

Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 22, 2016

S. Josefsson
SJD AB
I. Liusvaara
Independent
January 19, 2016

Edwards-curve Digital Signature Algorithm (EdDSA)
draft-irtf-cfrg-eddsa-02

Abstract

The elliptic curve signature scheme Edwards-curve Digital Signature Algorithm (EdDSA) is described. The algorithm is instantiated with recommended parameters for the Curve25519 and Curve448 curves. An example implementation and test vectors are provided.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 22, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

Table of Contents

1.	Introduction	3
2.	Notation and Conventions	4
3.	EdDSA Algorithm	5
3.1.	Encoding	6
3.2.	Keys	7
3.3.	Sign	7
3.4.	Verify	7
4.	PureEdDSA, HashEdDSA and Naming	7
5.	EdDSA Instances	8
5.1.	Ed25519ph and Ed25519	8
5.1.1.	Modular arithmetic	9
5.1.2.	Encoding	9
5.1.3.	Decoding	9
5.1.4.	Point addition	10
5.1.5.	Key Generation	11
5.1.6.	Sign	11
5.1.7.	Verify	12
5.2.	Ed448ph and Ed448	12
5.2.1.	Modular arithmetic	13
5.2.2.	Encoding	13
5.2.3.	Decoding	13
5.2.4.	Point addition	14
5.2.5.	Key Generation	14
5.2.6.	Sign	15
5.2.7.	Verify	15
6.	Ed25519 Python illustration	16
7.	Test Vectors	20
7.1.	Test Vectors for Ed25519	20
7.2.	Test Vectors for Ed25519ph	24
7.3.	Test Vectors for Ed448	24
7.4.	Test Vectors for Ed448ph	31
8.	Acknowledgements	33
9.	IANA Considerations	33
10.	Security Considerations	33
10.1.	Side-channel leaks	33
10.2.	Use of contexts	34
10.3.	Mixing different prehashes	34
10.4.	Signing large amounts of data at once	34
11.	References	35
11.1.	Normative References	35
11.2.	Informative References	35

Appendix A.	Ed25519/Ed448 Python Library	36
Appendix B.	Library driver	46
Authors' Addresses	47

[1.](#) Introduction

The Edwards-curve Digital Signature Algorithm (EdDSA) is a variant of Schnorr's signature system with (possibly Twisted) Edwards curves. EdDSA needs to be instantiated with certain parameters and this document describe some recommended variants.

To facilitate adoption in the Internet community of EdDSA, this document describe the signature scheme in an implementation-oriented way, and provide sample code and test vectors.

The advantages with EdDSA include:

1. High-performance on a variety of platforms.
2. Does not require the use of a unique random number for each signature.
3. More resilient to side-channel attacks.
4. Small public keys (32 or 57 bytes) and signatures (64 or 114 bytes).
5. The formulas are "strongly unified", i.e., they are valid for all points on the curve, with no exceptions. This obviates the need for EdDSA to perform expensive point validation on untrusted public values.
6. Collision resilience, meaning that hash-function collisions do not break this system. (Only holds for PureEdDSA.)

The original EdDSA paper [[EDDSA](#)] and the generalized version described in "EdDSA for more curves" [[EDDSA2](#)] provide further background. The [[I-D.irtf-cfrg-curves](#)] document discuss specific curves, including Curve25519 [[CURVE25519](#)] and Ed448-Goldilocks [[ED448](#)].

Ed25519 is intended to operate at around the 128-bit security level, and Ed448 at around the 224-bit security level. A large quantum computer would be able to break both. Reasonable projections of the abilities of classical computers conclude that Ed25519 is perfectly safe. Ed448 is provided for those applications with relaxed performance requirements and where there is a desire to hedge against analytical attacks on elliptic curves.

