

Инженерно-криптографическая защита ключа формирования подписи

Шифрование и цифровая подпись выполняются с использованием конфиденциального ключа. Чтение/запись ключа или информации, вычислимым образом зависящей от ключа, приводит к появлению слабых электромагнитных сигналов, несущих информацию о ключе. Для вскрытия конфиденциальной информации нарушитель может использовать лабораторные возможности, то есть использовать специальную аппаратуру. Выделение сигналов из шума методом накопления приводит к тому, что после определенного числа обращений к ключу стойкость резко снижается. Для противостояния инженерно-криптографическим атакам обычно используются устройства физической защиты (генераторы шума) или ограничивается время жизни ключа.

Предлагаются два метода инженерно-криптографической защиты конфиденциального ключа формирования электронной цифровой подписи на примере ГОСТ Р34.10–2001. Методы основаны на наложении случайной маски на ключ после формирования очередной подписи и последующем снятии этой маски. При этом изменяется уравнение формирования подписи по сравнению с ГОСТ Р34.10–2001, но уравнение проверки подписи не меняется.

Методы позволяют практически исключить инженерно-криптографические ограничения на срок службы конфиденциального ключа, вызванные его многократным использованием.

Предлагаемые методы пригодны и для других протоколов подписи (Эль-Гамала, Шнора, DSS, ECDSS, ГОСТ Р34.10–94).

Rostovtsev A. G. (SPbSPU)

Technology-cryptographic protection of the digital signature key

Encryption and digital signature procedures use secret key. Reading/writing of information, computably dependent of the key, produces weak electromagnetic signals that give information on the key. Intruder may use special laboratory technique to obtain this information. If number of these signals is large enough, strength of cipher (signature scheme) becomes small with respect to initial strength estimation. To protect key against such attacks key lifetime is restricted.

Two methods for digital signature secret key protection are suggested for Russian digital signature standard GOST R34.10–2001. Methods are based on random masking the secret key. Equation for signature generation is modified with respect to original algorithm, but signature verification algorithm is not changing.

The methods in practice delete key lifetime restriction. Methods can be applied to many signature protocols, such as ElGamal, Schnorr, DSS, ECDSS, GOST R34.10–94.

1. Задача дискретного логарифмирования на эллиптической кривой

В основу безопасности российского стандарта электронной цифровой подписи ГОСТ Р 34.10–2001 на эллиптической кривой $E(\mathbb{F}_p)$ над простым конечным полем из p элементов и его американского аналога ECDSS положена задача дискретного логарифмирования на эллиптической кривой. Эллиптическая кривая $E(\mathbb{F}_p)$ в форме Вейерштрасса задается уравнением

$$y^2 \equiv x^3 + Ax + B \pmod{p}, \quad (1)$$

где кубический многочлен в правой части не имеет кратных корней в поле \mathbb{F}_p .

Точки (x, y) кривой образуют конечную аддитивную абелеву группу, порядок $\#E(\mathbb{F}_p)$ которой согласно теореме Хассе близок к p [10]:

$$\left| \#E(\mathbb{F}_p) - p - 1 \right| \leq 2\sqrt{p}.$$

По основной теореме об абелевых группах группа точек эллиптической кривой изоморфна прямой сумме циклических групп, порядки которых являются степенями простых чисел. Для эллиптических кривых этот результат можно уточнить: группа то-

чек либо циклическая, либо является прямой суммой циклических групп. Если группа точек не циклическая, то число точек на кривой должно быть не свободным от квадратов [7].

Задача дискретного логарифмирования формулируется следующим образом: для точки P , лежащей в циклической группе, образованной точкой Q , найти показатель l такой, что $P = lQ$. Для обеспечения максимальной безопасности задача дискретного логарифмирования должна быть максимально сложной. Отметим, что сложность дискретного логарифмирования в значительной степени зависит от параметров задачи (уравнения эллиптической кривой, порядка циклической группы и др.).

