7. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов. – М.: Физматлит, 1997. – 192 с.
8. *Финько О.А.* Модулярная арифметика параллельных логических вычислений. – М.: ИПУ РАН, 2003. – 224 с.
9. *Yanushkevich S., Shmerko V., Lyshevski S.* Logic design of nanoICs. – CRCPress, 2005.

Статью реомендовал к опубликованию д.т.н., профессор В.Н. Марков.

Диченко Сергей Александрович
Филиал Военной академии связи (г. Краснодар).
E-mail: dichenko.sa@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79618588866.
Адъюнкт очной адъюнктуры.

Вишневский Артем Константинович
E-mail: vishn.artem@yandex.ru.
Тел.: +79181811798.
Адъюнкт очной адъюнктуры.

Финько Олег Анатольевич
E-mail: ofinko@yandex.ru.
Тел.: +79615874848.
Профессор.

Dichenko Sergey Alexsandrovich
Branch of the Military Academy of Communications (Krasnodar).
E-mail: dichenko.sa @yandex.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: +79618588866.
Associate Postgraduate Full-time.

VishnevskyArtemKonstantinovich
E-mail: vishn.artem@yandex.ru.
Phone: +79181811798.
Associate Postgraduate Full-time.

Finko Oleg Anatolievich
E-mail: ofinko@yandex.ru.
Phone: +79615874848.
Professor.

УДК 004.91

Д.А. Ржевский, Н.И. Елисеев, Н.Д. Абасов, О.А. Финько

ЭЛЕКТРОННАЯ ПОДПИСЬ, УСТОЙЧИВАЯ К ДЕСТРУКТИВНЫМ ВОЗДЕЙСТВИЯМ

Рассматривается устойчивая к ошибкам многоканальная криптосистема, которая при соответствующих условиях может быть использована и для построения устойчивой к ошибкам системы групповой электронной подписи, функционирующей в кольце положительных целых чисел по модулю p. Предложены решения, позволяющие обеспечить электронную подпись новым свойством самовосстановления с заданной вероятностью при различных деструктивных воздействиях на нее. По отношению к методам кратного дублирования достигается существенное уменьшение избыточности. Представлены оценки обнаруживающей способности.

Китайская теорема об остатках; модулярная арифметика; электронная подпись; электронный документооборот.

D.A. Rzhevskij, N.I. Eliseev, N.D. Abasov, O.A. Finko

ELECTRONIC SIGNATURE, TO SUSTAINABLE DESTRUCTIVE IMPACT

We consider the error-tolerant multi-channel cryptosystem, which under appropriate conditions, can be used to build fault-tolerance of a group of electronic signatures, which operates in a ring of positive integers modulo. Proposed solutions to provide an electronic signature the new self-healing property of a given probability at various destructive influences on it. With respect to the methods of multiple overlapping achieved a significant reduction of redundancy. Estimates of detecting ability.

Chinese Remainder Theorem; modular arithmetic; an electronic signature; electronic document management.

Преднамеренный вызов массовых, даже незначительных и не изменяющих смысл, искажений электронных документов и/или электронных подписей (ЭП) к ним – опасный вид атаки, приводящей к невозможности использования (порче) документов и, как следствие, «параличу» электронного документооборота в целом. С другой стороны, и непреднамеренные ошибки в электронных документах или ЭП «дорого» обходятся их владельцам, так как влекут за собой отказы в проведении операций (например, финансовых) с участием данных документов.

В [1] предложена устойчивая к ошибкам многоканальная криптосистема, которая при соответствующих условиях может быть использована и для построения устойчивой к ошибкам системы групповой ЭП.

