Харківський національний університет радіоелектроніки

Аналіз криптографічних властивостей перспективних симетричних перетворень

Магістерська робота

Руслан Кіянчук

ruslan.kiyanchuk@gmail.com

Науковий керівник: Олійников Р. В.

Харків 2013

Актуальність

Нагальні проблеми

- Незважаючи на розвиток криптографії, значна кількість сучасних комунікаційних систем використовують шифри, що не забезпечують належний рівень безпеки.

Стандарти мобільного зв'язку:

GSM: A5/1 можливо зламати за секунди (rainbow таблиці);

3G: KASUMI шифр базується на алгоритмі MISTY1, атака вимагає 2^{26} наборів даних, 2^{30} байт пам'яті, 2^{32} операцій.

Супутникові телефони:

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

GMR-2 неопублікований алгоритм (атака потребує 65 байт 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

Напрями розвитку симетричної криптографії

ГОСТ 28147-89

- прийнятий у 1989 р. стандартом блочного шифрування у СРСР;
- широко застосовується в Україні та країнах СНД;
- використовує структуру Фейстеля;
- запропонований для стандартизації в ISO у 2010 р;
- перспективний для використання у мало-ресурсній криптографії;
- відсутня оцінка стійкості до алгебраїчного криптоаналізу.

MISTY1

- розроблений у 1995 р. в Mitsubishi Electric;
- використовує рекурсивну структуру Фейстеля;
- обраний європейським проектом NESSIE;
- рекомендований для використання у державних структурах Японії проектом CRYPTREC;
- рекомендований для використання в Інтернет (RFC 2994);
- не вразливий до атаки, що застосована для криптоаналізу KASUMI;
- 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”.

Етапи атаки

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

Перетворення, що найчастіше використовуються у шифрах

- бітові перестановки;
- модульне додавання (XOR $\Leftrightarrow$ додавання за модулем 2);
- логічні операції (AND, OR, NOT);
- блоки замін (S-box).

Алгебраїчна нормальна форма (АНФ)

- многочлен на кільцем $\mathbb{Z}_2$;
- операція множення — кон'юнкція ($\wedge$);
- операція додавання — XOR ($\oplus$);

Функція OR

$$x \vee y = (x \wedge y) \oplus x \oplus y \ .$$

x	y	$x \vee y$
T	T	T
T	F	T
F	T	T
F	F	F

x	y	$x \veebar y \veebar (x \wedge y)$
T	T	T
T	F	T
F	T	T
F	F	F

Функція NOT

$$\neg x = x \oplus 1 \ .$$

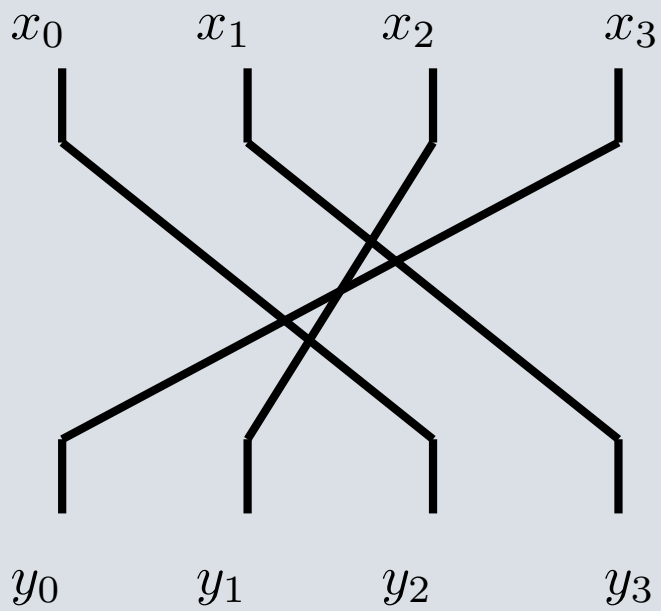
Побудова системи алгебраїчних рівнянь

Опис бітових перестановок

$$\begin{cases} y_0 \oplus x_3 = 0; \\ y_1 \oplus x_2 = 0; \\ y_2 \oplus x_0 = 0; \\ y_3 \oplus x_1 = 0. \end{cases}$$

- 4 рівняння від 8 змінних;
- бітовий зсув описується аналогічно;
- за можливості варто уникати додавання нових рівнянь та реалізовувати перестановку безпосередньою зміною порядку невідомих.

