# Захист інформації

УДК 004.056.55

Ю.І. Горбенко, М.В. Єсіна, В.А. Кулібаба

*Харківський національний університет імені В.Н. Каразіна, Харків*

## СУТНІСТЬ ТА УМОВИ ЗДІЙСНЕННЯ АТАКИ НА ЗВ'ЯЗАНИХ КЛЮЧАХ ВІДНОСНО ЕЛЕКТРОННИХ ПІДПИСІВ IBS-1 ТА IBS-2 ДСТУ ISO/IEC 14888-3

*У роботі розглядається стан захищеності електронних підписів на основі спарювання точок еліптичної кривої від атак на основі підписаних даних зі зв'язаними ключами. Визначаються умови та можливості організації та реалізації цих атак. Надаються рекомендації відносно захисту від вказаних вразливостей, в тому числі у пост квантовий період.*

***Ключові слова**: атака, електронний підпис, зв'язані ключі.*

### Вступ

Нині широке розповсюдження отримують електронні підписи (ЕП), стійкість яких ґрунтується на складності дискретного логарифмування в скінченних полях та групах точок еліптичних кривих (ЕК) [3 – 4]. Також пройшли дослідження та рекомендуються до застосування ЕП з додатком, що ґрунтуються на ідентичності – спарюванні точок ЕК. Відомі умови здійснення атак на зв'язаних ключах відносно ЕП, що ґрунтуються на стандартизованих криптографічних перетвореннях в скінченних полях та циклічних групах супернесингулярних кривих. Проведений аналіз значного числа джерел дозволив зробити висновок, що відносно захищеності та умов здійснення атак на зв'язаних ключах відносно ЕП IBS-1 та IBS-2, які ґрунтуються на ідентичності [1, 3 – 4], даних немає. В той же час попередні дослідження стійкості алгоритмів ЕП IBS-1 та IBS-2 показали, що атака на зв'язаних ключах може бути реалізована. Тому важливими є дослідження стійкості вказаних ЕП від атак на зв'язаних ключах.

Особливо актуальними проблеми стійкості стали після заяв та виступів провідних спеціалістів про потенціальні вразливості на ЕП в пост квантовий період. Так в технічному звіті АНБ США [1], стверджується що ЕП, алгоритми яких ґрунтуються на перетворенні в кільці [1 – 2] та в скінченному полі [1 – 2] будуть нестійкими при появі квантових комп'ютерів. Такі ж підозри висловлені і відносно криптографічних перетворень в групі точок еліптичної кривої [1 – 2]. Тому важливими є задачі, їх вирішення, відносно стійкості ЕП, що нині введені в Україні та які діють на міжнародному рівні. До такого стандарту необхідно віднести ДСТУ ISO/IEC 14888-3:2014 [4].

Одним із можливих шляхів розв'язання вказаного протиріччя є збільшення розмірів загальних параметрів для вказаних перетворень. На першому етапі розвитку квантової криптографії це може спрацювати. Але в подальшому потрібно застосовувати інші методи, наприклад, можливо, криптоперетворення на основі спарювання точок ЕК та ідентифікаційних даних. Такі алгоритми пропонуються в ДСТУ ISO/IEC 14888-3:2014 у вигляді алгоритмів ЕП IBS-1 та IBS-2 [4]. Але проведений аналіз показав, що хоч вони при певних умовах і можуть претендувати на пост квантові, необхідні подальші дослідження їх стійкості. На наш погляд однією із вразливостей алгоритмів ЕП IBS-1 та IBS-2 є їх незахищеність від атак на зв'язаних ключах.

**Метою цієї статі** є аналіз стану захищеності ЕП IBS-1 та IBS-2 від атак на основі підписаних даних зі зв'язаними ключами, визначення умов та можливостей їх організації та здійснення, а також розробка рекомендацій відносно захисту від вказаних вразливостей, в тому числі у пост квантовий період.

### 1. Сутність ЕП IBS-1 та IBS-2, що визначені та реалізовані в ДСТУ ISO/IEC 14888-3

Зважаючи на новизну та необхідність постановки задачі дослідження ЕП IBS-1 та IBS-2, спочатку розглянемо сутність механізмів цих ЕП та етапи налаштування.

