# КРИПТОГРАФІЧНА БЕЗПЕЧНІСТЬ СХЕМИ АВТЕНТИФІКАЦІЇ ШНОРРА

Оболоник Д.В., Шафоростов М.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У час, коли майже кожна комп'ютерна система передбачає налаштовування доступу до неї для мережних користувачів, автентифікація суб'єктів – невід'ємний процес комп'ютерної системи. Автентифікація – це процес підтвердження того, що користувач є тим, ким себе видає. На даний час існує багато методів та протоколів автентифікації користувачів у комп'ютерних та інформаційних системах [1, 2].

Одним із протоколів, які реалізують автентифікацію, є схема Шнорра. Її особливість із погляду швидкодії – попереднє обробляння операції піднесення до степеня за модулем, для якої випадкове число добирається як показник степеня.

Похідною до цієї схеми є однойменна схема цифрового підпису, яка поєднує ідеї схеми Ель-Ґамаля та схеми Фіата–Шаміра [3].

Криптографічна безпечність схеми Шнорра математично ґрунтується на складності задачі знаходження дискретного логарифма. Таке саме підґрунтя характерне, наприклад, для протоколу Діффі–Геллмана в кінцевих полях.

**Мета доповіді** – розглянути можливі значення параметра безпеки $t$ для використання схеми саме в контексті автентифікації.

Розкривається суть показника складності зламу $2^t$. Пояснюється розбіжність мінімального необхідного значення $t$ для схеми автентифікації та для схеми підпису.

Також пропонуються обмеження на значення відкритих параметрів схеми $p$ та $q$ з огляду на останні досягнення щодо знаходження дискретного логарифма за допомогою класичного комп'ютера.

Дослідний розрахунок, який розглядається, було виконано над 795-бітним простим числом. Він показав, що, зокрема, складність задачі знаходження дискретного логарифма лише в 3 рази (за грубою оцінкою) вища, ніж складність задачі розкладення на множники [4].

**Список літератури**

1. Сєвєрінов О.В., Кліпоносова В.С. Автентифікації користувачів веб-ресурсів, НТУ «ХПІ», 2022.

2. Власов А.В., Сєвєрінов О.В., Слиш О.В. Впровадження децентралізованої системи ідентифікації. НТУ «ХПІ», 2020.

3. Schorr C. P. Efficient Signature Generation by Smart Cards. *Journal of cryptology*. 1991. Т. 4, № 3. С. 161–174.

4. Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment / F. Boudot та ін. *Advances in Cryptology – CRYPTO 2020*. Springer, 2020. С. 62–91.