INTERNATIONAL STANDARD

ISO/IEC 29192-4

First edition
2013-06-01

AMENDMENT 1
2016-02-15

Information technology — Security techniques — Lightweight cryptography —

Part 4: Mechanisms using asymmetric techniques

AMENDMENT 1

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

Partie 4: Mécanismes basés sur les techniques asymétriques

AMENDEMENT 1

Reference number
ISO/IEC 29192-4:2013/Amd.1:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Information technology — Security techniques — Lightweight cryptography —

Part 4: Mechanisms using asymmetric techniques

AMENDMENT 1

Page v, Introduction

Change the first sentence to:

This part of ISO/IEC 29192 specifies four lightweight mechanisms based on asymmetric cryptography.

Add the following after the third bullet:

— ELLI is a unilateral authentication scheme based on discrete logarithms on elliptic curves over finite fields of characteristic two. The scheme is particularly designed with regard to use in passive RFID tags of vicinity type.

NOTE ELLI has been successfully implemented on a passive RFID tag fully compliant to ISO/IEC 15693/18000-3. Prototype tags with practical working distance of "vicinity type" were presented at CeBIT 2008 and EuroID 2008.

Add the following after the patent holder of Agency for Science, Technology and Research:

Siemens Aktiengesellschaft
CT IP LT M&A, Otto-Hahn-Ring 6, 81739 Muenchen, Germany

Page 1, Scope

Change the first sentence to:

This part of ISO/IEC 29192 specifies four lightweight mechanisms using asymmetric techniques:

Add the following item to the list:

— a unilateral authentication scheme (ELLI) based on discrete logarithms on elliptic curves defined over finite fields of characteristic two.

Page 1, Terms and definitions

Add the following and renumber all the terms and definitions alphabetically:

3.28
finite field of characteristic two
finite field whose number of elements is a power of two

Note 1 to entry: All finite fields of characteristic two containing the same number of elements are isomorphic. The specific model for the description of the finite field of characteristic two that is used in this part of ISO/IEC 29192 is given in Annex E.

3.29
ordinary elliptic curve over a finite field of characteristic two
elliptic curve over a finite field F of characteristic two defined by a short (affine) Weierstrass equation of type $Y^2 + XY = X^3 + aX^2 + b$, with $a, b \in F$ and $b \neq 0_F$

Note 1 to entry: A reference for the group properties of elliptic curves is ISO/IEC 15946-1:2008, Annex B.

Note 2 to entry: The set of points on E together with one extra symbol 0_E constitute a finite abelian group.

Page 4, Symbols and abbreviated terms

Replace the following symbol:

$|A|$ bit size of the number A if A is a non-negative integer (i.e. the unique integer i so that $2^{i-1} \leq A < 2^i$ if $A > 0$, or 0 if $A = 0$, e.g. $|65\,537| = |2^{16} + 1| = 17$), or bit length of the bit string A if A is a bit string

NOTE To represent a number A as a string of α bits with $\alpha > |A|$, $\alpha - |A|$ bits set to 0 are appended to the left of the $|A|$ bits.

with

$|\Phi|$ bit size of the number Φ if Φ is a non-negative integer (i.e. the unique integer i so that $2^{i-1} \leq \Phi < 2^i$ if $\Phi > 0$, or 0 if $\Phi = 0$, e.g. $|65\,537| = |2^{16} + 1| = 17$), or bit length of the bit string Φ if Φ is a bit string

NOTE To represent a number Φ as a string of α bits with $\alpha > |\Phi|$, $\alpha - |\Phi|$ bits set to 0 are appended to the left of the $|\Phi|$ bits.

Replace the following symbol:

$\lfloor A \rfloor$ the greatest integer that is less than or equal to the real number A

with

$\lfloor \Phi \rfloor$ the greatest integer that is less than or equal to the real number Φ

Replace the following symbol:

$A[i]$ the i^{th}-bit of the number A, where $A[1]$ is the right-most bit and $A[|A|]$ is the left-most bit

with

$\Phi[i]$ the i^{th}-bit of the number Φ, where $\Phi[1]$ is the right-most bit and $\Phi[|\Phi|]$ is the left-most bit

Replace the following symbol:

$B \,||\, C$ bit string resulting from the concatenation of data items B and C in the order specified.

with

$\Psi \,||\, \Gamma$ bit string resulting from the concatenation of data items Ψ and Γ in the order specified.