Для застосування ЕП IBS-1 та IBS-2 спочатку повинні бути введеними та налаштовані загальні параметри та сгенеровані асиметричні пари ключів.

Загальними параметрами ЕП IBS-1 та IBS-2 є [3, 4]:

- U – секретний майстер-ключ – ціле число, $U \in [1, q-1]$;
- V – відкритий майстер-ключ – точка ЕК, $V = [U]P \bmod q$, $V \in G_1$;
- X – особистий (секретний) ключ підписувача – точка ЕК, $X = [U]Y \bmod q$, $X \in G_1$;

- $Y$ – відкритий ключ (перевіряння) підписувача – точка ЕК, $Y = H_1(ID) \bmod q$, $Y \in G_1$;
- $P$ – базова точка центру сертифікації ключів порядку $q$.

Генерація чи обчислення загальних параметрів повинні здійснюватись з дотриманням таких умов:

- особистий ключ користувача $X$ обчислюється за його запитом у центрі генерації ключів (ЦГК) та надається користувачеві по захищеному каналу;
- відкритий ключ користувача $Y$ може обчислити кожен користувач домену;
- $ID$ – є рядок даних, що містить ідентифікатор підписувача;
- $H_1$ – функція гешування, яка перетворює рядок даних у елемент групи $G_1$;
- $H_2$ – функція гешування, що визначена у ДСТУ ISO/IEC 10118-3:2005;
- $G_1$ – циклічна група простого порядку $q$, елементами якої є точки на ЕК над GF(p);
- $G_2$ – циклічна група простого порядку $q$, елементами якої є елементи скінченого поля $GF(p^m)$.

В табл. 1, 2 наведені механізми IBS-1 та IBS-2 підписування та перевіряння [4].

Таблиця 1

Механізм ЕП IBS-1

| Підпис повідомлення | Перевірка підпису |
|---|---|
| 1. Генерування випадкового чи псевдовипадкового одноразового таємного ключа – цілого числа $K$, $1 < K < (q-1)$. | 1. Перевірник отримує цілісні загальні параметри та відкритий ключ підписувача. |
| 2. Здійснення спарювання: $\Pi =< X, P >^K$, $\Pi \in G_2$ над полем $GF(p^m)$, $\Pi$ – передпідпис | 2. Відновлення одноразового відкритого ключа:<br>– $R$ та $S$ відновлюються з доповнення;<br>– бітова довжина $R$ повинна дорівнювати довжині виходу функції $H_2$;<br>– $S \in G_1$.<br>Якщо хоча б одна з цих умов не виконується, підпис відхиляється. |
| 3. Повідомлення у вигляді цілого $M$ розбивається на його частини:<br>$M_2$ – порожня частина,<br>$M_1 = M$ – повідомлення, що треба підписати. | 3) Підготування повідомлення до перевіряння:<br>– відновлення $M$ з підписаного повідомлення;<br>– розбиття повідомлення на $M_1$ та $M_2$: $M_2$ – порожнє, $M_1 = M$. |
| 4. Обчислення одноразового відкритого ключа: $R = H_2(M_1 \| FE2BS(\Pi))$, $R \in G_2$. | 4. Відновлення призначення: $T = (T_1, T_2)$, $T_1 = -Y$, $T_2 = [R]Y$. |
| 5. Обчислення призначення: $T = (T_1, T_2) = (-Y, [R]Y)$. | 5. Здійснення спарювання: $\overline{\Pi} =< S, P > \times < Y, V >^R$. |
| 6. Обчислення компоненти підпису: $S = [K - R]X \bmod q$, $S \in G_1$. Підписом є $\Sigma = (R, S)$. | 6. Обчислення одноразового відкритого ключа перевірки: $\overline{R} = H_2(M_1 \| FE2BS(\overline{\Pi}))$. |
| 7. Побудова доповнення з конкатенуванням тексту у вигляді $(R, S) \| text$. | 7. Порівняння $\overline{R} = R$: якщо не співпадають, то підпис хибний, інакше – вірний. |
| 8. Побудова підписаного повідомлення у вигляді $M((R, S) \| text)$. | |

## 2. Атака «Повне розкриття» на ЕП IBS-1 на основі підписаних даних та зв'язуванні ключів

Нехай криптоаналітик перехопив та має повний доступ до $i$ підписаних повідомлень [2,4]:

$$\begin{cases} S_1 = [K_1 - R_1]X \bmod q; \\ ..... \\ S_i = [K_i - R_i]X \bmod q. \end{cases} \quad (1)$$

В систему (1) входить $i$ рівнянь та $i+1$ невідомих.

