Секция «Дискретная математика и математическая кибернетика»

Биометрическое личностное шифрование

Научный руководитель – Носов Валентин Александрович

Поляков Андрей Владимирович
Аспирант
Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра математической теории
интеллектуальных систем, Москва, Россия
E-mail: andre.levsha@gmail.com

Асимметричная криптография стала элегантным решением задачи распределения ключей. Однако этот подход стало причиной возникновения другой проблемы.

А именно, открытый ключ, в силу математических свойств асимметричных криптоалгоритмов, является набором случайных бит, не содержащих никакой информации о владельце, поэтому он не может служить средством аутентификации. Этот недостаток стал причиной появления иерархической системы сертификации открытых ключей.

В настоящее время аутентификация пользователей происходит следующим образом:

1) Пользователь Алиса проходит процедуру проверки в удостоверяющем центре и получает сертификат;
2) Алиса посылает свой сертификат Бобу;
3) Боб получает сертификат удостоверяющего центра;
4) С помощью полученных сертификатов Боб производит аутентификацию Алисы.

Личностное шифрование впервые было предложено А. Шамиром [2] в 1984 году, которое возникло как идея упрощения этой схемы. Шамир предположил, что если бы появилась возможность использовать в качестве открытого ключа имя или почтовый адрес Алисы, то это лишило бы сложную процедуру аутентификации всякого смысла.

Под личностным шифрованием подразумевается криптосистема с открытым ключом, в которой пользователю разрешено выбрать адрес своей электронной почты либо телефонный номер в качестве открытого ключа вместо генерации случайным образом пары открытого и секретного ключей. Генератор секретного ключа вычисляет секретный ключ пользователя по личным данным пользователя и секретный мастер-ключ, после чего передает пользователю его секретный ключ.

Долгое время идея Шамира оставалась всего лишь красивой криптографической головоломкой, главным недостатком подобной схемы долгое время была невозможность использования биометрии в этой системе в силу ее изменчивости.

Однако в 2005 году в статье [4] была предложена концепция нечеткого личностного шифрования, в которой личностные характеристики были представлены набором атрибутов, а не строкой символов. В 2007 в статье [6] была предложена концепция цифровой подписи, основанной на пользовательской биометрии. В ней была предложена идея использования биометрических данных для создания открытого ключа, но не было предложено конкретной схемы. В 2008 году в статье [8] был впервые предложен протокол биометрического личностного шифрования. В 2010 году в статье [10] были предложены общие схемы биометрического личностного шифрования.

Однако протоколы, описанные в этих статьях, обладают следующими ограничениями: размер шифртекста линеен по пользовательским данным и требует большого количества

операций при расшифровании. Целью настоящего исследования является устранение этих ограничений. В докладе представлен новый протокол биометрического личностного шифрования, удовлетворяющий следующим свойствам:
Постоянный размер шифртектста;
Быстрый алгоритм генерации ключей;
Эффективный алгоритм расшифрования. Представленный алгоритм расшифрования требует всего две операции спаривания, что лучше, чем количество операций в аналогичных алгоритмах (линейное число от параметра, определяющего допустимое количество ошибок);
Сводимость к билинейной задаче распознавания Диффи-Хеллмана. Сложность этой задачи считается выше сложности билинейной инверсионной задачи Диффи-Хеллмана, на которой основаны схемы nbsp;[8], [10];
Безопасность протокола. Протокол обладает стойкостью к атаке на основе адаптивно подобранных выбранной идентифицирующей информации и шифртекста (в то время как аналогичные схемы обладают устойчивостью только к атаке с выбранным открытым текстом).

Источники и литература

1)
2) Shamir, A., 1984. Identity-Based Cryptosystems and Signature Schemes. Proc. Crypto, p.47-53.
3)
4) Sahai, A., Waters, B., 2005. Fuzzy Identity-Based Encryption. Proc. EUROCRYPT, p.457-473
5)
6) Burnett, A., Byrne, F., Dowling, T., Duffy, A., 2007. A biometric identity based signature scheme. Int. J.Network Secur., 5(3):317-326
7)
8) Sarier, N.D., 2008. A New Biometric Identity Based Encryption Scheme. Proc. ICYCS, p.2061-2066
9)
10) Sarier, N.D., 2010. Generic Constructions of Biometric Identity Based Encryption Systems. Proc. WISTP, p.90-105.