Моделирование поведения программного обеспечения с точки зрения безопасности.– Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні": Київ.– вип. 2–2001. – с. 124–129. 6. Шлезингер М. И. Три лекции по математическим методам в распознавании образов. – ***www.iasa.kiev.ua.***

УДК 681.3.06:519.248.681

ПРОТОКОЛЫ НАПРАВЛЕННОГО ШИФРОВАНИЯ В ГРУППАХ ТОЧЕК НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ И ИХ СВОЙСТВА

Иван Горбенко, Станислав Збитнев, Андрей Поляков, Дмитрий Балагура
Харьковский Национальный Университет Радиоэлектроники

Анотація: **Розглядаються протоколи направленого шифрування з використанням еліптичних кривих на скінченних полях. Здійснюється аналіз класичних протоколів направленого шифрування та протоколів на еліптичних кривих. Аналізуються розміри параметрів і ключів.**
Summary: **Considered protocols of Elliptic Curve Integrated Encryption Scheme. Produce analysis of classical protocols and protocols of Elliptic Curve Integrated Encryption Scheme. Analyzed size of parameters and keys.**
Ключевые слова: **Эллиптическая кривая, направленное шифрование, поле Галуа, криптографические ключи.**

Введение

В последнее время в мире в качестве математического аппарата несимметричных преобразований все шире используется математика преобразований в группах точек на эллиптических кривых (ЕС) над полем. Создано и реализовано уже большое количество алгоритмов, реализующих известные схемы цифровой подписи, различных вариантов протоколов генерации общих секретов, алгоритмов направленного шифрования. В данной статье мы опираемся на уже известные комбинированные алгоритмы направленного шифрования. Рассматриваются схемы реализации направленного шифрования в группах точек эллиптических кривых, приводится их полное описание, а также основные свойства. Кроме того, в статье представлены результаты оценки сложности и скорости направленного шифрования в группах точек эллиптических кривых [1].

1 Анализ применяемых алгоритмов направленного шифрования

Вначале рассмотрим реализацию направленного шифрования RSA [2]. При использовании этого алгоритма получатель должен знать общесистемные параметры P_j и Q_j, причем P_j и Q_j должны быть «сильными» простыми числами. Этим повышается стойкость алгоритма. Используя эти числа, получатель выполняет следующие действия:

- формирует открытый ключ E_k такой, что $1 \le E_k \le \varphi(N_j)$, где $N_j = P_j \cdot Q$, а $\varphi(N_j)$ – функция Эйлера, и $(E_k, \varphi(N_j)) = 1$;
- вычисляет личный ключ D_k как обратный элемент к E_k в кольце; D_k вычисляется из соотношения $E_k \cdot D_k \equiv 1 (\mathrm{mod}\ \varphi(N))$;
- передаёт отправителю открытый ключ получателя E_k и модуль преобразования N_j, обеспечивая их целостность и подлинность.

Зашифрование выполняется по следующей схеме: всё сообщение делится на блоки, длина которых равна длине модуля преобразований $M = M_1 \,||\, M_2 \,||\, ... \,||\, M_n$, затем выполняется зашифрование каждого блока сообщения по формуле $C_i = M_i^{E_k} (\mathrm{mod}\ N)$.

Расшифрование каждого блока выполняется по формуле $M_i' = C_i^{D_k} (\mathrm{mod}\ N)$, а затем все блоки объединяются в сообщение.

Считается [3], что стойкость метода базируется на сложности факторизации модуля преобразований *N*.

Метод обладает двумя существенными недостатками:

1) в связи с разработкой новых методов и средств криптоанализа, сложность факторизации модуля становится субэкспоненциальной, например: $I = \exp\left(\delta(\ln N)^{\nu}(\ln\ln N)^{1-\nu}\right)$, где (δ, ν) – параметры используемого метода факторизации;
2) для повышения стойкости алгоритма необходимо увеличивать длину модуля преобразований, что приводит к повышению сложности прямого и обратного преобразований.

Вторым алгоритмом направленного шифрования является алгоритм, использующий схему Диффи-Хеллмана [4]. Алгоритм позволяет вырабатывать сеансовые ключи динамически, то есть непосредственно перед началом передачи данных. Для согласования ключей используется схема Диффи-Хеллмана [4]. При использовании данной схемы каждый из абонентов должен обладать сертифицированными общесистемными параметрами домена: большим простым числом P_j (модуль вычислений) и первообразным корнем θ_ν.

Абонент А $\qquad\qquad$ Абонент В

$$Y_A = \theta_\nu^{X_A}\left(\mathrm{mod}P_i\right) \qquad\qquad Y_B = \theta_\nu^{X_B}\left(\mathrm{mod}P_j\right)$$

$$Y_A \rightarrow$$

$$\leftarrow Y_B$$

$$K_{AB} = Y_B^{X_A}\left(\mathrm{mod}P_j\right) = \theta_\nu^{X_B X_A}\left(\mathrm{mod}P_j\right) \qquad K_{BA} = Y_A^{X_B}\left(\mathrm{mod}P_j\right) = \theta_\nu^{X_A X_B}\left(\mathrm{mod}P_j\right)$$

где:

Y_A, Y_B – открытые ключи абонентов А и В соответственно;

X_A, X_B – личные ключи абонентов А и В соответственно;

$K_{AB} = K_{BA}$ – общий секретный ключ абонентов.

После согласования ключей выполняется шифрование либо при помощи симметричного алгоритма шифрования, либо с помощью шифрующего устройства, выполняется разворачивание ключа до необходимой длины, а затем осуществляется направленное шифрование.

Стойкость метода базируется на сложности решения дискретного логарифма $X_A = \log_{\theta_\nu} Y_B\left(\mathrm{mod}P\right)$ [4].

В связи с разработкой новых методов криптоанализа сложность решения дискретного логарифмического уравнения носит субэкспоненциальный характер. Это является недостатком метода.

Указанные недостатки в значительной мере могут быть устранены за счёт реализации направленного шифрования в группах точек эллиптических кривых.

Для групп точек на эллиптических кривых определена операция сложения $P_1 + P_2 = P_3$ и операция скалярного произведения $P_1 = d \cdot P_2 = P_2 + P_2 + \ldots + P_2$, где суммируется *d* раз точка Р. Эти операции аналогичны операциям умножения и возведения в степень соответственно в поле или кольце. Существуют обратные элементы. Для точки $P = (x, y)$ обратным элементом будет точка $-P = (x, x + y)$. Кроме того, вводится точка бесконечности, которая является нулем аддитивной группы (обозначается О): $P + O = P$ и $P + (-P) = O$.

В табл. 1 показано соответствие между элементами и операциями мультипликативной группы по простому модулю F_p* и группой эллиптических кривых $E(F_q)$ [5].

Таблица 1

Группа	F_p*	$E(F_q)$
Элементы группы	Набор целых чисел {1, 2, ..., *p*–1}	Точки (*x*, *y*), удовлетворяющие уравнению задания эллиптической кривой, плюс точка на бесконечности О.

Продолжение таблицы 1

Операция группы	Мультипликативное умножение по модулю p	Сложение точек на эллиптической кривой
Обозначение	Элементы: g_1, g_2	Элементы: P_1, P_2
	Умножение: $g_1 \times g_2$	Сложение: $P_1 + P_2$
	Возведение в степень: g^k	Умножение точки (называемое также скалярным умножением): kP, где k – целое число
Задача дискретного логарифма	Для заданных $g_1 \in F_p^*$ и $g_2 = g_1^k \bmod p$ найти целое k.	Для заданных $P_1 \in E(F_q)$ и $P_2 = kP_1$ найти целое k.
Задача Диффи-Хеллмана	Для заданных g^{k1}, $g^{k2} \in F_p^*$ найти g^{k1k2}.	Для заданных k_1P, $k_2P \in E(F_q)$ найти k_1k_2P.