Для повышения сложности задачи дискретного логарифмирования порядок r циклической группы должен быть большим простым числом. Согласно ГОСТ Р 34.10–2001 число точек должно быть простым или иметь большой простой делитель длины не менее 254 бит, то есть число r должно быть короче числа p не более чем на 2 бита. Отсюда следует, что группа точек эллиптической кривой, допускаемой указанным стандартом, всегда циклическая или является прямой суммой циклической группы и группы порядка 2. Для противостояния специальным методам логарифмирования, основанных на вложении группы точек эллиптической кривой в мультипликативную $E(\mathbb{F}_p) \rightarrow \mathbb{F}_{p^k}^*$ или аддитивную группу поля с помощью спаривания Вейля [10], необходимо выполнение условий: $p^k \neq 1 \pmod{r}$ для $k = 1, \dots, 31$ и $p \neq r$.

В настоящее время наилучшими алгоритмами дискретного логарифмирования на эллиптической кривой являются алгоритм Полларда [9] и алгоритм встречи на случайном дереве [4]. Алгоритм Полларда обладает временной сложностью $O(\sqrt{r})$, емкостной сложностью $O(\log r)$ и не допускает распараллеливания. Алгоритм встречи на случайном дереве обладает временной и емкостной сложностью $O(\sqrt{r \log r})$, но зато допускает распараллеливание для произвольного числа параллельно работающих процессоров.

Если в правой части уравнения (1) многочлен задан неполным уравнением $f(x) = x^3 + Ax$ или $f(x) = x^3 + B$, то сложность логарифмирования может быть несколько снижена по сравнению с традиционной оценкой. Это обусловлено тем, что при переходе к алгебраическому замыканию поля \mathbb{F}_p эллиптическая кривая обладает автоморфизмами соответственно вида $(x, y) \rightarrow (-x, \sqrt{-1}y)$ или $(x, y) \rightarrow \left(\frac{-1 + \sqrt{-3}}{2}x, -y \right)$. Эти

автоморфизмы образуют мультипликативную группу порядка 4 в первом случае и порядка 6 во втором случае. В результате появляется возможность разбить задачу дискретного логарифмирования на две последовательные подзадачи: сначала вычислить логарифм для орбиты точек P, Q относительно группы автоморфизмов, а затем уточнить логарифм внутри орбиты. Это позволяет снизить сложность задачи логарифмирования на небольшую константу, не более чем в 2,5 раза.

Для вскрытия ключа подписи нарушитель может использовать математические, криптоаналитические, вычислительные, лабораторные и другие возможности, предусмотренные соответствующими нормативными документами. Оценка стойкости по отношению к атакам, обусловленным математическими, криптоаналитическими, вычислительными возможностями нарушителя, получается методами криптографического анализа. Оценка стойкости по отношению к атакам, обусловленным лабораторными возможностями нарушителя, получается методами инженерно-криптографического анализа.

2. Безопасность подписи с учетом лабораторных возможностей нарушителя

В основу протокола электронной цифровой подписи ГОСТ Р 34.10–2001 положен протокол Эль-Гамала [6]. Пусть m — подписываемое сообщение, h — хэш-функция по ГОСТ Р 34.11–94, $\{E(\mathbf{F}_p), Q, P\}$ — открытый ключ, число l , — секретный ключ, при этом $P = lQ$. Для формирования подписи выполняются следующие действия:

- 1) вычисляется хэш-функция $e \equiv h(m) \pmod{r}$, причем $e \neq 0$;
- 2) вырабатывается случайный показатель k , $0 < k < r$, и вычисляется точка $R = (x_R, y_R) = kQ$, причем $x_R \neq 0 \pmod{r}$;
- 3) вычисляется часть подписи¹

$$s \equiv (lx_R + ke) \pmod{r}, \quad (2)$$

причем $s \neq 0$.

Подписанное сообщение представляет собой тройку $(m, x_R \pmod{r}, s)$.

