A Secure, Accountable, and Collaborative Whiteboard

Werner Geyer and Rüdiger Weis

Praktische Informatik IV
University of Mannheim, 68131 Mannheim, Germany
{geyer,rweis}@pi4.informatik.uni-mannheim.de

Abstract. This paper addresses the design issues and the security concept of the digital lecture board which is an enhanced whiteboard tailored to the specific needs of collaborative types of work, for instance, in computer–based distance education. The development of the digital lecture board emerged from our experiences with synchronous, computer–based distance education in the TeleTeaching projects of the University of Mannheim. For almost two years, we have been using video conferencing tools for transmitting lectures and seminars. These tools prove to be far from optimal for this purpose since they do not take into account the specific requirements of teaching. Security issues such as authentication, secure key exchange, and fast symmetric encryption are almost completely neglected, even though security is extremely important to allow for confidential, private sessions, and billing.

1 Introduction

Computer–based video conferencing is one of today's most exciting multimedia applications. Powerful hardware and advances in communication technology have enabled the synchronous transmission of audio and video even over low–bandwidth networks, such as ISDN, in an acceptable quality. Besides pure teleconferencing, these systems are employed in a variety of application fields such as distance education, teleconsulting, telemedicine, telecooperation etc. Most of these advanced application fields impose a high demand on additional functionality, which is not satisfied by existing video conferencing software. Specifically, most systems do not provide secure data delivery or accounting. Moreover, the systems are not tailored to their field of application, i.e. video conferencing systems are too limited in their functionality for these more advanced applications. This concerns specifically the support of collaborative types of work.

The shared whiteboard is often the core part of these systems since it is used to transmit additional contents (e.g. slides) besides audio and video. In this paper, we present a novel whiteboard – called *digital lecture board* (dlb) – which is being developed in the context of computer–based distance education, i.e. the whiteboard takes into account the specific requirements of synchronous teaching and learning in higher education, continuous education or corporate education [GeEf98]. The development of the dlb has been motivated by the experiences we

T. Plagemann and V. Goebel (Eds.): IDMS'98, LNCS 1483, pp. 3-14, 1998.

gathered in the TeleTeaching projects of the University of Mannheim where, for almost two years, lectures and seminars have been transmitted using standard video conferencing tools [Ecea97].

In the first part of this paper, we discuss shortcomings of existing video conferencing tools and describe features, we had in mind while designing the digital lecture board. We then present our security concept which is a user–oriented approach taking into account the specific security requirements of different user groups. The last section covers implementation issues of the current prototype.

2 Related Work

Many existing video conferencing systems such as NetMeeting, CUSeeMe, ProShare, or PictureTel provide audio, video, application sharing, and standard whiteboard features but consider neither security issues nor the specific requirements of collaborative types of work, such as reference pointing, raising hands, forming work groups, controlling the course of instruction etc. The MBone tools vic (video conferencing tool), vat (visual audio tool), and wb (whiteboard) actually support security but only weak DES encryption [MaBr94]. Due to export limitations, the DES encryption cannot be used legally outside the US.

For the platform–independent whiteboard TeleDraw [TeDr98], which is being developed in the context of the MERCI project [MERCI98], it is planned to include MERCI security enhancements; the current version is still insecure. Since TeleDraw has been designed for video conferencing, it also does not consider requirements of collaborative work.

Security within the MERCI project is basically realized by the Secure Conferencing User Agent (SCUA), developed by GMD [Hiea96] . SCUA is an email–based approach which allows to initiate conferences securely using PEM (Privacy Enhanced Mail). For the actual transmission of data, SCUA relies on the built–in weak security mechanisms of the MBone tools. After key exchange, the tools have to be started with the session key as a parameter or the key has to be introduced by hand.

The following two projects focus on the specific needs of teleteaching but do not consider security issues: The "Authoring on the Fly" (AOF) concept [BaOt96] merges broadcasting of a lectures with authoring of CBT software. With AOF, lectures are transmitted by means of an extended whiteboard to a number of receivers. Interactivity is limited to audio and video, the whiteboard has no back channel. Thus, collaborative types of instruction are not supported.

