F A C E - L I G H T

FACE–LIGHT: Fast AES CTR Mode Encryption for Low-end Microcontrollers

https://www.youtube.com/watch?v=lCPLQmnn7As&t=1124s

2019 ICISC

CONTENTS

01

Introduction

F A C E - L I G H T

AES (Advanced Encryption Standard)

- World side block cipher standard
  - FIPS 197
  - ISO/IEC 18033-3
- AES Modes
  - ECB, CBC, CFB, OFB, **CTR**

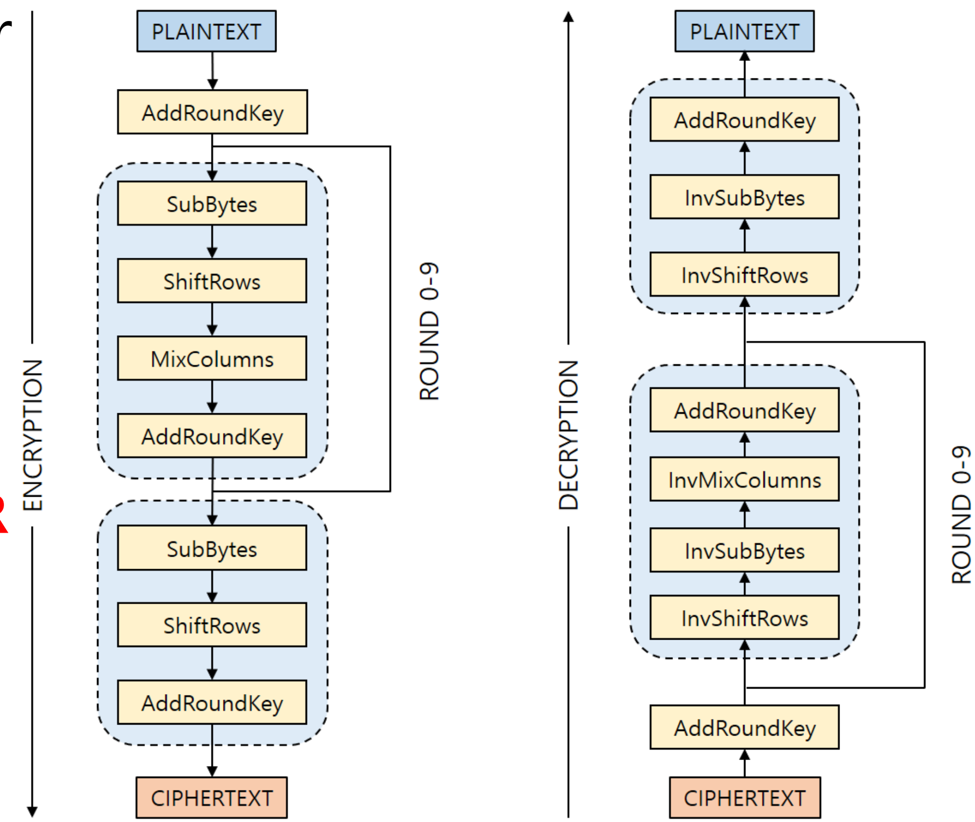


Fig 1. AES Structure

AES-CTR

- AES Counter Mode
- **Parallel Process**

- 128bits IV(Initial Vector)
  - 96bits Nonce
  - 32bits Counter
- Counter value increases by 1 on each block

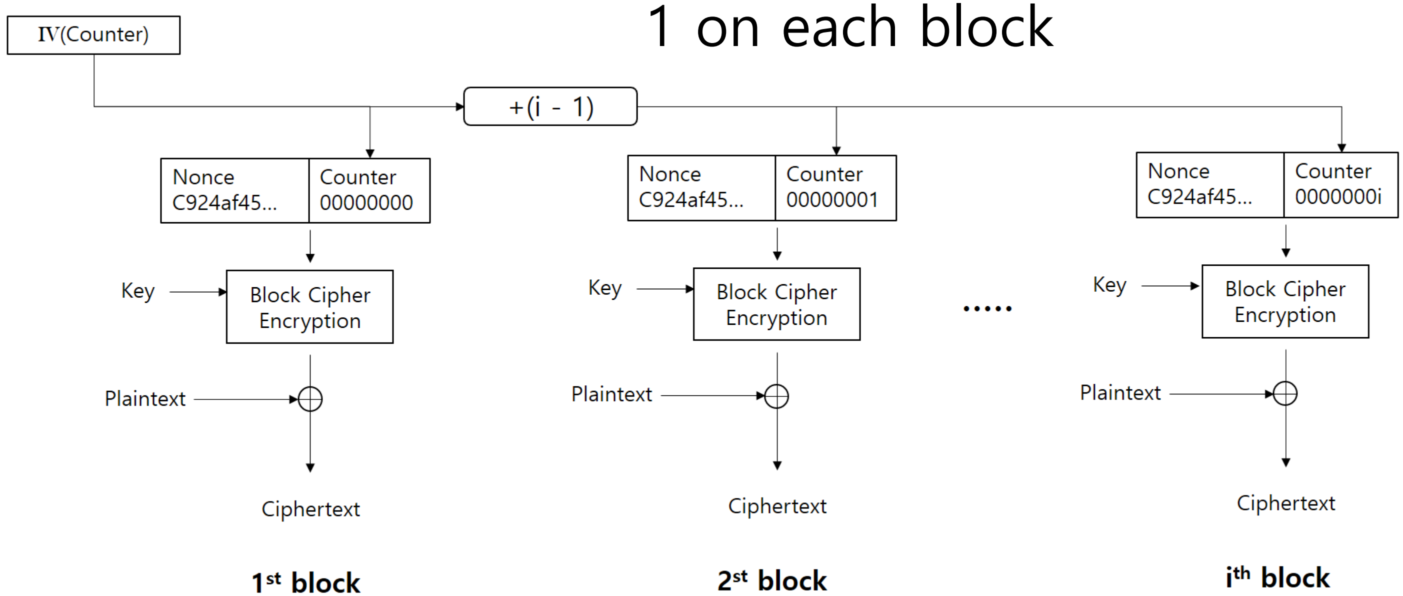


Fig 2. AES-CTR Structure

Side Channel Attack(SCA)

- Attack based on **additional information** during cipher operation
- Power Analysis
  - SPA(Simple Power Analysis)
  - DPA(Differential Power Analysis)
  - CPA(Correlation Power Analysis)

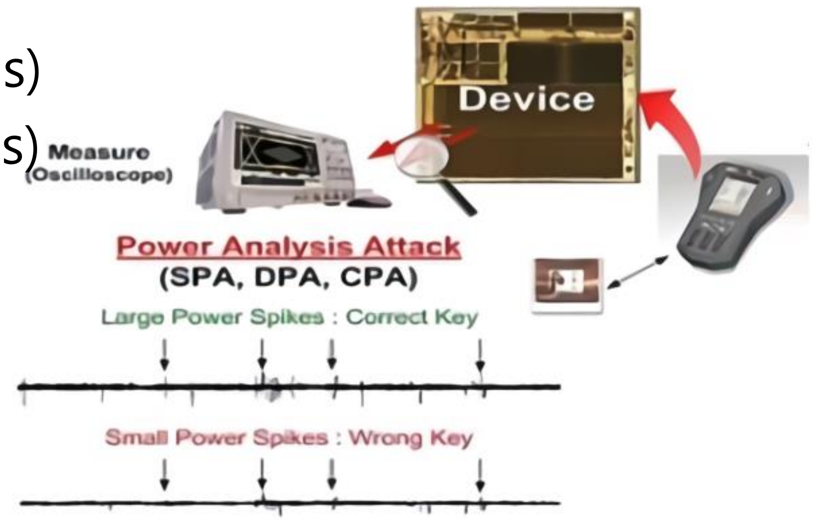


Fig 3. Power Analysis Attack

Masking

- SCA Countermeasure
  - Preventing power analysis

- Implemented with reference to the published masking technique*
  - **Optimized Implementation** on 8bits Microcontroller

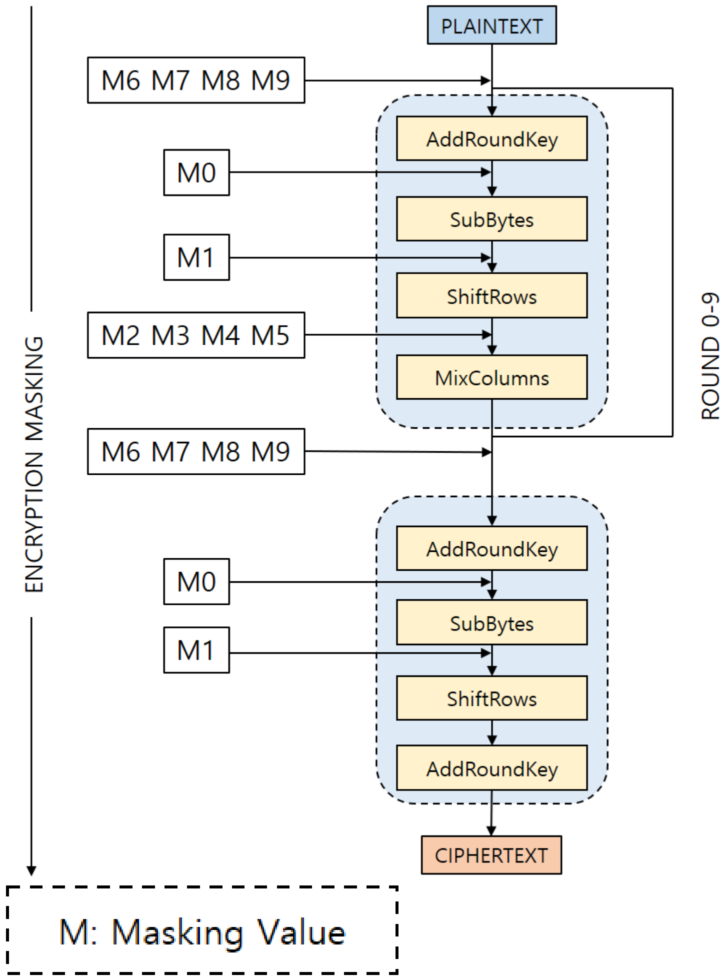


Fig 4. Masking Process

*C. Herbst, E. Oswald, and S. Mangard, "An aes smart card implementation resistant to power analysis attacks," in ACNS, pp. 239–252, Springer, 2006.

