УДК 681.3

НОВЫЕ ТЕХНОЛОГИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Червяков Н.И., Головко А.Н.

В статье рассмотрена технология построения криптосистемы, основанной на перспективных эллиптических кривых с представлением и обработкой информации в системе остаточных классов. Предложенный подход позволяет обеспечить высокую скорость и надежность шифрования информации.

В 1985 г. Н. Коблиц и В.С. Миллер предложили использовать эллиптические кривые в конечных полях для создания криптосистем с открытым ключом, после чего началось бурное развитие нового направления, названного эллиптической криптографией. Криптография на эллиптических кривых использует проблему дискретного логарифмирования, но в ней нет определения гладкости, поэтому для криптоанализа не применимы быстрые алгоритмы взлома, как кривые Ленстра, квадратичное решето и решето числового поля, но возможно применение довольно медленных методов Полларда. Следствием этого является применение более коротких ключей шифрования для обеспечения гарантированной стойкости криптосистемы [1].

В соответствии с ГОСТ Р 34.10-2001 эллиптической кривой E (рис.1), определенной над конечным полем F_p, называется множество точек $P(x, y)$ и точки O, называемой бесконечно удаленной точкой (рис. 2), удовлетворяющих тождеству

$$y^2 = x^3 + ax + b (\mathrm{mod} p > 3),\ a, b \in [0, p-1], \quad (1)$$

где a, b - параметры эллиптической кривой, задаваемые дискриминантом

$$\Delta E = 4a^3 + 27b^2 \neq 0. \quad (2)$$

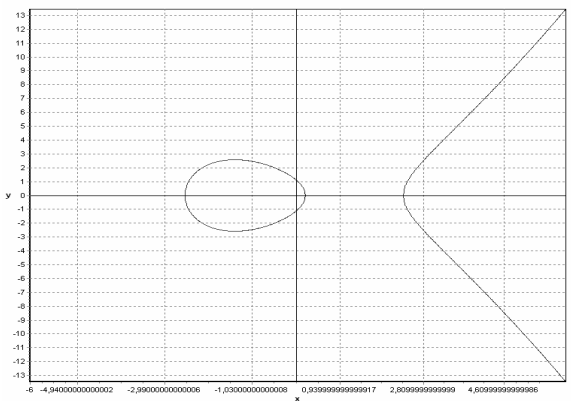

Рис. 1. Эллиптическая кривая $Y^2 = X^3 - 6X + 5$

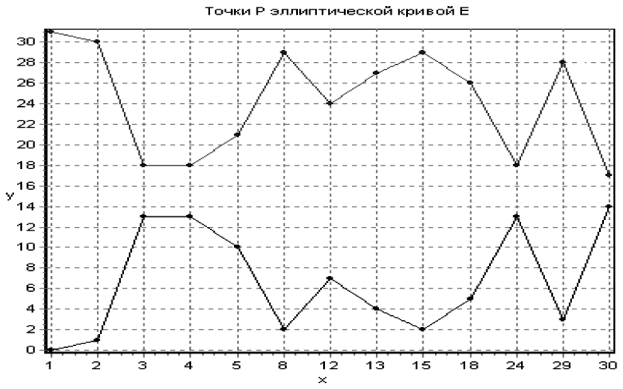

Рис. 2. Эллиптическая кривая
$Y^2 = X^3 - 6X + 5 (\mathrm{mod}\ 31)$

Базовым процессом шифрования на эллиптической кривой является скалярное умножение точки P эллиптической кривой E на константу k и получение точки kP. Этот процесс играет ту же роль, что и операция возведения в степень в криптосистемах RSA и Эль-Гамаля, и может осуществляться в соответствии с математическими определениями стандарта как [2]

$$kP = P + P + P + ... + P = \sum_{i=1}^{k} P, \quad (3)$$

при этом алгоритм сложения и удвоения точек на эллиптической кривой, лежащий в основе (3), имеет следующий вид [2].

