УДК 681.04

В.А. Краснобаев, С.А. Кошман

Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков

БЫСТРАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Анализ существующих методов повышения производительности решения задач криптографических преобразований показал, что ожидать существенных результатов в этом направлении используя позиционную систему счисления (ПСС) добиться практически невозможно. В тоже время обзор литературных источников по использованию непозиционных систем счисления для повышения пользовательской производительности модульных операций дал основание считать данное научное направления весьма перспективным и актуальным.

Так, использование непозиционной системы

счисления в остаточных классах (СОК) при решении отдельных задач обработки цифровой информации (решение задач фильтрации, решение задач реализации быстрого и дискретного преобразований Фурье, реализация модульных операций в конечных кольцах и полях и пр.) показало высокую эффективность применения модулярной арифметики.

Цель доклада – разработка метода быстрой реализации криптографических преобразований на основе использования СОК.

В докладе детально рассмотрено влияние основных свойств (независимость, равноправность, малоразрядность остатков, представляющих операнд) СОК на структуру и принципы функционирования системы обработки информации (СОИ). В частности показано, что малоразрядность остатков в представлении чисел в СОК даѐт возможность широкого выбора вариантов системотехнических решений при реализации модульных арифметических операций. Известно, что существует четыре принципа реализации арифметических операций в СОК: сумматорный принцип (СП) (на базе малоразрядных двоичных сумматоров), табличный принцип (ТП) (на основе использования ПЗУ); прямой логический принцип реализации арифметических операций, основанный на описании модульных операций на уровне систем переключательных функций, посредством которых формируются значения двоичных разрядов результирующих вычетов (в качестве элементной базы для технической реализации данного принципа целесообразно использовать систолические и программируемые логические матрицы, а также ПЛИС); принцип кольцевого сдвига (ПКС), основанный на использовании кольцевых регистров сдвига (КРС).

Отсутствие межразрядных связей (отсутствие процесса переносов) между двоичными разрядами в обрабатываемых в СОИ операндах в процессе криптопреобразований (при реализации модульных операций) на основе ТП или ПКС является одной из главных и наиболее привлекательных особенностей модулярной арифметики. В ПСС выполнение арифметической операции предполагает последовательную обработку разрядов операндов по правилам, определяемым содержанием данной операции, и не может быть закончено до тех пор, пока не будут последовательно определены значения всех промежуточных результатов с учетом всех связей между разрядами. Таким образом, ПСС, в которых представляется и обрабатывается информация в современных СОИ, обладают существенным недостатком – наличием межразрядных связей, которые накладывают свой отпечаток на методы реализации арифметических операций, усложняют аппаратуру, снижает достоверность вычислений и ограничивают быстродействие реализации криптографических преобразований. Поэтому естественно изыскание возможностей построения такой арифметики, в которой бы поразрядные связи отсутствовали. В этом плане обращает на себя внимание система счисления в остаточных классах. Система остаточных классов обладает ценным свойством независимости друг от друга остатков по принятой системе оснований. Эта независимость открывает широкие возможности в построении не только новой машинной арифметики, но и принципиально новой схемной реализации СОИ, которая в свою очередь заметно расширяет применение машинной арифметики. Во многих литературных источниках отмечается, что одним из практических направлений повышения пользовательской производительности вычислительных средств является внедрение нетрадиционных методов представления и обработки информации в числовых системах с параллельной структурой, и в частности, в так называемых модулярных системах счисления, обладающих максимальным уровнем внутреннего параллелизма в процессе обработки информации.

Список литературы

1. Шнайер Б. Прикладная криптография / Б. Шнайер. – М.: Триумф, 2002. – 797 с.

2. Горбенко И.Д. Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом полларда / И.Д. Горбенко, С.И. Збитнев, А.А. Полеков // Радиотехника: Всеукр. межвед. научн-тех. сб. – 2001. – Вып. 119. – С. 43-50.