СЕКЦІЯ 2.
Методи та засоби захисту інформації

Протокол обмена ключами шифрования на основе обобщенных матриц Галуа

Белецкий А. Я.[1]

[1]Проф., д.т.н., кафедра электроники, Национальный авиационный университет,
пр. Космонавта Комарова,1, Киев, Украина, abelnau@ukr.net

Аннотация — Рассмотрены методы построения матричных протоколов формирования секретных ключей шифрования легализованными абонентами открытых коммуникационных сетей. В основу протоколов положены алгоритмы ассиметричной криптографии. Решение проблемы предполагает вычисление односторонних функций и базируется на использовании обобщенных матриц Галуа, связанных отношением изоморфизма с образующими элементами, и зависящих от выбранных неприводимых полиномов, порождающих матрицы. Предлагается вариант организации алгебраической атаки на протоколы и обсуждаются варианты ослабления последствий атаки.

Ключевые слова: **протокол обмена ключами шифрования, односторонние функции, обобщенные матрицы Галуа, отношение изоморфизма, алгебраическая атака.**

Exchange Protocol Encryption Keys Based on Generalized Matrix Galois

Beletsky A. Ja.[1]

[1]Prof., Dr. Sc., Department of Electronics, National Aviation University,
pr. Kosmonavt Komarov, 1, Kiev, Ukraine, abelnau@ukr.net

***Abstract* — The methods of construction of matrix formation the secret protocols legalized subscribers of public communications networks encryption keys. The basis of the protocols laid asymmetric cryptography algorithms. The solution involves the calculation of one-way functions and is based on the use of generalized Galois arrays of isomorphism relationship with forming elements, and depending on the selected irreducible polynomial generating matrix. The variant of the organization of the algebraic attacks on protocols and discusses options for easing the consequences of attacks.**

Keywords: **exchange protocol encryption keys, one-way functions, generalized Galois matrix, isomorphism relation, algebraic attack.**

Введение

Одной из наиболее актуальных задач, решаемой современной криптографией, является формирование секретных ключей шифрования абонентами открытых коммуникационных сетей или иных открытых каналов передачи информации. Особую остроту приобретает данная проблема в системах управления беспилотными летательными аппаратами, поскольку несанкционированный доступ, например, в радиоканал приема-передачи командно-телеметрической информации сопряжен с риском потери аппарата или может привести к другим тяжким последствиям.

Для обмена зашифрованными сообщениями между двумя абонентами криптосистемы необходимо, чтобы обоим участникам обмена доставлялись сохраняемые в секрете ключи шифрования. Технология формирования секретных ключей по открытым каналам связи в случае, когда каждый из двух абонентов сети участвует в генерации этого секретного ключа, носит название *протокола обмена ключами* (ПрОК), являющегося частным случаем *протокола распределения ключей.* Вторым типом протокола предполагается не только выработка секретного ключа шифрования, но и его распределение между всеми абонентами (число которых может превышать два) некоторой легализованной группы сети.

Предметом исследования, излагаемого в данном докладе, являются исключительно протоколы первого типа, то есть протоколы обмена ключами.

Первым протоколом, заложившим основу *ассиметричной* (двухключевой) криптографии, и на ее основе – построения целой серии протоколов обмена ключами шифрования, является ставшим в настоящее время классическим *протокол Диффи-Хеллмана* [1] (DH-протокол или алгоритм), который позволяет двум сторонам, назовем их абонентами A и B, совместно создавать общий секретный ключ K, используя незащищенный канал связи. Этот ключ может быть применен для криптопреобразования последующих сообщений с помощью симметричного шифрования.

Главной недостаток DH-протокола заключается в том, что, во-первых, он не защищен от атаки «человек посередине» [2] и, во-вторых, требует для своего построения достаточно больших простых чисел p, генерация которых и проверка «на простоту» сопряжена, зачастую, со значительными ресурсными затратами. Поэтому были предложены и другие варианты протоколов обмена ключами, среди которых отметим так называемые *матричные аналоги* алгоритма Диффи-Хеллмана, а именно, алгоритмы Ероша-Скуратова [3], Мегрелишвили [4] и др. Хотя перечисленные протоколы также не защищены от атаки типа «человек посередине», но по сравнению с DH-протоколом гораздо проще в программно-аппаратной реализации.

