ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕЛІПТИЧНИХ КРИВИХ ЕДВАРДСА В ОНОВЛЕНОМУ СТАНДАРТІ ЦИФРОВОГО ПІДПИСУ

Мельникова О.А., Олійник Е.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Еліптичні криві (ЕК) Едвардса, які до оновленого стандарту цифрового підпису (ЦП) [1] було додано лише в 2023 році, досить давно використовуються у багатьох відомих криптографічних бібліотеках [2, 3], а також у популярних додатках (зокрема, для реалізації автентифікації користувачів).

Метою доповіді є аналіз властивостей, переваг, а також особливостей програмної реалізації алгоритмів ЦП із використанням ЕК Едвардса. **В доповіді** також розглянуто зв'язок специфіки реалізації базових операцій з точками ЕК Едвардса та стійкістю алгоритмів (зокрема, до атак за побічними каналами). В алгоритмах ЦП на еліптичних кривих Едвардса використовуються скручені криві Едвардса з параметрами Ed25519 та Ed448 [4], які забезпечують рівні криптографічної стійкості приблизно еквівалентні 128-бітовому та 224-бітовому значенням, відповідно.

Поточна версія стандарту пропонує лише детерміновані варіанти ЦП із використанням ЕК Едвардса, хоча є припущення щодо можливого подальшого доповнення недетермінованою версією підпису. Під детермінованістю мається на увазі, що при формування підпису використовується унікальне значення, сформоване з ґеш-значення від особистого конфіденційного ключа автора підпису та самої інформації, що підписується. Порівнюються два детерміновані варіанти ЦП: HashEdDSA (підписується ґеш-значення від інформації) та EdDSA (підписується безпосередньо сама інформація). Перший варіант, як вважається, є більш вразливим до можливих колізій ґеш-значень.

Список літератури

1. National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 186-5. DOI: https://doi.org/10.6028/NIST.FIPS.186-5

2. Мельникова О. А., Джурик О. В., Маслєннікова А. О. Еліптичні криві Едвардса. Порівняння криптографічних бібліотек // Радіотехніка. — 2018. — №. 195. — С. 41 - 45. DOI: https://doi.org/10.30837/rt.2018.4.195.05

3. Мельникова О. А., Джурик О. В., Масленникова А. О. Аналіз криптографічних бібліотек, які підтримують еліптичні криві Едвардса [Текст] // Проблеми інформатизації: тези доп. 6-ї міжнар. наук.-техн. конф. / Черк. держ. технолог. ун-т [та ін.]. — Харків : Петров В. В., 2018. — С. 14-15. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/41370

4. Chen L, Moody D, Regenscheid A, Robinson A, Randall K (2023) Recommendations for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-186. https://doi.org/10.6028/NIST.SP.800-186