Diss. ETH No. 17054

Weak Pseudorandomness and Unpredictability

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

ULF JOHAN SJÖDIN
MSc. in Computer Science and Engineering KTH

born 22.12.1977
citizen of Sweden

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner
Prof. Dr. Jesper Buus Nielsen, co-examiner

2007

Abstract

To base the security of practical cryptographic schemes on weakened assumptions (which are hence more likely to hold) and to improve their efficiency are general research goals in cryptography. In this thesis we continue this quest. We focus on the most traditional problems in cryptography, namely that of assuring *privacy* and *authenticity* of data in the *symmetric* setting (where both the sender and the receiver share a secret key).

We study the Feistel-network which is a popular structure underlying many block-ciphers – e.g. DES – where the cipher is constructed from many simpler rounds, each defined by some function. In particular, we investigate the security of the Feistel-network against *chosen-plaintext-attack* (CPA) distinguishers when the only security guarantee we have for the round functions is that they are secure against *non-adaptive chosen-plaintext attacks* (nCPA). Thus the round functions have a strictly weaker security guarantee than what we would like to achieve for the whole construction. We show that in the information-theoretic setting, four rounds with nCPA-secure functions are enough and necessary to get a CPA-secure permutation. We also prove that this result unfortunately does not translate into the more practically relevant pseudorandom setting.

Further, we focus on *weak* pseudorandom functions (WPRFs), defined similarly to pseudorandom functions (PRFs) but where the distinguisher only gets to see the outputs on random inputs (and not on inputs of its choice). We propose a *chosen-ciphertext-attack* secure encryption scheme, based on any WPRF, that is superior to all previous proposed schemes given in the literature (in terms of key-material and applications of the WPRF). This is achieved by an efficient strengthening of any WPRF to a PRF and by a range-extension method for WPRFs that is optimal within a large and natural class of range extensions (especially all known today).

We also introduce a general paradigm for domain extension of *message authentication codes* and an essentially optimal extension for practical use.

Zusammenfassung

Die Sicherheit kryptographischer Verfahren auf schwächere Annahmen abzustützen (welche dann plausibler sind) und die Verbesserung der Effizienz derer sind zentrale Ziele der kryptographischen Forschung, die wir auch in dieser Dissertation verfolgen werden. Wir konzentrieren uns dabei auf die traditionellen kryptographischen Probleme der *Authentisierung* und *Verschlüsselung* von Daten im *symmetrischen* Fall (in welchem Sender und Empfänger einen gemeinsamen Schlüssel besitzen).

Genauer untersuchen wir Feistelnetzwerke. Dabei handelt es sich um eine Struktur, der zahlreiche Blockchiffren wie z.B. DES zugrunde liegen. Diese Blockchiffren sind aus mehreren einfacheren Runden aufgebaut, welche jeweils durch eine Funktion definiert sind. Insbesondere betrachten wir die Sicherheit von Feistelnetzwerken gegen *Chosen-Plaintext* Attacken (CPA) für den Fall, in welchem die Rundenfunktionen nur die Sicherheit gegen nicht-adaptive *Chosen-Plaintext* Attacken (nCPA) garantieren. Folglich bieten die Rundenfunktionen deutlich schwächere Sicherheitsgarantien als wir für die Gesamtkonstruktion erreichen möchten. Wir zeigen, dass informationstheoretisch vier Runden mit nCPA-sicheren Funktionen notwendig und hinreichend sind, um eine CPA-sichere Permutation zu erhalten. Wir beweisen zudem, dass sich dieses Resultat leider nicht auf das praktisch relevantere pseudozufällige Szenario übertragen lässt.

Weiterhin beschäftigen wir uns mit so genannten *Weak Pseudorandom Functions* (WPRFs), welche ähnlich wie gewöhnliche *Pseudorandom Functions* (PRFs) mittels eines Unterscheiders definiert sind. Der Unterscheider bekommt aber nur Ausgaben auf zufällige Eingaben (statt Ausgaben auf vom Unterscheider gewählte Eingaben) zur Verfügung gestellt. Basierend auf einer beliebigen WPRF schlagen wir ein Verschlüsselungsverfahren vor, das gegen *Chosen-Ciphertext* Attacken sicher ist und (was

die Schlüssellänge und die Anzahl der Aufrufe der WPRF betrifft) sämtliche aus der Fachliteratur bekannten Verfahren überlegen ist. Wir erreichen dies durch eine effiziente Stärkung einer beliebigen WPRF zu einer PRF und durch eine Erweiterung des Bildbereiches der WPRF, welche innerhalb einer grossen und natürlichen Klasse von Bildbereichserweiterungen (insbesondere innerhalb der Klasse aller heute bekannten Erweiterungen) optimal ist.

Zusätzlich führen wir ein allgemeines Paradigma für Definitionsbereichserweiterungen von *Message Authentication Codes* ein und geben eine optimale Erweiterung an, die sich zur praktischen Anwendung eignet.