Московский Государственный Университет им. М. В. Ломоносова
факультет Вычислительной Математики и Кибернетики
кафедра Математической Кибернетики

Дипломная работа

Сравнительный анализ двух семейств схем электронной подписи

Масюка Дмитрия Викторовича

Москва, 2009 г.

Содержание

1 Введение

В настоящее время одним из наиболее широко применяемых криптографических примитивов являются схемы электронной цифровой подписи (ЭЦП). Данные схемы позволяют любому пользователю осуществлять йодписьёсообщений, которые впоследствии могут быть проверены любым другим пользователем. Точнее, любой пользователь схемы может сгенерировать секретный и открытый ключ таким образом, что лишь он сможет сгенерировать подпись (используя секретный ключ), при этом любой другой пользователь сможет ее проверить, используя открытый ключ подписывающего. При успешной проверке проверяющий может быть уверен в аутентичности подписи (т.е. в том, что подпись сгенерирована именно тем участником, открытый ключ которого используется для проверки) и целостности подписанного сообщения (т.е. в том, что подпись сгенерирована именно для того сообщения, которое было передано).

Схемы ЭЦП также обладают уникальным свойством асимметричности, заключающемся в использовании для формирования подписи секретного ключа, известного лишь одному участнику схемы. Данное свойство дает возможность для проведения эффективного арбитража, т.е. механизма разрешения споров об авторстве подписанного документа.

Таким образом, схемы ЭЦП позволяют решать следующие фундаментальные задачи криптографии:

- целостность
- аутентификация
- невозможность отказа от авторства

Как и всякая криптографическая схема, ЭЦП подвержена угрозам взлома. Последний может заключаться в

- полном раскрытии: взломщик может или вычислить секретный ключ интересующего его пользователя, либо имеет эффективный алгоритм, эквивалентный алгоритму подписи);
- выборочной подделке: взломщик может подделать подпись заданного множества сообщений;
- экзистенциональной подделке: взломщик может подделать подпись некоторого выбранного им сообщения;

К настоящему моменту существуют доказуемо-стойкие схемы ЭЦП на основе односторонних перестановок ([5]) и произвольной односторонней функции ([6]), однако они не могут быть практически использованы. Также существуют доказательства стойкости используемых на практике схем,

однако все они получены в далеких от реальности математических моделях.

Таким образом, встает задача проверки стойкости используемых на практике схем, а также создания новых доказуемо-стойких схем, использование которых будет возможно на практике.

В работе [1] доказывается стойкость модифицированной (реализуемой на практике) версии ГОСТ 34.10 в условиях двух стандартных предположений математической криптографии (о стойкости симметричного шифратора и хэш-функции) и гипотезе, выполнение которой оказывается также и необходимым условием для стойкости схемы. Данная гипотеза состоит в предположении о вычислительной сложности решения задачи о нахождении т.н. дискретного полулогарифма (ДПЛ). Под ДПЛ элемента y (открытого ключа пользователя) понимается подпись участника, имеющего своим открытым ключом y, сообщения с хэш-значением, равным 1. В [2] показано, что сложность данной задачи является необходимым условием для стойкости DSA, стандарта ЭЦП правительства США.

Таким образом, трудность решения задачи о нахождении подписи сообщения с единичным хэш-значением оказывается необходимым условием для стойкости двух широко используемых схем ЭЦП.

Именно эта задача и рассматривается в работе.

2 Основные понятия

Схема ЭЦП - схема электронной цифровой подписи. По [4], ЭЦП состоит из трех алгоритмов:

1. алгоритм генерации ключей G. Полиномиальный, в общем случае вероятностный алгоритм. На вход алгоритма подается параметр безопасности 1^q. Алгоритм генерирует пару (x, y), где x - секретный ключ, y - соответствующий ему открытый ключ.

2. алгоритм подписи σ. Полиномиальный, в общем случае вероятностный алгоритм. На вход алгоритма подается сообщение m и секретный ключ x. Алгоритм генерирует строку s, называемую *подписью сообщения*.

