Cryptology ePrint Archive: Report 2013/108

Unconditionally Secure and Universally Composable Commitments from Physical Assumptions

Ivan Damgard and Alessandra Scafuro

Abstract: We present a constant-round unconditional black-box compiler, that transforms any ideal straight- line extractable commitment scheme, into an extractable and equivocal commitment scheme, therefore yielding to UC-security [Can01]. We exemplify the usefulness of our compiler providing two (constant- round) instantiations of ideal straight-line extractable commitment using (malicious) PUFs [OSVW13] and stateless tamper-proof hardware tokens [Kat07]. This allows us to achieve the first unconditionally UC-secure commitment with malicious PUFs and the first unconditionally UC-secure commitment with stateless tokens. Our constructions are secure for adversaries creating arbitrarily malicious stateful PUFs/tokens. Previous results with malicious PUFs used either computational assumptions to achieve UC-secure commitments or were unconditionally secure but only in the indistinguishability sense [OSVW13]. Similarly, with stateless tokens, UC-secure commitments are known only under computational assumptions [CGS08, GIS+10, CKS+11], while the (not UC) unconditional commitment scheme of [GIMS10] is secure only in a weaker model in which the adversary is not allowed to create stateful tokens. Besides allowing us to prove feasibility of unconditional UC-security with (malicious) PUFs and stateless tokens, our compiler can be instantiated with any ideal straight-line extractable commitment scheme, thus allowing the use of various setup assumptions which may better fit the application or the technology available.

Category / Keywords: foundations / UC, hardware assumptions, unconditional security, commitment scheme

Date: received 24 Feb 2013, last revised 21 May 2013

Contact author: alescafu at gmail com
