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

Tr(a) Tr(a) = $a^{2{}^\wedge 0} + a^{2{}^\wedge 1} + \ldots.+ a^{2{}^\wedge (g\text{-}1)}$, for an arbitrary element a of $F(2^g)$. Tr is the “trace function” and 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.

$\left(X_R : Y_R : Z_R\right)$ projective coordinates of the point R. $\left(X_R : Y_R : Z_R\right)$ is the equivalency class of triples $\left(X_R, Y_R, Z_R\right)$ of elements of $F(2^g)$ that solve the adjoined (projective) Weierstrass equation $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$, where $\left(X_{R'}, Y_{R'}, Z_{R'}\right)$ is called equivalent to $\left(X_R, Y_R, Z_R\right)$, 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 $(0_F : 1_F : 0_F)$.

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

NOTE 1 $Z_R \neq 0_F$ and $\left(X_R : Z_R\right)$ 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 $\left(x_R : y_R : 1_F\right)$.

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

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.

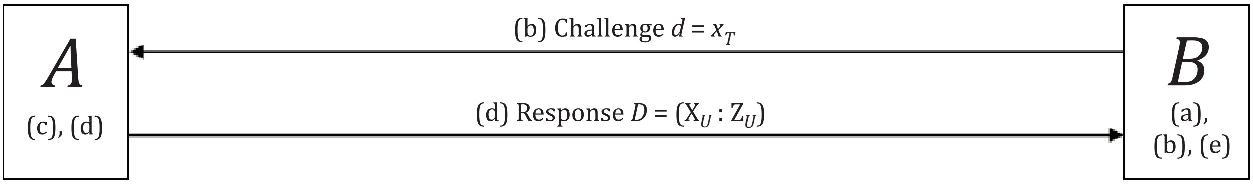

Figure 3 — ELLI

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 $MUL_{b,aff}\left(r, x_P\right)$ *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 $D = MUL_{b,\,proj}(Q,d) = \left(X_U : Z_U\right)$, the projective x-coordinate of the point $U = [Q]T$, consisting of two field elements X_U and Z_U in $F(2^g)$.

$D = \left(X_U : Z_U\right)$ 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 $MUL_{b,proj}$.

$$D = \left(X_U : Z_U\right) = MUL_{b,proj}(Q,d)$$

CHALLENGE GENERATION $d = MUL_{b,aff}\left(r, x_P\right)$	
RANDOM NUMBER r	93D4625C 890DE3CD 8889225C 180E03C3 DF647545
CHALLENGE d	5 3735DD9D 700B0617 D6B0FE8E B0BA11D8 65D9532F
POSSIBLE RESPONSE $D = \left(X_U : Z_U\right)$	
X-VALUE X_U	3 F625D290 2FE3297F A177959A AD59AA0B 9D913C07
Z-VALUE Z_U	0 447352DD 05B0568B 191865A5 1FA0779C DD81258D
$x_V = X_U Z_U^{-1}$ (affine)	4 531ADD58 617220E6 4A3915D5 6BCD69FD F434A2F2

NOTE The pair $\left(X_U : Z_U\right)$ is the “projective x-coordinate”, and hence is not unique as numerical value. The adjoined unique numerical value related to the response is the affine x-coordinate $x_V = X_U Z_U^{-1}$. This holds in the same way for all the following examples.

C.4.1.3 Example 2

KEY PAIR GENERATION	
PRIVATE KEY Q	DE5A6D34 F3A8C4E1 6E132FD4 33F4B4BD 65E20CB9
PUBLIC KEY $G(A)$	3 E8462A29 41BB3D71 433AEB2C 67877D4B 88D5529D
CHALLENGE GENERATION $d = MUL_{b,aff}\left(r, x_P\right)$	
RANDOM NUMBER r	F9B6C01B CD3A85A8 99986F79 F4AFD289 056A3842
CHALLENGE d	61FE5AEC F245ECE4 B504CD65F E2D70C9C F28E6626
POSSIBLE RESPONSE $D = \left(X_U : Z_U\right)$	
X-VALUE X_U	3 8487B630 029D21C3 0768C095 B2AEF06B 63FE8143
Z-VALUE Z_U	0 19BF93D2 222E56E0 B8B50A7D B9C41150 B9E9F93C
$x_V = X_U Z_U^{-1}$ (affine)	3 0DFD2997 2FD32C61 7356C895 D6912240 02752BFE

