Post-quantum 대칭키 암호 보안 강도 추정 (NIST)

https://youtu.be/1b_2b3BvvIc

장경배

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

NIST's Security Strength

- NIST는 **Post-quantum에 대한 보안 강도 추정**에 다음 2가지를 고려
  - 새로운 양자 알고리즘의 등장
  - Grover key search 공격 비용 추정 (양자 게이트, 회로 Depth)

NIST's Security Strength

- 기존 bit 기준이 아닌 다음 기준에 따라 보안 강도를 확인

  - Grover key search 공격 비용 추정 (양자 게이트, 회로 Depth)

1) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES128)
2) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)
3) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES192)
4) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)
5) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g. AES 256)

NIST's Security Strength

Applying Grover's algorithm to AES: quantum resource estimates

Markus Grassl[1], Brandon Langenberg[2], Martin Roetteler[3], and Rainer Steinwandt[2]

[1] Universität Erlangen-Nürnberg & Max Planck Institute for the Science of Light, Günther-Scharowsky-Straße 1, Bau 24, 91058 Erlangen, Germany, Markus.Grassl@fau.de
[2] Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, U.S.A., {blangenb,rsteinwa}@fau.edu
[3] Microsoft Research, One Microsoft Way, Redmond, WA 98052, U.S.A., martinro@microsoft.com

Abstract. We present quantum circuits to implement an exhaustive key search for the Advanced Encryption Standard (AES) and analyze the quantum resources required to carry out such an attack. We consider the overall circuit size, the number of qubits, and the circuit depth as measures for the cost of the presented quantum algorithms. Throughout, we focus on Clifford+T gates as the underlying fault-tolerant logical quantum gate set. In particular, for all three variants of AES (key size 128, 192, and 256 bit) that are standardized in FIPS-PUB 197, we establish precise bounds for the number of qubits and the number of elementary logical quantum gates that are needed to implement Grover's quantum algorithm to extract the key from a small number of AES plaintext-ciphertext pairs.

Keywords: quantum cryptanalysis, quantum circuits, Grover's algorithm, Advanced Encryption Standard

NIST's Security Strength

- Grover key search 공격 비용

AES 128	2^{170}/MAXDEPTH quantum gates or 2^{143} classical gates
SHA3-256	2^{146} classical gates
AES 192	2^{233}/MAXDEPTH quantum gates or 2^{207} classical gates
SHA3-384	2^{210} classical gates
AES 256	2^{298}/MAXDEPTH quantum gates or 2^{272} classical gates
SHA3-512	2^{274} classical gates

- □ 는 Total gates X Depth

	#gates		depth		#qubits
k	T	Clifford	T	overall	
128	$1.19 \cdot 2^{86}$	$1.55 \cdot 2^{86}$	$1.06 \cdot 2^{80}$	$1.16 \cdot 2^{81}$	2,953
192	$1.81 \cdot 2^{118}$	$1.17 \cdot 2^{119}$	$1.21 \cdot 2^{112}$	$1.33 \cdot 2^{113}$	4,449
256	$1.41 \cdot 2^{151}$	$1.83 \cdot 2^{151}$	$1.44 \cdot 2^{144}$	$1.57 \cdot 2^{145}$	6,681

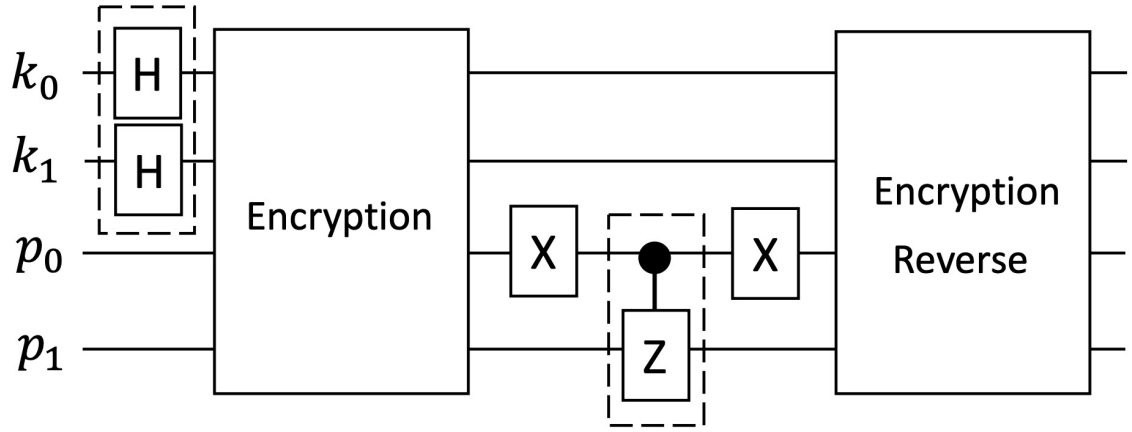
Table 5. Quantum resource estimates for Grover's algorithm to attack AES-k, where $k \in \{128, 192, 256\}$.

