УДК 004.056.2

А.А. КУЛАГА

ПОСТРОЕНИЕ БИЛИНЕЙНЫХ ЦИФРОВЫХ ПОДПИСЕЙ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ ЛИЧНОСТНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЯ

Ключевые слова: *билинейные отображения, подпись Эль-Гамаля, эллиптические кривые, пороговые схемы, криптосистемы с открытым индивидуальным ключом.*

ВВЕДЕНИЕ

В настоящее время научным сообществом рассматривается ряд перспективных направлений, связанных с использованием криптографических примитивов на билинейных отображениях (билинейных спариваниях) точек эллиптических кривых. Это позволяет упрощать некоторые криптосистемы, а также решать некоторые специфические задачи в криптографии, включая создание асимметричных криптосистем с открытым индивидуальным ключом (Identity Based Cryptosystems). В настоящей статье рассматриваются свойства билинейных отображений, описывается построение схем цифровой подписи с открытым индивидуальным ключом, которые являются билинейными аналогами алгоритмов, определенных в украинском (ДСТУ 4145-2002) [1], германском (EC-GDSA) и корейском (EC-KCDSA) стандартах формирования и проверки цифровой подписи, а также приводится построение пороговых схем на базе этих билинейных аналогов.

КРИПТОСИСТЕМЫ С ОТКРЫТЫМ ИНДИВИДУАЛЬНЫМ КЛЮЧОМ

Идея создания систем с открытым индивидуальным ключом пользователя была предложена А. Шамиром в 1984 г. [2] как альтернатива системам с инфраструктурой открытого ключа (Public Key Infrastructure — PKI), использующая сертификаты. Однако проблема построения таких асимметричных криптосистем оставалась открытой до 2001 г., когда Д. Боне и М. Фрэнклин представили свою схему шифрования [3], использующую свойства билинейного спаривания Вейля на эллиптической кривой, поскольку ни одна схема, предложенная ранее, не отвечала всем требованиям безопасности и эффективности. Она является первой полнофункциональной, эффективной и безопасной схемой шифрования. После работы Боне и Фрэнклина появились другие асимметричные схемы, среди которых получили известность схемы шифрования Генри–Сильверберга [4], Боне–Бойена [5] и др., а также схемы подписи Занга–Кима [6], Хессе [7].

В криптосистемах с открытым индивидуальным ключом нет необходимости пользователям обмениваться своими сертификатами открытых ключей, так как

открытые ключи выводятся из личностных данных пользователя, которые общеизвестны (например, e-mail пользователя, его имя или номер его мобильного телефона и др.). Секретные ключи пользователей схемы и системные параметры генерируются доверенным органом — Центром генерации ключей (Private Key Generator — PKG).

В таких системах вместо того чтобы поддерживать работу PKI, необходимо поддерживать работу PKG, что значительно проще, поскольку нет необходимости в обслуживании, управлении, создании, удалении и распределении сертификатов, а это приводит к уменьшению затрат на управление инфраструктурой открытых ключей [8]. Но для этого обязательно выполнение таких условий: пользователь должен быть полностью уверен в корректности данных, идентифицирующих пользователя, которые он использует, и PKG должен передавать закрытые ключи только их хозяевам. Необходимо отметить, что один из недостатков классических криптосистем с открытым индивидуальным ключом — возможность со стороны PKG контроля над секретными ключами пользователей, а одним из способов преодоления этого недостатка является использование пороговых схем. В научной литературе описано большое количество пороговых схем на основе разных алгоритмов. Так, например, в работах [9–11] предложены пороговые схемы цифровой подписи (ЦП) на основе российских стандартов ГОСТ 34.10-94 и ГОСТ 34.10-2001.