1. Начало.
2. Вход алгоритма: коэффициент a эллиптической кривой вида $E: Y^2 = X^3 + aX + b$, точки $P = (x_1, y_1)$ (или $P=O$) и $Q = (x_2, y_2)$ (или $Q = O$).
3. Выход алгоритма: $R = P + Q$.
4. Если $P = O$, то $R = Q$.
5. Если $Q = O$, то $R = P$.
6. Если $P = -Q$, то $R = O$.
7. Если $x_1 \neq x_2$, то вычислить

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, x_3 = \lambda^2 - x_1 - x_2,$$

8. Вернуть $R = (x_3, -y_1 + \lambda (x_1 - x_3))$,
9. Иначе принять $x = x_1, y = y_1$,
10. Вычислить $\lambda = \frac{3x^2 + a}{2y}, x_3 = \lambda^2 - 2x,$

11. Вернуть $2P = (x_3, -y + \lambda(x - x_3))$.

Используя свойство эллиптической кривой приводить константы, на которые умножаются ее точки по модулю ее порядка, возможна организация уникального протокола передачи сообщений между абонентами *A* и *B* по открытому каналу связи без предварительной передачи какой бы то ни было ключевой информации.

Пусть *E* – эллиптическая кривая порядка *N*, *e* – целое число, $1 < e < N$, взаимно простое с *N*. Используя свойство обратных мультипликативных величин, найдем

$$d \equiv e^{-1} (\mathrm{mod}\, N). \quad (4)$$

По определению сравнимости по модулю имеем $e \cdot d = jN + 1$. Поэтому для любой точки *P* эллиптической кривой *E* порядка *N*

$$(d \cdot e)P = (j \cdot N + 1)P =$$
$$= (j \cdot N)P + P = jO + P = O + P = P,$$

то есть выполняется тождество

$$(e \cdot d)P = P. \quad (5)$$

Используя *e* и *d* и любую точку *P* эллиптической кривой можно вычислить $Q = eP$, $\mathrm{R} = dQ$. Очевидно, что $\mathrm{R} = P$.

Для организации протокола шифрования данных открытыми параметрами системы назначаются уравнение эллиптической кривой и поле, над которым она задается. Этими параметрами определяется группа точек эллиптической кривой и ее порядок, который также публикуется как открытый ключ, либо он может быть вычислен по известному уравнению.

После согласования открытых ключей абонент *A* выбирает как ключ шифрования число $k_{ША}$, взаимно простое с порядком кривой *N* и вычисляет ключ расшифрования $k_{РА}$ как число обратно к $k_{ША}$. Аналогично, абонент *B* генерирует свои ключи шифрования и расшифрования $k_{ШВ}$ и $k_{РВ}$. Затем абонент *A* помещает свое сообщение *M* в точку P_1 высокого порядка установленной эллиптической кривой, и умножая ее на свой ключ шифрования, получает точку P_2

$$P_2 = k_{ША} P_1 . \quad (6)$$

Эту точку абонент *A* посылает по незащищенному каналу абоненту *B*.

Абонент *B* вычисляет

$$P_3 = k_{ШВ} P_2 \quad (7)$$

и посылает результат абоненту *A*, который расшифрование на своем ключе

$$P_4 = k_{РА} P_3 \quad (8)$$

и возвращает полученную точку абоненту *B*.