3. алгоритм проверки подписи V. Полиномиальный, в общем случае вероятностный алгоритм. На вход алгоритма подается открытый ключ y, подпись сообщения s и сообщение m. Алгоритм возвращает 1 или 0, что означает успешность или неуспешность проверки подписи, соответственно. От данного алгоритма требуется успешная проверка корректным образом сгенерированной подписи сообщения.

В большинстве используемых на практике схем используются детерминированные алгоритмы генерации и проверки подписи. Также обычно подписываются образы сообщений, вычисляемые хэш-функциями.

ПВМТ - полиномиальная вероятностная машина Тьюринга

ДПЛ(y) - дискретный полулогарифм y. Рассматривается относительно конкретной схемы ЭЦП и определяемый как подпись участника с открытым ключом y хэш-значения, равного единице. С точки зрения определения схемы подписи достаточным условием корректности подписи является успешное выполнение алгоритма проверки подписи. В терминах используемых на практике схем это означает выполнение уравнения проверки с хэш-значением, равным единице. Именно такое уравнение мы и будем рассматривать в качестве уравнения ДПЛ.

ДЛ(y) - дискретный логарифм элемента y. В группе $G = \langle g \rangle$ ДЛ(y) - это число $x \in N_0 : \ g^x = y$ (элемент некоторой группы)

ЭК - эллиптическая кривая. Точки эллиптической кривой над числовым полем образуют аддитивную группу, удобную для использования в криптографии из-за компактности описания точек и сложности решения задачи дискретного логарифмирования в группе

3 Постановка задачи

Основная задача работы состояла в исследовании задачи ДПЛ в семействе схем подписи типа Эль-Гамаль. Требовалось построить стойкую схему ЭЦП, в которой задача ДПЛ была бы трудноразрешимой.

4 Основная часть

4.1 Задача дискретного полулогарифма в семействе схем подписи Эль-Гамаль

Будем рассматривать обобщенное семейство схем подписи Эль-Гамаль (по [2]). Семейство схем параметризуется перестановкой вектора (u, v, w) и задается следующим образом:

4.1.1 Описание семейства

- q - простое число - порядок группы $G = \langle g \rangle$
- хэш-функция $H : \{0,1\}^* \to \{0,\ ...,\ q-1\} = Q$. Значения хэш-функции будем обозначать через h
- $f, F : G \to Q$ - отображения, используемые для формирования подписи и передачи элементов группы
- $x \in_R Q;\ y = g^x$ - секретный и открытый ключи подписывающего;
- $k \in_R Q;\ r = g^k$ - секретный и открытый сеансовые ключи;
- $(F(r), s)$ - подпись сообщения, s получается из уравнения $u = vx + wk\ (mod\ q)$, (u, v, w) - одна из перестановок $(s, f(r), h)$
- $(g^u\ y^{-v})^{w^{-1}(mod\ q)} = r$ - уравнение верификации подписи

Опишем конкретные варианты схем семейства. Укажем также уравнение задачи ДПЛ (относительно неизвестных r и s), т.е. уравнение верификации подписи при $h = 1$

Вариант 1 (схема ГОСТ)

1. $(u, v, w) = (s, f(r), h)$
2. $s = f(r)x + kh$ - подпись; $(g^s\ y^{-f(r)})^{h^{-1}} = r$ - верификация
3. $g^s\ y^{-f(r)} = r$ - уравнение ДПЛ

Вариант 2

1. $(u, v, w) = (s, h, f(r))$
2. $s = hx + f(r)k$ - подпись; $(g^s\ y^{-h})^{f(r)^{-1}} = r$ - верификация
3. $(g^s\ y^{-1})^{-f(r)^{-1}} = r$ - уравнение ДПЛ

Вариант 3

1. $(u, v, w) = (f(r), s, h)$
2. $s = x^{-1}(f(r) - kh)$ - подпись; $(g^{f(r)}\ y^{-s})^{h^{-1}} = r$ - верификация
3. $g^{f(r)}\ y^{-s} = r$ - уравнение ДПЛ