ЭЛЬ-ГАМАЛЯ–ПОДОБНЫЕ СХЕМЫ ПОДПИСИ

Решение задач построения схем асимметричного шифрования и ЦП осуществляется с помощью односторонней функции с «лазейкой», что было впервые предложено Эль-Гамалем в [12], где для построения такой функции он применил идею использования двух ключей. Что касается криптосистем на эллиптических кривых, которые появились позднее, то они наследуют основные протоколы Эль-Гамаля–подобных схем, поскольку их алгебраические структуры построены на конечных группах элементов. Все криптоалгоритмы с алгеброй поля адаптируются в аддитивной группе точек эллиптической кривой с операцией скалярного умножения точки вместо экспоненцирования в мультипликативной группе [13]. Таким образом, большинство алгоритмов ЦП, которые построены на арифметике группы точек эллиптической кривой, основаны на схеме Эль-Гамаля [12]. В 90-х годах был принят национальный стандарт ЦП США, который представил алгоритм ЦП DSA как модификацию схемы Эль-Гамаля. После 1999 г. появились национальные и международные стандарты криптографии на эллиптических кривых. Существующие стандарты и их проекты [1, 14–16] описывают разные алгоритмы с различной стойкостью и вычислительной сложностью, что расширяет возможности выбора при разработке криптосистем. Рассмотрим наиболее распространенные алгоритмы, начиная с обобщенной подписи схемы Эль-Гамаля [12, 17] в аддитивной группе.

Системными параметрами являются уравнение эллиптической кривой E, определение поля $\mathbb{F}$ и точка P кривой известного большого порядка N, которая является образующим элементом подгруппы G группы точек эллиптической кривой $E(\mathbb{F})$. Открытым ключом проверки является точка $Q = dP$, где d — секретный ключ подписи. Подпись сообщения m, которую формирует пользователь A, это пара (R, s), где $R = kP$ — случайная точка (элемент группы G), определяемая случайным числом k, $0 < k < N - 1$, что удовлетворяется уравнением

$$h(R)Q + sR = h(m)P, \qquad (1)$$

где $h(m)$ — хеш-значение от сообщения m, а $h(R)$ — хеш-значение от конкатенации координат точки $R = (x, y)$.

Решить уравнение (1) относительно s можно, зная только секретное значение d:

$$sR = h(m)P - h(R)Q = h(m)P - h(R)dP .$$

Таким образом, $sP = k^{-1}(h(m) - h(R)d)P$. Из этого уравнения следует, что

$$s = k^{-1}(h(m) - h(R)d) . \qquad (2)$$

Чтобы подписать сообщение m, пользователь A должен выполнить такие действия:

1) выбрать k, $0 < k < N - 1$, и вычислить $R = kP$;

2) вычислить значение s в соответствии с (2).

Пользователь B с целью проверки подписи должен проверить верификационное соотношение (1).

Рассмотрим некоторые атаки на такую схему ЦП (более подробно атаки на Эль-Гамаля–подобные схемы рассматриваются в [13, 8]).

Чтобы подделать подпись под сообщением m', необходимо вычислить случайное $R = kP$ и затем параметр s, $s = k^{-1}(h(m') - h(R)d)$. Для этого нужно, зная $Q = dP$, вычислить секретное значение d, т.е. решить задачу дискретного логарифмирования в группе точек эллиптической кривой G над конечным полем, которая более сложная, чем эта же задача в мультипликативной группе конечного поля при условии выполнения некоторых требований к эллиптической кривой.

Если существует другой способ подделки подписи под сообщением m' (т.е. вычислить пару (R, s) так, чтобы выполнялось соотношение (1)), то этим способом можно решать задачи дискретного логарифмирования в этой группе: вычислить секретный ключ подписи $d = (h(m') - sk)h(R)^{-1}$. Таким образом, проблема подделки подписи настолько же сложная, как и задача дискретного логарифмирования в группе точек эллиптической кривой G.

При реализации такой схемы подписи следует значение k уничтожить сразу после формирования подписи, поскольку атакующий по значению k и значению подписи (R, s) может вычислить секретный ключ $d = (h(m) - sk)h(R)^{-1}$.

Вычислить секретный ключ также возможно при повторном использовании числа k. Предположим, что с одним и тем же значением k сформированы две подписи: (R, s_1) и (R, s_2) от сообщений m_1 и m_2 соответственно. При этом

$$s_1 = k^{-1}(h(m_1) - h(R)d) \text{ и } s_2 = k^{-1}(h(m_2) - h(R)d) .$$

Тогда $s_1 - s_2 = k^{-1}(h(m_1) - h(m_2))$. При $s_1 \neq s_2$ имеем $k = (h(m_1) - h(m_2)) \times$ $\times (s_1 - s_2)^{-1}$, а зная значение k, можно вычислить d.

