Новости криптографии:
новые задачи и новые методы передовых направлений

Яна АВЕЗОВА,
НПО «Эшелон»

Современное общество живет в эпоху под названием «Интернет вещей» (Internet of Things – IoT). Большинство устройств, ежедневно упрощающих нашу жизнь, имеют ограниченные вычислительные ресурсы, однако этим устройствам необходимо постоянно взаимодействовать. Не возникает сомнений, что информация, циркулирующая между всевозможными устройствами во время того или иного процесса, может носить конфиденциальный характер. Ярким примером, пожалуй, здесь будут смарт-карты. Компрометация данных такого устройства может привести к серьезным финансовым потерям как отдельного лица, так и целого государства.

Постоянно развивающиеся технологии и увеличение вычислительных мощностей открывают все новые и новые возможности для злоумышленников. Некоторые алгоритмы, еще недавно считавшиеся стойкими, становятся уязвимы к атакам простого перебора для поиска ключа.

Кроме того, с появлением новых технологий, например облачных вычислений, появились совершенно новые проблемы, требующие принципиально иных подходов к их решению.

Эллиптическая криптография

Датой зарождения идеи применения математического аппарата эллиптических кривых для решения задачи защиты информации криптографическими методами можно считать 1985 г., когда Миллер и Коблиц независимо представили свои работы [1] и [2] мировому сообществу. Главное преимущество криптографии на эллиптических кривых заключается в том, что для задачи дискретного логарифмирования в группе точек эллиптической кривой не существует субэкспоненциальных алгоритмов решения, что позволяет уменьшить длину ключа и увеличить производительность.

В конце прошлого года группа американских ученых проанализировала четыре популярных протокола, использующих эллиптическую криптографию: Bitcoin, SSH, TLS и Austrian e-ID [3]. Эксперты подсчитали, что из 12 млн хостов, поддерживающих SSH, в 10,3% реализован ECDSA (алгоритм цифровой подписи, основанный на эллиптических кривых) для аутентификации и в 13,8% – ECDH (аналог протокола Диффи-Хеллмана с использованием эллиптической криптографии) для обмена ключами. Авторы также исследовали 30,2 млн TLS-серверов, обнаружив, что 7,2% из них поддерживают ECDH. Из 829 тыс. сертификатов Austrian Citizen Card в 58% используется ECDSA. Отмечается также, что вся асимметричная криптография, на которой построена защита системы Bitcoin, основана на математическом аппарате эллиптических кривых.

Однако, как показало исследование, эллиптическая криптография не является панацеей от таких уязвимостей, как низкая энтропия и ошибки программной реализации. Эксперты выявили немало примеров повторяющихся SSH- и TLS-ключей, принадлежащих разным владельцам сертификатов. В системе Bitcoin были выявлены цифровые подписи, позволяющие узнать временный ключ, который, в свою очередь, даст злоумышленнику соответствующий закрытый ключ и возможность похитить криптовалюту.

В январе текущего года исследователи Neha Tirthani и R. Ganesan из Индии предложили механизм защиты данных в облачных хранилищах, основанный на сочетании «классической» проблемы Диффи-Хеллмана и проблемы дискретного логарифмирования в группе точек эллиптической кривой [4]. Авторы

отмечают, что протокол, основанный на эллиптических кривых, имеет небольшой размер ключа без ущерба криптостойкости, что делает эллиптическую криптографию привлекательной для использования в тех областях, где существуют проблемы из-за ограничения памяти и вычислительных мощностей.

Гомоморфное шифрование

Развитие гомоморфного шифрования данных началось с публикации работы известных криптографов [5] в 1978 г. Суть идеи гомоморфного шифрования состоит в возможности совершать операции с зашифрованными данными, получая зашифрованный результат, который соответствовал бы тем же операциям, выполняемым над открытым текстом. Почти 30 лет оставалась нерешенной задача полного гомоморфного шифрования − создание системы, гомоморфной для операций сложения и умножения одновременно. Наконец в 2009 г. эта задача была решена Крейгом Джентри [6].

В 2010 г. на конференции EUROCRYPT'10 Ван Дижк предложил систему полного гомоморфного шифрования, основанную на сложности решения проблемы нахождения приближений для общих делителей [7], а в следующем году на той же конференции была предложена более эффективная система полного гомоморфного шифрования [8].

