ВАРИАНТЫ СКРЫТОЙ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ ДЛЯ РАЗРАБОТКИ ПОСТКВАНТОВЫХ ПРОТОКОЛОВ ЦИФРОВОЙ ПОДПИСИ[1]

Молдовян Д. Н., с.н.с. НИЛ КБ и ПКС СПИИРАН, mdn.spectr@mail.ru

Молдовян А. А., г.н.с. НИЛ КБ и ПКС СПИИРАН, maa1305@yandex.ru

Абросимов И. К., м.н.с., НИЛ КБ и ПКС СПИИРАН, ivnabr@yandex.ru

А.И. Галанов, н.с., НИЛ КБ и ПКС СПИИРАН, daiver@cobra.ru

Аннотация

Рассмотрены варианты задания усиленной формы скрытой задачи дискретного логарифмирования в качестве базового примитива постквантовых протоколов электронной цифровой подписи. Стойкость предлагаемого примитива к квантовым атакам достигается за счет использования вспомогательного маскирующего преобразования элементов базовой циклической группы с помощью операций гомоморфного отображения и за счет того, что имеется возможность не предоставлять субъекту, проверяющему подлинность подписи, ни одного значения из базовой циклической группы. Процедура проверки подлинности подписи включает вычисления в двух различных циклических группах, отличных от базовой.

.

Введение

В связи с тем, что используемые в настоящее время алгоритмы электронной цифровой подписи (ЭЦП) не обеспечивают требуемого уровня стойкости при использовании атакующим квантового компьютера [1,2], криптографы проявляют значительный интерес к некоммутативным группам. Конечные некоммутативные группы расширяют возможности синтеза криптосхем с открытым ключом благодаря возможности задания над ними новых вычислительно трудных задач, среди которых можно указать 1) задачу поиска сопрягающего элемента [3,4] и 2) задачу

[1] Санкт-Петербургский институт информатики и автоматизации Российской Академии Наук. Работа выполнена при частичной финансовой поддержке РФФИ (проект № 18-07-00932-а).

дискретного логарифмирования в скрытой подгруппе [5]. С использованием первой из указанных двух задач разработаны двухключевые криптосхемы различных типов [6,7], однако на настоящий момент времени она представляется сравнительно мало изученной. Кроме того, по некоторым результатам [8] можно предположить, что могут быть найдены полиномиальные алгоритмы ее решения.

Для построения постквантовых криптосхем с открытым ключом более перспективным представляется применение скрытой задачи дискретного логарифмирования (СЗДЛ), которая формулируется в конечных некоммутативных ассоциативных алгебрах (КНАА), а именно следующим обобщенным способом. Выбирается некоторый элемент G, всевозможные степени которого порождают базовую циклическую группу Γ. Выбирается случайное натуральное число x и вычисляется элемент $Y'=G^x$. Затем выполняется автоморфное или гомоморфное отображение одного из элементов Y' и G или обоих этих элементов в элементы Y и Z соответственно, причем Y и Z принадлежат различным циклическим группам, содержащихся в КНАА. При этом конкретные параметры операции автоморфного и гомоморфного отображения являются неизвестными.

Впервые СЗДЛ была задана в конечной алгебре кватернионов с маскированием значения G^x путем выполнения над ним операции автоморфного отображения элементов алгебры. Эта форма СЗДЛ позволяет построить протокол открытого согласования ключей и алгоритмы открытого и коммутативного шифрования [9]. Сравнительно недавно предложены новые формы задания СЗДЛ, ориентированные на использование в качестве базового примитива схем ЭЦП [10,11].

В данной сообщении рассматриваются новые форма задания СЗДЛ, ориентированные на разработку на их основе схем ЭЦП, и различные типы их алгебраических носителей. Конкретная форма задания СЗДЛ характеризуется конкретным механизмом маскирования значений базовой циклической группы, задающей криптосхему.

Формы задания скрытой задачи дискретного логарифмирования

При использовании алгебраических носителей СЗДЛ, представляющих собой КНАА с глобальной двухсторонней единицей в качестве маскирующих операций могут быть использованы операции автоморфного отображения. Любой обратимый элемент Q алгебры задет

автоморфизм, выражаемый следующей формулой:

$$Y = Q^{-1} \circ X \circ Q,$$

где X пробегает все значения алгебры; $\circ$ - обозначает операцию умножения.

СЗДЛ состоит в нахождении x из уравнения

$$Y = D^{-1} \circ G^{x} \circ D.$$

В этом уравнении потенциальному злоумышленнику известны элементы открытого ключа $Z = Q^{-1} \circ G \circ Q$, $T = D^{-1} \circ Q$ и Y, а обратимые элементы Q и G, $G \circ Q \neq Q \circ G$ - неизвестны.

