УДК 681.188:004.451.54

Лех В.О.
Запорізький національний технічний університет

Клептографічна атака на ECDSA

Сучасні комп'ютерні технології та нові математичні методи дають можливість крипто- аналітикам створювати різного роду небезпечні програми і впроваджувати шкідливі крипто- алгоритми в криптосистеми.

В 1996 році А. Янг та М. Юнг [1-3] ввели поняття клептографії, як метод використання криптографії проти криптографії з метою отримання секретної інформації.

Існують різні клептографічні атаки, в ході яких зловмисник використовує асиметричну систему криптографії для здійснення злому.

При здійсненні клептографічних атак створюються приховані канали, які є частиною криптоалгоритму і дозволяють непомітно передавати інформацію з криптографічної системи або, навпаки, в криптографічну систему. Наприклад, додаткова інформація може міститися в цифровому підпису [4] або у відкритому ключі шифрування.

Метою даної роботи є ознайомлення та аналіз клептографічної SETUP–атаки [5] на алгоритм цифрового підпису на еліптичних кривих ECDSA, а також реалізація цієї атаки.

В роботі наведено характеристики клептографчних атак, описи алгоритму ECDSA та SETUP–атаки.

Практична реалізація клептографічної SETUP – атаки була здійснена на 2-х різних еліптичних кривих над простим полем GF(43) та GF(57896044618658097711785492504343953926634992332820282019728792003956564821041).

В результаті атаки знайдено секретний ключ, за допомогою якого був сформований цифровий підпис за алгоритмом ECDSA.

Для здійснення цієї атаки крипто аналітику необхідно створити додаткові параметри, які використовуються при формуванні цифрового підпису, а також прихований канал для зберігання необхідних параметрів.

Аналіз SETUP–атаки на алгоритм ECDSA показав, що ця атака може бути здійснена при умові лише разового доступу до модифікації програмного забезпечення.

Список використаних джерел

1. *Young A., Yung M. Kleptography: Using Cryptography against Cryptography, Advances in Cryptology – EUROCRYPT '97 Proceedings, Springer-Verlag, 1997. p. 62–74.*
2. *Young A., Yung M. The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems, Advances in Cryptology – CRYPTO '97 Proceedings, Springer-Verlag, 1997. p. 264–276.*
3. *Young A., Yung M. Malicious Cryptography: Exposing Cryptovirology. Wiley Publishing. 2004.*
4. *Коржев В. Цифровая подпись. Эллиптические кривые [Електронний ресурс] / В. Коржев // Открытые системы. – 8. – Режим доступу до ресурсу: www.morepc.ru/security/crypt/os200207010.html.*
5. *Чепик Н. А. Атаки на схему электронной цифровой подписи на эллиптических кривых [Електронний ресурс] / Н. А. Чепик, М. А. Иванов // Безопасность информационных технологий. – 2014. – Режим доступу до ресурсу: http://elibrary.ru/item.asp?id=23404788.*