# Final Report for Check Point Scholarship

Achiya Bar-On
September 2016

## Research Summary

During the last year, we studied the security level of several block ciphers, as well as generic techniques of block cipher cryptanalysis. We obtained new results in three projects: MISTY1, GOST2, and generic slide attacks. We briefly describe these results below.

MISTY1. MISTY1 is a 64-bit block cipher with 128-bit keys designed in 1997 by Matsui. In the 18 years since then, MISTY1 withstood numerous cryptanalytic attempts till Yosuke Todo presented at CRYPTO'2015 [3] the first attack on the full MISTY1. The attack, based on a new variant of integral cryptanalysis, breaks the full MISTY1 with data complexity of $2^{63.994}$ chosen plaintexts and time complexity of $2^{107.3}$ encryptions.

After examining Todo's attack we presented a new attack on the full MISTY1 that improves over Todo's attack by a factor of $2^{38}$ using the 'partial sums' and 'multi-dimensioned meet-in-the-middle' techniques. Our attack is modular and has two phases (the first one is in itself a stand-alone attack). The first phase requires $2^{64} - 2^{50}$ chosen ciphertexts and allows to recover the equivalent of 49 key bits in time of $2^{64}$ encryptions. There are two options for second phase. One is simple exhaustive search that increases the time complexity to $2^{79}$ (with no change in the data complexity). The other allows to use the rest of the codebook and recover all remaining key bits in time of $2^{69.5}$ encryptions.

The paper describing this attack was published at the CRYPTO'2016 conference [1].

GOST2. GOST is a block cipher designed during the 1970's by the Soviet Union (USSR) government. GOST has a 32-round Feistel structure with a 64-bit block and a 256-bit master key. The round keys are derived from the master key by a simple key schedule. This simple key schedule was exploited in many attacks. In 2015, Dmukh, Dygin, and Marshalko presented GOST2 that is a modification of GOST [2]. The modified version differs from the original only in the order of the round sub-keys. The modification is aimed of strengthening the cipher (and thus making it resistant against the attacks on GOST) by a minor change.

Our research, joint with Prof. Orr Dunkelman from Haifa University and Tomer Ashur from KU Leuven, lead to three main attacks. The first one works for a weak class of $2^{256-32}$ possible keys and has complexities of $2^{192}$ time, $2^{32}$ known plaintexts and $2^{64}$ memory. The second attack only assumes that the round function is invertible and is in some sense a completion of the first attack. The attack requires $2^{63}$ chosen plaintexts, $\frac{2^{256}}{2e}$ full GOST2 encryptions and has memory complexity of $2^{160}$. The last attack uses a fixed point property and makes no assumption on the keys. It has time complexity of $2^{237}$ and memory complexity of $2^{196}$. Our attack is the first attack on GOST2

faster than exhaustive key search. It shows that the changes made in the transition from GOST to GOST2 are insufficient.

A paper presenting the attack was submitted for publication at the CT-RSA'2017 conference.

Slide attack on a Feistel cipher with 3-round self regularity. Another work, which is still in progress, concerns a generic attack rather than a specific primitive. In a joint work with Prof. Orr Dunkelman from Haifa University, we study the slide attack technique and apply it to a new family of ciphers.

We found a slide attack on a 3K-DES like cipher (a DES like cipher with 3-round self similarity), which is an n-bit Feistel cipher with an $\frac{n}{2}$-bit round function that can be presented as $E_K(P) = g^t(P)$, where $g = f_{K_3} \circ f_{K_2} \circ f_{K_1}$. A straightforward use of the slide technique would require roughly $2^{\frac{n}{2}}$ known plaintexts (because of the Birthday Paradox) or $2^{\frac{n}{4}}$ chosen plaintexts (exploiting the Feistel structure) and time complexity of $\approx 2^n \cdot r$, where $r$ is the time required for breaking $g$ given two input/output pairs.

We present an attack with time and data complexity of $2^{5n/6}$ (where the data is known plaintexts). The basic idea of the attack is to search for slid pairs (i.e., a pair $(P, P')$ of plaintexts such that $P' = g(P)$) that satisfy an additional property. The extra property allows us, combining it with a differential property, to discard quickly pairs that don't satisfy the relevant conditions. For the remaining pairs we can derive key candidates efficiently.

## Acknowledgements and Future Plan

I would like to thank the Checkpoint institute for their financial support in this research. I gratefully acknowledge this funding for giving me the ability to concentrate on my research much more easily during the funding period. As for the near future, I intend to continue my research (in the same area as the previous works), as part of my PHD studies.

## References

[1] Achiya Bar-On and Nathan Keller. A 2^70 attack on the full MISTY1. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 435–456, 2016.

[2] Andrey Dmukh, Denis Dygin, and Grigory Marshalko. A lightweight-friendly modifcation of GOST block cipher. *IACR Cryptology ePrint Archive*, 2015:65, 2015.

[3] Yosuke Todo. Integral cryptanalysis on full MISTY1. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 413–432, 2015.