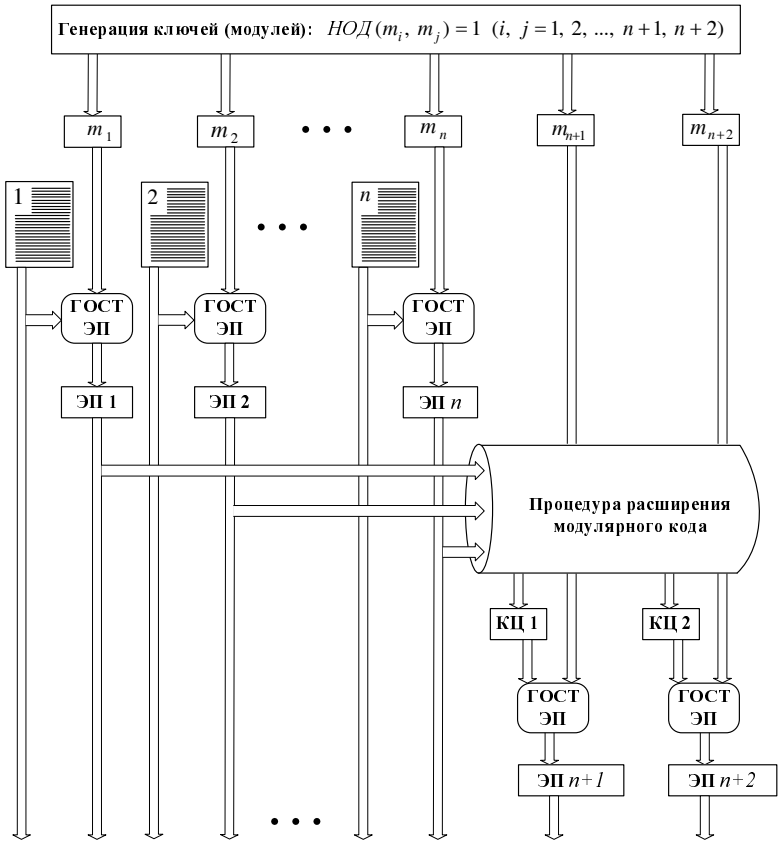

Рис. 1. Схема формирования устойчивой к ошибкам системы ЭП (зашифрование-кодирование), где КЦ 1 – контрольная цифра 1, КЦ 2 – контрольная цифра 2

Имеется n электронных документов $M^{(1)}, M^{(2)}, \ldots, M^{(n)}$, подготовленных для выполнения процедуры ЭП. Этим документам соответствуют n хэш-функций: $h\left(M^{(1)}\right), h\left(M^{(2)}\right), \ldots, h\left(M^{(n)}\right)$.

Используем допущение – ЭП одного i-го документа представлена одним числом $S^{(i)}$. Тогда процедура получения ЭП-зашифрования имеет вид

$$\begin{cases} S^{(1)} = \mathrm{E}_{k_1^{(1)}}\left(h\left(M^{(1)}\right)\right) \pmod{m^{(1)}}, \\ S^{(2)} = \mathrm{E}_{k_1^{(2)}}\left(h\left(M^{(2)}\right)\right) \pmod{m^{(2)}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ S^{(n)} = \mathrm{E}_{k_1^{(n)}}\left(h\left(M^{(n)}\right)\right) \pmod{m^{(n)}}, \end{cases} \quad (1)$$

где $k_1^{(1)}, k_1^{(2)}, \ldots, k_1^{(n)}$ – система секретных ключей владельца сертификата ЭП.

Процедура проверки подлинности ЭП заключается в выполнении процедуры расшифрования

$$\begin{cases} \hat{h}\left(M^{(1)}\right) = \mathrm{D}_{k_2^{(1)}}\left(S^{(1)}\right) \pmod{m^{(1)}}, \\ \hat{h}\left(M^{(2)}\right) = \mathrm{D}_{k_2^{(2)}}\left(S^{(2)}\right) \pmod{m^{(2)}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \hat{h}\left(M^{(n)}\right) = \mathrm{D}_{k_2^{(n)}}\left(S^{(n)}\right) \pmod{m^{(n)}}, \end{cases} \quad (2)$$

на открытых ключах $k_2^{(1)}, k_2^{(2)}, \ldots, k_2^{(n)}$ и определения значения предиката:

$$f^{(i)} = \begin{cases} 1, & \text{если} \quad \hat{h}\left(M^{(i)}\right) = h\left(\hat{M}^{(i)}\right), \\ 0, & \text{если} \quad \hat{h}\left(M^{(i)}\right) \neq h\left(\hat{M}^{(i)}\right). \end{cases}$$

Здесь $\hat{h}\left(M^{(i)}\right)$ – расшифрованное значение хэш-функции документа $M^{(i)}$, $h\left(\hat{M}^{(i)}\right)$ – значение хэш-функции документа $\hat{M}^{(i)}$, подлинность которого устанавливается. Процедура проверки подлинности документа $\hat{M}^{(i)}$ пройдена успешно, если $f^{(i)} = 1$.

