Study of Correlation Intractable Hash Functions

Endrit VORFAJ

School of Computer and Communication Sciences

Semester Project

June 2024

Responsible
Prof. Serge Vaudenay
EPFL / LASEC

Supervisor
Abdullah TALAYHAN
EPFL / LASEC

1 Introduction

Non-interactive zero-knowledge (NIZK) proofs enable a prover to convince a verifier of the validity of an NP-statement with just one round of communication, where a single message is sent from the prover to the verifier. One of the most prominent methods for creating non-interactive proofs is the Fiat-Shamir (FS) transform. This transformation takes a sigma-protocol and converts it into a NIZK proof.

We briefly mention interactive proof protocols and we consider the definitions of sigma-protocols which are a specific type of three-round public-coin interactive proof conducted between a prover P and a verifier V.

In these protocols, the only interaction between the prover P and the verifier V happens in the second round where the verifier with a challenge e to the initial message of the prover (denoted as a). The FS transform makes a sigma-protocol non-interactive by allowing the prover to generate the challenge itself. Specifically, the prover computes $e \leftarrow H(a)$, where H is a hash function. The security of this construction can be argued by modeling H as a Random Oracle, introduced in [BR93]. However, recent research ([CX23], [Can+18a]) has demonstrated that if the hash function is correlation-intractable (CI) for certain relations, then it is possible to construct a NIZK protocol using only the CI property instead of the random oracle model. Informally, the CI property ensures that given a random hash key k, it is computationally difficult to find any input x such that $(x, H_k(x)) \in R$ for a particular relation R.

In greater detail, [Can+19] demonstrated that the FS transform remains secure if the hash function is CI for efficiently searchable relations. Their results apply to a specific class of sigma-protocols known as trapdoor sigma-protocols. These protocols are defined in the Common Reference String (CRS) model and possess three main properties: honest verifier zero-knowledge (HVZK), optimal soundness, and a bad-challenge extractor.

The HVZK property is quite standard, ensuring the existence of a simulator that, given the challenge (the second round), produces a transcript indistinguishable from one generated by an honest prover and verifier. Optimal soundness guarantees that for any statement $x \notin L$ and any first-round message a, there is at most one challenge e that would make the verifier accept the transcript (a, e, z) for some third-round message z. This unique challenge e is referred to as the bad-challenge. Lastly, the bad-challenge extractor is an algorithm that, given a false statement x, a valid first-round message a, and some trapdoor information τ, can efficiently compute the bad-challenge e.

By exploring these foundational concepts, this paper aims to provide a comprehensive study of correlation intractability, focusing on the theoretical underpinnings and practical implementations of these functions, and providing insights into their role in modern cryptography. We then examine the failures of the random oracle model as described in [CGH04], discussing its limitations in the face of real-world implementations and security. From there, we discuss more formally the nature and utility of CI hash functions and we mention a CI construction that employs shiftable shift-hiding functions as outlined in [LV20]. Our objective is to define basic cryptographic primitives as pedagogically as possible, aiming to produce a report that is both self-contained and comprehensive. This document is designed to serve as a foundational basis for individuals embarking on research in correlation intractable hash functions, equipping them with the necessary tools and knowledge to advance the field.