КІБЕРНЕТИКА

УДК 519.7

А.В. АНІСІМОВ
Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: *a.v.anisimov@knu.ua.*

ЦИФРОВА АВТЕНТИФІКАЦІЯ «СВІЙ-ЧУЖИЙ»

Анотація. Запропоновано протокол багаторазової цифрової двораундової автентифікації типу «свій-чужий» для групи користувачів. В основу протоколу покладено таку конструкцію. В кожній сесії автентифікації члени групи підписом Вінтернітца підписують окремі w-блоки повідомлення, яке надає верифікатор. Він перевіряє валідність всього підпису. Поточні публічні ключі пересилаються верифікатору в попередній сесії. У такий спосіб публічні ключі утворюють структуру блокчейну. Безпека протоколу випливає з відомої безпеки підпису Вінтернітца і блокчейну публічних ключів. У криптографічній моделі випадкового оракула запропонований протокол також має властивість «доведення з нульовим розголошенням».

Ключові слова: автентифікація, коаліційна група, цифровий підпис, підпис Вінтернітца, блокчейн.

ВСТУП

Автентифікація — це процедурна ідентифікація об'єкта для перевірки прав доступу до визначеного ресурсу. За допомогою автентифікації об'єкт доводить свою автентичність. У процедурах автентифікації беруть участь дві сторони: сутність, що доводить свою ідентичність (прувер) і сутність, яка перевіряє це доведення і приймає рішення (верифікатор). Зазвичай у сучасних комп'ютерних системах доведення полягає в доведенні знання (можливості машинного обчислення) деяких ідентифікаційних параметрів без розкриття самих параметрів. При цьому вважають, що всі комунікаційні взаємодії відбуваються незахищеними каналами передавання даних. Через це безпековому аспекту автентифікації приділяють особливу увагу.

Віддалена автентифікація разом з процедурою встановлення ключів — це типова і добре досліджена задача криптографії з відкритими ключами. До найвідоміших відповідних протоколів можна віднести схему Нідхема–Шредера (типу Kerberos), яка потребує участі довіреного сервера [1]; у багатьох випадках, зокрема у мережі «Інтернет речей» (IoT), застосовують рішення, які ґрунтуються на процедурі встановлення початкового спільного секрету типу «рукостискання» Діффі–Хеллмана [2] або її модифікаціях. Безпековим недоліком базового протоколу Діффі–Хеллмана є вразливість до атаки «людина посередині» (man-in-the-middle attack). Як наслідок, з'явилися різні модифікації цього протоколу. Наприклад, порівняно з оригінальним протоколом Діффі–Хеллмана покращена схема створення спільного секрету — протокол Менезеса, Кью і Ванстоуна (MQV, HMQV) [3, 4], значно зменшує можливість несанкціонованого втручання в комунікаційні обміни. Але, як з'ясувалося, для забезпечення