УДК 681.3.06

Додаткові властивості безпеки електронних транзакцій у системах, що використовують сервіси комбінованої ІВК

Ю. М. Іщенко, А. В. Лєншин
Харківський національний університет радіоелектроніки, Україна

Рассматривается решение задачи обеспечения непередаваемости электронной цифровой подписи (ЭЦП) и скрытости исходного сообщения на основе использования хамелеон-подписи, применимой в комбинированной инфраструктуре открытых ключей. Показывается, что хамелеон-подпись является результатом последовательного применения хеш-хамелеона и базовой ЭЦП, что позволяет обеспечить новые свойства безопасности и стойкость не ниже стойкости базовой ЭЦП. Изложены схемы формирования и проверки хамелеон-подписи. Рассмотрено как обеспечиваются заявленные свойства безопасности при злоумышленном поведении получателя.

Ключевые слова: *электронная цифровая подпись, хеш-хамелеон, комбинированная инфраструктура открытых ключей.*

Розглядається розв'язання завдання забезпечення непередаваності електронного цифрового підпису (ЕЦП) та прихованості вихідного повідомлення на основі застосування хамелеон-підпису, що застосовний у комбінованій інфраструктурі відкритих ключів. Показується, що хамелеон-підпис є результатом послідовного застосування геш-хамелеону та базової ЕЦП, що дозволяє забезпечити нові властивості безпеки та стійкість не нижчу за стійкість базової ЕЦП. Викладені схеми формування та перевіряння хамелеон підпису. Розглянуто як забезпечуються заявлені властивості безпеки при зловмисній поведінці отримувача.

Ключові слова: *електронний цифровий підпис, геш-хамелеон, комбінована інфраструктура відкритих ключів.*

The problem solving based on using chameleon-signature in a combined public key infrastructure for providing non-transferability of digital signature and original message hiding is considered. The scheme of sequential applying of chameleon hash and original digital signature resulting in chameleon-signature that has new security properties and resistance not less than resistance of original digital signature is shown. The provision of new security properties in case of malicious behavior of reception is discussed.

Key words: *digital signature, chameleon hash, combined Public Key Infrastructure.*

Вступ

Прискорений розвиток інформаційних технологій та системи Інтернет призводить поширення електронного документообігу майже у всіх сферах діяльності людини. На зміну звичайним паперовим документам приходять електронні, що значно спрощує розповсюдження, копіювання, зберігання та знищення інформації на всіх етапах бізнес-процесу. Введення електронного документообігу призвело до необхідності забезпечення послуг автентичності електронного повідомлення та властивості неспростовності. Ці послуги вдало надає механізм електронного цифрового підпису (ЕЦП). Але для деяких сучасних систем, пов'язаних з електронною комерцією (наприклад, систем таємного голосування, клієнт-банк систем, анонімних аукціонів) цих послуг виявилося недостатньо [1]. Необхідними вимогами для захищеного

функціонування подібних систем є забезпечення властивостей непередаваності ЕЦП та прихованості повідомлення. Під вимогою непередаваності розуміється неможливість доведення валідності ЕЦП будь-якій третій стороні без участі підписувача. Вимога прихованості полягає у відсутності необхідності розкриття змісту повідомлення третій стороні у ході вирішення можливих протиріч [1-4].

Звичайно, забезпечення автентичності повідомлення та неспростовності джерела та відправлення залишається обов'язковим. Важливо і те, що при умові забезпечення усіх вищенаведених властивостей, авторизований суддя повинен мати можливість визначити валідність відповідного підписаного документу. Актуальною задачею є визначення шляхів надання нових послуг безпеки у системах електронного документообігу, які цього потребують.

1. Комбінована ІВК та властивості геш-хамелеону

Орієнтуючись на національну систему електронного документообігу у якості легітимної системи асиметричної криптографії будемо розглядати інфраструктуру відкритих ключів (ІВК). ІВК є сукупністю програмно-апаратних та організаційно-технічних засобів, що дозволяють користувачу використовувати у системах захисту інформації криптографію з відкритими ключами [5,6]. ІВК призначена для забезпечення шифрування та надання послуг ЕЦП. Але останнім часом у літературі з'явилося багато посилань на суттєві недоліки існуючої ІВК [7]. Тому важливим напрямом вдосконалення систем асиметричної криптографії в Україні, є створення комбінованої ІВК з метою усунення існуючих недоліків стандартної ІВК [8]. Створення комбінованої ІВК передбачає об'єднання ІВК та системи на базі ідентифікаторів (СНБІ [9,10]) на відповідних рівнях ієрархії. Тобто ІВК – на верхніх рівнях ієрархії, та СНБІ – на нижньому. Таке об'єднання дозволить вирішити багато протиріч, та об'єднати переваги обох систем (ІВК та СНБІ).

