ISO/IEC JTC 1/WG 7
Working Group on Sensor Networks

Document Number:	N054
Date:	2010-07-05
Replace:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison Statement from JTC 1/SC 27/WG 2 to JTC 1/WG 7 on the ISO/IEC 1st CD 29192-1
Document Source:	JTC 1/SC 27/WG 2
Document Status:	For consideration at the 2nd WG 7 meeting in US.
Action ID:	FYI
Due Date:	
No. of Pages:	20

ISO/IEC JTC 1/WG 7 Convenor:
Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)
ISO/IEC JTC 1/WG 7 Secretariat:
Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

Committee Draft **ISO/IEC 1st CD 29192-1**	Reference number: ISO/IEC JTC 1/SC 27 **N8753**
Date: **2010-06-22**	Supersedes document SC 27 N8199
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.	
ISO/IEC JTC 1/SC27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2010-09-23** Please submit your votes and comments via the online balloting application by the due date indicated.

ISO/IEC 1st CD 29192-1

Title: Information technology -- Security techniques – Lightweight cryptography – Part 1: General

Project: 1.27.82.01 (29192-1)

Explanatory Report

Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
Study Period on Low power encryption	18th SC 27 Plenary meeting, Apr. 2006, Resolution 31 (N5199).	20th JTC 1 Plenary, Nov. 2005, resolution 35 (N4891=JTC 1 N8010)	Call f. Contr. (N5245).
	33rd WG 2 meeting, Nov. 2006, resolutions 2, 5 (N5901).	JP[1] contr. (N5345)	Report (N5447) (N/A);
	34th WG 2 meeting, May 2007, resolutions 3, 12 & 31 (N5), May 2007; 19th Plenary meeting, May 2007, resolutions 1, 31 (N5939).		Extention by 6 months (WG2 resolution 31); Report (N5846); Call f. contr. (N5904).
Study Period on Light-weight cryptographic mechanisms ***(title changed)***	35th WG 2 meeting, Oct. 2007, resolutions 2, 23 (N6211).	JP[1] contr. (N6002); KR[1] contr. (N6115).	Report (N6199); Call f. contr. (N6201).
	36th WG 2 meeting, April 2008, resolutions 1, 12, 27 (N6793); 20th Plenary, Apr. 2008, resolutions 2, 20 (N6799).	SoContr. (N6480); JP[1] (N6597).	Extention by 6 months (WG 2 resolution 27); Report (N6709); Call f. contr. (N6715).
NWIP **1st WD**	37th WG 2 meeting, October 2008, resolutions 2, 3, 9 (NWIP), 15, 25 (N7303).	VISA contr. (N6860).	Termination of SP WG 2 resolution 25; Report (N7167); NWIP (N7276rev1); Text f. 1st WD (N7276).
NP 29192 **2nd WD 29192**	38th WG 2 meeting, May 2009 resolutions 1, 10 (N7718) & 21st Plenary, May 2009, resolution 2 (N7777).	SoCom. (N7413); JP[1] (N7526).	Report (N7716); Calls f. contr. (N7682, N7683); DoC (N7675); Text f. 2nd WD 29192 (N7688).
3rd WD 29192-1* * subject to JTC 1 endorsement on subdivision	39th WG 2 meeting, November 2009, resolutions 1, 2, 3, 8, 11 (subdivision) 12 (N8299).	SoCom (N7862).	Recommend on subdivisiion (N8202); Request / Conformation for / of endorsement/subdivision (N8313/N8888); DoC (N8200); Report (N8201); Text f. 3rd WD (N8199).
1st CD 29192-1	40th WG 2 meeting, April 2010, resolutions 1, 12 (N8789); SC 27 resolution 1 (N8916).	SoCom (N8519); JTC 1/WG 7 com. (N8483); DE[1] com. (N8558).	DoC (N8752); Text f. 1st CD (N8753).

