

# BISON

## Instantiating the Whitened Swap-Or-Not Construction

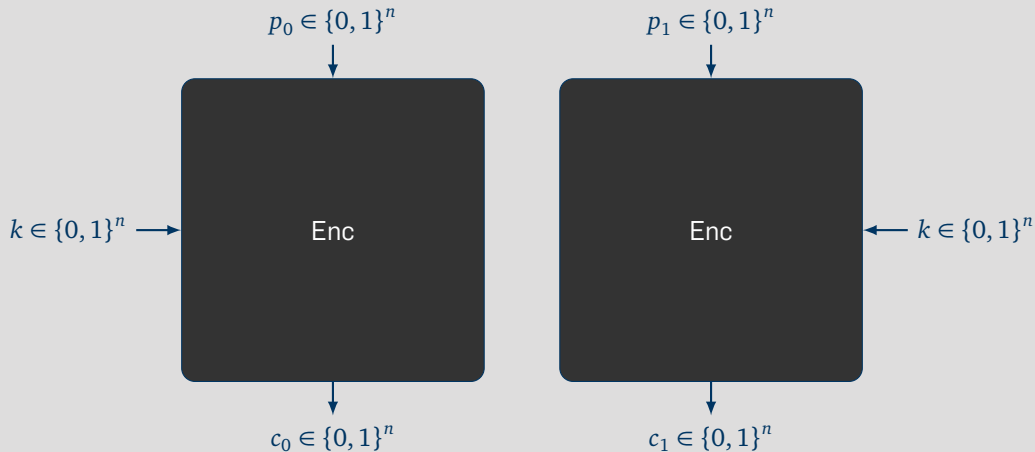
### September 6th, 2018

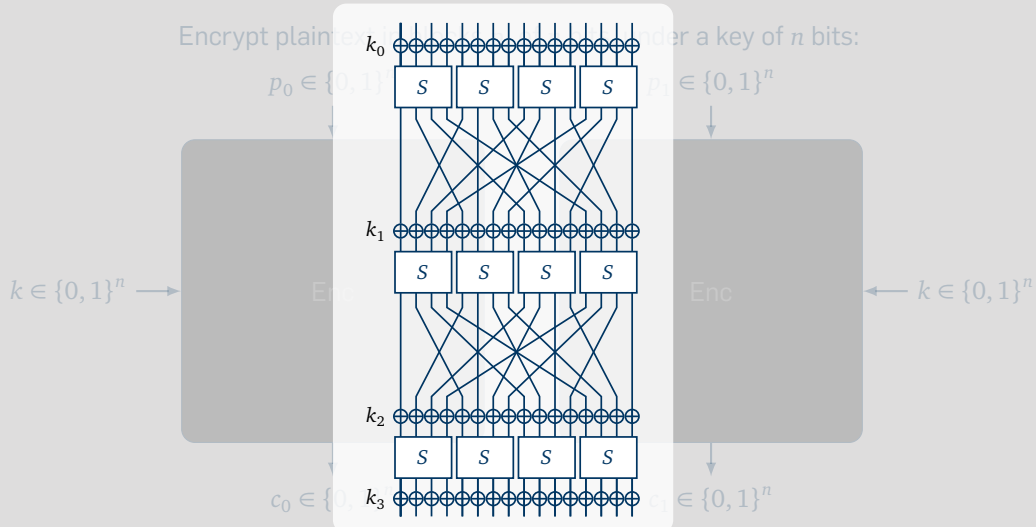
Horst Görtz Institute for IT Security  
Ruhr-Universität Bochum

Virginie Lallemand, Gregor Leander, Patrick Neumann, and *Friedrich Wiemer*



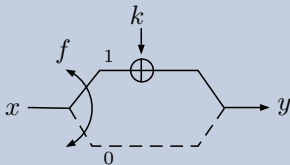
Encrypt plaintext in blocks  $p_i$  of  $n$  bits, under a key of  $n$  bits:





Published by Tessaro at AsiaCrypt 2015 [[ia.cr/2015/868](http://ia.cr/2015/868)].

## Overview round, iterated $r$ times



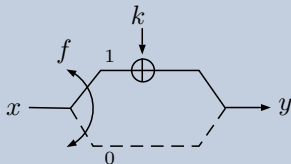
## Whitened Swap-Or-Not round function

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

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

Published by Tessaro at AsiaCrypt 2015 [[ia.cr/2015/868](http://ia.cr/2015/868)].