Ввиду того, что в группе точек эллиптической кривой операция скалярного умножения эквивалентна операции возведения в степень, она может быть использована для реализации направленного шифрования. Рассмотрим основные схемы направленного шифрования.

II Простая схема шифрования с использованием аппарата эллиптических кривых [5]

Необходимыми условиями для реализации простой схемы шифрования с использованием аппарата эллиптических кривых является набор ЕС параметров *q, a, b, G, n* и *h*, а также хеш-функция вместе с функцией генерирования ключей, где $q = p$ или $q = 2^m$ – порядок поля, *a* и *b* – коэффициенты эллиптической кривой, *G* – базовая точка, *n* – порядок базовой точки на эллиптической кривой, *h* – кофактор.

Схема шифрования определяется следующим образом.

2.1. Алгоритм зашифрования данных.

Входные данные. Входными данными для преобразования шифрования являются:

1. Битовая строка шифруемых данных M_i длиной l_M.
2. Открытый ключ Q_r, получателя зашифрованных данных.
3. Битовая строка дополнительных данных *д_д*, совместно используемая отправителем и получателем (является необязательной компонентой).

Открытый ключ Q_r должен соответствовать параметрам эллиптической кривой *q, a, b, G, n, h* и быть подлинным.

Для выполнения зашифрования необходимо использовать примитив (модуль) генерирования пар ключей, Диффи-Хеллмана, и функции генерирования ключей на основе хеш-функции, например, SHA-1.

Зашифрование битовой строки M_i выполняется следующим образом:

1. Сгенерировать динамическую (сеансовую) пару ключей (d_e,Q_e), соответствующую ЕС с параметрами *q, a, b, G, n* и *h*, используя примитив генерирования пар ключей, где d_e – личный ключ, Q_e – открытый ключ.
2. Преобразовать Q_e в битовую строку *QE*.
3. Используя примитив Диффи-Хеллмана, выработать из d_e и Q_r общий секрет.
4. Преобразовать общий секрет $z \in F_q$ в битовую строку *Z*.
5. Используя общий секрет и дополнительные данные (необязательно), сгенерировать ключ зашифрования K^3 длиной $l_{K3} = l_M$.
6. Зашифровать открытые данные M_i, используя ключ зашифрования, $C_i = M_i \oplus K_i^з$.

Выходные данные. Битовая строка открытого ключа *QE* и строка C_i как зашифрованные данные.

2.2. Алгоритм расшифрования.

Преобразование расшифрования должно выполняться следующим образом.

Входные данные: Входными данными для преобразования расшифрования являются:

1. Битовая строка $QE'||C_i'$, заданная как открытый ключ отправителя и зашифрованная битовая строка.
2. Личный ключ d_r, принадлежащий получателю зашифрованных данных C_i.
3. Битовая строка данных *д_д*, совместно используемые отправителем и получателем (необязательно).

Личный ключ d_r должен быть сгенерирован с помощью примитива генерирования пар ключей получателем лично.

При выполнении преобразования расшифрования используется модуль подтверждения подлинности открытого ключа, модуль Диффи-Хеллмана и функции генерирования ключей.

Расшифрование производится следующим образом.

1. Проверить подлинность динамического (сеансового) открытого ключа Q_e'.
2. Используя примитив Диффи-Хеллмана вычислить на основе d_r и Q_e' значение общего секрета $z \in F_q$.
3. Преобразовать $z \in F_q$ в битовую строку Z.
4. Сгенерировать из Z и из дополнительных данных ключевые данные – ключ расшифрования K^p длиной l_{Kp}.
5. Расшифровать криптограмму C_i' по правилу $M_i = C_i' \oplus K_i^p$ (расшифрованные данные = зашифрованные данные'$\oplus$ ключ расшифрования).

Выходные данные: расшифрованные данные M_i'.

Схема, поясняющая процедуры зашифрования и расшифрования, приведена на рис. 1.

Приведенная схема предназначена для обеспечения защиты от пассивных вторжений или вторжений типа «выбранный открытый текст», в которых злоумышленник пытается скомпрометировать схему, используя только знание открытого ключа объекта.

