Алгоритм блочного симметричного шифрования

Qalqan

подходы к разработке, идеи, решения

Актуальность разработки: скептицизм, теория, практика

- Нужен ли алгоритм? Альтернативы:
  - США и мир: AES – шедевр науки и монументальная работа. Объект всеобщего интереса
  - РФ: Кузнечик – конкурс «найди закладку»
  - РФ: ГОСТ 28147-89 устарел
  - Украина: Калина (1 и 2) – пример правильного процесса
  - Узбекистан: O‘z DSt 1105:2009
- Кто может разработать и доказать?
  - Пустота в области науки (хотя есть 120+ статей за 20 лет)
  - Сложности оценки: у нас некому (?), КГБ не расскажет, Шнайеру не дозвонились
- А если взять и сделать?

АНБ тоже не расскажет!

Актуальность разработки: какие проблемы решаем

- Правильная работа в научной области
  - Открытость
  - Обмен знаниями
  - Ориентированность на результат
  - Востребованность и популяризация
- Разработка СКЗИ
  - Выгоды тем, кто правда может
  - Вопросы к тем, кто не хочет
  - Возможности для взращивания прикладных специалистов
- Потребители
  - Что мы потребляем?
  - Чьи риски и ответственность?
  - Базовая грамотность в области ИБ

Как разработать алгоритм?

- Выбор:
  - Архитектуры
  - Операций
  - Длин ключей и блока
- Заранее подумать:
  - Обоснование стойкости
  - Запас стойкости
  - Эксплуатационные характеристики

- Выбрали:
  - LSX
  - ADD/SUB, XOR, SB, CROTL
  - $\{256 + S * 128, S = 0..6\}; \{128, 256, 512\}$
- Принципы:
  - Изученные подходы
  - Расширяемость (раунды, длины)
  - Простые операции, поддержка всех платформ

Что получилось вначале

Наложение ключа K_1 — По модулю 2

Блок подстановки S

Линейная операция L

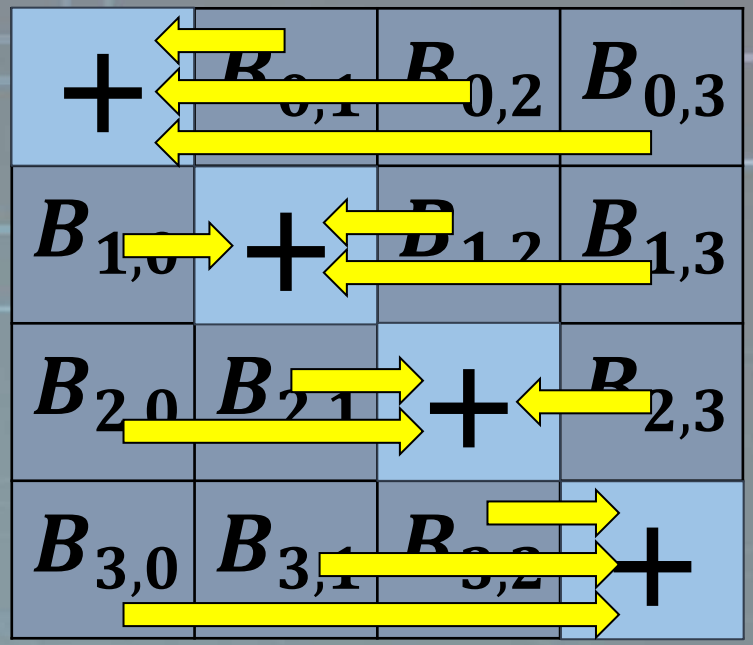
Наложение ключа K_R

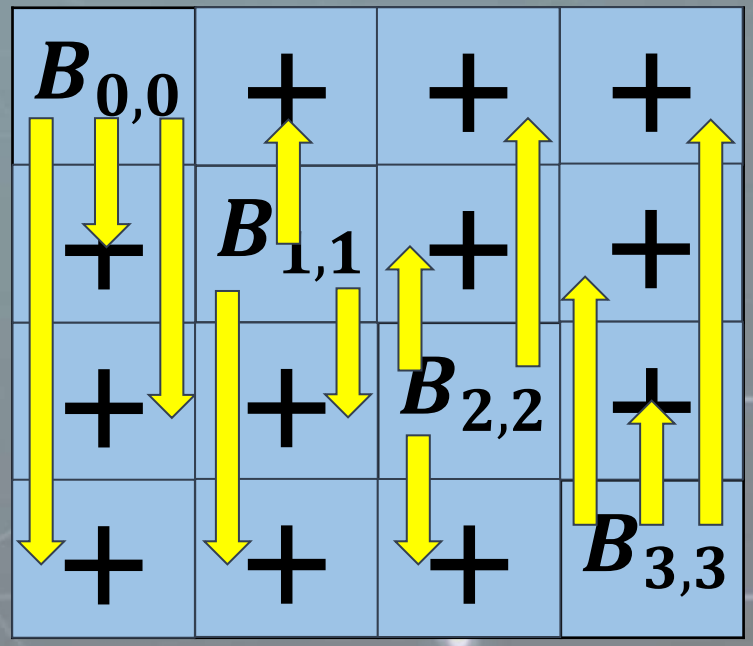
Основное преобразование (раунды R=2,..,N-1) Наложение ключа по модулю 2^{128}