Обмен секретными ключами шифрования решается, как правило, с помощью так называемых *односторонних* (*однонаправленных*) *функций*. В частности, стойкость асимметричного RSA криптографического шифра, популярном алгоритме, который часто используется для построения односторонних функций и протоколов обмена ключами, основывается на факторизации больших чисел и требует экпоненциального по числу знаков факторизуемого числа операций.

Основной недостаток RSA-протоколов, ограничивающий их применение в *системах обмена ключами шифрования*, состоит в их низком быстродействии, обусловленном необходимостью выполнения вычислений над двоичными операндами большой размерности, достигающих нескольких Кбит. В связи с вышеизложенным проблема разработки эффективных протоколов обмена ключами шифрования не снижает своей остроты и продолжает оставаться актуальной.

В докладе обсуждаются способы формирования односторонних функций, базирующийся на так называемых *обобщенных матрицах Галуа* (ОМГ), и предлагаются на их основе алгоритмы построения ОМГ-ПрОК, ориентированные на применение в системах оперативной смены ключей шифрования в каждом сеансе связи между наземным пунктом управления (НПУ) и бортовой аппаратурой БПЛА.

Обобщенные матрицы Галуа

Термин *матрицы Галуа*, как и биективно связанные с ними *матрицы Фибоначчи*, заимствованы из теории помехоустойчивого кодирования и криптографии, в которых широко применяются генераторы бинарных псевдослучайных последовательностей (ПСП) в конфигурациях Галуа и Фибоначчи, построенные на линейных регистрах сдвига (РС) с линейными обратными связями (ЛОС) [5]. Известно, что для того чтобы ЛРС являлся генератором ПСП максимального периода, соответствующий полином обратной связи должен быть *примитивным полиномом* (ПрП).

Каждый линейный РСЛОС-генератор ПСП максимального периода, может быть представлен эквивалентной ему примитивной матрицей Галуа, формирующей ту же самую бинарную $m-$ последовательность, что и генератор ПСП.

Обозначим через $\boldsymbol{G}_f^{(n)}$ двумерную матрицу Галуа $n-$го порядка над неприводимым полиномом (НП) f_n. С помощью $\boldsymbol{G}_f^{(n)}$ введем рекуррентное вычисление состояний $S(t)$ регистра в дискретные моменты времени t:

$$S(t) = S(t-1)\cdot \boldsymbol{G}_f^{(n)}, \quad t = 1, 2, \ldots \qquad (1)$$

В соответствии с (1) алгоритм синтеза классических матриц Галуа может быть сформулирован следующим образом. Пусть f_n – векторная форма примитивного полинома степени n такая, что $f_n = \{1, u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1\}$, $u_i \in \{0,1\}$, $i = \overline{1, n-1}$, и $\theta = 10-$ минимальный примитивный ОЭ поля $GF(2^n)$, порождаемого ПрП f_n. Поместим образующий элемент 10 справа в нижней строке матрицы Галуа и заполним элементы матрицы, придерживаясь простого правила. Поставим единицы в элементах диагонали, расположенной ниже главной диагонали матрицы, а в оставшихся элементах матрицы $\boldsymbol{G}_f^{(n)}$, кроме верхней строки, запишем нули. В верхней ($n-$й) строке матрицы Галуа следует ожидать появления $(n+1)-$битного вектора 100…0. Но это недопустимо, так как порядок матрицы равен n. Приведя $(n+1)-$битный вектор к остатку по модулю f_n, приходим к заключению, что в верхней строке матрицы $\boldsymbol{G}_f^{(n)}$ следует разместить ПрП f_n, исключая его старшую единицу, т.е. $n-$битный вектор $u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1$.

