ARIA 양자 회로 구현

발표자: 양유진

링크: https://youtu.be/mUYxUZ6EQpk

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

S-box 양자 구현 (1/3)

양자컴퓨팅 환경에서 측정 전까지 qubit 상태 알 수 없음 → Look-up table 방식의 S-box 생성 방법 사용 X

⇒ 양자 게이트 활용한 S-box 생성식 기반의 S-box 양자 회로 구현 필요함

S-box generation equation

(input) 8-bit blocks

8 x 8 Matrix

8 x 1 Matrix

$$S_1(x) = A \cdot x^{-1} \oplus [1,1,0,0,0,1,1,0]^T$$

$$S_2(x) = B \cdot x^{247} \oplus [0,1,0,0,0,1,1,1]^T$$

$$x^{-1} = x^{254} \bmod m(x)$$

$$x^{247} = (x^{-1})^8 \bmod m(x)$$

irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

process

1. Get $\boldsymbol{x^{-1}}$
2. Matrix-vector Multiplication
   (8 x 8 Matrix) $\cdot\, x^n$
3. constant(vector) Multiplication

S-box 양자 구현 (2/3)

Get x^{-1}

(1) Itoh Tsuji Inversion Algorithm

$$x^{-1} = x^{254} = ((x \cdot x^2) \cdot (x \cdot x^2)^4 \cdot (x \cdot x^2)^{16} \cdot x^{64})^2$$

(2) 제곱연산 – XZLBZ[3]

- XZLBZ[3] 는 이진 행렬의 인수분해를 기반으로 하는 휴리스틱 검색 알고리즘을 제안함
- in-place 구조로 구현
  → CNOT 게이트로만 구성
- 10 CNOT gates, circuit depth of 7

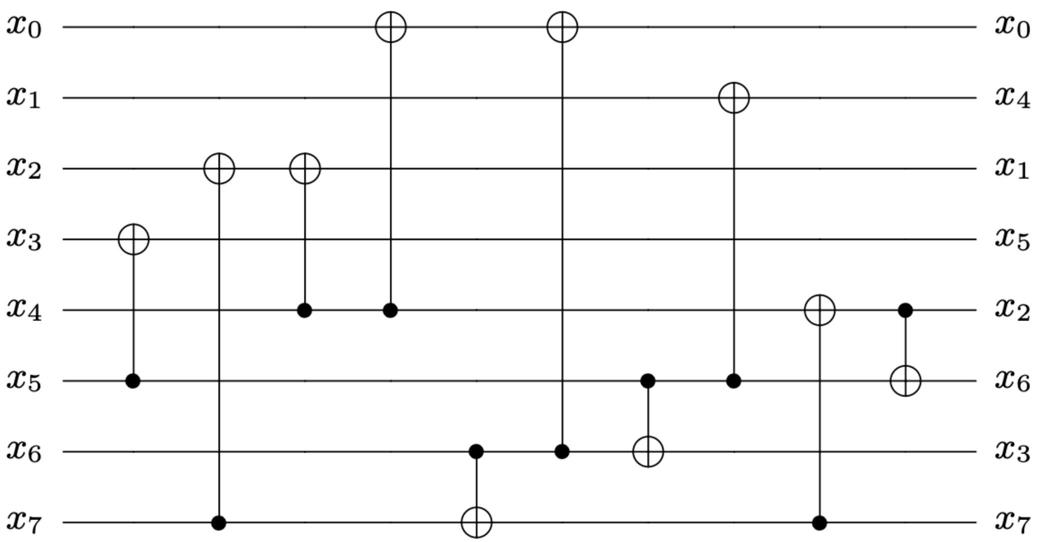

Fig. 5: Quantum circuit implementation for Squaring in $\mathbb{F}_{2^8}/(x^8 + x^4 + x^3 + x + 1)$

[3] Xiang, Z., Zeng, X., Lin, D., Bao, Z., Zhang, S.: Optimizing implementations of linear layers. IACR Transactions on Symmetric Cryptology (2020) 120–145

S-box 양자 구현 (3/3)

Get x^{-1}

(3) 곱셈연산 – Toffoli depth에 최적화된 Karatsuba 곱셈 사용

quantum-quantum 곱 → Karatsuba 곱셈 사용

Table 1: Quantum resources required for multiplication.

	Source	#Clifford	#T	Toffoli depth	Full depth
schoolbook	CMMP [2]	435	448	28	195
Karatsuba	J++ [13]	390	189	1	28

※: The multiplication size n is 8.

