чества и проведения целенаправленных исследований. Программное обеспечение позволяет производить разнообразные преобразования изображений: изменять масштаб, выделять фрагменты, инвертировать рисунок, осуществлять повороты и симметричные преобразования, выделять контуры, осуществлять фильтрацию и т.п.

В результате применения алгоритмов преобразований удалось улучшить качество рисунков, сформировать новые симметричные изображения и расшифровать элементы тайнописи Франциска Скорины.

БЫСТРЫЙ АЛГОРИТМ ЭКСПОНЕНЦИАЛЬНОГО ПРЕОБРАЗОВАНИЯ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Поденок Л.П., Садыхов Р.Х.

Предлагаемая работа посвящена разработке метода и алгоритмов для защиты и аутентификации информации в открытых системах связи.

Производительность криптосистем с открытыми ключами, основанных на нелинейных преобразованиях шифрования/дешифрования, в большой степени определяется тем, как быстро эти преобразования могут быть выполнены. Классическими примерами таких преобразований являются, в частности, вычисление экспоненциальной функции в поле $GF(n)$ по некоторому основанию, представляющему собой один из первообразных корней поля (система открытого распространения ключей Диффи и Хеллмана [1]) и вычисление степенной функции в кольце $Z/(N)$ классов вычетов по модулю N неизвестной структуры (RSA [2]).

В [3] описан бинарный метод возведения целого числа a в целую степень d, выполняемый максимум за $\lfloor log_2 d \rfloor + \nu_1(d)$ операций умножения и возведения в квадрат, где $\nu_1(d)$- количество единиц в двоичном представлении d, основанный на построении аддитивных цепочек $\{1=d_0,\ldots,d_i,\ldots,d_r=d\}$ с элементами $d_i = 2d_{i-1}$ или $d_{i-1}+1$, которые определяют последовательность вычисления a^d с помощью возведения в квадрат и умножений.

В данном докладе представлен метод и алгоритм вычисления экспоненциальной функции в поле $GF(n)$ по основанию a, имеющему мультипликативно обратный элемент a^{-1} в этом поле, максимум за $\lfloor log_2 d \rfloor + min(\nu_1(d), \nu_0(d)) + 1$ операций умножения и возведения в квадрат. Метод основан на представлении показателя d в виде последовательности целых чисел $\{1=d_0,\ldots,d_i,\ldots,d_r=d\}$ с элементами $2d_{i-1}$ или $d_{i-1}\pm 1$, не являющейся аддитивной цепочкой.

В отличие от бинарного метода [3], данный метод помимо возведения в квадрат и умножения на основание a, использует умножение на мультипликативно обратный элемент a^{-1} (деление) в поле, которое соответствует элементу $d_i = d_{i-1}-1$ построенной последовательности. Поскольку нахождение мультипликативно обратного элемента в $GF(n)$ не пред-

ставляет труда, а также в связи с тем, что основание a является константой, затраты на нахождение a^{-1} можно считать несущественными.

Предложен эффективный алгоритм построения такой последовательности, заключающийся в просмотре двоичного представления показателя справа налево с инвертированием всех встречающихся битовых групп вида 011...1, результатом которого является факторизованное представление показателя, содержащее небольшое количество единиц. Информация о расположении инвертированных групп используется для управления умножением на a^{-1}.

ЛИТЕРАТУРА:

1. W. Diffie, M. Hellman "New directions in cryptography" // IEEE Transactions on Information Theory, v. IT-22, Nov. 1976, pp. 644-654.

2. R.L. Rivest, A. Shamir, L. Adleman, "A method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of ACM, Feb. 1978, Vol. 21. № 2.

3. Д.Кнут. Искусство программирования для ЭВМ. Т.2 Получисленные алгоритмы. М.: Мир, 1977, с.482-510.

ИНСТРУМЕНТАЛЬНАЯ СИСТЕМА ФУНКЦИОНАЛЬНОГО ПРЕКТИРОВАНИЯ МУЛЬТИПРОЦЕССОРНЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Радишевский В.А.

В докладе рассматривается система функционального проектирования мультимикропроцессорных управляющих вычислительных комплексов (ММПУВК) реального времени.

Система предназначена для решения задачи доказательства однозначности и безтупиковости параллельного алгоритма и задачи назначения задач на процессоры. Математическая модель ММПУВК базируется на информационно-логическом графе, отражающем связи по управлению внутри задач и информационные связи между задачами. Для ММПУВК с заранее определенными свойствами задач возможно применение точных или близких к точным методов решения этих задач, которые в данном случае становятся задачами статического планирования и диспетчеризации.

Инструментальная система проектирования ММПУВК реального времени состоит из подсистем, взаимодействующих следующим образом.

Входное описание *. RTX (от Real Time eXecutive) представляет собой текстовый файл, описывающий структуру задач параллельной программы и их предопределенные атрибуты. Препроцессор описания ТР определяет вычисляемые атрибуты задач (например, время выполнения) и проверяет безтупиковость параллельной программы. Подсистема аналитического моделирования АМ кроме входного описания получает файл