[2.](#) Notation and Conventions

FIXME: make sure this is aligned with irtf-cfrg-curves

The following notation is used throughout the document:

$\text{GF}(p)$ --- finite field with p elements

x^y --- x multiplied by itself y times

B --- generator of the group or subgroup of interest

$[n]B$ --- B added to itself n times.

h_i --- the i 'th bit of h

$a || b$ --- (bit-)string a concatenated with (bit-)string b

$a \leq b$ --- a is less than or equal to b

$i+j$ --- sum of i and j

$i \times j$ --- multiplication of i and j

$i \times j$ --- cartesian product of i and j

$\text{SHAKE256}(x, y)$ is the y first octets of SHAKE256 [[FIPS202](#)] output for input x .

OCTET(x) is the octet with value x

OLEN(x) is the number of octets in string x

dom(x, y) is "SigEd448" || octet(x) || octet(OLEN(y)) || y, where x is in range 0-255 and y is octet string of at most 255 octets. "SigEd448" is in ASCII (8 octets).

Use of parenthesis (i.e., '(' and ')') are used to group expressions, in order to avoid having the description depend on a binding order between operators.

Bit strings are converted to octet strings by taking bits from left to right and packing those from least significant bit of each octet to most significant bit, and moving to the next octet when each octet fills up. The conversion from octet string to bit string is the reverse of this process. E.g. the 16-bit bit string:

b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15

Is converted into two octets x0 and x1 (in this order) as:

$$x0 = b7*128+b6*64+b5*32+b4*16+b3*8+b2*4+b1*2+b0$$
$$x1 = b15*128+b14*64+b13*32+b12*16+b11*8+b10*4+b9*2+b8$$

Little-endian encoding into bits places bits from left to right from least significant to most significant. If combined with bit string to octet string conversion defined above, this results in little-endian encoding into octets (if length is not multiple of 8, the most significant bits of last octet remain unused).

[3.](#) EdDSA Algorithm

EdDSA is a digital signature system with eleven parameters.

The generic EdDSA digital signature system with its eleven input parameters is not intended to be implemented directly. Choosing parameters is critical for secure and efficient operation. Instead, you would implement a particular parameter choice for EdDSA (such as Ed25519 or Ed448), sometimes slightly generalized to achieve code reuse to cover Ed25519 and Ed448.

Therefore, a precise explanation of the generic EdDSA is thus not particularly useful for implementers. For background and completeness, a succinct description of the generic EdDSA algorithm is given here.

The definition of some parameters, such as n and c , may help to explain some non-intuitive steps of the algorithm.

This description closely follows [\[EDDSA2\]](#).

EdDSA has eleven parameters:

1. An odd prime power p . EdDSA uses an elliptic curve over the finite field $GF(p)$.
2. An integer b with $2^{(b-1)} > p$. EdDSA public keys have exactly b bits, and EdDSA signatures have exactly $2*b$ bits. b is recommended to be multiple of 8, so public key and signature lengths are integral number of octets.
3. A $(b-1)$ -bit encoding of elements of the finite field $GF(p)$.
4. A cryptographic hash function H producing $2*b$ -bit output. Conservative hash functions are recommended and do not have much impact on the total cost of EdDSA.

5. An integer c that is 2 or 3. Secret EdDSA scalars are multiples of 2^c . The integer c is the base-2 logarithm of the so called cofactor.
6. An integer n with $c \leq n < b$. Secret EdDSA scalars have exactly $n + 1$ bits, with the top bit (the 2^n position) always set and the bottom c bits always cleared.
7. A nonzero square element a of $GF(p)$. The usual recommendation for best performance is $a = -1$ if $p \bmod 4 = 1$, and $a = 1$ if $p \bmod 4 = 3$.
8. An element $B \neq (0,1)$ of the set $E = \{ (x,y) \text{ is a member of } GF(p) \times GF(p) \text{ such that } a * x^2 + y^2 = 1 + d * x^2 * y^2 \}$.

