УДК 681.3.07

АЛГОРИТМИ ВІДНОВЛЕННЯ ПОВІДОМЛЕННЯ ЕЦП СТАНДАРТУ ISO/IEC 9796-3 ТА ЕКЗИСТЕНЦІАЛЬНА ПІДРОБКА ПІДПИСІВ, ЩО ЗАСНОВУЮТЬСЯ НА НИХ

О. А. ШЕВЧУК

Досліджено дійсну кількість збитковості, повідомлення, що відновлюється, у схемах ЕЦП стандарту ISO/IEC 9796-3 та порівняно з оціненою. Вироблено загальну модель процесу перевірки підпису у схемах з відновленням повідомлення.

Ключові слова: ЕЦП, відновлення повідомлення, екзистенційна підробка, стандарт ISO/IEC 9796-3.

ВСТУП

ЕЦП з відновленням може мати більший бітовий обсяг повідомлення, за рахунок істотного збільшування ймовірності екзистенційної підробки, але в усякому разі ймовірність екзистенційної підробки підпису з відновленням повідомлення значно вишче, ніж у підпису з доповненням.

Основними особливими характеристиками підпису з відновленням повідомлення, є ймовірність екзистенційної підробки у залежності від різних параметрів: довжини модуля обчислень у полі, що сформовано над групою точок еліптичної кривої, модуля перетворень $GF(P)$, функції відображення точки до $GF(P)$, тощо.

Метою статті є практична перевірка деяких відомих показників екзистенційної підробки для ЕЦП, які базуються на перетвореннях у групі точок еліптичної кривої, що обчислено аналітично.

1. МОДЕЛЬ ВИКОРИСТАННЯ ЕЦП З ВІДНОВЛЕННЯМ ПОВІДОМЛЕННЯ

Механізм прийняття рішень щодо дійсності цифрового підпису ґрунтується на сутності збитковості повідомлення.

Визначимо математичну модель обміну повідомлення з використанням схем ЕЦП з відновленням повідомлення між двома абонентами A та B. Нехай абонент A бажає передавати абоненту B деякі повідомлення $\{S_1, S_2, \ldots S_l\}$ з множини доступних повідомлень $\mu = \{M_0, M_1, \ldots M_{n-1}\}$. Абонент A обирає деяке повідомлення $M \in \mu$, та формує цифровий підпис $C' = Sign(M, Param)$, де $Param$ – деяка множина параметрів ЕЦП, що потрібна для його формування, після чого передає C' абонентові B.

Наступним кроком абонент B відновлює з підпису повідомлення M'', як $M'' = Sign^{-1}(C', Param')$. Для перевірки того, що повідомлення M'' відправив A, перевіряється

$$M'' \in \mu. \qquad (1)$$

Визначимо вірогідність $P(M'')$ того, що абонент відновить деяке повідомлення M'', що не було сформоване абонентом A, та прийме рішення щодо дійсності цього повідомлення.

Для цього введемо множину повідомлень $\nu = \{N_0, N_1, \ldots N_{k-1}\}$ таких, що $\forall N \in \nu : N \notin \mu$. Тоді

$$P(M'') = \frac{\#\nu}{\#\mu}. \qquad (2)$$

В схемах ЕЦП з відновленням повідомлення загальна кількість можливих повідомлень скінченна. Це означає, що для кожного відновленого повідомлення M' справедливо $M' \in \Omega$, де $\Omega = \mu \cup \nu$. Це означає, що $\#\nu = \#(\Omega \cap \mu)$. Наявність множини ν називають існуванням природної збитковості повідомлення. Зрозуміло, що природна збитковість повідомлення може існувати лише тоді, коли $\#\Omega < \#\nu$. Для повідомлень з природною збитковістю вірогідність $P(M'')$ дорівнюватиме

$$P(M'') = \frac{\#(\Omega \cap \mu)}{\#\mu} = \frac{\#\Omega - \#\mu}{\#\mu}. \qquad (3)$$

