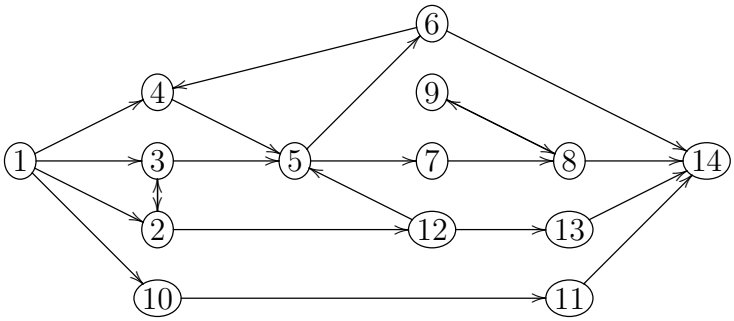

Рис. 1. Орграф $\Gamma(1, 14)$

К 0-му ярусу относится вершина 1, к 1-му — ксс U_1 и U_2, ко 2-му — ксс U_3 и U_4, к 3-му — вершина 14. Множества предшественников: $P(U_1) = \{1\}$, $P(U_2) = \{1, 2, 3, 12, 13\}$, $P(U_3) = P(U_2) \cup \{4, 5, 6, 7\}$, $P(U_4) = \{1, 2, 3\}$.

С помощью этой модели опишем перемешивающий орграф генератора с перемежающимся шагом [3, гл. 18], построенный на базе двоичных регистров правого сдвига: управляющего длины m и двух генерирующих длин n и r, $m, n, r > 1$. В зависимости от управляющего знака сдвигается либо первый, либо второй генерирующий регистр.

Перемешивающий орграф $\Gamma(h)$ преобразования h множества V_{m+n+r} состояний генератора является $i \times (m + n)$- и $i \times (m + n + r)$-примитивным [4] для любого $i \in \{1, \ldots, m\}$; $\Gamma(h)$ содержит $i, (m+n)$-ксс U_1 и U_2 (с множествами вершин $\{1, \ldots, m\}$ и $\{m + 1, \ldots, m + n\}$ соответственно) и $i, (m + n + r)$-ксс U_3 с множеством вершин $\{m + n + 1, \ldots, m + n + r\}$. Для любого $i \in \{1, \ldots, m\}$ в орграфе $\Gamma(i, m + n)$ имеется два яруса: к 0-му ярусу относится ксс U_1, к 1-му — ксс U_2; в орграфе $\Gamma(i, m + n + r)$ также имеется два яруса: к 0-му ярусу относится ксс U_1, к 1-му — ксс U_3.

ЛИТЕРАТУРА

1. *Кяжин С. Н.* О применении условий локальной примитивности и оценок локальных экспонентов орграфов // Прикладная дискретная математика. 2016. № 4(34). С. 81–98.
2. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
3. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
4. *Кяжин С. Н., Фомичев В. М.* Перемешивающие свойства двухкаскадных генераторов // Прикладная дискретная математика. Приложение. 2016. № 9. С. 60–62.

УДК 004.056.55 DOI 10.17223/2226308X/10/36

ВЕРСИЯ ПРОТОКОЛА ДИФФИ — ХЕЛЛМАНА, ИСПОЛЬЗУЮЩАЯ ДОПОЛНИТЕЛЬНЫЕ СКРЫТЫЕ МНОЖИТЕЛИ[1]

А. А. Обзор

Приводится версия протокола Диффи — Хеллмана, использующая скрытые множители из подгрупп мультипликативной группы конечного поля. Для раскрытия секрета данного протокола недостаточно решить проблему дискретного логарифма, необходимо также вычислить порядки некоторых элементов группы.

[1]Исследование выполнено за счёт гранта Российского научного фонда (проект №16-11-10002).

Ключевые слова: *криптография, протокол Диффи — Хеллмана, скрытые множители.*

В серии работ [1 – 4] В. А. Романьков предложил использовать скрытые множители из подгрупп мультипликативных групп соответствующих колец вычетов и конечных полей, чтобы придать системе шифрования RSA и ряду других криптографических схем свойства семантической секретности. В данной работе представлен аналог классического протокола Диффи — Хеллмана, основанного на трудности вычисления дискретного логарифма в мультипликативной группе конечного поля, также использующий скрытые множители из подгрупп этого поля.

Пусть $G = \mathbb{F}_q^*$ — мультипликативная группа конечного поля $\mathbb{F}_q$, $q = p^t$ (p — простое число), g — порождающий элемент этой группы. Целое x, $0 \leqslant x \leqslant q-2$, удовлетворяющее уравнению вида

$$g^x = f,$$

где f — произвольный элемент группы G, называется *дискретным логарифмом* элемента f по основанию g. Задача нахождения $\log_g(f)$ по порождающему элементу g и произвольному f известна как *проблема дискретного логарифма*. Она считается вычислительно трудной, значит, функция $\delta(x) = g^x$ может рассматриваться как односторонняя. Задача вычисления дискретного логарифма составляет основу целого ряда алгоритмов криптографии, в частности, на её сложности основывается криптографическая стойкость классического протокола Диффи — Хеллмана [5 – 7].

Версия протокола Диффи — Хеллмана

Протокол Диффи — Хеллмана строится на мультипликативной группе конечного поля. В предлагаемой версии этого протокола в качестве основы берётся мультипликативная группа $\mathbb{F}_p^*$ простого конечного поля $\mathbb{F}_p$ характеристики p, которая выбирается корреспондентами Алисой и Бобом на основе некоторых других данных (см. подробности далее). Алгоритмы построения больших простых чисел, в данном случае числа p, хорошо известны и эффективны [5, 6].