9. An odd prime l such that $[l]B = 0$ and $2^c * l = \#E$. The number $\#E$ (the number of points on the curve) is part of the standard data provided for an elliptic curve E .
10. A "prehash" function PH . PureEdDSA means EdDSA where PH is the identity function, i.e., $PH(M) = M$. HashEdDSA means EdDSA where PH generates a short output, no matter how long the message is; for example, $PH(M) = \text{SHA-512}(M)$.

Points on the curve form a group under addition, $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, with the formulas

$$x_3 = \frac{x_1 * y_2 + x_2 * y_1}{1 + d * x_1 * x_2 * y_1 * y_2}, \quad y_3 = \frac{y_1 * y_2 - a * x_1 * x_2}{1 - d * x_1 * x_2 * y_1 * y_2}$$

The neutral element in the group is $(0, 1)$.

Unlike many other curves used for cryptographic applications, these formulas are "strongly unified": they are valid for all points on the curve, with no exceptions. In particular, the denominators are non-zero for all input points.

There are more efficient formulas, which are still strongly unified, which use homogeneous coordinates to avoid the expensive modulo p inversions. See [[Faster-ECC](#)] and [[Edwards-revisited](#)].

3.1. Encoding

An integer $0 < S < l - 1$ is encoded in little-endian form as a b -bit string $\text{ENC}(S)$.

An element (x, y) of E is encoded as a b -bit string called $\text{ENC}(x, y)$ which is the $(b-1)$ -bit encoding of y concatenated with one bit that is 1 if x is negative and 0 if x is not negative.

The encoding of $\text{GF}(p)$ is used to define "negative" elements of $\text{GF}(p)$: specifically, x is negative if the $(b-1)$ -bit encoding of x is lexicographically larger than the $(b-1)$ -bit encoding of $-x$.

3.2. Keys

An EdDSA secret key is a b -bit string k . Let the hash $H(k) = (h_0, h_1, \dots, h_{(2b-1)})$ determine an integer s which is 2^n plus the sum of $m = 2^i * h_i$ for all integer i , $c \leq i \leq n$. Let s determine the multiple $A = [s]B$. The EdDSA public key is $ENC(A)$. The bits $h_b, \dots, h_{(2b-1)}$ is used below during signing.

3.3. Sign

The EdDSA signature of a message M under a secret key k is defined as the PureEdDSA signature of $PH(M)$. In other words, EdDSA simply uses PureEdDSA to sign $PH(M)$.

The PureEdDSA signature of a message M under a secret key k is the $2*b$ -bit string $ENC(R) || ENC(S)$. R and S are derived as follows. First define $r = H(h_b, \dots, h_{(2b-1)}, M)$ interpreting $2*b$ -bit strings in little-endian form as integers in $\{0, 1, \dots, 2^{(2*b)} - 1\}$. Let $R = [r]B$ and $S = (r + H(ENC(R) || ENC(A) || P(M))) s \bmod l$. The s used here is from the previous section.

3.4. Verify

To verify a PureEdDSA signature $ENC(R) || ENC(S)$ on a message M under a public key $ENC(A)$, proceed as follows. Parse the inputs so that A and R is an element of E , and S is a member of the set $\{0, 1, \dots, l-1\}$. Compute $h = H(ENC(R) || ENC(A) || M)$ and check the group equation $[2^c * S] B = 2^c * R + [2^c * h] A$ in E . Verification is rejected if parsing fails or the group equation does not hold.

EdDSA verification for a message M is defined as PureEdDSA verification for $PH(M)$.

4. PureEdDSA, HashEdDSA and Naming

One of the parameters of the EdDSA algorithm is the "prehash" function. This may be the identity function, resulting in an algorithm called PureEdDSA, or a collision-resistant hash function such as SHA-512, resulting in an algorithm called HashEdDSA.

be more important between 1) collision resilience, and 2) a single-pass interface for creating signatures. The collision resilience property means EdDSA is secure even if it is feasible to compute collisions for the hash function. The single-pass interface property means that only one pass over the input message is required to create a signature. PureEdDSA requires two passes over the input. Many existing APIs, protocols and environments assume digital signature algorithms only need one pass over the input, and may have API or bandwidth concerns supporting anything else.

Note that single-pass verification is not possible with most uses of signatures, no matter which signature algorithm is chosen. This is because most of the time one can't process the message until signature is validated, which needs a pass on the entire message.

This document specifies parameters resulting in the HashEdDSA variants Ed25519ph and Ed448ph, and the PureEdDSA variants Ed25519 and Ed448.

[5.](#) EdDSA Instances

This section instantiates the general EdDSA algorithm for the Curve25519 and Ed448 curves, each for the PureEdDSA and HashEdDSA variants. Thus four different parameter sets are described.

[5.1.](#) Ed25519ph and Ed25519

Ed25519 is PureEdDSA instantiated with: p as the prime $2^{255}-19$, $b=256$, the 255-bit encoding of $GF(p)$ being the little-endian encoding of $\{0, 1, \dots, p-1\}$, H being SHA-512 [\[RFC4634\]](#), c being 3, n being 254, a being -1 , $d = -121665/121666$ which is a member of $GF(p)$, and B is the unique point $(x, 4/5)$ in E for which x is "positive", which with the encoding used simply means that the least significant bit of x is 0, l is the prime $2^{252} + 27742317777372353535851937790883648493$.

Ed25519ph is the same but with PH being SHA-512 instead, i.e., the input is hashed using SHA-512 before signing with Ed25519.

Written out explicitly, B is the point (15112221349535400772501151409588531511454012693041857206046113283949847762202, 46316835694926478169428394003475163141307993866256225615783033603165251855960).

The values for p , a , d , B and l follows from the "edwards25519" values in [\[I-D.irtf-cfrg-curves\]](#).

The curve used is equivalent to Curve25519 [[CURVE25519](#)], under a change of coordinates, which means that the difficulty of the discrete logarithm problem is the same as for Curve25519.

[5.1.1.](#) Modular arithmetic

For advice on how to implement arithmetic modulo $p = 2^{255} - 19$ efficiently and securely, see Curve25519 [[CURVE25519](#)]. For inversion modulo p , it is recommended to use the identity $x^{-1} = x^{(p-2)} \pmod{p}$.

For point decoding or "decompression", square roots modulo p are needed. They can be computed using the Tonelli-Shanks algorithm, or the special case for $p \equiv 5 \pmod{8}$. To find a square root of a , first compute the candidate root $x = a^{((p+3)/8)} \pmod{p}$. Then there are three cases:

$x^2 = a \pmod{p}$. Then x is a square root.

$x^2 = -a \pmod{p}$. Then $2^{((p-1)/4)} x$ is a square root.

a is not a square modulo p .

[5.1.2.](#) Encoding

All values are coded as octet strings, and integers are coded using little endian convention. I.e., a 32-octet string $h[0], \dots, h[31]$ represents the integer $h[0] + 2^8 h[1] + \dots + 2^{248} h[31]$.

A curve point (x,y) , with coordinates in the range $0 \leq x,y < p$, is coded as follows. First encode the y -coordinate as a little-endian string of 32 octets. The most significant bit of the final octet is always zero. To form the encoding of the point, copy the least significant bit of the x -coordinate to the most significant bit of the final octet.

[5.1.3.](#) Decoding

Decoding a point, given as a 32-octet string, is a little more complicated.

1. First interpret the string as an integer in little-endian representation. Bit 255 of this number is the least significant bit of the x -coordinate, and denote this value x_0 . The y -coordinate is recovered simply by clearing this bit. If the resulting value is $\geq p$, decoding fails.

