Атака со связанными ключами на один из шифров сети Фейстеля

Исаев К.М.
Руководитель: Кирюхин В.А.

Базовая кафедра №252 - компьютерной безопасности
Институт исскусственного интеллекта
МИРЭА - Российский технологический университет

23 января 2024 г.

Задачи

1. Обзор существующих вариантов дифференциального метода криптоанализа
2. Построение дифференциальных путей шифра Khazad
3. Разработка атак на шифр
4. Определение сложности разработанных атак

Основные работы

Alex Biryukov and Ivica Nikolić, Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others, `https://eprint.iacr.org/2010/248`

В. А. Кирюхин, Атака методом бумеранга на связанных ключах на 5 раундов шифра Кузнечик, *Обозрение прикладной промышленной математики*, 26(3), 2019

Описание шифра Khazad

- Khazad - инволюционный блочный LSX шифр
- Стандартное количество раундов - 8
- Блок - 64 бит
- Ключ - 128 бит

Раундовое преобразование:
X - сложение по модулю с раундовым ключом
S - параллельное применение фиксированной байтовой подстановки
L - линейное преобразование MDS, разностный коэффициент рассеивания $\mathcal{B} = 9$

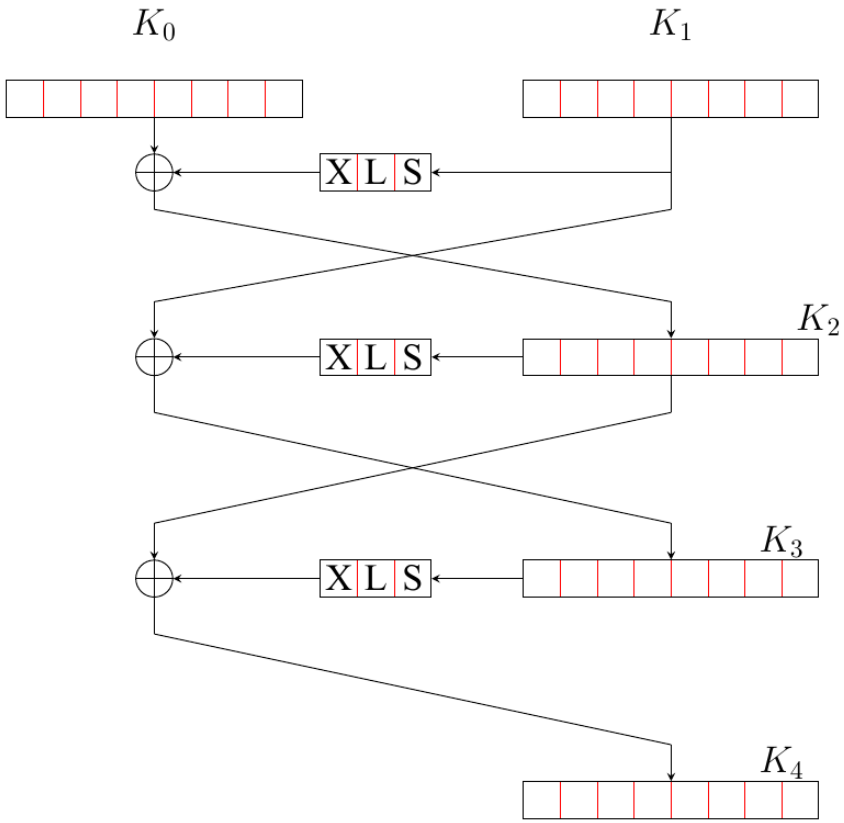
4-раундовый Khazad

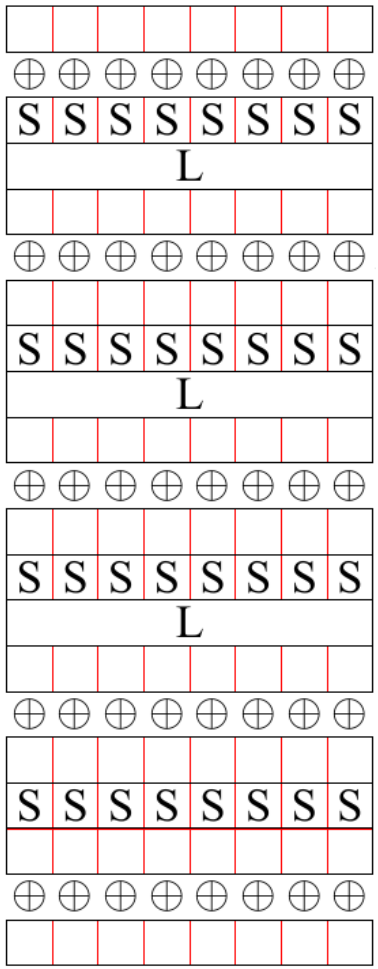
Число раундов шифрования - 4 из 8
Число раундов развертки ключа - 3 и используем части мастер-ключа в шифровании

