КВАНТОВАЯ КРИПТОГРАФИЯ И ТЕОРЕМА В. А. КОТЕЛЬНИКОВА ОБ ОДНОРАЗОВЫХ КЛЮЧАХ

С. Н. Молотков

В наше время, когда техника, и особенно вычислительная техника и информационно-телекоммуникационные системы, развиваются стремительными темпами, все большее значение приобретает надежность защиты информации. Те методы защиты информации, которые еще вчера считались надежными, могут перестать быть таковыми в ближайшем будущем. Могут ли в принципе существовать системы защиты информации, которые гарантируют конфиденциальность передаваемой информации, даже если подслушиватель (злоумышленник) обладает неограниченными финансовыми, вычислительными и другими техническими ресурсами? Ответ на этот вопрос оказывается положительным. Самое удивительное, что такие системы возможны не только в принципе (теоретически или умозрительно), а уже существуют на сегодняшний день в мире реально в виде экспериментальных образцов, в том числе и в России.

Криптография (проще говоря, шифрование, или тайнопись) имеет, пожалуй, такую же длинную историю, как и само человечество, и исчисляется несколькими тысячелетиями. Еще древние египтяне, греки, римляне использовали, на тот момент времени, достаточно изощренные способы тайнописи. В России тайнопись (или, как ее называли, цифирь) также использовалась еще во времена удельных феодальных княжеств. В свое время, когда Петр I своим указам основал Российскую академию наук, он пригласил в Россию выдающихся математиков Леонарда Эйлера и Христиана Гольбаха, которые стали одними из первых российских академиков. Христиан Гольбах внес неоценимый вклад в развитие шифровального дела в России. Например, он сумел дешифровать («взломать») письма французского посланника в России, что в итоге существенно повлияло на внешнюю политику Российской империи.

Кстати, интересно отметить, что Леонардом Эйлером в то же время была доказана одна замечательная теорема из теории чисел, которая в тот момент представляла интерес лишь для узкого круга математиков. Не буду вдаваться в детали, но я упомянул об этом специально. Удивительным фактом является то, что защита информации в современных Интернет — технологиях основана на данной теореме. Данная

теорема работает когда вы осуществляете банковские трансферты, оплачиваете счета со своей банковской карты, делаете покупки через Интернет-магазин и т. д. Миллионы людей пользуются этим каждый день, даже не подозревая о том, что основы этого заложены почти три столетия назад. Не будь этого, мы бы были лишены многих удобств. На современном языке это называется шифрованием с открытым ключом, и ученые додумались до того, как можно это использовать, лишь в семидесятых годах двадцатого столетия. Это один из ярких примеров того, что не бывает бесполезных фундаментальных знаний, и собираются они по крупицам.

На чем же зиждется наша психологическая уверенность и спокойствие, например, в сохранности наших денег при переводе со счета на счет, или оплате покупок, или конфиденциальности нашей личной переписки по электронной почте? Это основано на доверии к профессиональной квалификации ученых, разрабатывающих системы защиты информации. Но тогда возникает вполне законный вопрос, почему сами ученые уверены в надежности своих систем шифрования. Касательно систем шифрования с открытым ключом такая уверенность базируется на том, что в результате долгих поисков ученым пока не удалось найти эффективных и быстрых методов «взлома» таких систем. Однако даже в этом случае никто не гарантирует, что появится какой-нибудь гений-математик, который создаст быструю «дешифрующую программу».

Возникает законный вопрос, а могут ли существовать такие шифры, которые невозможно «взломать» в принципе? Оказывается, что существуют, и называются они шифрами с одноразовыми ключами.

Прежде чем двигаться дальше, кратко коснемся истории вопроса.

Впервые строгое обоснование того факта, что системы шифрования с одноразовыми ключами являются абсолютно стойкими, было получено в работе Владимира Александровича Котельникова. Эта работа была закончена за несколько дней до начала великой отечественной войны, 18 июня 1941 г., и вошла в один из закрытых отчетов (Отчет 18 июня 1941 г. «Основные положения автоматической шифровки»). Впервые в широкой печати работа публикуется в настоящем сборнике.

