УДК 004.75:004.05

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНДАРТИЗОВАНИХ ВЕРСІЙ КРИПТОАЛГОРИТМУ ECIES

І.Д. ГОРБЕНКО, М.І. ХАРЛАМБ

Криптографія на еліптичних кривих (КЕК) може бути використана як інструмент для шифрування даних, створення цифрових підписів або в ході виконання обміну ключовими даними. Інтегрований механізм шифрування (ECIES) є відомою схемою, заснованою на КЕК, тому він був включений в кілька криптографічних стандартів. У даній роботі надається огляд і порівняння версій ECIES, включених у документи ANSI, IEEE,ISO / IEC, і SECG, виділяються основні відмінності між ними та можливості використання схеми для різних систем.

Ключові слова: протокол шифрування, криптографія з відкритим ключем, ECIES.

ВСТУП

З розвитком криптографії з відкритим ключем Діффі і Геллманом у 1976 році, було запропоновано декілька криптосистем. У будь-якій криптосистемі головними особливостями є ступінь захищеності та ефективність, проблема забезпечення яких завжди належить до математичної бази, на якій її засновано. На сьогодні обчислювано неможливими вважаються: задача дискретного логарифмування, задача факторизації цілих чисел та задача дискретного логарифмування на еліптичних кривих.

У 1985 році Мілер та Кобільц незалежно один від одного запропонували криптосистему, що заснована на використанні еліптичних кривих у скінченних полях, стійкість яких заснована на дискретному логарифмуванні на еліптичних кривих. У порівнянні з іншими криптосистемами (такими як RSA), криптографічні методи, засновані на еліптичних кривих, використовують ключ значно меншої довжини. Причина цього пов'язана із високою стійкістю поданих систем, що, як вважає більшість спеціалістів, пов'язана із значною складністю розв'язання математичних рівнянь, ніж це можна розглядати при дискретному логарифмуванні чи факторизації цілих чисел.

На сьогодні з усіх відомих криптоалгоритмів, заснованих на еліптичних кривих, можна виділити інтегрований механізм шифрування на еліптичних кривих[1]. У даній роботі ми надаємо детальний аналіз та порівняння існуючих версій цього механізму, використовуючи офіційні документи та стандарти [1–3] та виділяючи головні відмінності в них, що можуть бути повністю сумісними в ході використання різних версій.

Робота побудована так, що в першій частині наведені положення щодо функціонального дизайну механізму, розділ 2 порівнює його різні версії за функціональним складом, розділ 3 демонструє стандартний набір функцій у кожній версії стандарту, в четвертому розділі підбиваються підсумки роботи та робляться висновки з проведених аналізів та отриманих результатів.

[1] Elliptic Curve Integrated Encryption Scheme (ECIES)

1. ІНТЕГРОВАНИЙ МЕХАНІЗМ ШИФРУВАННЯ НА ЕЛІПТИЧНИХ КРИВИХ

У 1997 році Міхір Белар та Філіп Рогавей представили світу доповнений механізм шифрування на дискретному логарифмі[2], який згодом був довершений ними та Мікаелєм Абдалою. Тоді в перший раз алгоритм був названий доповненим механізмом шифрування Діффі-Геллмана, а пізніше, у 1998 році, інтегрованим алгоритмом шифрування Діффі-Геллмана, з метою уникання колізій у назві з доповненим алгоритмом шифрування[3].

Механізм інтегрованого шифрування є довершеною схемою шифрування Ель-Гамаля, використовуючи інтегровану криптографію еліптичних кривих, що включає операції з відкритими ключами, схеми шифрування, MAC-коди та геш-значення. Завдяки інтеграції перелічених функцій, цей механізм є стійким проти атак на шифротекст без необхідності збільшення кількості заснованих операцій чи довжини ключа.

На схемі 1 наведено модель роботи алгоритму з [9], де M – це вхідне повідомлення, g – генератор мультиплікативної групи G, gu, gv – відкриті ключі отримувача та відправника, u та v – секретні ключі отримувача та відправник, ε – симетричний алгоритм шифрування, τ – функція генерації MAC-кодів, H – геш-функція.Даний механізм був дороблений ANSI[4] та з деякими модифікаціями включений до стандарту ANSI X9.63 у 2001 році. Незалежно від цього IEEE у 2000 році затвердила стандарт IEEE 1363. Коли у 2004 році ANSI X9.63 було надано широкому розголосу, IEEE розглянув обидві версії та запропонував новий стандарт 1363a. Всі ці версії об'єднались під однією назваою ECIES (Elliptic Curve Integrated Encryption Scheme), але їх не можна назвати ідентичними.