C.4.1.4 Example 3

KEY PAIR GENERATION	
PRIVATE KEY Q	7E96501F 876C785B 1511893E 97F1E923 0967945E
PUBLIC KEY $G(A)$	0 2F1B219C DD1FEBA1 64FB2B1E 805CF6F7 D65C15F7
CHALLENGE GENERATION $d = MUL_{b,aff}\left(r, x_P\right)$	
RANDOM NUMBER r	E3F72EA8 DF9A7E56 3039CBB3 745C14F9 759E40CF
CHALLENGE d	6 9EC45765 264CBA69 BBA3F698 789B06DF 26578B02
POSSIBLE RESPONSE $D = \left(X_U : Z_U\right)$	
X-VALUE X_U	0 5EE19683 164ABCDC F021A091 8046AA5B 56C6B128
Z-VALUE Z_U	2 15B2A8AB 8CFCF47D E173C38A A6BB8F0E 46B19463
$x_V = X_U Z_U^{-1}$ (affine)	7 6F2BC182 34FDAD56 743C0387 90CEC425 54A5BD25

C.4.2 Examples based on ELLI_193.1

C.4.2.1 Common properties

The elliptic curve ELLI_193.1 and the underlying field $F(2^g)$ are defined as in Annex E.4. 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 the following examples for ELLI_193.1.

BASE POINT P	
x_P	1 C035F1CF E40C8BC6 B09F59E5 60953526 BB67E2A9 1CCD97B3
y_P	1 C848D5FF 00F24C02 63DB3036 3550F134 83769167 68EB72F5
NOTE The y-coordinate y_P of the base point P is not necessarily used in the ELLI mechanism.	

C.4.2.2 Example 1

A key pair for claimant A is constructed.

KEY PAIR GENERATION	
PRIVATE KEY Q	12A4B91B 45E0E29E 54717EB7 3149B344 260DB6C5 85829BA1
PUBLIC KEY $G(A)$	0 D74E3E63 ABECFFB7 4A57BC37 F0BBA4C2 A9436EF6 2C0C3331

A challenge d is generated by the verifier with input a random number r and the x-coordinate x_P of the base point P 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 the challenge d and the private key Q as input to the function $MUL_{b,proj}$.

$$D = \left(X_U : Z_U\right) = MUL_{b,proj}(Q,d)$$

CHALLENGE GENERATION $d = MUL_{b,aff}\left(r, x_P\right)$	
RANDOM NUMBER r	3B5E7757 6B069EBC 757E6D99 366255E8 64EE6E64 BA8D4318
CHALLENGE d	1 342322E0 A5A77B74 92886779 09545939 E590A632 9FF797FD
POSSIBLE RESPONSE $D = \left(X_U : Z_U\right)$	
X-VALUE X_U	1 3FE539BC 35CAC440 9A30AAAC 9B416E09 44EBBEF8 ED42C259
Z-VALUE Z_U	1 8FA597E9 D28CA94D 98C2872B D31D1297 8DEE3580 CC66DFCE
$x_V = X_U Z_U^{-1}$ (affine)	0 E1F66999 BE367042 C851A9E7 33B6A0CE 708C6165 1E6F0F7B

C.4.2.3 Example 2

KEY PAIR GENERATION	
PRIVATE KEY Q	610C5354 FADFB86E 2893DDC8 D864416F 8E85FFC3 EFC430B2
PUBLIC KEY $G(A)$	1 7AF97A22 51AF656C 054D4F8F D29AAA31 DEF9148B D1B62940
CHALLENGE GENERATION $d = MUL_{b,aff}\left(r, x_P\right)$	
RANDOM NUMBER r	47B631CF 510FE318 3D4CE47E 42A7F97B 70B3FD05 E9AEB4BE
CHALLENGE d	1 48BC609E ECE1EE7A 448900D6 5B2312A2 BB6928EC A7E21FC8
POSSIBLE RESPONSE $D = \left(X_U : Z_U\right)$	
X-VALUE X_U	1 21A6A15C 09345264 811AD857 6833CAEB 4D1AA265 AB8E3E94
Z-VALUE Z_U	0 9D64B2AF 1B5232E7 091B5D9A 9D3A7914 A28EA572 5B760D66
$x_V = X_U Z_U^{-1}$ (affine)	1 0321B38B 4EEFC4B3 A08107E7 D1159CC2 965D3DEC F509A71F

