© 2013 FIZ Karlsruhe

io-port 06059181

Libert, Benoît; Paterson, Kenneth G.; Quaglia, Elizabeth A.

Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model.

Fischlin, Marc (ed.) et al., Public key cryptography – PKC 2012. 15th international conference on practice and theory in public key cryptography, Darmstadt, Germany, May 21–23, 2012. Proceedings. Berlin: Springer (ISBN 978-3-642-30056-1/pbk). Lecture Notes in Computer Science 7293, 206-224 (2012).

Summary: In this paper we consider anonymity in the context of broadcast encryption (BE). This issue has received very little attention so far and all but one of the currently available BE schemes fail to provide anonymity. Yet, we argue that it is intrinsically desirable to provide anonymity in standard applications of BE and that it can be achieved at a moderate cost. We provide a security definition for anonymous broadcast encryption (ANOBE) and show that it is achievable assuming only the existence of IND-CCA secure public key encryption (PKE). Focusing on reducing the size of ciphertexts, we then give two generic constructions for ANOBE. The first is from any anonymous (key-private) IND-CCA secure PKE scheme, and the second is from any IBE scheme that satisfies a weak security notion in the multi-TA setting. Furthermore, we show how randomness re-use techniques can be deployed in the ANOBE context to reduce computational and communication costs, and how a new cryptographic primitive – anonymous hint systems – can be used to speed up the decryption process in our ANOBE constructions. All of our results are in the standard model, achieving fully collusion-resistant ANOBE schemes secure against adaptive IND-CCA adversaries.

Keywords: broadcast encryption; anonymity
doi:10.1007/978-3-642-30057-8_13