MATHEMATICS OF COMPUTATION
Volume 70, Number 236, Pages 1751–1759
S 0025-5718(01)01400-4
Article electronically published on May 22, 2001

REVIEWS AND DESCRIPTIONS OF TABLES AND BOOKS

The numbers in brackets are assigned according to the American Mathematical Society classification scheme. The 2000 Mathematics Subject Classification can be found in print starting with the 1999 annual index of *Mathematical Reviews*. The classifications are also accessible from `www.ams.org/msc/`.

11[70F25, 34A09, 65L80]—*Nonholonomic motion of rigid mechanical systems from a DAE viewpoint*, by Patrick J. Rabier and Werner C. Rheinboldt, SIAM, Philadelphia, PA, 2000, viii+140 pp., 25 cm, softcover, $36.00

Over centuries people have been fascinated by the problem of how to determine the motion of systems of rigid bodies or mass points that are subject to external forces and constraints. Today the computer aided systematic generation of the equations of motion and specially adapted numerical solution techniques form the backbone of modern multibody system simulation tools that are successfully used in vehicle dynamics, robotics, and biomechanics.

In the book under review the most general case of nonconservative three-dimensional multibody systems with mixed holonomic and nonholonomic constraints is considered in detail. Generalizing the Gauss principle of least constraint, the equations of motion may be derived as second-order differential equations that are supplemented by nonlinear constraints (differential-algebraic equations, DAEs). Based on ideas of modern DAE theory, these equations are studied analytically and a new approach to the construction of time integration methods is proposed.

The book has nine chapters and starts with an Introduction and short review of the state-of-the-art in Chapter 1. The theoretical results are developed step by step in Chapters 2–7. Numerical solution methods and computational examples are the topics of Chapters 8 and 9.

In Chapter 2 principles of classical mechanics and their application to constrained systems of mass points are discussed providing, at a rather elementary level, background for the substantially more complex analysis of rigid bodies. In Chapter 3 the confirmation space $\mathcal{C}_0$ of a rigid body is studied to include the rotational degrees of freedom. From the numerical point of view, the use of quaternions, i.e., $\mathcal{C}_0 = \mathbb{R}^3 \times S^3 \subset \mathbb{R}^3 \times \mathbb{R}^4$ is found to be favourable. In Chapter 4 this representation of $\mathcal{C}_0$ is applied to show that the equations of motion for an unconstrained rigid body may be written as a second-order ordinary differential equation on $\mathbb{R}^3 \times S^3$. This is the essential prerequisite for the analysis of constrained systems of rigid bodies in Chapter 5 since now the generalized Gauss principle may be used to derive the equations of motion in DAE form.

Because of $\mathbb{R}^3 \times S^3 \subset \mathbb{R}^3 \times \mathbb{R}^4$, these equations may be considered both as a classical DAE in $\mathbb{R}^n$ and as a DAE on a manifold $\mathcal{M} \subset \mathbb{R}^n$. Both approaches are considered separately in Chapters 6 and 7 to prove for initial value problems the existence and uniqueness of a solution. This analysis is based on a formulation $\Gamma(t, x, \dot{x}) = 0$ of the constraints that involves position coordinates x as well as velocities $\dot{x}$ (the *index-2 formulation* in DAE terminology [2]). It is assumed that the Jacobian $D_{\dot{x}}\Gamma$ has full rank. Therefore, holonomic constraints or more generally

all geometric constraints $\Gamma(t, x) = 0$ do not fit a priori into this framework since $D_{\dot{x}}\Gamma = 0$. For these systems it is proposed to substitute $\Gamma(t, x(t)) = 0$ by its time derivative (*index reduction* in classical DAE theory). In Sections 6.2 and 7.3 this strategy is carefully extended to general systems with mixed holonomic and nonholonomic constraints.

As soon as the equations of motion are given in DAE form they may be solved by DAE methods. An approach that is based on local parametrizations of manifolds is discussed in more detail in Chapter 8. The successful practical application of this method is nicely illustrated by numerical tests for typical nonholonomic examples from the literature (Chapter 9). Finally, an appendix was added to make the book essentially self-contained. This appendix summarizes shortly some material on submanifolds of finite-dimensional spaces.