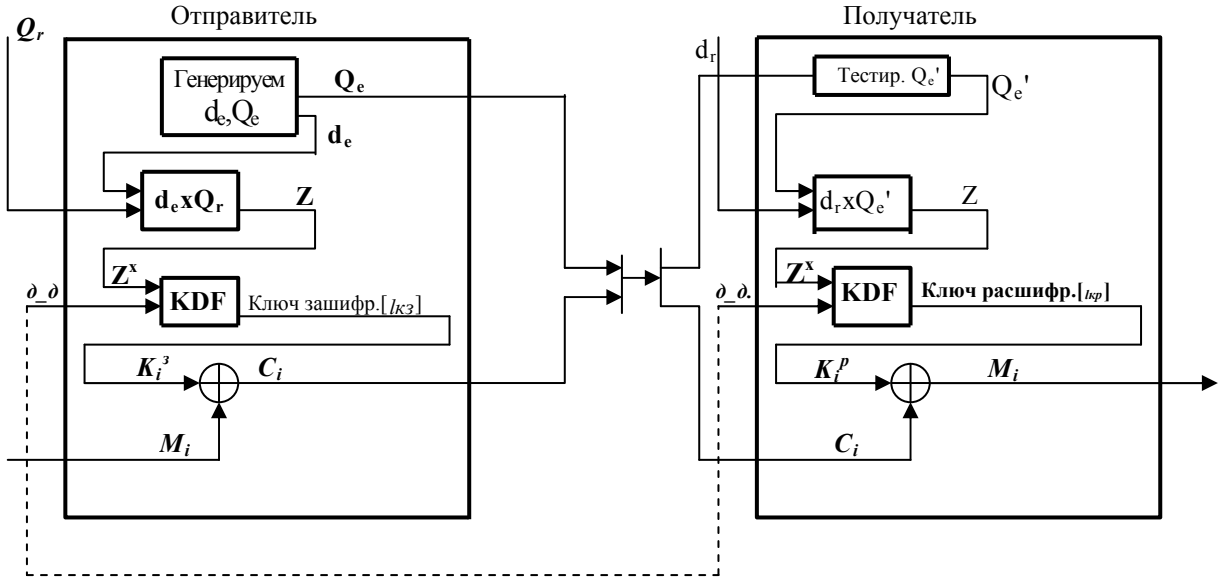

Рисунок 1 – Схемы выполнения процедур зашифрования и расшифрования при использовании аппарата эллиптических кривых

Проведенный анализ показал, что более высокий уровень стойкости может быть обеспечен при использовании усиленной схемы направленного шифрования.

III Усиленная схема направленного шифрования с использованием эллиптических кривых [5]

При использовании усиленной схемы направленного шифрования в группах точек эллиптических кривых необходимо знать параметры *q, a, b, G, n* и *h*, а также выбрать хеш-функцию и функцию генерирования ключей. Кроме того, объекты, использующие схему, должны согласованно использовать схему вычисления кода аутентификации – MAC.

3.1. Преобразование зашифрования.

Зашифрование выполняется следующим образом (рис. 2):

Входные данные. Входными данными для преобразования шифрования являются:

1. Битовая строка шифруемых данных M_i длиной l_M.
2. Открытый ключ Q_r, принадлежащий получателю.

3. Битовые строки дополнительных данных ∂_∂_1 и ∂_∂_2, совместно используемые отправителем и получателем (необязательно).

Открытый ключ Q_r должен соответствовать параметрам домена *q, a, b, G, n,* и *h*, и быть целостным и подлинным.

При зашифровании используются: примитив генерирования пар ключей, примитив Диффи-Хеллмана, преобразование вычисления контрольной суммы, установленное MAC схемой, и функция генерирования ключей.

Зашифрование битовой строки M_i осуществляется следующим образом:

1. Генерируется динамическая (сеансовая) пара ключей (d_e, Q_e), с использованием параметров эллиптической кривой *q, a, b, G, n* и *h*.

2. Преобразуется Q_e в битовую строку *QE*.

3. На основе d_e и Q_r вычисляется значение общего секрета $z \in F_q$.

4. Значение общего секрета $z \in F_q$ преобразовать в битовую строку *Z*.

5. Из *Z* формируются ключевые данные длиной *lкз+lкм*, где *lкз* – длина ключа зашифрования, *lкм* – длина MAC ключа. Ключевые данные делятся на ключ зашифрования $K^з$ длиной *lкз* и MAC ключ $K^м$ длиной *lкм*, т. е. ключевые данные = ключ зашифрования||мак ключ.

6. Зашифровать данные по правилу как $C_i = M_i \oplus K_i^з$.

7. Вычислить контрольную сумму *KC* для битовой строки $C_i||[\partial\_\partial_2]$, используя $K^м$ и одинаковые преобразования вычисления контрольной суммы.

Выходные данные. Битовая строка *QE||C||KC*.

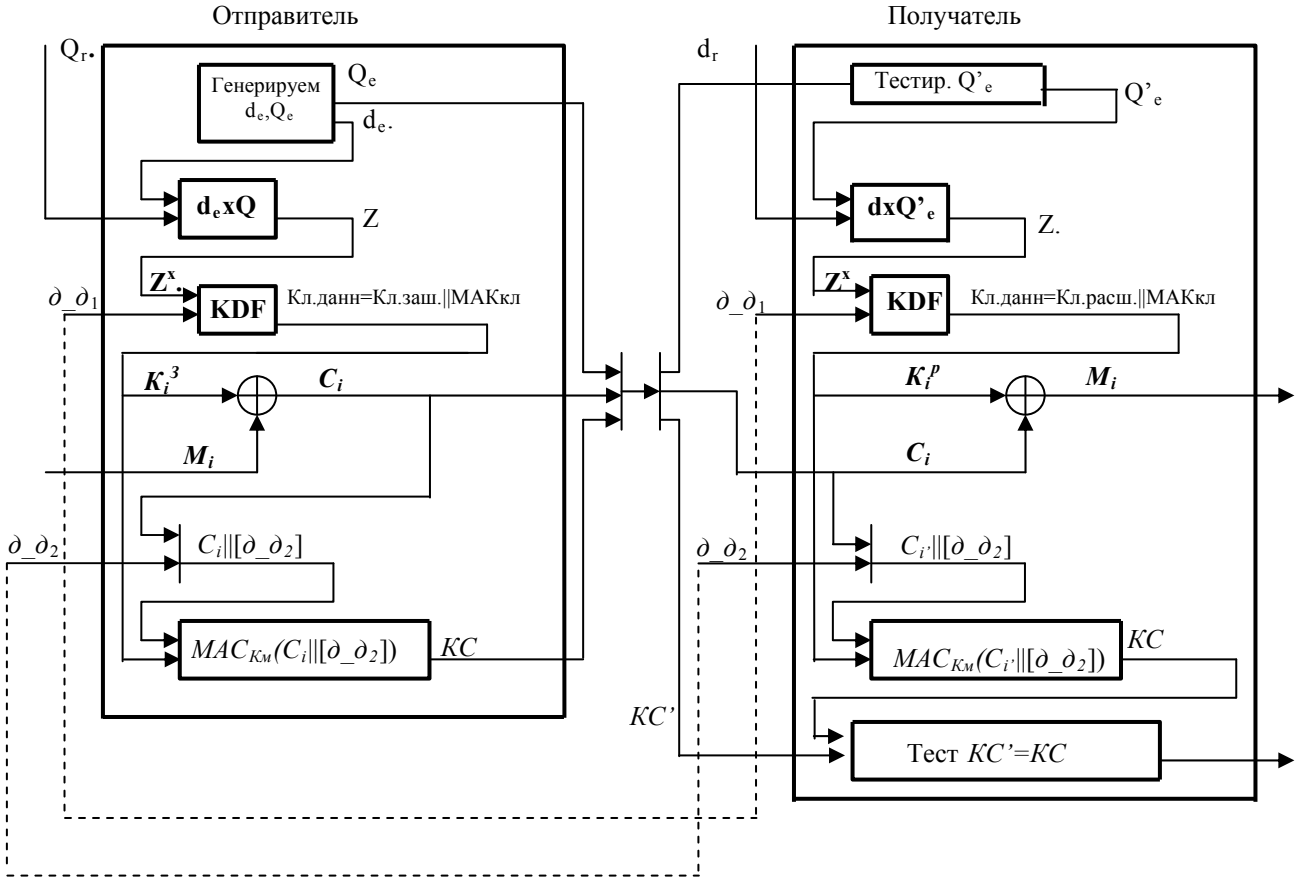

Рисунок 2 – Схемы выполнения усиленных процедур зашифрования и расшифрования в группах на эллиптических кривых

3.2 Преобразование расшифрования.

Преобразование расшифрования должно быть выполнено следующим образом.

Входные данные. Входные данные для преобразования расшифрования.

1. Битовая строка $QE'\|C'\|KC'$, задаваемая как зашифрованная битовая строка.
2. Личный ключ d_r, принадлежащий получателю.
3. Битовые строки дополнительных данных ∂_∂_1 и ∂_∂_2, совместно используемые отправителем и получателем (необязательно).

Личный ключ d_r должен быть генерирован с помощью примитива генерирования пар ключей.

При преобразовании расшифрования используется примитив подтверждения подлинности открытого ключа, примитив Диффи-Хеллмана и преобразование теговой проверки установленной MAC схемы и функции генерирования ключей.

Расшифрование битовой строки $QE'\|C'\|KC'$, состоящей из заданной точки эллиптической кривой Q_e', битовой строки зашифрованных данных длиной l_M и битовой строки KC' соответствующей длины, выполняется в следующем порядке:

1. С использованием примитива подтверждения подлинности открытого ключа проверяется подлинность динамического (сеансового) открытого ключа Q_e'.
2. С использованием d_r и Q_e' вычисляется значение общего секрета $z \in F_q$.
