СТАНДАРТИЗАЦИЯ АЛГОРИТМОВ ЭЦП И ТРАНСПОРТА КЛЮЧА НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

С. В. Агиевич

НИИ прикладных проблем математики и информатики БГУ
Минск, Беларусь
E-mail: Agievich@bsu.by

Обсуждаются характеристики стандарта СТБ 34.101.45 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых», который вводится в 2014 году.

Ключевые слова: электронная цифровая подпись, транспорт ключа, эллиптические кривые.

Завершается разработка нового государственного стандарта СТБ 34.101.45 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых». Планируется, что стандарт будет введен в действие в начале 2014 года и станет использоваться в создаваемой Государственной системе управления открытыми ключами, а также в проектируемой Единой системе идентификации физических и юридических лиц. Перечислим характеристики алгоритмов разработанного стандарта.

Уровни стойкости. Поддерживаются три уровня стойкости. Выбор уровня определяется параметром безопасности $l \in \{128, 192, 256\}$. На уровне l поддерживается паритет стойкости с алгоритмами шифрования и имитозащиты, в которых используются l-битовые ключи. Аналогичные уровни стойкости заданы в стандартах СТБ 34.101.31 (шифрование, имитозащита, управление ключами), СТБ 34.101.60 (разделение секрета), СТБ 34.101.66 (протоколы формирования общего ключа).

Выбор эллиптической кривой. Алгоритмы стандарта основаны на вычислениях в группе точек эллиптической кривой над простым конечным полем Φ_p. Кривая задается уравнением $y^2 = x^3 + ax + b$, где $a, b \in \Phi_p$. Одна и та же кривая может использоваться как в алгоритмах СТБ 34.101.45, так и в протоколах СТБ 34.101.66.

Требуется, чтобы модуль p был сравним с 3 по модулю 4. По такому модулю удобно извлекать квадратные корни и поэтому можно быстро определять y-координаты точек по их x-координатам. При обмене точками можно передавать только x-координаты, вдвое сокращая объем данных и незначительно теряя в эффективности вычислений. Сокращение объема данных обмена использовано нами в алгоритмах транспорта ключа.

Ограничение на p позволяет использовать алгоритм SWU, предложенный Шалле (S), Вестайном (W) и Уласом (U). Этот алгоритм за детерминированное время находит представление двоичной строки точкой эллиптической кривой. Алгоритм SWU использован в протоколе BPACE, определенном в СТБ 34.101.66.

Коэффициент b выбирается как квадратичный вычет по модулю p. При этом точка $(0, b^{(p+1)/4} \bmod p)$ обязательно лежит на кривой. Эта точка объявляется базовой. Требуется, чтобы группа точек эллиптической кривой, порожденная базовой, совпадала с группой всех Φ_p-рациональных точек кривой. Это требование упрощает проверку открытых ключей.

Модуль p и порядок q группы точек эллиптической кривой являются простыми числами в диапазоне от $2^{2l-1}+1$ до $2^{2l}-1$. Числа p и q представляются двоичными словами строго определенной длины $2l$. Фиксированная длина чисел упрощает управление параметрами эллиптической кривой в прикладных системах.

Генерация долговременных параметров. Определены алгоритмы генерации и проверки долговременных параметров, определяющих группу точек эллиптической кривой. Алгоритм генерации построен так, что навязывание специальной кривой затруднено.

Алгоритм генерации параметров оставляет свободу и позволяет задать удобные для вычислений модуль p и коэффициент a. В целом всю группу точек, в том числе базовую точку, можно однозначно построить по модулю p, коэффициенту a и 64-битовому слову *seed*, которое используется при генерации.

В стандарте определены стандартные наборы долговременных параметров для каждого из трех уровней стойкости. С учетом перспектив использования эллиптических кривых в криптографии, в стандартных наборах порядок q группы точек удовлетворяет дополнительному условию: числа $q \pm 1$ имеют большие простые делители. Кроме этого, стандартные модули p имеют вид $2^{2l} - c$, где c невелико. Такой выбор p существенно ускоряет вычисление остатков mod p.

Предварительное хэширование. Сообщение X, электронная цифровая подпись (ЭЦП) которого вырабатывается или проверяется, предварительно обрабатывается функцией хэширования h. В дальнейших вычислениях вместо X используется полученное хэш-значение $h(X)$. Предварительное хэширование упрощает встраивание реализаций алгоритмов ЭЦП в распространенные программные интерфейсы. Дело в том, что эти интерфейсы построены по принципу hash-and-sign: на вход программных функций, реализующих алгоритмы ЭЦП, подается не X, а $h(X)$.

Допускается использование достаточно произвольной функции предварительного хэширования. Тем не менее, идентификатор h учитывается при выработке ЭЦП, что защищает от атак по построению коллизий вида $h(X) = h'(X')$.

