Lecture Notes in Computer Science 1726

Vijay Varadharajan Yi Mu (Eds.)

Information and Communication Security

Second International Conference, ICICS'99
Sydney, Australia, November 1999
Proceedings

Springer

Vijay Varadharajan Yi Mu (Eds.)

Information and Communication Security

Second International Conference, ICICS'99
Sydney, Australia, November 9-11, 1999
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Vijay Varadharajan
Yi Mu
School of Computing and Information Technology
University of Western Sydney NEPEAN
P.O. Box 10, Kingswood, NSW 2747, Australia
E-mail: {vijay/y.mu}@cit.nepean.uws.edu.au

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information and communication security : second international conference ; proceedings / ICICS '99, Sydney, Australia, November 9 - 11, 1999. Vijay Varadharajan ; Yi Mu (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1726)
ISBN 3-540-66682-6

CR Subject Classification (1998): E.3, G.2.1, D.4.6, F.2.1-2, C.2, K.6.5

ISSN 0302-9743
ISBN 3-540-66682-6 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN: 10705505 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Lecture Notes in Computer Science 1726

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

PREFACE

ICICS'99, the Second International Conference on Information and Communication Security, was held in Sydney, Australia, 9-11 November 1999. The conference was sponsored by the Distributed System and Network Security Research Unit, University of Western Sydney, Nepean, the Australian Computer Society, IEEE Computer Chapter (NSW), and Harvey World Travel. I am grateful to all these organizations for their support of the conference.

The conference brought together researchers, designers, implementors and users of information security systems and technologies. A range of aspects was addressed from security theory and modeling to system and protocol designs and implementations to applications and management. The conference consisted of a series of refereed technical papers and invited technical presentations. The program committee invited two distinguished key note speakers. The first keynote speech by Doug McGowan, a Senior Manager from Hewlett-Packard, USA, discussed cryptography in an international setting. Doug described the current status of international cryptography and explored possible future trends and new technologies. The second keynote speech was delivered by Sushil Jajodia of George Mason University, USA. Sushil's talk addressed the protection of critical information systems. He discussed issues and methods for survivability of systems under malicious attacks and proposed a fault-tolerance based approach. The conference also hosted a panel on the currently much debated topic of Internet censorship. The panel addressed the issue of censorship from various viewpoints namely legal, industrial, governmental and technical. It was chaired by Vijay Varadharajan with panel members from the Australian National Office of the Information Economy, Electronic Frontiers Association, the Australian Computer Society, and the Internet Industry Association.

There were 62 technical papers submitted to the conference from an international authorship. The program committee accepted 24 papers and these were presented in eight sessions covering cryptanalysis, language based approach to security, electronic commerce and secret sharing, digital signatures, security protocols, applications, cryptography, and complexity functions. The accepted papers came from a range of countries, including some 7 papers from Australia, 6 from Japan, 3 from the USA, 2 from Sweden, 2 from the UK, 1 from China, France, Spain, and Singapore. I would like to thank the authors of all the papers submitted to the conference, both those whose work is included in the proceedings and those whose work could not be accommodated.

I would like to thank all the people involved in organizing the conference. In particular, I would like to thank the members of the program committee for

their effort in reviewing the papers and putting together an excellent program. I would like to thank all the speakers, session chairs, and panelists for their time and effort. Special thanks to members of the organizing committee for their tireless work in organizing and helping with many local details, especially Yi Mu, Irene Ee, Rajan Shankaran, Kenny Nguyen, and Chuan Kun Wu. Finally, I would like to thank all the participants of ICICS'99. I hope that the professional contacts made at this conference, the presentations, and the proceedings have offered you additional insights and ideas that you can apply to your own efforts in information and communication security.

August 1999 Vijay Varadharajan

The Second Conference on Information and Communication Security ICICS'99 (Sydney, Australia)

Sponsored by
Distributed System & Network Security Research Unit, UWSN
Institute of Electrical & Electronics Engineers (IEEE Computer, NSW)
Australian Computer Society
Harvey World Travel (Penrith), Australia

General Chair:

Vijay Varadharajan	*University of Western Sydney*

Program Chairs:

Vijay Varadharajan	*University of Western Sydney*
Josef Pieprzyk	*University of Wollongong*

Program Committee:

