DHE-1 Cryptosystem

Hybrid SPN-Fiestel Structure

By
Rahul Kejriwal, CS14B023
Bikash Gogoi, CS14B039

Problem with AES and DES

Linear Cryptanalysis

1. Build LAT for S-boxes
2. Find trails with maximum bias

Differential Cryptanalysis

1. Build DAT for S-boxes
2. Find trails with maximum propagation ratio

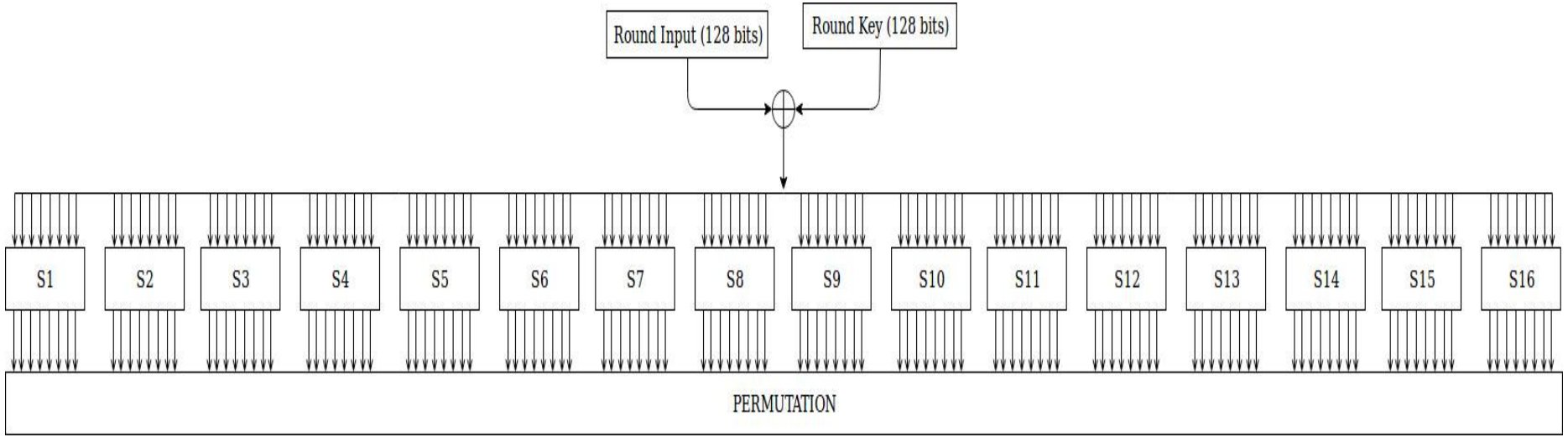
Issue

Static structure of rounds that enables the computation of weakest trails.

