Quantum Speedup on S-DES Known Plaintext Attack

과목 75 최종보고서

2017320009 이상헌
2017320023 조민규

June 16, 2020

1 서론

한 학기동안, Simplified DES에 대한 Known Plaintext Attack을 Quantum computer (simulator)을 사용하여 공격하는 방법에 관하여 연구하였다. 이를 위해 Microsoft Q#을 사용하여 Quantum S-DES Oracle을 만들어 이에 Grover's Algorithm을 적용시켰다.

2 연구 내용

Simplified DES는 Symmetric-key cryptosystem으로, DES와 유사한 구조로 되어 있지만, key size가 10bit, block size가 8 bit으로 줄어들고, 라운드 수 역시 2라운드로 줄어든 간략화된 구조로 되어 있다.

S-DES의 경우 일반 컴퓨터를 사용해서도 공격을 하는 데에 오랜 시간이 걸리지 않는다. 하지만 S-DES는 그 전신인 DES와 유사한 구조로 되어 있고, classic logic gate(And, Or, Not, Xor 등)를 사용하기에 타 Symmetric-key cryptosystem에 이 방법을 적용시켜 활용할 수 있을 것으로 예상된다.

타 cryptosystem을 사용하지 않고 S-DES을 선정한 이유는 비교적 작은 크기라는 점이 가장 크게 작용했다. 현재 상용화되어 있는 Quantum computer의 경우 사용 가능한 Qubit의 수가 굉장히 적고, 일반 컴퓨터에서 활용할 수 있는 Quantum simulator의 경우에는 Qubit의 수가 하나 증가할때마다 실행 시간이 두 배로 증가하여, 어느 쪽을 사용하든 상관없이 Qubit의 수가 적어야 실행이 가능하다는 문제점이 있다. 그렇기 때문에 DES, AES 등 Large-scale cryptosystem이 아닌 Small-scale인 S-DES를 선정하였다.

2.1 개별 연구 내용

2.1.1 조민규

Quantum S-DES Oracle에 대한 Theoretical Circuit Diagram을 만들었고, 이에 대한 Q# implementation이 끝난 후 해당 circuit[1]에 대한 Gate analysis를 진행했다.

2.1.2 이상헌

Quantum S-DES Oracle과 그를 사용하여 key를 찾는 Grover's Algorithm을 Microsoft Q#을 사용하여 구현했다.

3 연구 결과

S-DES에서

[1] Theoretical Circuit에서 Q#에서 제공하는 feature으로 인해 몇몇 Gate가 삭제되거나 변형되었다.

4 향후 연구 계획

해당 implementation에 대해서 가장 문제가 되었던 부분은 임의의 Plaintext P, Ciphertext C쌍에 대해 $\{K|C = SDES(P, K)\}$ 의 크기, 즉 Key count가 다르다는 것에 있었다. Grover's Algorithm은 solution set의 크기에 따라 iteration 수를 다르게 해야하는데, 이 수가 균일하지 않다는 것은 Key count를 미리 알아야만 이 Attack을 수행할 수 있다는 것을 의미한다.