Ross Anderson	*Cambridge Uni., UK*
Ed Dawson	*Queensland Uni. of Tech., Australia*
Robert Deng	*KRDL, Singapore*
Yvo Desmedt	*Florida State Uni., USA*
Yong Fei Han	*GemPlus, Singapore*
Kwangjo Kim	*ICU, South Korea*
Wenbo Mao	*HP Labs, UK*
Mitsuru Matsui	*Mitsubishi, Japan*
Cathy Meadows	*NRL, USA*
Chris Mitchell	*London Uni., UK*
Yi Mu	*UWSN, Australia*
Luke O'Connor	*IBM, Switzerland*
Eiji Okamoto	*JAIST, Japan*
Tatsuaki Okamoto	*NTT, Japan*
Josef Pieprzyk	*Wollongong Uni., Australia*
Ravi Sandhu	*George Mason Uni., USA*
Jim Schindler	*HP, USA*
Jennifer Seberry	*Wollongong Uni., Australia*
Vijay Varadharajan	*UWSN, Australia*

Lecture Notes in Computer Science

For information about Vols. 1–1652
please contact your bookseller or Springer-Verlag

Vol. 1653: S. Covaci (Ed.), Active Networks. Proceedings, 1999. XIII, 346 pages. 1999.

Vol. 1654: E.R. Hancock, M. Pelillo (Eds.), Energy Minimization Methods in Computer Vision and Pattern Recognition. Proceedings, 1999. IX, 331 pages. 1999.

Vol. 1655: S.-W. Lee, Y. Nakano (Eds.), Document Analysis Systems: Theory and Practice. Proceedings, 1998. XI, 377 pages. 1999.

Vol. 1656: S. Chatterjee, J.F. Prins, L. Carter, J. Ferrante, Z. Li, D. Sehr, P.-C. Yew (Eds.), Languages and Compilers for Parallel Computing. Proceedings, 1998. XI, 384 pages. 1999.

Vol. 1657: T. Altenkirch, W. Naraschewski, B. Reus (Eds.), Types for Proofs and Programs. Proceedings, 1998. VIII, 207 pages. 1999.

Vol. 1659: D.G. Feitelson, L. Rudolph (Eds.), Job Scheduling Strategies for Parallel Processing. Proceedings, 1999. VII, 237 pages. 1999.

Vol. 1660: J.-M. Champarnaud, D. Maurel, D. Ziadi (Eds.), Automata Implementation. Proceedings, 1998. X, 245 pages. 1999.

Vol. 1661: C. Freksa, D.M. Mark (Eds.), Spatial Information Theory. Proceedings, 1999. XIII, 477 pages. 1999.

Vol. 1662: V. Malyshkin (Ed.), Parallel Computing Technologies. Proceedings, 1999. XIX, 510 pages. 1999.

Vol. 1663: F. Dehne, A. Gupta. J.-R. Sack, R. Tamassia (Eds.), Algorithms and Data Structures. Proceedings, 1999. IX, 366 pages. 1999.

Vol. 1664: J.C.M. Baeten, S. Mauw (Eds.), CONCUR'99. Concurrency Theory. Proceedings, 1999. XI, 573 pages. 1999.

Vol. 1665: P. Widmayer, G. Neyer, S. Eidenbenz (Eds.), Graph-Theoretic Concepts in Computer Science. Proceedings, 1999. XI, 414 pages. 1999.

Vol. 1666: M. Wiener (Ed.), Advances in Cryptology – CRYPTO '99. Proceedings, 1999. XII, 639 pages. 1999.

Vol. 1667: J. Hlavička, E. Maehle, A. Pataricza (Eds.), Dependable Computing – EDCC-3. Proceedings, 1999. XVIII, 455 pages. 1999.

Vol. 1668: J.S. Vitter, C.D. Zaroliagis (Eds.), Algorithm Engineering. Proceedings, 1999. VIII, 361 pages. 1999.

Vol. 1669: X.-S. Gao, D. Wang, L. Yang (Eds.), Automated Deduction in Geometry. Proceedings, 1998. VII, 287 pages. 1999. (Subseries LNAI).

Vol. 1670: N.A. Streitz, J. Siegel, V. Hartkopf, S. Konomi (Eds.), Cooperaltive Buildings. Proceedings, 1999. X, 229 pages. 1999.

Vol. 1671: D. Hochbaum, K. Jansen, J.D.P. Rolim, A. Sinclair (Eds.), Randomization, Approximation, and Combinatorial Optimization. Proceedings, 1999. IX, 289 pages. 1999.

Vol. 1672: M. Kutylowski, L. Pacholski, T. Wierzbicki (Eds.), Mathematical Foundations of Computer Science 1999. Proceedings, 1999. XII, 455 pages. 1999.