C.4.2.4 Example 3

KEY PAIR GENERATION	
PRIVATE KEY Q	63825DA5 88BEDD37 3BFE2F2C 9E1E022D 32087314 4401AAD2
PUBLIC KEY $G(A)$	1 D37D06DC 331EB141 03ABFBDD 4BACF334 10EDD836 F79CED32
CHALLENGE GENERATION $d = MUL_{b,aff}\left(r, x_P\right)$	
RANDOM NUMBER r	69F78993 92558F1A D85A0D9B 853A7880 3F022000 4b28814C
CHALLENGE d	0 37D725B7 DB2A168E 9E52BE09 014A3AC3 8B2F802C B8808050
POSSIBLE RESPONSE $D = \left(X_U : Z_U\right)$	
X-VALUE X_U	1 94F6B90F D19DF28C A91FF7E0 B201F02E E0D4DC31 7BF187AF
Z-VALUE Z_U	1 756CEDB1 5052992A 4CD47C22 84487603 FD95FC75 A0BF197E
$x_V = X_U Z_U^{-1}$ (affine)	0 74C9F956 B4E4E893 98A70D23 9C119D7A DE9D5D50 740CD1B7

Page 22, Annex D

Replace Table D.1 by the following:

Table D.1 — Compliance of algorithms properties with the requirement of ISO/IEC 29192-1

		Algorithm name				
		cryptoGPS[5]	ALIKE[3]	IBS[9]	ELLI_163.1	ELLI_193.1
Constraints	Chip area	X			X	X
	Energy consumption	X		X	X	X
	Code size and RAM size		X	X	X	X
	Communication bandwidth	X	X	X	X	X
	Execution time	X	X		X	X

Page 21, Annex D

Add the following after Table D.4:

Table D.5 — ELLI characteristics

		ELLI_163.1	ELLI_193.1
Security level [bits]		80	80
Chip area [GE] based on Hardware Prototype my-d-ECC[30]	ELLI module in total	12 876	approx. 15 000
	Storage	5 273	approx. 6 243
	Arithmetic unit + control logic	6 171 + 1 432 = 7 003	approx. 8 750
Authentication process [CLK] based on the architecture of hardware prototype my-d-ECC (163 bit)[30]		80 465	approx. 95 000
Energy consumption [µJ]		7,5	approx. 10,5
Data to be transferred [bits]		3 × 163	3 × 193

NOTE 1 For the curve ELLI_163.1, the data in Table D.5 are based on the architecture of the hardware prototype described in Reference [30]. The values for ELLI_193.1 are partially extrapolated based on the results of Reference [30] assuming an analogous architectural approach.

NOTE 2 Based on the Pollard-Rho algorithm to compute discrete logarithms, one could argue that the security level entries in row two should be set to 81 and 95, respectively. But, according to ISO/IEC 29192, the allowed entries are restricted to the values 80, 112, 128, 192, and 256.

NOTE 3 For the entries in row two of Table D.5, attacks requiring a large number of queries of the algorithm and a large amount of memory are not considered, e.g. exceeding 2^{34} queries and storage of size 2^{64}. If the number of queries to the device is allowed to be $2^{34,3}$ and a storage of size 2^{64} is assumed to be available for the attack, the security level is decreased to 72 in the case of ELLI_163.1. See also G.3.

Add the following new Annexes after Annex D:

Annex E

(normative)

ELLI_163.1 and ELLI_193.1

E.1 General

Annex E specifies two elliptic curves — ELLI_163.1 and ELLI_193.1 — that shall be used in the ELLI-mechanism. In addition, necessary information on how to construct a full set of domain parameters is given.

The elliptic curve ELLI_163.1 provides a security level of $\sim 2^{80}$ with respect to the ECDL-problem. The respective value for ELLI_193.1 is $>2^{95}$.

E.2 Representation of the field $F(2^g)$ and its elements

The field $F(2^g)$ is given as $F(2)[X]/f(X)$, where $f(X)$ is an irreducible polynomial over $F(2)$ of degree g. In this model, the elements of $F(2^g)$ are the polynomials $b_{g-1}X^{g-1} + b_{g-2}X^{g-2} + \ldots + b_1X + b_0$, with $b_i \in \{0,1\}$.

