Об одном подходе к оценке усеченных дифференциалов в низкоресурсной хэш-функции «Мора»

Бондакова Ольга Сергеевна

РТУ МИРЭА, Институт кибернетики, БК №252

25 марта 2020 года

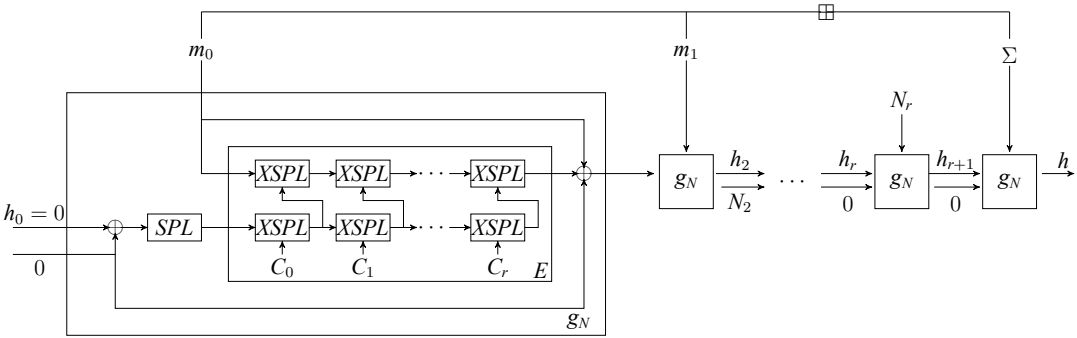
Содержание доклада

1. Низкоресурсная хэш-функция «Мора».
2. Дифференциальные атаки и способы их оптимизации. Новый подход к вычислению EDP.
3. Трудности применения нового подхода к шифрам с МДР-матрицами. Способы модификации.
4. Оценка трудоемкости и получение значения EDP.

Хэш-функция «Мора». Общие сведения

- Впервые представлена – «РусКрипто’2020».
- Использование – обеспечение контроля целостности на уровне полевых устройств АСУ ТП.
- «Стрибог»-подобная конструкция (уменьшены размеры преобразований, сохранены синтезные принципы).
- Размер блока – 64 бита.

Хэш-функция «Мора». Конструкция



Дифференциальный метод криптографического анализа

Один из основных методов оценки стойкости блочных шифров и основанных на них примитивов.

Для функций хэширования на основе дифференциального метода можно построить алгоритм поиска коллизий.

Основная идея

Наблюдение за изменением разности α пары сообщений в процессе шифрования до момента получения разности β соответствующих шифртекстов.


Biham E., Shamir A., Differential Cryptanalysis of DES-like Cryptosystems, LNCS, 1991.

Дифференциальный метод криптографического анализа.

Для блочного шифра $\varepsilon_K : V_k \times V_n \to V_n,\ \varepsilon_K(P) = C$:

Дифференциал

$(\alpha,\ \beta)$ – пара разностей $\alpha,\ \beta \in V_n$, вероятность которой при фиксированном ключе оценивается величиной:

$$\mathbb{P}(\alpha \xrightarrow{\varepsilon_K} \beta) = 2^{-k}|\{P \in V_n \mid \varepsilon_K(P) \oplus \varepsilon_K(P \oplus \alpha) = \beta\}|$$

При случайном равновероятном распределении ключа $K \in V_k$:

$$EDP(\alpha \xrightarrow{\varepsilon} \beta) = 2^{-k} \cdot \sum_{K \in V_2^k} \mathbb{P}(\alpha \xrightarrow{\varepsilon_K} \beta)$$

Мощность $|V_k| \geq 2^{64}$ $\Rightarrow$ получить оценку невозможно $\Rightarrow$ необходимо снизить количество перебираемых значений.

Усеченные дифференциалы

Дифференциал, у которого разность α выбирается из некоторого заданного множества $\mathcal{U}$ и разность β из некоторого множества, где $\mathcal{U},\ \mathcal{V} \subset V_n$.

EDP усеченного дифференциала: $EDP(\mathcal{U} \xrightarrow{\varepsilon} \mathcal{V}) = \frac{1}{|\mathcal{U}|} \sum_{\substack{\alpha \in \mathcal{U} \\ \beta \in \mathcal{V}}} EDP(\alpha \xrightarrow{\varepsilon} \beta)$

- L. Knudsen, Truncated and Higher Order Differentials, FSE, 1994.
- V. Kiryukhin, An algorithm for bounding non-minimum weight differentials in 2-round LSX-ciphers, CTCrypt 2020, 2020.

Варианты оптимизаций

- Каждому ненулевому полубайту разности ставится в соответствие две **переменных**.
- «Граф» EDP.
  - Вершина – одна переменная.
  - Ребро – наличие связи между переменными.
  - Вершины равноудаленные от начальной (начальных) соответствуют полубайтам одного раунда.
- **Суммирование по переменной.**

Eichlseder M., Leander G., Rasoolzadeh S., Computing Expected Differential Probability of (Truncated) Differentials and Expected Linear Potential of (Multidimensional) Linear Hulls in SPN Block Ciphers, 2020.

