AIM 양자 회로 구현

장경배

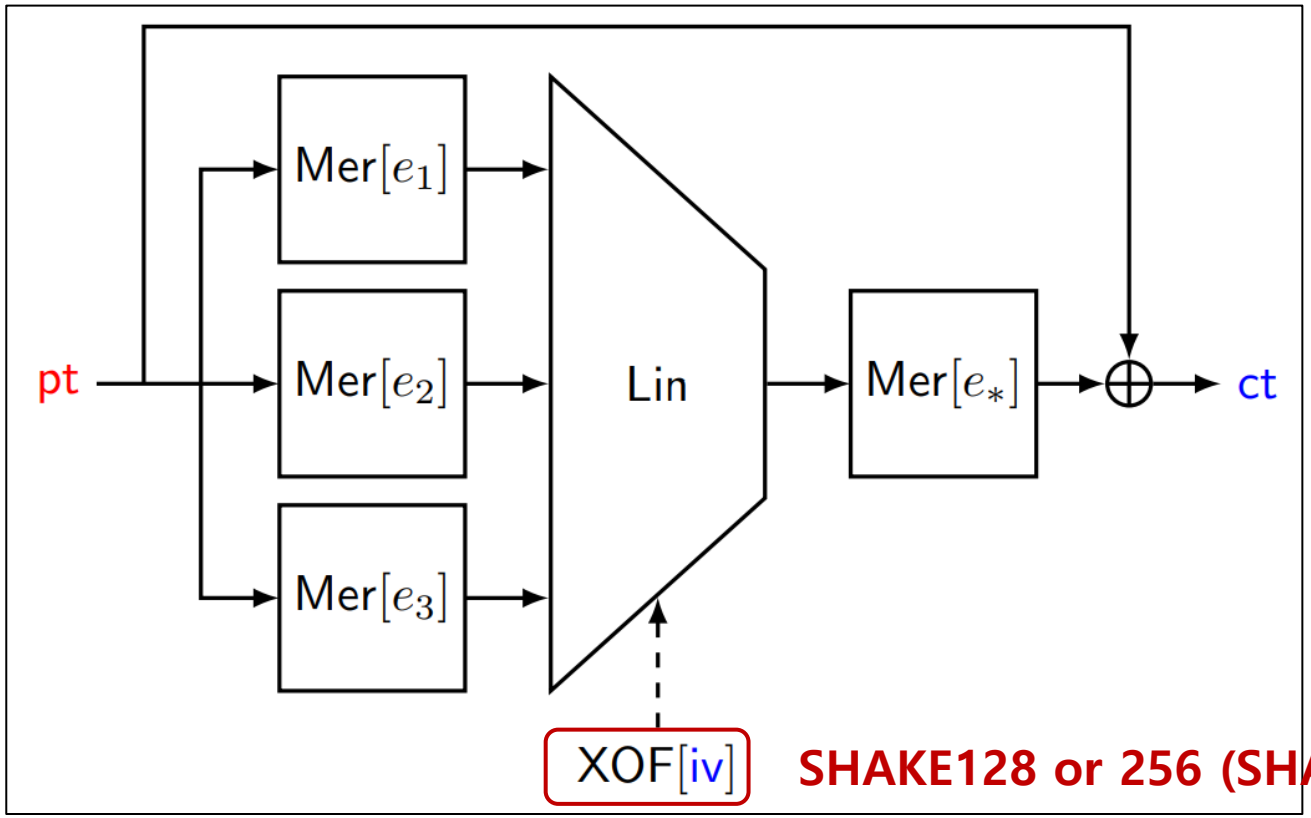
https://youtu.be/-mGRaRhqFMU

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

AIMer & AIM

- AIMer는 대칭키 기반의 전자 서명 알고리즘, KPQC 공모전 후보 알고리즘 중 하나
- **AIM**은 AIMer에서 사용되는 대칭키 프리미티브



SHAKE128 or 256 (SHA3), 그러나 iv가 public

Scheme	λ	n	ℓ	e_1	e_2	e_3	e_*
AIM-I	128	128	2	3	27	-	5
AIM-III	192	192	2	5	29	-	7
AIM-V	256	256	3	3	53	7	5

Table 2: Recommended sets of parameters of AIM.

