Strategy and Synergy for Security

Hardware Architecture of Efficient Crypto Engine

Presented by

Sarvesh K

Project Associate,

SETS Chennai.

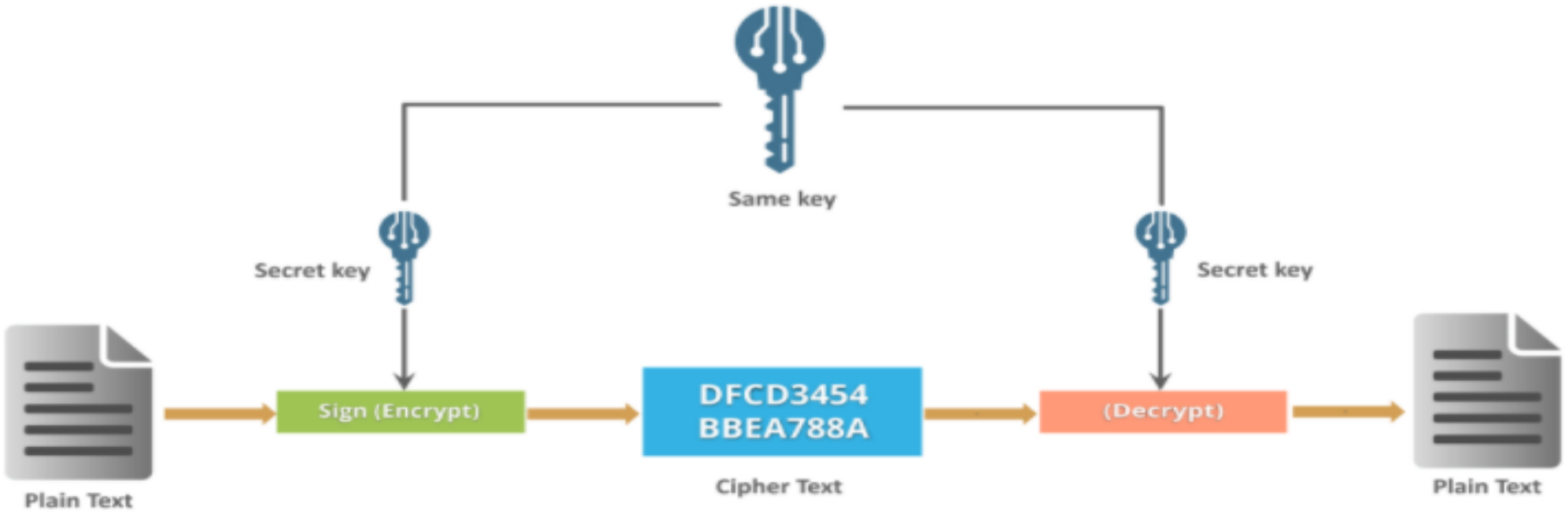
sarvesh@setsindia.net

Introduction

- Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.
- Classified into
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography

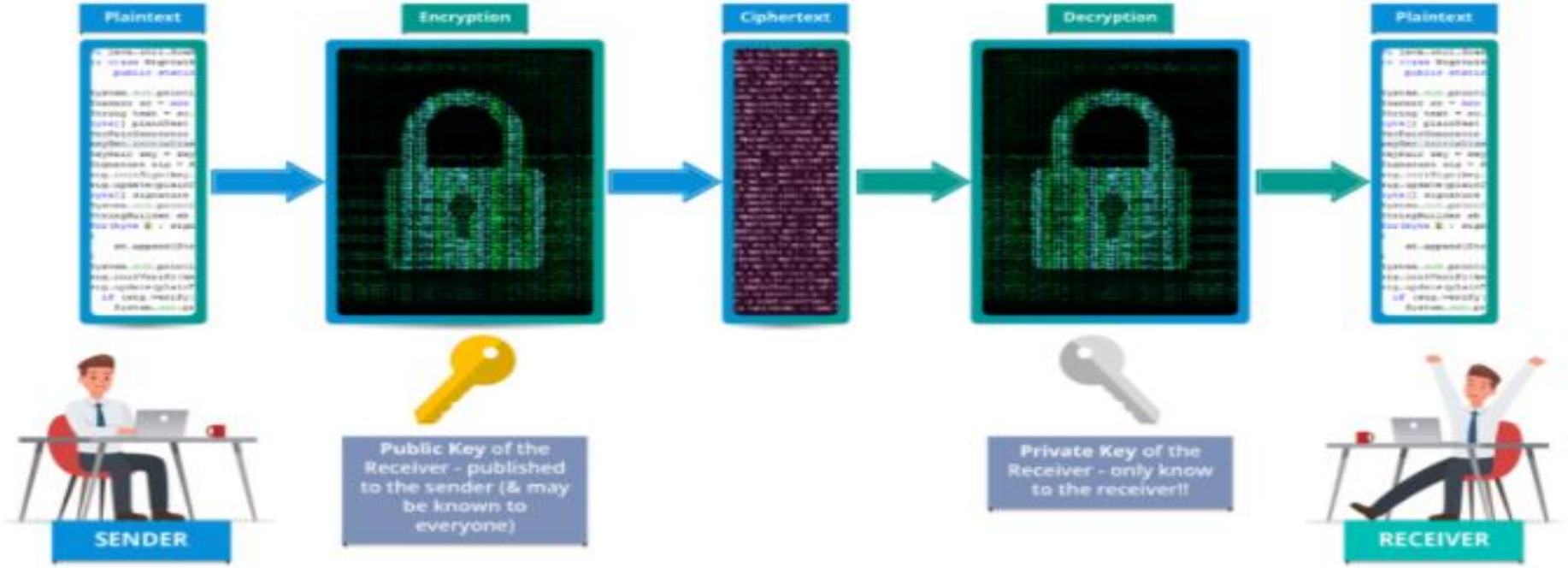
Symmetric Key Cryptography

- An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message



Asymmetric Key Cryptography

- The encryption process where different keys are used for encrypting and decrypting the information. Keys are different but are mathematically related, such that retrieving the plain text by decrypting ciphertext is feasible



