УДК 681.3

НЕКОТОРЫЕ ЭЛЕМЕНТЫ КОНЦЕПЦИИ АКТИВНОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОЙ КРИПТОГРАФИИ

А.Н. ЛАВРИНЕНКО
Н.И. ЧЕРВЯКОВ

Северо-Кавказский федеральный университет

e-mail: GreatAntonchik-r@yandex.ru, chervyakovni@yandex.ru

В статье проведен обзор основных положений концепции активной безопасности в современной криптографии. Представлены математические алгоритмы, реализующие основные положения концепции активной безопасности, затронуты вопросы применения концепции активной безопасности в криптосистемах на эллиптической кривой.

Ключевые слова: концепция активной безопасности, схема разделения секрета, пороговая криптосистема.

Используемые в настоящее время криптографические алгоритмы обеспечивают достаточно высокий уровень защиты передаваемых данных. Известные временные оценки скорости работы криптоаналитических алгоритмов взлома позволяют утверждать, что их использование на практике вероятным противником будет возможно только при условии обладания им достаточно серьезными вычислительными ресурсами.

Помимо непосредственного перехвата шифрованных сообщений и использования криптоаналитических алгоритмов взлома систем криптографической защиты информации (СКЗИ) на практике существует еще и опасность прямой утечки секретных ключей вследствие воздействия внутренних и внешних угроз (например, вредоносные действия обслуживающего персонала либо хакерские атаки).

Основные методы защиты от прямых угроз СКЗИ [1, 5]:

— периодическое обновление секретной информации;

— пространственное разделение секретной информации.

Для повышения уровня безопасности СКЗИ предлагается одновременно использовать и методы периодического обновления секретной информации и методы её пространственного разделения. Такое сочетание методов защиты от прямых угроз СКЗИ получило в науке название — *системы активной безопасности.*

Все математические преобразования, применяемые в методах активной безопасности могут быть обобщены для криптосистем, использующих эллиптическую кривую над F_p.

Периодическое обновление секретной информации является неотъемлемой частью безопасного функционирования любой криптосистемы, так как даже при самых изощренных способах защиты и самых современных криптографических алгоритмах не один секретный ключ не может просуществовать в тайне вечно.

При этом периодичность смены ключевой информации должна носить случайный характер и происходить максимально внезапно для гипотетического противника. Кроме того, проводя плановую либо внеплановую смену ключевой информации, необходимо позаботиться о должном уровне организации всех процессов *управления ключевой информацией* (безопасная генерация, хранение и распространение ключевой информации между пользователями системы).

При использовании методов периодического обновления секретной информации первая проблема, с которой мы сталкиваемся — это разработка криптографически стойких алгоритмов *генерации ключей*, обеспечивающих равновероятность выбора случайных значений по всему ключевому диапазону. Используемый *генератор псевдослучайной последовательности* должен обладать тем свойством, что созданная им последовательность статистически ничем не будет отличаться от абсолютно случайной последовательности и ее значения не будут предсказуемы.

Известны детерминированные и недетерминированные генераторы псевдослучайных чисел. В основу *детерминированных* генераторов положены арифметические рекуррентные соотношения, обладающие хорошими статистическими свойствами. Строго говоря, никакой детерминированный алгоритм не может генерировать полностью случайные числа, он может только аппроксимировать некоторые их свойства. Однако выбранный особым образом хороший детерминированный алгоритм может дать такой результат, что полученная с его помощью числовая последовательность будет проходить большинство тестов на случайность. Поэтому такие числа еще называют *псевдослучайными числами.* Недетерминированные генераторы используют в своей работе случайные физические процессы, например физические шумы в радиоэлектронной аппаратуре и т.п. Однако применяются такие генераторы случайных чисел крайне редко.

В работах [2,3] показана эффективность использования арифметических рекуррентных последовательностей с использованием точек эллиптической кривой. Среди методов данного класса можно рассмотреть датчик псевдослучайной последовательности, предложенный S.Hallgren в 1994г., использующий арифметическую прогрессию на E с начальным членом $P_0 \in E$ и разностью $G \in E$ в виде рекуррентного соотношения:

$$P_n = P_{n-1} + G = nG \oplus P_0,\ n = 1,2,3,\ldots, \quad (1)$$

Выходными значениями (1) могут быть либо точки P_n, либо только их абсциссы x_n, либо только их ординаты y_n.