6. $z \in F_q$ преобразовывается в битовую строку Z.
7. Из Z формируются ключевые данные длиной $lкз+lкм$, где $lкз$ – длина ключа зашифрования, $lкм$ – длина MAC ключа. Ключевые данные делятся на ключ зашифрования $K^з$ длиной $lкз$ и MAC ключ $K^м$ длиной $lкм$, т. е. ключевые данные = ключ зашифрования||мак ключ.
8. Расшифровывается криптограмму C_i' по правилу $M_i = C_i' \oplus K_i^p$ (расшифрованные данные = зашифрованные данные'$\oplus$ ключ расшифрования).
9. Используя преобразование проверки контрольной суммы установленной MAC схемы, выполняется проверка, является ли KC' контрольной суммой для $C_i\|[\partial\_\partial_2]$ на ключе $K^м$.

Выходные данные: расшифрованные данные M_i' как результат расшифрования $QE'\|C'\|KC'$.

Описанная усиленная схема обеспечивает защиту от вторжений типа «выбранный открытый текст» и «выбранный криптотекст», при которых злоумышленник использует знание открытого ключа объекта и, кроме того, дополнительно пытается использовать знания, полученные путем перехвата некоторого расшифрованного криптотекста.

IV Анализ схем, условия их применения

Таким образом, усиленная схема направленного шифрования на эллиптической кривой, является более предпочтительной, так как она обеспечивает контроль целостности передаваемого зашифрованного текста. Простая схема шифрования (рис. 1) может использоваться только тогда, когда протокол и канал передачи данных гарантируют неизменяемость передаваемой информации.

По сравнению со схемами RSA и Диффи-Хеллмана схема на эллиптических кривых обладает рядом преимуществ.

Математический аппарат групп точек на эллиптических кривых над полем Галуа обеспечивает значительно более высокую стойкость. Стойкость в зависимости от метода криптоанализа определяется несколькими соотношениями [6]:

- Метод λ-Полларда. Сложность криптоанализа $I_\lambda = 2\sqrt{n}$;
- Метод ρ-Полларда. Сложность криптоанализа $I_\rho = \sqrt{\frac{\pi n}{2}}$;
- Метод ρ-Полларда оптимальный. Сложность криптоанализа $I_\rho = \sqrt{\frac{\pi n}{4}}$.

