

ISO/IEC JTC 1/SC 27 N15619

Date: 2017-08-10

ISO/IEC 14888-3

ISO/IEC JTC 1/SC 27/WG 2

Secretariat: DIN

**Information technology — Security techniques — Digital signatures with
appendix — Part 3: Discrete logarithm based mechanisms**

*Technologies de l'information — Techniques de sécurité — Signatures numériques avec appendice — Partie 3:
Mécanismes basés sur un logarithme discrète*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 14888-3:2016

<https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016>

Style Definition	... [1]
Field Code Changed	... [2]
Formatted	... [3]
Field Code Changed	
Formatted	... [4]
Field Code Changed	
Formatted	... [5]
Deleted: 2015-11-11	
Formatted: French (Switzerland)	
Field Code Changed	
Formatted	... [6]
Field Code Changed	
Formatted	... [7]
Field Code Changed	
Formatted	... [8]
Field Code Changed	
Formatted	... [9]
Field Code Changed	
Formatted	... [10]
Field Code Changed	
Formatted	... [11]
Field Code Changed	
Formatted	... [12]

Contents

Page

Foreword	10
Introduction	11
1 Scope	14
2 Normative references	14
3 Terms and definitions	14
4 Symbols and abbreviated terms	16
5 General model	18
5.1 Parameter generation process	18
5.2 Signature process	20
5.3 Verification process	23
6 Certificate-based mechanisms	25
6.1 General	25
6.2 DSA	26
6.3 KCDSA	29
6.4 Pointcheval/Vaudenay algorithm	32
6.5 SDSA	34
6.6 EC-DSA	37
6.7 EC-KCDSA	40
6.8 EC-GDSA	43
6.9 EC-RDSA	45
6.10 EC-SDSA	47
6.11 EC-FSDSA	50
7 Identity-based mechanisms	52
7.1 General	52
7.2 IBS-1	53
7.3 IBS-2	56
Annex A (normative) Object identifier	59
Annex B (normative) Conversion functions (I)	62
B.1 Conversion from a field element to an integer: $FE2I(r, x)$	62
B.2 Conversion from an integer to a field element: $I2FE(r, x)$	63
B.3 Conversion from a field element to a binary string: $FE2BS(r, x)$	64
B.4 Conversion from a binary string to an integer: $BS2I(g, x)$	65
B.5 Conversion from an integer to a binary string: $I2BS(g, x)$	65
B.6 Conversion between an integer and an octet string: $I2OS(h, x)$ & $OS2I(h, M)$	65
Annex C (informative) Conversion functions (II)	67
Annex D (normative) Generation of DSA domain parameters	69
D.1 Generation of the prime p and q	69
D.2 Generation of the generator G	70
D.2.1 Unverifiable generation of G	70
D.2.2 Verifiable generation of G	70

Annex E (informative) The Weil and Tate pairings	71
E.1 General	71
E.2 The functions f, g and d	71
E.3 The Weil pairing.....	72
E.4 The Tate pairing.....	72
E.5 The reduced Tate pairing	73
Annex F (informative) Numerical examples	74
F.1 General	74
F.2 DSA mechanism.....	74
F.2.1 Example 1: 2048-bit Prime P, SHA-224	74
F.2.1.1 General	74
F.2.1.2 Parameters.....	74
F.2.1.3 Signature key and verification key.....	75
F.2.1.4 Per message data	75
F.2.1.5 Signature.....	75
F.2.1.6 Verification	75
F.2.2 Example 2: 3072-bit Prime P, SHA-256	75
F.2.2.1 General	75
F.2.2.2 Parameters.....	76
F.2.2.3 Signature key and verification key.....	77
F.2.2.4 Per message data	78
F.2.2.5 Signature.....	78
F.2.2.6 Verification	78
F.3 KCDSA mechanism	78
F.3.1 Example 1: 2048-bit Prime P, 224-bit Prime Q, SHA-224	78
F.3.1.1 General	78
F.3.1.2 Parameters.....	78
F.3.1.3 Signature key and verification key.....	79
F.3.1.4 Per message data	80
F.3.1.5 Signature.....	80
F.3.1.6 Verification	80
F.3.2 Example 2: 3072-bit Prime P, 256-bit Prime Q, SHA-256	80
F.3.2.1 General	80
F.3.2.2 Parameters.....	80
F.3.2.3 Signature key and verification key.....	81
F.3.2.4 Per message data	82
F.3.2.5 Signature.....	82

F.3.2.6 Verification.....	83
F.3.3 Example 3: 2048-bit Prime P, 224-bit Prime Q, SHA-256.....	83
F.3.3.1 General.....	83
F.3.3.2 Parameters.....	83
F.3.3.3 Signature key and verification key.....	84
F.3.3.4 Per message data.....	84
F.3.3.5 Signature.....	84
F.3.3.6 Verification.....	85
F.4 Pointcheval-Vaudenay mechanism.....	85
F.4.1 Example 1: 2048-bit Prime P, SHA-224.....	85
F.4.1.1 General.....	85
F.4.1.2 Parameters.....	85
F.4.1.3 Signature key and verification key.....	86
F.4.1.4 Per message data.....	86
F.4.1.5 Signature.....	86
F.4.1.6 Verification.....	87
F.5 SDSA mechanism.....	87
F.5.1 Example 1: 2048-bit Prime P, SHA-224.....	87
F.5.1.1 General.....	87
F.5.1.2 Parameters.....	87
F.5.1.3 Signature key and verification key.....	88
F.5.1.4 Per message data.....	88
F.5.1.5 Signature.....	89
F.5.1.6 Verification.....	89
F.5.2 Example 2: 2048-bit Prime P, SHA-256.....	90
F.5.2.1 General.....	90
F.5.2.2 Parameters.....	90
F.5.2.3 Signature key and verification key.....	90
F.5.2.4 Per message data.....	91
F.5.2.5 Signature.....	91
F.5.2.6 Verification.....	92
F.6 EC-DSA mechanism.....	92
F.6.1 General.....	92
F.6.2 Example 1: Field F_{2^m} , $m = 191$, SHA-1.....	92
F.6.2.1 Parameters.....	92
F.6.2.2 Signature key and verification key.....	93
F.6.2.3 Per message data.....	93

F.6.2.4 Signature.....	93
F.6.2.5 Verification	93
F.6.3 Example 2: Field F_p , 192-bit Prime P , SHA-1	93
F.6.3.1 Parameters.....	93
F.6.3.2 Signature key and verification key.....	94
F.6.3.3 Per message data	94
F.6.3.4 Signature.....	94
F.6.3.5 Verification	95
F.6.4 Example 3: Field F_{2^m} , $m=283$, SHA-256	95
F.6.4.1 Parameters.....	95
F.6.4.2 Signature key and verification key.....	95
F.6.4.3 Per message data	96
F.6.4.4 Signature.....	96
F.6.4.5 Verification	96
F.6.5 Example 4: Field F_p , 256-bit Prime P , SHA-256	96
F.6.5.1 Parameters.....	96
F.6.5.2 Signature key and verification key.....	97
F.6.5.3 Per message data	97
F.6.5.4 Signature.....	97
F.6.5.5 Verification	97
F.7 EC-KCDSA mechanism.....	98
F.7.1 Example 1: Field F_p , 224-bit Prime P , SHA-224	98
F.7.1.1 General	98
F.7.1.2 Parameters.....	98
F.7.1.3 Signature key and verification key.....	98
F.7.1.4 Per message data	99
F.7.1.5 Signature.....	99
F.7.1.6 Verification	99
F.7.2 Example 2: Field F_p , 256-bit Prime P , SHA-256	99
F.7.2.1 General	99
F.7.2.2 Parameters.....	99
F.7.2.3 Signature key and verification key.....	100
F.7.2.4 Per message data	100
F.7.2.5 Signature.....	101
F.7.2.6 Verification	101
F.7.3 Example 3: Field F_{2^m} , $m=233$, SHA-224	101
F.7.3.1 General	101

F.7.3.2 Parameters	101
F.7.3.3 Signature key and verification key	101
F.7.3.4 Per message data.....	102
F.7.3.5 Signature	102
F.7.3.6 Verification.....	102
F.7.4 Example 4: Field F_{2^m} , $m=233$ (Koblitz Curve), SHA-224	103
F.7.4.1 General.....	103
F.7.4.2 Parameters	103
F.7.4.3 Signature key and verification key	104
F.7.4.4 Per message data.....	104
F.7.4.5 Signature	104
F.7.4.6 Verification.....	104
F.7.5 Example 5: Field F_{2^m} , $m=283$, SHA-256.....	105
F.7.5.1 General.....	105
F.7.5.2 Parameters	105
F.7.5.3 Signature key and verification key	105
F.7.5.4 Per message data.....	105
F.7.5.5 Signature	106
F.7.5.6 Verification.....	106
F.7.6 Example 6: Field F_{2^m} , $m=283$ (Koblitz Curve), SHA-256	106
F.7.6.1 General.....	106
F.7.6.2 Parameters	106
F.7.6.3 Signature key and verification key	107
F.7.6.4 Per message data.....	107
F.7.6.5 Signature	107
F.7.6.6 Verification.....	108
F.8 EC-GDSA mechanism	108
F.8.1 General.....	108
F.8.2 Example 1: Field F_p , 192-bit Prime P , SHA-256.....	108
F.8.2.1 Parameters	108
F.8.2.2 Signature key and verification key	108
F.8.2.3 Per message data.....	108
F.8.2.4 Signature	109
F.8.2.5 Verification.....	109
F.8.3 Example 2: Field F_p , 224-bit Prime P , SHA-224.....	109
F.8.3.1 Parameters	109
F.8.3.2 Signature key and verification key	109

F.8.3.3 Per message data	110
F.8.3.4 Signature.....	110
F.8.3.5 Verification	110
F.8.4 Example 3: Field F_p , 256-bit Prime P , SHA-256	110
F.8.4.1 Parameters.....	110
F.8.4.2 Signature key and verification key.....	111
F.8.4.3 Per message data	111
F.8.4.4 Signature.....	111
F.8.4.5 Verification	112
F.9 EC-RDSA mechanism.....	112
F.9.1 Example 1: Field F_p , 256-bit Prime P , SHA-256	112
F.9.1.1 General	112
F.9.1.2 Parameters.....	112
F.9.1.3 Signature key and verification key.....	112
F.9.1.4 Per message data	113
F.9.1.5 Signature.....	113
F.9.1.6 Verification	113
F.9.2 Example 2: Field F_p , 512-bit Prime P , SHA-512	113
F.9.2.1 General	113
F.9.2.2 Parameters.....	114
F.9.2.3 Signature key and verification key.....	114
F.9.2.4 Per message data	114
F.9.2.5 Signature.....	115
F.9.2.6 Verification	115
F.10 EC-SDSA mechanism	116
F.10.1 Example 1: Field F_p , 256-bit Prime P , SHA-256.....	116
F.10.1.1 General.....	116
F.10.1.2 Parameters	116
F.10.1.3 Signature key and verification key	116
F.10.1.4 Per message data.....	116
F.10.1.5 Signature	118
F.10.1.6 Verification.....	118
F.10.2 Example 2: Field F_p , 384-bit Prime P , SHA-384.....	118
F.10.2.1 General.....	118
F.10.2.2 Parameters	118
F.10.2.3 Signature key and verification key	119
F.10.2.4 Per message data.....	119

