Cryptology ePrint Archive: Report 2013/120

An Attack Against Fixed Value Discrete Logarithm Representations

Gergely Alpár and Jaap-Henk Hoepman and Wouter Lueks

Abstract: Attribute-based credentials (ABCs) are an important building block of privacy-enhancing identity management. Since non-identifying attributes can easily be abused as the anonymity they provide hides the perpetrator, cryptographic mechanisms need to be introduced to make them revocable. However, most of these techniques are not efficient enough in practice. ABCs with practical revocation have recently been proposed by Hajny and Malina~\cite{Hajny-Malina-2012}. Their ABCs make use of different discrete logarithm representations of a fixed value. Although this technique is attractive as the verification of a particular issuer's credentials is easy, it has an intrinsic weakness. Colluding users can efficiently forge new credentials that are indistinguishable from legally issued ones.

Category / Keywords: cryptographic protocols / attribute-based credentials, revocation, cryptanalysis, discrete logarithm representation

Date: received 28 Feb 2013, last revised 5 Mar 2013

Contact author: gergely at cs ru nl