The Interactive Remote Instruction (IRI) system developed at Old Dominion University [Maea96] is a very powerful, integrated teaching and learning environment. The system allows to view or make multimedia class presentations, to take notes in a notebook, and to interact via audio/video and shared tools. The system differs from ours in that IRI partly relies on analog transmission of NTSC video signals. Collaboration is limited to application sharing and the secure transmission of data is not supported.

3 The Digital Lecture Board

3.1 Motivation

The digital lecture board is being developed in the context of the TeleTeaching project of the University of Mannheim [Ecea97]. The project aims at an improvement in quality and quantity of teaching and learning by using multimedia technology and high speed networks for the distribution of lectures and seminars. We have implemented three different instructional settings which are characterized by their scope of distribution, interactivity, and individualization of the learning process. In the *Remote Lecture Room* (RLR) scenario, large lecture rooms, equipped with audio/video facilities, are connected via high speed networks, and courses are exchanged synchronously and interactively between participating institutions. *Remote Interactive Seminars* (RIS) describe a more interactive type of instruction. Small groups of participants are distributed across few seminar rooms which are also connected by a network. The focus of RIS is the cooperative, on–line construction and presentation of reports. The *Interactive Home Learning* (IHL) scenario aims at a maximization of the distribution degree of all class participants. Each students learns asynchronously as well as synchronously at home in front of his or her PC.

We use the Internet and the MBone video conferencing tools for remote lecturing. Observations, surveys, and interviews with the students and lecturers during the last two years indicate that these tools can provide satisfactory results if the lecturer adapts the layout of the lecture exactly to the limited features of these tools. But they are far from optimal for teleteaching since they have not been designed for this purpose. This concerns specifically the whiteboard, which can be considered to be a substitute for the traditional blackboard. Along with audio, the whiteboard is most important for conveying knowledge to distributed participants. In order to overcome the weaknesses of the whiteboard, we decided to develop the digital lecture board (dlb) which will better satisfy the needs of computer–based teaching and learning.

3.2 Functional Requirements

In this Section, we present, in more detail, the shortcomings of the existing MBone tools[1], and we discuss the most important features which we had in mind when designing the dlb.

Integrated User Interface. The MBone tools do not provide an integrated user interface. Teachers and students complained about many confusing windows and control panels which are not important for remote instruction but make it more difficult to operate the tools. Since computer–based distance education should not be restricted to computer experts, we find it especially important

[1] The described shortcomings more or less concern also other video conferencing systems such as NetMeeting, CuSeeMe etc.

that the dlb provides an easy–to–operate user interface which integrates also audio and video communication. In order to allow the interface to adapt to different instructional settings, it should be configurable.

Media Usage and Handling. One of the most limiting factors of the MBone whiteboard is media usage and handling: only postscript and plain ASCII text are supported as external input formats, and the later or joint editing of the built–in graphic and text objects is not possible. For instance it is not possible for a distributed group to create a common text or graphic, or to modify objects created by different participants. Since media are very important for a modern instruction, the dlb should support a variety of media formats (e.g. GIF, HTML, AIFF, MPEG etc.) as well as many built–in object types (e.g. lines, rectangles, circles, text etc.). Objects must be editable by every participant, and the dlb should provide functions like select, cut, copy, paste, group, raise, lower etc. similar to a word or graphic processing software.

Workspace Paradigm. The shared workspace of wb is limited to a two–layer concept with a postscript slide in the background and drawings and text in the foreground. It is, for instance, not possible to render two different postscript slides onto a single page so that results of two distributed work groups may be compared. Moreover, participants cannot have a private workspace where they can prepare materials, for instance, when doing on–line group work. Modern telecooperation software requires a more flexible workspace concept with multiple layers where arbitrary media objects (audio, video, images, animations etc.) can be displayed, grouped, raised, lowered etc. Single participants or small groups should be offered private workspaces (invisible to the rest of the whole group) in order to allow for modern types of instruction such as group work. The outcome of the group work can be transferred to the shared workspace so as to allow a wider discussion of the results.

Collaborative Services. Today's video conferencing systems suffer a lack of communication channels compared to the traditional face–to–face situation. Social protocols or rules, which control the human interaction and the course of instruction in a classroom, are not automatically available in a remote situation and are difficult to reproduce. These mechanisms include, for instance, raising hands, giving the right to talk or to write on the black board, setting up work groups, and reference pointing. Collaborative services provide mechanisms to support the communication of persons through computers and to increase social awareness. In this sense, collaborative services provide an electronic surrogate to compensate as far as possible for the lack of inter–personal communication channels. Basic services such as floor control, session control, telepointers, or voting should be supported by the dlb. Floor control realizes concurrency control for interactive, synchronous cooperation between people by using the metaphor of a *floor*. A floor is basically a temporary permission to access and manipulate shared resources (e.g. a shared drawing area). Session control denotes the

administration of multiple sessions with its participants and media. Session control increases social awareness in distributed work groups because members gain knowledge of each other and their status in the session. A detailed analysis of collaborative requirements in teleteaching for the dlb can be found in [HiGe97].

Synchronized Recording and Playback of Sessions. The dlb should also provide the possibility to record a transmitted lecture or course including all media streams (audio, video, whiteboard actions and media, telepointers etc.). Students will then be able to retrieve the lecture in order to review certain topics, or the complete lecture if they have missed it. In order to achieve a synchronized recording, data has to be time–stamped. The data streams could then be recorded by existing systems like the VCRoD service (Video Conference Recording on Demand) [Holf97] . These systems rely on the Real–Time Transport Protocol RTP for synchronized recording [Schea96]. The current release of the MBone whiteboard wb does not implement the RTP standard.

Storage and Retrieval of Pages and Teaching Materials. Lectures or courses given with the computer need to be prepared in advance like any lecture, i.e. producing slides, images, animations etc. The preparation of materials with the MBone whiteboard is limited to a list of postscript files which can be imported by mouse click during a session. In order to allow for a better preparation of on–line lectures and for saving results after a lecture, the dlb should support storage and retrieval of pages and objects in a structured, standardized file format such as SGML. Moreover, it would also be desirable for the dlb to have access to a multimedia database which stores teaching and learning materials of teachers and students.

4 Secure Communication

The exponential growth of the Internet in recent years has fostered the importance of secure communication. Security has become a major research task in computer science. Especially for commercial applications, security in the Internet is a "conditio sine qua non".

4.1 State–of–the–Art

The well–known DES encryption algorithm, which was originally designed for confidential, not–classified data, is used in many applications today (e.g. electronic banking). The MBone whiteboard wb also relies on DES for encryption. The weaknesses of DES have been disclosed by several brute force attacks , which indicate that the key length for symmetrical algorithms should be at least 75–90 bits [Blea96].

DES was originally developed for the hardware of the seventies. Many multimedia applications today have high demands on performance, which cannot be

satisfied by DES software encryption. In recent years, novel algorithms with better performance but similar to the DES scheme have been developed [Weis98]. Some of these algorithms are even specifically designed for fast software encryption on modern processor generations or for bulk encryption. Due to export restrictions of the US government, export versions of many software products have the DES encoding disabled. Hence, outside the US, the DES encryption feature of wb cannot be used. Moreover, the source code of wb is not publicly available which inhibits the evaluation or modification of the cryptographic implementation.

These security limitations of the MBone whiteboard have stimulated the integration of modern encryption algorithms into the digital lecture board in order to provide secure video conferencing with a powerful, collaborative whiteboard also outside the US.

4.2 Security Requirements

Besides the functional requirements described in Section 3.2, a secure digital lecture board has to satisfy the following security requirements:

- **Fast symmetric encryption** for the secure transmission of confidential whiteboard data. Data streams will be encrypted by the use of a session key.
- **Flexibility for different user groups** with different requirements concerning legal issues, costs, level of security, and performance.
- **Strong and flexible public key cryptography** allows for authentication and automated, secure exchange of session keys.
- **Light–weight payment protocols** are required for the automated billing of telecourses and teleseminars which are offered by educational institutes or by companies. Since the group of session participants may be rather large and the paid amounts rather small, we prefer light–weight protocols with minimal overhead.
- **New voting schemes** for light–weight and secure voting in a session. Voting as a collaborative service adds an additional communication channel to a distributed group which increases social awareness (see Chapter 3).