Блок подстановки S

Линейная операция L

Наложение ключа K_N — По модулю 2





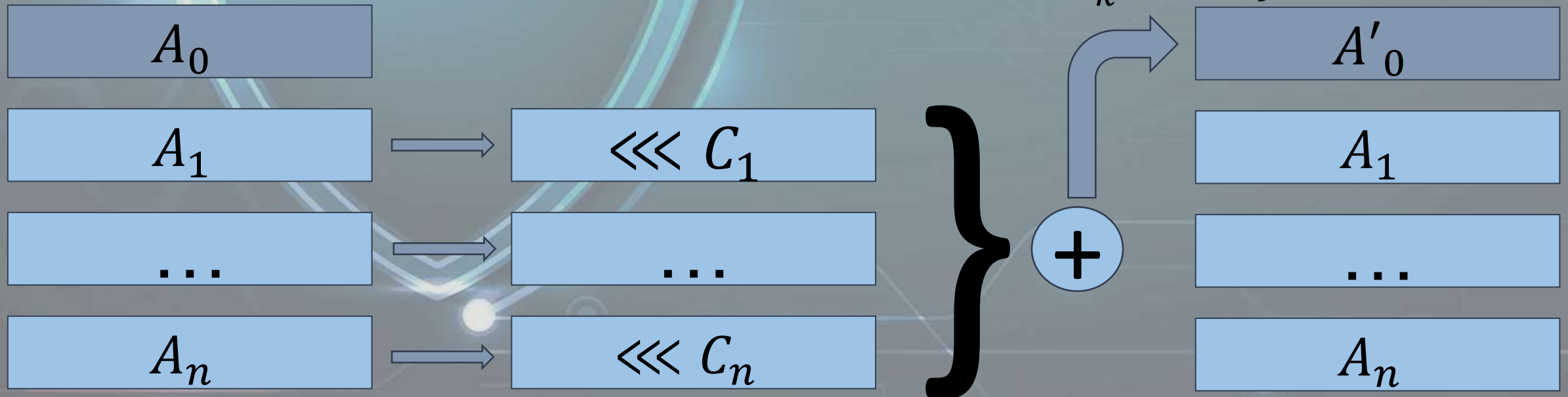
История появления второй версии

- А.Н.Алексейчук, Л.В.Ковальчук, С.В.Яковлев и др.:
  - Проблема доказательства стойкости из-за сложения
  - Размер блока для хеширования
- Serhii Yakovliev, Mykhailo Stolovych: On the Security of Qalqan Cipher Against Differential Cryptanalysis :
  - Плохие частные случаи
  - Цикл длины 2 в подстановке

Вторая версия

- Подход “Wide trail”, индекс ветвления не менее 5.
- Смена линейной функции:

$$g_j: a^{(n+1)} = g_j\left(a^{(n)}\right) \Leftrightarrow a_k^{(n+1)} = \begin{matrix} \oplus_{i=0}^{u-1}\left(a_{i+j \bmod u}^{(n)} \lll C_i\right), k = j \\ a_k^{(n)}, k \neq j \end{matrix}$$



Что же со стойкостью?

- Оценка в соответствии с Wide trail strategy:
  - Нелинейная функция не хуже по характеристикам
  - Исходные данные для генерации S-box по методу К.Найберг: poly = $x^8 + x^6 + x^5 + x^4 + x^2 + x^1 + 1$ (т.е.177_{16}), matrix = $4c_{16}$, mask = $d1_{16}$.
  - Индекс ветвления не ниже 5: Linear Layer Architecture Based on Cyclic Shift and XOR, Symmetry, 2023.
- Отзывы от учёных РК, Украины и Индии.
- Полный доступ ко всем статьям и материалам.
- Никаких бэкдоров, понятная структура.

Алгоритм блочного симметричного шифрования

Qalqan

подходы к разработке, идеи, решения