Matrix-vector Multiplication & constant(vector) Multiplication

classical-quantum 곱 → XZLBZ 사용

Cheung, D., Maslov, D., Mathew, J., Pradhan, D.K.: On the design and opti mization of a quantum polynomial-time attack on elliptic curve cryptography. In: Kawano, Y., Mosca, M. (eds.) TQC 2008. LNCS, vol. 5106, pp. 96-104. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89304-2-9
Jang, K., Kim, W., Lim, S., Kang, Y., Yang, Y., Seo, H.: Optimized implementation of quantum binary field multiplication with toffoli depth one. In: International Conference on Information Security Applications, Springer (2022) 251–264

Diffusion layer 양자 구현

- Diffusion 함수 A 는 16 x 16 이진 행렬곱으로 표현 가능

$$A : GF(2^8)^{16} \rightarrow GF(2^8)^{16}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} = \begin{pmatrix}
0&0&0&1&1&0&1&0&1&1&0&0&0&1&1&\boxed{0} \\
0&0&1&0&0&1&0&1&1&1&0&0&1&0&0&1 \\
0&1&0&0&1&0&1&0&0&0&1&1&1&0&0&1 \\
1&0&0&0&0&1&0&1&0&0&1&1&0&1&1&0 \\
1&0&1&0&0&1&0&0&1&0&0&1&0&0&1&1 \\
0&1&0&1&1&0&0&0&0&1&1&0&0&0&1&1 \\
1&0&1&0&0&0&0&1&0&1&1&0&1&1&0&0 \\
0&1&0&1&0&0&1&0&1&0&0&1&1&1&0&0 \\
1&1&0&0&1&0&0&1&0&0&1&0&0&1&0&1 \\
1&1&0&0&0&1&1&0&0&0&0&1&1&0&1&0 \\
0&0&1&1&0&1&1&0&1&0&0&0&0&1&0&1 \\
0&0&1&1&1&0&0&1&0&1&0&0&1&0&1&0 \\
0&1&1&0&0&0&1&1&0&1&0&1&1&0&0&0 \\
1&0&0&1&0&0&1&1&1&0&1&0&0&1&0&0 \\
1&0&0&1&1&1&0&0&0&1&0&1&0&0&1&0 \\
0&1&1&0&1&1&0&0&1&0&1&0&0&0&0&1
\end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix}$$

1byte (8-bit)

- 0 : 8 x 8 zero matrix
- 1 : 8 x 8 identity matrix

- XZLBZ 를 사용하여 CNOT gates 는 51.04%, depth는 45.16% 감소시킴 (큐비트수는 유지)

Table 2: Quantum resources required for Diffusion layer.

Source	#CNOT	qubit	Depth
PLU factorization	768	128	31
XZLBZ [25]	376	128	17

768 (= 96 × 8) , 376 (= 47 × 8)

Key-Schedule 양자 구현 (1/2)

1) Key Initialization

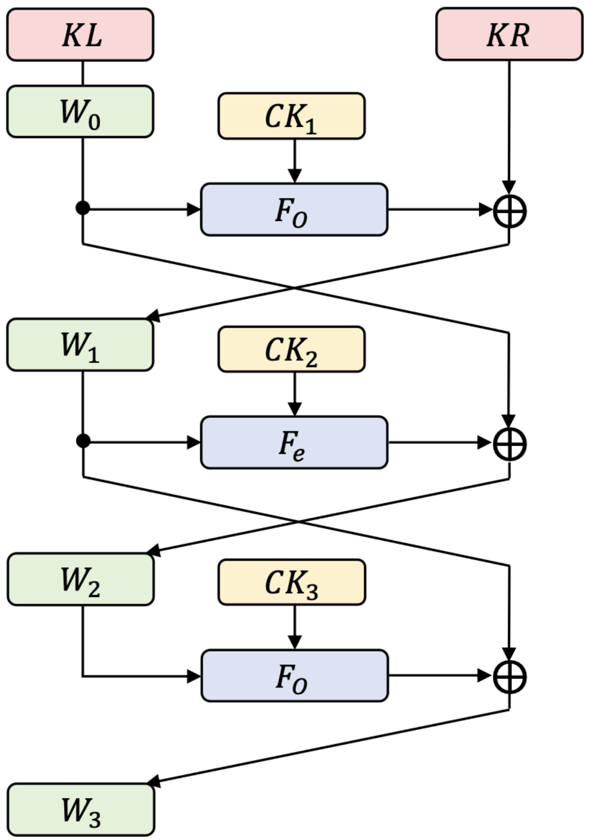

Fig. 3: Key Initialization of ARIA

Algorithm 1: Quantum circuit implementation of key schedule for ARIA.

