Lightweight Circuits with Shift and Swap

Subhadeep Banik

Asian Symmetric Key Workshop,
ISI Kolkata

November 18, 2018

Introduction

- Types of Circuits: Brief background.
- Block cipher circuits: Round based vs Serial.

  $\Rightarrow$ Eg: Working example with PRESENT

- Relevance of lightweight circuits to current problem.
- Results.

Combinatorial vs Sequential

- Combinatorial Circuits:
- Behavior of the circuit is described completely by logic gates.
- Eg: Multiplexer, AES S-box etc.

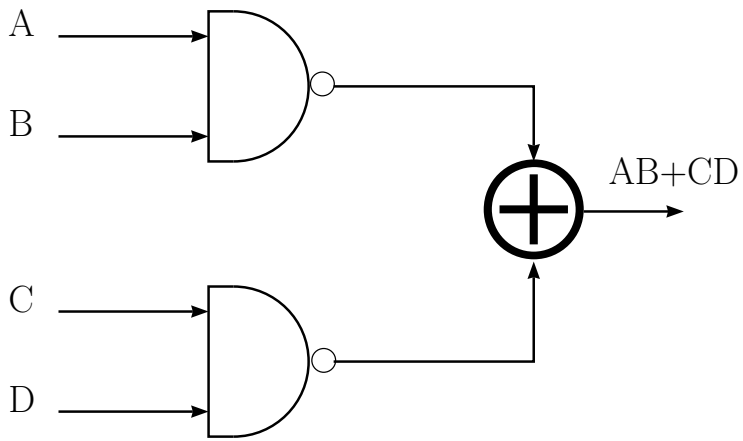
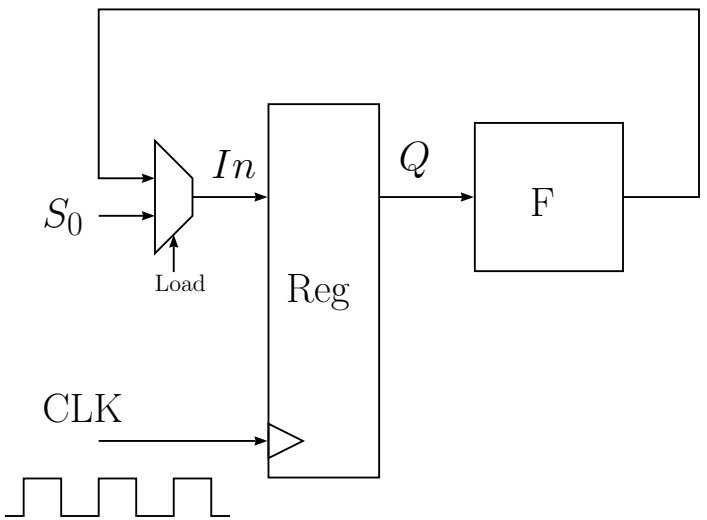


Figure: Combinatorial Circuit

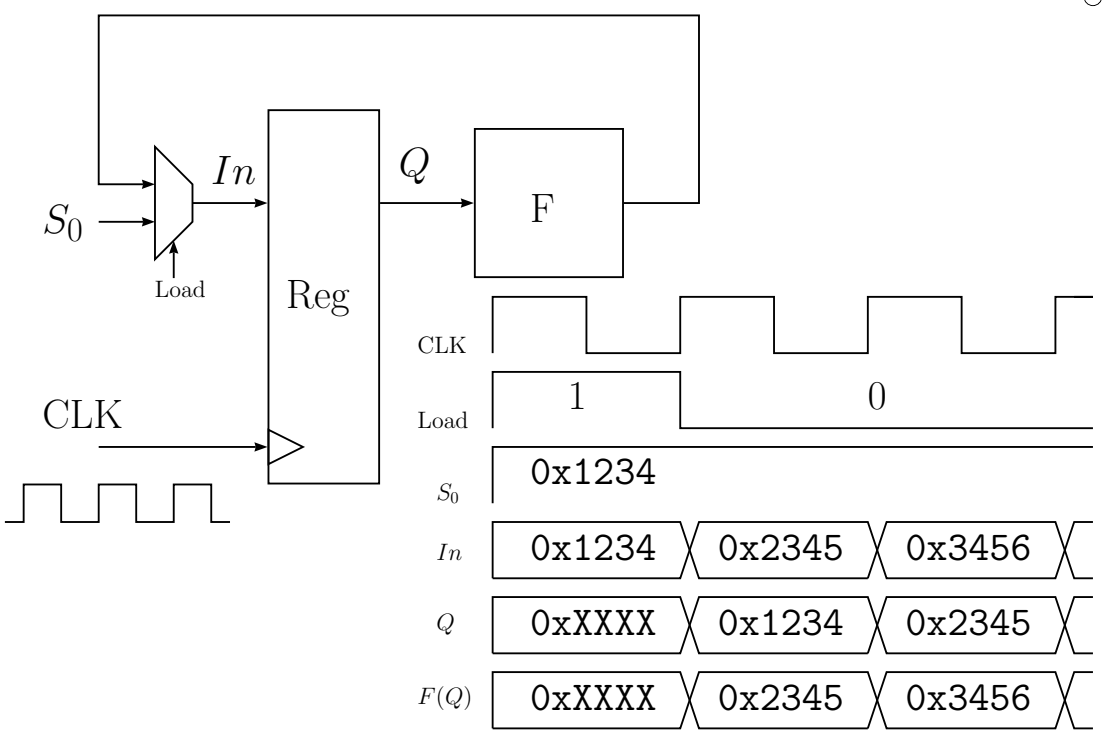
Combinatorial vs Sequential

- Sequential Circuits:
- Behavior of the circuit is described over time.
- Eg: Any circuit in which $S_{t+1} = F(S_t)$.



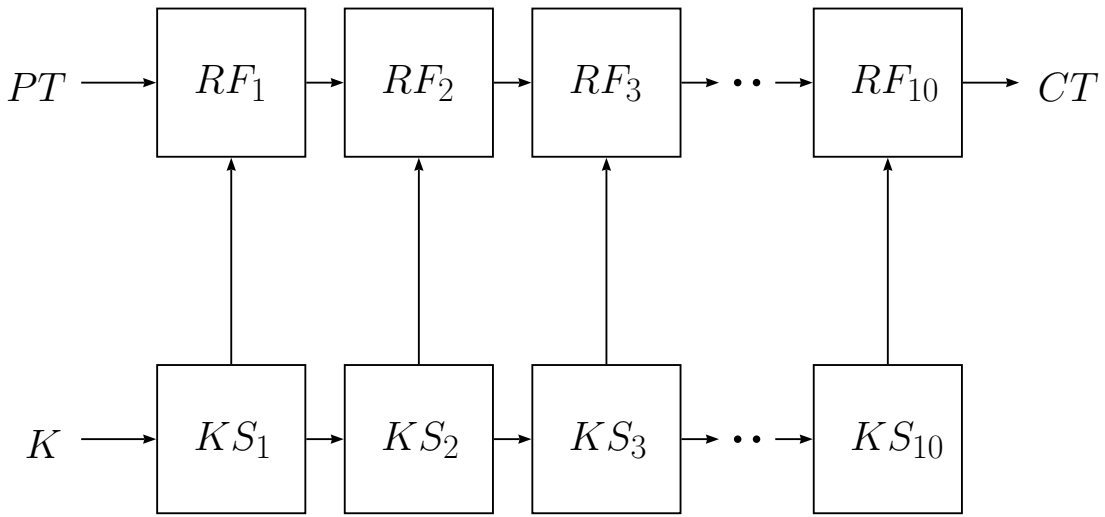
Combinatorial vs Sequential

- Sequential Circuits:
- Behavior of the circuit is described over time.
- Eg: Any circuit in which $S_{t+1} = F(S_t)$.



