Последние достижения российской криптографии

в продуктах и задачах

Российская криптография отсчитывает свою историю с далеких царских времен: с так называемых черных кабинетов и цифирных комитетов. С тех пор в нашей стране сформировалась сильная криптографическая школа, разработано множество методов защиты информации, открылись профильные кафедры в технических и математических вузах. Сегодня отечественная криптография движется в русле общемировых тенденций – вплоть до создания собственных постквантовых алгоритмов шифрования. Рассмотрим текущее состояние российской криптографии, ее ключевые разработки и достижения, а также основные задачи, которые сегодня стоят перед отраслью.

Кратко о состоянии российской криптографии

Криптография – это не только наука о расчетах и цифрах. Это стратегическая отрасль, влияющая на жизнь государства, бизнеса, обычных людей. Криптографические методы и инструменты защищают коммерческую, банковскую и врачебную тайну, конфиденциальные персональные данные, оперативные военные и дипломатические сведения и все коммуникации в интернете.

Направления российской криптографии и госрегулирование

Криптографическая работа в России развивается по четырем ключевым направлениям. Каждое из них регулируется государственными стандартами.

ГОСТ 34.10-2012 и ГОСТ 34.10-2018. Цифровая подпись. Эти стандарты содержат алгоритмы формирования и проверки электронной подписи. Они основаны на современной эллиптической криптографии и функции хеширования. Электронная подпись гарантирует подлинность и целостность цифровых документов.

ГОСТ 34.11-2018. Хеш-функция. Здесь регламентирован принятый в России алгоритм вычисления хеш-функции со звучным названием «Стрибог». Он принимает сообщения произвольной длины, дробит их на блоки размером 512 бит и преобразует в хеш-код, который может быть асимметричным.

ГОСТ 34.12-2018. Шифры. В этом нормативе описываются российские блочные шифры, такие как алгоритмы «Магма», «Кузнечик» и др.

ГОСТ 34.13-2018. Режимы работы шифров. Документ описывает методы преобразования блоков открытого текста в шифротекст и наоборот. В стандарт включены следующие режимы работы с блочными шифрами:

- простая замена;
- гаммирование;
- гаммирование с обратной связью – по выходу и шифротексту;
- простая замена с зацеплением;
- выработка имитовставки.

Разработкой и актуализацией нормативных актов в криптографической сфере занимается преимущественно Центр информационной безопасности ФСБ (ЦИБ ФСБ), известный как «18-й центр». Его основные функции:

- разработка и обновление нормативных актов в сфере криптографии;
- утверждение ГОСТов в Минцифре и их выпуск;
- определение стандартов шифрования, длины ключей и других технических аспектов.

На основе этих нормативов коммерческие разработчики, такие как «КриптоПро» или «Контур», создают свои практические реализации шифрования.

Отдельное подразделение «18-го центра» занимается лицензированием и сертификацией средств криптозащиты. Важно отметить, что все ввозимое из-за рубежа оборудование с технологиями шифрования подлежит обязательной государственной сертификации.

ЦИБ ФСБ не действует в одиночку при регулировании криптографической отрасли. Вопреки распространенному мнению, центр активно сотрудничает с бизнесом и разработчиками, учитывая их опыт и экспертизу. Например, среди консультантов «18-го центра» – компания «КриптоПро», специалисты которой разработали ГОСТ 34.10-2012 по цифровой подписи, а также группа «Криптонит». Последняя выступает локомотивом в создании российских стандартов постквантовой криптографии.

Основные потребители, разработки и продукты отечественной криптографии

Описанные ГОСТы должны обеспечить надежную защиту информации для всех, кто пользуется отечественной криптографией.

В первую очередь это касается организаций и ресурсов, применяющих электронные подписи и системы документооборота. К ним относятся портал «Госуслуги», Федеральная налоговая служба, электронные тендерные площадки и др.

Отдельная группа пользователей – промышленные предприятия. У некоторых добывающих холдингов есть свои тендерные площадки с использованием технологии цифровой подписи.

Стоит отметить и крупные коммерческие банки, которые все чаще переходят на SSL-соединения на базе российских алгоритмов шифрования.

Отечественную криптографию активно применяют в госсекторе. В 2020 г. государственные информационные системы начали переходить на российские средства шифрования. В эксперименте приняли участие ГИС ЖКХ, Единый реестр российского ПО, Единый портал государственных и муниципальных услуг (ЕПГУ) и Единая государственная информационная система социального обеспечения (ЕГИССО). Сейчас госструктуры продолжают внедрять отечественную криптографию.

