Diss. ETH No. 11625

Cryptanalysis of iterated block ciphers

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
Doctor of Technical Sciences

presented by
CARLO HARPES
dipl. El. Ing. ETH
born December 6, 1968
citizen of Rippweiler(Luxemburg)

accepted on the recommendation of
Prof. Dr. J.L. Massey, referee
Prof. Dr. U. Maurer, co-referee

1996

Abstract

Matsui's linear cryptanalysis for iterated block ciphers is first generalized by replacing his linear expressions with I/O sums. For a single round, an I/O sum is the XOR of a balanced binary-valued function of the round input and a balanced binary-valued function of the round output. A last-round attack is described and conditions for it to be successful are given. A procedure for finding effective "homomorphic" I/O sums to be used in an attack is given. A cipher contrived to be secure against linear cryptanalysis but vulnerable to this generalization of linear cryptanalysis is given. It is argued that the ciphers IDEA and SAFER are secure against this generalization of linear cryptanalysis. Statistical evidence is provided for the hypotheses of fixed-key equivalence and of fixed-key randomization, on which the success of the attack relies.

A second generalization of linear cryptanalysis is obtained by replacing an I/O sum with the m-ary group difference of a function of the round input and a function of the round output. A corresponding attack on an iterative cipher is developed. Several different measures for the effectiveness of m-ary group differences are defined and analyzed.

The previous attacks are generalized to an attack called partitioning cryptanalysis. This attack exploits a weakness that can be described by an effective partition-pair, i.e., a partition of the plaintext set and a partition of the next-to-last-round output set such that, for every key, the next-to-last-round outputs are non-uniformly distributed over the blocks of the second partition when the plaintexts are chosen uniformly from a particular block of the first partition. The last-round attack by partitioning cryptanalysis is formalized and requirements for

it to be successful are stated. The success probability is approximated and a procedure for finding effective partition-pairs is formulated. The usefulness of partitioning cryptanalysis is demonstrated by applying it successfully to 6-rounds of the Data Encryption Standard (DES).

The possibility to insert into a cipher a backdoor, i.e., a hidden weakness, for partitioning cryptanalysis is considered. Substitution boxes that act as linear-block transducers are defined and used to build ciphers that are easily breakable by partitioning cryptanalysis but are secure against both linear and differential cryptanalysis. A general construction of such S-boxes is given and their properties are discussed. Some techniques for finding the backdoor in an S-box are presented, and they suggest that it is impossible to hide the existence of an effective partition-pair in an invertible S-box with only a small number of inputs and outputs.

Keywords. Block cipher, cryptanalysis, linear cryptanalysis, partitioning cryptanalysis, differential cryptanalysis, piling-up lemma, backdoor, trapdoor, IDEA, SAFER, DES.

Zusammenfassung

Matsui's lineare Kryptoanalye von gestuften Blockverschlüsselungsverfahren wird zuerst dadurch verallgemeinert, daß linearen Ausdrücke durch Eingangs/Ausgangs-Summen ersetzt werden. Für eine einzelne Stufe ist eine Eingangs/Ausgangs-Summe eine exklusiv-oder Verknüpfung einer ausgeglichenen Boole'schen Funktion des Eingangs und einer ausgeglichenen Boole'schen Funktion des Ausgangs. Der Angriff mit verallgemeinerter linearer Kryptoanalyse auf die letzte Stufe wird beschrieben und Bedingungen für dessen Erfolg werden angegeben. Es wird ferner eine Vorgehensweise erläutert, um wirksame "homomorphe" Eingangs/Ausgangs-Summen für eine Angriff zu finden. Ein Verschlüsselungssystem, welches zwar sicher gegen lineare Kryptoanalyse, aber mit der besprochenen Verallgemeinerung angreifbar ist, wird gebaut. Die Verschlüsselungssysteme IDEA und SAFER sind hingegen sicher gegen diese Verallgemeinerung. Der Erfolg der betrachteten Angriffe beruht auf der Hypothese, daß sich alle Schlüssel fast gleich verhalten, und auf der Hypothese, dass falsches Schlüsselraten die geschätzen Eingangs/Ausgangs-Summen ausgleicht. Diese Hypothesen werden statistisch untermauert.

Als nächstes wird eine zweite Verallgemeinerung der linearen Kryptoanalyse beschrieben. Sie entsteht durch Ersetzen der Eingangs/Ausgangs-Summen durch m-wertige Gruppendifferenzen einer Funktion des Eingangs und einer Funktion des Ausgangs. Mehrere Maße für die Wirksamkeit solcher m-wertigen Eingang/Ausgang-Differenzen werden definiert und untersucht.

