УДК 004.056.55

МАТЕМАТИЧНА ТА ПРОГРАМНА МОДЕЛІ РЕАЛІЗАЦІЇ АТАКИ НА ЗВ'ЯЗАНИХ КЛЮЧАХ ВІДНОСНО МЕХАНІЗМУ ЕЛЕКТРОННОГО ПІДПИСУ IBS-1

М.В. ЄСІНА, В.А. КУЛІБАБА

У роботі розглядається стан захищеності електронних підписів на основі спарювання точок еліптичної кривої від атаки на зв'язаних ключах. Визначаються умови та можливості організації та реалізації цього виду атак. Будуються математична та програмна моделі реалізації атаки на зв'язаних ключах щодо механізму електронного підпису IBS-1. Надаються рекомендації відносно захисту від вказаних уразливостей, у тому числі у постквантовий період.

Ключові слова: атака, електронний підпис, зв'язані ключі, спарювання точок еліптичної кривої.

ВСТУП

На сьогоднішній день ретельно досліджуються та рекомендуються до застосування електронні підписи (ЕП) з додатком, що ґрунтуються на ідентичності – спарюванні точок еліптичної кривої (ЕК) [4, 5]. 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 джерел дозволив зробити висновок, що відносно захищеності та умов здійснення атак на зв'язаних ключах відносно ЕП IBS-1 даних практично немає [4 – 6]. Водночас попередні дослідження стійкості алгоритму ЕП IBS-1 показали, що атака на зв'язаних ключах може бути реалізована [5]. Тому важливими є дослідження стійкості вказаного ЕП від атаки на зв'язаних ключах, а також побудова математичних та програмних моделей реалізації визначеної атаки.

Проблеми стійкості стали особливо актуальними після заяв та виступів провідних спеціалістів про потенціальні уразливості на ЕП у постквантовий період. Технічний звіт АНБ США [1] стверджує, що ЕП, алгоритми яких ґрунтуються на перетворенні в кільці та в скінченному полі [3, 6] будуть нестійкими за появи квантових комп'ютерів. Аналогічні припущення висловлені також відносно криптографічних перетворень в групі точок еліптичної кривої [3,6]. Таким чином важливими є задачі та їх вирішення, відносно стійкості ЕП, що базуються на ідентичності [4 – 6].

Отже, метою цієї статі є аналіз стану захищеності механізму ЕП IBS-1 від атаки на зв'язаних ключах та демонстрація можливості практичного здійснення такої атаки на прикладі бібліотеки PBC [2], що свідчить про недопустимість застосування цього алгоритму як перспективного стандарту ЕП в Україні в тому вигляді, в якому він був наведений, або про необхідність використання сертифікованих апаратних або апаратно-програмних засобів генерації ключів..

1. СУТНІСТЬ ЕЛЕКТРОННОГО ПІДПИСУ IBS-1

Зважаючи на новизну та необхідність постановки задачі дослідження ЕП IBS-1, спочатку розглянемо сутність цього механізму ЕП та етапи налаштування.

Для застосування ЕП IBS-1 спочатку мають введеними та налаштовані загальні параметри та сгенеровані асиметричні пари ключів [4 – 6].

В таблиці 1 наведено процес підписування та перевіряння за механізмом ЕП IBS-1 [5, 6].

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 $GF(p^m)$, Π – передпідпис	2. Відновлення одноразового відкритого ключа: – R та S відновлюються з доповнення; – бітова довжина R має дорівнювати довжині виходу функції H_2; – $S \in G_1$. Якщо хоча б одна з цих умов не виконується, підпис відхиляється.

Продовження таблиці 1

3. Повідомлення у вигляді цілого M розбивається на його частини: M_2 – порожня частина, $M_1 = M$ – повідомлення, що треба підписати.	3. Підготування повідомлення до перевірки: – відновлення M з підписаного повідомлення; – 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: $T = (T_1, T_2)$, $T_1 = -Y$, $T_2 = [R]Y$.
Підпис повідомлення	Перевірка підпису
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 – істинний.
8. Побудова підписаного повідомлення у вигляді $M((R, S) \| text)$.	

2. МАТЕМАТИЧНА МОДЕЛЬ РЕАЛІЗАЦІЇ АТАКИ НА ЗВ'ЯЗАНИХ КЛЮЧАХ НА МЕХАНІЗМ ЕП IBS-1

Нехай криптоаналітик перехопив та має повний доступ до i підписаних повідомлень [3, 5]:

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

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

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

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

У 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. Дану систему (2) можна розв'язати тільки за допомогою силового методу пониження порядку системи, але проведений аналіз показав, що таким чином понизити систему рівнянь практично неможливо. Тому можна вважати, що атака на основі підписаних даних має експоненційну складність [3].