AIM 양자 회로 구현

- **AIM-I**만 우선적으로 구현

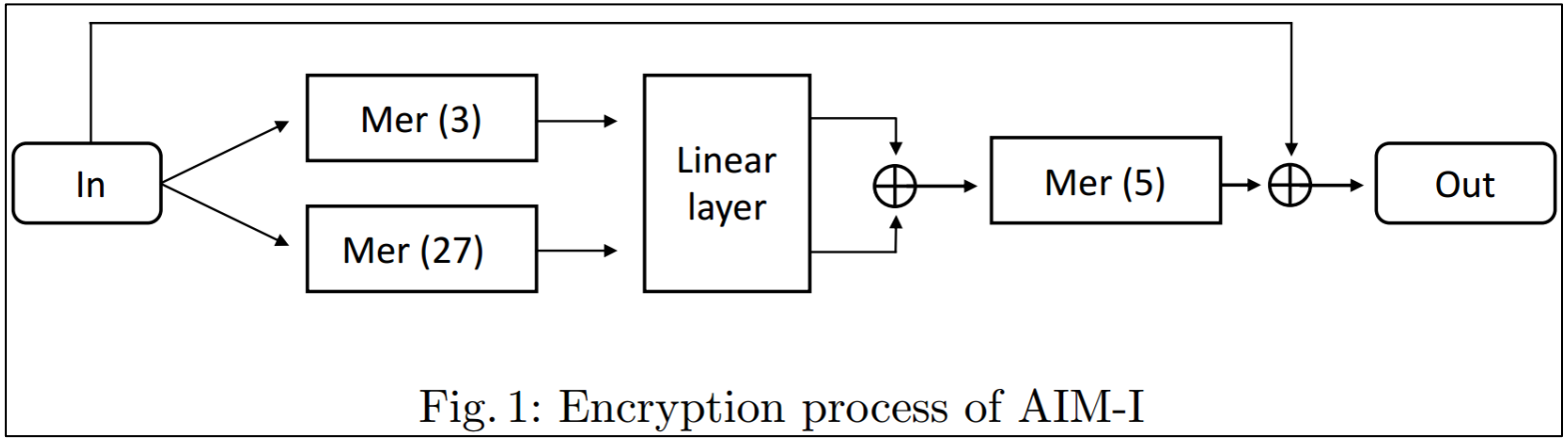


Fig. 1: Encryption process of AIM-I

- **Mer(e)**는 x^{2^e-1}을 계산
  - $\mathbb{F}_{2^{128}}/(x^{128}+x^7+x^2+x+1)$상에서의 곱셈 + 제곱 연산들로 구성
- **LinearLayer**는 (128×128) × (128×1)의 Matrix-Vector 곱셈
  - 사용되는 Matrix의 경우, **IV에 SHAKE-128를 사용한 확장 된 해시 값을 사용**
  - IV는 Public이므로, LinearLayer에서 사용되는 Matrix는 Constant
    → 즉, Quantum-Classical 구현

AIM 양자 회로 구현

- $\mathbb{F}_{2^{128}}/(x^{128}+x^7+x^2+x+1)$의 곱셈은 WISA 곱셈 기법 적용
  - 낮은 T-depth, Full depth로 구현 가능, 하지만 많은 큐비트 사용

Table 1: Quantum resources required for multiplication of $\mathbb{F}_{2^{128}}/(x^{128}+x^7+x^2+x+1)$

Field size 2^n	#CNOT	#1qCliff	#T	T-depth※	#Qubit	Full depth
$n=128$	29867	4374	15309	4	6561	78

※: Toffoli depth one has a T-depth of four.

- WISA 곱셈의 경우, stand-alone 곱셈이 아닌 경우, 큐비트 수를 줄일 수 있음
  - 낮은 비용(CNOT 게이트, Depth 오버헤드 X)만으로, 많은 수의 ancilla 큐비트를 재사용 가능
  - 첫 번째 곱셈을 제외하고, 6561이 아닌 감소된 2443개의 큐비트만이 필요함

AIM 양자 회로 구현

- $\mathbb{F}_{2^{128}}/(x^{128}+x^7+x^2+x+1)$의 제곱은 적은 비용으로 구현 가능
  - 선형 연산으로 분류됨으로써, PLU 분해를 기반으로 한 In-place 구현이 가능하지만,
    - Temp 값을 위한 3개의 ancilla 큐비트를 사용하였음 → naive하게 구현

Table 2: Quantum resources required for squaring of $\mathbb{F}_{2^{128}}/(x^{128}+x^7+x^2+x+1)$

Field size 2^n	#CNOT	#Qubit	Full depth
$n = 128$	205	131	127

- In-place 구현으로 ancilla 큐비트를 아예 사용하지 않거나, depth를 좀 더 줄일 수 있긴 함

AIM 양자 회로 구현

- Mer(3) 양자 회로 구현 → Multiplication + Squaring

Algorithm 1: Quantum circuit implementation of Mer(3).

Input: x
Output: x^{2^3-1}, x^{2^3-1}(copy), *ancilla*
//Allocate ancilla qubits for Mul
1: *ancilla* ← allocate 4118 qubits

//Compute Mer(3)
//Copy x to $x1$
2: $x1$ ← allocate new 128 qubits
3: CNOT128(x, $x1$)

//x^{2^2-1}
4: $x1$ ← Squaring($x1$)

5: $x2$ ← Mul(x, $x1$, *ancilla*)
6: $x2$ ← Reduction($x2$)
7: *ancilla* ← CleanAncilla(x, $x1$, *ancilla*)

//x^{2^3-1}
8: $x2$ ← Squaring($x2$)

9: *out* ← Mul(x, $x2$, *ancilla*)
10: *out* ← Reduction(*out*)
11: *ancilla* ← CleanAncilla(x, $x2$, *ancilla*)

//Copy *out* to $x3$ for Mer (27)
12: $x3$ ← allocate new 128-qubit
13: CNOT128(*out*, $x3$)
14: **return** *out*, $x3$, *ancilla*

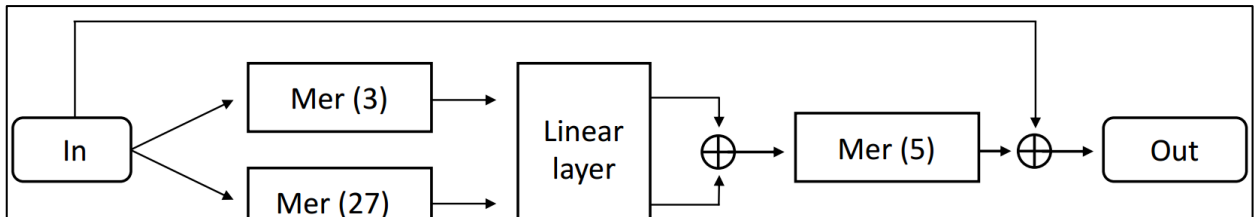


Fig. 1: Encryption process of AIM-I

AIM 양자 회로 구현

- Mer(3), (27), (5) 구현 비용

Table 3: Quantum resources required for the components of AIM-I.

Component	#CNOT	#1qCliff	$\#T$	T-depth[※]	#Qubit	Full depth
Mer(3)	68636	8748	30618	8	8882	411
Mer(27)	226224	26244	91854	16	13840	2488
Mer(5)	115385	13122	45927	12	6957	678
LinearLayer	16889	·	·	·	640	426

AIM 양자 회로 구현

- LinearLayer의 경우, LowMC와 유사함
  - PLU 기반의 구현의 경우, In-place 구현이 가능하지만 depth가 증가함.
  - Naïve한 구현의 경우, ouptut을 위한 큐비트를 따로 사용하지만, depth를 줄일 수 있음
    - 공간이 넓어짐에 따라, 많은 CNOT 게이트들이 병렬적으로 실행되기 때문

(b) Linear layer.

Method	#CNOT ✻	#1qCliff ❁	#qubits ❂	Full depth ❋
Linear layer L1 [30]	8,093	60	128	2,365
Linear layer L3 [30]	18,080	90	192	5,301
Linear layer L5 [30]	32,714	137	256	8,603
Linear layer L1	8,205	0	256	225
Linear layer L3	18,418	0	384	339
Linear layer L5	32,793	0	512	455

Table 3: Quantum resources required for the components of AIM-I.

Component	#CNOT	#1qCliff	#T	T-depth※	#Qubit	Full depth
Mer(3)	68636	8748	30618	8	8882	411
Mer(27)	226224	26244	91854	16	13840	2488
Mer(5)	115385	13122	45927	12	6957	678
LinearLayer	16889	·	·	·	640	426

AIM 양자 회로 성능 평가

- AIM-I 양자 회로 성능
  - 총 9 번의 곱셈이 사용되어 T-depth = 9 × 4 = 36으로 낮은 편,
  - Qubit은 많이 사용되는 편이며, Full depth는 보통인 편

Table 4: Quantum resources required for the AIM-I quantum circuit.

Cipher	#CNOT	#1qCliff	#T	T-depth※	#Qubit	Full depth	$TD \times M$	$FD \times M$
AIM-I	358754	39430	137781	36	25299	3499	227691	88521201

- AIM-I의 Grover's key search 비용은 2^{160} → 양자 후 보안 Level-1 달성
  - NIST 기준 (Grassl et al.)은 2^{170}, AES-128 최신 구현은 2^{157}

Table 5: Cost of the Grover's key search for AIM-I

Cipher	Total gates	Total depth	Cost (complexity)	#Qubit	$TD \times M$	$FD \times M$	For parallel search	
							$TD^2 \times M$	$FD^2 \times M$
AIM-I	$1.612 \cdot 2^{83}$	$1.342 \cdot 2^{76}$	$1.082 \cdot 2^{160}$	25300	$1.351 \cdot 2^{82}$	$1.036 \cdot 2^{91}$	$1.182 \cdot 2^{150}$	$1.39 \cdot 2^{167}$

결 론

- Depth를 좀 더 줄일 수 있을 것 같지만, 그래도 AIM-I는 양자 후 보안 강도 Level-1 달성 가능

- 다른 파라미터들 (-III, -V) 또한 적정 보안 레벨을 달성할 듯 함 (Level -3, -5)

Table 6: Comparison of the Grover's key search costs

Post-quantum Secuirty	NIST [15] (based on [7])	J++ [10]	AIM		
			-I	-III	-V
Level-1 (AES-128)	2^{170}	2^{157}	2^{160}		
Level-3 (AES-192)	2^{233}	2^{222}		.	
Level-5 (AES-256)	2^{298}	2^{286}			.

Thank you!