$$E(P) = X[K^4]SX[K^3]LSX[K^2]LSX[K^1]LSX[K^0](P)$$

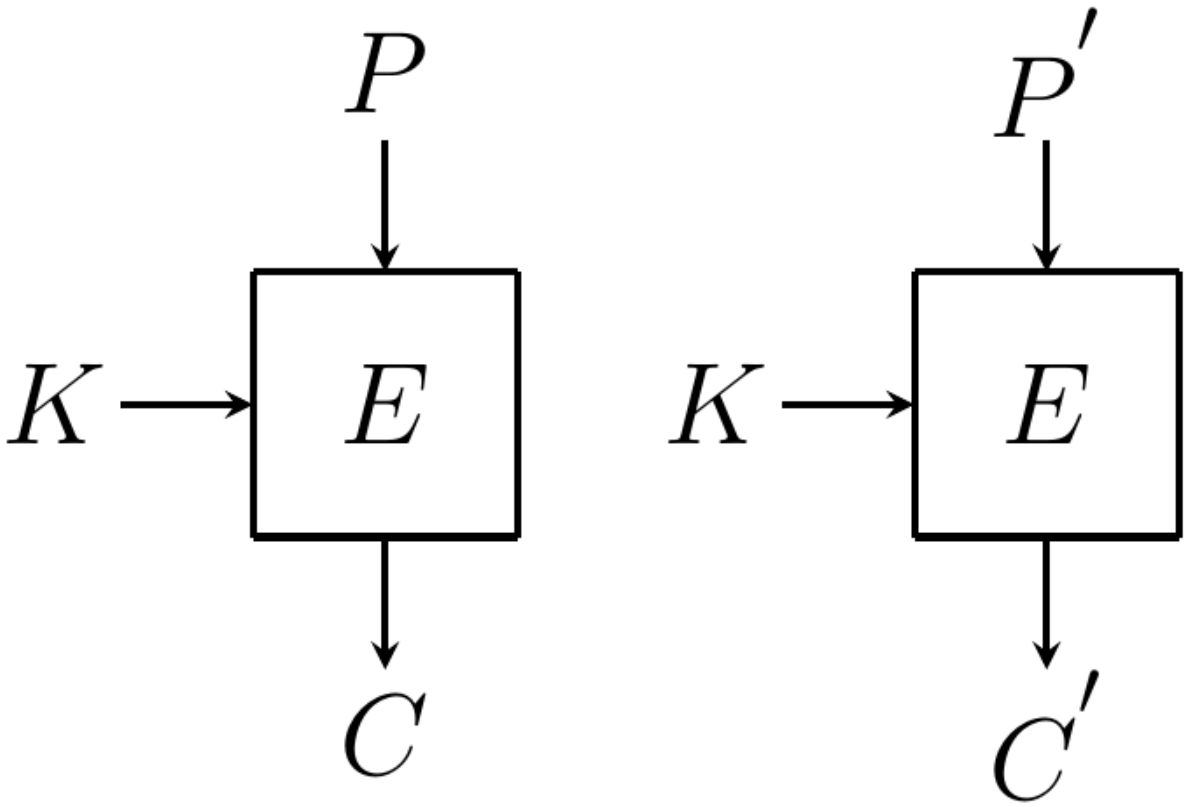
$$K^0, K^1, K^i = K^{i-2} \oplus LS(K^{i-1}), i \in \overline{2,5}$$

4-раундовый Khazad



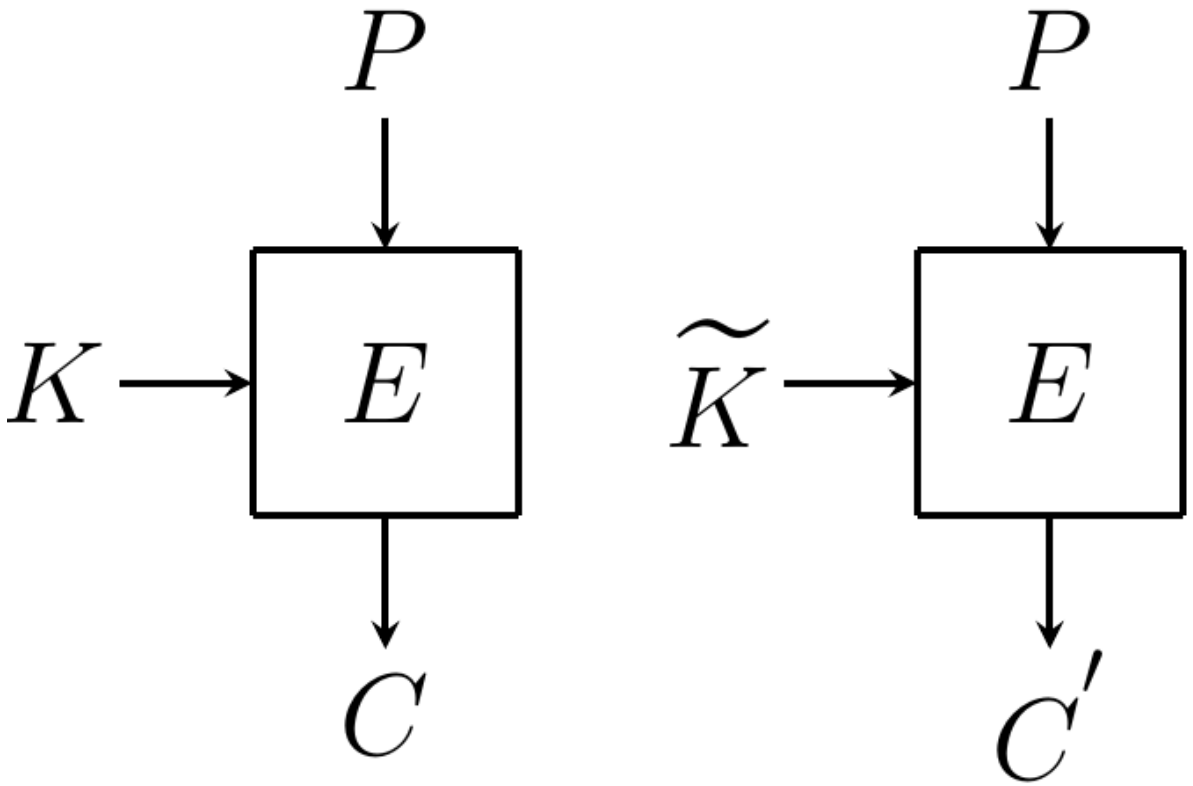


Классическая модель



Модель связанных ключей

Известно некоторое отношение между ключами.