4.3 Security Concept

User–Orientated Cryptography. The digital lecture board dlb uses a flexible user–oriented security concept which can be adapted to different user requirements. Users may choose from predefined security profiles or even customize their own security requirements. The choice may be driven, for instance, by legal issues, costs, required level of security, and performance. We identify the following main profiles or user groups: *public research*, *financial services*, and *innovative companies*.

Since users who work in the *public research* often benefit from license–free employment of patented algorithms, we rely on the *IDEA* cipher [Lai92]. The algorithm has a strong mathematical foundation and possesses good resistance

against differential cryptoanalysis. The key length of 128 bit immunizes against brute force attacks. IDEA was the preferred cipher in the PGP–Versions (Pretty Good Privacy) until 2.63. However, commercial users have to pay high license fees.

In the *financial services* business we find a strong preference for DES–based systems. Since DES has been cracked by brute force attacks, we suggest to use *Triple–DES*, *DESX* or *DES²X* in this application field. In addition to the fact that Triple–DES has a poor performance, it also does not provide the same high security level like IDEA. Recent work of Stefan Lucks showed that the effective key length for exhaustive search attacks can be reduced to 108 bits [Luck98a] while still being immune against brute force attacks. A cheaper method to avoid brute force attacks on DES is whitening. With one key–depended permutation before and after the DES encryption, exhaustive key search is provably not feasible. RSA Data Security Inc uses this procedure under the name DESX [KiRo96] in their toolkit BSAFE. In addition, we have implemented DES²X [Luck98b] which combines whitening and double encryption. It seems that DES²X is more secure and faster than Triple–DES.

For *innovative companies,* which are not afraid of new algorithms, we use the novel, license–free algorithm *CAST*. CAST is a very fast DES–like Substitution–Permutation Network cryptosystem designed by Carlisle Adams and Stafford Tavares. The system has rather good resistance to differential cryptoanalysis, linear cryptanalysis, and related–key cryptoanalysis. The CAST–128 [RFC2144] implementation uses 128 bit keys. CAST possesses a number of other desirable cryptographic advantages compared to DES, e.g. no complementation property and an absence of weak and semi–weak keys. CAST is the preferred cipher in the PGP–Versions 5.x.

In addition to these predefined user profiles, we have implemented options for full compatibility to *PGP 2.63i*, *PGP 5.x* and *GPG* [Koch98]. GPG is a free PGP replacement which does not rely on patented algorithms. For users with low computing power, speed issues are most important. *Blowfish* [Schn94] is one of the fastest secure block ciphers which encrypts plaintext on 32–bit microprocessors at a rate of 26 block cycles per byte while being very compact. It was designed by Bruce Schneier with a variable key length up to 448 bit. We use a key length of 128 bit for the Open–PGP Blowfish–128 and 160 bit for GPG compatibility.

Table 1: Predefined Profiles.

Profile	**Public key**	**Secret key**	**Hash**
Public research	Rabin	IDEA	RIPEMD–160
Financial services	RSA	Triple–DES	RIPEMD–160
Innovative companies	Rabin	CAST	RIPEMD–160
PGP 2.63i	RSA	IDEA	MD5
PGP 5.x	DLP	CAST	SHA–1
GPG	DLP	Blowfish	RIPEMD–160

Automatic Key Exchange and Authentication. For authentication and to simplify the key exchange, we use asymmetric cryptography. In addition to *RSA,* we offer signature and key exchange procedures based on the *Discrete Logarithm Problem* (ElGamal/DSA) in order to avoid problems with US patents.

We have also included *Rabin's* scheme for key exchange and signatures. Rabin's scheme achieves security through the difficulty of finding square roots modulo a composite number, which is equivalent to factorization. Due to this fact, Rabin's scheme is *provably* at least as secure as RSA. Rabin encryption needs only one modular squaring which provides faster encryption than in RSA. After decryption of the session key, we get four possible results. Using a specific padding designed by Lucks and Weis, we can easily find the right result.

This Scheme improves cryptographic security and strengthens Rabin against several attacks [LuWe98a].

