РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

О применении квантово-вычислительных методов в некоторых атаках на алгоритм «Магма»

Андрей Щербаченко

ООО «СФБ Лаб»

РусКрипто’2025
20 марта 2025

andrey.shcherbachenko@sfblaboratory.ru

Введение

Квантовые вычисления в криптографии

- Квантовые компьютеры представляют угрозу для криптографических алгоритмов

Введение

Квантовые вычисления в криптографии

- Квантовые компьютеры представляют угрозу для криптографических алгоритмов
- Универсальный метод для ключевых алгоритмов – перебор ключей за $\sqrt{2^k}$ операций с использованием алгоритма Гровера

Введение

Квантовые вычисления в криптографии

- Квантовые компьютеры представляют угрозу для криптографических алгоритмов
- Универсальный метод для ключевых алгоритмов – перебор ключей за $\sqrt{2^k}$ операций с использованием алгоритма Гровера
- Актуально исследование квантовых атак, направленных на конкретные конструктивные свойства шифров

Модели квантового противника

Модель Q1

- Противник имеет классический доступ к оракулу
- Неизвестно эффективных атак на симметричные механизмы (с трудоемкостью лучше, чем корневая)

Примеры: алгоритмы Гровера, Шора

Модели квантового противника

Модель Q1

- Противник имеет классический доступ к оракулу
- Неизвестно эффективных атак на симметричные механизмы (с трудоемкостью лучше, чем корневая)

Примеры: алгоритмы Гровера, Шора

Модель Q2

- Противник имеет квантовый доступ к оракулу
- Известны эффективные атаки на некоторые механизмы и режимы

Примеры: полиномиальные атаки на конструкции Even-Mansour, Wegman-Carter, CBC-MAC, GMAC

Алгоритм «Магма»

Ключ $K = (k_1, k_2, ..., k_8) \in V^{256}$

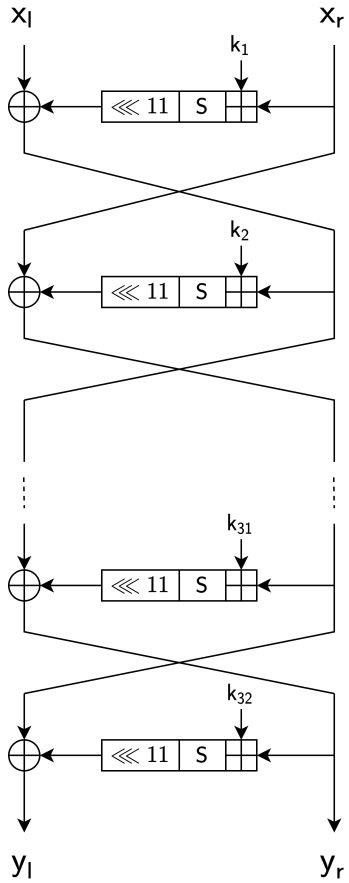
Длина блока $n = 64$ бит

Сеть Фейстеля, 32 раунда

Раундовые ключи:

$$\underbrace{k_1, ..., k_8}_{1–8}, \underbrace{k_1, ..., k_8}_{9–16}, \underbrace{k_1, ..., k_8}_{17–24}, \underbrace{k_8, ..., k_1}_{25–32}$$

ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры»



Метод Исобе

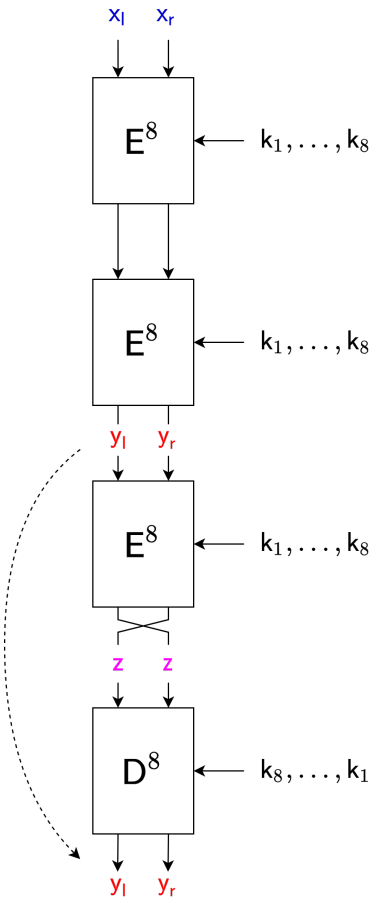
Событие типа «точка отражения»

$$E^8(E^8(E^8(X))) = z \parallel z$$

$$P_{ref} = 2^{-32}$$

Трудоемкость атаки:

$$\underbrace{2^{32}}_{\substack{\text{пар} \\ \text{от/шт}}} \left(\underbrace{2^{192}}_{\substack{\text{MITM} \\ \text{16 раундов}}} + \underbrace{2^{192}}_{\substack{\text{опробование} \\ \text{ключей}}} \right) \geq 2^{224}$$



T. Isobe (2011)

A Single-Key Attack on the Full GOST Block Cipher

Метод Динура-Дункельмана-Шамира

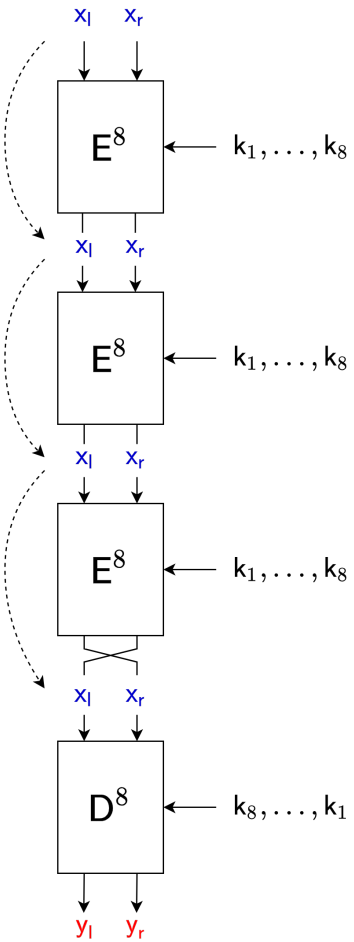
Событие типа «фиксированная точка»

$$E^8(X) = X$$

$$P_{fix} = 2^{-64}$$

Трудоемкость атаки:

$$\underbrace{2^{64}}_{\substack{\text{пар} \\ \text{от/шт}}} \left(\underbrace{2^{128}}_{\substack{\text{MITM} \\ \text{8 раундов}}} + \underbrace{2^{128}}_{\substack{\text{опробование} \\ \text{ключей}}} \right) \geq 2^{192}$$



I. Dinur, O. Dunkelman, A. Shamir (2012)

Improved Attacks on Full GOST

Общая схема атаки

Противнику известны q пар ОТ/ШТ: $(X_1, Y_1), \ldots, (X_q, Y_q)$

Трудоемкость: $q\left(T_{mitm} + T_{test}\right)$

Общая схема атаки

Противнику известны q пар ОТ/ШТ: $(X_1, Y_1), ..., (X_q, Y_q)$

1. Противник опробует q пар ОТ/ШТ (предполагая, что событие в опробуемой паре реализовалось),
   1.1 выполняет MITM-атаку на 8/16 раундов шифра,
   1.2 формирует списки $L_1, ..., L_q$ подходящих ключей.

Трудоемкость: $q\left(T_{mitm} + T_{test}\right)$

Общая схема атаки

Противнику известны q пар ОТ/ШТ: $(X_1, Y_1), ..., (X_q, Y_q)$

1. Противник опробует q пар ОТ/ШТ (предполагая, что событие в опробуемой паре реализовалось),
   1.1 выполняет MITM-атаку на 8/16 раундов шифра,
   1.2 формирует списки $L_1, ..., L_q$ подходящих ключей.
2. Противник выполняет опробование ключей в списках L_i на дополнительных парах ОТ/ШТ

Трудоемкость: $q\left(T_{mitm} + T_{test}\right)$

Алгоритм Гровера (1)

Алгоритм Гровера (квантовый поиск)

$f : \{0,1\}^N \to \{0,1\}$ – булева функция от N переменных, доступ к которой задается оракулом

$$O_f|x\rangle_N|y\rangle = |x\rangle_N|y \oplus f(x)\rangle$$

Задача: найти $x \in \{0,1\}^N$, такой, что $f(x) = 1$.

L. Grover (1996)

A fast quantum mechanical algorithm for database search

Алгоритм Гровера (2)

Псевдокод алгоритма Гровера

1. Инициализировать систему в состоянии $|0^{\otimes N}\rangle|1\rangle$;
2. Применить оператор $H^{\otimes N+1}$; // $\frac{1}{\sqrt{2^N}}\sum_{x\in\{0,1\}^N}|x\rangle\otimes|-\rangle$
3. Для $i := 1$ до $t = \left\lceil\frac{\pi}{4}\sqrt{N}\right\rceil$:
   - 3.1 Вызвать O_f;
   - 3.2 Применить $H^{\otimes N}\otimes I$;
   - 3.3 Применить $(2|0^{\otimes N}\rangle\langle 0^{\otimes N}| - I^{\otimes N})\otimes I$;
   - 3.4 Применить $H^{\otimes N}\otimes I$;
4. Провести измерение.

Сложность: $O(\sqrt{2^N})$ итераций.