Vol. 1673: P. Lysaght, J. Irvine, R. Hartenstein (Eds.), Field Programmable Logic and Applications. Proceedings, 1999. XI, 541 pages. 1999.

Vol. 1674: D. Floreano, J.-D. Nicoud, F. Mondada (Eds.), Advances in Artificial Life. Proceedings, 1999. XVI, 737 pages. 1999. (Subseries LNAI).

Vol. 1675: J. Estublier (Ed.), System Configuration Management. Proceedings, 1999. VIII, 255 pages. 1999.

Vol. 1676: M. Mohania, A M. Tjoa (Eds.), Data Warehousing and Knowledge Discovery. Proceedings, 1999. XII, 400 pages. 1999.

Vol. 1677: T. Bench-Capon, G. Soda, A M. Tjoa (Eds.), Database and Expert Systems Applications. Proceedings, 1999. XVIII, 1105 pages. 1999.

Vol. 1678: M.H. Böhlen, C.S. Jensen, M.O. Scholl (Eds.), Spatio-Temporal Database Management. Proceedings, 1999. X, 243 pages. 1999.

Vol. 1679: C. Taylor, A. Colchester (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI'99. Proceedings, 1999. XXI, 1240 pages. 1999.

Vol. 1680: D. Dams, R. Gerth, S. Leue, M. Massink (Eds.), Theoretical and Practical Aspects of SPIN Model Checking. Proceedings, 1999. X, 277 pages. 1999.

Vol. 1681: D. A. Forsyth, J. L. Mundy, V. di Gesú, R. Cipolla (Eds.), Shape, Contour and Grouping in Computer Vision. VIII, 347 pages. 1999.

Vol. 1682: M. Nielsen, P. Johansen, O.F. Olsen, J. Weickert (Eds.), Scale-Space Theories in Computer Vision. Proceedings, 1999. XII, 532 pages. 1999.

Vol. 1683: J. Flum, M. Rodríguez-Artalejo (Eds.), Computer Science Logic. Proceedings, 1999. XI, 580 pages. 1999.

Vol. 1684: G. Ciobanu, G. Păun (Eds.), Fundamentals of Computation Theory. Proceedings, 1999. XI, 570 pages. 1999.

Vol. 1685: P. Amestoy, P. Berger, M. Daydé, I. Duff, V. Frayssé, L. Giraud, D. Ruiz (Eds.), Euro-Par'99. Parallel Processing. Proceedings, 1999. XXXII, 1503 pages. 1999.

Vol. 1686: H.E. Bal, B. Belkhouche, L. Cardelli (Eds.), Internet Programming Languages. Proceedings, 1998. IX, 143 pages. 1999.

Vol. 1687: O. Nierstrasz, M. Lemoine (Eds.), Software Engineering – ESEC/FSE '99. Proceedings, 1999. XII, 529 pages. 1999.

Vol. 1688: P. Bouquet, L. Serafini, P. Brézillon, M. Benerecetti, F. Castellani (Eds.), Modeling and Using Context. Proceedings, 1999. XII, 528 pages. 1999. (Subseries LNAI).

Vol. 1689: F. Solina, A. Leonardis (Eds.), Computer Analysis of Images and Patterns. Proceedings, 1999. XIV, 650 pages. 1999.

Vol. 1690: Y. Bertot, G. Dowek, A. Hirschowitz, C. Paulin, L. Théry (Eds.), Theorem Proving in Higher Order Logics. Proceedings, 1999. VIII, 359 pages. 1999.

Vol. 1691: J. Eder, I. Rozman, T. Welzer (Eds.), Advances in Databases and Information Systems. Proceedings, 1999. XIII, 383 pages. 1999.

Vol. 1692: V. Matoušek, P. Mautner, J. Ocelíková, P. Sojka (Eds.), Text, Speech and Dialogue. Proceedings, 1999. XI, 396 pages. 1999. (Subseries LNAI).

Vol. 1693: P. Jayanti (Ed.), Distributed Computing. Proceedings, 1999. X, 357 pages. 1999.

Vol. 1694: A. Cortesi, G. Filé (Eds.), Static Analysis. Proceedings, 1999. VIII, 357 pages. 1999.

Vol. 1695: P. Barahona, J.J. Alferes (Eds.), Progress in Artificial Intelligence. Proceedings, 1999. XI, 385 pages. 1999. (Subseries LNAI).

Vol. 1696: S. Abiteboul, A.-M. Vercoustre (Eds.), Research and Advanced Technology for Digital Libraries. Proceedings, 1999. XII, 497 pages. 1999.

