УДК 681.3.07

СХЕМИ ЕЦП ДЛЯ ГРУП ПІДПИСІВ СКОРОЧЕНИХ ПОВІДОМЛЕНЬ

О.А. ШЕВЧУК

Запропоновано метод формування ЕЦП для множин невеликих повідомлень з відсутньою збитковістю. Запропоновано критерій ефективності подібних схем. Розглянуто ЕЦП з відновленням повідомлення в стандарту ISO/IEC 9796-3.

Ключові слова: ЕЦП, відновлення повідомлення, оптимізація обчислень.

ВСТУП

В сучасних інформаційних системах актуальні питання перевірки дійсності та справжності множин невеликих повідомлень, та подальше їх зберігання.

Наведемо модель, що розглядається. Нехай A передає B деякі повідомлення $m_1, m_2, \ldots m_\infty$. В деякий проміжок часу t_i A може передати $n \in [1;n]$ повідомлень як $M_i = \{m_{i,1}, m_{i,2}, \ldots m_{i,n}\}$. Абонентові B у будь-який проміжок часу $t_j, j > i$ необхідно встановити такі $m \in M_i, M_i \in \{M\}$, що не є цілісними та справжніми. В статті розглядається випадок для стислих m.

Пропонуються критерії порівняння схем ЕЦП, використовуючи які можливо зменшити постійні затрати на зберігання множин стислих повідомлень з їх цифровими підписами.

Задача є актуальною для систем перевірки цілісності компонентів програмного забезпечення, журналювання, мережевих протоколів тощо. Загальна схема

Запропонуємо наступне визначення стислого повідомлення. Нехай повідомлення m є стислим, якщо для забезпечення визначеного рівня стійкості до атаки селективної підробки необхідно геш значення h таке що $L_b(h) > L_b(m)$, де $L_b(x) = \lceil log_2 x \rceil$.

Оберемо показник ефективності схеми, як відношення доданої частки $\{H, S\}$ повідомлення до основної $\{M\}$:

$$\Delta = \frac{L_b(H) + L_b(S)}{L_b(M)}, \qquad (1)$$

де $M = \{m_1, m_2, \ldots m_n\}$ – повідомлення, такі що $\forall m \in M : L_b(m) = const$; $H = \{h_1, h_2, \ldots h_n\}$ – геш значення повідомлень та S – цифровий підпис H.

Ідеальною схемою будемо вважати таку, що задовольняє

$$\Delta \le 1 \qquad (2)$$

Загальний обсяг повідомлення складає

$$L_b(\{M, H, S\}) = \\ = L_b(S) + \sum_{\forall m \in M} (L_b(m) + L_b(Hash(m))) \qquad (3)$$

Якщо $\forall m : L_b(Hash(m)) = const$, доданий обсяг для $\{m_1, m_2, \ldots m_n\}$ складе

$$L_d = const = n \cdot L_b(Hash(0)) + L_b(S). \qquad (4)$$

Легко побачити, що не (2) задовольняється, коли $\forall m \in M : m \le L_b(Hash(m))$.

Задачею, що вирішується в статті, є пошук такої схеми цифрового підпису, що має найбільш подібну до (2) схему цифрового підпису.

1. ІСНУВАННЯ ІДЕАЛЬНОЇ СХЕМИ /ДЛЯ СКОРОЧЕНИХ ПОВІДОМЛЕНЬ

Для обчислення вірних параметрів значення $L_b(Hash())$ розглянемо складність атаки селективної та екзистенційної підробки для підписів з відновленням повідомлення у випадку використання схеми з множиною скорочених повідомлень.

Нехай зловмисник Z хоче створити підпис (r,s), $r \in [1, n-1]$ для деякого повідомлення m. Зловмисник має створити такі (r,s), що $V((r,s)) \neq \perp$. Для всіх схем ЕЦП обидві компоненти r,s обчислюються у групі точок ЕК за допомогою сеансового ключа k. Відновлення k має експоненційну складність. Тому Z має вгадувати r.

