Doctoral Thesis

Untersuchungen zur Sicherheit und Realisierbarkeit von analogen und digitalen kryptologischen Systemen

Author(s):
Schoebi, Paul

Publication Date:
1983

Permanent Link:

https://doi.org/10.3929/ethz-a-000324599 →

Diss. ETH Nr. 7433

Untersuchungen zur Sicherheit und Realisierbarkeit von analogen und digitalen kryptologischen Systemen

ABHANDLUNG

zur Erlangung des Titels eines
Doktors der technischen Wissenschaften
der
EIDGENÖSSISCHEN TECHNISCHEN HOCHSCHULE
ZÜRICH

vorgelegt von
PAUL SCHOEBI
dipl. El.-Ing. ETH
geboren am 5. Juni 1953
von Berneck (SG)

Angenommen auf Antrag von
Prof. Dr. P. Leuthold, Referent
Prof. Dr. J.L. Massey, Korreferent

Zürich 1983

UEBERSICHT

Hauptsächlich zwei Elemente haben in den letzten Jahren zu grossen Umwälzungen im Gebiet der Kryptologie geführt, nämlich die rasante Entwicklung von Halbleitertechnologie und Computertechnik sowie die Einführung der Public Key-Systeme. Auf diesem Hintergrund stellt die vorliegende Arbeit eine Beschreibung des aktuellen Standes dar. Ferner werden Vorschläge zur Beurteilung und Verbesserung einiger Systeme gemacht.

Kapitel 1 definiert das Sicherheitsproblem, wie es sich in elektronischen Datenverarbeitungssystemen stellt. Dazu werden zuerst die Schwachpunkte in Netzwerken und Rechnern diskutiert. Mit Hilfe einiger weniger kryptologischer Grundeinheiten lassen sich mögliche Protokolle entwickeln.

Kapitel 2 behandelt die mathematischen und informationstheoretischen Beziehungen, welche den meisten kryptologischen Systemen zugrundeliegen. Elemente der Gruppentheorie, der Theorie der Schieberegistersequenzen, der Informationstheorie von Shannon und der "Many User Communications"- Theorie werden dargestellt.

In Kapitel 3 wird das Konzept der kryptologischen Sicherheit definiert. Dies geschieht einerseits aufgrund der Informationstheorie bzw. der "Many User Communications"-Theorie, anderseits aufgrund der Komplexität der entsprechenden Attacken. Das Kapitel schliesst mit einem Abschnitt über Möglichkeiten und Grenzen erhältlicher elektronischer Rechner sowie über die Verwendbarkeit von mehrfach parallel arbeitenden Maschinen zur Lösung bestimmter Probleme.

Kapitel 4 beschreibt die wichtigsten der bekannten

konventionellen Systeme, beginnend mit den analogen Sprachverschlüsselungsverfahren. Das auf der Verwendung von orthogonalen Transformationen beruhende Verfahren von Wyner wird dargestellt und bezüglich Realisierbarkeit untersucht. Nach einem Abschnitt über die hauptsächlichen digitalen Methoden (inklusive DES) erfolgt eine eingehende Behandlung der Pseudozufallssequenzen. Verschiedene der bekannten Generatoren werden dargestellt, und eine neue, recht effektive Attacke, die sog. Korrelationsattacke, wird vorgeschlagen. Ein spezieller Abschnitt behandelt die Synchronisation von binären Schieberegistersequenzen mit langer Periode, und den Abschluss des Kapitels bildet die Beschreibung neuer Verfahren zur Erzeugung solcher Sequenzen in Hardware und Software.

Kapitel 5 enthält einen Ueberblick über die wichtigsten Public Key-Systeme und -Algorithmen. Im Zusammenhang mit der kryptologischen Verwendbarkeit der Potenzierung in einem $GF(2^n)$ werden Logarithmieralgorithmen untersucht. In diesem Zusammenhang lassen sich einige neue zahlentheoretische Funktionen herleiten und tabellieren. Eine Zusammenstellung der wichtigsten Attacken-Verfahren auf die behandelten Systeme führt zu Regeln für die Wahl der Parameter in einem sicheren Algorithmus.