Какие российские криптографические разработки доступны пользователям? Среди ключевых игроков на этом рынке – компании «КриптоПро», «Актив», ЦБИ, «Криптософт», «Код Безопасности», «Элвис Плюс», «Аладдин», «ИнфоТеКС» и др.

Популярное решение – программно-аппаратный комплекс «КриптоПро DSS». Он централизованно хранит закрытые ключи и удаленно формирует электронные подписи. Еще одна разработка – облачная подпись «КриптоПро». С ней можно подписывать документы со смартфона через специальное приложение. «КриптоПро DSS» широко применяют в интернет-банкинге, электронной коммерции, документообороте и на порталах госуслуг.

Востребованы на рынке и российские сетевые шлюзы безопасности, например, ViPNet Coordinator HW4 разработки «ИнфоТеКС». Такие решения используются для передачи данных между защищенными сегментами виртуальной сети и фильтрации IP-трафика. Спрос на подобное ПО во многом объясняется ростом популярности удаленной работы и необходимостью обеспечить безопасный обмен информацией между сотрудниками.

Еще один важный сегмент отечественного рынка – решения для создания квантовых криптографических сетей. В этом контексте можно вспомнить систему выработки и распределения ключей ViPNet Quantum Trusted System (ViPNet QTS) от того же «ИнфоТеКС» и ряд других продуктов.

Отечественные разработчики освоили и нишу защищенных операционных систем. Так, компания «Криптософт» создала систему QP ОС, которая получила сертификацию ФСБ России для обработки гостайны, вплоть до уровня «совершенно секретно».

Отдельные российские криптографические разработки предназначены для защиты мобильных соединений. Пример такого продукта – клиентское приложение «Континент АП/ZTN» (мобильный) от компании «Код Безопасности». Оно обеспечивает защищенный доступ в корпоративную сеть с удаленных планшетов и смартфонов сотрудников.

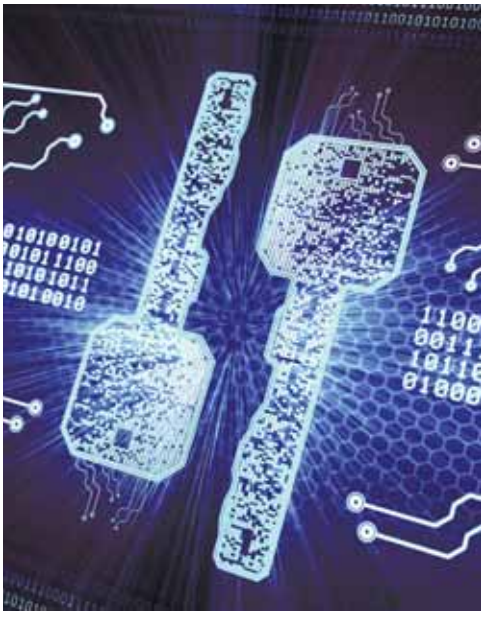
Таким образом, наиболее активно отечественная криптография развивается в двух направлениях: защищенные соединения и электронные подписи. В сфере хранения данных криптографические инструменты используются реже.

Технологические и фундаментальные достижения российской криптографии

Сегодня изобрести принципиально новое в шифровании и дешифровании информации сложно. Большинство алгоритмов в мире основано на одних и тех же принципах, поэтому нельзя говорить о специфике российской криптографии. Все сводится к режимам работы шифров, описанным в ГОСТ 34.13-2018. Шифрование делится на раунды – циклы обработки данных в блочном алгоритме. Проще говоря, это количество раз, когда шифротекст шифрует сам себя.

И все же криптография продолжает развиваться. Четыре основных фактора стимулируют прогресс российской криптографической науки и технологий:

- цифровизация ускоряет перевод информации с бумажных носителей в цифровой формат. Это повышает спрос на современные методы защиты данных;
- курс на импортозамещение в текущих экономических условиях вынуждает многие организации и даже целые отрасли переходить на российскую криптографию. К этому подталкивают и требования законодательства;
- рост вычислительной мощности компьютеров заставляет работать над повышением криптостойкости шифров и увеличением длины ключей;
- развитие квантовых компьютеров требует создания криптографических алгоритмов и технологий, устойчивых к атакам с помощью этих вычислительных машин будущего.



Источник: https://avatars.dzeninfra.ru/

Российская криптография следует мировым тенденциям. Она постепенно переходит от алгоритмов на простых числах, таких как RSA, к работе с эллиптическими кривыми. Алгоритмы на простых числах достигли предела эффективности из-за роста вычислительных мощностей компьютеров. Теперь они требуют слишком длинных ключей. Например, при шифровании с помощью RSA для защиты цифровой подписи в 256 бит рекомендуется использовать ключ длиной минимум 15360 бит. В системах на основе эллиптических кривых для обеспечения криптостойкости уровня 256 бит симметричного шифрования достаточна длина ключа от 521 бит.

