Lightweight Cipher Resistivity against Brute-Force Attack: Analysis of PRESENT

Jan Pospíšil, Martin Novotný
Department of Digital Design
Czech Technical University in Prague, Faculty of Information Technology
Prague, Czech Republic
Email: pospij17@fit.cvut.cz, novotnym@fit.cvut.cz

***Abstract*—The PRESENT cipher is symmetric block cipher with 64 bits of data block and 80 (or 128) bits of key. It is based on Substitution-permutation network and consists of 31 rounds. PRESENT is intended to be implemented in small embedded and contactless systems, thus its design needs only small amount of chip area and consumes low power.**

In this work we evaluate the resistance of PRESENT against brute-force attack. We determine the computational demand of this type of attack conducted on special parallel hardware COPACOBANA consisting of array of FPGA chips with custom design.

***Index Terms*—reconfigurable hardware, FPGA, COPACOBANA, brute-force attack, PRESENT, cryptanalysis.**

I. Introduction

Lightweight cryptography is dealing with security of such products like tickets, RFID tags, car immobilizers or door openers. As many of those systems are powered from electromagnetic field, they must satisfy very strong design constrains on area and power consumption. Lightweight ciphers like Crypto1, KeeLoq or Hitag2 have been already broken [1], [2], [3], [4] or [5]. Surprisingly, although these ciphers are insecure either for their short key or for their wrong design, they are still used in many systems.

PRESENT [6] was designed as a replacement of above mentioned insecure ciphers. The goal of this work is exploration of its resistance against brute-force attack. We implement the breaker performing the brute-force attack on reconfigurable platform COPACOBANA, we measure the performance of the breaker and based on these measurements we evaluate the complexity of brute-force attack.

II. PRESENT cipher

PRESENT is a symmetric block cipher with 64-bit block and 80-bit (or 128-bit) key. It is based on Substitution-permutation network which consists of 31 rounds. Each round has three parts: bite-wise XOR of data with the round key, S-box modification (non-linear substitution) of data and permutation of data. Along with the data modification, the round key is modified too (it is done by S-box and XOR with actual number of round).

III. Implementation Platform—COPACOBANA

The COPACOBANA (Cost-Optimized Parallel Code Breaker) machine [7] is a high-performance, low-cost cluster consisting of 120 Xilinx Spartan3-XC3S1000 FPGAs. Currently, COPACOBANA and its successor RIVYERA appear to be the only such reconfigurable parallel FPGA machines optimized for code breaking tasks reported in open literature. Depending on the actual algorithm, the parallel hardware architecture can outperform conventional computers by several orders of magnitude.

IV. Related work

There are some existing works of cryptanalysis of PRESENT cipher, but no one with the brute-force approach. None of these works uses parallel computing systems like the COPACOBANA used in this work. Existing mathematical attacks are based on reduced cipher, mostly with round count up to 25. Overview of these attacks can be seen in [8]. Concerning this work there is implementation of DES cipher cryptanalysis for COPACOBANA hardware in [7].

V. Implementation of attack

The design was written in VHDL and synthesized and implemented in Xilinx ISE 11.5. We have implemented the PRESENT cipher in three different ways: simple core, pipelined core and serial (iterated). The variant with the best time-area product was used in the final design for the measurement.

A. Design overview

We have chosen the **pipelined core** for the implementation due to its highest performance. We managed to implement two pipelined cores in one FPGA, i.e. 240 computing units can be implemented in fully occupied COPACOBANA. Because of better scalability and distribution of the work, we have decided to create controlling logic for each core separately. The topmost entity in every chip interfaces the bus signals and cracker entity itself. Moreover, it does clock conversion - COPACOBANA bus runs at 20 MHz clock, our cracker runs at 100 MHz.

To parallelize the attack, the search space is divided into *key subspaces*. Each FPGA is by the host computer assigned with one subspace to search in. All keys in key subspace are then generated by internal counter. If the search in the subspace is finished without any success, then the FPGA is assigned with another subspace. The attack runs until the key is found or until all key subspaces are explored.