Введем в правила подготовки ключей $m^{(1)}, m^{(2)}, \ldots, m^{(n)}$ новое требование: $\gcd(m^{(i)}, m^{(j)}) = 1$, где $\gcd(a, b)$ – наибольший общий делитель a и b; $i, j = 1, 2, \ldots, n$. Тогда система уравнений (1) в соответствии с Китайской теоремой об остатках имеет единственное решение:

$$S = \overset{n}{\underset{i=1}{\mathrm{CRT}}}\, S^{(i)} \pmod{m^{(i)}}, \quad 0 \le S < \prod_{i=1}^{n} m^{(i)},$$

где CRT – групповой оператор решения системы сравнений в соответствии с Китайской теоремой об остатках (Chinese remainder theorem) [2–4].

Дополним систему модулей $m^{(1)}, m^{(2)}, \ldots, m^{(n)}$ еще r избыточными модулями $m^{(n+1)}, \ldots, m^{(n+r)}$ такими, что $\gcd(m^{(i)}, m^{(j)}) = 1$, где $i, j = 1, 2, \ldots, n+r$. Потребуем также, чтобы выполнялось условие $m^{(1)}, m^{(2)}, \ldots, m^{(n)} < m^{(n+1)} < \ldots < m^{(n+r)}$. Тогда можем получить следующую

расширенную систему чисел ЭП: $S^{(1)}, S^{(2)}, \ldots, S^{(n)}, \ldots, S^{(n+r)}$, где $S^{(n+1)} = S \pmod{m^{(n+1)}}, \ldots, S^{(n+r)} = S \pmod{m^{(n+r)}}$.

В соответствии с положениями модулярной арифметики [2, 3] расширенная система чисел $S^{(1)}, S^{(2)}, \ldots, S^{(n)}, \ldots, S^{(n+r)}$ представляет расширенный модулярный тип, обладающий свойствами обнаружения и исправления ошибок.

Введем метрику МК.

Метрика МК: *весом кодового вектора* S в МК является количество ненулевых криптограмм (вычетов) и обозначается $w(\{S\})$.

Кодовое расстояние между $\{S\}$ и $\{H\}$ определяется как вес их разности $w(\{C-H\})$.

Минимальное кодовое расстояние МК – наименьшее расстояние между двумя любыми кодовыми векторами по Хэммингу с учетом данного определения веса.

Под одиночной ошибкой будем понимать произвольное искажение одной ЭП $S^{(i)}$. t-кратная ошибка – произвольное искажение t ЭП. Известно [2, 3], что: 1) избыточный модуль обнаруживает все одиночные ошибки, если $r \geq 1$ и 2) избыточный модуль-код исправляет t или менее ошибок, если $2t \leq r$. Признаком обнаруживаемой ошибки является выполнение неравенства

$$S^* \geq \prod_{i=1}^{n} m^{(i)}, \text{ где } S^* = \mathrm{CRT}_{i=1}^{n+r} S^{(i)} \pmod{m^{(i)}}.$$

Процедуры коррекции ошибок модулями широко освещены в литературе [2, 3, 6–8].

Ввиду способности системы групповой ЭП обнаруживать и исправлять ошибки, возникает необходимость в оценке обнаруживающей способности. Выполним расчет обеспечиваемой обнаруживающей способности для предложенной системы групповой ЭП.

Введем допущение: ошибки кратности t в передаваемой последовательности ЭП $S^{(1)}, S^{(2)}, \ldots, S^{(n)}, \ldots, S^{(n+r)}$ происходят независимо друг от друга, и их распределение подчиняется биномиальному закону:

$$P(q) = \sum_{t=0}^{l} \binom{l}{t} p^t (1-p)^{l-t},$$

где $l = n + r.$

Для того чтобы оценить степень деструктивных воздействий на передаваемую последовательность ЭП $S^{(1)}, S^{(2)}, \ldots, S^{(n)}, \ldots, S^{(l)}$, необходимо знать величину p вероятности ошибочного приема ЭП $S^{(i)}$. Так как действия противника на ЭП $S^{(i)}$ носит аналитический характер, то последствия таких воздействий для приемной стороны будут *непредсказуемыми и случайными*. Примем допущение: искажения, вызванные действиями противника в ЭП $S^{(i)}$, носят равновероятный характер. Тогда с учетом принятых допущений полную вероятность необнаруживаемых ошибок, которая и определяет искажение ЭП $S^{(i)}$ в передаваемой последовательности $S^{(1)}, S^{(2)}, \ldots, S^{(n)}, \ldots, S^{(l)}$, можно найти по формуле

$$P_{er} = 1 - \sum_{t=0}^{d_{\min}-1} \binom{l}{t} p^t (1-p)^{l-t},$$

где $d_{\min}$ – минимальное кодовое расстояние в метрике МК.