Input: master key MK, key length l, vector a, b, ancilla qubit anc, round number r
Output: round key ek

K_L ▷ Key Initialization

$W_1 \leftarrow F_o(MK[:128], a, b, anc)$ ▷ $MK[:128]$ is K_L

K_R

Constant_XOR($W_1[l-128:128]$, $MK[l-128:l]$) ▷ $MK[l-128:l]$ is K_R

$W_2 \leftarrow F_e(W_1, a, b, anc)$
$W_2 \leftarrow$ CNOT128($MK[:128], W_2$)

$W_3 \leftarrow F_o(W_2, a, b, anc)$
$W_3 \leftarrow$ CNOT128(W_1, W_3)

- K_L 는 W_0 와 같은 값을 가짐 → W_0를 생성하는 대신, **K_L사용**
⇒ 큐비트 수 감소시킴

- K_R 은 **상수** → **CNOT gates 연산을 X gates 연산으로 바꿀 수 있음**
⇒ 게이트 수와 게이트 비용을 줄일 수 있음

Key-Schedule 양자 구현 (2/2)

2) Key Generation

Algorithm 1: Quantum circuit implementation of key schedule for ARIA.

Input: master key MK, key length l, vector a, b, ancilla qubit anc, round number r
Output: round key ek

$\lll \rightarrow \ggg$

```
num = [19, 31, 67, 97, 109]
for i ← 0 to r do
    if i = 0 (mod 4) then          K_L = W_0
        Constant_XOR(ek, MK[: 128])
    else
        ek ← CNOT128(W_(i%4), ek)
    ek ← CNOT128(W_((i+1)%4) ⋙ num[i%4], ek)
return ek
```

$$
\begin{array}{ll}
ek_1 = (W_0) \oplus (W_1 \ggg 19), & ek_2 = (W_1) \oplus (W_2 \ggg 19) \\
ek_3 = (W_2) \oplus (W_3 \ggg 19), & ek_4 = (W_0 \ggg 19) \oplus (W_3) \\
ek_5 = (W_0) \oplus (W_1 \ggg 31), & ek_6 = (W_1) \oplus (W_2 \ggg 31) \\
ek_7 = (W_2) \oplus (W_3 \ggg 31), & ek_8 = (W_0 \ggg 31) \oplus (W_3) \\
ek_9 = (W_0) \oplus (W_1 \lll 61), & ek_{10} = (W_1) \oplus (W_2 \lll 61) \\
ek_{11} = (W_2) \oplus (W_3 \lll 61), & ek_{12} = (W_0 \lll 61) \oplus (W_3) \\
ek_{13} = (W_0) \oplus (W_1 \lll 31), & ek_{14} = (W_1) \oplus (W_2 \lll 31) \\
ek_{15} = (W_2) \oplus (W_3 \lll 31), & ek_{16} = (W_0 \lll 31) \oplus (W_3) \\
ek_{17} = (W_0) \oplus (W_1 \lll 19) &
\end{array} \tag{3}
$$

- $\boldsymbol{ek}$ 에 W를 할당시킬 때, $\boldsymbol{W_0}$ 는 K_L(상수)과 같기 때문에 CNOT gates 연산을 X gates 연산으로 바꿀 수 있음

⇒ 게이트 수와 게이트 비용을 줄일 수 있음

평가

($Clifford\ +\ T$ Level)

Table 4: Required decomposed quantum resources for ARIA quantum circuit implementation

Cipher	Source	#Cliford	#T	T-depth	#Qubit (M)	Full depth	Toffoli depth (TD)	TD-M cost ($TD \times M$)
ARIA-128	CS [2]◇	1,494,287	1,103,872	17,248	1,560	37,882	4,312	6,726,720
	This work	481,160	181,440	240	29,216	4,241	60	1,752,960
ARIA-192	CS [2]◇	1,742,059	1,283,576	20,376	1,560	44,774	5,096	7,949,760
	This work	551,776	205,632	272	32,928	5,083	68	2,239,104
ARIA-256	CS [2]◇	2,105,187	1,555,456	24,304	1,688	51,666	6,076	10,256,288
	This work	616,920	229,824	304	36,640	5,693	76	2,784,640

◇ Extrapolated result

Full depth: 88.8% 감소 · Toffoli depth: 98.7% 감소 · TD-M cost: 72.9% 감소

- 이전 연구[1]에서 분해된 양자 자원은 명시적으로 제공되지 않았음
  → 표4에서 제시한 양자 자원은 논문에 제공된 정보를 기반으로 추정한 값임
- qubit와 depth 간의 균형을 고려하면서 depth 관련 측정항목(full depth, Toffoli depth, TD-M cost)을 크게 감소시켰음

[1] Chauhan, A.K., Sanadhya, S.K.: Quantum resource estimates of grover's key search on aria. In: Security, Privacy, and Applied Cryptography Engineering: 10th International Conference, SPACE 2020, Kolkata, India, December 17–21, 2020, Proceedings 10. Springer (2020) 238–258

평가

$$[\text{Table 5}] = [\text{Table 4}] \times \left\lceil \frac{\text{key size}}{\text{block size}} \right\rceil \times 2 \times \left\lfloor \frac{\pi}{4}\sqrt{2^k} \right\rfloor$$

Total gates X Full depth = Cost(complexity)

Table 5: Cost of the Grover's key search for ARIA

Cipher	Source	Total gates	Full depth	Cost (complexity)	#Qubit	*TD-M* cost	NIST Level[6,7]
ARIA-128	CS [2]	$1.946 \cdot 2^{85}$	$1.816 \cdot 2^{79}$	$1.767 \cdot 2^{165}$	1,561	$1.26 \cdot 2^{87}$	(Level 1) 2^{157}
	This work	$1.985 \cdot 2^{83}$	$1.626 \cdot 2^{76}$	$1.614 \cdot 2^{160}$	29,217	$1.313 \cdot 2^{84}$	
ARIA-192	CS [2]	$1.133 \cdot 2^{119}$	$1.073 \cdot 2^{113}$	$1.216 \cdot 2^{232}$	3,121	$1.489 \cdot 2^{121}$	(Level 3) $2^{192}, 2^{221}$
	This work	$1.135 \cdot 2^{117}$	$1.949 \cdot 2^{109}$	$1.106 \cdot 2^{227}$	65,857	$1.672 \cdot 2^{119}$	
ARIA-256	CS [2]	$1.371 \cdot 2^{151}$	$1.238 \cdot 2^{145}$	$1.698 \cdot 2^{296}$	3,377	$1.921 \cdot 2^{153}$	(Level 5) $2^{274}, 2^{285}$
	This work	$1.268 \cdot 2^{149}$	$1.092 \cdot 2^{142}$	$1.385 \cdot 2^{291}$	73,281	$1.04 \cdot 2^{152}$	

모두 NIST Level 달성

[6] Jang, K., Baksi, A., Song, G., Kim, H., Seo, H., Chattopadhyay, A.: Quantum analysis of aes. Cryptology ePrint Archive (2022)
[7] Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing grover oracles for quantum key search on aes and lowmc. Cryptology ePrint Archive, Report 2019/1146 (2019)

평가

Table 5: Cost of the Grover's key search for ARIA

Cipher	Source	Total gates	Full depth	Cost (complexity)	#Qubit	TD-M cost
ARIA-128	CS [2]	$1.946 \cdot 2^{85}$	$1.816 \cdot 2^{79}$	$1.767 \cdot 2^{165}$	1,561	$1.26 \cdot 2^{87}$
	This work	$1.985 \cdot 2^{83}$	$1.626 \cdot 2^{76}$	$1.614 \cdot 2^{160}$	29,217	$1.313 \cdot 2^{84}$
ARIA-192	CS [2]	$1.133 \cdot 2^{119}$	$1.073 \cdot 2^{113}$	$1.216 \cdot 2^{232}$	3,121	$1.489 \cdot 2^{121}$
	This work	$1.135 \cdot 2^{117}$	$1.949 \cdot 2^{109}$	$1.106 \cdot 2^{227}$	65,857	$1.672 \cdot 2^{119}$
ARIA-256	CS [2]	$1.371 \cdot 2^{151}$	$1.238 \cdot 2^{145}$	$1.698 \cdot 2^{296}$	3,377	$1.921 \cdot 2^{153}$
	This work	$1.268 \cdot 2^{149}$	$1.092 \cdot 2^{142}$	$1.385 \cdot 2^{291}$	73,281	$1.04 \cdot 2^{152}$

NIST MAXDEPTH[8]

$2^{40}, 2^{64}, 2^{96}$

- 유일하게 ARIA-128만 MAXDEPTH를 만족함 (ARIA-128 < 2^{96})
- MAXDEPTH를 초과한 경우(ARIA-192, 256), cost에 MAXDEPTH 제한을 직접적으로 적용하는 대신 관련 측정항목 ($FD^2 \times M, TD^2 \times M$)의 비용을 최소화하는 데 집중해야 함

[8] NIST.: Call for additional digital signature schemes for the post-quantum cryptography standardization process (2022) https://csrc.nist.gov/csrc/media/ Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022. pdf.

Thank you