Встановимо ймовірність того, що Z вгадає геш значення обраного повідомлення. Нехай Z вгадує $h \in [1, 2^{L_{bh}}]$ для повідомлення $m \in [1, 2^{L_{bm}}]$, де

$$\begin{cases} \forall h \in H : L_{bh} = L_b(h) = const \\ \forall m \in M : L_{bm} = L_b(m) = const \end{cases}$$

Нехай Z за допомогою випадкової функції обирає деяке $r' \in [1, n-1], r' \neq r$. Зробимо припущення, що

$$\forall r' \in [1, n-1] : \exists H : Sign(H) = (r', s)$$

Тоді, якщо $H = \{h_1, h_2, \ldots h_k\}$, ймовірність вгадування геш значення деякого повідомлення $j \in [1, k]$ в множині геш значень становить

$$P_j(k, L_{bh}) = 2^{L_{bh}(1/k-1)}$$

Нехай $L_{bh} > L_{bm}$. Тоді ймовірність того, що Z вгадає $Hash(m)$ повідомлення m складе L_{bh}^{-1}. Ймовірність того, що Z обере для вгаданого h повідомлення, навіть за умов, що йому відомі усі пари

$$(m, Hash(m)) : P_v(L_{bh}, L_{bm}) = 2^{(L_{bm} - L_{bh})}$$

Дійсно, кількість геш значень для дійсних повідомлень складе $2^{L_{bm}}$, коли простір геш значень складе $2^{L_{bh}}$. Так як $L_{bh} > L_{bm}$, тоді

$$\forall h \in H : \exists m \in M : h = Hash(m).$$

Встановимо ймовірність того, що Z вгадає обране значення m, навіть так що $m \notin M$:

$$P_h(L_{bh}) = 2^{-L_{bh}}$$

Тепер можемо обрахувати складність екзистенційної та селективної підробки на схеми цифрового підпису. Для селективної підробки повідомлення m_1' з вірного повідомлення $\{m_1, m_2, \ldots m_k\}$ зловмиснику Z необхідно знайти таку пару (r', s'), що є вірним підписом для $\{m_1', m_2, \ldots m_k\}$.

Ймовірність селективної підробки є сумою ймовірностей вгадування значення у j повідомленні та ймовірності вгадування обраного значення. Ймовірність екзістенційної підробки є сумою ймовірностей вгадування значення у j повідомленні, ймовірності існування повідомлення для вгаданого геш значення та складності пошуку такого повідомлення. Складність пошуку повідомлення складає $2^{L_{bm}}$ обчислень/зберігань геш значень, у випадку використання ідеальної функції гешування. За парадоксом днів народження, кількість обчислень можна зменшити до $2^{L_{bm}/2}$.

Необхідно зауважити, що проведення атаки за парадоксом днів народження можливе тільки тоді, коли зловмисник має значення цифрового підпису для знайденого прообразу, та має сенс лише у разі високої активної власника ключа. Таким чином, за умови, що кількість повідомлень у множини, що підписуються дорівнює $k = const, L_{bm} = const$, безпечна кількість сформованих підписів дорівнюватиме $2^{L_{bm}/2}$. Надалі будемо розглядати екзистенційну підробку як атаку, коли Z може сформувати деякий вірний підпис (r', s) для випадкового повідомлення m з одного отриманого вірного підпису (r, s).

Тобто, враховуючи розрахунки та зауваження, ймовірність селективної підробки

$$P_s(k, L_{bh}) = 2^{-L_{bh}} P(k, L_{bh})$$

а ймовірність екзістенційної підробки в гіршому випадку

$$P_e(k, L_{bh}) = P(k, L_{bh}) \cdot 2^{L_{bm} - L_{bh}} \cdot 2^{-L_{bm}}$$

Легко побачити, що $P_e(k, L_{bh}, L_{bm}) = P_s(k, L_{bh})$. Надалі будемо використовувати $P_e(k, L_{bh})$.