Расчетные вероятности необнаруживаемых ошибок представлены на рис. 2, 3.

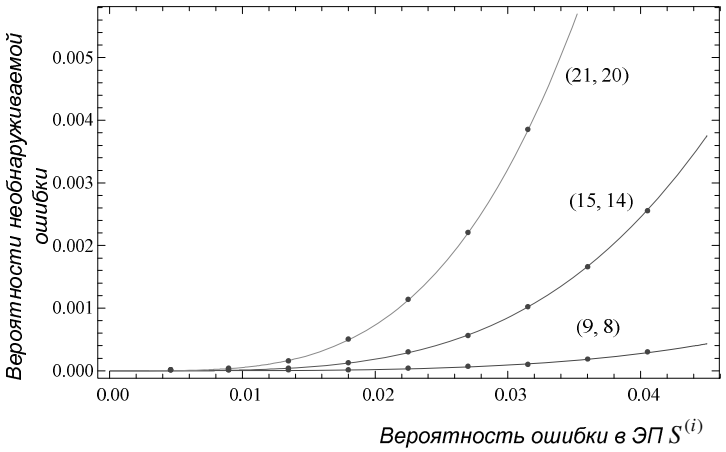

Рис. 2. Зависимость вероятности необнаруживаемой ошибки от вероятности ошибки p в $S^{(i)}$

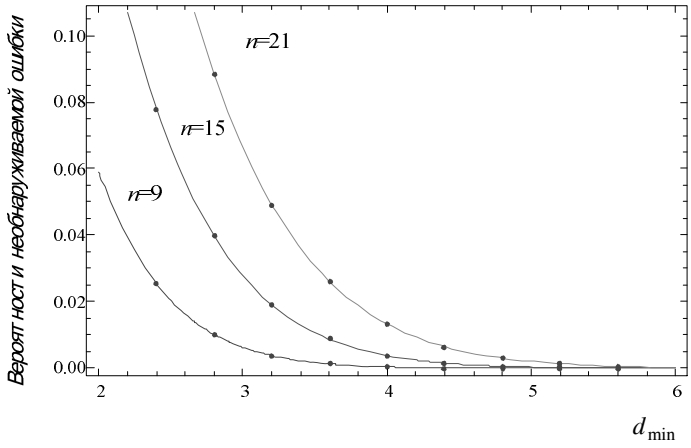

Рис. 3. Зависимость вероятности необнаруживаемой ошибки от $d_{\min}$

Главные достоинства рассмотренной системы ЭП является обеспечение новой возможности не только обнаружения фактов модификации ЭП по каким-либо причинам (непреднамеренным – сбой или преднамеренным – атака злоумышленника), но и *восстановления* правильных (исходных) значений ЭП с заданной вероятностью. Кроме того, в отличие от традиционных методов контроля, основанных на различных способах дублирования, связанного с кратным увеличением объема избыточной информации, разработанный метод предполагает существенное уменьшение избыточной информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Финько О.А., Чечин И.В., Николаев С.Л.* Устойчивая к ошибкам электронная цифровая подпись для групп документов // Материалы X Международной научно-практической конференции «Информационная безопасность» (июль, 2008 г. Таганрог). – Таганрог: ТТИ ЮФУ, 2008.

