Advanced cryptology (GBX9SY06)

✧

Exercice

Pierre Karpman

2017-11

1 Meet-in-the-middle attack on a tweakable block cipher

The goal of this exercice is to describe Wang et al.'s attack [WGZ+16] on Mennink's original $\widetilde{\mathrm{F}}[2]$ tweakable block cipher construction [Men15a]. This scheme was claimed to have security up to 2^n queries (when instantiated with an n-bit block cipher), but it in fact suffers from a meet-in-the-middle attack of complexity $2^{n/2}$. A patched version of $\widetilde{\mathrm{F}}[2]$ nonetheless achieves the resistance originally claimed [Men15b].

We first focus on the simple tweakable block cipher construction $\widetilde{\mathrm{E}} : \{0,1\}^\kappa \times \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ that from a block cipher $\mathrm{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ defines $\widetilde{\mathrm{E}}(k,t,\cdot) = \mathrm{E}(k \oplus t, \cdot)$. Consider adversaries who are given oracle access to $\widetilde{\mathrm{E}}^{\pm}(k,\cdot,\cdot)$ with an unknown key k (i.e. the adversaries may obtain encryption (resp. decryption) of chosen plaintexts (resp. ciphertexts) with a chosen tweak), and who can as well compute $\mathrm{E}^{\pm}$.

Q.1

Show that there is an adversary who runs in time t and makes q queries to its oracle that succeeds in recovering the key k with probability $\approx qt/2^\kappa$.

We now move to $\widetilde{\mathrm{F}}[2] : \{0,1\}^\kappa \times \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$, where $\widetilde{\mathrm{F}}[2]$ is defined from E in the following way:

1. $y_1 := \mathrm{E}(k,t)$
2. $x_2 := y_1 \oplus p$
3. $y_2 := \mathrm{E}(k \oplus t, x_2)$
4. $c := \widetilde{\mathrm{F}}[2](k,t,p) = y_1 \oplus y_2$

Consider adversaries given oracle access to $\widetilde{\mathrm{F}}[2]^{\pm}(k,\cdot,\cdot)$ and who can compute $\mathrm{E}^{\pm}$, and wish to recover k.

Q.2

Show that $\widetilde{\mathrm{F}}[2]^{-1}(k,0,0) = \mathrm{E}(k,0)$.

Q.3

Show that knowing $\mathrm{E}(k,0)$, an adversary can further recover $\mathrm{E}(k,t)$ for any t, by making the query $\widetilde{\mathrm{F}}[2](k,0,\mathrm{E}_k(0) \oplus t)$

Q.4

Show that it is then possible to obtain $\mathrm{E}(k \oplus t, \mathsf{const})$ for any value const by querying $\widetilde{\mathrm{F}}[2](k, t, \mathrm{E}(k, t) \oplus \mathsf{const})$

Q.5

Conclude by describing an attack that succeeds with probability $\approx qt/2^{\kappa}$, where q denotes the number of oracle queries to $\widetilde{\mathrm{F}}[2]^{\pm}$.

2 The XKCD S-box

What is seriously wrong with the S-box depicted in this comic?

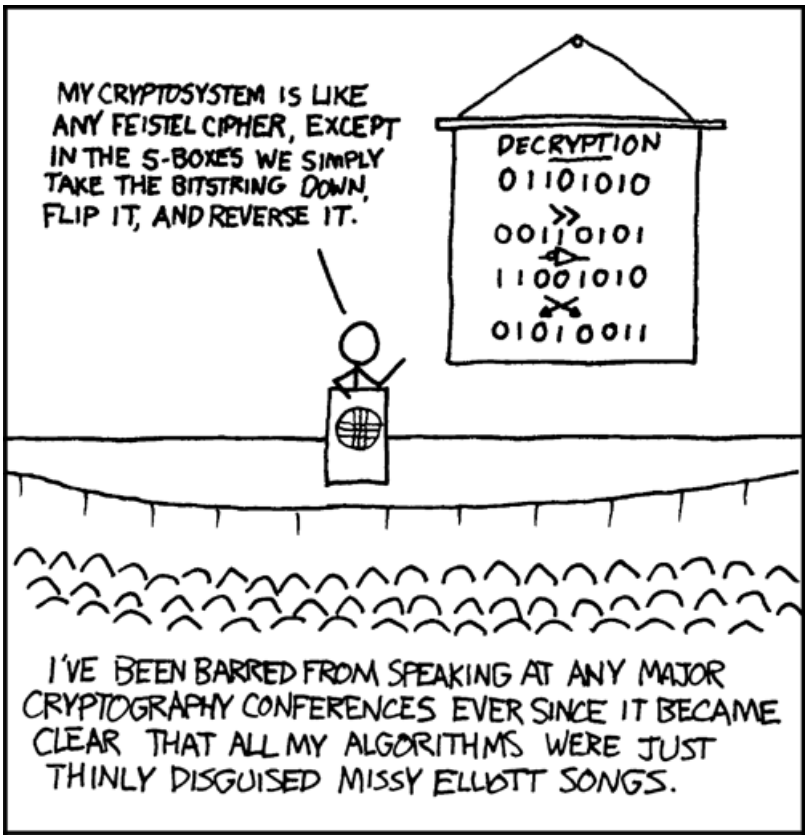

Figure 1: If you got a big keyspace, let me search it

References

[Men15a] Bart Mennink. Optimally secure tweakable blockciphers. In Gregor Leander, editor, *FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 428–448. Springer, 2015.

[Men15b] Bart Mennink. Optimally secure tweakable blockciphers. *IACR Cryptology ePrint Archive*, 2015:363, 2015.

[WGZ+16] Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, and Dawu Gu. How to build fully secure tweakable blockciphers from classical blockciphers. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016*, volume 10031 of *Lecture Notes in Computer Science*, pages 455–483, 2016.