QRAM: Квантовая оперативная память

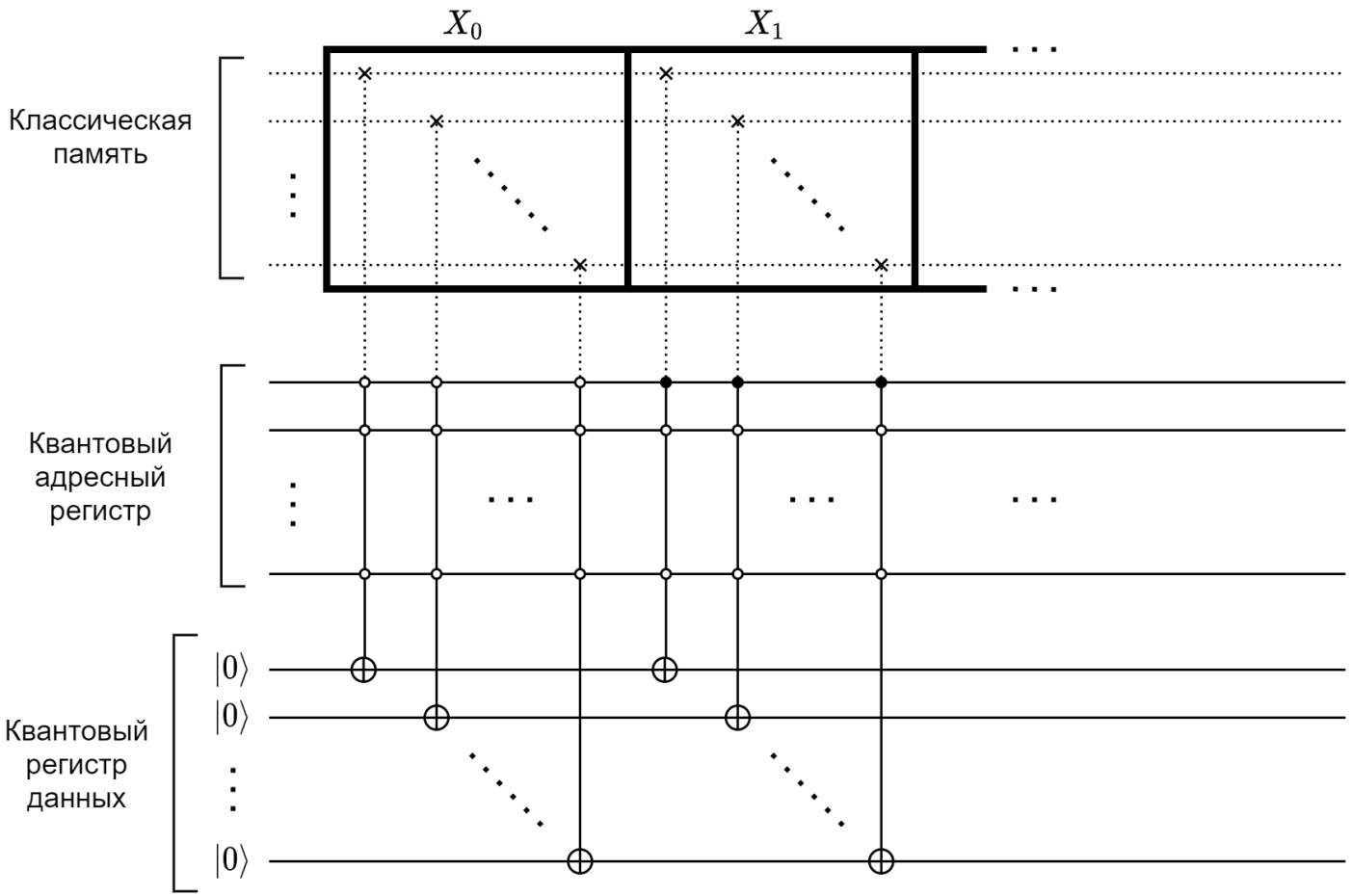
1. QRACM (Classical Memory with Quantum Random Access)

$$X_0 X_1 ... X_{M-1} |i\rangle |y\rangle \overset{\text{QRACM}}{\rightarrow} X_0 X_1 ... X_{M-1} |i\rangle |y \oplus X_i\rangle$$

2. QRAQM (Quantum Memory with Quantum Random Access)

$$|X_0 X_1 ... X_{M-1}\rangle |i\rangle |y\rangle \overset{\text{QRAQM}}{\rightarrow} |X_0 X_1 ... X_{M-1}\rangle |i\rangle |y \oplus X_i\rangle$$

QRACM: эквивалентная линейная схема



Сложность запроса: $O(M \log M)$

Метод 1: последовательный поиск

1. Противник классическим образом формирует q списков $\approx 2^{\lfloor 256 - 2\log_2 q \rfloor}$ ключей $L_1, \ldots, L_q$

Трудоемкость: $T_{M1} = q(T_{mitm} + \sqrt{T_{test}}) \geq 2^{192}/2^{224}$

Память: 2^{128} классических ячеек, ≥ 512 кубит.