In less than 150 pages this book provides a compact discussion of a very general class of mechanical problems and gives a strong theoretical justification for a DAE formulation of the equations of motion. It is very helpful that the clear and detailed mathematical presentation refers frequently to simple special cases, like systems of mass points, single unconstrained rigid bodies or planar systems to explain the ideas and technical problems of this analysis.

The topic of this book is not restricted to the mathematical background of a classical mechanical problem. The extension of classical DAE theory to DAEs on manifolds in Chapter 7 has independent value since this analysis covers a much larger class of constrained problems.

Readers who consider the terms holonomic and nonholonomic constraint in the classical sense of H. Hertz as antonyms will be surprised to find a complete analysis of the holonomic case and the mixed holonomic/nonholonomic case in a book entitled "Nonholonomic motion...". However, in one of the first paragraphs of the Introduction, the use of the terms holonomic, nonholonomic, geometric, and kinematic constraints is clarified.

The publisher claims that "mechanical engineers and robotics engineers will find this book valuable", but the potential reader should be aware that this is a book written by mathematicians in a way that is typical of *mathematical* presentations. References to the work of E. J. Haug [3] create a link to computational mechanics.

Besides the theoretical results, the book contributes also to two central practical problems in multibody dynamics: the choice of coordinates and the efficient numerical solution of the equations of motion. There is a vast literature on both topics and several different strategies have been developed and implemented successfully over the last two decades ("... nothing can really be new that addresses the motion of rigid bodies ..., page vii). In view of the state-of-the-art, it is questionable to present one specific choice of coordinates (quaternions) as the "correct" one (pages vii, 2 and Chapter 3).

Furthermore, the efficiency of the new numerical methods of Chapter 8 should have been compared with standard DAE methods for multibody systems like BDF [1, Section 6.2] or implicit Runge-Kutta methods [2, Chapter VII]. The initial statement of Section 8.3, "Standard DAE software, such as the widely used code DASSL ... are certainly not useable for the production solution of the DAEs (6.1)", is wrong. DASSL has been used very successfully in academic research and industrial multibody software for more than a decade (see, e.g., [4]).

Despite these critical remarks there is no doubt that the book will help to decrease the gap between abstract differential geometry and its applications in computational mechanics. It may be recommended to all mathematicians and engineers who are interested in the theoretical analysis of constrained mechanical systems and in practical applications of differential geometry.

References

1. K. E. Brenan, S. L. Campbell, and L. R. Petzold. *Numerical solution of initial-value problems in differential-algebraic equations*. SIAM, Philadelphia, 2nd edition, 1996. MR **96h:**65083
2. E. Hairer and G. Wanner, *Solving ordinary differential equations II. Stiff and differential-algebraic problems*. Springer-Verlag, Berlin, Heidelberg, New York, 2nd edition, 1996. MR **97m:**65007
3. E. J. Haug. *Computer aided kinematics and dynamics of mechanical systems*, volume I. Allyn and Bacon, Boston, MA, 1989.
4. W. Rulka. SIMPACK—A computer program for simulation of large-motion multibody systems. In W. O. Schiehlen, editor, *Multibody Systems Handbook*. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

Martin Arnold
DLR German Aerospace Center
Vehicle System Dynamics Group
D-82230 Wessling, Germany
E-mail address: martin.arnold@dlr.de

12[90C30, 90C25, 65K05]—*Trust-region methods*, by Andrew R. Conn, Nicholas I. M. Gould, and Philippe L. Toint, SIAM, Philadelphia, PA, 2000, xix+959 pp., 26 cm, softcover, $119.00

This giant monograph is the first book (until now, it is also the only one) published on trust-region methods. Trust-region methods are a class of numerical methods for solving nonlinear optimization problems. These methods are reliable and robust, they can be applied to ill-conditioned problems, and they have very strong convergence properties. The authors are three distinguished researchers having long been involved in the development and implementation of algorithms for large-scale numerical optimization. They were corecipients of the 1994 Beale–Orchard–Hays prize for their work on the Lancelot optimization package.

