УДК 004.428.4

О.А. МЕЛЬНИКОВА, канд. техн. наук, О.В. ДЖУРИК, А.О. МАСЛЄННІКОВА

ЕЛІПТИЧНІ КРИВІ ЕДВАРДСА. ПОРІВНЯННЯ КРИПТОГРАФІЧНИХ БІБЛІОТЕК

Вступ

У 2007 році Едвардс [1] виявив цікаву нормальну форму для еліптичних кривих (ЕК), яка була введена Бернштейном і Ланге [2] та нині відома як модель Едвардса. Криві Едвардса – це сімейство еліптичних кривих, яке широко використовується у криптографічних перетвореннях і є найбільш цікавим з точки зору практичних застосувань. Зручність програмування і висока швидкість виконання операцій – головні переваги кривих даного класу у порівнянні з іншими відомими формами представлення еліптичних кривих (Вейерштраса, Монтгомері і т.і.). Окремим випадком цієї моделі кривої є скручена крива Едвардса, яка дозволяє зменшити обчислювальну складність операцій подвоєння та додавання точок ЕК. Такі криві також мають інші привабливі властивості, а саме: підтримка повного закону додавання та сумісність з моделлю Монтгомері, що у свою чергу відкриває можливість для використання так званої “ступінчатої схеми Монтгомері” – швидкого алгоритму визначення кратних точок.

Симетрія точок кривих Едвардса щодо обох координатних осей тягне за собою цікаві та зручні властивості цих кривих. Для кривих Едвардса досить використовувати один параметр d замість звичайних двох параметрів a і b класичної кривої в канонічній формі.

У 2017 році було оголошено, що визначені в RFC 7748 еліптичні криві Curve25519 та Curve448 будуть додані до списку ЕК, схвалених до використання в розробках для державних проектів, які надаються документом NIST SP 800-186. Інтерес до їх використання суттєво зріс внаслідок виникнення припущення, що рекомендовані NSA у стандарті електронного цифрового підпису (ЕЦП) FIPS 186-4 константи еліптичних кривих над GF(P) можуть надавати їм переваги при веденні криптоаналізу. Curve25519 та Curve448 є позначеннями для кривих Монтгомері, яким відповідають еквівалентні скручена крива Едвардса Ed25519 та крива Едвардса Ed448.

Крива Едвардса Ed25519 знайшла своє практичне застосування в ряді протоколів, бібліотек і програмних продуктів. Зокрема, вона використовується для автентифікації та обміну ключами в таких системах, як OpenSSH, I2p, Tor, Tox. Ця крива запропонована IETF для використання в алгоритмі TLS.

Криптографічна бібліотека Libsodium

Еліптична крива Бернштейна та підтримка її математичного апарату реалізовані в Libsodium [3] – криптографічній бібліотеці, що призначена для створення програмного інструментарію зашифрування / розшифрування контенту, ґешування паролів, формування та перевірки електронних цифрових підписів інформації.

Проект Libsodium анонсувала компанія OpenDNS у вигляді аналога створеної раніше криптографічної бібліотеки NaCl (Networking and Cryptography library), архітектура якої так само побудована на еліптичній кривій Ed25519. NaCl не отримала широкого поширення в зв'язку з проблемами перенесення на інші платформи.

Libsodium представлена як універсальна бібліотека, що забезпечує сумісність з NaCl на рівні API та підтримку ряду платформ. Бібліотека включається в пакети для багатьох операційних систем, її функції доступні користувачам через API. Серед платформ, які підтримують Libsodium, найбільш відомі: Bitrig, OpenBSD, Dragonfly BSD, NetBSD, FreeBSD, SmartOS, OSX, Linux, Windows, iOS і Android.

Libsodium надає спрощений API з набором безпечних криптографічних опцій і методів. За рахунок цього використання Libsodium вимагає менше спеціальних знань, у порівнянні з аналогами. Так, наприклад, OpenSSL має надлишкову функціональність, зокрема містить

безліч криптографічних примітивів і режимів, що ускладнює вибір користувачем безпечного набору. Наявність великої кількості параметрів команд призводить до складностей при роботі, а також до періодичного виявлення вразливостей.

