УДК 681.3. 06

ПОПЕРЕДНІ РЕЗУЛЬТАТИ АНАЛІЗУ РОБОЧОГО ПРОЕКТУ ФЕДЕРАЛЬНОГО СТАНДАРТУ ЕЦП США FIPS-186-3

І. Д. ГОРБЕНКО, А.О. БОЙКО

В статті розглянуті і проаналізовані зміни в робочому проекті федерального стандарта США FIPS-186-3 у порівнянні з нині діючою версією. Окреслені перспективи використання кожного з описаних в стандарті алгоритмів.

The paper considers and analyzed changes in the contract design of the US Federal EDS standard FIPS-186-3 compared to the version used at present. Perspectives of using each of the algorithms described in the standard are defined.

З березня 2006 р. в Сполучених Штатах розглядається робочий проект третьої версії стандарта FIPS-186-3, який регламентує три алгоритма електронних цифрових підписів: RSA, DSA та ECDSA.

Основною метою дослідження цього стандарта є визначити напрямки розвитку систем PKI в США. Для цього необхідно: по-перше, порівняти нині діючу версію стандарта FIPS-186-2 та робочий проект, що пропонується до розгляду; по-друге, порівняти алгоритми ЕЦП в проекті стандарту з метою визначити перспективи використання і запас міцності кожного з них.

У порівнянні з попередньою діючою версією стандарта FIPS-186-2 внесено багато змін з метою збільшення криптографічної стійкості всіх трьох алгоритмів.

Внесені зміни стосуються в основному алгоритмів RSA та DSA. Щодо ECDSA то в другій версії федерального стандарта цей алгоритм не описувався, а лише робилося посилання на стандарт ANSI X9.62. Еліптичні криві та інші загальні параметри для алгоритма ECDSA, рекомендовані до використання в державних установах Сполучених Штатів наведені в додатку FIPS-186-2 в повному обсязі без змін включені в робочий проект FIPS-186-3. На відміну від FIPS-186-2, в робочому проекті FIPS-186-3 наведено повний опис алгоритма електронного цифрового підпису ECDSA, алгоритми генерації та верифікації загальних параметрів ЕЦП. Тобто, алгоритм ECDSA в нинішньому вигляді більш-менш влаштовує розробників.

Разом з тим редакція алгоритма ECDSA, викладена в проекті FIPS-186-3 має всі ті ж вразливості, які існували в FIPS-186-2.

Найбільш відомі з них дві: вразливість до селективної підробки на зв'язаних ключах та до створення так званого подвійного підпису – вибору зловмисником таких загальних параметрів, відкритого і секретного ключів підпису, що коректний підпис (r,s), сформований на одному наборі загальних параметрів, буде успішно перевірятися і на наборі загальних параметрів і відкритому ключі зловмисника. Якщо для перекриття першої вразливості необхідно видозмінити алгоритм ЕЦП, що є неприйнятним через несумісність з попередньою версією, то перекрити іншу вразливість досить легко. Розглянемо її сутність. Атака подвійного підпису описана Генезисом [1] В цьому випадку зловмисник має можливість сформувати загальні параметри і відкритий ключ так, що коректно проходила перевірка ЕЦП, сформованого користувачем на власному секретному ключі. Для цього зловмисник отримує з відкритих джерел загальні параметри користувача А $D_A = (q,a,b,G,n,h)$, його відкритий ключ Q_A та підписане повідомлення $\{M(r,s)\}$. Зловмисник обирає свій секретний ключ c, з інтервалу $1 \le c \le n-1$ обчислює:

$$t = s^{-1}(h + rc) \bmod n, \qquad (1)$$

де $h = Hash(M)$ і перевіряє виконання умови (10)

$$t \neq 0 \bmod n. \qquad (2)$$

Якщо умова (10) виконується, то наступним кроком зловмисник обчислює точку на еліптичній кривій:

$$X = s^{-1}(hG + rQ). \qquad (3)$$

Після чого обчислює свою базову точку

$$\bar{G} = (t^{-1} \bmod n)X \qquad (4)$$

і свій відкритий ключ

$$\bar{Q} = c\bar{G}. \qquad (5)$$

Легко перевірити, що підпис повідомлення $\{M(r,s)\}$ буде коректно перевірятися на вироблених відкритому ключі і загальних параметрах зловмисника. Таким чином, зловмисник отримує можливість стверджувати, що авторство повідомлення $\{M(r,s)\}$ належить йому. Очевидно, що зловмисник міг би просто підписати повідомлення M своїм випадково згенерованим секретним ключем, але в цьому випадку мітка часу, якщо вона є в повідомленні, була б порушена. У випадку здіснення атаки подвійного підпису ні повідомлення, ні мітка часу, на сам підпис (r,s) не змінюються, тобто залишаються дійсними. В цій суперечці також неможливо однозначно довести факт шахрайства.

Причина появи вище описаної вразливості в недосконалому механізмі генерування загальних параметрів для ЕЦП. Еліптична крива генерується дійсно випадково, і випадковість її формування може бути перевірена. Але ні діючий FIPS-186-2, ні робочий проект FIPS-186-3 не встановлюють алгоритма доказово випадкової генерації базової точки. А алгоритм доказово випадкової генерації базової точки насправді нескладний.

Вхід:
a,b – параметри еліптичної кривої;
N – порядок кривої;
n – порядок базової точки.
Вихід:
$seedG$ – випадкова послідовність, з якої вироблена базова точка;
G – базова точка.
Алгоритм:
1. Виробити випадкову послідовність $seedG$.
2. Обчислити $r = Hash(seedG)$.
3. Перетворити r на елемент поля, над яким визначена крива, результат занести в змінну x.
4. Підставити x в рівняння еліптичної кривої і обчислити y.
5. Встановити точку на еліптичній кривій $G' = (x, y)$.
6. Обчислити $G = \frac{N}{n} G'$.
7. Якщо $G = O$, то повернутися на крок 1 інакше G – випадкова базова точка.