The aims of the book are best stated by the authors in the Preface:

> *Three major aims are, firstly, a detailed description of the basic theory of trust-region methods and the resulting algorithms for unconstrained, linearly constrained, and generally constrained optimization*; *secondly, the inclusion of implementation and computational details*; *and finally, substantive material on less well-known advanced topics, including structured trust regions, derivative-free methods, approximate methods* (*including noise*), *nonmonotone algorithms, and nonsmooth problems.*

Chapter 1 is a brief introduction, which gives a description of fundamental trust-region ideas, overviews the history of trust-region methods, and tables some references of applications of trust-region methods in science and engineering. Chapters 2 to 5 are some background mathematics, including vector spaces, matrix analysis, optimality conditions, and methods for solving linear systems and eigenproblems.

Chapters 6 to 11 are about trust-region methods for unconstrained optimization. The formal description of a Basic Trust Region (BTR) algorithm is given and convergence analysis is presented. One whole chapter is devoted to the trust-region subproblem, including its theoretical properties and the numerical methods for solving it. The final chapter of this part of the book is about trust-region methods for nonsmooth problems.

Trust-region methods for convex constrained problems are the focus of Chapters 12 and 13. One chapter is about projection methods and the other is about barrier methods.

Chapters 14 to 16 are dedicated to general nonlinear constrained problems. Various penalty function methods are described in Chapter 14, and in this chapter, trust-region methods are not mentioned except that they are used for minimizing the penalty functions. Trust-region methods based on Sequential Quadratic Programming (SQP) type approaches are discussed extensively in Chapter 15, which is the longest chapter in the book. Chapter 16 is about methods for nonlinear equations, nonlinear least squares, and nonlinear complementarity problems.

The last chapter of the boo, Chapter 17, is devoted to software and implementation issues. Questions, such as how to choose algorithmic parameters, how to choose initial trust-region radius, and how to compute Cauchy points, are addressed in this chapter.

The book gives a detailed, systematic, and comprehensive description of trust-region methods. It is a very good summary of works having been done. In some sense, it can be regarded as an encyclopedia of trust-region methods, and I believe that it will be an important reference in this area for many years. I like very much the comments under the title "Notes and References" at the end of each section. These discussions are not only good supplements to the main text but also give nice guidance for further research ideas. The long list of annotated bibliography entries is very helpful to researchers and graduate students who want to explore the field in depth.

The thickness (consequently the price) might be a burden if the book is used as a graduate text book. Also, for graduate students, it would be better if exercises were added at the end of each chapter.

Ya-xiang Yuan
School of Mathematics
Chinese Academy of Science
Beijing
P.R. China

13[65F05, 65F25, 65F35]—*Fast reliable algorithms for matrices with structure*, T. Kailath and A. H. Sayed (Editors), SIAM, Philadelphia, PA, 1999, xvi+342 pp., 25 1/2 cm, softcover, $59.50

The topic of these unusual proceedings is the design of fast and reliable algorithms for large scale matrix problems with structure. Here structure is mostly understood as "displacement structure" and encompasses Toeplitz-, Hankel-, Loewner-, Cauchy-matrices and others. As the standard stable matrix algorithms usually destroy the structure and are thus not fast, it is a problem to construct fast and reliable ones. Three recent meetings in Santa Barbara, USA, Cortona, Italy,

and St. Emilion, France, in 1996/97 were devoted to this problem, and the chapters of this book are a selection of works presented there.

The chapters contain in the beginning ample background material to put the new results into the right perspective. Notation, style, and presentation in the different chapters, though written by different authors, show a high uniformity. Also cross-references between the chapters have been introduced.

In this respect the editors have done a good job, also by adding two chapters containing some useful matrix results and some material on unitary and hyperbolic transformations. Thus the book gives a very good overview of an exciting field.

The first four chapters deal with fast direct methods for linear systems, and Chapters 5–7 with iterative methods. The last three chapters deal with further applications and generalizations, such as the block case and the tensor case.

Following is a list of the chapters of the book, with the authors in parentheses.