Для проверки подписи выполняются следующие действия:

- 1) проверяются условия $0 < x_R \pmod{r} < r$ и $0 < s < r$;
- 2) вычисляется $e \equiv h(m) \pmod{r}$ и если $e = 0$, то считается $e = 1$;
- 3) вычисляется точка $R' = (se^{-1} \pmod{r})Q - (x_R e^{-1} \pmod{r})Q$;
- 4) проверяется сравнение $x_{R'} \equiv x_R \pmod{r}$. Если сравнение выполняется, то подпись верна.

Предположим, что нарушитель, ставящий задачу вскрытия ключа, обладает лабораторными возможностями, то есть может использовать специализированную аппаратуру для выделения из шума сигналов, несущих информацию о ключе (СНИК).² Процесс обращения к ключу (или обработки информации с использованием ключа) в электронной аппаратуре сопровождается появлением слабых электромагнитных сигналов. Использование техники обработки сигналов может снизить стойкость устройства цифровой подписи, если число обращений к ключу достаточно велико, чтобы выделить сигналы из шума. В истории криптоанализа такие случаи отмечены ранее для вскрытия ключей шифровальной аппаратуры посольств нескольких государств, см., например, работу [2].

Для вскрытия ключа нарушитель может воспользоваться следующим алгоритмом. На этапе предвычислений он, используя штатную аппаратуру, для каждого возможного слова ключа находит соответствующий сигнал, выделяет его из шума и записывает в базу данных. Затем для неизвестного ключа он выделяет СНИК из шума, сравнивает их с сигналами из базы данных и получает приближение для неизвестного ключа. Истинный ключ уточняется перебором вблизи найденного приближения.

Конфиденциальный ключ используется при формировании подписи (уравнение (2)), а также при считывании его из памяти ключей, в этих случаях возникают и СНИК.

Несмотря на то, что эти сигналы намного меньше уровня шумов, их можно принять с использованием техники накопления, так как сигнал при каждой новой реализации один и тот же, а шум всегда разный. Это объясняется тем, что суммарная энергия сигнала пропорциональна числу одиночных сигналов, а суммарная энергия шума — квадратному корню из этого числа.

Для защиты от атак со стороны нарушителя, обладающего лабораторными возможностями, обычно используются технические или организационные меры защиты (в состав аппаратуры вводятся генераторы шума, увеличивается радиус охраняемой зоны или ограничивается время жизни ключа). Отметим, что экранирование аппаратуры, шумление каналов утечки СНИК и другие аналогичные меры защиты не решают про-

¹ В стандарте ECDSS m и s переставлены местами.

² Под информацией о ключе понимается информация, заданная вычислимой функцией ключа.

блему кардинально, а лишь только увеличивают допустимое число подписей. Эти меры вызывают удорожание аппаратуры электронной цифровой подписи, связаны с определенными неудобствами при эксплуатации, а также не всегда эффективны. Поэтому представляет интерес разработка алгоритмических методов защиты от нарушителя, обладающего лабораторными возможностями. Такие методы могут быть реализованы программно, не несут неудобств при эксплуатации и практически не удорожают аппаратуру. При этом алгебраические методы значительно эффективнее, чем экранирование, зашумление и т.п.

3. Алгоритмические методы защиты ключа цифровой подписи

Для вскрытия ключа l согласно уравнению (2) достаточно найти $lx_R \pmod{r}$. Предположим, что формирование подписи реализуется программно, нарушитель знает текст программы в машинных кодах и может оптимальным образом принимать необходимые сигналы. Если разрядность процессора равна 32 (16) битам, то наилучшим алгоритмом умножения по модулю p является алгоритм Монтгомери [8, 3], согласно которому вначале операнды переводятся в p -вычеты, затем p -вычеты умножаются «в столбик» и наконец выполняется циклический сдвиг. Сигналы, несущие информацию о данном слове ключа, возникают при записи слова ключа из памяти в регистр (аккумулятор) процессора, при умножении его на каждое из слов координаты x_R , при нахождении вычета по модулю r , при сложении со слагаемым ke . Таким образом, при однократном формировании подписи происходит 12 (20) обращений к каждому слову ключа.