02

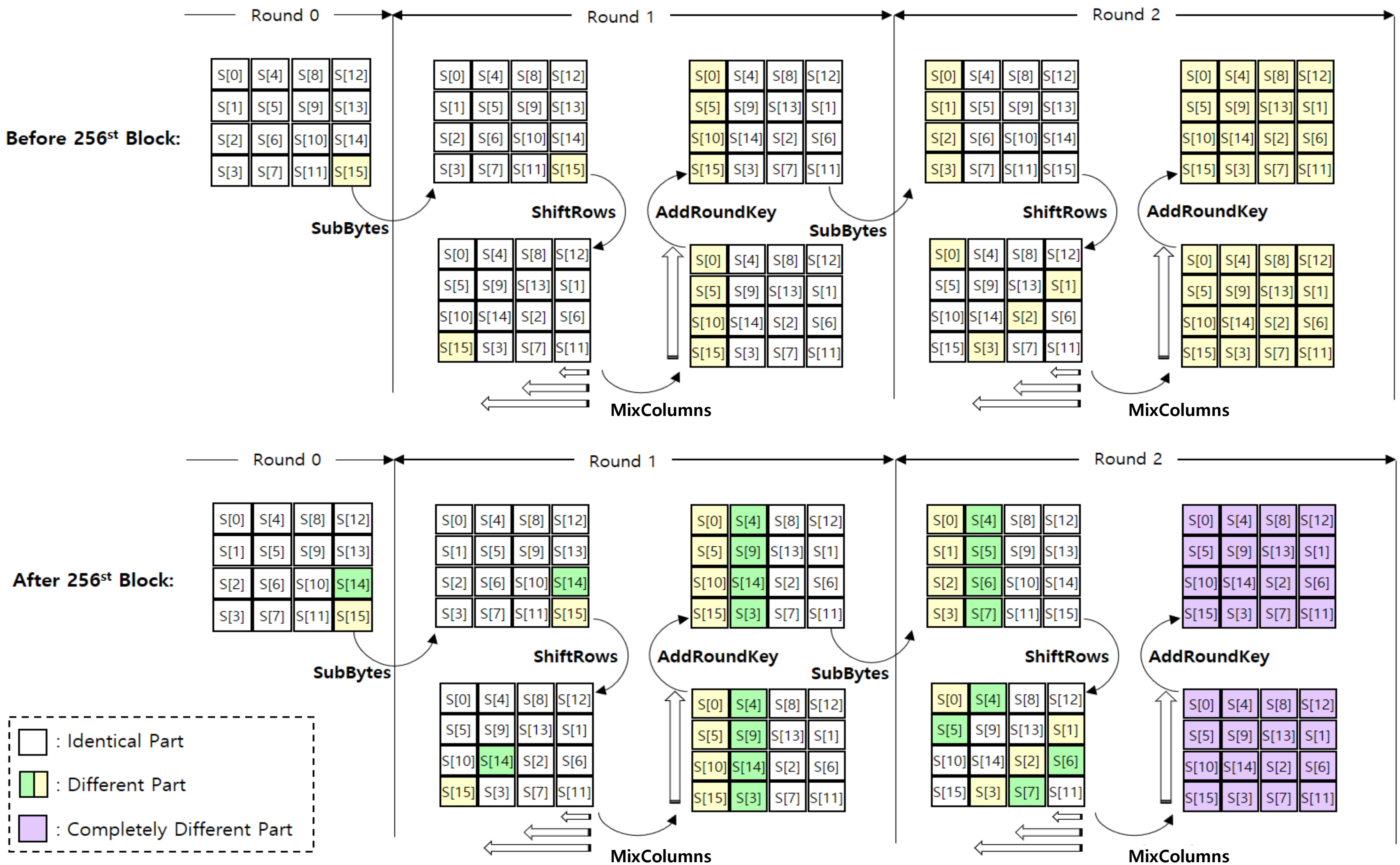
FACE

F A C E - L I G H T

Outline

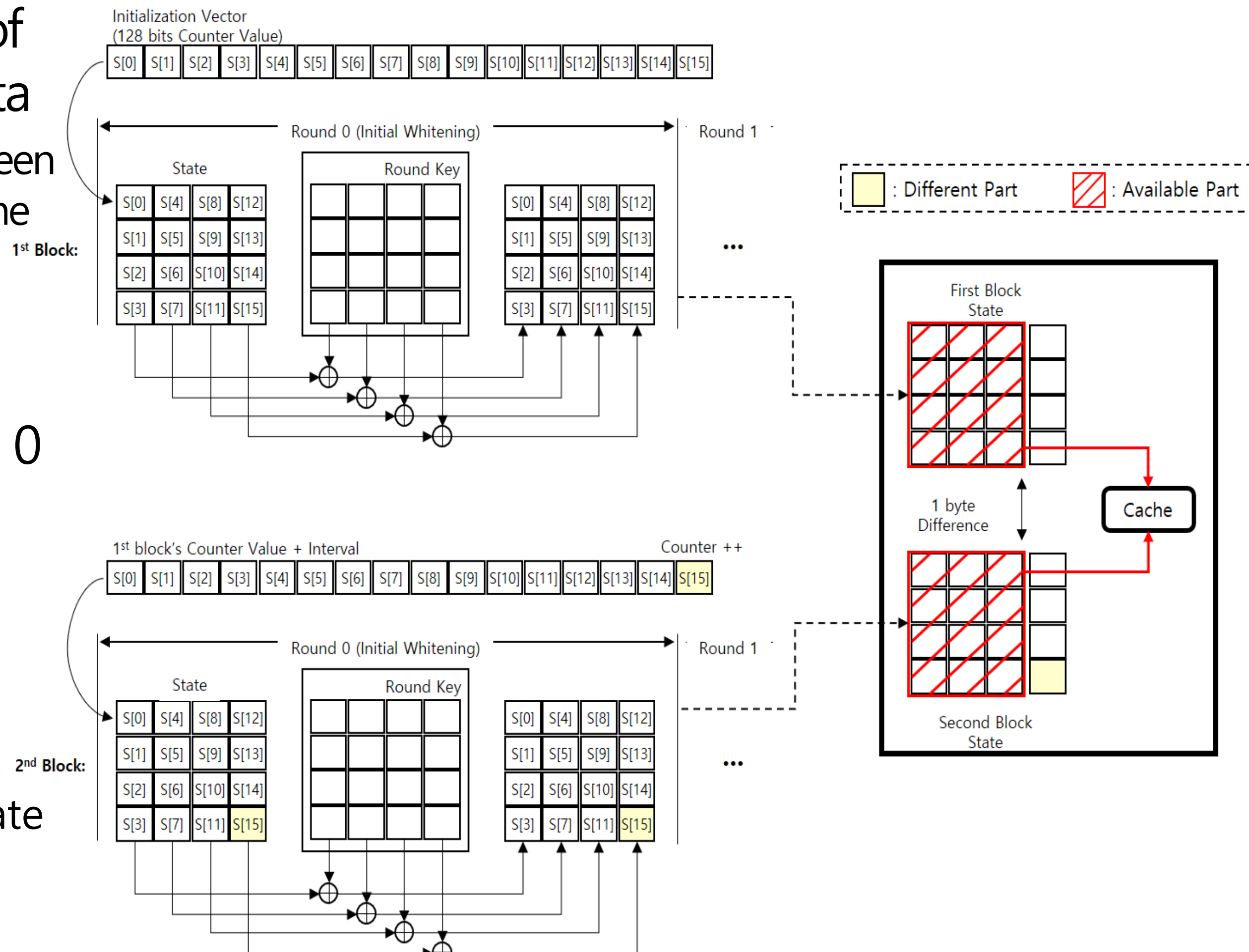
- Optimized implementation using AES-CTR technique
  - Last byte saves the counter value
  - The only difference between the first and the next block is **the last byte**
- Stores the repeated value except the counter value
  - Stores the value in the **Look Up Table(LUT)**
  - Refer to the LUT for specific round
  - Requires 5 LUT(**5KB**)

- **Need to update LUT** every period according to the change of the counter value


Round 0
Round 1
Round 2
Before 256st Block:
SubBytes
ShiftRows
AddRoundKey
MixColumns
Round 0
Round 1
Round 2
After 256st Block:
SubBytes
ShiftRows
AddRoundKey
MixColumns
: Identical Part
: Different Part
: Completely Different Part

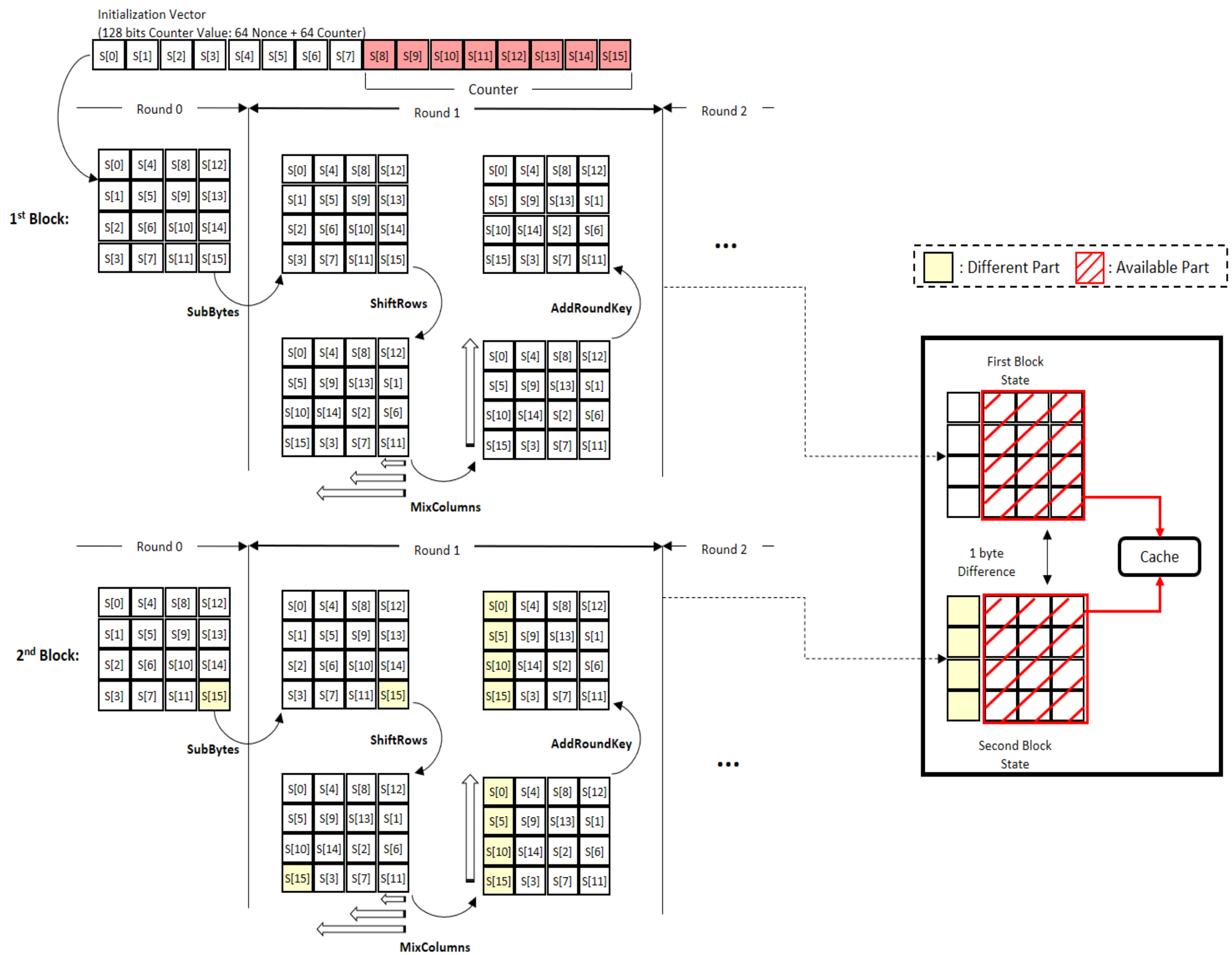
Structure (Round 0)

- Utilize the change of last bytes of the data
  - The difference between the first block and the next block is 1byte
- 12 Bytes can be utilized after Round 0
  - S[12], S[13], S[14], S[15]
- Table can be used (**2^{32} – 1**)times
  - No need for update