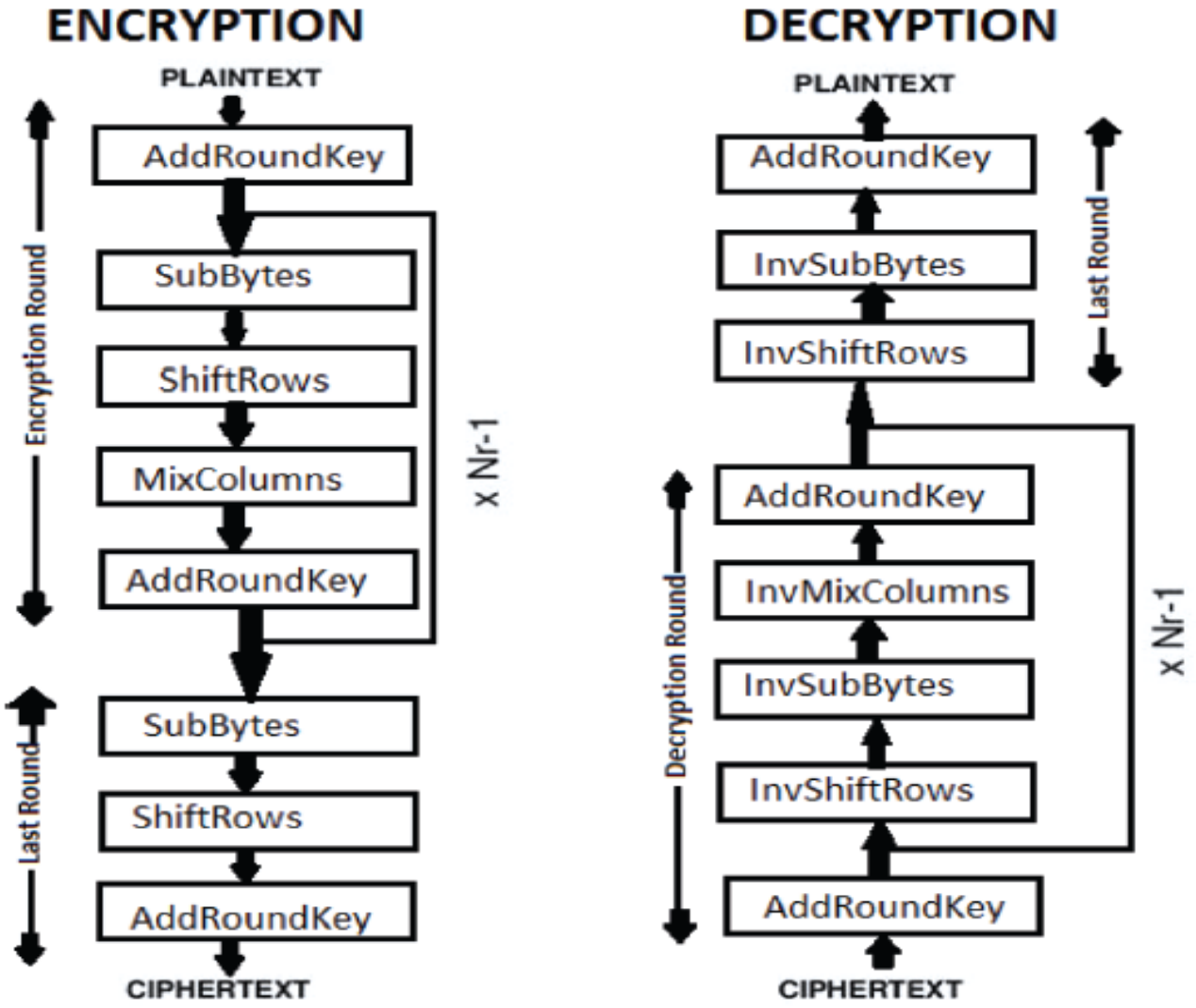
Advanced Encryption Standard (AES)

- Original name **Rijndael**
- Specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001
- 128-bit data, 128/192/256-bit keys

Why AES ?

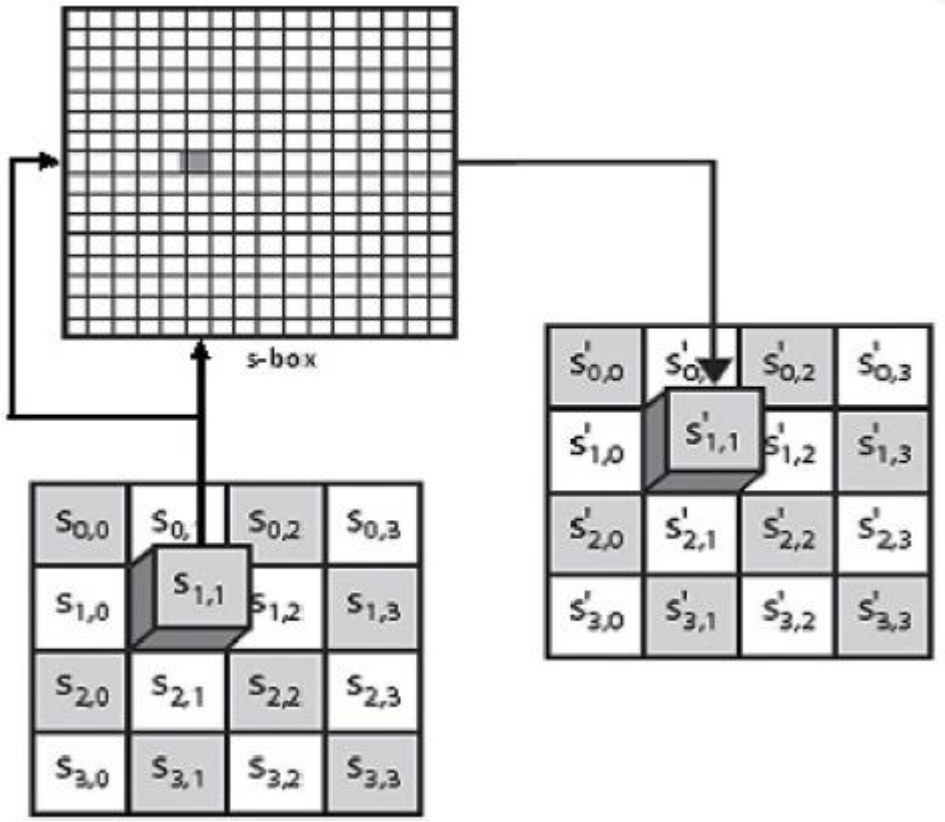
- A replacement for DES was needed as its key size was too small, considered vulnerable against exhaustive key search attack
- It is found at least six time faster than triple DES
- Triple DES was designed to overcome this drawback but it was found slow