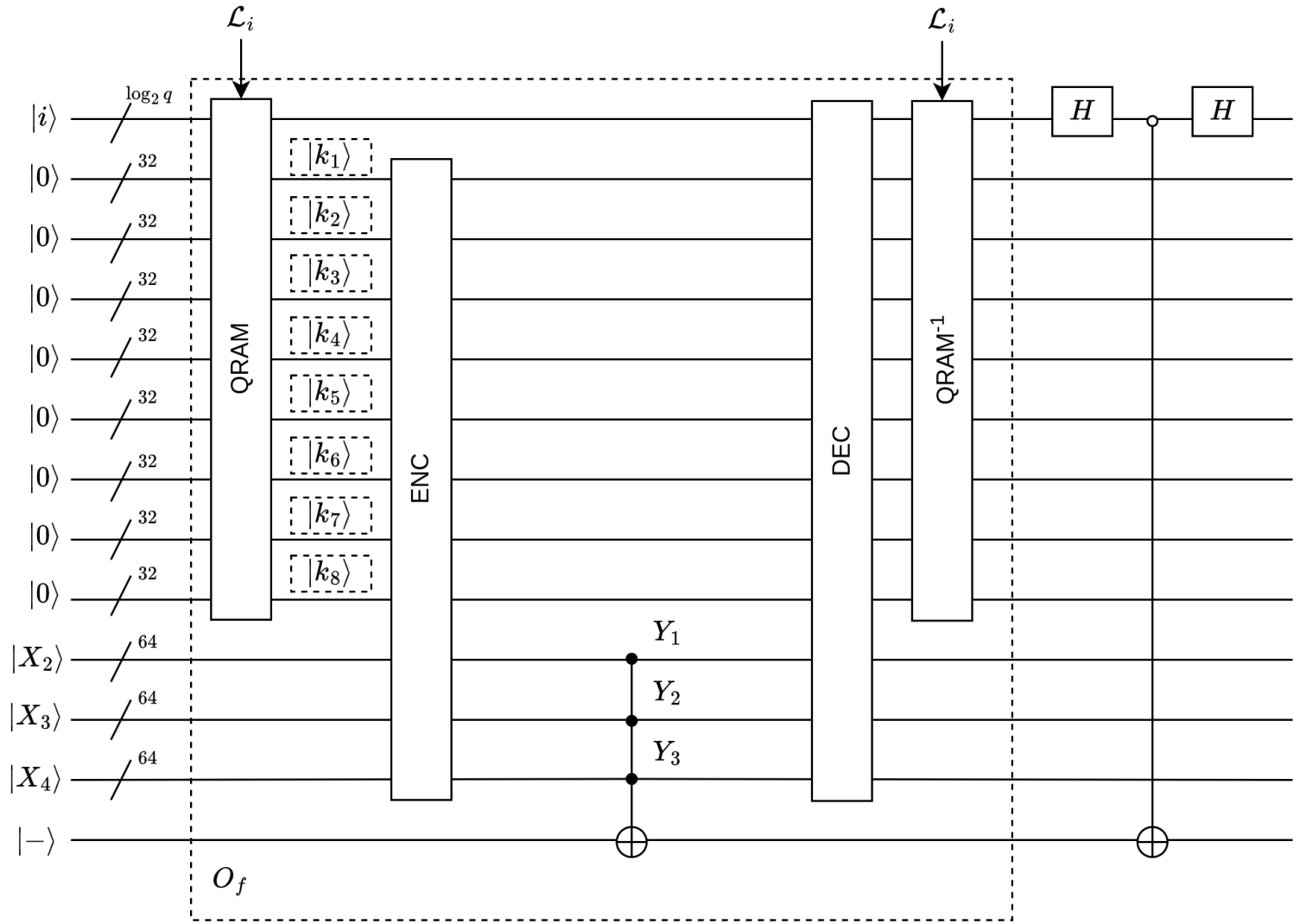
Метод 1: последовательный поиск

1. Противник классическим образом формирует q списков $\approx 2^{\lfloor 256 - 2\log_2 q \rfloor}$ ключей $L_1, ..., L_q$
2. В каждом списке выполняется квантовый поиск с использованием QRACM на 3-х дополнительных парах ОТ/ШТ – $2^{|L_i|/2}$ итераций

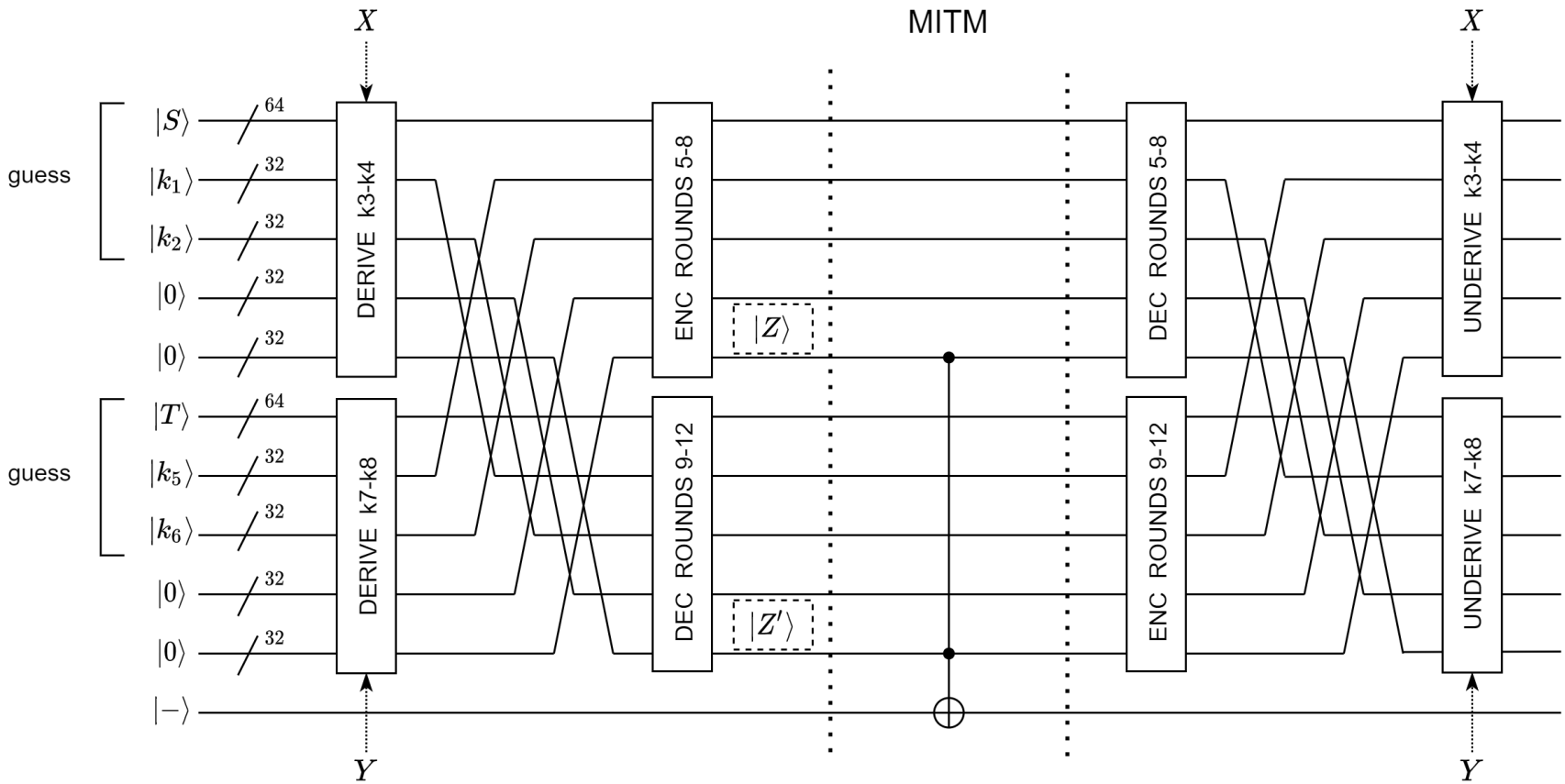
Трудоемкость: $T_{M1} = q(T_{mitm} + \sqrt{T_{test}}) \geq 2^{192}/2^{224}$

Память: 2^{128} классических ячеек, ≥ 512 кубит.