Набирает обороты развитие технологий постквантовой криптографии. С этим направлением связаны основные прорывы последних лет. Причина понятна: в будущем классические криптографические системы не смогут противостоять атакам мощных квантовых компьютеров. К слову, Россия входит в число лидеров в сфере квантовых вычислений. В сентябре 2024 г. в стране был создан 50-кубитный ионный квантовый компьютер. Это самый мощный квантовый компьютер в России на сегодняшний день. Он входит в шестерку мировых лидеров среди аналогичных систем.

Вернемся к криптографии. В России разработка стандартов постквантовой криптографии началась в 2019 г. Процесс курирует Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) «Росстандарта». Как и «18-й центр» с Минцифрой, ТК 26 активно привлекает экспертов от бизнеса и разработчиков.

Группа «Криптонит» на протяжении пяти лет занимается созданием постквантового асимметричного алгоритма инкапсуляции ключа электронной подписи «Шиповник». В 2022 г. разработчик предоставил ТК 26 первый пакет документов по этой цифровой подписи.

Как отмечают в «Криптоните», теоретическая стойкость «Шиповника» к квантовой атаке составляет 2^170 битовых операций. Таким образом, алгоритм будет сложно взломать даже при помощи компьютеров будущего с миллиардами рабочих кубитов, которые пока остаются чем-то из области научной фантастики.

Высокая стойкость «Шиповника» достигается методикой декодирования случайного линейного кода. Другое преимущество алгоритма – сравнительно небольшой размер открытого ключа. Это позволяет уменьшить трафик и ускорить обмен ключами.

В отличие от упомянутых компьютеров с миллиардами рабочих кубитов, «Шиповник» уже стал рабочей технологией настоящего.

В 2023 г. компания КУАПП (часть Российского квантового центра) создала открытую реализацию этого алгоритма. Код написан на языке C, оптимизирован под наборы команд SSE4.1, SSE2 и MMX и опубликован на GitHub. Как показали тесты на Intel Core i7-8700, на выработку ключевой пары уходит 3 мс, а на подпись одного сообщения – 848 миллисекунды. Проверка подписи занимает всего 11 мс.

Еще одним успехом стало разработанное той же компанией расширение для браузера Chrome, которое позволяет защитить интернет-соединение постквантовыми криптографическими алгоритмами. Сегодня на базе расширения создается новый продукт – квантовоустойчивый TLS-шлюз.

Вместо заключения: ключевые вызовы и зоны роста российской криптографии

Успехи в отрасли не означают отсутствия проблем и зон роста. Основной курс для российской криптографии сегодня – ускорить обновление нормативов и стандартов в соответствии с современными реалиями.

Пример: ГОСТ по цифровой подписи разработали в 2012 г., но он вошел в практику только в 2018-м. Шесть лет потребовалось для корректировки и адаптации стандарта. Кроме того, решали вопрос – делать форсированный или плавный переход с ГОСТа 2001 г.

Другой вызов – исправить ситуацию с сертификацией в криптографии.

Раньше в России работало много мелких и средних коммерческих центров сертификации (удостоверяющих центров). Подтвердить подлинность ключей шифрования было относительно просто. Однако после серии реформ был установлен минимальный размер собственных средств удостоверяющих центров – 2 млрд руб. В результате осталось несколько наиболее крупных учреждений.

Еще одна важная задача – упростить процедуры ввоза зарубежного оборудования и компонентов. Важность импортозамещения в криптографии очевидна. Но зарубежные устройства часто необходимы российским специалистам для исследований. Законодательство же запрещает ввозить в страну подобное оборудование с длиной ключа более 64 бит. Из-за этого криптоаналитики-энтузиасты не могут заказать нужную аппаратуру для анализа применяемых в ней технологий шифрования.

Такой порядок установлен из соображений безопасности, однако в то же время в России почти не ограничен ввоз смартфонов, планшетов и других гаджетов, на которые можно установить любые мессенджеры с поточным шифрованием. При этом нельзя заказать цифровую или аналоговую рацию с длиной ключа всего на 4 бита больше норматива.

Отечественная криптография не отстает от общемировых стандартов в части фундаментальной науки и развития ключевых технологий шифрования и дешифрования информации. ■

Константин ЛАРИН,
руководитель направления «Киберразведка» компании «Бастион»