Суммирование по переменной

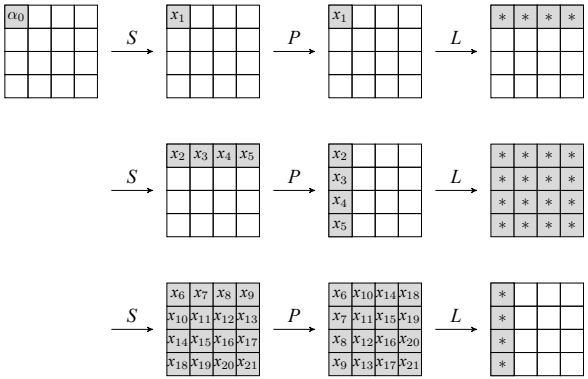
Для каждой переменной $x_i,\ i \in 1, ..., N$ заполняется таблица T_i на основе T_{i-1}:

1. Составляется множество соседних переменных $\mathcal{I}_i = \{x_{i_1}, ..., x_{i_t}\}$.
   $x_{i_1}, ..., x_{i_l}$ – переменные, расположенные в том же блоке, что и x_i.
   $x_{i_{l+1}}, ..., x_{i_t}$ – переменные, получаемые из x_i после применения преобразования S на следующей итерации шифра.
2. Вычисляется значение $\sum\limits_{x_i} p(x_i \to x_{i_l}) \cdot ... \cdot p(x_i \to x_{i_r}) T_{i-1}[I_{i-1}]$.
   Где I_{i-1} – набор значений переменных из $\mathcal{I}_{i-1}$.

Значение EDP=$(\sum\limits_{I_N} T[N]) \cdot (2^m - 1)^{-\omega(\alpha)}$, где $\omega(\alpha_0)$ – вес α_0.

Трудоемкость вычислений оценивается: $2^{s \cdot \max_i |\mathcal{I}_i| + 1}$ ячеек памяти и $2^s \sum\limits_i 2^{s \cdot |\mathcal{I}_i|}$ операций.

Применение подхода к блочному шифру хэш-функции «Мора»



Трудоемкость вычислений составит не менее $2^{4 \cdot 16} = 2^{64}$ операций.

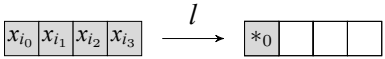
Сокращение числа переменных

Матрица линейного преобразования приводится к виду, соответствующему расположению ненулевых полубайт разностей, после чего определяется наличие линейных зависимостей. Исключение переменных связанных такими зависимостями позволяет оптимизировать процесс вычисления.

МДР-матрица не допускает применения такого подхода.

Решение: найти классы векторов, для которых можно найти дополнительные зависимости между элементами.

Выявленные особенности

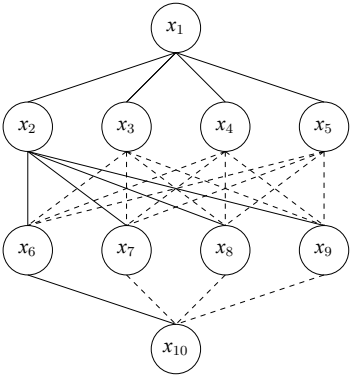


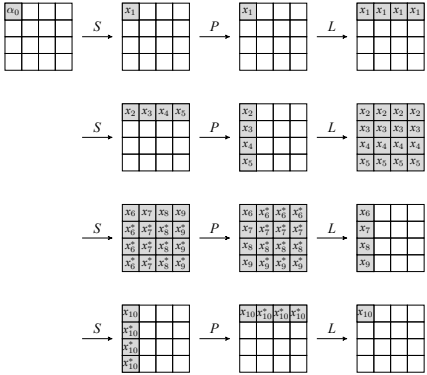
$*_0 = x_0 \cdot b_{00}^{-1},\ x_{i_2} = x_{i_0} \cdot b_{00}^{-1} \cdot b_{02}$
$x_{i_2} = x_{i_0} \cdot b_{00}^{-1} \cdot b_{02},\ x_{i_3} = x_{i_0} \cdot b_{00}^{-1} \cdot b_{03}$
b_{ij} – элемент матрицы B, обратной для матрицы A.

В произвольном случае $* = x_i \cdot b_{ti}^{-1},\ x_{i_j} = x_{i_i} \cdot b_{ti}^{-1} \cdot b_{tj}$

Можно сократить 12 переменных из 16 на 3 итерации блочного шифра.

Пример графа EDP для 4-раундовой версии блочного шифра «Моры»





Полученные результаты

Количество раундов	Операций	Память
4	2^{32}	2^{29}
5	2^{32}	2^{28}

Количество раундов	EDP	Успех коллизии	Успех почти коллизии
4	$2^{-59.05568...}$	$2^{-63.05568...}$	$2^{-59.05568...}$
	$2^{-58.57357...}$	$2^{-62.57357...}$	$2^{-58.57357...}$
5	$2^{-59.05568...}$	–	$2^{-59.05568...}$
	$2^{-58.57357...}$	–	$2^{-58.57357...}$

Выводы

1. Получены оценки трудоемкости применения подхода к блочному шифру хэш-функции «Мора».
2. Вычислены вероятности успеха применения атаки поиска коллизий для сообщений, различающихся в одном полубайте.
3. Вычислены значения EDP для нескольких усеченных дифференциалов.
4. Возможные направления дальнейших исследований:
   - 4.1 Поиск дополнительных зависимостей для новых классов векторов.
   - 4.2 Получение оценок трудоемкости применения подхода к дифференциалам с иными шаблонами.
   - 4.3 Вычисление значений EDP для иных усеченных дифференциалов.

Вопросы?