BISON
Instantiating the Whitened Swap-Or-Not Construction

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

Horst Görtz Institute for IT-Security,
Ruhr-Universität Bochum, Germany

29th Crypto Day, 6/7 September 2018

While the majority of block cipher designs today are based on the key-alternating structure, this structure tends to be rather hard to tame from a provable security point of view – e. g. key-alternating ciphers do not achieve full domain security, that is security up to almost 2^n queries, and need one pseudorandom permutation for every round. Thus it is an interesting task to look for alternative design structures. Tessaro (2015) showed that the whitened Swap-or-Not construction (WSN), mapping in one round

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

is secure up to $2^{n-\mathcal{O}(\log n)}$ queries to the construction and $2^{n-\mathcal{O}(1)}$ queries to only two underlying pseudorandom functions $f_{b(i)}$. Nevertheless such a theoretical security result is of no avail for practitioners, if no instance of the construction is known.

To remedy this situation, we first extend Tessaros analysis from a cryptanalytic point of view, resulting in generic restrictions for any instantiation of the WSN construction. Subsequently, we propose BISON – a first WSN instance. For BISON we utilize n-bit Boolean functions that are bent for realizing the $f_{b(i)}$.

The strong cryptanalytic properties of bent functions then allow us to thoroughly understand the differential behaviour of BISON. In particular, we can give an elegant argument that for n or more rounds, the probability of any non-trivial *differential* in BISON is upper bounded by 2^{-n+1}. Note that one typically can only bound *differential characteristics*, which give only a weaker statement on the ciphers resistance against differential cryptanalysis.

While our arguments for security in the differential cryptanalysis case are strong, we unfortunately cannot give similar strong results for linear cryptanalysis – instead we fall back to standard arguments in this case. A second drawback of BISON, and due to the generic restrictions of the WSN construction of any instance, is its poor performance: to achieve security, the encryption has to iterate $2 \cdot n$ rounds.

References

Stefano Tessaro (2015). Optimally Secure Block Ciphers from Ideal Primitives. In *ASIACRYPT 2015, Part II*, Tetsu Iwata & Jung Hee Cheon, editors, volume 9453 of *LNCS*, 437–462. Springer, Heidelberg.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-06