О. В. Куликова

БИОМЕТРИЧЕСКИЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ИХ ПРИМЕНЕНИЕ

Введение

В настоящее время существуют два основных направления применения биометрии: аутентификация личности и криптография. Использование биометрии для аутентификации личности является традиционным, имеет большую историю изучения и применения. В целом методы биометрической аутентификации хорошо отработаны и успешно применяются на практике, несмотря на существование до сих пор нерешенных вопросов, связанных с качеством биометрических систем. Эти методы постоянно развиваются и совершенствуются, что делает их привлекательными для массового применения, например, в системах контроля и управления доступом в режимные помещения и к источникам информации, в том числе к компьютерам и вычислительным сетям.

Применение биометрических методов в криптографии имеет свои особенности. Криптографические методы широко применяются для обеспечения секретности и аутентичности информации. Их стойкость основана на предположении, что секретный ключ известен только законному пользователю. На практике сохранение секретности ключа является одной из основных задач при эксплуатации криптосистем. Ключи обычно хранятся в безопасном месте и для контроля доступа к ним чаще всего используется парольная аутентификация, которая имеет ряд недостатков: пароли могут быть легко потеряны, украдены, забыты и т. д. Недостатки парольной аутентификации можно преодолеть с помощью более надежных схем аутентификации, таких как биометрические. Биометрические методы аутентификации личности имеют ряд преимуществ по сравнению с традиционными, а именно: 1) биометрические признаки очень трудно фальсифицировать; 2) в силу уникальности биометрических признаков достоверность аутентификации очень высока; 3) биометрический идентификатор нельзя забыть, как пароль, или потерять, как пластиковую карточку; 4) для биометрической аутентификации требуется присутствие владельца биометрических признаков. Таким образом, биометрические системы предоставляют естественное и надежное решение задачи аутентификации в криптографических системах.

В последнее время выделилось новое направление применения биометрии в системах криптографической защиты информации: она стала применяться не только для защиты от несанкционированного доступа к ключам, но и в качестве источника ключевого материала. Однако применение биометрического материала в качестве источника ключей наталкивается на ряд сложностей: биометрические данные нечетко воспроизводимы и не имеют равномерного распределения, в то время как большинство криптографических преобразований биективны, а следовательно, требуют точного значения ключа. Для решения задач такого рода биометрия начала использоваться сравнительно недавно и в настоящее время развивается по нескольким направлениям. В зависимости от цели применения биометрии в криптографии появилось несколько видов биометрических криптографических систем: *системы с освобождением ключа* (англ. *key release cryptosystems*), *системы со связыванием ключа* (англ. *key binding cryptosystems*), *системы с генерацией ключа* (англ. *key generation cryptosystems*).

1. Биометрические криптографические системы с освобождением ключа

В режиме освобождения ключа биометрическая аутентификация осуществляется независимо от механизма освобождения ключа. Биометрический эталон и ключ хранятся отдельно друг от друга, при этом ключ освобождается только при условии, что биометрическая аутентификация прошла успешно.

Несмотря на простоту реализации биометрических криптографических систем такого типа, подобные системы непригодны для применения в приложениях, требующих высокой степени защиты, поскольку они имеют две основные уязвимости. Во-первых, биометрические эталоны не являются защищенными, поскольку они хранятся локально и к ним требуется доступ в процессе сравнения биометрических данных. Во-вторых, поскольку аутентификация и освобождение ключа абсолютно не связаны между собой, то представляется возможным заменить модуль сравнения при выполнении аутентификации, используя вредоносное программное обеспечение. В случае реализации этой уязвимости будет принято неверное решение об аутентификации и, соответственно, получен доступ к секретному ключу.

Данный метод биометрической аутентификации неприменим в большинстве криптографических приложений, поскольку он использует незашифрованную биометрическую информацию в незащищенных каналах связи [1].

2. Биометрические криптографические системы со связыванием ключа

В криптографических системах такого типа ключ и биометрический эталон криптографически связаны между собой и представляют единое целое. В этом случае декодирование ключа из биометрического эталона без знания биометрических данных пользователя является вычислительно сложной задачей. Для обеспечения возможности извлечения ключа из эталона используются коды, исправляющие ошибки, которые позволяют извлекать ключ в случае, если биометрические данные пользователя отличаются от эталона, но не более чем на определенное количество битов.

