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