Вирахуємо відповідну до атаки селективної підробки кількість бітів захисту:

$$\xi(k, L_{bh}) = \left\lceil log_2 \left(P_s(k, L_{bh}) \right)^{-1} \right\rceil. \quad (5)$$

Засновуясь на розрахунках, розглянемо можливість існування оптимальної схеми для скорочених повідомлень. Будемо вважати, що оптимальна схема існує, якщо для заданого рівня стійкості, що дорівнює Ξ бітам захисту, існує деяка функція $\mu(x)$, для якої справедливі наступні твердження:

$$\begin{cases} \psi(x) = \mu \circ Hash(x) \\ L_b(m_1 \| m_2 \| \ldots m_k) \geq \\ \quad \geq L_b\left(\psi(m_1) \| \psi(m_2) \ldots \| \psi(m_k)\right) + L_b(S). \end{cases} \quad (6)$$

Нескладно побачити, що якщо $\mu(x)$ існує та має наведені властивості, тоді Δ для схеми відповідає визначеному критерію (2).

Визначимо

$$\mu(x) = MSB(x, \varepsilon), \quad (7)$$

де $MSB(x, n)$ функція що вертає n старших бітів значення x та ε деяке таке значення, що

$$\forall m \in [m_1, m_2, \ldots m_k] : \varepsilon = \xi(k, L_b(\psi(m))) \geq \Xi. \quad (8)$$

Підставимо (6) до (8) та спростимо, враховуючи (7) та $\forall m \in \{m_1, m_2, \ldots m_k\} : L_b(m) = const$:

$$k(L_{bm} - \varepsilon) \geq L_b(S). \quad (9)$$

Знайдемо необхідну кількість повідомлень в множині, та ε, для створення ідеальної схеми (для випадку $L_{bm} = \Xi$):

$$\begin{cases} \xi(k, \varepsilon) \geq \Xi \\ k(\Xi - \varepsilon) \geq L_b(S) \end{cases} \quad (10)$$

Для підписів з доповненням, $L_b(S) = 4\Xi$.

Одним з рішень (10) є

$$\{k = 9, \varepsilon = \left\lceil ((\sqrt{65} - 7) * \Xi)^{-1} \right\rceil\}.$$

Наведемо приклад. Нехай $\Xi = 128$, тоді $L_b(S) = 2 * 256 = 512$, та $\varepsilon = 68$, $\lceil \xi(k, \varepsilon) \rceil = 128 = \Xi$. Безпечна кількість підписів становитиме 2^{64}.

Змінимо (10) для випадку $L_{bm} < \Xi$ (стисле повідомлення):

$$\begin{cases} \xi(k, \varepsilon) \geq \Xi \\ k(L_{bm} - \varepsilon) \geq L_b(S) \end{cases} \quad (11)$$

Наведемо приклад. Нехай $\Xi = 128$ та $L_{bm} = 80$. Обчислимо мінімальне k та ε такі, що кількість бітів захисту задовольняє Ξ.

$$\varepsilon = \left\lfloor L_{bm} - \frac{-\left(\sqrt{80\Xi^2 - 16 L_{bm}\Xi + {L_{bm}}^2} - 8\Xi - L_{bm}\right)}{2} \right\rfloor = 66$$

$$k = 4E(L_{bm} - \varepsilon)^{-1} = 8 \quad (12)$$

$$\xi(8, 80 - 14) = 130$$

Для створення ідеальної схеми з підпису з доданком з характеристиками $\Xi = 128$ та L_{bm} досить групи з $14 * 37 > 128 * 4 - 37$ повідомлень.

Зробимо висновок про існування схем, що задовольняють (2).

Необхідно зауважити, що у випадку, коли $L_{bm} < \Xi$, складність екзистенційної підробки становить не більше $2^{\varepsilon/2}$ та ймовірність проведення атаки для другої множини підписів $P_{e2}(\varepsilon, L_{bm}) = 2^{\varepsilon - L_{bm}}$.

