УДК 004.42

Д. В. Арсенюк

РОЗРОБКА ПРОГРАМНОГО МОДУЛЮ ГРУПОВОГО ЦИФРОВОГО ПІДПИСУВАННЯ НА ЕЛІПТИЧНИХ КРИВИХ У СИСТЕМАХ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

У даній роботі проводиться аналіз алгоритмів цифрового підпису. Описується груповий цифровий підпис, який базується на задачі факторизації великого числа. Показано переваги алгоритмів на еліптичних кривих..

Ключові слова: цифровий підпис, криптографія, груповий цифровий підпис, еліптичні криві.

Abstract

An analysis of algorithms of digital signature is performed in this work. A group digital signature, which is based on the problem of factorization of large numbers is described. The advantages of algorithms on elliptic curves are shown.

Keywords: digital signature, cryptography, group digital signature, elliptic curves.

Розвиток глобальних комунікацій в діловому і повсякденному житті привів до появи нової області взаємовідносин, предметом яких є електронний обмін даними. У такому обміні даними можуть брати участь органи державної влади, комерційні і некомерційні організації, а також громадяни в своїх офіційних і особистих стосунках[1].

Проблема збереження електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення специфічних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є електронний цифровий підпис, який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою[2].

Електронний цифровий підпис (ЕЦП) - реквізит електронного документа, отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа підпису, що дозволяє перевірити відсутність спотворення інформації в електронному документі з моменту формування підпису (цілісність), приналежність підпису власникові сертифіката ключа підпису(авторство), а в разі успішної перевірки підтвердити факт підписання електронного документа (неспростовності)[3].

Однією із реалізацій цифрового підпису є груповий підпис. Поняття колективного підпису співзвучно з поняттям групового підпису, однак ці поняття різні і використовуються для побудови криптографічних протоколів, які вирішують різні завдання. У протоколі групового підпису вирішується завдання забезпечення можливості будь-якому користувачеві з деякої групи сформувати підпис від імені всієї групи, в якій є суб'єкти, наділені повноваженнями виявлення конкретних осіб, які сформували підпис, тоді як інші суб'єкти не можуть цього зробити. Колективний підпис надає рішення задачі одночасного підписання контракту (електронного документа), так як він формується в результаті єдиного неподільного перетворення і не може бути розділений на індивідуальні або інші урізані колективні підписи; крім цього, його не можна розширити, тобто вбудувати в нього додатковий підпис ще одного або декількох користувачів[4].

Більшість продуктів і стандартів, в яких для шифрування і перевірки автентичності застосовуються методи криптографії з відкритим ключем, базуються на алгоритмі RSA. Однак довжина ключа, необхідна для успішного захисту даних при використанні алгоритму шифрування RSA за останні роки різко збільшилася, що зумовило відповідне зростання завантаження систем, що використовують RSA. [5]

Теорія еліптичних кривих над скінченними полями в даний час все більше починає застосовуватися в криптографії. Основна причина цього полягає в тому, що еліптичні криві над кінцевими полями

дають невичерпне джерело кінцевих абелевих груп, які зручні для обчислень і володіють багатою структурою[6].

Велика відмінність шифрування за допомогою еліптичних кривих в порівняні з RSA полягає в тому, що з використанням еліптичних кривих забезпечується еквівалентний рівень захисту при меншій довжині ключів, внаслідок чого зменшується навантаження на ЦП[7].

Швидкість роботи еліптичних алгоритмів набагато вища, ніж у класичних. Це пояснюється як розмірами поля, так і застосуванням ближчою для комп'ютерів структури бінарного скінченного поля.

Через маленьку довжину ключа і високу швидкості роботи, алгоритми асиметричної криптографії на еліптичних кривих можуть використовуватися в смарт-картках та інших пристроях з обмеженими обчислювальними ресурсами[8].

Тому, беручи до уваги вище сказане, рекомендується реалізовувати цифровий підпис на еліптичних кривих.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Молдовян Н. А. Теоретический минимум и алгоритмы цифровой подписи. / Н. А. Молдовян. – Санкт-Петербург: БХВ-Петербург, 2010. – 304 с.
2. Схемы цифровой подписи [Електронний ресурс] – Режим доступу до ресурсу: http://cryptowiki.net/index.php?title=Схемы_цифровой_подписи.
3. Хоффман, Л. Дж. Современные методы защиты информации / Л.Дж. Хоффман. - Москва: СПб. Питер, 2014. - 264 с.
4. Васильев И. Н. Протокол групповой цифровой подписи на основе алгоритма коллективной подписи и маскирования открытых ключей // Вопросы защиты информации / И. Н. Васильев, Д. Н. Молдовян, А. А. Молдовян., 2014. – С. 35–39.
5. Шаньгин, В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - Москва: Огни, 2016. - 551 с.
6. Жданов О. Н. Эллиптические кривые. Основы теории и криптографические приложения / О. Н. Жданов, В. А. Чалкин. -М.: Кн. дом «ЛИБРОКОМ», 2012.
7. Панасенко С. П. Алгоритмы шифрования. Специальный справочник. / С. П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 576 с.
8. Семёнов Г. Цифровая подпись. Эллиптические кривые.«Открытые системы» / Г. Семёнов., № 7-8 / 2002.

Арсенюк Дмитро Володимирович – Вінницький національний технічний університет, м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-19м, dima23790@gmail.com.

Науковий керівник: **Яремчук Юрій Євгенович** — доктор технічних наук, професор, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.

Dmytro Arseniuk - Vinnytsia National Technical University, Vinnytsia, Department of Management and Security of Information Systems, dima23790@gmail.com.

Supervisor: **Yaremchuk Yuriy** — D. Sc., professor, Department of Management and Security of Information Systems, Vinnitsa.