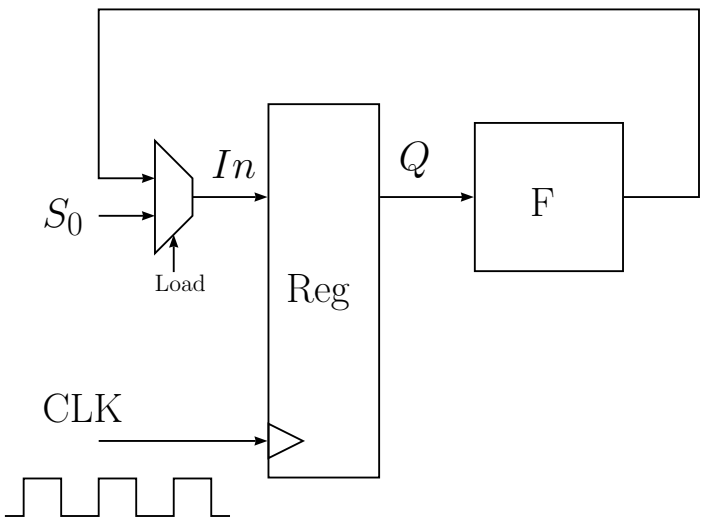
Block Cipher Circuits

- Repeated application of Round Fn: similar to previous circuit.
- However can be implemented using both ideologies.
- Eg: Fully unrolled AES.



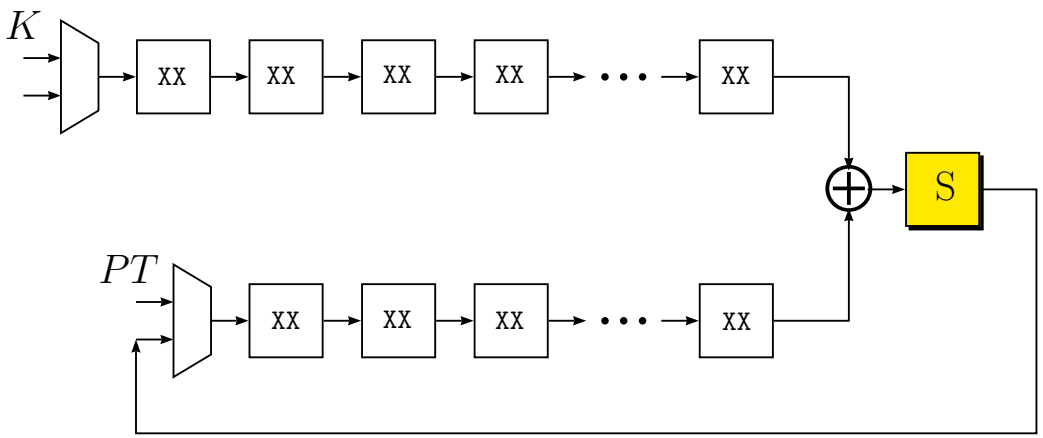
Block Cipher Circuits

- Round Based Circuits.
- One round Function Executed per clock cycle.
- $S_0 = PT||K||0$, $F = RF||KS||(i \rightarrow i+1)$.



Block Cipher Circuits: PRESENT

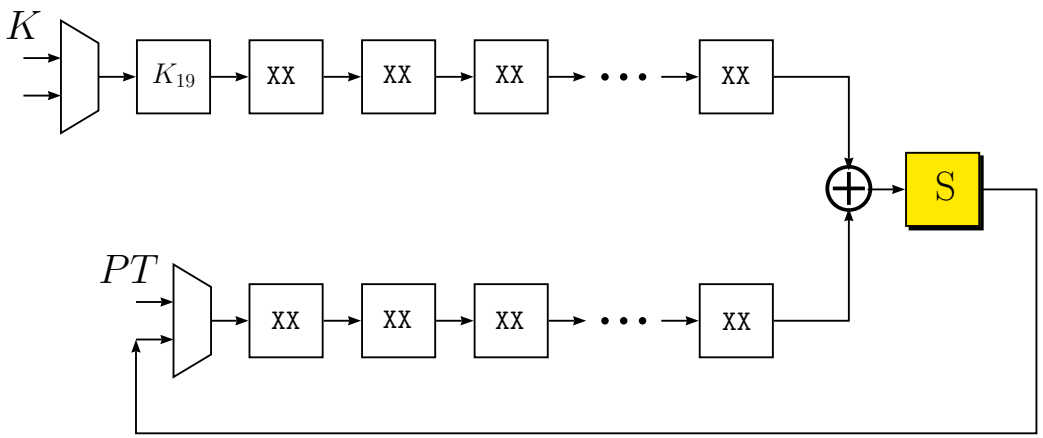
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

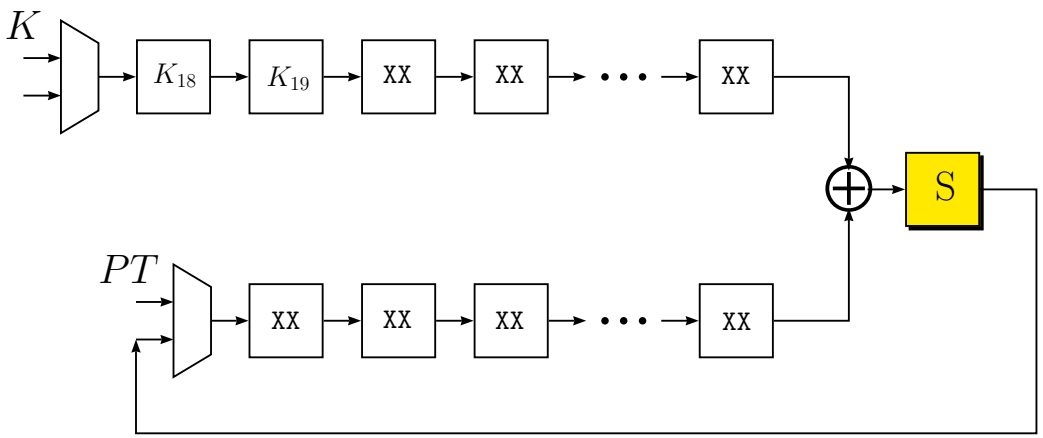
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