Знайдемо невідому точку ЕК – особистий довгостроковий ключ $X$, який для усіх підписів є постійним. У результаті отримаємо систему виду:

$$\begin{cases} X = [K_1 - R_1]^{-1} S_1 \bmod q; \\ ... \\ X = [K_i - R_i]^{-1} S_i \bmod q. \end{cases} \quad (2)$$

В системі (2) невідомими є особистий довгостроковий ключ $X$ та $i$ невідомих $K_1, K_2, ..., K_i$. Для повного розкриття, тобто визначення секретного ключа $X$ за $i$ ЕП, необхідно розв'язати систему

$i$ -го порядку з $i+1$ невідомими. Проведений аналіз показав, що силовим методом понизити систему рівнянь практично неможливо. Тому можна вважати, що атака на основі підписаних даних має експоненційну складність [2, 4].

Таблиця 2

Механізм ЕП IBS-2

| Підпис повідомлення | Перевірка підпису |
|---|---|
| 1. Генерування випадкового чи псевдовипадкового одноразового таємного ключа – цілого числа $K$, $1 < K < (q-1)$. | 1. Перевірник отримує цілісні чинні загальні параметри та чинний відкритий ключ підписувача. |
| 2. Здійснення скалярного множення: $\Pi = [K]Y \bmod q$, $\Pi \in G_1$, $\Pi$ – передпідпис, точка ЕК. | 2) Відновлення одноразового відкритого ключа:<br>– $R$ та $S$ відновлюються з доповнення;<br>– $R \in G_1$, $S \in G_1$.<br>Якщо хоча б одна з цих умов не виконується, підпис відхиляється. |
| 3. Повідомлення у вигляді цілого $M$ розбивається на його частини:<br>$M_1$ – порожня частина,<br>$M_2 = M$ – повідомлення, що треба підписати. | 3. Підготування повідомлення до перевіряння:<br>– відновлення $M$ з підписаного повідомлення;<br>– розбиття повідомлення на $M_1$ та $M_2$: $M_1$ – порожнє, $M_2 = M$. |
| 4. Обчислення одноразового відкритого ключа:<br>$R = \Pi$, $R \in G_1$. | 4. Відновлення призначення: $T = (T_1, T_2)$,<br>$T_1 = -Y$, $T_2 = [-H]Y$,<br>$H = H_2(M_2 \,\|\|\, \mathrm{FE2BS}(R_x))$. |
| 5. Обчислення призначення:<br>$T = (T_1, T_2) = (-Y, [-H]Y)$, $H \in G_2$,<br>$H = H_2(M_2 \,\|\|\, \mathrm{FE2BS}(\Pi_x))$. | 5. Обчислення перед підпису:<br>$\overline{\Pi} = R$, $\overline{\Pi} \in G_1$. |
| 6. Обчислення компоненти підпису:<br>$S = [K + H]X \bmod q$, $S \in G_1$.<br>Підписом є $\Sigma = (R, S)$. | 6. Обчислення:<br>$\overline{R}_1 =< P, S >$ та $\overline{R}_2 =< V, \overline{\Pi} + [H]Y >$. |
| 7. Побудова доповнення: $(R, S) \,\|\|\, \text{text}$. | 7. Порівняння $\overline{R}_1 = \overline{R}_2$: якщо не співпадають, то підпис хибний, інакше – вірний. |
| 8. Побудова підписаного повідомлення:<br>$M((R, S) \,\|\|\, \text{text})$. | |

Як показав аналіз, одним із можливих варіантів пониження порядку системи рівнянь може бути зв'язування ключів, наприклад, у вигляді [2]:

$$K_1 + K_2 = q \qquad (3)$$

чи іншим способом. Розглянемо атаку на зв'язаних ключах.

Запишемо систему (1) для випадку двох рівнянь та розглянемо алгоритми підписування для двох повідомлень $M_1$ та $M_2$, та ключів, що задовольняють умові (3):

| Для повідомлення $M_1$ | Для повідомлення $M_2$ |
|---|---|
| $K_1 \in [1, q-1]$ | $K_2 = (q - K_1) \in [1, q-1]$ |
| $\Pi_1 =< X, P >^{K_1}$ | $\Pi_2 =< X, P >^{K_2}$ |
| $R_1 = H_2(M_1 \,\|\|\, \mathrm{FE2BS}(\Pi_1))$ | $R_2 = H_2(M_2 \,\|\|\, \mathrm{FE2BS}(\Pi_2))$ |
| $S_1 = [K_1 - R_1]X \bmod q$ | $S_2 = [(q - K_1) - R_2]X \bmod q$ |

Далі знайдемо умову, при яких $S_1 = S_2$, тобто знайдемо особистий ключ $X$, при якому ЕП повідомлень $M_1$ та $M_2$ співпадають. В результаті маємо:

$$[K_1 - R_1]X \bmod q = [(q - K_1) - R_2]X \bmod q. \qquad (4)$$

Скоротимо в (4) на $X$, у результаті отримаємо:

$$[K_1 - R_1] \bmod q = [(q - K_1) - R_2] \bmod q; \qquad (5)$$

$$[K_1 - R_1] \bmod q = [-K_1 - R_2] \bmod q; \qquad (6)$$

$$2K_1 \bmod q = [R_1 - R_2] \bmod q. \qquad (7)$$

Далі знайдемо із (7) одноразовий ключ $K_1$, так як $R_1$ та $R_2$ відомі і містяться у підписі:

$$K_1 = \frac{R_1 - R_2}{2} \bmod q. \qquad (8)$$

Таким чином, порядок системи рівнянь понижено на невідомий одноразовий таємний ключ, в нашому випадку $K_1$:

$$\begin{cases} X = [K_1 - R_1]^{-1} S_1 \bmod q; \\ \ldots \\ X = [K_i - R_i]^{-1} S_i \bmod q. \end{cases} \qquad (9)$$

Підставивши $K_1$, а взагалі $K_j$, у систему (9), маємо систему з і рівнянь з і невідомими, яка має розв'язок.

## 3. Атака «повне розкриття» на ЕП IBS-2 на основі підписаних даних та зв'язуванні ключів

Аналогічно з (1), для IBS-2 з урахуванням табл. 2, маємо [2, 4]:

$$\begin{cases} S_1 = [K_1 + H_1]X \bmod q; \\ ..... \\ S_i = [K_i + H_i]X \bmod q. \end{cases} \quad (10)$$

Далі, знайдемо із (10) особистий довгостроковий ключ $X$ та відносно нього одержимо наступне:

$$\begin{cases} X = [K_1 + H_1]^{-1} S_1 \bmod q; \\ ... \\ X = [K_i + H_i]^{-1} S_i \bmod q. \end{cases} \quad (11)$$

В систему (10) при отриманні і підписаних повідомлень входить і рівнянь та $i+1$ невідомих. Основною задачею криптоаналітика є визначення особистого довгострокового ключа $X$.

Як і у випадку (2), як показує аналіз, понизити систему рівнянь (11) силовим методом практично неможливо. Причому складність силової атаки визначається порядком циклічної групи $q$. Тому можна вважати, що складність атаки на основі підписаних даних носить експоненційний характер [2, 4].

У той же час, як і у випадку (2), одним із можливих варіантів пониження порядку системи рівнянь (11) може бути зв'язування ключів, наприклад, у вигляді (3) чи іншим способом [2].