1. Displacement structure and array algorithms (T. Kailath)
2. Stabilized Schur algorithms (S. Chandrasekaran, A. H. Sayed)
3. Fast stable solvers for structured linear systems (A. H. Sayed, S. Chandrasekaran)
4. Stability of fast algorithms for structured linear systems (R. Brent)
5. Iterative methods for linear systems with matrix structure (R. Chan, M. K. Ng)
6. Asymptotic spectral distribution of Toeplitz related matrices (P. Tilli)
7. Newton's iteration for structured matrices (V. Pan, S. Branham, R. Rosholt, A. Zheng)
8. Fast algorithms with applications to Markow chains and queueing models (D. Bini, B. Meini)
9. Tensor displacement structures and polyspectral matching (V. Grigorascu, P. Regalia)
10. Minimal complexity realization of structured matrices (P. Dewilde)

L. Elsner
Bielefeld
Germany

14[94-02, 94A60, 14H52]—*Elliptic curves in cryptography*, by Ian Blake, Gadiel Seroussi, and Nigel Smart, Cambridge University Press, New York, NY, 1999, xv+204 pp., 23 cm, softcover, $39.95

Elliptic curves have been studied for more than a century from the perspectives of modular forms, complex analysis, algebraic geometry, and number theory. Schoof's discovery [10, 1984], that there is a polynomial time algorithm for establishing the size of the elliptic curve group over any finite field opened the way to various computational applications of these groups.

One by one, most applications which were customary in the multiplicative group of finite fields were adapted to the elliptic curve group. In the space of a few years, elliptic curves emerged in primality proving [5], integer factoring [6], and cryptography [8]. The first two applications take advantage of the large variety of available groups of the chosen order of magnitude, while the interest of the latter is based on the fact that in general no subexponential algorithm for computing the discrete logarithm in the elliptic curve group is known or likely to be found. Such

algorithms had been known for some time in the multiplicative groups. However, many practical questions were still asking for improvements and clarity, so the last 15 years have seen intense research in this domain of applications.

The book at hand is a welcome, in-depth treatment of the various research and improvements up to 1999. It offers a comprehensive presentation of both the deeper theoretical background of algorithmic developments and the implementational bottlenecks. Whoever wants to deal with algorithmal aspects of elliptic curves will find here an excellent and, in most cases, sufficient starting point. The book is therefore not intended either as primary didactical material (proofs are scarcely given) nor as a compendium of the various short or long lived cryprographical mechanisms related to elliptic curves. For the first, books such as [7] for the practical and [3] for the mathematical aspects, are recommendable. For the latter, the technical IEEE standard P1363, which has been meanwhile released, is the relevant source for those mechanisms which are likely to be spread in practice.

The first two chapters offer a succinct introduction to general ideas of public key cryptography and the underlying arithmetic in finite fields. The important third chapter introduces the arithmetic of elliptic curves together with the various connections to division polynomials, Weil pairing, and modular functions, which have found explicit use in applications. The fourth chapter gives an overview of efficient implementations of elliptic curves arithmetic for the practitioner, and the fifth treats the discrete logarithm problem on elliptic curves. From the sixth to the eighth chapters the authors discuss the determination of the group order, by Schoof's algorithm and its later improvements and by an a priori choice of the complex multiplication fields of the target curve. The book closes with an overview of primality proving and integer factoring using elliptic curves in the ninth chapter, and with generalizations of cryptosystems to abelian varieties of higher genus in the tenth chapter.

Let $\mathbb{F}_q$ be a finite field with q elements. An elliptic curve E over $\mathbb{F}_q$ is defined by a *long Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$ are such that the equation is nonsingular. This is equivalent to saying that the *discriminant*

