УДК 519.688

ОСОБЛИВОСТІ ЕЦП З ВІДНОВЛЕННЯМ ПОВІДОМЛЕННЯ

О. А. ШЕВЧУК

Досліджуються відмінності підписів з відновленням повідомлення з підписами з додатком. Робляться зауваження щодо використання підписів з відновленням повідомлення. Шляхом декомпозиції показується структурова схожість підписів з відновленням та доповненням.

Ключові слова: ЕЦП, доповнення повідомлення, відновлення повідомлення.

ВСТУП

У найближчі роки Україна планує завершити гармонізацію підписів з відновленням повідомлення. Ці схеми ЕЦП на відміну від загальновживаних підписів з додатком мають особливості. У специфічних ситуаціях ці особливості можуть зробити використання ЕЦП виправданим, коли впровадження звичайного підпису з додатком може бути неефективним, або неможливим.

Ефективному впровадженню підписів з відновленням повідомленням заважає обмеженість інформації щодо їх спеціальних властивостей, їх порівняння та визначення відповідної до кожного підпису галузі застосування.

Метою статті є огляд деяких властивостей схем ЕЦП з відновленням міжнародного стандарту ISO/IEC 9796-3.

Для досягнення цієї мети необхідно сформувати абстрактну модель підпису, визначити властивості підписів з відновленням, у тому рахунку і ті, що не мають прямого відношення до надання послуг безпеки інформації, порівняти ЕЦП з відновленням повідомлення та ЕЦП з доповненням.

1. ДЕКОМПОЗИЦІЯ ЕЦП

Стандарти ISO/IEC мають схематичні позначення процесів формування/перевірки ЕЦП, але для задач порівняння властивостей вони є дещо збитковими та не наочними. На початкових етапах можна знехтувати такими елементами схем: виробленням доменних параметрів (у зв'язку з еквівалентністю алгоритму в усіх схемах ЕЦП з доповненням у стандарті з однаковим математичним апаратом), функціями морфізмів даних між різними категоріями (морфізм точки до цілого тощо). Ці функції є технічними, хоча від їх адекватності залежить загальна безпека усієї схеми, але у межах стандарту функції морфізмів вживаються однаково та однакові, тому на переваги схеми відносно стандарту не впливають.

Першу наочну властивість ЕЦП з відновленням повідомлення отримаємо за допомогою структурової декомпозиції та порівняння загальної схеми з відновленням повідомлення Ніберг-Рюпеля, та схеми з доповненням повідомлення. Для схеми ЕЦП з доповненням повідомлення можливо попередньо зробити таку декомпозицію (у дужках еквівалентні компоненти схеми ECDSA):

1. Вироблення доменних параметрів
2. Вироблення особистого ключа $d \in [1, n-1]$
3. Обчислення відкритого ключа $Q = d \times G$
4. Вироблення передпідпису Π: $k \in [1, n-1]$ $\Pi = k \times G$
5. Обчислення ідентифікатору повідомлення $i = Hash(M)$
6. Формування зворотньої компоненти підпису $\pi((x, y)) = x$; $r = \pi(\Pi)$
7. Обчислення незворотньої компоненти підпису (s-компоненти) $s = k^{-1}(i + dr)$
8. Формування пакету ЕЦП зі зворотньою та незворотньою компонентами та тілом повідомлення (r, s, M)
9. Передача пакету $sizeof(r, s, M)$
10. Відновлення передпідпису з переданої незворотньої компоненти за допомогою ідентифікатору повідомлення та зворотньої компоненти, що було передано у складі підпису $i = Hash(M)$; $\Pi = iw \times G + rw \times G$
11. Обчислення зворотньої компоненти з передпідпису $r' = \pi(\Pi)$
12. Прийняття рішення щодо дійсності підпису, виходячи з еквівалентності обчисленої та переданої відновлюваної частини підпису. (Якщо $r' = r$ підпис вірний)

Відповідно, схеми ЕЦП з відновленням повідомлення мають мати такі компоненти (у дужках еквівалентні компоненти схеми ECNR).