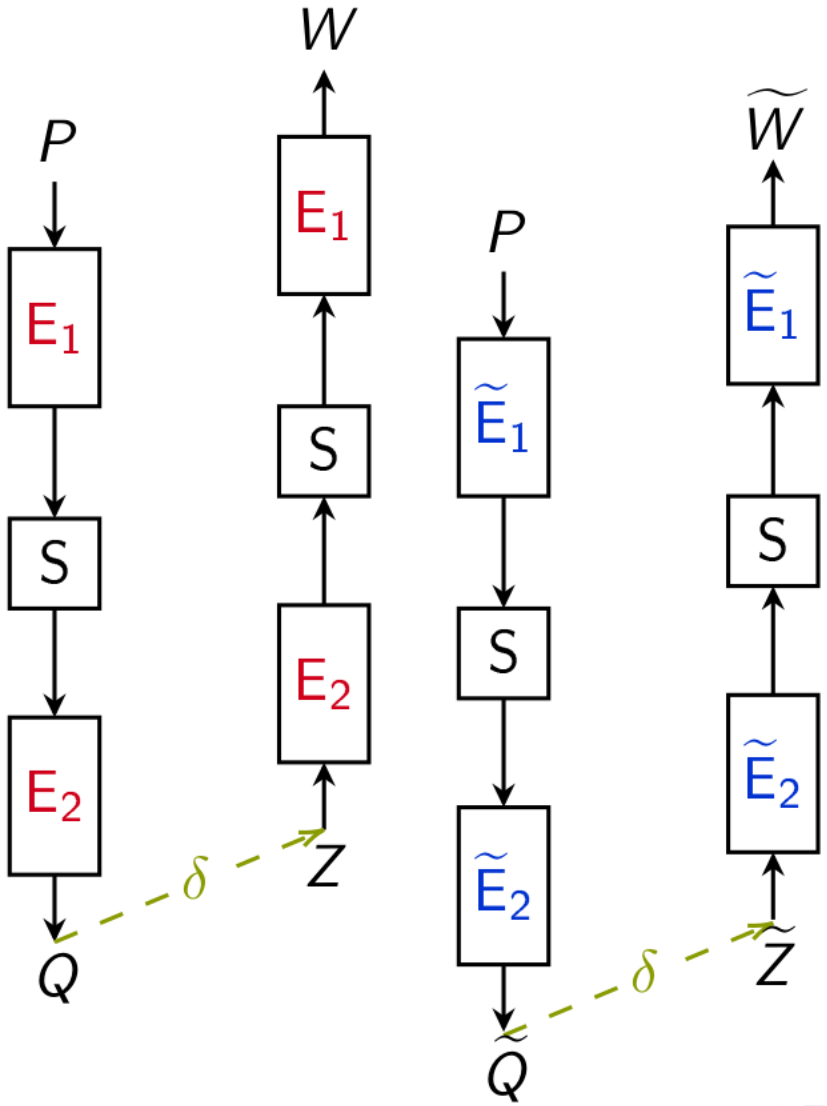
$$\Delta K = K \oplus \widetilde{K}$$

Атака: бумеранг

Делим процесс шифрования на три части:

$$E(P) = X[K^4]SX[K^3]L \circ S \circ X[K^2]LSX[K^1]LSX[K^0](P)$$

Атака: бумеранг

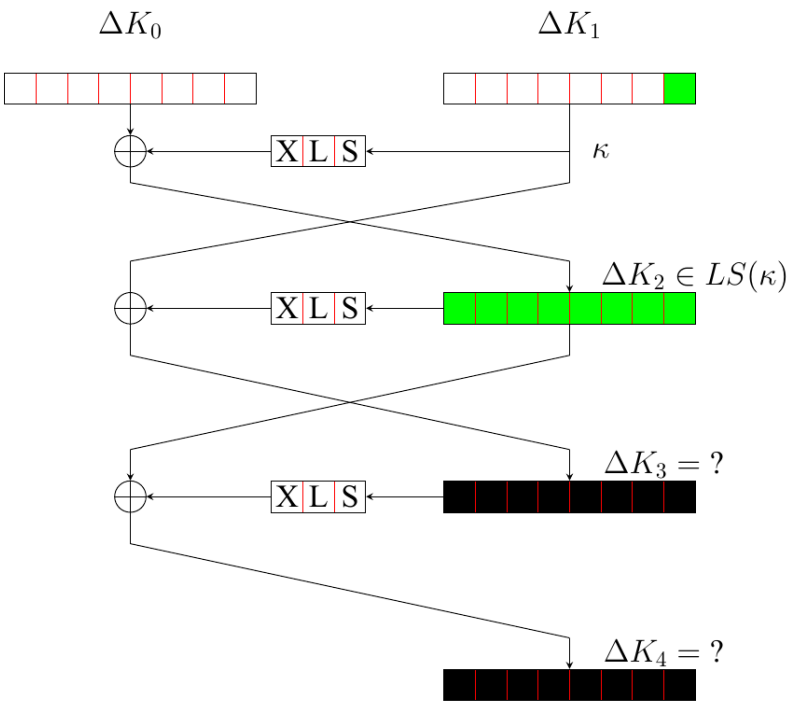


Особенности дифференциальных путей

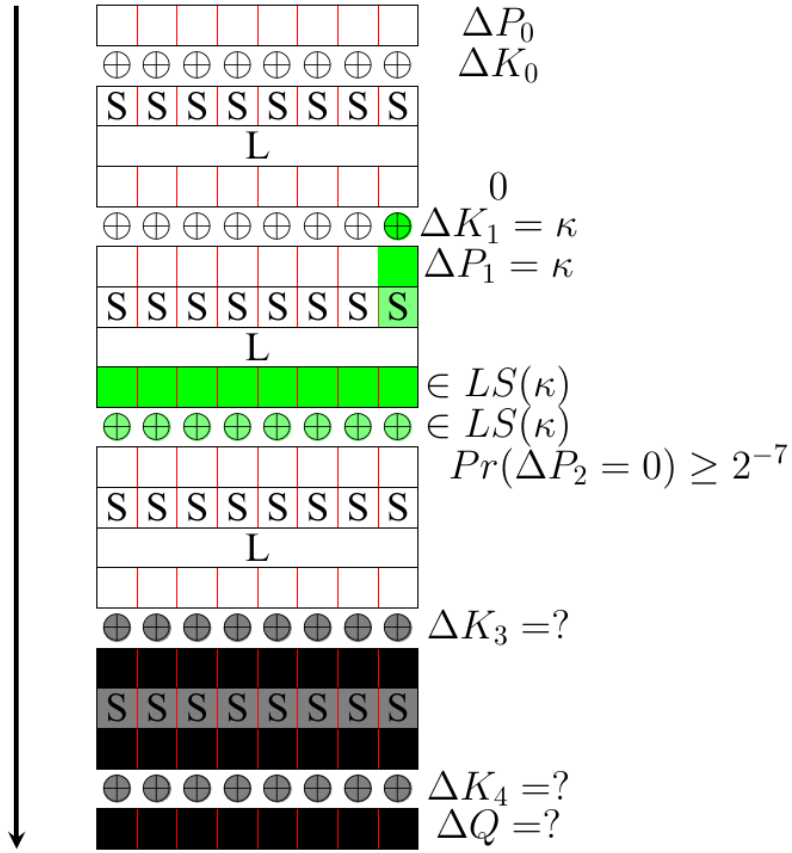
- Вниз идём на связанных ключах
- Вверх сначала идём на несвязанных ключах
- Потом снова перепрыгиваем в дифф. путь на связанных ключах через s-box switch

Атака: распространение разностей сверху-вниз

Выберем:
$\Delta K_0 = 0$,
$\Delta K_1 = \kappa$ - однобайтовая



Ключи связаны!

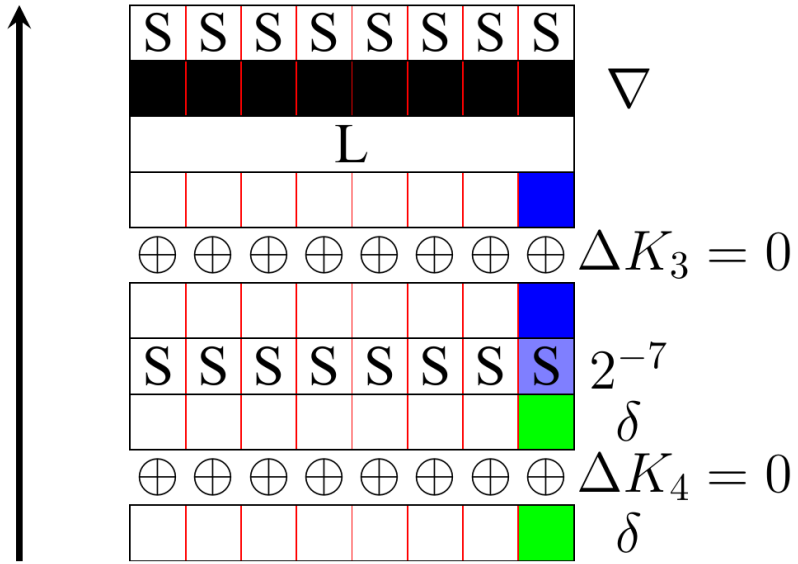


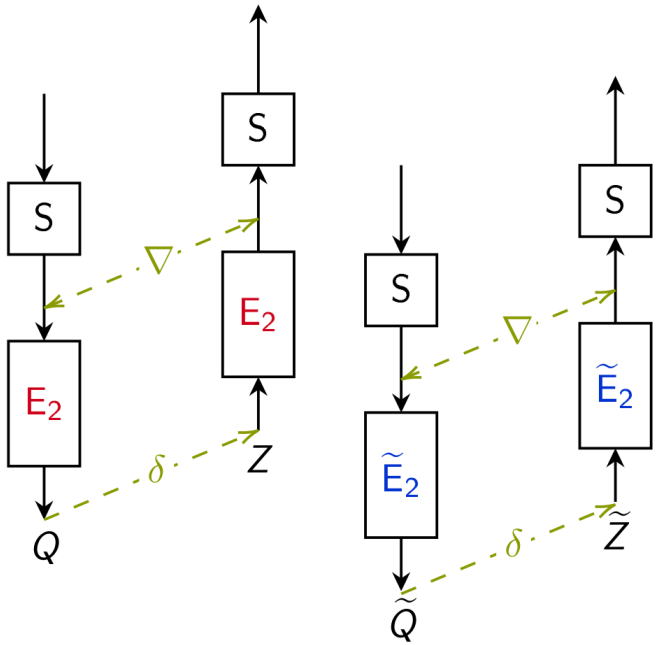
Атака: вероятность коллизии

$$Pr(X[K^2]LSX[K^1]LSX[K^0](P) \oplus$$
$$X[\widetilde{K^2}]LSX[\widetilde{K^1}]LSX[K^0](P) = 0) \geq 2^{-7}$$

Атака: распространение разностей снизу-вверх

Ключи здесь не связаны!