Единственным алгоритмическим способом защиты является периодическое случайное изменение конфиденциального ключа, заключающееся в наложении маски на ключ и последующем снятии маски с подписи. Ниже рассматриваются два способа защиты ключа.

Первый способ наложения и снятия маски основан на использовании эндоморфизмов $\text{End}(\mathbb{Z}/r\mathbb{Z})$ модуля $\mathbb{Z}/r\mathbb{Z}$.

Лемма. Имеет место изоморфизм колец $\text{End}(\mathbb{Z}/r\mathbb{Z}) \cong \mathbb{Z}/r\mathbb{Z}$.

Доказательство. Согласно работе [1] эндоморфизмы модуля образуют кольцо. Эндоморфизмом является умножение элемента модуля на любой элемент кольца $\mathbb{Z}/r\mathbb{Z}$, поэтому $\text{End}(\mathbb{Z}/r\mathbb{Z}) \supseteq \mathbb{Z}/r\mathbb{Z}$. Покажем, что других эндоморфизмов нет. Пусть φ — эндоморфизм модуля $\mathbb{Z}/r\mathbb{Z}$. Тогда $\varphi(a + b) = \varphi(a) + \varphi(b)$. Поскольку $\mathbb{Z}/r\mathbb{Z}$ — поле, то либо $\varphi(a) = 0$, либо существует ненулевой элемент $c \in \mathbb{Z}/r\mathbb{Z}$, такой что $ca = \varphi(a)$. Поэтому $\text{End}(\mathbb{Z}/r\mathbb{Z}) \subseteq \mathbb{Z}/r\mathbb{Z}$ и, следовательно, $\text{End}(\mathbb{Z}/r\mathbb{Z})$ и $\mathbb{Z}/r\mathbb{Z}$ совпадают. Поскольку арифметика $\text{End}(\mathbb{Z}/r\mathbb{Z})$ и $\mathbb{Z}/r\mathbb{Z}$ тоже совпадает, выполняется требуемый изоморфизм колец. ■

Для защиты ключа эндоморфизмы модуля $\mathbb{Z}/r\mathbb{Z}$ должны быть случайными и периодически изменяться. На первой реализации электронной цифровой подписи вместо постоянного ключа l используется замаскированное значение $k_1^{-1}l$, где k_1 — случайное число, обратимое по модулю r . Преобразуем уравнение формирования подписи (2) с учетом наложения и снятия маски. Получим

$$s \equiv k_1(k_1^{-1}lx_R + e) \pmod{r}. \quad (3)$$

Для формирования первой подписи отправитель вырабатывает случайный показатель k_1 , полагает $u_1 = k_1$, вычисляет $u_1^{-1}l \pmod{r}$, вычисляет точку $R_1 = (x_R, y_R) = k_1Q$ и вычисляет подпись s согласно выражению (3). Поскольку показатель s не зависит от наложения и снятия маски, уравнение проверки подписи не меняется.

На второй процедуре формирования подписи уравнение создания подписи изменяется по сравнению с (3) и принимает вид:

$$s \equiv k_2 u_1 (k_2^{-1} (u_1^{-1} l) x_R + u_1^{-1} e) \pmod{r}, \quad u_2 \equiv u_1 k_2 \pmod{r}.$$

На последующих процедурах при $i = 3, 4, \dots$ уравнение формирования подписи преобразовывается по индукции:

$$s \equiv k_i u_{i-1} (k_i^{-1} (u_{i-1}^{-1} l) x_R + u_{i-1}^{-1} e) \pmod{r}, \quad u_i \equiv u_{i-1} k_i \pmod{r}. \quad (4)$$

Для формирования i -й подписи необходимо хранить текущее значение u_{i-1} и $u_{i-1}^{-1}l$ вместо ключа l . При этом конфиденциальный ключ l не используется ни на одной из процедур формирования подписи, начиная со второй. Таким образом, на каждой процедуре используется замаскированное значение конфиденциального ключа, причем маска u_i постоянно меняется. Поскольку параметры s, x_R не зависят от маски, процедура проверки подписи соответствует стандарту ГОСТ Р 34.10–2001.