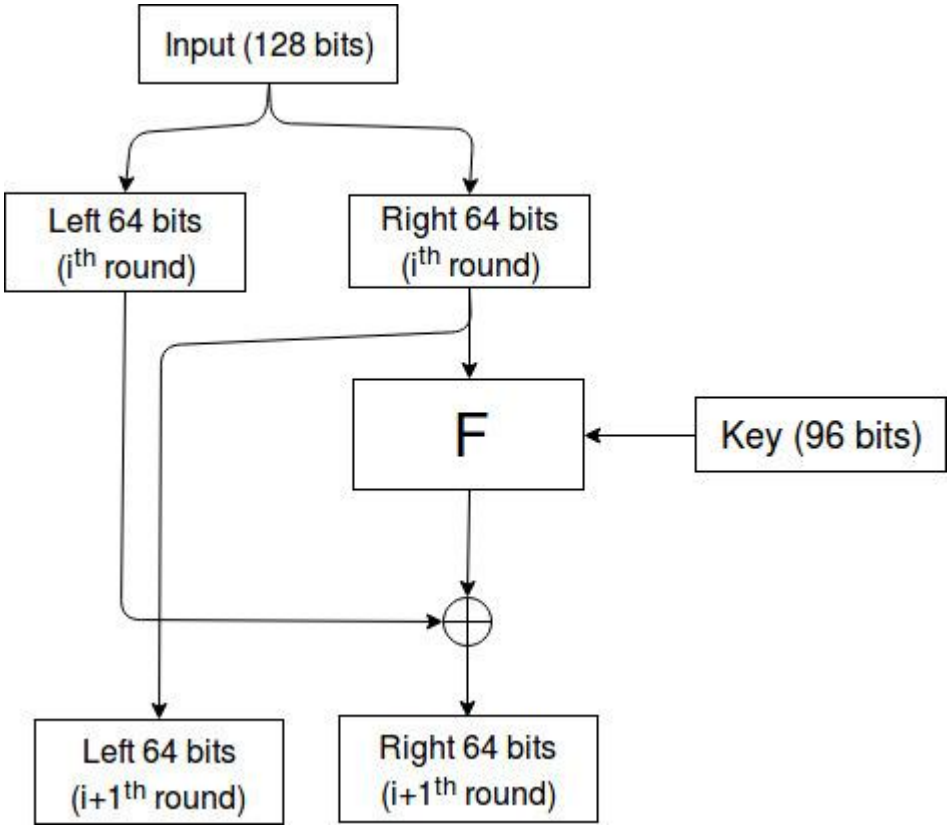
Cipher Structure

- Consists of 20 rounds
- Each round is either SPN type or Fiestel Type
- Round structures are determined by a function `rounds_structure()` using the input key
- Cipher can be customized easily by changing the `rounds_structure()` function
- Or, we can increase cipher to 148-bit security by using additional 20-bits for rounds rather than generating from the master key itself
- Inverted round structure is used during decryption

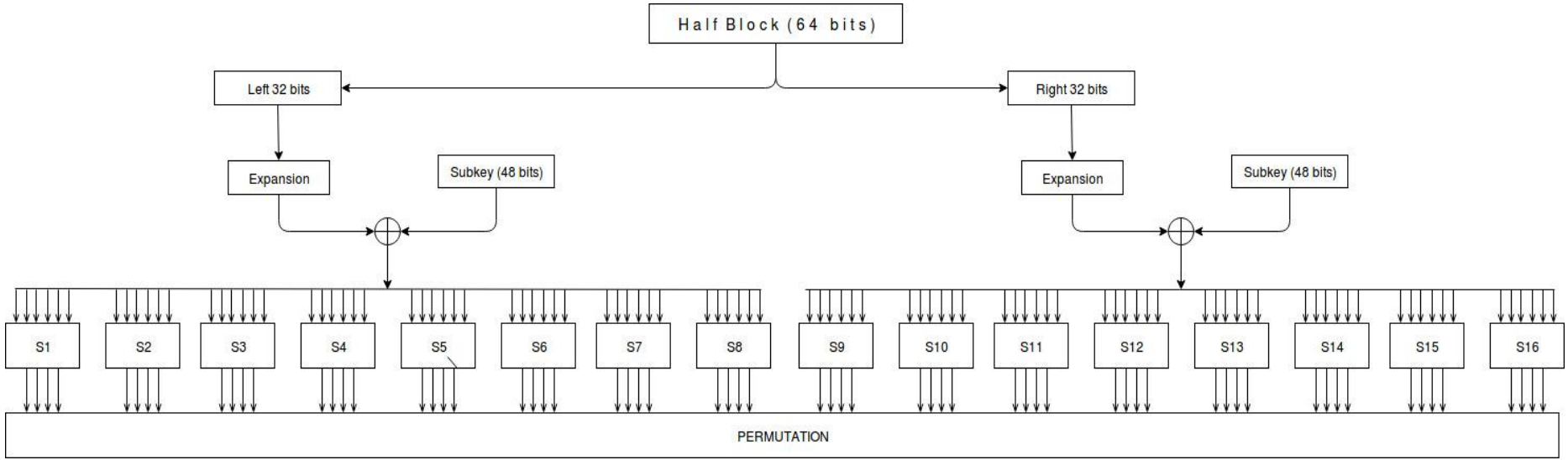
SPN Round


Round Input (128 bits)
Round Key (128 bits)
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
S13
S14
S15
S16
PERMUTATION

