

ISO/IEC 29192-5:2016-08 (E)

Information technology - Security techniques - Lightweight cryptography - Part 5: Hash-functions

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols	3
5	Lightweight hash-functions optimized for hardware implementations	3
5.1	General	3
5.2	PHOTON	3
5.2.1	General	3
5.2.2	PHOTON specific notation	4
5.2.3	Domain extension algorithm	4
5.2.4	Internal permutation	5
5.3	SPONGENT	10
5.3.1	General	10
5.3.2	SPONGENT specific notation	10
5.3.3	Domain extension algorithm	10
5.3.4	Internal permutation	11
6	Lightweight hash-functions optimized for software implementations	12
6.1	General	12
6.2	Lesamnta-LW	13
6.2.1	General	13
6.2.2	Message padding	13
6.2.3	Lesamnta-LW specific notation	13
6.2.4	Compression function and domain extension	13
6.2.5	Block cipher	14
Annex A (normative)	Object identifiers	17
Annex B (informative)	Numerical examples	19
Annex C (informative)	Feature tables	23
Bibliography		26