М. Э. Т у ж и л и н (Москва, ТВП)**. Итоги конкурса ESTREAM.**

В 2004–2008 годах ассоциация ECRYPT, объединяющая более 30 ведущих европейских университетов, под эгидой Европейской Комиссии провела конкурс ESTREAM, целью которого являлось создание европейских стандартов поточных шифрсистем. Конкурс проводился по двум профилям: 1) поточная шифрсистема, предназначенная для программной реализации с длиной ключа 128 битов; 2) поточная шифрсистема, предназначенная для аппаратной реализации с длиной ключа 80 битов.

Победителями по первому профилю признаны алгоритмы HC-128, Rabbit, Salsa20, SOSEMANUK, по второму профилю — Grain, MICKEY 2.0, Trivium.

Выделим основные принципы построения криптосистем-победителей.

В основе HC-128 лежат две таблицы, один элемент которых обновляется в каждом такте при помощи нелинейной функции.

Алгоритм Rabbit использует восемь основных переменных, изменяемых в каждом такте при помощи нелинейной функции, и восемь счетчиковых переменных, изменяемых линейно и обеспечивающих период выходной последовательности не менее 2256-1.

Алгоритм Salsa20 использует хеш-функцию с 20-ю циклами, основные преобразования алгоритма навеяны алгоритмом AES.

Алгоритм SOSEMANUK объединяет идеи поточного алгоритма SNOW 2.0 и блочного алгоритма Serpent, в нем есть линейный регистр, обеспечивающий период выходной последовательности не менее 2230-1, и блок из двух регистров, вырабатывающих последовательность для входа на редуцированную версию алгоритма Serpent.

Алгоритм Grain использует два регистра: линейный, гарантирующий период выходной последовательности не менее 280-1, и нелинейный, выходы с которых поступают на нелинейную функцию.

Алгоритм MICKEY 2.0 использует два регистра длиной 100 битов, линейный и нелинейный. Функционирование нелинейного регистра определяется таблично заданными последовательностями.

Алгоритм Trivium использует три регистра общей длиной 288 битов. Работа каждого регистра нелинейно зависит от этого регистра и еще от одного из трех.

Отметим то, что объединяет все алгоритмы несколько принципов построения, отражающих современные тенденции в криптографии: 1) большой период выходной последовательности; 2) использование нелинейной функции, близкой к равновероятной и обладающей рядом показателей, затрудняющих применение современных методов криптоанализа; 3) гарантия зависимости любого знака выходной последовательности от всех битов ключа.