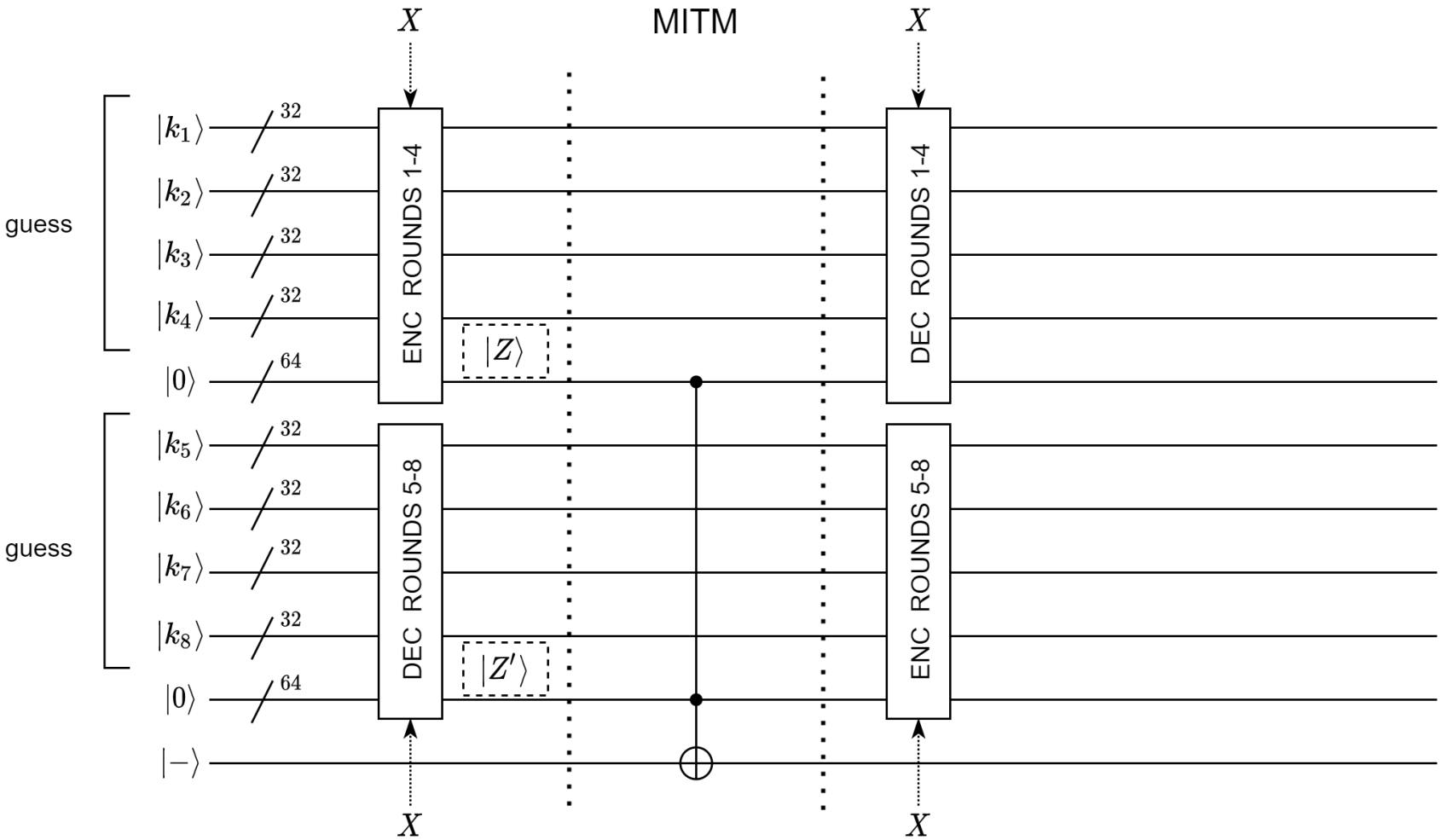
Метод 1: одна итерация



MITM-оракул на 16 раундов (точка отражения)



MITM-оракул на 8 раундов (фикс. точка)



Метод 2: параллельный поиск

1. Квантовым образом для всех q пар ОТ/ШТ формируется суперпозиции $|L_1\rangle, ..., |L_q\rangle$, содержащие ключи этапа MITM с усиленными амплитудами – $q \cdot 2^{\lfloor \log_2 q \rfloor / 2}$ итераций

Трудоемкость: $T_{M2} = q(\sqrt{T_{mitm}} + \sqrt{qT_{test}}) + T_{mitm} + \sqrt{T_{test}} \geq 2^{176}/2^{208}$

Память: $O(1)$ классических ячеек, $\geq 2^{65}$ кубит.

Метод 2: параллельный поиск

1. Квантовым образом для всех q пар ОТ/ШТ формируется суперпозиции $|L_1\rangle, ..., |L_q\rangle$, содержащие ключи этапа MITM с усиленными амплитудами – $q \cdot 2^{\lfloor \log_2 q \rfloor / 2}$ итераций
2. Выполняется квантовый поиск с использованием QRAQM на 3-х дополнительных парах ОТ/ШТ в системе $|L_1\rangle, ..., |L_q\rangle|i\rangle$. Находится индекс $|i\rangle$ системы, в которой содержится истинный ключ

Трудоемкость: $T_{M2} = q(\sqrt{T_{mitm}} + \sqrt{qT_{test}}) + T_{mitm} + \sqrt{T_{test}} \geq 2^{176}/2^{208}$

Память: $O(1)$ классических ячеек, $\geq 2^{65}$ кубит.

