Efficient Concurrent $n^{\text{poly} \left( \log n \right)}$-Simulatable Argument of Knowledge*

Guifang Huang$^{1,3}$, Dongdai Lin$^{1,3}$, and Yanshuo Zhang$^{2}$

$^1$ The State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, 100190, P.R. China
{hgf,ddlin}@iscas.ac.cn

$^2$ Beijing Institute of Electronic Science and Technology, Beijing, 100070, P.R. China
zhangyanshuo@amss.ac.cn

$^3$ Graduate University of Chinese Academy of Sciences, P.R. China, 100049

Abstract. In [16], Pass generalized the definition of zero knowledge proof and defined $n^{O(\sigma(n))}$-simulatable proof which can be simulated by a simulator in $n^{O(\sigma(n))}$ time. Assuming the existence of one-way permutation secure against sub-exponential circuits and 2-round perfect hiding commitment scheme, an efficient 4-round perfect $n^{\text{poly} \left( \log n \right)}$-simulatable argument of knowledge was presented there.

In this paper, we construct an efficient concurrent $n^{\text{poly} \left( \log n \right)}$-simulatable argument of knowledge under more general assumption. The new scheme is 5-round and is based on the existence of one-way permutation secure against sub-exponential circuits. However, for the scheme in [16], if using ordinary $\Sigma$-protocol for the corresponding statement as sub-protocol, instead of $\Sigma$-protocol with honest verifier perfect zero knowledge, the resulting protocol is not necessarily closed under concurrent composition.

Keywords: straight-line $n^{\text{poly} \left( \log n \right)}$-simulatable, argument of knowledge, $\Sigma$-protocol.

1 Introduction

Zero knowledge (short for ZK) proof, brought out by Goldwasser, Micali and Rack-off [11], is a protocol between two parties: prover and verifier, in which prover can convince verifier the validity of a statement but reveals nothing. Since its invention, ZK proof has attracted much attention and a great deal of work has been done on it. One of the most fundamental results achieved is that every language in $NP$ has a ZK proof [12]. Nowadays, ZK proof has played a central role in study of cryptographic protocols. For example, it can be used in multi-party computation [89] to have the parties prove the correctness of their computations.

The definition of ZK proof is formalized through simulation paradigm. That is, for every probabilistic polynomial time verifier, there exists a probabilistic

* This work is supported by NSFC under grant No. 60673069, 60803128, and the National 863 Program under grant No. 2007AA01Z447.
polynomial time simulator such that what the simulator outputs is indistinguishable from the real interaction. Although ZK proof is very useful in the design of increasingly complex cryptographic tasks, many limitations are known \[10,13,14\]. As a result, general protocols, whose security requirements are formalized by simulation paradigm of ZK proof, inherit these limitations. For example, recently several limitations have been shown concerning the concurrent composition [6] of secure two-party and multi-party protocols [14,15]. In order to overcome some of these limitations, some relaxed notions which are good enough for applications are brought out. A first step in this direction is the definition of witness indistinguishability [7]. Recently, Pass [16] defined another relaxed notion—\(n^{O(\sigma(n))}\)-simulatable proof (argument). It was pointed out that \(n^{O(\sigma(n))}\)-simulatable argument can be used as a sub-protocol to construct universal composable secure protocols.

\(n^{O(\sigma(n))}\)-simulatable argument is that for every probabilistic polynomial time verifier, there exists a simulator with running time \(n^{O(\sigma(n))}\) which can simulate the real conversation. From definition of ZK argument, it is concluded that ZK argument is \(n^{O(1)}\)-simulatable argument. Therefore, \(n^{O(\sigma(n))}\)-simulatable argument is a generalization of definition of ZK argument. Furthermore, \(n^{O(\sigma(n))}\)-simulatable argument is witness indistinguishable. Therefore, \(n^{O(\sigma(n))}\)-simulatable argument is a notion between ZK and witness indistinguishability.

In [16], based on the assumption that there exist one-way permutation secure against sub-exponential circuits and 2-round perfect hiding commitment scheme, an efficient 4-round concurrent perfect \(n^{\text{poly}(\log n)}\)-simulatable argument of knowledge was constructed. Honest verifier perfect ZK property of \(\Sigma\)-protocol contributes to the “perfect” property of the construction, which in turn results in its closeness under concurrent composition. However, if using ordinary \(\Sigma\)-protocol instead of \(\Sigma\)-protocol with honest verifier perfect ZK property as a tool, the resulting scheme is not necessarily closed under concurrent composition.

In this paper, using ordinary \(\Sigma\)-protocol as a tool, we give an efficient concurrent \(n^{\text{poly}(\log n)}\)-simulatable argument of knowledge under more general assumption. The scheme is 5-round and is based on the existence of one-way permutation secure against sub-exponential circuits.

It is organized as follows. In section 2, some related notions and definitions are given. In section 3, we present the 5-round concurrent \(n^{\text{poly}(\log n)}\)-simulatable argument of knowledge and gives the corresponding proofs.

2 Preliminaries

A function \(f(n)\) is called negligible, if for every positive polynomial \(q(n)\), there exists \(N\) such that for all \(n \geq N\), we have \(f(n) \leq 1/q(n)\).

**Definition 1.** (one-way function secure against sub-exponential circuits [16]) \(f : \{0,1\}^* \rightarrow \{0,1\}^*\) is called one-way function secure against \(2^{\alpha k}\) adversary, if the following conditions hold: