- при построении нелинейных функций данные функции должны удовлетворять критериям стойкости: быть сбалансированными, обладать высокой нелинейностью, удовлетворять критерию распространения (обладать корреляционным иммунитетом), иметь высокую алгебраическую степень.
- при длине ключа k бит внутреннее состояние генератора (внутренняя память) должно быть не менее $2k$ бит;
- генерируемая гамма шифрующая не должна превышать значения N_{max}, определенного согласно (20);
- каждый бит начального состояния регистра должен являться функцией от нелинейного преобразования всех бит ключа.

Литература: ***1.*** *T. Siegenthaller. Decrypting a class of stream cipher using ciphertext only. IEEE Trans. Comput.,vol. C–34, pp. 81–85, Jan. 1985.* ***2.*** *T. Siegenthaller. Cryptanalysis Representation of Nonlinearly Filtered ML-Sequences. Advances in Cryptology: Proc. Eurocrypt'85, pp. 103–110, Springer-Verlag, 1986.* ***3.*** *W. Meier, O. Staffelbach. Fast correlation attacks on stream ciphers. Journal of Cryptology, vol. I, no. 3, pp. 159–176, 1989.* ***4.*** *R. Forre. A Fast Correlation Attack on Nonlinearly Feedforward Filtered Shift-Register Sequences. Advances in Cryptology: Proc. Eurocrypt'89, pp. 586–595, Springer-Verlag, 1990.* ***5.*** *Michalevich, J. Golic. A Generalized Correlation Attack on a Class of Stream Ciphers Based on the Levenshtein Distance. Journal of Cryptology, 3:201–212, 1991.* ***6.*** *V. Chepyzhov, B. Smeets. On a Fast Correlation Attacks on Certain Stream Ciphers. Advances in Cryptology: Proc. Eurocrypt'91, pp. 176–185, Springer-Verlag, 1991.* ***7.*** *F. Jonsson, T. Johansson. Improved Fast Correlation Attacks on Stream Ciphers via Convolutional Codes. http: //www.it.lth.se./thomas/, 1999.* ***8.*** *F. Jonsson, T. Johansson. Fast Correlation Attacks Based on Turbo Code Techniques. http: //www.it.lth.se./thomas/, 1999.* ***9.*** *F.Jonsson, T. Johansson. Fast Correlation Attacks Through Reconstruction of Linear Polinomials. http: //www.it.lth.se./thomas/, 2000.* ***10.*** *V. Chepyzhov, T. Johansson, B. Smeets. A simple algorithm for fast correlation attacks on stream ciphers. http: //www.it.lth.se./thomas/, 2000.* ***11.*** *S. Babbage. A Space/Time Trade-Off in Exhaustive Search Attacks on Stream Ciphers. Vodafone Ltd, Newbury, UK. 09.04.1996.* ***12.*** *A. Biryukov, A. Shamir. Cryptanalytic Time/Memory/Data tradeoffs for Stream Ciphers. 2000.* ***13.*** *J. D. Golic. On the Security of Nonlinear Filter Generators.* ***14.*** *J. D. Golic. Cryptanalysis of Alleged A5 Stream Cipher. Advances in Cryptology: Proc. Eurocrypt'97, pp. 239–255, Springer-Verlag, 1997.* ***15.*** *E. Biham, O. Dunkelman. Cryptanalysis of the A5/1 GSM Stream Cipher. NES/DOC/TEC/WP3/005/a.* ***16.*** *A. Biryikov, A. Shamir. Real Time Cryptanalysis of the Alleged A5/1 on a PC. 09.09.1999.* ***17.*** *Горбенко И. Д., Потий А. В., Избенко Ю. А., Орлова С. Ю. Анализ схем поточного шифрования, представленных на европейский конкурс Nessie// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 5. – 2002. – С. 92–110.*

УДК 681.3.06

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ХАРАКТЕРИСТИК И ПРИНЦИПОВ ПОСТРОЕНИЯ СТАНДАРТОВ ЭЦП НА СВОЙСТВАХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Анатолий Кочубинский, Александр Шаталов
Малое предприятие "ДИНА"