AES Algorithm

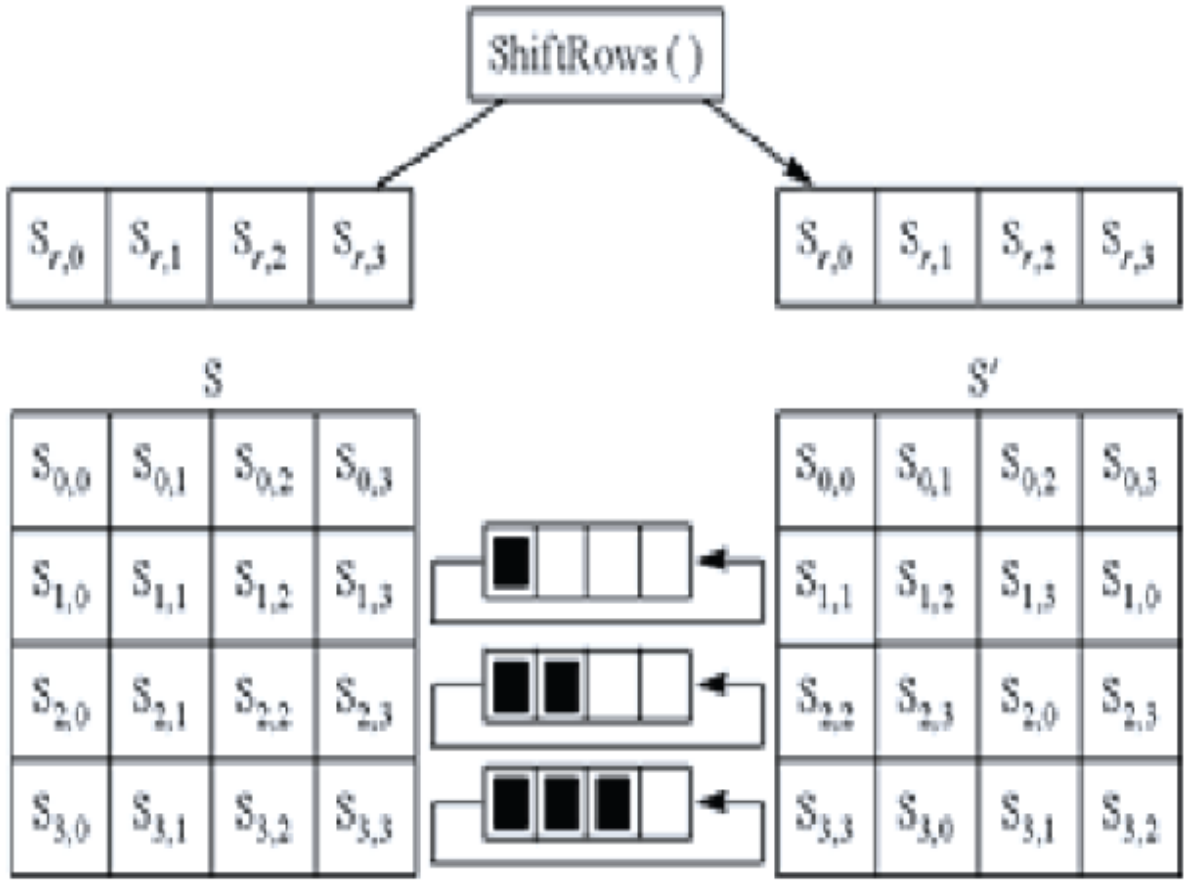


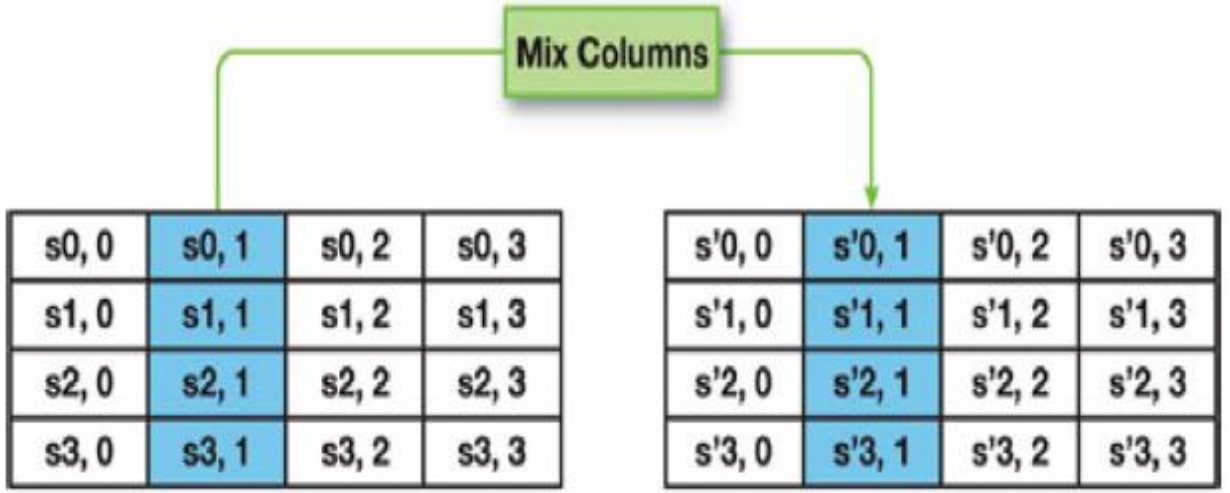
Sub-Bytes Transformation

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16



Shift rows & Mix Column

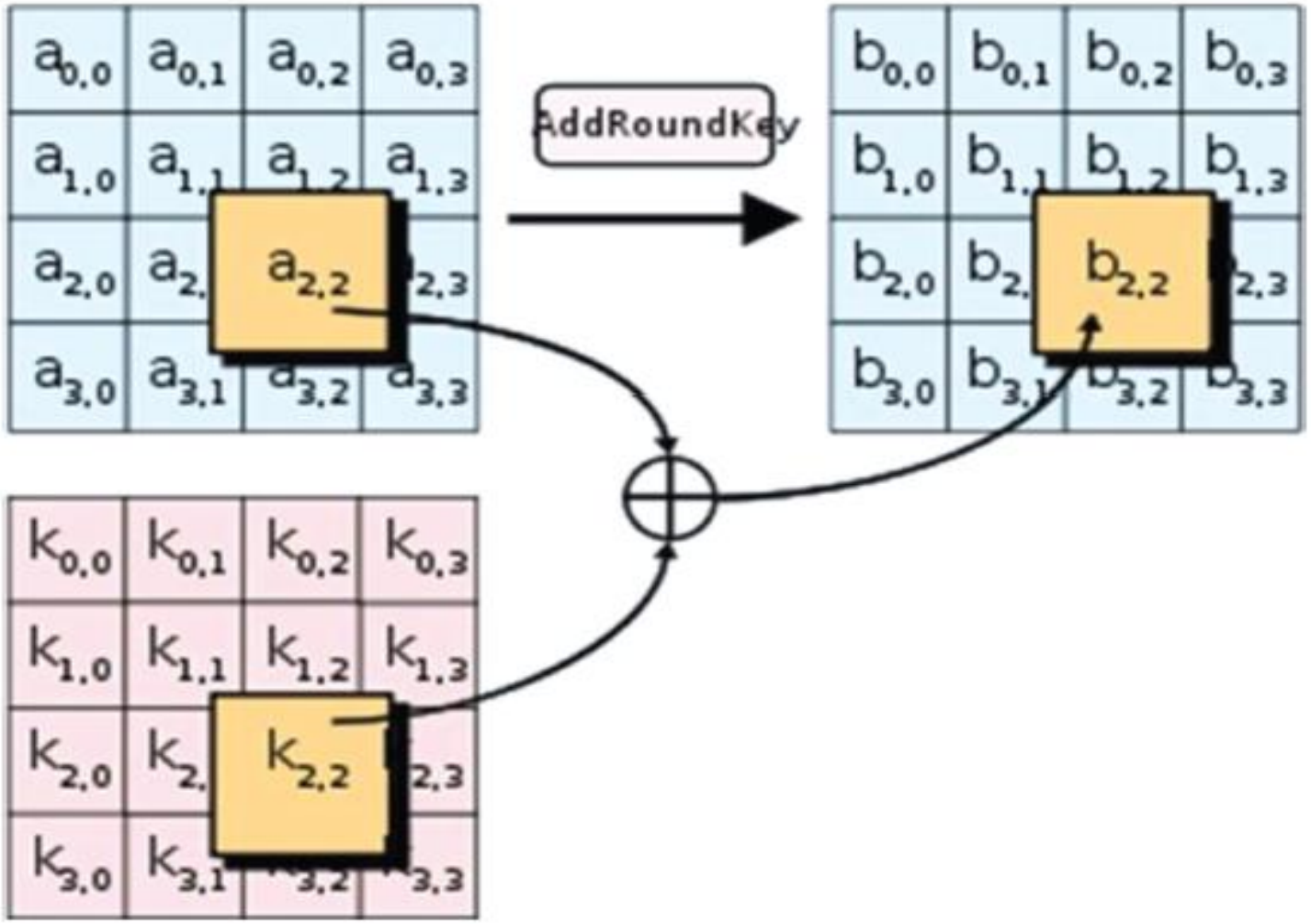




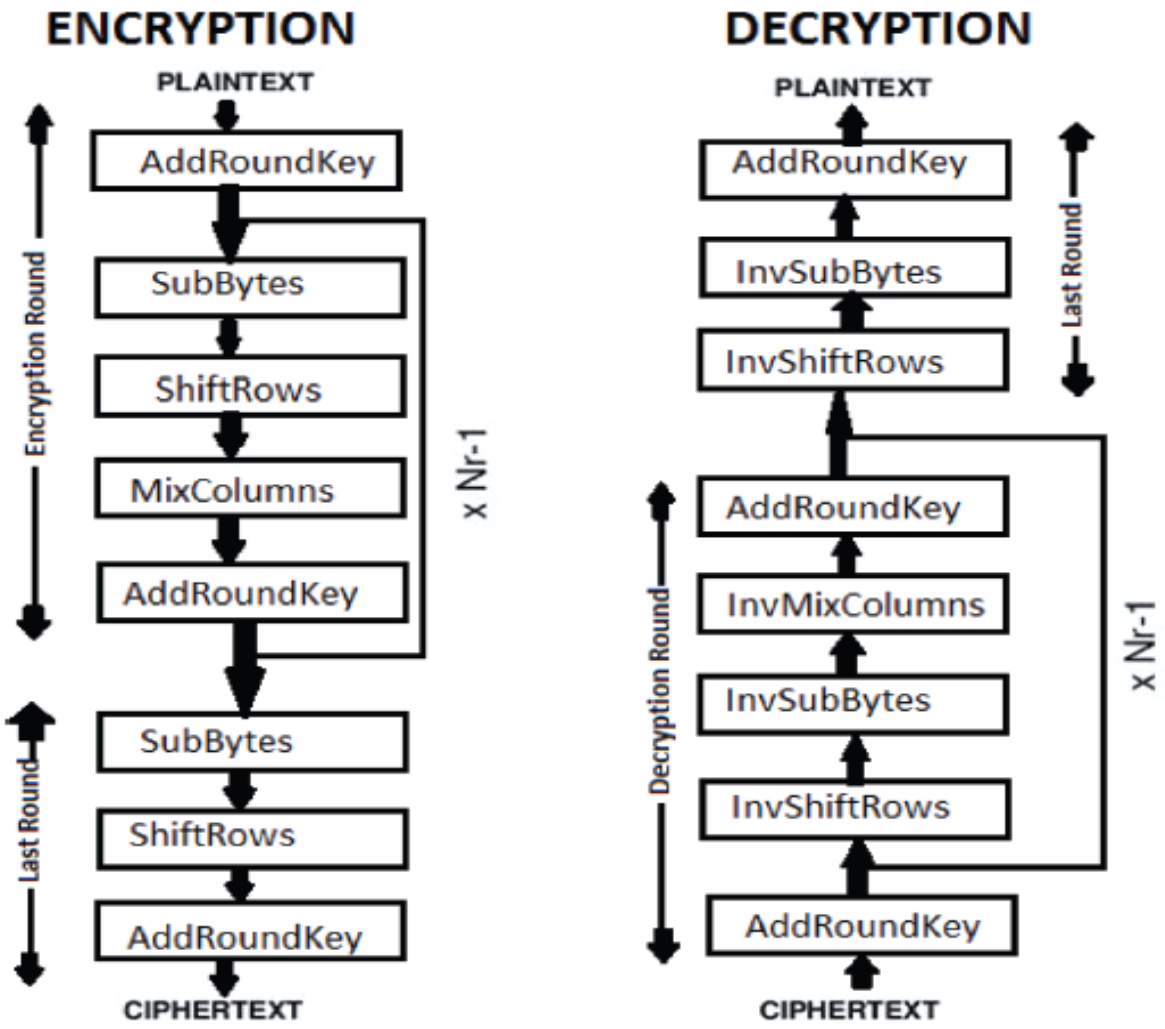
$$\begin{pmatrix} s'0,1 \\ s'1,1 \\ s'2,1 \\ s'3,1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} s0,1 \\ s1,1 \\ s2,1 \\ s3,1 \end{pmatrix}$$

Transform Matrix of Mix Columns

Add Round Key



Decryption


ENCRYPTION
PLAINTEXT
AddRoundKey
SubBytes
ShiftRows
MixColumns
AddRoundKey
SubBytes
ShiftRows
AddRoundKey
CIPHERTEXT
Encryption Round
Last Round
x Nr-1
DECRYPTION
PLAINTEXT
AddRoundKey
