FAST HASH FUNCTIONS BASED ON CONTROL PERMUTATION.

Đỗ Thị Bắc, Nguyễn Hiếu Minh, .., .

TÓM TẮT:

Using variable bit permutations there are designed hash functions prossessing high performance while hardware, firmware, and software implementation. Controlled bit permutation operation have been selected in correspondence with earlier proposed topology of the permutation network for implementing on its base the controlled bit permutation in struction oriented to embedding in the mass microprocessors. Due to the last fact the designed algorithms for computing cryptographic checksums are perspective for application as fast software-suitable hash function.