On the Security of Multi-Party Ping-Pong Protocols *

Shimon Even
Department of Computer Science
Technion - Israel Institute of Technology
Haifa, ISRAEL.
E-mail: even@cs.technion.ac.il

Oded Goldreich
Department of Computer Science
and Applied Mathematics
Weizmann Institute of Science
Rehovot, ISRAEL.
E-mail: oded@wisdom.weizmann.ac.il

June 1983, Revised July 1985, Reproduced February 1996

Abstract

This paper is concerned with the model for security of cryptographic protocols suggested by Dolev and Yao. The Dolev and Yao model deals with a restricted class of protocols, known as *Two-Party Ping-Pong Protocols.* In such a protocol, messages are exchanged in a memoryless manner. That is, the message sent by each party results from applying a predetermined operator to the message he has received.

The Dolev and Yao model is presented, generalized in various directions and the affect of these generalizations is extensively studied. First, the model is trivially generalized to deal with multi-party ping-pong protocols. However, the problems which arise from this generalization are very far from being trivial. In particular, it is no longer clear how many saboteurs (adversaries) should be considered when testing the security of p-party ping-pong protocols. We demonstrate an upper bound of $3(p-2)+2$ and a lower bound of $3(p-2)+1$ on this number. Thus, for every fixed p, the security of p-party ping-pong protocols can be tested in polynomial time. In contrast, we show that testing the security of multi-party protocols (i.e. the number of participants is part of the input) is NP-Hard. A different extension of the Dolev and Yao model, obtained by allowing operators to operate on "half words", is shown to have an undecidable security problem.

Keywords: Cryptographic Protocols, Security, Public-Key Cryptosystems, String Replacement Problems, Undecidability, Concrete Complexity, NP-Completeness, Combinatorial Analysis, Routing Problems, Graph Theory.

This version contains only the Abstract and Introduction. The full version (59 pages) can be found in Technical Report No. 285, Computer Science Dept., Technion, Haifa, Israel, June 1983. An extended abstract has appeared in the *24th FOCS*, 1983.

*Part of this research was done while the authors visited the EECS Dept., UC-Berkeley, and were supported by NSF grant No. MCS 82-04506. The first author was partially supported by the Fund for the Promotion of Research at the Technion. The second author was partially supported by a Weizmann Post-Doctoral Fellowship.

1 Introduction

The use of public-key encryption [DH, RSA] for secure network communication has received considerable attention. Such systems are effective against a "passive" eavesdropper, namely one who merely taps the communication line and tries to decipher the intercepted messages. However, as pointed out by Needham and Schroeder [NS], an improperly designed protocol can be vulnerable to "active" sabotage.

The "active" saboteur (adversary) may be a legitimate user in the network. He can intercept and alter messages, impersonate other users, or initiate instances of the protocol between himself and other users in order to use their responses. It is possible that through such complex manipulations he can read messages that are supposed to be protected without cracking the cryptosystem in use.

In view of this danger it is desirable to have a formal model for discussing security issues in a precise manner. The first such model was introduced by Dolev and Yao [DY], and constitutes the subject of this paper. The Dolev and Yao model consists of a restricted class of "memoryless protocols" and a related definition of insecurity. Loosely speaking, a protocol is insecure if there is a way to obtain the initial message (which is transferred by it), even if the public-key encryption in use are "ideal". This insecurity definition captures all possible weaknesses in the "high level structure" of the protocol; that is, weaknesses that are independent of the particular encryption function used to implement the abstract protocol.

Dolev and Yao considered two-party protocols that proceed in phases as follows. In the first phase the "first" party applies a predetermined sequence of encryption and decryption operators to an *initial message* of his choice and transmit the result. In each later phase, a predetermined party applies a predetermined operator sequence to the last message he/she received and transmits the result. The set of operators was later extended to contain name appending/deletion operators, and the resulting protocols were called *ping-pong* protocols. The related insecurity definition captures all possible "generic" manipulations that the saboteurs can apply to messages they intercept, by possibly using "replays" of the very protocol. In "generic manipulations" we mean actions which do not depend on the specific cryptosystem in use, but rather relate only to the "high level structure" of the protocol. (More details are given in section 2.1.)

Dolev and Yao have demonstrated that testing the security of a two-party ping-pong protocol can be done in polynomial time. A much more efficient algorithm was presented by Dolev, Even and Karp [DEK]. Its running time is $O(n^3)$, where n is the length of the input.
The purpose of this paper is to further investigate the Dolev and Yao model by considering two natural extensions of it.