Загальна модель цифрового підпису з відновленням повідомлення передбачає можливість ситуації, коли $\#\mu \geq \#\Omega$, або вірогідність $P(M'')$ є неприпустимою. Тоді множна вхідних повідомлень μ відображається до μ_{rec} та μ_{clr} таким чином, щоб визначене $P(M'')$ було придатним до використання. Нехай $\delta(M)$ – функция, що на вході отримує бажане повідомлення, та два повідомлення $\{M_{rec}, M_{clr}\}$ на виході. Тоді

$$\forall M \in \mu : \{M_{rec}, M_{clr}\} = \delta(M), M_{rec} \in \mu'$$

$$\mu' = \{M_{rec,0}, M_{rec,1}, \ldots M_{rec,n-1}\}$$

Легко побачити, що для такої схеми ймовірність $P(M'')$ може бути обчислена як

$$\delta^{-1}(\delta(M)) = \delta(M)$$

$$\forall \{M_{rec}, M_{clr}\} : M'' = \delta^{-1}(M_{rec}, M_{clr})$$

$$\forall \{M_{rec}, M_{clr}\} : \{M_{rec}, M_{clr}\} \in \mu$$

$$\Omega' = \mu \cap \nu$$

$$P'(M''_{rec}, M''_{clr}) = \frac{\#\Omega' - \#\mu}{\#\mu}$$

$$P(M'') = \frac{\#\Omega - \#\mu'}{\#\mu'} + P'(M''_{rec}, M''_{clr}). \qquad (4)$$

Для обчислення необхідно мати цілком визначену множину ν. Якщо для випадку ν визначалось автоматично, то у ν необхідно визначати як передобчислену множину. Якщо $M=\infty$, тоді для немає методу визначення дійсності повідомлення M''.

Для цілісності схеми ЕЦП з відновленням повідомлення вводиться допоміжна сутність – надана збитковість повідомлення.

Надана збитковість d визначається як $d=\Theta(M_{rec},M_{clr})$, де Θ деяке перетворення, яке задовольняє вимогам, що висуваються до криптографічних незворотних функцій. Далі використовується у наступний спосіб:

$$d_i=i$$

$$\#\{d_0,d_1,\dots d_{l-1}\}=\#\Omega-\#\{M_{rec,0},M_{rec,1},\dots M_{rec,n-1}\}$$

$$M''_{rec},M''_{clr}=Sign^{1}(C',Params')$$

$$\Theta(M''_{rec},M''_{clr})\in\{d_0,d_1,\dots d_{l-1}\}. \qquad (5)$$

Якщо (5) – дійсне, тоді приймається рішення щодо дійності повідомлення M'', та факту його відправлення абонентом A.

Так як кожна пара $\{M''_{rec},M''_{clr}\}$ має своє відображення до $\{d_0,d_1,\dots d_{l-1}\}$, то вірогідність $P(M'')$ може бути обчислена як:

$$P(M'')=1/\#\{d_0,d_1,\dots d_{l-1}\}. \qquad (6)$$

2. АНАЛІТИЧНІ РЕЗУЛЬТАТИ, ЩО ПЕРЕВІРЯЮТЬСЯ

Попередні обчислення, що стосуються екзистенційної підробки повідомлень ЕЦП з відновленням повідомлення, використовують обрахунок вірогідності за (6).

Таблица 1

Показники підписів

	$L(d)$	$L(H^*(M_{rec}))$
NR	$L(n)-1$	$d: L(n)-L(M_{rec})$
ECNR	$L(n)-1$	$d: L(n)-L(M_{rec})$
ECMR	L(n); $L(\{0,1\}^{8(2L_+1)})$	$d: L(n)-L(M_{rec})$
ECAO	$L(\{0,1\}^{8(L_F+1)})$	$L(M_{rec})_1+[L(n)-M_{rec}]_2$
ECKNR	$L(\{0,1\}^{8L(n)})$	$d: L(n)-L(M_{rec})$

У попередніх статтях були зроблені проміжні висновки щодо вірогідності $P(M'')$ у залежності від доданої збитковості d. Вони наведені у таблиці 1, де $P(M'')$ вираховувалась як вірогідність коллізії функції гешування з виходом $L(H^*(M_{rec}))$ біт.