Итак, двум корреспондентам Алисе и Бобу необходимо выбрать секретным образом достаточно большое случайное число (секретный ключ), с помощью которого будет производиться дальнейшее шифрование, или для каких-то других целей. Считается, что переписка по поводу выбора этого числа происходит по открытому каналу связи.

Установка. Сначала Алиса выбирает секретное простое число r, а Боб — секретное простое число s. Затем Алиса случайным образом выбирает число x и передаёт Бобу произведение $r_1 = rx$. Боб выбирает случайным образом число y и передаёт Алисе произведение $s_1 = sy$. После этого они открытым образом договариваются о выборе простого числа p, такого, что $p = 1 + 2r_1s_1z$. Далее Алиса и Боб используют группу $G = \mathbb{F}_p^*$ для реализации алгоритма. Они договариваются о выборе элемента g группы G достаточно большого порядка $|g|$. Как и в классическом случае, в качестве g можно выбрать порождающий элемент. Данные p и g являются открытыми.

Выбор циклических подгрупп. Алиса выбирает циклическую подгруппу F группы G порядка r. Для этого она находит порождающий элемент этой подгруппы $f \in \mathbb{F}_p^*$, $|f| = r$, который существует, так как $r|(p-1)$ по построению p. Для нахождения этого элемента она случайным образом выбирает последовательно элементы f_i, $i = 1, 2, \ldots$, каждый раз вычисляя степень f_i^t, где $t = 2xs_1z = (p-1)/r$, до тех пор, пока не получит неравенство $f_i^t \neq 1$. Тогда она полагает $f = f_i^t$. Ясно, что $f^r = f^{p-1} = 1$. Так как r — простое число, то $|f| = r$. В группе $\mathbb{F}_p^*$ в точности

t элементов являются корнями из 1 степени t. Вероятность выбора такого элемента при случайном равномерном распределении равна $t/(p-1) = 1/r$. Следовательно, вероятность неудачи при выборе в m последовательных испытаниях равна $(1/r)^m$. При достаточно большом r и сравнительно небольшом значении m (20–30) вероятностью неудачи можно пренебречь.

После того как f найден, Алиса передаёт его Бобу. Аналогично Боб выбирает циклическую подгруппу H группы G порядка s и отправляет её порождающий элемент h Алисе.

Далее Алиса выбирает случайным образом натуральное число a и элемент $z \in H$ (случайную степень элемента h), вычисляет $u = zg^{ar}$ и передаёт результат Бобу. Тем временем Боб аналогичным образом выбирает натуральное число b и элемент $y \in F$ (случайную степень элемента f) и сообщает по сети элемент $v = yg^{bs}$ Алисе.

Формирование секретного ключа. Алиса, зная a, v и r, вычисляет $v^{ra} = y^{ra}g^{bsra} = g^{abrs}$, так как $y^r \equiv 1 \pmod{n}$. Боб, зная b, u и s, вычисляет $u^{sb} = z^{sb}g^{arsb} = g^{abrs}$. Таким образом, корреспонденты Алиса и Боб сформировали секретное число g^{abrs}.

Криптографическая стойкость. Криптографическая стойкость данного протокола основывается на трудной разрешимости двух проблем — дискретного логарифма и определения порядка элемента мультипликативной группы конечно поля. Известна разрешимость второй задачи за полиномиальное время при знании разложения порядка мультипликативной группы поля на примарные множители [5]. Тогда можно со сравнимой трудоёмкостью находить дискретные логарифмы, например алгоритмом Полига — Сильвера — Хеллмана. Такого разложения потенциальный взломщик не имеет. Более того, указанный алгоритм допускает практическое применение далеко не всегда. При наличии больших простых делителей в разложении необходимая база данных становится очень большой, что существенно замедляет работу алгоритма [5, 6].

Замечание 1. В предложенной версии числа r и s простые. Это условие можно исключить. Подгруппы F и H можно выбирать не обязательно циклическими. Можно, например, выбрать $F = gp(f_1, \ldots, f_k)$, где наименьшее общее кратное порядков элементов f_i равно r. Точно так же можно выбирать H, где аналогичное наименьшее общее кратное равно s.

ЛИТЕРАТУРА

1. *Романьков В. А.* Новая семантически стойкая система шифрования с открытым ключом на базе RSA // Прикладная дискретная математика. 2015. № 3 (29). С. 32–40.
2. *Roman'kov V. A.* New probabilistic public-key encryption based on the RSA cryptosystem // Groups, Complexity, Cryptology. 2015. V. 7. No. 2. P. 153–156.
3. *Roman'kov V. A.* How to make RSA and some other encryptions probabilistic. arXiv: 1603.0203v1 [cs: CR] 7 Mar 2016. P. 1–7.
4. *Романьков В. А.* Вариант семантически стойкого шифрования на базе RSA // Вестник Омского ун-та. 2016. № 3 (81). С. 7–9.
5. *Menezes A., van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. Boca Raton, London, New York, Washington: CRC Press, 1996. 816 p.
6. *Романьков В. А.* Введение в криптографию. М.: Форум, 2012. 239 с.
7. *Романьков В. А.* Алгебраическая криптография. Омск: ОмГУ, 2013. 135 с.