InvSubBytes
InvShiftRows
AddRoundKey
InvMixColumns
InvSubBytes
InvShiftRows
AddRoundKey
CIPHERTEXT
Last Round
Decryption Round
x Nr-1

Efficient implementation of AES

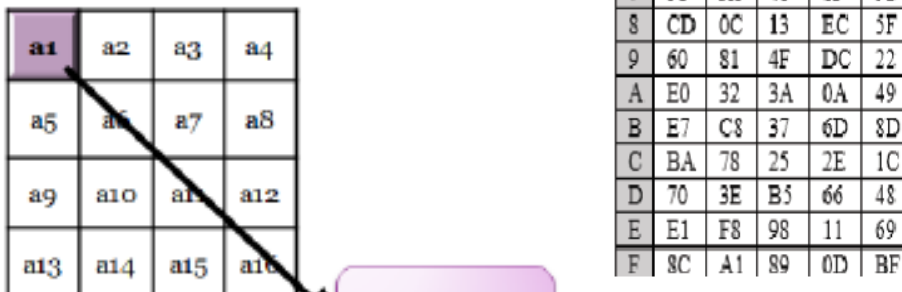
- Component and gate level optimization
  - Parallel S-Box implementation
  - Gate level reductions

- Architectural level optimization
  - Pipelined architecture
  - Unrolling architecture
  - Bit Serial architecture

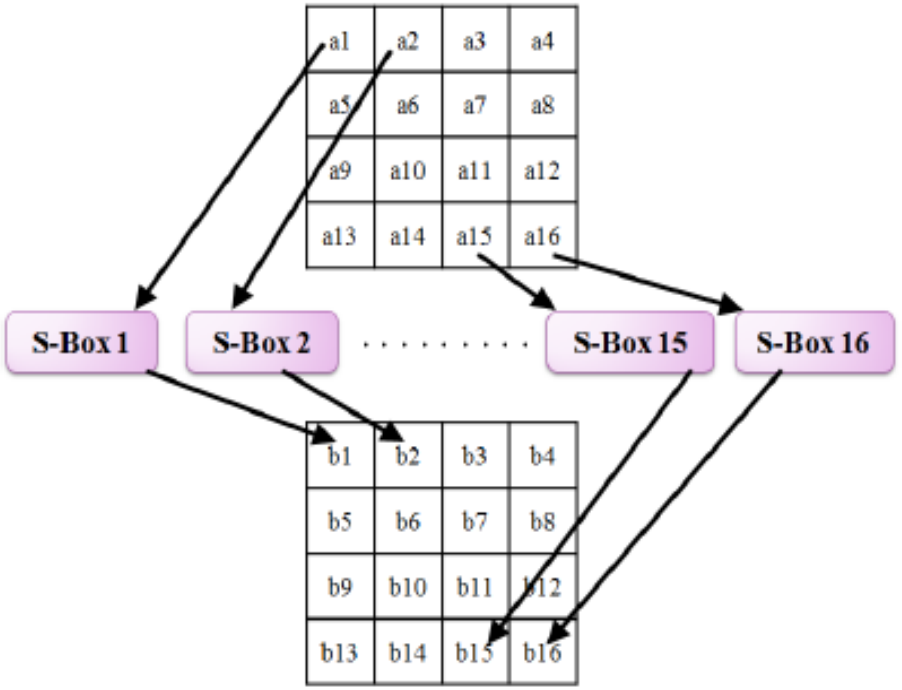
Component and Gate level Optimization

A Highly Parallel Area Efficient S-Box Implementation

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

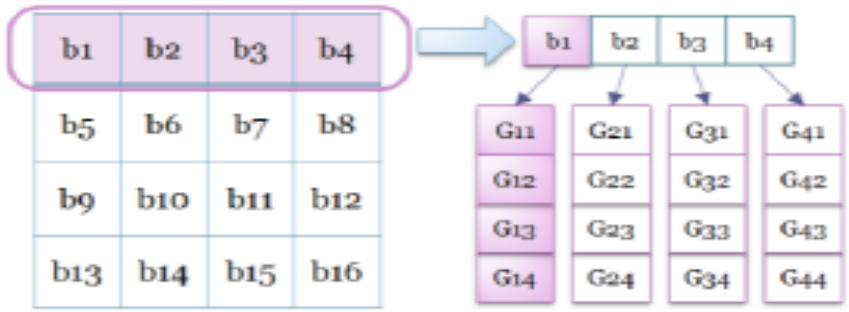


(a) Totally serial s-box architecture.