В алгоритме подписи используется не само сообщение, а его хеш-значение, так как можно подобрать сообщение по известному значению подписи, например выбрать случайные числа i и j, а затем принять

$$R = iP + jQ = (i + dj)P ; \; s = -h(R)j^{-1} \bmod N .$$

Тогда пара (R, s) будет подписью сообщения $m = si \bmod N = -h(R)j^{-1}i \bmod N$, так как

$$(mP - h(R)dP)s^{-1} = (-h(R)j^{-1}iP - h(R)dP)(-h(R)j^{-1})^{-1} =$$

$$= -h(R)j^{-1}i(-h(R))^{-1}jP - h(R)d(-h(R))^{-1}jP = iP + djP = R .$$

Из этого следует равенство $(mP - h(R)dP) = sR$ и подтверждение подписи $h(R)Q + sR = mP$.

Также подпись хеш-значения от сообщения необходима для предотвращения атаки на основе гомоморфизмов.

Из уравнения (1) параметр $R \in G$ можно выразить следующим образом:

$$R = s^{-1}(h(m)P - h(R)Q) = s^{-1}(h(m)P + h(R)(-d)P). \quad (3)$$

Решая уравнение (3) относительно s, получим $sR = skP = h(m)P + h(R)(-d)P$, откуда следует

$$s = k^{-1}(h(m) + h(R)(-d)). \quad (4)$$

Подпись под сообщением m обозначается как пара $(h(R), s)$, при этом пользователь A, который формирует эту подпись, вычисляет случайную точку $R \in G$ и параметр s в соответствии с формулой (4), используя секретный ключ подписи $-d$. Для проверки этой подписи необходимо использовать формулу (3), но не как предикат проверки, а для вычисления точки R по известным значениям $h(R)$, s, $h(m)$ и по значению $-dP$, которое представляет собой открытый ключ подписи. Хеш-значение вычисленной на этапе проверки точки R и значение $h(R)$, которое вычислил пользователь A, должны быть одинаковыми. На этом основывается предикат проверки.

В (3) и (4) вместо $h(R)$ можно использовать другое значение, которое обозначим r. Пусть в данном случае r будет равно некоторому целому числу $\bar{x}$, вычисляемому из элемента поля $\mathbb{F}$ координаты $x \in \mathbb{F}$ точки R. Для формирования подписи (r, s) в этом случае используется формула $s = k^{-1}(h(m) + r(-d))$, а для проверки вычисляется точка $R \in G$ по формуле $R = s^{-1}(h(m)P + r(-d)P)$ и сравнивается целое число $\bar{x}$, которое определяется из элемента поля $\mathbb{F}$ координаты x вычисленной точки R, с параметром подписи r. Такая схема используется в стандарте ECDSA (Elliptic Curve Digital Signature Algorithm).

Рассмотрим примеры наиболее известных Эль-Гамаля–подобных схем подписи, которые отличаются от приведенных выше основным уравнением подписи, значением параметра r и формованием соответствующего предиката проверки.

— ECSS (Elliptic Curve Signature Scheme). Вместо уравнения (1) используется равенство $R - sP = rQ$ (где $r = \bar{x} + h(m)$), из которого можно найти s: $s = k - rd$, а при проверке в соответствии с этим уравнением вычисляется R.

— ГОСТ 34.10-2001 (Российский стандарт) [16]. Вместо уравнения (1) используется уравнение $R = h(m)^{-1}sP + h(m)^{-1}rQ$ (где $r = \bar{x}$), из которого можно найти s: $s = kh(m) + rd$. При проверке подписи (r, s) по основному уравнению вычисляются R, а затем r.

— ДСТУ 4145-2002 (Украинский стандарт, подобный ECSS) [1]. Вместо уравнения (1) используется уравнение $R - sP = rQ$, где $r = \bar{x}\, h(m)$, $Q = -dP$, $s = k + rd$. При проверке подписи (r, s) вычисляется R, а затем r.

