XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VI: С.196-197, 2003.

УДК 621.391.15

Л.М. Курочкин (4 курс каф. РВиКС), Е.А. Крук, д.т.н. проф.

ПРОТОКОЛ РАЗДЕЛЕНИЯ СЕКРЕТА НА БАЗЕ КОДА РИДА-СОЛОМОНА

Одна из областей криптологии – разделение секрета. Секретная информация (пароль доступа, ключ дешифрации) при разделении секрета распределяется между определенными лицами таким образом, чтобы в последствии эти лица смогли ее восстановить. Секрет распределяется дилером между участниками по определенному закону или, другими словами, по определенной схеме.

Схема разделения секрета на базе кодов исправляющих ошибки (код Рида-Соломона) обладает особыми свойствами, по сравнению, например, со схемой Шамира. Эта схема основана на свойствах кодовых конструкций (исправление ошибок).

Разделение секрета подразумевает участие нескольких лиц. Каждое лицо должно знать, как себя вести во время разделения секрета, во время восстановления секрета. Протокол разделения секрета определяет последовательность шагов, которые должны выполнить дилер и участники. В данной работе исследуется протокол разделения секрета на базе кода Рида-Соломона, разработанный Игорем Железняком.

Этот протокол состоит из двух фаз: фазы разделения секрета и фазы восстановления секрета. Основное внимание при построении протокола уделялось фазе разделения секрета, а точнее, той ее части, где происходит проверка долей секрета участниками. При построении протокола основной задачей являлось построение механизмов защиты от поведения дилера, направленного на срыв разделения/восстановления секрета.

Разделение Секрета применяется в случае, когда доступ к информации может получить только определённая группа пользователей. Например, существуют ситуации, когда сетевой ресурс должна получить строго определенная группа лиц (секретом является пароль доступа).

Целью работы являлись программная реализация и анализ протокола.

Результатом работы явилось: реализация протокола и предложение дополнительных требований, которые позволили повысить надёжность протокола.

Проведённый анализ протокола показал, что

- проверка $\sum_{i=1}^{d} M_i = \sum_{i=1}^{d} (K_i + S_i) \cdot H = (K + S) \cdot H \overset{?}{=} 0$ *(d – число участников),* проводимая участниками на фазе разделения секрета может не выполняться при корректном разделении секрета дилером. При этом восстановление секрета становится невозможным.

Для исправления этой ошибки в протокол введено дополнительное требование:

- длина кода, используемого в протоколе, должна быть кратна числу участников.

При разделении секрета участники могут получить априорной информации о секрете, что понижает стойкость протокола. Для исправления этой ситуации в протокол ввдено дополнительное требование:

- ненулевые позиции в проекциях A_i, K_i должны совпадать.

На стадии восстановления секрета недобросовестный участник может сорвать восстановление, отослав участникам восстановления неверную проекцию секрета. Во избежание этой ситуации предлагается:

- участникам восстановления не обмениваются проекциями и не восстанавливать секрет самостоятельно, а отсылать проекции дилеру, который и восстанавливает секрет, а в случае попытки срыва восстановления участником компрометирует его.

Программная реализация протокола с учётом выработанных предложений выполнена на VC++ 6.0. Протокол стал более надёжным, по сравнению с предыдущей версией.