СИНТЕЗ УНИВЕРСАЛЬНЫХ УМНОЖИТЕЛЕЙ В КОНЕЧНЫХ ПОЛЯХ С ПОСЛОВНО-ПОСЛЕДОВАТЕЛЬНОЙ АРХИТЕКТУРОЙ

Гормакова И.В.

Национальный технический университет «Харьковский политехнический институт», г.Харьков

В настоящее время для защиты информации в банковских структурах, телекоммуникационных сетях, правоохранительных, промышленных и транспортных объектах широко используются различные методы теории кодирования информации, криптографические протоколы и различные криптосистемы. Одним из широко развивающихся направлений защиты информации является использование программно-аппаратных средств криптографических систем.

При программно-аппаратной реализации различных криптосистем широко используются основные арифметические операции (сложение, умножение, инверсия) в простых $GF(p)$ и двоичных полях расширения $GF(2^m)$. Длина операндов, над которыми производятся арифметические операции, в криптосистемах может составлять от 160 до 2048 бит. Поэтому создание компактных арифметических модулей, оперирующих в конечных полях с операндами большой размерности, является актуальной научно-практической задачей.

В работе представлены методы синтеза пословно-последовательных умножителей, выполняющих операцию обычного умножения элементов конечного поля $GF(2^m)$ и умножения по методу Монтгомери. Также представлен метод синтеза универсального умножителя с пословно-последовательной архитектурой. Основным достоинством предложенного универсального умножителя является возможность изменения конфигурации умножителя и, соответственно, выбора алгоритма вычисления произведения элементов конечного поля: обычное умножение или умножение Монтгомери.

В полученных архитектурах умножителей используются унифицированные блоки из сетей клеточных автоматов, комбинационных модулей и регистров, что позволяет легко модифицировать архитектуры умножителей при изменении длины операндов, длины слова, образующего полинома поля и просто реализовать умножитель на ПЛИС типа FPGA. Кроме этого, синтезированные архитектуры умножителей отвечают требованиям тестопригодности.