Як показав проведений аналіз, одним із можливих варіантів пониження порядку системи рівнянь може бути зв'язування ключів, наприклад, у вигляді [3]:

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

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 умови (3).

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

Після цього знайдемо умову, за якої $S_1 = S_2$, тобто знайдемо особистий ключ X, при якому ЕП повідомлень M_1 та M_2 будуть однаковими. У результаті маємо:

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

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

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

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

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

Із (7) знайдемо одноразовий ключ K_1, оскільки R_1 та R_2 відомі і містяться у підписі:

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

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

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

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

Далі розглянемо інший підхід до реалізації атаки на зв'язаних ключах на алгоритм ЕП IBS-1. Нехай криптоаналітик перехопив та має повний доступ до i підписаних повідомлень аналогічно до (1) [3, 5].

Знайдемо невідому точку ЕК – особистий довгостроковий ключ X, який для усіх підписів є постійним. Вихідні дані аналогічні даним, що наведені для першого випадку реалізації атаки на зв'язаних ключах.

У результаті отримаємо для IBS-1 систему вигляду:

$$\begin{cases} S_1 = [K_1 - R_1]X \bmod q \\ S_2 = [-K_1 - R_2]X \bmod q \end{cases}$$
$$S_1 + S_2 = [(K_1 - R_1) + (-K_1 - R_2)]X \bmod q$$
$$S_1 + S_2 = [-R_1 - R_2]X \bmod q \qquad , \qquad (10)$$
$$X = (S_1 + S_2)[-R_1 - R_2]^{-1} \bmod q$$
$$X = -[R_1 + R_2]^{-1}(S_1 + S_2) \bmod q$$

де $[R_1 + R_2]^{-1}$ – обернений елемент у полі до $R_1 + R_2$.

3. ПРОГРАМНА МОДЕЛЬ РЕАЛІЗАЦІЇ АТАКИ НА ЗВ'ЯЗАНИХ КЛЮЧАХ НА МЕХАНІЗМ ЕП IBS-1

Розглянемо програмну модель реалізації атаки на зв'язаних ключах. Програмне моделювання виконувалось мовою програмування С із використанням бібліотеки зі спарюванням точок ЕК РВС [2]. Нижче наведемо фрагмент лістингу програми та результати виконання програми (рис. 1 – 4).

```
      printf("Протокол электронной подписи IBS-1
(Hess)\n");
      printf("ГЕНЕРАЦИЯ КЛЮЧЕЙ\n");
      element_random(P);    //P базова точка
      element_random(U);   //U особистий майстер
ключ
      element_from_hash(Y, "ID", 2);  //Y від-
критий ключ користувача Y=H1(ID)
      element_mul_zn(V, P, U);       //V вироб-
лення відкритого майстер ключа
      element_mul_zn(X, Y, U);      //X вироб-
лення особистого ключа користувача
      element_printf("Y = %B\n", Y);
      element_printf("P = %B\n", P);
      element_printf("V = %B\n", V);
      element_printf("X = %B\n", X);
      printf("ПОДПИСЬ\n");
      //element_random(k);          //K особис-
тий сеансовий ключ, set()
      element_set_str(k,
"838771892695481325788669822479875374727297897 53
", 10);
      element_printf("K1 = %B\n", k);
      element_pairing(t1, X, P);   //спарювання
element_pairing(t1, X, P)
      element_pow_zn(pi, t1, k);  //П передпід-
пис
      element_to_mpz(t2, pi);     //FE2BS()
      element_from_hash(t3, "Message", 7);  //M
- елемент - ціле mod r
      element_mul_mpz(R, t3, t2);  //R відкритий
сеансовий ключ
      element_mul_zn(t4, X, R);
      element_mul_zn(t5, X, k);
      element_neg(t4, t4);
      element_add(S, t4, t5);    //S друга час-
тина підпису
      //(M || (R,S)))
      printf("Подпись сообщения \"Message\"
:\n");
      element_printf("t4 = %B\n", t4);
      element_printf("t5 = %B\n", t5);
      element_printf("S = %B\n", S);
      element_printf("R = %B\n", R);
      mpz_init(t22);
      printf("ПОДПИСЬ 2 ----------\n");
      // k2 = r - k
      element_set_str(k2,
"646873629395903488782252263323517363933246769864
", 10);
      element_printf("K2 = %B\n", k2);
      element_pairing(t12, X, P);   //спарювання
element_pairing(t1, X, P)
      element_pow_zn(pi2, t1, k2);  //П передпі-
дпис
      element_to_mpz(t22, pi2);    // FE2BS()
      element_from_hash(t32, "Message2", 8);
//M - елемент - ціле mod r
      element_mul_mpz(R2, t32, t22);  //R від-
критий сеансовий ключ
      element_mul_zn(t42, X, R2);
      element_mul_zn(t52, X, k2);
      element_neg(t42, t42);
      element_add(S2, t42, t52);  //S друга час-
тина підпису
      // (M || (R,S)))
      printf("Подпись сообщения \"Message2\"
:\n");
      element_printf("t42 = %B\n", t42);
      element_printf("t52 = %B\n", t52);
      element_printf("S2 = %B\n", S2);
      element_printf("R2 = %B\n", R2);
      element_t R1R2, PROB_X;
      element_init_Zr(R1R2, pairing);
      element_add(R1R2, R, R2);
      element_invert(R1R2, R1R2);
      element_t S12;
      element_init_G1(S12, pairing);
      element_init_G1(PROB_X, pairing);
      element_add(S12, S, S2);
      element_mul_zn(PROB_X, S12, R1R2);
      element_neg(PROB_X, PROB_X);
      element_printf("PROB_X = %B\n", PROB_X);
      if (!element_cmp(X, PROB_X)) {    // R' ?=
R
        printf("Атака удалась!\n");
      } else {
        printf("Атака НЕ удалась!!\n");
      }
```