Повернемося до необхідності забезпечення властивостей інноваційного характеру у комбінованій ІВК. Механізмом, що дозволяє забезпечити властивості непередаваності та прихованості є геш-хамелеон (разом з ЕЦП – хамелеон-підпис) [1-4]. Геш-хамелеон представляє собою геш-функцію з лазівкою. Іншими словами, геш-хамелеон – це геш-функція, що є колізійно-стійкою без знання секретного ключа отримувача, та задовольняє деяким спеціальним вимогам, в тому числі непередаваності та прихованості.

Цікаво, що геш-хамелеон може "співпрацювати" з будь-яким алгоритмом ЕЦП. Для того, щоб автентифікувати повідомлення m, відправник (підписувач) обчислює його геш-значення, використовуючи геш-хамелеон. Потім підписує це геш-значення, використовуючи будь-який основний алгоритм ЕЦП. Таким чином досягається вимога сумісності геш-хамелеону з різними алгоритмами ЕЦП.

Визначимо основні властивості, що забезпечує використання геш-хамелеону у стандартних протоколах ЕЦП:

– неінтерактивність – можливість перевірки підпису off-line;

– сумісність – можливість узгодженої роботи зі стандартними протоколами ЕЦП;

– стійкість, що базується на вирішенні задач дискретного логарифму та факторизації у залежності від обраного протоколу ЕЦП;
– реверсивність – можливість перетворення хамелеон-підпису у стандартний (при необхідності);
– непередаваність та прихованість підписаного повідомлення.

2. Алгоритм формування геш-хамелеону

Для більш чіткого розуміння механізму геш-хамелеону, у якості прикладу розглянемо геш-хамелеон на ідентифікаторах (ID) [2], схема якого представлена на рис.1.

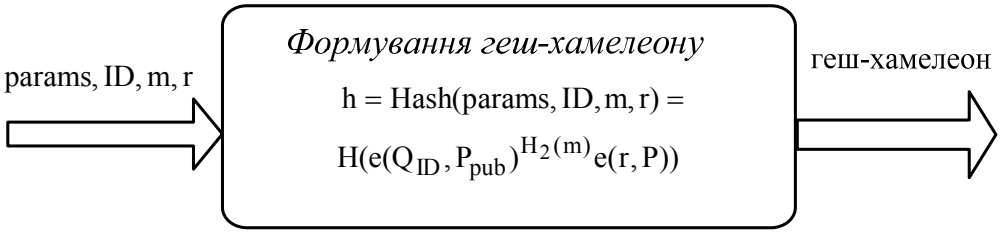

Рис. 1. Схема формування геш-хамелеону

На рис.1 використано позначення: $\text{params} = \langle G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H \rangle$ – відкриті системні параметри, G_1 – циклічна адитивна група з генератором групи P, q – порядок P, G_2 – циклічна мультиплікативна група порядку q, $e: G_1 \times G_1 \to G_2$ – спарювання, $H_1\{0,1\} \to G_1$, $H_2: \{0,1\} \to Z_q$, $H: G_2 \to \{0,1\}^n$ - геш-функції (n – довжина повідомлення, Z_q – кільце цілих чисел порядку q), $\text{ID} \in \{1,0\}^n$ – ідентифікаційні дані отримувача, m – повідомлення. Ключова пара отримувача: $Q_{ID} = H_1(ID) \in G_1$, $B = sQ_{ID}$ –відкритий та секретний ключі отримувача відповідно. Ключова пара третьої довіреної сторони (ТДС): $P_{pub} = sP$ – відкритий ключ, s – майстер-ключ.

Функціонування геш-хамелеону на ID можна подати у вигляді 4-х алгоритмів:
– установка системних параметрів;
– обчислення ключів;
– гешування;
– формування підробки.

Розглянемо докладніше кожен з них.

Установка системних параметрів безпосередньо генеруються params .

Обчислення ключів алгоритм обчислює $Q_{ID} = H_1(ID) \in G_1$ та встановлює інформацію про лазівку $B = sQ_{ID}$.