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 90b_2b_4b_6 \neq 0,$$

where $b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6, b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. From the definition of the discriminant, it follows that it has special behavior in fields of characteristic 2 or 3. In fact, most applications in finite fields are treated differently in characteristic $p \leq 3$ and $p > 3$. In the book the clear choice to deal only with the cases of characteristics 2 and prime fields $\mathbb{F}_p$ with $p > 3$ was made. It is customary to indicate by $E(\mathbb{F}_q)$ the set of points on $\mathbb{F}_q^2$ of the equation defining E together with an extra point $\mathcal{O}$ at infinity, which one may think of as lying on the top of the y-axis. For two points, $P_1 = (x_1, y_1), P_2(x_2, y_2) \in E(\mathbb{F}_q)$, the sum is $P_1 \oplus P_2 = (x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \mu - a_3)$, where

$$(\lambda, \mu) = \begin{cases} \left(\frac{y_2-y_1}{x_2-x_1}, \frac{y_1x_2-y_2x_1}{x_2-x_1}\right) & \text{if } x_1 \neq x_2, \\ \left(\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_2x_1+a_3}, \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_2x_1+a_3}\right) & \text{if } x_1 = x_2. \end{cases}$$

This composition rule makes $(E(\mathbb{F}_q), \oplus)$ into a commutative group with $\mathcal{O}$ as its neutral element and $E(\mathbb{F}_q) \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})$, where d_1 divides both d_2 and $q-1$. The n-fold addition of P to itself is $[n]P$ and $E[n] \cong (\mathbb{Z}/(n \cdot \mathbb{Z}))^2$ is the n-torsion group of E over $\overline{\mathbb{F}}_q$. The x-coordinates of the n torsion points are zeroes of the division polynomials Ψ_n. These notions, together with the more subtle connections to modular functions and complex multiplication, which we shall not describe here, are introduced in the third chapter, yielding a self-sufficient base for the understanding of all algorithms treated subsequently. The fourth chapter is an extensive overview of the main practical aspects which the implementer will encounter, from arithmetic tricks to point compression—a technical term (in cryptography) for the idea that a point on the curve carries essentially the information of its x coordinate plus one bit allowing to distinguish a solution of a quadratic equation.

The problem of taking the discrete logarithm on elliptic curves is the door to cryptographic applications of these groups. The known general techniques are treated comprehensively in chapter five. In the following special cases, described in this chapter, more performant algorithms than the generic ones are possible: First, the supersingular curves for which the Weil pairing yields an isomorphism to the roots of unity of the ground field or a small extension thereof, where subexponential index calculus methods can be applied. Second, the recent algorithm of Smart for computing the discrete logarithms on curves with the number of points equal to the (prime) characteristic of the field over which they are defined.

Unsurprisingly, the problem of determining the number of points in the elliptic curve group, which brought curves into computational algebra, is covered in three extensive chapters. The first short one gives an overview of naive approaches and problems related to subgroups of the elliptic curve group.

The sixth and seventh chapters cover the generic algorithm of Schoof and its ulterior improvements and adaptations to *tricky* characteristics (i.e., $p = 2, 3$, with special behavior of the discriminant). The basic algorithm of Schoof for computing $\#E(\mathbb{F}_q)$ (that we briefly outline being the first step in the journey of which the book is telling the story) is based on the fact that from Hasse's Theorem, namely $\#E(\mathbb{F}_q) = q + 1 - t$ with $|t| \leq 2\sqrt{q}$, it is enough to determine t modulo l for sufficiently many small primes l. More precisely, it suffices to take primes $l \leq l_{\max}$ with $\prod_{l \leq l_{\max}} l > 4\sqrt{q}$. One uses the fact that the Frobenius endomorphism ϕ satisfies the equation $\phi^2 - t\phi + q = 0$. Considering a nontrivial point $P = (x, y) \in E[l]$, one lets $q_l = q \bmod l$. Then $(x^{q^2}, y^{q^2}) + [q_l](x, y) = [\tau](x^q, y^q)$ must be satisfied exactly for $\tau = t \bmod l$. The value of τ can be found by computing symbolically $(x^{q^2}, y^{q^2}) + [q_l](x, y)$ modulo the l-division polynomials Ψ_l and comparing with the possible values of $[\tau](x^q, y^q)$, $(\tau = 1, \ldots, l)$. The computations are polynomially bounded by $O(\log q)$ and the degree $\frac{l^2-1}{2}$ of the l-division polynomials. This degree grows in practice quite fast, which makes the arithmetic modulo division polynomials the essential bottleneck in the original version of Schoof's algorithm.