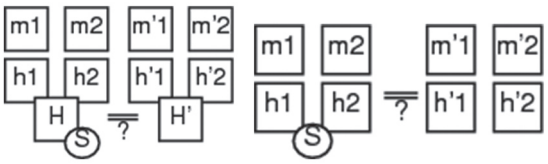
2. ЕЦП З ВІДНОВЛЕННЯМ ПОВІДОМЛЕННЯ

Загальновживаний метод вирішення поставленої задачі полягає у формуванні пакету

$\{M, H, S\}$, де $\forall m_i \in M, i \in [0,n): h_i = Hash(m_i)$, $S = Sign(H, K_a)$, та $Sign$ – алгоритм цифрового підпису з доданком. Схеми цифрового підпису, що базуються на перетвореннях у групі точок еліптичної кривої, мають бути побудовані над полем з бітовою довжиною у двічі більшою ніж заданий рівень стійкості, та зазвичай мають дві компоненти. Схеми гешування повинні мати вихід у двічі більший, ніж заданий рівень стійкості. Таким чином, в загальному випадку цифровий підпис має вдвічі більший обсяг ніж скорочене повідомлення.

Вирішити задачу більш ефективно можливо за рахунок використання підписів з відновленням повідомлення. Ці схеми більш відповідають встановленої семантиці.

Розглянемо схематичне зображення процесу підпису двох скорочених повідомлень. На рис. 1 зображено підпис з використанням підписів з доповненням. В процесі підпису формується нове геш значення H, що приймає участь в формуванні даних підпису. На відміну від схеми з доповненням, при використанні ЕЦП з відновленням (рис. 1 *а*) додаткове геш значення не формується: з підпису відновлюються безпосередні геш значення повідомлень, що потім мають бути перевірені окремо.



а *б*

Рис. 1. Підпис скорочених повідомлень з доповненням (*а*) та відновленням (*б*)

Схеми з відновленням повідомлення дозволяють скоротити $L_b(S)$. Це дозволяє зменшити кількість повідомлень в множині ідеальної схеми. Необхідно зауважити, що виграш можливо отримати тільки якщо множина геш-значень повідомлень буде цілком відновлена з підпису. В іншому випадку, схема зводиться до ЕЦП з доданком.

Повернемося до прикладу. Нехай $\Xi = 128$ та $L_{bm} = 80$. Обчислимо мінімальне k та ε такі, що кількість бітів захисту задовольняє Ξ для абстрактної схеми з відновленням повідомлення, що може відновлювати повідомлення з довільним L_{bh}.

$$\varepsilon = L_{bm} - \frac{-\left(\sqrt{24E^2 - 8L_{mb}E + L_{bm}{}^2} - 4E - L_{bm}\right)}{2} = 66$$
$$k = 2E(L_{bm} - \varepsilon)^{-1} = 18 \qquad (13)$$
$$\xi(18,66) = 128.$$

Для створення ідеальної схеми з підпису з доданком з характеристиками $\Xi = 128$ та L_{bm} досить групи з 19 повідомлень. Легко побачити, що використання підписів з відновленням повідомлення дозволяє створювати ідеальні схеми з кількістю повідомлень майже в двічі меншою.

Надалі будемо розглядати підписи з відновленням повідомлення.

3. КРИТЕРІЇ ВИБОРУ ОПТИМАЛЬНОЇ СХЕМИ ЕЦП ДЛЯ ПІДПИСУ МНОЖИН СКОРОЧЕНИХ ПОВІДОМЛЕНЬ

Задача підпису множин скорочених повідомлень є частковим випадком задачі підпису довільного повідомлення. Тому, довільні умовні та безумовні критерії оцінки перетворень ЕЦП з доданком можуть бути застосовані і для цього випадку.

Проаналізуємо п'ять алгоритмів, що засновано на перетвореннях у групі точок еліптичної кривої, з відновленням повідомлення стандарту ISO/IEC 9796-3 за наведеними критеріями. Надалі під підписами будемо розуміти ECNR, ECMR, ECAO, ECPV та ECKNR з стандарту ISO/IEC 9796-3.

Наведемо загальні безумовні та умовні критерії.

• *Експоненційна складність атаки повного, універсального розкриття.*

Усі підписи побудовані схемою подібною до класичної NR (наведено на рис. 1.б). Захист від атаки повного розкриття забезпечуються незворотнім перетворенням у групі точок еліптичної кривої та має експоненційну складність, для усіх підписів.

• *Практична захищеність схем ЕЦП від відомих атак.* Підписи з відновленням повідомлення базуються на схемі Ніберг-Рюпеля, та мають властивості подібні до інших підписів, що базуються на цій схемі. Таким чином, складність атаки повного розкриття та універсальної підробки еквівалентні ДСТУ 4145. Складність селективної та екзистенційної підробки підписів співпадає с задачею пошуку першого та другого прообразу геш значень повідомлень, що підписуються.

