Cryptology ePrint Archive: Report 2011/096

Computing on Authenticated Data

Jae Hyun Ahn and Dan Boneh and Jan Camenisch and Susan Hohenberger and abhi shelat and Brent Waters

Abstract: In tandem with recent progress on computing on encrypted data via fully homomorphic encryption, we present a framework for computing on *authenticated* data via the notion of slightly homomorphic signatures, or P-homomorphic signatures. With such signatures, it is possible for a third party to derive a signature on the object m' from a signature of m as long as P(m,m')=1 for some predicate P which captures the ``authenticatable relationship" between m' and m. Moreover, a derived signature on m' reveals no extra information about the parent m.

Our definition is carefully formulated to provide one unified framework for a variety of distinct concepts in this area, including arithmetic, homomorphic, quotable, redactable, transitive signatures and more. It includes being unable to distinguish a derived signature from a fresh one even when given the original signature. The inability to link derived signatures to their original sources prevents some practical privacy and linking attacks, which is a challenge not satisfied by most prior works.

Under this strong definition, we then provide generic constructions for all univariate and closed predicates, and specific efficient constructions for a broad class of natural predicates such as quoting, subsets, weighted sums, averages, and Fourier transforms. To our knowledge, these are the first efficient constructions for these predicates (excluding subsets) that provably satisfy this strong security notion.

Category / Keywords: public-key cryptography / authentication, homomorphic signatures, quoting

Publication Info: Full version of paper in TCC 2012.

Date: received 24 Feb 2011, last revised 26 Dec 2011

Contact author: susan at cs jhu edu

Available formats: PDF | BibTeX Citation

Version: 20111226:193805 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]