УДК 004.912

А. С. Евдокимов[*]

РАЗРАБОТКА СИСТЕМЫ ХРАНЕНИЯ ДЕПОНИРОВАННЫХ КЛЮЧЕЙ ШИФРОВАНИЯ

В последние годы все большую популярность набирают различные мессенджеры, использующие сквозное шифрование и криптовалюты, основанные на технологии блокчейна.

Использование в мессенджерах стойких алгоритмов шифрования позволило бы обеспечить защиту тайны личной жизни граждан, но, в то же время это неизбежно создает угрозу национальной безопасности, так как ими могут воспользоваться террористы, экстремисты и другие преступники.

Криптовалюты, по сути своей, являются децентрализованными. В случае потери доступа к банковскому счету, пользователь банка может написать запрос в филиал, подтвердить свою личность, после чего, банк восстанавливает доступ к счету. В случае криптовалют, при потере доступа к кошельку, средства, содержащиеся на нем, будут утеряны навсегда. Таким образом, пользователь сам заинтересован в раздельном сохранении теней секрета, чтобы не потерять доступ к криптовалюте, к примеру, при повреждении оборудования, на котором хранится ключ.

Пороговая схема разделения секрета Шамира позволяет обеспечить безопасное хранение ключей шифрования [1]. Если какой-либо центр хранения потеряет ключ, или будет взломан, это не приведет к негативным последствиям для пользователей. Данная идея может позволить вывести криптовалюты из теневой части рынка, введя их в правовое поле. Необходимо лишь создать соответствующие законы, которые не позволят использовать криптовалюты, без выдачи теней государственным центрам хранения. Так же, данная схема может использоваться для «холодного» хранения теней на внешних носителях данных, таких как оптические диски. Это позволит восстановить секрет даже при поломке или утере части накопителей.

---

[*] Работа выполнена под руководством канд. техн. наук, доцента кафедры «Информационные системы и защита информации», ФГБОУ ВО «ТГТУ» В. А. Гриднева.

Депонирование ключей – это предоставление ключей шифрования или их частей (теней), третьей стороне. Депонирование необходимо для обеспечения баланса между тайной личной переписки граждан и полной криптоанархией, позволяющей криминальным элементам безопасно общаться по каналам связи, используя стойкое шифрование, таким образом, угрожая интересам национальной безопасности.

В США были попытки депонировать ключ, используемый для шифрования данных, передаваемых по каналам *Integrated Services Digital Network*, факсам, и любой связи того времени. Для этого даже был разработан стандарт, который называется *Escrowed Encryption Standard.* Реализованы эти попытки были при помощи микросхемы *Clipper*, занимающейся шифрованием, и расшифрованием данных. Так же, агентство национальной безопасности США (*NSA*) разработало дисциплину раскрытия уникального ключа микросхемы. Микросхема была разработана таким образом, чтобы было невозможно считать с нее данные по каналам побочных электромагнитных излучений и наводок (название технологии – *TEMPEST*) [4].

Проектируемая система должна иметь как можно большое число ЗЦОДов (защищенных центрах обработки данных) и, соответственно, большое число теней. Структурная схема проектируемой системы представлена на рис. 1.

Перейдем к конкретным примерам схем, которые могли бы помочь пользователям мессенджеров сохранять тайну личной переписки при обеспечении национальной безопасности, а владельцам криптовалютных кошельков обеспечить сохранность своих средств при утере ключа. Основная идея состоит в том, что в геометрии двумерного пространства, по двум точкам можно построить прямую, по трем параболу, по четырем кубическую параболу, и так далее, повышая степени.

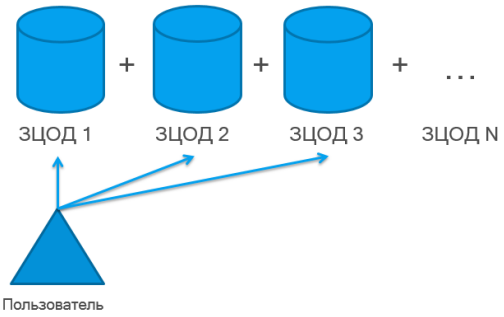

Рис. 1. Схема системы хранения депонированных ключей

Иными словами, для задания степенного многочлена k требуется число точек, большее на единицу, то есть $k + 1$.

Для того чтобы восстановить ключ шифрования можно было бы только по определенному числу долей (теней) n, его сворачивают в многочлен степени $n + 1$, над конечным полем G. Таким образом, чтобы восстановить секрет, необходимо будет собрать вместе n теней, а значит и значений многочлена в определенных точках. Если при невосстановлении секрета не удастся собрать необходимое число теней, то точек будет недостаточно, и восстановление секрета будет невозможно. В теории, число точек многочлена не ограничено, но ввиду конечности памяти ЭВМ и разумной достаточности оно всегда ограничено размерностью поля Галуа порядка G.