• *Відсутність слабких особистих ключів.* Для підписів з відновленням повідомлення дійсні дослідження стосовно слабких особистих ключів, що проведено до інших схем ЕЦП, заснованих за схемою Ніберг-Рюпеля. ДСТУ 4145 є однією з таких схем ЕЦП. Відомостей щодо слабких особистих ключів для ДСТУ 4145 немає.

• *Використання патентів на алгоритми в схемі ЕЦП, що передбачають ліцензування, та інші обмеження до застосування.* Згідно до звіту комітету JC-27:

– ECNR, ECKNR – не мають запатентованих алгоритмів

– ECPV – має запатентованих алгоритмів, але PVSSR, що є еквівалентом, запатентовано. Дозволяється вільне використання.

– ECAO – запатентовано (JP 3 434 251). Дозволяється вільне використання.

– ECMR – запатентовано (JP H09-160492). Дозволяється вільне використання.

• Відомий світовий досвід використання схеми ЕЦП. Стандартизація на державному та світовому рівнях. Відоме використання схем ЕЦП

з доданком, що засновуються на схемі Ніберг-Рюпеля – ДСТУ 4145. Використання схем з відновленням повідомлення не є розповсюдженою практикою.

– ECNR, ECKNR, ECMR, ECAO – прикладів використання не знайдено

– ECPV – знайдено приклади використання в виробах, що запатентовано в Сполучених Штатах Америки. Зазвичай – ігрові пристрої, засоби RFID. Приклади впровадження (за патентною базою США): US20100062844, US20080045342, US20110131401, US20110119474, US20080069347.

• *Часова складність обчислення підпису.* Доцільно порівнювати часову складність аналітично, використовуючи абстрактний результат для аналізу доцільності використання схеми ЕЦП на визначеному апаратному забезпеченні.

Для оцінки практичних показників схем ЕЦП з відновленням повідомлення було реалізовано макет. Експериментально встановлено, що часові характеристики схем ЕЦП не розрізняються. Найбільш витратні перетворення у групі точок еліптичної кривої, що займають 80% витраченого часу, та накладні операції – 10%. Якщо визначити показники як (E,S,O) як E – витрачено на перетворення у групі точок еліптичної кривої, S – витрачено на інші криптографічні перетворення, O – витрачено на взаємодію з ОС, та $E+S+O=1$, тоді

– $ECNR=(0.81,0.03,0.16)$

– $ECKNR=(0.82,0.06,0.13)$

– $ECAO=(0.81,0.033,0.153)$

– $ECMR=(0.81,0.029,0.16)$

– $ECPV=(0.81,0.02,0.17)$

• *Просторова складність обчислення підпису.* Просторова складність обчислення для всіх підписів знаходиться на одному рівні. Експериментально дослідити відмінність не вдалося.

Оберемо критерії, що є винятковими для схем ЕЦП підпису множин скорочених повідомлень:

• *Максимальний обсяг повідомлення, що відновлюється.* Покращення показника Δ можлива за рахунок скасування підсумкового гешування. Кількість гешів повідомлень, що можна відновити, зумовлює обмеження використання схеми на великих множинах скорочених повідомлень.

Для схем ЕЦП з відновленням з стандарту ISO/IEC 9796-3 дійсні наступні твердження:

– $ECNR, ECMR, ECKNR$ – $L_b(n-1)$, де n – бітова довжина поля ЕК

– $ECPV$ – довільна

• *Мінімальний обсяг повідомлення, що відновлюється.* Погіршує показник Δ за рахунок збільшення доданої частини повідомлення на малих множинах та повідомленнях.

