INTERNATIONAL STANDARD

ISO/IEC 29192-1

First edition
2012-06-01

Information technology — Security techniques — Lightweight cryptography —

Part 1: General

Technologies de l'information — Techniques de sécurité — Cryptographie pour environnements contraints — Partie 1: Généralités

Reference number
ISO/IEC 29192-1:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Terms and definitions 1

3 Categories of constraints for lightweight cryptography 2
3.1 Chip area 2
3.2 Energy consumption 2
3.3 Program code size and RAM size 2
3.4 Communication bandwidth 2
3.5 Execution time 3

4 Requirements 3
4.1 Security requirements 3
4.2 Classification requirements 3
4.3 Implementation requirements 4

5 Lightweight cryptographic mechanisms 5
5.1 Block ciphers 5
5.2 Stream ciphers 6
5.3 Mechanisms using asymmetric techniques 6

Annex A (informative) **Selection criteria for inclusion of mechanisms in ISO/IEC 29192** 7

Annex B (informative) **Obtaining metrics for hardware implementation comparison** 8

Annex C (normative) **Metrics for hardware targeted block and stream ciphers** 11

Annex D (informative) **Gate equivalents** 12

Bibliography 13

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29192-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 29192 consists of the following parts, under the general title *Information technology — Security techniques — Lightweight cryptography*:

— *Part 1: General*

— *Part 2: Block ciphers*

— *Part 3: Stream ciphers*

— *Part 4: Mechanisms using asymmetric techniques*

Further parts may follow.

Introduction

ISO/IEC 29192 is a multi-part International Standard that specifies lightweight cryptography for the purposes of data confidentiality, authentication, identification, non-repudiation, and key exchange. Lightweight cryptography is suitable in particular for constrained environments. The constraints normally encountered can be any of the following:

— chip area;

— energy consumption;

— program code size and RAM size;

— communication bandwidth;

— execution time.

The purpose of ISO/IEC 29192 is to specify standardized mechanisms which are suitable for lightweight cryptographic applications, including radiofrequency identification (RFID) tags, smart cards (e.g. contactless applications), secure batteries, health-care systems (e.g. Body Area Networks), sensor networks, etc.

This part of ISO/IEC 29192 sets the security requirements, classification requirements and implementation requirements of mechanisms that are proposed for inclusion in subsequent parts of ISO/IEC 29192.

Lightweight cryptography delivers adequate security in the context for which it is intended. The cryptographic mechanisms standardized in ISO/IEC 29192 provide their full security strength if they are used within the limitations of the mechanisms as specified.

EXAMPLE For a block cipher with a block size of n bits and a key size of k bits, when limiting the use of the block cipher to encrypting no more than 2n/2 blocks of plaintext under a single key in say counter mode, it will provide k-bit security. The security degrades with more than 2n/2 blocks.

There are overlaps in some security techniques between ISO/IEC 29192 and existing standards such as ISO/IEC 18033, ISO/IEC 9798, and ISO/IEC 11770. The exclusion of particular mechanisms does not imply that these mechanisms are not suitable for lightweight cryptography. The criteria used to select the cryptographic mechanisms specified in subsequent parts of ISO/IEC 29192 are described in Annex A.

Information technology — Security techniques — Lightweight cryptography —

Part 1: General

1 Scope

This part of ISO/IEC 29192 provides terms and definitions that apply in subsequent parts of ISO/IEC 29192. This part of ISO/IEC 29192 sets the security requirements, classification requirements and implementation requirements for mechanisms that are proposed for inclusion in subsequent parts of ISO/IEC 29192.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
chip area
area occupied by a semiconductor circuit

2.2
communication bandwidth
number of bits per second that can be transmitted over a specified communication channel

2.3
energy consumption
power consumption over a certain time period

NOTE In ISO/IEC 29192, energy consumption during the cryptographic process is evaluated. In some constrained devices the total energy required to perform the cryptographic operation is important, for instance, in RFID and sensors.

2.4
gate equivalent
unit of measure which allows for the specification of the complexity of digital electronic circuits, commonly the silicon area of a two-input drive-strength-one NAND gate

2.5
latency
delay introduced by the cryptographic mechanism in real-time communication systems

2.6
lightweight cryptography
cryptography tailored for implementation in constrained environments

NOTE The constraints can be aspects such as chip area, energy consumption, memory size, or communication bandwidth.

2.7
program code size
size of a cryptographic mechanism code in bytes

2.8
RAM size
size of temporary storage space a cryptographic mechanism requires in random access memory including the registers in the processor

2.9
security strength
number associated with the amount of work (i.e. the number of operations) that is required to break a cryptographic algorithm or system

NOTE 1 A security strength of n implies that the required workload of breaking the cryptosystem is equivalent to 2n executions of the cryptosystem.