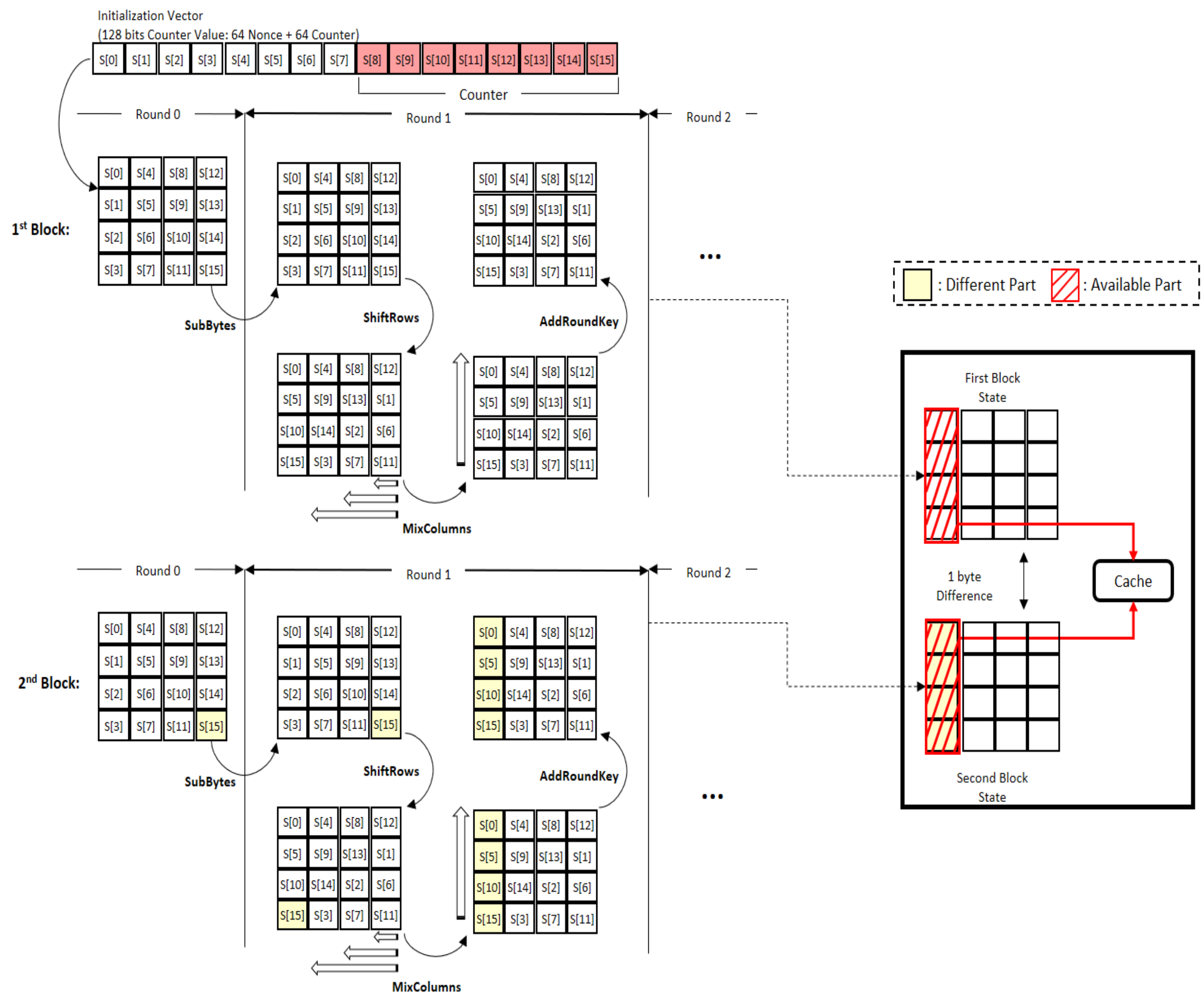
Structure (Round 1)

- Last byte spreading
  - Spreads across two stages
  - ShiftRows
  - MixColumns
- LUT generation available
  - Excpet first column
- Table can be used ($2^8 - 1$) times



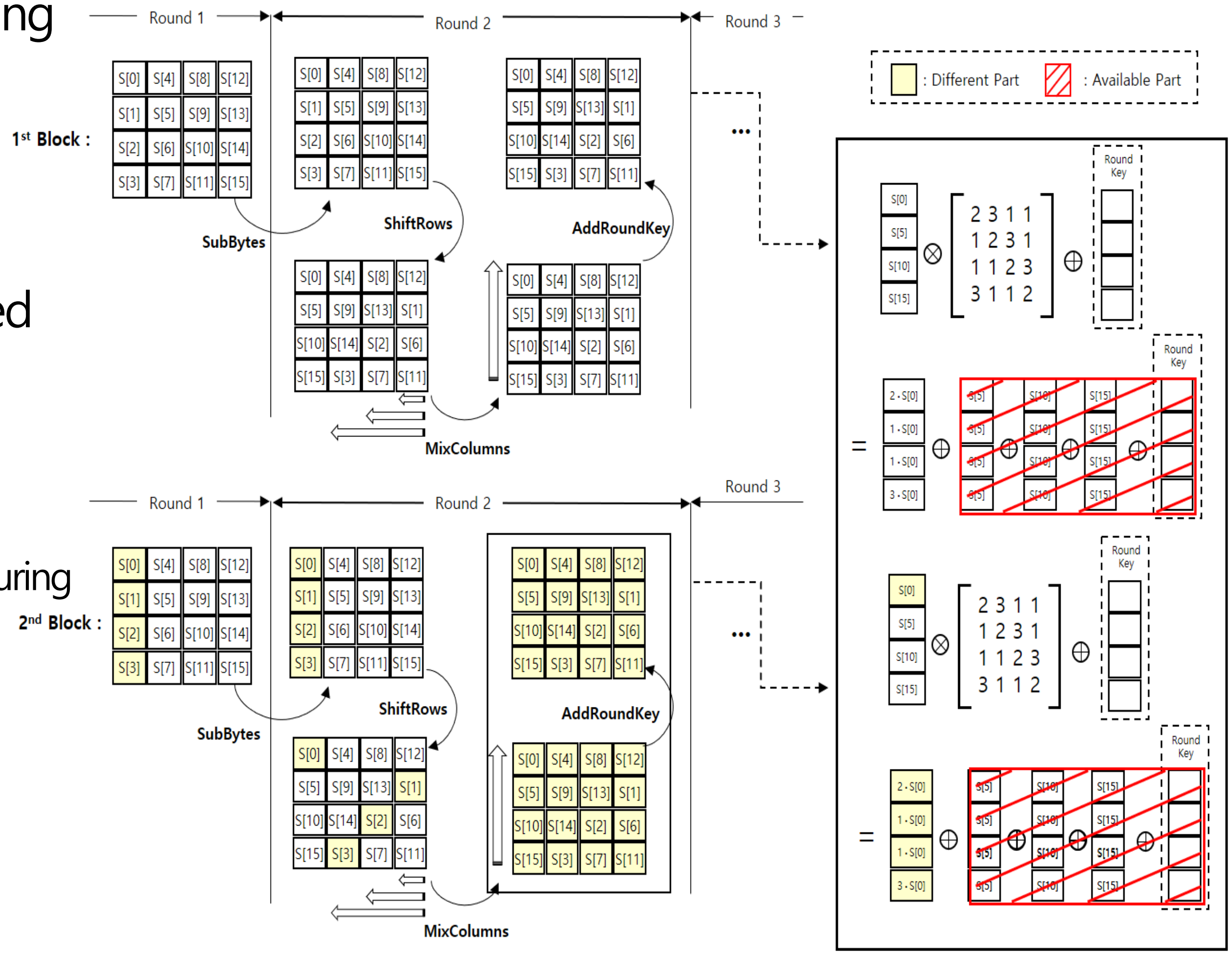
Structure (Round 1+)

- Last byte spreading
  - Spreads across two stages
  - ShiftRows
  - MixColumns
- LUT generation available
  - Utilize S[15] as index
  - Table Size: $1KB$
- Table can be used ($2^8 \times 2^{32}$) times



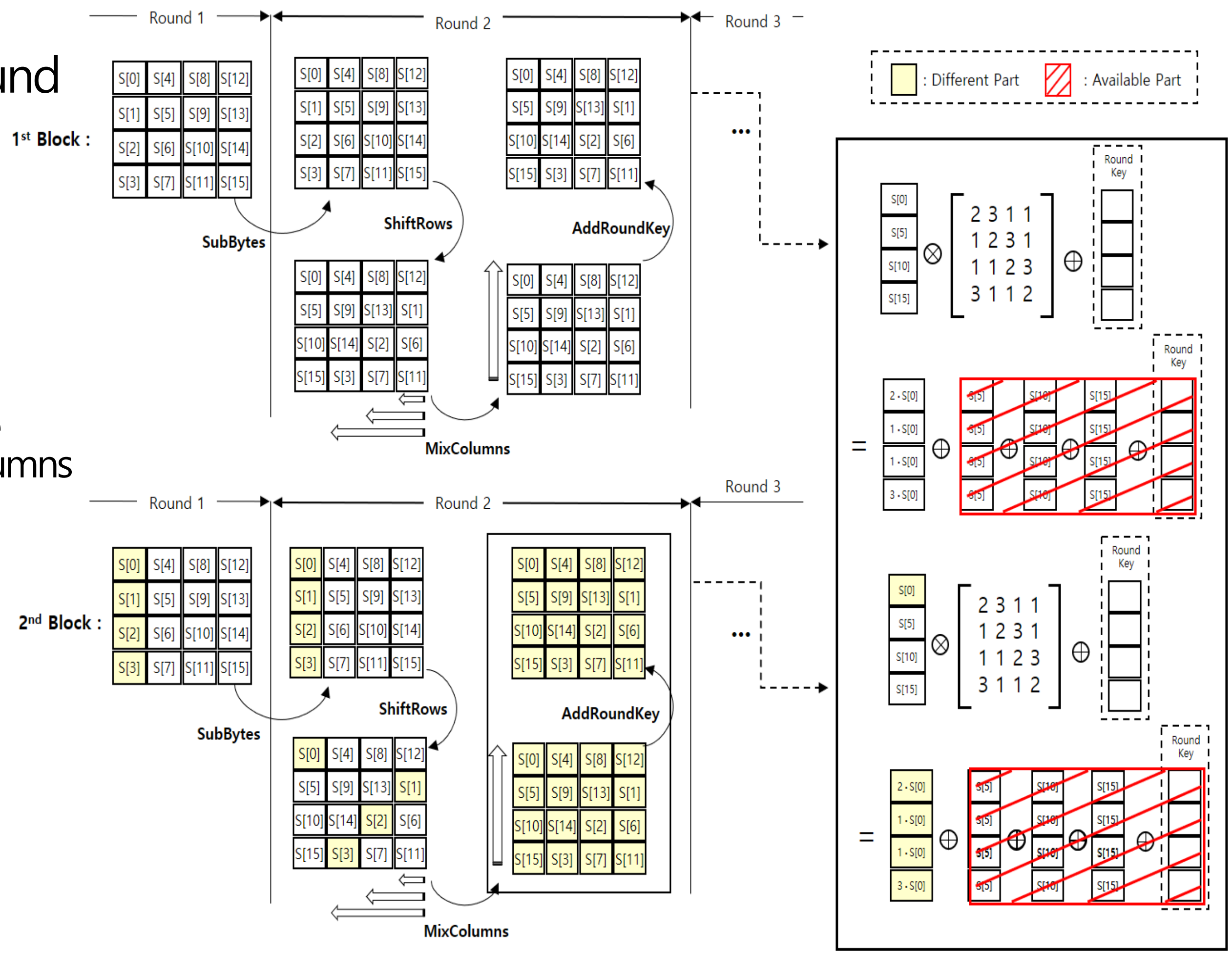
Structure (Round 2)

- First column spreading
  - Spreads across two stages
  - ShiftRows
  - MixColumns
- All values are affected after Round 2
- LUT generation available
  - Intermediate value during MixColumns
- Table can be used (2^8 - 1) times



Structure (Round 2+)

- Values that are not stored in LUT in Round 2
  - S[0], S[1], S[2], S[3]
- LUT generation available
  - Unused Intermediate value during MixColumns
  - Table Size: $4KB$
- Table can be used (2^8 x 2^{32}) times



Limitation of FACE

- Difficult to utilize on 8bits Microcontroller
  - **LUT capacity** issues
  - Requires minimum $5KB$ of memory
- Requires **updates of LUT** at regular intervals

