УДК 004.23

Ю.М. Лєншина, Д.С. Беляк

Харківський національний університет радіоелектроніки, Харків

РЕАЛІЗАЦІЯ ПОСЛУГИ ПРИВАТНОСТІ У СХЕМІ ІНТЕРНЕТ-АУКЦІОНУ З ВИКОРИСТАННЯМ ХАМЕЛЕОН-ПІДПИСУ

Наводиться розв'язок завдання криптографічної підтримки послуги приватності (непередаваність електронного цифрового підпису та прихованість змісту пропозиції) у схемі інтернет-аукціону. Розглянуто процедури формування та перевіряння хамелеон-підпису. Виконано аналіз захищеності запропонованої схеми інтернет-аукціону від зловмисних дій учасників або власника аукціону.

Ключові слова: *електронний цифровий підпис, хамелеон-підпис, інтернет-аукціон.*

Вступ

Стрімкий розвиток інформаційних технологій та мережі Інтернет призвели до появи низки нових сервісів, серед яких помітними є інтернет-аукціони. Це достатньо молода, але перспективна сфера електронної комерції. Обіг інтернет-аукціонів сьогодні можна порівняти з обігом решти роздрібної торгівлі через Інтернет. Щорічно на них здійснюють угоди більш мільйону користувачів Інтернету. Популярності цій сфері надає той факт, що приймати участь у аукціонах можна навіть сидячи вдома.

Розвиток сфери призвів до необхідності забезпечення таких послуг як: доступність, автентичність повідомлення та неспростовність. Але для деяких видів інтернет-аукціонів, де необхідно приховувати зроблену ставку (наприклад, закриті інтернет-аукціони) цих послуг – недостатньо. Для роботи таких систем необхідно реалізувати послугу приватності.

У роботі пропонується забезпечувати криптографічну підтримку цієї послуги за рахунок використання властивостей хамелеон-підпису. У такому контексті приватність буде забезпечуватися за рахунок непередаваності електронного цифрового підпису (ЕЦП) та прихованості повідомлення (тобто ставки). Вимога непередаваності полягає у неможливості доведення справжності ЕЦП будь-якій третій стороні без участі учасника аукціону.

Властивість прихованості повідомлення полягає у відсутності необхідності розкриття змісту повідомлення третій стороні при вирішенні можливих протиріч.

Схеми інтернет-аукціонів та вимоги до них

Основними ознаками класифікації схем аукціонів слід вважати напрямок зроблених ставок, та ступінь відкритості.

Інтернет-аукціони поділяються за напрямком зроблених ставок на:

1. Зростаючі – кожна наступна ставка повинна бути вище, ніж попередня.
2. Спадаючі – кожна наступна ставка повинна бути нижче, ніж попередня.

За ступенем відкритості торги на аукціоні можна поділити на закриті та відкриті. До відкритих відносяться:

1. Стандартний (англійський) – використовується відкритий формат пропозицій, учасники пропонують ціну на виставлений товар в порядку її зростання, перемагає той учасник, який запропонував найбільшу ставку в період проведення аукціону.
2. Голандський – використовується відкритий формат пропозицій, але торги починаються з завчасно завищеної невигідної ціни, яка послідовна знижується поки один з учасників не погодиться з нею.
3. Подвійний – пропозиції одночасно надходять від власника та учасника аукціону (встановлюється рівноважна ціна), найбільш поширений на електронних біржах.

До закритих аукціонів відносяться:

1. Аукціон одночасної пропозиції – усі учасники встановлюють ціну на товар, не знаючи цін, які встановили опоненти, перемагає той, хто запропонував найбільшу ціну.
2. Аукціон закритих пропозицій – учасник та власник аукціону роблять пропозиції, що зберігаються в таємниці у період встановленого часу, переможець купує товар за ціною, яка йде передостанньою у пропозиціях (наприклад, учасник А пропонує \$10 за товар, В – \$20, С – \$30, тоді учасник С – перемагає, але сплачує ціну запропоновану учасником В).

Оскільки при проектуванні інтернет-аукціону необхідно зберігати рівновагу між оптимальною кількістю учасників, швидкістю обробки пропозицій та захищеністю системи, слід враховувати такі вимоги:

1. Клієнтське програмне забезпечення, повинне бути простими, наприклад веб-браузер або навіть клієнт передачі текстових повідомлень (прототип IM-клієнтів).

2. Використання протоколу, який не зберігає стани клієнтських операцій після закінчення аукціону – чим менший час існування інформації існує, тим легше її контролювати (забезпечувати необхідний рівень захищеності).

3. Складність протоколу зв'язку визначається об'ємом та кількістю повідомлень (кількість повідомлень впливає на швидкість аналізу та роботи протоколу, в той час як об'єм впливає на смугу пропускання).