F.10.2.5	Signature.....	120
F.10.2.6	Verification.....	120
F.11	EC-FSDSA mechanism	121
F.11.1	Example 1: Field F_p , 256-bit Prime P , SHA-256	121
F.11.1.1	General	121
F.11.1.2	Parameters.....	121
F.11.1.3	Signature key and verification key.....	122
F.11.1.4	Per message data	122
F.11.1.5	Signature.....	122
F.11.1.6	Verification.....	122
F.11.2	Example 2: Field F_p , 384-bit Prime P , SHA-384	123
F.11.2.1	General	123
F.11.2.2	Parameters.....	123
F.11.2.3	Signature key and verification key.....	123
F.11.2.4	Per message data	124
F.11.2.5	Signature.....	124
F.11.2.6	Verification.....	124
F.12	IBS-1 mechanism	125
F.12.1	Example 1: Field F_p , 512-bit Prime p , SHA-1	125
F.12.1.1	General	125
F.12.1.2	Parameters.....	125
F.12.1.3	Signature key and verification	126
F.12.1.4	Per message data	127
F.12.1.5	Signature.....	127
F.12.1.6	Verification.....	128
F.12.2	Example 2: Field F_p , 512-bit Prime p , SHA-1	128
F.12.2.1	General	128
F.12.2.2	Parameters.....	128
F.12.2.3	Signature key and verification key.....	129
F.12.2.4	Per message data	130
F.12.2.5	Signature.....	130
F.12.2.6	Verification.....	130
F.13	IBS-2 mechanism	131
F.13.1	Example 1: Field F_p , 512-bit Prime p , SHA-1	131
F.13.1.1	General	131
F.13.1.2	Parameters.....	131
F.13.1.3	Signature key and verification key.....	132

F.13.1.4	Per message data.....	132
F.13.1.5	Signature	133
F.13.1.6	Verification	133
Annex G (informative)	Comparison of the signature schemes.....	135
G.1	Symbols and abbreviated terms for comparing the signature schemes	135
G.2	Comparison of the signature schemes	135
Annex H (informative)	Claimed features for choosing a mechanism	137
Bibliography	138

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 14888-3:2016

<https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016>

Deleted: 2016

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.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

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).

Formatted: English (U.K.)

Formatted: Default Paragraph Font

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).

Formatted: English (U.K.)

Formatted: Default Paragraph Font

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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

Formatted: Default Paragraph Font, English (U.K.)

This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

Deleted: The committee responsible for this

Deleted: is

This third edition cancels and replaces the second edition (ISO/IEC 14888-3:2006), which has been technically revised. It also incorporates the Amendments ISO/IEC 14888-3:2006/Amd 1:2010 and ISO/IEC 14888-3:2006/Amd 2:2012 and the Technical Corrigenda ISO/IEC 14888-3:2006/Cor 1:2007 and ISO/IEC 14888-3:2006/Cor 2:2009.

This corrected version of ISO/IEC 14888-3:2016 incorporates the following corrections:

Deleted: consists of

— the formula has been changed in 5.1.1.2;

Deleted: parts, under

— " G^{x-1} " has been changed to " G^{x-1} " in 6.3.1 and 6.3.3;

Formatted: List Continue 1, Don't keep with next, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

— " β " has been changed to " β " in 6.7.1, 6.7.4.4 and 6.7.4.5;

Deleted: general title *Information technology — Security techniques — Digital signatures with appendix:*

— the reference has been changed in 6.9.1;

Deleted: — Part 1: General¶
— Part 2: Integer factorization based mechanisms¶
— Part 3: Discrete logarithm based mechanisms¶

— the code for K has been changed in F.9.2.4.

A list of all parts in the ISO/IEC 14888 series can be found on the ISO website.

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation and data integrity. A digital signature mechanism satisfies the following requirements.

- Given either or both of the following two things:
 - the verification key, but not the signature key;
 - a set of signatures on a sequence of messages that an attacker has adaptively chosen;it should be computationally infeasible for the attacker
 - to produce a valid signature on a new message,
 - in some circumstances, to produce a new signature on a previously signed message, or
 - to recover the signature key;
- it should be computationally infeasible, even for the signer, to find two different messages with the same signature.

NOTE 1 Computational feasibility depends on the specific security requirements and environment.

NOTE 2 In some applications, producing a new signature on a previously signed message without knowing the signature key is allowed. One example of such applications is a membership credential in an anonymous digital signature mechanism as specified in ISO/IEC 20008.