Libsodium вирішує проблему оптимального вибору, надаючи користувачеві готовий до використання компактний і простий набір функцій, що містить тільки безпечні методи. Libsodium підтримується різними компіляторами й операційними системами, включаючи Windows (з MinGW або Visual Studio, x86 і x86-64), iOS і Android.

Функції Libsodium, які надаються за допомогою API:

1) зашифрування з використанням автентифікації з відкритими (public-key) і загальними (shared-key) ключами, які забезпечують надійність передачі зашифрованого повідомлення і гарантують його цілісність;

2) створення та перевірка електронних цифрових підписів з використанням кривої Ed25519 за відкритим і особистим ключами дозволяє одержувачеві перевірити, що повідомлення надіслано саме тим, від кого його очікували отримати, і що воно не було змінено третьою особою;

3) операції ґешування, які дозволяють сформувати так званий "зліпок" від повідомлення, який має фіксовану довжину і надає можливість перевірити відповідність ґеш-значення та початкового повідомлення, але не дозволяє відновити елементи повідомлень з ґеш-значення;

4) формування ключів з коротких повідомлень для ґеш-таблиць, що дозволяють виключити проведення DoS-атак через колізії ґеш-значень;

5) безпечний генератор псевдовипадкових чисел для використання в криптографічних перетвореннях.

У бібліотеці реалізовано цифровий підпис з використанням кривої Бернштейна та алгоритму ґешування SHA-512. Команда Бернштейна оптимізувала Ed25519 для сімейства процесорів Nehalem / Westmere x86-64. Верифікація може виконуватися порціями по 64 підписи для підвищення пропускної спроможності. Ed25519 призначена для забезпечення стійкості до атак, порівняної з якістю 128-бітових симетричних шифрів. Відкритий ключ має довжину 256 біт, а підпис – 512. Серед програмного забезпечення для DNS користується популярністю ЕЦП з відкритим ключем довжиною 32 байт та підписом 64 байт, які мають таку саму стійкість, як і 256-байтовий RSA-2048 підпис.

Приблизно з квітня 2016 року в багатьох відомих месенджерах, таких як Facebook Messanger, Viber, WhatsApp, з'явилася функція секретного обміну повідомленнями. Повідомлення, які надсилаються та отримуються, доступні лише для читання на пристрої, який використовується для створення або відкриття бесіди. Це означає, наприклад, що користувач не може переглядати попередню розмову на своєму ноутбуці, якщо спочатку створив або відкрив її на своєму смартфоні. Крім того, секретні бесіди створюють ефемерний характер процесу секретного обміну повідомленнями, надаючи користувачу можливість контролювати, як довго одержувач може бачити повідомлення. Описаний функціонал було реалізовано за допомогою end-to-end шифрування, яке використовує відкриті реалізації протоколу Signal.

.Net Core бібліотека NSec

На базі Libsodium була розроблена криптографічна бібліотека для .Net Core – NSec [4], що також реалізує алгоритм електронного цифрового підпису Ed25519 та інші сучасні криптографічні примітиви, такі як X25519 (протокол обміну ключами Діфі-Гелмена, який базується на еліптичній кривій) та ChaCha20-Poly1305 (симетричний шифр та формування коду автентифікації повідомлень). Перевагами цієї бібліотеки є легкість у використанні, швидке виконання операцій та потокобезпечність. Також слід зазначити, що NSec є бібліотекою з відкритим програмним кодом. Крім послуг безпеки, що надаються самими криптографічними примітивами, NSec намагається зробити навіть саме використання цих примітивів максимально безпечним за замовчуванням. Це стосується, наприклад, особливостей організації зберігання та вилучення конфіденційних даних, таких як ключі.