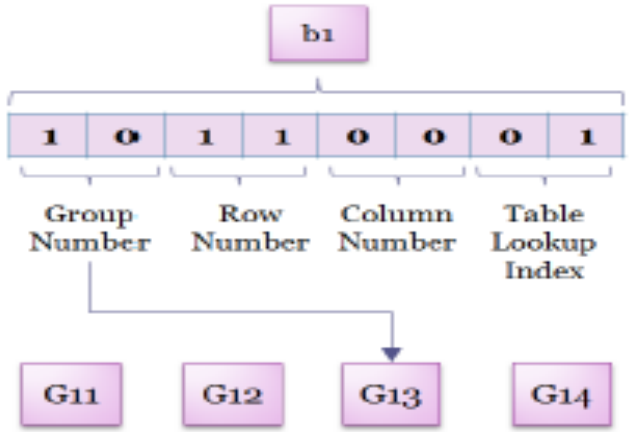


(b) Totally parallel s-box architecture

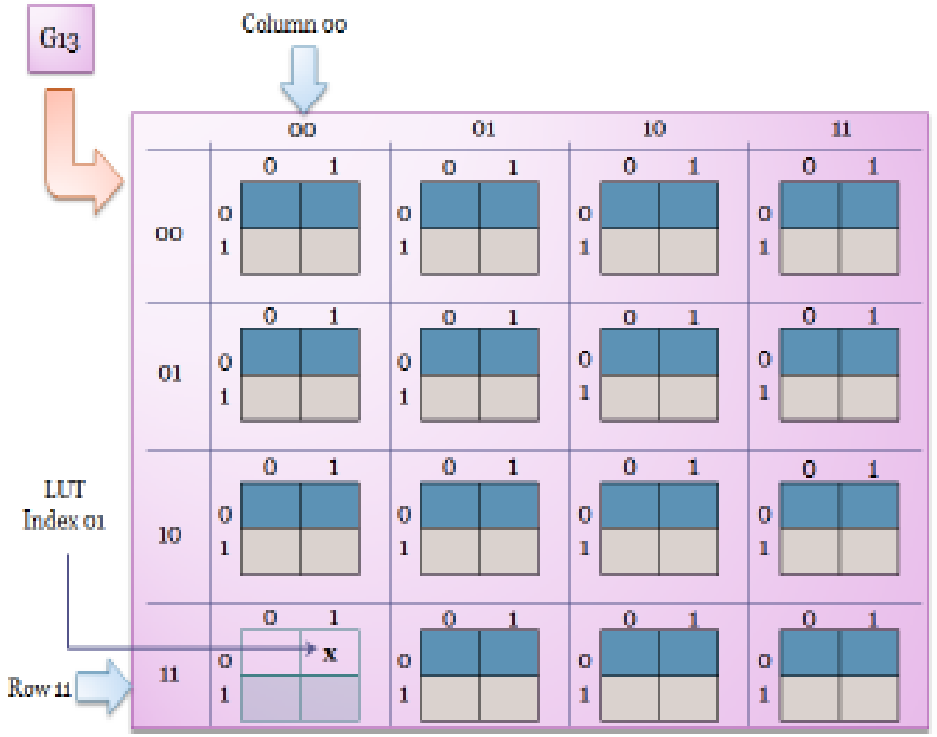
Proposed S-box



(a) The first four bytes of a given state are processed.



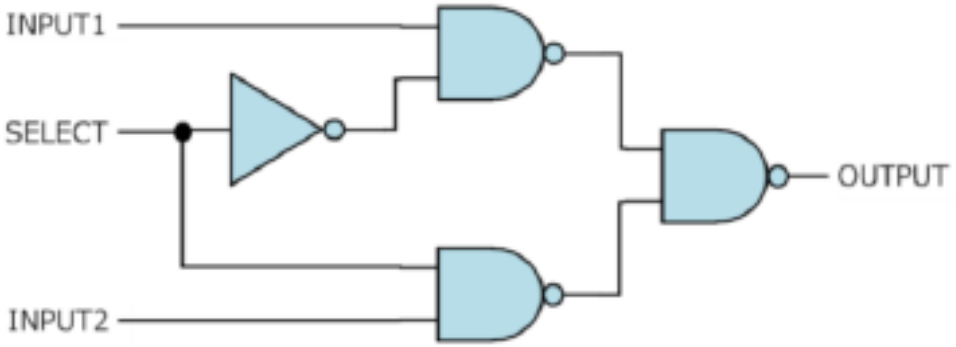
(b) Selecting a group.



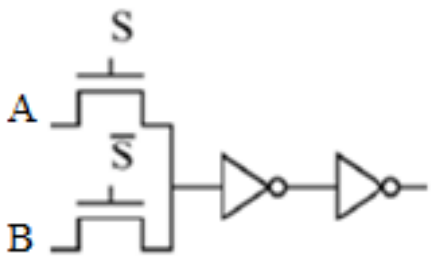
(c) Identifying the row, the column, and the LUT containing the substitution value

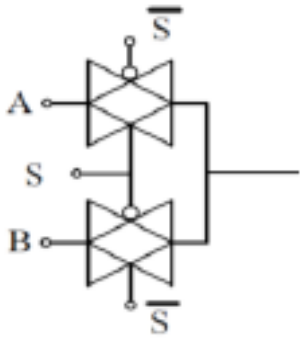
- Simplifies S-box
- Reduced Power Consumption

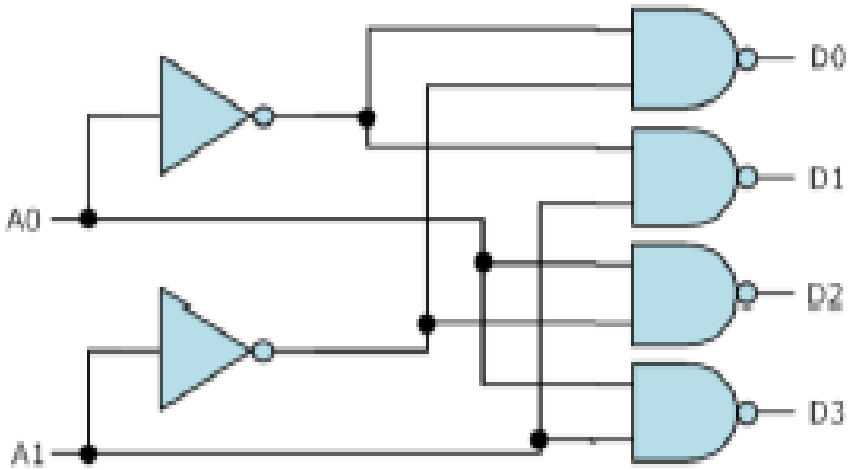
Gate level reductions



(c) NAND-based realization of 2-to-1 MUX.