Die vorherigen Angriffe werden anschließend zur partitionierenden Kryptoanalyse weiterentwickelt. Dieser Angriff nutzt Schwächen aus,

welche mit einem "wirksamen Partitionspaar" beschrieben werden. Dieses besteht aus zwei Partitionen der Menge der Eingänge und der Ausgänge und wird so gewählt, daß der zweitletzte Stufenausgang für jeden Schlüssel nicht gleichförmig über die Blöcke der zweiten Partition verteilt ist, wenn der Eingang gleichförmig aus einem bestimmten Block der ersten Partition gewählt wurde. Der Angriff mit partitionierender Kryptoanalyse wird beschrieben und Bedingungen für dessen Erfolg werden angegeben. Die Erfolgswahrscheinlichkeit wird angenähert und eine Vorgehensweise, um wirksame Partitionspaare zu finden, wird entwickelt. Der Nutzen der partitionierenden Kryptoanalyse wird dadurch untermauert, dass sie erfolgreich gegen sechs Stufen des "Data Encryption Standard (DES)" angewendet werden kann.

Am Ende wird die Möglichkeit betrachtet, Hintertüren, das heißt versteckte Schwachstellen, für partitionierende Kryptoanalyse in ein Verschlüsselungssystem einzubauen. Substitutionsboxen, auch S-Boxen genannt, welche lineare Blöcke in lineare Blöcke verwandeln, werden definiert und können zur Herstellung von Verschlüsselungssystemen dienen. Solche Systeme sind zwar einfach mit partitionierender Kryptoanalyse zu brechen, können aber sicher gegen lineare und differentielle Kryptoanalyse sein. Eine allgemeine Konstruktion solcher S-Boxen wird angeben und es werden Eigenschaften dieser S-Boxen erläutert. Einige Methoden, um Hintertüren in S-Boxen aufzuspühren, werden vorgestellt. Sie deuten an, dass es unmöglich ist, die Existenz von wirksamen Partitionspaaren in S-Boxen mit nur einer kleiner Anzahl Eingängen gut zu verstecken.

Schüsselwörter. Blockverschlüsselungssysteme, Kryptoanalyse, lineare Kryptoanalyse, partitionierende Kryptoanalyse, differentielle Kryptoanalyse, "Piling-up Lemma", Hintertüren, IDEA, SAFER, DES.

Résumé

La cryptanalyse linéaire de Matsui des fonctions de chiffrement par blocs est généralisée par le remplacement des expressions linéaires par des sommes d'entrée/sortie. Pour un simple tour d'une fonction de chiffrement, une somme d'entrée/sortie est le résultat d'une opération ou-exclusif d'une fonction binaire balancée de l'entrée et d'une fonction binaire balancée de la sortie. L'attaque sur le dernier tour est décrite et des conditions de réussite sont données. Ensuite, une procédure pour trouver des sommes d'entrée/sortie "homomorphes" qui sont effectives dans une attaque est développée. Un chiffrement sécurisée contre la cryptanalyse linéaire mais vulnérable par la généralisation de celle-ci est construite. Les fonctions de chiffrement IDEA et SAFER sont argumentées être sécurisées contre cette généralisation de la cryptanalyse linéaire. Finalement, des méthodes statistiques servent à valider les hypothèses sur lesquelles sont basées les attaques décrites, c'est-à-dire l'hypothèse d'équivalence des clés et l'hypothèse de balancement par mauvaise estimation de la clé.

Une deuxième généralisation de la cryptanalyse linéaire est obtenue par le remplacement des sommes d'entrée/sortie par des différences de groupes à m éléments d'une fonction de l'entrée et d'une fonction de la sortie d'un tour. Une telle attaque est développée, et plusieurs mesures de l'efficacité d'une telle différence de groupe sont définies et analysées.

Les attaques précédentes sont ensuite généralisées dans une attaque appelé cryptanalyse partitionnante. Celle-ci exploite une faiblesse qui se traduit par l'existence d'une "paire efficace de partitions", c'est-à-dire d'une partition de l'ensemble des entrées et d'une partition de l'ensemble des sorties de l'avant-dernier tour telles que, pour chaque clé, la sortie

de cet avant-dernier tour ne soit pas uniformément distribuée entre les classes de la deuxième partition lorsque l'entrée a été choisie uniformément au hasard dans une classe particulière de la première partition. Cette attaque est formalisée et des exigences à son bon fonctionnement sont précisées. La probabilité de réussite est approchée et une procédure pour trouver des paires efficaces de partitions est développée. L'utilité de la cryptanalyse partitionnante est démontrée par l'application réussie contre six tours du "Data Encryption Algorithm (DES)".

Finalement, les possibilités d'insérer une "trappe" dans une fonction cryptographique sont considérées. Une telle trappe est une faiblesse cachée pour la cryptanalyse partitionnante. Des boîtes de substitution, agissant comme des transformateurs de classes linéaires, sont définies et utilisées dans la construction de fonctions cryptographiques faibles contre la cryptanalyse partitionnante mais résistantes contre la cryptanalyse différentielle et la cryptanalyse linéaire. Une construction générale de telles boîtes de substitution est donnée et leurs propriétés sont discutées. Quelques techniques pour retrouver des trappes dans ces boîtes sont présentées et elles suggèrent qu'il est impossible de cacher convenablement l'existence de paires efficaces de partitions dans de petites boîtes.

Mots clés. Chiffrement par blocs, cryptanalyse, cryptanalyse linéaire, cryptanalyse différentielle, cryptanalyse partitionnante, lemme du "piling-up", trappe, IDEA, SAFER, DES.