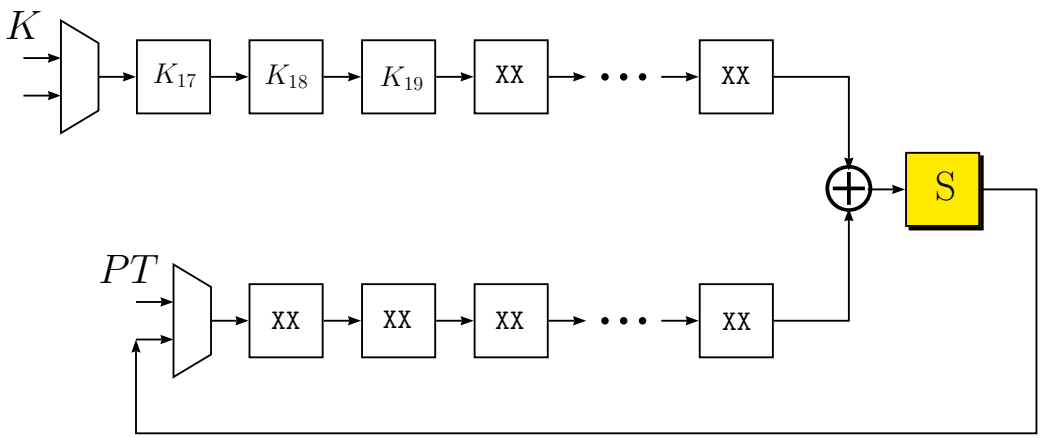
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

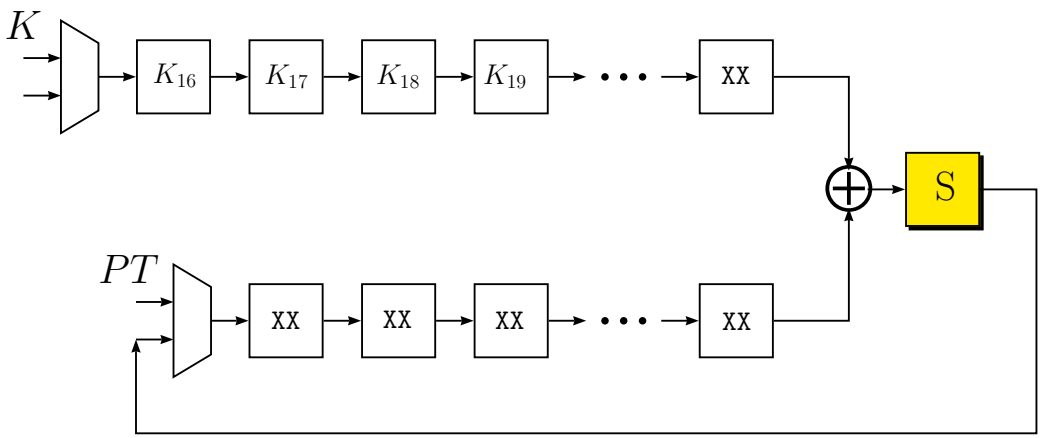
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

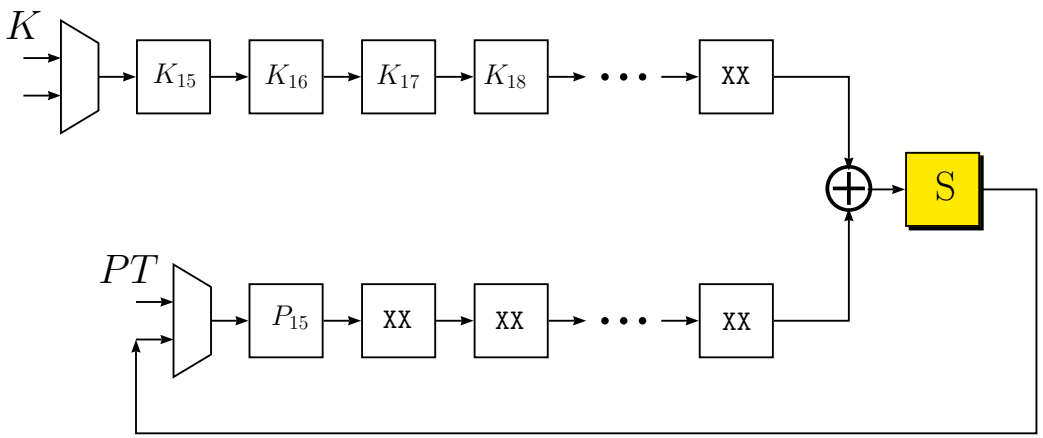
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

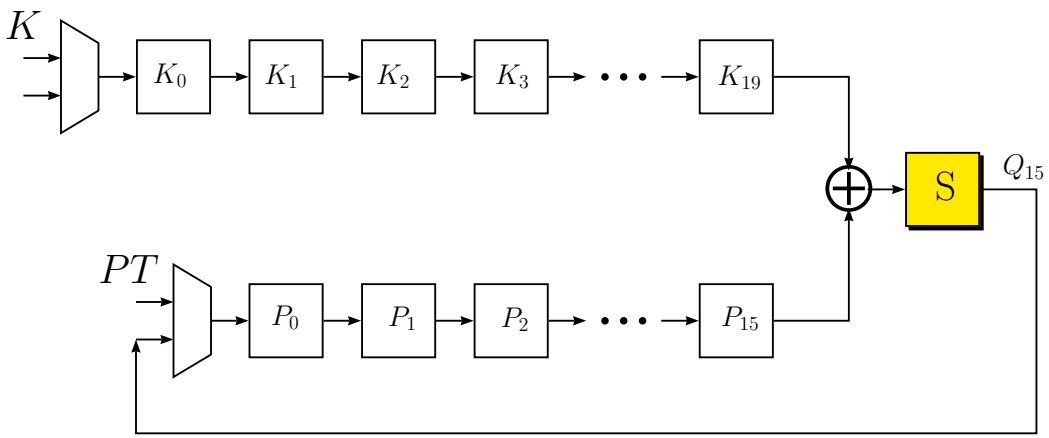
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

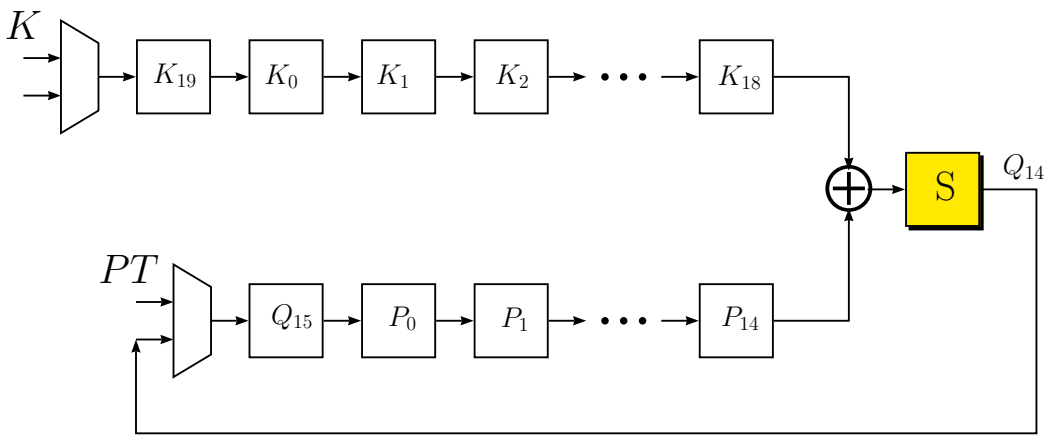
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

