КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И ПРОТОКОЛЫ, ПОСТРОЕННЫЕ НА ПЛАТФОРМЕ НЕКОММУТАТИВНЫХ ГРУПП

Кайманова Е.А.
Оренбургский государственный университет

В настоящее время наиболее распространены криптосистемы и протоколы с открытым ключом. Данные алгоритмы и протоколы являются ассиметричными. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH. Также используется в PGP, S/MIME.

Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» Уитфилда Диффи и Мартина Хеллмана, опубликованной в 1976 году. Метод стал известен как обмен ключами Диффи - Хеллмана, был первым опубликованным практичным методом для установления разделения секретного ключа между заверенными пользователями канала. В 1977 году учёными Рональдом Ривестом, Ади Шамиром и Леонардом Адлеманом из Массачусетского технологического института был разработан алгоритм шифрования, основанный на проблеме о разложении на множители. Система была названа по первым буквам их фамилий (RSA — Rivest, Shamir, Adleman). RSA стал первым алгоритмом, пригодным и для шифрования, и для цифровой подписи [1] . Так же примерами ассиметричных алгоритмов и протоколов являются алгоритмы: DSA, EDSA, ГОСТ Р 34.10-2012, McEliece, схема Эль-Гамаля. Они основаны на теории чисел, следовательно, зависят от структуры абелевых групп. Развитие вычислительной техники сделало эти методы восприимчивыми к атакам, так же ожидание разработки квантового компьютера, для которого решение «трудных» задач станет возможным за полиномиальное время, привело к исследованиям некоммутативных групп, как основы для построения криптографических примитивов. Эта линия исследования получила название некоммутативная алгебраическая криптография. Основы некоммутативной криптографии изложены в монографии А. Мясникова, В. Шпильрайна и А. Ушакова.

Новые исследование так же связаны с использованием новых трудных задач, сложность которых была бы сверхполиномиальна и в случае применения квантового вычислителя.

Некоммутативная криптография предполагает исследование общих алгебраических приемов для построения криптосистем, изучение потенциальных алгебраических платформ (групп, колец) для реализации методов и схем, криптоанализ и анализ безопасности систем.

Для обоснования возможности использования группы рассматриваются следующие аспекты: группа должна быть хорошо изучена; должна существовать эффективно вычислимая нормальная форма для элементов группы, т.е.

проблема слов в группе должна быстро (за линейное или квадратичное время) решаться детерминированным алгоритмом; должен существовать способ сокрытия элементов группы такой, что было бы невозможно восстановить; группа должна быть группой суперполиномиального (т. е. экспоненциального) роста [2].

Среди первых попыток использования некоммутативных групп в криптографии были схемы Аншеля-Аншела-Голдфелда и Ко-Ли и др. Авторы примерно в одно и то же время предложили использовать некоммутативные группы как основы для криптосистем с открытыми ключами. Платформа для данных схем является группа кос Артина. Группа кос достаточно хорошо изучена, в них можно эффективно выполнять вычисления разного толка. В то же время существуют трудноразрешимые проблемы, дающие возможность построения стойких криптосистем.

Позже несколько других некоммутативных структур как группы Томпсона, полициклические группы, группы Григорчука и матричные группы были идентифицированы как потенциальные кандидаты на шифровальные заявления. Многие из них описаны в монографии А. Мясникова, В. Шпильрайна и А. Ушакова [5].

В основу криптосистемы кладется одна из сложных математических проблем. К основным «трудным » задачам, на основании которых построены криптографические протоколы и алгоритмы с открытым ключом на некоммутативных группах относятся: проблема равенства, проблема сопряжения, проблема факторизации и декомпозиции, проблема вхождения, проблема изоморфизма.

Для обеспечения достаточной стойкости алгоритмов и протоколов криптографии с открытым ключом требуется положить в основу вычислительно трудные задачи, для которых сложность решения имела бы сверхполиномиальную сложность как при решении на компьютерах обычного типа, так и при решении на квантовых компьютерах. В качестве базовой задачи была предложена задача нахождения сопрягающего элемента в некоммутативных группах кос и проблема одновременного поиска множества сопряжений.