Запишемо систему (11) для випадку двох рівнянь та вказаного зв'язування ключів, і розглянемо алгоритми підписування для двох повідомлень $M_1$ та $M_2$, та ключів, що задовольняють умові (3):

| Для повідомлення $M_1$ | Для повідомлення $M_2$ |
|---|---|
| $K_1 \in [1, q-1]$ | $K_2 = (q - K_1) \in [1, q-1]$ |
| $\Pi_1 = [K_1]Y \bmod q$ | $\Pi_2 = [K_2]Y \bmod q =$ $= [q - K_1]Y \bmod q =$ $= [-K_1]Y \bmod q$ |
| $R_1 = \Pi_1$ | $R_2 = \Pi_2$ |
| $S_1 = [K_1 + H_1]X \bmod q$ | $S_2 = [K_2 + H_2]X \bmod q =$ $= [(q - K_1) + H_2]X \bmod q =$ $= [-K_1 + H_2]X \bmod q$ |

Знайдемо умову, при якій $S_1 = S_2$. У результаті маємо, що

$$[K_1 + H_1]X \bmod q = [(q - K_1) + H_2]X \bmod q. \quad (12)$$

Скоротивши в (12) на $X$, отримуємо, що:

$$[K_1 + H_1] \bmod q = [(q - K_1) + H_2] \bmod q$$

або $$[K_1 + H_1] \bmod q = [-K_1 + H_2] \bmod q$$

та $$2K_1 \bmod q = [H_2 - H_1] \bmod q. \quad (13)$$

На останок із (13) отримуємо, що

$$K_1 = \frac{H_2 - H_1}{2} \bmod q. \quad (14)$$

Таким чином, порядок системи рівнянь (11) понижено, так як за значеннями $H_1$ та $H_2$ можна визначити невідомий одноразовий таємний ключ $K_1$.

## 4. Приклад атаки «повне розкриття» на механізми ЕП IBS-1 та IBS-2 на основі підписаних даних та зв'язуванні ключів

Покажемо коректність виконання атак на прикладі. Визначимо значення необхідних параметрів – значення базової точки $P$, особистого ключа користувача $X$ та порядок базової точки $q$: $X = (13,16)$, $P = (13,7)$, $q = 7$. ЕК над основним полем: $y^2 = (x^3 + x + 1) \bmod 23$.

Розглянемо приклад для механізму IBS-1 [3 – 4].

Запишемо систему (1) для випадку двох рівнянь та розглянемо алгоритми підписування для двох повідомлень $M_1$ та $M_2$, та ключів, що задовольняють умові (3):

| Для повідомлення $M_1$ | Для повідомлення $M_2$ |
|---|---|
| $K_1 = 6$ | $K_2 = (q - K_1) = 1$ |
| $\Pi_1 = <X, P>^{K_1}$ | $\Pi_2 = <X, P>^{K_2}$ |
| $R_1 = H_2(M_1 \,\|\| \, FE2BS(\Pi_1))$ | $R_2 = H_2(M_2 \,\|\| \, FE2BS(\Pi_2))$ |
| $S_1 = [K_1 - R_1]X \bmod q$ | $S_2 = [K_2 - R_2]X \bmod q$ |
| $S_1 = [6-4](13,16) \bmod 7 =$ | $S_2 = [1-20](13,16) \bmod 7 =$ |
| $= 2(13,16) \bmod 7 = (5,19)$ | $= (-19)(13,16) \bmod 7 = (5,19$ |

Згідно формули (8) для $K_1$ отримаємо:

$$K_1 = \frac{4-20}{2} \bmod 7 = \frac{-16}{2} \bmod 7 = (-8) \bmod 7 = 6.$$

Розв'яжемо рівняння із системи (2), підставивши в нього отримане значення $K_1$:

$$\widetilde{X} = [K_1 - R_1]^{-1} S_1 \bmod q;$$

$$\widetilde{X} = [6-4]^{-1}(5,19) \bmod 7 = (2)^{-1}(5,19) \bmod 7.$$

Знайдемо обернений елемент у полі:

$$z = \frac{1}{k} \bmod q;\ z \cdot k = 1 \bmod q;\ z \cdot 2 = 1 \bmod 7;\ z = 4.$$

Отже, після знаходження оберненого елемента, отримаємо наступне:

$$\widetilde{X} = 4(5,19) \bmod 7 = (13,16).$$

Ми знайшли значення особистого ключа підписувача $\widetilde{X}$. Порівняємо його з $X$:

$$\widetilde{X} = (13,16), X = (13,16) \Rightarrow \widetilde{X} = X.$$

Отже, для механізму IBS-1 розглянута атака є реалізуємою.

Розглянемо приклад для механізму IBS-2 [3 – 4].

