АНАЛІЗ ВЛАСТИВОСТЕЙ ДЕТЕРМІНОВАНОГО ЦИФРОВОГО ПІДПИСУ В ГРУПАХ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ ІЗ ОНОВЛЕНОГО СТАНДАРТУ

Мельникова О.А., Грасмік С.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Серед суттєвих змін в оновленому стандарті ЦП (цифрового підпису) [1] — нові механізми формування детермінованого варіанту підпису, а також можливість використання еліптичних кривих Едвардса, які досить давно використовуються у відомих бібліотеках та додатках [2].

Метою доповіді є аналіз властивостей та особливостей реалізації детермінованого варіанту цифрового підпису. **В доповіді** розглянуто переваги та недоліки використання детермінованого підпису, у порівнянні з недетермінованим варіантом, а також особливості його ефективної програмної реалізації. Попередні версії стандарту визначали тільки недетермінований ЦП, однією з переваг якого є можливість використання передпідписів $\{k_i^{-1} \bmod n, r_i\}$. Що потенційно дозволяє реалізовувати розширений варіант передпідписів $\{k_i^{-1} \bmod n, r_i,\ d \cdot r_i \bmod n\}$ для зменшення обчислювальної складність основного етапу формування ЦП [3], що важливо при використанні в режимі реального часу.

Детермінований ЦП не передбачає використання передпідписів через те, що формування конфіденційного сеансового значення k_i залежить від особистого конфіденційного ключа d автора підпису та від ґеш-значення $H(M)$ інформації M, що підписується. Тоді як в недетермінованому варіанті k_i формується на основі генерування унікальної випадкової / псевдовипадкової послідовності бітів. Таким чином, перевагою детермінованого алгоритму є те, що його реалізація не потребує використання сертифікованого криптографічно сильного генератору випадкових / псевдовипадкових послідовностей бітів. Якісна реалізація якого, в ідеалі, має включати не тільки сертифіковані варіанти алгоритмів, а й апаратну підтримку (для створення саме випадкових, а не псевдовипадкових послідовностей). Завдяки тому, що конфіденційне сеансове значення k_i є функцією від інформації, що підписується, та особистого конфіденційного ключа d автора підпису, маємо детерміноване відображення інформації, що підписується, в цифрові підписи. При цьому відпадає необхідність контролювати унікальність та якість статистичних властивостей значень k_i для забезпечення стійкості ЦП до криптографічних атак, які можуть використовувати недостатню випадковість k_i для підробки ЦП або навіть розкриття особистого ключа d автора підпису (як згадується в самому стандарті).

Для детермінованого ЦП передбачається формування k_i на основі алгоритму HMAC_DRBG [4, 5]. При цьому, в якості внутрішньої допоміжної ґеш-функції для HMAC_DRBG, рекомендовано використовувати в точності той самий варіант сертифікованого криптографічно стійкого алгоритму ґешування (FIPS 202, FIPS 180-4), що й в основному алгоритмі формування

ЦП. Початкові значення для HMAC_DRBG формуються на основі конкатенації значень d та $H(M)$, представлених рядками у вісімковий системі подання. Крім того, за основним алгоритмом формування підпису, діапазон значень k_i обмежується простим порядком n базової точки, що може викликати повторні ітерації основного циклу алгоритму HMAC_DRBG для створення значень-кандидатів k_i у випадках $k_i \notin [1, n-1]$.

За варіантом [5] алгоритму HMAC_DRBG дозволяється застосовувати повторні ітерації ще й при отриманні на основі поточного k_i першого компоненту підпису $r_i = 0$. Тобто до циклу формування значень-кандидатів k_i включаються ще й розрахунки першого компонента r_i підпису: визначення афінної координати x_R точки $R = [k_i]G = (x_R, y_R)$, перетворення x_R на елемент базового поля r_i та перевірку $r_i \neq 0$. Проблемним моментом є те, що детермінованість значення k_i для певної інформації M, що підписується, теоретично може привести до формування другого компоненту цифрового підпису $s_i = 0$. Статистично така ситуація є вкрай малоймовірною. Але, за її виникнення, алгоритм формування підпису повертає помилку. Теоретично, цієї ситуації можна уникнути при включенні перевірки $s_i = 0$ в умови повторних ітерацій формування значень-кандидатів k_i., але в стандарті такий варіант не розглядається.

Згідно до своїх властивостей, детермінований алгоритм підпису може надати перевагу при реалізації ЦП для пристроїв, які не дозволяють підтримувати криптографічно стійкий генератор випадкових послідовностей з певних технічних обмежень або через високу вартість розробки.

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., Польовий О.А. Аналіз обчислювальної складності варіантів передпідписів за стандартами ЦП в групах точок ЕК [Текст] // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 14-ї міжнар. наук.-техн. конф., 25-26 квітня 2024 р., Баку–Харків–Жиліна : [у 2 т.]. Т. 2 : секція 3-6 / Нац. ун-т оборони Азербайджанської Республіки [та ін.]. — Харків : Impress., 2024. — С. 50. DOI: https://doi.org/10.32620/ICT.24.t2

4. Barker EB, Kelsey JM (2015) Recommendation for Random Number Generation Using Deterministic Random Bit Generators. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-90A, Rev. 1. DOI: https://doi.org/10.6028/NIST.SP.800-90Ar1

5. Pornin T (2013) Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). (Internet Engineering Task Force (IETF)), IETF , Request for Comments (RFC) 6979. DOI: https://doi.org/10.17487/RFC6979