УДК 004.056.55

О. С. АКОЛЬЗІНА, О.О.БАКЛИКОВ

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЕРСПЕКТИВНИХ СТАНДАРТІВ ЕП В ГРУПІ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

Вступ

У зв'язку з орієнтацією України на електронно-довірчі послуги Європейського союзу постала необхідність уніфікації та стандартизації механізмів таких послуг. В Україні методом погодження прийнято ряд міжнародних та національних стандартів. Так, наказом Мінекономрозвитку №1493 з 01.01. 2016 р. вводяться в дію електронні підписи, що ґрунтуються на уже відомих та новітніх математичних методах криптології. Такі підписи забезпечують різні властивості, та можуть бути застосовані в різних додатках в залежності від вимог, що у них висуваються. Таким чином постають задачі визначення вимог до електронних підписів зі сторони додатків, першим чином, по критерію стійкість-складність (швидкодія), а також оцінка їх властивостей. Метою цієї статті є огляд основних стандартів електронного підпису, що вводяться в Україні з 01.01.2016 р. та їх порівняльний аналіз за критеріями стійкість-складність, а також розробка відповідних рекомендацій із застосування.

Нині найбільш ефективними та випробуваними часом є криптографічні перетворення в групі точок еліптичних кривих, що широко застосовуються при реалізації таких криптосистем як: електронний підпис, схеми направленого шифрування, криптографічні протоколи встановлення ключа. У будь-якому разі вони застосовуються для реалізації електронного
підпису в таких стандартах: міжнародному ISO/IEC 9796-3, національних ДСТУ ISO/IEC 14888 – 3 та ДСТУ 4145-2002, федеральному стандарті США Fips 186-3 та російському ГОСТ Р 34.10-2012 [6, 3,2, 5, 4].

1. Оцінки стійкості перспективних стандартів

При побудові криптосистем одним із важливих показників є значення n – довжина блоку перетворення. З показником n пропорційно зв'язані два параметри криптоалгоритма – складність та стійкість. В залежності від рівня безпеки, що вимагається, можна обирати різні значення модуля перетворення. Стандарти, що розглядаються, допускають різні значення n, тож доцільно оцінити їх за даним параметром. У табл. 1 наведені розміри модулів перетворення для різних стандартів.

Таблиця 1

Стандарт	ДСТУ ISO/IEC 14888 – 3	ДСТУ 4145-2002	ГОСТ Р 34.10-2012	Fips 186-3	ISO/IEC 9796-3
n	$2^{224}, 2^{256}$	$2^{163} - 2^{509}$	$2^{256}, 2^{512}$	$2^{160} - 2^{512}$	$2^{158} - 2^{163}$

Варто зазначити, що ДСТУ 4145-2002 має найбільший спектр значень (60 значень). Що є значною перевагою, так як з'являється можливість «обмінювати» стійкість на складність та навпаки і, як наслідок, адаптувати алгоритм до різних задач і потреб зі сторони додатків.

Одним із провідних показників для визначення стійкості криптосистеми є безпечний час $t_б$ – математичне сподіваннячасу розкриття криптосистеми, у нашому випадку – знаходження таємного ключа, із використанням конкретного методу.

Безпечний час можна розрахувати за формулою

$$t_б = \frac{1}{\gamma \cdot k} P_y, \qquad (1.1)$$

де I – складність криптоаналізу, γ – потужність криптоаналітичної системи, k – кількість секунд у одному році, $k = 3{,}15 \cdot 10^7$[с/рік], P_y – ймовірність, з якою повинен чи може бути успішно здійснений криптоаналіз.

Для прикладу розглянемо атаку, що здійснюється за методом Полларда. У цьому випадку показник складності криптоаналізу I_ρ буде визначатися як

$$I_\rho \approx \sqrt{\frac{\pi n}{4}}, \tag{1.2}$$

тоді

$$t_б = \frac{I}{\gamma k} P_y = \frac{\sqrt{\pi n}}{2\gamma k} P_y. \tag{1.3}$$

В рівняннях n – порядок базової точки ЕК. Будемо вважати, що маємо справу з криптоаналітиком 3-го рівня (має науково-технічний ресурс спецслужби економічно розвиненої держави), потужність криптоаналітичної системи $\gamma = 10^{12}$оп/с.