Известны также генераторы псевдослучайных последовательностей, построенные на арифметической прогрессии *EC*-последовательности эллиптической кривой.

Последовательность $P_0, P_1, P_2, \ldots$ точек на $E(F_p)$, удовлетворяющих рекуррентному соотношению:

$$P_{n+k} = \sum_{i=0}^{n-1} c_i P_{i+k} + Q,\ k = 0,1,2,\ldots \quad (2)$$

называют EC – *последовательностью* порядка n, а $f(x) = x^n - \sum_{i=0}^{n-1} c_i x^i$ – характеристическим многочленом над Z_r, где $r = \#E(F_p)$.

Максимальный период последовательности (2) достигается при примитивном характеристическом многочлене $f(x)$.

Следующей важной задачей надежного управления ключевой информации является обеспечение её *безопасного хранения и распространения.* Для того чтобы на сервере ключи были надежно защищены, их хранение должно осуществляться в зашифрованном виде. Таким образом, мы приходим к понятию *многоуровневой иерархической концепции ключевой информации* или просто *иерархии ключей.*

В современной криптографии обычно выделяют *три уровня иерархии ключей* [4]:

1) Главные ключи (мастер-ключи)
2) Ключи шифрования ключей (ключи обмена между узлами сети).
3) Ключи шифрования данных (рабочие (сеансовые) ключи).

Самый верхний уровень иерархии занимают мастер-ключи. Они хранятся в открытом виде, но в специальной памяти и доступ к ним строго ограничен. Их назначение — шифрование нижележащих ключей обмена между узлами сети. В свою очередь ключи шифрования ключей, как следует из названия, используются для непосредственного шифрования рабочих ключей пользователей, с помощью которых устанавливаются сеансы связи. Таким образом, достигается максимальная безопасность хранения и распространения в зашифрованном виде ключевой информации. Механизмы распространения ключевой информации могут быть организованы как напрямую между конечными пользователями системы, так и с использованием доверенных корневых

центров сертификации. При этом центры сертификации обеспечивают перешифрование хранящейся у них ключевой информации, но в то же время любые проблемы, возникающие у центра сертификации, могут обернуться проблемами для всех пользователей системы, что также делает систему уязвимой.

Методы *пространственного разделения* ключевой информации основываются на том, что исходная ключевая информация может быть разделена между различными участниками криптосистемы таким образом, чтобы компрометация ключа была невозможной при компрометации определенной части секрета, хранящейся у отдельных пользователей. При этом для выполнения криптографических преобразований требуется восстановление секретного ключа, что возможно только при объединении секретов, хранящихся у отдельных пользователей системы.

Особое место среди схем пространственного разделения секрета занимают (n, k) – пороговые схемы разделения секрета. Чаще всего именно они применяются на практике для криптографической защиты секретных ключей.

(n, k) – *пороговая криптосистема* — схема разделения секрета, основанная на том обстоятельстве, что исходный секрет, разделенный между n пользователями системы, может быть раскрыт только определенной группой из k пользователей той же системы, при этом для любого меньшего числа пользователей секрет будет недоступен.

Идеи схем порогового разделения секрета были независимо предложены в 1979 году Ади Шамиром и Джорджем Блэкли. Кроме этого подобные процедуры исследовались Гусом Симмонсом.

Среди всех участников пороговой криптосистемы принято выделять *разрешенные группы* (то есть группы пользователей, которые, предварительно объединив хранящиеся у них части секрета, могут самостоятельно восстановить секрет) и *неразрешенные группы* (то есть те группы пользователей, внутри которых восстановление секрета самостоятельными усилиями невозможно по различным причинам).

В криптосистеме такого типа защита будет считаться взломанной, если пороговое количество k частей секретов в одной из разрешенных групп пользователей будет каким-либо способом раскрыто.

Существуют различные варианты схем разделения секрета. Рассмотрим некоторые из них [6, 8].