Протягом останніх років ще одна група вчених з ISO/IEC об'єдналася для прийняття стан-

[2] Discrete Logarithm Augmented Encryption Scheme (DLAES)

[3] Advanced Encryption Standard (AES)

[4] ANSI – American National Standards Institute

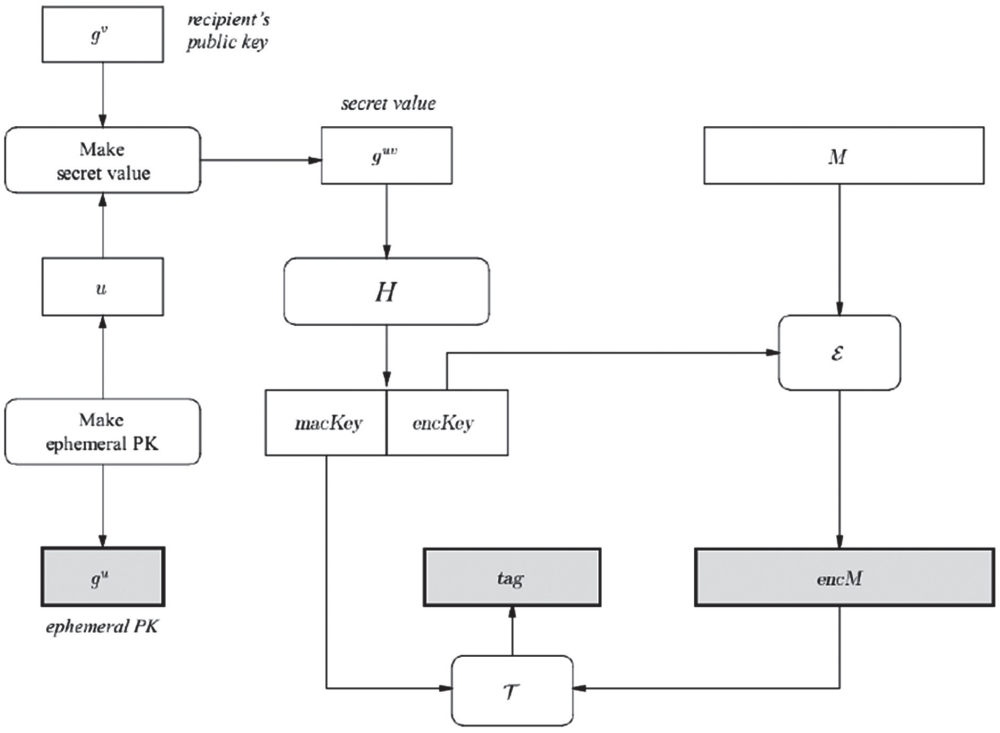

Схема 1. DHIES функціональна схема

дарту сімейства 18033. За основу вони взяли усі існуючі на той момент версії ECIES та базові дослідження стійкості алгоритму. В результаті з'явилася ще одна версія стандарту, що була додана до ISO/IEC 18033-2 у 2006 році .

Таким чином, головним документом стандарту прийнято вважати опис алгоритму ECIES, що був прийнятий на консорціумі групи із стандартизації криптографічних продуктів у 2000 році, та дороблений у 2009 році.

2. БАЗОВІ КОНЦЕПЦІЇ МЕХАНІЗМУ

Як визначає назва алгоритму, ECIES інтегрує схему шифрування, використовуючи такі функції:

- Функція генерації ключів (ФГК). Використовується для вироблення спільного секретного ключа між двома абонентами.
- Функція вироблення ключів (ФВК). Механізм застосовується для вироблення ключів з вихідного матеріалу та параметрів.
- Геш-функція (ГФ). Функція, що дозволяє генерувати геш-значення для будь-якого повідомлення.
- Алгоритм шифрування (АШ). Симетричний алгоритм шифруваня.
- Код автентифікації повідомлення (КАП). Необхідний для того, щоб ідентифікувати повідомлення.

Після порівняння версій схеми шифрування ANSI, IEEE, ISO/IEC та SECG можна виділити дві групи різновидів:

- Функціональні: деталі реалізації, опції, подання у двійковому вигляді тощо.
- Вибір між існуючими алгоритмами: алгоритми шифрування, геш-функції тощо [1].

3. ПОРІВНЯННЯ ФУНКЦІОНАЛЬНОСТІ ВЕРСІЙ

У цьому розділі ми проаналізуємо версії механізму попарно та знайдемо відмінності між існуючими версіями.

