I-O-2.7

MẬT MÃ DÙNG ÁNH XẠ SONG TUYẾN TÍNH

Nguyễn Thành Nhựt
Khoa Toán-Tin học, Trường Đại học Khoa học Tự nhiên – ĐHQG Tp.HCM

Tóm tắt

Các ánh xạ song tuyến tính như ánh xạ Weil và ánh xạ Tate vừa được nghiên cứu để xây dựng các giao thức mật mã trên đường cong elliptic và siêu elliptic vào đầu thế kỷ 21. Một số giao thức mật mã mới ra đời dựa trên ứng dụng của ánh xạ song tuyến tính như giao thức trao đổi khoá một lần giữa ba người, mã hoá dựa trên định danh và giao thức chữ ký số ngắn đã mở ra một chương mới trong ứng dụng mật mã hiện đại. Bài báo này xin giới thiệu sơ lược một số giao thức dùng ánh xạ song tuyến tính, cách tính ánh xạ Weil và Tate, và cách chọn đường cong thích hợp cho ứng dụng thực tế.

Từ khóa: hệ mã dùng đường cong elliptic, ánh xạ song tuyến tính, giao thức mật mã.

PAIRING-BASED CRYPTOGRAPHY

Nguyen Thanh Nhut
Faculty of Mathematics and Computer Science, University of Science – VNU HCMC

Abstract

The bilinear pairing such as Weil pairing or Tate pairing on elliptic and hyperelliptic curves have recently been found applications in design of cryptographic protocols such as one-round three-party key agreement, identity-based encryption, and short signatures. This article gives an introduction to the protocols, Weil and Tate pairing computation, and curve selection.

Key words: elliptic curve cryptography, bilinear pairing, cryptographic protocol.