Анотація: **Розглядаються державні та галузеві стандарти цифрового підпису, які використовують особливості еліптичних кривих. Обгрунтовуються умови необхідності введення більш криптографічно стійких алгоритмів. Робиться порівняльний аналіз прийнятих стандартів ЕЦП з еліптичною криптографією.**
Summary: **They are considered already taken state and branch standards digital signature, using particularities elliptical curves. They are motivated condition to need of the introduction more cryptographic rack algorithm. It is done benchmark analysis taken standard ECS with elliptical cryptography.**
Ключові слова: **Криптографічний захист інформації, цифровий підпис, еліптична криптографія.**

Широкое распространение информационных технологий, которые включают в себя взаимодействие множества абонентов, разнообразной информации и широкого спектра телекоммуникационных услуг, предусматривает развитие средств, дающих возможность гарантировать в должной степени целостность обрабатываемой информации, ее аутентичность и, при необходимости, конфиденциальность. Решить эту задачу в настоящее время возможно только, применяя криптографические алгоритмы вычисления и проверки цифровой подписи и алгоритмы шифрования. Причем в случае, когда в информационном процессе участвует

очень ограниченное число абонентов и коммуникации между ними ограничены, вопросы идентичности и аутентичности можно решить, вычисляя имитовставку, как рекомендует ГОСТ 28147-89. Но здесь есть еще одно ограничение – участники информационного обмена должны полностью доверять друг другу и только таким образом исключить возможность несанкционированной передачи секретного ключа, который по сложному протоколу пересылается всем участникам обмена, и возможность изменения информационной посылки с вычислением на нее новой имитовставки. В случае же большого количества участников информационного взаимодействия и разветвленных связей применение для установления идентичности и аутентичности информационных документов метода вычисления имитовставки крайне сложно и неэффективно из-за крайне сложной организации протоколов рассылки секретных ключей и неэффективности условия "всеобщего и полного" доверия.

Единственный разумный способ добиться корректной реализации процедуры идентификации и аутентификации предоставляют криптографические алгоритмы вычисления и проверки цифровой подписи, основанные на криптографических преобразованиях с несимметричными ключами. Эти алгоритмы идеально подходят для больших информационных сетей, поскольку их применение не связано с предварительным обменом секретной информацией и, следовательно, полностью снимается сложная задача управления секретными ключами. Поэтому не вызывает сомнения, что разработка и принятие в 1994 г. российского стандарта цифровой подписи Р 34.10-94 и связанного с ним стандарта вычисления функции хеширования Р 34.11-94 было своевременным и сыграло и продолжает играть важную роль в решении задач обеспечения целостности информации и подлинности ее происхождения. Упомянутые выше стандарты были адаптированы как стандарты Украины соответственно ГОСТ 34.310-95 и ГОСТ 34.311-95 и действуют в настоящее время.

Действующий стандарт цифровой подписи использует надежные алгоритмы вычисления и проверки цифровой подписи. Его стойкость основана на неимоверной сложности решения так называемой задачи дискретного логарифмирования в мультипликативной группе простого конечного поля большого порядка. Стандарт достаточно прост в реализации и по своим алгоритмическим и криптографическим свойствам находится на уровне аналогичных ныне действующих зарубежных стандартов: национального стандарта США DSS FIPS 186-2 и ряда отраслевых и международных стандартов, использующих алгоритм DSA, закрепленный в стандарте США, например, стандарта ANSI X9.30-1, используемого в банковской сфере, и стандарта ISO/IEC 14888. При сохранении нынешних тенденций развития вычислительной техники и алгоритмической теории он может безопасно использоваться в ответственных применениях, по крайней мере до 2005 г., а в менее ответственных – вплоть до 2010 г. Тем не менее, по нашему мнению, настало время готовить замену этому стандарту. Причин для этого достаточно много и они связаны как с особенностями самого стандарта, так и мировыми тенденциями развития информационных технологий.

Действующий стандарт не лишен недостатков алгоритмического и структурного свойства.

Недостатки алгоритмического характера.

1. Используется неудачный способ генерации основных параметров алгоритма, имеющий тонкие места. Опыт сертификации показывает, что это часто приводит к ошибкам при реализации алгоритма и усложняет процесс сертификации. Этот способ лишает стандарт гибкости в выборе параметров безопасности стандарта.

