ЗАСТОСУВАННЯ ГЕШ-ХАМЕЛЕОНУ У ПРОТОКОЛАХ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ БІЛІНІЙНИХ ВІДОБРАЖЕНЬ У СИСТЕМАХ НА ІДЕНТИФІКАТОРАХ

Погребняк К.А., Іщенко Ю.М.
Науковий керівник – д.т.н., професор Долгов В.І.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Леніна,14, каф. БІТ, тел. (057) 702-14-25)

The advantages of deployment of Identity-Based systems and Hash-Chameleons are considered. The analysis of protocols of signatures with Hash-chameleon based on using bilinear maps was made.

Останнім часом спеціалісти в сфері криптографічного захисту особливу увагу приділяють системам з асиметричною криптографією. Найбільш розвинутою та науково-обґрунтованою системою, що забезпечує застосування асиметричної криптографії, вважається інфраструктура відкритих ключів (ІВК).

Але практичний досвід виявив певні недоліки пов'язані із використанням сервісів ІВК: висока складність підтримання бази сертифікатів відкритих ключів та управління ключовими даними користувачів ІВК. Зазначені недоліки можуть бути усунені завдяки використанню альтернативних систем, наприклад систем на ідентифікаторах, основою побудування яких є використання білінійних відображень Вейля або Тейта та їх аналогів. Використання зазначених відображень дозволило створити більш гнучкі протоколи, які задовольняють певним додатковим вимогам.

Традиційні цифрові підписи, наприклад ЕЦП ДСТУ 4145-2002, можуть бути перевірені будь-яким користувачем ІВК, що може бути небажаним у багатьох системах. Враховуючи таку необхідність виникає протиріччя у побудуванні зазначених систем, а саме одночасні вимоги невідмовності та контрольованої розповсюдженості. Розв'язання цього протиріччя полягає у використанні цифрових підписів основним компонентом яких є геш-хамелеон. Основна концепція такого типу підписів полягає у участі підписувача при перевірці підпису та неможливості перевіряючого довести валідність підпису іншим користувачам системи.

Зважаючи на перспективи розвитку та необхідність застосування таких систем актуальними задачами є: проведення додаткового аналізу з метою визначення обґрунтованих умов та єдиного підходу побудування ЕЦП з використанням геш-хамелеону. У докладі представлено порівняння найбільш відомих схем цифрового підпису та визначені переваги їх застосування.