Resource estimation

- **NCT → Clifford + T**

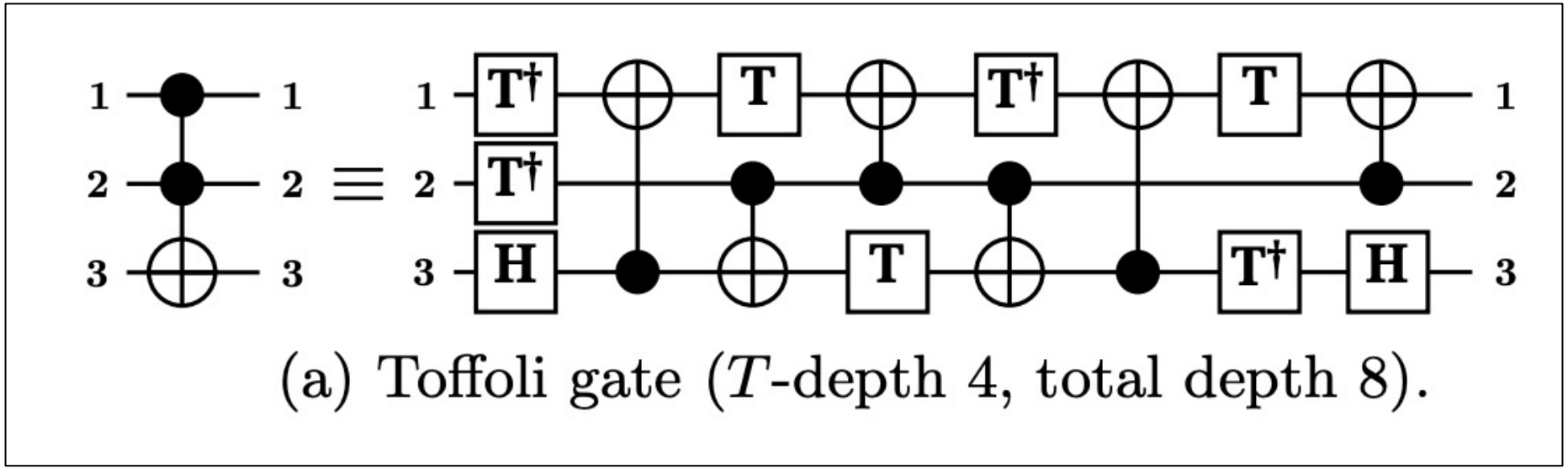
Cipher	Qubits	Toffoli gates	CNOT gates	X gates	Depth
KNOT-AEAD (128, 256, 64)	352	28,074	21,600	6,875	899
KNOT-AEAD (128, 384, 192)	480	51,464	39,264	12,683	1,091
KNOT-AEAD (192, 384, 96)	480	60,506	46,176	14,899	1,283
KNOT-AEAD (256, 512, 128)	608	105,164	79,968	25,964	1,667

- 2배 + l-bit 암호문 비교에 대한 자원 ($32 \cdot l - 84$ T gates)



Resource estimation

- **Toffoli gate = 7 T + 8 Clifford**



Resource estimation

- **NCT → Clifford + T**
  - 393036 (28074 · 2) + 4012 (32 · 128 – 84)

- Toffoli gate = 7 T + 8 Clifford
- $32 \cdot l$ – 84 T gates

Cipher	Qubits	Toffoli gates	CNOT gates	X gates	Depth
KNOT-AEAD (128, 256, 64)	352	28,074	21,600	6,875	899
KNOT-AEAD (128, 384, 192)	480	51,464	39,264	12,683	1,091
KNOT-AEAD (192, 384, 96)	480	60,506	46,176	14,899	1,283
KNOT-AEAD (256, 512, 128)	608	105,164	79,968	25,964	1,667

Cipher	Qubits	Clifford gates	T gates	T depth	Depth
KNOT-AEAD (128, 256, 64)	353	506,134	398,072	224,592	1,799
KNOT-AEAD (128, 384, 192)	481	927,318	725,532	411,712	2,183
KNOT-AEAD (192, 384, 96)	481	1,090,246	854,168	484,048	2,567
KNOT-AEAD (256, 512, 128)	609	1,894,488	1,481,428	841,312	3,335

Resource estimation

- 최종 Grover key search 자원
  - $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ 번 반복, 128-bit key 의 경우 $\lfloor \frac{\pi}{4} \cdot 2^{64} \rfloor$
    - Clifford gates → $1.516 \cdot 2^{82}$

Table 5: Quantum resources required for Grover oracle

Cipher	Qubits	Clifford gates	T gates	T depth	Depth
KNOT-AEAD (128, 256, 64)	353	506,134	398,072	224,592	1,799
KNOT-AEAD (128, 384, 192)	481	927,318	725,532	411,712	2,183
KNOT-AEAD (192, 384, 96)	481	1,090,246	854,168	484,048	2,567
KNOT-AEAD (256, 512, 128)	609	1,894,488	1,481,428	841,312	3,335