2. Зафиксированный в стандарте способ генерации параметров приводит к тому, что в настоящее время можно использовать только одно значение размера ключа – 1024 бита. Предусмотренное стандартом значение 512 бит сейчас использовать нельзя по соображениям безопасности. Стандарт не позволяет использовать промежуточные значения, что было бы удобным для многих применений, поскольку от размера ключа зависит скорость выполнения вычислений. В то же время нельзя и увеличить это значение, что, несомненно, потребуется после 2005 г. в ответственных применениях. Устранить этот недостаток без существенной переделки стандарта нельзя.

3. Использован неудачный способ проверки псевдопростоты целых чисел. Несложно построить составное число, которое этим способом будет признано псевдопростым. Эту особенность теоретически можно использовать для компрометации подписи.

Структурные недостатки.

1. Крупный недостаток действующего стандарта – отсутствие нормированного алгоритма генерации секретных постоянного и разовых ключей.

2. Стандарт привязан к конкретной функции хеширования ГОСТ 34.311-95, в которой, как известно, используется стандарт шифрования данных ГОСТ 28147-89. Это усложняет сертификацию реализаций стандарта, удорожает ее и требует приобретения долговременных ключей у уполномоченной организации. По нашему мнению, вычисление функции хеширования должно быть самостоятельным алгоритмом, не имеющим отсылок к другим стандартам.

3. Отсутствует формализация входных и выходных данных, что затрудняет использование стандарта в больших разнородных сетях. В настоящее время стандарт практически используется только в корпоративных сетях, созданных одним разработчиком. Это затрудняет использование цифровой подписи в больших сетях, создаваемых разными разработчиками, и препятствует созданию общенациональной системы использования и сертификации цифровой подписи.

Теперь о причинах необходимости разработки нового стандарта, которые имеют технологический характер и не связаны напрямую с действующим стандартом.

1. Быстрое развитие вычислительной техника и разработка эффективных методов криптоанализа, применимых именно к алгоритмам того типа, который используется в действующем стандарте, потребовали увеличить длину ключа до 1024 бит, а к 2005г. безопасная длина ключа будет не менее 1600 бит. Это усложняет использование стандарта и уменьшает его быстродействие.

2. Алгебраические структуры, которые используются в действующем стандарте, плохо подходят для реализации на микропроцессорах, используемых в смарт-картах. Известно, как широко такие устройства используются в самых разных целях.

3. Для обеспечения долговременной информационной безопасности от маловероятного, но все же возможного, прорыва в теоретической области, который может повлечь полную дискредитацию ныне действующих алгоритмов, желательно иметь алгоритмы, использующие иные теоретические принципы.

Новый стандарт по нашему мнению должен обладать следующими свойствами:

1) обеспечивать очень высокую стойкость и основываться на новых теоретических принципах, исключающих применение существующих эффективных методов криптоанализа;
2) быть гибким в отношении выбора параметров безопасности и достаточно простым в реализации;
3) допускать простую аппаратную реализацию;
4) использовать нормированный, принятый нормативным документом, например ГОСТом, датчик случайных чисел для получения секретных ключей;
5) не быть привязанным к конкретной функции хеширования;
6) обеспечивать однозначное представление входных и выходных данных.

В первую очередь необходимо выбрать алгебраическую структуру, наиболее подходящую для реализации алгоритмов нового стандарта. Мы выбрали группу точек эллиптической кривой над конечным полем характеристики 2. Этот выбор определен как собственным многолетним опытом работы с этим объектом, так и очевидной мировой тенденцией все более широкого внедрения алгоритмов этого типа в криптографические протоколы. Впервые криптографические алгоритмы в таких группах были предложены в 1985 г. Виктором Миллером [1] и Нилом Коблицем [2] и долгое время считались экзотикой, непригодной для практического применения. Вычисление порядка эллиптической кривой казалось очень сложной задачей, поэтому сначала предлагалось использовать специальные виды эллиптических кривых, где эта задача решалась достаточно просто. Впоследствии многие из этих типов кривых оказались непригодными для криптографических применений, например, суперсингулярные кривые. Поэтому очень важным является чисто теоретический результат Р. Схофа [3], из которого следует, что вычисление порядка эллиптической кривой есть задача полиномиальной сложности, т. е. очень простая задача. Вскоре были построены эффективные практические алгоритмы вычисления порядка эллиптических кривых.