Схема Шамира (схема интерполяционных полиномов Лагранжа). Основная идея данной схемы разделения секрета заключается в том, что двух точек достаточно для задания прямой, трех точек — для задания параболы, четырёх точек — для кубической параболы, и так далее. Чтобы задать многочлен степени k-1 требуется k точек. Поэтому, чтобы секрет могли восстановить k человек, он должен быть спрятан в формулу соответствующего многочлена. Искомый многочлен, заданный над большим конечным полем размерности p, может быть представлен в виде:

$$F(x) = (a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + M) \bmod p, \qquad (3)$$

где M – разделяемый секрет $(p > M)$, a_k – коэффициенты многочлена, выбранные как некоторые случайные числа, которые можно будет забыть после разделения секрета. Частичные секреты для каждого из n пользователей системы $(n \geq k)$ вычисляются по формуле:

$$k_i = F(i) = (a_{k-1}i^{k-1} + a_{k-2}i^{k-2} + \ldots + a_1 i + M) \bmod p, \; i = \overline{1..n}. \qquad (4)$$

После разделения секрета каждый пользователь получает четыре значения: номер частичного секрета i и его значение k_i, размерность поля p, степень многочлена k-1.

Для восстановления секрета любые k пользователей, собравшись вместе, могут восстановить исходный многочлен (3) используя интерполяционные формулы Лагранжа

$$F(x) = (\sum_i l_i(x) y_i) \bmod p, \qquad (5)$$

где $l_i(x) = \left(\prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \right) \bmod p$, (x_i, y_i) – координаты точек многочлена.

Схема Блэкли (векторная схема разделения секрета). Основная идея данной схемы разделения секрета в целом аналогична схеме Шамира с той лишь разницей, что вместо многочлена используется уравнение плоскости в *k*–мерном пространстве.

Схемы, основанные на китайской теореме об остатках (схема Миньотта, схема Асмута–Блума). В схеме Асмута–Блума для разделения некоторого секрета *M* над большим простым полем размерности *p* $(p > M)$ между *n* пользователями выбираются *n* взаимно простых чисел d_i, таких что $\forall i : d_i > p$; $\forall i : d_i < d_{i+1}$; $\prod_{i=1}^{k} d_i > p * \prod_{i=n-k+2}^{n} di$. Далее выбирается случайное число *r*, такое что: $\sqrt[k]{M'} < d_i << \sqrt[k-1]{M'}$, $i = \overline{1..n}$, где $M' = M + rp$. Вычисляются доли

$$k_i = M' \bmod d_i . \tag{6}$$

Участникам раздаются тройки чисел $\{p, d_i, k_i\}$. Восстановление секрета производится с использованием китайской теоремы об остатках.

Схемы, основанные на решении систем уравнений (схема Карнина–Грина–Хеллмана). Для разделения секрета между *n* различными сторонами так, чтобы минимум *k* сторон могли его восстановить выбирается *n*+1 векторов $\vec{v_i}$ размерности *k*, так чтобы ранг любой матрицы, составленной из *k* данных векторов, был равен *k*. Вектор $\vec{v_0}$ известен всем участникам. Секретом является скалярное произведение $(\vec{u}, \vec{v_0})$, долями — скалярные произведения $(\vec{u}, \vec{v_i})$ и векторы $\vec{v_i}$. Для восстановления секрета по известным долям (и набору векторов) решается система из *k* уравнений для нахождения вектора $\vec{u}$.

Схема, основанная на эллиптической кривой. Пусть задана эллиптическая кривая *E* над конечным полем F_p. Используя операции с точками эллиптической кривой можно провести аналогию с математическим аппаратом нейронных сетей конечного кольца и его адаптацией для систем разделения секрета. Так, операция сложения точек $P(x,y) = P_1(x_1, y_1) + P_2(x_2, y_2)$ описывает суммирование на нейроне, а операция умножения точки на число $P(x,y) = k * P_1(x_1, y_1)$ — весовую операцию. На основе изложенного можно сформировать полином вида

$$S = P_0 + tP_1 + t^2 P_2 + \ldots + t^{k-1} P_{k-1}, \tag{7}$$

где $P_1, P_2, \ldots, P_{k-1}$ – случайные точки на эллиптической кривой, P_0 – общий секрет. Заменяя $t_{i,j} = w_{j,i}$ получаем матрицу весовых коэффициентов нейронной сети

$$W = \begin{pmatrix} w_{00} & w_{01} & \cdots & w_{0(k-1)} \\ w_{10} & w_{11} & & w_{1(k-1)} \\ \vdots & & \ddots & \vdots \\ w_{(n-1)0} & w_{(n-1)1} & \cdots & w_{(n-1)(k-1)} \end{pmatrix} = \begin{pmatrix} 1 & t_0^1 & \cdots & t_0^{k-1} \\ 1 & t_1^1 & & t_1^{k-1} \\ \vdots & & \ddots & \vdots \\ 1 & t_{n-1}^1 & \cdots & t_{n-1}^{k-1} \end{pmatrix}. \tag{8}$$

