Cryptology ePrint Archive: Report 2013/090

Functional Encryption Supporting Recursive Languages

Somindu C. Ramanna and Palash Sarkar

Abstract: We provide a construction for functional encryption over the set of recursive languages. In this scheme, a secret key $\sk_{\mathcal{M}}$ encodes a halting double-stack deterministic pushdown automaton (2DPDA) $\mathcal{M}$ that accepts by final state. Encryption algorithm takes a message m and a string w as input and outputs a ciphertext $\cipher$. A user possessing $\sk_{\mathcal{M}}$ can decrypt $\cipher$ only if $\mathcal{M}$ accepts w. Halting 2DPDAs can simulate halting deterministic Turing machines and hence our construction essentially covers all recursive languages.

The construction is built upon Waters' bilinear pairing-based functional encryption scheme over regular languages. The main technical novelty is in handling stack contents and λ-transitions (i.e., transitions that do not advance the input pointer) of the automata. This is reflected both in the construction and the security arguments. The scheme is shown to be selectively secure based on the decision ℓ-expanded bilinear Diffie-Hellman exponent assumption introduced by Waters.

Category / Keywords: public-key cryptography / functional encryption, recursive languages, pushdown automata

Date: received 20 Feb 2013, last revised 12 Mar 2013, withdrawn 20 Mar 2013

Contact author: somindu_r at isical ac in

Available format(s): (-- withdrawn --)

Version: 20130320:112515 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]