Долгое время оставалось неясным, как соотносятся между собой задача дискретного логарифмирования в группе точек эллиптической кривой и аналогичная задача в поле определения кривой. В 1993 г. А. Менезес, Т. Окамото и С. Вэнстон показали, что в принципе первая задача сводится ко второй, но условия сведения легко контролируются и всегда можно выбрать эллиптическую кривую, для которой это сведение не дает субэкспоненциального алгоритма решения задачи дискретного логарифмирования в группе точек эллиптической кривой (знаменитое MOV−condition). Можно считать, что с этого момента началась активная работа в области создания и внедрения практических криптографических алгоритмов с использованием эллиптических кривых. Этому способствовало быстрое развитие микропроцессорной техники, которое потребовало реализации криптографических алгоритмов на этой технике, а существовавшие тогда алгоритмы явно не подходили для этой цели. К настоящему времени эллиптическая криптография достигла такого уровня развития, который позволяет включать эллиптические криптографические алгоритмы в национальные и международные стандарты. Уже приняты стандарты ANSI X9.62 и X9.63 (банковская сфера, 1999 г.), национальный стандарт США FIPS 186-2 (2000 г.) и стандарт IEEE P1363-2000. Рассматривается включение криптографических алгоритмов на эллиптических кривых в стандарты ISO/IEC 14888 (цифровая подпись), ISO/IEC 9796 (цифровая подпись с восстановлением сообщения), ISI/IEC 14946 (цифровая подпись, направленное шифрование, транспортировка ключей и установление общего ключа). Известно, что ведутся работы по включению алгоритмов эллиптического типа в целый ряд отраслевых стандартов, в том числе стандартов обеспечения безопасности в сети Интернет.

Вся совокупность известных теоретических результатов и собственный опыт работы с эллиптическими кривыми убедительно показывают, что эллиптические кривые дают уникальные возможности для построения надежных и эффективных криптографических алгоритмов. Основные достоинства групп, связанных с эллиптическими кривыми, таковы.

1. Относительная простота вычисления параметров этих групп.
2. Отсутствие эффективных алгоритмов решения задачи дискретного логарифмирования в этих группах и крайне малая вероятность их появления в будущем. Это позволяет использовать ключи небольшой длины с гарантией очень высокой стойкости. Например, эллиптическая криптосистема с ключом длиной 160 бит эквивалентна по стойкости алгоритму действующего стандарта, а при ключе длиной 320 бит она эквивалентна по стойкости обычному алгоритму с ключом длиной 5200 бит.
3. Если вычисление параметров группы (прежде всего, самой эллиптической кривой и ее порядка) связано с определенными техническими сложностями, то сами вычисления в этих группах очень эффективны и легко реализуются в аппаратном виде.
4. Очень широкая возможность выбора эллиптических кривых и связанных с ними групп при фиксированном базовом поле. В обычных алгоритмах такого выбора практически нет.
5. Наличие ясных и простых необходимых и достаточных условий, выполнение которых исключает применение известных специфических для эллиптических кривых методов криптоанализа.

Поэтому государственный стандарт Украины разработан на основе криптографических преобразований на эллиптических кривых. Для обеспечения высокой криптографической стойкости цифровой подписи эллиптические кривые и поля их определения должны удовлетворять жестким требованиям. Такие требования выработаны на основе анализа известных методов решения задачи дискретного логарифмирования на эллиптических кривых. Созданы эффективные вычислительные алгоритмы генерации эллиптических кривых с заданными криптографическими свойствами.

Постараемся сделать некоторый сравнительный анализ современных алгоритмов вычисления и проверки ЭЦП, которые основаны на задаче дискретного логарифмирования в группе точек эллиптической кривой.

В настоящее время стойкость всех несимметричных криптографических преобразований, которые практически применяются в алгоритмах вычисления цифровой подписи и включены в национальные и международные стандарты, основана на сложности решения одной из двух задач, задачи факторизации и задачи дискретного логарифмирования. Попытки использовать в криптографических целях другие вычислительно сложные математические задачи (например, задачу о рюкзаке или задачу декодирования линейных кодов общего вида) пока к успеху не привели. Широкое практическое использование таких несимметричных криптографических систем привлекло внимание исследователей к созданию новых способов решения двух фундаментальных задач теории чисел – задачи дискретного логарифмирования и задачи факторизации. В результате были созданы достаточно мощные алгоритмы субэкспоненциальной сложности решения этих задач, причем сложность решения обоих задач одинакова, хотя эти две задачи не сводятся друг к другу.