Crypto++

Серед існуючих бібліотек слід відмітити також бібліотеку Crypto++ [5], реалізації якої надають захист від атак зі сторонніх каналів. Це атаки, засновані на припущенні, що деяка інформація зі сторонніх каналів (наприклад, час обчислень) залежить від команд, що виконуються, або від вхідних даних. Для забезпечення такого захисту використовуються, за можливістю, апаратні інструкції. Також, для мінімізації витоків у бібліотеці використовуються алгоритми та шаблони доступу до кеш-пам'яті.

Бібліотека підтримує цифровий підпис з використанням кривої Едвардса з наступними параметрами: розмірність поля – 2^{255}- 19, параметр кривої d – 121665 / 121666, SHA-512 в якості функції ґешування, базова точка $B(x, y)$, де x – парне число, порядок кривої – просте 253-бітове число.

Серед недоліків можна відмітити невелику популярність у використанні бібліотеки програмним забезпеченням: лише i2pd (некомерційна реалізація i2p клієнта).

Bouncy Castle

Bouncy Castle – це програмна бібліотека [6], у якій представлена велика кількість криптографічних примітивів. Існують реалізації Bouncy Castle мовами програмування Java та C#. Бібліотека підтримує як стандартні високорівневі криптографічні API відповідних платформ, так і низькорівневі API для більш гнучкого й ефективного доступу до функціоналу. Відповідно до RFC 8032 у Bouncy Castle було введено низькорівневі реалізації кривих Ed25519 та Ed448.

Існує також версія Bouncy Castle, яка була розроблена для операційної системи Android. Ця бібліотека одержала назву Spongy Castle. На жаль, платформа Android супроводжується скороченою версією Bouncy Castle.

Крім того, слід зазначити, що у листопаді 2016 року вийшли перші релізи Bouncy Castle, сертифіковані FIPS. На відміну від попередніх розробок, у сертифікованих версіях бібліотеки контролюється виконання вимог FIPS щодо алгоритмів, які підтримують низькорівневі API.

OpenSSL

OpenSSL – відкритий програмний продукт, розроблений як універсальна бібліотека для криптографії, що використовує протоколи Secure Sockets Layer і Transport Layer Security. Використовується, зокрема, в бібліотеці cUrl для реалізації роботи за протоколом https. Доступна для більшості UNIX-подібних операційних систем (включаючи Solaris / OpenSolaris, Linux, Mac OS X, QNX4, QNX6 і чотирьох операційних систем BSD з відкритим програмним кодом), а також для OpenVMS і Microsoft Windows. Існують реалізації мовами програмування C, assembly, Perl. OpenSSL заснований на SSLeay, розробка якого була неофіційно призупинена в 1998 році.

OpenSSL не було сертифіковано, але для забезпечення багатьох його можливостей був створений криптографічний модуль OpenSSL FIPS Object Module, який отримав сертифікат відповідності стандарту безпеки FIPS 140-2, що визначає вимоги до криптографічних модулів, необхідні для їх використання в державних установах США. Сертифікат виданий Американським інститутом стандартів і технологій (NIST) після проведення відповідного аудиту коду проекту. Причому сертифікат було видано на програмний код продукту, а не конкретну бінарну збірку, що розширює область використання OpenSSL в державних проектах.

Серед несиметричних криптографічних алгоритмів OpenSSL підтримує також X25519 та X448 (протокол узгодження ключів Діфі-Гелмена, заснований на використанні ЕК Curve25519 та Curve448, або еквівалентних Ed25519 та Ed448 із оцінками рівнів безпеки у 128 та 224 біт, відповідно), ЕЦП PureEdDSA та EdDSA згідно RFC8032 (використовує Curve448 у формі кривої Едвардса Ed448 та Curve25519 у формі скрученої кривої Едвардса Ed25519 із ґешуванням SHA-512).