Иными словами, ключ закрывается биометрическим эталоном пользователя и сохраняется в таком виде в базе данных. Это делается, например, с помощью надежного алгоритма замещения секретных битов, который может заменить криптографическим ключом небольшое количество значащих битов в биометрическом эталоне. При успешном сравнении биометрических данных ключ извлекается из биометрического эталона, хранимого в базе данных, и может дальше использоваться в системе. Безопасность данного метода зависит от секретности алгоритмов закрытия и восстановления ключа. В том случае, если эти алгоритмы детерминированны (т. е. закрывают ключ в одних и тех же местах в эталоне), они могут быть легко скомпрометированы. Однако такие биометрические криптографические системы более безопасны по сравнению с предыдущими, но более сложны в реализации из-за сильной изменчивости биометрических данных с течением времени.

Данный вид биометрических криптосистем изначально был разработан для защиты криптографических ключей. Тем не менее он также может быть применим и в качестве механизма защиты биометрических эталонов. Схема, предложенная в работе [2], стала одним из наиболее популярных методов защиты эталонов. Позднее были разработаны варианты ее применения к отпечаткам пальцев, лицу, радужной оболочке глаза и собственноручной подписи. А в последнее время с развитием мультибиометрических технологий появились схемы для нескольких отпечатков пальцев, а также для голоса и отпечатка пальца.

3. Биометрические криптографические системы с генерацией ключа

В такой биометрической криптосистеме ключ извлекается непосредственно из биометрических данных пользователя и не хранится в базе данных. Возможность не хранить ключ, полученный из биометрических данных, является неоспоримым преимуществом метода генерации криптографических ключей из биометрических данных пользователя по сравнению с другими существующими методами. Из биометрических данных пользователя извлекаются параметры, из которых при помощи специального алгоритма генерируется секретный ключ пользователя. Таким образом, главным отличием двух последних видов биометрических криптосистем является то, что в одном из них криптографический ключ только закрывается при помощи биометрического эталона, а в другом ключ генерируется непосредственно из биометрических данных пользователя.

Основной проблемой, которая существует при использовании биометрических данных для генерации криптографических ключей, является то, что биометрические данные неточно воспроизводимы и не имеют равномерного распределения вероятностей, в криптографии требуется использовать точное значение ключа. Кроме того, биометрические данные обладают рядом особенностей, которые создают сложности при использовании этих данных в качестве источника ключевого материала.

• Биометрические данные могут меняться со временем и в зависимости от физического и эмоционального состояния их владельца.

• Биометрические данные неотзываемы. Биометрические параметры присущи личности, поэтому они не могут быть легко изменены. Отсюда возникает проблема смены ключей: пользователь может захотеть иметь разные ключи для различных приложений, при этом иметь возможность отзывать один из ключей, не влияя на другие.

• Биометрические данные не являются секретными, поскольку люди оставляют их повсеместно, например, отпечатки пальцев могут быть оставлены на различных поверхностях, а изображение радужной оболочки глаза может быть зафиксировано скрытой камерой.

• Биометрические данные неточно воспроизводимы, что приводит к возникновению трудностей при их сравнении с зашифрованным эталоном, хранящимся в базе данных.

• Биометрия тесно связана с проблемой защиты персональных данных. Многие люди не хотят хранить свои биометрические эталоны в центральных базах данных из соображений конфиденциальности своих персональных данных.

Несмотря на сложности, существующие при использовании биометрических данных для генерации криптографических ключей, данное направление в криптографии постоянно развивается. Синтез биометрических технологий и криптографии позволяет повысить стойкость систем криптографической защиты информации. За последние несколько лет были предприняты многочисленные попытки создания методов генерации ключей из различных биометрических данных. Однако в большинстве работ длина ключей очень мала, а вероятность ошибки второго рода превышает 20 %, что неприемлемо для практического применения.

Сравнительно недавно в работе [3] был предложен новый метод генерации ключей, получивший название метод «нечетких экстракторов» (fuzzy extractors). Данный способ кардинально отличается от предложенных ранее тем, что позволяет однозначно восстанавливать секретный ключ из неточно воспроизводимых биометрических данных. Этот способ позволяет задавать длину ключа в виде параметра. При этом для воспроизведения ключа требуются дополнительные открытые данные, соответствующие этому ключу, которые хранятся в памяти. «Нечеткий экстрактор» позволяет получать только один ключ. Однако из всех способов этот способ — самый лучший, поскольку качество выходной ключевой последовательности удовлетворяет всем критериям качества криптографических ключей. Метод нечетких экстракторов извлекает случайную равномерно распределенную последовательность из первоначальных входных данных и далее правильно восстанавливает ее из любых данных, достаточно схожих с первоначальными. Однако энтропия извлеченной последовательности меньше энтропии входной последовательности. При этом качество «нечетких экстракторов» определяется качеством применяемых в них кодов, исправляющих ошибки. Случайная равномерно распределенная последовательность, полученная при помощи «нечеткого экстрактора», может быть использована в криптографических целях (например, в качестве секретного ключа), но, в отличие от традиционных ключей, не требует сохранения. Метод нечетких экстракторов применим как к биометрической информации, так и к любому ключевому материалу, который, в отличие от обычных криптографических ключей, точно не воспроизводим и не распределен равномерно.