Криптографические алгоритмы на эллиптических кривых строятся вполне аналогично обычным теоретико-числовым алгоритмам. Фактически для любого такого алгоритма можно построить эллиптический аналог путем замены основного криптографического преобразования – возведения в степень – операцией скалярного умножения в группе точек эллиптической кривой. Все стандарты, определяющие эллиптические криптографические преобразования, построены именно этим способом.

Первый действующий стандарт цифровой подписи на основе эллиптической криптографии – стандарт Американского национального института стандартов ANSI X 9.62-1998 “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, ориентированный на применение в банковской сфере. В этом стандарте используются эллиптические кривые над простым конечным полем $GF(p)$, p – простое число, и конечным полем $GF(2^m)$ характеристики 2. В качестве алгоритма вычисления и проверки цифровой подписи используется эллиптический аналог алгоритма DSA (алгоритма Кравица), определенного в первой редакции национального стандарта цифровой подписи США FIPS 186 (1993 г.) и сохраненного в последующих редакциях FIPS 186-1 (1996г.) и FIPS 186-2 (2000 г.).

При вычислении цифровой подписи используется разовый секретный ключ k. Секретные ключи цифровой подписи формируются с помощью датчика случайных чисел, определенного стандартом ANSI X 9.17 “American National Standard. Financial Institution Key Management (Wholesale)”, 1985. Кроме того, допускается использование датчика случайных чисел, приведенного в приложении к стандарту. В этом приложении повторяются датчики, определенные стандартом FIPS 186-2, в которых в качестве криптографического преобразования применяются алгоритм шифрования DES (ANSI X 9.92 “Data Encryption Algorithm”) или функция хеширования SHA-1 (Национальный стандарт США FIPS 180-1 “Secure Hash Standard”, 1995 и ANSI

X 9.30 “American National Standard for Financial Services. Public Key Cryptography Using Irreversible Algorithms for Financial Services Industry. – Part 2. The Secure Hash Algorithm “, 1993).

Исходное сообщение преобразуется в строку длиной 160 бит с помощью функции хеширования SHA-1, эта строка преобразуется в целое число *e*. Основное криптографическое преобразование выполняется путем вычисления точки эллиптической кривой $Q(x_1, y_1) = kG$, k – разовый секретный ключ, затем элемент базового поля x_1 преобразуется в целое число $\overline{x}_1$. Далее подпись вычисляется точно так же, как и в стандартном алгоритме DSA.

Причина использования алгоритма DSA в этом стандарте понятна. Алгоритм DSA используется давно и хорошо знаком западным пользователям. Из описания процесса вычисления цифровой подписи видно, что основная масса вычислений с целыми числами по сравнительно небольшому модулю остается без изменений, скалярным произведением заменена самая трудоемкая операция – возведение в степень по большому модулю. Поэтому реализации старого стандарта достаточно легко переделать в реализацию нового стандарта.

Национальный стандарт цифровой подписи США FIPS 186 “Digital Signature Standard (DSS)” был принят в 1993 г. и включал в себя теоретико-числовой алгоритм DSA. В 1995 г. в него был включен алгоритм вычисления и проверки цифровой подписи с использованием алгоритма RSA. Это было сделано путем простого включения стандарта ANSI X9.31 “Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)”. Новый стандарт получил наименование FIPS 186-1. Аналогичным образом в этот стандарт был включен алгоритм вычисления и проверки цифровой подписи на эллиптических кривых. В новый стандарт FIPS 186-2 просто включена ссылка на описанный выше стандарт ANSI X 9.62 как на стандарт, одобренный NIST (National Institute of Standards and Technology).

Основное отличие заключается в способе выбора эллиптических кривых. В стандарте ANSI X 9.62 имеется необязательное приложение, в котором описано создание эллиптических кривых методом комплексного умножения. Таким образом, фактически можно использовать любую эллиптическую кривую, которая удовлетворяет сформулированным в стандарте требованиям. В FIPS 186-2 просто перечислены разрешенные кривые под заголовком “Recommended Elliptic Curves for Federal Government Use”, т. е. нет прямого запрета использовать другие кривые. Кривые выбраны исходя из принципа равенства стойкости цифровой подписи и стойкости используемого совместно с подписью алгоритма симметричного шифрования (см. табл. 1).

