Mathematics > Number Theory

Cubic Curves, Finite Geometry and Cryptography

A.A. Bruen, J.W.P. Hirschfeld, D.L. Wehlau

(Submitted on 21 Jul 2011)

Some geometry on non-singular cubic curves, mainly over finite fields, is surveyed. Such a curve has 9,3,1 or 0 points of inflexion, and cubic curves are classified accordingly. The group structure and the possible numbers of rational points are also surveyed. A possible strengthening of the security of elliptic curve cryptography is proposed using a `shared secret' related to the group law. Cubic curves are also used in a new way to construct sets of points having various combinatorial and geometric properties that are of particular interest in finite Desarguesian planes.

Comments:	This is a version of our article to appear in Acta Applicandae Mathematicae. In this version, we have corrected a sentence in the third paragraph. The final publication is available at springerlink.com at this http URL
Subjects:	**Number Theory (math.NT)**
DOI:	10.1007/s10440-011-9620-z
Cite as:	**arXiv:1107.4387v1 [math.NT]**

Submission history

From: David Wehlau [view email]
[v1] Thu, 21 Jul 2011 21:48:24 GMT (180kb)

Which authors of this paper are endorsers?