2. To recover the x coordinate, the curve equation implies $x^2 = (y^2 - 1) / (d y^2 + 1) \pmod{p}$. The denominator is always nonzero mod p. Let $u = y^2 - 1$ and $v = d y^2 + 1$. To compute the square root of (u/v) , the first step is to compute the candidate root $x = (u/v)^{((p+3)/8)}$. This can be done using the following trick, to use a single modular powering for both the inversion of v and the square root:

$$x = (u/v)^{(p+3)/8} = u^3 v^{(p-5)/8} (u v^7)^{-1} \pmod{p}$$

3. Again, there are three cases:

1. If $v x^2 = u \pmod{p}$, x is a square root.
 2. If $v x^2 = -u \pmod{p}$, set $x \leftarrow x \cdot 2^{((p-1)/4)}$, which is a square root.
 3. Otherwise, no square root exists modulo p, and decoding fails.
4. Finally, use the x_0 bit to select the right square root. If $x = 0$, and $x_0 = 1$, decoding fails. Otherwise, if $x_0 \neq x \bmod 2$, set $x \leftarrow p - x$. Return the decoded point (x,y) .

5.1.4. Point addition

For point addition, the following method is recommended. A point (x,y) is represented in extended homogeneous coordinates (X, Y, Z, T) , with $x = X/Z$, $y = Y/Z$, $x y = T/Z$.

The following formulas for adding two points, $(x_3,y_3) = (x_1,y_1)+(x_2,y_2)$ are described in [\[Edwards-revisited\]](#), section 3.1. They are strongly unified, i.e., they work for any pair of valid input points.

$$\begin{aligned} A &= (Y_1 - X_1) * (Y_2 - X_2) \\ B &= (Y_1 + X_1) * (Y_2 + X_2) \\ C &= T_1 * 2 * d * T_2 \end{aligned}$$

$D = Z1 * 2 * Z2$
 $E = B - A$
 $F = D - C$
 $G = D + C$
 $H = B + A$
 $X3 = E * F$
 $Y3 = G * H$
 $T3 = E * H$
 $Z3 = F * G$

[5.1.5.](#) Key Generation

The secret is 32 octets (256 bits, corresponding to b) of cryptographically-secure random data. See [\[RFC4086\]](#) for a discussion about randomness.

The 32-byte public key is generated by the following steps.

1. Hash the 32-byte secret using SHA-512, storing the digest in a 64-octet large buffer, denoted h . Only the lower 32 bytes are used for generating the public key.
2. Prune the buffer: The lowest 3 bits of the first octet are cleared, the highest bit of the last octet is cleared, and second highest bit of the last octet is set.
3. Interpret the buffer as the little-endian integer, forming a secret scalar a . Perform a fixed-base scalar multiplication $[a]B$.
4. The public key A is the encoding of the point $[a]B$. First encode the y coordinate (in the range $0 \leq y < p$) as a little-endian string of 32 octets. The most significant bit of the final octet is always zero. To form the encoding of the point $[a]B$, copy the least significant bit of the x coordinate to the most significant bit of the final octet. The result is the public key.

[5.1.6.](#) Sign

The inputs to the signing procedure is the secret key, a 32-octet string, and a message M of arbitrary size.

1. Hash the secret key, 32-octets, using SHA-512. Let h denote the resulting digest. Construct the secret scalar a from the first half of the digest, and the corresponding public key A , as described in the previous section. Let prefix denote the second half of the hash digest, $h[32], \dots, h[63]$.
2. Compute $\text{SHA-512}(\text{prefix} || M)$, where M is the message to be signed. Interpret the 64-octet digest as a little-endian integer r .
3. Compute the point $[r]B$. For efficiency, do this by first reducing r modulo l , the group order of B . Let the string R be the encoding of this point.
4. Compute $\text{SHA512}(R || A || M)$, and interpret the 64-octet digest as a little-endian integer k .

5. Compute $S = (r + k * a) \bmod l$. For efficiency, again reduce k modulo l first.
6. Form the signature of the concatenation of R (32 octets) and the little-endian encoding of S (32 octets, three most significant bits of the final octet are always zero).