Запишемо систему (10) для випадку двох рівнянь та розглянемо алгоритми підписування для двох повідомлень $M_1$ та $M_2$, та ключів, що задовольняють умові (3):

| Для повідомлення $M_1$ | Для повідомлення $M_2$ |
|---|---|
| $K_1 = 6$ | $K_2 = (q - K_1) = 1$ |
| $\Pi_1 = [K_1]Y \bmod q$<br>$\Pi_1 = 6(17,20) \bmod 7 =$<br>$= (17,3)$ | $\Pi_2 = [-K_1]Y \bmod q$<br>$\Pi_2 = -6(17,20) \bmod 7 =$<br>$= (17,20)$ |
| $R_1 = \Pi_1 = (17,3)$ | $R_2 = \Pi_2 = (17,20)$ |
| $S_1 = [K_1 + H_1]X \bmod q$<br>$H_1 = 3$<br>$S_1 = [6+3](13,16) \bmod 7 =$<br>$= 2(13,16) \bmod 7 = (5,19)$ | $S_2 = [(q - K_1) - R_2]X \bmod q$<br>$H_2 = 15$<br>$S_2 = [-6+15](13,16) \bmod 7 =$<br>$= 2(13,16) = (5,19)$ |

Згідно формули (14) для $K_1$ отримаємо:

$$K_1 = \frac{15-3}{2} \bmod 7 = \frac{12}{2} \bmod 7 = 6.$$

Розв'яжемо рівняння із системи (11), підставивши в нього отримане значення $K_1$:

$$\widetilde{X} = [K_1 + H_1]^{-1} S_1 \bmod q;$$

$$\widetilde{X} = [6+3]^{-1}(5,19) \bmod 7 = (9)^{-1}(5,19) \bmod 7.$$

Знайдемо обернений елемент у полі:

$$z = \frac{1}{k} \bmod q;\ z \cdot k = 1 \bmod q;\ z \cdot 9 = 1 \bmod 7;\ z = 4.$$

Отже, після знаходження оберненого елемента, отримаємо наступне:

$$\widetilde{X} = 4(5,19) \bmod 7 = (13,16).$$

Ми знайшли значення особистого ключа підписувача $\widetilde{X}$. Порівняємо його з $X$:

$$\widetilde{X} = (13,16), X = (13,16) \Rightarrow \widetilde{X} = X.$$

Отже, для механізму IBS-2 розглянута атака є реалізуємою.

## 5. Атака «повне розкриття» на ЕП IBS-1 та IBS-2 на основі підписаних даних та зв'язуванні ключів: альтернативний підхід

Нехай криптоаналітик перехопив та має повний доступ до і підписаних повідомлень: аналогічно до (1) та (10). Знайдемо невідому точку ЕК – особистий довгостроковий ключ $X$, який для усіх підписів є постійним.

Розглянемо атаку на ЕП IBS-1 на основі зв'язування ключів. Вихідні дані будуть аналогічні даним, що наведені у розділі 2 [4]. У результаті отримаємо для IBS-1 систему вигляду:

$$\begin{cases} S_1 = [K_1 - R_1]X \bmod q; \\ S_2 = [-K_1 - R_2]X \bmod q; \end{cases}$$

$$S_1 + S_2 = [(K_1 - R_1) + (-K_1 - R_2)]X \bmod q;$$

$$S_1 + S_2 = [-R_1 - R_2]X \bmod q;$$

$$X = (S_1 + S_2)[-R_1 - R_2]^{-1} \bmod q; \qquad (15)$$

$$X = -[R_1 + R_2]^{-1}(S_1 + S_2) \bmod q.$$

Розглянемо атаку на ЕП IBS-2 на основі зв'язування ключів. Вихідні дані будуть аналогічні даним, що наведені у розділі 3 [4]. У результаті отримаємо для IBS-2 систему вигляду:

$$\begin{cases} S_1 = [K_1 + H_1]X \bmod q; \\ S_2 = [-K_1 + H_2]X \bmod q; \end{cases}$$

$$S_1 + S_2 = [(K_1 + H_1) + (-K_1 + H_2)]X \bmod q; \qquad (16)$$

$$S_1 + S_2 = [H_1 + H_2]X \bmod q;$$

$$X = [H_1 + H_2]^{-1}(S_1 + S_2) \bmod q.$$

Тепер наведемо математичний приклад і коректність виконання атак на прикладі.

Спочатку розглянемо приклад для механізму IBS-1. Вихідні дані будуть аналогічні даним, що наведені у розділі 4. Використовуючи (15), для знаходження особистого ключа підписувача $X$ маємо:

$$\widetilde{X} = -[R_1 + R_2]^{-1}(S_1 + S_2) \bmod q;$$

$$\widetilde{X} = -[4+20]^{-1}((5,19) + (5,19)) \bmod 7;$$

$$\widetilde{X} = (-24)^{-1}(2(5,19)) \bmod 7.$$

Знайдемо обернений елемент у полі:

$$z = \frac{1}{k} \bmod q;\ z \cdot k = 1 \bmod q;$$

$$z \cdot (-24) = 1 \bmod 7;\ z = 2.$$

Отже, після знаходження оберненого елемента, отримаємо наступне:

$$\widetilde{X} = 2(17,3) \bmod 7 = (13,16); \qquad (17)$$

$$\widetilde{X} = (13,16), X = (13,16) \Rightarrow \widetilde{X} = X.$$

Отже, виходячи з (17), для механізму IBS-1 розглянута атака є реалізуємою.

Розглянемо приклад для механізму IBS-2. Вихідні дані будуть аналогічні даним, що наведені у розділі 4. Використовуючи (16), для знаходження особистого ключа підписувача $X$ отримаємо:

$$\widetilde{X} = [H_1 + H_2]^{-1}(S_1 + S_2) \bmod q;$$

$$\widetilde{X} = [3+15]^{-1}((5,19) + (5,19)) \bmod 7;$$

$$\widetilde{X} = [4]^{-1}(17,3) \bmod 7.$$

Знайдемо обернений елемент у полі:

$$z = \frac{1}{k} \bmod q;\ z \cdot k = 1 \bmod q;\ z \cdot 4 = 1 \bmod 7;\ z = 2.$$

Отже, після знаходження оберненого елемента, отримаємо таке:

$$\widetilde{X} = 2(17,3) \bmod 7 = (13,16); \qquad (18)$$

$$\widetilde{X} = (13,16), X = (13,16) \Rightarrow \widetilde{X} = X.$$

Отже, виходячи з (18), для механізму IBS-2 розглянута атака може бути реалізована з поліноміальною складністю.

## 6. Пропозиції з захисту алгоритмів ЕП IBS-1 та IBS-2 від атак на зв'язаних ключах

Проведений аналіз дозволив запропонувати наступні механізми захисту ЕП IBS-1 та IBS-2 від атак на зв'язаних ключах [2, 4].

1. На основі шифрування підписаних повідомлень з використанням симетричних чи асиметричних шифрів. З точки зору складності (швидкодії) шифрування та стійкості, краще застосовувати симетричні шифри – блокові чи потокові. Тоді криптоаналітику потрібно буде розв'язувати систему із $2i+1$ невідомими, але для системи з $i$ рівняннями. Така задача при реальних значення параметрів є експоненційно складною.

2. Іншим механізмом захисту від атак на зв'язаних ключах ЕП IBS-1 та IBS-2 є виключення можливостей зв'язування одноразових ключів $K$ в процесі здійснення підписування потоку повідомлень. Вказане може бути здійснене на основі застосування апаратних чи апаратно-програмних засобів ЕП, які виключали б можливість втручання в процес підписування повідомлень. Можливі і інші механізми ЕП.

## Висновки та рекомендації

1. В процесі удосконалення ЕП, запропоновані алгоритми ЕП IBS-1 та IBS-2 на ідентифікаторах зі спарюванням точок ЕК, в них в якості особистого ключа запропоновано використовувати точку еліптичної кривої $X$. В результаті при перехопленні $i$ підписаних повідомлень для визначення довгострокового ключа $X$ необхідно розв'язувати систему рівнянь з $i+1$ невідомим, $i$ з яких є великими випадковими числами, одне – $X$ є точкою ЕК. В процесі аналізу не було виявлено ефективних методів розв'язку такої системи.

