УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 201-209

ПРАКТИЧЕСКОЕ ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ СИСТЕМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В.А. Болтенков, Р.И. Еникеев

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vaboltenkov@mail.ru

Исследованы современные алгоритмы электронной цифровой подписи (ЭЦП). Алгоритмы проанализированы с точки зрения удобства программной реализации и быстродействия на различных этапах ЭЦП. Исследованы наиболее применяемые криптографические хэш-функции как составная часть системы ЭЦП. Исследование проведено путем программной реализации различных систем ЭЦП на языке Java с использованием библиотеки Open SSL и последующим программным профилированием.

Ключевые слова: электронная цифровая подпись, хэш-функция, стандарты цифровой подписи, асимметричные криптографические системы, быстродействие

Введение

Электронная цифровая подпись (ЭЦП) (англ. digital signature) за почти сорокалетнюю историю своего существования прошла стремительную эволюцию от математической идеи У. Диффи и М. Хеллмана, высказанной в 1976 г. [1], до неотъемлемого элемента современного защищенного сетевого электронного документооборота. ЭЦП – реквизит электронного документа, предназначенный для защиты электронного документа от подделки или внесения изменений, полученный в результате криптографического преобразования информации с использованием секретного ключа подписи и позволяющий идентифицировать владельца ключа подписи и установить отсутствие искажения информации в электронном документе. ЭЦП также обеспечивает невозможность отказа лица, подписавшего документ от его акта подписания. Благодаря этим свойствам ЭЦП широко применяется в следующих сферах:

- безопасный банковский финансовый оборот,
- юридически значимый электронный документооборот,
- юридическая и финансовая обязательная отчетность перед государственными органами,
- таможенное декларирование товаров и услуг,
- расчетные и трейдинговые системы,
- дистанционные торговые сделки.

Несмотря на повсеместное использование ЭЦП в перечисленных сферах применения, на сегодняшний день сложилась достаточно парадоксальная ситуация – параллельно существуют и применяются различные государственные и коммерческие стандарты ЭЦП, при этом пользователь системы ЭЦП обычно плохо представляет себе эффективность и качество применяемой им системы, ее степень криптостойкости и может реально оценить только удобство интерфейса программной реализации ЭЦП и ее быстродействие. Следует отметить, что многие из применяемых систем ЭЦП основаны на вычислительно трудоемких алгоритмах, что вызывает ощутимые пользователем временные задержки и вызывает неудовлетворенность применяемой им

системой. Несмотря на обилие публикаций по криптографическим протоколам, к которым относится и ЭЦП [2,3], авторам неизвестен обстоятельный сравнительный анализ существующих и применяемых систем ЭЦП. В этом плане задача сравнительного исследования различных алгоритмов и систем ЭЦП по набору критериев эффективности является достаточно актуальной.

Практически все протоколы ЭЦП используют криптографические хэш-функции, позволяющие путем применения математического сжимающего преобразования получить из документального файла произвольного размера результат фиксированной длины – дайджест сообщения. В целях уменьшения вычислительного объема ЭЦП и снижения времени на ее формирование и проверку алгоритмы формирования ЭЦП применяются к дайджестам, которые существенно короче исходных сообщений. В этом плане качество системы ЭЦП в значительной мере определяется применяемым алгоритмом хэш-функции. Поэтому сравнительный анализ систем ЭЦП обязательно должен сопровождаться исследованием показателей эффективности применяемых хэш-функций [4].

Целью настоящего исследования является сравнительный анализ наиболее популярных систем ЭЦП, включая исследование применяемых хэш-функций, путем их программной реализации с последующим тестированием и профилированием.

Критериями для сравнения систем были выбраны: удобство программной реализации системы ЭЦП и время ее работы, которое как указано выше, напрямую связано с удобством пользователя. Под удобством программной реализации будем понимать:

- наличие открытого исходного кода,
- наличие криптопримитивов данной системы ЭЦП в открытых библиотеках программных кодов,
- возможность распараллеливания алгоритма и наличие других путей ускорения действия алгоритма при его программной реализации.