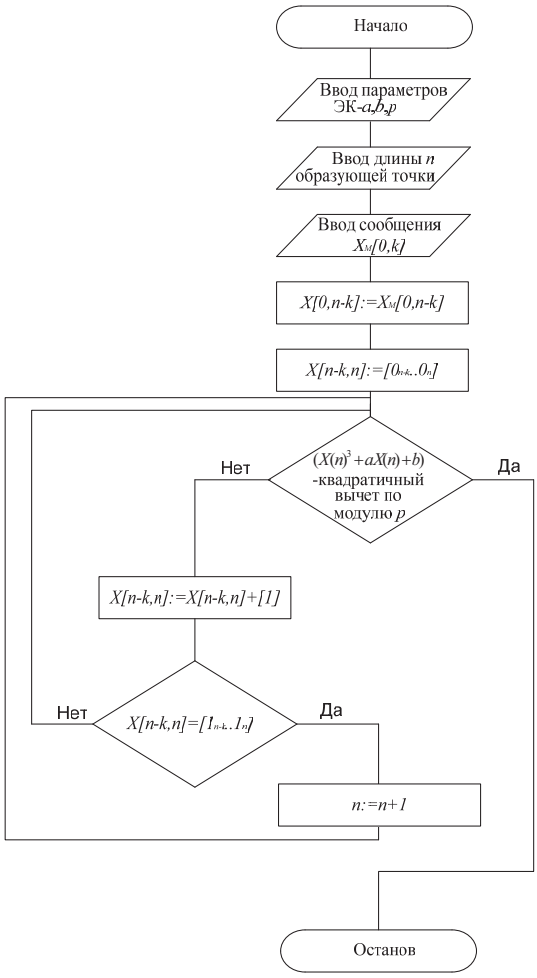

Рис. 3. Блок-схема алгоритма размещения сообщения в точке эллиптической кривой

Последнему остается расшифровать сообщение на своем ключе расшифрования и получить исходную точку, в которую вложено сообщение

$$P_1 = P_5 = k_{РВ} P_4 . \quad (9)$$

Действительно, с учетом коммутативности и ассоциативности операции группы

$$k_{РВ} P_4 = (k_{РВ} \cdot k_{РА}) P_3 = (k_{РВ} \cdot k_{РА} \cdot k_{ШВ}) P_2 =$$
$$= (k_{РВ} \cdot k_{РА} \cdot k_{ШВ} \cdot k_{ША}) P_1 =$$
$$= (k_{ША} \cdot k_{РА}) \cdot (k_{ШВ} \cdot k_{РВ}) P_1 = P_1 .$$

Таким образом, для организации такого протокола передачи и приема зашифрованных сообщений потребуется только опубликованные параметры эллиптической кривой и не требуется обмена какими-либо секретными параметрами.

При реализации этого протокола возникает проблема размещения исходного сообщения абонента в точке эллиптической кривой. Эта проблема тесно связана с теорией квадратичных вычетов, которая утверждает, что на множестве точек эллиптической кривой (1), которое можно представить как

$$E: y = \sqrt{(x^3 + ax + b) + ip}\ ,\ p > 2\ \ i = 0,1... \quad (10)$$

поровну вычетов и невычетов. Иными словами, не для любого открытого двоичного сообщения x выражение (1) имеет решение.

Для предотвращения конфликта процесса шифрования предлагается алгоритм, представленный на рис. 3.

Недостатком криптосистемы на эллиптических кривых, присущим всей криптографии с открытым ключом, является низкая скорость шифрования при реализации на существующих вычислительных средствах (ВС).

Таблица 1. Скорость шифрования ВС

Вид ВС (ключ 163 бита)	P-IV/ 2,4GHz	ULTRA SparcII 400 MHz	Strong ARM 200MHz
Скорость шифрования (кбит/с)	89,37	26,09	6,95

Одним из наиболее перспективных путей повышения производительности средств криптографической обработки информации является внедрение новых высокоэффективных параллельных структур, ориентированных на широкое использование ПЛИС. Одним из приоритетных направлений в развитии параллельных вычислительных средств является применение системы остаточных классов (СОК).

В СОК, имея набор взаимно-простых чисел или модулей $p_1, p_2, \ldots, p_n$, любое число X представляется в виде кортежа небольших вычетов [5]

$$\left(x_1, x_2, \ldots, x_n\right),\ x_i = X \bmod p_i\ ,\ i = 1,2,...,n\ . \quad (11)$$

Такое представление возможно и определяется Китайской теоремой об остатках: если $X \in Z$, $p \in Z$, $p \neq 0$, то существует единственные $m \in Z$ и $X \in Z$, такие, что

$$X = m \cdot p + \alpha\ ,\ 0 \le \alpha \le |p|\ ,\ m = \left[\frac{A}{p}\right]. \quad (12)$$