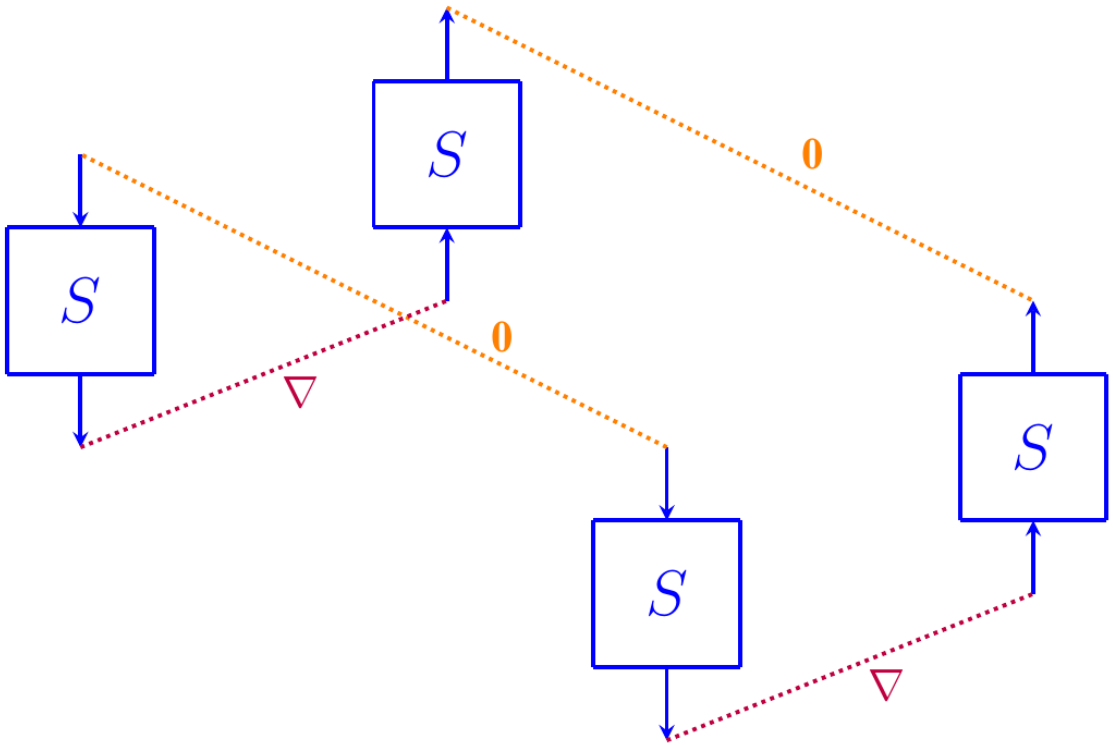


$$\nabla = LX[K^3]SX[K^4](Z) \oplus LX[K^3]SX[K^4](Q),$$

$$\tilde{\nabla} = LX[K^3]SX[K^4](\tilde{Z}) \oplus LX[K^3]SX[K^4](\tilde{Q}),$$

$$Pr(\nabla = \tilde{\nabla}) \geq 2^{-7}.$$

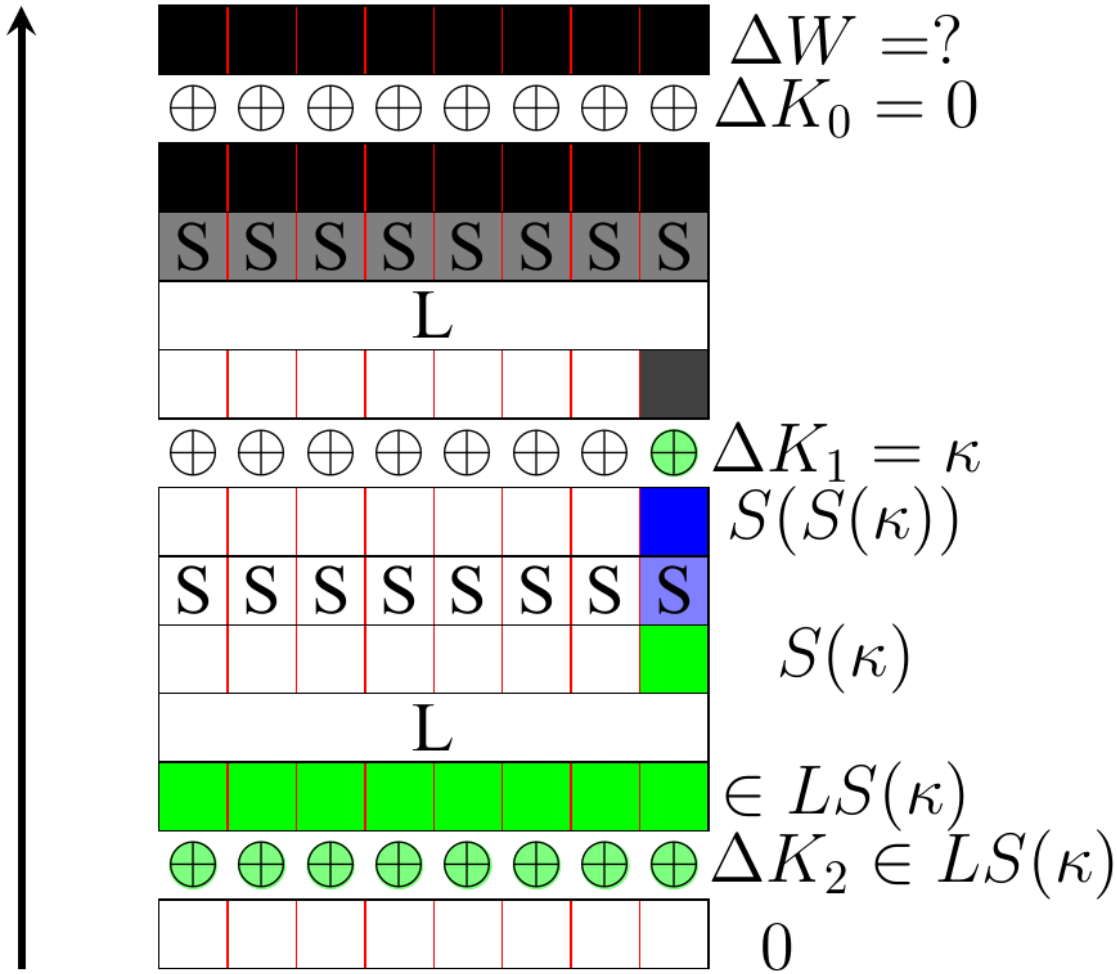
Атака: sbox switch



$$D = X[K^2]LSX[K^1]LSX[K^0](P),$$

$$Pr(S(S(D) \oplus \nabla) \oplus S(S(D \oplus 0) \oplus \nabla) = 0) = 1.$$

Дифф. путь на связанных ключах в напр. вверх



Построение множества ключей K_0

ΔY - однобайтовая разность после первого L-преобразования.

