УДК 004.021

**В. П. Семеренко**

# ПАРАЛЛЕЛЬНАЯ РЕАЛИЗАЦИЯ ПОТОЧНОГО ШИФРОВАНИЯ

В современных вычислительных системах данные передаются побайтно и поблочно, поэтому устройства для поточного шифрования должны генерировать параллельные последовательности псевдослучайных чисел с максимально высокими криптографическими свойствами: нелинейностью, сбалансированностью, корреляционной устойчивостью. Наиболее часто такое устройство состоит из нескольких регистров сдвига с линейными обратными связями (РСЛОС), выходы которых соединены с криптографическим преобразователем, реализующем нелинейные булевы функции (бент-функции).

Для уменьшения аппаратных затрат и повышения гибкости таких устройств предлагается два усовершенствования. Во-первых, вместо совокупности нескольких РСЛОС можно использовать аппаратную реализацию $n$-канальной $m$-разрядной линейной последовательностной машины (ЛПМ), позволяющей генерировать *M*-последовательности по каждому из $n$ ее выходов [1].

Во-вторых, предлагается параллельная реализация криптографического преобразователя в виде программируемой систолической матрицы. Теоретической основой для проектирования такой матрицы является булева алгебра кубических функций, использующей операции пересечения, объединения и дополнения кубов.

Таким образом, в предлагаемом устройстве реализован параллелизм на макроуровне, благодаря наличию $n$ каналов, и на микроуровне, благодаря конвейерно-матричному вычислению бент-функции. В итоге повышается производительность работы, обеспечивается возможность быстрого перепрограммирования на новую нелинейную функцию и пригодность реализации устройства на современной элементной базе.

*Литература*

1. Семеренко В.П., Степанишин Ю.В., Гаєвський М.Л. Потокове шифрування на основі теорії лінійної послідовнісної машини. // Інформаційні технології та комп'ютерна інженерія. – 2007. №3. – С.86-93.