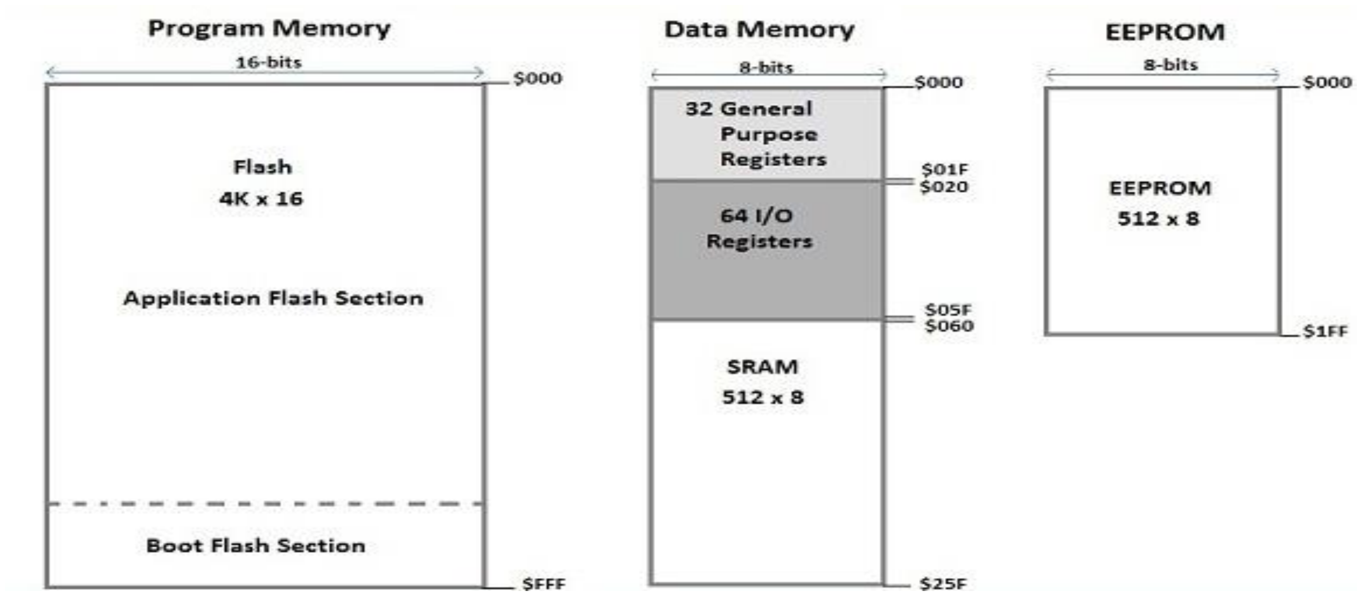


Fig 6. Arduino Uno Memory Structure

03

Our Work

FACE - LIGHT

F A C E - L I G H T

Target Board

- 8bits Microcontroller
  - **Arduino Uno ATmega328P**

- Hardware Spec
  - Flash Memory: $32KB$
  - SRAM: $2KB$
  - EEPROM: $1KB$
  - Clock Speed: 16MHz

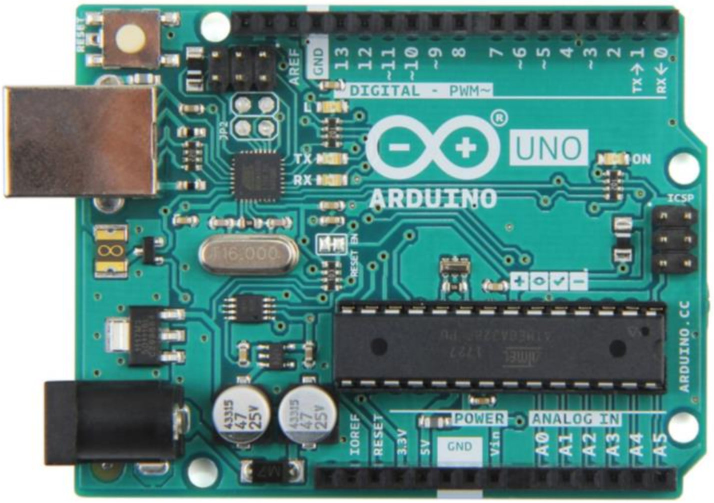


Fig 7. Arduino Uno

Overview

- Optimized implementation based on FACE
  - Optimized for low-power processor
- Stores the iterated value dependent on the counter value
  - Stores the value in the **Look Up Table(LUT)**
  - **Multiple rounds omitted** with a single reference
  - Requires 4 LUT (**$4KB$**)
- **No Need to update LUT** every period according to the change of the counter value
- Improved performance by combining with FACE

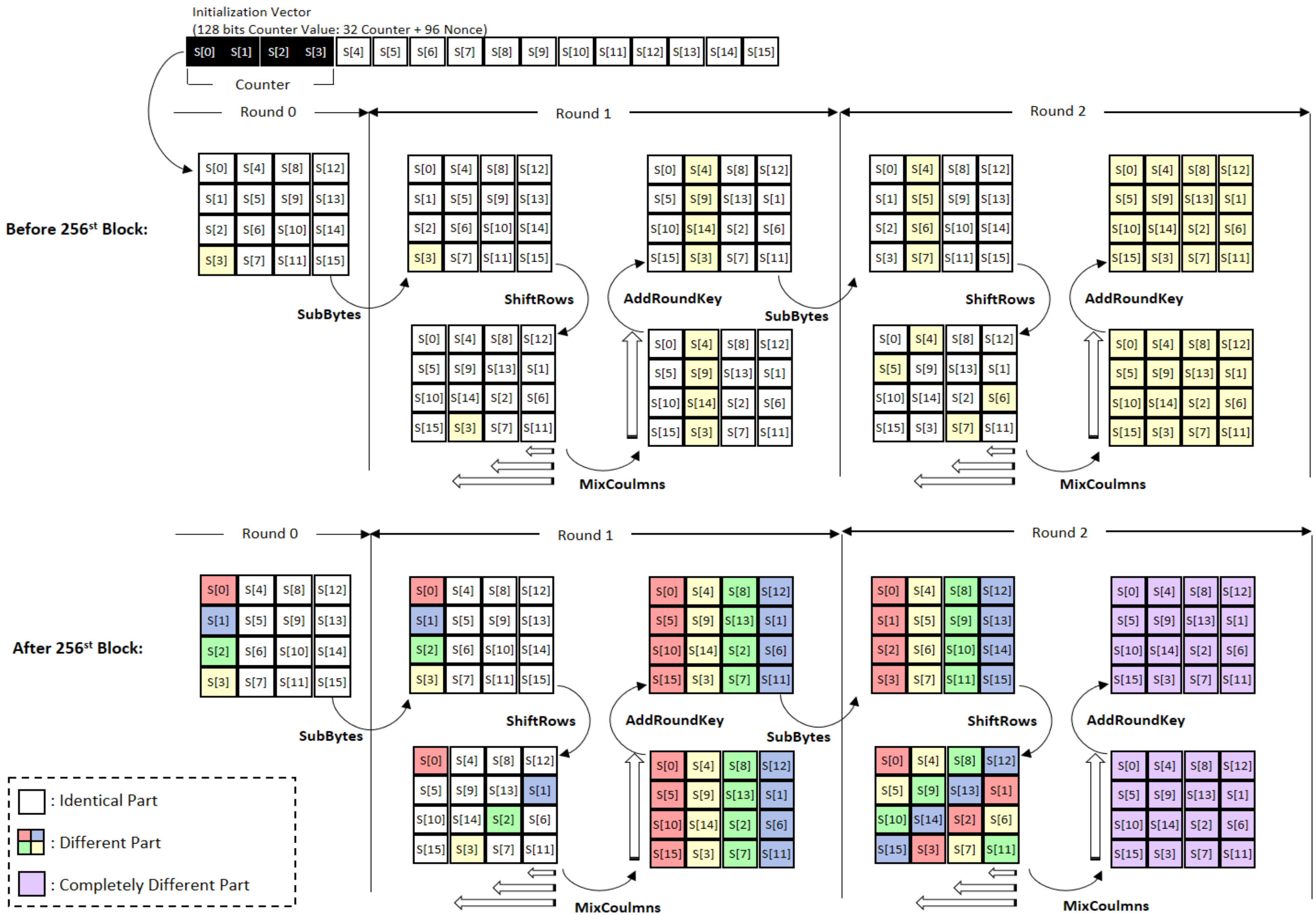


Fig 8. Overview of FACE-LIGHT

Initialization Vector
(128 bits Counter Value: 32 Counter + 96 Nonce)

00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Counter

CIPHER KEY

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f

	Start of round				After SubBytes				After ShiftRows				After MixColumns			
Round 0	00	00	00	00												
	00	00	00	00												
	00	00	00	00												
	00	00	00	00												
Round 1	00	04	08	0c	63	f2	30	fe	63	f2	30	fe	6a	2c	b0	27
	01	05	09	0d	7c	6b	01	d7	6b	01	d7	7c	6a	6d	d9	9c
	02	06	0a	0e	77	6f	67	ab	67	ab	77	6f	5c	33	5d	21
	03	07	0b	0f	7b	c5	2b	76	76	7b	c5	2b	45	51	61	5c
Round 2	bc	fe	6a	f1	65	bb	02	a1	65	bb	02	a1	a0	37	e7	6f
	c0	c2	7f	37	ba	25	d2	9a	25	d2	9a	ba	54	85	13	30
	28	41	25	57	34	83	3f	5b	3f	5b	34	83	70	6b	56	a6
	b8	ab	90	a2	6c	62	60	3a	3a	6c	62	60	c1	87	6c	01

Initialization Vector
(128 bits Counter Value: 32 Counter + 96 Nonce)

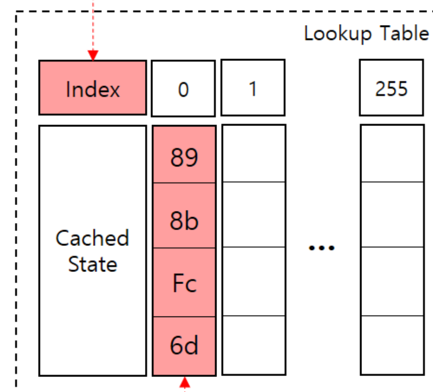
00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00

Counter

CIPHER KEY

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f

	Start of round				After SubBytes				After ShiftRows				After MixColumns			
Round 0	00	00	00	00												
	00	00	00	00												
	00	00	00	00												
	01	00	00	00												
Round 1	00	04	08	0c	63	f2	30	fe	63	f2	30	fe	6a	20	b0	27
	01	05	09	0d	7c	6b	01	d7	6b	01	d7	7c	6a	61	d9	9c
	02	06	0a	0e	77	6f	67	ab	67	ab	77	6f	5c	27	5d	21
	02	07	0b	0f	77	c5	2b	76	76	77	c5	2b	45	49	61	5c
Round 2	bc	f2	6a	f1	65	89	02	a1	65	89	02	a1	49	53	e8	10
	c0	ce	7f	37	ba	8b	d2	9a	8b	d2	9a	ba	13	b7	1c	b1
	28	55	25	57	34	fc	3f	5b	3f	5b	34	fc	de	59	47	58
	b8	b3	90	a2	6c	6d	60	3a	3a	6c	6d	60	6f	d1	72	7e



Initialization Vector
(128 bits Counter Value: 32 Counter + 96 Nonce)