Параллельно и независимо вопросы теоретической стойкости шифров изучались Клодом Шенноном (C. E. Shannon). Результаты этих исследований были первоначально представлены в закрытом отчете «A Mathematical Theory of Cryptography», датированным 1 сентября 1946 г. После окончания войны данный доклад был рассекречен (здесь имеет смысл упомянуть высказывание одного из основателей криптографии с открытым ключом У. Диффи W. Diffie, по мнению которого, возможно, работа К. Шеннона была рассекречена ошибочно, см. предисловие к монографии B. Schneier «Applied Cryptography», John Wiley & Sons, Inc., 1996) и опубликован в виде статьи «Communication Theory of Secrecy Systems» в журнале Bell System Technical Journal в 1949 г., которая стала широко известным классическим трудом по теоретической криптографии.

Идея, очень близкая режиму шифрования с одноразовым блокнотом, возникла еще в работе Вернама (G. S. Vernam, «Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communication», опубликованной в J. Amer. Inst. Elect. Eng., 55, 109 (1926)). В этой же работе было утверждение, правда без каких бы то ни было математических обоснований, о том, что шифры с «бегущим» случайным ключом (running key) будут абсолютно недешифруемыми. Приведем высказывание из этой работы «If, now, instead of using English words or sentences, we employ a key composed of letters selected absolutely at random, a cipher system is produced which is absolutely unbreakable.»

Cipher Printing Telegraph Systems

For Secret Wire and Radio Telegraphic Communications

BY G. S. VERNAM[1]

Associate, A. I. E. E.

Synopsis.—This paper describes a printing telegraph cipher system developed during the World War for the use of the Signal Corps, U. S. Army. This system is so designed that the messages are in secret form from the time they leave the sender until they are deciphered automatically at the office of the addressee. If copied while en route, the messages cannot be deciphered by an enemy, even though he has full knowledge of the methods and apparatus used. The operation of the equipment is described, as well as the method of using it for sending messages by wire, mail or radio.

The paper also discusses the practical impossibility of preventing the copying of messages, as by wire tapping, and the relative advantages of various codes and ciphers as regards speed, accuracy and the secrecy of their messages.

* * * * *

Introduction

THE purpose of this paper is to discuss briefly certain methods for obtaining secrecy in connection with messages sent by wire or radio telegraphy, and to describe in particular printing telegraph cipher systems that were developed for this purpose during the World War.

The desirability of obtaining secrecy in telegraphic communications and the possible advantages of a system that would be capable of sending messages in such form as to be entirely secret, and which at the same time, would be more rapid and accurate than the codes and ciphers ordinarily used, were brought out in conversations with officers of the Signal Corps, U. S. Army. Those discussions made it evident to the engineers of the Bell System that it would be very helpful if the well-known automatic features of the printing telegraph art could be made available for enciphering and deciphering telegraph messages, and could at the same time be made practical for use under service conditions.

The engineers recognized that printing telegraphs[2] were rapid and accurate, but were not secret except to the extent that their signals could not be read from a telegraph sounder. With the general requirements for secrecy systems in mind, studies were made of printing telegraph systems to determine how their messages could be made secret. The result of this work was the development of a cipher system that is capable of rendering messages entirely secret, is rapid and accurate, and is practical to use.

This "Cipher Printing Telegraph System" was called to the attention of the Signal Corps. The Signal Corps became very much interested, tested the secrecy of communications handled by the system and tried it out between New York and Washington. This trial proved that the system could be successfully used to send messages secretly and at a speed many times faster than by methods previously in use.[3]

Each message is automatically enciphered at the sending station and deciphered in the same manner at the receiving station. The method of ciphering will be described later in this paper and is such that under certain conditions of use, the messages are rendered entirely secret, and are impossible to analyze without the key, even if it is assumed that the enemy can capture a machine, learn its method of operation in all details, and intercept a large number of messages.

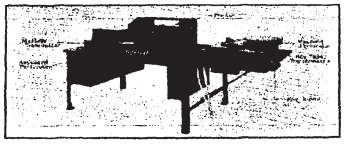

Fig. 1.—Cipher Printing Telegraph Machine

Flexibility of System

This method of ciphering can be used with machines of various types. The electrically-driven machine shown in Fig. 1 was developed during the war particularly for the Signal Corps, U. S. Army. In order to save time in production, standard printing telegraph parts were used wherever possible with the result that this machine has the appearance of a "start-stop" printing telegraph set with some additional units mounted on a shelf at the right end of the table. This type of cipher set is particularly suitable for handling large amounts of traffic at high speed.

1. Engineer, Dept. Development and Research, Am. Tel. & Tel. Co.

2. See John H. Bell, "Printing Telegraph Systems," Trans. A. I. E. E. for 1920, Vol. XXXIX, Part 1, p. 167, and A. H. Reiber, "Printing Telegraph Systems Applied to Message Traffic Handling," Trans. A. I. E. E. for 1922, Vol. XLI, p. 30.