Данный метод защиты ключа, очевидно, пригоден и в случае аппаратного или программно-аппаратного построения устройства формирования подписи.

Предложенный метод защиты ключа с минимальными изменениями может быть применен и к протоколам подписи Эль-Гамала, Шнорра, ECDSS, а также для произвольных групп, например, для мультипликативной группы простого поля (стандарты ГОСТ Р 34.10–94, DSS). Например, в протоколах Эль-Гамала и ECDSS уравнение (2) имеет вид $e \equiv (lx_R + ks) \pmod{r}$. Отсюда получаем

$$s \equiv (e - k^{-1}lx_R) \pmod{r}.$$

При этом выражение (4) примет вид

$$s \equiv (e - k_i^{-1} u_{i-1} ((u_{i-1}^{-1} l) x_R)) \pmod{r}, \quad u_i \equiv u_{i-1} k_i \pmod{r}.$$

Действие меры защиты, определяемой выражением (4) аналогично экранированию или зашумлению. Оценим ее эффективность. Предположим, что нарушитель создает базу данных из СНИК для известных слов ключа и хочет ускорить вскрытие ключа с помощью метода, рассмотренного в п. 2. Тогда он должен измерять случайные реализации сигналов, представляющие случайные числа u_i и $u_i^{-1}l$.

Защита ключа осуществляется двумя составляющими. Во-первых, независимое вскрытие слов ключа l становится затруднительным, так как каждое слово ключа зависит от всех слов чисел u_i и $u_i^{-1}l$, то есть ключ становится «единым и неделимым». Во-вторых, вместо одиночного числа l будет использоваться пара чисел u_i и $u_i^{-1}l$ того же размера, содержащая полную информацию о ключе, при этом суммарное число обращений к каждому из этих чисел — то же, что и число обращений к ключу при однократном формировании подписи согласно (2).

Вычисление ключа при использовании предложенного метода защиты требует определения всех битов u_i и $u_i^{-1}l$. Поскольку ошибка в одном бите любого из этих битов с вероятностью $\approx 0,5$ меняет любой бит ключа, для вскрытия ключа требуется правильный прием обоих слов, что практически невозможно, так как энергия шума значительно превышает энергию одиночного сигнала. Использование методов выделения сигнала из шума практически не повышает достоверность приближения для ключа по сравнению с одиночным сигналом. Это обусловлено тем, что накапливать отклики нужно для ключа l , а не для чисел u_i и $u_i^{-1}l$. Однако даже малые в хемминговом смысле ошиб-

ки при определении этих чисел приводят к случайным изменениям ключа. Действительно, если вместо чисел u_i и $u_i^{-1}l$ получены $v_1 = u_i + \Delta_1$ и $v_2 = u_i^{-1}l + \Delta_2$ соответственно, то их произведение даст приближение для ключа l :

$$l \equiv l(1 + u_i^{-1}\Delta_2) + v_1\Delta_2 \pmod{r}.$$

Предположим, что нарушитель знает хеммингов вес вероятной ошибки. По-видимому, наилучшим алгоритмом для вычисления l является перебор по всем Δ_1, Δ_2 и по всем весам, начиная с нулевого. Для $r \approx 2^{255}$ сложность перебора будет превышать оценку сложности алгоритма Полларда (2^{128}), если хеммингов вес вероятной ошибки Δ_1 и Δ_2 не превышает некоторого значения z . Найдем z из условия

$$2^{128} \leq \left(\sum_{i=0}^z \binom{256}{i} \right)^2.$$

Если задаться вероятностью P того, что сложность данной атаки будет меньше, чем сложность алгоритма Полларда, то можно определить допустимую погрешность приема одиночного бита сигналов $u_i, u_i^{-1}l$:

$$P = \sum_{i=0}^{11} \binom{256}{i} (0,5 + \delta)^{256-i} (0,5 - \delta)^i.$$

Численное решение этого уравнения для $P = 10^{-3}$ показывает, что $\delta \approx 0,403$. Следовательно, если вероятность правильного приема одного бита информации специализированным приемником нарушителя меньше, чем $0,5 + \delta = 0,903$, то нарушитель не может улучшить оценку сложности для алгоритма Полларда. На практике это условие обычно выполняется, поэтому данный метод защиты ключа подписи практически исключает атаки, обусловленные лабораторными возможностями нарушителя.

