MPRI Internship

Cryptanalysis of Tweakable Block Ciphers

Research area:	Symmetric Cryptography
Location:	Inria Paris, EPI Secret
Supervision:	Gaëtan Leurent

Block ciphers. Symmetric encryption schemes are designed with a bottom-up approach. We first design block ciphers processing messages with a fixed size (n bits, usually $n = 64$ for lightweight ciphers, and $n = 128$ for conventional ciphers). Mathematically, a block cipher with a k-bit key and n-bit blocks defines of family of permutations of n-bit strings, indexed by the key. The main security notion is that a block cipher should be indistinguishable from a pseudo-random permutation (PRP): the block cipher E_K with a random key K should be hard to distinguish from a random permutation. Block ciphers are used within a mode of operation (or mode) to deal with arbitrary-length messages, and to reach a specific security goal. A mode divides the message M into n-bit blocks M_i, and process the blocks one by one through the block cipher E with various chaining rules to produce ciphertext blocks C_i and/or an authentication tag T.

Tweakable block ciphers. In 2002, Liskov, Rivest and Wagner [LRW02] introduced *tweakable* block ciphers, a stronger primitive that takes a *tweak* input in addition to the key and plaintext. The tweak is a public input that provides variability to the scheme: for a given key, each tweak should provide an independent pseudo-random permutation.

Like block ciphers, tweakable block ciphers are very versatile: they can be used to provide confidentiality, authenticity, or integrity protection, using an appropriate mode of operation. Moreover, thanks to the extra input, modes for tweakable block ciphers are easier to design, and often reach higher security. For instance, the TAE mode proposed in [LRW02] (and its variant OCB) provide authenticated encryption with security up to 2^n queries, while the block cipher version of OCB is only secure up to $2^{n/2}$ queries.

Tweakable block cipher were mostly a theoretical model for a while, but they gained importance more recently, with several dedicated constructions, such as Kiasu, Deoxys, SCREAM, Skinny or QARMA. These designs use the same construction principles as block ciphers, and the extra tweak input is processes with the key in a tweak-key schedule. For instance, Kiasu-BC is a tweakable block cipher that is build from the AES, with an extra tweak addition after the key addition [JNP14]. When the tweak is fixed to zero, Kiasu-BC is just the AES.

Cryptanalysis. The goal of this internship is to study cryptanalysis techniques applicable to tweakable block ciphers. Cryptanalysis is an important topic in cryptography, as it is the only way to evaluate the concrete security of primitives. Many cryptanalysis techniques have been developed for block ciphers such as differential cryptanalysis, linear cryptanalysis, or integral attacks. These attacks can be applied to tweakable block ciphers, but the extra tweak input gives more power to the attacker, and he can usually break a few more rounds.

For instance, attacks based on differential cryptanalysis can use a difference in the tweak to cancel a difference in the state, in the same fashion as related-key differential attacks. This has been applied to Kiasu-BC by Dobraunig *et al.* [DL17], and they show that attacks can reach 8 rounds, while attacks against the AES only reach 7 rounds.

However, attacks based on related-key differential techniques typically use a small number of different tweaks, while the tweakable block cipher model allows for many different tweaks. Another approach is to adapt integral attacks, using a set of tweak where some bytes take all possible values. This has also been applied to Kiasu-BC [DEM16], and results in stronger integral attacks than on the AES.

More analysis is needed in order to better understand the security of tweakable block cipher. In particular, there are recent attack on the AES that could be improved using the tweak added in Kiasu-BC, such as the Demirci-Selçuk Meet-in-the-Middle [DS08]. During this internship, we plan to build a variant of this attack applicable to Kiasu-BC. Another potential research direction is to get a better understand of integral atatcks against tweakable block ciphers, to improve the results of [DEM16].

References

[DEM16] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. Square attack on 7-round kiasu-BC. In Mark Manulis, Ahmad-Reza Sadeghi, and Steve Schneider, editors, *ACNS 16*, volume 9696 of *LNCS*, pages 500–517. Springer, Heidelberg, June 2016.

[DL17] Christoph Dobraunig and Eik List. Impossible-differential and boomerang cryptanalysis of round-reduced kiasu-BC. In Helena Handschuh, editor, *CT-RSA 2017*, volume 10159 of *LNCS*, pages 207–222. Springer, Heidelberg, February 2017.

[DS08] Hüseyin Demirci and Ali Aydin Selçuk. A meet-in-the-middle attack on 8-round AES. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 116–126. Springer, Heidelberg, February 2008.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 274–288. Springer, Heidelberg, December 2014.

[LRW02] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, Heidelberg, August 2002.