4. Практические применения биометрических криптосистем с генерацией ключа

Биометрические криптосистемы с генерацией ключа в основном находят применение в идентификационных криптосистемах, в протоколах распределения ключей и протоколах аутентификации. Рассмотрим особенности их применения более подробно.

Идентификационные криптосистемы. Благодаря тому, что появилась возможность точно воспроизводить ключи из зашумленных данных, выделились новые классы идентификационных криптосистем, которые получили название *нечеткие идентификационные криптосистемы* (англ. fuzzy identity based cryptosystems (FIBC)) и *биометрические идентификационные криптосистемы* (англ. biometric identity based cryptosystems (BIO-IBC)). Метод «нечетких экстракторов» позволил использовать биометрические данные для формирования ключей в идентификационных криптосистемах. Наиболее известными работами, выполненными в данном направлении, являются статьи [4, 8, 9].

Конструкция под названием *биометрическая идентификационная схема цифровой подписи* (Biometric Identity Based Signature (FIBS)) была предложена в работе [9]. В ней используются биометрические данные пользователя для формирования открытого ключа. Преимущество такой схемы в том, что в ней открытый ключ является уникальным в силу физиологических особенностей человека. Для генерации ключевой последовательности из биометрических данных авторы применяют метод «нечетких экстракторов». Открытый ключ и соответствующий секретный ключ создаются при помощи полученной ключевой последовательности и метода внедрения этой последовательности в точку эллиптической кривой. Далее для выполнения операций генерации и проверки подписи применяется идентификационная схема цифровой подписи на основе парных отображений. Такая схема подписи может успешно применяться для обеспечения невозможности отказа от подписи на документах, поскольку для подтверждения достоверности подписи пользователю необходимо всего лишь предоставить арбитру свои биометрические данные.

Концепция *нечеткого идентификационного шифрования* (fuzzy identity based encryption (FIBE)) была впервые предложена в работе [4]. В FIBE пользователь с секретным ключом, полученным из идентификационных данных w, может расшифровать шифртекст, зашифрованный на открытом ключе, полученном из идентификационных данных w', при условии, что w и w' достаточно близки друг к другу. В отличие от предыдущих подходов, биометрические данные в FIBE, которые используются в качестве идентификационных, не нужно держать в секрете. FIBE может также использоваться для такого приложения, как атрибутное шифрование (attribute-based encryption), когда участник может зашифровать данные для всех пользователей, имеющих определенный набор атрибутов. Общая схема FIBE, согласно [4], состоит из четырех алгоритмов: инициализации параметров, генерации секретного ключа, зашифрования и расшифрования. В последующих работах [5–7] были предложены модификации данной схемы. В частности, в [5] разработаны две новые схемы, в которых открытые параметры имеют меньший размер. Позднее в [6] было использовано гибридное шифрование совместно с FIBE и предложен первый нечеткий идентификационный механизм инкапсуляции ключей (fuzzy identity-based key encapsulation mechanism (Fuzzy-IB-KEM)). А совсем недавно в работе [7] появилась схема FIBE, которая является полностью безопасной.

Более поздний примитив под названием *нечеткая идентификационная схема цифровой подписи* (Fuzzy Identity Based Signature (FIBS)) появился в работе [8] и является аналогом схемы FIBE. Данная схема позволяет пользователю, обладающему идентификационными данными w, получить подпись, которая может быть проверена при помощи идентификационных данных w' тогда и только тогда, когда w и w' достаточно близки на некоторой метрике. Данная схема непосредственно применима как в идентификационных схемах подписи, использующих биометрические данные, так

и в атрибутных схемах подписи, в которых пользователь может создать подпись от лица группы, имеющей определенный набор атрибутов. Общая схема предложенной авторами этой работы подписи состоит из алгоритмов инициализации параметров, генерации секретного ключа, генерации и проверки подписи.