2. Виявлено, що криптоперетворення ЕП IBS-1 та IBS-2 не забезпечують криптографічної стійкості проти атак на зв'язаних ключах. При чому було отримано 2 різних варіанти здійснення атак на зв'язаних ключах.

3. Для алгоритму ЕП IBS-1 атака на зв'язаних ключах може бути здійснена з використанням отриманих співвідношень (8) та (9). Причому її складність носить поліноміальний характер.

4. Для алгоритму ЕП IBS-2 атака на зв'язаних ключах може бути здійснена з використанням отриманих співвідношень (11) та (14). Її складність також носить поліноміальний характер.

5. Можливість здійснення атак відносно алгоритмів ЕП IBS-1 та IBS-2 підтверджена не тільки програмним моделюванням, а і на прикладах, що наведені в розділі 4 цієї статі.

6. Також виявлено інший метод здійснення атак на алгоритми ЕП IBS-1 та IBS-2, сутність якого викладена в розділі 5 цієї статі, зокрема з використанням систем (15) та (16). Вказані атаки також мають поліноміальну складність. Можливість здійснення вказаних атак також продемонстрована на прикладах.

7. Таким чином, як теоретично, так і на прикладах показано, що алгоритми ЕП IBS-1 та IBS-2 є нестійкими проти атак на зв'язаних ключах, тому при їх застосуванні потрібно використовувати механізми захисту від таких атак.

8. Також вище викладено пропозиції із можливих варіантів захисту ЕП для алгоритмів ДСТУ ISO/IEC 14888-3:2014 – IBS-1 та IBS-2 від атак на зв'язаних ключах. Основними з них є шифрування підписаних повідомлень та застосування кваліфікованих апаратно-програмних засобів ЕП.

## Список літератури

*1. Neal Koblitz A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes [Електронний ресурс]. – Режим доступу до ресурсу: https://eprint.iacr.org/2015/1018.pdf.*

*2. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Х.: «Форт», 2012. – 870 с.*

*3. Горбенко Ю.І. Електронні підписи на основі ідентифікаторів та бінарного відображення / Ю.І. Горбенко, Р.С. Ганзя, О.С. Акользіна // Прикладная радиоэлектроника. – Х. : ХНУРЭ, 2015. – Т. 14, № 4. – С. 284-290.*

*4. Інформаційні технології – Методи захисту – Цифрові підписи з доповненням – Частина 3. Механізми, що ґрунтуються на дискретному логарифмі : (ISO/IEC 14888-3:2008, IDT) ДСТУ ISO/IEC 14888-3:2014 : 2014. – 113 с.*

*Надійшла до редколегії 13.04.2016*

**Рецензент:** д-р техн. наук, проф. О.О. Кузнецов, Харківський національний університет імені В.Н. Каразіна, Харків.

### СУЩНОСТЬ И УСЛОВИЯ ВЫПОЛНЕНИЯ АТАКИ НА СВЯЗАННЫХ КЛЮЧАХ ОТНОСИТЕЛЬНО ЭЛЕКТРОННЫХ ПОДПИСЕЙ IBS-1 И IBS-2 ДСТУ ISO/IEC 14888-3

Ю.И. Горбенко, М.В. Есина, В.А. Кулибаба

*В работе рассматривается состояние защищенности электронных подписей на основе спаривания точек эллиптической кривой от атак на основе подписанных данных со связанными ключами. Определяются условия и возможности организации и реализации этих атак. Предоставляются рекомендации относительно защиты от указанных уязвимостей, в том числе в пост квантовый период.*

***Ключевые слова:*** *атака, связанные ключи, электронная подпись.*

### THE ESSENCE AND CONDITIONS OF RELATED KEYS ATTACK RELATIVELY ELECTRONIC SIGNATURES IBS-1 AND IBS-2 OF DSTU ISO/IEC 14888-3

Yu.I. Gorbenko, M.V. Yesina, V.A. Kulibaba

*The paper deals with the state of protection electronic signatures based on the pairing of points of an elliptic curve from attacks by the signing data with related keys. It is defined the conditions and possibilities of the organization and implementation of these attacks. It is provided the recommendations on protection from these vulnerabilities, including in the post quantum period.*

***Keywords:*** *attack, related keys, electronic signature.*