Бітова перестановка



Стандартний опис модульного додавання

- $R = X + Y \mod n$;
  $X = (x_0, \ldots, x_{n-1})$; $Y = (y_0, \ldots, y_{n-1})$; $R = (r_0, \ldots, r_{n-1})$;
- $r_i = x_i \oplus y_i \oplus c_{i-1}$; $\quad c_i = r_{i+1} \oplus x_{i+1} \oplus y_{i+1}$.

- Головна мета — описати суматор системой рівнянь другого степеня, не вводячи додаткових змінних для бітів переносу.
- $0 < i < (n-1)$:
  $(x_i \oplus r_i)(x_i \oplus c_i) = 0$;
  $(y_i \oplus r_i)(y_i \oplus c_i) = 0$;
  $(x_i \oplus y_i) \cdot r_i \oplus x_i y_i \oplus x_i \oplus y_i \oplus c_i = 0$.

Опис суматора рівняннями другого степеня

$r_0 = x_0 \oplus y_0$;
$x_i \oplus x_i r_i \oplus x_i r_{i+1} \oplus x_i x_{i+1} \oplus x_i y_{i+1} \oplus r_i r_{i+1} \oplus r_i x_{i+1} \oplus r_i y_{i+1} = 0$;
$y_i \oplus y_i r_i \oplus y_i r_{i+1} \oplus y_i x_{i+1} \oplus y_i y_{i+1} \oplus r_i r_{i+1} \oplus r_i x_{i+1} \oplus r_i y_{i+1} = 0$;
$x_i r_i \oplus y_i r_i \oplus x_i y_i \oplus x_i \oplus y_i \oplus r_{i+1} \oplus x_{i+1} \oplus y_{i+1} = 0$.

Побудова системи алгебраїчних рівнянь

Опис S-блоків

Підстановка 8-го степеня

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 0 & 4 & 2 & 5 & 1 & 3 \end{pmatrix}$$

1. Побудова матриці 8×22; кожний рядок містить значення кожного з 22 мономів для кожного з 8 можливих вхідних значень;
2. пошук ядра лінійного відображення (вирішення методом Гауса);
3. підстановка описується 14 рівняннями.

$$\left(\begin{array}{ccccccccc|c}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & & x_0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & & x_1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & & x_2 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & & y_0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & & y_1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & & y_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & & x_0x_1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & & x_0x_2 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & & x_0y_0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & & x_0y_1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & & x_0y_2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & & x_1x_2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & & x_1y_0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & x_1y_1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & & x_1y_2 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & & x_2y_0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & & x_2y_1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & & x_2y_2 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & & y_0y_1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & & y_0y_2 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & y_1y_2
\end{array}\right)$$

Побудова системи алгебраїчних рівнянь

Опис S-блоків

$$\left(\begin{array}{cccccccc|l}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_0y_0 + x_1 + x_2 + y_0 + y_1 + 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & x_0y_0 + x_0 + x_1 + y_2 + 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & x_0y_0 + x_0 + y_0 + 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & x_0y_0 + x_0 + x_2 + y_1 + y_2 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & x_0y_0 + x_0 + x_1 + x_2 + y_0 + y_1 + y_2 + 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & x_0y_0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & x_0y_0 + x_2 + y_0 + y_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_0y_0 + x_1 + y_1 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_0x_2 + x_1 + y_1 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_0x_1 + x_1 + x_2 + y_0 + y_1 + y_2 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_0y_1 + x_0 + x_2 + y_0 + y_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_0y_0 + x_0y_2 + x_1 + x_2 + y_0 + y_1 + y_2 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_1x_2 + x_0 + x_1 + x_2 + y_2 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_0y_0 + x_1y_0 + x_0 + x_2 + y_1 + y_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_0y_0 + x_1y_1 + x_1 + y_1 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_1y_2 + x_1 + x_2 + y_0 + y_1 + y_2 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_0y_0 + x_2y_0 + x_1 + x_2 + y_1 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_2y_1 + x_0 + y_1 + y_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_2y_2 + x_1 + y_1 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y_0y_1 + x_0 + x_2 + y_0 + y_1 + y_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y_0y_2 + x_1 + x_2 + y_0 + y_1 + 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y_1y_2 + x_2 + y_0
\end{array}\right)$$

Методи вирішення систем нелінійних рівнянь

Зведений базис Ґробнера

- узагальнення методу Гауса для систем нелінійних рівнянь;
- алгоритми Бухберґера, $F4$, $F5$.