### Overview round, iterated $r$ times



### Whitened Swap-Or-Not round function

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

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

### Properties of $f$ (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

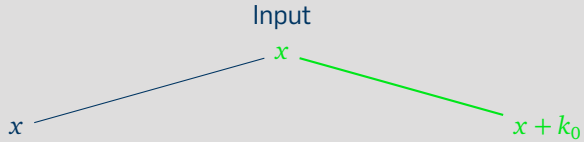
## Encryption

Input

$x$

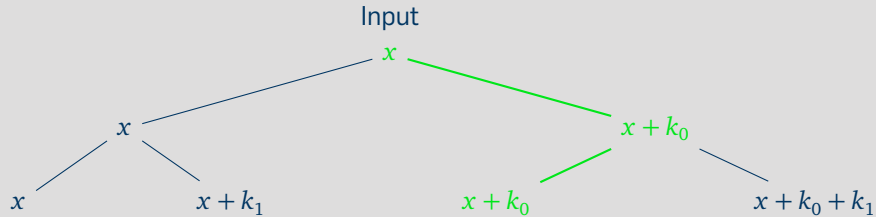
# The WSN construction

Encryption



# The WSN construction

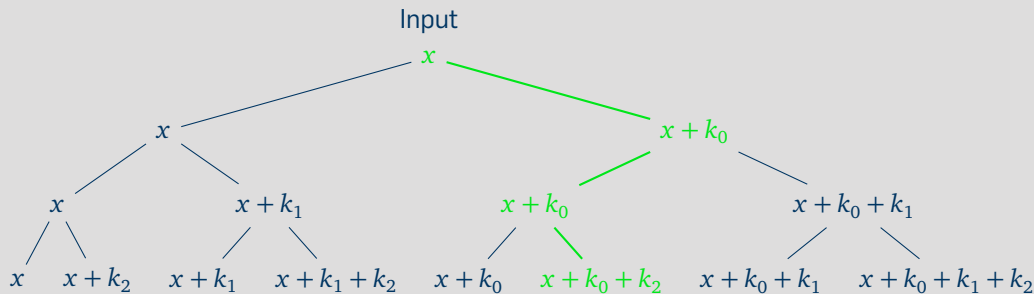
Encryption





# The WSN construction

## Encryption



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

# An Implementation

# An Implementation



## Construction

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

Theoretical vs. practical constructions

# 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  $x_i, y_i$ :  $\text{span}\{x_i + y_i\} \subseteq \text{span}\{k_j\}$ .

## 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  $x_i, y_i$ :  $\text{span}\{x_i + y_i\} \subseteq \text{span}\{k_j\}$ .

## 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  $u \in \text{span}\{k_1, \dots, k_r\}^\perp \neq \{0\}$

# 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  $x_i, y_i$ :  $\text{span}\{x_i + y_i\} \subseteq \text{span}\{k_j\}$ .

## 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  $u \in \text{span}\{k_1, \dots, k_r\}^\perp \neq \{0\}$

## Rationale 1

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

# Generic Analysis

On the Boolean functions  $f$

A bit out of the blue sky, but:

## Rationale 2

For any instance,  $f$  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

## Rationale 1

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

## Rationale 2

For any instance,  $f$  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*)



# A genus of the WSN family: BISON

## Rationale 1

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

## Rationale 2

For any instance,  $f$  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

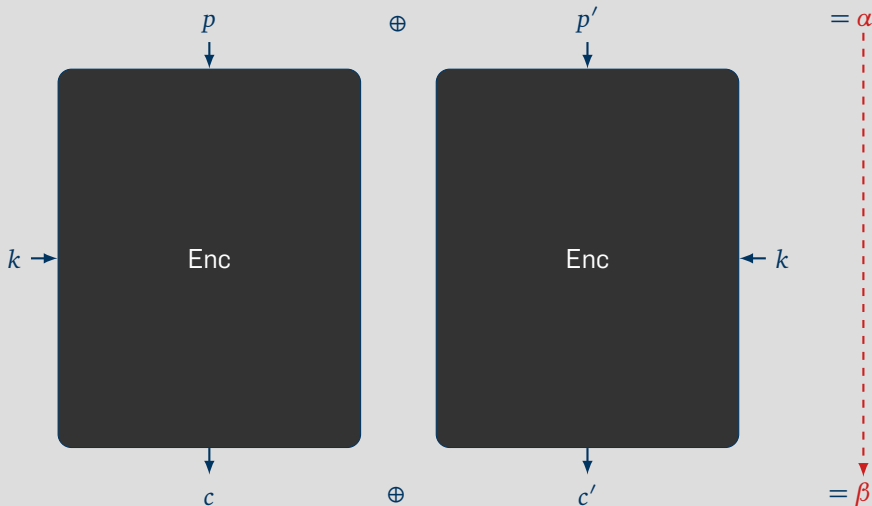
- At least  $n$  iterations of the round function
- Consecutive round keys linearly independent
- The round function depends on all bits
- $\forall \delta : \Pr[f_k(x) = f_k(x + \delta)] = \frac{1}{2}$  (*bent*)

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

But what about  
Differential Cryptanalysis?

