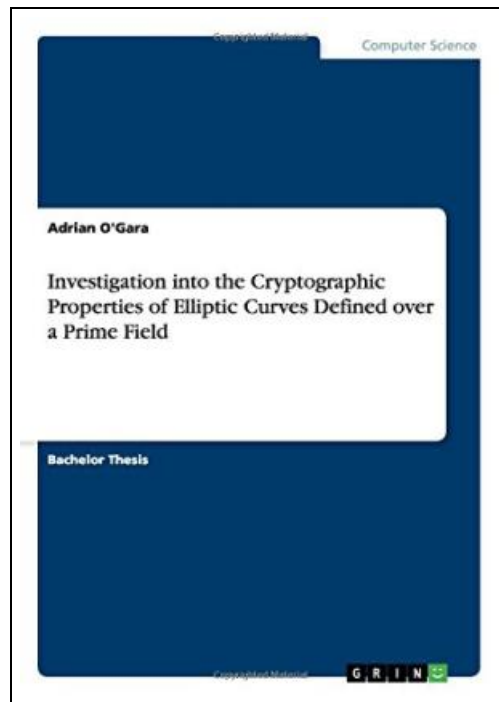


Investigation into the Cryptographic Properties of Elliptic Curves Defined over a Prime Field



Filesize: 4.14 MB

Reviews

*The very best pdf i at any time read through. This is for all those who statte there had not been a worthy of studying. You wont sense monotony at whenever you want of your own time (that's what catalogs are for concerning when you request me).
(Fabian Kuhlman II)*

INVESTIGATION INTO THE CRYPTOGRAPHIC PROPERTIES OF ELLIPTIC CURVES DEFINED OVER A PRIME FIELD



To save **Investigation into the Cryptographic Properties of Elliptic Curves Defined over a Prime Field** eBook, remember to refer to the hyperlink beneath and save the file or get access to other information that are related to INVESTIGATION INTO THE CRYPTOGRAPHIC PROPERTIES OF ELLIPTIC CURVES DEFINED OVER A PRIME FIELD ebook.

GRIN Verlag GmbH. Paperback. Condition: New. This item is printed on demand. 44 pages. Dimensions: 8.3in. x 5.8in. x 0.1in. Bachelor Thesis from the year 2014 in the subject Computer Science - IT-Security, grade: 90.00, , course: Computer Security and Digital Forensics, language: English, abstract: Elliptic curves, as used in cryptography, are essentially points bounded by a finite prime field which display group properties that facilitate their usage in a cryptosystem. The Discrete Log Problem (DLP) - based on a large prime order subgroup of (\mathbb{Z}_p) - constitutes the essence of Elliptic Curve Cryptography (ECC) and can be summed up as such; find an integer, k , such that $Q = kP$ where $k \in \log_p(Q)$ and $P, Q \in (\mathbb{Z}_p)$. Compared to the Integer Factorisation Problem - upon which RSA is constructed - the DLP achieves a greater level of complexity in terms of resistance to attack. This project seeks to describe the mathematical properties that enable ECC to outperform RSA, culminating in the construction of a software system to demonstrate ECCs ability to securely encipher and decipher files and text, according to the National Security Agency's (NSA) Cryptographic Interoperability Strategy (CIS) or Suite B Cryptography. This item ships from La Vergne, TN. Paperback.



[Read Investigation into the Cryptographic Properties of Elliptic Curves Defined over a Prime Field Online](#)

[Download PDF Investigation into the Cryptographic Properties of Elliptic Curves Defined over a Prime Field](#)

[Download ePUB Investigation into the Cryptographic Properties of Elliptic Curves Defined over a Prime Field](#)

Related Books



[PDF] **Fun to Learn Bible Lessons Preschool 20 Easy to Use Programs Vol 1 by Nancy Paulson 1993 Paperback**

Follow the link listed below to download "Fun to Learn Bible Lessons Preschool 20 Easy to Use Programs Vol 1 by Nancy Paulson 1993 Paperback" PDF document.

[Download ePub »](#)



[PDF] **Index to the Classified Subject Catalogue of the Buffalo Library; The Whole System Being Adopted from the Classification and Subject Index of Mr. Melvil Dewey, with Some Modifications .**

Follow the link listed below to download "Index to the Classified Subject Catalogue of the Buffalo Library; The Whole System Being Adopted from the Classification and Subject Index of Mr. Melvil Dewey, with Some Modifications." PDF document.

[Download ePub »](#)



[PDF] **Crochet: Learn How to Make Money with Crochet and Create 10 Most Popular Crochet Patterns for Sale: (Learn to Read Crochet Patterns, Charts, and Graphs, Beginner s Crochet Guide with Pictures)**

Follow the link listed below to download "Crochet: Learn How to Make Money with Crochet and Create 10 Most Popular Crochet Patterns for Sale: (Learn to Read Crochet Patterns, Charts, and Graphs, Beginner s Crochet Guide with Pictures)" PDF document.

[Download ePub »](#)



[PDF] **The Trouble with Trucks: First Reading Book for 3 to 5 Year Olds**

Follow the link listed below to download "The Trouble with Trucks: First Reading Book for 3 to 5 Year Olds" PDF document.

[Download ePub »](#)



[PDF] **Book Finds: How to Find, Buy, and Sell Used and Rare Books (Revised)**

Follow the link listed below to download "Book Finds: How to Find, Buy, and Sell Used and Rare Books (Revised)" PDF document.

[Download ePub »](#)



[PDF] **Read Write Inc. Phonics: Orange Set 4 Storybook 2 I Think I Want to be a Bee**

Follow the link listed below to download "Read Write Inc. Phonics: Orange Set 4 Storybook 2 I Think I Want to be a Bee" PDF document.

[Download ePub »](#)



[PDF] Found around the world : pay attention to safety(Chinese Edition)

Follow the hyperlink listed below to download "Found around the world : pay attention to safety(Chinese Edition)" document.

[Read Book »](#)



[PDF] The Preschool Inclusion Toolbox: How to Build and Lead a High-Quality Program

Follow the hyperlink listed below to download "The Preschool Inclusion Toolbox: How to Build and Lead a High-Quality Program" document.

[Read Book »](#)



[PDF] A Smarter Way to Learn JavaScript: The New Approach That Uses Technology to Cut Your Effort in Half

Follow the hyperlink listed below to download "A Smarter Way to Learn JavaScript: The New Approach That Uses Technology to Cut Your Effort in Half" document.

[Read Book »](#)



[PDF] Environments for Outdoor Play: A Practical Guide to Making Space for Children (New edition)

Follow the hyperlink listed below to download "Environments for Outdoor Play: A Practical Guide to Making Space for Children (New edition)" document.

[Read Book »](#)



[PDF] Ne ma Goes to Daycare

Follow the hyperlink listed below to download "Ne ma Goes to Daycare" document.

[Read Book »](#)



[PDF] Mass Media Law: The Printing Press to the Internet

Follow the hyperlink listed below to download "Mass Media Law: The Printing Press to the Internet" document.

[Read Book »](#)