A Statistical Saturation Attack against the Block Cipher PRESENT

- Errata and Improvement -

B. Collard*, F.-X. Standaert**

UCL Crypto Group, Microelectronics Laboratory, Université catholique de Louvain,
Place du Levant 3, Louvain-la-Neuve, Belgium

baudoin.collard;fstandae@uclouvain.be

The following remarks are related to Reference [1], Sections 2.1 and 2.2.

Errata.

In Section 2.1, the time complexity of the attack, using an FFT-based partial decryption process for a single round with 4 active S-boxes is given as $16 \cdot 2^{16}$. This evaluation is underestimated since this FFT computation has to be repeated for each value of the distribution to approximate. Given that the trail in [1] contains 8 variable bits, it means a corrected time complexity of $16 \cdot 2^{16} \cdot 2^8 = 2^{28}$.

Then, in the third extension of Section 2.2, it is proposed to reduce the data complexity of the attack at the cost of an increased time complexity, by performing a partial decryption of two rounds. Straightforwardly applying this trick implies 8 active S-boxes in the last round and 4 active S-boxes in the penultimate one. Hence, the same correction of the time complexity has to be applied, which yield a increased value of $(32 \cdot 2^{32} \cdot 2^{16}) \cdot (16 \cdot 2^{16} \cdot 2^8) = 2^{81}$.

Improvement.

Fortunately, the 2-round partial decryption process can also be improved in the following way. Just observe that it can actually be divided in two independent partial decryptions, as illustrated in Figure 1. Using this trick allows reducing the time complexity down to: $2 \cdot (16 \cdot 2^{16} \cdot 2^8) \cdot (8 \cdot 2^8 \cdot 2^4) = 2^{44}$.

Summarizing. The time complexity of the attacks in [1] have to be updated as in Table 1. In short, the time complexity of the attack using a 1-round partial decryption is increased from 2^{20} elementary operations to 2^{28} ones. And the (more critical) time complexity of the attack using a 2-round partial decryption is decreased from 2^{57} elementary operations to 2^{44} ones.

* Work supported by the Walloon Region under the project Nanotic-Cosmos.

** Associate researcher of the Belgian Fund for Scientific Research (FNRS-F.R.S.).

References

1. B. Collard, and F.-X. Standaert, *A Statistical Saturation Attack on the Block Cipher PRESENT*, in the proceedings of CT-RSA 2009, Lecture Notes in Computer Science, vol 5473, pages 195-210, San Francisco, California, USA, April 2009.

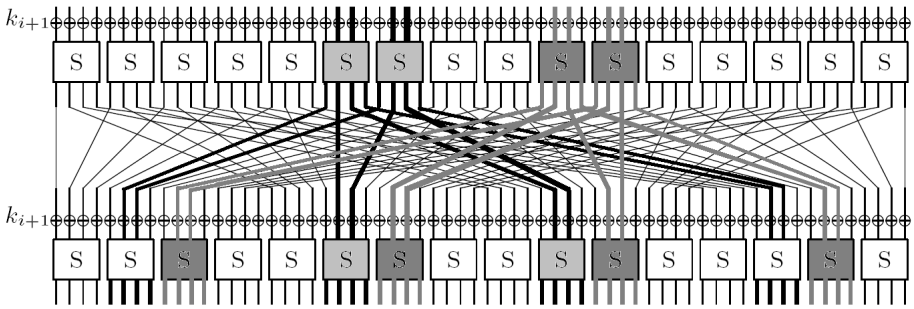

Fig. 1: Practical trails for 2-round partial decryption in PRESENT with reduced time complexity. The two independent trails are shown in different shades of gray.

#rounds	type of attack	data compl.	time compl.	memory compl.	gain	reference
8	our attack*	$c * 2^{12}$	2^{28} op.*	2^{16} counters	≤ 16	this paper
	our attack**	$c * 2^{9}$	2^{44} op.*	2^{32} counters	≤ 38	this paper
12	our attack*	$c * 2^{24}$	2^{28} op.*	2^{16} counters	≤ 16	this paper
	our attack**	$c * 2^{21}$	2^{44} op.*	2^{32} counters	≤ 38	this paper
16	our attack*	$c * 2^{36}$	2^{28} op.*	2^{16} counters	≤ 16	this paper
	our attack**	$c * 2^{33}$	2^{44} op.*	2^{32} counters	≤ 38	this paper
20	*our attack**	$c * 2^{48}$	2^{28} op.*	2^{16} counters	≤ 16	this paper
	*our attack***	$c * 2^{45}$	2^{44} op.*	2^{32} counters	≤ 38	this paper
24	*our attack**	$c * 2^{60}$	2^{28} op.*	2^{16} counters	≤ 16	this paper
	*our attack***	$c * 2^{57}$	2^{44} op.*	2^{32} counters	≤ 38	this paper

* 1-round decryption, ** 2-round decryption

Table 1: Summary of attacks (italic are not experimented and use **ext. 2**).