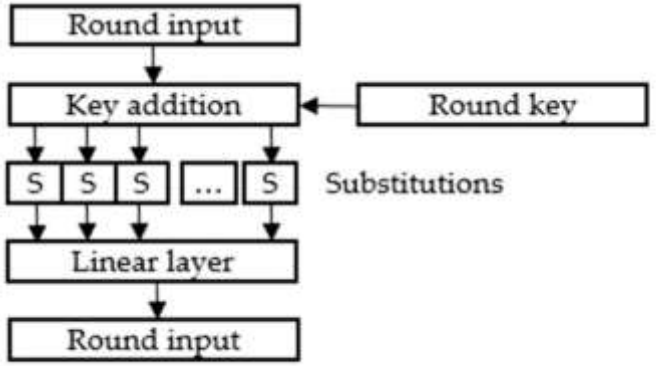
Qalqan version 2

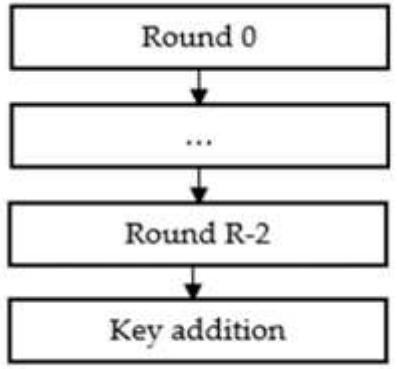
Motivation for development

- Algorithm was presented:
  - Conference RusCrypto-2021, March 23-26, 2021
  - Seminar in Kiev, November 4, 2021
  - Seminar in Almaty, November 29 2021
- Publications:
  - Анализ криптографических свойств таблиц замен современных блочных алгоритмов симметричного шифрования, Сатпаевские чтения - 2020
  - Подходы к разработке собственного блочного алгоритма симметричного шифрования, Сатпаевские чтения - 2020
  - О некоторых методах к генерации таблиц замен блочных алгоритмов симметричного шифрования, Сатпаевские чтения - 2020
  - Принципы синтеза нелинейного узла алгоритма блочного шифрования, Вестник КазНИТУ №6(142)
  - Алгоритм шифрования Qalqan, VI международная научно-практическая конференция «Информатика и прикладная математика»
  - Cryptographic properties of a nonlinear node of a block symmetric encryption algorithm Qalqan, News of the National Academy of Sciences of the Republic of Kazakhstan, physico-mathematical series, 2021
  - About cryptographic properties of the Qalqan encryption algorithm, CEUR Workshop Proceedings 2022
  - Linear Layer Architecture Based on Cyclic Shift and XOR, Symmetry, 2023, 15(8)

Architecture of Qalqan (initially)

- SP-network
- Block size: 128 bits
- Key length: 256..1024 bits
- Number of rounds: 17..23
  - N=17+($KLen$−256)/128
- Key addition modulo 2^{128} in the first and last rounds
- Key addition modulo 2 in middle rounds





Improvements

- Block lengths of 256 and 512 bits added
  - Decreases collisions in hash function mode
  - Improves speed of parallel gamma generators
- New S-box with maximum cycle length developed
- Key addition operation switched
  - Makes it easier to strictly prove security
- Linear layer totally remastered

New S-box

- Maximum table of linear approximations: 32;
- Maximum differential table: 4;
- Degree of Zhegalkin polynomial: 7;
- Minimum distance to linear statistical analogues: 112;
- Avalanche criterion: 120;
- Minimum cycle: 256.