[5.1.7.](#) Verify

1. To verify a signature on a message M , first split the signature into two 32-octet halves. Decode the first half as a point R , and the second half as an integer S , in the range $0 \leq s < l$. If the decoding fails, the signature is invalid.
2. Compute $\text{SHA512}(R || A || M)$, and interpret the 64-octet digest as a little-endian integer k .
3. Check the group equation $[8][S]B = [8]R + [8][k]A$. It's sufficient, but not required, to instead check $[S]B = R + [k]A$.

[5.2.](#) Ed448ph and Ed448

Ed448 is PureEdDSA instantiated with p as the prime $2^{448} - 2^{224} - 1$, $b=456$, the 455-bit encoding of $\text{GF}(2^{448}-2^{224}-1)$ is the usual little-endian encoding of $\{0, 1, \dots, 2^{448} - 2^{224} - 2\}$, H is

Shake256(dom(phflag,context)), phflag being 0, c being 2, n being 448, a being 1, d being - 39081, B is (X(P), Y(P)), and l is the prime $2^{448} - 13818066809895115352007386748515426880336692474882178609894547503885$.

Ed448ph is the same but with P being SHAKE256(dom(2,context)||x) and phflag being 1, i.e., the input is hashed before signing with Ed448 with a hash constant modified.

The values of p, a, d, X(p), Y(p), and l are taken from curve named "edwards448" in [[I-D.irtf-cfrg-curves](#)].

Value of context is set by signer and verifier (maximum of 255 octets, the default is empty string) and has to match octet by octet for verification to be successful.

The curve is equivalent to Ed448-Goldilocks under change of basepoint, which preserves difficulty of the discrete logarithm.

[5.2.1.](#) Modular arithmetic

For advice on how to implement arithmetic modulo $p = 2^{448} - 2^{224} - 1$ efficiently and securely, see [[ED448](#)]. For inversion modulo p, it is recommended to use the identity $x^{-1} = x^{(p-2)} \pmod{p}$.

For point decoding or "decompression", square roots modulo p are needed. They can be computed by first computing candidate root $x = a^{(p+1)/4} \pmod{p}$ and then checking if $x^2 = a$. If it is, then x is square root of a.

[5.2.2.](#) Encoding

All values are coded as octet strings, and integers are coded using little endian convention. I.e., a 57-octet string $h[0], \dots, h[56]$ represents the integer $h[0] + 2^8 h[1] + \dots + 2^{448} h[56]$.

A curve point (x,y), with coordinates in the range $0 \leq x, y < p$, is

coded as follows. First encode the y-coordinate as a little-endian string of 57 octets. The final octet is always zero. To form the encoding of the point, copy the least significant bit of the x-coordinate to the most significant bit of the final octet.

5.2.3. Decoding

Decoding a point, given as a 57-octet string, is a little more complicated.

1. First interpret the string as an integer in little-endian representation. Bit 455 of this number is the least significant bit of the x-coordinate, and denote this value x_0 . The y-coordinate is recovered simply by clearing this bit. If the resulting value is $\geq p$, decoding fails.
2. To recover the x coordinate, the curve equation implies $x^2 = (y^2 - 1) / (d y^2 - 1) \pmod{p}$. The denominator is always nonzero mod p . Let $u = y^2 - 1$ and $v = d y^2 - 1$. To compute the square root of (u/v) , the first step is to compute the candidate root $x = (u/v)^{((p+1)/4)}$. This can be done using the following trick, to use a single modular powering for both the inversion of v and the square root:

$$x = (u/v)^{(p+1)/4} = u^{(p+1)/4} v^{-1/4} \pmod{p}$$

3. If $v * x^2 = u$, the recovered x coordinate is x . Otherwise no square root exists, and the decoding fails.

4. Finally, use the x_0 bit to select the right square root. If $x = 0$, and $x_0 = 1$, decoding fails. Otherwise, if $x_0 \neq x \bmod 2$, set $x \leftarrow p - x$. Return the decoded point (x,y) .

