Bauhaus-Universität Weimar
Faculty of Media
Degree Program Computer Science and Media

Can't touch this - Public Pointing Interaction

Master Thesis

Michael Pannier
born 19th December 1984 in Dessau

Registration Number 51755

1st Reviewer: Prof. Dr. Eva Hornecker
2nd Reviewer: Prof. Dr. Sven Bertel

Date of Submission: 17th September 2014

Acknowledgement

Great thanks goes to my parents Annemarie and Joachim and my brothers Justus and Jan, who have supported me during the past two years, morally and financially. Furthermore, I would like to thank the owner of the Chair of Media Security professor Stefan Lucks, who has given me the opportunity to work in the ever-growing reasearch area of cryptography. I owe my gratitude to my advisor Christian Forler, who, with his constructive criticism and helpful remarks, helped guide this thesis to its proper destination. I also thank Christof Bräutigam, Ewan Fleischmann, Lars Harmsen, Alexander Kümmel, Eik List, Thomas Knapke, Michael Pannier und Michael Völske, for their interminable support during the time I spent working on this thesis, as well as Benno Stein for co-supervising it.

Danksagung

Mein größter Dank geht an meine Eltern Annemarie und Joachim und meine Brüder Justus und Jan, die mich während der letzten zwei Jahre moralisch und finanziell unterstützt haben. Danken möchte ich dem Inhaber des Lehrstuhls für Mediensicherheit Professor Stefan Lucks, der mir die Möglichkeit gegeben hat, in dem stetig wachsenden Forschungsgebiet der Kryptographie zu arbeiten. Meinem Betreuer Christian Forler gehört Dank, denn mit seiner konstruktiven Kritik und seinen guten Anmerkungen hat er diese Arbeit zu einem guten Ziel geführt. Weiter danke ich Christof Bräutigam, Ewan Fleischmann, Lars Harmsen, Alexander Kümmel, Eik List, Thomas Knapke, Michael Pannier und Michael Völske, die mir während meiner Bearbeitungszeit stets mit Rat und Tat zur Seite standen sowie meinem Zweitbetreuer Professor Benno Stein.

Abstract

In cryptography it is necessary to show how well some cryptographic constructs are built against potential adversaries. Usually this is done by presenting a security proof regarding to a group of adversaries to this constructs. This master thesis introduces a special case of security proofs, namely game-playing proofs. The motivation for using game-playing proofs instead of normal proofs is given through their natural and intuitive structure and understanding. This thesis is written as a students' guide and should introduce this topic to bachelor and master students in computer science. It describes the several techniques of game-playing proofs and provides examples that help the reader to understand the underlying concept.

Zusammenfassung

In der Kryptografie ist es notwendig zu zeigen, wie sicher ein kryptografisches Konstrukt gegen vorstellbare Angreifer ist. Normalerweise wird diese Sicherheit durch die Veröffentlichung eines Sicherheitsbeweises gezeigt, der sich meist auf eine Gruppe von Angreifern bezieht. Diese Masterarbeit gibt eine Einführung in einen speziellen Fall der Sicherheitsbeweise, die Game-Playing Beweise. Motiviert wird die Benutzung von Game-Playing Beweisen anstelle von normaler Beweise durch ihre natürliche und intuitive Struktur. Desweiteren sind Game-Playing Beweise im Regelfall leichter zu verstehen und nachzuvollziehen. Diese Arbeit ist als eine Einführung in das Thema für Bachelor- und Masterstudenten der Informatik geschrieben. Die Arbeit enthält eine Reihe einfach zu verstehender Beispiele, um dem Leser das Konzept der Game-Playing Beweise nahezubringen und zeigt Techniken, um diese zu realisieren.

Contents

List of Figures

Abbrevations

1 Introduction

"All modern cryptographic systems are breakable in principle; it is just a question of how long it takes." – Bellare and Rogaway from [BR05]

Security

Security is a criterion for how well some object is steeled against any form of aggressors. The term security is present in nearly all areas of the world we are living in. If you want to protect your home against intruders; if you want to avoid people stealing things from a shopping center; if you want your child to be safe in school; if you want to save your country from wars or other political disagreements or if you want to see your money safe and untouchable for others, it is all security.

This is just a small choice of realms where security is anchored and necessary. With the arrival in the computer age, IT security was born, which includes the need to keep third parties from reading your secret information, to save your applications from crashing or being destroyed or to install a network which should keep people from hacking your servers. And finally, the area of cryptography is anxious to increase security in all areas where it is necessary.

Security and Cryptography

Cryptography – the science of hiding information in practice and theory – is a very large field. The techniques developed in cryptography are used to assure that some confidential data stays confidential and no adversary can reach them. Security of data,

authenticity of an author and the integrity of data are also goals of cryptography. To be sure that some cryptographic system is secure, a proof of its security against an imaginable adversary or more than one has to be presented. Thus, assuming such a proof exists, a system can be described as being provably secure. A security proof is often done by assuming that a specific adversary to the system exists and the proof shows that the success probability of this adversary is for example smaller than some chosen threshold.

