BISON
Instantiating the Withened Swap-Or-Not Construction

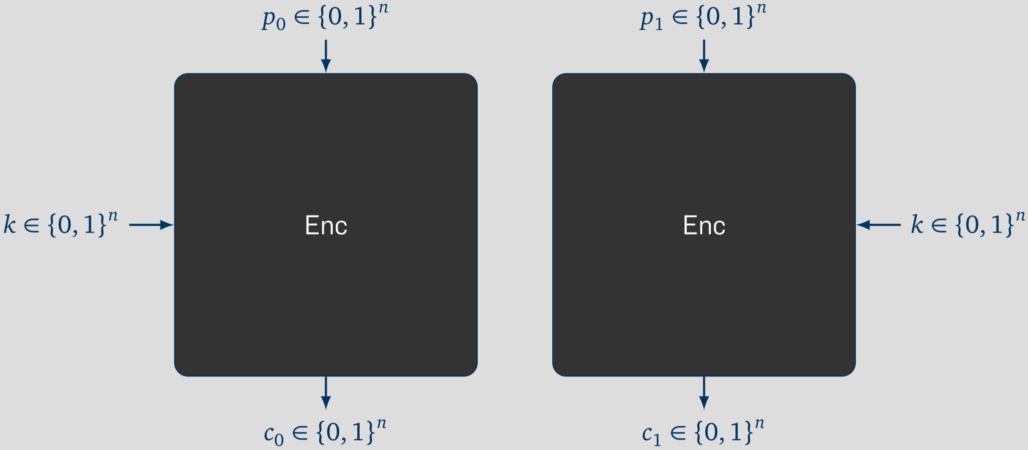
September 6th, 2018

Horst Görtz Institute for IT Security
Ruhr-Universität Bochum

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

Block Ciphers

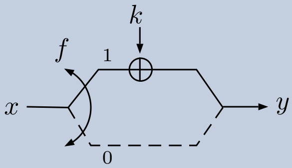
Encrypt plaintext in blocks p_i of n bits, under a key of n bits:



The WSN construction

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

Overview round, iterated r times



Whitened Swap-Or-Not round function

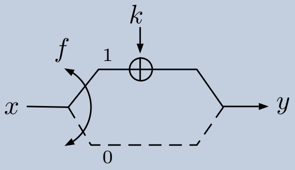
$$x, k \in \{0,1\}^n \quad \text{and} \quad f : \{0,1\}^n \to \{0,1\}$$

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

The WSN construction

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

Overview round, iterated r times



Whitened Swap-Or-Not round function

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

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

Properties of f (needed for decryption)

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

Security Proposition (informal)

The WSN construction with $r = \mathcal{O}(n)$ rounds is $(2^{n-\mathcal{O}(\log n)}, 2^{n-\mathcal{O}(1)})$-secure.

(p, q)-secure: Attackers querying the encryption at most p and the underlying f_i's q times have only negl. advantage.