Для розрахунку безпечного часу скористаємось відомими значеннями мінімальних порядків базових точок для алгоритмів ДСТУ ISO/IEC 14888-3 (ECDSA, EC-GDSA та EC-KCDSA), ДСТУ 4145-2002, ГОСТ Р 34.10-2012, Fips 186-3, ISO/IEC 9796-3, що наведені в табл. 1, результати подамо у табл. 2.

Таблиця 2

Алгоритм		n	$t_б$,років
ДСТУ 4145- 2002		2^{164}	$3{,}2 \cdot 10^7$
ГОСТ Р 34.10 – 2012		2^{255}	$3{,}3 \cdot 10^{22}$
ДСТУ ISO/IEC 14888 – 3	ECDSA	2^{161}	$3{,}6 \cdot 10^6$
	EC-GDSA	2^{161}	$3{,}6 \cdot 10^6$
	EC-KCDSA	2^{192}	$1{,}4 \cdot 10^{12}$
Fips 186-3		2^{160}	$7 \cdot 10^7$
ISO/IEC 9796-3		2^{158}	$3{,}2 \cdot 10^7$

Згідно з отриманими результатами можна зробити висновок, що при мінімальних значеннях порядку базової точки, найкращим значенням безпечного часу характеризується алгоритм ГОСТ Р 34.10 – 2012, та EC-KCDSA, найгірші характеристики у ECDSA та EC-GDSA. Але за великих значеннях модуля ДСТУ 4145 – 2002 та Fips 186-3 більш захищені від погрози повного розкриття при великих значеннях порядку базової точки ніж KCDSA.

2. Порівняння складності виконання ЦП

У табл. 3 наведені результати порівняння складності виконання стандартів ЦП – ДСТУ 4145-2002, ДСТУ 15946-2 (ECDSA, EC-GDSA, EC-KCDSA), ГОСТ Р 34.10-2012, ISO/IEC 9796-3 та Fips 186-3.

Таблиця 3

Процес	Операція	ECDSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2012	ISO/IEC 9796-3	Fips 186-3
Вироблення цифрового підпису	$h()$	1	1	2	1	1	1	1
	$\pi()$	1	1	0	1	1	1	1
	$k^{-1} \bmod n$	1	0	0	0	1	0	1
Перевірка цифрового підпису	$h()$	1	1	2	1	1	1	1
	$\pi()$	1	1	0	0	1	1	1
	s^{-1} ($чи$ r^{-1}) $\bmod n$	1	1	0	0	1	0	1

Нижче наведені результати порівняння складності виконання стандартів ЦП з табл. 3.

В усіх алгоритмах, крім EC-KCDSA, використовується $\pi()$ функція для перетворення точки еліптичної кривої на ціле число, в алгоритмі EC-KCDSA замість функції $\pi()$ використовується геш-функція $h()$. Складність обчислення значення геш-функції $h()$ перевищує складність обчислення функції перетворення $\pi()$. Однак частка обчислень геш-значень відносно загальних обчислень є незначною. Крім того, використання геш-функції в алгоритмі EC-KCDSA є способом доведення стійкості.

При здійсненні цифрового підпису алгоритми EC-KCDSA, ДСТУ 4145-2002, ISO/IEC 9796-3 не виконують обчислення мультиплікативної інверсії за модулем n, що суттєво зменшує складність, бо операція ділення за модулем є ресурсоємною. Тож, у цілому, оскільки найбільш складною є операція ділення за модулем у полі, то алгоритми ECDSA, ГОСТ Р 34.10-2001 та Fips 186-3, у порівнянні з іншими, є більш складними.

3. Огляд існуючих атак на алгоритми ЦП

Найважливішими вимогами до криптографічного протоколу є забезпечення функцій безпеки, у даному випадку – криптостійкості проти існуючих атак [1].

На сьогодні існують різні види атак на асиметричні криптосистеми, зокрема алгоритми цифрового підпису, серед них:

1. Атака на основі відомого відкритого ключа (key-only attack). Це найслабкіша з атак, вона практично завжди доступна порушнику (криптоаналітику) і може бути реалізованою. Ця атака може виконуватися за умов знання реалізації ЦП, загальносистемних параметрів, а також при діючих відкритих ключах.
2. Атака на основі відомих підписаних повідомлень (known-message attack). Щодо цієї атаки передбачається, що в розпорядженні криптоаналітика є деяке число пар $(m,\langle r,s\rangle)$ підписаних повідомлень *m*, при цьому він не може вибирати повідомлення *m*. Крім того, криптоаналітик знає систему та загальні параметри ЦП.
3. Проста атака з вибором підписаних повідомлень (generic chosen-message attack). У цьому випадку криптоаналітик має можливість вибрати деяку кількість підписаних повідомлень, знає загальносистемні параметри і має після вибору підписаних повідомлень доступ до відкритих ключів.
4. Спрямована атака з вибором повідомлення (direct chosen-message attack). Криптоаналітик знає ЗСП, може за своїм розсудом вибирати відкритий ключ і після цього вибирати підписані повідомлення.
5. Адаптивна атака з вибором підписаного повідомлення (adaptive chosen-message attack). При здійсненні атаки криптоаналітик може вибирати відкритий ключ, а також підписане повідомлення. При цьому вибір наступного підписаного повідомлення він може робити на основі знання припустимого підпису попередньо обраного повідомлення.

Основні види загроз ЦП

Аналіз підтверджує, що кожна атака відносно ЦП спрямована на досягнення певної мети. З урахуванням цього для всіх схем електронних цифрових підписів у порядку зростання небезпеки можна виділити такі види загроз [1].

1. Екзистенційна підробка (existential forgery).
2. Селективна підробка (selective forgery).
3. Універсальна підробка (universal forgery).
4. Повне розкриття (total break).

Найбільш надійними є схеми ЦП, стійкі проти найслабкіших із загроз на основі найдужчої з атак, тобто проти екзистенційної підробки на основі атаки з адаптивним вибором підписаних повідомлень. Найбільш небезпечною є атака типу «повне розкриття». Розглянемо
методи її здійснення більш детально.

4. Методи здійснення атак типу повне розкриття

Основний сенс здійснення атак – повне розкриття для еліптичних кривих зводиться до вирішення одного з трьох рівнянь:

для Fips 186-3, ГОСТ Р 34.10-2012, ДСТУ ISO/IEC 14888 – 3 (ECDSA) рівняння:

$$Q = d_i \cdot G \bmod p \quad ; \tag{4.1}$$

для ДСТУ 4145-2002:

$$Q = -d_i \cdot G \bmod p \; ; \tag{4.2}$$

дляДСТУ ISO/IEC 14888 – 3 (EC-GDSA, EC-KCDSA):

$$Q = {d_i}^{-1} \cdot G \bmod p. \tag{4.3}$$

Задача криптоаналітика – використовуючи найбільш швидкий (ефективний) метод, розв'язати задачу визначення особистого ключа d_i з рівняння (4.1), (4.5) або (4.3) (задачу дискретного логарифмування). Але ця задача має розглядатися більш широко, тобто для загального випадку стоїть задача захисту асиметричної пари ключів (d_i, Q), тобто включаючи сертифікат відкритого ключа.

Найпоширенішою (стандартною) умовою криптоаналізу систем є відомі криптоаналітику методи, алгоритми й протоколи виконання узгодження ключів або іншого протоколу, що використовує скалярне множення в групі точок еліптичних кривих. Криптоаналітик має доступ і знає системні параметри, базову точку, її порядок та відкриті ключі. Відоме також рівняння, що використовується для обчислення відкритих ключів за особистим ключем. Додатково може бути відомий інтервал або клас, якому належить особистий ключ, вага Хеммінга, або його ймовірнісний розподіл. Звичайно ці відомості значно спрощують задачу знаходження дискретного логарифма.

До найефективніших методів дискретного логарифмування в групі точок еліптичних кривих належать алгоритми:

- ρ-Полларда
- λ-Полларда
- Поліга – Геллмана
- великих та малих кроків (алгоритм Shanks'a)
- множинного логарифмування
- Index – calculus
- Xedni – calculus
- GenLog

Проведемо аналіз деяких із них.

1) *Метод великих і малих кроків(алгоритм Шенкса).*

Ідея цього алгоритму заключається у вдосконаленому переборі можливих значень особистого ключа. Алгоритм Шенкса базується на переборі x, таких, що $x = im - j$, де $m = \lfloor \sqrt{n} \rfloor + 1 1 \le i \le m$та$0 \le j < m$. Обмеження на i та j випливає з того, що порядок групи не більше за m, а значить, достатньо перебрати всіx у проміжку$[0, m)$. Звідси випливає

$$Q + jG = imG \tag{4.4}$$

Алгоритм попередньо розраховує imG для деяких значень i при фіксованому m. Далі необхідно перебрати всі можливі значення j такі, щоб рівність (4.4) виконувалась.