The statement from Bellare and Rogaway given above describes some fundamental knowledge about cryptographic systems. If an adversary has access to infinite resources like time or storage it can break the most of the existing cryptographic systems. This is obvious, this is true, but this does not conform to the real world. An adversary is always restricted by its resources and so security proofs are mostly done by upper bound on the probability that some given adversary is able to break some given construct. A system is called secure if no practical adversary to this system exists. A counterexample, which cannot be broken with infinite resources is the One-Time-Pad (OTP) [Tan11], if it is used correctly, i.e. a new key – which has the same length as the message – is used for every new encryption. The OTP was introduced by Gilbert Vernam in 1918 and applied the first time by Joseph O. Mauborgne.

Game-Playing Proofs

This master thesis deals with a special case of security proofs called game-playing proofs. "In our opinion, many proofs in cryptography have become essentially unverifiable. Our field may be approaching a crisis of rigor [...] game-playing may play a role in the answer." This cite is from [BR06] and the authors claim that game-playing proofs are usually less error-prone and better structured than normal proofs. Thus, they give a great opportunity to increase the understanding of security proofs.

When we began to learn the concepts of game-playing proofs, we realized that the given descriptions and proofs have a very steep learning curve. So it was quite hard to understand the complex methodology due to the lack of a tutorial. To us, there was a need of an introduction that helps us and other developing a solid understanding of the concept of game-playing proofs. The examples given in [BR06] are from our point

of view too complex to introduce game-playing and thus we decided to give some basic examples to you which are easier to understand while showing the basic techniques applied in the game-playing scenario. After reading this thesis one should be able to understand some more complex examples like the proof for the CBC MAC or the triple encryption given in [BR06] and should be able to generate first examples on one's own. To convince the reader to use game-playing proofs instead of normal proofs we give an example of these two approaches in the proof of the PRP/PRF switching lemma in Chapter **??**. Furthermore, the whole thesis should suggest the well chosen structure and the simplicity of game-playing proofs in comparison to normal proofs to the reader.

Everyone knows what a game is. And games can have alot of different characteristics and numbers of players. In the scenario of game-playing proofs, two players are usually considered, an adversary A and a challenger C; and a game G is constructed in regard to some rules and restrictions given to both the challenger C and the adversary A. The challenger itself provides the game G to A. An example for such a challenge can be given by describing the *shell game*. As we can see in Figure **??** the challenger C provides the game G by hiding a small ball under one out of three shells and shuffling in front of the player, i.e., the adversary A. After C stops, A has to decide, under which shell the ball lies.

In this scenario, considering an adversary which has only one chance to find the ball, A has a success probability of at least $1/3$ under the assumption that the challenger C is an honest player. The probability can be higher than $1/3$, if the power of observation of the adversary is taken into consideration. This example can be extended to a so called *chain of games*. A *chain of games* is generated by transforming the orginal game (in this case the game described as above) which leads to a new game H. A transformation of Game H will lead to another game I and so on. At the end of a *chain of games*, a terminal game is placed. The terminal game is usually reducable to a mathematic hard problem and thus, the success probability of an adversary in the context of the terminal game is negligible. A chain can also be defined the other way around, s.t. the chain ends with the original game. For our example a new game H can be achieved by adding another shell. Considering again an adversary A with only one chance to find the ball, its success probability for game H is at least $1/4$.

Outline

This guide provides the basic knowledge about game-playing in the first and second chapter by introducing the game-playing technique itself, showing some widely spread examples and introducing pseudorandom functions and permutations, respectively. Chapter **??** and **??** describe some techniques to build up a game and to generate a *chain of games*. Beneith the definition of these techniques we are showing easy to understand examples, where these techniques can be applied in games. Chapter **??** concludes this tutorial with a question-and-answer part with the most frequently asked questions that arose when giving this thesis to some of our fellow students.

Bibliography

[BR05] Mihir Bellare and Phillip Rogaway. Introduction to modern cryptography. In *UCSD CSE 207 Course Notes*, 2005.

[BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *EUROCRYPT*, pages 409–426, 2006.

[Tan11] Till Tantau. The one-time pad algorithm - the simplest and most secure way to keep secrets. In *Algorithms Unplugged*, pages 141–146. 2011.

Affidavit

Eidesstattliche Erklärung

Hiermit versichere ich, dass ich die Masterarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, alle Ausführungen, die anderen Schriften wörtlich oder sinngemäß entnommen wurden, kenntlich gemacht sind und die Arbeit in gleicher oder ähnlicher Fassung noch nicht Bestandteil einer Studien- oder Prüfungsleistung war.

Affidavit

I hereby declare that this master thesis has been written only by the undersigned and without any assistance from third parties. Furthermore, I confirm that no sources have been used in the preparation of this thesis other than those indicated in the thesis itself, as well as that the thesis has not yet been handled in neither in this nor in equal form at any other official comission.

Jakob Wenzel