Таблица 1 – Размеры полей, рекомендованных FIPS 186-2 (в битах) (AES – advanced encryption standard)

Длина ключа симметричного алгоритма шифрования	Симметричный алгоритм шифрования	Размер простого поля в битах	Степень поля характеристики 2
80	Skipjack	192	163
112	Тройной DES	224	233
128	Малый AES	256	283
192	Средний AES	284	409
256	Сильный AES	521	571

Таким образом, в случае простого поля рекомендовано 5 эллиптических кривых. В случае поля характеристики 2 рекомендовано 5 пар эллиптических кривых, для каждого поля одна случайная кривая и одна аномальная.

Стандарт IEEE P1363-2000 “Standard Specifications for Public Key Cryptography” является результатом выполнения очень большого проекта, цель которого состояла в нормировании почти всех криптографических алгоритмов, использующих несимметричные преобразования, основанных на задаче дискретного логарифмирования в мультипликативной группе простого конечного поля, задаче факторизации и задаче дискретного логарифмирования в группе точек эллиптической кривой. В этот стандарт включены два алгоритма вычисления и проверки цифровой подписи на эллиптических кривых. Один из них – алгоритм ECDSS, в точности совпадающий с алгоритмом, включенным в стандарт X 9.62 (и FIPS 186-2). Второй алгоритм – эллиптическая версия алгоритма вычисления и проверки цифровой подписи с восстановлением сообщения Нюберга-Рюппеля [4].

Очевидно, что алгоритм Нюберга-Рюппеля существенно проще алгоритма DSA, в последнем, например, используется достаточно трудоемкая операция обращения целых чисел по модулю простого числа. В теоретико-числовом случае эта не так заметно, основная криптографическая операция выполняется с целыми числами, поэтому полномасштабная арифметика выполнения операций с этими числами нужна в любом случае. При переходе к эллиптическим кривым желательно свести арифметику целых чисел к самому необходимому минимуму.

Стандарт P 1363-2000 рекомендует использовать в качестве функции хеширования либо функцию SHA-1, либо функцию RIPEMD 160.

Сейчас ведется работа по включению алгоритма цифровой подписи на эллиптических кривых в стандарты ISO, стандарты Интернета (RFC) и ряд отраслевых стандартов. В 2001 г. в Российской Федерации был принят стандарт Р34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи". Этот стандарт отличается от стандарта Р34.10-94 только тем, что операция возведения в степень в циклической группе простого конечного поля заменена скалярным умножением в группе точек эллиптической кривой, определенной над простым конечным полем. Стойкость нового стандарта существенно повысилась, однако структурные недостатки, на которые мы указывали выше, остались. Отметим также, что использование простого конечного поля в качестве определения эллиптической кривой делают вычислительные процедуры формирования и проверки подписи достаточно медленными. Итак, можем констатировать, что большинство принятых и разрабатываемых государственных и отраслевых стандартов, использующих эллиптическую криптографию, сохраняет ранее действующие в этих стандартах алгоритмы.

Переход на особенности эллиптических кривых был произведен заменой операции возведения в степень в циклической группе простого конечного поля на умножение на скаляр в группе точек эллиптической кривой, определенной над простым конечным полем.

С одной стороны использование старых алгоритмов удобно, они изучены и привычны. С другой стороны при таком подходе теряется возможность воспользоваться значительно более простым алгоритмом и, как следствие, значительно ускорить процесс вычисления и проверки подписи. Представим таблицу, где действующие сегодня алгоритмы сопоставляются по ряду критериев (см. табл. 2).

Таблица 2 – Характеристики действующих криптографических стандартов, использующих особенности эллиптических кривых

Наименование стандарта, область его применения	Используемый криптоалгоритм	Способ перехода на эллиптическую криптографию	Способ задания эллиптической кривой	Возможность использования нефиксированных значений длины ключа
ANSIX9.62 ANSIX9.63 (банковская сфера, 1999 г.)	DSA	Замена возведения в степень на скалярное умножение в группе точек эллиптической кривой	Заданы алгоритмы	Да
FIPS 186-2 (2000 г.) Национальный стандарт США	DSA	-"-	Приведен список кривых	Да
IEEE P1362-2000	DSA Нюберга-Рюппеля	-"-	Указан способ вычисления	Да
Р34.10-2001 Россия	Р34.10-94	-"-	Отсутствует	Нет
ДСТУ 4145-2002 Украина	Нюберга-Рюппеля	-"-	Приведены рекомендованные кривые	Да

Отсюда видно, что ДСТУ 4145-2002 выигрывает, используя более простой алгоритм – вместо DSA используется алгоритм Нюберга-Рюппеля и, как следствие, при всех других равных качествах обладает более высокой скоростью вычисления и проверки подписи.

