РОЗДІЛИ СУЧАСНОЇ КРИПТОЛОГІЇ
Комп'ютерний практикум №2

Лінійний криптоаналіз блокових шифрів

1. Мета роботи

Опанування сучасних методів криптоаналізу блокових шифрів, набуття навичок у дослідженні стійкості блокових шифрів до лінійного криптоаналізу.

2. Основні теоретичні відомості

Далі буде.

3. Порядок і рекомендації щодо виконання роботи

1. Узяти реалізацію шифру Хейса із комп'ютерного практикуму №1 (із таким само варіантом).

2. Реалізувати методом «гілок та границь» пошук п'ятираундових лінійних апроксимацій шифру Хейса із великим потенціалом. Так само, як і в попередньому практикумі, для пошуку рекомендується використовувати початкові маски α із однією ненульовою тетрадою. Для виконання практикуму вам знадобиться 300-700 різних апроксимацій.

3. Реалізувати атаку на сьомий раундовий ключ шифру Хейса за такою схемою.

а) Одержати необхідну кількість пар «відкритий текст-шифротекст». Зауважимо, що кількість пар повинна бути обернено пропорційна до найменшого лінійного потенціалу серед усіх апроксимацій, які використовуються для атаки (краще за все із коефіцієнтом 8 або 16).

б) Для кожної апроксимації реалізувати алгоритм атаки M2. Відмітити кожний кандидат у ключі, для якого лічильник алгоритму M2 перевищив певний поріг (значення цього порогу залишається на ваш розсуд; наприклад, ви можете розглядати першу десятку, перші 50 або перші 100 ключів).

в) Серед усіх відмічених кандидатів для усіх знайдених апроксимацій обрати десять, які найчастіше обирались алгоритмом M2.

Атака вважається успішною, якщо правильний раундовий ключ потрапив у фінальну десятку кандидатів.

Необхідний статистичний матеріал (шифровані тексти) одержується із тестової програми **Heys.exe**, що додається.

Зауваження. Програма **Heys.exe** має консольний інтерфейс.

4. Оформити звіт з практикуму.

4. Оформлення звіту

Звіт до комп'ютерного практикуму оформлюється згідно зі стандартними правилами оформлення наукових робіт, за такими винятками:

– дозволяється використовувати шрифт Times New Roman 12pt та одинарний інтервал між рядками;
– для оформлення текстів програм дозволяється використовувати шрифт Courier New 10pt (8pt) та друкувати тексти в дві колонки;
– дозволяється не починати нові розділи з окремої сторінки.

До звіту можна не включати анотацію, перелік термінів та позначень та перелік використаних джерел. Також не обов'язково оформлювати зміст.

Звіт має містити:

– мету лабораторної роботи;
– постановку задачі;
– хід роботи, опис труднощів, що виникали, та шляхів їх розв'язання;
– опис методу пошуку високоімовірних диференціалів, обрані порогові значення імовірностей (із обґрунтуванням вибору);
– таблицю диференціальних імовірностей S-блоку вашого варіанту;
– знайдені за допомогою методу «гілок та границь» диференціали для кожного раунду шифрування та їх імовірності (якщо перелік відповідних диференціалів завеликий, дозволяється обмежитись певною вибіркою значень);
– знайдений в ході диференціальної атаки ключ останнього раунду шифрування тестової програми, із зазначенням кількості шифртекстів, що були потрібні для знаходження;
– висновки до роботи;
– тексти всіх програм.

5. Контрольні запитання

Дивіться лекції

6. Оцінювання комп'ютерного практикуму

За виконання комп'ютерного практикуму студент може одержати до 10 рейтингових балів; зокрема, оцінюються такі позиції:

– реалізація програм – до 5-х балів (в залежності від правильності та швидкодії);
– теоретичний захист роботи – до 5-ти балів;
– несвоєчасне виконання роботи – (-1) бал за кожні два тижні пропуску.

7. Рекомендовані джерела

1. Heys Howard M. A Tutorial on Linear and Differential Cryptanalysis [електронний ресурс] / Howard M. Heys. – Режим доступу : http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf

2. Biham E. Differential cryptanalysis of DES-like cryptosystems / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3-72.

3. Ковальчук Л.В. Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа / Л.В. Ковальчук // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25 – 27 октября 2006 г. – М.: МЦНМО, 2007. – С. 595 – 599.

4. Ковальчук Л.В. Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів шифрування до методів різницевого криптоаналізу / Л.В. Ковальчук, С.В. Пальченко, Л.В. Скрипник // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – К.: НДЦ «Тезіс», 2009 – №2 (19) – стор. 45-56.

5. Яковлєв С.В. Аналітичні оцінки стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу : кандидатська дисертація. – К.: НТУУ «КПІ», 2014. – 160 стор.