**Причини зняття з конкурсу:**  існування криптоатак.

**SSS**

**Параметри:** шифр, що самосинхронізується, довжина ключа до 128 біт, максимальна допустима довжина вихідної послідовності на фіксованому ключі 2128 16-бітових слів; генерує за такт 16 бітів.

**Основні операції:** додавання за модулем 2 (XOR), додавання за модулем 216, циклічний зсув, підстановка (S-блок) 816.

**Конструктивні особливості:** є продовженням родини потокових шифрів SOBER, використана схема нелінійної фільтрації лінійного регістра зсуву над полем GF(216).

**Переваги:** вимагає невеликої пам’яті, можливість використання для аутентифікації повідомлення (МАС).

**Криптоатаки:** атака [36] дозволяє знайти секретний ключ за 10 сек на 2,8 GHz PC з вибраним шифротекстом довжиною менше 10 Кбайт.

**Причини зняття з конкурсу:** існування криптоатаки.

**Moustique (**попередня версія називалася **Mosquito)**

**Параметри:** шифр, що самосинхронізується, довжина ключа 96 біт, довжина IV від 0 до 13 байтів.

**Основні операції:** додавання та множення за модулем 2.

**Конструктивні особливості:** зчеплення елементів шифрованого тексту (подібно до режиму СFВ у блоковому шифруванні); використання регістрів з умовним доповненням.

**Переваги:** незвичайна архітектура, можливість використання для аутентифікації повідомлення (МАС), наявність режиму, в якому шифр працює як синхронний.

**Криптоатаки:** знайдено корельовані шифруючі гамми [7].

**Причини зняття з конкурсу:** наявність криптоатаки.