00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Counter

CIPHER KEY

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f

	Start of round				After SubBytes				After ShiftRows				After MixColumns			
Round 0	00	00	00	00												
	00	00	00	00												
	00	00	00	00												
	00	00	00	00												
Round 1	00	04	08	0c	63	f2	30	fe	63	f2	30	fe	6a	2c	b0	27
	01	05	09	0d	7c	6b	01	d7	6b	01	d7	7c	6a	6d	d9	9c
	02	06	0a	0e	77	6f	67	ab	67	ab	77	6f	5c	33	5d	21
	03	07	0b	0f	7b	c5	2b	76	76	7b	c5	2b	45	51	61	5c
Round 2	bc	fe	6a	f1	65	bb	02	a1	65	bb	02	a1	a0	37	e7	6f
	c0	c2	7f	37	ba	25	d2	9a	25	d2	9a	ba	54	85	13	30
	28	41	25	57	34	83	3f	5b	3f	5b	34	83	70	6b	56	a6
	b8	ab	90	a2	6c	62	60	3a	3a	6c	62	60	c1	87	6c	01

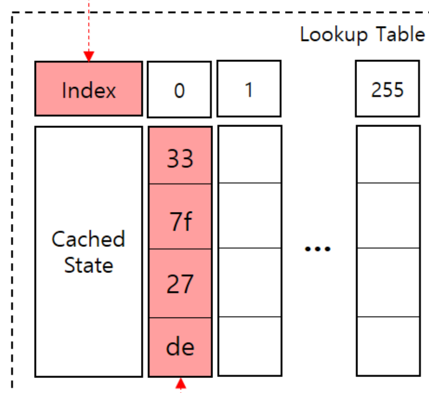
Initialization Vector
(128 bits Counter Value: 32 Counter + 96 Nonce)

Counter															
00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00

CIPHER KEY

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f

	Start of round				After SubBytes				After ShiftRows				After MixColumns			
Round 0	00	00	00	00												
	00	00	00	00												
	01	00	00	00												
	00	00	00	00												
Round 1	00	04	08	0c	63	f2	30	fe	63	f2	30	fe	6a	2c	b0	27
	01	05	09	0d	7c	6b	01	d7	6b	01	d7	7c	6a	6d	d9	9c
	03	06	0a	0e	7b	6f	67	ab	67	ab	7b	6f	5c	33	45	21
	03	07	0b	0f	7b	c5	2b	76	76	7b	c5	2b	45	51	6d	5c
Round 2	bc	fe	66	f1	65	bb	33	a1	65	bb	33	a1	b8	db	85	6f
	c0	c2	6b	37	ba	25	7f	9a	25	7f	9a	ba	7c	c4	22	8e
	28	41	3d	57	34	83	27	5b	27	5b	34	83	40	c6	67	7f
	b8	ab	9c	a2	6c	62	de	3a	3a	6c	62	de	d9	2a	3f	66



Initialization Vector

(128 bits Counter Value: 32 Counter + 96 Nonce)

00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Counter															

CIPHER KEY

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f

Round 0

Start of round			
00	00	00	00
00	00	00	00
00	00	00	00
00	00	00	00

Round 1

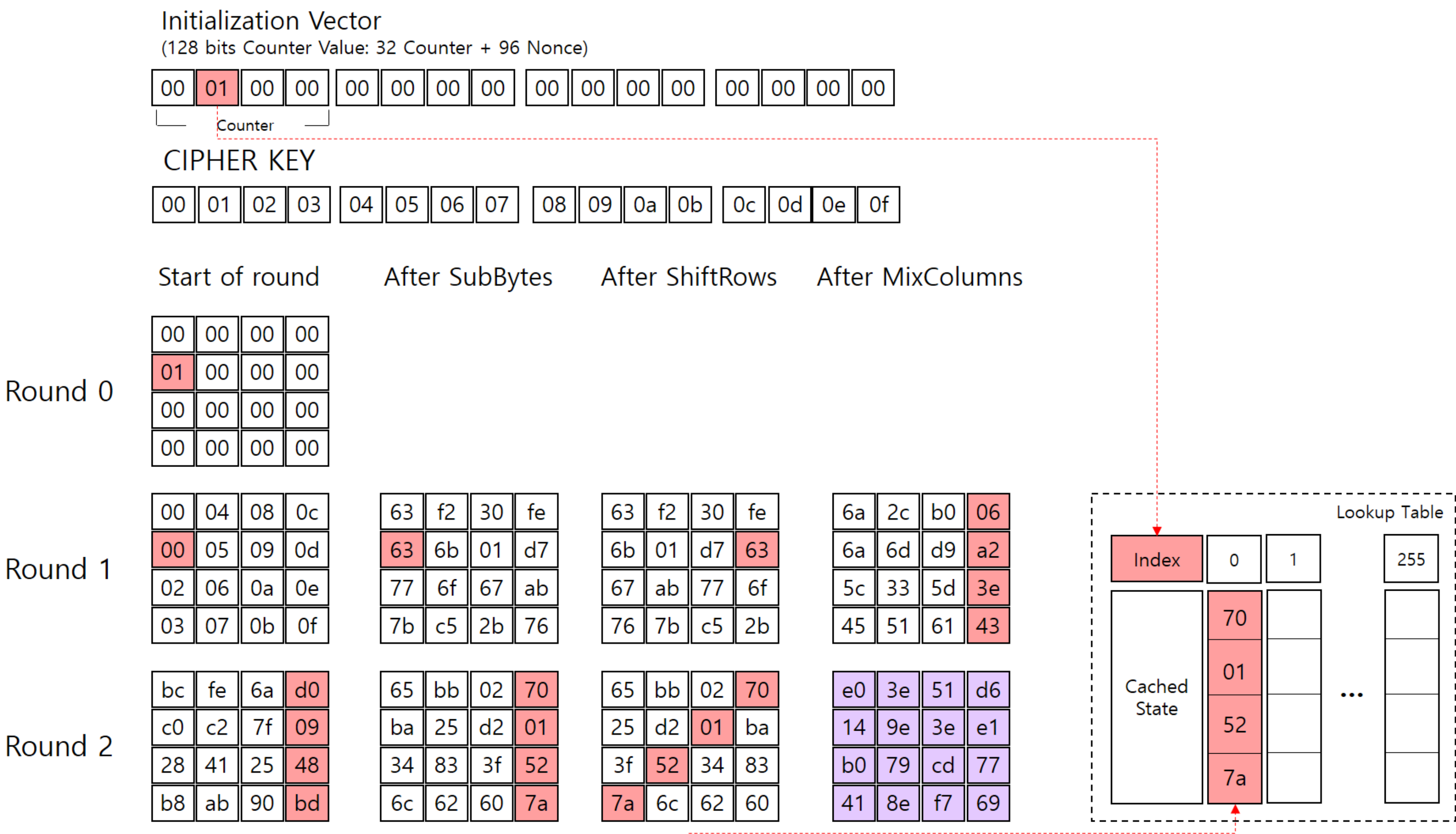
Start of round				After SubBytes				After ShiftRows				After MixColumns			
00	04	08	0c	63	f2	30	fe	63	f2	30	fe	6a	2c	b0	27
01	05	09	0d	7c	6b	01	d7	6b	01	d7	7c	6a	6d	d9	9c
02	06	0a	0e	77	6f	67	ab	67	ab	77	6f	5c	33	5d	21
03	07	0b	0f	7b	c5	2b	76	76	7b	c5	2b	45	51	61	5c

Round 2

Start of round				After SubBytes				After ShiftRows				After MixColumns			
bc	fe	6a	f1	65	bb	02	a1	65	bb	02	a1	a0	37	e7	6f
c0	c2	7f	37	ba	25	d2	9a	25	d2	9a	ba	54	85	13	30
28	41	25	57	34	83	3f	5b	3f	5b	34	83	70	6b	56	a6
b8	ab	90	a2	6c	62	60	3a	3a	6c	62	60	c1	87	6c	01

Our Work

03


Initialization Vector
(128 bits Counter Value: 32 Counter + 96 Nonce)
00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Counter
CIPHER KEY
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
Start of round
After SubBytes
After ShiftRows
After MixColumns
Round 0
00 00 00 00
01 00 00 00
00 00 00 00
00 00 00 00
Round 1
00 04 08 0c
00 05 09 0d
02 06 0a 0e
03 07 0b 0f
63 f2 30 fe
63 6b 01 d7
77 6f 67 ab
7b c5 2b 76
63 f2 30 fe
6b 01 d7 63
67 ab 77 6f
76 7b c5 2b
6a 2c b0 06
6a 6d d9 a2
5c 33 5d 3e
45 51 61 43
Round 2
bc fe 6a d0
c0 c2 7f 09
28 41 25 48
b8 ab 90 bd
65 bb 02 70
ba 25 d2 01
34 83 3f 52
6c 62 60 7a
65 bb 02 70
25 d2 01 ba
3f 52 34 83
7a 6c 62 60
e0 3e 51 d6
14 9e 3e e1
b0 79 cd 77
41 8e f7 69
Lookup Table
Index
0
1
255
Cached State
70
01
52
7a
...

Initialization Vector
(128 bits Counter Value: 32 Counter + 96 Nonce)

00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Counter

CIPHER KEY

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f

Start of round / After SubBytes / After ShiftRows / After MixColumns

Round 0 — Start of round

00	00	00	00
00	00	00	00
00	00	00	00
00	00	00	00

Round 1

Start of round				After SubBytes				After ShiftRows				After MixColumns			
00	04	08	0c	63	f2	30	fe	63	f2	30	fe	6a	2c	b0	27
01	05	09	0d	7c	6b	01	d7	6b	01	d7	7c	6a	6d	d9	9c
02	06	0a	0e	77	6f	67	ab	67	ab	77	6f	5c	33	5d	21
03	07	0b	0f	7b	c5	2b	76	76	7b	c5	2b	45	51	61	5c

Round 2

Start of round				After SubBytes				After ShiftRows				After MixColumns			
bc	fe	6a	f1	65	bb	02	a1	65	bb	02	a1	a0	37	e7	6f
c0	c2	7f	37	ba	25	d2	9a	25	d2	9a	ba	54	85	13	30
28	41	25	57	34	83	3f	5b	3f	5b	34	83	70	6b	56	a6
b8	ab	90	a2	6c	62	60	3a	3a	6c	62	60	c1	87	6c	01

Initialization Vector
(128 bits Counter Value: 32 Counter + 96 Nonce)

01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Counter

CIPHER KEY

00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f

Round 0

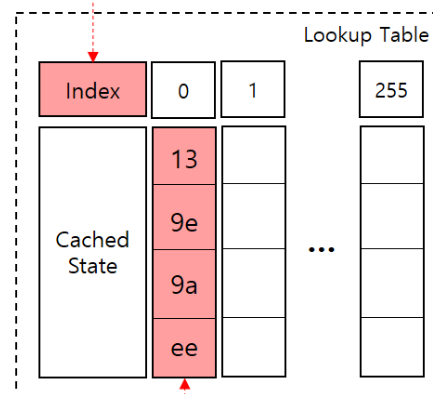
Start of round			
01	00	00	00
00	00	00	00
00	00	00	00
00	00	00	00

Round 1

Start of round				After SubBytes				After ShiftRows				After MixColumns			
01	04	08	0c	7c	f2	30	fe	7c	f2	30	fe	54	2c	b0	27
01	05	09	0d	7c	6b	01	d7	6b	01	d7	7c	75	6d	d9	9c
02	06	0a	0e	77	6f	67	ab	67	ab	77	6f	43	33	5d	21
03	07	0b	0f	7b	c5	2b	76	76	7b	c5	2b	64	51	61	5c

Round 2

Start of round				After SubBytes				After ShiftRows				After MixColumns			
82	fe	6a	f1	13	bb	02	a1	13	bb	02	a1	4c	b5	49	03
df	c2	7f	37	9e	25	d2	9a	25	d2	9a	9e	22	07	fa	78
37	41	25	57	9a	83	3f	5b	3f	5b	9a	83	06	f6	11	82
99	ab	90	a2	ee	62	60	3a	3a	ee	62	60	5b	98	c2	25



