Cryptographically Strong Elliptic Curves of Prime Order

Tytuł
Cryptographically Strong Elliptic Curves of Prime Order

Typ publikacji
Artykuł

Rok
2021

Data dokładna
2021

Autorzy słownie

Autorzy
Barański Marcin Gliwa Rafał Szmidt Janusz

ISBN/ISSN
eISSN: 2300-1933, ISSN 2081-8491

Informacje dodatkowe

IJET International Journal of Electronics and Telecommunications,

(A periodical of Electronics and Telecommunications Committee of Polish Academy of Sciences)

DOI: 10.24425/ijet.2021.135966

Abstract: The purpose of this paper is to generate cryptographically strong elliptic curves over prime fields Fp, where p is a Mersenne prime, one of the special primes or a random prime. We search for elliptic curves which orders are also prime numbers. The cryptographically strong elliptic curves are those for which the discrete logarithm problem is computationally hard. The required mathematical conditions are formulated in terms of parameters characterizing the elliptic curves. We

present an algorithm to generate such curves. Examples of elliptic curves of prime order are generated with Magma.

Keywords: Mersenne primes, elliptic curves, security requirements, search algorithm, Magma.

Powiązane publikacje

-

Adres url strony

http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-6b9bf067-d108-49e3-9e31-360c8ea825ab

Plik