Dynamics of Continuous, Discrete and Impulsive Systems
Series **B:** *Applications & Algorithms* **12 (2005)** 633-648

Some Observations on Zap and Its Applications

Yunlei Zhao[1], C. H. Lee[2], Yiming Zhao[1] and Hong Zhu[1]

[1]Department of Computer Science and Engineering
Fudan University, Shanghai 200433, P. R. China
[2]Department of Computer Science
City University of Hong Kong, Hong Kong

Abstract. In this paper we make some observations on the zaps and their applications developed by Dwork and Naor [13]. We clarify the relations among public-coin witness indistinguishability (WI), public-coin honest verifier zero-knowledge (HVZK) and public-coin special honest verifier zero-knowledge (SHVZK). Specifically, we observe that the existence of zaps under the existence of one-way permutations actually strictly separates public-coin WI and public-coin SHVZK assuming $\mathcal{NP} \nsubseteq \mathcal{BPP}$. We also show that public-coin HVZK does not implies WI assuming the existence of one-way permutations. For zap-based applications, we present an improved Dwork-Naor 2-round timed deniable authentication scheme that improves the communication and computation complexity of the original protocol presented by Dwork and Naor [13]. Specifically, in the improved protocol the first message (from the verifier to the authenticator) is independent on the message to be authenticated by the authenticator.

Keywords. cryptography, interactive proof systems, zap, deniable authentication, software copyright protection

1 Introduction

Zap, first introduced by Dwork and Naor [13], is itself a 2-round public-coin witness indistinguishable (WI) proof system for $\mathcal{NP}$. Zaps are a very powerful cryptographic tool to significantly simplify many cryptographic tasks. As a notable example, it is used to achieve the first 2-round timed deniable authentication scheme [13].

Deniable authentication first appears in [10, 12], and is then formalized in [14]. Roughly speaking, a deniable authentication scheme is a *public-key interactive* authentication scheme in which an authenticator AP convinces a second party V, only accessing to AP's public-key, that AP is willing to authenticate a message m. However, different from the case of digital signatures, deniable authentication does not permit V to convince a third party that AP has authenticated m. That is, there is no “paper trail” of the conversation other than what could be produced by V alone. Several 4-round timed deniable authentication protocols appear in [14, 15] and the first 2-round timed deniable authentication is presented by Dwork and Naor in [13].