A New Efficient Construction for Non-Malleable Zero-Knowledge Sets

Wenpan Jing, Haixia Xu, and Bao Li

State Key Laboratory of Information Security,
Graduate University of Chinese Academy of Sciences,
No.19A Yuquan Road, 100049 Beijing, China
{wpjing,hxxu,lb}@is.ac.cn

Abstract. The idea of Zero-Knowledge Sets (ZKS) was firstly proposed by Micali, Rabin and Kilian. It allows the prover to commit to a secret set and then prove either “\(x \in S\)” or “\(x \notin S\)” without revealing any more knowledge of the set S. Afterwards, R. Gennaro defined the concept of independence for ZKS and gave two tree-based constructions. In this paper, we define the independence property for ZKS in a more flexible way than the definition of Gennaro’s and prove that for ZKS, our independence implies non-malleability and vice versa. Then an independent ZKS scheme is constructed in an algebraic way by mapping values to unique primes, accumulating the set members and hiding the set. Comparing with the tree-based constructions: our scheme is more efficient while proving a value belongs (resp. not belongs) to the committed set; furthermore, the committed set is easier to update.

Keywords: zero-knowledge set, commitment, non-malleability, independence.

1 Introduction

Two roles are involved in a zero-knowledge sets (ZKS) protocol, known as the prover and the verifier. The main purpose of ZKS is that for any finite set \(S\), which consists of some finite strings, the prover can produce a commitment of the set and prove either “\(x \in S\)” or “\(x \notin S\)” (\(x \in \{0, 1\}^*\) is an arbitrary string) without revealing any more knowledge of the set \(S\), even the size of the set. Furthermore, the verifier could not be cheated, which means that any prover can not successfully prove both “\(x \in S\)” and “\(x \notin S\)” once the commitment is fixed.

One can see that ZKS is a basic cryptographic primitive which is highly related to commitment scheme and zero-knowledge proof protocol. A ZKS protocol can be regarded as a special commitment scheme that commits to multiple strings, requiring “hiding” and “binding” properties as a normal commitment scheme, but can be partially opened (only revealing one string each time). It also can be regarded as a special zero-knowledge argument system which not only gives a proof when “\(x \in L\)”, but also gives a proof when “\(x \notin L\)”, where \(L\) is a language. Besides, ZKS has a brilliant application perspective in protecting the security of database access [12].

* Supported by the National Natural Science Foundation of China (No.60673073), the National High-Tech Research and Development Plan of China (863 project) (No.2006AA01Z427) and the National Basic Research Program of China (973 project)(No.2007CB311201).
1.1 Background

The idea of Zero-Knowledge Sets was first proposed by Micali, Rabin and Kilian [12]. A very creative construction of ZKS was given in the same issue. They used Pederson’s commitment scheme and Merkle tree to generate the commitment to a set \( S \). They claimed that if discrete logarithm problem was hard, then their construction was a ZKS scheme. Moreover, Micali et al. introduced the notion of “Fake” commitment to prune the tree and greatly reduced the complexity. A new variety of commitment, which is called “Mercurial Commitment”, was abstracted by Chase et al. in [3] from the idea of “Fake” commitment. Mercurial Commitment is a trapdoor commitment with relaxation in binding property. With the notion of mercurial commitment abstracted, to build ZKS falls into a routine job: one needs only to combine any mercurial commitment and any collision-resistant hash function together. Afterwards, Catalano et al. in [1] studied further on mercurial commitment, especially on their constructions.

Gennaro and Micali gave the notion of independent ZKS [8]. They claimed that independence is a security requirement which is at least as secure as non-malleability. A cryptographic system is non-malleable means that it could resist the so-called man-in-the-middle attack [7]. In the ZKS system particularly, any adversary could not correlate produce commitments of sets or proofs after interact with the prover. They constructed commitment schemes both being non-malleable and mercurial, and built independent zero-knowledge sets from them.

Catalano, Fiore and Messina proposed a ZKS scheme with short proofs [2]. They used tree-based structure with a new mercurial commitment called “trapdoor q-mercurial commitment” which allowed a sequence of elements to be committed at one time. As a result, the depth of the tree was effectively reduced and consequently the proofs of each element was shortened.

All of the ZKS schemes above are based on mercurial commitment and collision-resistant hash functions. They all use the tree-based structure which has lots of advantages, e.g., the design is modularized; the commitment of the set is easy to generate and efficient to store. However, the proof to each \( x \) grows along with the increase of the depth of the tree; moreover, the tree based structure makes the ZKS hard to be updated. Unfortunately, these flaws are fatal while coming into practice and hard to conquer with this specific structure.

Xue et al. proposed a completely different algebraic construction of ZKS based on strong RSA assumption [15]. They introduced a new collision-free hash function which mapped each natural number to a unique prime number, then built the commitment using an accumulator like construction. The scheme has many advantages: easy to be updated; easy to be programmed; the commitment and the proofs are all very short; the elements in the set do not need to be ordered, etc. However, the scheme could not resist malleability attack.

1.2 Our Contributions

A new definition of independence for zero-knowledge sets is presented. Comparing with the definition in [8], our definition is more simplified and fixes a slight flaw of the definition in [8]. Moreover, the author of [8] claimed independence was at least as