Cryptology ePrint Archive: Report 2011/035

A New Family of Practical Non-Malleable Protocols

Andrew C. Yao and Yunlei Zhao

Abstract: Nowadays, achieving cryptosystems secure in an asynchronous network like the Internet is demanded to be necessary, where concurrent non-malleable proof-of-knowledge and universal composability are among the most powerful and fundamental security properties. But, when achieving more and more complex cryptosystems secure in an open network like the Internet, it is often the case that generic solutions are either impossible or infeasible.

In this work, we investigate highly practical approaches for achieving non-malleable cryptosystems secure against concurrent man-in-the-middles. We start our study with the Diffie-Hellman key-exchange (DHKE) protocol, which is at the root of public-key cryptography and is one of the main pillars of both theory and practice of cryptography. We develop the mechanisms of non-malleable joint proof-of-knowledge (NMJPOK) and self-sealed joint proof-of-knowledge (SSJPOK), which are of independent values. In particular, using NMJPOK and SSJPOK as the key building tools, we present a new family of DHKE protocols, with remarkable performance among security, privacy, efficiency and easy deployment. Particularly important to applied crypto engineering, the newly developed DHKE protocols add novelties and values to a range of key industry standards for ensuring network security (e.g., IKE, (H)MQV, SSH, etc). Along the way, we also reinvestigate the security definition frameworks for DHKE, and clarify various subtleties surrounding the design and analysis of non-malleable DHKE protocols.

Then, motivated by the building tools, NMJPOK and SSJPOK, proposed and justified in this work, we formulate non-malleable extractable joint one-way function (NME-JOWF), and demonstrate general applications of NME-JOWF (including 3-round CNMZK and UCZK in the plain model). Then, we propose candidates of NME-JOWF based upon bilinear pairings, and show various concrete applications of the pairing-based NME-JOWF candidates.

Category / Keywords: cryptographic protocols /

Publication Info: The results originally appeared in a Chinese patent in 2007, and later in a PCT patent in 2008 (with the 2007 patent as priority reference). More details and protocol variants can also be found in the patent files.

Date: received 20 Jan 2011, last revised 27 Jan 2011

Contact author: yunleizhao at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110127:101027 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]