— EC-GDSA (Elliptic Curve based German Digital Signature Algorithm). В качестве основного уравнения подписи используется уравнение $R - r^{-1}sQ = r^{-1}h(m)P$, где $r = \bar{x}$, $Q = dP$, $s = (kr - h(m))d$, в соответствии с которым при проверке подписи (r, s) вычисляется параметр R.

— EC-KCDSA (Korean Certificate-based Digital Signature Algorithm using Elliptic Curves). Основное уравнение подписи: $R - sQ = (r \oplus h(C_A \circ m))P$, где $r = h(R)$, $Q = d^{-1}P$, C_A — сертификат открытого ключа пользователя A. В соответствии с этим уравнением при проверке подписи (r, s) находится R, параметр s вычисляется следующим образом: $s = (k - (r \oplus h(C_A \circ m)))d$.

Сравнительные характеристики этих алгоритмов, включая объем необходимых вычислений для формирования и проверки подписи, а также их стойкость более детально приводятся в [13].

ПОСТРОЕНИЕ СХЕМ ЦП С ОТКРЫТЫМ ИНДИВИДУАЛЬНЫМ КЛЮЧОМ

Для Эль-Гамаля–подобных схем ЦП является возможным построением их аналогов с использованием математического аппарата билинейных отображений с целью построения схем ЦП с открытым индивидуальным ключом пользователя.

Пусть G_1 и G_2 — соответственно аддитивная и мультипликативная группы простого порядка q. Билинейным спариванием (или парным отображением) называется легко вычисляемое невырожденное билинейное отображение $e: G_1 \times G_1 \to G_2$, т.е. отображение со следующими свойствами.

1. Билинейность.

Для $\forall P, Q, R \in G_1 : e(P+Q, R) = e(P, R)e(Q, R)$ и $e(P, Q+R) = e(P, Q)e(P, R)$. Из этого следует, что для $\forall P, Q \in G_1$ и $\forall a, b \in \mathbb{Z}_q^*$: $e(aP, bQ) = e(P, Q)^{ab}$.

2. Невырожденность.

Существует $P \in G_1$, $e(P, P) \neq 1$, т.е. если P является образующим элементом G_1, то $e(P, P)$ будет образующим элементом G_2, так как G_1 и G_2 — группы простого порядка.

3. Вычислимость.

Существует эффективный полиномиальный алгоритм вычисления $e(P, Q) \in G_2$ для $\forall P, Q \in G_1$.

Пусть $ID \in \{0,1\}^*$ — личностные данные пользователя схемы, который формирует подпись сообщения m, Q_{ID} — его открытый ключ, s — секретный мастер-ключ PKG, $P_{pub} = sP$ — открытый мастер-ключ PKG. Открытый ключ Q_{ID} пользователя вычисляется из его ID с помощью хеш-функции $h_1: \{0, 1\}^* \to G_1$.

Подпись под сообщением m, которую формирует пользователь с его общеизвестными данными ID, это пара (r, S) (где $S \in G_1$, $r = h(m)\overline{R}$, $R = e(P, P)^k$ — случайный элемент группы G_2, определяемый случайным параметром $k \in \mathbb{Z}_q^*$) такая, что выполняется равенство

$$e(P, P)^k = e(S, P)e(Q_{ID}, P_{pub})^r . \tag{5}$$

Решить это уравнение относительно неизвестной точки эллиптической кривой S можно, зная только секретное значение s. Поэтому имеем $e(kP, P) = e(S, P)e(rsQ_{ID}, P)$, величину sQ_{ID} обозначим D_{ID}. Тогда $e(kP, P) = e(S + rD_{ID}, P)$. Из этого следует, что $kP = S + rD_{ID}$, а значение параметра подписи S выражается следующим образом:

$$S = kP - rD_{ID} . \tag{6}$$

Для формирования подписи пользователем A с его личностными данными ID_A необходимо, чтобы PKG сгенерировал секретный мастер-ключ s, вычислил P_{pub} и параметр D_{ID_A}, который является секретным ключом пользователя A. Пользователь A получает $D_{ID_A} \in G_1$ от PKG по защищенному каналу и генерирует случайное значение $k \in \mathbb{Z}_q^*$, затем вычисляет r и в соответствии с (6) находит параметр S.