Криптостойкость ЭЦП как и всех криптографических протоколов с открытым ключом не имеет теоретического обоснования, поэтому в данном вопросе мы ориентировались на концепцию «практической границы уровня безопасности в 80 бит длины ключа», согласно которой асимметричная криптосистема с длиной ключа 80 бит и более не может быть взломана атакой грубой силы за разумное время [5], а также соответствующими стандартами ЭЦП.

Под временем работы алгоритма электронной подписи будем понимать сумму затрат времени на операции «генерация ключа подписи», «постановка подписи», «верификация подписи». Время работы зависит от скоростных качеств криптоалгоритма, реализующего цифровую подпись и скорости применяемой хэш-функции.

В силу существенной нелинейности как алгоритмов криптографического хэширования, так и алгоритмов ЭЦП, не представляется возможным получить хотя бы грубые оценки вычислительной сложности систем ЭЦП. Поэтому основным методом их сравнительного анализа была выбрана программная реализация различных систем ЭЦП с последующим их тестированием и профилированием.

Основная часть

Общая схема ЭЦП. Независимо от применяемого алгоритма общая схема ЭЦП в системе асимметричного шифрования может быть представлена следующим образом [3]. На первом шаге вычисляется хэш-функция h от передаваемого документа (сообщения) M и создается дайджест документа $m = h(M)$. При помощи секретного ключа отправителя A k_A и алгоритма формирования ЭЦП E создается

зашифрованный дайджест сообщения M $C(m)$. В пакет для получателя B включаются: сообщение M, ЭЦП $C(m)$ и открытый ключ отправителя K_A, пакет передается получателю B по открытому каналу связи (отметим, что открытый ключ K_A может не передаваться по каналу связи, а публиковаться каким-либо другим образом, например, размещаться на сайте) (рис.1). На этапе верификации подписи получатель B вычисляет хэш-функцию $h(M)$ и получает дайджест m', расшифровывает ЭЦП алгоритмом дешифрования D, получает при этом дайджест m'. Далее производится сравнение двух хэш-функций m' и m. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства, в случае несовпадения подпись отвергается (рис.2).

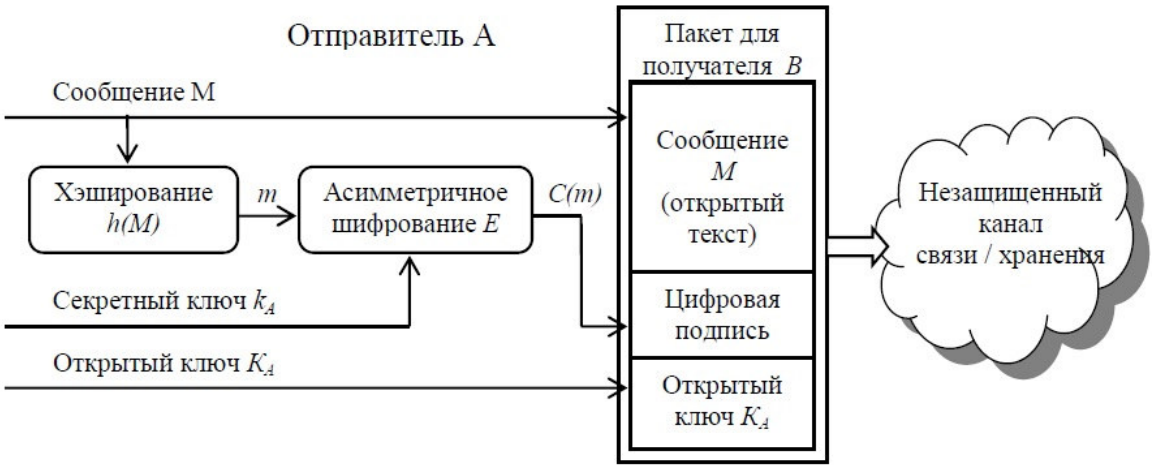


Рис.1. Общая схема ЭЦП (этап формирования)