Вариант 4 (схема DSA)

1. $(u, v, w) = (f(r), h, s)$
2. $s = k^{-1}(f(r) - hx)$ - подпись; $(g^{f(r)}\ y^{-h})^{s^{-1}} = r$ - верификация
3. $(g^{f(r)}\ y^{-1})^{s^{-1}} = r$ - уравнение ДПЛ

Вариант 5

1. $(u, v, w) = (h, f(r), s)$
2. $s = k^{-1}(h - f(r)x)$ - подпись; $(g^{h}\ y^{-f(r)})^{s^{-1}} = r$ - верификация
3. $(g\ y^{-f(r)})^{s^{-1}} = r$ - уравнение ДПЛ

Вариант 6

1. $(u, v, w) = (h, s, f(r))$
2. $s = x^{-1}(h - f(r)k)$ - подпись; $(g^{h}\ y^{-s})^{f(r)^{-1}} = r$ - верификация
3. $(g\ y^{-s})^{f(r)^{-1}} = r$ - уравнение ДПЛ

4.1.2 Анализ задачи ДПЛ в описанном семействе

Утверждение. Отсутствие эффективного алгоритма решения задачи ДПЛ в схемах 1-4 является необходимым условием для стойкости этих схем.

Наличие эффективного алгоритма решения задачи ДПЛ позволяет подделывать подпись любого сообщения для участника с заданным ключом y. Чтобы осуществить подделку подписи сообщения с хэшем h участника с ключом y, следует решить задачу ДПЛ для $y' = y'(y, h)$, найдя таким образом подпись (F(r), s) сообщения с единичным хэшем участника с ключом y'. Необходимые замены:

1. Вариант 1. $y' = y^{h^{-1}}$, Если ДПЛ$(y') = (F(r), s)$, искомая подпись определяется как $F(r), sh)$
2. Вариант 2. $y' = y^{-h}$, Искомая подпись совпадает с ДПЛ$(y') = (F(r), s)$
3. Вариант 3. $y' = y^{h^{-1}}$, Если ДПЛ$(y') = (F(r), s)$, искомая подпись определяется как $F(r), sh)$
4. Вариант 4. $y' = y^{-h}$, Искомая подпись совпадает с ДПЛ$(y') = (F(r), s)$

Для схем 5 и 6 алгоритм, решающий задачу ДПЛ, по-видимому, дает лишь непосредственно подпись сообщения с единичным хэш-значением, однако подделать подпись другого сообщения через замену открытого ключа y не позволяет. Хэш-значение в уравнении верификации подписи появляется в множителе g^h. Любая замена y с добавлением мультипликативной константы вида $c_1 g^{c_3 h}$ в уравнении верификации будет возведена в неизвестную заранее степень $-f(r)$ или $-s$ (вариант 5 и 6, соответственно). Т.е. такая замена не позволит найти подпись для сообщения с заданным хэшем h (являясь, по-видимому, единственным эффективным средством для подделки подписи через решение задачи ДПЛ).

Утверждение. Описанное семейство схем распадается на три класса, в рамках которых задачи ДПЛ сводятся друг к другу при выполнении описанного ниже условия на преобразование $f(r)$.

Можно увидеть, что с точностью до преобразования $f(r)$ задачи ДПЛ в парах схем $(1)-(2), (3)-(6)$ и $(4)-(5)$ оказываются взаимно-сводимыми. Точнее, если $f_i(r) = f_j^{-1}(r)\ (mod\ q)$, т.е. в указанных парах преобразования $f(r)$ взаимно-обратны по модулю q, то решение задачи ДПЛ в одной схеме из пары позволяет получить решение задачи в другой схеме через замену $s_i = s_j f_i(r)$

Вопрос о вычислительной сложности решения задачи ДПЛ является, по-видимому, достаточно трудным. При этом, как видно, для реально используемых схем задача дает необходимое условие стойкости.

Ниже предлагается схема ЭЦП, в которой задачи ДПЛ(y) и дискретного логарифмирования y являются взаимо-сводимыми за линейное время.