4. Асинхронність комунікаційної моделі - єдиний випадок, коли власник та учасники аукціону можуть домовитись, чи було доставлене повідомлення вчасно або після закриття аукціону.

5. Гнучкість правил – у кожному типі аукціону повинні бути свої методи знаходження кінцевої ціни, тобто повинен бути свій математичний апарат.

Так як у відкритих аукціонах кожен учасник аукціону має змогу бачити пропозиції опонентів, то вони потребують забезпечення лише основних властивостей повідомлення, в той час як у закритих аукціонах необхідно забезпечити додаткові властивості повідомлення, серед яких:

1. Коректність – переможець та кінцева ціна повинні бути коректно визначені після завершення аукціону.

2. Конфіденційність – пропозиції мають залишатися у таємниці до завершення аукціону (також може встановлюватися вимога, прихованості усіх програшних пропозицій навіть після завершення аукціону), при вирішенні суперечностей ця вимога також не повинна порушуватись.

3. Справжність – жоден учасник не може змінити свою ціну після завершення аукціону, також висувається вимога щодо наявності алгоритму перевірки справжності учасників для запобігання підвищення ціни за допомогою бот-учасників.

4. Неспростовність – учасник аукціону не повинен мати змогу відмовитись від зробленої їм ставки.

5. Надійність – жодна зі сторін не повинна мати змоги навмисно чи випадково поставити під загрозу правильне функціонування системи.

6. Непередаваність – відсутність необхідності передачі ставок третій стороні у разі вирішення суперечностей.

Протокол інтернет-аукціону, що використовує механізм хамелеон-підпису

Складність проведення закритих інтернет-аукціонів полягає у тому, що його учасники надсилають ставки, значення яких мають зберігатися у таємниці від інших учасників, але при цьому мають існувати гарантії того, що за необхідності учасник зможе зробити значення ставки не лише загальнодоступним але і довести її автентичність. У той самий час власник аукціону має бути впевнений у реалізації послуги неспростовності подання ставки учасником.

Такі властивості потребують застосування механізму ЕЦП. У роботі розглядається застосування вдосконаленого базового алгоритму ЕЦП за рахунок його поєднання з геш-хамелеоном. Це поєднання має назву хамелеон-підпису і володіє такими властивостями:

1. Неможливість підробки – жодна третя сторона не може створити правильний набір $m, r, ChamSig$ до генерації його учасником аукціону.

2. Непередаваність ЕЦП – неможливість доведення справжності ЕЦП будь-якій третій стороні без учасника аукціону.

3. Неспростовність – неможливість відмовитись від факту передачі повідомлення.

4. Прихованість повідомлення – відсутність необхідності розкриття змісту повідомлення третій стороні при вирішенні можливих протиріч.

Розглянемо протокол інтернет-аукціону, в якому використовується хамелеон-підпис. У протоколі беруть участь учасник аукціону, власник аукціону та суддя, який необхідний для вирішення протиріч. На вхід алгоритму підпису подається повідомлення m (ставка учасника), особистий ключ учасника аукціону SK та відкритий ключ PK_{Ch-H}. Учасник аукціону генерує загальносистемні параметри

$$params(r, g, q, p, k) \in Z_q$$

та обчислює значення геш-функції за формулою

$$ChamHash(m, r) = g^m \times PK^r \bmod p,$$

де p, g – прості цілі числа, які задовольняють умові $p = k * q + 1$. Далі учасник аукціону формує підпис, $sig(m) = (m, r, ChamSig)$. Схеми формування ЕЦП (учасником аукціону) та його перевірка (власником аукціону) наведені на рис. 1 та 2 відповідно.

Отримавши підпис

$$sig(m) = (m, r, ChamSig)$$

власник аукціону за допомогою відкритого ключа ЕЦП PK та відкритого ключа геш-хамелеону PK_{Ch-H} обчислює геш-значення

$$ChamHash_r(m, r) = ChamHash(m, r) = g^m * y^r \bmod p$$

та перевіряє підпис, використовуючи функцію перевірки

$$VERIFY_{PK}((ChamHash, PK_{Ch-H}), ChamSig) ..$$

Рис. 1. Схема формування хамелеон-підпису

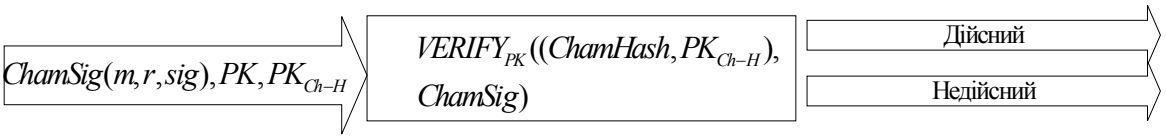

Рис. 2. Схема перевірки хамелеон-підпису

Протокол аукціону складатиметься з наступних кроків:

1. Кожний учасник аукціону підписує повідомлення, яке містить пропозицію із використанням хамелеон-підпису.