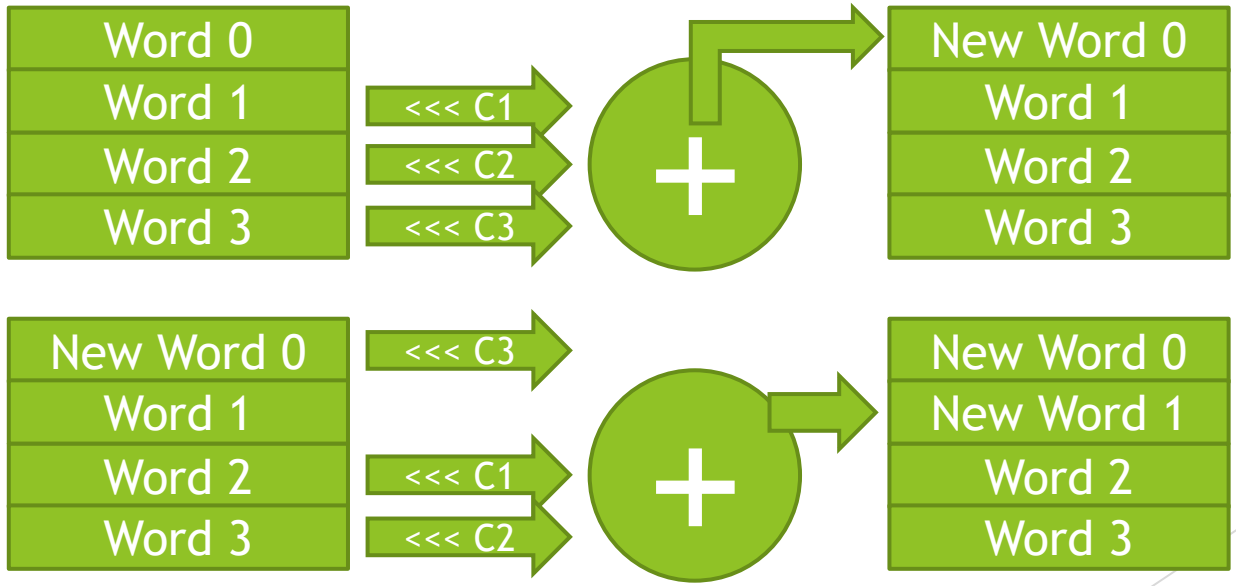
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	ce	cf	1a	56	a4	21	82	30	fb	03	6d	88	e8	ac	b1	0c
1	00	17	7c	d6	4b	bf	ed	77	dd	7d	ff	12	25	6b	af	75
2	a9	a7	76	d8	97	79	c2	ad	58	34	22	38	0b	1d	46	f1
3	13	d4	43	1e	02	c6	a0	a2	6f	3e	48	66	2a	81	47	e1
4	29	4c	2e	ba	92	0f	c5	6c	36	06	41	9e	c8	31	2b	f3
5	85	40	b3	5f	b8	19	b5	3c	78	ea	73	7e	8a	0e	05	51
6	74	d0	c3	e9	5c	5b	a6	ee	a8	ef	ca	20	f9	a1	f8	a3
7	4a	db	b6	61	8d	2f	9a	18	bc	60	3d	98	5e	9c	0d	c0
8	69	53	8f	28	be	da	f4	67	e0	f0	7a	33	1f	fc	9f	84
9	b2	9d	aa	5a	5d	ab	e6	35	cd	1b	65	70	68	4f	04	91
a	3f	f6	89	c4	24	d3	52	4e	f5	49	71	54	27	3a	b7	bd
b	95	72	dc	d7	44	32	96	eb	ec	d9	ae	d1	7f	94	55	64
c	93	8b	c1	b0	1c	e2	09	08	87	37	50	90	fa	c7	de	16
d	fd	42	0a	e3	cc	57	b9	9b	01	df	2d	11	d5	fe	2c	15
e	8c	bb	10	14	f2	80	4d	8e	3b	62	6a	d2	e4	39	a5	cb
f	f7	6e	99	b4	63	26	e5	23	86	07	e7	59	7b	45	c9	83

Linear layer

- Primitive: $g_j : a^{(n+1)} = g_j\left(a^{(n)}\right) \Leftrightarrow a_k^{(n+1)} = \begin{cases} \bigoplus_{i=0}^{u-1}\left(a_{i+j \bmod u}^{(n)} \lll C_i\right), k = j \\ a_k^{(n)}, k \neq j \end{cases}$
- Linear function: $f(a) = g_{(0)}(a) \circ \ldots \circ g_{(u-1)}(a)$