Для того, щоб перевірити та уточнити наведені данні, необхідно навести схеми формування доданої збитковості підписів.

Для ECNR M_{rec} обчислюється як

$$M_{rec}:=[Hash(I2OSP(L_{rec},4)\|I2OSP(L_{clr},4)\|\|M_{rec}\|M_{clr}\|EC2OSP(kG,COMP)\|C)]_{L_{red}}\|M_{rec} \qquad (7)$$

Для ECMR:

$$M_{rec}:=[Hash(EC2OSP(kG,UNCOMP)\|M)]_{L_{red}} \qquad (8)$$

Для ECAO:

$$M_{rec}:=[h]_{L_{red}}\|[h]_{L_{max}-L_{red}+1}\oplus pad \qquad (9)$$

де $pad=[[1]_{L_{max}-L_{red}-L_{rec}+1}\|M_{rec}]_{L_{max}+1-L_{red}}$ та $h=H(pad)$.

Для ECKNR спосіб подібний до ECNR.

Як можна побачити, для та відповідає як $\#d=2^{L_{red}}$, та цілком погоджується з таблицею 1.

У повідомлення M_{rec} пов'язане з доданою збитковістю симетричною функцією, але вона не задає ніяких додаткових обмежень. Тому у попередніх розрахунках загальна бітова довжина гешування враховувалась як $L(n)$, але $\#d=2^{L_{red}}$.

Таким чином, для підписів ECNR, ECMR, ECPV, ECKNR очікується

$$P(M'')=\frac{1}{2^{L_{red}}}. \qquad (10)$$

Варто зазначити, що фактична довжина L_{red}, та наданна як доменний параметр перетворення можуть розрізнятись. Якщо $L(n)\neq 0 \bmod L(n)$, тоді фактична $L'_{red}=L_{red}+(L(n)\bmod L(n))$.

3. ПОСТАНОВКА ЕКСПЕРИМЕНТУ

Для перевірки результатів, що отримані аналітично, була реалізована програмна модель підписів, що досліджуються. Програмна модель виконує усі перетворення, що описані стандартом ISO/IEC 9796-3 у спосіб ідентичний вказанному. Критерієм справжності визначено проходження тестів наданих у стандарті.

Для дослідження у якості доменних параметрів було обрано $L_{red}=\{2,3\}$, та еліптичні криві, що наведені у стандарті у якості тестів для кожного з підписів.

Для пошуку $P(M'')$ використаємо наступний алгоритм:

1. виробити підпис за допомогою секретного ключа абоненту A;
2. перевірити підпис;
3. додавати $2^{(}L(n)/2)$ до r компоненти підпису до тих пір, коли отримане значення не буде відновлене як деякий валідний підпис A;
4. кількість спроб зарахувати як необхідну для отримання результату.

Реалізація ISO/IEC 9796-3 виконує близько 3000 підписів за секунду (ECNR, EC160v1, C2D E7500), тому на кожен експеремент для $L_{red}=2$ мало підти не більше $T_2=2^{2*8}/3000=21$ с, та $L_{red}=3; T_3=2^{3*8}/3000=5592$ с для кожного з підписів.

У табл. 2 модулі перетворень, що використовувались у експерементах.

ДОСЛІДЖЕННЯ ECNR, ECKNR

Як можна побачити з таблиці 2, модуль n ECNR має неповні 6 бітів, тому за () L_{red} є більшим на 6 бітів, за рахунок того, що максимально можливе повідомлення буде на 1 байт меншим. Така сама ситуація з параметрами для ECKNR. Таким чином, фактичне L'_{red} підписів ECNR та ECKNR буде більшим.