Повідомлення містить термін пропозиції та підпис.

2. Власник аукціону підтверджує внесення пропозиції.

3. Власник аукціону оголошує переможця після закінчення аукціону.

Дана схема забезпечує усі властивості, які надає хамелеон-підпис та властивість довіри, так як без доведення валідності підпису неможливо брати участь у аукціоніСправжність всіх підписаних повідомлень після їх подачі може визначити тільки власник аукціону. Він перевіряє підписану заявку, але не може розголосити значення повідомлення. Така схема забезпечує непередаваність ЕЦП та прихованість повідомлення, але якщо зловмисником виявиться власник аукціону, то жоден з учасників аукціону не зможе визначити достовірність тверджень власника аукціону.

Формування підробки повідомлення та вирішення протиріч

В процесі проведення інтернет-аукціону не виключається можливість підробки повідомлення (ставки) власником аукціону. Схема підробки наведена на рис. 3.

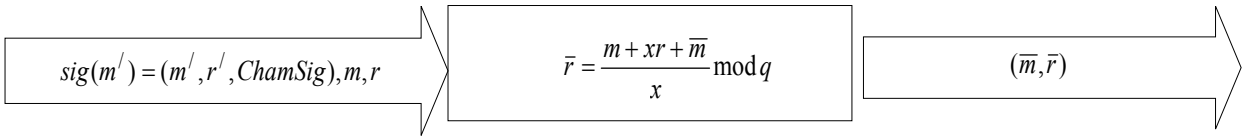

Рис. 3. Схема підробки підпису

Маючи params , значення r, x та геш-значення ChamHash від повідомлення m, власник аукціону може підробити повідомлення, при цьому видаючи оригінальне повідомлення за підроблене. Обчислюється випадкове значення $\bar{r} \in Z_q$ за допомогою виразу $\bar{r} = \frac{m + xr + \bar{m}}{x} \bmod q$. На виході власник аукціону отримує підроблене повідомлення $\bar{m}$ та значення $\bar{r}$.

Для вирішення таких протиріч та виявлення підробленого повідомлення залучається суддя.

За допомогою наступного алгоритму (рис. 4) учасник аукціону доводить судді, що підпис $sig(m') = (m', r', ChamSig), m, r$ – підробка:

1. Учасник аукціону використовує оригінальні m, r для обчислення ChamSig , такі, що $g^m * y^r \bmod p = g^{m'} * y^{r'} \bmod p$ та $m \neq m'$.

2. Учасник аукціону обчислює $x = \frac{m - m'}{r' - r}$

3. Учасник аукціону вибирає будь-яке повідомлення $\bar{m}$ та обчислює $\bar{r} = \frac{m + xr + \bar{m}}{x} \bmod q$

4. Вихідними даними алгоритму є $(\bar{m}, \bar{r})$.

Надавши $sig(\bar{m}) = (\bar{m}, \bar{r}, ChamSig)$, учасник аукціону доводить, що $sig(m') = (m', r', ChamSig)$ є підробкою, що була сформована власником аукціону.

Важливою властивістю запропонованої схеми є те, що власнику аукціону невигідно робити підробку ставок, так як в результаті вирішення протиріччя учасник аукціону зможе створити колізію для повідомлення, що призведе до розкриття довгострокового або сеансового секретного ключа власника аукціону. Такі знання дозволять учаснику аукціону анулювати усі його ставки при розкритті довгострокового ключа та анулювати поточний аукціон при розкритті сеансового ключа.

