Секция «Вычислительная математика и кибернетика»

Моделирование и исследование пороговой схемы разделения секрета на основе системы остаточных классов

Дерябин М.А.[1]***, Зайцев А.А.***[2]

1 - Северо-Кавказский федеральный университет, Институт естественных наук, 2 - Северо-Кавказский федеральный университет, Институт естественных наук, Ставрополь, Россия

E-mail: maxim.deryabin@gmail.com

Важной проблемой в современной криптографии является задача хранения ключей. Организацию хранения можно реализовать различными методами. Один из эффективных способов решения данной задачи связан с использованием принципа пороговых схем разделения секрета [2]. Данные схемы позволяют разделить один общий секрет (ключ) на n компонентов (пользователей, ЭВМ, данных и др.). При этом для восстановления исходных данных требуется знание не менее чем m компонентов. Сложность построения таких схем состоит в том, что, согласно современным требованиям к длине криптографических ключей, оперировать приходится с числами большой разрядности.

В качестве пороговой схемы предлагается схема, основанная на применении системы остаточных классов (СОК) [4]. Применение непозиционного представления чисел позволяет эффективно работать с числами большой разрядности за счет гомоморфного перехода к адекватно заменяющим их числам малой разрядности. Исследования показали, что прирост производительности при использовании СОК может намного превосходить число независимых потоков, в которых производятся расчеты [1].

Подбирая особым образом основания системы остаточных классов, можно построить эффективную схему разделения секрета между произвольным числом абонентов [5]. Ускорение вычислений достигается за счет применения современных методов перевода чисел из СОК в позиционную систему счисления [3]. В данной работе сравнивается эффективность и время работы построенной схемы и схемы Шамира. Рассматриваемые схемы имеют общую математическую природу, однако схема Шамира требует выполнения большего числа операций сложения и умножения и большего количества генераций случайных чисел, что отражается и при моделировании на компьютере. При этом, для обеспечения правильной работы схемы, основанной на СОК, требуется учет большего числа условий. Несмотря на это можно сделать вывод, что схема на СОК позволяет организовать разделение секрета с большей эффективностью.

Литература

1. Дерябин М.А., Зайцев А.А. Использование модулярной арифметики для ускорения выполнения операций с числами большой разрядности. // Материалы XII Всероссийской конференции «Высокопроизводительные вычисления на кластерных системах». Нижний Новгород, 2012. С. 129-133.

2. Червяков Н. И., Евдокимов А. А., Галушкин А. И., Лавриненко И. Н., Лавриненко А. В. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М. 2012.

3. Червяков Н. И. Реализация высокоэффективной модулярной цифровой обработки сигналов на основе программируемых логических интегральных схем. // Нейрокомпьютеры: разработка и применение, №10, 2006. С 24-36.

4. Omondi A., Premkumar B. Residue number systems. Theory and Implementation. London. 2007.

5. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. New York. 1995.