Insert the following symbols and abbreviated terms and rearrange Clause 4 alphabetically:

A claimant

B verifier

$E_{\{a,b\}}$ ordinary elliptic curve over $F(2^g)$ given by its short (affine) Weierstrass equation $Y^2 + XY = X^3 + aX^2 + b$, together with a point 0_E at infinity, with $a, b \in F(2^g)$ and $b \neq 0_F$. (domain parameter)

E_{twist} elliptic curve twisted to the elliptic curve E (domain parameter, but not explicitly used)

$\#(E_{\{a,b\}})$ order (cardinality) of $E_{\{a,b\}}$ (domain parameter)

$F(2^g)$ finite field consisting of exactly 2^g elements, g a positive integer

$f(X)$ irreducible polynomial over $F(2)$ which is used in the construction of $F(2^g)$

$MUL_{b,aff}\left(k, x_R\right)$ function depending on the field element $b \neq 0_F$ that adjoins to the element x_R from $F(2^g)$ and the integer k the (affine) x-coordinate $X_S Z_S^{-1}$ of the point $S = [k]R = \left(X_S : Y_S : Z_S\right)$ on an ordinary elliptic curve defined over $F(2^g)$ with parameter b and with R a point on this curve with affine x-coordinate x_R

NOTE For the mathematical background of $MUL_{b,aff}\left(k, x_R\right)$, see Annex F.

$MUL_{b,proj}\left(k, x_R\right)$ function depending on the field element $b \neq 0_F$ that adjoins to the element x_R from $F(2^g)$ and the integer k the projective x-coordinate $\left(X_S : Z_S\right)$ of the point $[k]R = S = \left(X_S : Y_S : Z_S\right)$ on an ordinary elliptic curve defined over $F(2^g)$ with parameter b and with R a point on this curve with affine x-coordinate x_R

NOTE For the mathematical background of $MUL_{b,proj}\left(k, x_R\right)$, see Annex F.

S, T, U points on the elliptic curve E

$\mathrm{Tr}(a)$ $\mathrm{Tr}(a) = a^{2\wedge 0} + a^{2\wedge 1} + \ldots + a^{2\wedge(g-1)}$, for an arbitrary element a of $F(2^g)$. Tr is the "trace function" and $\mathrm{Tr}(a)$ is the "trace of the field element a". The trace function takes only the two values 1_F and 0_F.

$\left(X_R, Y_R\right)$ affine coordinates of point R, where x_R denotes the x-coordinate and Y_R denotes the y-coordinate of point R

NOTE The point 0_E does not have a representation using affine coordinates.

$(X_R : Y_R : Z_R)$ projective coordinates of the point R. $(X_R : Y_R : Z_R)$ is the equivalency class of triples (X_R, Y_R, Z_R) of elements of $F(2^g)$ that solve the adjoined (projective) Weierstrass equation $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$, where $(X_{R'}, Y_{R'}, Z_{R'})$ is called equivalent to (X_R, Y_R, Z_R), if and only if $X_{R'} = \lambda X_R$, $Y_{R'} = \lambda Y_R$ and $Z_{R'} = \lambda Z_R$, with some element $\lambda \neq 0_F$

NOTE The point 0_E has projective coordinates $(0_F : 1_F : 0_F)$.

$(X_R : Z_R)$ projective x-coordinate of point R

NOTE 1 $Z_R \neq 0_F$ and $(X_R : Z_R)$ corresponds to the affine coordinate $X_R Z_R^{-1} \in F(2^g)$.

NOTE 2 A point R with affine coordinates (x_R, y_R) has projective coordinates $(x_R : y_R : 1_F)$.

NOTE 3 A point R with projective coordinates $(X_R : Y_R : Z_R)$ has affine coordinates $(X_R Z_R^{-1}, Y_R Z_R^{-1})$.

Page 13

Add the following new Clause 8 after 7.5:

8 Unilateral authentication mechanism based on discrete logarithms on elliptic curves over finite fields of characteristic two

8.1 General

This mechanism, ELLI, has been designed to make asymmetric cryptography available on passive RFID tags of vicinity type (working distance of up to 1 m) for the intended main application of brand protection/anti-counterfeiting in large decentralized systems. The ELLI scheme and the concept to implement it on a passive RFID tag were firstly presented in a submission to the German IT-Security Competition held by the Horst-Görtz foundation in 2006. The scheme is also described (without using the name ELLI) in References [30] and [31].