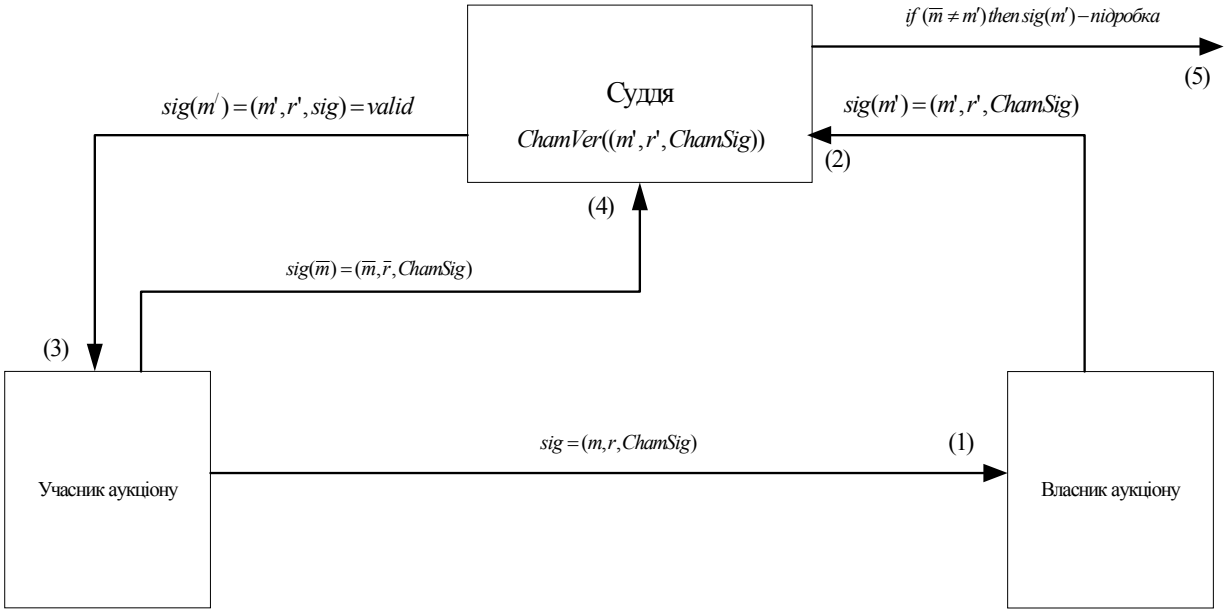

Рис. 4. Схема вирішення протиріч

Висновки

Стан розвитку схем інтернет-аукціонів вимагає криптографічної підтримки послуг, що задовольняють вимоги, які висуваються з боку учасників та власника аукціону. Перелік необхідних для надійного функціонування інтернет-аукціону послуг: неспростовності, цілісності, автентичності, які можуть бути забезпечені за рахунок використання стандартних алгоритмів ЕЦП не є вичерпним. Проведені у роботі дослідження вказують на можливість реалізації послуги приватності (непередаваності ЕЦП та прихованості повідомлення) за рахунок механізму хамелеон-підпису. При цьому поєднання геш-хамелеону разом із стандартним алгоритмом ЕЦП не впливає на стійкість перетворення (хамелеон-підпису).

Результати моделювання алгоритму проведення інтернет-аукціону дозволяють стверджувати про захищеність запропонованої моделі від зловмисних дій з боку власника та учасників аукціону.

Список літератури

1. Baudron O. Non-interactive private auctions / O. Baudron, J. Stern // LNCS, Springer-Verlag. – 2002. – Vol. 2339. – P. 364

2. Ateniese G. Identity-based chameleon hash and applications / G. Ateniese, B. de Medeiros // FC. – 2004. – P. 63-68.

3. Lipmaa H. Secure Vickrey auctions without threshold trust / H. Lipmaa, N. Asokan, V. Niemi // Proc. of the 6th Annual Conference on Financial Cryptography. – 2002.

4. Chen X. Limited verifier signature from bilinear pairings / X. Chen, F. Zhang, K. Kim. – 2004.

Надійшла до редколегії 1.04.2011

Рецензент: д-р техн. наук, проф. О.В. Потій, ЗАТ «ІІТ», Харків.

РЕАЛИЗАЦИЯ УСЛУГИ ПРИВАТНОСТИ В СХЕМЕ ИНТЕРНЕТ-АУКЦИОНА С ИСПОЛЬЗОВАНИЕМ ХАМЕЛЕОН-ПОДПИСИ

Ю.М. Леншина, Д.С. Беляк

Приводится решение задачи криптоподдержки услуги приватности (непередаваемость электронной цифровой подписи и скрытость предложения) в схеме интернет-аукциона. Рассмотрены процедуры формирования и проверки хамелеон-подписи. Выполнен анализ защищенности схемы интернет-аукциона от злоумышленных действий участников или владельца аукциона.

Ключевые слова: *электронная цифровая подпись, хамелеон-подпись, интернет-аукцион.*

IMPLEMENTATION OF PRIVACY SERVICE FOR THE INTERNET AUCTION SCHEME USING CHAMELEON-SIGNATURE

U.M. Lenshina, D.S. Belyak

The solution of the problem of the cryptographic support for privacy service (non-transferability of digital signature and bid hiding) in the scheme of the internet auction is given. Procedures of generation and verification of chameleon signatures are considered. Security analysis of proposed internet auction scheme against malicious actions of auction participants and owner are conducted.

Keywords: *digital signature, chameleon hash, internet-auction.*