Tạp chí KHOA HỌC & CÔNG NGHỆ - Đại học Công nghiệp Hà Nội số 07 (9/2011):**32-36**

NÂNG CAO HIỆU QUẢ THUẬT TOÁN MẬT MÃ MC-ELIECE THEO HƯỚNG TĂNG TỶ LỆ MÃ HOÁ VÀ TĂNG KHÔNG GIAN CHÌA CỦA HỆ THỐNG

Raising the effects of MC-ELIECE Cryptograph Algorithm to Increase the Encoding Rate and Space Security System

Phạm Xuân Nghĩa[a], Lê Hải Nam[a], Lê Văn Thái[b*], Vũ Thanh Quang[c]

[a] Khoa Vô tuyến Điện tử, Học viện Kỹ thuật Quân sự

[b] Khoa Điện tử, Đại học Công Nghiệp Hà Nội

[c] Khoa Kỹ thuật cơ sở, Cao đẳng Truyền hình

[*] e-mail: lvthai@gmail.com

TÓM TẮT Nội dung chính của bài báo phân tích các đặc điểm của thuật toán bảo mật Mc-Eliece, từ đó đưa ra các phương án cải tiến nhằm nâng cao hiệu quả của thuật toán với các giải pháp sử dụng véc tơ lỗi mang tin và thay thế mã Goppa được sử dụng trong thuật toán truyền thống bằng các mã nối tiếp. Các thuật toán cải tiến này giúp cho tỷ lệ mã hoá tăng đến ~0,8 và khả năng chống nhiễu cũng như khả năng bảo mật của các thuật toán Mc-Eliece cải tiến tăng lên một cách đáng kể so với thuật toán gốc.

ABSTRACT This paper is mainly to analyse the features of the Mc-Eliece algorithm, in which it gives a variety of solutions in order to enhace the effect of the algorithm such as using error vector and replacing Goppa code used in the traditional by concatenated codé. The algorithm increases the coding rate to ~0,8 and improves the anti-interference ability as well as the security ability of Mc-Eliece algorithm. This algorithm is improved remarkably in comparison with the traditional one.