Cryptology ePrint Archive: Report 2011/495

Vector Commitments and their Applications

Dario Catalano and Dario Fiore

Abstract: We introduce a new primitive that we call {\em Vector Commitment} (VC, for short). Informally, VCs allow to commit to an ordered sequence of q values $(m_1, \ldots, m_q)$ (i.e., a vector) in such a way that one can later open the commitment at specific positions (e.g., prove that m_i is the i-th committed message). For security, Vector Commitments are required to satisfy a notion that we call \emph{position binding} which states that an adversary should not be able to open a commitment to two different values at the same position. Moreover, what makes our primitive interesting is that we require VCs to be {\em concise}, i.e. the size of the commitment string and of its openings has to be independent of the vector length.

We show two realizations of VCs based on standard and well established assumptions, such as RSA, and Computational Diffie-Hellman (in bilinear groups).

Next, we turn our attention to applications and we show that Vector Commitments turn out to be useful in a variety of contexts, as they allow for compact and efficient solutions which significantly improve previous works either in terms of efficiency of the resulting solutions, or in terms of "quality" of the underlying assumption, or both. These applications include: Verifiable Databases with Efficient Updates, Updatable Zero-Knowledge Databases, and Universal Dynamic Accumulators.

Category / Keywords: Vector Commitments, Commitments, Accumulator, Zero-Knowledge Databases, Verifiable Databases

Date: received 12 Sep 2011, last revised 17 Feb 2012

Contact author: fiore at cs nyu edu