Quantum-Enhanced Partial Leak Attack on a Symmetric Cipher

A D Moiseevskiy[1]

[1] *Quantum Technologies Center and Faculty of Physics, Lomonosov Moscow State University, 1, Leninskye Gory, 119991, Moscow, Russia. Contact Phone: +79680169732*
Contact Email: amoiseevskiy@gmail.com

This report is a further research of the key-leak based qubit-optimized attack on symmetric ciphers. Here I present a full algorithm for optimized Grover attack on two round 16-bit cipher Simplified-AES that allows to break the key with quadratic speedup using 25 qubits if consecutive bits of the key were compromised with side-channel attack.

At present, QKD systems operating on the principle of preparation and measurement of quantum states are well developed. But in practice, using of a one-time pad is often difficult or impossible. Then, symmetric cipher like AES need to be use over a quantum key distribution system to improve the security when the same initial key is used more than once.

An important advantage of Grover's quantum attack is the ability to break any ciphers in the presence of text and ciphertext. Even in case of AES over QKD, Grover's attack still provides a quadratic drop in key strength, which potentially expands the possibilities of its application.

Here I present a hybrid approach algorithm for attacking a symmetric cipher S-AES with partial key leakage. Compared to previous results [1], I managed to solve the problem of non-unitary transformations in intermediate round keys generation and get rid of the need to use ancilla qubits. The new approach concentrates on generating the ciphertext itself, using the key expansion quantum register as a workspace in between. Together with the 4-qubit S-AES S-box presented in [2], for the S-AES attack, it is possible to limit the qubit requirement to 25 qubits if 8 key bits were leaked. The S-AES topology retains restrictions on the leak configuration, but cases have been successfully simulated for leaking the first or second half of the initial key.

The new approach potentially allows to run the attack on today's NISQ-devices and perform numerical simulations with GPU, that may be useful for further research of errormitigation techniques. Simulations were performed using a PC with 8 GB RAM onboard, while a full S-AES attack without leaks requires 32 qubits and more than 32 GB of RAM as well as extreme processor performance. The obtained result makes possible the further study of error mitigation methods applied to this attack and potentially allows to experimentally perform elements of the attack with quadratic acceleration on the existing 25-qubit quantum computer. And using the IBM Osprey, the largest 433-qubit quantum computer to date, it becomes possible to carry out this attack with basic error correction.

Acknowledgements: I acknowledge support from JSCo Russian Railways.

References

[1] A Moiseevskiy, Proc of the 5-th International School on Quantum Technologies, Khosta, Sochi, 2-8, October, 2022, p. 3

[2] K B Jang, G J Song, H J Kim and H J Seo, Proc. of the 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 1-3 November 2021, p. 1