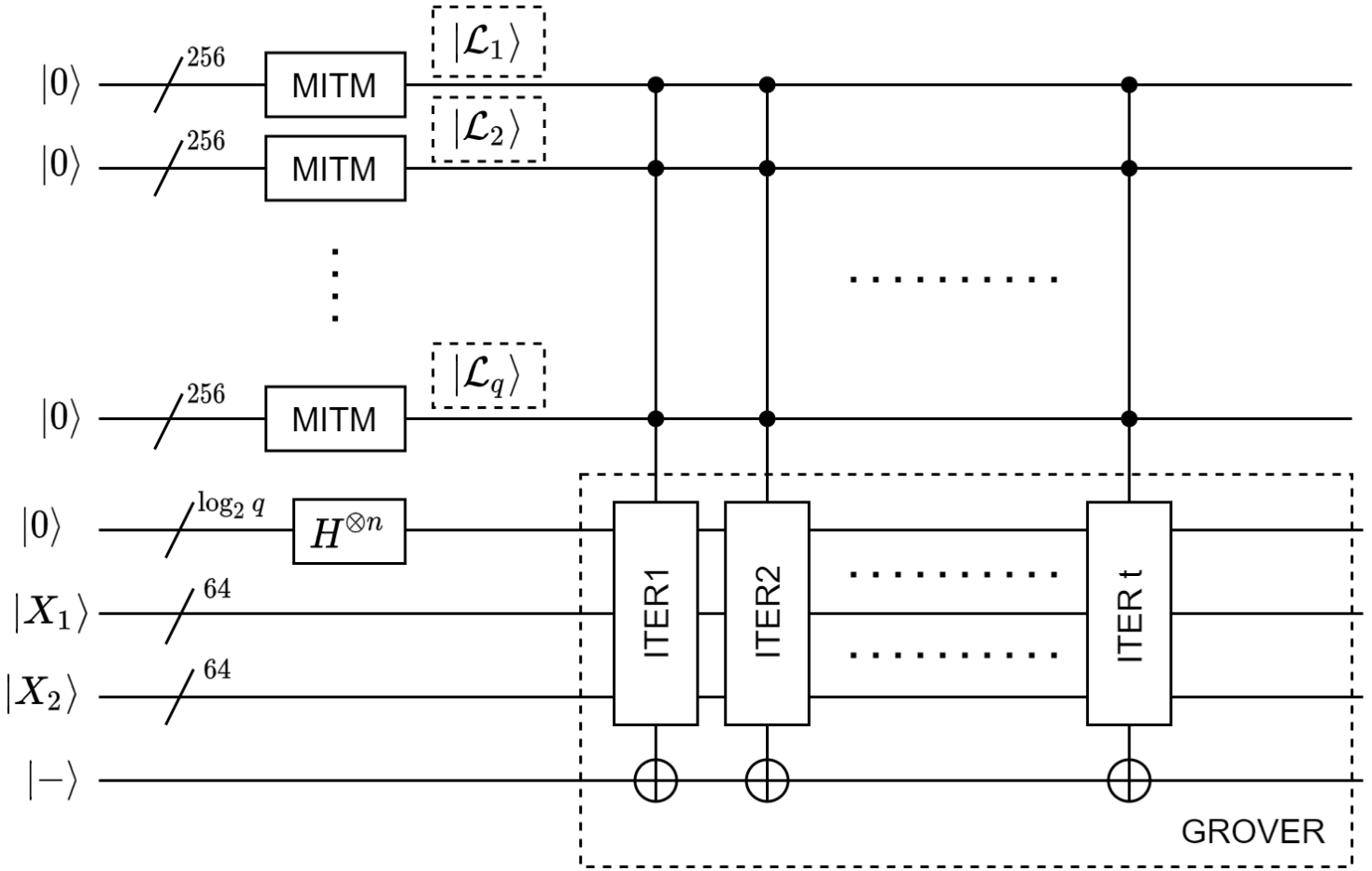
Метод 2: параллельный поиск

1. Квантовым образом для всех q пар ОТ/ШТ формируется суперпозиции $|L_1\rangle, ..., |L_q\rangle$, содержащие ключи этапа MITM с усиленными амплитудами – $q \cdot 2^{\lfloor \log_2 q \rfloor / 2}$ итераций
2. Выполняется квантовый поиск с использованием QRAQM на 3-х дополнительных парах ОТ/ШТ в системе $|L_1\rangle, ..., |L_q\rangle|i\rangle$. Находится индекс $|i\rangle$ системы, в которой содержится истинный ключ
3. При i-ой паре повторно выполняется MITM-атака

Трудоемкость: $T_{M2} = q(\sqrt{T_{mitm}} + \sqrt{qT_{test}}) + T_{mitm} + \sqrt{T_{test}} \geq 2^{176}/2^{208}$

Память: $O(1)$ классических ячеек, $\geq 2^{65}$ кубит.

Метод 2: параллельный поиск (2)



Метод 3: две специальные точки (1)

1. Известны две симметричные фиксированные точки вида (X, X) и $(\tilde{X}, \tilde{X})$

Средняя трудоемкость: $T_{M3}/2^{-64} = (T_{mitm} + \sqrt{T_{test}})/2^{-64} \geq 2^{192}$

О. Kara, F. Karakoç (2012)

Fixed Points of Special Type and Cryptanalysis of Full GOST

Метод 3: две специальные точки (1)

1. Известны две симметричные фиксированные точки вида (X, X) и $(\tilde{X}, \tilde{X})$
2. Выполняется MITM-атака на 8 раундов, формируется список 2^{128} ключей L

Средняя трудоемкость: $T_{M3}/2^{-64} = (T_{mitm} + \sqrt{T_{test}})/2^{-64} \geq 2^{192}$

