

АНАЛІЗ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ВАРІАНТІВ ПЕРЕДПІДПИСІВ ЗА СТАНДАРТАМИ ЦП В ГРУПАХ ТОЧОК ЕК

Мельникова О.А., Польовий О.А.

Харківський національний університет радіоелектроніки, Харків, Україна

Алгоритми ЦП (цифрового підпису) мають функціонувати в режимі реального часу. Передпідписи зменшують обчислювальну складність формування ЦП. Наразі велика кількість діючих КСЗІ (криптографічних систем захисту інформації) використовує стандарти ЦП в групах точок еліптичних кривих (ЕК) [1, 2], що модифікуються із урахуванням сучасних викликів. Так, до оновленого стандарту [1] додано ЕК Едвардса, що передбачалося досить давно [3].

Метою доповіді є аналіз можливостей зменшення обчислювальної складності формування ЦП за рахунок передпідписів із урахуванням особливостей різних стандартів. **В доповіді** також розглянуто зменшення обчислювальної складності формування передпідписів при надвеликому їх обсязі за рахунок методів скалярного множення, які одноразово формують великі таблиці передобчислень при використанні незмінної (базової) точки. Наприклад [4], методів Брікела, варіантів comb-методів із різною кількістю таблиць (методи Лімалі), тощо. Порівняння формування ЦП за стандартами [1, 2] показує, що варіант [1] дозволяє розширити попередні обчислення. Пропонується розширений варіант передпідписів: $\{k_i^{-1} \bmod n, r_i, d \cdot r_i \bmod n\}$ замість рекомендованого в стандарті $\{k_i^{-1} \bmod n, r_i\}$. Нажаль, для [2] можливе використання єдиного варіанту передпідписів: $\{k_i, x_i\}$.

Порівняння оцінок обчислювальної складності етапів передпідпису та швидкого формування ЦП в режимі реального часу показав, що при розширеному варіанті передпідпису обчислювальна складність передобчислень для [1] більша, ніж для [2]. Але етап ЦП для [1] стає швидшим, принаймні на одне множення за модулем елементів поля $GF(2^m)$.

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. ДСТУ 4145 – 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. — Перше видання; Введ. 1.07.2003. — К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003 р. — 44 с.
3. Мельникова О. А., Джурик О. В., Масленнікова 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>
4. Hankerson D., López J. H., Menezes A. Software implementation of the NIST elliptic curves over binary fields // Proceedings of CHES 2000, LNCS 1965 (2000), 1–24. DOI: http://dx.doi.org/10.1007/3-540-44499-8_1