Vol. 1697: J. Dongarra, E. Luque, T. Margalef (Eds.), Recent Advances in Parallel Virtual Machine and Message Passing Interface. Proceedings, 1999. XVII, 551 pages. 1999.

Vol. 1698: M. Felici, K. Kanoun, A. Pasquini (Eds.), Computer Safety, Reliability and Security. Proceedings, 1999. XVIII, 482 pages. 1999.

Vol. 1699: S. Albayrak (Ed.), Intelligent Agents for Telecommunication Applications. Proceedings, 1999. IX, 191 pages. 1999. (Subseries LNAI).

Vol. 1700: R. Stadler, B. Stiller (Eds.), Active Technologies for Network and Service Management. Proceedings, 1999. XII, 299 pages. 1999.

Vol. 1701: W. Burgard, T. Christaller, A.B. Cremers (Eds.), KI-99: Advances in Artificial Intelligence. Proceedings, 1999. XI, 311 pages. 1999. (Subseries LNAI).

Vol. 1702: G. Nadathur (Ed.), Principles and Practice of Declarative Programming. Proceedings, 1999. X, 434 pages. 1999.

Vol. 1703: L. Pierre, T. Kropf (Eds.), Correct Hardware Design and Verification Methods. Proceedings, 1999. XI, 366 pages. 1999.

Vol. 1704: Jan M. Żytkow, J. Rauch (Eds.), Principles of Data Mining and Knowledge Discovery. Proceedings, 1999. XIV, 593 pages. 1999. (Subseries LNAI).

Vol. 1705: H. Ganzinger, D. McAllester, A. Voronkov (Eds.), Logic for Programming and Automated Reasoning. Proceedings, 1999. XII, 397 pages. 1999. (Subseries LNAI).

Vol. 1706: J. Hatcliff, T. Æ. Mogensen, P. Thiemann (Eds.), Lectures on Partial Evaluation. Proceedings, 1998. IX, 433 pages. 1999. (Subseries LNAI).

Vol. 1707: H.-W. Gellersen (Ed.), Handheld and Ubiquitous Computing. Proceedings, 1999. XII, 390 pages. 1999.

Vol. 1708: J.M. Wing, J. Woodcock, J. Davies (Eds.), FM'99 – Formal Methods. Proceedings Vol. I, 1999. XVIII, 937 pages. 1999.

Vol. 1709: J.M. Wing, J. Woodcock, J. Davies (Eds.), FM'99 – Formal Methods. Proceedings Vol. II, 1999. XVIII, 937 pages. 1999.

Vol. 1710: E.-R. Olderog, B. Steffen (Eds.), Correct System Design. XIV, 417 pages. 1999.

Vol. 1711: N. Zhong, A. Skowron, S. Ohsuga (Eds.), New Directions in Rough Sets, Data Mining, and Granular-Soft Computing. Proceedings, 1999. XIV, 558 pages. 1999. (Subseries LNAI).

Vol. 1712: H. Boley, A Tight, Practical Integration of Relations and Functions. XI, 169 pages. 1999. (Subseries LNAI).

Vol. 1713: J. Jaffar (Ed.), Principles and Practice of Constraint Programming – CP'99. Proceedings, 1999. XII, 493 pages. 1999.

Vol. 1714: M.T. Pazienza (Eds.), Information Extraction. IX, 165 pages. 1999. (Subseries LNAI).

Vol. 1715: P. Perner, M. Petrou (Eds.), Machine Learning and Data Mining in Pattern Recognition. Proceedings, 1999. VIII, 217 pages. 1999. (Subseries LNAI).

Vol. 1716: K.Y. Lam, E. Okamoto, C. Xing (Eds.), Advances in Cryptology – ASIACRYPT'99. Proceedings, 1999. XI, 414 pages. 1999.

Vol. 1717: Ç. K. Koç, C. Paar (Eds.), Cryptographic Hardware and Embedded Systems. Proceedings, 1999. XI, 353 pages. 1999.

Vol. 1718: M. Diaz, P. Owezarski, P. Sénac (Eds.), Interactive Distributed Multimedia Systems and Telecommunication Services. Proceedings, 1999. XI, 386 pages. 1999.

Vol. 1719: M. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proceedings. 1999. XIII, 510 pages. 1999.

Vol. 1721: S. Arikawa, K. Furukawa (Eds.), Discovery Science. Proceedings, 1999. XI, 374 pages. 1999. (Subseries LNAI).

