А. И. Алексеев, О. С. Мезенцева (Ставрополь, СевКавГТУ). **О реализации пороговых схем на базе системы остаточных классов.**

В последнее время, на фоне бурного развития сетевых технологий все большее значение приобретает разработка действенных методов защиты передаваемой по сети информации. Одним из наиболее востребованных и эффективных методов является распределение функций центра сертификации среди всех участников сети с помощью некоторой (k, N) пороговой схемы [1]. Используемые в подобных системах протоколы, характеризуются двумя важными свойствами: проверяемость распределенных вычислений (возможность проверить информацию, поступающую от каждого узла, участвующего в распределенных вычислениях); заменяемость участников распределенных вычислений (нечувствительность к потере связи с одним или несколькими участниками). Как видно из приведенных свойств, системы, функционирующие на основе пороговых схем, представляют интерес не только в задачах защиты информации, но и в области распределенных вычислений. Одно из возможных применений пороговых схем для создания системы распределенного хранения данных показано в [2]. В настоящем докладе кратко освещаются вопросы применения модулярной арифметики для повышения производительности систем, функционирующих на основе пороговых схем.

В качестве пороговой схемы целесообразно использовать схему разделения секрета А. Шамира. Этот метод основан на создании по блоку D информации n теней таким образом, чтобы D могло быть восстановлено из любых $k < n$ теней, но по $(k-1)$ тени D невозможно было получить никакой информации о D. Предлагается использовать эту технологию для создания схем управления ключами и других криптографических механизмов, которые будут обеспечивать безопасность и надежность хранения данных в условиях уничтожения или компрометации до половины теней, на которые разделена информация.

Рассмотрим конечное поле $P = \mathbf{GF}(N)$. Любую последовательность бит для $N = 2n$ можно представить в виде последовательности n-битных последовательностей элементов P. Рассмотрим теперь k-мерное пространство векторов L над полем P. Теперь любую последовательность можно представить в виде последовательности векторов из L [2].

Очевидно, что операции построения элементов поля $\mathbf{GF}(N)$, формирования набора векторов, разделения исходной последовательности и нахождения матрицы, обратной A, выполняются лишь один раз, и хотя благодаря использованию векторного процессора (как показано ниже) количество операций, выполняемых на стадии «разборки» можно значительно сократить, практическая польза подобного подхода представляется сомнительной. Основная трудоемкость алгоритма заключается в выполнении операции $A^{-1}S_i$, где $S_i = Al_i$, и состоит, как показано в [2], из k^2 операций умножения и сложения в поле Галуа, что в свою очередь представляет собой k^2 операций обычного сложения и обычного умножения и $2k^2$ операции % (вычисление остатка от деления на N).

Как видно, переход от вычислений в поле Галуа к обычным операциям сложения и умножения связан со значительным увеличением общей трудоемкости алгоритма, а, учитывая, что число тактов на выполнение операции % для современных SISD процессоров превышает число тактов на выполнение операции умножения в среднем в четыре раза, представляется целесообразным отказаться от перехода и проводить все необходимые вычисления в поле Галуа.

Для этого предлагается использовать математический аппарат системы остаточных классов, что позволит обрабатывать каждый разряд числа независимо на разных процессорах или разных частях одного процессора в случае SIMD-архитектуры.

В качестве сумматора и умножителя предлагается использовать сумматор без использования LUT-таблиц и умножитель, основанный на исчислении степеней (умножитель Галуа), схемы которых приведены в [3].

Благодаря естественной параллельности вычислений в системе остаточных классов, представляется удачной реализация их на аппаратной базе векторных процессоров. Одной из наиболее высокопроизводительных моделей, реализующих векторную архитектуру, является разработка российской компании НТЦ «Модуль»— процессор NM6403, важнейшей особенностью которого является работа с операндами произвольной длины (даже не кратной степени двойки) в диапазоне 1–64 бит. Этим достигается оптимальное соотношение между скоростью и точностью вычислений. Умение динамично, в процессе вычислений изменять разрядность операндов позволяет значительно повысить производительность.

Помимо процессоров NM6403 предлагается использовать вычислительный кластер, составленный из машин SISD архитектуры.

СПИСОК ЛИТЕРАТУРЫ

1. *Фомин А.Д.*, *Фомина А.В.* Управление ключами в Ad-hoc сетях. — В сб.: Тезисы школы-семинара «Новые информационные технологии 2004». М.: МГИЭМ.
2. *Тормасов А.Г.*, *Хасин М.А.*, *Пахомов Ю.И.* Модель распределенного хранения данных с регулируемой избыточностью. — Электронный журнал «Исследовано в России», 2001, № 4, с. 355–364.
3. *Червяков Н.И.*, *Дьяченко И.В.* Принципы построения модулярных сумматоров и умножителей. — Сборник научных трудов. Зеленоград: 2006, с. 447–510.