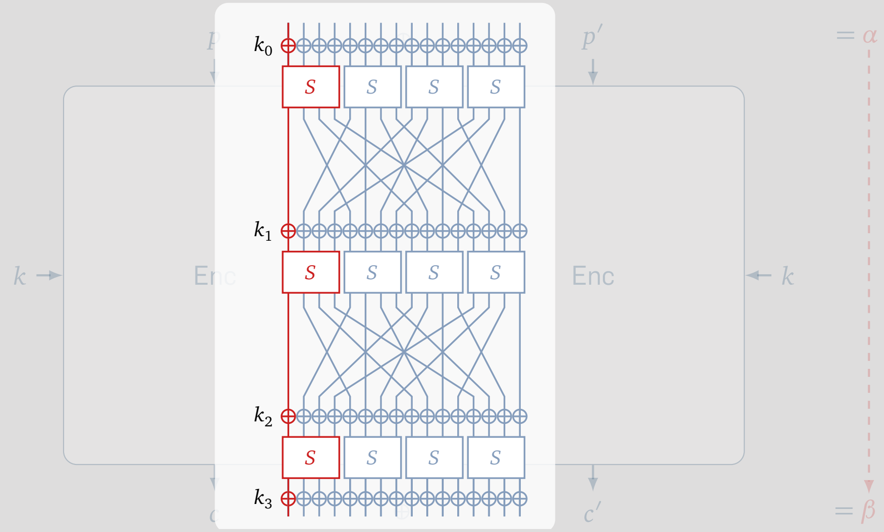
Primer





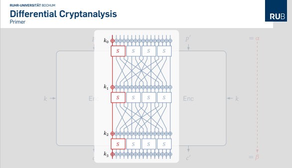
Differential Cryptanalysis

Primer



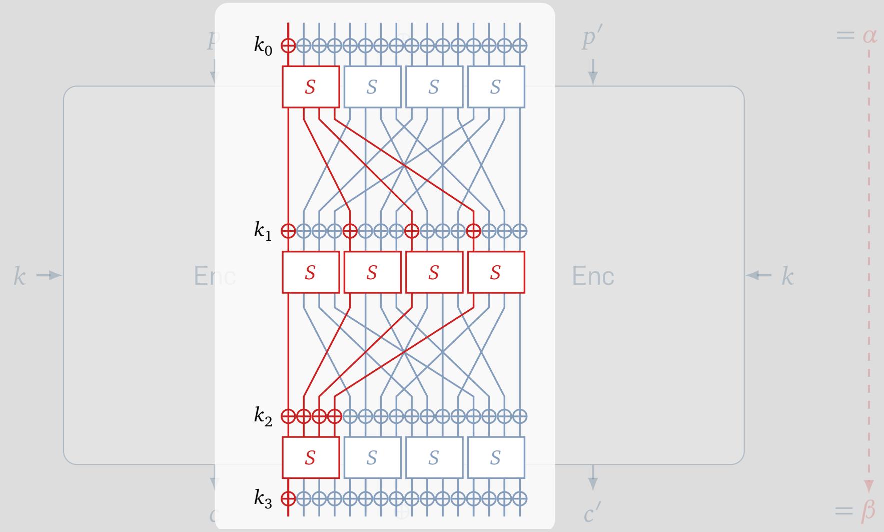
2019-04-01

BISON Instantiating the Whitened Swap-Or-Not Construction
└Differential Analysis
└Differential Cryptanalysis



Differential Cryptanalysis

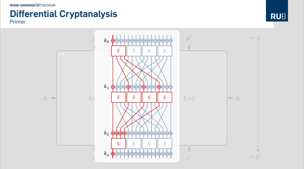
Primer



2019-04-01

BISON Instantiating the Whitened Swap-Or-Not Construction
└Differential Analysis

└Differential Cryptanalysis



Differential Cryptanalysis

One round

Proposition

For one round of BISON the probabilities are:

$$\Pr[\alpha \to \beta] = \begin{cases} 1 & \text{if } \alpha = \beta = k \text{ or } \alpha = \beta = 0 \\ \frac{1}{2} & \text{else if } \beta \in \{\alpha, \alpha + k\} \\ 0 & \text{else} \end{cases}$$

Differential Cryptanalysis

One round

Proposition

For one round of BISON the probabilities are:

$$\Pr[\alpha \to \beta] = \begin{cases} 1 & \text{if } \alpha = \beta = k \text{ or } \alpha = \beta = 0 \\ \frac{1}{2} & \text{else if } \beta \in \{\alpha, \alpha + k\} \\ 0 & \text{else} \end{cases}$$