Vol. 1722: A. Middeldorp, T. Sato (Eds.), Functional and Logic Programming. Proceedings, 1999. X, 369 pages. 1999.

Vol. 1723: R. France, B. Rumpe (Eds.), UML'99 – The Unified Modeling Language99. XVII, 724 pages. 1999.

Vol. 1726: V. Varadharajan, Y. Mu (Eds.), Information and Communication Security. Proceedings, 1999. XI, 325 pages. 1999.

Vol. 1727: P.P. Chen, D.W. Embley, J. Kouloumdjian, S.W. Liddle, J.F. Roddick (Eds.), Advances in Conceptual Modeling. Proceedings, 1999. XI, 389 pages. 1999.

Vol. 1728: J. Akoka, M. Bouzeghoub, I. Comyn-Wattiau, E. Métais (Eds.), Conceptual Modeling – ER '99. Proceedings, 1999. XIV, 540 pages. 1999.

Vol. 1729: M. Mambo, Y. Zheng (Eds.), Information Security. Proceedings, 1999. IX, 277 pages. 1999.

Vol. 1734: H. Hellwagner, A. Reinefeld (Eds.), SCI: Scalable Coherent Interface. XXI, 490 pages. 1999.

Vol. 1564: M. Vazirgiannis, Interactive Multimedia Documents. XIII, 161 pages. 1999.

Vol. 1591: D.J. Duke, I. Herman, S. Marshall, PREMO: A Framework for Multimedia Middleware. XII, 254 pages. 1999.

CONTENTS

KEYNOTE SPEECH

International Cryptography

Doug McGowan
Hewlett-Packard, USA

Abstract

Cryptography is a fundamental security technology. It is used in applications ranging from authentication and digital signatures to protecting the privacy and integrity of emails and other forms of interactions. Besides a technology, cryptography has become a topic for front page news. Governments around the world are debating and passing laws concerning the export and (sometimes) the use of cryptography. This talk will discuss the current international scene for cryptography technology. We will discuss today's situation with regards to cryptography export as well as future trends. We will also discuss some new technologies that may provide solutions for manufacturers and software developers while complying with international regulations.

Reaction Attacks Against Several Public-Key Cryptosystems

Chris Hall[1], Ian Goldberg[2], and Bruce Schneier[1]

[1] Counterpane Systems
hall,schneier@counterpane.com
101 E. Minnehaha Pkwy
Minneapolis, MN 55419
(612) 832-1098

[2] U.C. at Berkeley
iang@cs.berkeley.edu
Soda Hall
Berkeley, CA 94720-1776

Abstract. We present attacks against the McEliece Public-Key Cryptosystem, the Atjai-Dwork Public-Key Cryptosystem, and variants of those systems. Most of these systems base their security on the apparent intractibility of one or more problems. The attacks we present do not violate the intractibility of the underlying problems, but instead obtain information about the private key or plaintext by watching the reaction of someone decrypting a given ciphertext with the private key. In the case of the McEliece system we must repeat the attack for each ciphertext we wish to decrypt, whereas for the Ajtai-Dwork system we are able to recover the private key.

Keywords: public-key cryptosystems, lattice-based cryptosystems, error-correcting codes, Ajtai-Dwork lattice cryptosystem, McEliece.

1 Introduction

In an attempt to design cryptosystems based upon (believed) intractible problems different from factoring and discrete logarithms, several public-key cryptosystems have been presented, including the two systems in [M78,AD97]. The first system is based upon the intractibility of decoding an arbitrary error-correcting code, and the second upon finding the shortest vector in a lattice. The authors of the former rely upon the fact that the respective problem is known to be **NP**-complete. However, it is not known whether the particular instances used in their cryptosystem are equally difficult to solve. The general shortest vector problem is known to be **NP**-hard, but the lattice-based systems depend on the apparent difficulty of an easier shortest vector lattice problem (the unique shortest vector lattice problem). We refer the reader to [AD97] for more details.

In this paper we present attacks against the McEliece Public-Key Cryptosystem (PKC), a McEliece variant [HR88], the Ajtai-Dwork PKC, and a modified version of the Ajtai-Dwork PKC that appears in [GGH97]. In these attacks an attacker presents the owner of the private key with a ciphertext that may contain one or more errors (that is, the ciphertext may decrypt to a plaintext which fails a simple signature or checksum verification). By watching the reaction of the owner in order to determine whether or not the ciphertext decrypted correctly, the attacker can usually determine information about the plaintext (in the McEliece system) or the private key (in the Ajtai-Dwork systems).

