Cryptology ePrint Archive: Report 2011/408

Resettable Cryptography in Constant Rounds -- the Case of Zero Knowledge

Yi Deng and Dengguo Feng and Vipul Goyal and Dongdai Lin and Amit Sahai and Moti Yung

Abstract: A fundamental question in cryptography deals with understanding the role that randomness plays in cryptographic protocols and to what extent it is necessary. One particular line of works was initiated by Canetti, Goldreich, Goldwasser, and Micali (STOC 2000) who introduced the notion of resettable zero-knowledge, where the protocol must be zero-knowledge even if a cheating verifier can reset the prover and have several interactions in which the prover uses the same random tape. Soon afterwards, Barak, Goldreich, Goldwasser, and Lindell (FOCS 2001) studied the setting where the \emph{verifier} uses a fixed random tape in multiple interactions. Subsequent to these works, a number of papers studied the notion of resettable protocols in the setting where \emph{only one} of the participating parties uses a fixed random tape multiple times. The notion of resettable security has been studied in two main models: the plain model and the bare public key model (also introduced in the above paper by Canetti et. al.).

In a recent work, Deng, Goyal and Sahai (FOCS 2009) gave the first construction of a \emph{simultaneous} resettable zero-knowledge protocol where both participants of the protocol can reuse a fixed random tape in any (polynomial) number of executions. Their construction however required $O(n^\\epsilon)$ rounds of interaction between the prover and the verifier. Both in the plain as well as the BPK model, this construction remain the only known simultaneous resettable zero-knowledge protocols.

In this work, we study the question of round complexity of simultaneous resettable zero-knowledge in the BPK model. We present a \emph{constant round} protocol in such a setting based on standard cryptographic assumptions. Our techniques are significantly different from the ones used by Deng, Goyal and Sahai.

Category / Keywords: zero knowledge

Date: received 30 Jul 2011, last revised 2 Aug 2011

Contact author: ydeng cas at gmail com