2) *Розпаралелений метод ρ-Полларда.*

Введемо деякі позначення. Нехай n буде порядком базової точки G, що є генератором групи $\langle G \rangle$, відкритий ключ Q буде точкою на еліптичній кривій.Фізичний сенс методу

полягає в прискоренні знаходження особистого ключа d за допомогою інтерполяційної функції $F(Y)$:

$$Y_{i+1} = F(Y_i) = \begin{cases} (Y_i + c_1 G + d_1 Q), \text{ якщо } Y_i \in S_1; \\ (Y_i + c_2 G + d_2 Q), \text{ якщо } Y_i \in S_2; \\ \vdots \\ (Y_i + c_r G + d_r Q), \text{ якщо } Y_i \in S_r; \end{cases} \quad (4.5)$$

де c_j, d_j – випадкові цілі числа з інтервалу $[0, n-1]$.

Задача криптоаналітика зводится до пошуку таких коефіцієнтів (α_k) і (β_k), що

$$\alpha_j G + \beta_j Q \equiv \alpha_i G + \beta_i Q \pmod{p},\ i \neq j\ , \quad (4.6)$$

тобто при яких відбудеться збіг пари елементів Y_i і $Y_j (Y_i = Y_j$ при $i \neq j)$

Перетворюючи рівняння, одержимо:

$$Q = \frac{\alpha_j - \alpha_i}{\beta_i - \beta_j} G \pmod{p} \quad (4.7)$$

Якщо порівняти отримане рівняння з рівнянням дискретного логарифма еліптичних кривих вигляду (5.1), дістанемо, що особистий ключ можливо одержати, розв'язавши рівняння вигляду:

$$d = \frac{\alpha_j - \alpha_i}{\beta_i - \beta_j} (\mathrm{mod}\, n),\ \beta_i \neq \beta_j \quad (4.8)$$

У статті подан розпаралелений метод, де вся множина точок розбивається на $r > 3$ не пересічені множини так, як за великих значень n такий алгоритм стає неефективним. Було доведено, що таким чином можливо зменшити складність.

3) *λ-Полларда метод.*

λ-Полларда метод є модифікацією ρ-Полларда методу. У цьому методі ведеться розрахунок відразу двох дискретних логарифмів для чисел b та B, де b – число, дискретний логарифм якого треба знайти, B – число, дискретний логарифм якого вже відомий. Якщо результати розрахунків співпадуть, то є можливість знайти дискретний логарифм b. Важлива властивість даного методу – можливість його виконанняодночасно на декількох процесорах.

4) *Оцінка складності алгоритмів Шенкса, ρ-Полларда та λ-Полларда.*

Складність алгоритмів, що діють в групі точок ЕК, вимірюється груповими операціями, наприклад числом операцій додавання у групі точок ЕК, та залежить, перш за все, від порядку базової точки (розміру модуля) n.

У класичній реалізації метод Шенкса вимагає $\sqrt{n} + 2\lfloor l/\sqrt{n} \rfloor + O(\log_2 \sqrt{n})$ групових операцій. Розпаралелення алгоритму на r процесорах з необмеженим і миттєвим доступом до пам'яті зменшує складність на множник $\sqrt{r}$, але це не дає лінійного зменшення складності. Тому цей метод практично не використовується.

Розглянемо більш детально складності алгоритмів ρ- таλ-Полларда. Для виконання алгоритму Полларда у загальному випадку необхідно порядку $O(\frac{\sqrt{\pi n/4}}{r})$ групових операцій.

При розпаралелленні методу необхідно $O(\sqrt{\pi n/4r})$ групових операцій, тобто відбувається зменшення складності на $\sqrt{r}$.

Однак результати складності рішення завдання дискретного логарифма, наведені вище, на даний момент чисто теоретичні, тому що не існує можливості задіяти необмежений обчислювальний ресурс для полів великої розмірності. Таким чином, актуальною стає задача визначення ймовірності, з якою дії криптоаналітика при зломі системи досягнуть поставленої мети при обмеженому обчислювальному ресурсі.

Для ρ-Полларда методу складність з урахуванням ймовірності колізій

$$I_\rho = \sqrt{-2n\ \ln(1-P_k)}, \tag{4.9}$$

де P_k – ймовірність колізій. Наприклад при $P_k = 0.5$, $I = 1.17\sqrt{n}$.

