# Cryptology ePrint Archive: Report 2011/700

**Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model**

*Tatsuaki Okamoto and Katsuyuki Takashima*

**Abstract:** This paper presents a fully secure (adaptive-predicate unforgeable and private) attribute-based signature (ABS) scheme in the standard model. The security of the proposed ABS scheme is proven under standard assumptions, the decisional linear (DLIN) assumption and the existence of collision resistant (CR) hash functions. The admissible predicates of the proposed ABS scheme are more general than those of the existing ABS schemes, i.e., the proposed ABS scheme is the first to support general non-monotone predicates, which can be expressed using NOT gates as well as AND, OR, and Threshold gates, while the existing ABS schemes only support monotone predicates. The proposed ABS scheme is efficient and practical. Its efficiency is comparable to (several times worse than) that of the most efficient (almost optimally efficient) ABS scheme the security for which is proven in the generic group model.

**Category / Keywords:** public-key cryptography / attribute-based signatures, multi-authority system, non-monotone predicates

**Publication Info:** An extended abstract was presented at Public Key Cryptography -- PKC 2011, LNCS 6571, pages 35-52. This is the full paper.

**Date:** received 22 Dec 2011

**Contact author:** Takashima Katsuyuki at aj MitsubishiElectric co jp