КРИПТОЛОГІЯ / CRYPTOLOGY

КРИПТОГРАФІЧНА СТІЙКІСТЬ МОДИФІКАЦІЇ ПРОТОКОЛУ ДІФІ-ХЕЛМАНА ЗА ДОПОМОГОЮ ІНТЕГРАЛА ЕЙЛЕРА ІІ РОДУ

Григорій Кравцов

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ, Україна

КРАВЦОВ Григорій Олексійович

Рік та місце народження: 1977, м. Миколаїв, Україна.
Освіта: Севастопольський військово-морський інститут ім. П.С.Нахімова.
Посада: аспірант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.
Наукові інтереси: кібернетична безпека Smart Grid.
Публікації: 6 робіт з питань інформаційної безпеки.
E-mail: Java_Dev@i.ua.

Анотація: *Ця стаття розкриває питання криптографічної стійкості модифікованого протоколу Діффі-Хеллмана за допомогою інтеграла Ейлера 2 роду. На основі цього підходу в 2005 році був запропонований новий криптографічний протокол. Результати аналізу відкритих матеріалів друку показують, що методи атаки на протокол не публікувалися, що дозволяє чекати застосування протоколу на практиці в цілях захисту інформації, наприклад, в Smart Grid.*

Ключові слова: *алгоритм Діфі-Хелмана, інтеграл Ейлера ІІ роду, криптографічний протокол, криптографічна стійкість.*

Для впровадження точок обліку з здатністю ре-конфігурування криптографічних алгоритмів [1, 2] в інтелектуальних електричних мережах електроенергетичних систем [3] постає завдання розробки криптографічного протоколу, який би забезпечив можливість обліку транзакцій з наступним білінгом.

Відома задача Діфі-Хелмана [4] основана на використанні функції возведення у ступінь в мультиплікативній групі простого поля: $f(x) = a^x mod p$, де p – просте число, a - примітивний елемент поля GF(p), $1 < x < p-1$. Ця фунція є кандидатом в односпрямовані функції. Дійсно, вона легко обчислюється, так як, використовуючи метод квадратів, значення цієї функції можна знайти з поліноміальною складністю, яка оцінюється як $O((\log\log p)^3)$, в той час. Як зворотня задача є вкрай складною.

Для досягнення поставленої мети було досліджено значну кількість раціональних функцій (елементарних та спеціальних) в результаті чого було обрано гама-функцію (інтеграл Ейлера 2-го роду). За основу було взято добуток

$$\Gamma(z) = \lim_{n\to\infty} \frac{n^z}{z} \prod_{k=1}^{n} \frac{k}{z+k}, \qquad (1)$$

який був представлений у вигляді:

$$G(n,a) = \frac{n^a}{a} \prod_{k=1}^{n} \frac{k}{a+k}, \qquad (2)$$

Що дає можливість визначити основну властивість як

$$G^m(n,a) = \frac{n^{am}}{a^m} \prod_{k=1}^{n} \left(\frac{k}{a+k} \right)^m. \qquad (3)$$

Значення $G(n,a)$ можуть бути «розміщені» в полі Галуа метрики p як

$$G(n,a) = \left(\frac{n^a}{a} \prod_{k=1}^{n} \frac{k}{a+k} \right) mod\ p. \qquad (4)$$

При відомих n та a рівняння (3) зводиться до задачі Діфі-Хелмана [4]. При невідомих n та a задача значно ускладнюється. Вираз (4) має певний сенс при використанні в процесорах цифрової обробки сигналів. Для використання в системах, де операції з плаваючою крапкою неприйнятні, пропонується використовувати

$$\begin{aligned} G(n,a) &= \left(n^a \prod_{k=1}^{n} a^k \right) mod\ p = \\ &= \left(n^a\, a\ pow\left\{ \sum_{k=1}^{n} k \right\} \right) mod\ p, \end{aligned} \qquad (5)$$

де $a\ pow\{x\} = a^x$.

На підставі (5) пропонується криптографічний протокол з відкритими ключами з арбітром і центром сертифікації ключів. Властивість (3) в такому випадку має форму

$$G^m(n,a) = \left(n^{am} a\ pow\left\{ m\sum_{k=1}^{n} k \right\} \right) mod\ p. \qquad (6)$$

Припустимо, що

$$f(n,a) = n^a \prod_{k=1}^{n} a^k. \qquad (7)$$

Необхідно знайти значення n, якщо відомі a та $f(n,a)$ і знайти a, якщо відомі n та $f(n,a)$. Якщо шукати рішення через логарифмування, то отримаємо при невідомому n

$$log_a\left(f(n,a)\right) = a\,log_a(n) + \sum_{k=1}^{n} k, \qquad (8)$$

а при невідомому a

$$log_n\left(f(n,a)\right) = a + (log_n(a))\sum_{k=1}^{n} k. \qquad (9)$$

За формулою арифметичної прогресії рівняння (7) та (8) приймуть вигляд:

$$log_a\left(f(n,a)\right) = a\,log_a(n) + \frac{n(1+n)}{2}, \qquad (10)$$

$$log_n\left(f(n,a)\right) = a + (log_n(a))\frac{n(1+n)}{2}. \qquad (11)$$

Наведені рівняння (9) та (10) є трансцендентними, тобто можуть бути вирішені лише приблизно, а у випадку поміщення в поле Галуа – лише перебором, що є позитивною рисою.

Спробуємо вирішити рівняння $f_0(n,a) = n^a a^n$. Якщо це нам вдасться, то за аналогією ми зможемо знайти рішення рівняння $f(n,a) = n^a a^{\frac{n(n+1)}{2}}$.