O. Kara, F. Karakoç (2012)

Fixed Points of Special Type and Cryptanalysis of Full GOST

Метод 3: две специальные точки (1)

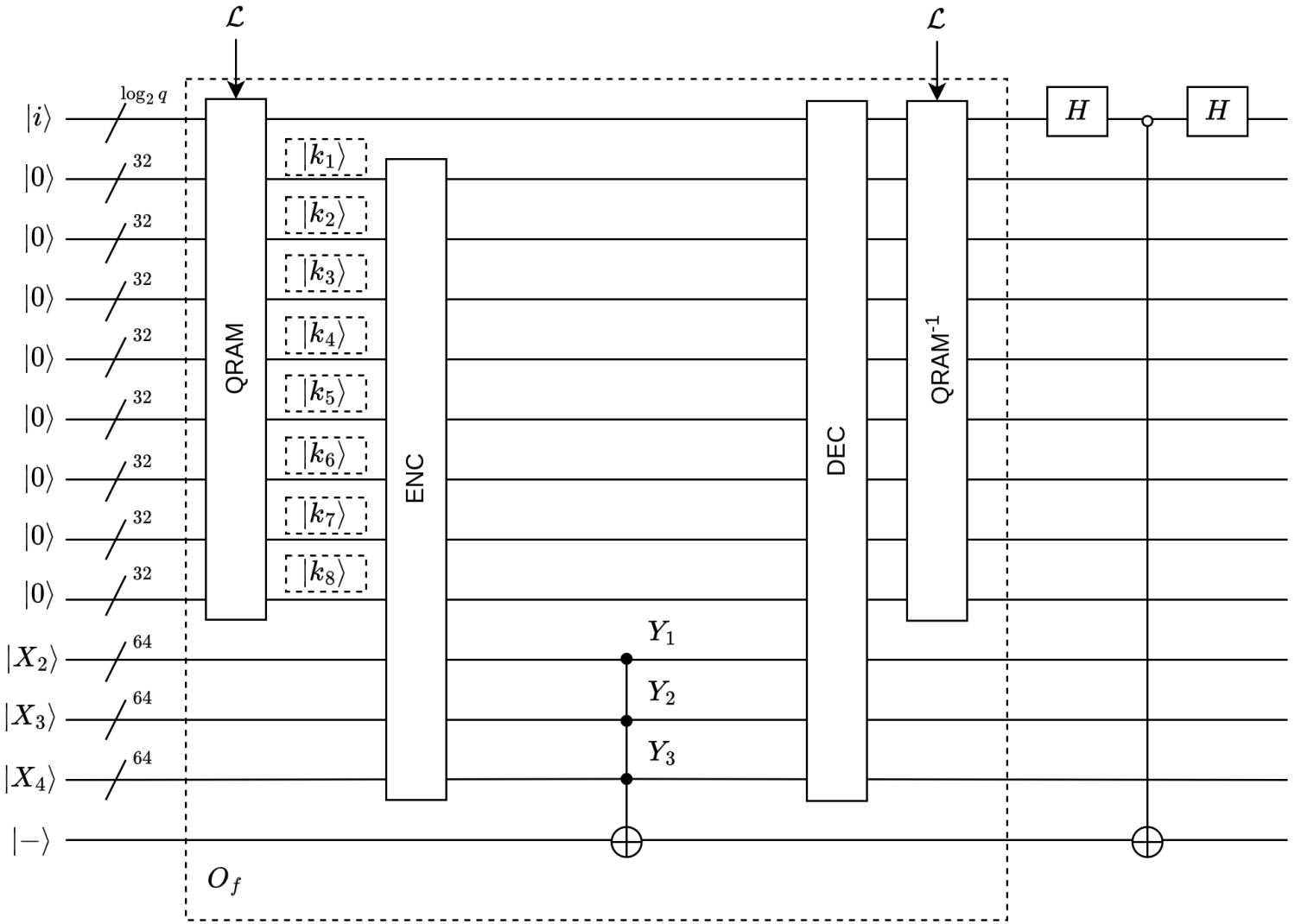
1. Известны две симметричные фиксированные точки вида (X, X) и $(\tilde{X}, \tilde{X})$
2. Выполняется MITM-атака на 8 раундов, формируется список 2^{128} ключей L
3. Выполняется квантовый поиск с использованием QRACM на 2-х дополнительных парах ОТ/ШТ в списке L

Средняя трудоемкость: $T_{M3}/2^{-64} = (T_{mitm} + \sqrt{T_{test}})/2^{-64} \geq 2^{192}$

O. Kara, F. Karakoç (2012)

Fixed Points of Special Type and Cryptanalysis of Full GOST

Метод 3: одна итерация



Особенности предложенных методов

1. Работают в модели Q1 – требуется только оффлайн-вычислитель

Особенности предложенных методов

1. Работают в модели Q1 – требуется только оффлайн-вычислитель
2. Требуют доступа к квантовой памяти (QRACM/QRAQRM)

Особенности предложенных методов

1. Работают в модели Q1 – требуется только оффлайн-вычислитель
2. Требуют доступа к квантовой памяти (QRACM/QRAQRM)
3. Используют схемы меньшей, чем у алгоритма Гровера глубины ($< 2^{128}$)

Метод Dong et al. (1)

Предложены атаки на 30 и 32 раунда «Магмы» соответственно в модели **Q2**.