При этом число X не должно во избежание ошибки превосходить диапазон представления данных, а диапазон представления данных должен удовлетворять размерности выбранного конечного поля $F(p)$, в котором ведутся криптографические преобразования

$$P = \prod_{i=1}^{n} p_i = F(p)\ . \quad (13)$$

Сложение и умножение двух любых кортежей $X = \left(x_1, x_2, \ldots, x_n\right)$ и $Y = \left(y_1, y_2, \ldots, y_n\right)$ в СОК производится по правилам

$$X + Y = \left(\left|x_1 + y_1\right|_{p_1}, \left|x_2 + y_2\right|_{p_2}, \ldots, \left|x_n + y_n\right|_{p_n}\right) \quad (14)$$

$$X \times Y = \left(\left|x_1 \times y_1\right|_{p_1}, \left|x_2 \times y_2\right|_{p_2}, \ldots, \left|x_n \times y_n\right|_{p_n}\right) \quad (15)$$

Благодаря параллелизму СОК, вычислительное устройство разбивается на вычислительные каналы по количеству модулей принятой системы оснований. Обеспечиваемая при этом регулярность модулярных вычислительных устройств идеально согласуется с принципами конвейерной обработки информации.

Основными традиционными элементами специализированных средств модулярной обработки являются:

- модулярные вычислительные каналы, количество которых определяется выбранной для вычислений системой остаточных классов;
- устройство согласования позиционных вычислительных устройств с модулярным вычислительным устройством;
- устройство согласования модулярного вычислительного устройства с позиционным вычислительным устройством;
- устройство обнаружения и коррекции ошибок;
- устройство выполнения немодульных операций масштабирования и деления.

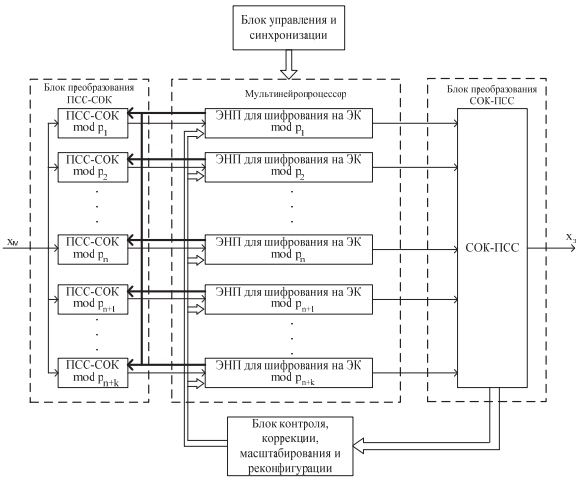

Рис. 4. Обобщенная вычислительная модель криптографического модулярного нейропроцессора

Традиционный подход к реализации модулярных вычислений позволяет синтезировать общую параллельную структуру криптографического модулярного нейропроцессора на эллиптических кривых для реализации на ПЛИС, которая представлена на рис. 4.

Предложенный криптографический модулярный нейропроцессор для шифрования информации с помощью эллиптических кривых представляет собой векторную архитектуру ЭВМ с одним потоком команд и многими потоками данных (SIMD) и с сокращенным набором команд (RISC) процессора в СОК. Сокращенный набор команд обеспечивает минимизацию сложности блока управления и синхронизации. Простота конечной арифметики над кольцами делает выгодным данную стратегию и обеспечивает короткое выполнение тактовых команд.

Предложенная модель содержит:

- мультинейропроцессор, содержащий $n+k$ элементарных нейропроцессоров по модулям $p_i\,(i=1,2,\ldots,n+k)$, реализующий вычислительные модели основных операций шифрования на эллиптических кривых – размещения исходного сообщения в точке кривой [2] и скалярного умножения на константу – секретный ключ k [1];
- блок преобразования ПСС-СОК, состоящий из $n + k$ нейронных сетей для преобразования ПСС – СОК;
- блок преобразования СОК-ПСС, включающий в себя нейронную сеть для преобразования СОК – ПСС;
- блок контроля, коррекции, масштабирования и реконфигурации, состоящий из нейронной сети для обнаружения, локализации и исправления ошибок, нейронных сетей для масштабирования.
- блок управления и синхронизации.