Block size	Shift values
128	1, 17, 14
256	3, 5, 11, 21, 16, 30, 19
512	4, 0, 22, 27, 47, 4, 61

- Illustration:



Bits ac lock

$$\begin{array}{c} 0 \\ \emptyset \\ \emptyset \\ \emptyset \end{array} \Rightarrow \begin{array}{c} a \\ a+d \\ a+c, a+2d \\ a+b, a+3d \end{array} \Rightarrow \begin{array}{c} 2a, a+2c, a+c+2d, a+4d \\ a+b+2d, a+2c+d, a+5d \\ 2a+2d, a+2b, a+3c, a+c+4d, a+6d \\ a+2b+d, a+b+2c, a+b+4d, a+7d \end{array}$$

$$\begin{array}{c} \emptyset \\ 0 \\ \emptyset \\ \emptyset \end{array} \Rightarrow \begin{array}{c} b \\ a, b+d \\ a+d, b+c, b+2d \\ a+c, a+2d, 2b, b+3d \end{array} \Rightarrow \begin{array}{c} a+3d, b+2c, b+c+2d, b+4d \\ 2a, a+2c, a+c+2d, a+4d, 2b+2d, b+2c+d, b+5d \\ a+2c+d, a+5d, 3b, b+3c, b+c+4d, b+6d \\ 2a+2d, a+2b, a+3c, a+c+4d, a+6d, 3b+d, 2b+2c, 2b+4d, b+7d \end{array}$$

$$\begin{array}{c} \emptyset \\ \emptyset \\ 0 \\ \emptyset \end{array} \Rightarrow \begin{array}{c} c \\ b, c+d \\ a, b+d, 2c, c+2d \\ a+d, b+2d, c+3d \end{array} \Rightarrow \begin{array}{c} a+2d, 2b, b+3d, 3c, 2c+2d, c+4d \\ a+3d, b+2c, b+4d, 3c+d, c+5d \\ 2a, a+2c, a+4d, 2b+c, 2b+2d, b+2c+d, b+5d, 4c, 2c+4d, c+6d \\ a+2c+d, a+5d, 3b, 2b+c+d, b+6d, c+7d \end{array}$$

$$\begin{array}{c} \emptyset \\ \emptyset \\ \emptyset \\ 0 \end{array} \Rightarrow \begin{array}{c} d \\ c, 2d \\ b, 3d \\ a, 2c, c+2d, 4d \end{array} \Rightarrow \begin{array}{c} b+2d, 2c+d, 5d \\ a+2d, 2b, 3c, c+4d, 6d \\ 2b+d, b+2c, b+4d, 7d \\ 2a, a+2c, a+4d, 2b+c, 4c, 2c+4d, c+6d, 8d \end{array}$$

Branch number

- Differential branch number: $B(r) = min_{a,b \neq a}\{w(a \oplus b) + w(r(a) \oplus r(b))\}$
- Examples of input and output blocks with the lowest total number of active bytes:

	Input with 3 Active Bytes	
Function input:	84 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00	$w = 3$
Function output:	00 00 00 00 00 00 00 00 01 00 00 00 00 40 00 00	$w = 2$
	Input with 3 Active Bytes	
Function input:	01 10 00 00 00 10 00 00 40 00 00 00 00 00 00 00	$w = 4$
Function output:	00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00	$w = 1$