1. Вироблення доменних параметрів
2. Вироблення особистого ключа $d \in [1, n-1]$
3. Обчислення відкритого ключа $Q = d \times G$
4. Вироблення передпідпису $\Pi = kG$
5. Доповнення повідомлення

$$M = M_{rec} \| M_{clr}$$
$$L(M_{rec}) \le L_{max}$$
$$pad = I2OSP(1, L_{max} + 1 - L(M_{rec}))$$
$$\tilde{M}_{rec} = pad \| M_{rec}$$
$$h = Hash_1(\tilde{M}_{rec})$$
$$d = h \| (Hash_2(h) \oplus \tilde{M}_{rec}),$$

де h – геш токен, а pad – доповнення

6. Формування зворотньої компоненти підпису шляхом маскування доповненого повідомлення з передпідписом $r = (\delta + \pi(\Pi)) \bmod n$
7. Обчислення незворотньої компоненти підпису $s = (k - dr) \bmod n$

8. Формування пакету ЕЦП зі зворотньої та незворотньої компонент та відкритої частини повідомлення (r, s, M_{clr})

9. Передача пакету $sizeof(r, s, M_{clr})$

10. Відновлення передпідпису з переданої незворотньої компоненти за допомогою ідентифікатору повідомлення та зворотньої компоненти, що було передано у складі підпису $\Pi = sP + rQ$

11. Обчислення доповненого повідомлення шляхом зворотнього маскування зворотньої компоненти підпису з передпідписом $\delta = (r - \pi(\Pi)) \bmod n$

12. Висновок щодо дійсності підпису, виходячи з семантики доповненого повідомлення. Якщо h має сенс, згідно до m – підпис дійсний.

Таким чином, можна навести структурну різницю між зазначеними типами підписів: схеми з відновленням не мають механізмів чіткої перевірки дійсності повідомлення (кроки (12), (12) відповідно). Якщо підпис з додатком представити як повідомлення $(r, s) \| M$, а процес перевірки – як перевірку семантичного змісту повідомлення $[(r, s) \| M]$, тоді розбіжності буде усунено. Дійсно, відірваний від повідомлення підпис (r, s) є не більш, ніж кортежем, що не має ніякого семантичного змісту.

Процесс формування пакету підпису у цих ЕЦП також є дещо іншим. Схеми з відновленням не обов'язково мають мати тіло повідомлення у складі пакету підпису (кроки (8)-(8) відповідно) – ситуація, коли частина повідомлення, або все, включається до r компоненти є штатною.

Таким чином, ЕЦП з відновленням повідомлення семантично відповідають схемам з додатком. Завдяки зазначеним розбіжностям, схеми з відновленням мають особливості: зменшення розміру підпису (за рахунок маскування у зворотній компоненті), та деякі додаткові властивості. Зменшення підпису має негативні наслідки – підпис може мати менший розмір за рахунок зменшення збитковості, але це робить його потенційно більш вразливим до екзистенційної підробки.

Доцільно досліджувати такі властивості підписів з відновленням повідомлення:

– стійкість до атаки екзистенційної та селективної підробки у залежності від кількості інформації, що вкладено до компоненти ЕЦП, що відновлюється

– часові показники

– можливість надання послуги конфіденційності та особливості

– складність вироблення підпису.

У наступній частині будуть зроблені базові дослідження за сформульованим напрямком підписів стандарту ISO/IEC 9796-3 – ECNR, ECPV, ECAO, ECMR, ECKNR.

2. ЕКЗИСТЕНЦІЙНА ТА СЕЛЕКТИВНА ПІДРОБКА, ДОДАТКОВІ ВЛАСТИВОСТІ

Як було відмічено, основним питанням до схем ЕЦП з відновленням повідомлення є визначення стійкості до екзистенційної та селективної підробки. У загальному вигляді остаточне прийняття рішення про дійсність повідомлення робиться через визначення дійсності збитковості відносно повідомлення. Таким чином, задача екзистенційної підробки зводиться до формування $n^{n/2}$ повідомлень δ_i, де n-бітовий обсяг збитковості повідомлення δ. Можливо казати про успішність атаки, коли для повідомлення δ' буде знайдене повідомлення δ'' таке, що усі n біт збитковості для повідомлень δ' та δ'' будуть еквівалентними.