Possible differences

$$\begin{array}{lllr} & x & + f_k(x) & \cdot k \\ \oplus & x + \alpha & + f_k(x+\alpha) & \cdot k \\ = & \alpha & + (f_k(x) + f_k(x+\alpha)) & \cdot k \end{array}$$

Differential Cryptanalysis

One round

Proposition

For one round of BISON the probabilities are:

$$\Pr[\alpha \to \beta] = \begin{cases} 1 & \text{if } \alpha = \beta = k \text{ or } \alpha = \beta = 0 \\ \frac{1}{2} & \text{else if } \beta \in \{\alpha, \alpha + k\} \\ 0 & \text{else} \end{cases}$$

Possible differences

$$\begin{array}{rllr} & x & + f_k(x) & \cdot k \\ \oplus & x + \alpha & + f_k(x+\alpha) & \cdot k \\ = & \alpha & + (f_k(x) + f_k(x+\alpha)) & \cdot k \end{array}$$

Remember

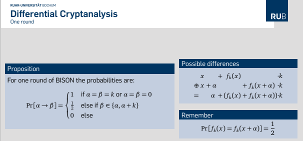
$$\Pr[f_k(x) = f_k(x+\alpha)] = \frac{1}{2}$$

2019-04-01

BISON Instantiating the Whitened Swap-Or-Not Construction

└Differential Analysis

└Differential Cryptanalysis

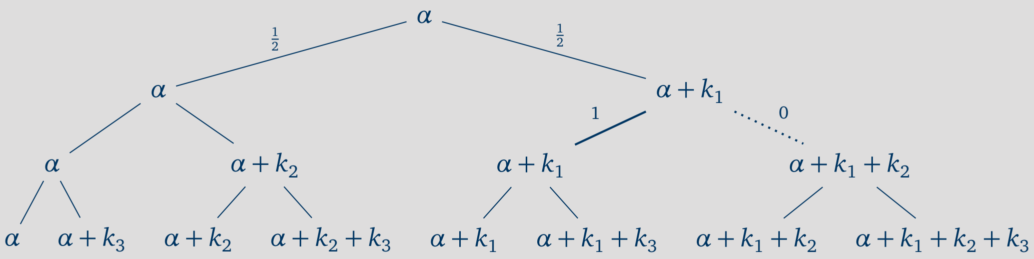


Differential Cryptanalysis

More rounds

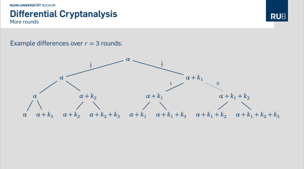
RUB

Example differences over $r = 3$ rounds:



2019-04-01

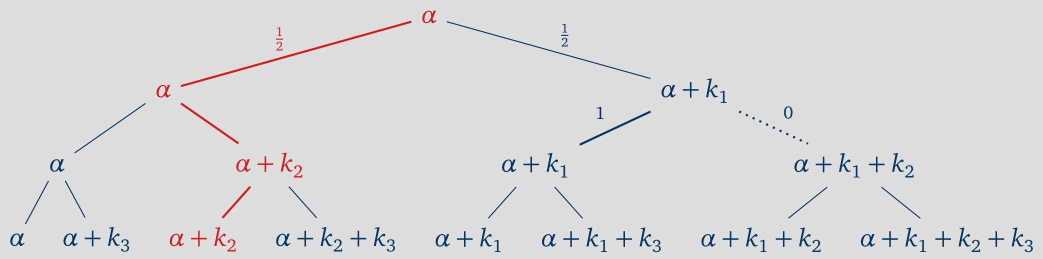
BISON Instantiating the Whitened Swap-Or-Not Construction
└Differential Analysis
└Differential Cryptanalysis



Differential Cryptanalysis

More rounds

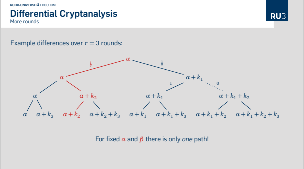
Example differences over $r = 3$ rounds:



For fixed α and β there is only *one* path!

2019-04-01

BISON Instantiating the Whitened Swap-Or-Not Construction
└Differential Analysis
└Differential Cryptanalysis



A concrete species

2019-04-01

BISON Instantiating the Whitened Swap-Or-Not Construction
└─The concrete Instance
└─BISON

Addressing Rationale 1

The Key Schedule

RUB

Rationale 1

Any instance must iterate at least n rounds; any set of n consecutive keys should be linearly indp.

