INTERNATIONAL STANDARD

ISO/IEC 29192-1

Information technology — Security techniques — Lightweight cryptography —

Part 1:
General

Technologies de l'information — Techniques de sécurité — Cryptographie pour environnements contraints —

Partie 1: Généralités

Contents

Page

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.

1

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

algorithm specified in ISO/IEC 9797-1. It is also possible to construct a lightweight hash function from the block cipher included in ISO/IEC 29192-2 using the hash function construction specified in ISO/IEC 10118-2.

The security of most modes of operation for block ciphers (including MAC and hash constructions) degrades at $q^2/2^n$, where n is the block size in bits and q is the number of blocks encrypted. For example, when n=64, encryption of 2^{32} blocks is sufficient to expose the block cipher to attack. Therefore, care has to be taken since a shorter block size implies that less data can be encrypted using a single key. Users of ISO/IEC 29192 are encouraged to read Standing Document 12 of ISO/IEC JTC 1/SC 27 at http://www.jtc1sc27.din.de/sbe/SD12 for details on the relationship between block size and rekeying.

5.2   Stream ciphers

Stream ciphers are also used to protect the confidentiality of stored or transmitted data. The definition of a stream cipher is given in ISO/IEC 18033-1. The stream ciphers included in ISO/IEC 18033-4 are selected based on the selection criteria in Annex A of ISO/IEC 18033-1:2005. On the other hand, the stream ciphers included in ISO/IEC 29192-3 are evaluated based on the selection criteria described in Annex A in this part of ISO/IEC 29192 considering suitability for constrained environments.

5.3   Mechanisms using asymmetric techniques

Mechanisms using asymmetric techniques most notably have the advantage of avoiding the management of secret keys. Moreover, the mechanisms included in ISO/IEC 29192-4 fulfil the implementation requirements of 4.3. Three kinds of lightweight asymmetric schemes are referenced:

— Authentication and key exchange schemes with strong time limitations. These offer implementation advantages when compared to conventional asymmetric solutions.

— Identity-based signature schemes. These offer a signing stage with very light computational overhead (a trusted third party is involved) and allow the verification process to take place without interaction between the signer and the verifier, either directly or through a proxy.

— Challenge-response identification schemes. They provide a form of strong entity authentication. Solutions for asymmetric challenge-response identification schemes are provided by zero-knowledge identification schemes, which are described, for instance, in ISO/IEC 9798-5.

Annex A
(informative)

Selection criteria for inclusion of mechanisms in ISO/IEC 29192

The mechanisms included in subsequent parts of ISO/IEC 29192 have been selected according to the following criteria, where the order of presentation of the criteria is of no significance.

Evaluations are made with respect to the following aspects of the cryptographic mechanism.

a) The security of the cryptographic mechanism. 80-bit security is considered to be the minimum security strength for lightweight cryptography. It is however recommended that at least 112-bit security be applied for systems that will require security for longer periods (refer to SD12 for security strength references, as the period of protection provided is determined by the security strength as well as the computing power of the adversary who wishes to break the algorithm.).

b) The hardware implementation properties (for hardware targeted mechanisms). The chip area occupied by the cryptographic mechanism (reduced compared to existing ISO standards) and the energy consumption (clear advantage over existing ISO standards, e.g. ISO/IEC 18033, ISO/IEC 9798, ISO/IEC 11770).

c) The software implementation properties (for software targeted mechanisms). In particular, the code size and the required RAM size. (Less resource requirements compared to existing standards on the same platform are considered as potentially lightweight for software environments).

d) The nature of any licensing issues affecting the cryptographic mechanism.

e) The maturity of the cryptographic mechanism.

f) The generality of the lightweight properties claimed for the cryptographic mechanism (i.e. the more independent the claimed lightweight property is from implementation in a specific technology, the better, as it will be useable by a wider audience).