NOTE 2 In ISO/IEC 29192, security strength is specified in bits, e.g. 80, 112, 128, 192, and 256.

2.10
short input performance
performance of the cryptographic primitive when processing short messages

2.11
side-channel attack
attack based on information gained from the physical implementation of a cryptosystem, rather than on brute force or theoretical weaknesses in the underlying algorithms

EXAMPLE Timing information, power consumption, or electromagnetic emissions can provide extra sources of information and can be exploited to attack the system.

3 Categories of constraints for lightweight cryptography

3.1 Chip area

Where cryptographic mechanisms are implemented in hardware, the actual chip area that the cryptographic mechanism requires may be constrained in some applications (e.g. RFID tags). For the purposes of this international standard, the chip area will be measured in gate equivalents.

3.2 Energy consumption

Energy consumption can be constrained in lightweight cryptography applications. Energy consumption is related to several factors including the processing time, the chip area (when implemented in hardware), the operating frequency and the number of bits transmitted between entities (in wireless transmissions, in particular). To minimize energy consumption, all of the related factors should be considered.

3.3 Program code size and RAM size

Program code size (loosely referred to as ROM) and RAM size can be constrained on what are loosely referred to as low end processors. These processors have simple instruction sets and limited space available for the program code, as well as limited available space in RAM for computations (e.g. embedded processors) when compared to general purpose computer processors.

3.4 Communication bandwidth

Communication bandwidth is limited in certain cases with respect to the maximum number of bits that can be transmitted during a session (e.g. RFID tags). Mechanisms that fall into this category are therefore tailored to

be more economical with regard to the number of bits that need to be transmitted over the communications channel when compared to other more generally used cryptographic mechanisms.

3.5 Execution time

For some applications such as contactless cards and RFID, for correct operation the execution time is constrained by the implementation (e.g. how long the card/token is present in the field). Note that this constraint typically occurs in applications where the constraints treated in previous subsections also apply.

4 Requirements

4.1 Security requirements

In ISO/IEC 29192, the security strength of a cryptographic mechanism is measured as defined in 2.9. This notion can be used for different cryptographic mechanisms. Two mechanisms are considered to be of comparable strength if the amount of work needed to break the mechanisms or determine the keys is approximately the same using a given resource.

In ISO/IEC 29192, 80-bit security is considered to be the minimum security strength for lightweight cryptography.

Resistance against side-channel attacks may be important in some applications of lightweight cryptography. Countermeasures against side-channel analysis often require additional chip area (for hardware targeted algorithms) or additional program code (for software targeted algorithms). The countermeasures vary depending on the technology, and the specific side-channel method applicable to a specific implementation. Side-channel resistance is therefore outside the scope of this international standard.

NOTE Many organisations recommend using cryptographic mechanisms with more than 80-bit security after 2010. However, there are some lightweight cryptographic applications that may allow lower security requirements, i.e. do not have to assume all powerful adversaries. In cases where 80-bit keys are used, this implies that less data can be encrypted safely with a single key before rekeying is required. It is therefore important that designers of cryptographic security systems make sure that the safe operation limitations of lightweight cryptographic mechanisms are not exceeded for a single key. The ECRYPT2 yearly report 2009-2010 [6] recommends 80-bit security for very short-term protection against intelligence agencies with a budget of $300M or for long-term protection against small organizations with budget of $10k. For more references and information regarding key length selection, see Standing Document 12 of ISO/IEC JTC 1/SC 27 at http://www.jtc1sc27.din.de/sbe/SD12.

4.2 Classification requirements

For a cryptographic mechanism to be classified as lightweight, it shall (by definition of ISO/IEC 29192) be tailored for a combination of the categories defined in Clause 3. For each category a lightweight cryptographic mechanism is tailored to, indication of the category of tailoring shall be made and evidence shall be provided that the lightweight cryptographic mechanism is suitable for the claimed category (e.g. the chip area, the energy consumption etc.). Note that a cryptographic mechanism tailored only for execution time is not always considered to be lightweight.

All evidence of suitability for a particular category shall be based on theoretical evidence, which may be further substantiated by actual implementation evidence. All claims of actual implementation evidence shall be fully documented so as to be verifiable.

EXAMPLE Mechanism A claims to be tailored to be suitable for low energy for communication systems. This claim can be substantiated theoretically by comparing the number of bits transmitted resulting from the use of mechanism A, compared to other mechanisms commonly in use that are not considered to be lightweight mechanisms. The claim can be further substantiated by referencing practical implementations in which the energy consumption is experimentally measured, and comparing it to other practical implementations in which similar measurements are made.