5.2.4. Point addition

For point addition, the following method is recommended. A point (x,y) is represented in projective coordinates (X, Y, Z) , with $x = X/Z$, $y = Y/Z$.

The following formulas for adding two points, $(x_3,y_3) =$

$(x_1, y_1) + (x_2, y_2)$ are described in [FIXME: Add reference]. They are strongly unified, i.e., they work for any pair of valid input points.

```
A = Z1*Z2
B = A^2
C = X1*X2
D = Y1*Y2
E = d*C*D
F = B-E
G = B+E
H = (X1+X2)*(Y1+Y2)
X3 = A*G*(H-C-D)
Y3 = A*G*(D-C)
Z3 = F*G
```

[5.2.5.](#) Key Generation

The secret is 57 octets (456 bits, corresponding to b) of cryptographically-secure random data. See [RFC4086] for a discussion about randomness.

The 57-byte public key is generated by the following steps.

1. Hash the 57-byte secret using $\text{SHAKE256}(x, 114)$, storing the digest in a 114-octet large buffer, denoted h . Only the lower 57 bytes are used for generating the public key.
2. Prune the buffer: The two least significant bits of the first octet are cleared, all 8 bits the last octet are cleared, and the highest bit of the second to last octet is set.
3. Interpret the buffer as the little-endian integer, forming a secret scalar a . Perform a known-base-point scalar multiplication $[a]B$.
4. The public key A is the encoding of the point $[a]B$. First encode the y coordinate (in the range $0 \leq y < p$) as a little-endian

string of 57 octets. The most significant bit of the final octet is always zero. To form the encoding of the point $[a]B$, copy the least significant bit of the x coordinate to the most significant bit of the final octet. The result is the public key.

[5.2.6.](#) Sign

The inputs to the signing procedure is the secret key, a 32-octet string, a flag F , which is 0 for Ed448, 1 for Ed448ph, context C of at most 255 octets and a message M of arbitrary size.

1. Hash the secret key, 57-octets, using $\text{SHAKE256}(x, 114)$. Let h denote the resulting digest. Construct the secret scalar a from the first half of the digest, and the corresponding public key A , as described in the previous section. Let prefix denote the second half of the hash digest, $h[57], \dots, h[113]$.
2. Compute $\text{Shake256}(\text{dom}(F, C) \parallel \text{prefix} \parallel M, 114)$, where M is the message to be signed, F is 1 for Ed448ph, 0 for Ed448 and C is the context to use. Interpret the 114-octet digest as a little-endian integer r .
3. Compute the point $[r]B$. For efficiency, do this by first reducing r modulo l , the group order of B . Let the string R be the encoding of this point.
4. Compute $\text{Shake256}(\text{dom}(\text{flag}, \text{context}) \parallel R \parallel A \parallel M, 114)$, and interpret the 114-octet digest as a little-endian integer k .
5. Compute $S = (r + k * a) \bmod l$. For efficiency, again reduce k modulo l first.
6. Form the signature of the concatenation of R (57 octets) and the little-endian encoding of S (57 octets, ten most significant bits of the final octets always zero).

[5.2.7.](#) Verify

1. To verify a signature on a message M using context C , with F being 0 for Ed448, 1 for Ed448ph, first split the signature into two 57-octet halves. Decode the first half as a point R , and the second half as an integer S , in the range $0 \leq s < l$. If the decoding fails, the signature is invalid.
2. Compute $\text{Shake256}(\text{dom}(F, C) \parallel R \parallel A \parallel M, 114)$, and interpret the 114-octet digest as a little-endian integer k .

3. Check the group equation $[4][S]B = [4]R + [4][k]A$. It's sufficient, but not required, to instead check $[S]B = R + [k]A$.

6. Ed25519 Python illustration

The rest of this section describes how Ed25519 can be implemented in Python (version 3.2 or later) for illustration. See [appendix A](#) for the complete implementation and [appendix B](#) for a test-driver to run it through some test vectors.

