Специальные разностные характеристики подстановок конечных полей и их приложение в криптографии.

Ф.М.Хоанг

5 ноября 2023 г.

Содержание

1 Специальные разностные характеристики подстановок

1.1 Специальные разностные характеристики подстановок

Пусть $P = GF(q)$ - конечное поле, и подстановка τ конечного поля P.

Определим число n_τ равенством

$$n_\tau = \max_{a \in P \setminus \{0,e\}, b \in P} N_{a,b}(*)$$

Такое число будем называть числом специальной разностной характеристики подстановки τ.

П р и м е р 1.

а) S-блок Rijndael — это таблица замен (таблица прямого поиска), используемая в шифре Rijndael, на котором основан криптографический алгоритм стандарта шифрования AES (Advanced Encryption Standard).

Пусть $P = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1)$ - конечное поле

0x63	0x7C	0x77	0x7B	0xF2	0x6B	0x6F	0xC5	0x30	0x01	0x67	0x2B	0xF
0xCA	0x82	0xC9	0x7D	0xFA	0x59	0x47	0xF0	0xAD	0xD4	0xA2	0xAF	0x9
0xB7	0xFD	0x93	0x26	0x36	0x3F	0xF7	0xCC	0x34	0xA5	0xE5	0xF1	0x7
0x04	0xC7	0x23	0xC3	0x18	0x96	0x05	0x9A	0x07	0x12	0x80	0xE2	0xE
0x09	0x83	0x2C	0x1A	0x1B	0x6E	0x5A	0xA0	0x52	0x3B	0xD6	0xB3	0x2
0x53	0xD1	0x00	0xED	0x20	0xFC	0xB1	0x5B	0x6A	0xCB	0xBE	0x39	0x4
0xD0	0xEF	0xAA	0xFB	0x43	0x4D	0x33	0x85	0x45	0xF9	0x02	0x7F	0x5
0x51	0xA3	0x40	0x8F	0x92	0x9D	0x38	0xF5	0xBC	0xB6	0xDA	0x21	0x1
0xCD	0x0C	0x13	0xEC	0x5F	0x97	0x44	0x17	0xC4	0xA7	0x7E	0x3D	0x6
0x60	0x81	0x4F	0xDC	0x22	0x2A	0x90	0x88	0x46	0xEE	0xB8	0x14	0xD
0xE0	0x32	0x3A	0x0A	0x49	0x06	0x24	0x5C	0xC2	0xD3	0xAC	0x62	0x9
0xE7	0xC8	0x37	0x6D	0x8D	0xD5	0x4E	0xA9	0x6C	0x56	0xF4	0xEA	0x6
0xBA	0x78	0x25	0x2E	0x1C	0xA6	0xB4	0xC6	0xE8	0xDD	0x74	0x1F	0x4
0x70	0x3E	0xB5	0x66	0x48	0x03	0xF6	0x0E	0x61	0x35	0x57	0xB9	0x8
0xE1	0xF8	0x98	0x11	0x69	0xD9	0x8E	0x94	0x9B	0x1E	0x87	0xE9	0xC
0x8C	0xA1	0x89	0x0D	0xBF	0xE6	0x42	0x68	0x41	0x99	0x2D	0x0F	0xB

Таблица 1: 16x16 S-Box

Имеем $\tau = 4$

Б) Кузнечик

Пусть $P = GF(2)[x]/(x^8 + x^7 + x^6 + x + 1)$ - конечное поле

0xfc	0xee	0xdd	0x11	0xcf	0x6e	0x31	0x16	0xfb	0xc4	0xfa	0xda	0x23	0xc5	0
0xe9	0x77	0xf0	0xdb	0x93	0x2e	0x99	0xba	0x17	0x36	0xf1	0xbb	0x14	0xcd	
0xf9	0x18	0x65	0x5a	0xe2	0x5c	0xef	0x21	0x81	0x1c	0x3c	0x42	0x8b	0x01	
0x05	0x84	0x02	0xae	0xe3	0x6a	0x8f	0xa0	0x06	0x0b	0xed	0x98	0x7f	0xd4	0
0xeb	0x34	0x2c	0x51	0xea	0xc8	0x48	0xab	0xf2	0x2a	0x68	0xa2	0xfd	0x3a	
0xb5	0x70	0x0e	0x56	0x08	0x0c	0x76	0x12	0xbf	0x72	0x13	0x47	0x9c	0xb7	0
0x15	0xa1	0x96	0x29	0x10	0x7b	0x9a	0xc7	0xf3	0x91	0x78	0x6f	0x9d	0x9e	0
0x32	0x75	0x19	0x3d	0xff	0x35	0x8a	0x7e	0x6d	0x54	0xc6	0x80	0xc3	0xbd	0
0xdf	0xf5	0x24	0xa9	0x3e	0xa8	0x43	0xc9	0xd7	0x79	0xd6	0xf6	0x7c	0x22	0
0xe0	0x0f	0xec	0xde	0x7a	0x94	0xb0	0xbc	0xdc	0xe8	0x28	0x50	0x4e	0x33	0
0xa7	0x97	0x60	0x73	0x1e	0x00	0x62	0x44	0x1a	0xb8	0x38	0x82	0x64	0x9f	0
0xad	0x45	0x46	0x92	0x27	0x5e	0x55	0x2f	0x8c	0xa3	0xa5	0x7d	0x69	0xd5	0
0x07	0x58	0xb3	0x40	0x86	0xac	0x1d	0xf7	0x30	0x37	0x6b	0xe4	0x88	0xd9	0
0xe1	0x1b	0x83	0x49	0x4c	0x3f	0xf8	0xfe	0x8d	0x53	0xaa	0x90	0xca	0xd8	0
0x20	0x71	0x67	0xa4	0x2d	0x2b	0x09	0x5b	0xcb	0x9b	0x25	0xd0	0xbe	0xe5	
0x59	0xa6	0x74	0xd2	0xe6	0xf4	0xb4	0xc0	0xd1	0x66	0xaf	0xc2	0x39	0x4b	0