На основании предложенного *метода диагонального заполнения*, получим общую форму классической матрицы Галуа $n-$го порядка

$$\boldsymbol{G}_f^{(n)} = \begin{bmatrix} u_{n-1} & u_{n-2} & \cdots & u_2 & u_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}.$$

Введем определение обобщенной матрицы Галуа (ОМГ).

Обобщенными будем называть матрицы Галуа $\boldsymbol{G}_{f,\omega}^{(n)}$, *образующий элемент которых* ω *совсем не обязательно является примитивным элементом* θ *поля* $GF(2^n)$, *порождаемого произвольным неприводимым полиномом* f_n *степени* n.

Синтез обобщенных матриц Галуа $\boldsymbol{G}_{f,\omega}^{(n)}$ осуществляется введенным ранее методом диагонального заполнения и сводится к таким действиям. В нижней строке формируемой ОМГ записывается образующий ее элемент $\omega \geq 10$, поля $GF(2^n)$ над НП f_n. Разряды строки, расположенные слева от ω, заполняются нулями. Последующие строки матрицы (снизу-вверх) образуются сдвигом предыдущей строки на один разряд влево, а в освобождающийся правый разряд заносится 0. Если при сдвиге старший ненулевой разряд строки выходит за пределы матрицы, то векторы, отвечающие таким строкам, приводятся к остатку по модулю f_n и, тем самым, строка вновь становится n разрядной.

Из теории полиномов одной переменной x известно, что умножение произвольного полинома $\omega_k(x)$ степени k на x эквивалентно его сдвигу на один разряд влево и, соответственно, увеличению на 1 степени полинома. Другими словами,

$$x \cdot \omega_k(x) \to \omega_{k+1}(x). \qquad (2)$$

Воспользовавшись соотношением (2) и, принимая во внимание способ формирования ОМГ, запишем цепочку преобразований:

$$\boldsymbol{G}_{f,\omega}^{(n)} \Rightarrow \begin{pmatrix} x^{n-1}\cdot\omega \\ x^{n-2}\cdot\omega \\ \vdots \\ x\cdot\omega \\ 1 \end{pmatrix} \bmod f_n = \omega \cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \vdots \\ x \\ 1 \end{pmatrix} \bmod f_n. \qquad (3)$$

.

Элементами правого вектор-столбца в соотношении (3) являются мономы, которые, будучи представленными в двоичной форме, обращают вектор-столбец в единичную матрицу $\boldsymbol{E}$, что позволяет сформулировать следующее утверждение.

Утверждение. *Обобщенная матрица Галуа* $\boldsymbol{G}_{f,\omega}^{(n)}$ *порядка* n *над неприводимым полиномом* f_n *изоморфна ее образующему элементу* ω.

$$\boldsymbol{G}_{f,\omega}^{(n)} \leftrightarrow \omega. \qquad (4)$$

Множество ОМГ может быть расширено за счет введения *подобных матриц Галуа* ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$, определяемых соотношением

$${}^*\boldsymbol{G}_{f,\omega}^{(n)} = \boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega}^{(n)} \cdot \boldsymbol{P},$$

где $\boldsymbol{P}$ – матрица преобразования подобия.

В качестве $\boldsymbol{P}$ – матриц выбраны перестановочные матрицы n – го порядка, для которых $\boldsymbol{P}^{-1} = \boldsymbol{P}^T$.

В отличие от исходных ОМГ $\boldsymbol{G}_{f,\omega}^{(n)}$ матрицы ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$, оставаясь коммутативными, утрачивают свойство изоморфизма. Данная особенность подобных матриц Галуа как раз и обеспечивает возможность построения *односторонних функций*, используемых в предлагаемых протоколах обмена ключами абонентами открытых коммуникационных каналов передачи информации.

ОМГ-ПРОТОКОЛ ОБМЕНА КЛЮЧАМИ ШИФРОВАНИЯ

Введем неформальное определение односторонней функции [6].