LUT Implementation VS Proposed implementation

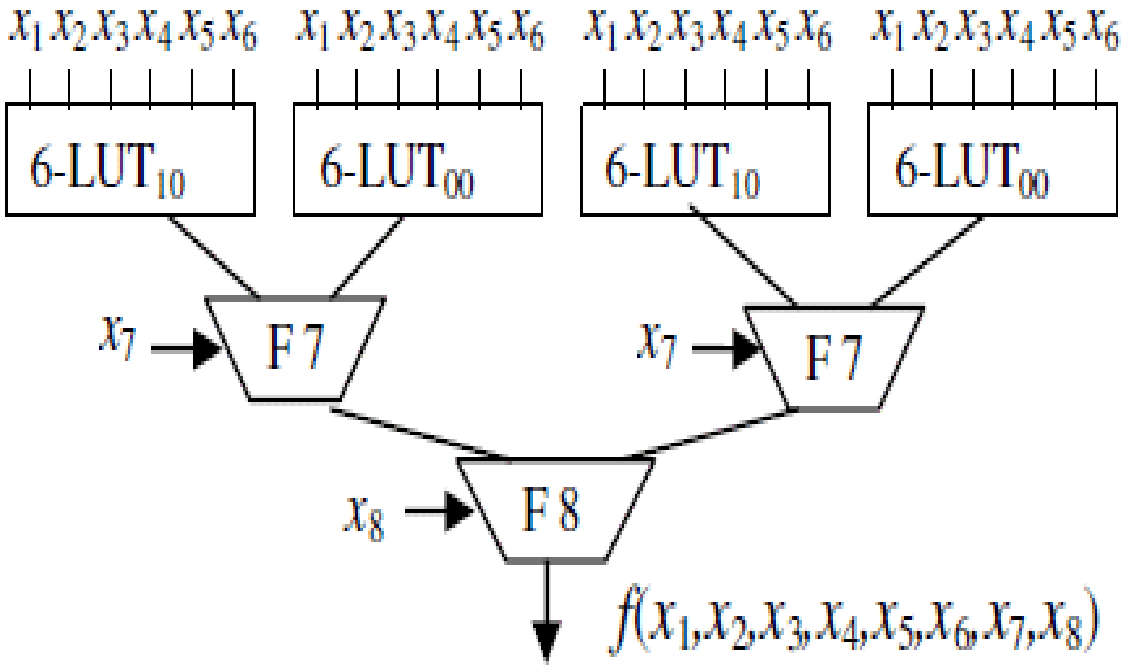
Implementation	First Proposed Solution (NAND)	Second Proposed Solution (Pass Transistor)	Third Proposed Solution (Transmission Gate)
Decoders Delay (ns)	1.6	1.6	1.6
Multiplexers Delay (ns)	2.4	2	0.8
Total Delay (ns)	**4**	**3.6**	**2.4**
Decoders Area (GE)	72	72	72
Multiplexers Area (GE)	48	42	24
Total Area (GE)	**120**	**114**	**96**

Implementation	Critical Path Delay (ns)	Area (GE)
Satoh [4]	9	360
Wolkerstorfer [11]	8	382.5
Canright [3]	8	281.3
hw_lut [5]	3	1203.8
sub16_lut [5]	4	1912.5
Bertoni [12]	3	1608.8
Our Proposed 1	4	120
Our Proposed 2	3.6	114
Our Proposed 3	2.4	96

Architecture level Optimization

Pipelined Architecture

Pipeline AES S-box Implementation Starting with Substitution Table



Non-Pipelined Architecture

From 00000000 to 00111111 there are no changes in x7 and x8

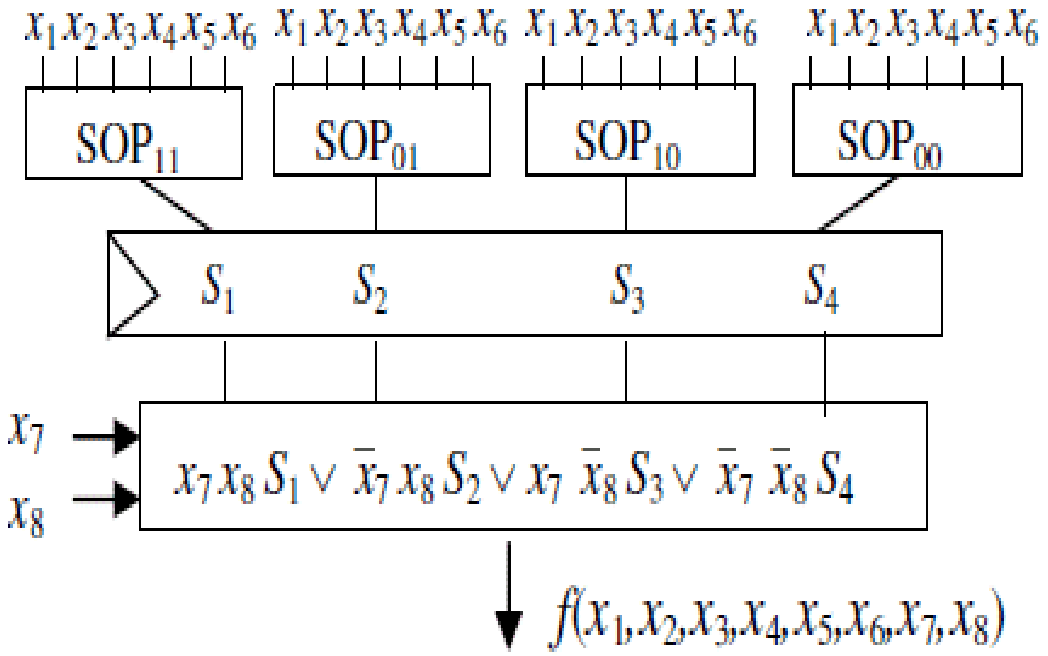
$$f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) =$$

$$= x_8 [\, x_7 \, SOP_{11} \vee \bar{x}_7 \, SOP_{01}] \qquad (1)$$

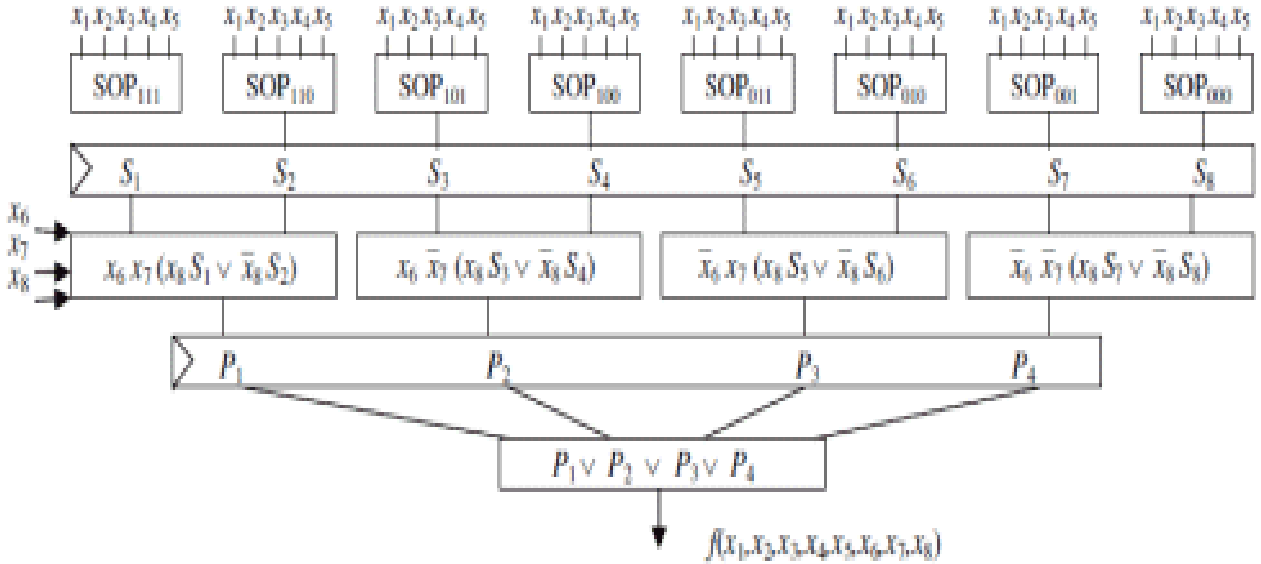
$$\vee \bar{x}_8 [\, x_7 \, SOP_{10} \vee \bar{x}_7 \, SOP_{00}].$$

Break down the initial 256 8 bit look-up-table into the set of smaller look-up tables.

