

ISO/IEC 20897-1:2020 (E)

Information security, cybersecurity and privacy protection — Physically unclonable functions — Part 1: Security requirements

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Abbreviated terms
5	Security requirements for PUFs
5.1	General
5.2	PUF interface
5.3	PUF building blocks
5.4	Use cases of PUF
5.4.1	Security parameter generation
5.4.2	Device identification
5.4.3	Device authentication
5.5	Security requirements
5.5.1	General
5.5.2	Steadiness
5.5.3	Randomness
5.5.4	Uniqueness
5.5.5	Tamper-resistance
5.5.6	Mathematical unclonability
5.5.7	Physical unclonability
5.6	Mapping between security requirements and use cases
Annex A	(informative) Classification of PUF
A.1	General
A.2	Confined vs extensive
A.3	Silicon vs non-silicon PUFs
A.4	Delay vs non-delay
Annex B	(informative) Some PUF implementations
B.1	General
B.2	Silicon PUF implementations
B.2.1	Arbiter PUF
B.2.2	SRAM PUF
B.2.3	Loop PUF
B.2.4	Glitch PUF
B.2.5	Clock PUF
B.2.6	MEMS PUF
B.2.7	PL-PUF
B.2.8	ReRAM PUF
B.3	Non-silicon PUF implementations
B.3.1	Coating PUF
B.3.2	Optical PUF
Annex C	(informative) PUF life-cycle