Diss. ETH No. 9752

On the Design and Security of Block Ciphers

A dissertation submitted to the

SWISS FEDERAL INSTITUTE OF TECHNOLOGY

ZÜRICH

for the degree of

Doctor of Technical Sciences

presented by

XUEJIA LAI

B.Sc. El.Eng., M.Sc. Math. Xidian University, Xian, China

born June 4, 1954

citizen of China

accepted on the recommendation of

Prof. Dr. J. L. Massey, referee

Prof. Dr. H. Bühlmann, co-referee

Zürich, 1992

Hartung-Gorre Verlag Konstanz

Abstract

Secret-key block ciphers are the subject of this work. The design and security of block ciphers, together with their application in hashing techniques, are considered. In particular, iterated block ciphers that are based on iterating a weak round function several times are considered. Four basic constructions for the round function of an iterated cipher are studied.

The iterated block cipher IDEA is proposed. This cipher is based on the new design concept of mixing different group operations on 16-bit subblocks. Using operations on subblocks facilitates the software implementation of the cipher. The regular structure of the cipher facilitates hardware implementation. The interaction of the three chosen "incompatible" group operations provides the necessary "confusion", and the chosen cipher structure causes the required "diffusion".

The security of iterated ciphers against Biham and Shamir's differential cryptanalysis is discussed. Differential cryptanalysis is described in terms of an i-round "differential", which is defined as a couple (α, β) such that a pair of distinct plaintexts with difference α can result in a pair of i-th round outputs having difference β. It is shown that the maximum probability of such a differential can be used to determine a lower bound on the complexity of a differential cryptanalysis attack. The concept of "Markov ciphers" is introduced because of its significance in differential cryptanalysis. It is shown that the security of a Markov cipher against differential cryptanalysis is determined by the transition probability matrix created by the round function. A design principle for Markov ciphers is formulated, viz., that its transition matrix should be non-symmetric. Differential cryptanalysis of the IDEA cipher is performed partly by theoretical analysis of the relationship between the three chosen group operations and the properties of the MA-structure within the cipher, and partly by numerical experiments on "mini versions" of the cipher.

The results suggest that the IDEA cipher is secure against differential cryptanalysis attack after only four of its eight rounds.

The application of block ciphers in constructing hash functions is also considered. Five different attacks on hash functions obtained by iterating a hash round function are formulated and examined. Relations between the security of such an iterated hash function and the strength of its round function are derived. Schemes for constructing hash round functions by using block ciphers are discussed and new hashing schemes using the IDEA cipher are proposed. In particular, the problem of constructing $2m$-bit hash round functions from available m-bit block ciphers is considered and two new constructions are proposed. Four attacks on three known hash schemes are presented by applying a new principle for evaluating the security of a hash round function.

Zusammenfassung

Diese Arbeit handelt vom Entwurf und der Sicherheit von Blockchiffrierern, sowie von desen Anwendung in Hash-Verfahren. Insbesondere werden die iterative Blockchiffrierer betrachtet, die auf mehrmaliger Wiederholung einer "schwachen" Rundenfunktion basieren. Vier grundlegende Konstruktionen dieser Rundenfunktion werden untersucht.

Das Blockchiffrierverfahren IDEA wird vorgeschlagen, welches mit Hilfe eines neuen Konzepts entworfen wurde. Es handelt sich dabei um eine Vermischung von unterschiedlichen Gruppenoperationen, die auf 16-Bit Teilblöcken operieren. Die Verwendung von Operationen auf Teilblöcken erleichtert die Software-Implementation dieses Chiffrierers, und die regelmässige Struktur des Chiffrierers ermöglicht eine effiziente Hardware-Implementation. Die Wechselwirkung der drei gewählten "inkompatiblen" Gruppenoperationen liefert die notwendige "Confusion", und die gewählte Struktur des Chiffrierers erzeugt die notwendige "Diffusion".

Die Sicherheit von iterativen Blockchiffrierern gegenüber der Differential-Kryptanalyse, welche von Biham und Shamir stammt, wird untersucht. Dabei wird die Differential-Kryptanalyse mit Hilfe eines i-Runden-Differentials (α, β) beschrieben, welches so definiert ist, dass ein Paar von verschiedenen Klartexten mit Differenz α nach i Runden ein Paar von Chiffriertexten mit Differenz β erzeugen kann. Es wird gezeigt, dass die maximale Wahrscheinlichkeit eines solchen Differentials benutzt werden kann, um eine untere Schranke der Komplexität einer Differential-Kryptanalyse-Attacke zu bestimmen. Der Begriff "Markov-Chiffrierer" wird wegen seiner Bedeutung für die Differential-Kryptanalyse eingeführt. Es wird gezeigt, dass die Sicherheit eines Markov-Chiffrierers durch die von der Rundenfunktion erzeugte Matrix der Übergangswahrscheinlichkeiten bestimmt werden kann. Ein Entwurfsprinzip für Markov-Chiffrierer wird formuliert, nämlich, dass die Matrix der Über-

gangswahrscheinlichkeiten asymmetrisch sein soll. Die Differential-Kryptanalyse des IDEA-Chiffrierers wird einerseits theoretisch durchgeführt, indem die Beziehungen zwischen den drei Gruppenoperationen und die Eigenschaften der verwendeten MA-Struktur analysiert werden. Andererseits liegen auch numerische Untersuchungen mit "Mini-Versionen" des IDEA-Chiffrierers vor. Die Ergebnisse dieser Untersuchungen legen den Schluss nahe, dass der IDEA-Chiffrierer nach nur vier von seinen acht Runden gegenüber der Differential-Kryptanalyse sicher ist.

Weiter wird die Anwendung von Blockchiffrierer zur Konstruktion von Hash-Funktionen besprochen. Fünf verschiedene Attacken auf Hash-Funktionen, die auf Wiederholungen einer Hash-Rundenfunktion beruhen, werden formuliert und untersucht. Zusammenhänge zwischen der Sicherheit einer solchen iterativen Hash-Funktion und der Stärke ihrer Rundenfunktion werden hergeleitet. Konstruktionsmethoden für Hash-Rundenfunktionen, welche auf einem Blockchiffrierer basieren, werden betrachtet. Neue Hash-Verfahren, welche auf dem IDEA-Chiffrierer beruhen, werden ebenfalls vorgeschlagen. Insbesondere wird das Problem der Konstruktion von $2m$-Bit Hash-Rundenfunktionen aus verfügbaren m-Bit Blockchiffrierern behandelt, und es werden zwei neue Konstruktionen vorgeschlagen. Vier Attacken auf drei bekannte Hash-Funktionen werden vorgestellt, die auf einem neuen Prinzip der Sicherheitsevaluierung von Hash-Rundenfunktionen beruhen.