Общее входное сообщение x_M преобразуется в координату x образующей точки P, а затем в двоичную СОК нейронными сетями преобразования ПСС – СОК, остаточные цифры

$$\left(\left|x_M\right|_{p_1},\left|x_M\right|_{p_2},\ldots,\left|x_M\right|_{p_n},\ldots,\left|x_M\right|_{p_{n+k}}\right)$$

обрабатываются параллельно мультинейропроцессором в соответствии с заданной программой, выходные сигналы нейропроцессоров

$$\left(\left|x_з\right|_{p_1},\left|x_з\right|_{p_2},\ldots,\left|x_з\right|_{p_n},\ldots,\left|x_з\right|_{p_{n+k}}\right)$$

преобразуются в выходные сигналы $x_з$ нейронной сетью преобразования СОК – ПСС.

Зашифрованное сообщение $x_з$ выдается в канал связи и принимается на приемной стороне аналогичным криптографическим модулярным нейропроцессором, где в соответствии с заданным протоколом осуществляется расшифрование. На приемной стороне может возникнуть следующая ситуация. При расшифровании сообщения необходимо знать в какой точке эллиптической кривой, положительной или отрицательной, находится $x_з$. Вместо того, чтобы передавать получателю обе координаты точки, пересылается только $x_з$ и один бит, служащий сигналом выбора y для нейронной сети для определения координат точек на приемной стороне. Данный подход позволяет вдвое сократить трафик в канале связи и из двух точек $P(x, y)$ и $-P(x, -y)$ на приемной стороне выбрать правильную.

Вычислительное ядро (мультинейропроцессор) может быть выполнено в виде отдельных независимых элементарных нейропроцессоров (ЭНП), выполняющих параллельно-конвейерное криптографическое шифрование на заданной эллиптической кривой по $\bmod p_i$, где $i=1;\ 2\ldots n+2$. В общем случае размерность матриц нейропроцессоров определяется динамическим диапазоном и величинами оснований СОК.

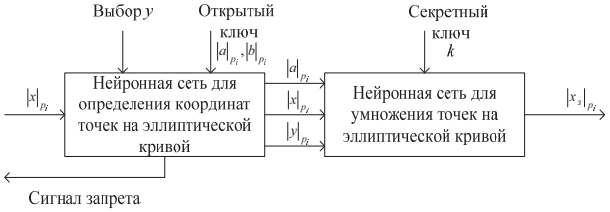

Рис. 5. Структурная схема элементарного нейропроцессора для шифрования на эллиптических кривых

Вычислительный канал по модулю p_i включает в себя нейронную сеть для определения координат точек на эллиптической кривой [2], нейронную сеть для умножения координат точек кривой [1]. Если в процессе вычислений нейронной сетью для определения координат точки i-остаток по модулю окажется квадратичным невычетом, то процесс шифрования считается остановленным и выдается сигнал запрета, адресованный всем преобразователям ПСС-СОК с целью реконфигурации и изменения образующей точки эллиптической кривой в соответствии с алгоритмом на рис. 3. Если конфликта не произошло и все остатки являются вычетами, то нейронная сеть для умножения точек осуществляет зашифрование остаточной информации на основе заданного k.

В случае переполнения динамического диапазона для правильного окончания вычислений необходимо промасштабировать результат вычислений, для этого блок контроля, коррекции ошибок, масштабирования и реконфигурации содержит нейронную сеть для масштабирования модулярных чисел, отличающуюся от известных расширенными функциональными возможностями [4].

Наличие аппаратных средств в системах мультинейропроцессора обуславливает вероятность того, что появляются смягченные и устойчивые отказы, которые разрушают результаты, поэтому такие системы должны обладать отказоустойчивостью.