На рис. 1 та 2 слід вважати $L_{red} = 14$ біт та $L_{red} = 22$ біт відповідно.

Треба зазначити, що доповнені біти не обчислюються окремо.

На рисунках – по осі x наведен номер експеременту, по осі y – кількість ітерацій до коллізії. Червоними лініями визначено: максимальна кількість спроб $\#d$, обрахована з доменного L_{red}, та фактична, обрахована як $2^{\lceil log_2 \delta \rceil}$, де δ – номер успішної спроби у експерименті. Назвемо $\lceil log_2 \delta \rceil$ фактичною бітовою довжиною доповнення Δ.

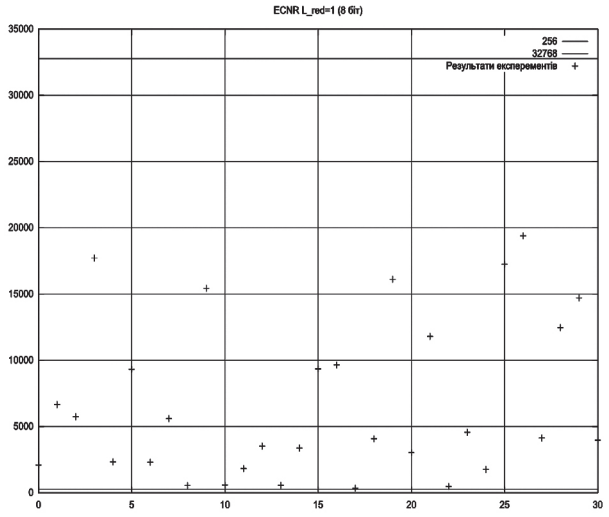

Рис. 1. ECNR, $L_{red} = 1$

На рисунку 1 можна побачити, що $\Delta = log_2 32765 = 15$, при заданному $L_{red} = 1$. Відповідно до таблиці 2 наш бітовий обсяг має складати $1*8+6 = 14$ біт. Фактичний обсяг дорівнює 15 бітам. Аналітичні розрахунки відрізняються на 1 біт.

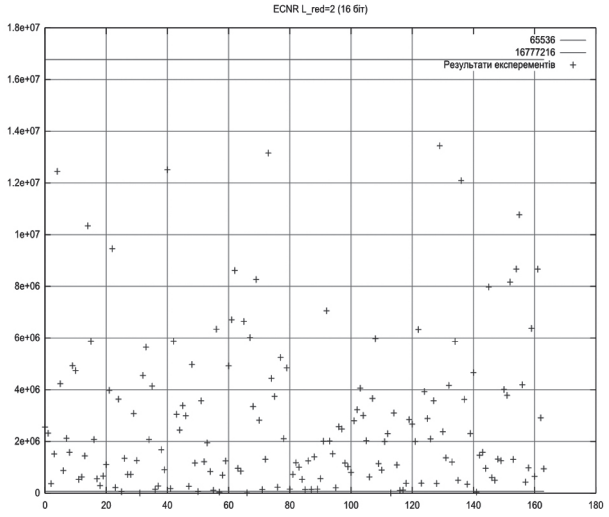

Рис. 2. ECNR, $L_{red} = 2$

На рисунку 2 $\Delta = log_2 16777216 = 24$, при заданному $L_{red} = 2$. Відповідно до таблиці 2 наш бітовий обсяг має складати $2*8+6 = 22$ біт. Фактичний обсяг дорівнює 22 бітам. Аналітичні розрахунки відрізняються на 2 біти.

Для ECKNR відповідно $L_{red} = 22$ біт.