Множество необратимых элементов КНАА с глобальной двухсторонней единицей содержит большие множества элементов, действующих как локальные единицы в подмножествах необратимых элементов. В работах [11,12] приведены конкретные алгебры, для которых получены формулы описывающие правосторонние, левосторонние и двухсторонние локальные единицы, относящиеся к некоторому заданному необратимому элементу алгебры. В каждом из этих трех подмножеств имеются обратимые и необратимые векторы. Наличие единичных элементов различных типов позволяет задать СЗДЛ в нескольких различных формах, которые будут представлены в докладе. При этом общим является выбор генератора базовой циклической группы в виде необратимого вектора.

При задании СЗДЛ в КНАА с большим множеством глобальных односторонних единиц маскирование осуществляется с помощью операций гомоморфного отображения. В работах [10,11] описан ряд КНАА включающих большое множество глобальных односторонних (правосторонних или левосторонних) единиц. В таких алгебрах не содержится глобальной двухсторонней единицы, поэтому для элементов таких КНАА вводится понятие локальной обратимости. К элементам такого типа относят векторы, для которых существует локальная двухсторонняя единица. Последняя является единицей циклической группы, генерируемой элементом, к которому она относится.

Рассмотрим шестимерную КНАА, заданную над полем $GF(p)$ и содержащую p^2 глобальных левосторонних единиц L_k ($k = 0,1,..., p^2 - 1$), которая описана в работе [10] (для размерности 6 существуют алгебры

содержащие p^2, p^3 и p^4 глобальных односторонних единиц). Алгебры такого типа будем называть L -алгебрами, а КНАА содержащие множество глобальных правосторонних единиц – R -алгебрами. Выбор тройки векторов A, B и L_k, таких, что выполняется условие $A \circ B = L_k$, задает следующее гомоморфное отображение рассматриваемой алгебры:

$$\psi_{L_k,A}(X) = B \circ X \circ A,$$

где X пробегает все элементы алгебры.

Выбор некоторой глобальной левосторонней единицы L задает гомоморфное отображение φ_L другого типа:

$$\varphi_L(X) = X \circ L,$$

где X принимает все значения алгебры.

Каждая из двух операций гомоморфного отображения $\psi_{L_k,A}(G)$ и $\varphi_L(G)$, выполняемая над некоторым элементом G является взаимно коммутативными с операцией возведения в степень G^x. Благодаря последнему операции $\psi_{L_k,A}(G)$ и $\varphi_L(G)$ могут быть использованы как операции, маскирующие базовую циклическую группу при задании СЗДЛ, т. е. для задания новых форм СЗДЛ.

Заключение

В данной работе представлены новые формы задания СЗДЛ при использовании алгебраических носителей различных типов, которые ориентированы на разработку постквантовых схем ЭЦП. Варианты задания СЗДЛ описаны в виде, по которому для каждого из вариантов легко составить несколько различных схем постквантовых ЭЦП, используя в качестве прототипа хорошо известные схемы ЭЦП (например, схему Шнорра [13], стандарты ГОСТ Р 34.10-94, ГОСТ Р 34.10-2012 и ECDSA), основанные на вычислительной трудности ЗДЛ.

Литература

1. Shor P.W. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. SIAM Journal of Computing. 26:1484-1509
2. Yan S. Y. 2014. Quantum Attacks on Public-Key Cryptosystems . Springer US. 207 p

3. Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang J.S., Park C. New Public-Key Cryptosystems Using Braid Groups // Advances in Cryptology - Crypto 2000 / Lecture Notes in Computer Science. Springer-Verlag, 2000. Vol. 1880. P. 166-183
4. Lee E., Park J.H. Cryptanalysis of the Public Key Encryption Based on Braid Groups // Advances in Cryptology - Eurocrypt 2003 / Lecture Notes in Computer Science. Springer-Verlag, 2003. Vol. 2656. P. 477-489
5. Moldovyan D.N. Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. Vol. 18. P. 165-176
6. Chaturvedi A., Lal S. An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups. International Journal of Network Security. 2008. Vol. 6. No 2. P. 181-184.
7. Verma G.K. Probable Security Proof of a Blind Signature Scheme over Braid Groups. International Journal of Network Security. 2011. Vol. 12. No 2. P. 118-120.
8. Myasnikov A., Shpilrain V., Ushakov A. A Practical Attack on a Braid Group Based Cryptographic Protocol. Advances in Cryptology ? CRYPTO'05. Lecture Notes in Computer Science. Springer-Verlag, 2005. Vol. 3621. P. 86-96.
9. Moldovyan D.N., Moldovyan N.A. Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms. Quasigroups and Related Systems. 2010. Vol. 18. P. 177-186.
10. Moldovyan N. A., Moldovyan A. A. Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS). 2019. Vol. 12. No. 1. P. 66-81.
11. Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science Journal of Moldova. 2018. Vol. 26. No. 3(78). P. 301-313.
12. Молдовян Н.А., Абросимов И.К., Ковалева И.В. Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3. С. 3-13.
13. Schnorr C.P. Efficient signature generation by smart cards // Journal of Cryptology. 1991. Vol. 4. P. 161-174