Cryptology ePrint Archive: Report 2011/316

Security of Blind Signatures Revisited

Dominique Schröder and Dominique Unruh

Abstract: We revisit the definition of unforgeability of blind signatures as proposed by Pointcheval and Stern (Journal of Cryptology 2000). Surprisingly, we show that this established definition falls short in two ways of what one would intuitively expect from a secure blind signature scheme: It is not excluded that an adversary submits the same message m twice for signing, and then produces a signature for $m'\neq m$. The reason is that the forger only succeeds if \emph{all} messages are distinct. Moreover, it is not excluded that an adversary performs k signing queries and produces signatures on $k+1$ messages as long as \emph{each} of these signatures does not pass verification with probability~1.

Finally, we proposed a new definition, honest-user unforgeability, that covers these attacks. We give a simple and efficient transformation that transforms any unforgeable blind signature scheme (with deterministic verification) into an honest-user unforgeable one.

Category / Keywords: public-key cryptography / blind signatures, definitions,

Date: received 15 Jun 2011

Contact author: schroeder at me com