

ISO/IEC 29192-7:2019 (E)

Information security — Lightweight cryptography — Part 7: Broadcast authentication protocols

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Symbols and abbreviated terms
5	TESLA-RD (Timed Efficient Stream Loss-tolerant Authentication — Rapid Disclosure)
5.1	General
5.2	Initialization
5.3	Setup
5.4	Sending a message
5.5	Receiving a message
5.6	Verifying the key
5.7	Verifying the message
Annex A	(normative) Object identifiers

Page count: 7