Для λ-Полларда методу складність з урахуванням колізій

$$I_\lambda = 2\sqrt{-n\ \ln(1-P_k)} \tag{4.10}$$

де P_k – ймовірність колізій. Наприклад при $P_k = 0.5, I \approx 1.68\sqrt{n}$.

Порівняємо обидва методи:

$$\mu_1 = \frac{I_\rho}{I_\lambda} = \frac{\sqrt{-2n\ln(1-P_k)}}{2\sqrt{-n\ln(1-P_k)}} = \frac{\sqrt{2}}{1} = 0.707.$$

Очевидно, що метод λ -Полларда є менш складним за метод ρ -Полларда. Крім того метод λ-Полларда є найшвидшим (найменш складним) алгоритмом атаки типу «повне розкриття» випадкових неслабких кривих над полями $F(p)$, $F(2^m)$ і $F(p^m)$ на сьогодні. Основна перевага методу λ -Полларда – можливість розпаралелення, також цей метод не потребує постійного зв'язку із сервером. Однак ці методи неможливо реалізувати вже при $n = 2^{512}$.

5. Оцінки захищеності перспективних стандартів від основних атак

1) *Атака «повне розкриття» на основі підписаних даних.*

Алгоритми цифрових підписів, описані у стандартах ДСТУ ISO/IEC 14888-3, ДСТУ 4145-2002, ГОСТ Р34.10-2012, Fips 186-3, ISO/IEC 9796-3, мають у своїй основі схеми Ель-Гамаля та DSA з невеликими варіаціями. Вироблення підпису, згідно цієї схеми, відбувається у такий спосіб:

$$s = k^{-1}(dr + e) \bmod n \tag{5.1}$$

де k– особистий ключ сеансу, d – особистий довгостроковий ключ, r – відкритий ключ сеансу, e – геш-значення повідомлення, n – модуль перетворення

Розв'язуючи рівняння (5.1) відносно *d*, одержимо

$$d = {(ks - e)}\big/{r} \ (\bmod n) \tag{5.2}$$

Для *i* повідомлень отримаємо*i* рівнянь з *i* + 1 невідомими, тобто k_1, k_2, …, k_i і *d*:

$$\begin{cases} d = {(k_1 s_1 - e_1)}\big/{r_1} \bmod n, \\ \vdots \\ d = {(k_i s_i - e_i)}\big/{r_i} \bmod n. \end{cases} \tag{5.3}$$

$$\begin{cases} d = (k_1 - s_1) / r_1 \bmod n, \\ \vdots \\ d = (k_i - s_i) / r_i \bmod n. \end{cases} \quad (5.4)$$

Таким чином, для повного розкриття, тобто визначення секретного ключа d за i отриманим ЦП, необхідно розв'язувати систему i-го порядку з $i + 1$ невідомими. Тобто всі атаки зводяться до пошуку одного невідомого s_i.Так як розмір s_i – щонайменше 2^{158} для схем ЦП, що розглядаються, то такі схеми є захищеними від цієї атаки.

У разі якщо повідомлення M є зашифрованим, невідомими є значення геш-функцій $e_1, e_2, ..., e_i$. Як результат одержимо систему рівнянь з $2i+1$ невідомими, тому шифрування підписаних повідомлень дозволяє істотно підвищити стійкість та захищає від атаки на основі підписаних даних.

2) *Атака типу «Екзистенційна підробка».*

Цей вид загрози виникає за наявності слабкостей у геш-функції, яка використовується при виробленні ЦП. Для захисту від екзистенційної підробки на геш-функцію накладається вимога, щоб складність алгоритму створення колізії мала експоненційний характер (була стійкою до колізій).

На практиці геш-функція повинна задовольняти, принаймні, таким вимогам:

- не вище ніж поліноміальна складність обчислення геш-значення h;

- односпрямованість, яка полягає у неможливості обчислення даних (прообразу) m за відомим образом h (наприклад, має не нижче ніж експонентну складність);

- захищеність від визначення для m_1 другого прообразу m_2 – такого, що $H(m_1) = H(m_2)$, складність знаходження m_2 повинна мати експоненційний характер;

- захищеність від колізій, при яких практично неможливо знайти два прообрази m_1 і m_2 – такі, що $H(m_1) = H(m_2)$, тобто складність знаходження двох прообразів m_1 і m_2 також повинна мати експоненційний характер.

