Cryptology ePrint Archive: Report 2013/078

Broadcast Steganography

Nelly Fazio and Antonio R. Nicolosi and Irippuge Milinda Perera

Abstract: We initiate the study of broadcast steganography (BS), an extension of steganography to the multi-recipient setting. BS enables a sender to communicate covertly with a dynamically designated set of receivers, so that the recipients recover the original content, while unauthorized users and outsiders remain \emph{unaware} of the covert communication. One of our main technical contributions is the introduction of a new variant of anonymous broadcast steganography that we term \emph {anonymous identity-based encryption with pseudorandom ciphertexts} (oABE$). Our oABE$ construction achieves sublinear ciphertext size and is secure in the standard model. Besides being of interest in its own right, oABE$ enables an efficient construction of BS secure in the standard model against adaptive adversaries that also features sublinear ciphertexts.

Category / Keywords: public-key cryptography / Steganography, Broadcast Encryption, Receiver Anonymity, Broadcast Steganography

Date: received 16 Feb 2013

Contact author: iperera at gc cuny edu