Annex B
(informative)

Obtaining metrics for hardware implementation comparison

B.1 Background

B.1.1 Active vs. passive devices

Active devices are battery-powered. Batteries, without re-charging can only store a limited amount of energy (in Joule or Wh) thus an important measure for this class of device is the energy consumption of a cryptographic mechanism.

Passive devices do not have their own power supply. The energy required for a passive device comes from a magnetic or electromagnetic field generated by the reading device [8]. The maximum strength of the field is typically limited by regulations specific to the location in which the device is used. The strength of the field at any point decreases as the distance between reading device and the passive device increases. The energy from the field is utilised by the device to power the chip. If the mean power consumption of the chip is larger than what can be provided from the energy storage, the passive device cannot operate properly. Thus the power consumption (in W) is an important measure for passive devices.

B.1.2 Power consumption

The following equation summarizes the power dissipation P in CMOS devices [7]:

$$P = (\frac{1}{2}CV_{dd}^2 + Q_{SC}V_{dd})fN + I_{leak}V_{dd} ,$$

where C denotes the circuit capacitance, V_{dd} the supply voltage, Q_{sc} the short-circuit charge, f the operating frequency, N the switching activity and I_{leak} the leakage current. The first summand represents the dynamic power consumption and the second the static power consumption. At higher operating frequencies the dynamic part becomes the dominant factor of the total power consumption.

The power consumption can be linearly decreased by lowering the operating frequency f, which also lowers the switching activity N, and quadratically by decreasing the supply voltage V_{dd}. The remaining terms of the dynamic part, C and Q_{sc}, are technology dependent and cannot be influenced by a hardware designer.

The static power consumption can be linearly decreased by applying a lower supply voltage V_{dd}, which is bounded by the technology used. Moreover, since the leakage current I_{leak} is directly proportional to the number of required GEs, decreasing the gate count directly decreases the power consumption of the circuit.

To lower power consumption independently of the algorithm and the architectural implementation strategy, lightweight applications are typically clocked at a low operating frequency, i.e. a few hundred KHz. In this frequency range the static power consumption is dominant and thus directly proportional to the gate count. Therefore the gate count, expressed in GE is used as a measure for both the chip area and the power consumption.

B.1.3 Architecture strategies

Cryptographic algorithms such as block ciphers, stream ciphers and hash functions transform an input to an output using a round function that is iterated several times. While software implementations have to process single operations in a serial manner, hardware implementations offer more flexibility for parallelisation and serialisation. Generally there exist three major architecture strategies for the implementation of cryptographic algorithms namely parallelised, round-based, and serialised.

A parallel, or loop unrolled, implementation of cryptographic algorithms performs several round operations of the hashing/encryption/decryption process within one clock cycle. Usually parallel implementations are pipelined, i.e. registers are inserted in the critical path so as to increase the maximum clock frequency. While parallel implementations have high throughput rates, this is rarely the focus for lightweight applications. Rather, the high chip area and power demands mean that parallel implementations of cryptographic algorithms are rarely suited for lightweight applications and thus are ignored within the scope of this annex.

In a round-wise implementation, one round function of a cryptographic algorithm is processed within one clock cycle. The decreased throughput comes at the benefit of decreased chip area and power consumption.

To lower power consumption and chip area requirements, implementations can be serialized; here only a fraction of one round is processed in a clock cycle. Up to a certain point this strategy can significantly decrease the chip area and the power consumption. However, it might not always be a suitable implementation strategy since the savings can sometimes be cancelled by the overheads for additional control logic. Nevertheless, from a low power and low chip area perspective, serial implementations appear to be best-suited for lightweight implementations. However, the energy consumption of serialized implementations is usually worse than round-based designs.

B.1.4 I/O overhead

The choice of an appropriate I/O interface is application specific, while at the same time it can have a significant influence on the chip area, power, and timing figures. Furthermore, most likely a cryptographic mechanism is part of a larger integrated circuit rather than a stand-alone solution. Therefore this standard ignores the I/O overhead, which allows for a fairer comparison of the properties of a mechanism rather than their implementation properties.

