Cryptographical Knowledge Comparator

Subject: ITS
Thesis advisor: Prof. Dr. Reto König
Expert: Stefan Berner (Diso Solution AG)

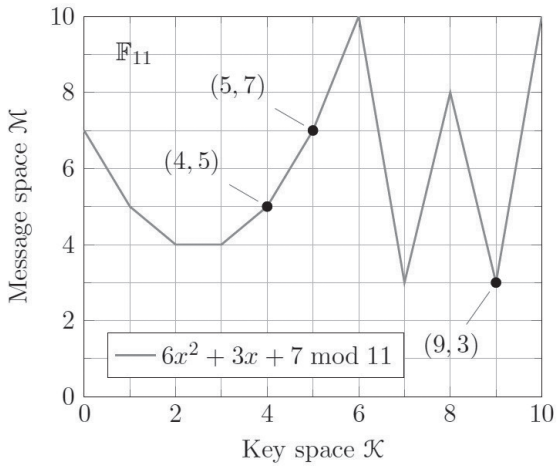
Based on a new cryptographic component, we designed and implemented a proof of concept protocol to encrypt knowledge in a way it can not be read unless you already know it. To show the protocol in practice, a game which is usually played with two players - Black Box - has been implemented in a way that it can be played offline by one player. The solution is already included, but you have to play the game to find it.

Introduction

Commitment schemes are the cryptographic equivalent of putting a value in a safe deposit box for later verification while ensuring that it has not been modified in the meantime. Depending on the protocol, the verification process may or may not require the value to be public. This thesis introduces a practical example of such a commitment scheme based on a new cryptographic component called multi-encryption, used to verify a previously committed value if, and only if, it is already known – hence the name Cryptographic Knowledge Comparator.

Theory

The multi-encryption scheme introduced by Koenig and Haenni allows encrypting multiple secrets into one ciphertext, a property it inherits from its underlying mathematical component, a univariate polynomial over a finite field. It is built using polynomial interpolation using the x values as the key and the y values as the corresponding secrets. The scheme itself and various enhancements such as randomization, key mapping and secret space randomization are discussed in detail.



We show that the multi-encryption scheme is indeed usable as a cryptographic building block for a commitment scheme, having the unique property of supporting multiple commitments per ciphertext without the need of an additional mapping layer. However, of the two basic properties of a commitment scheme – hiding and binding – only the first one is strong enough for a wide range of applications. As the binding property is considerably weaker, only specific use cases should be regarded as suitable for this scheme. Namely, where trust in the commiting party is a given or when additional committed values (either implicit or explicitly chosen) do not affect its functionality or security.

Implementation

To demonstrate the real world usage of said multi-commitment scheme, two offline applications for the Black Box game were developed. With the producer application, a user prepares a game which can be exported in a way that its solution is no longer obtainable and can only be verified by those who already know it. The export format is either an XML file or a QR code, both non-interactive protocols for offline usage. The consumer application is able to load an exported game and allows a player to play the game. If a possible solution was found, it can only be verified – the correct solution itself is hidden in the ciphertext and cannot be read from it, except by bruteforcing or attacking the underlying multi-encryption scheme.

The applications are created using the Google Web Toolkit (GWT) framework, allowing implementing web applications using Java and compiling it to native HTML5 and JavaScript for offline usage. The Android application is built using the Cordova container, which allows to package web applications in a way they can access device services like the camera, which is used to scan a QR code.

Matthias Blaser

Florian Leuenberger