Таблица 2: 16x16 Hexadecimal Array

Имеем $\tau = 36$

B) Блочный шифр KHAZAD уровня наследия

Пусть $P = GF(2)[x]/(x^8 + x^4 + x^3 + x^2 + 1)$ - конечное поле

0xBA	0x54	0x2F	0x74	0x53	0xD3	0xD2	0x4D	0x50	0xAC	0x8D	0xBF	0x70
0x10	0xEA	0xD5	0x97	0xD1	0x33	0x51	0x5B	0xA6	0xDE	0x48	0xA8	0x99
0xFC	0x20	0xE3	0x9E	0x91	0x9B	0xE2	0xBB	0x41	0x6E	0xA5	0xCB	0x6E
0xB1	0x02	0x30	0xCC	0xC4	0x1D	0x14	0xC3	0x63	0xDA	0x5D	0x5F	0xDC
0x5A	0x6C	0x5C	0x40	0xF7	0x26	0xFF	0xED	0xE8	0x9D	0x6F	0x8E	0x19
0x0F	0x07	0xAF	0xFB	0x50	0x08	0x15	0x0D	0x04	0x01	0x64	0xDF	0x76
0x16	0x3F	0x37	0x6D	0x38	0x60	0xB9	0x73	0xE9	0x35	0x55	0x71	0x7E
0xF6	0x2A	0x3E	0x5E	0x27	0x46	0x70	0x0C	0x65	0x68	0x61	0x03	0xC1
0x58	0xD8	0x66	0xD7	0x3A	0xC8	0x3C	0x80	0xFA	0x96	0xA7	0x98	0xEC
0x69	0x4B	0xAB	0xA9	0x67	0x0A	0x47	0xF2	0x90	0xB5	0x22	0xE5	0xEE
0x12	0x83	0x1B	0x0E	0x23	0xF5	0x45	0x21	0xCE	0xA0	0x49	0x2C	0xF9
0x17	0x82	0x1A	0x8B	0xFE	0x8A	0x09	0xC9	0x87	0x4E	0xB0	0xE1	0x2E
0x90	0xA4	0x1E	0x85	0x60	0x00	0x25	0xF4	0xF1	0x94	0x0B	0xC0	0xE7
0x31	0xD4	0xD0	0x86	0x7E	0xAD	0xFD	0x29	0x30	0x3B	0x9F	0xF8	0xD0
0x05	0xC5	0x11	0x77	0x7C	0x7A	0x78	0x36	0x1C	0x39	0x59	0x18	0x56
0x24	0x20	0xB2	0x92	0xA3	0xC0	0x44	0x62	0x10	0xB4	0x84	0x43	0x93

Таблица 3: 16x16 Hexadecimal Array

Имеем $\tau = 7$

ШИФР	τ
AES	4
Кузнечик	36
KHAZAD 3	7

Таблица 4: таблица чисел специальных разностных характеристик

τ	**частот**
6	8051
7	538196
8	389714
9	57520
10	5981
11	489
12	47
13	2

Таблица 5: таблица частот чисел специальных разностных характеристик

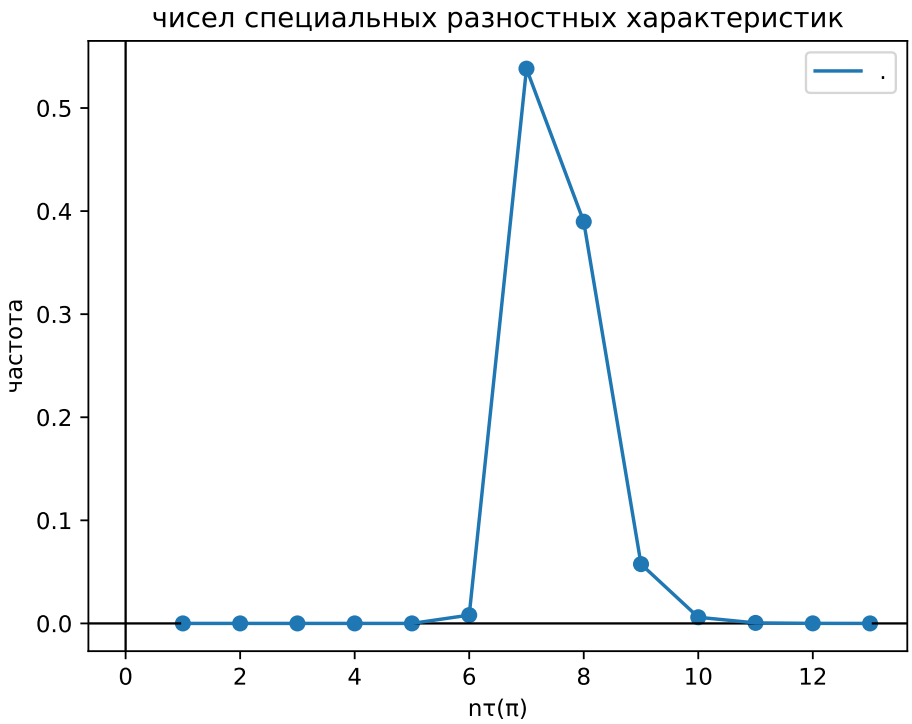

Рис. 1: График частот чисел специальных разностных характеристик