Определение. *Функция* $f : X -> Y$ *называется односторонней (однонаправленной), если* $f(x)$ *может быть легко вычислена для каждого* $x \in X$, *тогда как почти для всех* $y \in Y$ *вычисление такого* $x \in X$, *что* $f(x) = y$ *(при условии, что хотя бы один такой* x *существует), является сложным*.

Ниже приведены краткие пояснения к предлагаемому ОМГ-протоколу обмена ключами в открытых коммуникационных сетях [7]. Протоколом предполагается формирование абонентами сети новой односторонней функции, посредством которой и вычисляется общий секретный ключ шифрования.

В качестве *открытых ключей* протокола приняты: вектор инициализации V, являющийся $n-$битным вектором; неприводимый двоичный полином f_n степени n и перестановочная матрица $\boldsymbol{P}$ $n-$го порядка. Каждый из абонентов сети A и B вырабатывает *секретные* $n-$*битные ключи* ω_α и ω_β соответственно. Общий секретный ключ K определяется в результате выполнения абонентами таких двух этапов вычислений:

Этап 1. Абонент A генерирует случайный вектор ω_α, находит сначала ОМГ $\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$, затем подобную матрицу ${}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$, вычисляет вектор $V_\alpha = V \cdot {}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$ и направляет его абоненту B.

Аналогичные операции осуществляет абонент B, определяя вектор $V_\beta = V \cdot {}^*\boldsymbol{G}_{f,\omega_\beta}^{(n)}$, который направляет абоненту A.

Векторы V_α и V_β как раз и являются теми односторонними функциями, которые построены на основе подобных ОМГ.

Этап 2. Абонент A умножает принятый от абонента B вектор V_β на свою секретную матрицу ${}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$, формируя ключ

$$K_\alpha = V_\beta \cdot {}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)} = V \cdot {}^*\boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot {}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)} =$$

$$= V \cdot (\boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot \boldsymbol{P}) \cdot (\boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot \boldsymbol{P}) =$$

$$= V \cdot (\boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot \boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot \boldsymbol{P}).$$

Точно такие же вычисления выполняет абонент B, извлекая вектор

$$K_\beta = V \cdot (\boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot \boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot \boldsymbol{P}).$$

Поскольку ОМГ $\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$ и $\boldsymbol{G}_{f,\omega_\beta}^{(n)}$ коммутативны, то оказывается, что $K_\alpha = K_\beta = K$ и, следовательно, оба абонента сети получают одинаковый секретный ключ шифрования K.

Если же вместо подобных матриц ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$ использовать обычные ОМГ $\boldsymbol{G}_{f,\omega}^{(n)}$, то в силу их изоморфизма (4) противник, перехватив векторы V_α и V_β, может вычислить секретные ключи ω_α и ω_β, так как в общем случае

$$V_\gamma = V \cdot \boldsymbol{G}_{f,\omega_\gamma}^{(n)} = V \cdot \omega_\gamma (\mathrm{mod}\, f_n),$$
$$\gamma = \alpha \text{ или } \beta.$$

Отметим, что предлагаемый ОМГ-протокол, как и классический протокол Диффи-Хеллмана, не только не защищен от атаки типа «человек посередине», но, как и матричные протоколы Ероша-Скуратова и Мегрелишвили, подвержен также *алгебраической атаке*, которая сводится к следующим операциям:

1) Вычисляются значения векторов

$$\boldsymbol{E}\bar{V}, \boldsymbol{A}\bar{V}, \boldsymbol{A}^2\bar{V}, \ldots, \boldsymbol{A}^{n-1}\bar{V},$$

где $\boldsymbol{E}$ – единичная матрица (или матрица $\boldsymbol{A}^0$); $\boldsymbol{A}$ – матрица, параметризируемая открытыми ключами протокола и $\bar{V}$ – вектор-столбец (вектор инициализации).