Die unvermeidliche Datenexpansion bei Verschlüsselungen mit Knapsack-basierten Public Key-Systemen erschwert die Realisierung von Public Key-Authentikation. Kapitel 6 zeigt Lösungsmöglichkeiten für diesen Problemkreis. Eine neue Methode wird beschrieben, welche ein Merkle/Hellman-System so modifiziert, dass Authentikation effizient durchgeführt werden kann, ohne die Verwendbarkeit des Systems zur Datenverschlüsselung einzubüssen. Einige der in diesem Zusammenhang erhaltenen Resultate führen ausserdem zu einer Verbesserung der von Merkle und Hellman vorgeschlagenen Authentifikations-Methode.

Kapitel 7 behandelt Probleme im Zusammenhang mit der praktischen Realisierung von Public Key-Systemen in Hardware und Software. Eine Methode zur Potenzierung in einem $GF(p)$ unter Verwendung von Schieberegistern und kombinatorischer

Logik wird vorgestellt. Die Beschreibung erlaubt unmittelbar den Aufbau einer Schaltung mit diskreten Elementen oder die Konzeption eines LSI-Bausteins.

Die in Kapitel 8 zusammengefassten Schlussbemerkungen beginnen mit einem ausführlichen Vergleich von Public Key-Systemen und konventionellen Algorithmen. Es wird gezeigt wie - unter speziellen Voraussetzungen - Public Key-Eigenschaften mit konventionellen Systemen erreicht werden können. Ein Abschnitt beschreibt den aktuellen Stand der wichtigsten Systeme und die Entwicklungstendenzen. Das Kapitel schliesst mit einer Zusammenstellung der in dieser Arbeit enthaltenen neuen Ideen und Resultate.

ABSTRACT

In the last years, two main factors completely changed the conceptual character of cryptology. The first of them is the rapid development of semiconductor technology and computer techniques, the other is the invention of Public Key systems. With those changes in mind the present work reviews the current state of the art and introduces some new methods which permit to improve existing systems and to develop objective criteria for judging their performance.

In chapter 1 the security problem inherent in electronic data processing schemes is defined. First some of the weak points of networks and computers are discussed. With the help of a few simple cryptographic building blocks a number of possible protocols can be developed.

Chapter 2 is devoted to the mathematical and information-theoretical relations which form the basis of most cryptologic systems. Elements of group theory, shift register theory, information theory and many user communications theory are exposed.

In chapter 3 the concept of cryptologic security is defined both on the basis of information theory and many user communications theory, as well as with regard to the complexity of the corresponding attack. A section on the possibilities of modern computers and the advantages of parallel computing concludes this chapter.

In chapter 4 the most important conventional cryptographic schemes are described beginning with analog speech scrambling systems. The practical realizability of Wyner's method basing on orthogonal transformations is investigated. A special section treats the most important digital methods (including

DES) and pseudo noise (PN) sequences. Several examples of PN generators are shown and a new and quite effective attack (the correlation attack) is proposed. The last two sections treat synchronization of PN-sequences with long periods and the ways to produce them in hardware and software.

Chapter 5 reviews the most important public key systems and algorithms. In connection with the security of systems basing on exponentiation in a $GF(2^n)$, algorithms for computing logarithms are investigated. This makes it possible to develop an algorithm for calculation of some new number theoretic functions. An overview of the most important attacks and their efficacy serves as a basis for determining parameters of secure systems.

The considerable data expansion connected with enciphering in a knapsack-based public key system prevents fast authentication. Chapter 6 shows several solutions of this problem. A new method is introduced which modifies the Merkle/Hellman scheme so that efficient authentication is possible without losing the possibility to encipher data in the same system. Some of the results obtained further lead to an improvement of the authentication method proposed by Merkle and Hellman.

In chapter 7 problems with practical realizations of public key systems in hardware and software are treated. A circuit for exponentiation in a GF(p) containing shift registers and combinatoric logic is described. The description allows immediate implementation in discrete logic or LSI.

The final remarks in chapter 8 begin with a comparison of conventional systems and public key systems. It is shown that - under certain assumptions - public key properties can be obtained using conventional building blocks. A special section describes the current state of the art for the most important schemes and prospective future developments. In conclusion the new ideas and investigation results contained in this work are listed.