В связи с тем, что при использовании групп точек стойкость к криптоанализу достаточно высока, появляется возможность использовать модули преобразования меньших размеров, чем при преобразованиях в полях и кольцах. (Как показывает анализ для эффективной защиты в данный момент вполне достаточно размера модуля от 2^{192} и более.) Указанное позволяет ускорить процесс вычислений (криптографических преобразований). Кроме того, для вычислений может использоваться проективное представление (базис),

применение которого позволяет ускорить вычисления. Значения времени зашифрования и расшифрования на компьютере с процессором К6-233 приведены в табл. 1.

Таблица 1 – Время выполнения процедур зашифрования для данных разной длины и для модулей преобразования разной длины.

M		191	409	191	409
L_k		190	408	190	408
$L_д$		100кБайт	100кБайт	100Байт	100Байт
t,c	Обычная схема	0,5	2,98	0,44	2,91
	Усиленная схема	0,5	3,57	0,44	3,51

При рассмотрении данных таблицы необходимо учесть, что большинство времени выполнения процедур уходит на генерацию общего секрета и ключа. Конечно, время, затрачиваемое на выполнение зашифрования при модуле преобразования 409 бит, достаточно высоко, но при этом необходимо учитывать, что увеличение размера шифруемого текста не приведет к значительному увеличению суммарного времени шифрования (время, затрачиваемое на зашифрование 100 байт на 0,06 секунды меньше, чем время, затрачиваемое на зашифрование 100 кБайт). Кроме того, модуль преобразования 409 бит является слишком большим. При нынешнем развитии средств вычислительной техники и математическом аппарате криптоанализа при шифровании не требуется использования модулей такой длины. Заметим, что операции вычисления ключевой пары d_e и Q_e, а также вычисления общего секрета Z можно производить либо предварительно и затем хранить их соответствующим образом, либо возлагать на специальный сопроцессор. В этом случае скорость шифрования может быть увеличена на несколько порядков.

Заключение

Следует ожидать, что в ближайшее время в качестве направленного шифра будут использоваться алгоритмы (схемы), реализованные в группах точек на эллиптической кривой. Их использование позволяет с одной стороны обеспечить необходимый уровень стойкости, с другой – уменьшить сложность, т. е. повысить скорость преобразований.

Литература: 1. X9.62-1998 Public Key Cryptography For The Financial Services Industry:The Elliptic Curve Digital Signature Algorithm (ECDSA). 2. Стандарт ISO 11166 3. И. Д. Горбенко, П. В. Колесников Оценка стойкости RSA систем, в которых открытые ключи или параметры являются личными.: Радиотехника № 119. 2001 г. 4. X9.42 – 1998, Public Key Cryptography for The Financial Service Industry : Agreement of Symmetric Keys on Using Diffie-Hellman and MQV Algorithms. 5. X9.63-199x Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. 6. И. Д. Горбенко, С. И. Збитнев, А. А. Поляков Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда.: Радиотехника № 119. 2001 г.

УДК 638.235.231

ИСПОЛЬЗОВАНИЕ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ НА КОМПАКТ-ДИСКЕ ОТ НЕЛЕГАЛЬНОГО КОПИРОВАНИЯ И ТИРАЖИРОВАНИЯ

Павел Ткачев, Александр Синицкий, Павел Хлызов, Владимир Горчаков, Сергей Карловский

Научно-информационное предприятие "Виа 4С"

Аннотация: **Приводятся методы защиты информации, которая находится на компакт-диске, от нелегального копирования и тиражирования.**

Summary: **Compact disk unauthorized cloning protection methods are observed. Experemental results are taken and discussed.**

Ключевые слова: **Защита информации, компакт-диск, субканалы, тиражирование, TAO, SAO, RAW, несанкционированное копирование.**