양자 회로 물리적 자원 추정: Error Correction

장경배

https://youtu.be/viEG5eaLOR4

Runtime Estimation

- 2017년 SHA-2/3 (Asiacrypt'17) 에서 사용된 Runtime 추정 방법을 전반적으로 따름
  - Reed-Muller 15-to-1 magic state distillation 방법을 사용 [*].

Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3

Matthew Amy[1,4], Olivia Di Matteo[2,4], Vlad Gheorghiu[3,4], Michele Mosca[3,4,5,6], Alex Parent[2,4], and John Schanck[3,4]

[1] David R. Cheriton School of Computer Science, University of Waterloo, Canada
[2] Department of Physics & Astronomy, University of Waterloo, Canada
[3] Department of Combinatorics & Optimization, University of Waterloo, Canada
[4] Institute for Quantum Computing, University of Waterloo, Canada
[5] Perimeter Institute for Theoretical Physics, Canada
[6] Canadian Institute for Advanced Research, Canada

		SHA-256	SHA3-256
Grover	T-count	1.27×10^{44}	2.71×10^{44}
	T-depth	3.76×10^{43}	2.31×10^{41}
	Logical qubits	2402	3200
	Surface code distance	43	44
	Physical qubits	1.39×10^{7}	1.94×10^{7}
Distilleries	Logical qubits per distillery	3600	3600
	Number of distilleries	1	294
	Surface code distances	$\{33, 13, 7\}$	$\{33, 13, 7\}$
	Physical qubits	5.54×10^{5}	1.63×10^{8}
Total	Logical qubits	$2^{12.6}$	2^{20}
	Surface code cycles	$2^{153.8}$	$2^{146.5}$
	Total cost	$2^{166.4}$	$2^{166.5}$

Table 3. Fault-tolerant resource counts for Grover search of SHA-256 and SHA3-256.

[*] Bravyi, S., Kitaev, A.: Universal quantum computation with ideal Clifford gates and noisy ancillas. Phys. Rev. A 71, 022316 (Feb 2005),

Runtime Estimation: Assumptions

- 필요 가정들 (Surface code & Distillation)
  - Magic state injection error rate p_{in}: $\mathbf{10^{-3}}$
  - Per-gate error rate p_g : $\mathbf{10^{-4}}$ $(p_{in}/10)$
  - Output error rate $p_{out} = 1/\boldsymbol{T-count}$

- 이러한 파라미터들을 가지고, 다음 알고리즘은 magic state distillation에 필요한 레이어들의 정보를 계산할 수 있음

Algorithm 4 Estimating the required number of rounds of magic state distillation and the corresponding distances of the concatenated codes

Input: $\varepsilon, p_{in}, p_{out}, p_g (= p_{in}/10)$
$d \leftarrow$ empty list []
$p \leftarrow p_{out}$
$i \leftarrow 0$
repeat
    $i \leftarrow i + 1$
    $p_i \leftarrow p$
    Find minimum d_i such that $192 d_i (100 p_g)^{\frac{d_i+1}{2}} < \frac{\varepsilon p_i}{1+\varepsilon}$
    $p \leftarrow \sqrt[3]{p_i/(35(1+\varepsilon))}$
    d.append(d_i)
until $p > p_{in}$
Output: $d = [d_1, \ldots, d_i]$

Runtime Estimation: Distillation

- ECC with $n = 64$에 대한 양자 공격 자원을 대상으로 해당 알고리즘을 사용
  - Distillation을 위해서는 다음 2개의 레이어가 요구됨 → [12, 6]
    - $d_1 = 12,\ d_2 = 6$

- Total qubits: 27000, Total Cycle: 180, Total time: 6951s (cycle 당 **200ns** 가정)

```
Code distances: [12, 6]

## layer-1 (Magic Distillation) ##
Physical qubits for T:  27000.0
Suface code cycles:  60

## layer-2 (Magic Distillation) ##
Physical qubits for T:  7200.0
Suface code cycles:  120

## Total layer ##
Total cycle:  180
Pipeline:  3.0
Single magic state gen time (s):  3.6e-05
Total magic state gen time (s):  6951.360000000001
```

Layer-1

Layer-2

Total cycles

(Total T gates X Total cycles X 200ns / pipeline)

Assumptions

T-count: 579280000
p_{in}: 10^{-3}
p_g : 10^{-4}
p_{out}: 1 / T-count

Distillation layers

$d_1 = 12$
$d_2 = 6$

Total physical qubits & Total Cycles

27000 qubits
180 cycles (for 1 magic state)

Runtime Estimation: Distillation Pipeline

Warm-up

다시 정리하자면:

- **bottom**: 60 cycles마다 1개 magic state 준비
- **middle**: 각 magic state를 120 cycles 동안 처리
- 전체 자원은 bottom layer 1개만 실행할 수 있을 만큼

→ 파이프라인은 다음처럼 흘러갑니다:

시간 구간	실행 중인 magic state	완성되는 시점
0–60	bottom(#1)	
60–120	bottom(#2), middle(#1)	
120–180	bottom(#3), middle(#2)	#1 done
180–240	bottom(#4), middle(#3)	#2 done
240–300	bottom(#5), middle(#4)	#3 done
300–360	bottom(#6), middle(#5)	#4 done

Runtime Estimation: Distillation

- 앞선 magic state distillation 과정은 병렬화 될 수 있음
  - Based on the **T-count / T-depth ratio** (T_c_d) → 177 (=579280000 / 3291340)

- Magic state distillation에 대하여 177개의 Factory를 가동시킬 수 있음 (병렬로)
  - 앞서 pipeline = 3이였으니, 59 (=177/3)의 Factory를 가동
  - 큐빗 수는 59배 증가시키지만 Runtime 59배 감소

```
## Final stage ##
T_c_d:  177
Updated pyhsical qubits for T:  1593000.0
Updated total magic state gen time (s):  117.81966101694917
```

Runtime Estimation: Clifford Group

- Clifford 그룹에 대한 물리적 큐빗 또한 고려해야함
  - **Clifford 게이트 수** 그리고 논리적 큐빗 수에 따라 결정
    - 2069721680 Clifford gates
    - 3698 qubits

$\#p_{in} = 10^{-3}$

$$\left(\frac{p_{in}}{0.0125}\right)^{\frac{d+1}{2}} < \frac{1}{2069721680} \quad ,$$

< equation, 최소 d를 만족 >

```
## Clifford part ##
Threshold:  4.831567498486077e-10
d:  16
Physical qubits for Clifford:  2959200.0
```

- Clifford 그룹에 대한 Surface code cycle은 최종 Runtime에 영향을 주지 않음 (일반적으로)
  - 비용이 사소하며 Magic state distillation과 병렬로 동작 가능함

Result For Quantum Attack on ECC ($n = 64$)

- **Logical resources:**

```
T count:  579280000
Clifford count:  2069721680
Qubit count:  3699
T depth:  3291340
```

- **Physical Assumptions (1)**
  - Magic state injection error rate p_{in}: 10^{-3}
  - Per-gate error rate p_g : 10^{-4} $(p_{in}/10)$
  - Output error rate $p_{out} = \frac{1}{T-count}$
  - Two layers [12, 6]
  - Speed for a surface code cycle: 200ns

- **Total result (qubits, times, cycles) (1)**

```
## Result ##
Total physical qubits:  4552200.0
Total seconds:  117.81966101694917
Total surface code cycles:  592441200
```

- **Physical Assumptions (2)**
  - Magic state injection error rate p_{in}: 10^{-4}
  - Per-gate error rate p_g : $\mathbf{10^{-5}}$ $\mathbf{(p_{in}/10)}$
  - Output error rate $p_{out} = \frac{1}{T-count}$
  - **One layer [8]**
  - Speed for a surface code cycle: 200ns

- **Total result (qubits, times, cycles) (2)**

```
## Result ##
Total physical qubits:  1270800.0
Total seconds:  52.364293785310736
Total surface code cycles:  263307200
```

Quantum Attacks on SHA-2, SHA-3 and AES

- SHA-256

```
## Result ##
Total physical qubits:  44064450.0
Total seconds:  2.845506949764195e+38
Total surface code cycles:  142394607397453565264122949111075177496576000
```

(9.02×10^{30} years)

- SHA3-256

```
## Result ##
Total physical qubits:  722075512.5
Total seconds:  5.1305656898742 64e+36
Total surface code cycles:  256566860175592009484906214614549869363200 00
```

(1.63×10^{29} years)

- AES-256

```
## Result ##
Total physical qubits:  98329612.5
Total seconds:  1.1467880786104924e+37
Total surface code cycles:  57470976679332610124618992073659170737356800
```

(3.63×10^{29} years)

Quantum Attack on Binary ECC

- Binary ECC ($n = 571$)

Table 1: Comparison of classical security between ECC and RSA.

Classical security (bits)	RSA✳	ECC✸
80	1024	160 – 223
112	2048	224 – 255
128	3072	256 – 383
192	7680	384 – 511
256	15360	≥ 512

✳: Product of two primes (in number of bits).

✸: Order of generator point (in number of bits).

- Runtime Estimation

```
## Result ##
Total physical qubits:  1049891784.375
Total seconds:  11.348013945176435
Total surface code cycles:  56742400
```

13026 Factories

감사합니다