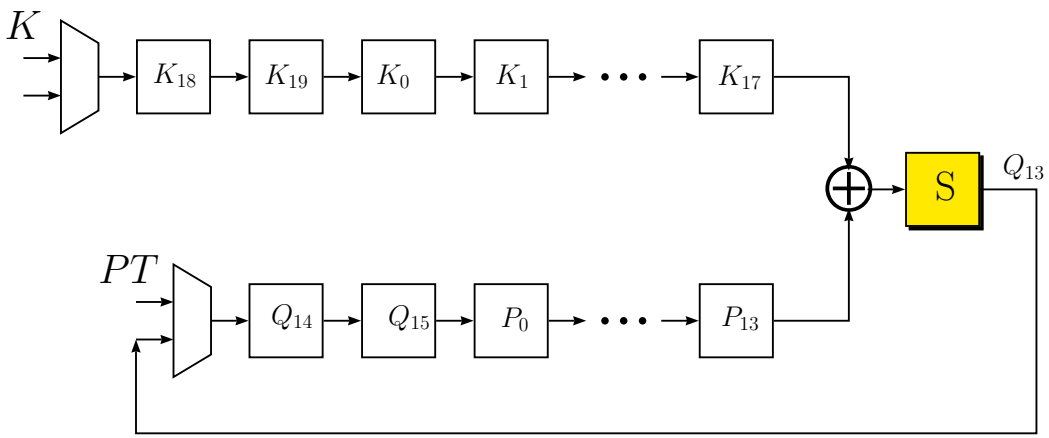
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

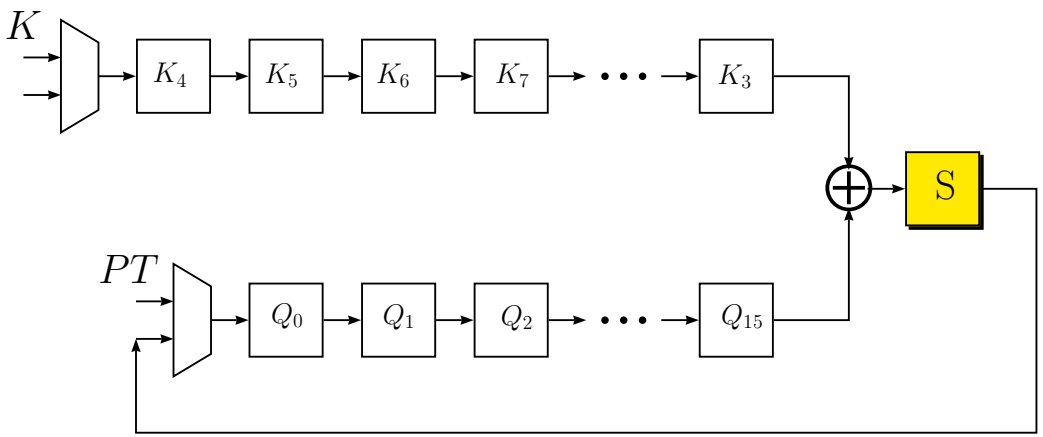
- Serialized Circuit: One S-box (lightweight implementation).
- Circuit by Rolfes et al. [CARDIS 08].
- Less than 1000 GE.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

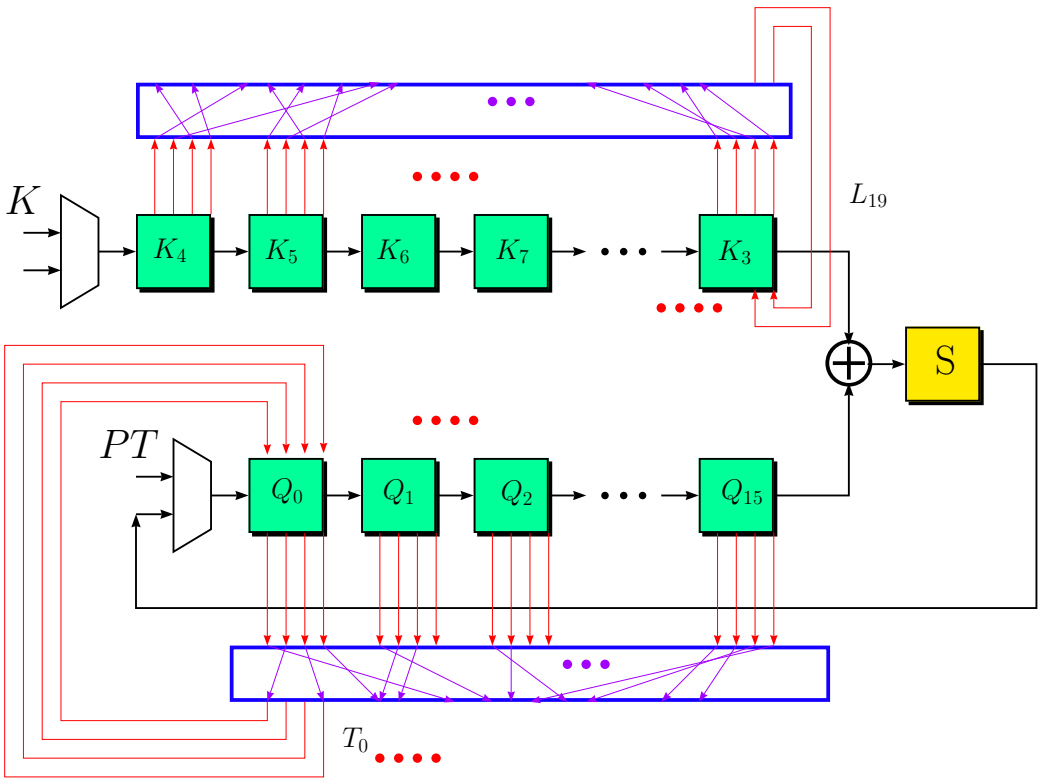
- After 20+16 cycles.
- 1st round key addition and Substitution done.
- Now to do the Permutation layer.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

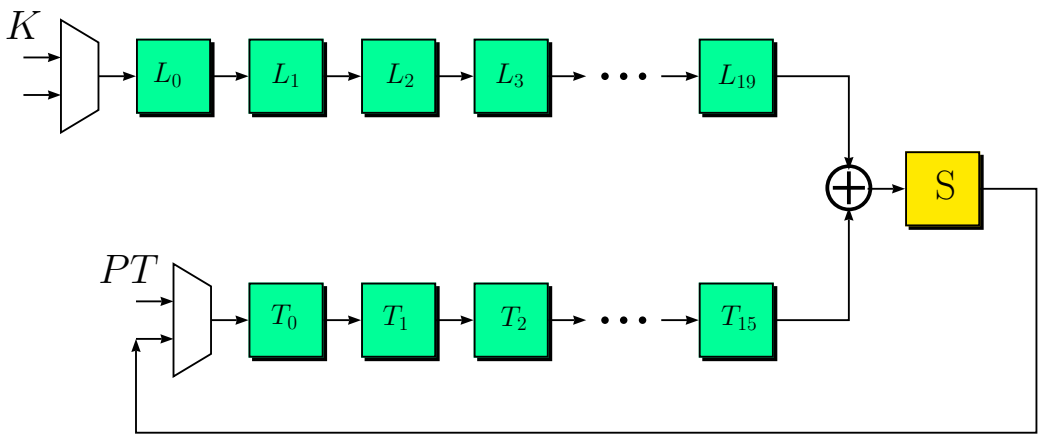
- 17th cycle dedicated to permutation layer.
- Also prepare the next roundkey.
- Each flip flop needs to be a scan flip-flop (144 in total).