Digital signature mechanisms are based on asymmetric cryptographic techniques and involve the following three basic operations:

- a process for generating pairs of keys, where each pair consists of a private signature key and the corresponding public verification key;
- a process that uses the signature key, called the signature process;
- a process that uses the verification key, called the verification process.

The following are the two types of digital signature mechanisms:

- when, for a given signature key, any two signatures produced for the same message are always identical, the mechanism is said to be deterministic (or non-randomized) (see ISO/IEC 14888-1 for further details);
- when, for a given message and signature key, any two applications of the signature process produce (with high probability) two distinct signatures, the mechanism is said to be randomized (or non-deterministic).

The mechanisms specified in this part of ISO/IEC 14888 are all randomized.

Digital signature mechanisms can also be divided into the following two categories:

- when the whole message has to be stored and/or transmitted along with the signature, the mechanism is termed a "signature mechanism with appendix" (such mechanisms are the subject of ISO/IEC 14888);

- when the whole message, or part of it, can be recovered from the signature, the mechanism is termed a "signature mechanism giving message recovery" (ISO/IEC 9796 specifies mechanisms in this category).

The verification of a digital signature requires access to the signing entity's verification key. It is, thus, essential for a verifier to be able to associate the correct verification key with the signing entity, or more precisely, with (parts of) the signing entity's identification data. This association between the signer's identification data and the signer's public verification key can either be guaranteed by an outside entity or mechanism, or the association can be somehow inherent in the verification key itself. In the former case, the scheme is said to be "certificate-based." In the latter case, the scheme is said to be "identity based." Typically, in an identity-based scheme, the verifier can calculate the signer's public verification key from the signer's identification data. The digital signature mechanisms specified in this part of ISO/IEC 14888 are classified into certificate-based and identity-based mechanisms.

NOTE 3 For certificate-based mechanisms, various PKI standards can be used as the basis of key management. For further information, see ISO/IEC 9594-8 (also known as X.509), ISO/IEC 11770-3 and ISO/IEC 15945.

The security of a signature mechanism is based on an intractable computational problem, i.e. a problem for which, given current knowledge, finding a solution is computationally infeasible, such as the factorization problem and the discrete logarithm problem. This part of ISO/IEC 14888 specifies digital signature mechanisms with appendix based on the discrete logarithm problem, and ISO/IEC 14888-2 specifies digital signature mechanisms with appendix based on the factorization problem.

NOTE 4 The first edition of ISO/IEC 14888 grouped identity-based mechanisms into ISO/IEC 14888-2 and certificate-based mechanisms into ISO/IEC 14888-3, with both parts covering mechanisms based on both the discrete logarithm and the factorization problems. Since the second edition was published, the mechanisms have been reorganized. ISO/IEC 14888-2 now contains integer factoring-based mechanisms, and this part of ISO/IEC 14888 now contains discrete logarithm based mechanisms.

This part of ISO/IEC 14888 includes 12 mechanisms, two of which were in ISO/IEC 14888-3:1998, three of which were from ISO/IEC 15946-2:2002 and three of which were added in ISO/IEC 14888-3:2006. The Elliptic Curve Russian Digital Signature Algorithm (EC-RDSA) and three mechanisms based on Schnorr digital signature are added in ISO/IEC 14888-3:2006/Amd.1:2010.

The mechanisms specified in this part of ISO/IEC 14888 use a collision resistant hash-function to hash the message being signed (possibly in more than one part). ISO/IEC 10118 specifies hash-functions.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 14888 may involve the use of patents.

The ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holder of these patent rights has assured the ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with the ISO and IEC. Information regarding relevant patents is given in the following:

Certicom Corp.

4701 Tahoe Blvd., Building A, Mississauga, ON L4W0B5 Canada.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 14888 may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (<http://patents.iec.ch>) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

NOTE 5 The mechanisms of EC-DSA, EC-GDSA, EC-RDSA and EC-FSDSA may be vulnerable to a key substitution attack.^[10] The attack is realized if an adversary can find two distinct public keys and one signature such that the signature is valid for both public keys. There are several approaches of avoiding this attack and its possible impact on the security of a cryptographic system. For example, the public key corresponding to the private signing key can be added into the message to be signed.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 14888-3:2016

<https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016>

Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms

1 Scope

This part of ISO/IEC 14888 specifies digital signature mechanisms with appendix whose security is based on the discrete logarithm problem.