$$S(W \oplus K^0) \oplus S(\tilde{W} \oplus K^0) = L(\Delta Y)$$

Перебираем все 255 значений ΔY и решаем уравнение относительно K^0. В среднем для каждого такого уравнения будет одно решение.
Ложные ключи встретятся один раз.
Истинный ключ встретится два раза.

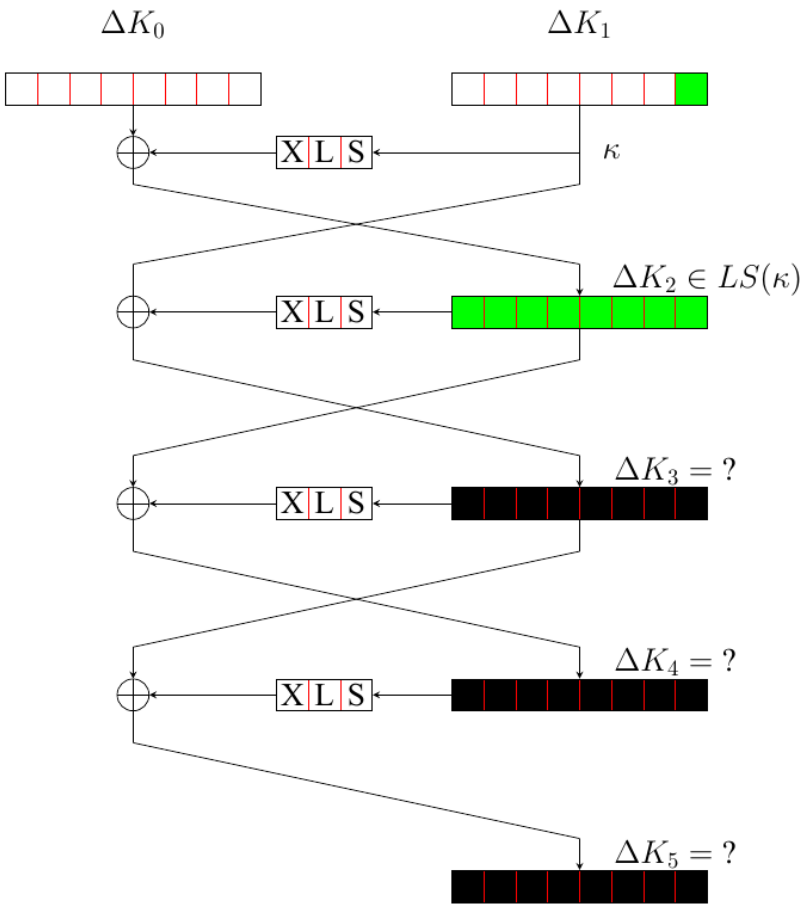
Трудоёмкость атаки

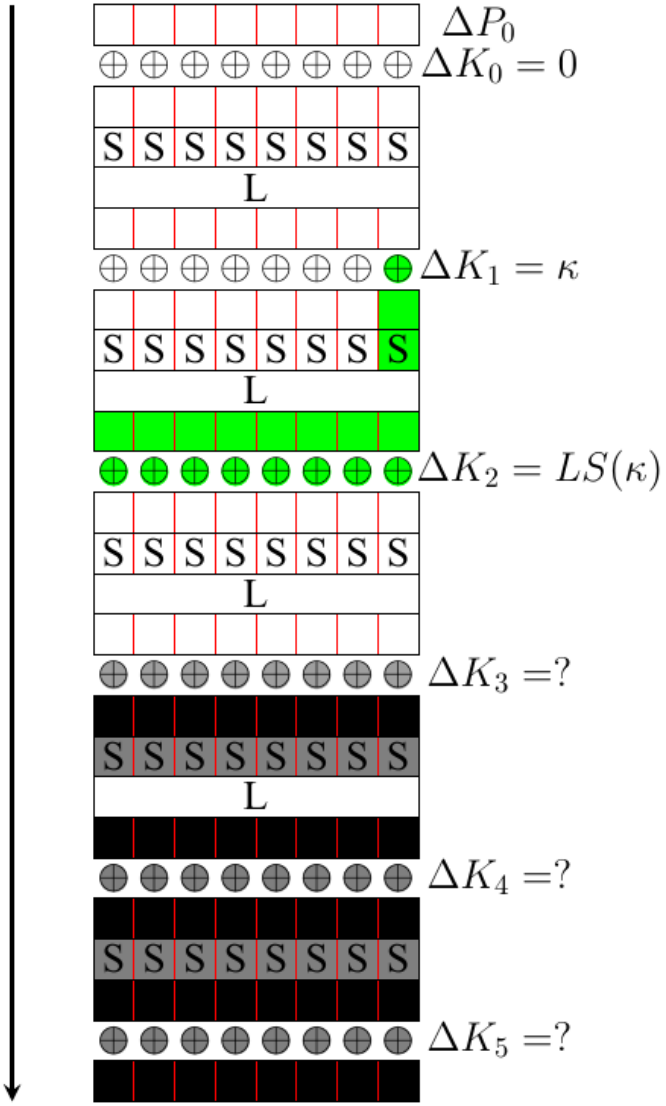
Параметр	Оценка
Связанные ключи	2
8-байтовых блоков памяти(K^0)	$2^{22} = p^{-1} \cdot 2 \cdot 255 \cdot 2^{-1}$
Операций доступа к памяти	$2^{25} = p^{-1} \cdot 2 \cdot 255 \cdot 8$
Пар OT/ШТ	$2^{17} = p^{-1} \cdot 2 \cdot 4$