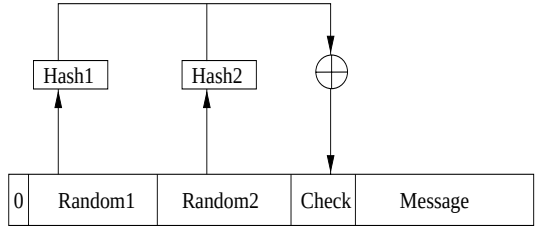

Fig. 1. Simple Scheme of redundant use of random oracles [LuWe98b].

As innovative, new procedure group, we further implement ElGamal and DSA procedures over *elliptic curves.* These cryptosystems are assumed to provide the same security as the discussed RSA scheme while operating with a shorter key length. This allows, for instance, for shorter signatures, reduced communication, less storage space, and faster computation.

4.4 Research Issues

Fast Multimedia Encryption. All presented algorithms are well tested and state–of–the–art in cryptography. But we are also developing new algorithms for fast software encryption of continuous multimedia streams. A very interesting idea is to use *Luby–Rackoff* [LuRa88] ciphers. These ciphers can operate very fast on large block sizes [Luck96a]. Anderson and Biham have proposed two fast block ciphers: *Lion* and *BEAR* [AnBi96]. The fastest new algorithm in this class is *BEAST* (Block Encryption Algorithm with Shortcut in the Third round) [Luck96b]. BEAST is assembled from key–dependent hash functions and a stream cipher and it is *provably* secure if these building blocks are secure. The performance is very good when operating on large blocks sizes. We have tested different versions of BEAST in a real application for the first time [WeLu98].

Light–weight Payment. Based on encrypted communication, it is rather easy to implement light–weight payment protocols. After the transmission of an electronic coin, the current session key – encrypted with the public key of the client (payer) – is transmitted. This method of separating encrypted multi-/broadcast transmission of the bulk data and the key transmission can be found in many distributed multimedia systems. Since for many information on the Internet only small and inexpensive payments are acceptable, some light–weight payment systems have been developed.

The *Payword* system proposed by Rivest and Shamir seems to be most suitable [RiSh96]. Payword uses the values of a hash chain as coins. This idea can be also found in the S/Key–protocol of Lamport [Lamp81]. The cost for the required calculations is very low. Even the frequently required verification of a payment needs only one hash. According to Rivest and Shamir, the calculation of a hash function is up to ten thousand times faster than public key operations. Therefore, we will rely on the payword scheme for billing multimedia applications.

Voting Schemes. The implementation of secure election and voting as a collaborative service is subject to current research. One idea is to build a "Virtual Hyde Park" where the participants can decide in a confidential vote who should manage the floor. So far, no light–weight, group–oriented, and secure voting schemes are known.

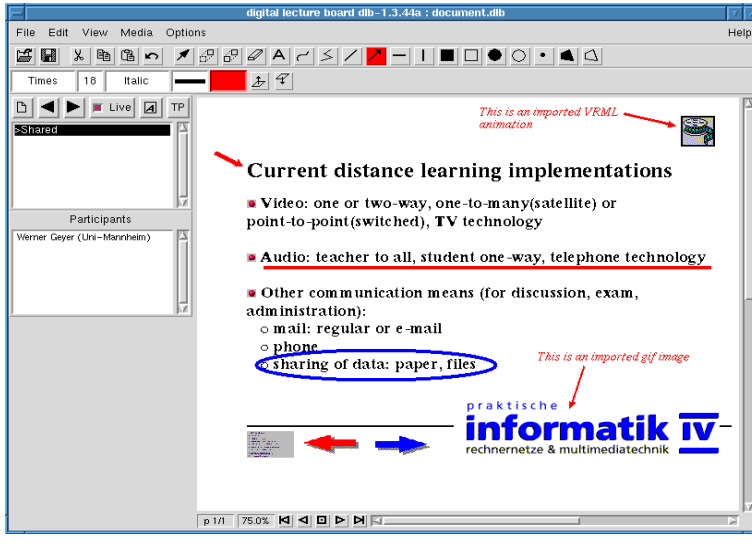

Fig. 2. User interface of the digital lecture board.