DHIES та ANSI X9.63

- Наведемо головні відмінності між оригінальною версією механізму DHIES та його імплементацією ANSI X9.63:
- DHIES не дозволяє використання довільних параметрів у функції виготовлення ключів та у функції генерування коду повідомлення, в той час як ANSI X9.63 припускає такий варіант.
- DHIES використовує функцію шифрування для генерації коду повідомлення та для формування геш-значення. ANSI X9.63 використовує конструкцію, де дані проходять декілька раундів.
- DHIES інтерпретує ліві біти на виході як значення функції генерації ключів, а праві як MAC-код повідомлення. ANSI X9.63 виконує навпаки.
- DHIES дозволяє використовувати як алгоритми симетричного шифрування потокові або блокові шифри, крім того залишається можливість використовувати альтернативні алгоритми. X9.63 дозволяє використання тільки функції XOR.

ANSI X9.63 та IEEE 1363a

У цьому розділі порівнюємо стандарти ANSI X9.63 та IEEE 1363a

- ANSI X9.63 дозволяє як функція вироблення спільного секрету лише схема Діффі-Геллмана, IEEE 1363a підтримує її використання, але і дозволяє застосовувати альтернативний варіант.

• ANSI X9.63 дозволяє використовувати довільні параметри для функції вироблення ключів, але не вимагає чітких вимог до цих параметрів. IEEE 1363a використовує двійкове уявлення відкритого ключа відправника як вхідний параметр.

• ANSI X9.63 використовує першу координату, генеровану функцією вироблення спільного секрету, коли IEEE 1363a використовує елемент у цілому.

• ANSI X9.63 завжди перетворює ліву частину бітів функції вироблення ключів як ключ шифрування та праву частину, як код автентифікації повідомлення. IEEE 1363a інтерпретує вихідний потік як *kMAC||kENC*, коли використовується поточний шифр та навпаки, коли використовується блоковий [2–4].

IEEE 1363a та ISO/IEC 18033-2

У цьому розділі порівнюємо стандарти *ISO/IEC 18033-2* та IEEE 1363a

• IEEE 1363a дозволяє використовувати довільні параметри у функції генерації ключів, але *ISO/IEC 18033-2* не дозволяє це робити.

• IEEE 1363a дозволяє обробляти повідомлення як в бітовому, так і в байтовому уявленні. ISO/IEC 18033-2 підтримує роботу тільки з байтовими рядками.

• IEEE 1363a вимагає завжди використовувати однаковий набір параметрів для даного відкритого ключа. ISO/IEC 18033-2 дозволяє змінювати параметри і функції залежно від ключа.

• IEEE 1363a вимагає мінімальну довжину ключа 160 біт. ISO/IEC 18033-2 не вимагає мінімальної довжини ключа.

Ці відмінності прибрали з останніх версій стандартів для того, щоб забезпечити вищий рівень сумісності між схемами [1–2].

ISO/IEC 18033-2 та SECG SEC 1

У цьому розділі порівнюємо стандарти ISO/IEC 18033-2 та SECG SEC 1.

• ISO/IEC 18033-2 не вимагає вхідних параметрів до функції вироблення ключів, в той час як SEC 1 потребує цю інформацію.

• SEC 1 не вимагає включення відкритого ключа відправника до функції виготовлення ключів. Тут відкритий ключ розглядається як вхідний параметр.

• ISO/IEC 18033-2 не потребує мінімальної довжини ключа.

4. ФУНКЦІОНАЛЬНІ СКЛАДОВІ МЕХАНІЗМУ

В цій частині розглянемо функції та додатки, що використовуються в механізмі для створення проміжних параметрів та формування шифротексту: функція генерування ключів, функція вироблення MAC-коду повідомлення, алгоритм шифрування, геш-функція. Основні положення наведені у вигляді табл. 1.

Пояснення до табл.1 :

• DH – механізм обміну спільним секретом Діффі-Геллмана.

• X9.63-KDF – описано в [10], KDF1 та KDF2 розглядаються в [13], функція NIST-800-56 KDF конкатенації з [18].

• SHA-1, SHA-2(256, 384, 512), RIPEMD, WHIRPOOL – геш-алгоритми формування значень.

• TDES – Triple DES алгоритм, що виконує шифрування. Разом з ним використовується стандарт AES – (28, 192, 256),MISTY1, CAST-128.

• DEA, HMAC-SHA (..), CMAC-AES– функції для формування MAC-коду повідомлення.

ВИСНОВКИ

Після детального аналізу відмінностей між версіями механізму ECIES стає явним той факт, що в одному програмному компоненті неможливо поєднати використання усіх стандартів.

