Харківський національний університет радіоелектроніки

Аналіз криптографічних властивостей симетричних шифрів

Бакалаврська робота

Харків 2013

Актуальність

Нагальні проблеми

- Сучасні криптоалгоритми базуються на складній математиці.
- Реальні системи безпеки часто є вразливими із-за некоректного використання та помилок реалізації.

стандарт GSM:

A5/1 можливо зламати за секунди (використовуючи rainbow таблиці).

Супутникові телефони:

GMR-1 базується на A5/2 (виведений з експлуатації з 2007 р.);

GMR-2 неопублікований алгоритм (атака потребує 65 б гами).

Безпровідний інтернет:

WEP необхідно 80000 пакетів для проведення криптоаналізу;

E0 атака вимагає 2^{38} операцій та $2^{23.8}$ фрагментів даних.

Необхідно проводити детальний аналіз та відкриту експертизу шифрів перед застосуванням у реальних системах безпеки.

Актуальність ГОСТ 28147

- прийнятий у 1989 р. стандарт шифрування ГОСТ широко застосовується в Україні та країнах СНД;
- запропонований для стандартизації в ISO у 2010 р;
- перспективний для використання у мало-ресурсній криптографії;
- відсутня оцінка стійкості до алгебраїчного криптоаналізу.

Алгебраїчний криптоаналіз

Клод Шеннон

“Злам стійкого шифру має потребувати такий же обсяг обчислень, що і вирішення системи рівнянь від багатьох невідомих”.

Основні принципи

1. криптоалгоритм описується системою рівнянь другого степеня від багатьох змінних;
2. за наявності відкритих повідомлень та шифротекстів, система рівнянь вирішується для знаходження бітів ключа.

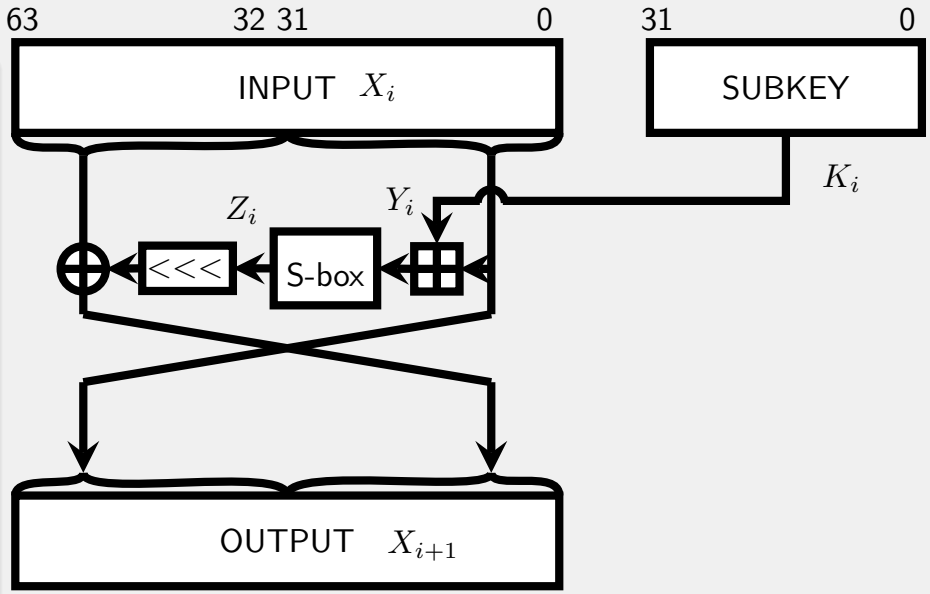

Рисунок: Циклова функція ГОСТ 28147-89

Система рівнянь ГОСТ 28147-89

- реалізовано з використанням системи символьної алгебри SAGE;
- один раунд шифру містить 325 рівнянь другого степеня;
- повний шифр описується 10432 поліномами від 4416 змінних;
- можливо вирішити алгебраїчну систему для 5 раундів ГОСТ 28147-89.

Використання CryptoMiniSat

1. формується система рівнянь шифра в АНФ за допомогою SAGE;
2. система рівнянь конвертується з АНФ формату до КНФ;
3. `CryptoMiniSat` знаходить набір змінних, що задовольняє систему рівнянь.

Приклад

Висновки

Алгебраїчний криптоаналіз

- алгоритм ГОСТ вдало описується системою рівнянь другого степеня;
- на даний момент можливо вирішити алгебраїчну систему, що описує 5 раундів шифрування ГОСТ 28147;
- подальша оптимізація може дозволити успішно вирішити алгебраїчну систему для більшої кількості раундів.

Список публікацій I

Oliynykov R. V., Kiyanchuk R. I.

Perspective Symmetric Block Cipher optimized for Hardware Implementation //
6-th International Conference "Dependable Systems, Services & Technologies (DESSERT'12)". — 2012.

Kiyanchuk R. I., Oliynykov R. V.

Linear transformation properties of ZUC cipher //
Visnyk. — 2012. — Mathematical modeling. Information technologies. Computer-aided control systems.

Kiyanchuk, R. I. and Oliynykov R. V.

Linear transformation properties of ZUC cipher //
Computer modeling in high-end technologies / Kharkiv national university of radio electronics. — Kharkiv, 2012. — P. 199 – 202.

Кіянчук Р. І.

Диференційний аналіз S-функцій //
Наукові дослідження молоді вирішенню проблем європейської інтеграції / Харківський університет банківської справи. — Харків, 2012. — Електронне видання на CD-ROM.

Кіянчук Р. І.

Диференційний аналіз S-функцій //
Радіоелектроніка та молодь у XXI столітті / Харківський національний університет радіоелектроніки. — Харків, 2012. — с. 130 – 131.

Список публікацій II

Кіянчук Р. І.

Порівняльний аналіз IDEA-подібних блочних симетричних шифрів //
Міжнародна конференція "Комп'ютерна інженерія" / Харківський національний університет радіоелектроніки. — Харків, 2011. — с. 225 – 227.

Олійников Р. В., Кіянчук Р. І.

Перспективний блочний симетричний шифр оптимізований для апаратної реалізації //
Міжнародна конференція "Телекомунікаційні системи та технології" / Харківський національний університет радіоелектроніки. — Т. II. — Харків, Україна, 2011. — с. 321 – 330.

Олейников, Р. В. and Киянчук, Р. И.

Использование T-функций в симметричных криптографических преобразованиях //
Материалы международной научно-практической конференции «Перспективы развития информационных и транспортно-таможенных технологий в таможенном деле, внешнеэкономической деятельности и управлении организациями» / Харьковский национальный университет радиоэлектроники. — Днепропетровск, 2011. — с. 213 – 215.

Долгов, В. И. and Лисицкая, И. В. and Киянчук, Р. И.

RIJNDAEL – это новое или хорошо забытое старое? //
Компьютерные Науки и Технологии / — 2009. — с. 32 – 35.