

Table of contents

Preface	vii
<i>Andrew Odlyzko</i> Mathematics, cryptology, and technology	ix
<i>Johannes Buchmann and Safuat Hamdy</i> A survey on IQ cryptography	1
<i>Jean-Marc Couveignes</i> Algebraic groups and discrete logarithm	17
<i>Karl Dilcher</i> Fermat numbers, Wieferich and Wilson primes: computations and generalizations	29
<i>Andreas Enge</i> How to distinguish hyperelliptic curves in even characteristic	49
<i>Steven D. Galbraith</i> Limitations of constructive Weil descent	59
<i>Otokar Grošek, Spyros S. Magliveras and Wandl Wei</i> On the security of a public-key cryptosystem	71
<i>Jeffrey Hoffstein and Joseph Silverman</i> Optimizations for NTRU	77
<i>Michael J. Jacobson, Jr., Renate Scheidler and Hugh C. Williams</i> The efficiency and security of a real quadratic field based key exchange protocol	89
<i>Przemysław Kubiak</i> Extending the binary gcd algorithms	113
<i>Daniel Kucner and Mirosław Kutylowski</i> Stochastic kleptography detection	137
<i>Arjen K. Lenstra and Eric R. Verheul</i> An overview of the XTR public key system	151
<i>Siguna Müller</i> A survey of IND-CCA secure public-key encryption schemes relative to factoring	181
<i>Volker Müller</i> Efficient point multiplication for elliptic curves over special optimal extension fields	197

<i>Harald Niederreiter</i>	
Error-correcting codes and cryptography	209
<i>Jacques Patarin</i>	
Secret public key schemes	221
<i>Attila Pethő</i>	
Index form surfaces and construction of elliptic curves over large finite fields	239
<i>Herman te Riele</i>	
On the size of solutions of the inequality $\phi(ax + b) < \phi(ax)$	249
<i>Claus Peter Schnorr</i>	
Security of DL-encryption and signatures against generic attacks—a survey	257
<i>Edlyn Teske</i>	
Square-root algorithms for the discrete logarithm problem (a survey)	283
<i>Horst G. Zimmer</i>	
Height functions on elliptic curves	303
List of participants	323
List of contributors	329