Для схем ЕЦП з відновленням з стандарту ISO/IEC 9796-3 дійсні наступні твердження:

– $ECNR, ECMR, ECKNR$ – $L_b(n-1)$, де n – бітова довжина поля ЕК

– $ECPV$ – позначення обсягу – 2 байти

• *Можливість використовувати власний алгоритм формування відновлених даних.* Для підпису поодиноких повідомлень стандартами ЕЦП з відновленням повідомлень передбачається надання додаткової збитковості, для можливості перевірки підпису. В випадку вирішення задачі з підписом множини повідомлень та визначеними умовами, в визначенні додаткової збитковості немає необхідності -- повідомлення перевіряються окремо. Визначені алгоритми обчислення додаткової збитковості зменшують обсяг повідомлення, що можна відновити, та зменшують Δ.

– ECNR, ECKNR, ECMR – дозволяють використовувати довільні алгоритми формування частини що відновлюється.

– ECPV – додає значення довжини повідомлення до повідомлення що відновлюється

– ECAO – визначає алгоритм формування, але можливо використовувати схему з відсутньою додатковою збитковістю.

• Показник Δ

ECNR, ECMR, ECKNR, ECAO мають однакові обмеження щодо максимального/мінімального обсягу повідомлення. З (11) та (10) легко побачити, що не можливо створити ідеальну схему ЕЦП для підпису скорочених повідомлень за допомогою наведених алгоритмів -- загальний обсяг повідомлень, що необхідно утворювати для є значно більшою, ніж $n-1$ біт, де $n=2\Xi$, що можна відновлювати з цих підписів. Дійсно, якщо для створення ідеальної схеми необхідно знайти додаткові 2Ξ біт, та 2Ξ біт є максимальним обсягом, тоді кількість біт, що може бути використана для формування геш значеннь повідомлень становитиме $2\Xi-2\Xi=0$ бітів.

ECPV – не має обмежень на повідомлення що відновлюється. Згідно з (11) та (10) ідеальна схема для скорочених повідомлень може бути створена.

ВИСНОВКИ

В системах, де необхідно журналювати, або зберігати з інших причин отримані підписані повідомлення, постає питання ефективності використання простору.

В загальному випадку, ЕЦП електронного документу займає обсяг менший, ніж сам документ. У разі, коли документ є меншим за підпис не доцільно використовувати стандартні схеми ЕЦП з доданком. Використання ЕЦП з доданком збільшує загальний обсяг повідомлення з підписом більше ніж на 100%.

Запропоновано показник для схем ЕЦП – відсоток збільшення повідомлення. Запропоновано критерій ефективності та порівняння – збільшення повідомлення не має перевищувати 100%.

Запропоновано визначення скороченого повідомлення як такого, чий бітовий обсяг є

меншим, ніж бітовий обсяг геш значення необхідного для забезпечення визначеного рівня стійкості від селективної підробки.

Проаналізовано часний випадок - користувач ЕЦП підписує множину повідомлень скорочених повідомлень

Доведено можливість створення схем, збільшення повідомлень яких не перевищує 100%.

Визначено, що такі схеми можуть бути створені за допомогою ЕЦП з відновленням повідомлення стандарту ISO/IEC 9796-3 ECPV

Визначено, що серед інших підписів з відновленням повідомлення, що базуються на перетвореннях в групі точок ЕК, стандарту ISO/IEC 9796-3 немає таких, що мають переваги над ECPV

Пропонується використовувати ECPV для схем підписів скорочених повідомлень

Література

[1] ISO/IEC 9796-3: Discrete logarithm based mechanisms. – 2006

[2] Digital Signature Standart (DSS): FIPS 186-3

[3] Daniel R. L. Brown , Don B. Johnson, Formal Security Proofs for a Signature Scheme with Partial Message Recovery/ Lecture Notes in Computer Science.

Надійшла до редколегії 12.04.2012

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

УДК 681.3.07

Схемы ЭЦП для групп подписей маленьких сообщений / О.А. Шевчук // Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 240–244.

Предлагается метод формирования ЭЦП для множеств маленьких сообщений с отсутствующей избыточностью. Предлагается критерий эффективности для подобных схем

Ключевые слова: ЭЦП, восстановление сообщения, оптимизация вычислений.

UDC 681.3.07

Digital signtature schemes for sets of small messages / O.A. Shevchuk // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 240–244.

The paper proposes the method of DS generation for sets of small messages with missing data redundancy and efficiency criteria for such schemes.

Keywords: DS, message recovery, optimization of calculations.