Look Up Table Structure

- Size of LUT: 4KB
- Update **not required**

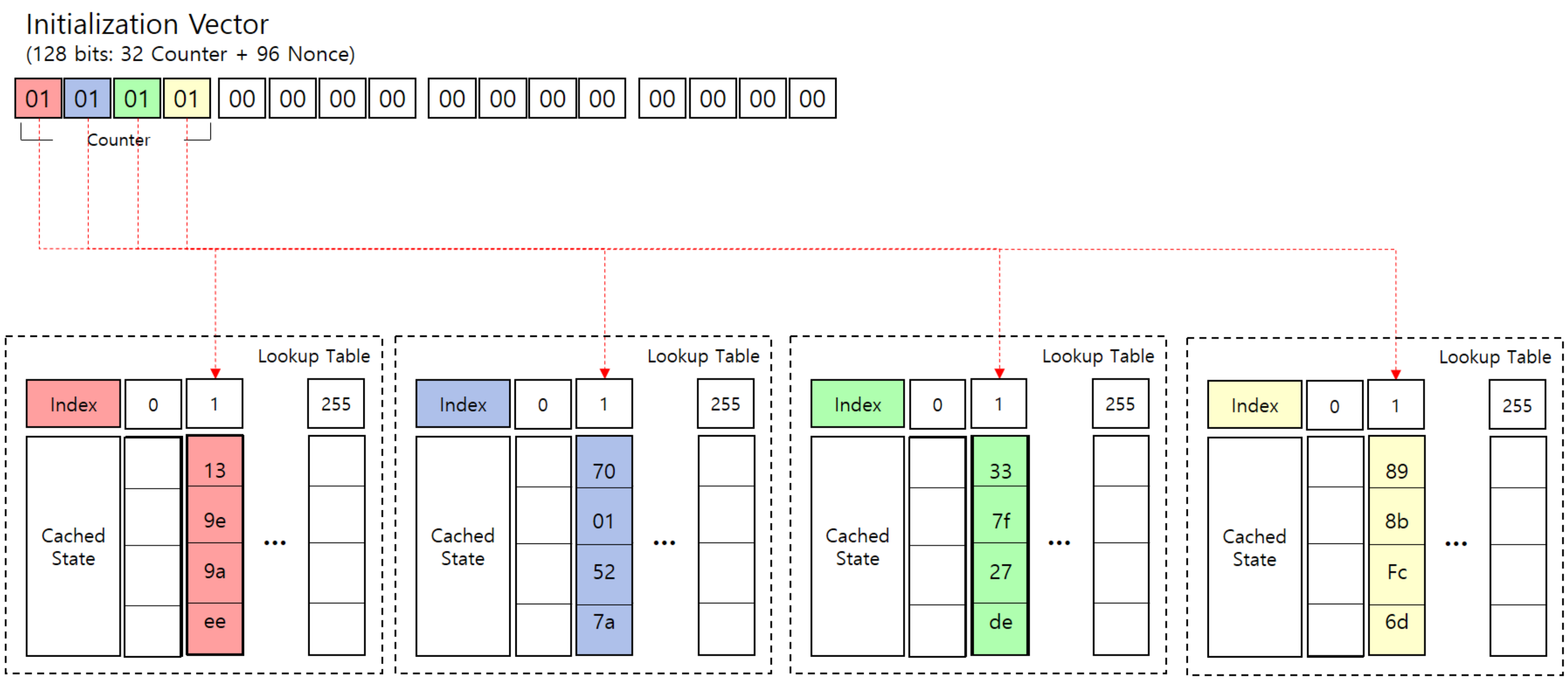
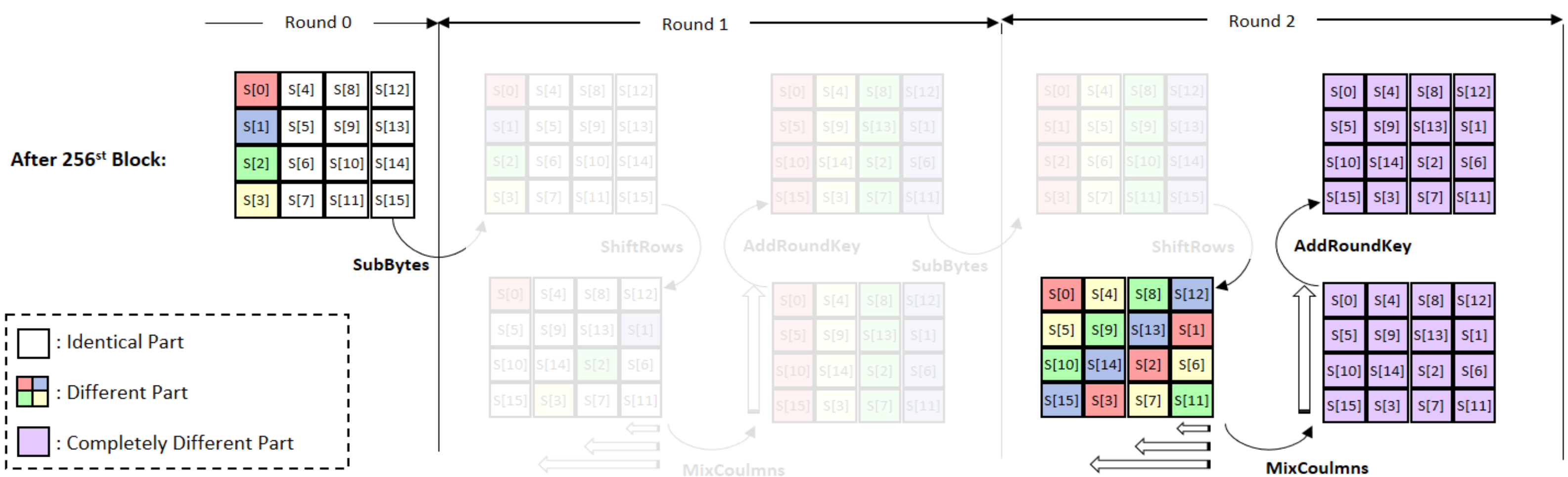
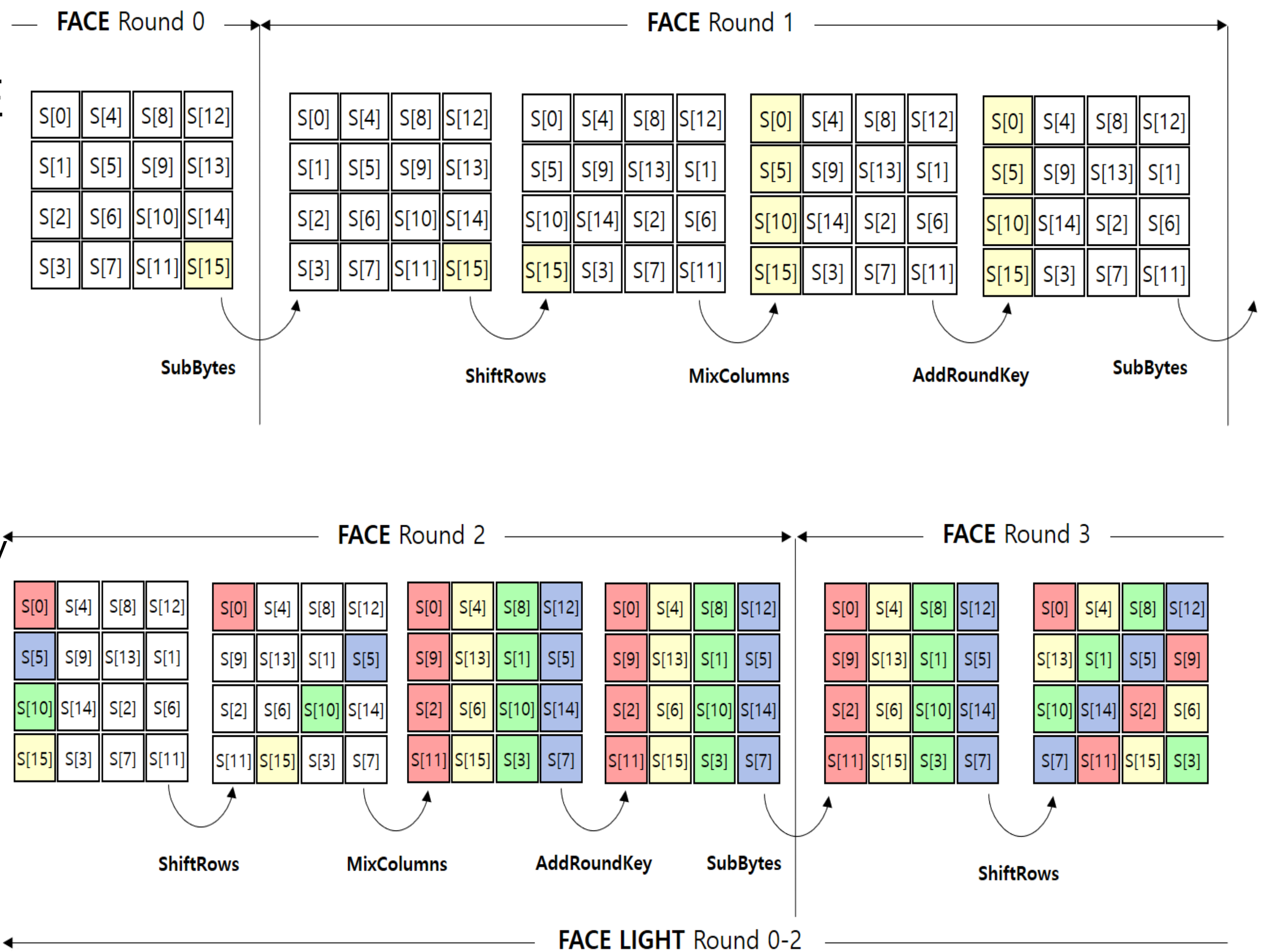


Fig 9. FACE-LIGHT Look Up Table

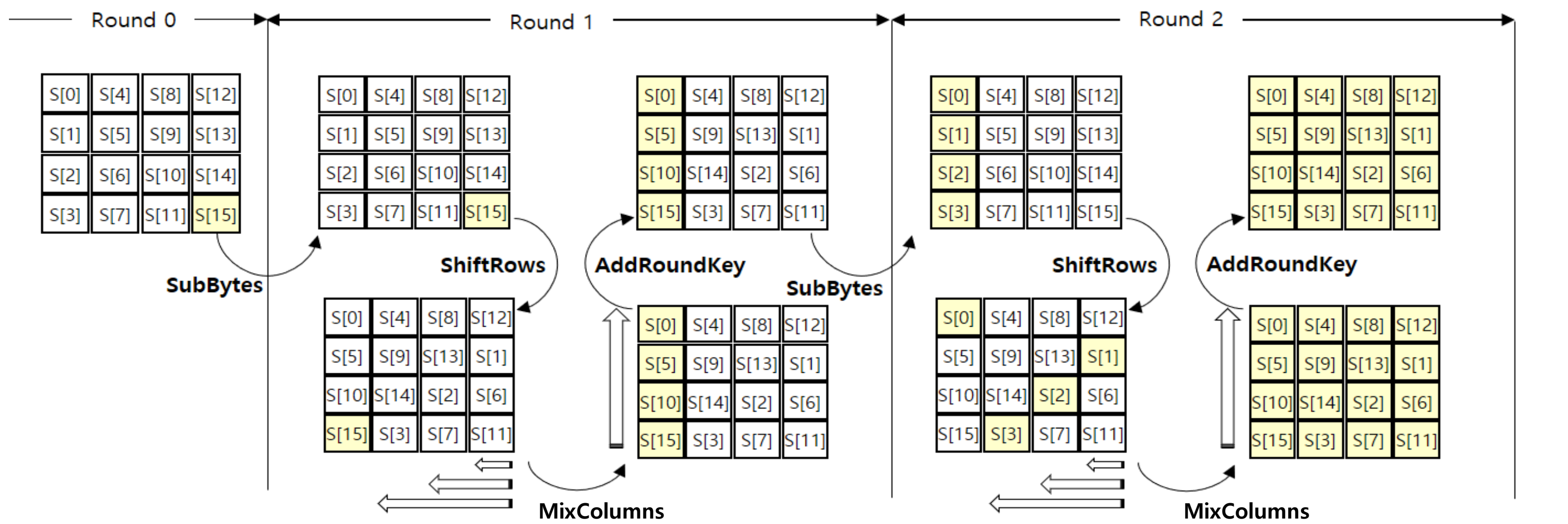

Round 0
Round 1
Round 2
After 256st Block:
SubBytes
ShiftRows
AddRoundKey
SubBytes
ShiftRows
MixCoulmns
AddRoundKey
MixCoulmns
: Identical Part
: Different Part
: Completely Different Part

