ВИЯВЛЕННЯ ЗАЛЕЖНОСТІ МІЖ СЕАНСОВИМИ КЛЮЧАМИ ЕЦП ECNR СТАНДАРТУ ISO/IEC 15946-4

Шевчук О. А.
Науковий керівник — проф. Горбенко І. Д.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Леніна, 14. каф. БІТ, тел. (057) 702-14-25)

In modern schemes of digital signature signing algorithm divided in two steps: generation of pre-signature, and signing message with pre-signature. Main component of pre-signature is session key. Session key must be received absolutely randomly. Discovered situation when certain connection between session keys may be detected.

Стандарт ISO/IEC 15946-4 став результатом об'єднання алгоритмів Нюрберга, Рюпеля, Міяджі, Абе, Окамото та інших матеріалів, присвячених цифровим підписам з відновленням повідомлень, що був опублікований у кінці 90-х років. Останню версію стандарту було опубліковано у 2004-му році.

У сучасних ЕЦП використовується сутність, що має назву «передпідпис». Основною компонентою передпідпису, що визначає його стійкість, є сеансовий ключ *k*, що обирається випадково з інтервалу $[1, n-1]$, де n – порядок базової точки *G*. Сеансовий ключ безпосередньо використовується для обчислення однієї з компонент ЕЦП. Стандарт застерігає від повторного використання сеансового ключа, та його зберігання. Визначення сеансового ключа дає змогу однозначно обчислити секретний ключ користувача. Таким чином викривлені алгоритми формування випадкових послідовностей та приховані залежності між сеансовими ключами повідомлень можуть становити загрозу безпеці ЕЦП.

Було досліджено, що для двох випадкових повідомлень M_1 та M_2 може бути однозначно визначена залежність сеансових ключів k_1 та k_2, що будуть використані для формування підписів повідомлень, якщо

$$k_1 = n - k_2 (mod n).$$

Дійсно, передпідпис обчислюється як $(x, y) = kG$, $П = x$; перша компонента підпису обчислюється як $r = x + M(mod n)$. Таким чином, якщо $k_1 = n - k_2 (mod n)$, то у рівняннях $(x_1, y_1) = k_1 G$ та $(x_2, y_2) = k_2 G$ координата $x_1 = x_2$. Тоді буде виконуватись рівняння

$$r_1 - r_2 = M_1 - M_2$$

Таким чином, ситуацію, коли для обчислення підпису двох довільних повідомленнь було обрано сеансові ключі, пов'язані вказаним рівнянням, легко детектувати, і використовувати отриману інформацію для проведення атаки.