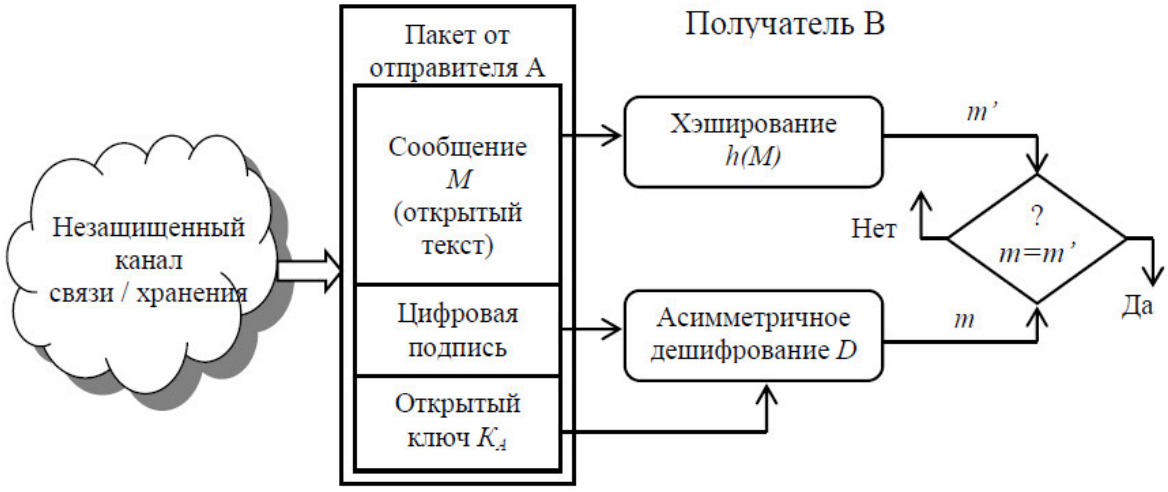


Рис.2. Общая схема ЭЦП (этап верификации)

Алгоритмы ЭЦП. Кратко рассмотрим современные алгоритмы ЭЦП, применяемые на практике. Все они основаны являются асимметричными, т.е. применяют открытый ключ. По типу применяемой односторонней функции с лазейкой (one-way function with trapdoor) они делятся на системы основанные на:

- факторизации произведения двух больших простых чисел,
- вычислении дискретного логарифма в конечном поле,
- задаче дискретного логарифмирования на эллиптических кривых в конечном поле.

Алгоритм RSA (аббревиатура от фамилий создателей Rivest, Shamir и Adleman) – первый практический криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Был создан в Массачусетском технологическом институте (MIT) в 1977 г. Защищен патентом США 4405829, выданным 20 сентября 1983 г. и действующим с продлениями до сих пор. В 1982 году Ривест, Шамир и Адлеман организовали компанию RSA Data Security, являющуюся единственным владельцем и распространителем алгоритма. На сегодняшний день RSA является фактически неофициальным мировым коммерческим стандартом ЭЦП, это самый применяемый в мире алгоритм подписи, по некоторым экспертным оценкам им подписывается до 90% всех документов. Однако главным недостатком RSA является его закрытый код и необходимость приобретения лицензии.

Алгоритм DSA (Digital Signature Algorithm) разработан Национальным институтом стандартов и технологий США (НИСТ) в августе 1991г. и защищен патентом США 5 231 668, однако НИСТ сделал этот патент доступным для использования без лицензионных отчислений. Поскольку алгоритм стал свободным для использования, его можно свободно реализовывать программным, аппаратным или любым другим образом. Основан на сложности задачи дискретного логарифмирования. Алгоритм вместе с криптографической хеш-функцией SHA-1 является частью стандарта США DSS (Digital Signature Standard), впервые опубликованного в 1994 г.

Остальные рассмотренные алгоритмы основаны на эллиптической криптографии – разделе криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. Основное преимущество эллиптической криптографии заключается в том, что на сегодняшний день неизвестно существование субэкспоненциальных алгоритмов решения задачи дискретного логарифмирования.

Алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм с открытым ключом для создания цифровой подписи, аналогичный, по своему строению, DSA, но определённый, в отличие от него, не над полем целых чисел, а в группе точек эллиптической кривой. ECDSA является очень привлекательным алгоритмом для реализации ЭЦП. Самым важным преимуществом ECDSA является возможность его работы на значительно меньших конечных полях. Как, и вообще в криптографии на эллиптических кривых, предполагается, что битовый размер открытого ключа, который будет необходим для ECDSA, равен двойному размеру секретного ключа в битах. Для сравнения, при обеспечении уровня безопасности в 80 бит (т.е. когда атакующему полным перебором необходимо рассмотреть примерно 2^{80} версий подписи для нахождения секретного ключа), размер открытого ключа DSA равен, по крайней мере, 1024 бит, тогда как открытого ключа ECDSA – 160 бит. С другой стороны размер подписи одинаков и для DSA, и для ECDSA: $4t$ бит, где t – уровень безопасности, измеренный в битах, то есть – примерно 320 бит для обеспечения уровня безопасности в 80 бит. Иными словами, любая криптосистема на эллиптической кривой обеспечивает ту же криптостойкость, что и система, основанная на дискретном логарифмировании при существенно меньшей длине ключа.

Алгоритм ГОСТ Р34.10-2012 – российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи. Принят и введён в действие в 2012 г.

ДСТУ 4145-2002 (полное название: «ДСТУ 4145-2002. Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная

на эллиптических кривых. Формирование и проверка») – украинский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи [6]. Принят и введён в действие в 2002 г. Несмотря на достаточно долгое существование ДСТУ 4145-2002 в качестве государственного стандарта ЭЦП, он остается декларированным, но мало применимым, несмотря на то, что его основные криптопримитивы реализованы в открытых Java-библиотеках OpenSSL и Bouncy Castle. По нашему мнению, существует две причины этого:

- очень сложное изложение текста самого стандарта; хотя официальное издание [6] содержит всего 39 страниц, чтение документа и его понимание занимает длительное время даже у достаточно подготовленных профессиональных программистов,
- практически полное отсутствие возможностей распараллеливания при программной реализации алгоритма.

Результаты предварительного анализа всех перечисленных алгоритмов сведены в таблицу 1.

Таблица 1.

Основные характеристики алгоритмов ЭЦП

Алгоритм	Хэш-функция	Рекомендованный размер открытого ключа	Рекомендованный размер закрытого ключа	Год создания, страна
DSA	SHA1 или SHA2	1024-3072 бит	160-256 бит	1994, США
ECDSA	SHA1 или SHA2	112-320 бит	80-521 бит	1999, США
ГОСТ Р 34.10-2012	ГОСТ Р34.112012	80-320 бит	256-512 бит	2012, РФ
ДСТУ 4145-2002	ГОСТ 34.311	162-768 бит	256-1024 бит	2002, Украина

Не останавливаясь детально на обзоре применяемых в ЭЦП критографических хэш-функций, скажем только, что все они основаны на алгоритмах блочного шифрования. В данном исследовании ЭЦП были применены хэш-функции MD-2 MD-5 SHA-1 SHA-2 (с размерами блока 256, 384, 512 бит), также ГОСТ 34311.95 и ГОСТ Р34.112012, специфицированные соответствующими стандартами ЭЦП [2,3] .

Программное средство для моделирования и сравнительного анализа систем ЭЦП

Для сравнительного анализа систем ЭЦП путем моделирования разработано универсальное программное средство со следующими функциями:

- блок хэширования,
- блок генерации открытого ключа,
- блок генерации секретного ключа,
- блок формирования ЭЦП,
- блок верификации ЭЦП.

Программа разработана на языке Java с применением библиотеки криптопримитивов Open SSL. Open SSL (secure socket layer - система безопасных сокетов) – криптографический пакет с открытым исходным кодом, предоставляющий богатые средства для профилирования программных фрагментов по затратам процессорного времени [7]. На рис.3 приведена основная экранная форма программы.

