



VARIANTS OF BLIND SIGNATURES - A PRACTICAL AUTHENTICATION SCHEME

SANGEETHA JOSE¹ & SUDIN S²

¹Assistant Professor, Department of Information Technology Government Engineering College Idukki, Kerala, India

²Head and Assistant Professor, Department of Mathematics Government Engineering College Idukki, Kerala, India

ABSTRACT

Blind signature is a variant of digital signature which helps the user to obtain a signature without giving any information about the message to the signer and the signer cannot tell which session of the signing protocol corresponds to which message. Blind signatures may seem to be a myth; it is a practical reality due to its wide applications in real life like e-coin and e-voting. This paper focuses on the study of variants of blind signatures with its eminent real world applications. It also discusses about future research scope of blind signatures.

KEYWORDS: Blindness, Blind Signature, Unforgeability, Unframeability