DES에 대한 양자회로 최적화 구현

Implementation of optimized quantum circuit for DES

송경주 * 엄시우 * 김상원 ** 서화정 *†
* 한성대학교 대학원 정보컴퓨터공학과
** 한성대학교 대학원 암호보안학과
*† 한성대학교 대학원 IT융합공학부

요 약

- DES 암호를 타겟으로 큐비트 및 depth에 최적화된 양자회로를 제안하고 요구되는 양자자원을 추정
- 큐비트 최적화 DES 양자회로에서 큐비트가 5,832개 (약 87.72%), Depth 최적화 DES 양자회로에서 Depth가 약 67.43% 감소한 결과를 보임

서 론

- 양자컴퓨터의 등장은 현재 사용하는 대칭키 암호 및 공개키 암호의 안전성에 위협이 되고 있음
- 사용하는 암호를 양자회로로 구현하고 양자자원을 추정함으로서 대상 암호가 양자컴퓨터 공격으로부터 위험할 시기를 예측하고 이에 대응가능
- 가용 큐비트가 증가하더라도 양자회 로의 Depth가 크면 오류 발생률이 커져 유효한 결과를 도출하기 어려우므로 큐비트 수 최적 화 및 Depth 최적화 모두 중요하게 연구되어야 할 분야
- DES 양자 회로에 대한 효율적인 양자회로를 제시하고 동작에 필요한 양자자원을 추정
- 큐비트 및 양자회로 Depth에 최적화된 양자회로를 각각 제시: 유사한 핵심 연산을 갖지만 DES 함수 $f(R_{i-1}, K)$에서 구조적인 차이를 보임

큐비트 최적화 양자회로

- 각 S-box의 연산들을 역연산에 포함하여 사용한 ancilla 큐비트를 다음 라운드에서 다시 재사용할 수 있도록 inverse point 설정 **(inverse end point를 S-Box 이후로 설정)**
- 큐비트 수 6,720 (a_1~ a_8 (448)×round (15))개 줄어듦
- S-box 역연산에 요구되는 depth가 증가함

Algorithm 1. 큐비트 최적화 양자회로의 DES 함수 $f(R_{i-1},K_i)$ 동작

Input : x, y, k, a_1 to a_8
Output : Updated y

※ inverse start point
1 : $x \leftarrow$ **P-box**(x) # Expansion P-Box
2 : $x \leftarrow x \oplus k$ # Round key XOR

S-boxes

⋮

10 : $a_8 \leftarrow$ **S-Box8**($x[42:48]$, a_8)
※ inverse end point

11 : $[a_1 : a_8] \leftarrow$ **P-box**($[a_1 : a_8]$) # Straight P-Box

11 : **for** i **in range**(length(y)):
12 : $y \leftarrow [a_1 : a_8] \oplus y$
Start inverse (start to end)

return Updated y

Depth 최적화 양자회로

- S-Box 연산들을 역연산에 포함하지 않아 사용한 ancilla 큐비트를 재사용 불가능 **(inverse end point를 S-Box 이전으로 설정)**
- 매 라운드마다 S-box의 연산에 필요한 ancilla (a_1 to a_8)를 할당하여 사용해야 함
- 큐비트 수 6,720 (a_0~ a_8 (448)×round (15))개 증가됨
- S-Box 역 연산에 필요한 양자자원 및 depth를 포함하지 않아 DES 양자회로 depth가 줄어듦

Algorithm 2. Depth 최적화 양자회로의 DES 함수 $f(R_{i-1},K_i)$ 동작

Input : x, y, k, a_1 to a_8
Output : Updated y

※ inverse start point
1 : $x \leftarrow$ **P-box**(x) # Expansion P-box
2 : $x \leftarrow x \oplus k$ # Round key XOR
※ inverse end point

S-boxes

⋮

10 : $a_8 \leftarrow$ **S-Box8**($x[42:48]$, a_8)

11 : $[a_1 : a_8] \leftarrow$ **P-box**($[a_1 : a_8]$) # Straight P-box

11 : **for** i **in range**(length(y)):
12 : $y \leftarrow [a_1 : a_8] \oplus y$
Start inverse (start to end)

return Updated y

결 론

- 큐비트 최적화 양자회로: 약간의 양자 게이트 trade-off를 통해 사용 큐비트를 5,832개 (약 87.72%) 줄임 (Depth도 약 32.54% 감소)
- Depth 최적화 양자회로: 사용된 큐비트가 888개(약 13.36%) 늘었지만 Depth가 약 67.43% 감소함

Algorithm		Quantum resources				
		Qubit	X	CNOT	Toffoli	Depth
DES	[8]	6,648	7,552	8,032	3,536	3,205
	Our (Qubit Opt.)	816	11,232	20,160	6,848	2,162
	Our (Depth Opt.)	7,536	7,184	12,992	3,424	1,044