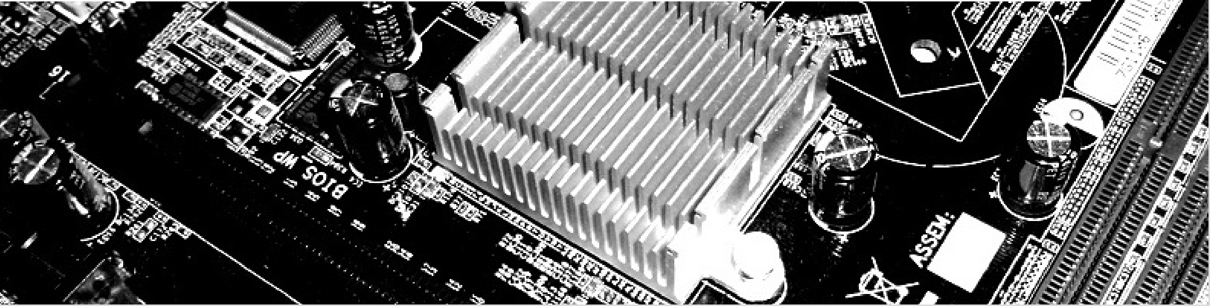
RUHR-UNIVERSITÄT BOCHUM

BISON
Instantiating the Withened Swap-Or-Not Construction

September 6th, 2018

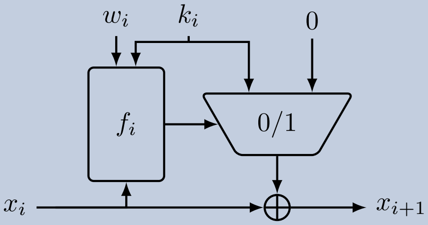
Horst Görtz Institute for IT Security
Ruhr-Universität Bochum
Virginie Lallemand, Gregor Leander, Patrick Neumann, and *Friedrich Wiemer*



The WSN construction

Published by Tessaro [Tes15] at AsiaCrypt 2015.

Overview



Whitened Swap-Or-Not round function

$$x_i \mapsto x_i + f_{b(i)}(w_i + \max\{x_i, x_i + k_i\}) \cdot k_i$$

Security Proposition (informal)

The WSN construction with $\mathcal{O}(n)$ rounds is

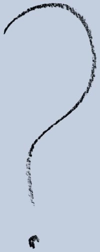
$(2^{n-\mathcal{O}(\log n)}, 2^{n-\mathcal{O}(1)})$-secure.

Is this a practical alternative to AES?

An Implementation

Is this a practical alternative to AES?

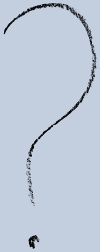
An Implementation



Is this a practical alternative to AES?

RUB

An Implementation



Outline

Generic Analysis

On the number of rounds

Observation

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

$$c = p + \sum_{i=1}^{r} \lambda_i k_i$$

- For pairs p_i, c_i: $\mathrm{span}\{p_i + c_i\} \subseteq \mathrm{span}\{k_j\}$.

Problematic because

- $\mathrm{span}\{k_j\} \subset \mathbb{F}_2^n$ reveals one bit of information on the round keys
- for $r < n$ there exists probability one linear hulls,
- for $r < 2n - 3$ there exists zero correlation linear hulls.

Rationale 1

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

Generic Analysis

On the Boolean functions f_i

Observation

- If the f_i do not depend on a (linear combination of) bit(s), i. e.

$$f_i(x) = f_i(x + \delta)$$

this difference propagates through the whole encryption with non-negligible probability.

Rationale 2

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

The Instance

Generic considerations

- Use a bent function for f_i
- Use LFSRs for key schedule

The Instance

BISON's round function

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} is defined as in ???,
- $f_{b(i)}$ is defined as

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

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

The Instance

BISON's key schedule

RUB

BISON's key schedule

For two primitive polynomials $p_w(x), p_k(x) \in \mathbb{F}_2[x]$ with degrees $\deg(p_w) = n-1$ and $\deg(p_k) = n$ and the master key $K = (k, w) \in \mathbb{F}_2^n \times \mathbb{F}_2^{n-1}$, $k, w \neq 0$ the key schedule computes the ith round keys as

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

where $C(\cdot)$ is the companion matrix of the corresponding polynomial, and

- $k_i = C(p_k)^i k$
- $c_i = C(p_w)^{-i} e_1$
- $w_i = C(p_w)^i w$

Differential Cryptanalysis

One round

Differential Cryptanalysis

More rounds

Further Cryptanalysis

- Linear Cryptanalysis
- Impossible Differentials
- Zero Correlation
- Invariant Attacks

Conclusion/Questions

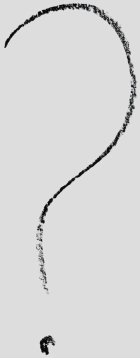
Thank you for your attention!

BISON

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

Open Problems

- Construction with similar good results for linear cryptanalysis
- Further analysis: division properties



References I

[Tes15] S. Tessaro. “Optimally Secure Block Ciphers from Ideal Primitives”. In: *ASIACRYPT'15*. Vol. 9453. LNCS. Springer, 2015, pp. 437–462. doi: 10.1007/978-3-662-48800-3_18.