Якщо використовувана геш-функція не забезпечує захист від колізій, то криптоаналітик знаходить $H(m_1) = H(m_2)$, де m_1 дійсні, заздалегідь підписані легальним користувачем дані. Потім він приєднує ЦП $\langle r, s \rangle$ для даних m_1 до даних m_2 та відсилає підписані дані $\langle m_2, \langle r, s \rangle \rangle$. Одержувач при перевірці ЦП не виявить підробки, і йому будуть нав'язані хибні дані m_2.

Підписи, що розглядаються, використовують геш-функції, описані у стандарті ISO/IEC 10118-3. Ці геш-функції є стійкими до колізій, крім SHA-1,що була скомпрометована. Тобто усі підписи, що розглядаються, є захищеними від такого виду атак.

3) *Оцінка стійкості ЦП від атак типу «селективна підробка»*

Сутність такої підробки полягає в тому, що при невідомому особистому ключі d для заздалегідь обраних даних (повідомлення) m необхідно сформувати такий підпис $\langle r, s \rangle$, щоб перевірка на цілісність і справжність підписаних даних m давала позитивний результат.

Криптоаналітик для здійснення такої підробки формує ключ сеансу $k_x \in (1,2,...,n-1)$, далі обчислює відкритий ключ сеансу $r_x = \pi(k_x \times G)$ та обирає такий підпис повідомлення $M_x, s_x \in \{1,...,n-1\}$, що $s_x = (k_x)^{-1}(dr_x + e') \bmod n$. Після цього записує в базу даних хибне M_x з підписом $\langle r_x, s_x \rangle$. Одержувач прийме це повідомлення за вірне, якщо порушник правильно обрав пару $\langle r_x, s_x \rangle$.

Аналіз цього виразу показує, що ймовірність правильного вибору s_x у ході підробки однозначно визначається ймовірністю підбору чи вгадування ключа d і складає для ЦП в групі точок еліптичних кривих дуже малу величину, наприклад порядку 2^{-Ld}, де Ld – довжина особистого ключа. Тобто всі підписи, що розглядаються, є захищеними від цього виду атак.

4) *Аналіз захищеності існуючих ЦП від атак на зв'язаних ключах.*

Особливістю ЦП як криптографічного перетворення є те, що асиметрична пара ключів генерується кожним власником особисто у складі особистого та відкритого ключів. Це означає, що власник такої пари ключів може генерувати її, використовуючи спеціальні засоби, у тому числі й такі, що створюються порушником для шахрайства.

Сутністю атаки на зв'язаних ключах є те, що порушник обирає такий відкритий ключ шифрування k_2, що $k_1 + k_2 = n$, де k_1– дійсний відкритий ключ, n – порядок базової точки. Далі він робить спробу для повідомлень *Mi* та *Mj* виробити однакові ЦП, зловмисник може маніпулювати цими підписаними повідомленнями, пред'являючи або передаючи при реалізації загроз те чи інше повідомлення.

Розглянемо можливості створення колізій підписів для *Mi* та *Mj* на зв'язаних ключах k_1 та $k_2 = n - k_1$.

Для повідомлення *Mi*	Для повідомлення *Mj*
1. $k_1 \in [1, n-1]$. $f_{k1} = \pi(k_1 G) =$	1. $k_2 = (n - k_1) \in [1, n-1]$. $f_{k2} = \pi((n - k_1)G) =$
2. $= \pi(x_{R_1}, y_{R_1}) =$ $= x_{R_1}$	2. $= \pi(nG - k_1 G) =$ $= \pi(x_{R_1}, -y_{R_1}) = x_{R_1}$.
3. Формується передпідпис $(k_1, f_{k_1}) = (k_1, x_{R_1})$.	3. Формується передпідпис $(k_2, f_{k_2}) = (k_2, x_{R_1})$.
4. Обчислити $h_1 = H(M_i)$.	4. Обчислити $h_2 = H(M_j)$.
5. Обчислити елемент основного поля $y_1 = h_1 x_{R_1} = r_1$.	5. Обчислити елемент основного поля $y_2 = h_2 x_{R_1} = r_2$.
6. Обчислити $s_1 = (k_1 + dr_1) \bmod n$	6. Обчислити $s_2 = (k_2 + dr_2) \bmod n$

Проведемо аналіз результатів, що одержані у другому рядку. Як бачимо f_{k_1}=f_{k_2}. Хоча у пятому рядку $r_1 \neq r_2$, але r_1 та h_1 відомі, тому:

$$x_{R_1} = \frac{y_1}{h_1}; \tag{5.5}$$

$$y_2 = r_2 = h_2 \frac{y_1}{h_1} = y_1 \frac{h_2}{h_1} = r_1 \frac{h_2}{h_1}. \tag{5.6}$$

Це означає, що, знаючи r_1 та h_1, можна знайти x_{R_1}.