Для проверки этой подписи, т.е. пары (r, S) под сообщением m, следует вычислить значение R в соответствии с (5), затем значение $h(m)\overline{R}$ и сравнить его с параметром подписи r. Эти значения должны быть одинаковыми. Такую схему можно считать билинейным аналогом алгоритма ЦП, который определен в ДСТУ 4145-2002.

Стойкость этой схемы обусловлена трудностью решения слабой задачи Диффи–Хеллмана в аддитивной группе (W-DH — Weak Diffie–Hellman problem),

которая формулируется следующим образом: для заданного набора $\langle P, Q, sP \rangle$, где $P, Q \in G_1$ и $s \in \mathbb{Z}_q^*$, вычислить точку sQ. Считается, что эта задача не сложнее, чем вычислительная задача Диффи–Хеллмана (CDH problem — Computational Diffie-Hellman problem) в аддитивной группе. В настоящее время неизвестно, можно ли ее решить, минуя задачу дискретного логарифма для эллиптических кривых.

Допустим, что атакующему известны параметры P, Q_{ID} и $P_{pub} = sP$. Для того чтобы подделать подпись, он должен уметь находить ключ $D_{ID} = sQ_{ID}$, т.е. решить задачу W-DH. Далее построим билинейную схему ЦП с открытым индивидуальным ключом на базе алгоритма, который определен в EC-GDSA. Как и в вышеприведенной схеме, чтобы пользователь A с его личностными данными ID_A сформировал подпись под сообщением m, необходимо, чтобы PKG сгенерировал секретный мастер-ключ s, вычислил $P_{pub} = sP$, а также секретный ключ $D_{ID_A} = sQ_{ID_A}$ пользователя A. Пользователь A должен получить $D_{ID_A} \in G_1$ от PKG и сгенерировать случайное значение $k \in \mathbb{Z}_q^*$, затем вычислить $r = \overline{R} = \overline{e(P,P)^k}$ и S по формуле $S = rkP - h(m)D_{ID}$.

Для проверки подписи (r, S) под сообщением m необходимо вычислить параметр R : $R = e(S,P)^{r^{-1}} e(Q_{ID}, P_{pub})^{r^{-1}h(m)}$, затем сравнить параметр $\overline{R}$ с параметром подписи r, которые должны быть одинаковыми.

Корректность схемы можно доказать, используя следующие соотношения:

$$e(S,P)^{r^{-1}} e(Q_{ID}, P_{pub})^{r^{-1}h(m)} = e(rkP - h(m)D_{ID}, P)^{r^{-1}} e(Q_{ID}, P_{pub})^{r^{-1}h(m)} =$$

$$= e(kP - r^{-1}h(m)D_{ID}, P)e(r^{-1}h(m)Q_{ID}, sP) =$$

$$= e(kP - r^{-1}h(m)D_{ID}, P)e(r^{-1}h(m)D_{ID}, P) = e(kP, P).$$

В билинейной схеме ЦП с открытым индивидуальным ключом на базе алгоритма EC-KCDSA параметр S вычислим по формуле $S = kP - eD_{ID}$, где $e = (r \oplus h(ID_A \circ m))$, $r = h(R)$, $R = e(P,P)^k$.

Для проверки подписи (r, S) следует вычислить R в соответствии с выражением $R = e(S,P)e(Q_{ID}, P_{pub})^e$, затем вычислить $h(R)$. Это значение должно быть равно параметру подписи r.

Корректность этой схемы следует из следующих тождеств:

$$h(e(S,P)e(Q_{ID}, P_{pub})^e) =$$

$$= h(e(kP - eD_{ID}, P)e(Q_{ID}, P_{pub})^e) = h(e(kP - eD_{ID}, P)e(esQ_{ID}, P)) =$$

$$= h(e(kP - eD_{ID} + esQ_{ID}, P)) = h(e(kP, P)) = h(e(P,P)^k).$$

ПОРОГОВАЯ СХЕМА ПОДПИСИ

Известно, что безопасность асимметричных криптосистем существенно зависит от конфиденциальности секретных ключей. Эти ключи должны быть недоступными для атакующих, т.е. безопасность криптосистемы зависит от неспособности получения ими доступа к ключам. В работах [18, 19] предлагаются способы защиты от атак подобного рода на основе схем разделения секрета, когда секретный ключ разделяется между несколькими участниками, поскольку восстановление ключа в одном месте представляет собой привлекательную мишень для атаки. Для решения этой проблемы были предложены пороговые схемы [20].

