P. Leuthold
5.7.90

Diss. ETH No. 9137

Problems and methods related to cryptographic applications of Smart Cards

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH
for the degree of
Doctor of Technical Sciences

presented by
RÉJANE FORRÉ
dipl. El.-Ing. ETH
born July 25, 1963
citizen of Saxon (VS)

accepted on the recommendation of
Prof. Dr. P. Leuthold, referee
Prof. Dr. J.L. Massey, co-referee

ADAG Administration & Druck AG
Zurich, 1990

Abstract

The portability of Smart Cards, their storage capacity, their computing capabilities and their relatively modest price makes of them very promising elements for future access control and information systems. In the present work, attention is paid to the problems connected with the implementation of cryptographic algorithms in Smart Cards, as well as to security aspects of some of these cryptographic schemes.

After a brief introduction, the various kinds of Smart Cards and their possible applications are reviewed in chapter 2. The advantages of Smart Cards over magnetic stripe cards or other passive tools are shown to lie principally in the higher security they are able to guarantee. However, there are still many unsolved or only partially-solved problems in the implementation of stream ciphers, block ciphers and public-key ciphers in Smart Cards, most of them due to the limited storage capacity and computing power of the embedded microprocessors. After a sketch of these problems in chapter 3, a concrete running-key generator is investigated with regard to the specific questions raised by its realization in a Smart Card.

In chapter 4, a cryptanalytic attack against a class of running-key generators is presented. The original version of this attack works for running-key generators composed of several distinct linear feedback shift registers whose outputs are combined by some function. Modifications of this basic scheme allow one to cryptanalyze another type of running-key generator, namely those containing only one linear feedback shift register and a state filter function. The fact that these generators contain only one shift register makes them attractive for Smart Card applications. It is shown that careful design can prevent the described attacks from succeeding.

Chapter 5 deals with the design of S-boxes for product ciphers. The Strict Avalanche Criterion was defined to characterize input/output dependencies of boolean functions. The original definition is extended and its implications for the Walsh-transform of a function are derived. In order to quantify these input/output dependencies, the definition of the entropy profile of a boolean function is introduced. An algorithm to determine functions with good entropy profiles is proposed. Since the statistical independence among the outputs of an S-box seems to be cryptographically desirable, the conditions for statistical independence of boolean functions are derived. S-boxes composed of independent functions with good entropy profiles are then investigated, as well as S-boxes defined by simple algebraic expressions.

The results of the dissertation are summarized in chapter 6.

Zusammenfassung

Die Tragbarkeit, die Speicherkapazität, die rechnerischen Leistungen und die verhältnismässig bescheidenen Kosten machen die Chipkarte zu einem vielversprechenden Element von Zutrittskontroll- und Informationssystemen der nahen Zukunft. In der vorliegenden Arbeit werden Probleme betrachtet, die sowohl mit der Implementierung von kryptographischen Algorithmen in Chipkarten als auch der Sicherheit von gewissen kryptographischen Methoden verbunden sind.

Nach einer kurzen Einleitung wird ein Überblick über die verschiedenen Typen von Chipkarten und ihre möglichen Anwendungen im Kapitel 2 gegeben. Es wird gezeigt, dass die Vorteile der Chipkarte gegenüber der Magnetstreifenkarte oder anderen passiven Instrumenten hauptsächlich in der höheren Sicherheit bestehen. Jedoch sind viele Probleme bei der Implementierung von "stream cipher", "block cipher" und "public-key"-Systemen nur teilweise oder gar nicht gelöst. Die meisten Probleme resultieren aus der Begrenzung der Speicherkapazität und der Rechenleistung der eingebauten Mikroprozessoren. Nach einer Schilderung dieser Probleme im Kapitel 3 wird ein konkreter Schlüsselstromgenerator in Bezug auf die implementierungsspezifischen Aspekte untersucht.

Kapitel 4 enthält die Beschreibung einer kryptoanalytischen Attacke gegen eine Klasse von Schlüsselstromgeneratoren. Die Originalversion dieser Attacke ist wirksam gegen Generatoren, die aus verschiedenen linear rückgekoppelten Schieberegistern und einer Kombinierfunktion bestehen. Durch Modifikationen der Attacke kann eine andere Art von Generatoren geknackt werden, nämlich solche, die aus einem einzigen linear rückgekoppelten Schieberegister und einem nichtlinearen Zustandsfilter bestehen. Die Tatsache, dass diese Generatoren nur ein Schieberegister beinhalten, macht sie für Chipkartenapplikationen besonders interessant. Es wird gezeigt, dass die vorgeschlagenen Attacken durch entsprechende vorbeugende Massnahmen verhindert werden können.