4.2 Описание схемы ЭЦП со взаимно-сводимыми задачами ДПЛ и ДЛ

Исходные параметры схемы

q - простое число

G - группа, $\#G = q,\ G = \langle g \rangle$, например, группа точек ЭК

$f : G \to \{0, \ldots, q-1\}$. - отображение, необходимое для использования элементов группы в генерации подписи. Если G - группа точек ЭК порядка q, в качестве f можно взять $f(g) = x_g\ (mod\ q)$, т.е. первую координату точки по модулю порядка группы

$F : G \to \{0, \ldots, q-1\}$ - известное всем участникам эффективно-обратимое взаимно-однозначное отображение элементов группы в числа, используемое для передачи подписи

Алгоритм генерации подписи

1. $h = H(m)$ - хэш подписываемого сообщения

2. $x \in_R \{0, \ldots, q-1\}$ - секретный ключ пользователя
3. $k \in_R \{0, \ldots, q-1\}, f(g^k) \neq 0$
4. $y = g^x$ - открытый ключ пользователя
5. $r = g^k$ - открытый сеансовый ключ
6. $s = f(r)x - k(h-1) \ (mod\ q)$
7. $(F(r), s)$ - подпись сообщения (отображение F используется для передачи r - элемента группы).

Алгоритм верификации подписи

Проверяющая сторона имеет $(g, h, y, r = F^{-1}(F(r)), s)$.
Верификация подписи состоит в проверке выполнения равенства

$$r^{h-1} g^s y^{-f(r)} = e,$$

где e - единичный элемент группы G

Корректность схемы

Схема корректна в том смысле, что уравнение проверки будет выполняться для корректно созданной подписи, т.е. $s = f(r)x - k(h-1) \ (mod\ q)$:

$$r^{h-1} g^s y^{-f(r)} = g^{k(h-1)} g^{f(r)x - k(h-1)} g^{-f(r)x} = g^0 = e$$

Задача ДПЛ в описанной схеме

Опишем задачу получения ДПЛ. Для участника с открытым ключом y дискретным полулогарифмом будет являться подпись сообщения с единичным хэшем, т.е. пара $(r, s) : g^s y^{-f(r)} = e$.

Утверждение. В описанной схеме задачи ДПЛ и ДЛ являются взаимносводимыми за линейное время.

Приведенное уравнение ДПЛ эквивалентно $g^s = y^{-f(r)}$.

Предположим, есть алгоритм, эффективно решающий задачу ДЛ, т.е. по $y \in G = \langle g \rangle$ искать $x : y = g^x$. Тогда, приняв $-f(r) = 1$, можем найти ДПЛ(y) как $(-1, (y))$.

Обратно, если имеется алгоритм, решающий задачу ДПЛ$(y) = (F(r), s)$, то дискретным логарифмом элемента y будет являться число $f(r)^{-1} s \ (mod\ q)$. $f(r)$ будет обратимо вследствие простоты порядка группы q.

4.3 Стойкость предлагаемой схемы

Покажем, что стойкость описанной схемы в модели со случайным оракулом не ниже стойкости схемы подписи ГОСТ. Опишем модель.

Оракул O - ПВМТ, работающая следующим образом. Получая на вход сообщение m, машина проверяет, получала ли она его прежде, просматривая содержимое ленты. Если сообщение поступает впервые, машина генерирует случайное число из множества $Q = \{2, \ \dots \ , \ q-1\}$, записывает его и поступившее сообщение на ленту и выдает полученное случайное число в качестве ответа. Если же сообщение уже получалось раннее, машина выдает случайное число, полученное прежде и записанное на ленте. Данный оракул будет выступать в качестве модели хэш-функции h.

Также определим оракул O'. Получая на вход сообщение m, O' также проверяет, получено ли оно впервые и, если нет, генерирует случайное число h из множества Q, после чего увеличивает его на единицу, если $h \in \{2, \ \dots \ , \ q-2\}$ или присваивает h значение 2, если в качестве случайного значения было получено $q-1$. В остальном O' работает аналогично оракулу O.

