Cryptology ePrint Archive: Report 2011/092

Characterization of the relations between information-theoretic non-malleability, secrecy, and authenticity

Akinori Kawachi and Christopher Portmann and Keisuke Tanaka

Abstract: Roughly speaking, an encryption scheme is said to be non-malleable, if no adversary can modify a ciphertext so that the resulting message is meaningfully related to the original message. We compare this notion of security to secrecy and authenticity, and provide a complete characterization of their relative strengths. In particular, we show that information-theoretic perfect non-malleability is equivalent to perfect secrecy of two different messages. This implies that for n-bit messages a shared secret key of length roughly $2n$ is necessary to achieve non-malleability, which meets the previously known upper bound. We define approximate non-malleability by relaxing the security conditions and only requiring non-malleability to hold with high probability (over the choice of secret key), and show that any authentication scheme implies approximate non-malleability. Since authentication is possible with a shared secret key of length roughly $\log n$, the same applies to approximate non-malleability.

Category / Keywords: secret-key cryptography / Information-theoretic security, non-malleability, relations among notions of security

Publication Info: In proceedings of ICITS 2011

Date: received 23 Feb 2011

Contact author: chportma at gmail com

Note: This is the full version of our ICITS 2011 paper. Section 6, Appendix A, and Appendix B do not appear in the published version.

Version: 20110228:223640 (All versions of this report)