2. *Амербаев В.М.* Теоретические основы машинной арифметики. – Алма-Ата: Наука, 1976.
3. *Бояринов И.М.* Помехоустойчивое кодирование числовой информации. – М.: Наука, 1983.
4. *Финько О.А.* Восстановление числа в системе остаточных классов с минимальным количеством оснований // Электронное моделирование. – 1998. – Т. 20, № 3.– С. 56-61.
5. *Финько О.А.* Групповой контроль ассиметричных криптосистем методами модулярной арифметики // XIV Междунар. школа-семинар «Синтез и сложность управляющих систем». Н. Новгород, 27 окт. – 2 ноябр. 2003. Сб. тр. / Под ред. акад. РАН О.Б. Лупанова. – Н. Новгород: Изд-во Нижегород. пед. ун-та, 2003. – С. 85-86.
6. *Mandelbaum D.M.* Error correction in residue arithmetic // IEEE Trans. Comput. – 1972. – Vol. 21, № 6. – P. 538-545.
7. *Mandelbaum D.M.* On a class of arithmetic codes and decoding algorithm // IEEE Trans. On Information Theory. – 1976. – № 21. – P. 85-88.
8. *Mandelbaum D.M.* Further results on decoding arithmetic residue codes // IEEE Trans. On Information Theory. – 1978. – № 24. – P. 643-644.

Статью рекомендовал к опубликованию д.т.н. В.Н. Марков.

Ржевский Дмитрий Александрович
Филиал Военной академии связи (г. Краснодар).
E-mail: ofinko@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79615874848.
Старший специалист отдела.

Елисеев Николай Иванович
E-mail: eliseev_81_09@mail.ru.
Тел.: +79094476289.
Доцент.

Финько Олег Анатольевич
E-mail: ofinko@yandex.ru.
Тел.: +79615874848.
Профессор.

Абасов Низам Джавидович
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: and@radiansb.ru.
347928, г. Таганрог, ул. Чехова, 22.
Тел.:+79528169696.
Аспирант.

Rzhevskij Dmitriy Alexsandrovich
Branch of the Military Academy of Communications (Krasnodar).
E-mail: ofinko@yandex.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: +79615874848.
Senior Specialist of the Department.

Eliseev Nikolay Ivanovich
E-mail: eliseev_81_09@mail.ru.
Phone: +79094476289.
Associate Professor.

Finko Oleg Anatolievich
E-mail: ofinko@yandex.ru.
Phone: +79615874848.
Professor.

Abasov Nizam Dzhavidovich
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: and@radiansb.ru.
22, Chekhova Street, Taganrog, 347928, Russia.
Phone: +79528169696.
Postgraduate Student.

УДК 004.91

Н.И. Елисеев, Д.А. Ржевский

ОБЕСПЕЧЕНИЕ ПОДЛИННОСТИ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

Предложены в общем виде решения, позволяющие обеспечить подлинность документированной информации на всех этапах ее обработки, независимо от формы (электронная или бумажная (аналоговая)) и формата (xml, txt, tiff, pdf и пр.) ее представления.

Предложено конкретное решение обеспечения подлинности документированной информации на материальном носителе средствами электронной подписи со всеми вытекающими преимуществами, прежде всего, обеспечением криптографической стойкости.

Предложена структура системы, позволяющей обеспечить возможность проверки подлинности информации при отсутствии реквизитов.

Проверка подлинности; электронная подпись; система электронного документооборота; электронный документ; аналоговый документ; гибридный документ.

N.I. Eliseev, D.A. Rzhevskij

DOCUMENTED INFORMATION FOR THE EFFECTIVE

Are offered decisions of the supporting authenticities at all Information processing stages independently of the form (electronic or paper) and format (xml, txt, tiff, pdf etc.).

Offered concrete decisions of supporting authenticities documentary information on the material carrier with using electronic signature for cryptography resistance supporting.

Offered the structure of system allowing allow the authentication information in the absence of details.

Authentication; electronic signature; electronic document management system; electronic document; an analog document; a hybrid document.

Введение. В настоящее время существуют две основные формы представления документированной информации: аналоговая и электронная [1]. *Аналоговый документ (АнД)* – форма представления информации в среде физических объектов (явлений) [7]. *Электронный документ (ЭД)* – документ, в котором информация представлена в электронно-цифровой форме [8]. Одним из основных требований, предъявляемых в настоящее время к системам документооборота является возможность обработки различных форматов и форм представления документированной информации. Таким образом, можно утверждать, что процесс обработки документов в современных системах документооборота имеет смешанный характер (электронный и аналоговый) [2, 3]. Определим такой вид систем как *системы смешанного документооборота.*

В процессе обработки документов формат ЭД (способ представления данных в электронной среде) и внешние признаки АнД (размер, носитель и т.д.) могут подвергаться различным преобразованиям. Одна и та же документированная информация может преобразовываться. Например, при обработке входящего АнД