Болотова Е.А., Титов С.С.

РАЗДЕЛЕНИЕ СЕКРЕТА И РЕШЕТКИ

Уральский государственный университет путей сообщения

В работе рассмотрены схемы разделения секрета, которые в общем случае являются совершенными, если при их реализации справедлив принцип «всё или ничего». Для линейных схем (реализуемых при помощи подпространств векторного пространства) этот принцип соответствует наличию определённых соотношений в решётке подпространств используемого в схеме векторного пространства. Эти соотношения накладываются на подрешётку, порождённую подпространствами, соотнесёнными с участниками и секретом. В общем случае для всей схемы разделения секрета с n участниками возникает задача построения подрешеток, соответствующих разрешенным и запрещенным множествам участников, представление этих подрешеток гомоморфными образами известных решеток, с последующей «сборкой» этих подрешеток в единую решетку, соответствующую схеме разделения секрета. При минимальном гомоморфизме существует возможность для неидеальности. Если добавить к этому отождествление элементов, то можно получить идеальность.

Основным инструментом для изучения свойств решеток является разбиение их на классы эквивалентности. Доказано, что решетка разбиений конечного множества не является модулярной. Доказано, что структура доступа, указанная в [13, пример 3 на с. 125] не допускает идеальной реализации. Данная структура доступа не соответствует матроиду и, следовательно, не допускает идеальной реализации по теореме Брикелла – Дэвенпорта [13]. Также доказано, что матроид Вамоса не является линейным, так как решетка его подпространств немодулярна. Таким образом, абстрактные свойства решеток «управляют» вопросами существования и реализации структур доступа в схемах разделения секрета. Так, для класса решеток в случае дистрибутивности имеем решетку, соответствующую принципу «Ничего». Рассмотрен самый свободный случай, то есть все остальные решетки этого типа с двумя участниками (V и W) и секретом U должны получаться из данной решетки посредством гомоморфизма. Рассмотрены смежные классы конгруэнции "≡", ядерной конгруэнции этого гомоморфизма. Так, $\{0, V \wedge W\}$ – ядерный идеал данного гомоморфизма, то есть смежный класс соответствующей конгруэнции, содержащий 0 этой решетки. Другой неодноэлементный смежный класс – это $\{U, V \vee (V \vee W)\}$, что вытекает из импликации $0 \equiv V \wedge W \Rightarrow U = 0 \vee U \equiv (V \wedge W) \vee U$.

Для линейных совершенных СРС характерен класс модулярных решеток. Для структуры доступа, реализованной в качестве примера в [13, с. 125] можно рассмотреть подрешетки, порожденные тремя участниками: L_0, L_i, L_j, где L_0 – пространство секрета, L_i, L_j – пространства i-го и j-го участника. Эти подрешетки являются гомоморфными образами свободной модулярной решетки с тремя образующими [1], реализующимися как решетка подпространств векторного пространства. Свободная модулярная решетка с тремя образующими конечна, а свободная модулярная решетка с четырьмя образующими уже бесконечна [5, 14]. Построенные диаграммы иллюстрируют реализацию процедуры построения под-

решеток соответствующих разрешенным и запрещенным множествам участников представляющих собой гомоморфные образы свободной модулярной решетки с тремя образующими. Таким образом, аппарат теории решеток полезен, востребован и применим не только в задачах разграничения доступа к информации, но и в задачах построения и изучения схем разделения секрета.

Авторы благодарят Н.А. Гайдамакина и В.А. Баранского за постановку задач и внимание к работе, а также А.С. Худеньких и ЕНТЦ ФГУП «НПП «Гамма» за поддержку.

Литература

1. Е.А. Аникина, Е.С. Худорожкова, С.С. Титов. Реализация свободных решеток в виде решеток подпространств в семимерном, восьмимерном и девятимерном векторных пространствах. Безопасность информационного пространства. Региональная науч.-практ. конференция. Екатеринбург, 2003.

2. Е.А. Аникина, Е.С. Воробьева, В.И. Гусева, С.С. Титов. Доверительные отношения и безопасность удаленного доступа в иерархических моделях. Информационная безопасность региона: Материалы Всерос. науч.-практ. конф., Челябинск, 7 окт. 2004 г./Под ред. А.А. Соловьева. Челябинск: ЧелГУ, 2005.

3. В.А. Баранский. Введение в общую алгебру и ее приложения. Екатеринбург. 1998.

4. Н.П. Варновский Математическая криптография. Несколько этюдов. Мат. конф. «Московский университет и развитие криптографии в России» (МГУ 17 – 18 октября 2002 г.).

5. Глухов М.М., Стеллецкий И.В., Фофанова Т.С. Структуры. «Итоги науки. Алгебра. Геометрия. Топология. 1968», М., 1970.

6. П.Н. Девянин. Модели безопасности компьютерных систем. М.:Academia. 2005.

7. Теоретические основы компьютерной безопасности. Учеб. пособие для ВУЗов/П.Н. Девянин, О.О. Михальский, А.С. Першаков и др. М.: Радио и связь 2000.

8. Д.П. Зегжда, А.М. Ивашко Технология создания безопасных систем обработки информации на основе отечественной защищенной операционной системы. Проблемы информационной безопасности. Комп. системы. - 1999. №2.

9. В. Липский Комбинаторика для программистов. Москва, 1988.

10. Р. Сикорский Булевы алгебры. М.: Мир, 1969 (пер. с англ).

11. В.М. Фомичев Дискретная математика и криптология. Курс лекций. Москва, 2003 г. 397 с.

12. А.Ю. Щербаков. Введение в теорию и практику компьютерной безопасности. М.: изд. Молгачева С. В. 2001. - 352 с.

13. Введение в криптографию / Под ред. В.В. Ященко. СПб.: Питер, 2001.

14. Скорняков Л.А. Элементы теории структур. М.: Наука, 1970. 148 с.