Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Алгоритм шифрования QALQAN

Горлов Лев, Ибраев Ренат
Научно-исследовательская лаборатория
информационной безопасности

СӘТБАЕВ УНИВЕРСИТЕТІ
SATBAYEV UNIVERSITY

Цель и задачи проекта

- Создание национального стандарта шифрования Республики Казахстан
- Устранение зависимости Республики Казахстан от иностранных институтов информационной безопасности
- Развитие научного потенциала в области теоретической криптографии

Основные параметры алгоритма QALQAN

- Длина блока: 128 бит
- Длина ключа: 256..1024 бита (шаг 128 бит)
- Количество раундов: 17..23
  N=17+($KLen$−256)/128

Подходы к разработке

- Принцип перемешивания и рассеивания
- Использование простых и хорошо исследованных примитивов
- Переменная длина ключа
- Различная архитектура для шифрования и разворачивания ключа
- Эффективность программной и аппаратной реализации

Нелинейный блок

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

Нелинейный блок: характеристики

- Максимум абсолютных значений таблицы линейных аппроксимаций: 32.
- Максимум дифференциальной таблицы по XOR: 4.
- Максимум дифференциальной таблицы по сложению: 8.
- Степень полинома Жегалкина координатных булевых функций: 7.
- Расстояние до класса аффинных функций: 112.

Нелинейный блок: метод генерации

1. Генерация входных параметров с использованием ГСЧ.
2. Основное преобразование:
    1. Взятие обратного элемента в поле.
    2. Линейное преобразование над полем GF2.
    3. Наложение маски по модулю 2.
3. Проверка свойств:
    1. Устойчивость к дифференциальному анализу.
    2. Устойчивость к линейному анализу.
    3. Лавинный критерий.
    4. Алгебраическая степень.
    5. Расстояние до класса линейных функций.

Линейная операция

Архитектура «Квадрат»

$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$B_{0,3}$
$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$
$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$B_{2,3}$
$B_{3,0}$	$B_{3,1}$	$B_{3,2}$	$B_{3,3}$

Линейная операция

Архитектура «Квадрат»

Определяющие байты

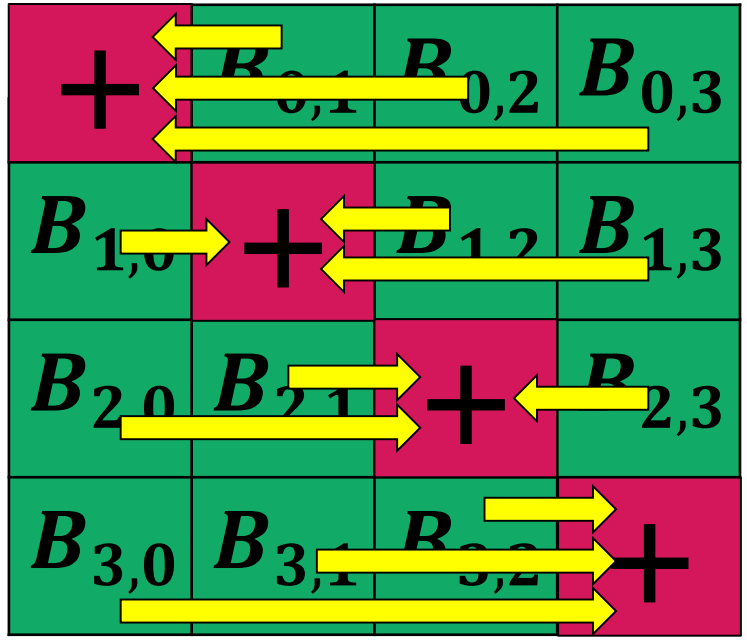
$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$B_{0,3}$
$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$
$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$B_{2,3}$
$B_{3,0}$	$B_{3,1}$	$B_{3,2}$	$B_{3,3}$

Линейная операция

Архитектура «Квадрат»

Определяющие байты

Сложение («впитывание»)