1. First we consider *multi*-party ping-pong protocols. This naive-looking extension causes a lot of trouble. In contrast to the case of two-party ping-pong protocols, where it was sufficient to consider the actions of a single saboteur, the situation in the general case is more involved: At least $3(p-2)+1$ saboteurs should be considered for testing the security of a p-party ping-pong protocols. On the other hand, we show that $3(p-2)+2$ saboteurs suffice for this purpose. A natural extension of [DEK] implies that for every fixed p, there is a polynomial-time algorithm for testing the security of p-party ping-pong protocols. For unfixed p this is not likely to be the case, since we show that testing the security of multi-party ping-pong protocols is NP-Hard (here p the number of participants is part of the input).

2. Next, we slightly relax the "memoryless condition" by introducing operators that operate on "half words". It is shown that testing the security of protocols in this class in non-recursive.

Organization of the Paper

The rest of the paper is partitioned to three parts. The first part (Chapter 2) deals with multi-party ping-pong protocols, the second (Chapter 3) with the “half word” operators, and the third part contains various comments and conclusions.

References

(BGM) Ben-Or, M., Goldreich, O., Micali, S., and Rivest, R.L., "A Fair Protocol for Signing Contracts", to appear in the *proceedings of the 12th ICALP*, 1984.

(CR) Church, A., and Rosser, J.B., "Some Properties of Conversion", *Trans. Amer. Math. Soc. 39*, (1936), pp. 472-482.

(DLM) DeMillo, R., Lynch, N., and Merritt, M., "Cryptographic Protocols", *Proc. of the 14th ACM Symp. on Theory of Computation*, 1982, pp. 383-400.

(DH) Diffie, W., and Hellman, M.E., "New Directions in Cryptography", *IEEE Trans. on Inform. Theory*, Vol. IT-22, No. 6, November 1976, pp. 644-654.

(DEK) Dolev, D., Even, S., and Karp, R.M., "On the Security of Ping-Pong Protocols", *Inform. and Control*, Vol. 55, 1982, pp. 57-68.

(DY) Dolev, D., and Yao, A.C., "On the Security of Public-Key Protocols", *IEEE Trans. on Inform. Theory*, Vol. IT-29, 1983, pp. 198-208.

(EG) Even, S., and Goldreich, O., "On the Security of Multi-Party Ping-Pong Protocols", TR No. 285, Computer Science Dept., Technion, Haifa 32000, Israel, June 1983, (59 pages).

(EGL) Even, S., Goldreich, O., and Lempel, A., "A Randomized Protocol for Signing Contracts", *Advances in Cryptology: Proceedings of Crypto82*, (Chaum D. et. al. eds.), Plenum Press, 1983, pp. 205-210. To appear in the *Comm. of the ACM*.

(FT) Fredman, M.L., and Tarjan, R.E., "Fibonacci Heaps and their uses in Improving Network Optimization Algorithms", *Proc. of the 25th IEEE Symp. on Foundation of Computer Science*, 1984, pp. 338-346.

(GJ) Garey and Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman and Co., 1979.

(GM) Goldwasser, S., and Micali, S., "Probabilistic Encryption", *Jour. Comp. and Sys, Sci.*, Vol. 28, 1984, pp. 270-299.

(GMR) Goldwasser, S., Micali, S., and Rackoff, C., "The Knowledge Complexity of Interactive Proof-Systems", *Proc. of the 17th ACM Symp. on Theory of Computation*, 1985, pp. 291-304.

(I) Itzhaik, Y., "A Protocol-Word Problem which is NP-Complete", private communication, 1983.

(LP) Lewis, and Papadimitriou, C.H., *Elements of the Theory of Computation*, Prentice-Hall, Inc., 1981.

(LMR) Luby, M., Micali, S., and Rackoff, C., "How to Simultaneously Exchange a Secret Bit by Flipping a Symmetrically-Biased Coin", *Proc. of the 24th IEEE Symp. on Foundation of Computer Science*, 1983, pp. 11-21.

(NS) Needham, R.M., and Schroeder, M.D., "Using Encryption for Authentication in Large Networks of Computers", *Comm. of the ACM*, Vol. 21, No. 12, 1978, pp. 993-999.

(PY) Papadimitriou, C.H., and Yannakakis, M., "The Complexity of Restricted Spanning Tree Problems", *Jour. of the ACM*, Vol. 29, April 1982, pp. 285-309.

(P) Post, E.L., "A Variant of a Recursively Unsolvable Problem", *Bull. of the Amer. Math. Soc.*, 52, 1946, pp. 264-268.

(RSA) Rivest, R.L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Comm. of the ACM*, Vol. 21, February 1978, pp. 120-126.

(R) Rosen, B.K., "Tree-Manipulation Systems and Church-Rosser Theorems", *Jour. of the ACM*, Vol. 20, No. 1, January 1973, pp. 160-187.