ДОСЛІДЖЕННЯ БІОМЕТРИЧНИХ КРИПТОГРАФІЧНИХ СИСТЕМ

Андрющенко А.О., Фесенко А.В.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, навчально-наукова лабораторія «Систем технічного захисту інформації (відеоспостереження, охоронні сигналізації і контроль доступу)», тел. (057) 702-14-78

The work considers the class of information security systems based on the analysis of data on the behavior of users and IT entities.

Інтеграція біометричних і криптографічних технологій відкриває нові перспективи у сфері забезпечення інформаційної безпеки. Основними задачами біометричної криптографії є захист криптографічних ключів за допомогою біометричних даних, захист біометричних еталонів та генерування криптографічних ключів. В наш час існують три основні види біометричних криптографічних систем: системи із звільненням ключа (key release cryptosystems), зі зв'язуванням ключа (key binding cryptosystems) та з генерацією ключа (key generation cryptosystems).

Біометричні криптографічні системи зі звільненням ключа. В режимі звільнення ключа біометрична аутентифікація здійснюється незалежно від механізму звільнення ключа, біометричний еталон і ключ зберігаються окремо один від одного, сам ключ звільняється після успішної біометричної аутентифікації. Даний вид біометричних криптосистем непридатний в більшості випадків, оскільки існує можливість заміни модуля порівняння при виконанні аутентифікації.

Біометричні криптографічні системи зі зв'язуванням ключа. В криптографічних системах такого типу ключ і біометричний еталон криптографічно пов'язані між собою. Ключ закривається біометричним еталоном користувача і зберігається в такому вигляді в базі даних, відповідно розкрити ключ представляється можливим тільки власникові біометричних параметрів.

Біометричні криптографічні системи з генерацією ключа. У такій біометричній криптосистемі ключ отримується безпосередньо з біометричних даних користувача і не зберігається в базі даних. Можливість не зберігати ключ, отриманий з біометричних даних, є незаперечною перевагою методу генерації криптографічних ключів з біометричних даних користувача в порівнянні з іншими існуючими методами. Таким чином, головною відмінністю двох останніх видів біометричних криптосистем є те, що в першому з них криптографічний ключ тільки закривається за допомогою біометричного еталона, а в другому ключ генерується безпосередньо з біометричних даних користувача.

Основною проблемою, яка існує при використанні біометричних даних для генерації криптографічних ключів, є те, що біометричні дані

неточно відтворювані і не мають рівномірного розподілу ймовірностей, в криптографії ж потрібно використовувати точне значення ключа. Порівняно нещодавно в роботі [3] було запропоновано новий метод генерації ключів, що отримав назву «метод нечітких екстракторів» (fuzzy extractors). Цей спосіб дозволяє однозначно відновлювати секретний ключ з неточно відтворюваних біометричних даних за участю так званих допоміжних даних (helper data), що є відкритими. При цьому якість нечітких екстракторів визначається якістю застосовуваних в них кодів, що виправляють помилки. Безсумнівним достоїнством способу є відсутність необхідності зберігання секретного ключа, однак потрібно зберігання допоміжних даних. Недолік способу в тому, що він дозволяє отримати тільки один ключ з одних біометричних даних.

Розвитком біометричних криптографічних є мультимодальні біометричні криптографічні системи. Наприклад, об'єднання мультимодальної біометрії (наприклад, обличчя плюс голос), порогової криптографії з поділом секрету (наприклад, за схемою Шаміра) та методів перетворення нечітких біометричних параметрів в ключові послідовності дозволяє створити криптосистеми поділу секрету за біометричними параметрами учасників системи. Відновити секрет такої мультимодальної біометричної порогової криптосистеми може користувач, який володіє необхідним набором відповідних біометричних параметрів, або користувачі, які в сукупності володіють необхідною кількістю параметрів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Uludag U., Pankanti S., Prabhakar S., Jain A. K. Biometric cryptosystems: issues and challenges // Proceedings of the IEEE. 2004. Vol. 92. № 6. P. 948–960.

2. Juels A., Sudan M. A Fuzzy Vault Scheme // Proceedings of IEEE International Symposium on Information Theory. Lausanne, Switzerland, 2002. P. 408.

3. Dodis Y., Reyzin L., Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data // Advances in Cryptology – EUROCRYPT 2004. Christian Cachin and Jan Camenisch, ed. Vol. 3027 of Lecture Notes in Computer Science. Springer – Verlag, 2004. P. 79–100.

4. Sahai A., Waters B. Fuzzy identity-based encryption // Proceedings of EUROCRYPT 2005, LNCS 3494. Springer – Verlag, 2005. P. 457–473.

5. Burnett A., Duffy A., Dowling T. A Biometric Identity Based Signature Scheme. Cryptology ePrint Archive: Report 2004/176. URL: http://eprint.iacr.org/2004/176.