УДК 681.322:621.391

# ПРОБЛЕМИ ВИБОРУ ПАРАМЕТРІВ У СИСТЕМАХ ЦИФРОВОГО ПІДПИСУВАННЯ, ЩО БАЗУЮТЬСЯ НА МАТЕМАТИЧНОМУ АПАРАТІ ЕЛІПТИЧНИХ КРИВИХ

Слободиський О. В.
Наукові керівники - доц., к.т.н. Яремчук Ю.Є., Черняхович К.В.

Сьогодні неможливо уявити електронний документообіг без використання цифрового підпису. Цифровий підпис можна визначити як сукупність даних в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для вирішення таких основних задач, як цілісність, автентичність та неможливість відмови від авторства.

Значна частина сучасних систем цифрового підписування використовують математичний апарат еліптичних кривих. В основу криптосистем на основі математичного апарату еліптичних кривих покладено проблему дискретного логарифмування в групі точок еліптичної кривої. Головними перевагами криптографічних механизмів, заснованих на математичному апараті еліптичних кривих, є відсутність алгоритмів для вирішення задачі дискретного логарифмування в групі точок еліптичної кривої за поліноміальний час, ефективність та відносна простота практичної реалізації обчислень, наявність простих необхідних умов для виключення можливості застосування специфічних методів криптоаналізу. Попри ці переваги, однією з актуальних проблем в системах цифрового підписування на основі математичного апарату еліптичних кривих є проблема вибору загальних параметрів для застосування в системі цифрового підписування, а також перевірка цих параметрів. Актуальність цього, пов’язана в першу чергу з тим, що складність вирішення задачі дискретного логарифмування в групі точок еліптичної кривої в великій мірі залежить від загальних параметрів, що використовуються в системі цифрового підписування, що побудована на основі математичного апарату еліптичних кривих.

При цьому, до загальних параметрів зазвичай відносять: параметри основного поля, а саме степінь його розширення; параметри рівняння еліптичної кривої виду; базова точка еліптичної кривої; порядок базової точки та ін.

Зважаючи на існуючі підходи щодо вирішення задачі вибору параметрів еліптичної кривої, а зокрема генерування потрібних параметрів відповідно до вимог заданого рівня крипостійкості, що визначені рядом існуючих стандартів на цифрове підписування, варто відзначити проблему, що пов’язана із швидкістю генерування таких параметрів за обмежений період часу із заданими вимогами щодо криптостійкості. В зв’язку з цим, сьогодні актуальною є розробка методів, що дозволять ефективно вирішувати цю задачу.