Задача здійснимості бульових формул (SAT-solvers)

- пошук значень змінних, що задовольняють систему рівнянь.

Цілочислове лінійне програмування (Mixed Integer Solvers)

- вирішення екстремальної задачі — знаходження мінімуму (або максимуму) функції при заданих обмеженнях.

Алгебраїчні диференціали вищого порядку

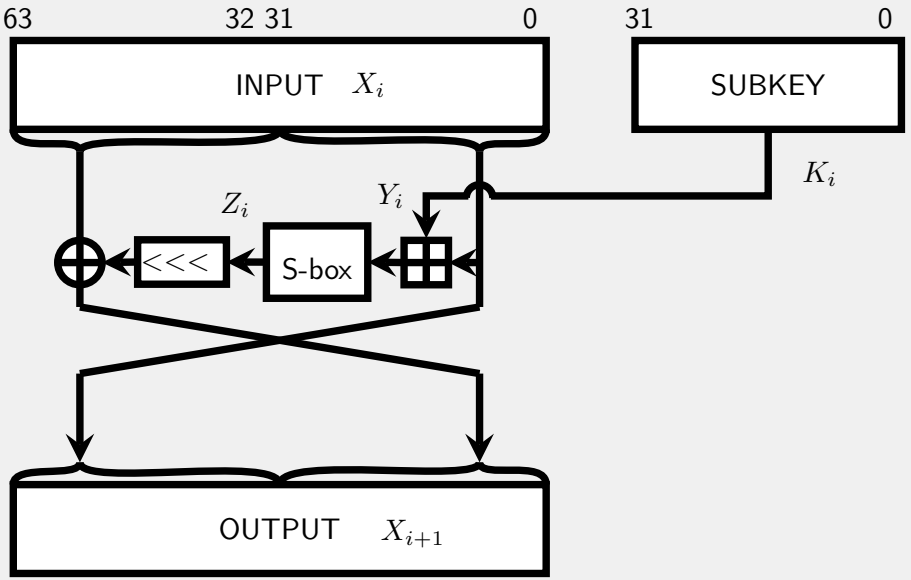
- “кубічні атаки” — представлення функції шифрування у виді поліноміальних рівнянь низького степеня

Блоковий симетричний шифр ГОСТ 28147-89

Система алгебраїчних рівнянь

Змінні одного раунда

$X_{r,\,0\ldots63}$ вхідний блок;
$K_{r\%8,\,0\ldots31}$ біти ключа;
$Y_{r,\,0\ldots31}$ результат додавання;
$Z_{r,\,0\ldots31}$ результат заміни;
$X_{r+1,\,0\ldots63}$ вихід раунда.



Характеристика системи

- $31 \cdot 3 + 1 = 94$ рівняння для складання з ключем;
- $21 \cdot 8 = 168$ рівнянь для S-блоків;
- один раунд шифру містить 325 поліномів другого степеня;
- повний шифр — 10432 рівняння від 4416 змінних (при використанні S-блоків з ГОСТ 34.311);