1st CD Registration and Consideration

In accordance with resolution 12 (in SC 27 N8789) of the 40th SC 27/WG 2 meeting held in Melaka (Malaysia), 19th – 23rd April 2010, the attached document SC 27 N8753 has been registered with the ISO Central Secretariat (ITTF) as a 1st Committee Draft (CD) and is hereby circulated for a 3-month 1st CD LB closing by

2010-09-23

[1)] **MB** = Member body (the ISO 3166 two-letter country code, e.g. CN for China)

Secretariat, ISO/IEC JTC 1/SC27 -
DIN Deutsches Institut fuer Normung e.V., Burggrafenstr. 6, 10772 Berlin , Germany
Telephone: + 49 2601-2652; Facsimile: + 49 2601-1723; E-Mail: krystyna.passia@din.de, http://www.jtc1sc27.din.de/en

ISO/IEC JTC 1/SC 27 N 8753

Date: 2010-06-13

ISO/IEC CD 29192-1

ISO/IEC JTC 1/SC 27/WG 2

Secretariat: DIN

Information technology — Security techniques - Lightweight cryptography — Part 1: General

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

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (30) Committee
Document language: E

X:\TA3\TG3-3\NA043\NA043_Sekretariate\JTC1_SC27\03_Projekte\PROJECT_admin\29192-1_Light-weight_cryptography_Nov2009\03_01_1stCD_29192-1_20100622\N8753_1stCD_29192-1_20100622\SC27N8753_1stCD_29192-1_Lightwieght_cryptography Tatsuta 20100619.doc STD Version 2.1

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Categories of constraints for lightweight cryptography 2
4.1 Chip area 2
4.2 Energy consumption 2
4.3 Program code size and RAM size 2
4.4 Communication bandwidth 3

5 Requirements 3
5.1 Security requirements 3
5.2 Classification requirements 3
5.3 Implementation requirements 4
5.3.1 Hardware implementation requirements 4
5.3.2 Software implementation requirements 5
5.4 General requirements 5

6 Lightweight cryptographic mechanisms 5
6.1 Block ciphers 5
6.2 Stream ciphers 5
6.3 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
B.1 Background 8
B.1.1 Active vs. passive devices 8
B.1.2 Power consumption 8
B.1.3 Architecture strategies 8
B.1.4 I/O overhead 9
B.2 Common hardware measures 9

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

Bibliography 12

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, *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, and identification. 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, or

— Communication bandwidth.

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

Lightweight cryptography does not imply a weakening of security. All cryptographic mechanisms standardized in ISO/IEC 29192 therefore provide full security strength if they are used within the limitations of the mechanism as specified.

Information technology — Security techniques - Lightweight cryptography — Part 1: General

1 Scope

This part of ISO/IEC 29192 is general in nature, and provides definitions that apply in subsequent parts of ISO/IEC 29192. The requirements for lightweight cryptography are introduced, and which cryptographic mechanisms are suitable and required for lightweight cryptography are described. There are overlaps in some security techniques between ISO/IEC 29192 and existing standards such as ISO/IEC 18033. 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.

2 Normative references

There are no normative references for this part of ISO/IEC 29192.

3 Terms and definitions

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

3.1
chip area
area occupied by a semiconductor circuit

3.2
communication bandwidth
number of bits per second that can be transmitted over a specified communication channel

3.3
energy consumption
power consumption over a certain time period

NOTE In ISO/IEC 29192, energy consumption during the cryptographic process is evaluated.

3.4
gate equivalent
unit of measure which allows to specify manufacturing-technology-independent complexity of digital electronic circuits, commonly the silicon area of a two-input drive-strength-one NAND gate

NOTE 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.

