RUHR-UNIVERSITÄT BOCHUM

BISON
Instantiating the Whitened Swap-Or-Not Construction

November 14th, 2018

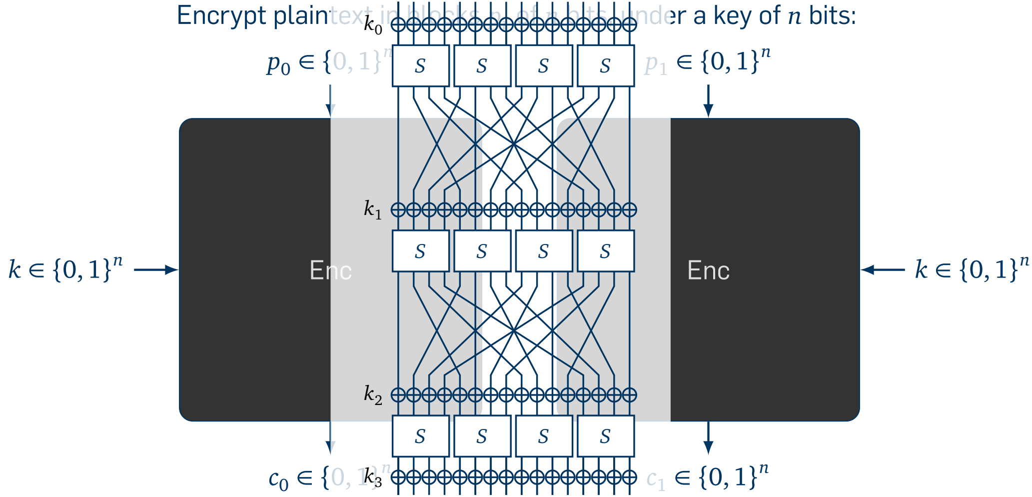
FluxFingers

Workgroup Symmetric Cryptography, Ruhr University 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:

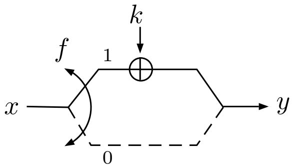


The WSN construction

RUB

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

Overview round, iterated r times



Whitened Swap-Or-Not round function

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

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

Properties of f_k (needed for decryption)

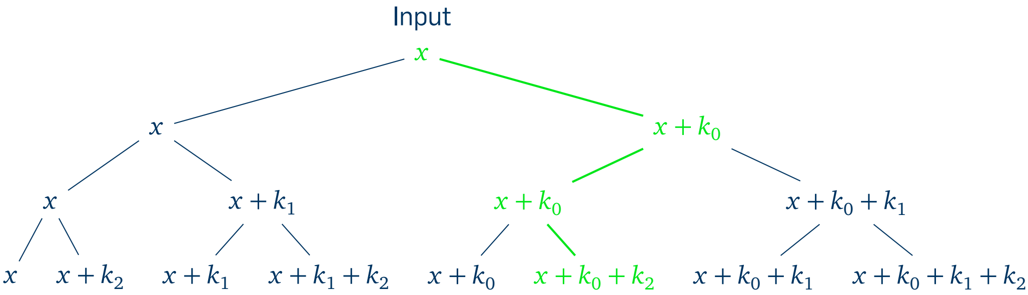
$$f_k(x) = f_k(x + k)$$

Security Proposition (informal)

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

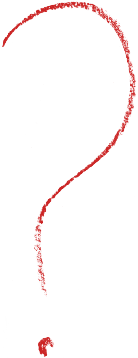
The WSN construction

Encryption



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

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

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

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_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

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

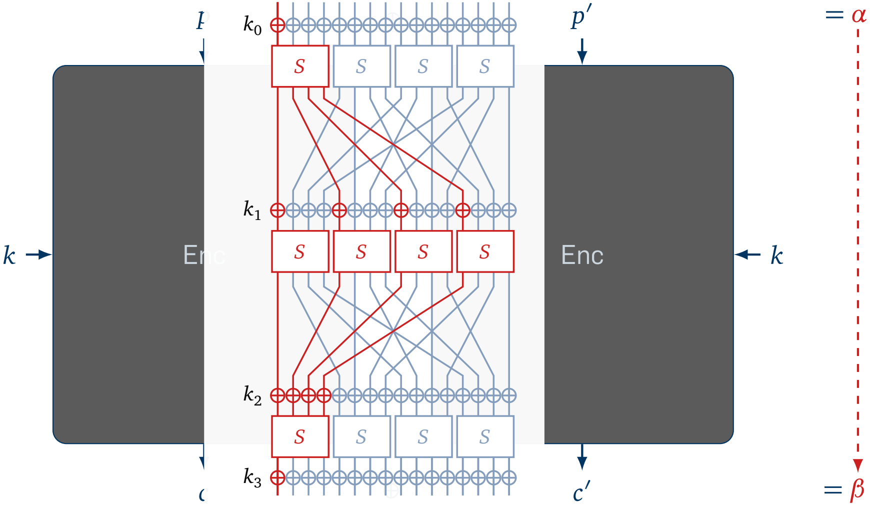
Rational 1 & 2: WSN is *slow* in practice!

But what about

Differential Cryptanalysis?

Differential Cryptanalysis

Primer



Differential Cryptanalysis

One round

RUB

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

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

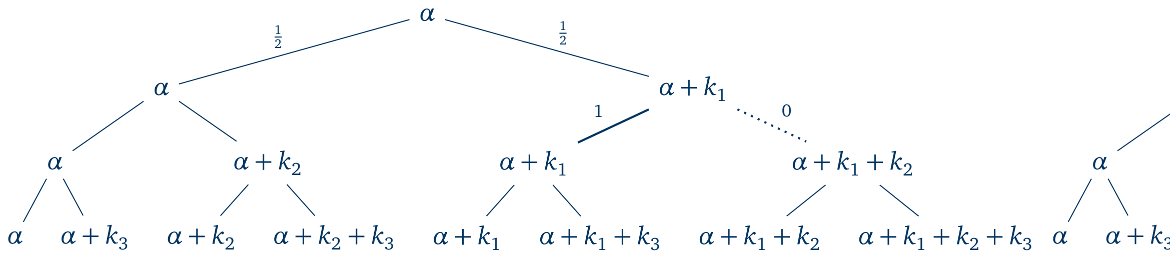
Remember

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

Differential Cryptanalysis

More rounds

Example differences over $r = 3$ rounds:



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

BISON

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 $3 \cdot n$
- Round keys derived from the state of LFSRs
- Add round constants 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

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/XXX

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

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.