Quantum Key Distribution Networks

Miralem Mehic • Stefan Rass •
Peppino Fazio • Miroslav Voznak

Quantum Key Distribution Networks

A Quality of Service Perspective

Springer

Miralem Mehic
Department of Telecommunications,
Faculty of Electrical Engineering
University of Sarajevo
Sarajevo, Bosnia and Herzegovina

Stefan Rass
Secure Systems Group, LIT Secure and
Correct Systems Lab
Johannes Kepler University
Linz, Austria

Peppino Fazio
Department of Telecommunications
VSB-Technical University of Ostrava
Ostrava, Czech Republic

Miroslav Voznak
Department of Telecommunications
VSB-Technical University of Ostrava
Ostrava, Czech Republic

ISBN 978-3-031-06607-8 ISBN 978-3-031-06608-5 (eBook)
https://doi.org/10.1007/978-3-031-06608-5

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Miralem: to Lejla and my family
Stefan: dedicated to my loving family
Peppino: to my lovely family, mom, dad, and Francesco
Miroslav: to my beloved family

Acknowledgments

The research leading to the published results was supported by the Ministry of the Interior of the Czech Republic under grant ID VJ01010008 within the project Network Cybersecurity in Post-Quantum Era.

We would like to thank Oliver Maurhart, Marcin Niemiec, and Emir Dervisevic for helpful discussions and comments on the manuscript.

Contents

Acronyms

5G	The fifth generation of cellular networks
AAU	Active Antenna Unit
AES	Advanced Encryption Standard
AIT	Austrian Institute of Technology
API	Application Programmers Interface
ASMT	Arbitrarily Secure Message Transmission
ATM	Asynchronous Transfer Mode
BBN	Bolt Beranek and Newman
BBU	Base Band Unit
BF	Bellman-Ford
BGP	Border Gateway Protocol
CAC	Call Admission Control
CC	Common Criteria
CIA	Confidentiality-Integrity-Availability
CLI	Command Line Interface
CO	Central Office
CV-QKD	Continuous-Variable QKD
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial-of-Service
DH	Diffie-Hellman key agreement primitive
DHE	Ephemeral Diffie-Hellman (DHE)
DiffServ	Differentiated Services
DIQKD	Device-Independent Quantum Key Distribution
DoS	Denial-of-Service
DSCP	Differentiated Services Code Point
DSDV	Destination-Sequenced Distance-Vector
DU	Digital Unit
DV	Distance Vector
DV-QKD	Discrete Variables QKD
E2E	End-to-End
ECN	Explicit Congestion Notification

eCPRI	Enhanced Common Public Radio Interface
ERO	Explicit Route Object
ESP	Encapsulating Security Payload
FEC	Forwarding Equivalence Class
Fi-Wi	Fiber/Wireless
FQKD	Flexible QoS model for QKD Networks
FR	Frame Relay
GMPLS	Generalized Multi-Protocol Label Switching
GPL	GNU Public License
GPSR	Greedy Perimeter Stateless Routing in Wireless Networks
GPSRQ	Greedy Perimeter Stateless Routing Protocol for QKD Networks
GUI	Graphical User Interface
HARQ	Hybrid Automatic Retransmit reQuest
HMAC	Hash Message Authentication Code
HOM	Hong-Ou-Mandel
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IntServ	Integrated Services
IoT	Internet of Things
IPComp	IP payload compression protocol
IPsec	Internet Protocol security
ISAKMP	Internet Security Association and Key Management Protocol
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
ITS	Information-Thoeretic Security
IV	Initialization Vector
KMS	Key Manager System
KSID	Key_Stream_ID
LDPC	Low Density Parity Check
LER	Label Edge Routers
LKMS	Local Key Manager System
LP	Linear Program
LS	Link-State
LSA	Link-State Advertisement
LSP	Label Switch Path
LSU	Link-State Update
MAC	Message Authentication Code
MACsec	Media Access Control security
MANET	Mobile Ad Hoc Network
MANO	Management and Orchestration
MDI-QKD	Measurement Device Independent Quantum Key Distribution
MGSS	Multi-Goal Security Strategy
MPLS	Multi-Protocol Label Switching
MPT	Multipath Transmission
MSS	Maximum Segment Size

MTU	Maximum Transmission Unit
NAT	Network Address Translation
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
NR	New Radio
NVD	National Vulnerability Database
OLA	Operational Level Agreement
OS	Operating System
OSPF	Open Shortest Path First
OTP	One-Time Pad
P2MP	Point-to-MultiPoint
P2P	Point-to-Point
PCE	Path Computation Element
PCEP	Path Computation Element Protocol
PER	Provider Edge Router
PFS	Perfect Forward Secrecy
PITM	Person-in-the-Middle
PKI	Public Key Infrastructure
PON	Passive Optical Network
PPP	Point-to-Point Protocol
PSMT	Perfectly Secure Message Transmission
Q3P	Quantum Point-to-Point Protocol
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDNetSim	QKD Network Simulator
QKRA	Quantum Key Reservation Approach
QoS	Quality of Service
QPFS	Quantum Perfect Forward Secrecy
QRNG	Quantum Random Number Generator
QSIP	QKD Signaling Protocol
QUANTUM5	Quantum Cybersecurity in 5G Networks
RAN	Radio Access Network
RAT	Radio Access Technology
REST	REpresentational State Transfer
RIP	Routing Information Protocol
RRH	Remote Radio Head
RRU	Remote Radio Unit
RSVP	Resource Reservation Protocol
RTT	Round-Trip Time
RU	Radio Unit
SAD	Security Association Database
SAE	Secure Application Entity
SDN	Software Defined Networking
SECOQC	Secure Communication based on Quantum Cryptography
SeQKEIP	Secure Quantum Key Exchange Internet Protocol

SIP	Session Initiation Protocol
SKEYID	Session Key ID
SLA	Service Level Agreement
SPAD	Single-Photon Avalanche Diodes
SPD	Security Policy Database
SPD	Single-Photon Detector
SPI	Security Parameter Index
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time to Live
TVA	Topological Vulnerability Analysis
UDP	User Datagram Protocol
UE	User Equipment
URI	Uniform Resource Identifier
VANET	Vehicular Ad Hoc Network
vCPE	Virtual Customer Premise Equipment
vEPC	Virtual Evolved Packet Core
VoIP	Voice over IP
VPN	Virtual Private Network
vRAN	Virtual Radio Access Network
VSB	Technical University of Ostrava
WDM	Wavelength Division Multiplexing

List of Symbols

$\{0,1\}^n$	Set of bitstrings of length n
$\{0,1\}^*$	Set of bitstrings of any length ($= \bigcup_{n\in\mathbb{N}}\{0,1\}^n$)
$\|m\|$	Length of bitstring $m \in \{0,1\}^*$
$\oplus$	Bitwise XOR between two strings
π	Path, represented as ordered subset $\pi \subseteq E$ of edges in a graph $G = (V, E)$
$V(\pi)$	Nodes along a path π
$\|\pi\|$	Length of a path π as number of edges (hops)
$\mathscr{A}$	Adversary structure; a family (set) of sets
$\mathscr{P}(X)$	Power-set of the set X
$\mathbb{Z}_p$	Finite field of prime order p, with modulo arithmetic