Lecture Notes in
Computer Science 537

A. J. Menezes S. A. Vanstone (Eds.)

Advances in Cryptology – CRYPTO '90

Proceedings

Springer-Verlag

A. J. Menezes S. A. Vanstone (Eds.)

Advances in Cryptology – CRYPTO '90

Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Department of Computer Science
Cornell University
Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Alfred J. Menezes
Scott A. Vanstone
Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

CR Subject Classification (1991): E.3

ISBN 3-540-54508-5 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-54508-5 Springer-Verlag New York Berlin Heidelberg

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

CRYPTO '90

A Conference on the Theory and Application of Cryptography

held at the University of California, Santa Barbara,
August 11-15, 1990
through the cooperation of the Computer Science Department

Sponsored by:

International Association for Cryptologic Research

in cooperation with

The IEEE Computer Society Technical Committee
On Security and Privacy

General Chair
Sherry McMahan, Cylink

Program Chair
Scott Vanstone, University of Waterloo

Program Committee

Gordon Agnew	University of Waterloo
Thomas Berson	Anagram Laboratories
Johannes Buchmann	Universität des Saarlandes
Yvo Desmedt	University of Wisconsin
Amos Fiat	Tel-Aviv University
Kenji Koyama	NTT Basic Research Lab
Ronald Rivest	Massachusetts Institute of Technology
Rainer Rueppel	Crypto AG
Marijke De Soete	Philips Research Labs
Doug Stinson	University of Nebraska
Hugh Williams	University of Manitoba

Foreword

Crypto '90 marked the tenth anniversary of the Crypto conferences held at the University of California at Santa Barbara. The conference was held from August 11 to August 15, 1990 and was sponsored by the International Association for Cryptologic Research, in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Department of Computer Science of the University of California at Santa Barbara.

Crypto '90 attracted 227 participants from twenty countries around the world. Roughly 35% of attendees were from academia, 45% from industry and 20% from government. The program was intended to provide a balance between the purely theoretical and the purely practical aspects of cryptography to meet the needs and diversified interests of these various groups.

The overall organization of the conference was superbly handled by the general chairperson Sherry McMahan. All of the outstanding features of Crypto, which we have come to expect over the years, were again present and, in addition to all of this, she did a magnificent job in the preparation of the book of abstracts. This is a crucial part of the program and we owe her a great deal of thanks.

Each year the number and quality of submissions to Crypto has been increasing. This is of course very good for the conference but it does make the task of the program committee more difficult. This year we had 104 papers and abstracts submitted from 18 countries. In anticipation of this larger number, the committee was expanded to twelve members representing seven countries. Having a bigger committee and a wider global representation poses certain problems with communication, but we believe these problems are minute in comparison to the benefits obtained from having each paper scrutinized by more people and by involving a much larger cross-section of the cryptographic community in this process. Each paper was assigned to three committee members who were then responsible for its refereeing. Of the 104 submissions, one was withdrawn, 43 were accepted for presentation and, of these 43, two were merged into one presentation. All papers and abstracts accepted for presentation which contained sufficient detail for the committee to make a reasonably accurate evaluation of the final form of the paper have not been been re-refereed. Rump session contributions and papers accepted for presentation based on abstracts with very little detail have been refereed.

As in other years, Whitfield Diffie kindly agreed to coordinate the Rump Session. We would like to take this opportunity to thank Whit for running this very important aspect of Crypto over the years and for graciously accepting to do it again. In an effort to contain the number of short talks given in this session, a much harder line was adopted this year. Of the 22 abstracts submitted only 12 were accepted for presentation. Of these 12, only 6 were submitted for the proceedings and all of these have gone through a thorough refereeing process.

For this conference there were three invited speakers and each was given fifty minutes to lecture. It was our goal to have topics of current interest, given by noted authorities in the area and presented in a manner which would make the lectures accessible to a large audience of diversified backgrounds. With this in mind we approached Whitfield Diffie (Bell Northern Research), Adi Shamir (Weizmann Institute) and Gus Simmons (Sandia National Laboratories) and all accepted. We thank them for their outstanding presentations and the enthusiasm which they conveyed for the subject.

We would also like to thank Dr. Tatsuaki Okamoto (NTT Tokyo) for the very valuable assistance he provided to us. Dr. Okamoto was on sabbatical leave from NTT and was spending this time (August 1989 – August 1990) at the University of Waterloo. He kindly volunteered his services and made many very important and significant contributions to our efforts with the program.