В таких системах каждый участник содержит часть секретного ключа, отдельные доли ключа сохраняются конкретно у них и никогда не раскрываются другим сторонам, а для выполнения нужной функции, например формирования

подписи, необходимо, чтобы достаточно большое количество участников (пороговое число) действовали совместно. Каждый из них получает частичный результат. Эти части объединяются с помощью открытой, т.е. несекретной, функции, для получения нужного результата. В этом случае явного восстановления разделенного ключа не происходит.

Таким образом, для компрометации системы атакующему нужно скомпрометировать такое количество долей секрета, которое является не меньшим, чем пороговое число, при этом исключается существование единого места, в котором система может быть скомпрометированной.

На основе схемы подписи, которая описывается уравнениями (5) и (6), можно построить пороговую схему, где секретный ключ D_{ID} для формирования подписи не принадлежит отдельному пользователю, а разделяется между некоторыми пользователями, количество которых равно n, с помощью пороговой схемы Шамира (t, n) [18]. Таким образом, восстановить D_{ID} может любое подмножество Ω из этих пользователей, размер которого не меньше t. Части (доли, проекции) секретного ключа D_{ID} обозначим $D_{ID_1}, D_{ID_2}, \ldots, D_{ID_n}$. Тогда $D_{ID} = \sum_{i \in \Omega} L_i D_{ID_i}$, где $L_i = \prod_{j \in \Omega \setminus \{i\}} \frac{-x_j}{x_i - x_j}$, а x_i, $i = \overline{1, n}$, принадлежит i-му пользователю.

PKG формирует секретный мастер-ключ s, который представляется в виде долей $s_1, s_2, \ldots, s_n$ таких, что $s = \sum_{i \in \Omega} L_i s_i$, формирует открытые мастер-ключи $P_{pub_i} = s_i P$, а также $P_{pub} = sP$, далее вычисляет $D_{ID_i} = s_i Q_{ID}$, при этом $D_{ID} = \sum_{i \in \Omega} L_i D_{ID_i} = \sum_{i \in \Omega} L_i s_i Q_{ID} = \left(\sum_{i \in \Omega} L_i s_i \right) Q_{ID} = sQ_{ID}$. Затем по защищенному каналу PKG передает i-му пользователю долю D_{ID_i} или долю мастер-ключа s_i, используя схему Фельдмана или Петерсена [21, 22], а закрытый ключ D_{ID_i} вычисляет i-й пользователь.

Для формирования части подписи (R_i, S_i) каждый i-й пользователь генерирует $k_i \in \mathbb{Z}_q^*$, вычисляет $R_i = e(P, P)^{k_i}$, передавая его всем другим пользователям, и в соответствии с (6) вычисляет $S_i = k_i P - rD_{ID_i}$. При этом R определяется по формуле

$$R = \prod_{i \in \Omega} R_i^{L_i} = \prod_{i \in \Omega} (e(P, P)^{k_i})^{L_i} = e(P, P)^{\sum_{i \in \Omega} L_i k_i} = e(P, P)^k . \qquad (7)$$

Проверка каждой доли подписи осуществляется в соответствии с предикатом (5), т.е. $e(P, P)^{k_i} = e(S_i, P) e(Q_{ID}, P_{pub_i})^r$, с учетом (7).

Реконструкция подписи также выполняется с помощью интерполяции Лагранжа:

$$S = \sum_{i \in \Omega} L_i S_i = \sum_{i \in \Omega} L_i (k_i P - rD_{ID_i}) = \sum_{i \in \Omega} L_i k_i P - \sum_{i \in \Omega} L_i r D_{ID_i} =$$

$$= \left(\sum_{i \in \Omega} L_i k_i \right) P - r \sum_{i \in \Omega} L_i D_{ID_i} = kP - rD_{ID},$$

$$R = \prod_{i \in \Omega} R_i^{L_i} = e(P, P)^k .$$

Таким образом, реконструированная подпись (R, S) аналогична подписи, сформированной одним пользователем со случайным $k = \sum_{i \in \Omega} L_i k_i \in \mathbb{Z}_q^*$ и секретным ключом D_{ID}.