Fiestel Round

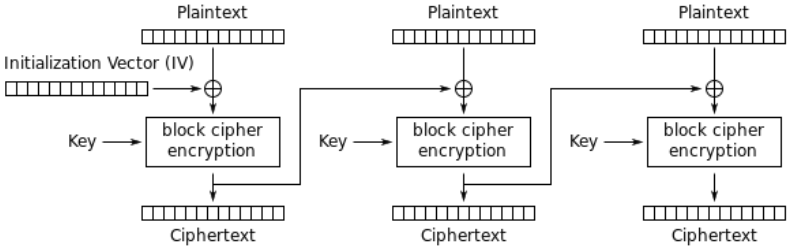


F-function

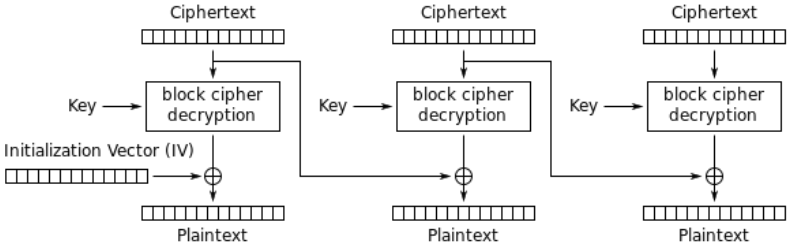

Half Block (64 bits)
Left 32 bits
Right 32 bits
Expansion
Subkey (48 bits)
Expansion
Subkey (48 bits)
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
S13
S14
S15
S16
PERMUTATION

Block Cipher Mode of Operation

- Use Cipher Block Chaining (CBC) to encrypt multiple blocks



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

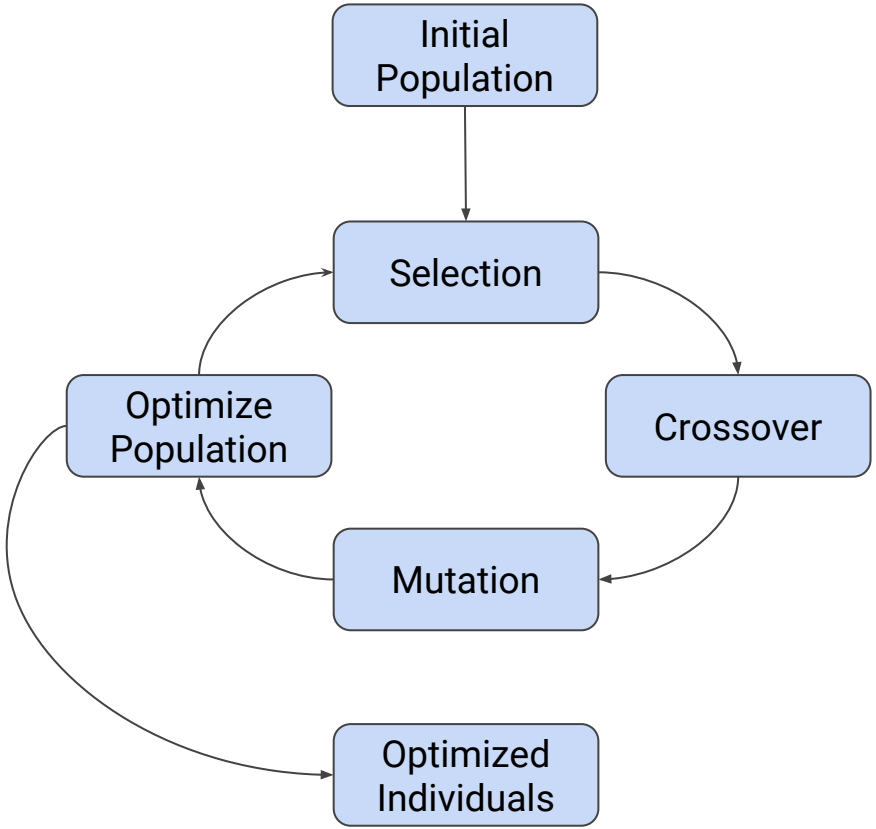
SBox Generation - Genetic Optimization

- Parameters Used:
  - Population Size = 200
  - Optimize population using best k from offspring generation, k=100
  - Mutation Probability = 0.4
  - No. of iterations = 100

- Crossover: Ordered crossover
- Mutation: Invert mapping of 2 random input values

- Fitness Function Used:
  n_i and nl_i are the rank (in terms of non-linearity) and non-linearity of i^{th} bit of SBox output

$$fitness \propto \sum_{n_i=1}^{len\_of\_sbox\_op} n_i \times nl_i$$



SBox Generation - Genetic Optimization (contd.)