Finally, we thank the members of the program committee itself for the very fine job they did. Theirs is a task which takes a great deal of time and effort and which receives a disproportionate amount of gratitude. Without a complete commitment by all members, the task would be impossible. We thank each of them for a very thorough and conscientious effort and also for their very deep dedication in making Crypto '90 successful. Many thanks to Gordon Agnew, Thomas Berson, Johannes Buchmann, Yvo Desmedt, Amos Fiat, Kenji Koyama, Ronald Rivest, Rainer Rueppel, Marijke De Soete, Doug Stinson, and Hugh Williams.

Alfred J. Menezes and Scott A. Vanstone
University of Waterloo
December 1990

Table of Contents

Session 1: Cryptanalysis

Chair: S. Vanstone

Session 2: Protocols

Chair: Y. Desmedt

Session 3: Algebra and Number Theory

Chair: H. Williams

Session 4: Signatures and Authentication

Chair: D. Stinson

Session 5: Secret Sharing

Chair: M. De Soete

Session 6: Key Distribution

Chair: T. Berson

Session 7: Hash Functions

Chair: R. Rueppel

Session 8: Zero-Knowledge

Chair: A. Fiat

Session 9: Randomness

Chair: R. Rivest

Session 10: Applications

Chair: G. Agnew

Session 11: Design and Analysis I

Chair: K. Koyama

Session 12: Design and Analysis II

Chair: J. Buchmann

Rump Session: Impromptu Talks

Chair: W. Diffie

Session 1
Cryptanalysis
Chair: S. Vanstone, University of Waterloo

Differential Cryptanalysis of DES-like Cryptosystems

(Extended Abstract)

Eli Biham *Adi Shamir*

The Weizmann Institute of Science
Department of Applied Mathematics

Abstract

The Data Encryption Standard (DES) is the best known and most widely used cryptosystem for civilian applications. It was developed at IBM and adopted by the National Buraeu of Standards in the mid 70's, and has successfully withstood all the attacks published so far in the open literature. In this paper we develop a new type of cryptanalytic attack which can break DES with up to eight rounds in a few minutes on a PC and can break DES with up to 15 rounds faster than an exhaustive search. The new attack can be applied to a variety of DES-like substitution/permutation cryptosystems, and demonstrates the crucial role of the (unpublished) design rules.

1 Introduction

Iterated cryptosystems are a family of cryptographically strong functions based on iterating a weaker function n times. Each iteration is called a *round* and the cryptosystem is called an *n round cryptosystem.* The *round function* is a function of the output of the previous round and of a *subkey* which is a key dependent value calculated via a *key scheduling* algorithm. The round function is usually based on S boxes, bit permutations, arithmetic operations and the exclusive-or (denoted by $\oplus$ and XOR) operations. The *S boxes* are nonlinear translation tables mapping a small number of input bits to a small number of output bits. They are usually the only part of the cryptosystem that is not linear and thus the security of the cryptosystem crucially depends on their choice. The bit permutation is used to rearrange the output bits of the S boxes in order to make the input bits of each S box in the following round depend on the output of as many S boxes as possible. The XOR operation is often used to mix the subkey with the data. In most applications the encryption algorithm is assumed to be known and the secrecy of the data depends only on the secrecy of the randomly chosen key.

An early proposal for an iterated cryptosystems was Lucifer[7], which was designed at IBM to resolve the growing need for data security in its products. The round function of Lucifer has a combination of non linear S boxes and a bit permutation. The input bits are divided into groups of four consecutive bits. Each group is translated by a reversible S box giving a four bit result. The output bits of all the S boxes are permuted in order to mix them when they become the input to the following round. In Lucifer only two fixed S boxes (S_0 and S_1) were chosen. Each S box can be used at any S box location and the choice is key dependent. Decryption is accomplished by running the data backwards using the inverse of each S box.

The Data Encryption Standard (DES) [14] is an improved version of Lucifer. It was developed at IBM and adopted by the U.S. National Bureau of Standards (NBS) as the standard cryptosystem for sensitive but unclassified data (such as financial transactions and email messages). DES has become a well known and widely used cryptosystem. The key size of DES is 56 bits and the block size is 64 bits. This block is divided into two halves of 32 bits each. The main part of the round function is the *F function*, which works on the right half of the data using a subkey of 48 bits and eight (six bit to four bit) S boxes. The 32 output bits of the F function are XORed with the left half of the data and the two halves are exchanged. The complete specification of the DES algorithm appears in [14]. In this paper the existence of the initial permutation and its inverse are ignored, since they have no cryptanalytic significance.

An extensive cryptanalytic literature on DES was published since its adoption in 1977. Yet, no short-cuts which can reduce the complexity of cryptanalysis to less than half of exhaustive search were ever reported in the open literature.

