УДК 681.12

О. Салієва

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ПРОТОКОЛУ СЛІПОГО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ЧАУМА

Вінницький національний технічний університет

Анотація

В доповіді здійснено аналіз захищеності протоколу сліпого електронного цифрового підпису, що базується на криптосистемі RSA. Враховано чотири складові безпечної схеми сліпого підпису. Досліджено основні моделі атак на сліпий електронний цифровий підпис Чаума.

Ключові слова: сліпий електронний цифровий підпис, криптопротокол, атаки на криптосистему.

Abstract

The report analyzes the security of a blind electronic digital signature protocol based on the RSA cryptosystem. The four components of the safe signature blind pattern are taken into account. The main models of attacks on the blind electronic digital signature of Chaum are investigated.

Keywords: blind electronic digital signature, cryptoprotocol, attacks on the cryptosystem.

Вступ

Останнім часом все більшої актуальності набуває використання засобів електронних платіжних систем та систем таємного електронного голосування, що здатні забезпечити анонімність суб'єктів [1-3]. Одним з підходів до реалізації такого механізму є використання сліпого електронного цифрового підпису (ЕЦП) [3, 4], який вирішує задачу підтвердження справжності документів без розкриття їхнього авторства. Вирішення задачі такого типу запропонував Девід Чаум [4], який ввів поняття сліпого підпису та розробив варіанти його реалізації. Однак актуальним до цих пір залишається питання дослідження стійкості запропонованих методів.

Метою роботи є дослідження захищеності протоколу сліпого ЕЦП Чаума.

Результати дослідження

Під сліпим підписом розуміється двоключова криптосистема, яка дозволяє здійснити підписування електронних повідомлень таким чином, щоб підписант не мав доступу до інформації, що міститься у повідомленні. В протоколі сліпого ЕЦП один учасник формує документ, а інший підписує його всліпу без можливості ознайомитися із вмістом. При цьому важливо, щоб навіть підписант не зміг встановити автора документа [1].

У загальному вигляді ідея протоколу сліпого підписування може бути представлена таким чином. Нехай суб'єкт A бажає підписати у суб'єкта B деяке повідомлення M так, щоб останній не знав його змісту, але у той же час підпис був дійсним. Для цього необхідно здійснити такі кроки:

1. Користувач A (суб'єкти є користувачами даної криптосистеми) бере повідомлення M і множить його на деяке випадкове число, яке називається маскуючим множником.
2. Користувач A передає замасковане повідомлення користувачу B.
3. Користувач B підписує замасковане повідомлення і передає користувачу A.
4. Користувач A знімає маскуючий множник, отримуючи оригінальне повідомлення, підписане користувачем B.

При цьому передбачаються додаткові процедури, що надають гарантії підписанту, що його не обманути та накладають відповідальність на сторону, яка надає документ для сліпого підписування. Звісно, що для вирішення задачі кожна із сторін має згодитися на той чи інший ризик і на деякі визначені гарантії.

Сліпий електронний цифровий підпис може бути реалізований за допомогою різних математичних апаратів, зокрема, на піднесенні до степеня великих цілих чисел у скінченому полі, обчисленні у групі точок еліптичних кривих та ін. Тому можна побудувати протокол сліпого підписування з використанням таких відомих криптосистем як RSA, Ель-Гамаля, Шнорра, Рабіна, Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера, DSA та ін. [2, 3].

Схема сліпого підписування є безпечною, якщо вона володіє такими властивостями [3]: (a) ***невразливість випадкових параметрів*** – неможливість вилучення параметрів маскування із замаскованих величин; (b) ***неможливість підробки*** – ніхто, крім підписанта, не в змозі виробити вірний електронний підпис; (c) ***сліпота*** – властивість, яка гарантуватиме, що змінні, які підписант отримує під час протоколу вироблення підпису та отриманий підпис є статистично незалежними; (d) ***анонімність*** – неможливість встановити особу або інші дані про користувача, який надавав повідомлення на підпис.

Сліпий підпис може піддаватися таким відомим атакам [2]:

1. ***Адаптивна атака на основі відібраних повідомлень***. Дана атака спрямована на отримання секретного ключа. У будь-якому протоколі отримання секретного ключа підпису базується на математичних обчислювально-складних задачах, таких як факторизація чисел або обчислення дискретного логарифма.

2. ***Атака на основі передбачуваних випадкових величин***. Якщо підписант використовує декілька разів поспіль однакові або передбачувані випадкові параметри, то це дозволяє клієнтові вибрати зі свого боку однакові маскувальні параметри, що дозволить шляхом вирішення системи з двох лінійних рівнянь обчислити секретний ключ підписанта.

3. ***Атака на морфізм схеми підпису***. Дана атака полягає в тому, що користувач може підмінити підписане масковане повідомлення. Здійснюється це за допомогою морфізму схеми підписування, тобто можливості обчислити на підставі однієї пари повідомлення-підпис безлічі інших, формально правильних.

У роботі було проведено дослідження основних моделей атак, сформульованих Мікалі та Рівестом [4], в рамках яких встановлено можливі наслідки вразливості протоколу сліпого ЕЦП Чаума. Здійснено порівняльний аналіз стійкості до атак протоколів сліпого підписування, що базуються на криптосистемах Ель-Гамаля та RSA. Враховано основні критерії безпечної схеми сліпого підпису. Здійснено системний аналіз мультиплікативної та селективної атаки [5] на протокол сліпого ЕЦП Чаума.

Висновки

В роботі здійснено аналіз захищеності протоколу сліпого ЕЦП Чаума, що базується на криптосистемі RSA. Досліджено вразливості протоколу сліпого ЕЦП Чаума до мультиплікативної атаки, внаслідок чого можливе розкриття алгоритму сліпої ЕЦП, що дозволяє отримати підпис для будь-яких повідомлень. Здійснено порівняльний аналіз стійкості до атак основних протоколів сліпого підписування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Молдовян Н. А. Введение в криптосистемы с открытым ключом / Н. А. Молдовян, А. А. Молдовян — СПб.: БХВ-Петербург, 2005. — 288 с.
2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С [Текст] / Б. Шнайер. — М.: Триумф, 2002. — С. 31-48.
3. Ростовцев, А.Г. Введение в криптографию с открытым ключом [Текст] / А. Г.Ростовцев, Е. Б. Маховенко. — СПб.: Мир и Семья, 2001. — 336 С.
4. Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology: Proc. of CRYPTO'82. Plenum Press, 1983. P. 199-203.
5. Молдовян Н. А. Повышение безопасности протоколов слепой подписи / Н. А. Молдовян, Д. Ю. Гурьянов, Д. Н. Молдовян // Вопросы защиты информации. – 2012. – № 4. – С. 3-6.

Ольга Салієва – аспірант, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Науковий керівник: **Юрій Євгенович Яремчук** – доктор технічних наук, професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Olga Salieva – postgraduate, assistant of the Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia,

Supervisor: **Yaremchuk Yu.E**. – doctor of Engineering, Professor of the Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia.