1. Record Nr. UNINA9910743388903321

Autore	Ali Ikram
Titolo	Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks / / by Ikram Ali, Yong Chen, Mohammad Faisal, Meng Li
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2022
ISBN	981-16-8585-1 981-16-8586-X
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (237 pages)
Collana	Engineering Series
Disciplina	629.272
Soggetti	Wireless communication systems Mobile communication systems Computer networks - Security measures Cryptography Data encryption (Computer science) Automotive engineering Wireless and Mobile Communication Mobile and Network Security Cryptology Automotive Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Introduction -- Preliminaries -- IDC-Based Authentication Scheme using Bilinear Pairings for V2I Communications -- IDC-Based Authentication Scheme using ECC for V2V Communications -- CLC-Based Authentication Scheme using Bilinear Pairings for V2I Communications -- CLC-Based Authentication Scheme using ECC for V2V Communications -- IDC to PKI-Based Hybrid Signcryption Scheme using Bilinear Pairings for Heterogeneous V2I Communications.
Sommario/riassunto	This book focuses on the design of secure and efficient signature and signcryption schemes for vehicular ad-hoc networks (VANETs). We use methods such as public key cryptography (PKI), identity-based cryptography (IDC), and certificateless cryptography (CLC) to design bilinear pairing and elliptic curve cryptography-based signature and

signcryption schemes and prove their security in the random oracle model. The signature schemes ensure the authenticity of source and integrity of a safety message. While signcryption schemes ensure authentication and confidentiality of the safety message in a single logical step. To provide readers to study the schemes that securely and efficiently process a message and multiple messages in vehicle to vehicle and vehicle to infrastructure communications is the main benefit of this book. In addition, it can benefit researchers, engineers, and graduate students in the fields of security and privacy of VANETs, Internet of vehicles securty, wireless body area networks security, etc.