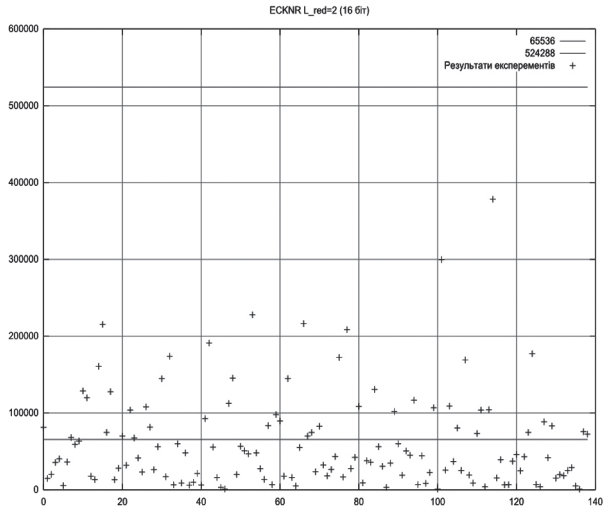

Рис. 3. ECKNR, $L_{red} = 2$

Таблиця 2

Модулі перетворень

	$p = ffd5d55fa9934410d3eb8bc04648779f13174945$	160 біт
ECNR	$n = 2aa3a38ff1988b58235241ee59a73f4646443245$	158 бі
	$p = 800000000000000000000000000000000000000000c9$	163 біт
ECMR	$n = 400000000000000000000292fe77e70c12a4234c33$	162 біт
	$p = ffffffffffffffffffffffffffffffffeffffffffffffff$	192 біт
ECAO	$n = ffffffffffffffffffffffff99def836146bc9b1b4d22831$	192 біт
	$p = ffd5d55fa9934410d3eb8bc04648779f13174945$	160 біт
ECKNR	$n = 2aa3a38ff1988b58235241ee59a73f4646443245$	158 біт

На рис. 3 $\Delta = log_2 524288 = 19$, при заданному $L_{red} = 2$. Відповідно до таблиці 2 наш бітовий обсяг має складати $2*8+6=22$ біт. Фактичний обсяг дорівнює 19 бітам. Аналітичні розрахунки відрізняються на 2 біти у зворотній бік. Це може бути роз'яснене як слідство недостатньої кількості експериментів.

ДОСЛІДЖЕННЯ ECMR

Для прикладів з ECMR також доповнення буде більшим, ніж зозначене параметрами: $\lceil log(n,2) \bmod 8 \rceil = 3$. Таким чином, фактичне L'_{red} підписів ECMR буде більшим на 3 біти.

На рис. 4 та 5 слід вважати $L_{red} = 19$ біт та $L_{red} = 27$ біт відповідно.

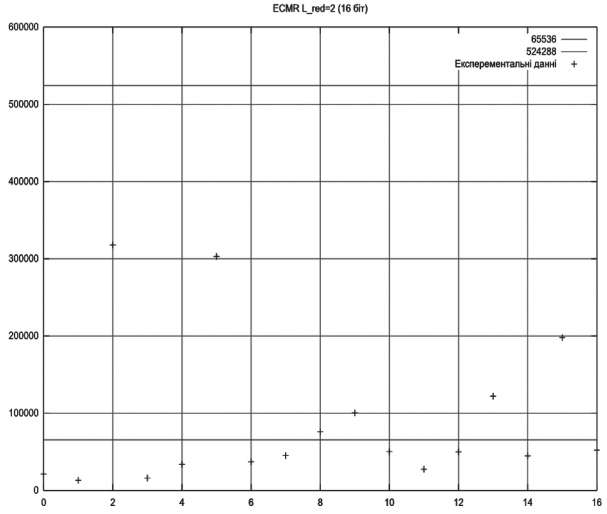

Рис. 4. ECMR, $L_{red} = 2$

На рисунку $\Delta = log_2 524288 = 19$, при заданному $L_{red} = 2$. Відповідно до таблиці 2 наш бітовий обсяг має складати $2*8+3=19$ біт. Практичний результат відповідає отриманному аналітично.