- Generated 16 8x8 invertible straight S-Boxes for SPN rounds
- Generated 16 6x4 non-invertible compression S-Boxes for Fiestel Rounds
- Highest dimensions generated were 8x8 S-Boxes as higher dimensions required much larger time to generate via Genetic Optimizations
- All S-Boxes generated are balanced
  (crossover and mutation do not disturb balancedness)
- Optimized S-Boxes based on non-linearity of output bits
  (see fitness function)

Diffusion Layer for SPN round

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
bit 1	1	114	99	84	69	54	39	24	9	122	107	92	77	62	47	32
bit 2	17	2	115	100	85	70	55	40	25	10	123	108	93	78	63	48
bit 3	33	18	3	116	101	86	71	56	41	26	11	124	109	94	79	64
bit 4	49	34	19	4	117	102	87	72	57	42	27	12	125	110	95	80
bit 5	65	50	35	20	5	118	103	88	73	58	43	28	13	126	111	96
bit 6	81	66	51	36	21	6	119	104	89	74	59	44	29	14	127	112
bit 7	97	82	67	52	37	22	7	120	105	90	75	60	45	30	15	128
bit 8	113	98	83	68	53	38	23	8	121	106	91	76	61	46	31	16

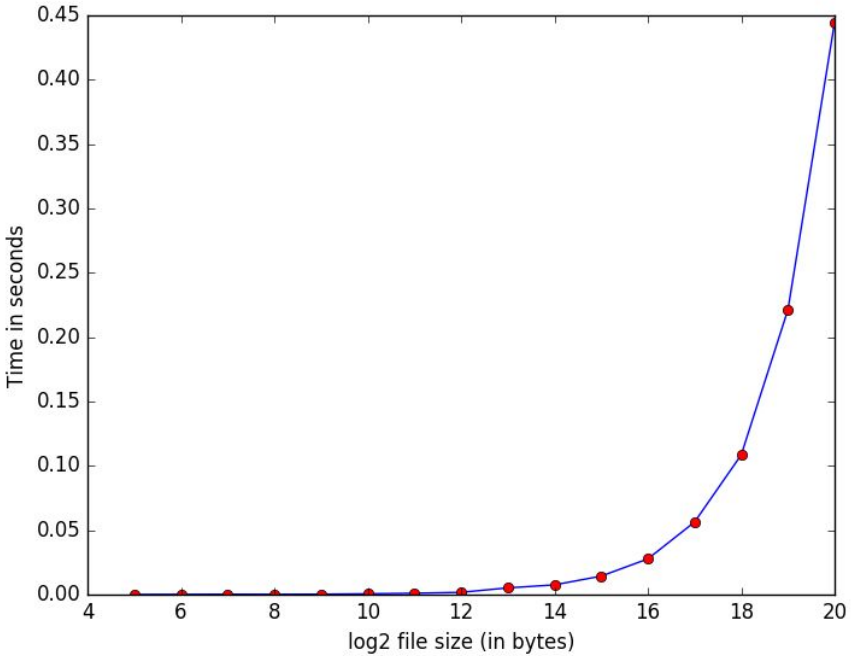
Diffusion Layer for Fiestel round

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
bit 1	1	50	35	20	5	54	39	24	9	58	43	28	13	62	47	32
bit 2	17	2	51	36	21	6	55	40	25	10	59	44	29	14	63	48
bit 3	33	18	3	52	37	22	7	56	41	26	11	60	45	30	15	64
bit 4	49	34	19	4	53	38	23	8	57	42	27	12	61	46	31	16

Linear and Differential Cryptanalysis

- Since the structure of cipher is dynamic, it was not possible to find trails for each possible structure.
- As a representative, we have analyzed trails for the structure where each round is SPN type. In general, our cipher would be 2^{20} times harder to break.
- Used a greedy algorithm to find weakest trails, as brute-force is not possible on this large search space
- Bias for weakest linear trail is $\cong 10^{-104}$ ($\cong 2^{-345}$)
- Propagation ratio for weakest differential trail is $\cong 10^{-43}$ ($\cong 2^{-140}$)

Execution Speed (including I/O time)



File Size (log_2 file size in bytes)	Time Taken (in seconds)
6	0.000192
8	0.000216
10	0.000600
12	0.001765
14	0.007553
16	0.027721
18	0.108517
20	0.444569

Thank You!