Частные секреты получаются подстановкой в (7) и (8) различных значений *t*, равных номеру абонента *i*. В общем виде получается выражение

$$S_i \,|_0^{n-1} = \sum_{i=0}^{k-1} P_i t_j^i = \sum_{i=0}^{k-1} P_i (x_i)_j , \tag{9}$$

где *n* – общее количество секретов на первом шаге, а *j* – номер секрета. Для восстановления секрета необходимо провести рекуррентный итерационный процесс. На первом шаге имеем

$$S_{1,j} \,|_0^{k-2} = S_j (x_1)_{j+1} - S_{j+1} (x_1)_j = \sum_{i=0}^{k-1} P_i ((x_i)_j (x_1)_{j+1} - (x_i)_{j+1} (x_1)_j) = \sum_{i=0}^{k-1} P_i (x_2)_j ,$$

где слагаемое при *i*=1 равно нулю. Путем аналогичных преобразований можно окончательно получить

$$R = S_{k-1,j} = S_{k-2,j} (x_{k-1})_{j+1} - S_{k-2,j+1} (x_{k-1})_j = P_0 x_k , \tag{10}$$

где значения R и x_k и есть восстановленный секрет.

Таким образом, были кратко рассмотрены основные положения концепции активной безопасности и приведены в общем виде соответствующие математические алгоритмы, помогающие реализовывать на практике данные положения. Наряду с традиционными алгоритмами были рассмотрены и алгоритмы, использующие точки эллиптической кривой.

На практике реализация концепции активной безопасности представляет собой прикладную задачу, затрагивающую довольно обширный пласт алгоритмов, лежащих в относительно самостоятельной области относительно самого механизма выполнения криптографических преобразований (кодирования, шифрования, дешифрования и декодирования информации). Тем не менее данные алгоритмы очень важны для безопасного функционирования любой криптосистемы.

Список литературы

1. Артюхов Ю.В. Анализ схем разделения секрета, использующих вероятностный и комбинаторный подход в реализации пороговых криптосистем, функционирующих в распределенных компьютерных системах. // Актуальные вопросы технических наук: материалы междунар. заоч. науч. конф. (г. Пермь, июль 2011 г.) / Под общ. ред. Г.Д. Ахметовой. – Пермь: Меркурий, 2011. – 80 с.

2. Бабенко М.Г. Методы и алгоритмы моделирования вычислительных структур на эллиптических кривых с параллелизмом машинных операций. // Диссертация на соискание ученой степени кандидата физико-математических наук. – Ставрополь, 2011. 198 с.

3. Бондарь В.В. Разработка аналитических методов исследования математических моделей активной безопасности в распределенных вычислительных системах. // Диссертация на соискание ученой степени кандидата физико-математических наук. Ставрополь, 2001. 314 с.

4. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие. – М.: Логос, 2001. – 264 с: ил.

5. Коблиц Н. Курс теории чисел и криптографии. – М.: Научное издательство ТВП, 2001. – 254 с.

6. Пьянов С.М. Сравнительный анализ стойкости некоторых классов схем разделения секрета // Магистерская диссертация по программе “Математическое и программное обеспечение защиты информации”, научный рук. к.ф.м.н., доц. Применко Э.А., М.: МГУ им.Ломоносова, 2013. – 67 с.

7. Червяков Н.И., Бабенко М.Г. Анализ пороговых криптосистем на эллиптической кривой. // Научные ведомости БелГУ. Серия: История. Политология. Экономика. Информатика. – Белгород: БелГУ, 2010, № 13 (84), выпуск 15/1. – с.175-179.

8. http://ru.wikipedia.org/wiki/Пороговая_схема

SOME ELEMENTS OF THE CONCEPT OF ACTIVE SAFETY IN MODERN CRYPTOGRAPHY

A.N. LAVRINENKO,
N.I. CHERVYAKOV

North-Caucasian Federal University

e-mail: GreatAntonchik-r@yandex.ru, chervyakovni@yandex.ru

The article deals with a review of the main provisions of the concept of active safety in modern cryptography. The mathematical algorithms that implement the basic provisions of the concept of active safety is presented, discussed the questions of the application of the concept of active safety with elliptic curve cryptosystems.

Keywords: the concept of active safety, the scheme of secret sharing, the threshold for a cryptosystem.