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

Block Cipher Circuits: PRESENT

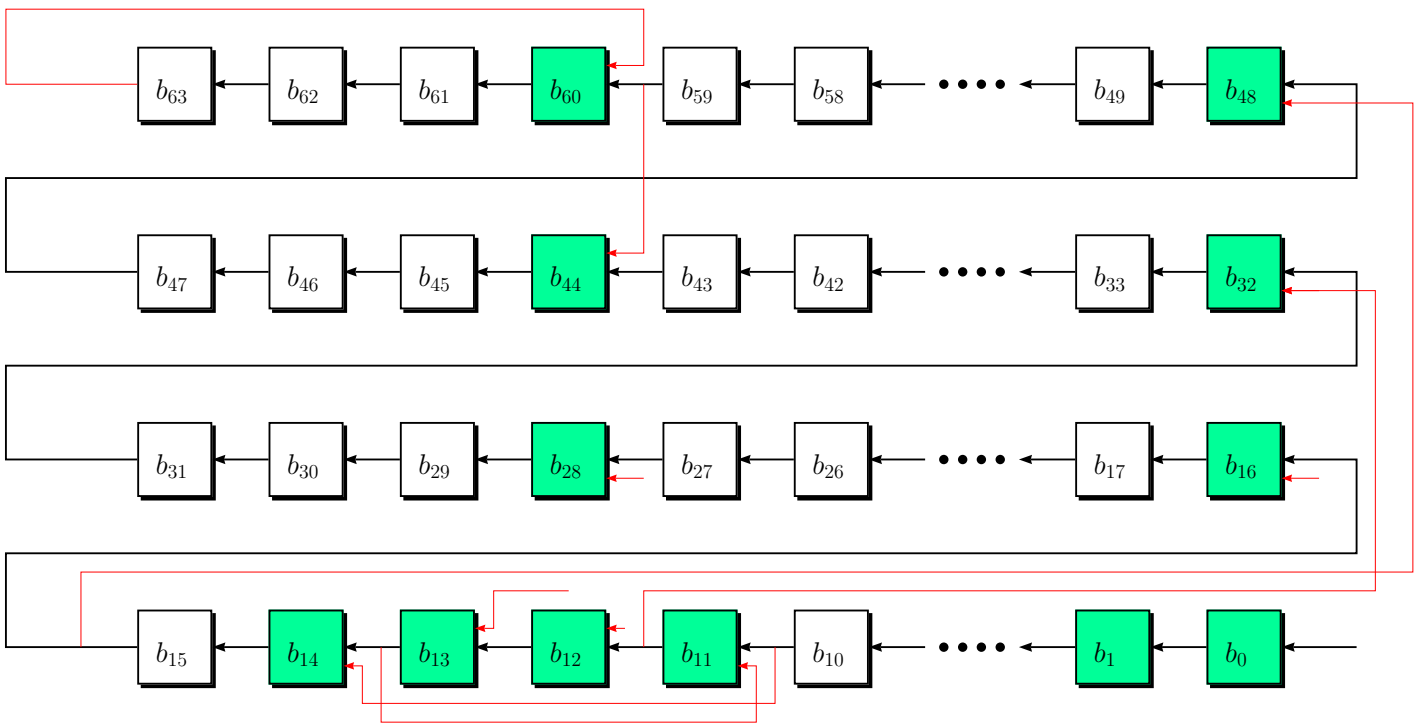
- 1st Round now completely done.
- Repeat the 17 cycles to do round 2.
- Repeat 31 times.



- $S_0 \leftarrow PT$
- For $i = 1 \rightarrow 31$ do
  - **A**. $U_i \leftarrow Sbox(S_{i-1} \oplus K_{i-1})$
  - **B**. $S_i \leftarrow P.Layer(U_i)$

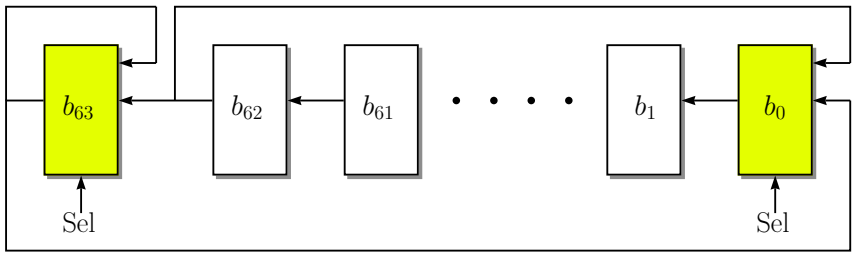
Block Cipher Circuits: PRESENT

- CHES 2017: Bit Sliding: (reducing datapath to 1 bit!!).
- Use the fact that $P = P_2^4 \circ P_1$.
- #Scan flip-flops: 35 (=24+11)$\rightarrow$ Area 850 GE.



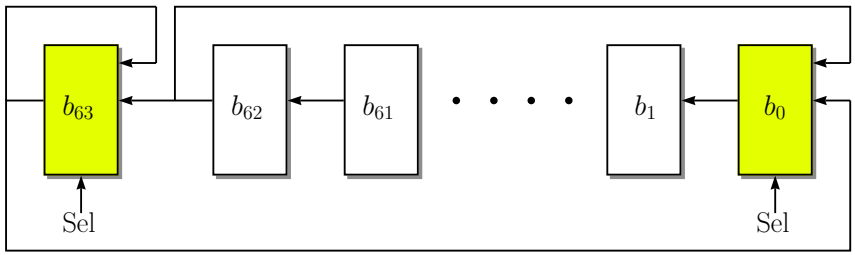
Current problem Before us

- More Scan flip-flops = More hardware area.
- Can we reduce #Scan flip-flops to 2 ?
- If so we reduce the number of implementable functions
- Only Possible if P can be implemented efficiently.



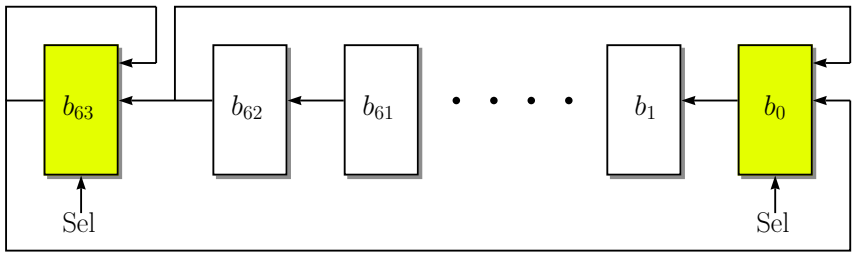
Current problem Before us

- What functions can be implemented?.
- If Sel=0, $r=$ One bit rotate towards the left.
- If Sel=1, $(b_{63}, b_{62}, \ldots, b_1, b_0) \rightarrow (b_{63}, b_{61}, \ldots, b_0, b_{62})$
- The above function $v = r \circ w$ where $w =$SWAP(b_{63}, b_{62}).