Чтобы ознакомиться с программной реализацией:

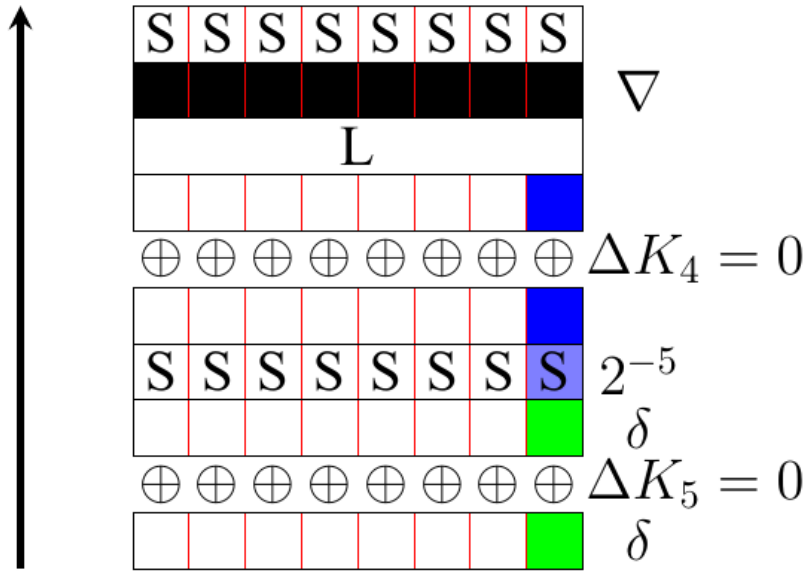
5-раундовый Khazad

Платим вероятностью $p \leq 2^{-5}$ за коллизию в 3 раунде.