2) Определяются коэффициенты $x_0, \ldots, x_{n-1}$, $x_i \in \{0,1\}$, $i = \overline{0, n-1}$, такие, что

$$x_0\boldsymbol{E}\bar{V} + x_1\boldsymbol{A}\bar{V} + x_2\boldsymbol{A}^2\bar{V}, \ldots, + x_{n-1}\boldsymbol{A}^{n-1}\bar{V} = \bar{\alpha} \quad (5)$$

.

3) Вычисляется секретный ключ $\bar{K}$ по формуле

$$\bar{K} = x_0\boldsymbol{E}\bar{\beta} + x_1\boldsymbol{A}\bar{\beta} + x_2\boldsymbol{A}^2\bar{\beta}, \ldots, + x_{n-1}\boldsymbol{A}^{n-1}\bar{\beta} \quad (6)$$

.

Вектор-столбцы $\bar{\alpha}$ и $\bar{\beta}$ в системах матричных уравнений (5) и (6) представляют собою векторы, которыми обмениваются операторы A и B.

ВЫВОДЫ

Отметим, прежде всего, что по результатам исследования разработаны достаточно простые алгоритмы синтеза обобщенных матриц Галуа, которым присущи такие основные особенности.

Во-первых, ОМГ могут быть построены для произвольных неприводимых полиномов, тогда как классические матрицы Галуа определяются лишь над примитивными полиномами. Во-вторых, каждому ПрП отвечает единственная примитивная матрица Галуа, тогда как для каждого НП число примитивных ОМГ совпадает с числом примитивных элементов θ расширенного поля $GF(2^n)$, порождаемого выбранным неприводимым полиномом f_n.

Теоретическая возможность взлома противником ОМГ-протокола алгебраической атакой, которая осуществима лишь при условии априорной определенности относительно открытых ключей и успешного перехвата пакетов V_α и V_β, не создает принципиальных проблем применению его в *аппаратуре специального назначения*, например, для формирования ключей шифрования информации, передаваемой по радиоканалу НПУ – борт БПЛА.

В самом деле, если публичные ключи ОМГ-протокола сделать закрытыми, то тем самым противник будет лишен возможности несанкционированного доступа к каналам передачи данных. Причина такого ограничения заключается в следующем. Поскольку в условиях отсутствия информации относительно параметров открытых ключей, противник, перехватив пакеты V_α и V_β, которыми обмениваются легализованные абоненты A и B, оказывается не в состоянии вычислить их общий секретный ключ шифрования K и, следовательно, ОМГ-протокол становится не взламываемым.

ЛИТЕРАТУРА REFERENCES

[1] Diffie W., Hellman M.E. "New Directions in Cryptography", IEEE Transactions on Information Theory, v. IT-22, no. 6, November 1976, 644-654.

[2] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. / Б. Шнайер. — М.: «ТРИУМФ», 2003. – 816 с.

[3] Ерош И. Л. Адресная передача сообщений с использованием матриц над полем GF (2). / И. Л. Ерош, В. В. Скуратов. // Проблемы информационной безопасности. Компьютерные системы. 2004, №1. – С. 72-78.

[4] Megrelishvili R. Investigation of new matrix-key function for the public cryptosystems. / R. Megrelishvili, M. Chelidze, G. Besiashvili. The Third International Conference “Problems of cybernetics and Information”, Volume 1, September 6-8, Baku, Azerbaijan, Section N1, “Information and Communication Technologies”, 2010, pp. 75-78.

[5] Поточные шифры. Результаты зарубежной открытой криптологии. – М., 1997. / [Электронный ресурс]. – Режим дост.: http//www/ssl/stu/neva/ru/psw/crypto/potok/str_ciph.htm

[6] Однонаправленные функции. / [Электронный ресурс]. – Режим доступа: http:// crypto.pp.ua/2010/06/odnonapravlennyefunkcii/

[7] Белецкий А. Я. Протокол формирования секретных ключей шифрования абонентами открытых каналов связи на основе оюоющенных матриц Галуа. / А. Я. Белецкий. // Захист інформації, Том 17, № 3. – С. 190-195.