B.2 Common hardware measures

This clause gives an overview of commonly used measures for hardware assessment and discusses their benefits and drawbacks.

To assess the efficiency of hardware implementations the following measures can be used:

NOTE 1   For the purposes of this international standard, only the hardware measures listed in 4.3.1 are used due to the computations required by Annex C. The measures as computed in Annex C provide for a fair comparison of hardware implementations of cryptographic algorithms, and the hardware measures listed above are for information only.

Chip area: Chip area requirements are usually measured in μm^2, but this value depends on the fabrication technology and the standard cell library. In order to compare the chip area requirements independently it is common to state the chip area as gate equivalents (GEs). One GE is the chip area which is required by the two-input NAND gate with the lowest driving strength of the appropriate technology. The chip area in GE is derived by dividing the area in μm^2 by the area of a two-input NAND gate. This measure can easily be obtained by using an electronic design automation synthesis tool. It is commonly used and widely accepted as a fair measure for comparison of the chip area requirements.

Word size: Amount of bits processed in one run of the cryptographic algorithm. For block ciphers this is the block size, for stream ciphers it is the output size of one execution of the stream cipher and for hash functions it is the input block size.

NOTE 2   A stream cipher usually outputs the keystream bits a bit at a time, a byte at a time, or a number of bytes at a time with each execution updating the internal state. Hash functions process arbitrary length messages, but in an iterated fashion. The input block size and a single execution of the hash function refer to processing of one block of message bits at its input for one iteration.

Cycles: Number of clock cycles [CLK] for one execution of the algorithm to produce the output. This measure is dependent on the architectural implementation strategy and can be easily obtained by paper and pencil.

NOTE 3   For a hash function, one execution of the algorithm implies one iteration of the hash algorithm for one message block at its internal input.

Time: The required amount of time for a certain operation can be calculated by dividing the amount of cycles by the operating frequency t = CLK/freq.

Since different algorithms may process a different amount of bits at the same time, this measure is only important in time-critical applications and can lead to unfair comparison otherwise. Furthermore it is dependent on the operating frequency used, which is highly application specific.

Throughput: The rate at which new output is produced with respect to time. The number of output bits is divided by the time, i.e. by the number of cycles and multiplied by the operating frequency. It is expressed in bits per second [bps] and is a fair and widely accepted measure for comparison. However it is dependent on the operating frequency used.

Power: The power consumption is often estimated on the gate level by an electronic design automation tool. In lightweight scenarios it is usually provided in micro Watt [μW]. Note that power estimations on the transistor level are more accurate, but this would also require further design steps in the design flow, e.g. the place&route step. It is common knowledge that estimated power figures greatly depend on the technology used and on the accuracy level of the electronic design automation tool. Thus it is not easy to compare the power consumption and consequently it is not well suited for the needs of this standard.

Current: The power consumption divided by the typical core voltage of the library. Again this measure is strongly technology dependent.

Energy: The energy consumption denotes the power consumption over a certain time period. It can be calculated by multiplying the power consumption with the required time of the operation. For the efficiency of a cryptographic algorithm (especially for active devices) it is also interesting to know the energy consumption per output bit. The energy consumption is provided in micro Joule [μJ].

Energy per Bit: Similar to the time measure it may lead to an unfair comparison if only the whole energy consumption is compared without considering the amount of bits processed. Thus by dividing the energy consumption by the amount of bits processed one gets a fair measure that can be expressed in micro Joule per bit [μJ/bit].

Hardware efficiency: The throughput to chip area ratio (or its reciprocal counterpart the Area-Time product) is used as a measure for hardware efficiency. The hardware efficiency is calculated by dividing the chip area requirements by the throughput, i.e. eff = chip area/throughput, and is expressed in gate equivalents per bits per second [GE/bps]. This measure is also dependent on the operating frequency used. For further measures and their discussion in the context of cryptographic algorithms, refer to [9].

