УДК 681.3.06:519.248.681

КРИПТОСИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ ГРУППЫ КОС

к.т.н. Б.И. Низиенко, Я.Ю. Стасева, В.Ю. Ковтун
(представил д.т.н., проф. С.В. Смеляков)

Рассматривается новая быстрая криптосистема с открытым ключом, предложенная на Crypto'2001. Приводится математический аппарат, положенный в основу криптосистемы, рассматриваются вопросы реализации, производится сравнение с другими широко используемыми криптосистемами.

Введение. На современном этапе интеграции Украины в мировое сообщество, участии в миротворческих операциях, возникает необходимость в обеспечении защиты автоматизированных систем управления на объектах государственной важности от возможных атак со стороны различных террористических и экстремистских организаций, которые активизируют свою деятельность по всему миру. Особенно это касается системы связи с мобильными рабочими местами с использованием устройств, с ограниченными возможностями, такими как PDA, мобильные телефоны, смарт-карт. Таким образом, возникает необходимость в разработке криптографических методов с открытым ключом, которые смогли бы эффективно функционировать на этих устройствах.

Целью данной статьи является исследование предлагаемых в открытой печати криптографических методов для последующего применения в мобильных устройствах с ограниченными возможностями.

Известно, что стойкость криптосистемы, основанной на функции с секретом, определяется сложностью получения обратной функции без знания секрета. Одной из таких обратных функций является задача дискретного логарифма в группе конечного порядка. Для решения задачи дискретного логарифма в конечных полях существует субэспоненциальный алгоритм, но для других групп такие алгоритмы еще не предложены [2 – 7].

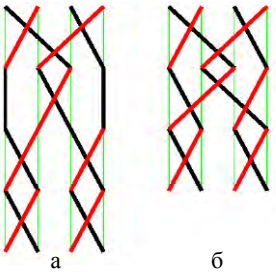
Криптосистема на группах кос. На конференции Crypto'2000 была предложена криптосистема на группах кос [2]. Она является частным случаем общей криптосистемы MOR, впервые предложенной в [3]. Ключевой задачей в криптосистеме на группах кос является задача эквивалентности. ***Задача эквивалентности*** – задача преобразования косы в группе кос к единственному представлению в канонической форме. Не существует алгоритма,

способного за полиномиальное время решить задачу эквивалентности [3].

N-косой называется множество неперекрывающихся n прядей, которые соединены с верхней и нижней горизонтальными плоскостями. Применим образующий элемент n, обозначенный как σ_n, к n-косе. Тогда концы ее нитей, принадлежащие нижней плоскости в позициях n и n + 1 чередуются слева направо. Соответственно σ_n^{-1} – тоже образующий элемент группы, причем нити чередуются справа налево. Каждая n-коса может быть представлена как код (образующих элементов, примененных один за другим) положительных и отрицательных образующих элементов. ***Индексом n-косы*** называется число нитей в косе. ***Единичная коса*** – коса, в которой каждая нить в соответствующей плоскости проходит по прямой к нижней плоскости. ***Фундаментальная коса*** – коса, где нить, начинающаяся в i-й позиции, заканчивается в позиции n – i + 1. Если фундаментальная коса положительна, то каждое пересечение – положительно, т.е. нить, проходящая слева направо, находится над нитью, проходящей справа налево. Аналогично формулируется понятие фундаментальной отрицательной косы и отрицательного пересечения. ***Группа n-кос*** B_n – множество n-кос. Каждая коса в группе может быть преобразована к произвольной косе группы с помощью генерирующих уравнений вида

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, \text{ если } |i-j|=1 \text{ и } \sigma_i\sigma_j = \sigma_j\sigma_i, \text{ если } |i-j|>1.$$

Две n-косы эквивалентны, если они находятся в одной и той же группе кос. Каждая группа кос B_n может быть представлена в канонической форме, которая является уникальной для каждой группы. Каноническая форма группы кос представляется фундаментальной косой и числом перестановок. Количество перестановок в канонической форме называется ***канонической длиной***. На рис. 1 приведена каноническая форма кос. Произведением ab двух кос является коса, полученная посредством размещения косы a поверх b [2].



а б

Рис. 1. Коса перед (а) и после (б) алгоритма эквивалентности

Пусть имеется три косы axa^{-1}. Преобразуем произведение к его каноническому виду. Факторизация произведения на исходные множители-косы является труднорешаемой задачей.

Все известные алгоритмы разложения на множители требуют экспоненциального времени решения. Применим аппарат кос для реализации ассиметричной криптосистемы. Криптосистема на косах обладает свойством коммутативности кос, построенных в левой группе LB_l (группе n-кос, образованной элементом, меньшим некоторого целого d) и правой группе RB_r (группе n-кос, образо-

ванной элементом, большим d).