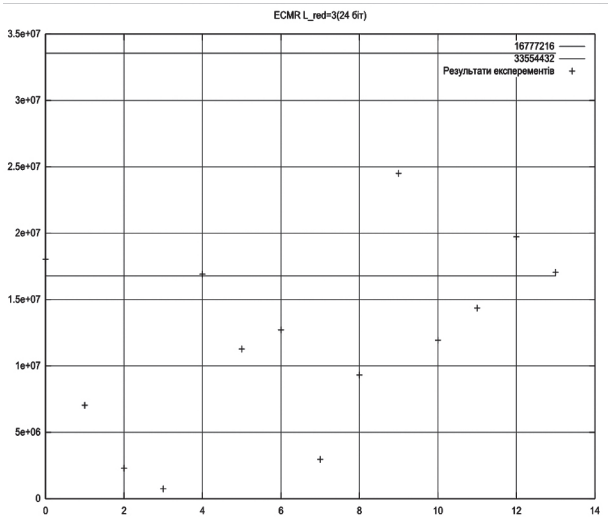

Рис. 5. ECMR, $L_{red} = 3$

На рисунку 5 $\Delta = log_2 33554432 = 21$, при заданному $L_{red} = 3$. Відповідно до таблиці 2 наш бітовий обсяг має складати $3*8+3=27$ біт. Фактичний обсяг дорівнює 21 бітам. Аналітичні розрахунки відрізняються на 6 бітів у зворотній бік. Це може бути роз'яснене як слідство недостатньої кількості експериментів.

ДОСЛІДЖЕННЯ ECAO

У цьому прикладі для підписів ECAO немає розбіжностей між показником збитковості, що зазначено у параметрах домену, та фактично обчисленній збитковості.

Треба зазначити, що доповнення ECAO не є однорідною: обчисленне внутрішнє доповнення в цьому прикладі має розмір 8 бітів. Але це враховано у доменному параметрі L_{rec} для цих прикладів.

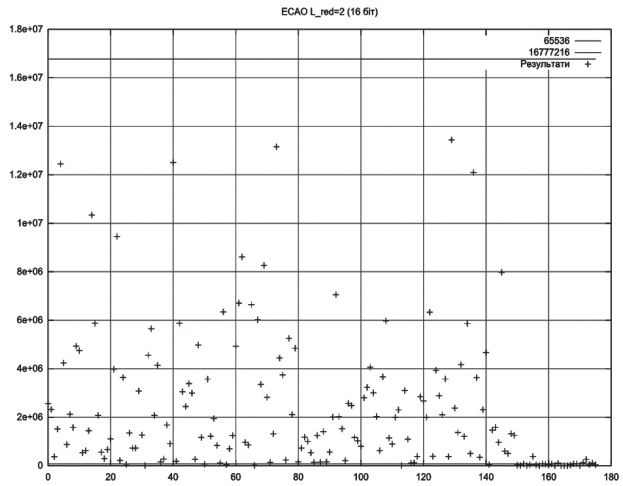

Рис. 6. ECAO, $L_{red} = 2$

На рисунку 6 $\Delta = log_2 16777216 = 249$, при заданному $L_{red} = 2$. Відповідно до таблиці 2 наш бітовий обсяг має складати 16 біт. Практичний результат більший аналітичного на 8 бітів.