Сокращение длины ЭЦП. Длина ЭЦП составляет $3l$ битов. Для сравнения, в аналогичных стандартах ECDSA, ГОСТ Р 34.10-2012, EC-KDSA вырабатываются $4l$-битовые подписи. «Обрезка» ЭЦП не только уменьшает объем памяти для хранения данных, но и ускоряет проверку подписи. Например, при использовании бинарных методов нахождения кратных точек проверка ЭЦП будет выполняться примерно на 8 % медленнее выработки. Для сравнения, без «обрезки» проверка замедляется на 17 %.

Схема Шнорра. Алгоритмы ЭЦП построены по схеме Шнорра – одной из наиболее эффективных и обоснованных схем ЭЦП. Использование схемы Шнорра сохраняет преемственность с действующим национальным стандартом СТБ 1176.2-99. Вычисления по схеме Шнорра – часть алгоритмов идентификационной ЭЦП, а также протоколов BMQV и BSTS, определенных в СТБ 34.101.66.

Детерминированный алгоритм выработки ЭЦП. В схеме ЭЦП Шнорра при выработке подписи используется одноразовый личный ключ k. Этот ключ должен вырабатываться случайно равновероятно с помощью генератора RNG или псевдослучайно с помощью алгоритма PRNG, который берет на вход ключ K и синхропосылку S.

Для организации случайной генерации разработчику средства ЭЦП требуется, по крайней мере, приобрести RNG, встроить RNG, контролировать работу RNG. Все это вызывает удорожание и усложнение средства ЭЦП. Имеются трудности с размещением RNG на микроустройствах. При использовании PRNG разработчик опять сталкивается с трудностями – следует обеспечить секретность K и уникальность S. Иногда поддержать уникальность даже труднее, чем секретность. Синхропосылки S сно-

ва можно строить с помощью RNG (но тогда переход к псевдослучайной генерации теряет смысл), либо определять по значениям монотонного счетчика. В последнем случае средство ЭЦП должно иметь перезаписываемую память, обновляемую при каждом подписывании или, в лучшем случае, запуске средства.

Выходом является псевдослучайная генерация с выбором в качестве K личного ключа ЭЦП, а в качестве S – хэш-значения подписываемого сообщения. В стандарте определен алгоритм PRNG, основанный на алгоритмах шифрования СТБ 34.101.31. При использовании PRNG алгоритм выработки ЭЦП перестает быть вероятностным. Подпись становится детерминированной, всегда одной и той же для конкретного сообщения. Это облегчает управление документами, позволяет использовать подпись в качестве контрольной суммы. У владельца личного ключа остается меньше возможностей отказаться от своей подписи из-за сбоев в RNG или повтора синхропосылок.

Транспорт ключа. Кроме алгоритмов ЭЦП в стандарте определены алгоритмы транспорта ключа, по сути, алгоритмы шифрования с открытым ключом. Алгоритмы построены по схеме шифрования ЭльГамаля. Связка «алгоритмы ЭЦП + алгоритмы транспорта» позволяет решить основные криптографические задачи: конфиденциальность, контроль целостности, контроль подлинности.

Алгоритмы транспорта могут работать с теми же долговременными параметрами, что и алгоритмы ЭЦП. Более того, алгоритмы транспорта могут работать на тех же ключах. Совмещение ключей ЭЦП и транспорта упрощает распространение открытых ключей транспорта в форме сертификатов. Стандартные правила выдачи таких сертификатов предполагают доказательство владения личным ключом путем подписывания на нем запроса на выдачу сертификата. Если бы личный ключ транспорта нельзя было использовать в алгоритмах ЭЦП, то правила нельзя было бы применить и распространение открытых ключей в стандартной инфраструктуре X.509 было бы затруднено.

В стандарте разрешен широковещательный транспорт, при котором один и тот же ключ рассылается сразу нескольким сторонам, причем при формировании рассылки используется одна и та же пара одноразовых ключей (личного и открытого).

Идентификационная ЭЦП. Стандартизированы алгоритмы идентификационной ЭЦП, которые обеспечивают одновременную проверку подлинности как сообщения, так и подписавшей его стороны. Открытый ключ подписавшейся стороны, который распространяется вместе с идентификационной ЭЦП, является своего рода облегченным сертификатом – его длина всего $4l$ битов.

Программная реализация. Стандарт рассылался на отзыв в заинтересованные организации вместе с программной библиотекой bee2, в которой реализованы все стандартизируемые криптографические алгоритмы. Программная библиотека может быть использована для сокращения цикла разработки, сертификации и внедрения средств криптографической защиты информации на основе СТБ 34.101.45. Планируется сделать библиотеку свободно распространяемой.