The concept underlying ELLI is closely related to the Diffie-Hellman analogue for elliptic curves over $F(2^g)$. But, as it makes use of some specific protocol and parameter optimization steps, it was given a name of its own. These optimizations comprise the following:

— The y-coordinates of points on elliptic curves are unused.

— Checks on whether or not a given field element is the x-coordinate of a point on a claimed elliptic curve are omitted.

NOTE ELLI stands for **EL**LIPTIC **LI**GHT.

8.2 Security requirements for the environment

The ELLI scheme is a unilateral authentication mechanism based on discrete logarithms on elliptic curves defined over a finite field of characteristic two. It enables a verifier to check that a claimant knows the elliptic curve discrete logarithm of a claimed public point with respect to a base point.

A general framework for cryptographic techniques based on elliptic curves is given in ISO/IEC 15946-1. For the ELLI mechanism, some additional properties of elliptic curves defined over finite fields $F(2^g)$ are used that are not described in ISO/IEC 15946-1. These properties are presented below.

Within a given domain, the following requirements shall be satisfied. Domain parameters that govern the operation of the mechanism shall be selected. These parameters comprise the following:

— a finite field $F(2^g)$ of characteristic two;

— an ordinary elliptic curve E defined over $F(2^g)$. The elliptic curve E shall be given by its short Weierstrass equation $Y^2 + XY = X^3 + aX^2 + b$, with $b \neq 0_F$, and shall be chosen in such a way that the following two conditions hold:

  — $\#(E) = 4q_1$, with a prime q_1;

  — $\#(E_{twist}) = 2q_2$, with a prime q_2;

— a point $P = (x_P, y_P)$ on E generating a subgroup of order q_1.

NOTE 1 In this situation, the condition $q_1 < q_2$ is automatically fulfilled. This is due to the fact that $\#(E)$ and $\#(E_{twist})$ are of the same order of magnitude as a consequence of the Hasse-Weil theorem (see Annex F).

The size of the finite field $F(2^g)$ and the parameters of the two curves E and E_{twist} are chosen in such a way that solving the elliptic curve discrete logarithm problem and solving the static Diffie-Hellman problem in both E and E_{twist} are computationally infeasible tasks.

The selected parameters shall be made available, to the necessary extent and in a reliable manner, to all entities within the domain.

a) Every claimant shall be equipped with a private key.

b) Every claimant shall have the ability to execute the operations addition and multiplication in $F(2^g)$.

c) Every claimant shall be able to execute the function $MUL_{b,proj}$ introduced in Clause 4, for the specific value b related to the elliptic curve E.

d) Every verifier shall obtain an authentic copy of the public key corresponding to the claimant's private key.

e) Every verifier shall be equipped with the base point P of the elliptic curve E and with the order q_1 of P.

f) Every verifier shall have the ability to execute the operations addition, multiplication and division in $F(2^g)$.

g) Every verifier shall be able to generate randomly positive integers $<q_1$.

h) Every verifier shall be able to execute the function $MUL_{b,aff}$ introduced in Clause 4, for the specific value b related to the elliptic curve E.

NOTE 2 There are various options to provide the verifiers with trusted copies of the claimant's public key. This topic is beyond the scope of this part of ISO/IEC 29192.

8.3 Key production

To produce a key pair, the following two steps shall be performed.

a) For claimant A an integer Q shall be uniformly and randomly selected from the set $\{2,\ldots,q_1\text{-}1\}$. The integer Q is A's private key.

b) A's public key $G(A)$ is $MUL_{b,aff}(Q, x_P)$, the (affine) x-coordinate of the point $G = [Q]P = (x_G, y_G)$.

8.4 Unilateral authentication mechanism

This mechanism, which enables verifier *B* to authenticate claimant *A*, is summarized in Figure 3. In Figure 3, the bracketed letters a) to e) correspond to the steps of the mechanism, including the exchanges of information, as described in detail below.

NOTE The authentication mechanism follows a "challenge-response" approach.