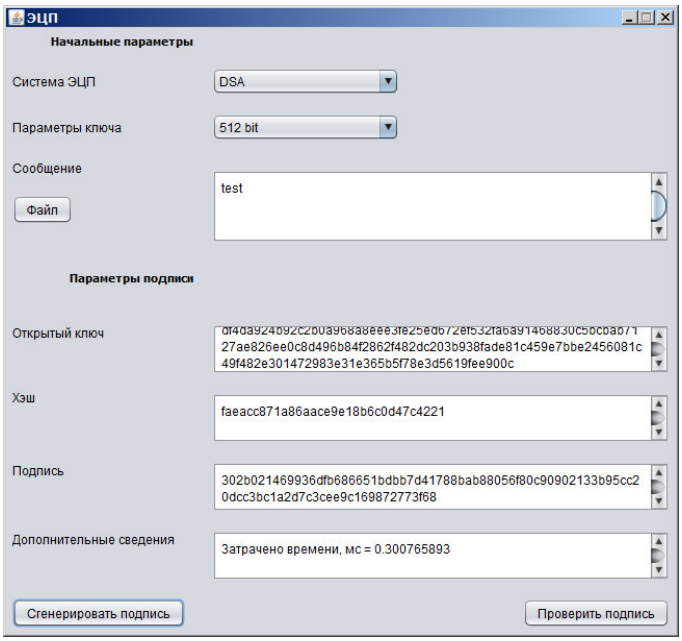


Рис.3. Основная экранная форма программы моделирования ЭЦП

Результаты исследований

Моделирование ЭЦП в целом и хэш-функций проводилось на аппаратно-программных конфигурациях двух типов:

- конфигурация А:
  CPU: Pentium 987(ядро Sandy Bridge) 1.5 ГГц (2 МБ L1 cache);
  RAM: 4 ГБ DDR3 1300 МГц;
  ОС: Win7,
- конфигурация Б:
  CPU: Core i5 3240T(ядро Ivy Bridge) 2.9 ГГц (3 МБ L1 cache);
  RAM: 8 ГБ DDR3 1600 МГц;
  ОС: Win7.

Конфигурация А моделирует типичный современный офисный компьютер в организациях и компаниях, применяющих ЭЦП, а конфигурация Б - типичный компьютер, применяемый в подразделениях компьютерной безопасности банков и других финансовых учреждений, верифицирующих ЭЦП.

В процессе моделирования была исследована производительность (скорость работы) хэш-функций. Усредненные по базе файлов документов различных форматов и размеров объемом $3 \cdot 10^4$ файлов результаты исследования быстродействия хэш-функций приведены в таблице 2 и на рис.4. Показатели скорости оценены программными профилировщиками, а также программными средствами Java и Open SSL.

Видно, что хэширование с помощью SHA-2 с длиной блока 512 бит является наиболее производительной вычислительной процедурой. С другой стороны, алгоритм SHA-2 является достаточно современной и перспективной функцией хэширования, что гарантирует ее криптостойкость.

Таблица 2.

Результаты исследования быстродействия хэш-фукций

Функция хэширования	Количество раундов	Язык реализации	Скорость работы на конфигурации А, Мбит/с	Скорость работы на конфигурации Б, Мбит/с
SHA-1	80	Java	206	344
SHA-2(256)	64	Java	81	135
SHA-2(512)	64	Java	41	68
ГОСТ 34311.95	256	Java	49	83
ГОСТ Р34.112012	256	Java	28	46

