Internship of Master II

Cryptanalysis of Symmetric Primitives: Improving Differential MITM Attacks

Mars-September 2022

with María Naya-Plasencia

1 Context of the Internship

The internship will take place at Inria-Paris, at the COSMIQ team[1] (Paris 12ème), in the context of the ERC project QUASYModo[2], that started in september 2017 and will end in september 2023. A PhD funding will be available for continuing the internship if pertinent.

2 Introduction

Cryptanalysis is the foundation of the confidence we have in the cryptographic primitives we use: trying to break them and determining their security margins are fundamental tasks in order to understand the security they can offer.

Symmetric cryptanalysis is a very active and innovative field. There are several families of attacks, the main ones being differential [4] and linear [8], but many others exist and they have all profited from many evolutions through the last years, like MITM (meet-in-the-middle) attacks and their variants (see [7]), differential-linear attacks [2], impossible differential attacks [3,6] each providing the best results on different constructions.

Though improvements and applications of these attacks are often published, the appearance of new attacks is less common. This year, we discovered a new type of attack, called the differential meet-in-the-middle attack, and using it, we managed to provide the best known attack on the popular cipher SKINNY [1], being the first one to reach 24 and 25 rounds. This work is currently under submission.

3 Work Description

There are many improvements to propose on this new type of attack, and many new applications to find. We plan to apply it on hash functions, to adapt it to bicliques, and to find possible further optimizations.

[1] `https://www.rocq.inria.fr/secret/`

[2] `https://www.inria.fr/en/centre/paris/news/erc-grant-for-maria-naya-plasencia`

During this stage, the intern will first study this new attack, and later we will work on combining it with biclique techniques [5] and applying further possible improvements.

Optionally, proposing a quantum version of the attack, optimizing it by applying quantum tools, can also be considered.

Contact

If you might be interested, please contact me and I can explain the details while having a coffee or tea:

maria.naya_plasencia@inria.fr

INRIA Paris
2 Rue Simone IFF
75012 Paris - France

References

1. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9815, pp. 123–153. Springer (2016), https://doi.org/10.1007/978-3-662-53008-5_5
2. Beierle, C., Leander, G., Todo, Y.: Improved differential-linear attacks with applications to ARX ciphers. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III. Lecture Notes in Computer Science, vol. 12172, pp. 329–358. Springer (2020), https://doi.org/10.1007/978-3-030-56877-1_12
3. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. Lecture Notes in Computer Science, vol. 1592, pp. 12–23. Springer (1999), https://doi.org/10.1007/3-540-48910-X_2
4. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1990), https://doi.org/10.1007/3-540-38424-3_1
5. Bogdanov, A., Khovratovich, D., Rechberger, C.: Biclique cryptanalysis of the full AES. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings. Lecture Notes in Computer Science, vol. 7073, pp. 344–371. Springer (2011), https://doi.org/10.1007/978-3-642-25385-0_19

6. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: Applications to clefia, camellia, lblock and simon. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I. Lecture Notes in Computer Science, vol. 8873, pp. 179–199. Springer (2014), https://doi.org/10.1007/978-3-662-45611-8_10
7. Canteaut, A., Naya-Plasencia, M., Vayssière, B.: Sieve-in-the-middle: Improved MITM attacks. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I. Lecture Notes in Computer Science, vol. 8042, pp. 222–240. Springer (2013), https://doi.org/10.1007/978-3-642-40041-4_13
8. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer (1993), https://doi.org/10.1007/3-540-48285-7_33