Quantum Boomerang Attacks and Some Applications

Paul Frixons[1,2]

[1] Orange Labs, Caen, France
[2] Inria, Paris, France

Nowadays, it is well-known that the existence of quantum computers is one of the most significant threats cryptography has ever faced. Its capacity to compute discrete logarithms and factorizations [Sho97], endangering current public key cryptography, and to speed up exhaustive search of keys [Gro96], concerning secret key cryptography, is understood. However, its potential use against special vulnerabilities of the cipher remains unclear.

In this context, we focus on a well-known family of attack, the boomerang attacks. Introduced by Wagner in [Wag99], they are a particular type of differential attacks that, instead of considering a long differential trail in the primitive (a propagation of differences from the plaintext through the ciphertext), combine several short ones that have high individual probabilities. While differential attacks usually consider pairs of plaintexts having a certain difference, boomerang attacks use quartets instead.

From classical boomerang attacks, we build quantum key-recovery attacks. Our work takes place in the Q2 model of quantum attacks, which means the attacker has a quantum access to the primitive and to a quantum machine for processing. This model allows for attacks on some classically proved constructions (namely the Even-Mansour [KM12] and 3-round Feistel [KM10] schemes). It makes possible for us to use freely the Grover's [Gro96] and Ambainis' [Amb07] algorithms.

In some cases, we can get a quadratic speedup from our conversion from classical to quantum attacks. Then, we apply this technique to a 5-round attack on SAFER++ [BCD03,Mas93] and on full AES-256 in the related-key model [BK09,DR99].

References

[Amb07] Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM J. Comput.*, 37(1):210–239, 2007.

[BCD03] Alex Biryukov, Christophe De Cannière, and Gustaf Dellkrantz. Cryptanalysis of SAFER++. In *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 195–211. Springer, 2003.

[BK09] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2009.

[DR99] Joan Daemen and Vincent Rijmen. AES proposal: Rijndael. Submission to NIST AES competition, 1999.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *STOC*, pages 212–219. ACM, 1996.

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *ISIT*, pages 2682–2685. IEEE, 2010.

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type even-mansour cipher. In *ISITA*, pages 312–316. IEEE, 2012.

[Mas93] James L. Massey. SAFER K-64: A byte-oriented block-ciphering algorithm. In *FSE*, volume 809 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 1993.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[Wag99] David A. Wagner. The boomerang attack. In *FSE*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.