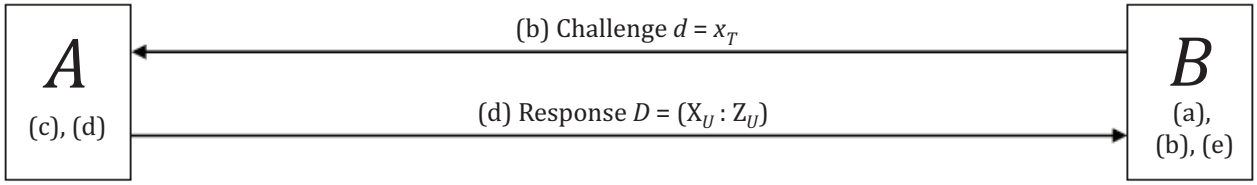

Figure 3 — ELLI

The following procedure shall be performed. The verifier *B* shall only accept the claimant *A* as valid if the following procedure completes successfully:

a) The verifier randomly chooses a fresh number r with $0 < r < q_1$ and computes $MUL_{b,aff}(r, x_P)$ *and* $MUL_{b,aff}[r,G(A)]$, i.e. the affine x-coordinate x_T of the point $T = [r]P$ and the affine x-coordinate x_V of the point $V = [r]([Q]P)$.

The challenge d is the field element $d = x_T$.

b) The verifier sends d to the claimant.

c) On receipt of the challenge d the claimant A computes $D = MUL_{b,proj}(Q,d) = (X_U : Z_U)$, the projective x-coordinate of the point $U = [Q]T$, consisting of two field elements X_U and Z_U in $F(2^g)$.

$D = (X_U : Z_U)$ is the response.

d) The claimant sends D to the verifier.

e) On receipt of the response D, the verifier B checks if $X_U = 0_F$ or $Z_U = 0_F$ holds. If one of these equations holds, the claimant is considered not authentic.

If $X_U \neq 0_F$ and $Z_U \neq 0_F$ the verifier computes $x_V Z_U$ in $F(2^g)$ and verifies whether or not the equation $X_U = x_V Z_U$ holds in $F(2^g)$. The claimant is considered authentic by the verifier if and only if the equation $X_U = x_V Z_U$ holds.

Page 14, Annex A

Replace the content with the following:

```
LightweightCryptography-4{
      iso(1) standard(0) lightweight-cryptography(29192)
      part4(4) asn1-module(0) algorithm-object-identifiers(0)}
      DEFINITIONS ::= BEGIN
EXPORTS ALL;

OID ::= OBJECT IDENTIFIER -- alias
-- Synonyms
is29192-4 OID ::= {iso(1) standard(0) lightweight-cryptography(29192) part4(4)}
```



```
mechanism OID ::= {is29192-4 mechanisms(1)}
-- Lightweight cryptographic mechanisms
lw-discrete-logarithms-ecc-CryptoGPS OID ::= {mechanism
lw-discrete-logarithms-ecc-CryptoGPS(1)}
lw-authenticated-key-exchange-ALIKE OID ::= {mechanism
lw-authenticated-key-exchange-ALIKE(2)}
lw-identity-based-signature-IBS OID ::= {mechanism
lw-identity-based-signature-IBS(3)}
lw-unilateral-authentication-ecc-ELLI OID ::= {mechanism
lw-unilateral-authentication-ecc-ELLI (4)}

END -- LightweightCryptography-4
```

Page 21, Annex C

Add the following after C.3.3.2, Example 2:

C.4 ELLI mechanism

C.4.1 Examples based on ELLI_163.1

C.4.1.1 Common properties

The elliptic curve ELLI_163.1 and the underlying field $F(2^g)$ are defined as in Annex E.3. In the following, numerical examples for the ELLI authentication scheme are given, comprising the steps key generation, challenge generation and response generation.

A common base point P is used in all examples for ELLI_163.1.

BASE POINT P	
x_P	6 2DAE88E2 17BEFF09 F408E8F8 91EC8E51 05C9E8AB
y_P	0 5B29A42D C1EBEB2D 14AC1914 421FC4AC 2B61C7E5
NOTE The y-coordinate y_P of the base point P is not necessarily used in the ELLI mechanism.	

C.4.1.2 Example 1

A key pair for claimant A is constructed.

KEY PAIR GENERATION	
PRIVATE KEY Q	DFCAC3BC 9A1E4B54 E03FAD6E E932F3BC 61170C51
PUBLIC KEY $G(A)$	2 33C2A2B8 8BEE7DD9 1DB430F9 161B0A88 B7FEB527

A challenge d is generated by the verifier with input a random number r and the x-coordinate x_P of the base point and using the function $MUL_{b,aff}$.

$$d = MUL_{b,aff}\left(r, x_P\right)$$

The response D is generated by the claimant with input the challenge d and the private key Q and using the function $MUL_{b,proj}$.