The elements $(b_{g-1}, b_{g-2}, \ldots, b_1, b_0)$ of $F(2^g)$ are represented as hexadecimal strings, as in ISO/IEC 15946-1.

E.3 ELLI_163.1 and related parameters

The following parameters shall be used with the curve ELLI_163.1:

$f(X)$	=	$X^{163} + X^{17} + X^6 + X + 1$
	=	8 00000000 00000000 00000000 00000000 00020043
a	=	0_F
b	=	7 640BFEA7 CC3B22CD 51B4217C 25A70C81 E7A7260A
$\#(E)$	=	$4 \cdot q_1$
q_1	=	1 FFFFFFFF FFFFFFFF FFFEBD90 042B33A9 48E95823
$\#(E_{twist})$	=	$2 \cdot q_2$
q_2	=	4 00000000 00000000 000284DF F7A998AD 6E2D4FBB
NOTE “*a*” is not necessarily used in the ELLI mechanism.		

E.4 ELLI_193.1 and related parameters

The following parameters shall be used with the curve ELLI_193.1:

$f(X)$	=	$X^{193} + X^{17} + X^{14} + X^{12} + 1$
	=	2 00000000 00000000 00000000 00000000 00000000 00025001
a	=	0_F
b	=	0 5BD20FC9 907A1E5F F4034D4A E883BDF7 5A8E05EA 5E41EC53
$\#(E)$	=	$4 \cdot q_1$
q_1	=	7FFFFFFF FFFFFFFF FFFFFFFF F38514E9 A5FB4D1E B499AF33
$\#(E_{twist})$	=	$2 \cdot q_2$
q_2	=	1 00000000 00000000 00000000 18F5D62C B40965C2 96CCA19B
NOTE “*a*” is not necessarily used in the ELLI mechanism.		

Annex F

(informative)

Some special properties of elliptic curves over $F(2^g)$

The ELLI scheme largely follows the Diffie-Hellman analogue for elliptic curves with the keys of one of the two communicating entities fixed. The ELLI mechanism deviates from this approach in two ways.

— The scheme makes use only of the *x*-coordinates of points on elliptic curves whereas *y*-coordinates are completely unconsidered and unused. (This is not to be confused with point compression.)

- There are no checks whether or not a submitted field element is actually the x-coordinate of some point on the used curve E.

It is the purpose of this Annex to describe the background of these two specific properties of the ELLI mechanism. It is assumed that the reader has basic knowledge on elliptic curves as far as it is necessary to understand the usage of elliptic curves in asymmetric cryptography.

Fact 1: Let $E = (E_{\{a,b\}})$ be an ordinary elliptic curve over $F(2^g)$. The point set $(E_{\{a,b\}})$ is a finite abelian group of order $\#(E_{\{a,b\}}) = 2^g + 1 - t$, *where t is an odd integer with* $|t| \le 2\cdot\sqrt{2^g}$. Furthermore, all the possible odd numbers t in the interval $-2\cdot\sqrt{2^g} \le t \le +2\cdot\sqrt{2^g}$ actually occur. (The parameter t is known as “trace of the Frobenius endomorphism”.)

Fact 2: Let $E = (E_{\{a,b\}})$ be an ordinary elliptic curve over $F(2^g)$ with $\#(E_{\{a,b\}}) = 2^g + 1 - t$. Then, for the order of an elliptic curve $(E_{\{a',b\}})$ *over* F 2)(^{g}, with arbitrary element $a' \in F(2^g)$, there are exactly two possibilities:

Case (1): $\#(E_{\{a',b\}}) = \#(E_{\{a,b\}}) = 2^g + 1 - t$;

Case (2): $\#(E_{\{a',b\}}) = \#(E_{\{a,b\}}) + 2\cdot t = 2^g + 1 + t$.

The mathematical background of Fact 2 is related to the concepts of isomorphic elliptic curves and twisted elliptic curves, namely:

Let $(E_{\{a,b\}})$ and $(E_{\{a',b'\}})$ be ordinary elliptic curves over the finite field $F(2^g)$ with Weierstrass equations $Y^2 + XY = X^3 + aX^2 + b$ *and* $Y^2 + XY = X^3 + a'X^2 + b'$, respectively. Then the following properties hold:

- $(E_{\{a,b\}})$and $(E_{\{a',b'\}})$ are isomorphic if and only if $b' = b$ *and* $\mathrm{Tr}(a') = \mathrm{Tr}(a)$;
- $(E_{\{a',b\}})$and $(E_{\{a,b\}})$ are twisted if and only if $b' = b$ *and* $\mathrm{Tr}(a') \ne \mathrm{Tr}(a)$;
- in Case (1), the curve $(E_{\{a',b\}})$ is *isomorphic* to $(E_{\{a,b\}})$;
- in Case (2), the curve $(E_{\{a',b\}})$ is *twisted* to $(E_{\{a,b\}})$.