Потрібно відрізняти вірогідність підробки для включеного в підпис повідомлення, та частини, що передається у відкритому вигляді.

Селективна підробка для підписів з відновленням повідомлення у загальному випадку має однаковий семантичний зміст з повним розкриттям, тому що частина повідомлення приймає безпосередню участь в обчисленні підпису.

Алгоритми з відновленням повідомлення також не мають рекомендацій відносно кількості біт надлишковості. Тому визначимо граничні показники відносно надлишковості.

Розглянемо особливості схем підписів.

Схема ECMR допускає можливість для багатопотокової оптимізації на етапі перевірки підпису. Один з етапів (обчислення R'):

$$R' = ((1 + OS2IP(r) + s)/OS2IP(r)) \times P + \\ + (s/OS2IP(r)) \times Q;$$

Таблиця 1

Показники підписів

	ECNR	ECAO	ECPV	ECMR	ECKNR
Мінімальний бітовий обсяг зворотньої компоненти	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$	2	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$
Максимальний бітовий обсяг зворотньої компоненти	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$	∞	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$
Максимальний бітовий обсяг повідомлення δ	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$	∞	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$
Максимальний бітовий обсяг збитковості	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$	∞	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$
Максимальний бітовий обсяг збитковості у залежності від обсягу повідомлення M	$\lceil \log_2 f \rceil$ - $\lceil \log_2 M \rceil$	$\lceil \log_2 f \rceil$ - $\lceil \log_2 M \rceil$	∞	$\lceil \log_2 f \rceil$ - $\lceil \log_2 M \rceil$	$\lceil \log_2 f \rceil$ - $\lceil \log_2 M \rceil$

Можна побачити, що компоненти

$$((1+OS2IP(r)+s)/OS2IP(r))\times P$$

$$\text{та } (s/OS2IP(r))\times Q$$

можуть бути обчислені паралельно після обчислення $(OS2IP(r))^{-1} \bmod n$.

Схема ECAO має додаткову властивість – гарантоване використання природної збитковості. Функція ділить повідомлення на частину, що включена до підпису (M_{rec}), та частину, що передається відкритою (M_{clr}). Частина M_{rec} подвійно гешується: перший геш використовується у незмінному вигляді, друга частина використовується як збитковість для першої, та додається до підпису.

$$M = M_{rec} \| M_{clr}$$
$$L(M_{rec}) \le L_{max}$$
$$pad = I2OSP(1, L_{max} + 1 - L(M_{rec}))$$
$$\tilde{M}_{rec} = pad \| M_{rec}$$
$$h = Hash_1(\tilde{M}_{rec})$$
$$d = h \| (Hash_2(h) \oplus \tilde{M}_{rec})$$

Схема ECPV представляє свою функцію маскування та формування зворотньої компоненти підпису, у якої зворотня компонента формується шляхом підстановки за ключем, що сформовано за функцією розгортання ключів з передпідпису.

Таким чином, максимальна складність атаки екзистенційної підробки для ECAO та ECNR складе $2^{n/2}$, а для ECPV – довільна. Визначимо мінімально необхідний бітовий обсяг наданої збитковості для забезпечення безпечного часу з вірогідністю 0.95 на протязі року, якщо криптоаналітик може обчислювати 10^8 збитковостей за секунду. Для цього випадку

$$n = \lceil log_2(\frac{\gamma tk}{P}) \rceil = \lceil log_2(\frac{10^8 * 1 * 3{,}15 * 10^7}{0{,}95}) \rceil = 52 .$$

Схема ECKNR відрізняється від ECNR додатковим кроком при формуванні r компоненти підпису: за передпідписом формується гамма, до якої додається гамма сформована за участю відкритої частини повідомлення. Таким чином, може бути досягнута деяка гнучкість при формуванні повідомлення зі збитковістю d.