Extended FACE

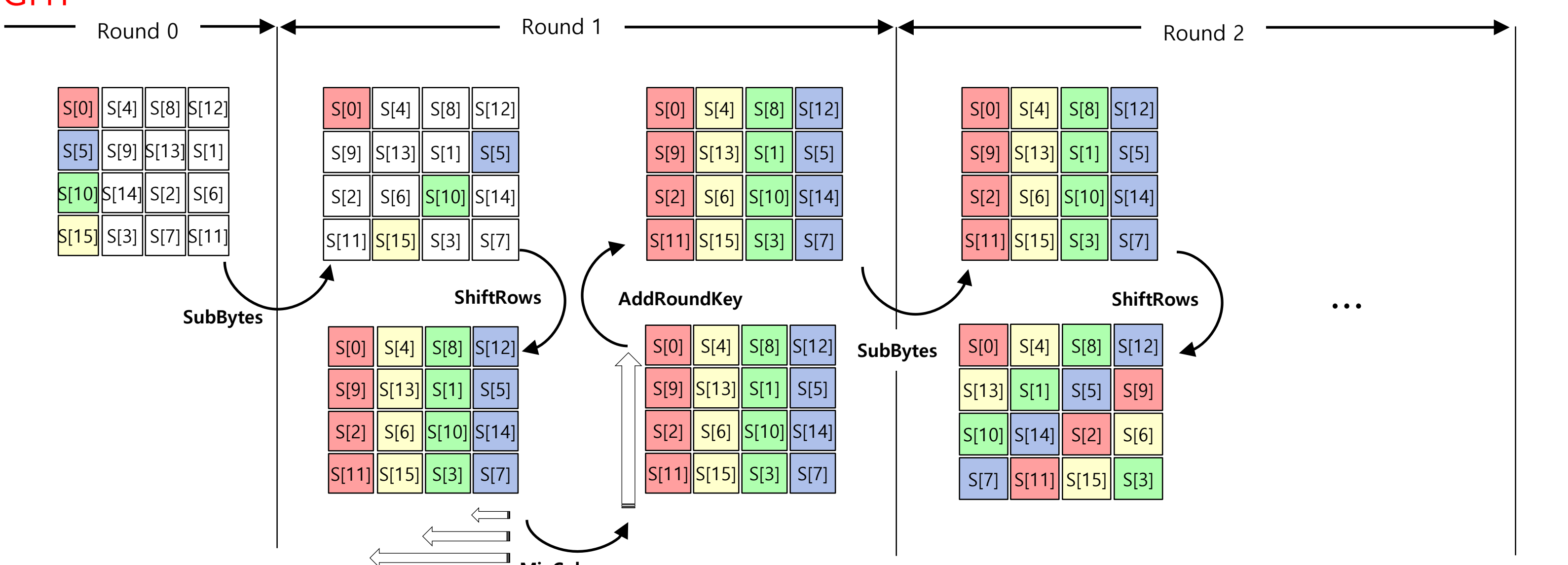
- Extended FACE
  - Original FACE
  - FACE-Light
- Operation reduction
  - Subbytes
  - AddRoundKey

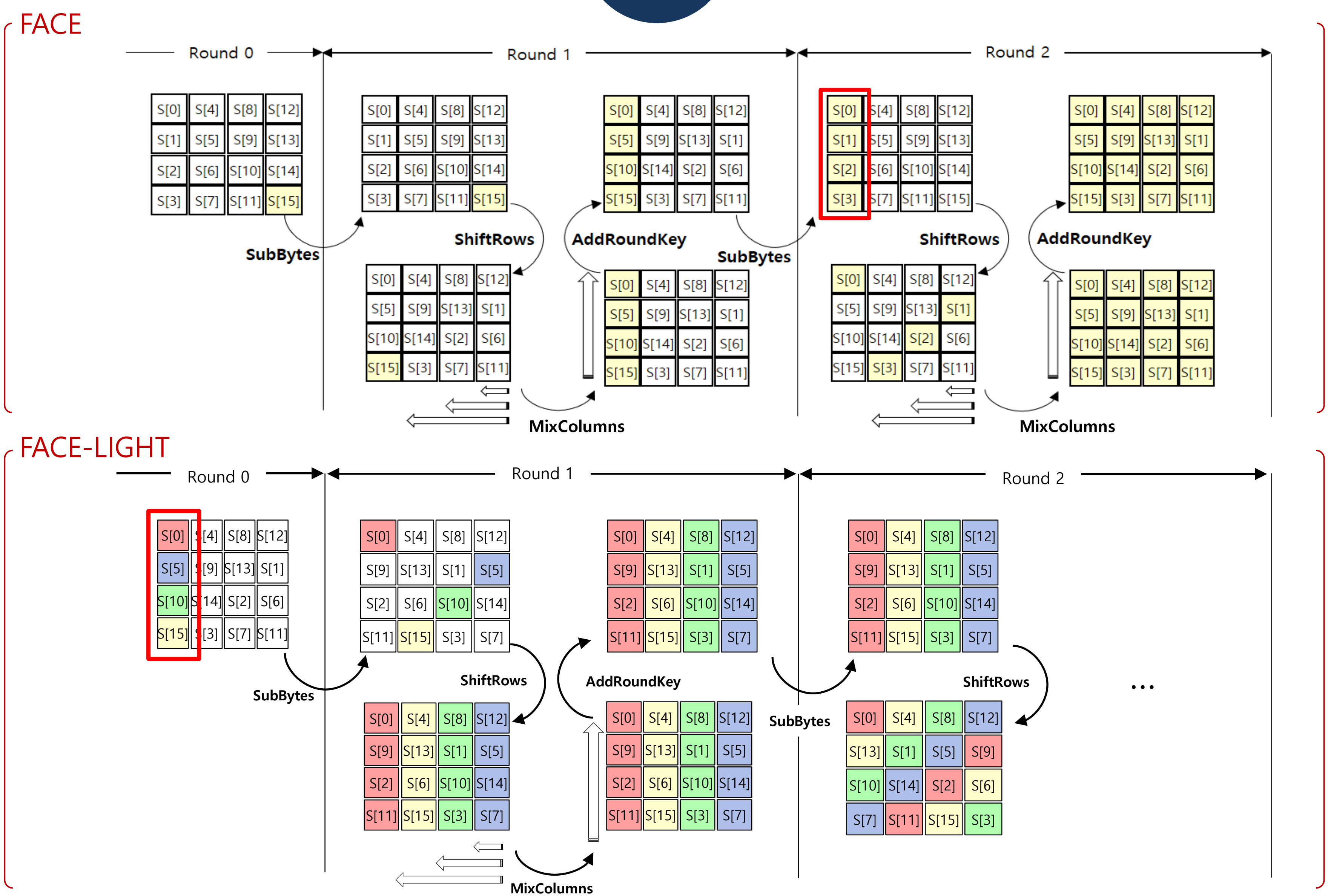


FACE

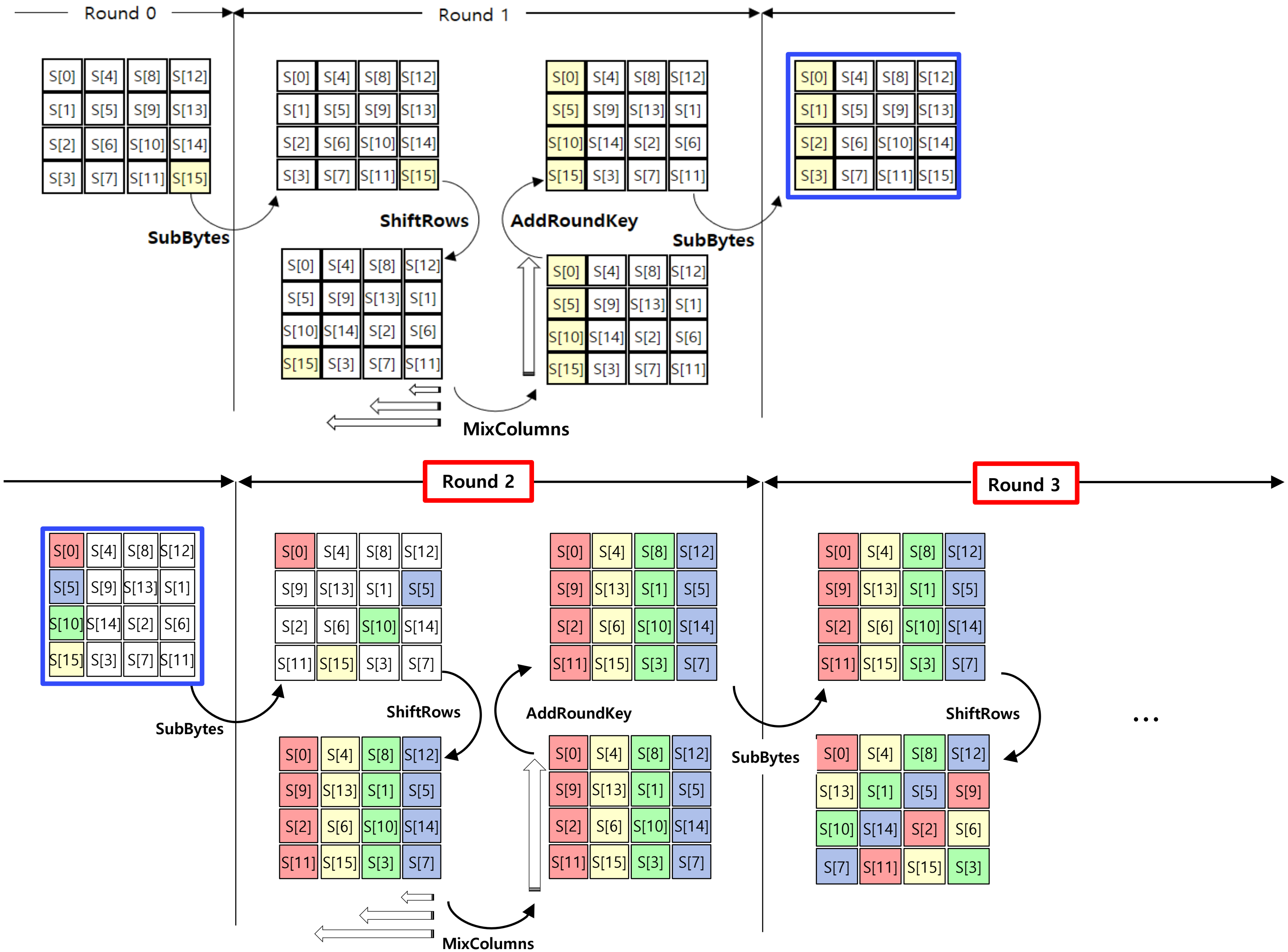


FACE-LIGHT




FACE
Round 0
Round 1
Round 2
SubBytes
ShiftRows
AddRoundKey
SubBytes
ShiftRows
AddRoundKey
MixColumns
MixColumns
FACE-LIGHT
Round 0
Round 1
Round 2
SubBytes
ShiftRows
AddRoundKey
SubBytes
ShiftRows
MixColumns
...