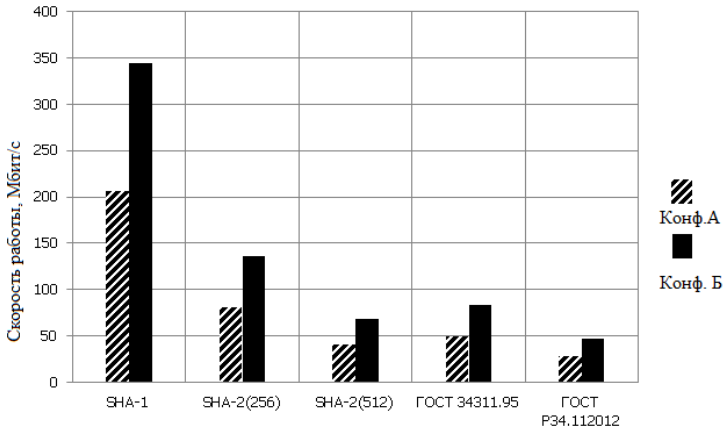
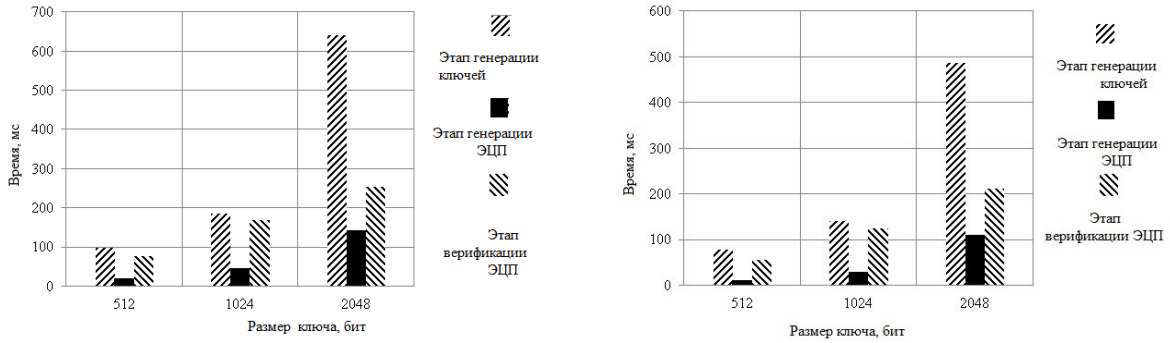


Рис. 4. Сравнительный анализ скорости работы хэш-функций

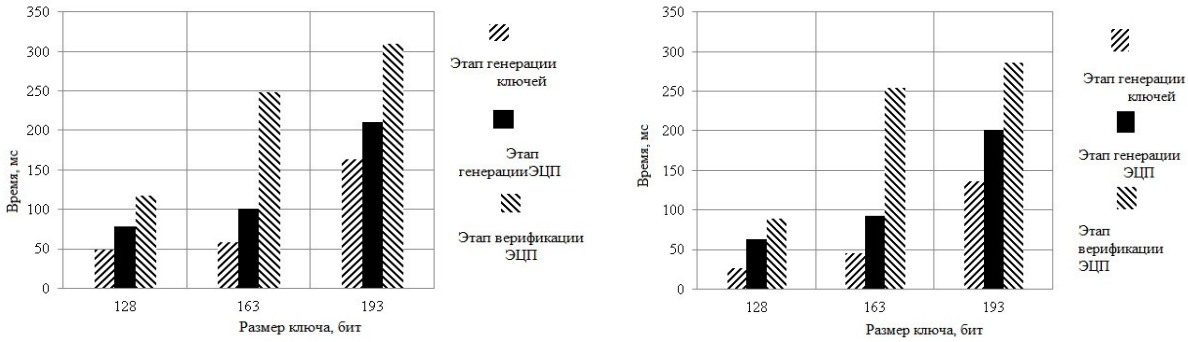
При исследовании алгоритмов ЭЦП был проведен предварительный анализ систем ЭЦП, приведенных выше в таблице 1. Он позволил вывести мягкую рейтинговую оценку, согласно которой программная реализация алгоритмов ГОСТ Р 34.10-2012 и ДСТУ 4145-2002 существенно сложнее алгоритмов DSA и ECDSA, поэтому при требуемых длинах ключей ГОСТ Р 34.10-2012 и ДСТУ 4145-2002 практически не выдерживают конкуренции с алгоритмами DSA и ECDSA по быстродействию. Ниже приведены результаты анализа быстродействия только для наиболее быстрых систем ЭЦП DSA и ECDSA.

Оценка быстродействия систем ЭЦП DSA и ECDSA, в зависимости от длины ключа с разбивкой по этапам, представлены на рис. 5-6 для обеих аппаратных конфигураций.