Группы кос крайне эффективны при обеспечении трудоёмких вычислительных процессов. Благодаря этому, различными группами исследователей были предложены протоколы с преобразованием на данных группах. Криптография на группе кос позволяет реализовать два протокола обмена ключами: протокол Аншеля-Аншеля-Гольдфельда; протокол обмена ключами К. Н. Ко, аналогичный алгоритму Диффи-Хеллмана.

В протоколе Аншеля-Аншеля-Гольдфельда в качестве открытого ключа принимается два набора кос $\{p_1,\ldots,p_l\},\{q_1,\ldots,q_m\}$ где $p_i,q_j \in B_n$ для $1\le i\le l$ и $1\le j\le m$. Секретный ключ u, принадлежащий участнику обмена А, состоит

из *l* нитей. Аналогично секретный ключ *v*, принадлежащий участнику обмена B, состоит из m нитей. Обмен происходит следующим образом:

1. A генерирует косу $s = u(p_1, \ldots, p_l)$, и использует ее, чтобы сгенерировать сопряженные $q_1' = sq_1s^{-1}, \ldots q_m' = sq_ms^{-1}$; пересылает $q_1', \ldots q_m'$
2. B генерирует косу $r = v(q_1, \ldots, q_m)$, и использует ее, чтобы сгенерировать сопряженные $p_1' = rp_1r^{-1}, \ldots, p_l' = rp_lr^{-1}$; пересылает $p_1', \ldots p_l'$
3. A вычисляет $t_A = su(p_1', \ldots, p_l')^{-1}$.
4. B вычисляет $t_B = rv(q_1', \ldots, q_m')r^{-1}$.

Искомый ключ $t_A = t_B$

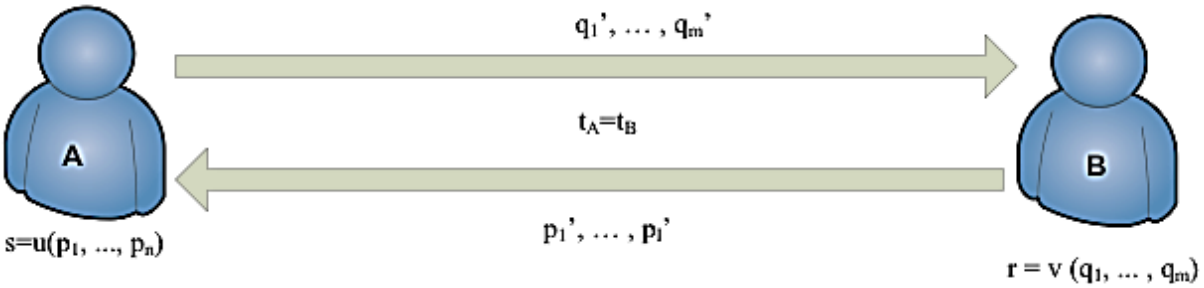

Рис. 1. Схема протокола Аншеля-Аншеля-Гольдфельда

Такая последовательность действий требует $2m + 2l + 2$ операций умножения и *m+l* операций нахождения обратных кос. Протокол основывается на проблеме одновременного поиска множества сопряжений.

Протокол, который предложен К.Н. Ко, базируется на протоколе Диффи-Хеллмана. Здесь, открытый ключ *p* это определённая коса в группе B_n. Секретный ключ, принадлежащий A, представляет собой косу *s* из подгруппы LB_n, а секретный ключ B — косу r из подгруппы RB_n. Обмен ключами происходит следующим образом:

1. A и B договариваются о выборе открытого ключа $p \in B_n$;
2. A генерирует сопряжение $p' = sps^{-1}$ пересылает его B;
3. B генерирует сопряжение $p'' = rpr^{-1}$ пересылает его A;
4. A вычисляет $t_A = sp''s^{-1}$;
5. B вычисляет $t_B = rp'r^{-1}$;