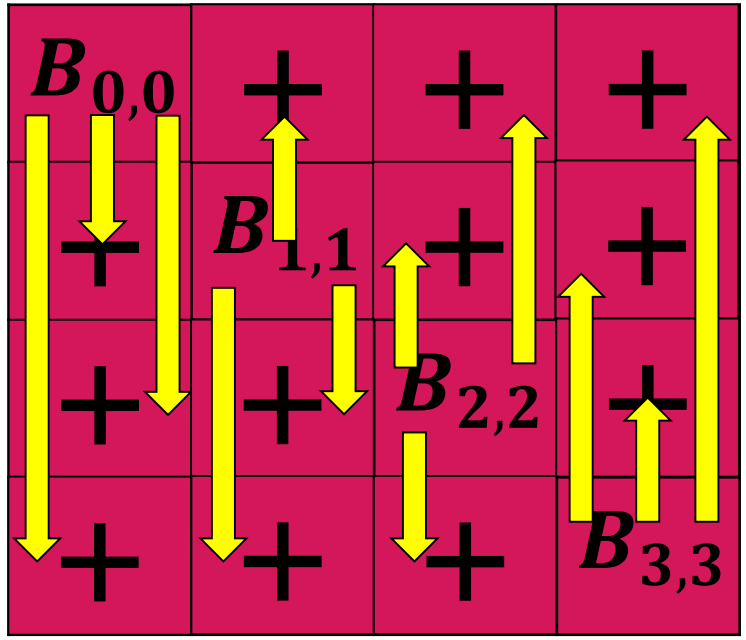
Линейная операция

Архитектура «Квадрат»

Определяющие байты

Сложение («впитывание»)

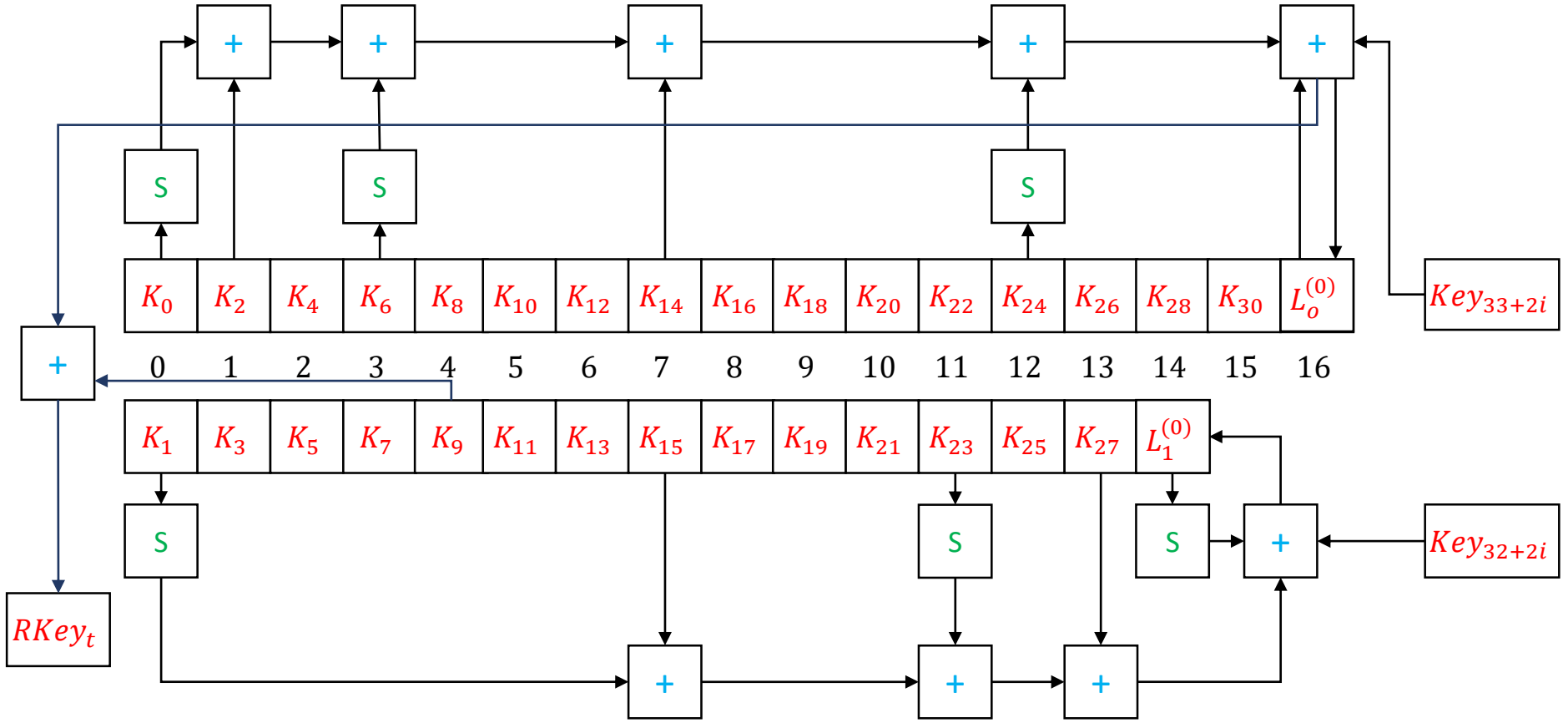
Наложение («распространение»)



