

GIẢI PHÁP NÂNG CAO TỶ LỆ MÃ HÓA CỦA SƠ ĐỒ MẬT MÃ DỰA TRÊN MÃ

PROPOSED SOLUTIONS TO IMPROVE THE CODE RATE
OF CODE-BASED CRYPTOGRAPHY

Lê Văn Thái

TÓM TẮT

Bài báo đề xuất hai giải pháp cải tiến hệ mật McEliece, giải pháp sử dụng vector lỗi mang tin và giải pháp sử dụng mã nối tiếp thay thế mã Goppa. Các giải pháp đề xuất cho phép tăng tỷ lệ mã hoá đến $\sim 0,8$, đạt độ lợi mã hóa 1,7dB, tăng khả năng sửa lỗi, khả năng chống nhiễu của hệ thống và độ bảo mật so với thuật toán đề xuất gốc.

Từ khóa: Hệ mật McEliece, sơ đồ mật dựa trên mã, mã hóa công khai, mã Goppa.

ABSTRACT

This paper is mainly to analyse the feature of the McEliece cryptosystem, in which it gives a variety of solutions in order to enhance the effect of the algorithm such as using error vector and replace Goppa code which use in the traditional by succeed concatenated coding. The algorithm improves the coding rate about ~ 0.8 , gain encoding 1.7dB and the security ability of McEliece algorithm improves more greatly than the traditional.

Keywords: McEliece cryptosystem, Code based cryptosystem, Public-key cryptography, Goppa codes.

Trường Đại học Công nghiệp Hà Nội

E-mail: thailv@hau.edu.vn

Ngày nhận bài: 28/5/2018

Ngày nhận bài sửa sau phản biện: 30/6/2018

Ngày chấp nhận đăng: 25/10/2018