Крім того, реалізації можуть зіткнутися з ще однією важливою проблемою, яку можна сформулювати як обмеження у функціях, доступних для розробника інтерфейсу програмування ці-

Таблиця 1

Функції та алгоритми стандартів сімейства ECIES

	X9.63	1363a	18033-2	SEC 1
KA	DH	DH DHC	DH DHC	DH DHC
KDF	X9.63-KDF	X9.63-KDF	KDF1 KDF2	X9.63-KDF NIST-800-56
HASH	SHA-1	SHA-1 SHA-2 RIPEMD	SHA-1 SHA-2 RIPEMD WHIRLPOOL	SHA-1 SHA-2*
ENC	XOR	TDES AES	TDES AES MISTY1 CAST-128	XOR AES
MAC	DEA ANSI X9.71	MAC1	H-SHA-1 H-SHA-2 H-RIPEMD	H-SHA-1 H-SHA-2* CMAC-AES

льового продукту. Прямим наслідком є те, що під час застосовування ECIES, першим кроком має бути оцінка можливостей кінцевої платформи використання та аналіз призначення з тієї точки зору, щоб вирішити яка версія ECIES є адекватною для конкретного використання.

Нові версії (наприклад, ISO / IEC 18033-2 iSEC 1) не можуть бути повністю сумісні з успадкованими пристроями, але вони забезпечують доступ до новіших стійких функцій(наприклад, SHA-2, AES і т.д.), тому вони повинні рекомендовано використовувати одну з цих версій.

Література

[1] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. Inform. Theory, vol. 22, pp. 644–654, 1976.

[2] Електронний ресурс: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdfhttps://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[3] T. Mather, S. Kumaraswamy, S. Latif, Cloud Security and Privacy:An Enterprise Perspectiveon Risks and Compiliance, O`ReillyMedia,2009. – 334 c.

[4] Електронний ресурс: http://www.cryptopp.com/wiki/Elliptic_Curve_Integrated_Encryption_Scheme

[5] BSI TR 03111, Elliptic Curve Cryptography, Bundesamt f¨ur Sicherheit in der Informationstechnik, 2009, http://www.bsi. de/literat/tr/tr03111/BSI-TR-03111.pdf.

[6] J. H. Silverman, The Arithmetic of Elliptic Curves, ser. Graduate texts in Mathematics. New York, NY, USA: Springer-Verlag, 1986, vol. 106.

[7] M. Bellare and P. Rogaway, “Minimizing the use of random oracles in authenticated encryption schemes,” Lecture Notes in Comput. Sci., vol. 1334, pp. 1–16, 1997.

[8] M. Abdalla, M. Bellare, and P. Rogaway, DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem, contribution to IEEE P1363a, 1998, http://grouper.ieee.org/groups/1363/P1363a/contributions/dhaes.pdf.

Надійшла до редколегії 21.06.2014

Харламб Марія Ігорівна, студентка 5-го курсу кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: програмування, криптографічні методи захисту інформації, хмарні технології.

УДК 004.75:004:0.5

Сравнительный анализ стандартизированных версий криптоалгоритма ECIES / И.Д. Горбенко, М.И. Харламб // Прикладная радиоэлектроника: науч.-техн. журнал. — 2014. — Том 13. — № 1. — С. 333–336.

Криптография на эллиптических кривых (КЭК) может быть использована как инструмент для шифрования данных, создания цифровых подписей или при выполнении обмена ключевыми данными. Интегрированный механизм шифрования (ECIES) является известной схемой, основанной на КЭК, поэтому он был включен в несколько криптографических стандартов. В данной работе предоставляется обзор и сравнение версий ECIES, включенных в документы ANSI, IEEE, ISO / IEC, и SECG, выделяются основные различия между ними и возможности использования схемы для различных систем.

Ключевые слова: протокол шифрования, криптография с открытым ключом, ECIES.

Табл.: 01. Ил.: 01. Библиогр.: 08 назв.

UDC 004.75:004:0.5

Comparative analysis of standardized versions of cryptographic algorithm ECIES / I.D. Gorbenko, M.I. Kharlamb // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 1. — P. 333–336.

Elliptic Curve Cryptography (ECC) can be used as a tool for data encryption, creation of digital signatures or performing of key data exchange. Integrated encryption mechanism (ECIES) is a well-known scheme based on the ECC, so it was included in several cryptographic standards. This paper provides an overview and comparison of ECIES versions included in ANSI, IEEE, ISO / IEC, and SECG documents, and highlights the main differences between them and the possibility of using the scheme for different systems.

Keywords: encryption protocol, public key cryptography, ECIES.

Tab.: 01. Fig.: 01. Ref.: 08 items.