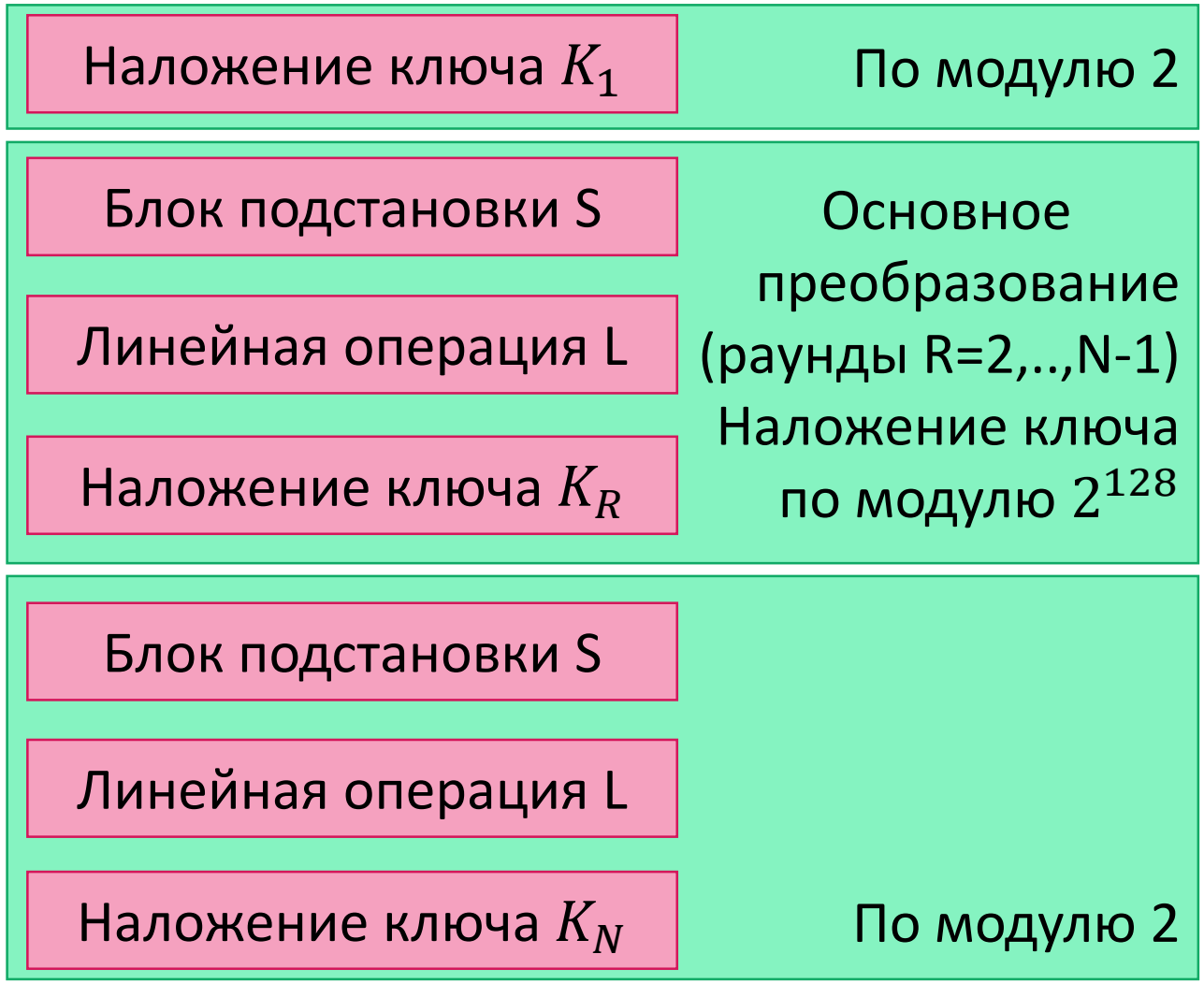
Генерация раундовых ключей

- Алгоритм принимает на вход ключи длиной от 256 до 1024 битов с шагом 128.
- Количество раундов зависит от длины ключа: N=17+⌊($KLen$−256)/128⌋
- Для ключа длиной 256 бит требуется развернуть 2176 битов раундовых ключей.
- Для ключа длиной 1024 бита требуется развернуть 2944 бита раундовых ключей.