NOTE 1 The notion of “isomorphic elliptic curves” is here to be understood in the sense of isomorphism of algebraic varieties, i.e. without consideration of the group structure induced on the elliptic curve. This notion of isomorphism is distinct from and should not be confused with “point groups of elliptic curves isomorphic as finite groups”.

NOTE 2 A first consequence of Fact 1 and Fact 2 is that the order of an ordinary elliptic curve over $F(2^g)$ is always even and that, if the curves from Case (1) have order $\equiv 2$ modulo 4, then the curves from Case (2) necessarily have order $\equiv 0$ modulo 4, and the other way around.

NOTE 3 For the ELLI scheme, the elliptic curves are chosen such that orders of both classes have the best possible prime factorization: $\#(E) = 4\cdot q_1$ and $\#(E_{\mathrm{twist}}) = 2\cdot q_2$, with q_1 and q_2 primes.

Fact 3: Let k be an arbitrary positive integer and let P be a point on the ordinary elliptic curve $(E_{\{a,b\}})$. Then, the x-coordinate of $[k]P$ is **independent** from the curve parameter a and the y-coordinate of the point P. It depends only on the curve parameter b and the x-coordinate of the point P.

(For a proof, see Reference [28], p. 42.)

Fact 4: Let x be an arbitrary element from $F(2^g)$. For a fixed value b from $F(2^g)$, x is **always** the x-coordinate x_R of a point R on some ordinary elliptic curve over $F(2^g)$ with parameter b, namely

- either R is on a curve isomorphic to $E = (E_{\{a,b\}})$, or
- R is on a twisted curve (E_{twist}) *of* E.

(For a proof, see Reference [28], p. 26 and p. 38.)

As a consequence of these facts, one can introduce the two functions ***MUL**$_{b,proj}$* and ***MUL**$_{b,aff}$* used in the ELLI mechanism.

— $\boldsymbol{MUL}_{\boldsymbol{b,proj}}(k,\ x_R) := \left(X_S : Z_S\right)$, if $S = [k]R = \left(X_S : Y_S : Z_S\right)$

— $\boldsymbol{MUL}_{\boldsymbol{b,aff}}(k,\ x_R) := X_S Z_S^{-1}$, if $S = [k]R = \left(X_S : Y_S : Z_S\right)$

Here, k is an arbitrary positive integer; x_R is a field element and hence, the affine x-coordinate of some point R on an elliptic curve, namely either on $E = (E_{\{a,b\}})$ or on a twisted curve, E_{twist} *of* E.

Annex G

(informative)

ELLI — Security Considerations

G.1 General

In this Annex, various attacks against the ELLI scheme are discussed and evaluated. Being based on the Diffie-Hellman analogue for elliptic curve over finite fields $F(2^g)$, the security of the ELLI mechanism clearly depends on the assumed hardness of the elliptic curve discrete logarithm problem (ECDLP) for elliptic curves defined over fields $F(2^g)$. Any progress in attacking this problem, and related problems, will automatically affect the security of the ELLI mechanism.

G.2 Attacks based on the ECDLP

The most obvious attack against the ELLI mechanism is an attempt to solve the ECDLP for the given public key $G(A)$ which is the x-coordinate of some point in the cyclic group of prime order q_1 generated by the base point P.

The best known general attack (Pollard ρ-algorithm) requires $O(\sqrt{q_1})$ operations in the point group generated by the point P. With the primes q_1 related to the elliptic curve ELLI_163.1 and ELLI_193.1 of bit lengths 161 resp. 191 such an attack is currently infeasible.

The MOV attack and the Frey-Rück attack transform the ECDL problem in the group generated by the point P to the discrete logarithm problem in some extension field $F(2^{gj})$ of $F(2^g)$. A necessary condition for the feasibility of these attacks is that the order of the point group divides $2^{gj} - 1$, with small j. This is not the case for the elliptic curves ELLI_163.1 and ELLI_193.1.