Будем рассматривать стойкость схемы против

- угрозы экзистенциональной подделки (подделки подписи некоторого сообщения)
- атаки с известным открытым ключом

В качестве противника, таким образом, будет рассматриваться ПВМТ A с оракулом O, получающая на вход $(g, 1^q, y)$ и пытающаяся подделать подпись некоторого сообщения участника с открытым ключом y.

Определение. Будем считать схему подписи стойкой в модели со случайным оракулом, если для любой ПВМТ A^O с оракулом и любого полинома $p(q)$

$$Pr\{A^O(g, 1^q, y) = (h, s, \ F(r)) : \ V(y, g, h, \ s, \ F(r)) = 1\} < 1/p(q)$$

для всех достаточно больших q. Под V понимается предикат, истинный в том и только в том случае, когда выполняется уравнение верификации подписи.

Теорема. В рамках описанной модели предложенная схема и ГОСТ эквивалентны по стойкости.

Рассмотрим уравнение верификации подписи в предложенной схеме. При $h \neq 1$ оно допускает следующие преобразования:

$$r^{-(h-1)} \ g^s \ y^{-f(r)} = e \ \Leftrightarrow \ g^s \ y^{-f(r)} = r^{h-1} \ \Leftrightarrow \ (g^s \ y^{-f(r)})^{(h-1)^{-1}} = r$$

Предположим, что существует ПВМТ A^O с оракулом O и полином $p(q)$ такие, что

$$Pr\{A^O(g, 1^q, y) = (s, \ F(r)) : \ (g^s \ y^{-f(r)})^{(h-1)^{-1}} = r\} \geq 1/p(q)$$

для бесконечного количества q.

Рассмотрим тогда машину $A^{O'}$ с оракулом, подмененным на O'.

С точки зрения возвращаемого значения оракул O' работает аналогично оракулу O, реализуя равномерно распределенную на $Q \setminus \{1\}$ величину. При этом, в рамках рассматриваемой модели, O' возвращает значение хэш-функции, увеличенное на 1 на множестве Q 0. Таким образом, машина $A^{O'}$ с оракулом O' будет работать аналогично машине A^O с оракулом O. При этом с точки зрения рассматриваемой модели она будет получать пары

$$(s,\ F(r)) :\ (g^s\ y^{-f(r)})^{((h+1)-1)^{-1}} = (g^s\ y^{-f(r)})^{h^{-1}} = r$$

с вероятностью, большей $1/p(n)$ для некоторого полинома $p(n)$ и бесконечного количества n, т.е. подделывать подписи в схеме ГОСТ.

Таким образом, машина A^O, подделывающая подписи описанной схемы, при замене оракула O на O' будет подделывать подписи в схеме ГОСТ. Аналогичным образом может быть осуществлено сведение задачи взлома ГОСТ к взлому предложенной схемы.

Отметим, что выбрасывание из области значений оракулов O и O' чисел 0 и 1 т.е. при росте основного параметра q доля множества этих точек в множестве Q бесконечно убывает, при этом для обеспечения нестойкости рассматриваемых схем атакующая машина должна быть способна подделывать подпись на множестве мощности, как минимум, $1/p(q)$.

4.4 Анализ полученных результатов и возможное обобщение задачи ДПЛ

В рамках [1] и [2] показано, что решение противником задачи ДПЛ (или случайная публикация владельцем секретного ключа подписи сообщения с единичным хэшем) позволяет осуществлять подделку подписи произвольного сообщения. При этом сложность задачи ДПЛ остается неизвестной.

В работе построена схема подписи, в которой решение ДПЛ также позволяет подделать любую подпись, при этом по вычислительной сложности задача ДПЛ равносильна ДЛ.

Построенная схема показывает, однако, что задача ДПЛ, возможно, нуждается в обобщении. Будучи определенная как подпись сообщения с хэш-значением, равным заданной константе, задача ДПЛ допускает построение схемы ЭЦП, в которой задача ДПЛ и ДЛ будут равносильны за счет линейного смещения хэш-значения в уравнении верификации подписи. Стойкость полученной таким образом схемы будет не ниже стойкости российского стандарта ГОСТ.