Як видно із рис. 1 та 4, отримуємо однакові значення особистого секретного ключа підписувача X. Отже, атака на зв'язаних ключах на механізм ЕП IBS-1 є реалізованою.

Для захисту від атаки такого типу можна використовувати, наприклад, такі механізми захисту ЕП IBS-1 [3, 5]:

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 є виключення можливостей зв'язування одноразових ключів K у 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.

```
ГЕНЕРАЦИЯ КЛЮЧЕЙ
Y = [59323062540823097642308886577488854296634276089044248850036472807195521714559686301849541937723467909693405605756324233363718114050659934262237014201644276204990424692742612844133137798350889364256199506150443326167422048055159002912162089661697059026635829505986683515385077853979316744506279398301219993]
P = [27019755677533949148849618844762931765550707770537488590804558326279699587608182609344577466671246451454429170110300323046903967100841391293324923213848523803621280079629763813506130008789537622442588017648737666273910694499023921241248276774528931290751875733479746342312509300699023019591502466513013293921243]
V = [33410041135490994371582127718601547167906898553763743252398181717574032435899171008362714455119605247427135768354257236622824010801450927315300981427274042540139100324430192798965226764816271267295020974582596605402795233577244598215697132142232180614415261091892650257641785623116236840709446738740161446625]
X = [41907138912510318233756922202948971861284711851267134026009722873927349177713136198122256565350431893067492746582369413319890351466019066464060928969012533,843881979608881217816891171633624435936439172466870194416876597709616041191089060023068649150814988266464599089663087694367231347196662518713780770002238 2]
```

Рис. 1. Генерація ключів підпису

```
ПОДПИСЬ
K1 = 838771892695481325788669822479875374727297897 53
Подпись сообщения "Message" :
t4 = [67347877286011863388207668409711979007138030523294987792862173651973228873553799189322489923477289937817172616419669758601273123400129859904565311124943122, 34959522819670825984415752610896959736588508500194177994104051951867046856141563870949670335399532658026511131312684508825818170170078806585951397684001491
t5 = [64449811951918345212021211946098316205527379590633843557430788576771095756920147588053753584754241313133439244280481797195510609131051686487276547749748844, 84369951776563247041405365087696088055358802921903637348911790838530759695220869481960336984091188287746987890620623848485873452106601720315780830138366721
S = [42706264656788790995662303961177990268121358494756787632304542874433008208456733193621590550443249365785303032258295492650538785806208973368372830775079444, 49969857226365125294851469253585833023737534754723004178208043145082164852942258372132466089867716642066820224658946299853552303858246354856732054958187771
R = 3006537972683928644994625915594117190485257450 39
```

Рис. 2. Підпис для повідомлення "Message"

```
ПОДПИСЬ 2 ----------
K2 = 64687362939590348878225226332351736393324676986 4
Подпись сообщения "Message2" :
t42 = [25482045869082784826645796116265621078362969546966848530449191597783401283243268092596840757101772906051150271095302667982157973562787832418187892445622376, 35967025223452103198406163061521922456824847444185637832971292651460071925028388699465699990723524281705497373186469892935907861124966440588909352549678104, 34371562200698781829724547598444101027100290722384447613747431541339966135813600888259148101354339264845706970751993261069036815665730929334704698438811 9]
t52 = [64449811951918345212021211946098316205527379590633843557430788576771095756920147588053753584754241313133439244280481797195510609131051686487276547749748844, 34371562200698781829724547598444101027100290722384447613747431541339966135813600888259148101354339264845706970751993261069036815665730929334704698438811 9]
S2 = [74061812041416760208377069138075687317902398556899055310386085908472843324728365246893843950000151672047835461980558390297412882593866143179914164702938844, 78836302600661495381431895767850301437793954597411074851679251638400792190341152208087637342362648075277446655555364603045742127924352803602843613669807581
R2 = 59916607918400964014382612025602329814753141970 8
```