The WSN construction

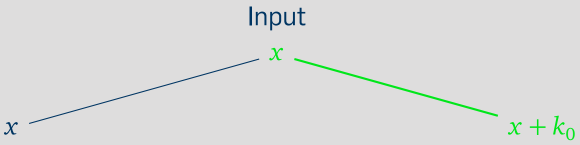
Encryption

Input

x

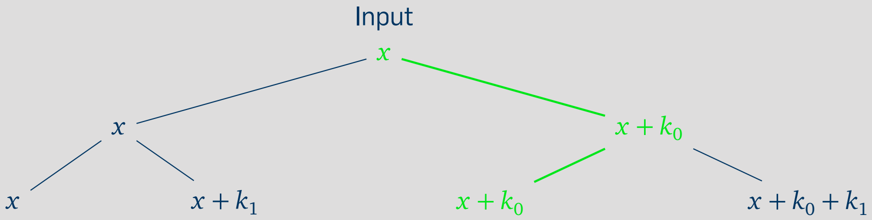
The WSN construction

Encryption



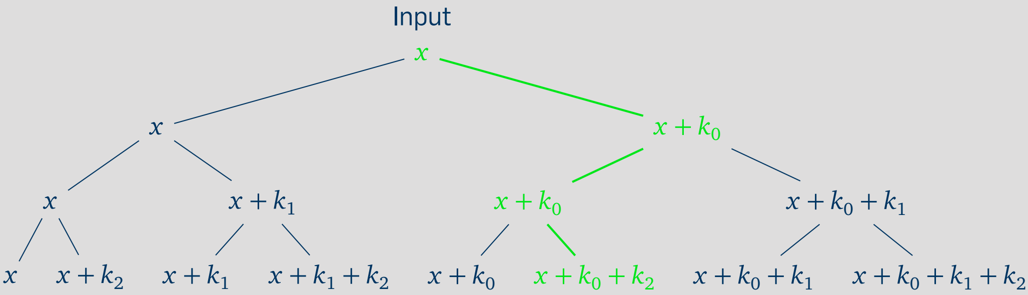
The WSN construction

Encryption



The WSN construction

Encryption



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

An Implementation

An Implementation

Construction

- $f(x) := ?$
- 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: $\operatorname{span}\{x_i + y_i\} \subseteq \operatorname{span}\left\{k_j\right\}$.

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

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: $\operatorname{span}\{x_i + y_i\} \subseteq \operatorname{span}\{k_j\}$.

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

Rationale 1

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

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

A genus of the WSN family: BISON

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
- $\forall \delta: \ \Pr[f(x) = f(x + \delta)] = \frac{1}{2}$ (*bent*)

A genus of the WSN family: BISON

RUB

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
- $\forall \delta : \Pr[f(x) = f(x + \delta)] = \frac{1}{2}$ (*bent*)

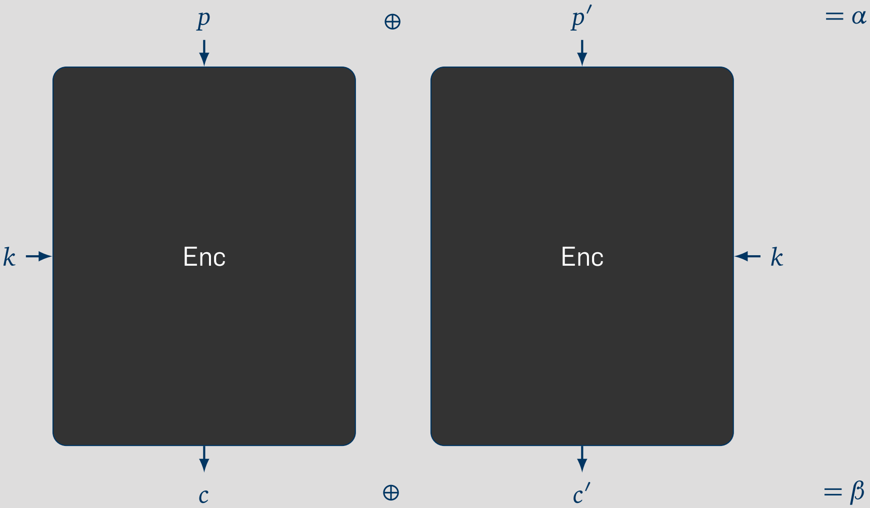
Rational 1 & 2: WSN is *slow* in practice!

But what about

Differential Cryptanalysis?