Extended FACE



Evaluation (Calculating Speed)

- **22% performance improvement** over standard AES
- No additional LUT update time required

Unit: Clock Cycles

Security Level	Dinu et al. *	Otte et al. **	FACE-Light (Our Work)	Ex-FACE (Our Work)
AES-128	2,835	2,507	**2,218**	**1,967**
AES-192	N/A	2,991	**2,702**	**2,449**
AES-256	N/A	3,473	**3,184**	**2,931**

Table 1. Comparison of calculating speed

* D. Dinu, A. Biryukov,"FELICS–fair evaluation of lightweight cryptographic systems," inNIST, 2015.
** D. Otteet al., "AVR-crypto-lib,"Online: http://www. das–labor. org/wiki/AVR–Crypto–Lib/en, 2009.

Evaluation (vs FACE)

- Optimized for FACE-LIGHT **8bits Microcontroller**
- Support Constant Timing(No need to LUT update)
- 8bits low-power processor available without restrictions

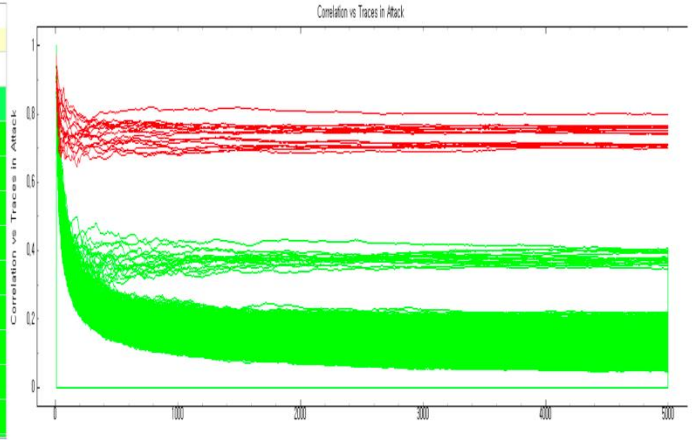
	FACE	FACE-LIGHT (Our Work)
Table Update	O	**X**
Constant Timing	Not Support	**Support**
Target Processor	32-bits or above	**8-bits or above**
Expandable Round	Round 2	**Round 3**

Table 2. Comparison with original FACE

Evaluation (Side Channel Attack Resistance)

- **Resistant** to power analysis attacks (CPA, DPA)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	2B 0.7013	7E 0.7601	15 0.7126	16 0.7651	28 0.7064	AE 0.7453	D2 0.7093	A6 0.7518	AB 0.7095	F7 0.7581	15 0.7409	88 0.7640	09 0.7067	CF 0.7530	4F 0.7115	3C 0.7998
1	2A 0.3791	7F 0.3795	14 0.3778	17 0.3984	29 0.3711	AF 0.3961	D3 0.3647	A7 0.3987	AA 0.3669	F6 0.4060	14 0.3464	89 0.3737	08 0.3563	CE 0.3780	4E 0.3653	3D 0.3930
2	24 0.1953	9A 0.2181	83 0.2100	E3 0.2041	DC 0.1975	4A 0.2078	A7 0.2149	99 0.1848	5E 0.1874	13 0.2106	BF 0.1899	BD 0.1909	81 0.1851	B4 0.1993	F5 0.2012	E1 0.1954
3	FB 0.1948	4B 0.2059	1E 0.2012	38 0.1840	82 0.1939	C3 0.1845	60 0.2144	53 0.1823	3F 0.1819	8C 0.1918	7E 0.1888	FD 0.1892	91 0.1844	3A 0.1939	B1 0.2003	21 0.1892
4	20 0.1947	0B 0.2035	E5 0.1889	29 0.1821	47 0.1927	D5 0.1730	F9 0.2119	75 0.1794	97 0.1780	02 0.1888	81 0.1811	33 0.1793	9D 0.1778	2B 0.1919	F7 0.1971	81 0.1878
5	DB 0.1881	8B 0.1896	A1 0.1879	E5 0.1780	9C 0.1890	9B 0.1719	FD 0.2074	8C 0.1770	EE 0.1767	C2 0.1817	8C 0.1783	9E 0.1782	D1 0.1724	F0 0.1833	0C 0.1935	C9 0.1790
6	06 0.1844	68 0.1885	E0 0.1864	5C 0.1769	D8 0.1830	5B 0.1696	D9 0.2046	DA 0.1668	01 0.1747	E4 0.1671	7A 0.1740	7D 0.1775	99 0.1696	05 0.1765	BD 0.1857	96 0.1765
7	9F 0.1825	41 0.1845	5A 0.1864	36 0.1760	98 0.1783	E0 0.1674	64 0.1995	6C 0.1657	32 0.1719	C8 0.1634	56 0.1722	B7 0.1725	A7 0.1688	12 0.1630	83 0.1816	02 0.1746
8	46 0.1791	75 0.1766	7E 0.1858	C6 0.1738	45 0.1778	5F 0.1671	20 0.1971	93 0.1644	28 0.1699	9A 0.1616	5A 0.1711	AE 0.1668	D4 0.1677	A2 0.1604	B9 0.1813	09 0.1713
9	F6 0.1756	6D 0.1747	5E 0.1858	18 0.1722	63 0.1766	BD 0.1663	42 0.1966	3A 0.1643	33 0.1692	CA 0.1608	C8 0.1704	58 0.1608	B9 0.1672	DC 0.1599	F9 0.1811	40 0.1712
10	64 0.1754	C6 0.1725	A3 0.1783	A5 0.1697	03 0.1756	90 0.1661	87 0.1952	51 0.1642	1B 0.1667	3D 0.1591	3D 0.1704	83 0.1607	35 0.1662	0C 0.1580	40 0.1808	49 0.1706



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE	201	87	49	195	145	140	231	80	238	146	220	216	29	249	86	151
0	42 0.0727	B4 0.0755	B8 0.0690	EF 0.0692	51 0.0683	69 0.0685	55 0.0728	7F 0.0686	7B 0.0773	CB 0.0727	78 0.0672	1D 0.0729	D8 0.0696	F6 0.0689	E2 0.0691	73 0.0720
1	20 0.0704	60 0.0679	48 0.0682	CF 0.0687	B3 0.0680	C1 0.0682	0F 0.0697	CB 0.0673	DF 0.0705	B5 0.0699	1E 0.0643	B9 0.0723	C1 0.0676	A1 0.0673	9C 0.0682	43 0.0704
2	F0 0.0695	1E 0.0649	CE 0.0680	A0 0.0676	B7 0.0679	7E 0.0647	06 0.0689	EB 0.0665	96 0.0652	22 0.0676	44 0.0642	0E 0.0686	0C 0.0664	AA 0.0666	01 0.0676	B6 0.0701
3	19 0.0682	44 0.0648	E5 0.0679	25 0.0676	A1 0.0672	99 0.0644	4A 0.0669	34 0.0658	06 0.0651	17 0.0643	C5 0.0638	85 0.0671	E6 0.0663	89 0.0647	39 0.0672	24 0.0686
4	2F 0.0680	84 0.0646	7A 0.0663	92 0.0672	4F 0.0671	D9 0.0634	60 0.0669	FA 0.0645	EE 0.0645	7D 0.0641	1F 0.0636	21 0.0667	7B 0.0645	65 0.0639	F9 0.0666	D3 0.0686
5	44 0.0675	D4 0.0640	FF 0.0660	D4 0.0665	82 0.0670	D2 0.0633	C2 0.0655	A7 0.0640	8E 0.0639	EE 0.0638	DA 0.0635	3D 0.0667	BE 0.0644	5D 0.0636	86 0.0655	B7 0.0681
6	57 0.0674	2B 0.0636	7E 0.0654	84 0.0657	E4 0.0648	49 0.0623	13 0.0640	05 0.0638	70 0.0630	2A 0.0629	2B 0.0627	73 0.0657	41 0.0638	74 0.0634	92 0.0651	EE 0.0662
7	17 0.0665	7B 0.0635	57 0.0634	B0 0.0654	BD 0.0645	45 0.0621	93 0.0638	1E 0.0627	1B 0.0627	37 0.0628	46 0.0627	3E 0.0650	CC 0.0635	51 0.0630	D3 0.0645	C3 0.0662
8	C3 0.0661	63 0.0629	FC 0.0627	71 0.0638	75 0.0644	6F 0.0618	63 0.0635	AF 0.0625	94 0.0624	00 0.0623	E5 0.0626	EF 0.0649	A1 0.0632	B9 0.0629	F6 0.0642	D6 0.0661
9	79 0.0659	96 0.0626	9A 0.0620	C5 0.0632	21 0.0643	6C 0.0618	BB 0.0631	AB 0.0624	17 0.0624	C2 0.0615	FA 0.0620	47 0.0640	9D 0.0629	CD 0.0629	FE 0.0635	BF 0.0647
10	0D 0.0627	5F 0.0623	D3 0.0619	F4 0.0631	48 0.0640	C9 0.0618	9E 0.0628	DA 0.0619	AD 0.0616	AA 0.0615	D0 0.0620	B1 0.0638	34 0.0627	01 0.0628	E3 0.0630	A7 0.0646

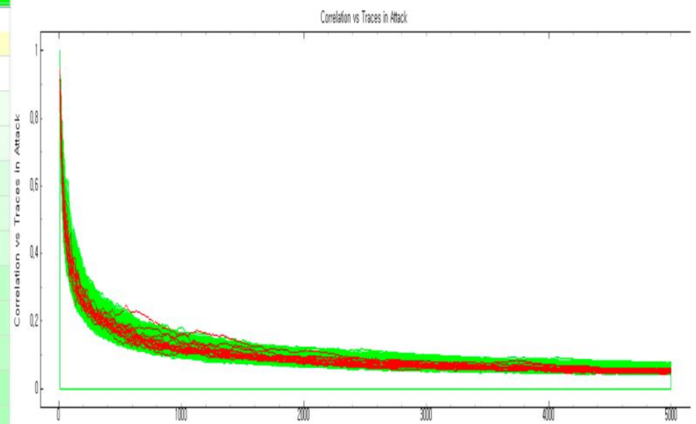


Fig 10. Graph of Power Analysis

Evaluation (vs LEA)

- **Better performance** compared to Masked LEA using ARX operation
- Improved performance over previous Masked AES
  - **FACE-LIGHT, software optimization**

Unit: Clock Cycles

LEA-128 *	Masked LEA-128 **	Masked AES-128 (Previous Work)***	Masked FACE-128 (Our Work)
2,688	36,589	25,970	**6,219**

Table 3. Comparison with LEA and Previous Work

* H. Seo, I. Jeong, J. Lee, and W. Kim, "Compact implementations of ARX-based block ciphers on IoT processors," ACM TECS, 2018.
** E. Park, S. Oh, and J. Ha, "Masking-based block cipher LEA resistant to side channel attacks," KIISC, 2017.
*** K. H. Kim, H. J. Seo, "Implementation of Optimized 1st-Order Masking AES Algorithm Against Side-Channel-analysis," KIPS, 2019.

04

Conclusion

F A C E - L I G H T

Contribution

- Effective optimization of AES-CTR on low-power processor
  - Clock Cycles optimization
- More Rounds are expandable than FACE
- Difficult in predicting attack points(Timing being constant)
- Masking operation to counter a side channel attack
- Lightweight AES

Future Work

- Optimization on various platforms
  - 16bits MSP … ETC
- Optimize other domestic cryptography using our proposal
  - Pre-calculation of LUT
  - Side channel attack resistant
  - Software optimization
- Apply proposed methods to AES modes
  - AES GCM

Fig 11. MSP430FR2433 LaunchPad kit

THANK YOU

pgm.kkh@gmail.com