G.3 Attacks based on the static Diffie-Hellman problem

The claimant A may be considered as a static Diffie-Hellman oracle. Roughly speaking, after feed-in of a point R (on the curve E or on a twisted curve), it outputs the multiple $[Q]R$. Brown and Gallant present in Reference [29] an algorithm to find Q in this scenario. The complexity of the algorithm depends on the factorization of the numbers q_1-1 and q_2-1. The relevant parameters of the elliptic curves ELLI_163.1 and ELLI_193.1, including the orders of the twisted curves, are chosen in such a way that attacks based on the Brown-Gallant algorithm are currently impossible.

Cheon describes in Reference [32] an extension of the Brown-Gallant algorithm that also exploits the factorization of the two numbers $q_1 + 1$ and $q_2 + 1$. For the suggested elliptic curve ELLI_163.1, Cheon's algorithm needs approximately 2^{34} queries of the ELLI algorithm to construct a data base comprising 2^{64} points of the involved elliptic curve. Given this data base, the private key of the ELLI algorithm can be calculated in approximately 2^{72} elliptic curve point additions. For the case of ELLI_193.1 the respective data are: 2^{51} queries of the ELLI scheme, memory to store 2^{71} elliptic curve points, time complexity is 2^{79} elliptic curve point additions.

It seems currently impossible to provide the necessary memory sizes.

G.4 Attacks based on invalid or weak input

As the claimant does not make any evaluation of input parameters, it is possible to feed the claimant with invalid or weak parameters. If the challenge is not the x-coordinate of a point on the elliptic curve, it is the x-coordinate of a point on a twisted curve. For the elliptic curves ELLI_163.1 and ELLI_193.1, $q_2 > q_1$ holds. Hence, the ECDL problem in a twisted curve is slightly harder than the ECDL problem in E.

The point group of E contains a subgroup of order four. Sending the x-coordinate of an element of order four to the claimant the response immediately reveals the residue of Q modulo 4. Hence, the two least significant bits of the private key Q have to be considered as known. This is not a relevant attack but an accepted design feature.

Annex H

(informative)

ELLI — Implementation options

H.1 General

In this Annex, various options to implement the functions $MUL_{b, proj}$ and $MUL_{b,aff}$ are presented.

H.2 Algorithm based on the Montgomery-ladder

This algorithm is a direct consequence of the so called “Montgomery-ladder”. The algorithm makes use of five variables X_S, Z_S, X_2, Z_2 and H (for temporary value).

Input:

— A positive integer $k = (k_g, \ldots, k_1)$, given in binary representation, with $k_g = 1$;

— The parameter b;

— The field element x_R (challenge).

Output calculation:

```
a)  $X_S \leftarrow 1_F, Z_S \leftarrow 0_F, X_2 \leftarrow x_R, Z_2 \leftarrow 1_F$;
b)  for i ← g down to 1 do:
    if $k_i = 1$ then
    $H \leftarrow Z_S, Z_S \leftarrow (X_S Z_2 + X_2 Z_S)^2$,
    $X_S \leftarrow x_R Z_S + X_S X_2 H Z_2, H \leftarrow X_2$,
    $X_2 \leftarrow X_2^4 + b Z_2^4, Z_2 \leftarrow H^2 Z_2^2$,
    else
    $H \leftarrow Z_2, Z_2 \leftarrow (X_2 Z_S + X_S Z_2)^2$,
    $X_2 \leftarrow x_R Z_2 + X_2 X_S H Z_S, H \leftarrow X_S$,
    $X_S \leftarrow X_S^4 + b Z_S^4, Z_S \leftarrow H^2 Z_S^2$,
    $(X_S : Z_S) := (X_S, Z_S)$.
```

Output:

— $MUL_{b, proj}(k, x_R) = (X_S : Z_S)$.

If protection against side channel attacks is a point of concern, as for the claimant A, where the private key is involved in the evaluation of $MUL_{b,proj}$, the following randomized version of algorithm may be used to implement $MUL_{b,proj}$. In this case, it is necessary to have means to generate random field elements in $F(2^g)$.

H.3 Algorithm based on the Montgomery-ladder — Randomized

Input:

— A positive integer $k = (k_g, \ldots, k_1)$, given in binary representation, with $k_g = 1$;

— The parameter b;

— The field element x_R (challenge).

