Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography

Submitted by aekwall on Thu, 04/08/2021 - 4:39pm

Title	Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography
Publication Type	Journal Article
Year of Publication	2018
Authors	Iwamoto, M., Ohta, K., Shikata, J.
Journal	IEEE Transactions on Information Theory
Volume	64
Pagination	654?685
ISSN	1557-9654
Keywords	composable security, cryptographic protocols, Encryption, Entropy, Human Behavior, indistinguishability, information theoretic security, Information-Theoretic Cryptography, information-theoretic indistinguishability, information-theoretic security, key agreement, Metrics, perfect secrecy, policy-based governance, private key cryptography, probability, Protocols, pubcrawl, relaxed perfect secrecy, Resiliency, Scalability, secret keys, security formalizations, security quantities, semantic security, Semantics, Shannon's perfect secrecy, symmetric-key encryption, telecommunication security, unconditional security

Abstract

This paper analyzes the formalizations of information-theoretic security for the fundamental primitives in cryptography: symmetric-key encryption and key agreement. Revisiting the previous results, we can formalize information-theoretic security using different methods, by extending Shannon's perfect secrecy, by information-theoretic analogues of indistinguishability and semantic security, and by the frameworks for composability of protocols. We show the relationships among the security formalizations and obtain the following results. First, in the case of encryption, there are significant gaps among the formalizations, and a certain type of relaxed perfect secrecy or a variant of information-theoretic indistinguishability is the strongest notion. Second, in the case of key agreement, there are significant gaps among the formalizations, and a certain type of relaxed perfect secrecy is the strongest notion. In particular, in both encryption and key agreement, the formalization of composable security is not stronger than any other formalizations. Furthermore, as an application of the relationships in encryption and key agreement, we simultaneously derive a family of lower bounds on the size of secret keys and security quantities required under the above formalizations, which also implies the importance and usefulness of the relationships.

DOI 10.1109/TIT.2017.2744650

Citation Key iwamoto_security_2018

Scalability encryption private key cryptography secret keys telecommunication security Cryptographic Protocols Protocols Resiliency Human behavior pubcrawl policy-based governance Metrics Entropy information-theoretic security key agreement probability Semantics Indistinguishability semantic security composable security Information-Theoretic Cryptography information-theoretic indistinguishability perfect secrecy relaxed perfect secrecy security formalizations security quantities Shannon's perfect secrecy symmetric-key encryption unconditional security information theoretic security