Рис. 3. Підпис для повідомлення "Message2"

```
PROB_X = [41907138912510318233756922202948971861284711851267134026009722873927349177713136198122256565350431893067492746582369413319890351466019066464060928969012533, 84388197960888121781689117163362443593643917246687019441687659770961604119108906002306864915081498826646459908966308769436723134719666251871378077000223821
```

Рис. 4. Результат атаки на зв'язаних ключах (знаходження особистого ключа X)

ВИСНОВКИ

1. В процесі удосконалення ЕП, запропоновано алгоритм ЕП IBS-1 на ідентифікаторах зі спарюванням точок ЕК, де як особистий ключ 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. У процесі аналізу не було виявлено ефективних методів розв'язку такої системи.

2. У процесі досліджень виявлено, що криптоперетворення ЕП IBS-1 не забезпечує криптографічної стійкості проти атак на зв'язаних ключах. При чому було отримано дві різні математичні моделі здійснення атаки на зв'язаних ключах – системи (8–9) та (10). Вказані атаки мають поліноміальну складність.

3. Реалізовано програмну модель здійснення атаки на зв'язаних ключах на механізм ЕП IBS-1. Дана

програмна модель базується на математичній моделі атаки, що описується системою (10).

4. Таким чином, як математично, так і програмно показано, що алгоритм ЕП IBS-1 є нестійким проти атаки на зв'язаних ключах, тому в ході його застосування потрібно використовувати механізми захисту від таких атак. Механізми захисту також запропоновані – основними з них є шифрування підписаних повідомлень та застосування кваліфікованих апаратно-програмних засобів ЕП.

Література

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

[2] PBC Library: The Pairing-Based Cryptography Library [E-resource]. – Access mode: https://crypto.stanford.edu/pbc/manual/.

[3] *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування: монографія. Харків: «Форт», 2012. – 870 с.

[4] *Горбенко Ю.І.* Електронні підписи на основі ідентифікаторів та бінарного відображення / Ю.І. Горбенко, Р.С. Ганзя, О.С. Акользіна // Прикладная радиоэлектроника. – Х. : Харьковский национальный университет радиоэлектроники, 2015. – Т. 14, № 4 – С.284–290.

[5] *Горбенко Ю.І.* Сутність та умови здійснення атаки на зв'язаних ключах відносно електронних підписів IBS-1 та IBS-2 ДСТУ ISO/IEC 14888-3 / Ю.І. Горбенко, М.В. Єсіна, В.А. Кулібаба // Системи обробки інформації. – Х. : Харківський університет Повітряних Сил, 2016. – № 7(144) – С.113–118.

[6] 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.

Єсіна Марина Віталіївна, аспірантка факультету комп'ютерних наук, кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: електронний підпис, атаки на електронний підпис, криптографічний захист інформації.

Кулібаба Владислав Андрійович, магістр факультету комп'ютерних наук, кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: криптографічний захист інформації, математичні та програмні моделі реалізації атак на електронні підписи.

УДК 004.056.55

Математическая и программная модели реализации атаки на связанных ключах относительно механизма электронной подписи IBS-1 / М.В. Есина, В.А. Кулибаба // Прикладная радиоэлектроника: науч.-техн. журнал. – 2016. – Том 15, № 3 . – С. 157 – 161.

В работе рассматривается состояние защищенности электронных подписей на основе спаривания точек эллиптической кривой от атаки на связанных ключах. Определяются условия и возможности организации и реализации этого вида атак. Строятся математическая и программная модели реализации атаки на связанных ключах относительно механизма электронной подписи IBS-1. Предоставляются рекомендации относительно защиты от указанных уязвимостей, в том числе в пост квантовый период.

Ключевые слова: атака, электронная подпись, связанные ключи, спаривание точек эллиптической кривой.

Ил.: 04. Табл.: 01. Библиогр.: 06 назв.

UDC 004.056.55

Mathematical and program models of related keys attack implementation on electronic signature IBS-1 mechanism / M.V. Yesina, V.A. Kulibaba // Applied Radio Electronics: Sci. Journ. – 2016. – Vol. 15, № 3. – P. 157 – 161.

The paper deals with the security of electronic signatures based on an elliptic curve points pairing from a related keys attack. The conditions and possibilities of this attack type organization and implementation are defined. Mathematical and program models of related key attack implementation on the electronic signature IBS-1 mechanism are constructed. Recommendations on protection from these vulnerabilities, including those in the post quantum period are provided.

Keywords: attack, electronic signature, related keys, elliptic curve points pairing.

Fig.: 04. Tab.: 01. Ref.: 06 items.