5 Implementation Issues

The prototype implementation of the digital lecture board includes already pretty much all of the features mentioned in Chapter 3 as well as the security concept described in Chapter 4. We do not have integrated audio and video communication yet; the interface to our VCRoD system is in preparation. For a high degree of portability, we implemented the prototype in C++ and the Tcl/Tk scripting language [Oust94], and we took great care to reuse only components which are available on all major platforms. Figure 2 shows a screen shot of dlb's user interface.

The security concept described above is integrated directly in the core part of the digital lecture board as indicated in Figure 3. We have implemented a security library, which includes the cryptographic algorithms and protocols discussed in the previous Chapter. The library provides full compatibility with the Open–PGP standard [OPGP97], i.e. dlb's RTP data packets are wrapped in OPGP packets. We then use either unreliable UDP connections (e.g. for telepointers) or reliable SMP connections to transmit the OPGP/RTP packets. SMP (scalable multicast protocol) is a reliable transport service which has been specifically developed for the dlb. Security functionality can be accessed and controlled through dlb's graphical user interface or via command line parameters.

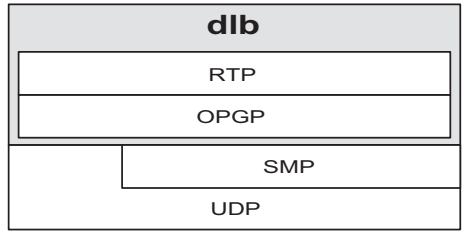

Fig. 3. Communication protocols.

6 Conclusion

Our experience with computer–based distance education indicates that standard video conferencing systems are far from optimal for collaborative types of instruction or work. Furthermore, they almost completely neglect security issues. As a consequence, we have developed the digital lecture board presented in this paper. The digital lecture board is an integrated, extended whiteboard tool which is tailored to the specific needs of computer–based distance education, but also integrates state–of–the–art security mechanisms. The digital lecture board can also be employed for high–secure video conferencing with extended demands on collaboration and media flexibility. Future research directions are distributed

VRML animations for the dlb, light–weight payment protocols and a novel secure voting scheme.

7 Acknowledgment

The authors would like to thank Prof. Dr. Wolfgang Effelsberg and Dr. Stefan Lucks for helpful comments and interesting discussions.

References

[AnBi96] Anderson, R., Biham, E., "Two Practical and Provable Secure Blockciphers: BEAR and LION", Proc. Fast Software Encryption (ed. D. Gollmann), LNCS 1039, Springer, 1996.

[BaOt96] Bacher, C., Ottmann, T., "Tools and Services for Authoring on the Fly", Proc. ED–MEDIA'96, Boston 1996.

[Blea96] Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E., Wiener, M., "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security", a report by an ad hoc group of cryptographers and computer scientists , January 1996.

[Ecea97] Eckert, A., Geyer, W., Effelsberg, W., "A Distance Learning System for Higher Education Based on Telecommunications and Multimedia – A Compound Organizational, Pedagogical, and Technical Approach", Proc. ED–MEDIA'97, Calgary, June 1997.

[GeEf98] Geyer, W., Effelsberg, W., "The Digital Lecture Board – A Teaching and Learning Tool for Remote Instruction in Higher Education", accepted at ED–MEDIA'98, Freiburg, Germany, June 1998.

[Geea97] Geyer, W., Eckert, A., Effelsberg, W. ,"Multimedia Technologie zur Unterstützung der Lehre an Hochschulen" (in German). To appear in: Multimediales Lernen in der beruflichen Bildung, Verlag BW, Nürnberg 1997.

[HiGe97] Hilt, V., Geyer, W., "A Model for Collaborative Services in Distributed Learning Environments", Proc. of IDMS'97, Darmstadt, LNCS 1309, 1997, pp. 364 –375.

[Hiea96] Hinsch, E., Jaegemann, A., Wang, L., "The Secure Conferencing User Agent – A Tool to Provide Secure Conferencing with MBONE Multimedia Conferencing Applications". Proc. IDMS'96, Berlin, LNCS 1045, 1996, pp. 131–142.

[Holf97] Holfelder, W., "Interactive Remote Recording and Playback of Multicast Videoconferences", Proc. IDMS'97, Darmstadt, LNCS 1309, 1997.