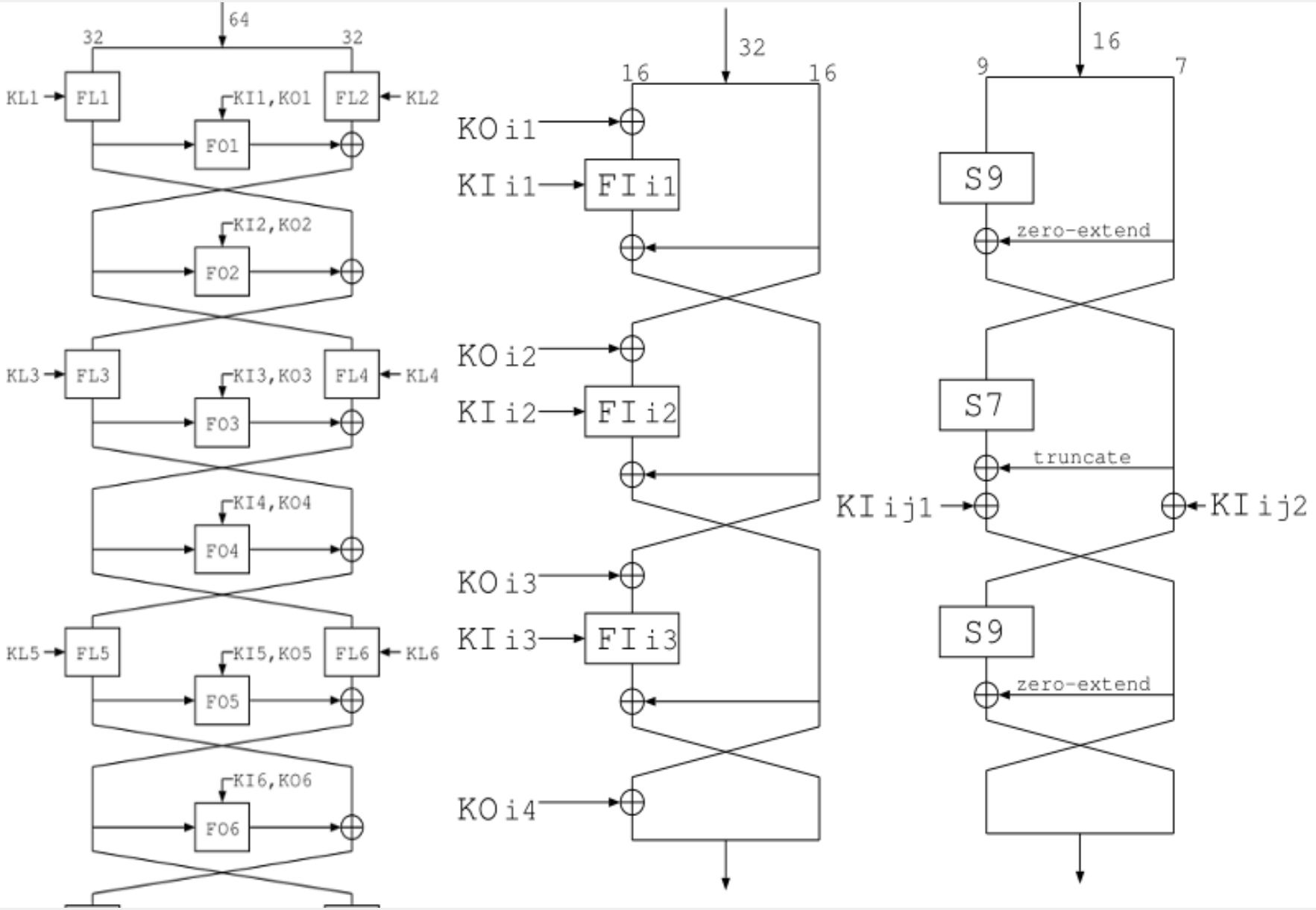
Апаратне забезпечення

CPU	Intel Core i3;
RAM	16 Gb RAM;
OS	Gentoo Linux ;
Software	Sage v5.6;
	CryptoMiniSat v2.8.

Атака

- Використано 4 пари відкритого та шифрованого тексту;
- Відновлено 192 біти використаного підключа (6 раундів);
- Вирішено систему 1950 рівнянь від 828 змінних.
- Час обчислення 40 год.