VI. Results

We were able to implement 2 pipelined cores in 1 FPGA. Each core has the throughput of 1 verified key per 1 clock cycle. Maximum achieved frequency was 100 MHz, i.e., one FPGA verifies 200 million keys per second and the whole COPACOBANA with 120 FPGAs verifies 24 billion keys per second. Searching the whole key space of 2^{80} keys takes

$$T_{worst} = \frac{2^{80}}{24 \cdot 10^9 \cdot 86400 \cdot 365.25} \approx 1.596 \cdot 10^6 \,\text{years}$$

with one COPACOBANA. Brute force attack on 80 bit PRESENT takes almost 800000 COPACOBANA-years on average, which makes PRESENT good solution for lightweight cryptography.

VII. Conclusions

We have implemented the PRESENT cipher in the VHDL for COPACOBANA platform in several ways. With the most favourable implementation we have created the design for the brute-force attack and verified it on the real hardware. According to our calculations this type of attack would last for more than 800 thousand years on average with one COPACOBANA. Due to the good scalability, this drawback can be counterbalanced by the greater amount of COPACOBANA machines. When buying 1 million of COPACOBANAs, the attack can be successfully mounted in one and half year in the worst case. However, according to [9], such an attack would cost around 10^{10} USD, which is comparable to the actual GDP of Mongolia.

Even without revealing any unknown key, our work was successful. We have evaluated the amount of resources necessary for mounting successful brute-force attack on PRESENT. Resources spent to break the cipher are too high with respect to application area of the cipher. Therefore, PRESENT is safe for daily usage in lightweight cryptography.

VIII. Acknowledgement

This work has been partially supported grant No. SGS12/094/OHK3/1T/18 and grant No. SGS10/119/OHK3/1T/18.

References

[1] G. de Koning Gans, J.-H. Hoepman, and F. Garcia, "A Practical Attack on the MIFARE Classic," in *Smart Card Research and Advanced Applications*, ser. LNCS. Springer, 2008, vol. 5189, pp. 267–282.

[2] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. Shalmani, "On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme," in *Advances in Cryptology — CRYPTO 2008*, ser. LNCS. Springer, 2008, vol. 5157, pp. 203–220.

[3] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel, "A Practical Attack on KeeLoq," in *Proceedings of EUROCRYPT'08*. Springer, 2008, pp. 1–18.

[4] N. Courtois, S. O'Neil, and J.-J. Quisquater, "Practical Algebraic Attacks on the Hitag2 Stream Cipher," in *Information Security*, ser. LNCS. Springer, 2009, vol. 5735, pp. 167–176.

[5] P. Štembera and M. Novotný, "Breaking Hitag2 with Reconfigurable Hardware," in *Proceedings of the 14th Euromicro Conference on Digital System Design*. IEEE Computer Society Press, 2011, pp. 558–563.

[6] A. Bogdanov, G. Leander, L. R. Knudsen, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT — An Ultra-Lightweight Block Cipher," in *Proceedings of CHES 2007*, ser. LNCS, vol. 4727. Springer, 2007, pp. 450–466.

[7] T. Gueneysu, T. Kasper, M. Novotný, C. Paar, and A. Rupp, "Cryptanalysis with COPACOBANA," *IEEE Transactions on Computers*, vol. 57, pp. 1498–1513, 2008.

[8] O. Özen, K. Varıcı, C. Tezcan, and e. Kocair, "Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT," in *Information Security and Privacy*, ser. LNCS. Springer, 2009, vol. 5594, pp. 90–107.

[9] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, and M. Schimmler, "Breaking Ciphers with COPACOBANA – A Cost-Optimized Parallel Code Breaker," in *Proceedings of CHES 2006*, ser. LNCS. Springer, 2006, vol. 4249, pp. 101–118.