This part of ISO/IEC 14888 provides

- a general description of a digital signature with appendix mechanism, and
- a variety of mechanisms that provide digital signatures with appendix.

For each mechanism, this part of ISO/IEC 14888 specifies

- the process of generating a pair of keys,
- the process of producing signatures, and
- the process of verifying signatures.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10118-3, *Information technology — Security techniques — Hash-functions*

ISO/IEC 14888-1:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 14888-1 and the following apply.

3.1

finite commutative group

finite set E with the binary operation "*" such that

- for all group elements $a, b \in E$, $a * b \in E$;
- for all group elements $a, b, c \in E$, $(a * b) * c = a * (b * c)$;
- there exists a group element $e \in E$ with $e * a = a$ for all $a \in E$, where e is called the identity element of the group;

- for all group elements $a \in E$, there exists a group element $b \in E$ with $b * a = e$;
- for all group elements $a, b \in E$, $a * b = b * a$

Note 1 to entry: In some cases, such as when E is the set of points on an elliptic curve, arithmetic in the finite set E is described with additive notation.

3.2 cyclic group

finite commutative group (3.1), E , of n elements that contains a group element $a \in E$, called the generator, of order n

3.3 elliptic curve group

cyclic group (3.2) defined on the points of an elliptic curve over a finite field

Note 1 to entry: Let $F = GF(r)$ denote the Galois field with cardinality, r , where either r is an odd prime, p , or r is equal to 2^m , for some positive integer, m .

An elliptic curve defined over F can be determined by an affine curve formula, either of the form $y^2 = x^3 + a_1x + a_2$ (when $r = p$ for some odd prime p) or of the form $y^2 + xy = x^3 + a_1x^2 + a_2$ (when $r = 2^m$ for some positive integer m), where the coefficients a_1 and a_2 are (appropriately chosen) elements of F . The corresponding elliptic curve E consists of a collection of certain affine points from $F \times F$ together with a special (non-affine) point "at infinity".

An affine point P of E is one that can be represented as an ordered pair $(P_x, P_y) \in F \times F$, such that the selection of $x = P_x$ and $y = P_y$ satisfies the given affine curve formula when the indicated arithmetic is performed in the field, F .

Let "+" denote the binary operation known as "elliptic-curve addition", defined for (most) affine points of E by the well-known secant-and-tangent rules. Once the collection of affine points of E is augmented by 0_E , a special point of E "at infinity" that serves as the identity element for "+" (but is not represented as an ordered pair), the set E together with the binary operation "+" forms a finite, commutative, elliptic-curve group, E .

Note 2 to entry: The cardinality of the elliptic-curve group, E , is one more than the number of ordered pairs in $F \times F$ that satisfy the affine curve formula for E .

3.4 order (of a group element a)

least positive integer n such that $a^n = e$, where e is the identity element of the group, a^n is defined recursively such that $a^0 = e$ and $a^n = a * a^{n-1}$ ($n > 0$), and $*$ is the group operation

3.5 pairing

function which takes two elements, P and Q , from an *elliptic curve group* (3.3) over a finite field, G_1 , as input, and produces an element from another *cyclic group* (3.2) over a finite field, G_2 , as output, and which has the following two properties (where it is assumed that the cyclic groups, G_1 and G_2 have order q , for some prime q , and for any two elements P, Q , the output of the pairing function is written as $\langle P, Q \rangle$)

- Bilinearity: If P, P_1, P_2, Q, Q_1, Q_2 are elements of G_1 , and a is an integer satisfying $1 \leq a \leq q - 1$, then

$$\langle P_1 + P_2, Q \rangle = \langle P_1, Q \rangle * \langle P_2, Q \rangle,$$

$$\langle P, Q_1 + Q_2 \rangle = \langle P, Q_1 \rangle * \langle P, Q_2 \rangle, \text{ and}$$