О квазигрупповом блочном шифре INRU

проект

К. Царегородцев[1, 2]

[1] МГУ им. М. В. Ломоносова
Москва, Россия

[2] АО «НПК «Криптонит»

3 августа 2023 г.

Блочный шифр in a nutshell

Строение “типичного” блочного шифра:

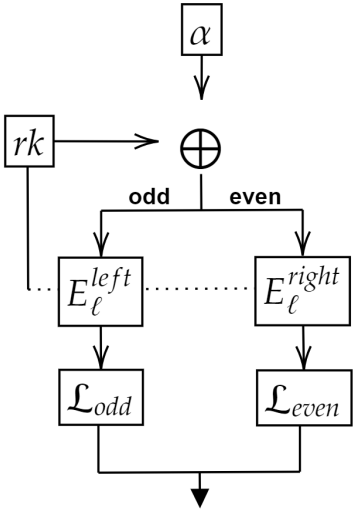
- мастер-ключ K с помощью некоторого ключевого расписания порождает раундовые ключи rk;
- на каждом раунде:
  - входной блок складывается с раундовым ключом (X-преобразование);
  - к полученному блоку применяется нелинейное преобразование (S-преобразование, S-блок);
  - к полученному блоку применяется линейное (рассеивающее) преобразование (L-преобразование).

Квазигрупповой шифр INRU

- Обычно S-блок алгоритма — конкретная тщательно выбранная подстановка; не зависит от ключа; одинаковая на каждом раунде.
- А что если заменить S-блок на некоторую квазигрупповую операцию?
- Причем можно внести зависимость от ключа: тогда будут использоваться различные подстановки на различных раундах.
- Что надо потребовать от квазигруппы?

Постановка задачи

- E^{left}, E^{right} — некоторые квазигрупповые преобразования;
- $\mathcal{L}$ — некоторые линейные преобразования;
- rk — раундовый ключ.



Постановка задачи-2

$*$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	5	c	1	0	2	e	9	8	f	d	3	b	7	a	4	6
1	f	4	3	a	8	d	6	2	5	e	1	7	b	0	c	9
2	6	7	d	2	0	3	f	a	9	1	e	4	c	8	b	5
3	8	d	7	9	f	4	0	5	2	c	b	3	1	6	e	a
4	4	f	0	1	d	8	7	e	c	2	a	6	9	3	5	b
5	9	b	e	8	a	1	5	0	6	3	d	c	4	2	7	f
6	a	1	c	f	9	b	2	6	0	7	4	e	d	5	3	8
7	e	2	9	7	c	5	1	4	d	f	6	a	0	b	8	3
8	7	6	8	e	3	0	4	1	b	a	2	f	5	d	9	c
9	2	e	b	6	5	c	a	f	8	4	7	1	3	9	d	0
a	b	9	2	d	1	a	c	3	7	0	8	5	f	e	6	4
b	0	3	4	5	6	7	8	9	a	b	c	d	e	f	1	2
c	3	0	f	c	7	6	d	b	1	9	5	8	2	4	a	e
d	1	a	5	4	b	9	e	7	3	6	f	2	8	c	0	d
e	d	8	6	b	4	f	3	c	e	5	9	0	a	7	2	1
f	c	5	a	3	e	2	b	d	4	8	0	9	6	1	f	7

- а можно ли лучше?
- а что вообще значит “лучше”?

Что хотелось бы получить в итоге?

В идеале...

1. Внимательно посмотреть на сам алгоритм (в частности, на используемую квазигруппу).
2. Посмотреть, какие у квазигрупп бывают полезные для криптографии свойства ($\approx$ алгебра).
3. Посмотреть различные способы задания квазигрупп ($\approx$ алгебра/дискретная математика).
4. Реализовать какие-нибудь "перспективные", но относительно простые способы задания квазигрупп и попробовать посчитать всяческие характеристики, связанные с этими квазигруппами на основе п.2 ($\approx$ программирование).
5. Попробовать предложить какую-нибудь более удачную квазигруппу/класс квазигрупп для рассматриваемого алгоритма.

Что требуется?

- умение читать статьи на английском языке;
- общее знакомство с тем, какие “хорошие” свойства бывают у S-блоков;
- общее знакомство с тем, что такое подстановки, группа подстановок, циклы, неподвижные точки, etc;
- навыки программирования — реализовать порождение квазигруппы, посчитать характеристики квазигруппы и т.д.;