Таким чином, хоч $r_1 \neq r_2$, але компоненти r_1, r_2 зв'язані між собою й обчислювально легко визначаються при відомих *Mi* та *Mj*.

Можна зробити висновок, що усі алгоритми, що використовують $\pi()$-функцію вирізання координати x з відкритого ключа, є слабкими до атаки на зв'язаних ключах. Такими є усі алгоритми ISO/IEC 9796-3, ДСТУ ISO/IEC 14888-3(ECDSA, EC-GDSA), ДСТУ 4145-2002, Fips 186-3 та ГОСТ 10-2012, крім EC-KCDSA, у якому використовується функція гешування замість $\pi()$-функції.

Таким чином, виникає ряд проблемних питань, сутність яких полягає в тому, що прийняті стандарти, які будуть застосовані і застосовуються, не відповідають ряду вимог, що висуваються до ЦП, перш за все щодо стійкості проти атак на зв'язаних ключах.

Висновки

Проведений аналіз електронних підписів, що базуються на 4145-2002, Fips 186-3 та ГОСТ 10-2012 згідно критерію стійкість-складність (швидкодія). В результаті зроблено такі висновки:

– найбільший спектр значень забезпечений в українському стандарті ДСТУ 4145-2002, що дозволяє варіювати критерієм стійкість-складність та адаптувати його механізм до потреб користувача;

– у ДСТУ 4145-2002 використання «-» в функції вироблення відкритого ключа $Q = -d_i \times G$, та вироблення передпідпису дозволяє прискорити алгоритм ЦП;

– найкращі характеристики стосовно показнику безпечний час мають алгоритми стандартів ГОСТ Р 34.10 – 2012, ДСТУ 4145 – 2002 та Fips 186-3;

– алгоритми EC-KCDSA, ДСТУ 4145-2002, ISO/ IEC 9796-3 забезпечують покращену процедуру підписування та, разом з EC-GDSA, вироблення ключа, так як вони не виконують операції ділення за модулем n. Ці обчислення є достатньо складними в обмеженому обчислювальному середовищі, такому як старт-карти. Тому в деяких середовищах алгоритм EC-KCDSA може бути обчислювально більш ефективним, ніж інші алгоритми;

– схему з відновленням повідомлення ISO/ IEC 9796-3 доцільно використовувати в інформаційних системах і протоколах з чітко визначеними повідомленнями, наприклад для захисту товарів та послуг в Інтернет-магазинах;

– усі розглянуті алгоритми захищені від «селективної», «екзистенційної» підробок та атаки «повне розкриття» на основі підписаних даних;

– використання $\pi()$ функції (вирізання тільки *x*-координати при обчисленні відкритого параметра сеансу *r* ЦП) робить усі розглянуті алгоритми не захищеними від атаки на зв'язаних ключах, крім EC-KCDSA, який є захищеним від такого виду атак;

– шифрування повідомлень захищає від атаки на основі підписаних повідомлень;

– на алгоритми ECDSA, EC-GCDSA, EC-KCDSA, ДСТУ 4145-2002, ГОСТ Р 34.10-2012 існують атаки на програмну реалізацію, тож необхідно використовувати надійні засоби КЗІ та забезпечити повністю апаратну реалізацію процедур вироблення та перевірки цифрових підписів.

Список літератури: 1. *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування. Вид. 2-е. – Харків : ФОРТ, 2012. – 878с. 2. *ДСТУ 4145-2002.* Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. 3. *ДСТУ ISO/IEC 14888-3.* Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів.4. *ГОСТ Р 34.10-2012.* Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. 5. *Fips 186-3:2013.* Federal information processing standards. Digital Signature Standard (DSS). 6. *ISO/IEC 10118-3.* Information technology -- Security techniques – Hash-functions – Part 3: Dedicated hash-functions. 7. *ISO/IEC 9796-3:2006*. Information technology. Security techniques. Digital signature schemes giving message recovery. Part 3: Discrete logarithm based mechanisms.

Харківський національний університет
імені В.Н.Каразіна

Надійшла до редколегії 27.04.2015