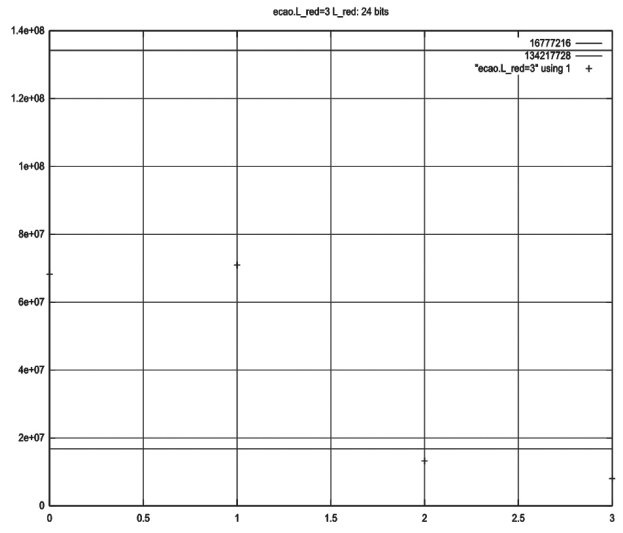

Рис. 7. ECAO, $L_{red} = 3$

На рис. 7 $\Delta = log_2 134217728 = 27$, при заданному $L_{red} = 3$. Відповідно до таблиці 2 наш бітовий обсяг має складати $3*8=24$ біт. Практичний результат більший аналітичного на 3 біти.

ВИСНОВКИ

Абонент, що перевіряє достовірність підпису, має віднести відновлене повідомлення до такого, що має сенс, або такого, що не має. Повідомлення вірне, якщо воно має сенс, тобто належить до деякої відомої усім абонентам множини μ.

У деяких випадках обсяг макисмально можливого повідомлення, що можна відновити, може бути меншим, ніж абонент хоче передати, або множина μ не визначена. У таких випадках вводиться нова множина μ', з компонентами множини d, що називається наданною збитковістю. Усі підписи стандарту ISO/IEC 9796-3 використовують саме надану збитковість для встановлення дійсності повідомлення, незалежно від розміру повідомлення.

Розмір доповнення визначає максимальну кількість різних підписів, які має сформувати зловмисник, щоб отримати дійсний підпис з деякою непердбаченною інфомацією.

При експерементальному дослідженні ефективний розмір доповнення у більшості випадків виявивася більшим, ніж аналітично розрахований. Необхідно продовжити дослідження причин розширення μ'.

Література

[1] *Горбенко Ю.І., Шевчук О.А.* Аналіз властивостей та областей застосування цифрових підписів стандарту ISO/IEC 9796-3:2006 (ISO/IEC 15946-4:2003) // Прикладная радиоэлектроника. – Том 8. 2009. – №3. –С. 304-315.

[2] *Шевчук О.А.* Особливості ЕЦП з відновленням повідомлення // Прикладная радиоэлектроника. – Том 9. 2010. – №3. –С. 489-492.

[3] ISO/IEC 9796-3: Discrete logarithm based mechanisms / ISO/IEC. – URL:http://www.iso.org/, 2006

[4] *Мао Венбо.* Современная криптография: Теория и практика / Венбо Мао; Ред. Тригуб С.Н. – 03150, Киев, а/я 152: Издательский дом Вильямс, 2005.

Надійшла до редколегії 11.05.2011

Шевчук Олексій Анатолійович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: захист інформації в ІТС.

УДК 681.3.07

Алгоритмы восстановления сообщения ЭЦП стандарта ISO/IEC 9796-3 и экзистенциальная подделка подписей, которые на них основаны / А.А. Шевчук // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 183–187.

В статье приводятся результаты исследования действительного количества избыточности сообщения для схем ЭЦП с восстановлением сообщения стандарта ISO/IEC 9796-3. В общем виде описана модель проверки подписи в схемах с восстановлением сообщения.

Ключевые слова: ЭЦП, восстановление сообщения, экзистенциальная подделка, стандарт ISO/IEC 9796-3.

Табл. 02. Ил.05. Библиогр.: 04 назв.

UDC 681.3.07

Algorithms of restoring a DSS message of standard ISO/IEC 9796-3 and existential counterfeit of signatures that are based upon / A.A. Shevchuk // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 183–187.

The paper presents results of investigating the real amount of redundancy of a message for DSS schemes with standard ISO/IEC 9796-3 message reconvery and outlines a model of verifying a signature in message recovery schemes.

Keywords: DSS, message recovery, existential counterfeit, standard ISO/IEC 9796-3.

Tab. 02. Fig. 05. Ref.: 04 items.