Current problem Before us

- Can P expressed as a composition of r, v ?
- Answer is YES.
- In fact r, w generate S_{64}.
- Delve into the theory of Permutation Groups.



$r, w = (63, 62)$ Generate S_{64}

Proof

- Set of all Swaps generates S_{64}.
- $G = \{(63, 62), (62, 61), (61, 60), \ldots (1, 0)\}$ generates S_{64}.

$$\begin{aligned}(i, j) &= (i, i-1) \circ (i-1, j) \circ (i, i-1) \\ &= (i, i-1) \circ (i-1, i-2) \circ (i-2, j) \circ (i-1, i-2) \circ (i, i-1)\end{aligned}$$

- Given the following identity

$$\pi \circ (i_1, i_2, \ldots, i_k) \circ \pi^{-1} = (\pi(i_1), \pi(i_2), \ldots, \pi(i_k)),$$

- Easy to see that

$$r^{-(63-i)} \circ (63, 62) \circ r^{(63-i)} = (r^{-(63-i)}(63), r^{-(63-i)}(62)) = (i, i-1)$$

Operations?

Analysis

- Consider $(49, 40)$. How many operations required ?

$$\begin{aligned}(49,40) &= (49,48)\circ(48,40)\circ(49,48)\\ &= (49,48)\circ(48,47)\circ(47,40)\circ(48,47)\circ(49,48)\\ &= (49,48)\circ(48,47)\circ\cdots(42,41)\circ(41,40)\circ(42,41)\cdots(48,47)\circ(49,48)\end{aligned}$$

- $(49,48) = r^{-14}\circ w\circ r^{14}, (48,47) = r^{-15}\circ w\circ r^{15}, \ldots, (41,40) = r^{-22}\circ w\circ r^{22}$
- So we have

$$\begin{aligned}(49,40) &= r^{-14}\circ w\circ \underbrace{[r^{-1}\circ w\circ\cdots\circ r^{-1}\circ w]}_{8\ times}\circ\underbrace{[r\circ w\circ\cdots\circ r\circ w]}_{8\ times}\circ r^{14}\\ &= [r^{49}\circ v\circ r^{14}]\circ[r^{48}\circ v\circ r^{15}]\circ\cdots\circ[r^{42}\circ v\circ r^{21}]\circ[r^{41}\circ v^{9}\circ r^{14}]\end{aligned}$$

- 9 brackets: each takes 64 operations $\rightarrow 64 * (49 - 40) = 576$ cycles !!!

Present Permutation

Table: Specifications of Present bit-permutation layer.

i	0	1	2	3	4	5	6	7
$P(i)$	0	16	32	48	1	17	33	49
i	8	9	10	11	12	13	14	15
$P(i)$	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23
$P(i)$	4	20	36	52	5	21	37	53
i	24	25	26	27	28	29	30	31
$P(i)$	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39
$P(i)$	8	24	40	56	9	25	41	57
i	40	41	42	43	44	45	46	47
$P(i)$	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55
$P(i)$	12	28	44	60	13	29	45	61
i	56	57	58	59	60	61	62	63
$P(i)$	14	30	46	62	15	31	47	63

Present Permutation

Table: Decomposition of the c_i's in the Present permutation

i	c_i	$s_i \circ t_i$	i	c_i	$s_i \circ t_i$
0	(1, 16, 4)	(4, 16) ∘ (1, 4)	10	(14, 35, 56)	(14, 35) ∘ (35, 56)
1	(2, 32, 8)	(8, 32) ∘ (2, 8)	11	(15, 51, 60)	(15, 51) ∘ (51, 60)
2	(3, 48, 12)	(12, 48) ∘ (3, 12)	12	(22, 37, 25)	(25, 37) ∘ (22, 25)
3	(5, 17, 20)	(5, 17) ∘ (17, 20)	13	(23, 53, 29)	(29, 53) ∘ (23, 29)
4	(6, 33, 24)	(24, 33) ∘ (6, 24)	14	(26, 38, 41)	(26, 38) ∘ (38, 41)
5	(7, 49, 28)	(28, 49) ∘ (7, 28)	15	(27, 54, 45)	(45, 54) ∘ (27, 45)
6	(9, 18, 36)	(9, 18) ∘ (18, 36)	16	(30, 39, 57)	(30, 39) ∘ (39, 57)
7	(10, 34, 40)	(10, 34) ∘ (34, 40)	17	(31, 55, 61)	(31, 55) ∘ (55, 61)
8	(11, 50, 44)	(44, 50) ∘ (11, 44)	18	(43, 58, 46)	(46, 58) ∘ (43, 46)
9	(13, 19, 52)	(13, 19) ∘ (19, 52)	19	(47, 59, 62)	(47, 59) ∘ (59, 62)

$\rightarrow$ Total Operations: $\sum_{s_i} 64(x_i - y_i) + \sum_{t_i} 64(x_i - y_i) = 36480$!!!

$\rightarrow$ This is way too high (compared to 17*31+20 =547)

Present Permutation

Table: Decomposition of the c_i's in the Present permutation

i	c_i	$s_i \circ t_i$	i	c_i	$s_i \circ t_i$
0	(1, 16, 4)	(4, 16) ∘ (1, 4)	10	(14, 35, 56)	(14, 35) ∘ (35, 56)
1	(2, 32, 8)	(8, 32) ∘ (2, 8)	11	(15, 51, 60)	(15, 51) ∘ (51, 60)
2	(3, 48, 12)	(12, 48) ∘ (3, 12)	12	(22, 37, 25)	(25, 37) ∘ (22, 25)
3	(5, 17, 20)	(5, 17) ∘ (17, 20)	13	(23, 53, 29)	(29, 53) ∘ (23, 29)
4	(6, 33, 24)	(24, 33) ∘ (6, 24)	14	(26, 38, 41)	(26, 38) ∘ (38, 41)
5	(7, 49, 28)	(28, 49) ∘ (7, 28)	15	(27, 54, 45)	(45, 54) ∘ (27, 45)
6	(9, 18, 36)	(9, 18) ∘ (18, 36)	16	(30, 39, 57)	(30, 39) ∘ (39, 57)
7	(10, 34, 40)	(10, 34) ∘ (34, 40)	17	(31, 55, 61)	(31, 55) ∘ (55, 61)
8	(11, 50, 44)	(44, 50) ∘ (11, 44)	18	(43, 58, 46)	(46, 58) ∘ (43, 46)
9	(13, 19, 52)	(13, 19) ∘ (19, 52)	19	(47, 59, 62)	(47, 59) ∘ (59, 62)

$\rightarrow$ Theorem 1: $P = s_{b_0} \circ s_{b_1} \circ \cdots \circ s_{b_{19}} \circ t_{a_0} \circ t_{a_1} \circ \cdots \circ t_{a_{19}}$

$\rightarrow$ $a_0, a_1, \ldots, a_{19}$ and $b_0, b_1, \ldots, b_{19}$, are any ordering of $0, 1, \ldots, 19$