Table 6: Quantum resources required for Grover key search

Cipher	Qubits	Clifford gates	T gates	T depth	Depth	Total gates
KNOT-AEAD (128, 256, 64)	353	$1.516 \cdot 2^{82}$	$1.193 \cdot 2^{82}$	$1.346 \cdot 2^{81}$	$1.378 \cdot 2^{74}$	$1.354 \cdot 2^{83}$
KNOT-AEAD (128, 384, 192)	481	$1.389 \cdot 2^{83}$	$1.087 \cdot 2^{83}$	$1.234 \cdot 2^{82}$	$1.673 \cdot 2^{74}$	$1.238 \cdot 2^{84}$
KNOT-AEAD (192, 384, 96)	481	$1.633 \cdot 2^{115}$	$1.279 \cdot 2^{115}$	$1.450 \cdot 2^{114}$	$1.968 \cdot 2^{106}$	$1.456 \cdot 2^{116}$
KNOT-AEAD (256, 512, 128)	609	$1.419 \cdot 2^{148}$	$1.109 \cdot 2^{148}$	$1.260 \cdot 2^{147}$	$1.278 \cdot 2^{139}$	$1.264 \cdot 2^{149}$

NIST's Security Strength

- NIST post-quantum 보안 강도와 비교 (Total gates X Depth)

Cipher	Total gates	Depth	D	NIST security
KNOT-AEAD $(128, 256, 64)$	$1.354 \cdot 2^{83}$	$1.378 \cdot 2^{74}$	$1.866 \cdot 2^{157}$	2^{170} (AES-128)
KNOT-AEAD $(128, 384, 192)$	$1.238 \cdot 2^{84}$	$1.673 \cdot 2^{74}$	$1.036 \cdot 2^{159}$	
KNOT-AEAD $(192, 384, 96)$	$1.456 \cdot 2^{116}$	$1.968 \cdot 2^{106}$	$1.433 \cdot 2^{223}$	2^{233} (AES-192)
KNOT-AEAD $(256, 512, 128)$	$1.264 \cdot 2^{149}$	$1.278 \cdot 2^{139}$	$1.615 \cdot 2^{288}$	2^{298} (AES-256)

(nonce는 known)

Depth?

- NCT 레벨에서의 depth? , 아니라면?

	#gates			depth		#qubits	
	NOT	CNOT	Toffoli	T	overall	storage	ancillae
128	176	21,448	20,480	5,760	12,636	320	96
192	136	17,568	16,384	4,608	10,107	256	96
256	215	27,492	26,624	7,488	16,408	416	96

Table 1. Quantum resource estimates for the key expansion phase of AES-k, where $k \in \{128, 192, 256\}$.

	#gates		depth		#qubits
	T	Clifford	T	overall	
Initial	0	0	0	0	128
Key Gen	143,360	185,464	5,760	12,626	320
10 Rounds	917,504	1,194,956	44,928	98,173	536
Total	1,060,864	1,380,420	50,688	110,799	984

Table 2. Quantum resource estimates for the implementation of AES-128.

Depth?

Table 1: Cost of implementing the ciphers

ciphers	# NOT	# CNOT	# Toffoli	depth	# qubits
Grain-128-AEAD($k = 128$)	127	13624	18116	13068	531
TinyJAMBU ($k = 128$)	209	29824	14848	22274	385
TinyJAMBU ($k = 192$)	209	32384	16128	24194	449
TinyJAMBU ($k = 256$)	209	34944	17408	26114	513
LIZARD ($k = 120/80$)	1611	23014	36284	33354	392
Grain-v1 ($k = 80$)	580	10830	15500	13031	346

Table 2: Cost of Grover oracle

cipher	# Clifford gates	# T gates	T-depth	full depth	# qubits
Grain-128-AEAD	317358	257956	144928	151902	532
TinyJAMBU ($k = 128$)	595524	423852	118784	252418	771
TinyJAMBU ($k = 192$)	646852	463788	129024	274178	899
TinyJAMBU ($k = 256$)	698180	503724	139264	295938	1027
LIZARD ($k = 120/80$)	629794	512052	290272	421986	393
Grain-v1 ($k = 80$)	270820	219796	124000	149772	347

operation	MC	r	#CNOT	#1qCliff	$\#T$	$\#M$	T-depth	full depth	width
AES-128	IP	1	292313	84428	54908	13727	121	2816	1665
AES-192	IP	1	329697	94316	61436	15359	120	2978	1985
AES-256	IP	1	404139	116286	75580	18895	126	3353	2305
AES-128	IP	2	585051	169184	109820	27455	121	2815	3329
AES-192	IP	2	659727	188520	122876	30719	120	2981	3969
AES-256	IP	2	808071	231124	151164	37791	126	3356	4609
AES-256	IP	3	1212905	347766	226748	56687	126	3347	6913
AES-128	M	1	294863	84488	54908	13727	121	2086	2817
AES-192	M	1	332665	94092	61436	15359	120	1879	3393
AES-256	M	1	407667	116062	75580	18895	126	1951	3969
AES-128	M	2	589643	168288	109820	27455	121	2096	5633
AES-192	M	2	665899	188544	122876	30719	120	1890	6785
AES-256	M	2	815645	231712	151164	37791	126	1952	7937
AES-256	M	3	1223087	346290	226748	56687	126	1956	11905

Q & A