Порівняння криптографічних бібліотек за сумісністю з операційними системами та за станом реалізації перетворень на кривих Едвардса

Табл. 1 і 2 відображають основні криптографічні бібліотеки, їх сумісність з різноманітними ОС та стан реалізації цифрового підпису на кривій Едвардса, окремих базових операцій над точками ЕК Едвардса та базових операцій над точками ЕК інших типів (Вейерштраса, Монтгомері).

Таблиця 1

Бібліотека	ЕК Едвардса	Інші типи ЕК	ЕЦП EdDSA
Botan	+	+	+
CryptoComply	+	+	+
Libgcrypt	+	+	+
Libsodium	+	+	+
Nsec	+	+	+
OpenSSL	+	+	+
wolfCrypt	+	+	+
Bouncy Castle	+	+	+
Crypto++	+	+	+
ACE	-	+	-
Nettle	-	+	-

Таблиця 2

Бібліотека	ОС	Потоко-безпечність
cryptlib	AMX, ARINC 653, BeOS, ChorusOS, CMSIS-RTOS/mbed-rtos, DOS, DOS32, eCOS, embOS, FreeRTOS/OpenRTOS, uItron, MQX, MVS, Nucleus, OS/2, Palm OS, QNX Neutrino, RTEMS, SMX, Tandem NonStop, Telit, ThreadX, uC/OS II, Unix (AIX, FreeBSD, HP-UX, Linux, macOS, Solaris, etc.), VDK, VM/CMS, VxWorks, Win16, Win32, Win64, WinCE/PocketPC/etc, XMK	+
wolfCrypt	Win32/64, Linux, macOS, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, NonStop, TRON/ITRON/µITRON, Micrium's µC/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP-UX	+
OpenSSL	Solaris, IRIX, HP-UX, MPE/iX, Tru64, Linux, Android, BSD (OpenBSD, NetBSD, FreeBSD, DragonflyBSD), NextSTEP, QNX, UnixWare, SCO, AIX, 32 and 64-bit Windows (Visual Studio, MinGW, UWIN, CygWin), UEFI, macOS (Darwin), iOS, HURD, VxWorks, uClinux, VMS, DJGPP (DOS), Haiku	+
Libsodium	macOS, Linux, OpenBSD, NetBSD, FreeBSD, DragonflyBSD, Android, iOS, 32 and 64-bit Windows (Visual Studio, MinGW, C++ Builder), NativeClient, QNX, JavaScript, AIX, MINIX, Solaris	+
CryptoComply	Linux (RHEL, CentOS, Debian, Ubuntu, etc.), Windows, iOS, Android, FreeBSD, macOS, Solaris, Java Runtime Environment	+
Crypto++	Unix (AIX, OpenBSD, Linux, MacOS, Solaris, etc.), Win32, Win64, Android, iOS, ARM	+
ACE	Unix, Windows, and more	+
Botan	Linux, Windows, macOS, Android, iOS, FreeBSD, NetBSD, OpenBSD, DragonflyBSD, AIX, QNX, Haiku, IncludeOS	+
NSec	Windows 10, macOS, CentOS, Debian, Fedora, OpenSUSE, Ubuntu	+
Libgcrypt	All 32 and 64 bit Unix Systems (GNU/Linux, FreeBSD, NetBSD, macOS etc.), Win32, Win64, WinCE and more	+
Bouncy Castle	General Java API: J2ME, Java Runtime Environment 1.1+, Android. Java FIPS API: Java Runtime 1.5+, Android. C# API (General & FIPS): CLR 4.	-

Порівняння обчислюваних характеристик криптографічних бібліотек

Було проведено експериментальні дослідження з метою порівняння швидкодії розглянутих бібліотек, а саме Libsodium v4.0 та NSec v 18.6, скомпільованих з використанням мови програмування C# та компілятора Roslyn. Експеримент проводився із