Output calculation:

a) Pick a random field element $\rho_1 \neq 0_F$;

b) $X_S \leftarrow \rho_1, Z_S \leftarrow 0_F, X_2 \leftarrow \rho_1\ x_R, Z_2 \leftarrow \rho_1$;

c) for i ← g down to 1 do:

```
    if $k_i = 1$ then
        $H \leftarrow Z_S, Z_S \leftarrow (X_S\ Z_2 + X_2\ Z_S)^2$,
        $X_S \leftarrow x_R\ Z_S + X_S\ X_2 H Z_2, H \leftarrow X_2$,
        $X_2 \leftarrow X_2^{\ 4} + b Z_2^{\ 4}, Z_2 \leftarrow H^2\ Z_2^{\ 2}$,
    else
        $H \leftarrow Z_2, Z_2 \leftarrow (X_2\ Z_S + X_S\ Z_2)^2$,
        $X_2 \leftarrow x_R\ Z_2 + X_2\ X_S H Z_S, H \leftarrow X_S$,
        $X_S \leftarrow X_S^{\ 4} + \mathrm{b} Z_S^{\ 4}, Z_S \leftarrow H^2\ Z_S^{\ 2}$;
```

d) Pick a random field element $\rho_2 \neq 0_F$;

e) $X_S \leftarrow \rho_2\ X_S, Z_S \leftarrow \rho_2\ Z_S$;

f) $(X_S : Z_S) := (X_S, Z_S)$.

Output:

— $MUL_{b,proj}(k, x_R) = (X_S : Z_S)$.

NOTE From $MUL_{b,proj}(k, x_R) = (X_S : Z_S)$, one obtains immediately $MUL_{b,aff}(k, x_R) = X_S\ Z_S^{\ -1}$ after executing one division in $F(2^g)$. (This holds for H.2 and H.3.)

H.4 Standard point multiplication approach

Setup: Two field elements a and a' are selected such that $\mathrm{Tr}(a) \neq \mathrm{Tr}(a')$. $E_{twist} = (E_{\{a',b\}})$ is an elliptic curve twisted to $E = (E_{\{a,b\}})$.

Input:

— A positive integer k;

— The parameter b;

— The field element x_R (challenge).

Output calculation:

1) Decide which of the two quadratic equations $y^2 + x_R y = x_R^3 + ax_R^3 + b$ and $y^2 + x_R y = x_R^3 + a'x_R^2 + b$ is solvable and determine a solution y_R .

NOTE See Annex F, Fact 4.

2) *Set* $R := (x_R , y_R)$.

NOTE R is a point either on E or on E_{twist}.

3) Determine $[k]R = (x_S , y_S)$ or $[k]R = (X_S : Y_S : Z_S)$.

NOTE This can be done using any technique to determine the result of point multiplication.

Output:

— $MUL_{b,proj} (k, x_R) = (X_S : Z_S) = (x_S : 1_F)$;

— $MUL_{b,aff}(k, x_R) = x_S = X_S (Z_S)^{-1}$.

Page 26, Bibliography

Add the following to the Bibliography:

[28] Blake I., Seroussi G., Smart N. *Elliptic Curves in Cryptography*, Cambridge University Press, 1999

[29] Brown D. and Gallant R. *The Static Diffie-Hellman Problem*, Cryptology ePrint Archive, Report 2004/306. Available via https://eprint.iacr.org/2004/306

[30] Bock H., Braun M., Dichtl M., Hess E., Heyszl J., Kargl W., Koroschetz H., Meyer B., Seuschek H. *A Milestone towards RFID Products Offering Asymmetric Authentication based on Elliptic Curve Cryptography*. In RFIDSEC-2008 - Proceedings of the 4th Workshop on RFID Security, July 9-11, 2008. Available via http://events.iaik.tugraz.at/RFIDSec08/Papers/index.htm

[31] Braun M., Hess E., Meyer B. *Using Elliptic Curves on RFID Tags*. IJCSNS International Journal of Computer and Network Security, 8(2), 1-9, February 2008

[32] Cheon J.H. *Security Analysis of the Strong Diffie-Hellman Problem,* Eurocrypt '06, LNCS 4004, Springer-Verlag, pp.1-11, 2006

ICS 35.040

Price based on 19 pages