New tools for quantum rebound attacks

Context

The rebound attack is a powerful cryptanalysis technique aimed at cryptographic permutations and hash functions. Notably, since its introduction in [8] it has been used to obtain some of the best collision attacks on hash functions like Grøstl, AES-DM or Saturnin (in the family of so-called "AES-like" designs, which follow the design principles of the AES cipher).

The goal of rebound attacks is to solve the following cryptographic problem. Given a permutation $P : \{0,1\}^n \to \{0,1\}^n$, and a pair of differences $\Delta_i, \Delta_o \in \{0,1\}^n$, find a pair of values x, x' such that $x \oplus x' = \Delta_i$ and $P(x) \oplus P(x') = \Delta_o$. This input-output condition can be modified in different ways; for example the differences may be *truncated*, i.e., replaced by sets of differences. The rebound attack constructs a suitable x by separating P in three parts: $P = P_o \circ P_m \circ P_i$. One first creates many difference pairs for the middle permutation P_m (*inbound phase*), then finds among these pairs one that leads to differences Δ_i, Δ_o through P_i and P_o respectively (*outbound phase*).

Quantum Rebound Attacks. Even though large-scale quantum computers are not available yet, there exists well-established frameworks for quantum algorithms, which allow to design such algorithms for cryptanalytic scenarios and to determine precisely their complexity. This is the context of *quantum cryptanalysis*, which has received significant attention in the last decade. Indeed, cryptanalysis aims at quantifying the security offered by cryptographic designs on the long term, which includes the possibility of future quantum computers.

Quantum rebound attacks were initially introduced by Hosoyamada and Sasaki [7]. They were subsequently improved in [4] by restricting the memory usage. Later in [5], the authors attacked compression functions by introducing differentials in the key schedule. In this context, the permutation P becomes a block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, where both the key input and the plaintext input are free to choose. As these attacks can quickly become complicated, different automatic tools have been developed to find them [3, 1]. With such tools, the choice of an attack path (e.g., the P_o, P_i, P_m and difference patterns) is encoded as a set of Boolean or continuous variables, and the best attack is found by optimizing some objective function of the variables. Since off-the-shelf solvers can be used for the optimization itself, the main difficulty is to find an appropriate modeling of the attack.

Goal of the Internship

The goal of this internship is to improve the analysis of quantum rebound attacks on AES-like permutations (thus, focusing on the key-less setting).

At first, we will do a literature review of these attacks and the algorithmic techniques which were applied. The goal will be to determine if more advanced techniques, like quantum list merging, can allow to obtain better attacks. By "better", we mean either decreasing the quantum time complexity or the memory requirements.

Then, if time permits, we will study automatic tools for searching attacks, and their application in the quantum setting. Indeed, the current available models [3, 1] combine different tools (mixed-integer linear programming, constraint programming) and typically focus on the probability of the differential path, not on the complexity of the complete attack. Our goal will be to design a more direct modeling.

Location and Prerequisites. The internship will be hosted at the Inria center at the University of Rennes (Campus de Beaulieu, 263 Av. Général Leclerc, Bât 12f 35042 - Rennes) in the CAPSULE team and supervised by André Schrottenloher (Chargé de Recherche, 02 99 84 75 02 - andre.schrottenloher@inria.fr).

Candidates should have experience with cryptography, but not necessarily symmetric cryptanalysis. Even though it could be a plus, prior experience with quantum computing is not a requirement. If the internship is successful, a fully funded PhD position will be available (the topic of the PhD will be similar to this internship proposal).

References

[1] Bao, Z., Guo, J., Li, S., Pham, P.: Automatic quantum multi-collision distinguishers and rebound attacks with triangulation algorithm. In: ACISP (2). Lecture Notes in Computer Science, vol. 14896, pp. 24–43. Springer (2024)

[2] Canteaut, A., Duval, S., Leurent, G., Naya-Plasencia, M., Perrin, L., Pornin, T., Schrottenloher, A.: Saturnin: a suite of lightweight symmetric algorithms for post-quantum security. IACR Trans. Symmetric Cryptol. **2020**(S1), 160–207 (2020). https://doi.org/10.13154/TOSC.V2020.IS1.160-207, https://doi.org/10.13154/tosc.v2020.iS1.160-207

[3] Dong, X., Guo, J., Li, S., Pham, P.: Triangulating rebound attack on aes-like hashing. In: CRYPTO (1). Lecture Notes in Computer Science, vol. 13507, pp. 94–124. Springer (2022)

[4] Dong, X., Sun, S., Shi, D., Gao, F., Wang, X., Hu, L.: Quantum collision attacks on aes-like hashing with low quantum random access memories. In: ASIACRYPT (2). Lecture Notes in Computer Science, vol. 12492, pp. 727–757. Springer (2020)

[5] Dong, X., Zhang, Z., Sun, S., Wei, C., Wang, X., Hu, L.: Automatic classical and quantum rebound attacks on aes-like hashing by exploiting related-key differentials. In: ASIACRYPT (1). Lecture Notes in Computer Science, vol. 13090, pp. 241–271. Springer (2021)

[6] Gauravaram, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: Grøstl-a sha-3 candidate. Schloss-Dagstuhl-Leibniz Zentrum für Informatik (2009)

[7] Hosoyamada, A., Sasaki, Y.: Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound. In: EUROCRYPT (2). Lecture Notes in Computer Science, vol. 12106, pp. 249–279. Springer (2020)

[8] Lamberger, M., Mendel, F., Rechberger, C., Rijmen, V., Schläffer, M.: Rebound distinguishers: Results on the full whirlpool compression function. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 5912, pp. 126–143. Springer (2009)