Алгоритм генерации ключа: выбирается достаточно сложная (запутанная) $(l+r)$-коса $x \in B_{l+r}$; далее выбирается коса $a \in LB_l$; тогда имеем открытый ключ (x, y), где $y = axa^{-1}$, и личный ключ a.

Алгоритм зашифровывания: даны сообщение $m \in \{0,1\}^k$ и (x, y) – открытый ключ; выбирается случайная коса $b \in RB_r$; зашифрованный текст – (c, d), где $c = bxb^{-1}$; $d = H\left(byb^{-1}\right) \oplus m$; $H(x)$ – хеш-функция.

Алгоритм расшифровывания: дан зашифрованный текст (c, d) и личный ключ a; вычисляется $m = H\left(aca^{-1}\right) \oplus d$, где $H(x)$ – хеш-функция.

Заметим, что хеш-функция применяется к одной и той же косе в процедуре зашифровывания и расшифровывания благодаря свойству коммутативности операции умножения

$$aca^{-1} = a\left(bxb^{-1}\right)a^{-1} = b\left(axa^{-1}\right)b^{-1} = byb^{-1}.$$

Приведем некоторые характеристики криптосистемы: размер блока открытого текста $O(pq\log n)$ бит; размер зашифрованного текста $O(4pn\log n)$ бит; сложность процедуры зашифровывания $O\left(p^2 n\log n\right)$ элементарных операций; сложность процедуры расшифровывания $O\left(p^2 n\log n\right)$ элементарных операций; увеличение размера сообщения 4–1; длина личного ключа $O\left(\frac{1}{2}pn\log n\right)$ бит; длина открытого ключа $O(3pn\log n)$ бит; сложность атаки полным перебором $O\left(\exp\left(\frac{1}{2}pn\log n\right)\right)$.

Сравнение. В [1] приводятся результаты сравнения производительности систем шифрования с открытым ключом, которые обеспечивают аналогичную стойкость. Результаты сравнения приведены в табл. 1. Хотелось отметить, что криптосистемы MOR(Braid) и ECC тестировались на рабочей станции с CPU Intel Celeron 533 MHz, а RSA тестировалась на Intel Pentium II 400 MHz.

Таблица 1

Результаты сравнения реализаций криптосистем

Характеристика	RSA1024	ECC168	MOR(Braid)
Степень расширения сообщения	1 – 1	2 – 1	4 – 1
Размер блока текста, бит	1024	160	1088
Размер открытого ключа, бит	1024	169	1000
Время генерации ключа, мс	1432	65	8,5
Время зашифровывания, мс	4,28	140	29,8

Время расшифровывания, мс	48,5	67	14,9

Выводы. Сравнение результатов, приведенных в табл. 1, показывает, что криптосистема, основывающаяся на группе кос, по своей производительности превосходит известные и хорошо зарекомендовавшие себя криптосистемы RSA и ECC. Но в тоже время бросаются в глаза размеры открытого и личного ключей, которые превосходят размеры ключа криптосистемы ECC, принятой в качестве стандарта [4 – 7].

Применение криптосистемы на группе кос в приложениях с критическими требованиями к защите информации невозможно в связи с недостаточной ее изученностью. Дальнейшим направлением является изучение стойкости криптосистемы MOR, в частности, основанной на группе кос.

ЛИТЕРАТУРА

1. *P. Karu. Practical comparison of fast public-key cryptosystems. Available at: http://eprint.iacr.org.*
2. *Ki Hyong Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, Choonsik Park. New public-key cryptosystem using braid groups (accepted at Crypto'2000). Available at: http://eprint.iacr.org.*
3. *Seong-Hun Paeng, Daesung Kwon, Kil-Chan Ha, Jae Heon Kim. Improved public key cryptosystem using finite non Abelian groups. Available at: http://eprint.iacr.org.*
4. *IEEE P1363-2000. Standard Specifications for Public Key Cryptography.*
5. *ISO/IEC FCD 15946-4. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part2: Digital signatures.*
6. *ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи. – М.: Росстандарт.*
7. *ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.*

Поступила 1.04.2004

***НИЗИЕНКО Борис Иванович**, канд. техн. наук, доцент, начальник кафедры ХВУ. В 1980 году окончил ХАИ. Область научных интересов – построение автоматизированных систем управления*

***СТАСЕВА Яна Юрьевна**, научный сотрудник ХВУ. В 2002 году окончила ХНУРЭ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*

***КОВТУН Владислав Юрьевич**, адъюнкт кафедры ХВУ. В 2000 году окончил ХВУ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*