Пороговая схема может использоваться для повышения стойкости схем с открытым индивидуальным ключом к компрометации ключей. Аналогично вышеприведенной пороговой схеме ЦП можно построить также пороговые схемы для билинейных аналогов алгоритмов EC-GDSA и EC-KCDSA.

СПИСОК ЛИТЕРАТУРЫ

1. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. — К.: Держстандарт України, 2003. — 94 с.
2. Shamir A. Identity-based cryptosystems and signature schemes // Advances in Cryptology — Proceedings of CRYPTO 84. Lecture Notes in Computer Science. — 1985. — **196**. — P. 47–53.
3. Boneh D., Franklin M. Identity based encryption from the weil pairing / Extended Abstract in Crypto 2001 // SIAM J. of Computing. — 2003. — **32**, N 3. — P. 586–615.
4. Gentry C., Silverberg A. Hierarchical ID-based cryptography / Y. Zheng (ed). Proceedings of Asiacrypt 2002. Lecture Notes in Computer Science. — Springer-Verlag. — 2002.
5. Boneh D., Boyen X. Efficient selective-ID secure identity based encryption without random oracles // In Proceedings of Eurocrypt, 2004.
6. Zhang F., Kim K. ID-Based blind signature and ring signature from pairings // Advances in Cryptology –Asiacrypt 2002. Lecture Notes in Computer Science. — Springer-Verlag. — 2002. — **2510**.
7. Hess F. Efficient identity based signature schemes based on pairings // SAC 2002. Lecture Notes in Computer Science 2595. — Springer-Verlag. — 2002. — P. 310–324.
8. Горбенко Ю.І., Горбенко І.Д. Інфраструктура відкритих ключів. Електронний підпис. Теорія та практика. — Харків: Форт, 2010. — 608 с.
9. Запечников С.В. Пороговые схемы цифровой подписи на основе стандарта ГОСТ 34.10-94 // Безопасность информационных технологий. — 2001. — № 4. — С. 45–51.
10. Запечников С.В. Обеспечение криптографической стойкости при компрометации части ключей // Там же. — 2008. — № 4. — С. 93–102.
11. Серов Р.Е. Пороговая схема шифрования/подписи на основе ГОСТ 34.10-2001 // Там же. — 2004. — № 3. — С. 87–90.
12. ElGamal T. Public key cryptosystems and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. — 1985. — **IT-31**, N 4. — P. 469–472.
13. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых. — Киев.: ІВЦ Вид-во «Політехніка», 2004. — 224 с.
14. ANSI X9.62-1999. Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA), 1999.
15. FIPS 186-2-2000. Digital signature standard. national institute of standard and technology, 2000.
16. ГОСТ 34.10-2001. Информационная технология. Криптографическая защита информации. Процедуры формирования и проверки электронной цифровой подписи. — М.: Госстандарт России, 2001. — 20 с.
17. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в элептическую криптографию. Протоколы криптографии на эллиптических кривых. Ч. 2. — М.: КомКнига, 2006. — 280 с.
18. Shamir A. How to share a secret // Communications of the ACM. — 1979. — **22**. — P. 612–613.
19. Blakley G.R. Safeguarding cryptographic keys // Proceedings of the National Computer Conference 48, 1979. — P. 313–317.
20. Seberry J. Crypto topics and applications. II. University of Wollongong, 1999. — http://ro.uow.edu.au/infopapers/348.
21. Feldman P.A. Practical scheme for non-interactive verifiable secret sharing // Proc. 28th Annual Symp. on Founds. of Comp. Sci., 1987. — P. 427–437.
22. Pedersen T.P. Non-interactive and information-theoretic secure verifiable secret sharing // Advances in Cryptology — CRYPTO'91. Lecture Notes in Computer Science. — Springer-Verlag. — 1992. — **576.** — P. 129–140.
23. Dutta R., Barua R., Sarkar P. Pairing-based cryptographic protocols: a survey. — Kolkata, India. — http://eprint.iacr.org/2004/064.

Поступила 22.11.2010