КРИПТОГРАФИЧЕСКАЯ СИСТЕМА НА ОСНОВЕ ХАРАКТЕРИСТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ТРЕТЬЕГО ПОРЯДКА

С.Б. САЛОМАТИН, А.А. ОХРИМЕНКО, А.М. МАКАРЕВИЧ

Криптографические системы на основе характеристических последовательностей третьего порядка являются технической альтернативой систем RSA и систем на эллиптических кривых. Характеристические последовательности формируются на основе кубического уравнения, с помощью регистра сдвига с обратными связями.

Техника характеристических последовательностей позволяет реализовать быстрые системы шифрования, аутентификации с открытым ключом, а также распределения и формирования ключей.

Система распределения с открытым ключом. Имеет два состояния: формирования ключей и установления общего ключа пользователей. В первом состоянии формируется двухуровневое ключевое пространство пользователей на основе кубического неприводимого полинома над полем $GF(p)$ периода $P=(p^2+p+1)$. Первый уровень содержит секретные ключи пользователей, второй уровень — открытые ключи системного взаимодействия. Ключи первого уровня представляют собой случайные числа, взаимно простые с числом P. Ключи второго уровня представляют собой пару элементов (s_k, s_{-k}) двух взаимных характеристических последовательностей, формируемых кубическим полиномом. Пространство ключей представляют собой множества, состоящие из всех лидеров смежных классов модуля p^2+p+1 и всех неприводимых полиномов над полем $GF(p)$ степени 3 с периодом p^2+p+1.

Во втором состоянии формируется общий ключ пользователей на основе свойства характеристических последовательностей: $s_k(s_e(a, b), s_{-e}(a, b))=s_{ke}(a, b)$, где k и e — положительные целые числа. Алгоритмы системы реализуются с использованием техники быстрых вычислений.

Оценка уровня защитных свойств. Защитные свойства характеристических последовательностей и криптосистем на их основе базируются на трудности решения задачи дискретного логарифма в конечном поле $GF(p^3)$, где p — простое число.

Оценка вычислительной сложности. Вычислительная сложность быстрого алгоритма криптосистемы может быть приблизительно оценена зависимостью $L \log n$ модулярных операций умножений.