УДК 004.056

ПОРІВНЯННЯ ШВИДКОДІЇ ДЕЯКИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ ІДЕНТИФІКАЦІЇ З НУЛЕВИМ РОЗГОЛОШЕННЯМ

Новокшонов А.К.
Київський національний університет імені Тараса Шевченка, аспірант

I. Вступ

У наш час інформація є цінністю як для організацій, так і для окремих осіб. Алгоритми ідентифікації та автентифікації користувачів є невід'ємними частинами інформаційної безпеки. Пропонується дослідити та порівняти деякі криптографічні протоколи ідентифікації з нулевим розголошенням – тобто протоколи ідентифікації, спрямовані на доведення одним суб'єктом іншому суб'єкту, що перший суб'єкт володіє певними знаннями, при цьому не розголошуючи жодного біту інформації про ці знання [1]. Найвідомішими та добре дослідженими протоколами ідентифікації з нулевим розголошенням є протокол Фіата-Шаміра [2] та протокол Шнорра [3].

II. Мета роботи

Метою дослідження є порівняння реальної швидкодії протоколу ідентифікації, запропонованого Анісімовим А.В. у роботі [4], з двома найбільш відомими аналогічними протоколами ідентифікації Фіата-Шаміра [2] та Шнорра [3].

III. Результати порівняння

Всі три вищезазначені протоколи були програмно реалізовані на мові програмування Python та протестовані на персональному комп'ютері з процесором AMD Athlon 2,8 ГГц. Результати обчислення швидкодії для різних довжин секретних параметрів (ключів) наведені у таблиці 1. Показником швидкодії є тривалість виконання процедур генерування параметрів та процедур ідентифікації, наведена у секундах, для конкретної зазначеної вище апаратної платформи.

Таблиця 1

Результати експериментального порівняння часу виконання протоколів ідентифікації

	Протокол Анісімова А.В.		Протокол Шнорра		Протокол Фіата-Шаміра	
Розмір ключів (біт)	Генерування (сек.)	Ідентифікація (сек.)	Генерування (сек.)	Ідентифікація (сек.)	Генерування (сек.)	Ідентифікація (сек.)
64	0,083493	0,000001	0,125256	0,000122	0,113108	0,000401
128	0,118805	0,000002	0,172885	0,000257	0,139222	0,000427
256	0,221966	0,000002	0,336767	0,000746	0,287717	0,000525
512	0,566922	0,000003	1,237706	0,003025	0,649274	0,000785
1024	2,724593	0,000005	7,784018	0,016503	2,160826	0,001594
2048	24,823547	0,000013	71,445066	0,089970	11,882965	0,004518

Висновок

Результати експериментального дослідження свідчать про те, що протокол, запропонований Анісімовим А.В., має прийнятну швидкодію, яка може бути порівняна зі швидкодією таких відомих протоколів як Фіата-Шаміра та Шнорра. Цікавою особливістю є те, що час виконання процедури ідентифікації у протоколі Анісімова А.В. є стабільно значно нижчим, майже незалежно від розміру секретних параметрів. Така особливість робить привабливим застосування цього протоколу для ресурсно-обмежених пристроїв. Напрямок, пов’язаний зі створенням криптографічних алгоритмів для таких пристроїв, наразі бурхливо розвивається і має назву «легковагова криптографія».

Список використаних джерел

1. Van Tilborg H.C., Jajodia S. Encyclopedia of cryptography and security / H.C. van Tilborg, S. Jajodia. – Springer Science & Business Media. – 2014. – 1435 с.
2. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems / A. Fiat, A. Shamir. – Conference on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg. – 1986. – С. 186-194.
3. Schnorr C. Efficient signature generation by smart cards / C. Schnorr. – Journal of Cryptology. – 1991. – Volume 4, Issue 3. – С. 161-174.
4. Анисимов А.В. Коалиционные схемы с ключами общего доступа / А.В. Анисимов. – Кибернетика и системный анализ. – 2001. – № 1. – С. 3-17.