Второй метод основан на том, что ключ l при выполнении арифметических операций сложения и умножения практически представлен полиномом, причем аналогом переменной является разрядность b процессора: $l = \sum_{i=0}^n l_i b^i$. Обычно l_i лежат в диапазоне

$0 \leq l_i \leq b - 1$. Однако можно использовать и другие представления, например:

- система абсолютно наименьших вычетов, $-b/2 < l_i < b/2$;
- система отрицательных вычетов $-b + 1 < l_i \leq 0$;
- знаковое троичное окно, при котором цепочка, содержащая несколько идущих подряд единиц, например $\underbrace{11\dots1}_{k \text{ единиц}}$, заменяется на число $\underbrace{1000\dots0}_{k-1 \text{ нулей}} - 1$;
- вместо показателя l можно использовать показатель $l \pm r$;
- при выполнении операций умножения, вызывающих наибольшее число обращений к ключу, слова ключа использовать в случайном порядке;
- если эллиптическая кривая допускает комплексное умножение на элемент мнимого квадратичного порядка O_D , то показатель l можно представлять не как элемент $\mathbb{Z}/r\mathbb{Z}$, а как элемент кольца классов вычетов кольца O_D по максимальному идеалу, образованному простым делителем числа r в O_D .

Если вычисления проводятся в одном и том же кольце, то каждый из коэффициентов l_i для очередной подписи может случайным образом иметь то или иное представление независимо от остальных коэффициентов. Если нарушитель не знает, какое именно представление используется, он не сможет использовать методы обработки

сигналов, следовательно, атака с использованием лабораторных возможностей становится практически невозможной.

Случайные числа, используемые для защиты ключа, могут вырабатываться с использованием алгоритмического генератора случайных чисел на эллиптической кривой [5]. Поскольку задача дискретного логарифмирования на эллиптической кривой сводится к задаче обращения такого генератора, этот генератор случайных чисел является наилучшим для подписи на эллиптических кривых.

Предложенные методы защиты могут использоваться и для защиты конфиденциального ключа расшифрования для алгоритма Эль-Гамала шифрования с открытым ключом.

Библиографический список

1. **Ван дер Варден Б. Л.** Алгебра. — М.: Наука, 1979.
2. **Павлов В.Г.** «Сезам, откройся!». Тайные разведывательные операции: из воспоминаний ветерана внешней разведки. — М.: Терра, 1999.
3. **Ростовцев А. Г.** Алгебраические основы криптографии. — СПб.: Мир и Семья, Интерлайн, 2000.
4. **Ростовцев А. Г., Маховенко Е. Б.** Введение в криптографию с открытым ключом. — СПб.: Мир и Семья, Интерлайн, 2001.
5. **Ростовцев А. Г., Маховенко Е. Б.** Подпись и шифрование на эллиптической кривой: анализ безопасности и безопасная реализация // Проблемы информационной безопасности. Компьютерные системы, СПб., 2003. № 1. С. 64–73.
6. **ElGamal T.** A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory, v. IT-31, 1985, pp. 469–472.
7. **Koblitz N.** A Course in Number Theory and Cryptography. — Springer-Verlag, 1987.
8. **Montgomery P. L.** Modular multiplication without trial division // Mathematics of Computation, v. 44, № 170, April 1985, pp. 519–521.
9. **Pollard J.** Monte Carlo methods for index computation (mod p) // Mathematics of Computation, v. 32, 1978, pp. 918–924.
10. **Silverman J. H.** The arithmetic of elliptic curves. — Springer-Verlag, 1986.