[KiRo96] Kilian, J., Rogaway, P., "How to protect DES against exhaustive key search", Proc. Advances in Cryptology–Crypto'96, Berlin, Springer, 1996.

[Koch98] Koch, Werner, "GPG – The free PGP Replacement", 1998. http://www.d.shuttle.de/isil/gnupg.html

[Lai92] X. Lai, "On the Design and Security of Blockciphers", ETH Series in Information Processing, v. 1, Hartmut–Gorre–Verlag, Konstanz, 1992.

[Lamp81] Lamport, L., "Password Authentication with Insecure Communication", Communications of the ACM 24(11), November 1981.

[LuRa88] Luby, M., Rackoff, C., "How to construct pseudorandom permutations from pseudo random functions", SIAM J. Computing, V17, N2, 1988.

[Luck96a] Lucks, S., "Faster Luby–Rackoff ciphers", Proc. Fast Software Encryption (ed. D. Gollmann), LNCS 1039, Springer, 1996.

[Luck96b] Lucks, S., "BEAST: A fast block cipher for arbitrary blocksize", (ed. Hoprster, P.), Proc. IFIP'96, Conference on Communication and Multimedia Security, Chapman & Hall, 1996, pp. 144–153.

[Luck98a] Lucks, S., "Attacking Triple Encryption", Proc. Fast Software Encryption 5, 1998, (ed. S. Vaudenay), LNCS 1372, Springer, 1998.

[Luck98b] Lucks, S., "On the Power of Whitening", Manuscript, Universtität Mannheim, Fakultät für Mathematik und Informatik, 1998.

[LuWe98a] Lucks, S., Weis, R., "How to Encrypt with Rabin", Technical Report, Universtität Mannheim, Fakultät Mathematik und Informatik, 1998.

[LuWe98b] Lucks, S., Weis, R., "Improced Security throw Redundant Random Oracle", Technical Report, Universtität Mannheim, Fakultät Mathematik und Informatik, 1998.

[MaBr94] Macedonia, M.R., Brutzmann, D.P., "MBone Provides Audio and Video Across the Internet", IEEE Computer. 27(4), 1994.

[Maea96] Maly, K., Wild, C., Overstreet, C., Abdel–Wahab, H., Gupta, A., Youssef, A., Stoica, E., Talla, R.,Prabhu, A., "Virtual Classrooms and Interactive Remote Instruction", International Journal of Innovations in Education", 34(1), 1996, pp. 44–51.

[MERCI98] Multimedia European Research Conferencing Integration, Telematics for Research Project 1007, 1996–1998. http://www-mice.cs.ucl.ac.uk/mice/merci/

[OPGP97] Callas, J., Donnerhacke, L., Finnley, H., "OP Formats – OpenPGP Message Format", Internet Draft, November 1997.

[Oust94] Ousterhout, J. K., "Tcl and Tk Toolkit", Addison–Wesley, 1994.

[RFC2144] Adams, C., "The CAST–128 Encryption Algorithm", May 1997.

[RiSh96] Rivest, R., Shamir, A., "Payword and Micromint", to appear, http://theory.lcs.mit.edu/ rivest/RivestShamir-mpay.ps

[Schn94] Schneier, B., "Description of a New Variable–Length Key, 64–Bit Block Cipher", Proc. Cambridge Security Workshop on Fast Software Encryption, LNCS 809, Springer, 1994, pp. 191–204.

[Schea96] Schulzrinne, H., Casner, S., Frederick, R., Jacobsen, V. , "RTP: A Transport Protocol for Real–Time Applications", Internet RfC 1889, IETF, Audio–Video Transport Working Group, 1996.

[TeDr98] Part of the Telematics for Research Project 1007 MERCI, 1996–1998. http://www.uni-stuttgart.de/Rus/Projects/MERCI/MERCI/TeleDraw/Info.html

[Weis98] Weis, R., "Moderne Blockchiffrierer" (in German), in: "Kryptographie", Weka–Fachzeitschriften–Verlag, Poing, 1998.

[WeLu98] Weis, R., Lucks,S., "Faster Software Encryption",Technical Report, Universtität Mannheim, Fakultät Mathematik und Informatik, 1998.