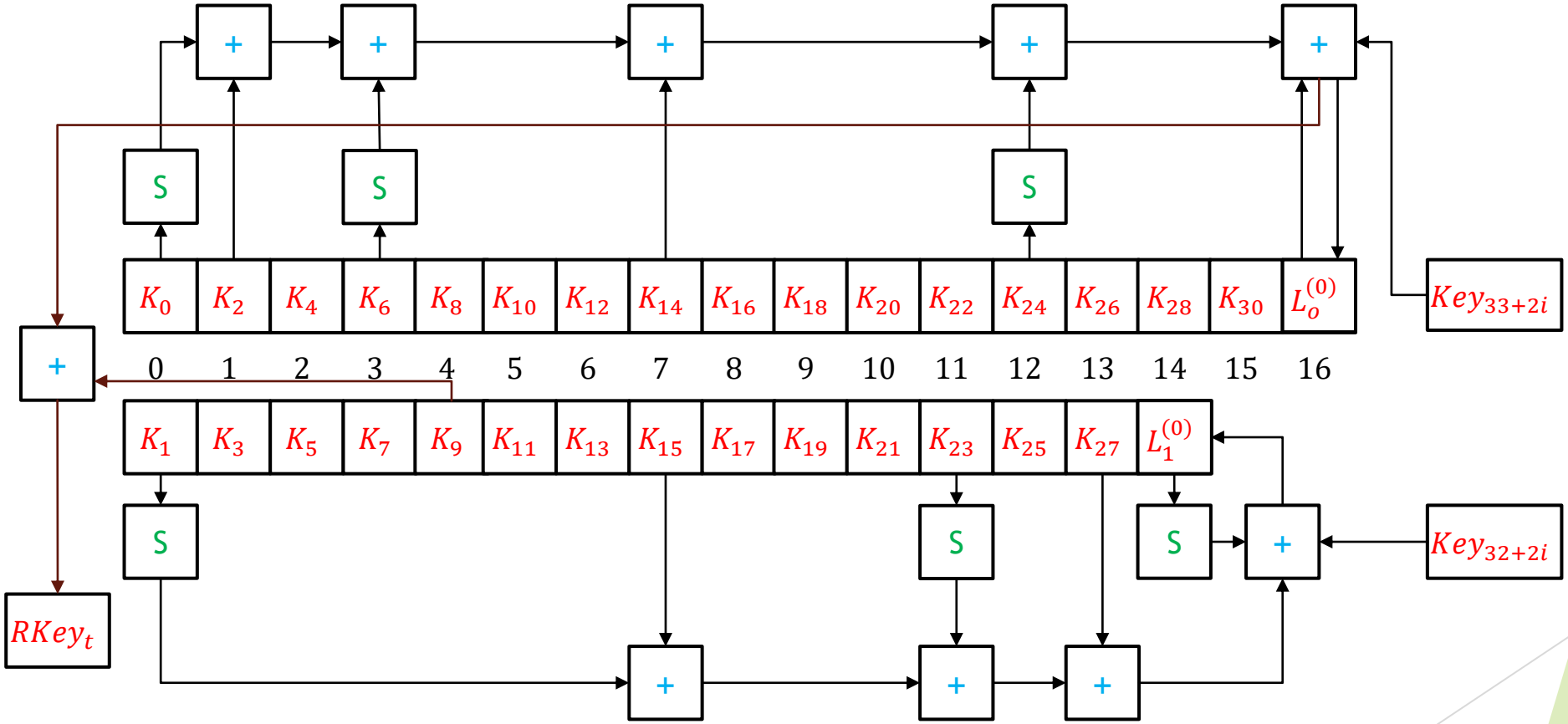
- Branch index of 4-word block in Qalqan is 5 (similar to AES)