Блоковий симетричний шифр MISTY1



S-блок S_7

$$
\begin{aligned}
y_0 = {} & x_0 + x_1x_3 + x_0x_3x_4 + x_1x_5 + x_0x_2x_5 + x_4x_5 + \\
& + x_0x_1x_6 + x_2x_6 + x_0x_5x_6 + x_3x_5x_6 + 1 \\
y_1 = {} & x_0x_2 + x_0x_4 + x_3x_4 + x_1x_5 + x_2x_4x_5 + x_6 + \\
& + x_0x_6 + x_3x_6 + x_2x_3x_6 + x_1x_4x_6 + x_0x_5x_6 + 1 \\
y_2 = {} & x_1x_2 + x_0x_2x_3 + x_4 + x_1x_4 + x_0x_1x_4 + x_0x_5 + x_0x_4x_5 + \\
& + x_3x_4x_5 + x_1x_6 + x_3x_6 + x_0x_3x_6 + x_4x_6 + x_2x_4x_6 \\
y_3 = {} & x_0 + x_1 + x_0x_1x_2 + x_0x_3 + x_2x_4 + x_1x_4x_5 + \\
& + x_2x_6 + x_1x_3x_6 + x_0x_4x_6 + x_5x_6 + 1 \\
y_4 = {} & x_2x_3 + x_0x_4 + x_1x_3x_4 + x_5 + x_2x_5 + x_1x_2x_5 + \\
& + x_0x_3x_5 + x_1x_6 + x_1x_5x_6 + x_4x_5x_6 + 1 \\
y_5 = {} & x_0 + x_1 + x_2 + x_0x_1x_2 + x_0x_3 + x_1x_2x_3 + x_1x_4 + \\
& + x_0x_2x_4 + x_0x_5 + x_0x_1x_5 + x_3x_5 + x_0x_6 + x_2x_5x_6 \\
y_6 = {} & x_0x_1 + x_3 + x_0x_3 + x_2x_3x_4 + x_0x_5 + x_2x_5 + \\
& + x_3x_5 + x_1x_3x_5 + x_1x_6 + x_1x_2x_6 + x_0x_3x_6 + x_4x_6 + x_2x_5x_6
\end{aligned}
$$

S-блок S_9

$$
\begin{aligned}
y_0 = {} & x_0x_4 + x_0x_5 + x_1x_5 + x_1x_6 + x_2x_6 + x_2x_7 + \\
& + x_3x_7 + x_3x_8 + x_4x_8 + 1 \\
y_1 = {} & x_0x_2 + x_3 + x_1x_3 + x_2x_3 + x_3x_4 + x_4x_5 + x_0x_6 + \\
& + x_2x_6 + x_7 + x_0x_8 + x_3x_8 + x_5x_8 + 1 \\
y_2 = {} & x_0x_1 + x_1x_3 + x_4 + x_0x_4 + x_2x_4 + x_3x_4 + x_4x_5 + \\
& + x_0x_6 + x_5x_6 + x_1x_7 + x_3x_7 + x_8 \\
y_3 = {} & x_0 + x_1x_2 + x_2x_4 + x_5 + x_1x_5 + x_3x_5 + x_4x_5 + \\
& + x_5x_6 + x_1x_7 + x_6x_7 + x_2x_8 + x_4x_8 \\
y_4 = {} & x_1 + x_0x_3 + x_2x_3 + x_0x_5 + x_3x_5 + x_6 + x_2x_6 + \\
& + x_4x_6 + x_5x_6 + x_6x_7 + x_2x_8 + x_7x_8 \\
y_5 = {} & x_2 + x_0x_3 + x_1x_4 + x_3x_4 + x_1x_6 + x_4x_6 + x_7 + \\
& + x_3x_7 + x_5x_7 + x_6x_7 + x_0x_8 + x_7x_8 \\
y_6 = {} & x_0x_1 + x_3 + x_1x_4 + x_2x_5 + x_4x_5 + x_2x_7 + x_5x_7 + \\
& + x_8 + x_0x_8 + x_4x_8 + x_6x_8 + x_7x_8 + 1 \\
y_7 = {} & x_1 + x_0x_1 + x_1x_2 + x_2x_3 + x_0x_4 + x_5 + x_1x_6 + \\
& + x_3x_6 + x_0x_7 + x_4x_7 + x_6x_7 + x_1x_8 + 1 \\
y_8 = {} & x_0 + x_0x_1 + x_1x_2 + x_4 + x_0x_5 + x_2x_5 + x_3x_6 + \\
& + x_5x_6 + x_0x_7 + x_0x_8 + x_3x_8 + x_6x_8 + 1
\end{aligned}
$$