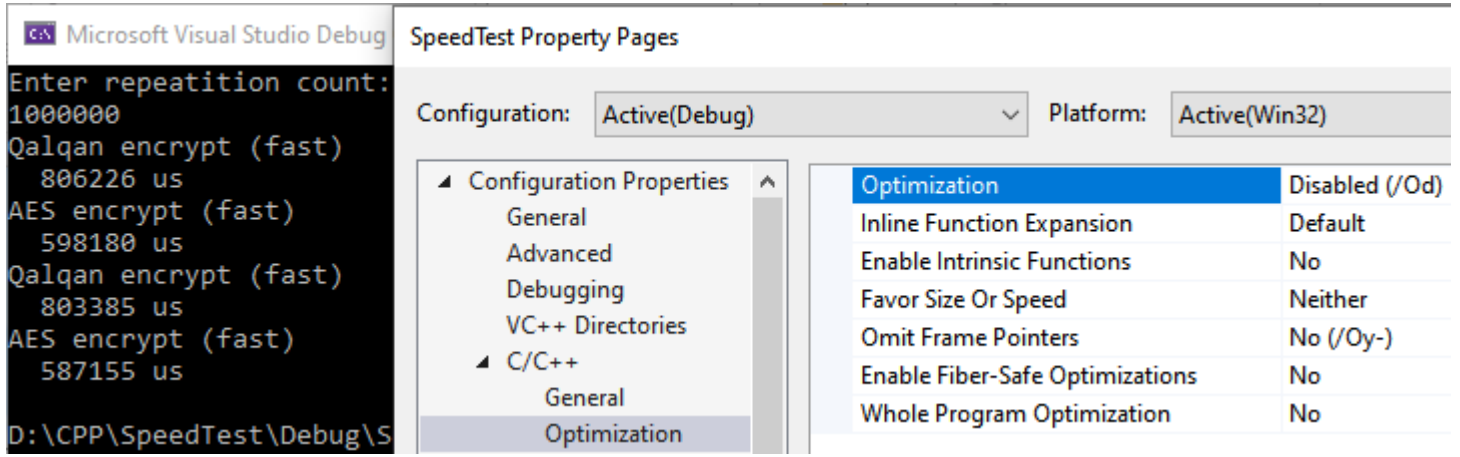
Генерация раундовых ключей

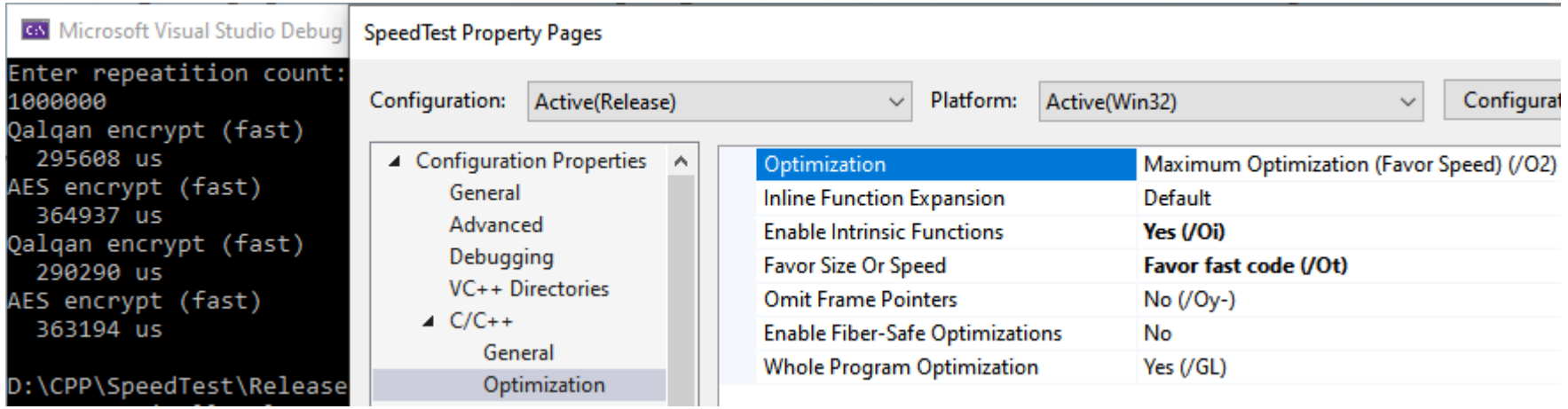


Архитектура алгоритма: LSX



Быстродействие (сравнение с AES)





Независимая экспертиза

Институт информационных и вычислительных технологий Комитета науки МОН РК:

Дифференциальный анализ на 3-раундовый алгоритм позволяет определить ключ с вероятностью 2^{-78}, после 4 раунда вероятность составляет 2^{-312}.

Линейный анализ требует 2^{259} пар открытых и шифрованных текстов.

Лавинный эффект обеспечивается на 4 раунде.

Результат

- Защита от дифференциальных атак после 4 раундов (из 17)
- Защита от линейных атак после 4 раундов
- Быстродействие на уровне AES
- Низкие требования к памяти (менее 1 Кб)
- Возможность эффективной реализации на ПЛИС
- Разворачивание ключа на лету

Контактная информация

Электронная почта:

renafm@mail.ru

lev.gorlov@gmail.com

Телефоны:

+7 747 270 2227

+7 747 166 5569