SCHOOL OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING
MONASH UNIVERSITY

TECHNICAL REPORT 2003/145

Content Extraction Signatures

R Steinfeld, L Bull and Y Zheng

ABSTRACT

Motivated by emerging needs in online interactions, we define a new type of digital signature called a 'Content Extraction Signature' (CES). A CES allows the owner, Bob, of a document signed by Alice, to produce an 'extended signature' on selected extracted portions of the original document, which can be verified to originate from Alice by any third party. Cathy, while hiding the unextracted (removed) document portions. The new signature therefore achieves verifiable content extraction with minimal multi-party interaction. We specify desirable functional and security requirements for a CES (including an efficiency requirement: a CES should be more efficient in either computation or communication than the simple multiple signature solution). We propose and analyze four CES constructions which are provably secure with respect to known cryptographic assumptions and compare their performance characteristics.