Im Kapitel 5 wird der Entwurf von "S-boxes" für die Produkt-Chiffrierung behandelt. Das strikte Lawinenkriterium (strict avalanche criterion, SAC) wurde zwecks qualitativer Beurteilung der Abhängigkeit zwischen den Ein- und Ausgangsgrössen bei booleschen Funktionen definiert. Die ursprüngliche Definition erfuhr eine Erweiterung und die Konsequenzen für das Walsh-Spektrum einer SAC-erfüllenden Funktion werden hergeleitet. Um die Abhängigkeit zwischen Ein- und Ausgangsgrösse quantitativ zu beurteilen, wird das Entropieprofil einer booleschen Funktion eingeführt. Ein Algorithmus zur Bestimmung von Funktionen mit gutem Entropieprofil liegt vor. Da die sta-

tistische Unabhängigkeit zwischen den Ausgangsgrössen einer "S-box" kryptographisch sicher wünschenswert ist, werden die entsprechenden Bedingungen für boolesche Funktionen hergeleitet. Schliesslich werden "S-boxen" mit statistisch unabhängigen Funktionen untersucht, die ein gutes Entropieprofil aufweisen und durch einfache, algebraische Ausdrücke gegeben sind.

Die Resultate sind im Kapitel 6 zusammengefasst.

Résumé

La portabilité des cartes à mémoire, leur capacité de stockage, leurs facultés de calcul et leur coût relativement modeste en font un élément très prometteur des systèmes de contrôle et d'information à venir. Le présent travail s'attache aux problèmes liés à l'implémentation d'algorithmes cryptographiques dans des cartes à mémoire ainsi qu'à la sécurité de certains de ces algorithmes.

Après une brève introduction (chapitre 1), les diverses sortes de cartes à mémoire et leurs applications possibles sont passées en revue dans le deuxième chapitre. Il est montré que les avantages des cartes à mémoire par rapport aux cartes magnétiques ou à d'autres dispositifs passifs résident principalement dans le niveau de sécurité plus élevé qu'elles offrent. Cependant, de nombreux problèmes n'ont pas encore été ou n'ont été que partiellement résolus en ce qui concerne l'implémentation de systèmes de chiffrement en continu, par blocs ou à clé publique dnas les cartes à mémoire. La plupart de ces problèmes proviennent de la capacité limitée des microprocesseurs intégrés dans les cartes, que ce soit pour le stockage ou le traitement de données. Après une esquisse de ces problèmes au chapitre 3, un générateur de clé en continu est étudié du point de vue des questions spécifiquement liées à sa réalisation dans une carte à mémoire.

Dans le chapitre 4, une attaque cryptoanalytique contre une classe de générateurs de clé en continu est présentée. La version originale de cette attaque vise les générateurs formés de différents registres à décalage à rétroaction linéaire dont les sorties sont combinées par une fonction donnée. Par des modifications du schéma de base, il est possible de cryptanalyser un autre type de générateurs, à savoir ceux composés d'un unique registre à décalage à rétroaction linéaire et d'une fonction de filtrage d'état. Le fait que ces générateurs ne nécessitent la réalisation que d'un seul registre à décalage les rend particulièrement attractifs pour des applications dans des cartes à mémoire. Il est montré que les attaques décrites peuvent être mises en échec par des mesures préventives adéquates.

Le chapitre 5 traite de la conception de S-boxes pour les systèmes de chiffrement composés (product ciphers). Le critère d'avalanche strict a été défini dans le but de qualifier certaines dépendances entre entrées et sorties de fonctions booléennes. La définition première est étendue et les implications pour la transformée de Walsh des fonctions concernées sont démontrées. L'introduction du concept de profil d'entropie vise à donner des mesures quantitatives aux dépendances entrée/sortie de fonctions booléennes. Un algorithme pour la détermination de fonctions dotées d'un bon profil d'entropie est présenté. L'indépendance des sorties d'une S-box étant certainement

souhaitable du point de vue cryptographique, les conditions pour l'indépendance statistique de fonctions booléennes sont dérivées. Enfin, des S–boxes constituées de fonctions mutuellement indépendantes aux bons profils d'entropie sont analysées, de même que des S–boxes définies par des expressions algébriques simples.

Un sommaire des résultats est donné au chapitre 6.