Блоковий симетричний шифр MISTY1

Система алгебраїчних рівнянь

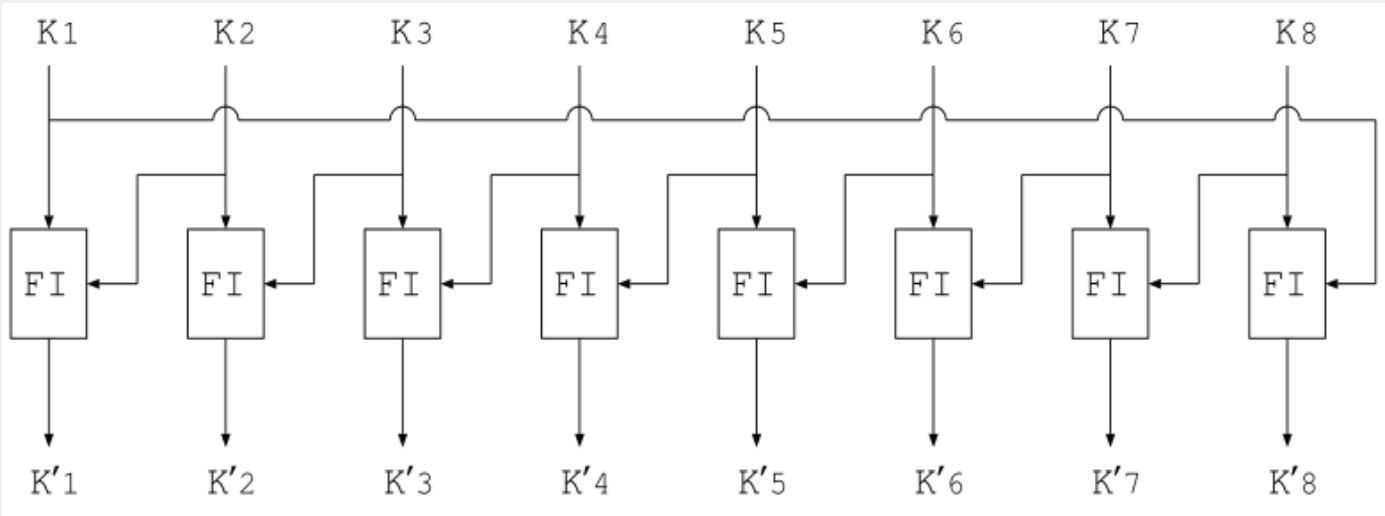


Рисунок: Схема розгортання ключа

Характеристика системи

функція FI	205 рівнянь від 82 змінних;
функція FO	695 рівнянь від 374 змінних;
key schedule	1640 рівнянь від 528 змінних;
раунд	1640 рівнянь від 988 змінних;
шифр	8448 рівнянь від 3680 змінних.