Попробуем описать алгоритм более кратко. Допустим, мы имеем поле Галуа G. Возьмем n случайных элементов данного поля, обладающих свойством дискретности, и не попадающих в ноль [2].

Выберем произвольный набор элементов t поля Галуа G. Число элементов набора будет необходимым для восстановления секрета. Именно из этого множества чисел будет составляться искомый пороговый многочлен над полем Галуа, степени $t - 1$, где $1 < t \leq n$.

Допустим, искомый многочлен получен, теперь найдем его значения (x, y) в n точках. Остается лишь распределить полученные значения каждому из ЗЦОД.

Заметим, что через две точки всегда можно провести неограниченное число квадратичных парабол (рис. 1). Но, чтобы выбрать из них нужную параболу понадобится третья точка [3].

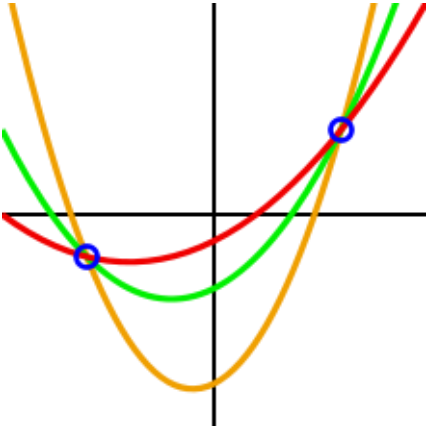

Рис. 1. Квадратичные параболы

Восстановление секрета не составит труда, его можно произвести с помощью любой формулы интерполяции, например, при помощи наиболее популярной формулы Ньютона, Бесселя или интерполяционного полинома Лагранжа [3].

Основное достоинство пороговой схемы Шамира – масштабируемость. Если возникнет необходимость добавить еще один или несколько ЗЦОД, то нам будет необходимо просто вычислить значение полинома в новой точке и добавить егозначение к уже созданным ранее несекретным элементам. Если же, наоборот, какой-либо ЗЦОД исключен, то это не приводит к необходимости генерации нового набора точек. По сути, это просто ослабит схему, переведя ее из состояния из (n, t)-пороговой в (n – 1, t – 1)-пороговую.

Решение проблемы депонирования ключей – сложная задача, потому что необходимо сохранять секретность ключевых данных, чтобы обеспечить безопасность хранения криптовалюты и тайну личной жизни.

Предложенная система позволяет пользователю безопасно хранить разделенный секрет в разных защищенных центрах обработки данных (ЗЦОД), что позволит восстановить его в случае потери доступа к тени, или в случае атаки на ЗЦОД.

Еще в 1997 году известнейший криптограф Б. Шнайер четко указал на то, что государственные системы шифрования не получат широкого распространения в будущем [1]. Тем не менее, депонирование ключей возможно осуществить, если оно будет выгодно самому пользователю.

Стоит добавить, что весь информационный обмен между субъектами взаимоотношений, приведенных в примерах использования депонирования ключей, может быть реализован в электронном виде, что неизбежно потребует принятия мер по обеспечению безопасности информации, передаваемой по каналам связи.

Актуальным остается вопрос защиты целостности и корректности депонируемых теней. Необходимо предусмотреть защиту депонируемых теней от умышленного или случайного искажения, а также возможность обнаружить любого недобросовестного участника схемы. Ведь любой из участников схемы может попытаться помешать успешному восстановлению ключа. Например, пользователь может после депонирования ключа шифрования использовать совсем другой ключ. И когда, после соблюдения всех предусмотренных формальностей, ключ не восстановится, заявить, что он не знает причину, по которой это могло произойти.

Список литературы

1. Шнайер, Б. Разделение секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = *Applied Cryptography*. *Protocols*, *Algorithms and Source Codein C* / Б. Шнайер. – М. : Триумф, 2002. – С. 93 – 96. – 816 с.

2. Шнайер, Б. Алгоритмы разделения секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Codein C / Б. Шнайер. – М. : Триумф, 2002. – С. 588 – 591. – 816 с.

3. Блэкли, Д. Обобщенные идеальные схемы, разделяющие секрет, и матроиды / Д. Блэкли, Г. А. Кабатянский // Проблемы передачи информации. – 1997. – Т. 33, вып. 3. – С. 102 – 110.

4. Шенец, Н. Н. Об идеальных модулярных схемах разделения секрета в кольцах многочленов от нескольких переменных / Н. Н. Шенец // Международный конгресс по информатике: информационные системы и технологии: материалы международного научного конгресса 31 окт. – Минск : БГУ, 2011. – Т. 1. Статьи факультета прикладной математики и информатики. – С. 169 – 173.

Кафедра «Информационные системы и защита информации»
ФГБОУ ВО «ТГТУ»