Present Permutation

Table: Decomposition of the c_i's in the Present permutation

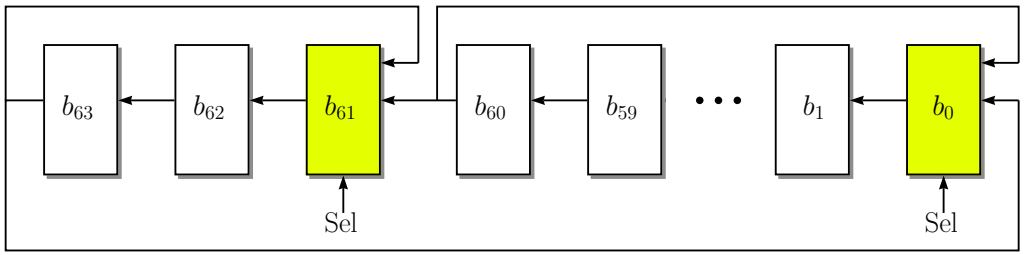
i	c_i	$s_i \circ t_i$	i	c_i	$s_i \circ t_i$
0	(1, 16, 4)	(4, 16) ∘ (1, 4)	10	(14, 35, 56)	(14, 35) ∘ (35, 56)
1	(2, 32, 8)	(8, 32) ∘ (2, 8)	11	(15, 51, 60)	(15, 51) ∘ (51, 60)
2	(3, 48, 12)	(12, 48) ∘ (3, 12)	12	(22, 37, 25)	(25, 37) ∘ (22, 25)
3	(5, 17, 20)	(5, 17) ∘ (17, 20)	13	(23, 53, 29)	(29, 53) ∘ (23, 29)
4	(6, 33, 24)	(24, 33) ∘ (6, 24)	14	(26, 38, 41)	(26, 38) ∘ (38, 41)
5	(7, 49, 28)	(28, 49) ∘ (7, 28)	15	(27, 54, 45)	(45, 54) ∘ (27, 45)
6	(9, 18, 36)	(9, 18) ∘ (18, 36)	16	(30, 39, 57)	(30, 39) ∘ (39, 57)
7	(10, 34, 40)	(10, 34) ∘ (34, 40)	17	(31, 55, 61)	(31, 55) ∘ (55, 61)
8	(11, 50, 44)	(44, 50) ∘ (11, 44)	18	(43, 58, 46)	(46, 58) ∘ (43, 46)
9	(13, 19, 52)	(13, 19) ∘ (19, 52)	19	(47, 59, 62)	(47, 59) ∘ (59, 62)

$\rightarrow$ GCD $(x_i - y_i)$ is 3. P belongs to a special class of permutations.

$\rightarrow$ Faster than 36480 cycle implementation may be possible !!!

Shift the position of scan Flip-flop to $64 - 3 = 61$

- What functions can be implemented?.
- If Sel=0, r= One bit rotate towards the left.
- If Sel=1,
  $(b_{63}, b_{62}, \ldots, b_1, b_0) \rightarrow (b_{62}, b_{61}, b_{63}, \quad b_{59}, b_{58}, \ldots, b_0, b_{60})$
- The above function $v_3 = r \circ w_3$ where w_3 =SWAP(b_{63}, b_{60}).



Proof

- Consider subclass of all permutations $\rightarrow$ each cycle has elements equivalent modulo 3. If $i \equiv j \bmod 3$:

$$\begin{aligned}(i,j) &= (i, i-3) \circ (i-3, j) \circ (i, i-3) \\ &= (i, i-3) \circ (i-3, i-6) \circ (i-6, j) \circ (i-3, i-6) \circ (i, i-3)\end{aligned}$$

- Given the following identity

$$\pi \circ (i_1, i_2, \ldots, i_k) \circ \pi^{-1} = (\pi(i_1), \pi(i_2), \ldots, \pi(i_k)),$$

- Easy to see that

$$r^{-(63-i)} \circ (63, 60) \circ r^{(63-i)} = (r^{-(63-i)}(63), r^{-(63-i)}(60)) = (i, i-3)$$

Operations?

Analysis

- Consider $(49, 40)$. How many operations required ?

$$\begin{aligned}(49,40) &= (49,46) \circ (46,40) \circ (49,46) \\ &= (49,46) \circ (46,43) \circ (43,40) \circ (46,43) \circ (49,46)\end{aligned}$$

- $(49,46) = r^{-14} \circ w_3 \circ r^{14},\ (46,43) = r^{-17} \circ w_3 \circ r^{17},\ (43,40) = r^{-20} \circ w_3 \circ r^{20}$
- So we have

$$\begin{aligned}(49,40) &= r^{-14} \circ w_3 \circ \underbrace{[r^{-3} \circ w_3 \circ \cdots \circ r^{-3} \circ w_3]}_{2 \text{ times}} \circ \underbrace{[r^{3} \circ w_3 \circ \cdots \circ r^{3} \circ w_3]}_{2 \text{ times}} \circ r^{14} \\ &= [r^{49} \circ v_3 \circ r^{14}] \circ [r^{46} \circ v_3 \circ r^{17}] \circ [r^{41} \circ (r^2 \circ v_3)^3 \circ r^{14}]\end{aligned}$$

- 3 brackets: each 64 cycles $\rightarrow 64 * \frac{(49-40)}{3} = \frac{576}{3} = 192$ cycles.

Present Permutation

Table: Decomposition of the c_i's in the Present permutation

i	c_i	$s_i \circ t_i$	i	c_i	$s_i \circ t_i$
0	(1, 16, 4)	(4, 16) ∘ (1, 4)	10	(14, 35, 56)	(14, 35) ∘ (35, 56)
1	(2, 32, 8)	(8, 32) ∘ (2, 8)	11	(15, 51, 60)	(15, 51) ∘ (51, 60)
2	(3, 48, 12)	(12, 48) ∘ (3, 12)	12	(22, 37, 25)	(25, 37) ∘ (22, 25)
3	(5, 17, 20)	(5, 17) ∘ (17, 20)	13	(23, 53, 29)	(29, 53) ∘ (23, 29)
4	(6, 33, 24)	(24, 33) ∘ (6, 24)	14	(26, 38, 41)	(26, 38) ∘ (38, 41)
5	(7, 49, 28)	(28, 49) ∘ (7, 28)	15	(27, 54, 45)	(45, 54) ∘ (27, 45)
6	(9, 18, 36)	(9, 18) ∘ (18, 36)	16	(30, 39, 57)	(30, 39) ∘ (39, 57)
7	(10, 34, 40)	(10, 34) ∘ (34, 40)	17	(31, 55, 61)	(31, 55) ∘ (55, 61)
8	(11, 50, 44)	(44, 50) ∘ (11, 44)	18	(43, 58, 46)	(46, 58) ∘ (43, 46)
9	(13, 19, 52)	(13, 19) ∘ (19, 52)	19	(47, 59, 62)	(47, 59) ∘ (59, 62)

$\rightarrow$ Total Operations: $\sum_{s_i} 64\frac{(x_i - y_i)}{3} + \sum_{t_i} 64\frac{(x_i - y_i)}{3} = 12160$!!!