В мае 2013 г. стало известно, что компания IBM выпустила свободно распространяемую криптографическую библиотеку HElib с поддержкой гомоморфного шифрования. Подобная криптосистема была реализована впервые. Разработка имеет особенную практическую ценность именно в наши дни, с распространением облачных сервисов. В основе реализованной системы лежит идея, предложенная Крейгом Джентри, улучшенная с использованием техники упаковки шифртекст Смарта-Веркаутерена и оптимизациями Гентри-Халеви-Смарта. В феврале этого года разработчики библиотеки, Виктор Шоуп и Шаи Халеви, выпустили совместную статью [9], в которой дано описание некоторых алгоритмов.

Легковесная криптография

Эпоха Интернета вещей, как известно, предполагает использование каждым из нас множества различных ограниченных в памяти и вычислительных мощностях устройств, повышающих уровень нашего комфорта и качества жизни. Под такими «вещами» понимаются всевозможные датчики, охранные сигнализации, бытовые приборы и др. Эти устройства должны взаимодействовать друг с другом посредством сети Интернет, и чтобы наслаждаться в полной мере эпохой Интернета вещей, необходимо задуматься над обеспечением безопасности такого взаимодействия. Однако из-за обозначенных выше ограничений, свойственных различным устройствам, возникла проблема обеспечения защиты криптографическими методами, решением которой и стало новое направление − легковесная криптография.

В области блочного шифрования наиболее популярными легковесными алгоритмами считаются CLEFIA [10] и PRESENT [11]. Оба алгоритма известны еще с 2007 г. В 2012 г. организации ISO и IEC включили алгоритмы PRESENT и CLEFIA в международный стандарт облегченного шифрования ISO/IEC 29192-2:2012. В феврале 2014 г. стало известно о разработке нового легковесного блочного шифра Halka [13]. Его основное отличие − использование

Мнение специалиста

Артем БЫЧКОВ,

ведущий аналитик отдела практического анализа защищенности Центра информационной безопасности, компания «Инфосистемы Джет»:

Передовые исследования в области криптографии несомненно впечатляют и являются важной инвестицией в будущее. Особенно на фоне достижений современного криптоанализа и непреклонного роста вычислительных мощностей. Однако следует помнить о том, что криптографические алгоритмы – лишь строительные блоки, используемые разработчиками систем и протоколов. И как показывает практика, уязвимой криптосистему в первую очередь делают ошибки проектирования и реализации, а не слабости того или иного алгоритма.

Если посмотреть на существующие системы, то выяснится, что давно существующие, изученные и апробированные криптографические строительные блоки (при их правильном применении) позволяют создавать системы, в обозримом будущем устойчивые к криптоаналитическим атакам. Например, международные платежные системы широко используют алгоритмы, разработанные еще в 70-х гг. XX века, и злоумышленникам, чтобы обойти шифрование, приходится использовать скимминг и накладные клавиатуры на банкоматы. И напротив, почти все самые громкие уязвимости в распространенных криптосистемах связаны именно с недостатками проектирования и реализации. Будь то протоколы (WEP и т. п.), популярные библиотеки (нашумевший OpenSSL) или же законченные продукты для массового рынка безопасности (например, сертифицированные шифрованные флеш-накопители, в которых использовался один общий, установленный на заводе ключ).

Пока нет оснований полагать, что этот тренд в ближайшее время изменится. Поэтому наравне с теоретическими исследованиями нельзя забывать и о повышении качества работы инженеров, проектирующих, разрабатывающих и внедряющих системы, использующие криптографию. Ведь даже продукты вендоров, специализирующихся на разработке криптосистем (не говоря уж о множестве собственных разработок), бывают уязвимы.

восьмибитных S-боксов, в то время как большинство других блочных алгоритмов с легковесными свойствами используют четырехбитные S-боксы. Использование же восьмибитных S-боксов гарантирует более высокую криптостойкость.

В рамках проекта eSTREAM, существовавшего с 2004 г. по 2008 г. в качестве конкурса на разработку поточных шифров, в числе «победителей» оказались такие легковесные поточные шифры, как Grain (версия 1), MICKEY (версия 2) и Trivium.