However, the division polynomials are in general not irreducible and one can sensibly reduce the complexity by replacing Ψ_l by some smaller—not necessarily irreducible—factors. Since $E[l] \cong (\mathbb{Z}/(l \cdot \mathbb{Z}))^2$, there is a representation of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ in $GL_2(\mathbb{F}_l)$, which yields information on the factorization patterns of Ψ_l. This fact was basically exploited in the subsequent contributions due to Atkin,

Elkies and worked out and implemented by F. Morain, some of his students, and V. Müller.

The applications of elliptic curves to factoring and primality proving are briefly outlined, for the sake of completeness, in the ninth chapter. The last chapter summarizes the main ideas about cryptographic use of hyperelliptic curves at the time the was book printed.

For the interested reader, it may be important to mention some of the outstanding results of the last few years, which are ulterior to the conception of this book and thus not covered by it.

Counting points on curves over fields of small characteristics p have been sensibly simplified by an algorithm of Satoh [9], based on p-adic logarithms. The algorithm has been implemented, and curves over the field $\mathbb{F}_{2^{8009}}$ can be currently treated; without Satoh's approach, the best methods could calculate the curve orders in extensions of $\mathbb{F}_2$ of degree up to 2000.

In the domain of implementation, a beautiful paper of H. Cohen, A. Miyaji, and T. Ono [2] studies a variety of curve representations, with the aim of optimizing the performance of group operations; this can certainly be of great help for implementors. Fields of odd characteristic which are adapted to machine world length—*medium Galois fields* or simply *extension fields*, according to different terminologies—receive some attention. A run time study, [12] by Smart, of implementations of elliptic curve operations over fields of characteristics of various sizes suggests that these fields may have interesting practical properties.

Finally, *Weil descents* have been proposed by G. Frey [4] as a possible method for solving special instances of the discrete logarithms problem. This has already motivated a series of important research with pro and con arguments, and is likely to become an important research topic.

References

1. Blake, I. F.; Seroussi, G.; Smart, N. P.: *Elliptic curves in cryptography*. Reprint of the 1999 original. London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 2000. CMP 2000:15
2. Cohen, H.; Miyaji, A.; Ono, T.: *Efficient elliptic curve exponentiation using mixed coordinates*, Asiacrypt 98, Lecture Notes in Comput. Sci., 1514, Springer, Berlin, 1998. CMP 2000:06
3. Cox, D. A.: *Primes of the form $x^2 + ny^2$*, Wiley & Sons, 1989. MR **90m:**11016
4. Frey, G.: *Applications of arithmetical geometry to cryptographic constructions*, Preprint.
5. Goldwasser, S.; Killian, J.: *Almost all primes can be quickly certified*, Proc. 18-th Annual ACM Symp. on Theory of Computing (1986), 316–329.
6. Lenstra, H. W.: *Factoring integers with elliptic curves*, Ann. of Math., **126** (1987), 649–673. MR **89g:**11125
7. Menezes, Alfred J.: *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993. MR **2000d:**94023
8. Miller, V.: *Use of elliptic curves in cryptography*, Advances in Cryptology, Proceedings of CRYPTO'85, Lecture Notes in Comput. Sci. **218**, Springer, Berlin, 1986, pp. 417–426. MR **88b:**68040
9. Satoh, T.: *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15** (2000), no. 4, 247–270. CMP 2001:05
10. Schoof, R.: *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44**, (1985), 483–494. MR **86e:**11122
11. Silverman, J. H.: *The arithmetic of elliptic curves*. Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1999. MR **95m:**11054

12. Smart, N.: *A comparison of different finite fields for use in elliptic curve cryptosystems*, University of Bristol, Department of Computer Science, June 2000 preprint.

Preda Mihăilescu
M_EC Consulting and Gesamthochschule Paderborn
Germany
E-mail address: preda@math.upb.de

F. Pappalardi
Dipartimento di Matematica
Università degli studi Roma Tre
Largo S. L. Murialdo 1
I-00146 Roma
Italy
E-mail address: pappa@mat.uniroma3.it