Available online at www.sciencedirect.com
ScienceDirect
Discrete Applied Mathematics 156 (2008) 3071
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Editorial

Applications of algebra to cryptography

Cryptography is an inherently multidisciplinary field, drawing techniques from a wide range of disciplines and connecting to many different subject areas. Looking at the mathematical part of the spectrum, one major resource for cryptographic research is provided by algebra. It turns out that many interesting cryptographic questions can naturally be phrased in the language of algebra.

In recent years, the connection between algebra and cryptography has tightened, and established computational problems and techniques have been supplemented by interesting new approaches and ideas. For instance, work connecting cryptography with algebraic geometry and with group theory has gained momentum. One of the driving forces behind this is the search for mathematical platforms that could serve as an alternative to currently used algebraic structures, even if large-scale quantum computers became available. Up until now there has been a very fruitful and intense exchange of ideas between research in cryptography and research in algebra. This special issue aims at giving an outline of current work in this line of research. Evidently, the list of topics covered in the subsequent pages is nowhere near complete, but we hope that this small collection of articles gives at least a basic idea of the research that is going on in this fascinating field.

We are extremely grateful to all authors who submitted their work to this special issue. Ultimately, only a small number of papers could be included due to space limitations, but we would like to thank all the authors who submitted their work. Each paper was sent to at least two referees, and we sincerely thank them for their thorough work and insightful comments. Their effort was of invaluable help in compiling this special issue. We also would like to express our gratitude to the editorial team of Discrete Applied Mathematics for their help and support. A special thanks goes to Katie D'Agosta for patiently and competently answering all our questions during the process of preparing this special issue.

Guest Editors
María Isabel González Vasco

Rainer Steinwandt

10 January 2008
Available online 5 March 2008

doi:10.1016/j.dam.2008.01.025