Протоколы распределения ключей. Метод генерации ключа на основе «нечетких экстракторов» и их модификаций стал успешно использоваться в протоколах обмена ключами. Одним из первых подобных протоколов на основе надежных «нечетких экстракторов» с использованием биометрических данных стал протокол из работы [10]. В протоколе участники договариваются о равномерно распределенном секретном ключе, используя конструкцию надежного «нечеткого экстрактора» и посылая сообщение по незащищенному каналу, контролируемому активным или пассивным противником. Для случая, когда зашумленными данными являются биометрические данные, в роли участников протокола могут выступать доверенный сервер, хранящий эталон биометрических данных, и пользователь, получающий каждый раз свежие данные, близкие к хранящемуся на сервере эталону. Возможен также вариант протокола, когда пользователь выполняет протокол согласования ключей с самим собой два раза. Спустя некоторое время в работе [11] появилась интерактивная версия этого протокола. В то время как конструкция надежных «нечетких экстракторов» [10] ввиду их неинтерактивной природы требует, чтобы энтропия была не меньше половины ее длины, в этом протоколе таких ограничений нет.

Протоколы биометрической аутентификации. За последние годы предпринималось множество попыток разработки безопасных протоколов биометрической аутентификации. Позднее в работе [3] было показано, как использовать биометрические данные для генерации криптографических ключей, которые потом могут быть использованы в целях аутентификации. Метод «нечетких экстракторов» был признан основным решением для защищенной биометрической аутентификации. Примерами протоколов для защищенной аутентификации, использующих этот метод, являются конструкции, предложенные в работах [3, 10, 12, 13]. Протокол, представленный в [3], гарантирует безопасность только в случае пассивного противника, но не обеспечивает защищенную биометрическую аутентификацию в присутствии активного противника, который может модифицировать сообщения, посылаемые между сервером и пользователем. В работе [12] показано, что невозможно гарантировать сохранение безопасности, если один и тот же нечеткий экстрактор используется для аутентификации пользователя на нескольких серверах. Основным недостатком метода, предложенного в этой работе, является то, что он обеспечивает аутентификацию только в одном направлении, т. е. только пользователя на сервере. Позднее в работах [10, 13] была предложена конструкция надежного нечеткого экстрактора, который позволяет выполнять взаимную аутентификацию по незащищенным каналам.

Заключение

В работе предложена классификация и проведен анализ различных типов биометрических криптографических систем. Основное отличие таких криптосистем от традиционных заключается в том, что биометрия в них служит не только для защиты, но и для генерации криптографических ключей. Главное преимущество биометрических криптографических систем с генерацией ключа заключается в том, что ключ, извлеченный непосредственно из биометрических данных пользователя, не требуется хранить в базе данных, поскольку при необходимости использования он всегда может быть восстановлен из биометрических данных пользователя. В работе показаны широкие возможности применения таких систем в идентификационных криптосистемах, в протоколах аутентификации и распределения ключей.

СПИСОК ЛИТЕРАТУРЫ:

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. *Baek J., Susilo W., Zhou J.* New construction of fuzzy identity-based encryption // Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. ACM New York. NY, USA, 2007. P. 368–370.
6. *Fang L. M., Wang J. D., Ren Y. J., Xia J. Y., Bian S. Z.* Chosen — Ciphertext Secure Fuzzy Identity — Based Key Encapsulation without ROM. Cryptology ePrint Archive: Report 2008/139, 2008. URL: http://eprint.iacr.org/2008/139.
7. *Fang L., Xia J.* Full Security: Fuzzy Identity Based Encryption. Cryptology ePrint Archive: Report 2008/307. URL: http://eprint.iacr.org/2008/30
8. *Yang P., Cao Z., Dong X. I.* Fuzzy Identity Based Signature. Cryptology ePrint Archive: Report 2008/002. URL: http://eprint.iacr.org/2008/002.
9. *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.
10. *Dodis Y., Katz J., Reyzin L., Smith A.* Robust fuzzy extractors and authenticated key agreement from close secrets // Advances in Cryptology — CRYPTO 2006. Cynthia Dwork, ed. Vol. 4117 of Lecture Notes in Computer Science. Springer — Verlag, 20 — 24 August 2006. P. 232–250.
11. *Kanukurthi B., Reyzin L.* Key Agreement from Close Secrets over Unsecured Channels. Cryptology ePrint Archive: Report 2008/494. URL: http://eprint.iacr.org/2008/494.
12. *Boyen X.* Reusable cryptographic fuzzy extractors // Eleventh ACM Conference on Computer and Communication Security. ACM, October 25–29 2004. P. 82–91.
13. *Boyen X., Dodis Y., Katz J., Ostrovsky R., Smith A.* Secure remote authentication using biometric data // Advances in Cryptology — EUROCRYPT 2005. R. Cramer, ed. Springer — Verlag, 2005. Vol. 3494 of LNCS. P. 147–163.