Design Decisions

- Choose number of rounds as $3 \cdot n$
- Round keys derived from the state of LFSRs
- Add round constants c_i to w_i round keys

Implications

- Clocking an LFSR is cheap
- For an LFSR with irreducible feedback polynomial of degree n, every n consecutive states are linearly independent
- Round constants avoid structural weaknesses

RUHR-UNIVERSITÄT BOCHUM
Addressing Rationale 1
The Key Schedule
RUB
Rationale 1
Any instance must iterate at least n rounds; any set of n consecutive keys should be linearly indp.
Design Decisions
Choose number of rounds as $3 \cdot n$
Round keys derived from the state of LFSRs
Add round constants c_i to w_i round keys
Implications
Clocking an LFSR is cheap
For an LFSR with irreducible feedback polynomial of degree n, every n consecutive states are linearly independent
Round constants avoid structural weaknesses

Addressing Rationale 2

The Round Function

RUB

Rationale 2

For any instance, the f_k should depend on all bits, and for any $\delta \in \mathbb{F}_2^n:\ \Pr[f_k(x) = f_k(x+\delta)] \approx \frac{1}{2}$.

Design Decisions

- Choose $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$ s. t.

$$\delta \in \mathbb{F}_2^n:\ \Pr[f_k(x) = f_k(x+\delta)] = \frac{1}{2},$$

  that is, f_k is a bent function.
- Choose the simplest bent function known:

$$f_k(x,y) := \langle x, y \rangle$$

Implications

- Bent functions well studied
- Bent functions only exists for even n
- Instance not possible for every block length n

Further Cryptanalysis

RUB

Linear Cryptanalysis

For $r \geqslant n$ rounds, the correlation of any non-trivial linear trail for BISON is upper bounded by $2^{-\frac{n+1}{2}}$.

Invariant Attacks

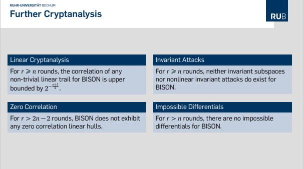
For $r \geqslant n$ rounds, neither invariant subspaces nor nonlinear invariant attacks do exist for BISON.

Zero Correlation

For $r > 2n-2$ rounds, BISON does not exhibit any zero correlation linear hulls.

Impossible Differentials

For $r > n$ rounds, there are no impossible differentials for BISON.



Implementation

TODO

RUHR-UNIVERSITÄT BOCHUM
Implementation
TODO

Conclusion/Questions

Thank you for your attention!

RUB

BISON

- A first instance of the WSN construction
- Good results for differential cryptanalysis

Open Problems

- Construction for linear cryptanalysis
- Further analysis: division properties

Thank you!

Questions?

2018/1011

RUHR-UNIVERSITÄT BOCHUM
Conclusion/Questions
Thank you for your attention!
RUB
BISON
A first instance of the WSN construction
Good results for differential cryptanalysis
Open Problems
Construction for linear cryptanalysis
Further analysis: division properties
Thank you!
Questions?
2018/1011

Details

BISON's round function

For round keys $k_i \in \mathbb{F}_2^n$ and $w_i \in \mathbb{F}_2^{n-1}$ the round function computes

$$R_{k_i,w_i}(x) := x + f_{b(i)}\big(w_i + \Phi_{k_i}(x)\big) \cdot k_i.$$

where

- Φ_{k_i} and $f_{b(i)}$ are defined as

$$\Phi_k(x) : \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$$
$$\Phi_k(x) := (x + x[i(k)] \cdot k)[j]_{\substack{1 \leqslant j \leqslant n \\ j \neq i(k)}}$$

$$f_{b(i)} : \mathbb{F}_2^{\frac{n-1}{2}} \times \mathbb{F}_2^{\frac{n-1}{2}} \to \mathbb{F}_2$$
$$f_{b(i)}(x,y) := \langle x, y \rangle + b(i),$$

- and $b(i)$ is 0 if $i \leqslant \frac{r}{2}$ and 1 else.

BISON's key schedule

Given

- primitive $p_k, p_w \in \mathbb{F}_2[x]$ with degrees $n, n-1$ and companion matrices C_k, C_w.
- master key $K = (k, w) \in \left(\mathbb{F}_2^n \times \mathbb{F}_2^{n-1}\right) \setminus \{0, 0\}$

The ith round keys are computed by

$$\begin{aligned} \mathrm{KS}_i : \mathbb{F}_2^n \times \mathbb{F}_2^{n-1} &\rightarrow \mathbb{F}_2^n \times \mathbb{F}_2^{n-1} \\ \mathrm{KS}_i(k, w) &:= (k_i, c_i + w_i) \end{aligned}$$

where

$$k_i = (C_k)^i k, \qquad c_i = (C_w)^{-i} e_1, \qquad w_i = (C_w)^i w.$$