Universal Hashing for Information-Theoretic Security

Title	Universal Hashing for Information-Theoretic Security
Publication Type	Journal Article
Year of Publication	2015
Authors	Tyagi, H., Vardy, A.
Journal	Proceedings of the IEEE
Volume	103
Pagination	1781?1795
Date Published	oct
ISSN	1558-2256
Keywords	2-universal hash family, Communication channels, Communication system security, cryptography, encoding, Human Behavior, information coding, information theoretic security, Information theory, information-theoretic security, Metrics, modular coding schemes, Noise measurement, Physical layer, policy-based governance, private key cryptography, pubcrawl, Random variables, Receivers, Resiliency, Scalability, secret key agreement, security, telecommunication services, wiretap codes, wiretap coding
Abstract	The information-theoretic approach to security entails harnessing the correlated randomness available in nature to establish security. It uses tools from information theory and coding and yields provable security, even against an adversary with unbounded computational power. However, the feasibility of this approach in practice depends on the development of efficiently implementable schemes. In this paper, we review a special class of practical schemes for information-theoretic security that are based on 2-universal hash families. Specific cases of secret key agreement and wiretap coding are considered, and general themes are identified. The scheme presented for wiretap coding is modular and can be implemented easily by including an extra preprocessing layer over the existing transmission codes.
DOI	10.1109/JPROC.2015.2462774
Citation Key	tyagi_universal_2015

Scalability private key cryptography Receivers security Resiliency Human behavior pubcrawl policy-based governance Communication system security Cryptography Metrics information theory information-theoretic security Physical layer Noise measurement encoding Communication channels information theoretic security secret key agreement Random variables telecommunication services 2-universal hash family information coding modular coding schemes wiretap codes wiretap coding