Апаратне забезпечення

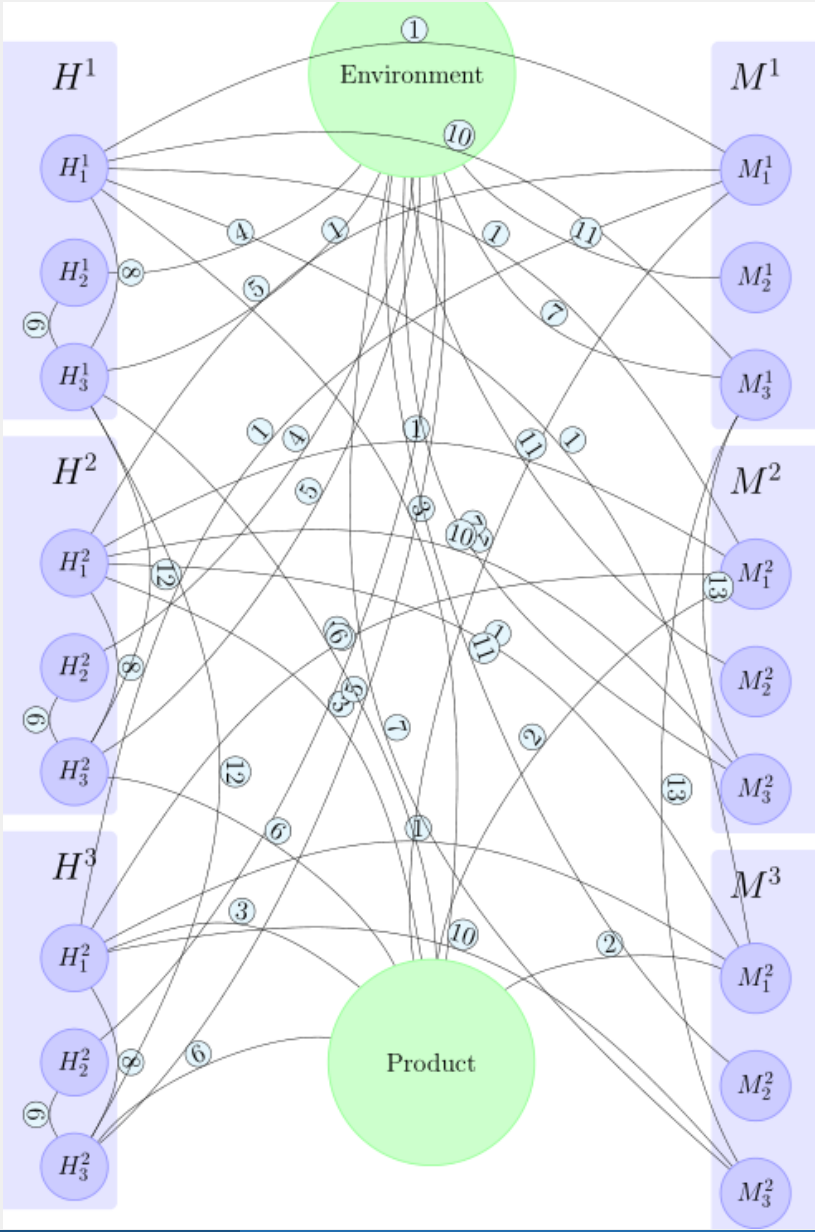
CPU	Intel Core i5-3570;
RAM	8 Gb RAM;
OS	Ubuntu Linux 12.04;
Software	Sage v5.9;
	CryptoMiniSat v3.0.

Атака

- Використано 4 пари відкритого та шифрованого тексту;
- Відновлено 176 біт використаного підключа;
- Вирішено систему 1640 рівнянь від 988 змінних (2 раунди).
- Час обчислення 50 год.

Охорона праці та безпека в надзвичайних ситуаціях

- Проаналізовано умови праці на відповідність нормативним документам з техніки безпеки та санітарії.
- Побудовано систему взаємодії «Людина-Машина-Середовище» з метою виявлення та оцінки можливих небезпечних та шкідливих виробничих факторів.
- Розраховано систему кондиціонування приміщення для забезпечення норм мікроклімату.



Висновки

- Запропоновані методи опису рівнянь для криптографічних перетворень дозволяють ефективно побудувати систему нелінійних рівнянь для більшості сучасних криптоалгоритмів.
- Використовуючи описані методики, визначено систему алгебраїчних рівнянь для шифрів ГОСТ 28147-89 та MISTY1.
- Представлена реалізація досліджуваних криптоалгоритмів (ГОСТ 28147-89, MISTY1) дозволяє побудувати відповідні системи алгебраїчних рівнянь для аналізу.

З використанням представленої реалізації

- Вирішено систему рівнянь, що описує 6 раундів шифру ГОСТ 28147-89 з відновленням усіх біт використаних підключів.
- Вирішено систему рівнянь, що описує 2 раунди шифру MISTY1 з відновленням усіх біт використаних підключів.
- Для більшої кількості раундів можливо знайти еквівалентні ключі.

- Використання ресурсів з потужнішими обчислювальними можливостями дозволить підвищити ефективність аналізу.

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 блоковий 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.

Список публікацій III

Олейников, Р. В., Киянчук, Р. И., Горбенко, И. Д.

Алгебраический криптоанализ ГОСТ 28147-89

XV Юбилейная Международная научно-практическая конференция 22–25 мая 2012 / Харьковский национальный университет радиоэлектроники. — Киев, 2012. — с. 130 – 131.

Киянчук Р. І.

Алгебраический криптоанализ ГОСТ 28147-89

Радиоэлектроника и молодёжь в XXI веке / Харьковский национальный университет радиоэлектроники. — Харків, 2013. — с. 119 – 120.