The 50% reduction[9] (under a chosen plaintext attack) is based on a symmetry under complementation. Cryptanalysis can exploit this symmetry if two plaintext/ciphertext pairs (P_1, T_1) and (P_2, T_2) are available with $P_1 = \bar{P}_2$.

Diffie and Hellman[6] suggested an exhaustive search of the entire key space in one day on a parallel machine. They estimate the cost of this machine to be $20-million and the cost per solution to be $5000.

Hellman[8] presented a time memory tradeoff method for a chosen plaintext attack. A special case of this method takes about 2^{38} time and 2^{38} memory, with a 2^{56} preprocessing time. Hellman suggests a special purpose machine which produces 100 solutions per day with an average wait of one day. He estimates that the machine costs about $4-million and the cost per solution is about $1–100. The preprocessing is estimated to take 2.3 years on the same machine.

The *Method of Formal Coding* in which the formal expression of each bit in the ciphertext is found as a XOR sum of products of the bits of the plaintext and the key was suggested in [9]. Schaumuller-Bichl[15,16] studied this method and concluded that it requires an enormous amount of computer memory which makes the whole approach impractical.

In 1987 Chaum and Evertse[2] showed that a meet in the middle attack can reduce the key search for DES with a small number of rounds by the following factors:

Number of Rounds	Reduction Factor
4	2^{19}
5	2^{9}
6	2^{2}
7	–

They also showed that a slightly modified version of DES with seven rounds can be solved with a reduction factor of 2. However, they proved that a meet in the middle attack of this kind is not applicable to DES with eight or more rounds.

In the same year, Donald W. Davies[3] described a known plaintext cryptanalytic attack on DES. Given sufficient data, it could yield 16 linear relationships among key bits, thus reducing the size of a subsequent key search to 2^{40}. It exploited the correlation between the outputs of adjacent S boxes, due to their inputs being derived from, among other things, a pair of identical bits produced by the bit expansion operation. This correlation could reveal a linear relationship among the four bits of key used to modify these S box input bits. The two 32-bit halves of the DES result (ignoring IP) receive these outputs independently, so each pair of adjacent S boxes could be exploited twice, yielding 16 bits of key information.

The analysis does not require the plaintext P or ciphertext T but uses the quantity $P \oplus T$ and requires a huge number of random inputs. The S box pairs vary in the extent of correlation they produce so that, for example, the pair S7/S8 needs about 10^{17} samples but pair S2/S3 needs about 10^{21}. With about 10^{23} samples, all but the pair S3/S4 should give results (i.e., a total of 14 bits of key information). To exploit all pairs the cryptanalyst needs about 10^{26} samples. The S boxes do not appear to have been designed to minimize the correlation but they are somewhat better than a random choice in this respect. The large number of samples required makes this analysis much harder than exhaustive search for the full DES, but for an eight round version of DES the sample size of 10^{12} or 10^{13} (about 2^{40}) is on the verge of practicality. Therefore, Davies' analysis had penetrated more rounds than previously reported attacks.

During the last decade several cryptosystems which are variants of DES were suggested. Schaumuller-Bichl suggested three such cryptosystems [15, 17]. Two of them (called C80 and C82) are based on the DES structure with the replacement of the F function by nonreversible functions. The third one, called The Generalized DES Scheme (GDES), is an attempt to speed up DES. GDES has 16 rounds with the original DES F function but with a larger block size which is divided into more than two parts. She claims that GDES increases the encryption speed of DES without decreasing its security.

Another variant is the Fast Data Encryption Algorithm (Feal). Feal was designed to be efficiently implementable on an eight bit microprocessor. Feal has two versions. The first[19], called Feal-4, has four rounds. Feal-4 was broken by Den-Boer[4] using a chosen plaintext attack with 100–10000 encryptions. The creators of Feal reacted by creating a new version, called Feal-8, with eight rounds and additional XORs of the plaintext and the ciphertext with subkeys[18,13]. Both versions were described as cryptographically better than DES in several aspects.

In this paper we describe a new kind of attack that can be applied to many DES-like iterated cryptosystems. This is a chosen plaintext attack which uses only the resultant ciphertexts. The basic tool of the attack is the *ciphertext pair* which is a pair of ciphertexts whose plaintexts have particular differences. The two plaintexts can be chosen at random, as long as they satisfy the difference condition, and the cryptanalyst does not have to know their values. The attack is statistical in nature and can fail in rare instances.

2 Introduction to differential cryptanalysis

Differential cryptanalysis is a method which analyses the effect of particular differences in plaintext pairs on the differences of the resultant ciphertext pairs. These differences can be used to assign probabilities to the possible