4.3 Implementation requirements

4.3.1 Hardware implementation requirements

Both of the following are important physical characteristics of lightweight cryptography in hardware implementations:

— Chip area

— Energy consumption

For the purpose of ISO/IEC 29192 the chip area is measured in gate equivalents (GE). This enables a standardized comparison between cryptographic mechanisms intended for hardware implementation. There are no concrete figures for a suitable target size for an implementation because this depends on the economic realities of the application, the cryptographic mechanism under consideration and its deployment. In some lightweight cryptographic applications, countermeasures against side-channel attacks are necessary which require additional overheads. All cryptographic algorithms intended for hardware implementation published in ISO/IEC 29192 include its expected size in GEs.

Comparing energy consumption between cryptographic mechanisms is difficult because it depends on the particular technology in which the cryptographic mechanism is implemented. Some cryptographic mechanisms can be implemented in hardware with low energy consumption but large chip area, however in ISO/IEC 29192 energy consumption is evaluated by using a hardware implementation with reasonably small chip area.

Real energy consumption measured experimentally, though technology and implementation dependent, is still a useful practical figure for readers of ISO/IEC 29192, and is provided where available. When experimental measurements are provided, the experimental measurement methodology used is properly documented, as well as details regarding the technology on which the cryptographic mechanism was implemented.

In particular, all block ciphers and stream ciphers targeted for implementation in hardware provides the following summary of information to assist users of ISO/IEC 29192 to choose the most appropriate mechanism for their application (the details of which can be obtained in Annex B for background information and Annex C for the detailed requirements):

a) Chip area

b) Cycles

c) Bits per cycle

d) Power

e) Energy

f) Energy per bit

g) Technology: the specific library and version number that was used to obtain these figures

4.3.2 Software implementation requirements

In some lightweight cryptography applications software implementations are preferred over hardware implementations. The following aspects can be critical in software implementations in constrained environments:

— Program code size

— RAM size

ISO/IEC 29192 does not set an absolute target size for software implementation requirements, because it depends on many aspects e.g. processor architecture, processor instruction set, available memory, optimisation techniques, speed/memory trade-offs, etc. Software targeted lightweight cryptographic mechanisms are compared by code size and required RAM size on the same technology to algorithms included in ISO/IEC 18033 (e.g. AES), ISO/IEC 9798 and ISO/IEC 11770. If the required code size and RAM size is considerably less, such mechanisms is considered for inclusion in ISO/IEC 29192. Preference will be given to lightweight cryptography mechanisms that is lightweight on a larger number of different processors, i.e. can be considered lightweight because the required instruction set to classify it as lightweight is less dependent on specific instruction sets found only on specific technologies.

In particular, all block and stream ciphers targeted for implementation in software provides the following summary of information to assist users of ISO/IEC 29192 to choose the most appropriate mechanism for their application:

a) Program code size

b) RAM size

c) Speed

4.3.3 Other preferable properties

4.3.3.1 Short input performance

In some lightweight cryptographic applications short messages / plaintexts / ciphertexts are processed by the cryptographic mechanism. When lots of short messages / plaintexts / ciphertexts are processed independently, the short input performance becomes an important factor to consider, and is applicable to all categories of lightweight cryptography. It is even possible that a lightweight cryptographic primitive is tailored to have a good short input performance and if it is the case, this fact is indicated by the mechanism.

Factors that affect short-input-performance are the ratio of the processing size (number of key bits, block size of the cipher, or block size of a hash compression function input) compared to the message size, as well as initial setup time per processing of each single message.

4.3.3.2 Latency

In some communication systems (e.g. sensor networks) latency introduced by a cryptographic mechanism is an important factor. Latency introduced by the mechanism is influenced by the technology used to implement the mechanism, and optimisation of the implementation.

EXAMPLE When encrypting real-time speech packets over a telephone link, the cryptographic algorithm processing time introduces latency. If the latency becomes too much (at the cost of a lightweight mechanism e.g. a serialised implementation with small code size), the telephone users will experience an uncomfortable delay in two way conversation.

5 Lightweight cryptographic mechanisms

5.1 Block ciphers

The primary purpose of block ciphers is to protect the confidentiality of stored or transmitted data. The definition of a block cipher is given in ISO/IEC 18033-1. The block ciphers included in ISO/IEC 18033-3 are selected based on the selection criteria in Annex A of ISO/IEC 18033-1:2005. On the other hand, the block ciphers included in ISO/IEC 29192-2 are evaluated based on the selection criteria described in Annex A in this part of ISO/IEC 29192 considering suitability for constrained environments.

Block ciphers can be used to ensure integrity and origin of data. It is possible to construct a lightweight message authentication code (MAC) from the block cipher included in ISO/IEC 29192-2 using the MAC