Что же касается легковесной хэш-функции, то стоит отметить, что среди финалистов конкурса NIST для стандарта SHA-3 не нашлось ни одного алгоритма с легковесными свойствами. На сегодняшний день известны такие механизмы легковесной хэш-функции, как S-Quark и D-Quark [14], PHOTON [15] и SPONGENT [16]. Все эти алгоритмы, как и победитель конкурса SHA-3 Keccak, основываются на принципе криптографической губки, что позволяет оперировать с данными произвольной длины как на входе, так и на выходе алгоритма. В конце декабря прошлого года криптографическому сообществу стало известно еще об одной разработке легковесной хэш-функции под названием LHash [17]. Авторы заявляют, что созданный ими механизм, расширяющий описанный ранее принцип криптографической губки, позволил разработать компромиссный по безопасности, скорости, энергозатратам и стоимости реализации алгоритм.

В области криптографии с открытым ключом вопрос поиска оптимального легковесного алгоритма, сравнимого по надежности с RSA или с алгоритмами, основанными на эллиптических кривых, остается открытым, поскольку асимметричные системы более требовательны к временным ресурсам, чем симметричные. Однако некоторые достижения в этом направлении все же имеются, например в работе [18], для пассивных RFID-систем.

> Эпоха Интернета вещей предполагает использование каждым из нас множества различных ограниченных в памяти и вычислительных мощностях устройств, повышающих уровень нашего комфорта и качества жизни.

Квантовая криптография

Квантовая криптография изучает возможность генерации криптографических ключей, секретность которых гарантируется фундаментальными законами квантовой механики. Становление квантовой криптографии как науки началось в 1984 г. с разработки первого квантового протокола распределения ключей BB84 [19]. Главным преимуществом криптографических протоколов является то, что злоумышленник может обладать сколь угодно неограниченными возможностями для перехвата ключевой информации, однако факт прослушивания канала всегда останется замеченным. Это делает использование квантовой криптографии привлекательным для борьбы со шпионажем и мошенничеством в банковской сфере.

В апреле текущего года появилась новость о том, что исследователи Центра квантовой фотоники в Бристоле в сотрудничестве с компанией Nokia разработали надежную схему защиты информации в мобильных устройствах с использованием последних достижений в области квантовой криптографии.

В России с 2011 г. успешно функционирует Российский квантовый центр (РКЦ). В 2013 г. исследователи из РКЦ и Лаборатории сверхпроводящих метаматериалов МИСиС под руководством профессора Алексея Устинова впервые в России произвели измерение кубита.

Одним из перспективных направлений в квантовой криптографии остается решение задачи квантовой телепортации – переноса состояния с одного объекта на другой, находящийся на расстоянии, при условии, что состояние первого необратимо разрушается. Решением этой задачи занимаются ученые Женевского университета, Центра квантовой оптики Гарвардского университета, а также копенгагенского Института Нильса Бора. В сентябре 2013 г. стало известно, что группа Акиры Фурусавы (Akira Furusawa) из Токийского университета смогла реализовать полную квантовую телепортацию фотонных кубитов при помощи гибридной техники.

Одной из основных проблем квантовой криптографии является экспоненциальная скорость роста потерь при их передаче по линиям оптоволоконной связи, поэтому по-прежнему актуальной задачей остается разработка квантового повторителя.

Новости российских криптостандартов

В заключение обзора последних новостей в области криптографии следует отдельно рассмотреть новости, касающиеся российских криптографических стандартов.

Принятый в 2012 г. стандарт на цифровую подпись ГОСТ Р 34.10-2012, как и его предшественник ГОСТ Р 34.10-2001, основан на сложности дискретного логарифмирования в группе точек эллиптической кривой. В докладе Евгения Константиновича Алексеева на конференции РусКрипто'2014 «О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе» исследована эффективность реализации операций подписи и проверки подписи на кривых в формах Вейерштрасса, Хессе, Эдвардса и на скрученных кривых Эдвардса. Автор приходит к выводу, что скрученные кривые в форме Эдвардса, эквивалентные кривым простого порядка в форме Вейерштрасса, которые используются на сегодняшний день, могут существовать только над расширенными полями, однако увеличение размера элементов поля нивелирует любое преимущество от использования скрученных кривых Эдвардса.