використанням програмного забезпечення Microsoft Visual Studio 2017 Community з проектним рішенням, яке застосовує бібліотеки, збудовані для 64-розрядних процесорів. Вимірювався час виконання операцій формування та перевірки ЕЦП із використанням перетворень на еліптичній кривій Едвардса Ed25519 при застосуванні ґеш-функції SHA-512 для текстів довжини 10000 символів (бібліотеки підтримують двобайтове кодування символів). Оскільки інтерфейс функцій цих бібліотек не дозволяє виклик ґешування окремо від функцій формування / перевірки підпису, для виключення з результатів аналізу часу виконання ґеш-функції такі самі експерименти було проведено для мінімальної довжини тексту (1 символ). Результати вимірювань та їх порівняльні оцінки відображені у табл. 3. Таким чином, із розглянутих варіантів бібліотек NSec має кращі оцінки за рядом показників. Експерименти проводилися на комп'ютері з такими характеристиками: процесор – Intel® Core™ I 5-3210M (x64) CPU @ 2.50 GHz, ОЗП – 6,00Гб, HDD – 1000 Гб, ОС – MS Windows 10.

Таблиця 3

Розмір тексту, символів		10 000		1		(1)/(2)	(3)/(4)
Напрям перетворення		формування ЕЦП, такти / нс	перевірка ЕЦП, такти / нс	формування ЕЦП, такти / нс	перевірка ЕЦП, такти / нс		
		1	2	3	4		
I	NSec	1794 / 717,6	2175 / 870,0	652 / 260,8	1572 / 628,8	0,83	0,42
II	Libsodium	1810 / 724,0	2085 / 834,0	858 / 343,2	1576 / 630,4	0,87	0,54
(II) / (I)		1,01	0,96	1,32	1,00		

Висновки

Криві Едвардса набули великої популярності у криптографічному суспільстві та серед програмістів. Бібліотеки з використанням криптографії на ЕК Едвардса можна знайти на багатьох відомих мовах програмування, а спектр їх застосування доволі великий: криптовалюти (Nano, Monero), підписуюче програмне забезпечення (signify, asignify), DNS Пз (dnscrypt-proxy, DNSCryptClient), SSH Пз (OpenSSH, PuTTY), ОС (OpenBSD, OpenWrt), мережі (Tor, I2P), протоколи (TLS 1.3, Signal Protocol, SSH). Еліптичні криві Едвардса та алгоритми з їх використання реалізовані у таких бібліотеках, як Libsodium, OpenSSL, NSec, Botan, CryptoComply, Libgcrypt, wolfCrypt, Bouncy Castle, Crypto++. Найбільшого поширення набула бібліотека Libsodium, що має також .Net Core аналог – NSec, перевагами якого є легкість у використанні та швидке виконання операцій. При цьому Crypto++ пропонує більш розширені можливості: не тільки застосування електронного цифрового підпису, але й використання базових операцій на кривій, таких як подвоєння та складання точок, що може бути корисним при проведенні власних досліджень, удосконалень та додаткових розробок.

Список літератури:

1. *Edwards H.M.* A normal form for elliptic curves // Bulletin of the American Mathematical Society. 2007. P. 393 – 422.

2. *D.J. Bernstein, T. Lange*. Faster addition and doubling on elliptic curves // In K. Kurosawa, editor, ASIACRYPT, volume 4833 of LNCS. 2007. P. 29-50.

3. Libsodium for .NET – A secure cryptographic library: [Електронний ресурс]. Режим доступу: https://github.com/adamcaudill/libsodium-net.

4. A modern and easy-to-use cryptographic library for .NET Core based on Libsodium: [Електронний ресурс]. Режим доступу: https://github.com/ektrah/nsec.

5. Crypto++ Library: [Електронний ресурс]. Режим доступу: https://www.cryptopp.com.

6. The Bouncy Castle Crypto APIs: [Електронний ресурс]. Режим доступу: https://www.bouncycastle.org.

7. OpenSSL. Cryptography and SSL / TLS Toolkit: [Електронний ресурс]. Режим доступу: https://www.openssl.org/.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 08.10.2018