**Дифференциальный криптоанализ**

Понятие, история, алгоритм, устойчивость к взлому, недостатки

***Понятие***

*Дифференциальный криптоанализ* — метод криптоанализа симметричных блочных шифров, хэш-функций и поточных шифров, основанный на изучении преобразования разностей между шифруемыми значениями на различных раундах шифрования. В качестве разности, как правило, применяется операция побитового суммирования по модулю 2, хотя существуют атаки и с вычислением разности по модулю 2^{32}. Применим для взлома алгоритмов DES, FEAL и некоторых других шифров.

***История***

Дифференциальный криптоанализ предложен в 1990 году израильскими специалистами Эли Бихамом и Ади Шамиром для взлома криптосистем, подобных DES. В своей работе они показали, что алгоритм DES оказался довольно устойчивым к данному методу криптоанализа, и любое малейшее изменение структуры алгоритма делает его более уязвимым.

В 1994 году Дон Копперсмит из IBM опубликовал статью[1], в которой заявил, что метод дифференциального криптоанализа был известен IBM уже в 1974 году, и одной из поставленных целей при разработке DES была защита от этого метода. У IBM были свои секреты. Копперсмит объяснял:

*«При проектировании использовались преимущества определенных криптоаналитических методов, особенно метода «дифференциального криптоанализа», который не был опубликован в открытой литературе. После дискуссий с АНБ было решено, что раскрытие процесса проектирования раскроет и метод дифференциального криптоанализа, мощь которого может быть использована против многих шифров. Это, в свою очередь, сократило бы преимущество США перед другими странами в области криптографии.»*

DES оказался криптостойким к дифференциальному криптоанализу, в отличие от некоторых других шифров. Так, например, уязвимым оказался шифр FEAL. Состоящий из 4 раундов FEAL-4 может быть взломан при использовании всего лишь 8 подобранных открытых текстов, и даже 31-раундовый FEAL уязвим для атаки.

***Алгоритм***

Идею относительно **дифференциального криптоанализа** предложили Эли Бихам и Ади Шамир. Это — *атака с выборкой исходного текста*.

Ева может каким-либо образом получить доступ к компьютеру Алисы и завладеть выборочно частью исходного текста и соответствующего зашифрованного текста. Цель состоит в том, чтобы найти ключ шифра Алисы.

Перед тем как Ева предпримет атаку с выборкой исходного текста, она должна проанализировать алгоритм шифрования, чтобы собрать некоторую информацию об отношениях зашифрованного и исходного текстов. Очевидно, Ева не знает ключ шифра. Однако некоторые шифры имеют слабости в структурах, которые могут позволить Еве найти различия исходного текста и различия зашифрованного текста, не зная ключ.

1. Не зная значения ключа, Ева может легко найти отношения между разностями исходного текста и разностями зашифрованного текста. Если разность исходного текста мы обозначим P_{1}\oplus P_{2} и разность зашифрованного текста мы обозначим C_{1}\oplus C_{2}, приведенные следующие преобразования доказывают, что C_{1}\oplus C_{2} = P_{1}\oplus P_{2}:

C_{1} = P_{1} \oplus  K  C_{2} = P_{2} \oplus  K \to  C_{1} \oplus  C_{2}  = P_{1} \oplus  K \oplus  P_{2} \oplus  K = P_{1} \oplus  P_{2}

1. Существование S -блока мешает Еве найти и определенные отношения между разностями исходного текста и разностями зашифрованного текста. Однако возможно установить вероятностные отношения. Ева может составить таблицу, которая показывает для разности исходного текста, сколько можно создать разностей зашифрованного текста — шифр.
2. С помощью предыдущей таблицы можно создать вероятностную информацию для Евы. Входы в таблице соответствуют вероятностям появления. Разности с нулевой вероятностью никогда не будут возникать.
3. Как мы увидим позже, Ева теперь располагает достаточным количеством информации, чтобы начать ее атаку. Таблица показывает, что вероятности распределены неоднородно из-за слабости в структуре S -блока. Таблица 7.5 упоминается иногда как дифференциальная таблица распределения или профайл **ИСКЛЮЧАЮЩЕЕ ИЛИ**.
4. Запуск атаки выборки исходного текста. После того как анализ однажды сделан, он может быть сохранен для будущего использования, пока структура шифра не изменится. Ева может выбрать для атак исходные тексты. Дифференциальная таблица распределения вероятности ([таблица 7.5](https://intuit.ru/studies/professional_retraining/940/courses/408/lecture/9360?page=6#table.7.5)) поможет Еве их выбирать — она возьмет те, которые имеют самую высокую вероятность в таблице.
5. Предположительное значение ключа. После запуска некоторых атак с соответствующей выборкой исходного текста Ева может найти некоторую пару "исходный текст / зашифрованный текст", которая позволяет ей предположить некоторое значение ключа. Процесс начинается от C и продвигается к P.

***Общая процедура.*** Современные блочные шифры имеют большую сложность, чем, та, которую мы обсуждали в этом разделе. Кроме того, они могут содержать различное количество раундов. Ева может использовать следующую стратегию:

1. Поскольку каждый раунд содержит одни и те же операции, Ева может создать таблицу дифференциальных распределений (профайл **ИСКЛЮЧАЮЩЕГО ИЛИ**) для каждого S -блока и комбинировать их, чтобы создать распределение для каждого раунда.
2. Предположим, что каждый раунд независим (справедливое предположение). Ева может создать таблицу распределения для всего шифра, умножая соответствующие вероятности.
3. Ева может теперь делать список исходных текстов для атак, основанных на таблице распределений на втором шаге. Заметим, что таблица в шаге 2 только помогает Еве выбирать меньшее количество пар "исходный текст / зашифрованный текст"
4. Ева выбирает зашифрованный текст и находит соответствующий исходный текст. Затем она анализирует результат, чтобы найти некоторые биты в ключе.
5. Ева повторяет шаг 4, чтобы найти больше битов в ключе.

После нахождения достаточного количества битов в ключе Ева может использовать атаку грубой силы, чтобы найти весь ключ.

Дифференциальный криптоанализ базируется на таблице неоднородных дифференциальных распределений, S -блоков в блочном шифре.

***Устойчивость к взлому***

DES изначально спроектированным устойчивым к дифференциальному криптоанализу, атака показала себя успешной против широкой группы DES-подобных шифров:

* Lucifer, укороченный до восьми раундов, взламывается с использованием менее 60 шифртекстов.
* FEAL-8 взламывается с использованием менее 2000 шифртекстов.
* FEAL-4 взламывается с использованием 8-и шифртекстов и одного открытого текста.
* FEAL-N и FEAL-NX могут быть взломаны при количестве раундов N <= 31

***Недостатки метода***

Метод дифференциального криптоанализа в большей степени является теоретическим достижением. Его применение на практике ограничено высокими требованиями к времени и объёму данных.

Являясь, в первую очередь, методом для вскрытия с выбранным открытым текстом, дифференциальный криптоанализ трудно реализуем на практике. Он может быть использован для вскрытия с известным открытым текстом, но в случае полного 16-этапного DES это делает его даже менее эффективным, чем вскрытие грубой силой.

Метод требует большого объема памяти для хранения возможных ключей. Эффективность метода также сильно зависит от структуры S-блоков взламываемого алгоритма.