Annex C
(normative)

Metrics for hardware targeted block and stream ciphers

C.1 Assumptions

The following assumptions are made for cryptographic mechanisms in lightweight hardware applications:

a) Constrained with regard to chip area, power (in case of passive devices), and/or energy (in case of active devices),

b) Clocked at a low operating frequency of a few hundred kHz,

c) Cryptographic core is one part of a larger integrated circuit.

The first assumption leads to the exclusion of parallelised hardware implementations. Instead the focus is on serialised and round-based architectures. The second assumption makes the power consumption dominated by the static part, while the dynamic part can be neglected. This allows estimating the power consumption with the same measure as for the chip area, i.e. GE. Finally, the third assumption allows one to ignore the I/O overhead. This in turn allows one to focus on the properties of the cryptographic mechanism and not on the properties of an application specific implementation.

C.2 Compulsory hardware metrics

To assess the efficiency of lightweight hardware implementations the following measures shall be provided by all hardware targeted block and stream ciphers:

a) **Chip area:** in [GE], obtained by an electronic design automation tool. Used to compare both the chip area and the power.

b) **Cycles:** in [CLK] cycles, obtained by the architecture of the hardware implementation.

c) **Bits per cycle:** in [bits/CLK], obtained by dividing the word size by the clock cycles required to process one word. Contrary to the throughput, this measure is independent of the operating frequency used. To estimate the throughput a simple multiplication with the target operating frequency of the device is required.

d) **Power:** estimated in [GE] (see Chip area).

e) **Energy:** estimated in [GE·CLK], obtained by multiplying the *power* with the cycle count.

f) **Energy per bit:** estimated in [(GE·CLK)/bits], obtained by dividing the *energy* by the word size or by dividing the *power* by the *bits per cycle*.

NOTE   All measures can be obtained easily and are as independent as possible from application specific features such as operating frequency, I/O, supply voltage etc.

Annex D
(informative)

Gate equivalents

Gate equivalents abbreviated GE is the most common measure used to express the chip area a circuit requires when implemented in ASIC devices. In order to get the gate equivalent for the different gates, one divides the area of the particular gate by the area of the two-input NAND gate in the appropriate technology.

The gate equivalents can only be accurately obtained by implementation and simulation with the specific libraries and technology the user of ISO/IEC 29192 wants to use. Users are therefore encouraged to implement and simulate different cryptographic mechanisms chosen from ISO/IEC 29192 to find the most optimal mechanism suitable for the particular choice of technology.

It is possible that any particular lightweight cryptographic mechanism standardized in ISO/IEC 29192 can be implemented with even less gate equivalents than claimed in this standard. For instance, an algorithm can be serialised to save on gate count at the cost of speed. Since there are many optimisations possible depending on the trade-offs of different applications, ISO/IEC 29192 cannot provide most optimised implementations GE count of each mechanism.

Bibliography

[1]   ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*

[2]   ISO/IEC 18033 (all parts), *Information technology — Security techniques — Encryption algorithms*

[3]   ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[4]   ISO/IEC 9798 (all parts), *Information technology — Security techniques — Entity authentication*

[5]   ISO/IEC 10118-2, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher*

[6]   *ECRYPT2 Yearly Report on Algorithms and Keysizes (2009-2010)*, D.SPA.13, March 2010

[7]   S. Devadas and S. Malik, *A survey of optimization techniques targeting low power VLSI circuit*, ACM/IEEE Conference on Design Automation, pages 242–247,1995

[8]   K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, John Wiley and Sons, 2003

[9]   T. Good and M. Benaissa, *New Stream Cipher Designs*, LNCS volume 4986, chapter ASIC Hardware Performance, pages 267–293, Springer-Verlag, 2008

ICS 35.040

Price based on 13 pages