Искомый ключ $t_A = t_B$

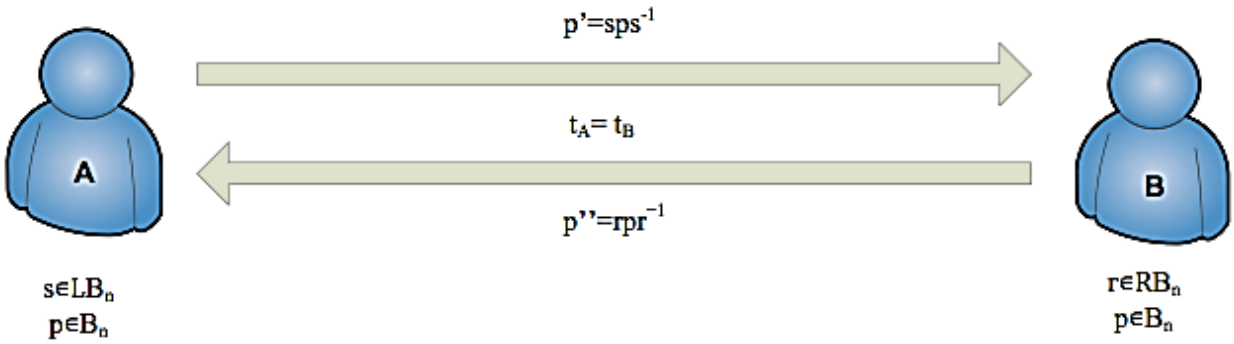

Рис.2. Схема протокола, предложенного К.Н.Ко

Такой протокол требует 8 операций умножения кос и 2 операции нахождения обратной косы. Протокол основывается на проблеме сопряжения кос.

К основным характеристикам криптографических систем, базирующихся на группе кос относятся:

Входящее сообщение, бит	$p \cdot l \cdot \log(n)$
Зашифрованное сообщение, бит	$4p \cdot n \cdot \log(n)$
Скорость зашифрования, операции	$O\left(p^{2n} \log(n)\right)$
Скорость расшифрования, операции	$O\left(p^{2n} \log(n)\right)$
Длина персонального ключа, бит	$\frac{1}{2} p \cdot n \cdot \log(n)$
Длина открытого ключа, бит	$3p \cdot n \cdot \log(n)$
Сложность атаки «грубая сила»	$\left(\left(\frac{n}{2}\right)!\right)^p = \exp\left(\frac{1}{2} p \cdot n \cdot \log(n)\right)$

где p - каноническая длина, n - индекс косы.

Таким образом, группы кос крайне эффективны при обеспечении трудоёмких вычислительных процессов. Представленные протоколы позволяют решить такие задачи информационной безопасности, как обеспечение конфиденциальности хранимой информации, обеспечение конфиденциальности передаваемой информации, обеспечение целостности хранимой информации, обеспечение целостности передаваемой информации, обеспечение подлинности информации; аутентификация пользователей, обеспечение анонимности пользователей и другие.

Рассмотренные криптографические системы показывают, что разработка алгоритмов, использующих группы кос является перспективным направлением в развитии современной криптографии.

Список литературы

1. *Глухов М. М. К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах. Матем. вопр. криптогр., 2010.*
2. *Молдовян Д.Н. Примитивы криптосистем с открытым ключом: конечные некоммутативные группы четырехмерных векторов. Журнал Информационно-управляющие системы, Выпуск№ 5 / 2010*
3. *Паршина Д. А., Митяева И. А., Горбенко И. Д. Анализ криптографических систем в группах КОС / Прикладная радиоэлектроника: наук. техн. журнал, 2012. – Том 11. № 2. — С. 210–215*
4. *Anshel I.,.Anshel M,.Goldfeld D, An Algebraic Method for Public Key Cryptography, Math.Res.Lett, 6, 1999, 287-291 Springer Verlag*
5. *Myasnikov A.G., Shpilrain V. and Ushakov A., Group-Based Cryptography Advanced Courses in Mathematics, CRM Barcelona, 2007*
6. *Cha J.C., Ko K.H., Lee S.J., Han J.W., Cheon J.H., An efficient implementation of braid groups, AsiaCrypt 2001, Springer Lect. Notes in Comput. Sci., 144–156.*