Представимо n^a та a^n в вигляді сум і найдемо їх добуток

$$n^a = \sum_{k=0}^{\infty} \frac{[aln(n)]^k}{k!}, a^n = \sum_{k=0}^{\infty} \frac{[nln(a)]^k}{k!}, \qquad (12)$$

$$a^n n^a = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} [a^i n^j (ln(n))^i (ln(a))^j (q)^{(-1)}], \qquad (13)$$

де

$$q = 4^{i+j} \prod_{k=1}^{\infty} \frac{\Gamma\left(\frac{1}{2} + \frac{i}{2^k}\right)\Gamma\left(\frac{1}{2} + \frac{j}{2^k}\right)}{\Gamma^2\left(\frac{1}{2}\right)}.$$

Функція $f_0(n,a) = n^a a^n$ має цікаві властивості:

$$\frac{df_0(n,a)}{da} = f_0(n,a)\left(\frac{n}{a} + \ln(n)\right). \qquad (14)$$

$$df_0(n,a) = f_0(n,a)\left(\left(\frac{n}{a} + \ln(n)\right)da + \left(\frac{a}{n} + \ln(a)\right)dn\right). \qquad (15)$$

Взявши (5) за основу, в 2007 році було запропоновано криптографічний протокол [5].

З метою визначення чисельних показників підвищення стійкості запропонованої модифікації покажемо зведення для визначення обчислювальної складності алгоритмів:

Порівняння показників обчислення Таблиця 1

Показник	**Діфі-Хелмана**	**Запропонований**
База алгоритму	$f(x) = a^n mod p,$	$G^m(n,a) = \frac{n^{am}}{a^m}\prod_{k=1}^{n}\left(\frac{k}{a+k}\right)^m$
Зведення	$a^n = \sum_{k=0}^{\infty}\frac{[nln(a)]^k}{k!}$	$a^n n^a = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\left[a^i n^j \left(ln(n)\right)^i \left(ln(a)\right)^j (q)^{-1}\right]$ $q = 4^{i+j}\prod_{k=1}^{\infty}\frac{\Gamma\left(\frac{1}{2}+\frac{i}{2^k}\right)\Gamma\left(\frac{1}{2}+\frac{j}{2^k}\right)}{\Gamma^2\left(\frac{1}{2}\right)}$
Експоненціальна складність	$\bigcup_{k=1}^{\infty} O(2^{n^k})$	$\bigcup_{k=1}^{\infty} O(2^{2n^k})$

Запропонований криптографічний протокол опубліковано в 2005 році [5]. Більш як 7 років з дати опублікування протоколу у відкритих джерелах не публікувалися роботи, які б свідчили про вразливість запропонованого протоколу.

Висновок. Запропонований підхід має вищу експоненціальну складність, що доводить його більшу криптографічну стійкість порівняно з базовою схемою Діфі-Хелмана.

Література

[1] Кравцов Г.О. Використання математич-них примітивів для реалізації криптографічних алгоритмів в пристроях криптографічного захисту інформації / Г.О. Кравцов. — Зб. наукових праць ІПМЕ ім. Г.Є.Пухова НАН України «Моделювання та інформаційні технології». — К., 2012. — Вип.65.-С.16-22.

[2] Кравцов Г.О. Спосіб застосування криптографічних алгоритмів у криптографічних

засобах захисту інформації/ Г.О. Кравцов — Зб. наукових праць ІПМЕ ім. Г.Є.Пухова НАН України «Моделювання та інформаційні технології». — Київ, 2012. — Вип.66. — С.30-37.

[3] Стогній Б.С. Інтелектуальні електричні мережі електроенергетичних систем та їхнє технологічне забезпечення / Б.С. Стогній, О.В. Кириленко, С.П. Денисюк. - Технічна електродинаміка, ISSN 1607-7970, №6, 2010 р. – с. 44-50. Режим доступу: http://techned.org.ua/article/10-6/st7.pdf — Дата доступу: серпень 2013. – Назва з екрану.

[4] Dh.W. Diffie, M.E. Hellman. New directions in cryptography, IEEE Trans. Inform. Theory, vol. IT-22, pp. 644-654, Nov. 1976

[5] Кравцов Г.А. Задача Диффи-Хелмана и ее развитие / Кравцов Г.А. — Зб. наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. — К., 2005. —Вип.28. — С.62-68.

УДК 621.391.7 (045)

Кравцов Г.А. Криптографическая стойкость модификации протокола Диффи-Хеллмана с помощью интеграла Эйлера второго рода

Аннотация: *Эта статья раскрывает вопрос криптографической стойкости модифицированного протокола Диффи-Хеллмана с помощью интеграла Эйлера 2 рода. На основе этого подхода в 2005 году был предложен новый криптографической протокол. Результаты анализа материалов открытой печати показывают, что методы атаки по протоколу не были опубликованы, что позволяет ожидать применения протокола на практике в целях защиты информации, например, в Smart Grid.*

Ключевые слова: *алгоритм Дифи-Хеллмана, интеграл Эйлера II рода, криптографический протокол, криптографическая стойкость.*

Kravtsov H.O. The cryptographic strength of the modified Diffie-Hellman key exchange protocol using Euler integral type II

Abstract: *This article shows the question of cryptographic strength of the modified Diffie-Hellman key exchange protocol using the Euler integral type II. On the basis of this approach in 2005 has been proposed a new cryptographic protocol. The results of the analysis of the press materials indicate that the methods of attack on the protocol have not been published, that allows us to expect the protocol into practice in order to secure the information, for example, in Smart Grid.*

Key words: *Diffie-Hellman key exchange, Euler integral type II, cryptographic protocol, cryptographic strength (security).*

Отримано *13 травня 2013 року*, затверджено редколегією *3 червня 2013 року*