To be presented at the Midwinter Convention of the A. I. E. E., New York, Feb. 3-11, 1926.

3. Note: See page 140, "Report of the Chief Signal Officer to the Secretary of War" for the year ending June 30, 1919.

Благодаря исследованиям В. А. Котельникова и Клода Шеннона возникло четкое и строгое понимание того, каким условиям должен удовлетворять абсолютно стойкий шифр.

Неформально шифр является абсолютно стойким, если

1) Ключ секретен — известен только легитимным образом.
2) Длина ключа в битах не меньше длины сообщения.

3) Ключ случаен.

4) Ключ используется только один раз.

В этом случае зашифрованное сообщение статистически независимо от исходного сообщения.

Принципиальная проблема при реализации криптосистем с одноразовыми ключами состоит в передаче (распространении) секретных ключей между пространственно удаленными легитимными пользователями.

Ключ между удаленными пользователями должен передаваться при помощи какого-то физического сигнала через открытый канал связи (открытый означает доступный для подслушивания третьими лицами). Если оставаться в рамках классической физики, то в этом случае не существует запретов на уровне законов классической физики на измерение передаваемого сигнала без его возмущения. Поэтому принципиально невозможно гарантировать секретность ключа при его распространении.

Если не вдаваться в детали, то системы шифрования с одноразовыми ключами выглядят примерно так. Стороны, обменивающиеся информацией, должны иметь общий и известный только им секретный ключ. Ключ это случайный набор 0 и 1. Далее одна из сторон шифрует на этом ключе свое сообщение и передает другой стороне. Вторая сторона, зная ключ, может его расшифровывать. Если стороны хотят передать следующее сообщение, то они опять должны создать другой ключ, известный только им. Короче говоря, для каждого сообщения требуется новый ключ. Если стороны играют по таким правилам, то их сообщения никто и никогда не сможет дешифровать, даже если злоумышленник имеет любые технические и финансовые возможности. Такие системы являются абсолютно секретными.

Казалось бы все очень здорово, кроме одного. Сам ключ надо тоже как-то передавать между сторонами, да еще при этом гарантировать, что при передаче никто не будет его знать. Казалось бы, возникает замкнутый круг. Однако — нет, выход из этой ситуации есть.

Как ни удивительно это звучит, но оказывается, что можно передавать ключи по открытым, например, оптоволоконным линиям связи и быть уверенным, что никакой злоумышленник не будет их знать. Технология, которая позволяет это делать, называется квантовой криптографией. На сегодняшний день квантовая криптография является достаточно развитой областью и представляет собой один из разделов более широкого научного направления, называемого квантовой информатикой.

Квантовая криптография, или более точно, квантовое распределение (передача) секретных ключей основана на фундаментальных законах природы — законах квантовой механики. Секретность ключей в квантовой криптографии гарантируется не техническими ухищрениями, а законами природы, которые никто не в силах изменить или игнорировать.

Первая идея в этой сфере появилась в 1973 г., ее высказал Стивен Визнер. Ученый изложил идею «квантовых денег», которые никто и никогда не сможет подделать. Визнер задался вопросом, а нельзя ли сделать так, чтобы подобные преступления в принципе невозможно было совершить — не зависимо от того, какими техническими возможностями обладает злоумышленник. Однако свою работу ему не удалось опубликовать: все научные журналы, как один, сочли идеи ученого, мягко говоря, фантазией. Лишь спустя 13 лет, в 1984 г. сотрудник знаменитой компании IBM Чарльз Беннет вместе с канадским математиком Жиллем Брассаром предложили конкретную схему передачи секретных ключей при помощи квантовых состояний — одиночных фотонов. С этого момента квантовая криптография стала развиваться бурными темпами.

В чем же суть квантовой криптографии?

