Diss. ETH No. 16619

Strengthening Key Agreement using Hard-Core Sets

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

Thomas Holenstein
Dipl. Inf. Ing. ETH

born June 14, 1976, in Zürich
citizen of Fischingen, TG

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner

Prof. Dr. Johan Håstad, co-examiner

2006

Abstract

Given an authentic communication channel, a key agreement protocol enables two parties to obtain a common bit string (the key), such that an eavesdropper does not have any information about it, even if he observes the whole communication. While no such protocol is secure in an information theoretic sense, it seems possible to give a key agreement protocol which is secure against eavesdroppers which do not have exceedingly large computational power. In fact, many protocols which promise to achieve such computational security are used in practice today. This holds even though no such protocol has been proven secure. Instead, the security of such a protocol is based on an unproven, but plausible assumption.

The goal of this thesis is to construct a computationally secure key agreement protocol whose security is based on an assumption which is as weak as possible. The assumption we use is the existence of a "weak key agreement protocol". Such a protocol works *partially*: in some executions the honest parties get the same key, but sometimes their respective keys differ. Furthermore, in some cases the resulting key is secret, while sometimes information about the key is leaked to an eavesdropper. We then strengthen such a protocol; i.e., we make it both secret and correct. In order to simplify the study, we restrict the given weak key agreement protocol to yield a single key bit.

To strengthen a weak key agreement protocol, we proceed in two steps. In a first step, we solve a related, completely information theoretic problem. More concretely we assume that some trusted source distributes random variables to the honest parties and to an eavesdropper according to a fixed and commonly known distribution. We then study whether the honest parties can use this randomness in order to obtain an information theoretically secure key. Such information theoretic key agreement from correlated information is a problem which has been studied before. It is interesting in its own right, and we look at it in some depth.

In a second step we show that certain protocols for the information theoretic setting we described can be used in the computational setting as well. Thus, we first use the weak key agreement protocol to obtain

random variables with certain computational security. We then use these random variables in a protocol designed for information theoretic security. We will see that for certain protocols the resulting key is computationally secure.

The two step process has many advantages. It greatly simplifies the constructions as well as the security proofs, since most of the work can be done in the easier information theoretic setting. It is also very intuitive, and it allows us to give constructions which work for optimal parameters.

In order to show that this two step process is possible, we use a powerful lemma about hard-core sets. Roughly speaking, the lemma shows that any computational problem which is mildly hard has a set of instances for which it is very hard. In our setting this implies that for a weak key agreement protocol as given, if the randomness of Alice and Bob is restricted to a certain subset, finding the key given the communication is a very hard problem. Such a lemma has been known before, and it has found various applications in theoretical computer science. In this thesis we improve on the known result in two ways. First, we increase the size of the hard set to the maximum possible. Further we give a variant which can be applied in the usual *uniform* setting (where the adversary is modeled as an algorithm). Previously, only a lemma applicable in the *non-uniform* setting (where the adversary is modeled using circuits) was known.

Zusammenfassung

Ein Schlüsselvereinbarungsverfahren erlaubt zwei Parteien eine geheime Bitfolge (einen sogenannten Schlüssel) zu erzeugen, falls ihnen ein authentischer Kanal zur Verfügung steht. Falls kein zusätzliches Hilfsmittel (wie zum Beispiel ein Kanal für einzelne Photonen) zur Verfügung steht, ist jedes Protokoll für diesen Zweck informationstheoretisch gesehen unsicher. Trotzdem scheint Schlüsselvereinbarung auch in diesem Fall möglich zu sein, falls Sicherheit nur gegen Gegner mit beschränkter Rechenzeit nötig ist. Tatsächlich werden in der Praxis verschiedene solche Verfahren verwendet. Unglücklicherweise kennt man für kein solches Verfahren einen Beweis für die Sicherheit. Diese beruht auf einer unbewiesenen (aber üblicherweise vernünftigen) Annahme.

Das Ziel dieser Arbeit ist die Konstruktion von einem Schlüsselvereinbarungsverfahren, basierend auf einer möglichst schwachen Annahme. Wir werden annehmen, dass ein solches Verfahren existiert, welches aber nur *teilweise* funktioniert: in einigen Ausführungen werden die ehrlichen Parteien unterschiedliche Schlüssel erhalten, und in anderen kann ein Gegner Information über den Schlüssel aus der Kommunikation folgern. Wir demonstrieren dann wie man aus einem solchen Protokoll ein sicheres erzeugt. Um dies zu erleichtern, beschränken wir uns auf den Fall in welchem das gegebene Verfahren einzelne Bits produziert.

Wir werden in zwei Schritten vorgehen. In einem ersten Schritt lösen wir ein verwandtes informationstheoretisches Problem. In diesem erhalten die ehrlichen Parteien und der Gegner korrelierte Information, wobei die Art der Korrelation allen bekannt ist. Wir studieren dann die Frage in welchen Fällen solche zusätzliche Information informationstheoretisch sichere Schlüsselvereinbarung erlaubt. Dieses Problem wurde schon in früheren Arbeiten intensiv studiert und ist auch ohne unsere ursprüngliche Motivation interessant; wir werden es deshalb eine Weile lang untersuchen.

In einem zweiten Teil werden wir zeigen dass wir gewisse Lösungen vom ersten Teil auch verwenden können, um unser ursprüngliches Problem zu lösen. Genauer: wir verwenden das gegebene teilweise funktionierende Protokoll und erzeugen damit Zufallsvariablen welche eine ge-

wisse Sicherheit gegen Gegner mit beschränkter Rechenzeit bieten. Wir verwenden diese dann in einem Protokoll für ähnliche, aber informationstheoretische sichere Zufallsvariablen, und zeigen dass der resultierende Schlüssel berechenmässige Sicherheit haben wird.

Dieser zweiteilige Beweis hat viele Vorteile. So ist er wesentlich einfacher als ähnliche bislang bekannte Beweise, und dazu auch noch recht intuitiv. Weiters erlaubt uns die Zweiteilung Konstruktionen welche für den grösstmöglichen Bereich von Parametern funktionieren.

Um zu zeigen dass diese Zweiteilung tatsächlich funktioniert verwenden wir ein mächtiges Lemma über harte Teilmengen. Salopp gesagt zeigt dieses Lemma dass jedes berechenmässig mittelschwere Problem einen "harten Kern" von Instanzen hat, auf welchem das Problem *sehr schwer* ist. In obigem Szenario impliziert es, dass in gewissen Fällen das Schlüsselbit von den ehrlichen Parteien sehr schwer vorherzusagen ist. Ein ähnliches Lemma war vor unserer Arbeit schon bekannt; wir verstärken dieses auf zwei Arten. Zum einen vergrössern wir den harten Kern auf das maximal mögliche. Zum anderen ist unser Lemma auch im üblicherweise verwendeten "uniformen" komplexitätstheoretischen Modell anwendbar. Das vorherige Lemma konnte dagegen nur im weniger verbreiteten "nicht-uniformen" Modell angewandt werden.