Рассмотрим возможное обобщение задачи. Для этого заметим, во-первых, что, к примеру, в схеме ГОСТ подделку любого сообщения можно осуществлять не только зная подпись сообщения $m : H(m) = 1$ любого участника, но и зная подпись сообщения $m : H(m) = h_1$ для фиксированного наперед h_1. В самом деле, предположим, что мы имеем эффективный алгоритм нахождения подписи сообщения с хэш-значением, равным h_1 для любого открытого ключа. Подделаем подпись участника с ключом y сообщения с хэш-значением h_2

Для этого найдем подпись сообщения $m : H(m) = h_1$ для участника с открытым ключом $y_1 = y^{h_2^{-1}/h_1^{-1}}$. Получим пару $(F(r), s)$:

$$g^{sh^{-1}} y_1^{-f(r)h^{-1}} = r$$

Тогда в качестве подписи участника с ключом y сообщения $m : H(m) = h_2$ можно взять $(F(r), sh_1^{-1}/h_2^{-1})$. В самом деле,

$$(g^{s\ h_1^{-1}/h_2^{-1}}\ y^{-f(r)})^{h_2^{-1}} = g^{sh^{-1}} y_1^{-f(r)h^{-1}} = r$$

Таким образом, можно сформулировать обобщенную задачу ДПЛ и необходимое условие стойкости на ее основе.

Определение. Обобщенной задачей ДПЛ (ОДПЛ) будем называть следующую задачу.

Вход: $(1^q,\ g,\ y,\ \nu(q))$, где $q,\ g$ - параметры группы, y - открытый ключ, $\nu(q)$ - эффективно-вычислимая функция, которая по параметру q возвращает значение из множества $Q = \{1,\ \ldots\ ,\ q-1\}$

Выход: $(F(r), s)$ - подпись участника с открытым ключом y сообщения с хэш-значением, равным $\nu(q))$

Тогда, с учетом таким образом определенной задачи ОДПЛ, можно сформулировать необходимое условие стойкости схемы ГОСТ (а также DSA и предложенной схемы с взаимно-сводимыми задачами ДПЛ и ДЛ).

Для любых ПВМТ A, решающей задачу ОДПЛ, эффективно-вычислимой функции $\nu(q)$ и полинома $p(q)$

$$Pr\{A(1^q,\ g,\ y,\ \nu(q)) = (s,\ F(r)) :\ V(y,\ g,\ h,\ s,\ F(r)) = 1\} < 1/p(q)$$

5 Полученные результаты

В работе проведен анализ семейства схем ЭЦП Эль-Гамаль, задачи ДПЛ в них. Получена схема ЭЦП со стойкостью не ниже стойкости схемы ГОСТ, в которой задача ДПЛ равносильна задаче ДЛ. Предложено обобщение задачи ДПЛ, в терминах которого сформулировано необходимое условие стойкости схемы ЭЦП ГОСТ.

6 Литература

1. Варновский Н.П., Стойкость схем электронной подписи в модели с защищенным модулем, Дискретная математика, 2008, том 20, вып. 3, с. 147–159.

2. P. P. Horster, M. Michels, H. Petersen, Generalized ElGamal signatures for one message block. Proceedings of Second International Workshop on IT-Security, Vienna, Oldenbourg Verlag, Munchen/Wien 1994, pp. 66-81.

3. D. Brown, On the provable security of ECDSA, Designs, Codes and Cryptography, v. 35, N 1, 2005, 119-152

4. S. Goldwasser, Lecture notes on Cryptography, 2008

5. M. Naor, M. Yung, Universal One-Way Hash Functions and their Cryptographic Applications, Proceedings of the 21st ACM Symposium on Theory of Computing, 1989, 33-34

6. J. Rompel, One-Way Functions are Necessary and Sufficient for Secure Signatures, Proceedings of the 22nd ACM Symposium on Theory of computing, 1990, 387-394