С позиции спектрального анализа возможно ввести иерархию объектов, предсказывать развитие их характеристик, а также оценивать целевые свойства объектов на базе лингвистических особенностей языка источника потока и его преобразующих особенностей.

Литература: 1. Осинский Л.М., Манухин А.В. Обработка текстовой информации. Портретный метод // Материалы международной научно–технической конференции "Повышение эффективности систем защиты информации". "Защита–97". – Киев: КМУГА, 1997. – с. 51–53. 2. Четвериков И.А., Манухин А.В. Спектральный анализ текстовой информации и ее кластеризация // Защита информации: Сборник научных трудов. – Киев: КМУГА, 1998. – с. 224–229.

УДК 621.391

ПРОБЛЕМИ РАХУВАННЯ КІЛЬКОСТІ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ НАД ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

Олександр Теліженко
Київський військовий інститут управління і зв'язку

Анотація: **Аналізується одна з важливих проблем створення ефективних криптографічних систем на еліптичних кривих.**
Summary: **Analyses one of important creation problems of effective cryptographic systems on elliptic curves.**
Ключові слова: **Еліптичні криві, відкриті ключі, несимитрічні криптосистеми.**

Застосування еліптичних кривих для проблем захисту інформації стає все більш поширеним у всьому світі. Це обумовлено тим, що криптографічна система, яка побудована на еліптичних кривих є системою з відкритими ключами, дає не меньшу стійкість ніж інші несиметричні криптосистеми, але має довжину ключів, що використовуються, в кілька разів менше. Найбільш ефективне використання мають криптосистеми, які створюються за допомогою еліптичних кривих над полями характеристики 2. В цьому випадку такі системи технічно реалізуються з меншими складнощами та дозволяють вирішувати питання не тільки шифрування, а й знаходження та виправлення помилок після передачі повідомлення каналом зв'язку. Для практичного застосування рекомендують не суперсингулярні криві, які мають наступний вигляд:

$$y^2+xy=x^3+a_2x^2+a_6, \quad \text{де } a_2,a_6 \in GF(2^n).$$

При цьому n обирається більш ніж 160. Звідти виникає питання підрахування кількості точок еліптичної кривої, тому як кількість елементів поля дуже велика. Відома теорема Хассе, в якій дана оцінка кількості точок N:

$$q + 1 - 2\sqrt{q} \le N \le q + 1 + 2\sqrt{q}\ , \text{ де } q=/GF(2^n)/.$$

Однак для максимальної стійкості криптосистеми необхідно обирати криві, для яких число, яке дорівнює кількості точок, було б максимальним, а крім того мало б великий простий дільник. Для знаходження кривих з такими властивостями необхідно знати точну кількість точок еліптичної кривої, яку ми обрали. Це дуже складна задача, однак в окремому випадку вона може бути вирішена саме для кінцевих полів.

Якщо число n має вигляд $n=h*m$, тобто має два прості множники, існує рекурсивна формула, за допомогою якої можна підрахувати кількість точок еліптичної кривої над полем $GF(2^{kh})$. Для цього вводиться спеціальна функція $L(p,Z,K)=V(K)$, яка має початкові дані:

$$V(0)=2,\ V(1)=p,\ V(K)=pV(k-1)-ZV(k-2).$$

Кількість точок R еліптичної кривої в цьому випадку буде дорівнювати:

$$R=2^{hm}+1-L(2^h-(N-1),2^h,K).$$

Значення Z залежить від кількості точок еліптичної кривої над полем $GF(2^h)$ [1].

Вибір значення n повинен задовольняти вимозі існування в кінцевому полі оптимального нормального базису для спрощення арифметичних операцій [2]. Мінімальне таке значення, яке задовольняє всім вимогам, буде 183=3*61. Крім того, існують складнощі в випадковому виборі самої еліптичної кривої, тобто вибір коефіцієнтів a_2 та a_6 таким чином, щоб кількість точок еліптичної кривої була максимальною, а для ефективного використання криптосистеми для полів характеристики 2 потрібно щоб:

$$R=2^s qb,$$

де b - велике просте число, q - невеликий множник.

В інших випадках знайти кількість точок еліптичної кривої є дуже складною задачею і потребує дуже багато обчислювальних ресурсів.

Література: 1. Dan Beaureal. Efficient algorithms for implementing elliptic curve public-key schemes. A Thesis submitted to the Faculty of the Worcester Polytechnic Institute. 1996. 2. R.Mullin, I.Onyszchuk, S.Vanstone and R.Wilson. Optimal normal bases in GF(p^n). Discrete Applied Mathematics, 22(1988/89). 149-161.

УДК 638.253.231

Differential Cryptanalysis of Feistel's Iterated Block Ciphers

Alexander Telizhenko, Sergey Limar
Kiev Military Institute for Command and Communication

*Анотація:***В статті обговорюються базові принципи Диференційного криптоаналіза, концепції, алгоритми, ідеї і методи, які забезпечують цей тип атаки, а також математичне обгрунтування.**
Summary: **Here are described the basic principles of Differential Cryptanalysis, concepts, algorithms, ideas and methods which provide this kind of attack and also its mathematical background.**
*Ключові слова:***Differential attack, round differentials, conditional characteristic, probabilistic influence, chosen plaintext.**

I Introduction

This paper will attempt to introduce some concepts of cryptography, and especially some ideas pertaining to cryptanalysis, the breaking of encryption. The first method which reduced the complexity of attacking DES below (half of) exhaustive search.

Note: In all the following discussion we ignore the existence of the initial and the final permutations, since they do not affect the analysis.

In this research announcement, we describe a related attack (which we call Differential Cryptanalysis), and show that it is applicable to almost any secret key cryptosystem proposed so far in the open literature. In particular, we have actually implemented it in the case of DES, and demonstrated that under the same software differential model, we can extract the full DES key from a sealed tamperproof DES encryptor by analysing fewer than 200 ciphertexts generated from unknown plaintexts. The power of Differential Cryptanalysis is demonstrated by the fact that even if DES is replaced by triple DES (whose 168 bits of key were assumed to make it practically invulnerable), essentially the same attack can break it with essentially the same number of given ciphertexts.

II Motivation

1. All the operations except the S boxes arc linear.
2. Mixing the key in all the rounds prohibits the attacker from knowing which entries of the S boxes arc actually used, and thus he cannot know their output.

How can we inhibit the key from hiding the information?

3. Ideas, methods and principles of Differential Attack.

The basic idea of differential cryptanalysis: Study the differences between two encryptions of two different plaintexts: P and P^*,

Notation: For any value X during the encryption of P, and the corresponding value X^* during encryption of P^*, denote the difference by $X' = X \oplus X^*$.

Advantages: It is easy to predict the output difference of linear operations given the input difference:

1. Unary operations (E, P, IP):
$$\left(P(X)\right)' = P(X) \oplus P\left(X^*\right) = P(X')$$
2. Boolean operations (XOR):
$$\left(X \oplus Y\right)' = \left(X \oplus Y\right) \oplus \left(X^* \oplus Y^*\right) = X' \oplus Y'$$
3. Mixing the key:
$$\left(X \oplus K\right)' = \left(X \oplus K\right) \oplus \left(X^* \oplus K\right) = X'$$

We conclude that the differences are linear in linear operations, and in particular, the result is key independent.