а **б**

Рис. 5. Временной анализ этапов ЭЦП DSA в зависимости от размера ключа: а – конфигурация А; б – конфигурация Б



а **б**

Рис. 6. Временной анализ этапов ЭЦП ECDSA в зависимости от размера ключа: а – конфигурация А; б – конфигурация Б

Анализ графических зависимостей позволяет установить следующие интересные факты.

Подпись на эллиптических кривых требует существенно большего времени на верификацию, чем на формирование ключей.

Для пользовательской конфигурации А вполне приемлемо с точки зрения быстродействия для системы DSA рекомендовать длину ключа 1024 бита, а для системы ECDSA - длину ключа 163 бита. Для профессиональной конфигурации Б эти рекомендации сохраняются.

Общие рекомендации, полученные в результате исследования, сформулируем таким образом. Наиболее эффективными по формулированным критериям удобства программной реализации и быстродействия являются системы ЭЦП DSA и ECDSA с применением хэш-функции SHA-2 длиной блока 256 или 512 бит. При сравнении систем DSA и ECDSA последнюю, безусловно, следует считать более перспективной, поскольку большинство действующих стандартов ЭЦП ориентированы на эллиптическую криптографию.

Выводы

Исследование современных систем ЭЦП путем их программного моделирования по критериям удобства программной реализации и быстродействия позволило

установить, что системы DSA и ECDSA в сочетании с хэш-функцией SHA-2 в наибольшей мере удовлетворяют сформулированным критериям и могут быть рекомендованы для практического применения. Выработаны практические рекомендации по длине блоков хэш-функции и длине ключа алгоритмов ЭЦП.

Список литературы

1. Diffie, W. New Directions in Cryptography / W. Diffie, M. Hellman. // IEEE Transactions on Information Theory. –Vol.22. No.6, 1976. – pp. 644–654.
2. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009. – 272 с.
3. Запечников, С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М.: Горячая линия-Телеком, 2007 – 320 с.
4. Єнікєєв, Р.І. Дослідження сучасних систем цифрового підпису / Р.І. Єнікєєв, В.О. Болтьонков. // Збірник матеріалів міжнародної наукової конференції «Сучасні інформаційні технології». – 2014 – С.21-22.
5. Nemati, H.R. Applied Cryptography for Cyber Security and Defence: Information Encryption and Cyphering / H.R. Nemati, L. Yang – N.-Y.: IGI Global, 2011– 383 p.
6. ДСТУ4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К.: Держстандарт України, 2003. –39 с.
7. Open SSL: [Электронный ресурс] // Режим доступ: https://www.openssl.org/ (Дата обращения: 01.08/2014).

ПРАКТИЧНЕ ДОСЛІДЖЕННЯ СУЧАСНИХ СИСТЕМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

В.О. Болтьонков, Р.І.Єнікєєв

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vaboltenkov@mail.ru

Досліджено сучасні алгоритми електронного цифрового підпису (ЕЦП). Алгоритми проаналізовані з точки зору зручності програмної реалізації та швидкодії на різних етапах ЕЦП. Досліджено найбільш застосовувані криптографічні хеш-функції як складова частина системи ЕЦП. Дослідження проведене шляхом програмної реалізації різних систем ЕЦП на мові Java с використанням бібліотеки Open SSL та подальшим програмним профілюванням.

Ключові слова: електронний цифровий підпис, хеш-функція, стандарти цифрового підпису, асиметричні криптографічні системи, швидкодія.

RESEARCH OF MODERN DIGITAL SIGNATURE SYSTEMS

V.O. Boltenkov, R.I. Yenikyeyev

Odessa National Polytechnical University,
1, Shevchenko ave., Odessa, 65044, Ukraine; e-mail: vaboltenkov@mail.ru

Modern digital signature (DS) systems were researched. The DS algorithms were analyzed with respect to easiness of software implementation and speed related to their different stages. Common cryptographic hash functions were researched as a part of a DS system. The research was performed by means of Java software implementation of different DS systems with the use of OpenSSL toolkit and further software profiling.

Keywords: digital signature, hash function, digital signature standards, asymmetric cryptographic systems, algorithm speed.