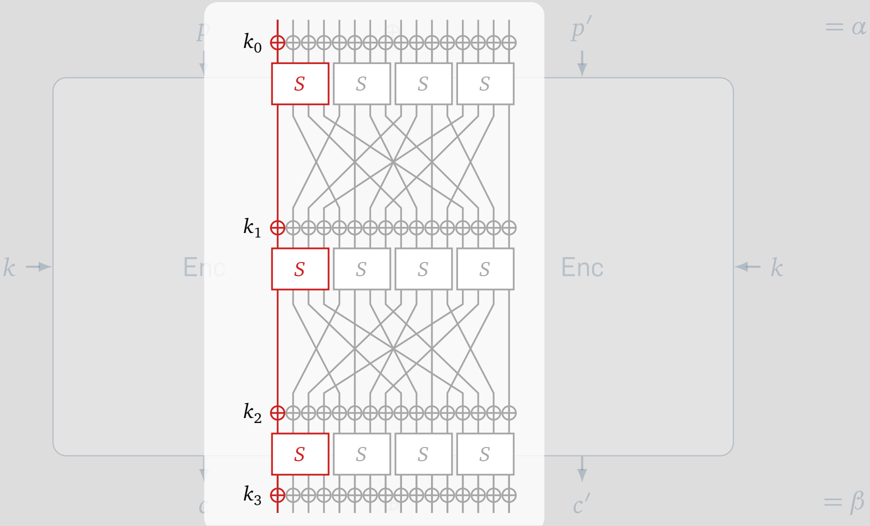
Differential Cryptanalysis

Primer



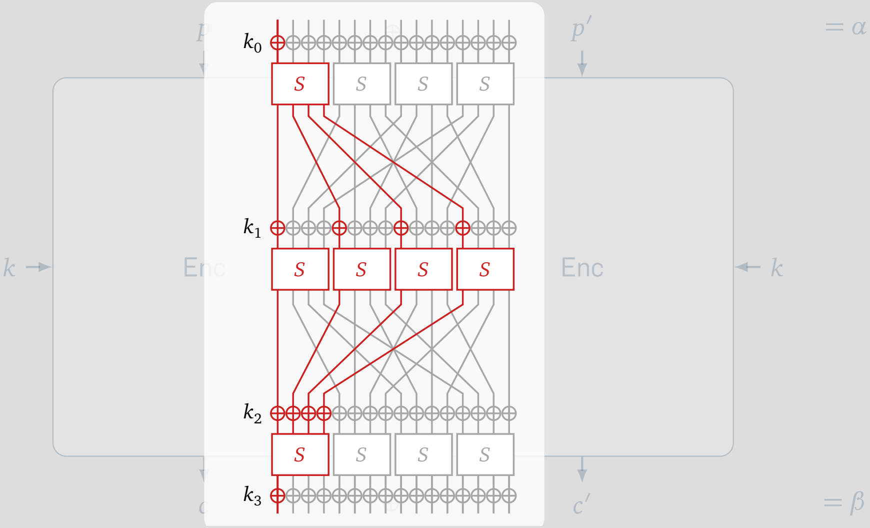
Differential Cryptanalysis

Primer



Differential Cryptanalysis

Primer



Differential Cryptanalysis

One round

RUB

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:

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

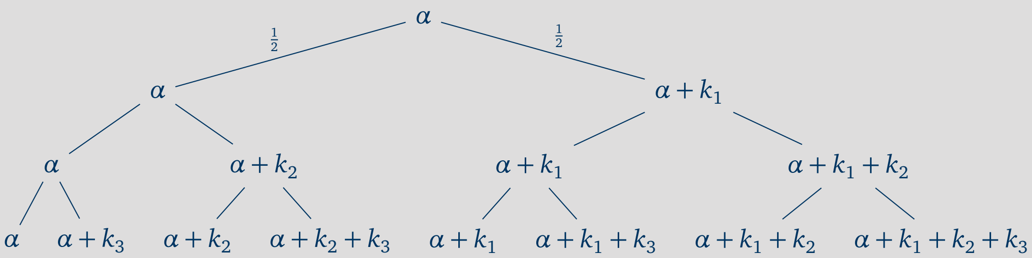
Possible differences:

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

Differential Cryptanalysis

More rounds

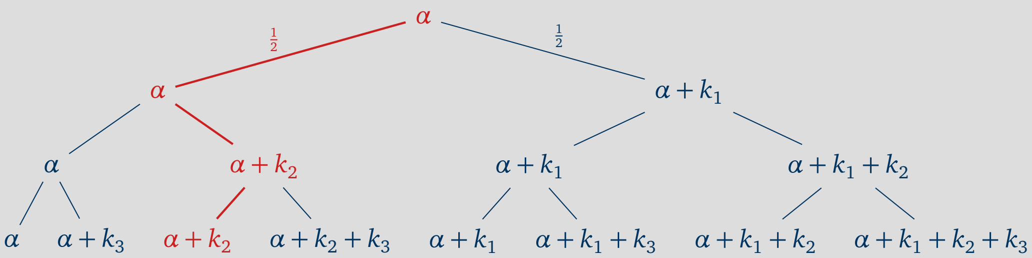
Example differences over $r = 3$ rounds:



Differential Cryptanalysis

More rounds

Example differences over $r = 3$ rounds:



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

A concrete species

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 $2 \cdot n$
- 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 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 $\delta \in \mathbb{F}_2^n : \Pr[f(x) = f(x+\delta)] \approx \frac{1}{2}$.

Design Decisions

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

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

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

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

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

RUB

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.

RUB

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

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

where

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

Further Cryptanalysis

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.