Гешування. Маючи $params = \langle G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H \rangle$, $\text{ID} \in \{1,0\}^n$, випадкове $r \in G_1$ та m, підписувач обчислює геш-значення. Алгоритм завжди запускається підписувачем. У результаті виконання цього етапу, маємо:

– $Q_{ID} = H_1(ID) \in G_1$ – відкритий ключ отримувача;

– $h = \mathrm{Hash}(params, ID, m, r) = H(e(Q_{ID}, P_{pub})^{H_2(m)} e(r, P))$ – геш-хамелеон.

Формування підробки. Маючи $params$, ідентифікаційні дані ID, інформацію про лазівку B, що пов'язана з ID, повідомлення m', та геш-значення h від повідомлення m, алгоритм обчислює $r' \in G_1$.

Алгоритм підробки реалізується наступним чином (рис. 2): $\mathrm{Forge}(params, ID, m, r, h, m') = r' = H_2(m)B + r - H_2(m')B$.

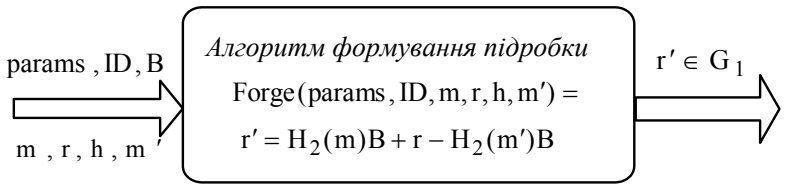

Рис. 2. Схема алгоритму формування підробки

Тобто, у разі виникнення протиріч, наприклад, якщо отримувач повторно використовує геш-значення для підпису іншого повідомлення, відправник може довести знання геш-колізії, так як підписане та заявлене повідомлення будуть мати однакове геш-значення.

3. Алгоритм хамелеон-підпису на ідентифікаторах

У якості приклада хамелеон-підпису, розглянемо механізм, що представлений у роботі Du та Wanga [2]. Почнемо з визначення учасників інформаційного обміну та установки необхідних параметрів.

Учасники. Підписувач та отримувач. Суддя, що необхідний для вирішення протиріччя між підписувачем та отримувачем.

Ключі. Ключова пара підписувача: VK_S та SK_S – відкритий та секретний ключі відповідно. Ключова пара отримувача, що були визначені у алгоритмі геш-хамелеону: ID – відкритий ключ підписувача та секретний ключ або інформація про лазівку $B = sQ_{ID}$.

На рис. 3 представлена схема алгоритму генерації хамелеон-підпису на ідентифікаторах:

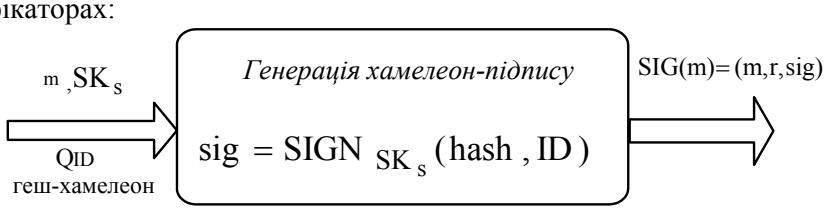

Рис. 3. Схема алгоритму генерації хамелеон-підпису

Генерація хамелеон-підпису на ідентифікаторах-CHAM-SIG.

Підписувач має: повідомлення m, свій секретний ключ SK_S, та ID.

– Генерується геш-хамелеон повідомлення m, обирається випадкове $r \in G_1$ та обчислюється: $h = \mathrm{Hash}(params, ID, m, r) = H(e(Q_{ID}, P_{pub})^{H_2(m)} e(r, P))$.

– Розраховується $sig = SIGN_{SK_s}(hash, ID)$.

ЕЦП повідомлення m має вигляд: $SIG(m) = (m, r, sig)$.

На рис. 4 представлена схема алгоритму перевірки хамелеон-підпису на ідентифікаторах:

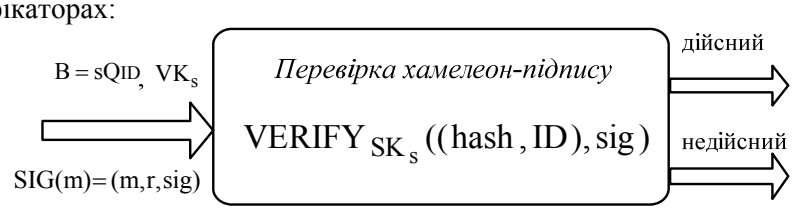

Рис. 4. Схема перевірки хамелеон-підпису

Перевірка хамелеон-підпису на ідентифікаторах – CHAM-VER.

Отримувач має: підпис $SIG(m) = (m, r, sig)$, відкритий ключ підписувача VK_S, інформацію про лазівку (або свій секретний ключ) $B = sQ_{ID}$.