В конце прошлого года Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), Академия криптографии Российской Федерации и ОАО «ИнфоТеКС» объявили о проведении конкурса по криптоанализу стандарта хэширования ГОСТ Р 34.11-2012. 30 апреля были определены три победителя первого этапа конкурса, одним из которых стал наш соотечественник Григорий Седов, а с 1 мая стартовал второй этап конкурса. Конкурс будет продолжаться до конца 2014 г.

На конференции РусКрипто'2013 в докладе Василия Шишкина впервые прозвучала мысль о необходимости разработки стандарта блочного шифрования взамен действующему ГОСТ Р 28147-89 в связи с появлением в 2010–2011 гг. ряда работ, где доказывалось снижение теоретической стойкости ГОСТ Р 28147-89. Предполагаемая длина блока перспективного блочного алгоритма составляет 128 бит, длина ключа осталась прежней – 256 бит. Базовая конструкция шифра предполагает использование SP-сети. Отмечено, что скорость шифрования на 64-битной платформе превосходит скорость шифрования действующим алгоритмом более чем в 1,4 раза. ■

Список литературы

1. *Miller V. Uses of elliptic curves in cryptography. Advances in Cryptology – CRYPTO'85, Lecture Notes in Computer Science, 218 (1986), pp. 417–426.*
2. *Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 48 (1987), pp. 203–209.*
3. *Joppe W. Bos and J. Alex Halderman and Nadia Heninger and Jonathan Moore and Michael Naehrig and Eric Wustrow. Elliptic Curve Cryptography in Practice. Cryptology ePrint Archive, Report 2013/734.*
4. *Neha tirthani and Ganesan, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. Cryptology ePrint Archive, Report 2014/049.*
5. *Ronald L. Rivest, Len Adleman, Michael L. Dertouzos. On Data Banks and Privacy Homomorphisms. Academic Press (1978).*
6. *Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices, ACM (2009).*
7. *Van Dijk M., Gentry C., Halevi S. et al. Fully homomorphic encryption over the integers, Advances in Cryptology-EUROCRYPT 2010. Springer Berlin Heidelberg, 2010, pp. 24–43.*
8. *Coron J. S., Mandal A., Naccache D. et al. Fully homomorphic encryption over the integers with shorter public keys. Advances in Cryptology-CRYPTO 2011, Springer Berlin Heidelberg, 2011, pp. 487–504.*
9. *Shai Halevi and Victor Shoup. Algorithms in HElib. Cryptology ePrint Archive, Report 2014/106.*
10. *T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-bit blockcipher CLEFIA, in Proceedings of Fast Software Encryption – FSE'07 (A. Biryukov, ed.). № 4593 in LNCS, pp. 181–195, Springer-Verlag, 2007.*
11. *A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. CHES 2007, № 4727 in LNCS, pp. 450–466, Springer-Verlag, 2007.*
12. *J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia. Quark: A Lightweight Hash. CHES 2010, № 6225 in LNCS, pp. 1–15, Springer-Verlag, 2010.*
13. *Sourav Das. Halka: A Lightweight, Software Friendly Block Cipher Using Ultra-lightweight 8-bit S-box. Cryptology ePrint Archive, Report 2014/110.*
14. *J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia. Quark: A lightweight hash. In Mangard and Standaert, pp. 1–15.*
15. *J. Guo, T. Peyrin, and A. Poschmann. The PHOTON family of lightweight hash functions. In P. Rogaway, editor, CRYPTO, volume 6841 of Lecture Notes in Computer Science, pp. 222–239, Springer, 2011.*
16. *A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, and I. Verbauwhede. Spongent: The design space of lightweight cryptographic hashing. IACR Cryptology ePrint Archive, 2011: 697, 2011.*
17. *Wenling Wu and Shuang Wu and Lei Zhang and Jian Zou and Le Dong. LHash: A Lightweight Hash Function (Full Version). Cryptology ePrint Archive, Report 2013/867.*
18. *Y.K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede. Elliptic-Curve-Based Security Processor for RFID. IEEE Trans. Comput., 57 (11): 1514–1527, 2008.*
19. *Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, 1984, pp. 175–179.*