Традиционный подход к решению задач отказоустойчивости состоит в использовании модульной избыточности. В этой технологии результаты отдельных модулей сравниваются по схеме голосования. Если ошибки не возникают, то выходы точно совпадают, в противном случае, если возникает ошибка, то ошибочный модуль может быть легко идентифицирован и правильный результат будет определен. Модульная избыточность является главной технологией и может быть применена к любой вычислительной задаче. К сожалению, модульная избыточность требует большого количества аппаратных средств (200% для исправления одиночной ошибки). Введенная в нейропроцессор нейронная сеть для обнаружения, локализации и исправления ошибок позволяет обнаружить и исправить любую ошибку с избыточностью 70%, в то время как традиционное аппаратное резервирование требует для этой цели 200%, которое необходимо при полной защите через аппаратную избыточность, при этом защита 90% вычислений обеспечивается корректирующими кодами, а 10% – с использованием более дорогой аппаратной избыточности [3].

Время шифрования *t l*-битного сообщения определяется формулой

$$t = N \cdot \left(t_{COK} + t_x\right) + t_{\text{k}} + t_{ПСС}\,, \qquad (16)$$

где N – число итераций для размещения сообщения в образующей точке, максимальное число определяется разрядностью счетчика в составе преобразователя ПСС-СОК; $t_{сок}$ – время преобразования абсциссы образующей точки в код СОК; t_x – время определения принадлежности абсциссы образующей точки к выбранному уравнению ЭК; t_k – время скалярного умножения полученной точки на ключ k, зависит от длины двоичной записи k; $t_{ПСС}$ – время преобразования СОК-ПСС.

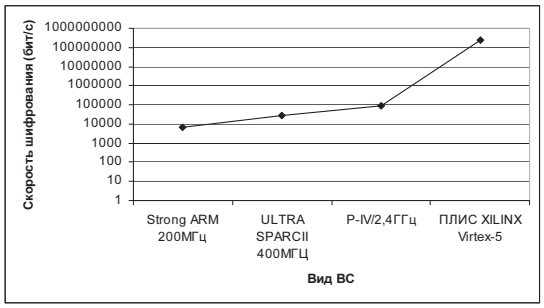

Рис. 6. График сравнительной оценки скорости шифрования для различных ВС

Скорость шифрования криптографического модулярного нейропроцессора определяется в соответствии с выражением

$$V = \frac{X_M}{t}\,. \qquad (17)$$

Оценка средней скорости шифрования на базе ПЛИС XILINX Virtex-5 при использовании 163-битной точки составляет 0,24 Гбит/с.

Таким образом, изложенный подход к организации технологий криптозащиты информации на эллиптических кривых в системе остаточных классов позволяет обеспечить высокую защищенность закрытых сообщений и достаточно высокую скорость шифрования, что делает предложенную модель перспективной для применения в современных ИКТ.

Литература

1. Червяков Н.И., Головко А.Н. Нейронная сеть сложения и удвоения точек на эллиптической кривой // Материалы межвузовской НТК «Перспективы развития средств и комплексов связи. Подготовка специалистов связи». Новочеркасск: НВВКУС. Ч.1. 2007. – С. 203-205.
2. Червяков Н.И, Головко А.Н., Лавриненко А.В., Лавриненко И.Н., Кириевский С.С. Нейронная сеть для определения координат точек на эллиптической кривой // Материалы III МНТК «Инфокоммуникационные технологии в науке, производстве и образовании (Инфоком-3)». Ставрополь: СевКавГТУ. Часть III. 2008. – С. 252-258.
3. Нейронная сеть для обнаружения, локализации и исправления ошибок. Патент РФ 2301442 // Червяков Н.И., Лавриненко И.Н., Сивоплясов Д.В., Дьяченко И.В., Иванов А.В., Головко А.Н. Заявл. 04.05.2005; опубл. 20.06.07, бюл. №17.
4. Нейронная сеть ускоренного масштабирования модулярных чисел // Червяков Н.И., Головко А.Н., Лавриненко А.В., Сляднев В.В.; Заявл. 13. 06. 07; решение о выд. патента РФ от 11.02.09.
5. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Рядов С.А. Модулярные параллельные вычислительные структуры нейропроцессорных систем. М.: Физматлит, 2003. – 288 с.