3.5
lightweight cryptography
cryptography tailored to be implemented in constrained environments

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

3.6
power consumption
electrical power consumed by a circuit during operation

3.7
program code size
size of the program code in bytes

3.8
RAM size
size of temporary storage space a program requires in random access memory

3.9
security strength
number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system

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

3.10
short input performance
performance of the cryptographic primitive when processing short inputs

3.11
side-channel attack
attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the underlying algorithms

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

4 Categories of constraints for lightweight cryptography

4.1 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). For the purpose of this international standard, the chip area will be measured in gate equivalents.

NOTE 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.

4.2 Energy consumption

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

4.3 Program code size and RAM size

Program code size (loosely referred to as ROM) and RAM size can be constrained on what is loosely referred to as low end processors. These processors have simple instruction sets and limited space available for the

program code, and also limited space available in RAM for computations (e.g. embedded processors) when compared to modern computer processors.

4.4 Communication bandwidth

Communication bandwidth is limited in certain cases with respect to a maximum number of bits that can be transmitted during a session (e.g. RFID). Mechanisms that fall into this category are therefore tailored to be more economical with regard to the number of bits that is required to transmit over the communications channel when compared to other more generally used cryptographic mechanisms.

5 Requirements

5.1 Security requirements

In ISO/IEC 29192, the security strength of cryptographic mechanisms is measured as defined in 3.10. This notion can be used for different cryptographic mechanisms. Two mechanisms are considered to be of comparable strength for the given sizes 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 general-purpose lightweight cryptography.

NOTE Many organisations recommend using cryptographic mechanisms with more than 80-bit security after 2010. However, there are some lightweight cryptographic applications with special properties that might allow lower security requirements, i.e. do not have to assume all powerful adversaries. It may imply that less data can be encrypted with a single key. 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 2008-2009 [5] recommends 80-bit security for very short-term protection against intelligence agencies with a budget of $300M or 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 SC 27 at http://www.jtc1sc27.din.de/sbe/SD12.

5.2 Classification requirements

For a cryptographic mechanism to be classified as lightweight cryptography, it must have (by definition of ISO/IEC 29192) been tailored for some of the categories defined in Clause 4. A mechanism shall be tailored for a combination of the categories defined in Clause 4. 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.).

All evidence of suitability for a particular category shall be based as far as possible, on well founded 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 Algorithm 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 algorithm A, compared to other algorithms commonly in use that are not considered as lightweight algorithms. The claim can be further substantiated by referencing real implementations in which the energy consumption was experimentally measured, and compare it to other real implementations in which similar measurements were made.

5.3 Implementation requirements

5.3.1 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 will be 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 are required to include its expected size in GEs.

It is possible that any particular lightweight cryptographic mechanism standardized in ISO/IEC 29192 can be implemented with even less gate equivalents. 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.

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, but in ISO/IEC 29192 energy consumption should be evaluated by using 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 can be provided where available. When experimental measurements are provided, the experimental measurement methodology used must be 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 shall provide 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

5.3.2 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 will be compared by code size and required RAM size on the same technology to existing standards (e.g. AES). If the required code size and RAM size is considerably less, such mechanisms can be considered for inclusion in ISO/IEC 29192. Preference will be given to lightweight cryptography mechanisms that will be 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 on only on specific technologies.

5.4 General requirements

In some lightweight cryptographic applications short messages / plaintexts / ciphertexts are processed on the input of the cryptographic mechanism. When lots of short messages / plaintexts / ciphertexts are processed in a short time, 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 was tailored to have a good short input performance and if it is the case, this fact shall be indicated by the mechanism.

6 Lightweight cryptographic mechanisms

6.1 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. On the other hand, the block ciphers included in ISO/IEC 29192-2 are evaluated based on the selection criteria described in Annex A 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 29192-1 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.

General purpose block ciphers process large blocks of data at a time. In the case of lightweight cryptography, some of the block ciphers may have smaller block lengths. The shorter block lengths pose no threat, but care has to be taken since a shorter block length 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 SC 27 at http://www.jtc1sc27.din.de/sbe/SD12 for details on the relation between block length and rekeying.