Обчислює $hash = Hash(params, ID, m, r)$.

Перевіряє дійсність підпису: $VERIFY_{SK_s}((hash, ID), sig) = valid$.

Вирішення протиріччя. У разі виникнення суперечки з приводу валідності підпису, отримувач звертається до авторизованого судді J.

1. Отримувач надсилає судді $SIG(\hat{m}) = (\hat{m}, \hat{r}, \hat{sig})$. Суддя перевіряє підпис, використовуючи CHAM-VER. Якщо перевірка не проходить, суддя вважає підпис недійсним.

2. Якщо перевірка першого кроку пройшла вдало, суддя J надсилає підписувачу $SIG(\hat{m}) = (\hat{m}, \hat{r}, \hat{sig})$, і вимагає прийняти/відмовитися від факту підпису.

3. Якщо підписувач хоче довести, що підпис є недійсним , він повинен представити колізію функції геш-хамелеона.

Генерація колізії:

Вхідними даними служить підробка $SIG(m') = (m', r', sig)$.

1. Підписувач використовує оригінальні m,r для обчислення sig.

$Hash(params, ID, m, r) = Hash(params, ID, m', r')$, поки $m \neq m'$.

2. Підписувач обчислює $B = \dfrac{r' - r}{H_2(m) - H_2(m')}$.

3. Підписувач обирає будь-яке повідомлення $\tilde{m}$ та обчислює $\tilde{r} = \dfrac{H_2(m) - H_2(\tilde{m})}{H_2(m) - H_2(m')}(r' - r) + r$.

4. Вихідними даними алгоритму будуть $(\tilde{m}, \tilde{r})$.

Надавши $SIG(\tilde{m}) = (\tilde{m}, \tilde{r}, sig)$, підписувач доводить, що $SIG(m') = (m', r', sig)$ є підробкою.

4. Висновки

Як було зазначено, ІВК не задовольняє вимогам багатьох бізнес-систем, що пов'язані з електронною комерцією. Одним із шляхів вдосконалення існуючої ІВК є створення комбінованої ІВК, тобто об'єднання класичної інфраструктури відкритих ключів з системами, що базуються на ідентифікаторах. Таке об'єднання, окрім вирішення проблемних питань, що супроводжують ІВК, надало б можливість впровадження геш-хамелеону (хамелеон-підпису). Впровадження геш-хамелеону стало б можливим за рахунок наявності СНБІ на нижніх рівнях комбінованої ІВК , адже вона лежить у основі геш-хамелеону.

Математичний апарат геш-хамелеону базується на спарюваннях в групі точок еліптичних кривих, завдяки чому стійкість схеми ґрунтується на класичній задачі складності вирішення проблеми дискретного логарифму в групі точок еліптичної кривої, тобто є достатньо високою. Важливо, що стійкість хамелеон-підпису ґрунтується на стійкості алгоритму стандартної ЕЦП, що обрана.

Отже впровадження геш-хамелеону (хамелеон-підпису) у комбіновану ІВК дозволить задовольнити вимоги інноваційного характеру систем електронного документообігу, а саме непередаваність ЕЦП та прихованість підписаного повідомлення.

ЛІТЕРАТУРА

1. G. Ateniese and B. de Medeiros, Identity-based chameleon hash and applications, CryptologyePrint Archive, http://eprint.iacr.org/2003/167/.
2. Xinjun Du, Ying Wang, Jianhua Ge and Yumin Wang ,Chameleon Signature from Bilinear Pairing
3. H. Krawczyk and T. Rabin, Chameleon signatures. In Proceedings of NDSS 2000, pp. 143-154,2000.
4. F. Zhang, R. Safavi-Naini, and W. Susilo. ID-based Chameleon hashes from bilinear pairings. http://eprint.iacr.org/2003/208.
5. ITU-T (International Telecommunications Union) Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework. 2000
6. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. – М.: Горячая линия – Телеком, 2004 – 246с.
7. Горбенко І.Д., Онопрієнко В.В. та ін. Стан та проблемні питання створення та розвитку Національної ІВК. Прикладна радіоелектроніка. Том.5 №1 2006 С. 41-51
8. A. Shamir, Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO `84, LNCS 196, pages 47-53, Springer-Verlag, 1984.
9. D. Boneh and M. Franklin, Identity-based Encryption from the Weil pairing, Proceedings of CRYPTO 2001, LNCS 2139, pages 213-229, Springer-Verlag, 2001.

Надійшла 24.03.2010.