В заключение отметим, что успехи математических исследований в области в области эллиптической криптографии дали возможность получить:

1) достаточно простые алгоритмы генерации эллиптических кривых;
2) совершенно ясные, простые, необходимые и достаточные условия, выполнение которых дает возможность выделить из множества получаемых эллиптических кривых те, которые обладают необходимыми свойствами и пригодны для криптографических применений.
3) достаточные гарантии того, что задача дискретного логарифмирования в поле точек эллиптической кривой будет оставаться в границах экспоненциальной сложности.

Мы надеемся, что все это обеспечит эффективное применение ДСТУ 4145-2002 в технологиях защиты информации.

Литература: ***1.*** *Miller V. S. Use of Elliptic Curves in Cryptography// Advances in Cryptology – Crypto'85. – LNCS 218. – 1986. – p. 417 – 426.* ***2.*** *N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, 48 (1987), 203-209.* ***3.*** *R. Schoof, "Elliptic Curves over Finite Fields and the Computation of Square Roots mod p", Mathematics of Computation, 44 (1985), 483–494.* ***4.*** *K. Nyberg and R. Rueppel, "A New Signature Scheme Based on the DSA Giving Message Recovery", 1st ACM Conference on Computer and Communication Security, 58–61, ACM Press, 1993.*

УДК 621.391

ПРИНЦИПЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Анатолий Кочубинский
МП "Дина"

Анотація: **Наведено принципи побудови криптографічних алгоритмів на еліптичних кривих, використані в стандарті ДСТУ 4145-2002, які забезпечують високу криптографічну стійкість цифрового підпису.**
Summary: **Design principles of elliptic curve cryptographic algorithms are explained. It is shown that implementation of these principles in the National digital signature standard DSTU 4145-2002 guarantees a high cryptographic strength of the digital signature.**
Ключові слова: **Захист інформації, автентифікація, цифровий підпис, скінченні поля, еліптичні криві, криптографічна стійкість, дискретне логарифмування.**

С 1 июля 2003 г. вступает в действие новый стандарт вычисления и проверки цифровой подписи ДСТУ 4145-2002. Новый стандарт имеет ряд преимуществ по сравнению с теми средствами аутентификации данных и их происхождения, которые используются сейчас в нашей стране. Стандарт ДСТУ 4145-2002 основан на новых теоретических принципах и обеспечивает очень высокую стойкость при сравнительно небольшом размере параметров цифровой подписи, включая размер ключей. Стандарт гибок в отношении выбора параметров безопасности и функции хеширования и легко адаптируется к конкретным условиям использования. Новый стандарт достаточно просто реализуется в программном и аппаратном виде. Он отличается от действующего унификацией представления входных и выходных данных при сохранении большой свободы в реализации основных алгебраических алгоритмов, составляющих стандарт. Важная особенность стандарта – нормирование датчика случайных чисел.

Основная причина создания и введения нового стандарта – невозможность с помощью существующих средств обеспечить уровень стойкости цифровой подписи, отвечающий современным требованиям. В табл. 1 приведена стойкость алгоритма ДСТУ 4145-2002 для трех значений степени m основного поля, отвечающих минимальному уровню стойкости $m = 163$, стандартному уровню стойкости с точки зрения современных требований $m = 257$ и очень высокому уровню стойкости $m = 509$. Высокая стойкость нового стандарта достигается при весьма скромных размерах параметров алгоритма, что дает возможность разрабатывать достаточно эффективные программные и аппаратные его реализации. Второй и третий столбцы этой таблицы показывают, что эквивалентные по стойкости реализации стандарта ГОСТ 34.310-95 и алгоритма RSA достаточно сложно создать для стандартного уровня стойкости и практически невозможно для высокого уровня стойкости.

Таблица 1 – Сравнительная стойкость основных алгоритмов цифровой подписи

Степень поля m	Стойкость	ГОСТ 34.310 (эквивалент)	RSA (эквивалент)
163	10^{24}	1024	3072
257	10^{38}	3250	9750
509	10^{78}	15500	46500