Несмотря на достаточно высокий уровень абстракции понятий в этой области и множество сложных технических подробностей, базовая идея на удивление крайне проста. Если ключ передается при помощи классического сигнала (электромагнитных волн — света), то этот сигнал (а значит и ключ) можно измерить. При этом с самим сигналом ничего не произойдет. По существу, это происходит, когда множество людей слушают одновременно одну и ту же радиостанцию. Их приемники обрабатывают (измеряют) один и тот же сигнал, они друг другу никак не мешают, и даже не знают, что кто-то еще слушает тот же сигнал. Свет состоит из множества неделимых квантов — фотонов. Чем больше фотонов, тем выше мощность сигнала. При подслушивании злоумышленник отбирает часть фотонов. Если сигнал интенсивный, то уход части фотонов практически невозможно заметить. Мы этого и не замечаем, когда кто-то еще включает свой приемник. Теперь представим себе, что произойдет, если мощность сигнала столь мала, что в нем присутствует лишь один фотон. Тогда попытка «послушать» сигнал приведет к потере фотона, что сразу станет известно. Здесь я намеренно для краткости несколько огрубляю ситуацию.

Квантовая криптография для передачи ключей (фактически 0 и 1) использует однофотонные сигналы (точнее, квазиоднофотонные) — сильно ослабленное лазерное излучение. Фундаментальные законы квантовой механики диктуют нам, что однофотонное квантовое состояние не может быть измерено без искажения. Если злоумышленник пытается узнать, что передается — 0 или 1, то он неизбежно «портит» сигнал, и это сразу становится известно. Любое вторжение в канал связи злоумышленника сразу детектируется. Нельзя подслушивать и остаться незаметным. Это уже хорошо. Однако это не все. Квантовая криптография дает возможность не только детектировать попытки подслушивания, но и быть уверенным в том, что ключи будут секретными. Однако для детальных объяснений этого обстоятельства пришлось бы прибегнуть к математическим и техническим деталям.

Уже созданы экспериментальные образцы систем квантовой криптографии для передачи ключей, как по оптоволоконным линиям связи, так и через открытое пространство. Сделаны первые эксперименты по встраиванию таких систем в существующие оптоволоконные телекоммуникационные сети. Такие работы ведутся практически во всех ведущих телекоммуникационных компаниях и национальных лабораториях: IBM, NEC, Mitsubishi, Toshiba, Hewlett-Packard, BBN Technologies, QinetiQ. Такие работы финансируются как государственными организациями, так и частными фирмами. Например, в США работы финансируются агентством перспективных оборонных разработок (DARPA). Кстати, нужно отметить, что данное агентство в свое время финансировало разработки по распределенным сетям, что впоследствии привело к сознанию Интернета.

Рекорд длины оптоволоконной линии в системе квантовой криптографии на сегодняшний день составляет 150 км, а при передаче ключей в однофотонном режиме через открытое пространство достигнуты фантастические результаты. Осуществлена передача ключей на расстоянии 144 км по открытому пространству между двумя островами в Атлантическом океане. В этом эксперименте было задействовано множество организаций из стран Европейского союза. Целью данных работ является передача ключей на большие расстояния через низкоорбитальные спутники.

Грубо говоря, система связи — это два «ящика», соединенные между собой, например, оптоволоконным кабелем. При этом кабель может быть незащищенным, проходить по открытому пространству. Тем не менее, по ней гарантированно можно передавать конфиденциальную информацию.

Нужно отметить следующее. На сегодняшний день данные системы находятся на пределе возможностей существующих технологий. И работа с ними представляет собой тонкий эксперимент. И даже, несмотря на объявленные первые коммерческие изделия, потребуется еще немало усилий и времени на совершенствование систем квантовой криптографии, чтобы довести их до степени легкости в обращении, скажем, как с современным телевизором. По оценкам экспертов из NEC и Mitsubishi потребуется еще 3–4 года для того, чтобы такие системы превратились в действительно рыночный продукт. При этом не нужно забывать, что системы квантовой криптографии представляют собой прежде всего криптографический продукт, к которому предъявляется масса специфических требований. Такие системы представляют собой интегрированный продукт, их разработка требует привлечения и четкой координации действий высококлассных специалистов из разных областей: квантовой оптики, математической криптографии, программирования, электроники, волоконной оптики. На Западе финансирование работ на стадии выполнения опытно-конструкторских разработок проводится не только государственными структурами, но и с привлечением

внебюджетных средств. Здесь, как показывает зарубежный опыт, ведущую роль могут сыграть крупные телекоммуникационные компании.

За сравнительно небольшой срок квантовая криптография прошла путь от абстрактных идей, изначально понятных лишь узкому кругу специалистов, до работающих экспериментальных изделий.

В заключение стоит отметить, что появление новых направлений в области конфиденциальной передачи информации является естественным логическим развитием идей, возникших в работах выдающихся ученых — основателей данной области Владимира Александровича Котельникова и Клода Шеннона.