3. НАДАННЯ ПОСЛУГИ КОНФІДЕНЦІЙНОСТІ

Схеми ЕЦП з відновленням повідомлення «приховують» частину повідомлення по суті у цифровому підписі.

В усіх схемах зворотня частина повідомлення сформована шляхом маскування повідомлення з передпідписом. У загальному вигляді перетворення можна представити у вигляді $c = Mask(Msg, KDF(kG))$.

Відновити повідомлення можливо у разі відтворення передпідпису kG, що у загальному випадку можливо тільки при перевірці ЕЦП. Таким чином, можна стверджувати, що повідомлення може відновити лише за наявності відкритого ключа. У відкритих системах така схема не має сенсу з надання послуг конфіденційності, але у разі, якщо циркуляція відкритих ключів в системі є контрольованою, є сенс у використанні цієї властивості схем з доповненням.

ВИСНОВКИ

Схеми з доповненням повідомлення мають усі властивості ЕЦП з відновленням повідомлення. Обмежене надання послуги конфіденційності можливе у закритих системах, де можна реалізувати контрольований процес поширення відкритого ключа.

ЕЦП з відновленням може мати більший бітовий обсяг повідомлення. Але при цьому істотно збільшується ймовірність екзистенційної підробки (в усякому разі ймовірність екзистенційної підробки підпису з відновленням повідомлення значно вижче, ніж у підпису з доповненням).

Основними характеристиками, що є особливими для підпису з відновленням повідомлення, є:

– ймовірність екзистенційної підробки у залежності від довжини модуля обчислень та повідомлення, що передається,

– ймовірність екзистенційної підробки у залежності від довжини модуля обчислень та повідомлення, що відновлюється,

– ефективність використання природньої збитковості повідомлення,

– можливість розпаралелювання, максимальний та мінімальний обсяг пакету підпису,

– варіативність обсягу пакету підпису.

Кожен з підписів з відновленням повідомлення стандарту ISO/IEC 9796-3 має особливості. Доцільно обирати більш раціональний підпис у залежності від ситуації. Наприклад:

– ECNR доцільно застосовувати для незбиткових повідомлень та не більше обраного модуля перетворень, але і не значно меньшого, наприклад, команд RPC,

– ECAO для збиткових повідомлень,

– ECPV для повідомлень з нефіксованою довжиною повідомлення, або надкоротких повідомлень, наприклад, команд контроллеру,

– ECKNR для великих повідомлень із захищеним заголовком, можливо для IP пакетів.

Литература.

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

[2] *Горбенко И.Д.* Защита информации в информационно-телекоммуникационных системах. Ч.1. Криптографическая защита инфомации / И.Д. Горбенко, Т.О. Гриненко. – ХНУРЭ, 2004.

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

[4] Nyberg K., Rueppel R. A new signature scheme based on the dsa giving message recovery / Rueppel R. Nyberg K. // ACM Conference on Computer and Communications Security. P. 58–61.

Надійшла до редколегії 8.07.2010.

Шевчук Олексій Анатолійович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: захист інформації в інформаційно-телекомунікаційних системах, ЕЦП з відновленням повідомлення.

УДК 519.688

Особенности ЭЦП с восстановлением сообщения / А. А. Шевчук // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 489–492.

Исследуются различия подписей с восстановлением сообщения. Вырабатываются замечания к использованию подписей с восстановлением сообщения. Путем декомпозиции показывается структурная схожесть подписей с восстановлением и дополнением.

Ключевые слова: ЭЦП, восстановление сообщения, дополнение сообщения.

Табл. 01. Библиогр.: 04 назв.

UDC 519.688

Particulars of digital signatures with message recovery / O.A. Shevchuk // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 489-492.

Differences between signatures with message recovery are investigated. Remarks relating to the use of signatures with message recovery are made. Structural similarity of recovery and addition signatures is shown by means of decomposition.

Key words: digital signature, message recovery, message addition.

Tab. 01. Ref.: 04 items.