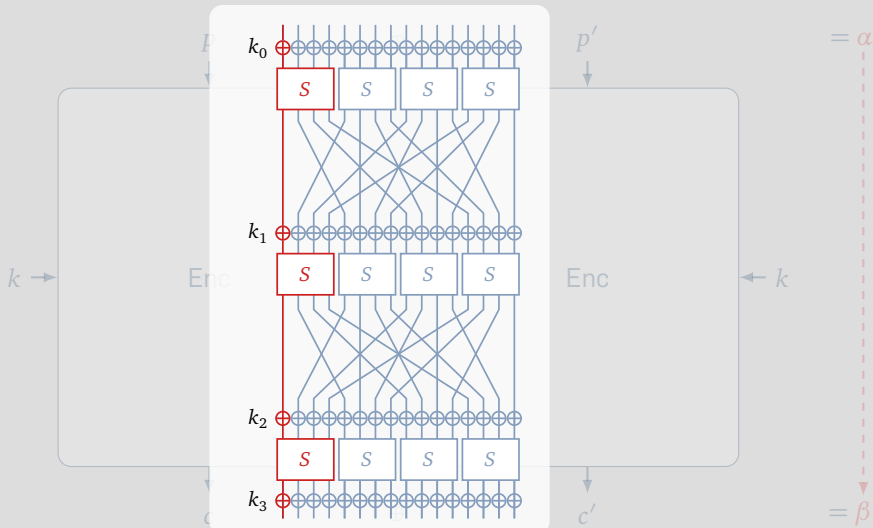
# Differential Cryptanalysis

## Primer



# Differential Cryptanalysis

Primer





# Differential Cryptanalysis

One round

## Proposition

For one round of BISON the probabilities are:

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

# Differential Cryptanalysis

One round

## Proposition

For one round of BISON the probabilities are:

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

## Possible differences

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

# Differential Cryptanalysis

One round

## Proposition

For one round of BISON the probabilities are:

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

## Possible differences

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

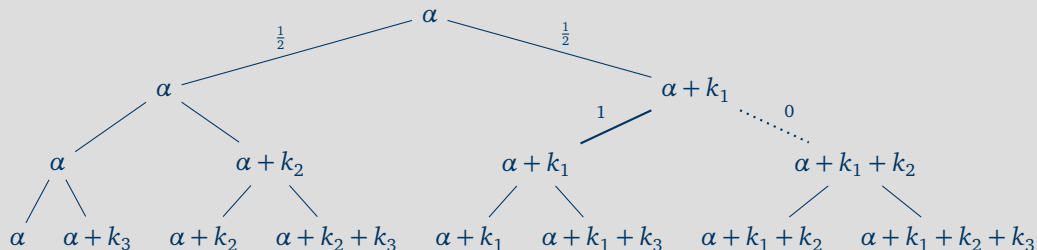
## Remember

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

# Differential Cryptanalysis

More rounds

Example differences over  $r = 3$  rounds:

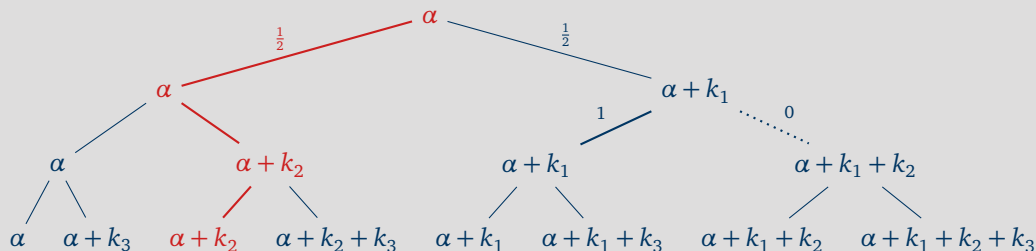




# Differential Cryptanalysis

More rounds

Example differences over  $r = 3$  rounds:



For fixed  $\alpha$  and  $\beta$  there is only *one* path!

## A concrete species



# Addressing Rationale 1

## The Key Schedule

### Rationale 1

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

#### Design Decisions

- Choose number of rounds as  $2 \cdot n$
- 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

### Rationale 2

For any instance, the  $f$  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  $f_k : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  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  $n$

# Conclusion/Questions

Thank you for your attention!

## 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?*

# 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

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

where

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

$$\Phi_k(x) : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^{n-1}$$

$$\Phi_k(x) := (x + x[i(k)] \cdot k)[j]_{\substack{1 \leq j \leq n \\ j \neq i(k)}}$$

$$f_{b(i)} : \mathbb{F}_2^{\frac{n-1}{2}} \times \mathbb{F}_2^{\frac{n-1}{2}} \rightarrow \mathbb{F}_2$$

$$f_{b(i)}(x, y) := \langle x, y \rangle + b(i),$$

- and  $b(i)$  is 0 if  $i \leq \frac{r}{2}$  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  $K = (k, w) \in (\mathbb{F}_2^n \times \mathbb{F}_2^{n-1}) \setminus \{0, 0\}$

The  $i$ th round keys are computed by

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

where

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



# Further Cryptanalysis

## Linear Cryptanalysis

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

## Zero Correlation

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

## Invariant Attacks

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

## Impossible Differentials

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