6.2 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. 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 ISO/IEC 29192 considering suitability for constrained environments.

6.3 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 5.3. Three kinds of lightweight asymmetric schemes are referenced:

— Challenge-response identification schemes. They provide a form of strong entity authentication and can be classified into schemes that are based on symmetric cryptography and those that are based on asymmetric cryptography. Schemes based on symmetric cryptography typically use a block cipher. Therefore lightweight symmetric challenge-response identification schemes will, in effect, be covered by the mechanisms in **Fehler! Verweisquelle konnte nicht gefunden werden.**. Solutions for asymmetric challenge-response identification schemes are provided by zero-knowledge identification schemes, which are described, for instance, in ISO/IEC 9798-5.

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

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

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 special-purpose lightweight cryptography. It is however recommended that at least 112-bit security be applied where for systems that will that will require security for longer periods (refer to SD12 for security strength references).

b) The hardware implementation properties (for mechanisms tailored for hardware). The chip area occupied by the cryptographic mechanism (much less resource requirements than existing standards) and the energy consumption (clear advantage over existing standards).

c) The software implementation properties (for mechanisms tailored for software). In particular, the code size and the required RAM size. (Much less resource requirements than 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 for 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 algorithm.

Passive devices do not have its own power supply. The energy required for a passive device comes from a magnetic or electromagnetic field generated by the reading device [7]. The maximum strength of the field is regulated by law and decreases as the distance between reading device and the passive device increases. The energy is stored on the passive device and is used 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 an important measure for passive devices is the power consumption (in W).

B.1.2 Power consumption

The following equation summarizes the power dissipation P in CMOS devices [6]:

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

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 l_{leak} the leakage current. The first summand represents the dynamic power consumption and the second the static power consumption. At higher 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 l_{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 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 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 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 appendix.

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 area and power consumption.

To lower power consumption and 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 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 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 area, power, and timing figures. Furthermore, most likely a cryptographic algorithm is part of a larger integrated circuit rather than a stand-alone solution. Therefore we propose to ignore the I/O overhead, which allows for a fairer comparison of the properties of an algorithm 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:

Area: 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 area requirements independently it is common to state the area as gate equivalents (GEs). One GE is the area which is required by the two-input NAND gate with the lowest driving strength of the appropriate technology. The 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 EDA (electronic design automation) synthesis tool. It is commonly used and widely accepted as a fair measure for comparison of the 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 the output size and for hash functions it is the input size.

Cycles: Number of clock cycles [CLK] to compute the result. This measure is dependent on the architectural implementation strategy and can be easily obtained by paper and pencil.

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 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 frequency used.

Power: The power consumption is often estimated on the gate level by an EDA 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 EDA tool. Thus it is not easy to compare the power consumption and consequently is not well suited for our needs.

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 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 area requirements by the throughput, i.e. eff = area/throughput, and is expressed in gate equivalents per bits per second [GE/bps]. This measure is also dependent on the frequency used. For further measures and their discussion in the context of cryptographic algorithms, we refer to [8].

Annex C
(normative)

Metrics for hardware targeted block and stream ciphers

C.1 Assumptions

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

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

b) Clocked at a low 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 we focus 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 area, i.e. GE. Finally, the third assumption allows us to ignore the I/O overhead. This in turn allows us to focus on the properties of the cryptographic algorithm 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) **Area:** in [GE], obtained by an EDA tool. Used to compare both the 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 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 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 frequency, I/O, supply voltage etc.

Bibliography

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

[2] ISO/IEC 9797-1:1999, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[3] ISO/IEC 9798-5:2004, *Information technology — Security techniques — Entity Authentication — Part 5: Mechanisms using zero-knowledge techniques*

[4] ISO/IEC 10118-2:2000, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher*

[5] *ECRYPT2 Yearly Report on Algorithms and Keysizes (2008-2009)*, D.SPA.7, July 2009

[6] 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

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

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