2 stage pipelining & 3 stage pipelining

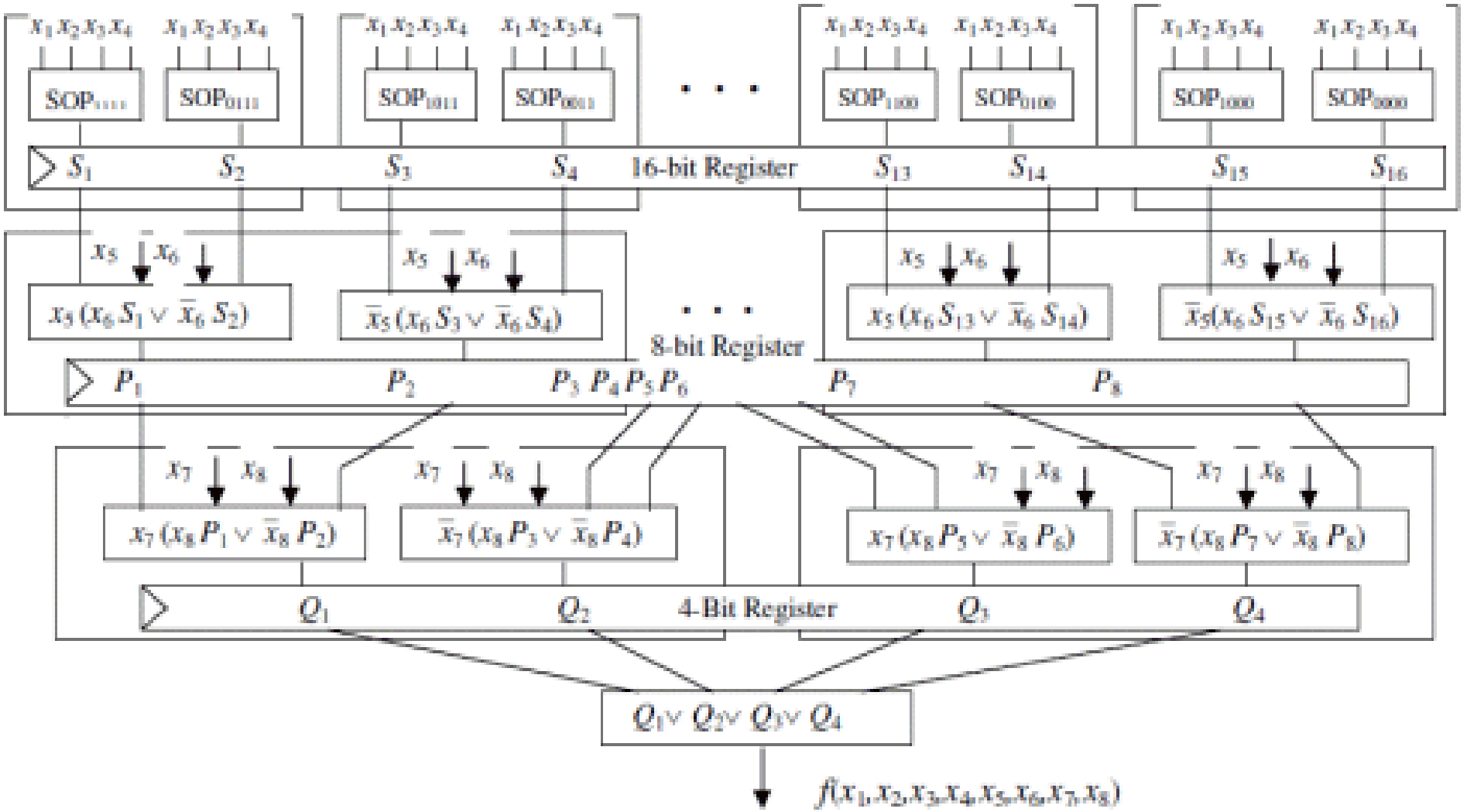


Stage delay of the circuit shown is 68% less than the non-pipelined circuit



Stage delay of the circuit shown is half of the non-pipelined circuit

4 stage pipelining



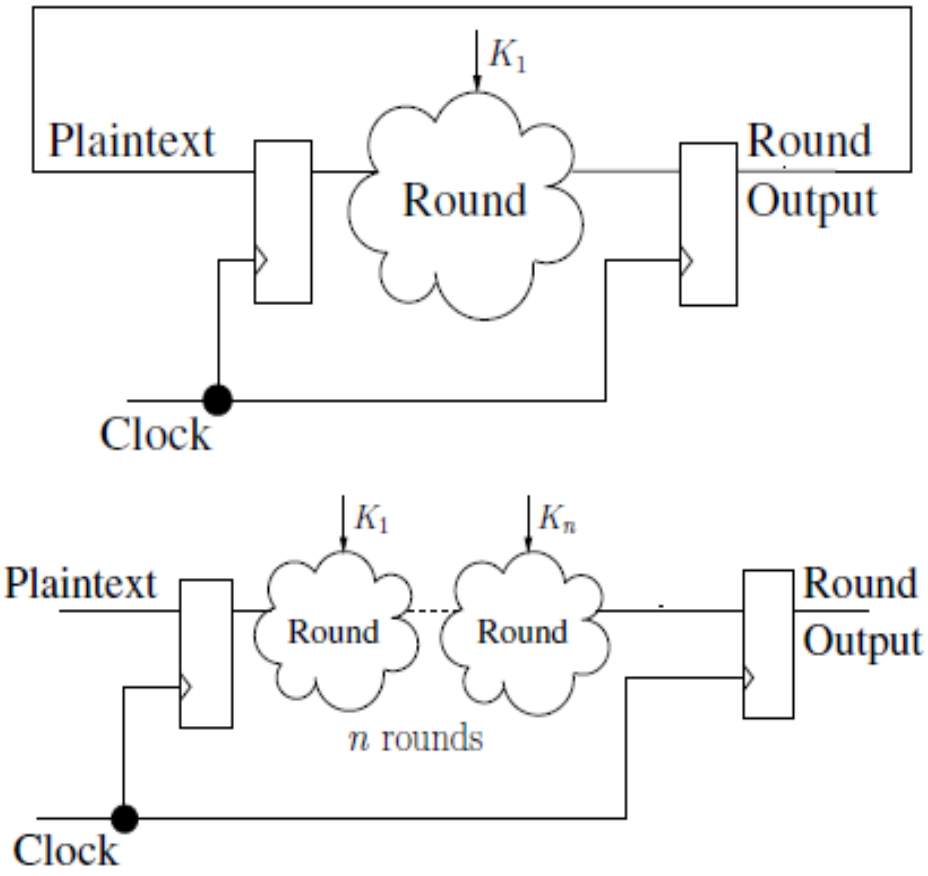
Non-Pipelined VS Pipelined

S-box Architecture (Xilinx Virtex-5, Speed Grade-3)	6-LUTs	Pipeline Registers	Frequency(MHz)	Stage Delay (ns)
Non-pipelined (1-stage)	4 x 8 = 32	0	438.673	2.280
2-stage pipeline	(4 +1) x 8 = 40	4 x 8 + 2* = 34	744.380	1.343
3-stage pipeline	(8+4+1) x 8 = 104	(8+4) x 8+3* = 99	914.746	1.093
(Xilinx Virtex-4, Speed Grade-12)	4-LUTs			
Non-pipelined(1-stage)	16 x 8 = 128	0	425.967	2.348
4-stage pipeline	(16+8+4) = 224	(16+8+4) x 8+6*=230	860.141	1.163