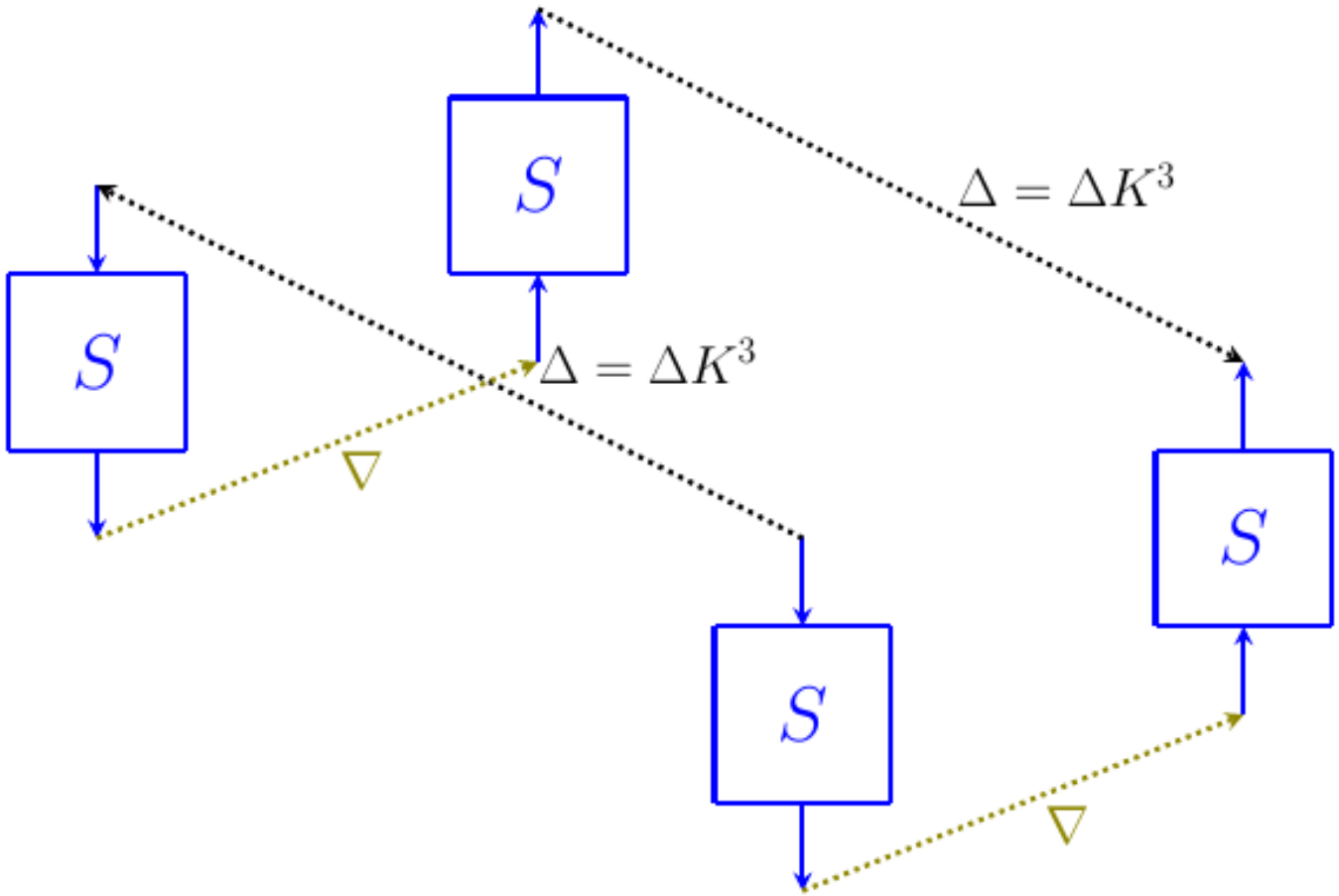
Дифф. путь на несвязанных ключах вверх



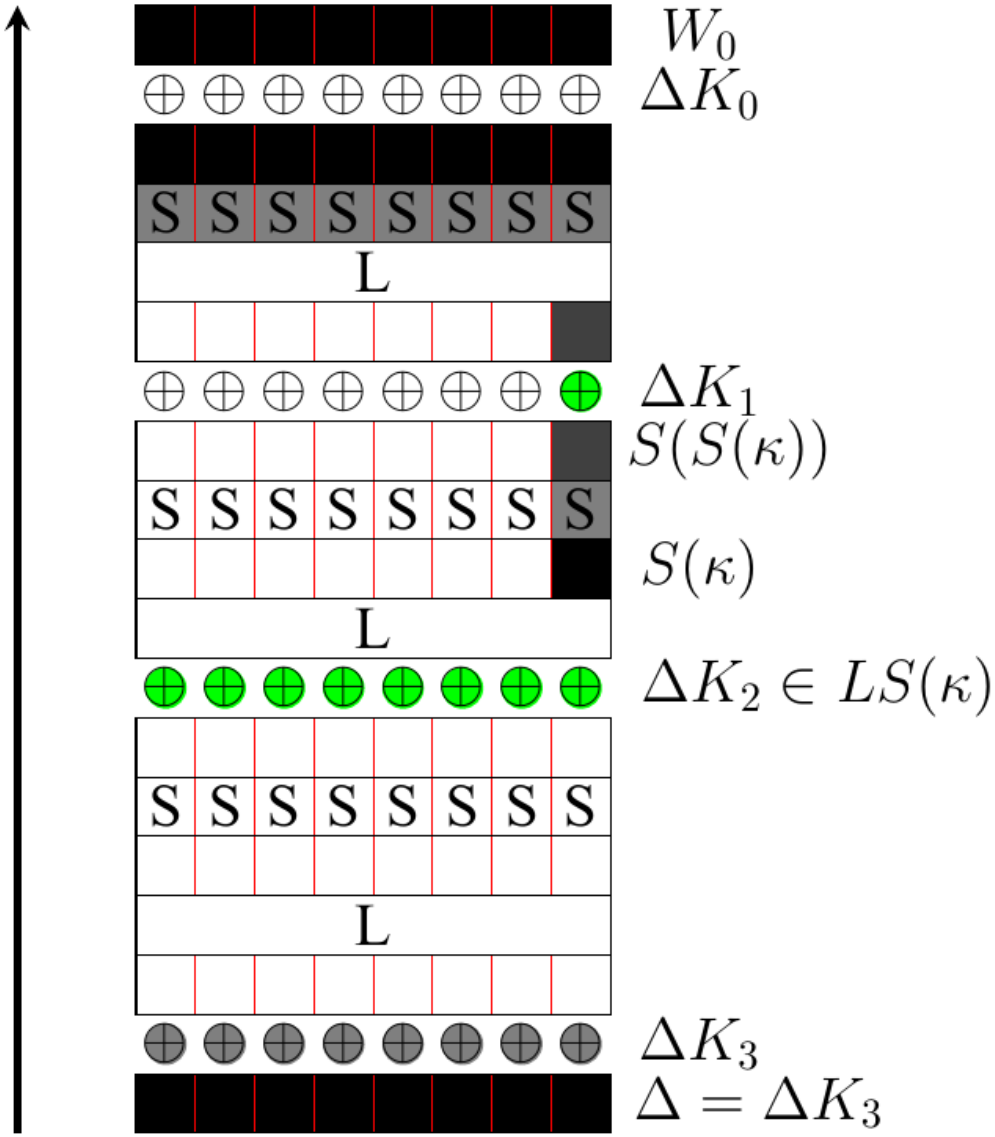
Далее на пути атаки стоит s-box switch.

S-box switch

$$D = X[K^3]LSX[K^2]LSX[K^1]LSX[K^0](P), \Delta = \Delta K_3,$$
$$Pr(S(S(D) \oplus \nabla) \oplus S(S(D \oplus \Delta) \oplus \nabla) = \Delta) \leq 2^{-40}.$$



Дифф. путь на связанных ключах вверх



Трудоёмкость

Далее схема атаки совпадает с атакой на 4 раунда. Как итог получили заметное ухудшение вероятности с оценкой в лучшем случае 2^{-50}.

Параметр	Оценка
Связанные ключи	2
8-байтовых блоков памяти(K^0)	$2^{58} = p^{-1} \cdot 2 \cdot 255 \cdot 2^{-1}$
Операций доступа к памяти	$2^{61} = p^{-1} \cdot 2 \cdot 255 \cdot 8$
Пар ОТ/ШТ	$2^{53} = p^{-1} \cdot 2 \cdot 4$

Однако, это позволяет нам соптимизировать полный перебор в атаке [A New Attack Against Khazad]. Такая комбинация атак позволяет восстановить обе части мастер-ключа и имеет суммарную сложность по времени $2^{61} + 2^{28} \approx 2^{61}$ вместо 2^{64+28} и по данным $2^{58} + 2^{8} \approx 2^{58}$ вместо полного словаря размером 2^{64}, что является серьёзным улучшением.

Результаты

- Атака со связанными ключами на 4 раунда шифра Khazad с модифицированной ключевой развёрткой, её программная реализация, оценка трудоёмкости.
- Теоретическая атака со связанными ключами на 5 раундов шифра Khazad с модифицированной ключевой развёрткой, её комбинация с уже существующей атакой в данной модели, оценка трудоёмкости.

Спасибо за внимание!