Легко перевірити, що базова точка була згенерована випадково з послідовності $seedG$, але якщо зловмисник спробує нав'язати невипадкову базову точку, то йому доведеться розв'язувати обчислювально складну задачу знаходження $seedG$ із заданим геш-значенням.

Оскільки алгоритм ECDSA є версією алгоритма DSA, перероблену для використання в групі точок еліптичної кривої, то алгоритм DSA також вразливий проти атаки подвійного підпису.

Однак слід зауважити, що в FIPS-186-3 багато зроблено для забезпечення криптографічної стійкості двох інших алгоритмів ЕЦП, а саме RSA та DSA.

В діючій версії федерального стандарта США FIPS-186-2 алгоритм RSA не описано, а наявне лише посилання на стандарт ANSI X9.31. FIPS-186-2 встановлює лише мінімальну довжину модуля перетворень. Відповідно до FIPS-186-2 довжина модуля перетворень N повинна бути не менше 1024 біт. В новій версії пропонується встановити три можливих значення довжини модуля перетворень 1024, 2048 та 3072 біта. Крім того, встановлені вимоги щодо множників модуля перетворень p та q. p та q повинні бути сильними простими числами, в розкладі $p \pm 1$ та $q \pm 1$ повинні містити в канонічному розкладі дільники з довжиною не менше певної величини, різниця між p та q також обмежена мінімальним і максимальним допустимим значеннями. Встановлено і алгоритм генерації сильних простих співмножників.

Такий підхід до вибору загальних параметрів для RSA направлений на те, щоб максимально ускладнити можливість взлому алгоритма без нарощування довжини загальних параметрів. Відомо, що складність факторизації в багатьох випадках, в тому числі і при використанні найбільш ефективного на сьогоднішній день алгоритма загального решета числового поля, сильно залежить від вигляду p та q. Це і використано розробниками проекта стандарта FIPS-186-3 для запобігання неконтрольованого збільшення довжин параметрів і ключів.

Сам алгоритм електронного цифрового підпису RSA в робочому проекті федерального стандарту США не наведено, а замість нього наявне посилання на X9.31 як і в FIPS-186-2.

Відомо, що крім класичних алгоритмів факторизації, які мають щонайменше субекспоненційну складність, відомий також квантовий алгоритм факторизації Шора, який має поліноміальну складність. Однак швидше за все RSA буде виведений з дії раніше через надмірні довжини ключів. Зараз цей алгоритм залишений з вимог сумісності з існуючим програмним забезпеченням.

Не менше розробники зробили для забезпечення стійкості DSA. В DSA також встановлено три можливих значення довжини модуля перетворень 1024, 2048, 3072 біта. В залежності від довжини модуля, встановлено значення порядку генератора.

L довжина модуля p	N розмір порядку генератора
1024	160
2072	224, 256
3072	256

В діючій версії встановлені наступні допустимі значення довжин модуля і порядку групи, яку утворює генератор g: $512 < L < 1024, N = 160$. Таким чином, у порівнянні з діючою версією, робочий проект стандарту США FIPS-186-3 значно підсилює стійкість алгоритму ЕЦП DSA. Як і в випадку з алгоритмом ЕЦП RSA, зроблено все, щоб досягти максимальної стійкості при помірному збільшенні довжин параметрів.

В FIPS-197 (AES) введено рівні стійкості в залежності від довжини ключа: базовий – еквівалентний стійкості AES з ключем 128 біт, середній – еквівалентний AES з ключем 192 біта та високий – еквівалентний AES з ключем 256 біт. Оцінимо стійкість всіх трьох алгоритмів на мінімальних та максимальних довжинах параметрів.

Шляхом розрахунків складності повного розкриття для кожного з алгоритмів на мінімальних та максимальних довжинах параметрів виявлено, що лише ECDSA забезпечує високий рівень стійкості. В загальному випадку асиметричні перетворення є слабким місцем в криптосистемі. Як видно, навіть на максимально допустимій довжині параметрів RSA та DSA не забезпечують навіть базовий рівень стійкості. В діючій версії наведена таблиця рекомендованих довжин ключів для AES в залежності від довжин параметрів RSA, DSA та ECDSA. В робочому проекті третьої версії така таблиця вже відсутня, що також вказує на неперспективність алгоритмів RSA та DSA.

З всього вищевикладеного можна зробити висновок, що ці алгоритми придатні для використання користувачами – фізичними особами; для побудування потужних високо захищених сис-

тем придатний лише ECDSA. Отже RSA та DSA залишені для сумісності з існуючим програмним забезпеченням і зі збільшенням обчислювальних потужностей їх використання стане неможливим через втрату стійкості і ріст довжин параметрів.

Література.

[1] S. Blake-Wilson and A. Menezes, «Unknown key-share attacks on the station-to-station (STS) protocol», Public Key Cryptography – Proceedings of PKC '99, Lecture Notes in Computer Science, 1560 (1999), 154-170.

[2] FIPS-186-2.

[3] Draft-FIPS-186-3 _March 2006.

Надійшла до редколегії 4.09.2008

Горбенко Іван Дмитрович, професор, зав. кафедрою БІТ ХНУРЕ, головний конструктор ЗАТ «ІІТ». Область наукових інтересів: проектування та розробка засобів КЗІ.

Бойко Артем Олександрович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: асиметричні перетворення, геш-функції.