We feel that this is a legitimate class of attacks that one must be careful to guard against when implementing systems that use these ciphers. In the simplest case one may have a tamper-resistance module (such as a smartcard) which contains a copy of the secret key. By feeding erroneous ciphertexts to the card, one may be able to decrypt ciphertexts without the private key or even recover the private key. In other systems one may have to rely upon social engineering to finesse the attacks, but that's a small price if one can recover the private key. The basic principle behind the attack is that someone's reaction to a question often reveals information that they didn't intend to give.

The organization of our paper is as follows. In section 2 we describe the McEliece PKC, as well as a variant of it, and attacks against them. In section 3 we describe the original Ajtai-Dwork PKC as presented in [AD97], a modified version that appears in [GGH97], and attacks against both of these systems. Finally, in section 4 we discuss the properties of these public-key cryptosystems which allowed our attacks to work in order to try and give some design criterion for new public-key cryptosystems so that they will not be vulnerable to the same sort of attack.

2 McEliece

In [M78], McEliece outlined a public-key cryptosystem based upon error correcting codes. A user chooses a $n \times k$ generator matrix G (for a (n, k) error-correcting code which can correct up to t errors), a $k \times k$ non-singular matrix S, a $n \times n$ permutation matrix P, and publishes the matrix $G' = SGP$ as his public key. To encrypt a message a user chooses a random vector Z of weight t and sends:

$$C = MG' + Z.$$

To decrypt the message, the owner of the key computes:

$$CP^{-1} = MSG + ZP^{-1}$$

and corrects the t-bit error ZP^{-1} using the known error-correction algorithm. After that M can be recovered using S^{-1}.

This system, like other systems [HR88,J83,N86], depends on the fact that in the worst case, decoding an arbitrary error-correcting code is NP-complete [BMvT78]. It is hoped that G' represents one of these difficult cases.

Since their introduction, public-key cryptosytems based on error-correcting codes have largely been of theoretical interest. They require enormous keys in order to achieve comparible security to currently implemented public-key cryptosystems based on factoring or the discrete logarithm problem. For example, the purported attack in [KT91] can break a cryptosystem based on a $(1024, 654)$ BCH code in 60 hours. Such a key would require a 654-kilobit generator matrix for part of the public key. This would seem to imply that secure keys would require one or more megabytes of storage for the generator matrix alone. Compare this to a 1024-bit RSA key which needs only a little more than 1Kb of storage and provides excellent security.

Large keys aside, error-correcting code cryptosystems have been touted as a potential saviour of public-key cryptography. These systems are based on the syndrome-decoding problem which was shown to be NP-complete in [BMvT78]. Other public-key cryptosystems, such as RSA, are based on problems such as factoring which are only thought to be difficult. It is possible that someone will discover an efficient factoring algorithm, whereas it would require proving that $P = NP$ to find an efficient general syndrome-decoding algorithm. Note, NP-completeness only implies that the worst case is hard to solve. It may be possible that the instances of problems produced by PKCs such as [M78] are much easier to solve.

Until recently, the two best attacks against McEliece's system appear in [AM87,KT91]. The attack in [AM87] relies on choosing k bits in an n-bit ciphertext that do not contain any errors. Given that the t incorrect bits are unknown, the probability of this event happening is low. However, once it occurs, one can solve for the message M using an algorithm outlined in the paper.

The attack outlined in [KT91] requires $O(n^3)$ operations for an arbitrary (n, k) code. It determines the error vector for the ciphertext C. The basic premise behind the attack is that a polynomial-time algorithm is introduced which will determine the error pattern for a received vector provided that the error pattern has weight at most $[(d-1)/2]$ (where d is the minimum distance of the code). The discovery of this algorithm does not contradict the NP-completness proof of [BMvT78] because it only corrects error patterns of weight at most $[(d-1)/2]$. If the received vector is further than $[(d-1)/2]$ from every codeword, then this algorithm cannot decode the vector to a codeword. Note, while the basic attack was outlined in [KT91], further information about the attack has failed to appear. It is possible that the authors were not able to make their attack scale as they had wished (when they present it, they had only run it against a toy problem).

An even more recent attack against the McEliece PKC was presented in [B97]. This attack relied about known linear relationships between two different ciphertexts (really their underlying plaintexts) in order to determine the error vectors used in encrypting the plaintexts. The author is quick to point out that the attack does not "break" the cryptosystem in the sense that it does not recover the private key, but it is still an interesting attack to note.