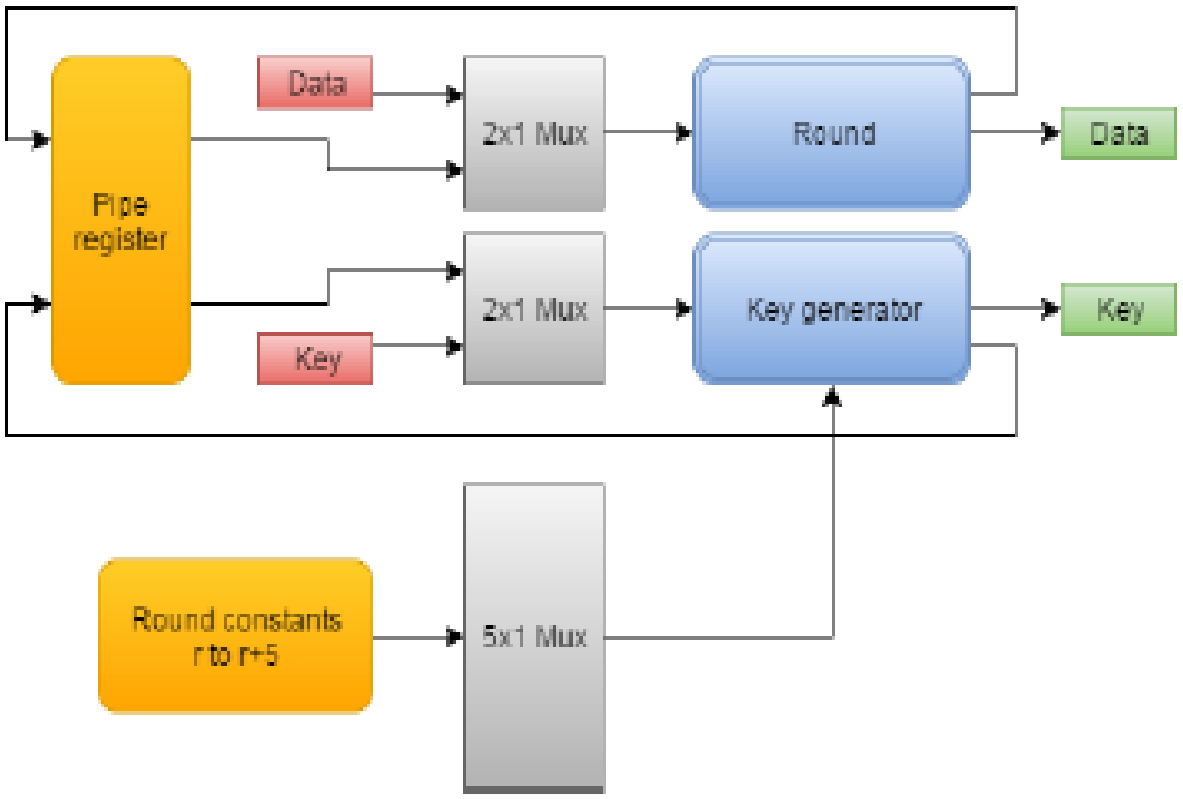
Unrolling Cryptographic Architecture

Unrolling Cryptographic Architecture: A Simple Countermeasure Against Side-Channel Attacks

- Executes multiple rounds in one clock cycle
- Unrolling factor as the number of rounds unrolled



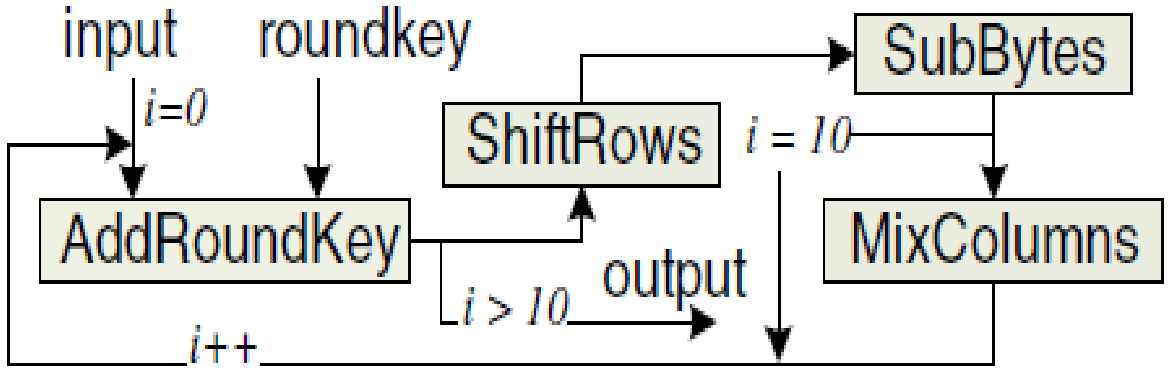
Unrolling Architecture using pipelining registers

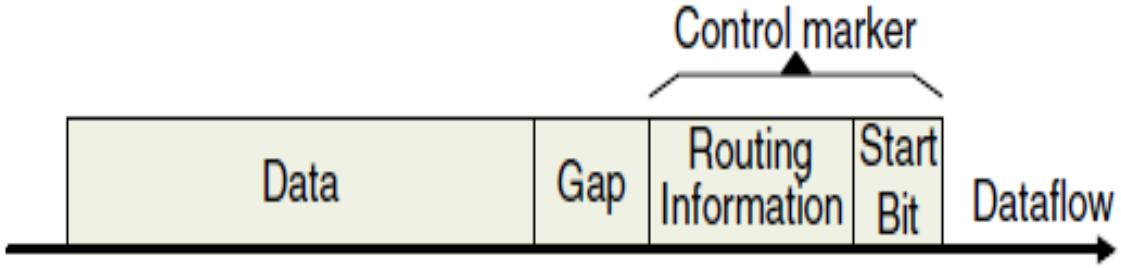


parameter	Design 1	[13]	[4]
Vendor	Xilinx	Xilinx	Xilinx
Device	XC5VLX 50-3	XC5VLX 50-3	XC5VLX 50-3
Slices	521	303	399
Slice LUTs	2490	564	1338
Frequency (MHz)	266.29	425.46	339.1
Throughput (Gbps)	34.08	1.33	4.34
Latency (ns)	45.06	96.35	29.5
Efficiency (Mbps/slice)	65.42	4.389	10.87

Bit Serial Architecture

Implementation of the AES Algorithm for a Reconfigurable, Bit Serial, Fully Pipelined Architecture





Add Round Key only involves XORs and Shift Rows only reroutes Wires

Runs at 50 MHz
One AES round takes 62 cycles, capable of processing two blocks at once

The packets are 13 bits long, so the minimum loop duration is
26 cycles

Tradeoffs in VLSI

Design	Advantage	Tradeoff
Unrolling	1.Faster than LUT, even at an unrolling factor of 2 we get the cipher in 5 clock cycles 2. Very Efficient	Very high area
Pipelining	1.Fast and can operate at a much higher frequency 2.Stage delay is less	Area occupied is high
Bit Serial	Very less area occupied	Very Slow

Strategy and Synergy for Security

Thank You

sarvesh@setsindia.net