$\rightarrow$ This is still way too high (compared to 17*31+20 =547)

Further Reduction

Definition

Define Let $\sigma = (x, y)$ be a transposition in S_{64} with $x > y$ in this subclass. $\overrightarrow{\text{Sel}}_\sigma$ to be the vector of Sel signals that achieves the computation of σ. The length of $\overrightarrow{\text{Sel}}_\sigma$ is therefore $\frac{64(x-y)}{3}$. Consider $\sigma = (49, 40)$. We have

$$\sigma = [r^{49} \circ v_3 \circ r^{14}] \circ [r^{46} \circ v_3 \circ r^{17}] \circ [r^{41} \circ (r^2 \circ v_3)^3 \circ r^{14}]$$

$$\overrightarrow{\text{Sel}}_\sigma = \underbrace{0^{49}\ 1\ 0^{14} \quad 0^{46}\ 1\ 0^{17} \quad 0^{41}\ 0^2 1\ 0^2 1\ 0^2 1\ 0^{14}}_{\longleftarrow \text{ Increasing Index}}$$

Further Reduction

Another Definition

For any permutation π, define $\mathbb{A}_\pi = \{x : \pi(x) \neq x\}$. Eg:

- If $\pi = (49, 40)$, $\mathbb{A}_\pi = \{40, 49\}$
- If $\pi = (49, 40, 34)$, $\mathbb{A}_\pi = \{34, 40, 49\}$ etc.
- If $\pi = (49, 40)$:

$$\pi = [r^{49} \circ v_3 \circ r^{14}] \circ [r^{46} \circ v_3 \circ r^{17}] \circ [r^{41} \circ (r^2 \circ v_3)^3 \circ r^{14}]$$

What is $\mathbb{A}_{\pi_0}$?

$$\mathbb{A}_{\pi_0} = \{40, 43, 46, 49\}.$$

Further Reduction

Theorem

Let $\sigma_1 = (x_1, y_1)$ and $\sigma_2 = (x_2, y_2)$ be two transpositions ($x_i > y_i$, $i = 1, 2$) in this subclass. Without loss of generality let their Sel vectors be of same size.

- $\sigma_1 = \pi_{z-1} \circ \pi_{z-2} \circ \cdots \circ \pi_2 \circ \pi_1 \circ \pi_0$
- $\sigma_2 = \theta_{z-1} \circ \theta_{z-2} \circ \cdots \circ \theta_2 \circ \theta_1 \circ \theta_0$
- If $\mathbb{A}_{\pi_0} \cap \mathbb{A}_{\theta_0} = \varnothing$, then

$\sigma_1 \circ \sigma_2$ can be executed in $64 \cdot z$ clock cycles using

$$\overrightarrow{\mathsf{Sel}}_{\sigma_1 \circ \sigma_2} = \overrightarrow{\mathsf{Sel}}_{\sigma_1} \hat{} \overrightarrow{\mathsf{Sel}}_{\sigma_2}$$

Further Reduction

Corollary

- Transpositions in different equivalence class can be executed simultaneously. eg:

$$(57, 39) \text{ AND } (61, 55)$$

  Their $\mathbb{A}_{\pi_0}$ sets contain elements in same equivalence class.
- Transpositions in same equivalence class can be executed simultaneously if their supports do not intersect. Eg:

$$(57, 39) \text{ AND } (36, 18)$$

Further Reduction

Table: Concurrent execution of the t_i's in the Present permutation

Group	mod3	t_i	$\max(x_i - y_i)$	#Cycles
1	0	$(57, 39)$, $(36, 18)$, $(12, 3)$	33	704
	1	$(61, 55)$, $(52, 19)$, $(4, 1)$		
	2	$(62, 59)$, $(44, 11)$, $(8, 2)$		
2	0	$(60, 51)$, $(45, 27)$, $(24, 6)$	21	448
	1	$(46, 43)$, $(40, 34)$, $(28, 7)$		
	2	$(56, 35)$, $(29, 23)$, $(20, 17)$		
3	1	$(25, 22)$	3	64
	2	$(41, 38)$		

Further Reduction

Table: Concurrent execution of the s_i's in the Present permutation

Group	mod3	s_i	$\max(x_i - y_i)$	#Cycles
1	0	$(51, 15)$	36	768
	1	$(55, 31)$, $(19, 13)$		
	2	$(53, 29)$, $(17, 5)$		
2	0	$(48, 12)$	36	768
	1	$(58, 46)$, $(34, 10)$		
	2	$(59, 47)$, $(32, 8)$		
3	0	$(54, 45)$, $(39, 30)$, $(18, 9)$	21	448
	1	$(49, 28)$, $(16, 4)$		
	2	$(50, 44)$, $(35, 14)$		
4	0	$(33, 24)$	12	256
	1	$(37, 25)$		
	2	$(38, 26)$		

$\rightarrow$ #Cycles = 704+448+64+768+768+448+256=3456.

Even Further Reduction

- Transpositions in same equivalence class can be executed simultaneously even if their supports intersect.
- Next part of the paper shows how to make that happen.
- The mathematics is very complicated.
- #Cycles can be brought down to $23 * 64 = 1472$.
- This is the lowest we could achieve in a 2 scan ff setup.

Combined Encryption+Decryption Circuit

- Circuits which can accommodate both Cipher and inverse Cipher.
- Functionality decided by an extra Encrypt/Decrypt signal.
- May be useful for some modes of operation.
- Given an implementation of P, P^{-1} is easy to construct
- HOW? Hint: Transpositions involutory.
- If $P = s_{b_0} \circ s_{b_1} \circ \cdots \circ s_{b_{19}} \circ t_{a_0} \circ t_{a_1} \circ \cdots \circ t_{a_{19}}$.

$$P^{-1} = t_{a_0} \circ t_{a_1} \circ \cdots \circ t_{a_{19}} \circ s_{b_0} \circ s_{b_1} \circ \cdots \circ s_{b_{19}}$$

RESULTS

Table: Tabulation of Results (Unless stated, power reported at 10 MHz)

Design	Conf.	Area (GE)	Power (μW)	Latency	Ref
PRESENT (E)	**A**	935	40.0	1472 per round	Our result
	B	727	35.8	1472 per round	Our result
		847[1]	0.43[2]	68 per round	CHES 17
PRESENT (ED)	**A**	1039	41.4	1472 per round	Our result
	B	809	37.7	1472 per round	Our result
		1238	56.0	17 per round	HOST 17
GIFT (E)	**A**	1132	49.8	1728 per round	Our result
	B	925	45.8	1728 per round	Our result
		930	35.9	96 per round	CHES 17
GIFT (ED)	**A**	1290	52.6	1728 per round	Our result
	B	1050	44.8	1728 per round	Our result
FLIP	2nd ckt	3581	164.9	$\approx 2^{17}$ per bit	Our result
	3rd ckt	8605	171.9	530 per bit	Our result

[1] Synthesized using IBM 130nm CMOS process

[2] Power reported at 100 KHz

Open Problems

1. Problem is closely related to Cayley diameter of the Permutation Group.
2. A more formal approach is possible ?
3. Reduction in number of cycles with slight increase in # scan flip-flops?
4. For example, 4 scan flip-flops ?

THANK YOU