Используются свойства «точка отражения» (30 раундов) и «фиксированная точка» (32 раунда):

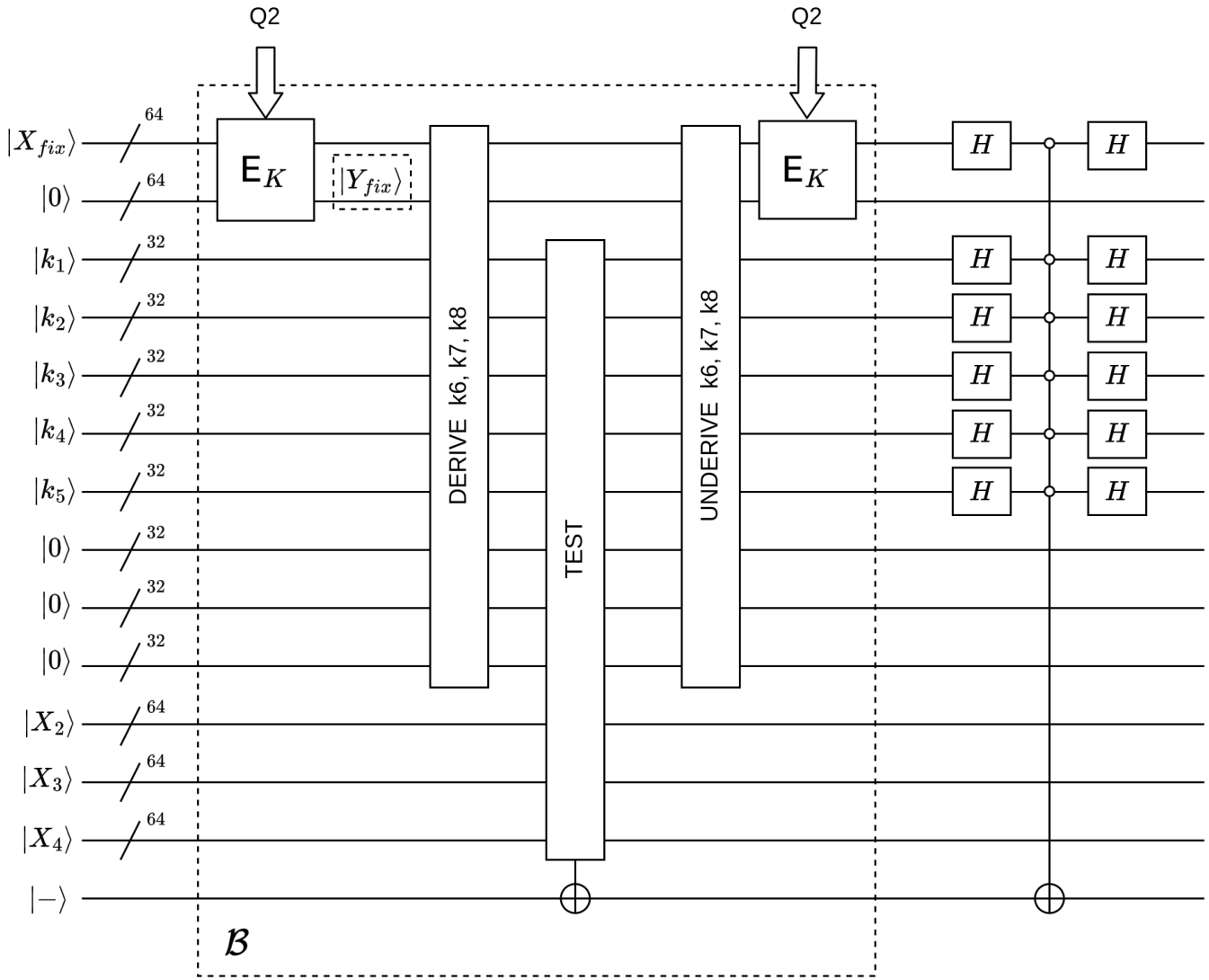
1. Квантовый поиск выполняется в пространстве $X, k_1, ..., k_5$ (224 бит / 2^{112} итераций)
2. Ключи k_6, k_7, k_8 вычисляются из $X, k_1, ..., k_5$
3. Каждую итерацию совершается запрос к оракулу Q2

Трудоемкость: 2^{112} итераций алгоритма Гровера

X. Dong, B. Dong, X. Wang.

Quantum Attacks on Some Feistel Block Ciphers

Метод Dong et al. (2)



Результаты

Атака	Условия	Трудоемкость	Память	Материал
Классические				
Isobe	Q0	2^{224}	2^{64} C	2^{32}
Dinur et al.	Q0	2^{192}	2^{64} C	2^{64}
Kara, Karakoç	Q0	2^{192}	2^{64} C	2^{64}
Квантовые				
Гровер	**Q1**	2^{128}	513 **Q**	4
Наст. работа	Q1	$2^{192}/2^{224}$	2^{128} C	$2^{32}/2^{64}$
Наст. работа	Q1	$2^{176}/2^{208}$	2^{65} Q	$2^{32}/2^{64}$
Наст. работа	Q1	2^{176}	2^{128} C	4
Dong et al.	Q2	2^{112}	513 Q	2^{112}*

* – запросов к оракулу Q2

Заключение

1. Предложены методы криптоанализа алгоритм «Магма» на основе точек отражения, фиксированных точек, их комбинации

Заключение

1. Предложены методы криптоанализа алгоритм «Магма» на основе точек отражения, фиксированных точек, их комбинации
2. Рассмотренные методы обладают не меньшей трудоемкостью, чем универсальная оценка (2^{128} по алгоритму Гровера)

Заключение

1. Предложены методы криптоанализа алгоритм «Магма» на основе точек отражения, фиксированных точек, их комбинации
2. Рассмотренные методы обладают не меньшей трудоемкостью, чем универсальная оценка (2^{128} по алгоритму Гровера)
3. К настоящему времени неизвестно эффективных оффлайн-атак (в модели Q1) на алгоритм «Магма» – шифр остается стойким при появлении квантового компьютера

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