Speed of novel linear function

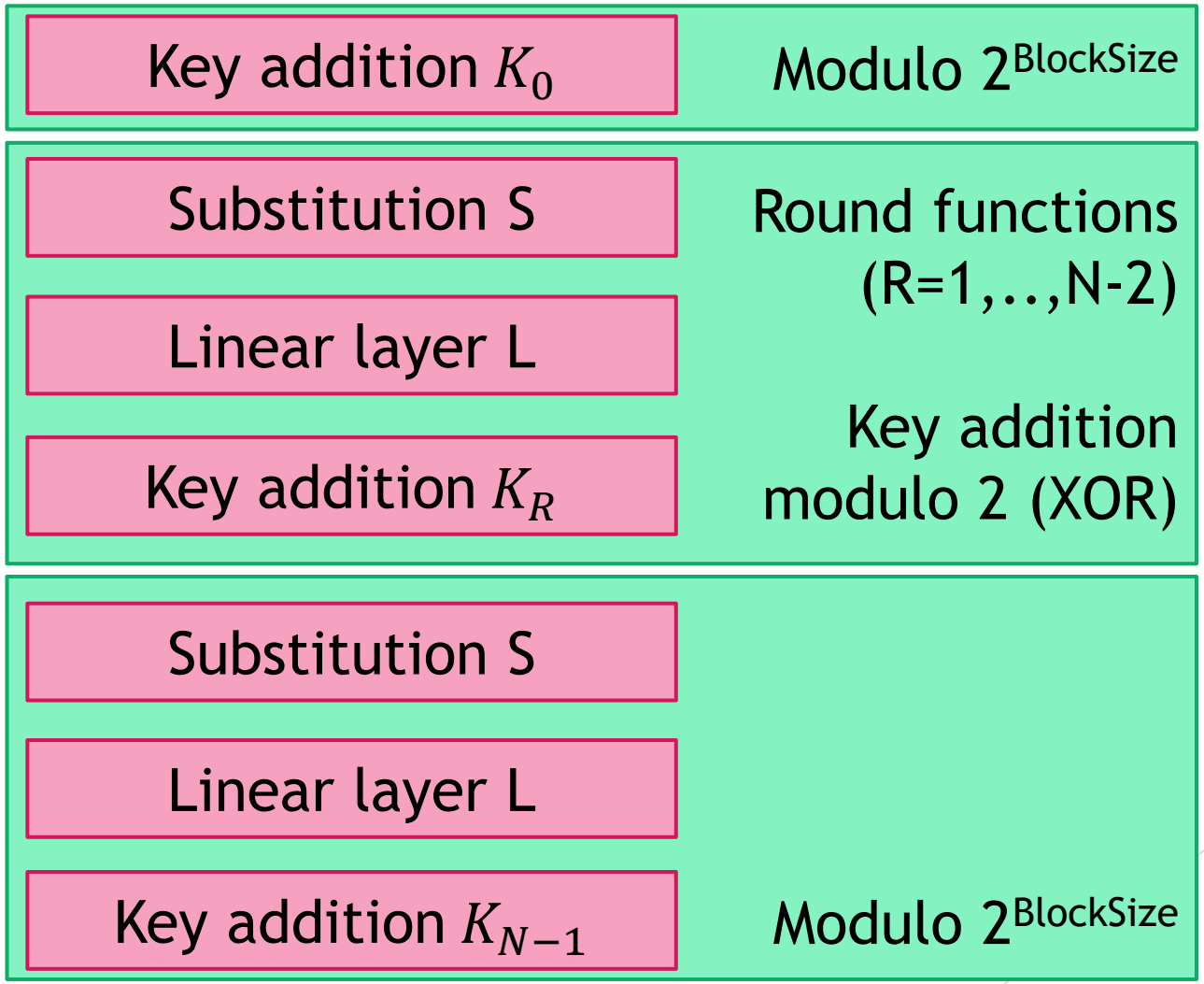
- Experiment: AES-256-LF, Rijndael-256/256-LF
- Shift values: {0,1,7,14}
- No optimizations that cost memory
- Visual Studio
  - /Ox (Favor Speed)
  - /Oi (Enable Intrinsic Functions)
  - /Ot (Favor Fast Code)

No.	Algorithm (128 Bit Block)	Time for 10 Million Runs, ms	Ratio
1	AES-256	249.4	1.216
2	AES-256-LF	205.1	0.822
No.	**Algorithm (128 Bit Block)**	**Time for 10 Million Runs, ms**	**Ratio**
3	Rijndael-256/256	474.5	1.107
4	Rijndael-256/256-LF	428.7	0.903

Key expansion



General view of encryption



Security and performance

- Differential analysis: resistant after 4 rounds
- Linear analysis: resistant after 4 rounds
- Low memory requirements (less than 1 Kb)
- Key expansion on-the-go
- Effective in both software and hardware implementations