Cryptology ePrint Archive: Report 2011/228

A Framework for Practical Universally Composable Zero-Knowledge Protocols

Jan Camenisch and Stephan Krenn and Victor Shoup

Abstract: Zero-knowledge proofs of knowledge (ZK-PoK) for discrete logarithms and related problems are indispensable for practical cryptographic protocols. At \emph{Eurocrypt 2009}, Camenisch, Kiayias, and Yung provided a specification language (the \emph{CKY-language}) for such protocols, which allows one to modularly design and analyze cryptographic protocols: protocol designers just need to specify the statement they want to prove in zero-knowledge and are ensured that an efficient proof protocol exists and indeed proves the specified statement, provided that the specification was in the CKY-language.

However, as specifications in the CKY-language are realized by so-called Σ-protocols, the resulting protocols only satisfy the classical notion of zero-knowledge proofs of knowledge, which \emph{not} retained if they are composed with themselves or with other protocols, e.g., when used as building blocks for higher-level applications. This problem can be tackled by moving to the Universal Composability (UC) framework, which guarantees retention of security when composing protocols and, in particular, when using them as building blocks in arbitrary contexts. While there exists generic transformations from Σ-protocols to protocols that are secure under this stronger security notion, these transformation are often not efficient enough for the design of practical protocols.

In this paper we are aiming for practically efficient ZK-PoK in the UC-framework by introducing a specification language akin to the CKY-language and a compiler such that protocols specified in our language are UC-secure and efficient. To this end we propose an extension of the UC-framework addressing the problem that UC-secure zero-knowledge proofs are always proofs \emph{of knowledge}, and state a special composition theorem which allows one to use the weaker -- but more efficient and often sufficient -- notion of proofs \emph{of existence} in the UC-framework for the first time. We believe that our contributions enable the design of practical protocols that are UC-secure and thus themselves can be used as building blocks.

Category / Keywords: cryptographic protocols / Universal Composability; Protocol Design; Zero-Knowledge; Proof of Knowledge;

Date: received 10 May 2011

Contact author: stephan krenn at bfh ch

Available formats: PDF | BibTeX Citation

Version: 20110512:035107 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]