Note that this code is not intended for production as it is not proven to be correct for all inputs, nor does it protect against side-channel attacks. The purpose is to illustrate the algorithm to help implementers with their own implementation.

First some preliminaries that will be needed.

```
import hashlib

def sha512(s):
    return hashlib.sha512(s).digest()

# Base field Z_p
p = 2**255 - 19

def modp_inv(x):
    return pow(x, p-2, p)

# Curve constant
d = -121665 * modp_inv(121666) % p

# Group order
q = 2**252 + 27742317777372353535851937790883648493

def sha512_modq(s):
    return int.from_bytes(sha512(s), "little") % q
```

Then follows functions to perform point operations.

Points are represented as tuples (X, Y, Z, T) of extended coordinates,
with $x = X/Z$, $y = Y/Z$, $x*y = T/Z$

```
def point_add(P, Q):
    A = (P[1]-P[0])*(Q[1]-Q[0]) % p
    B = (P[1]+P[0])*(Q[1]+Q[0]) % p
    C = 2 * P[3] * Q[3] * d % p
    D = 2 * P[2] * Q[2] % p
    E = B-A
    F = D-C
    G = D+C
    H = B+A
    return (E*F, G*H, F*G, E*H)

# Computes Q = s * Q
def point_mul(s, P):
    Q = (0, 1, 1, 0) # Neutral element
    while s > 0:
        # Is there any bit-set predicate?
        if s & 1:
            Q = point_add(Q, P)
        P = point_add(P, P)
        s >>= 1
    return Q

def point_equal(P, Q):
    #  $x_1 / z_1 == x_2 / z_2 \iff x_1 * z_2 == x_2 * z_1$ 
    if (P[0] * Q[2] - Q[0] * P[2]) % p != 0:
        return False
    if (P[1] * Q[2] - Q[1] * P[2]) % p != 0:
        return False
    return True
```

Now follows functions for point compression.

```
# Square root of -1
modp_sqrt_m1 = pow(2, (p-1) // 4, p)

# Compute corresponding x coordinate, with low bit corresponding to
# sign, or return None on failure
def recover_x(y, sign):
    x2 = (y*y-1) * modp_inv(d*y*y+1)
    if x2 == 0:
        if sign:
            return None
        else:
            return 0

    # Compute square root of x2
    x = pow(x2, (p+3) // 8, p)
    if (x*x - x2) % p != 0:
        x = x * modp_sqrt_m1 % p
    if (x*x - x2) % p != 0:
        return None

    if (x & 1) != sign:
        x = p - x
    return x

# Base point
g_y = 4 * modp_inv(5) % p
g_x = recover_x(g_y, 0)
G = (g_x, g_y, 1, g_x * g_y % p)

def point_compress(P):
    zinv = modp_inv(P[2])
    x = P[0] * zinv % p
    y = P[1] * zinv % p
```

```

        return int.to_bytes(y | ((x & 1) << 255), 32, "little")

def point_decompress(s):
    if len(s) != 32:
        raise Exception("Invalid input length for decompression")
    y = int.from_bytes(s, "little")
    sign = y >> 255
    y &= (1 << 255) - 1

    x = recover_x(y, sign)
    if x is None:
        return None
    else:
        return (x, y, 1, x*y % p)

```

These are functions for manipulating the secret.

```

def secret_expand(secret):
    if len(secret) != 32:
        raise Exception("Bad size of private key")
    h = sha512(secret)
    a = int.from_bytes(h[:32], "little")
    a &= (1 << 254) - 8
    a |= (1 << 254)
    return (a, h[32:])

def secret_to_public(secret):
    (a, dummy) = secret_expand(secret)
    return point_compress(point_mul(a, G))

```

The signature function works as below.

```

def sign(secret, msg):
    a, prefix = secret_expand(secret)
    A = point_compress(point_mul(a, G))
    r = sha512_modq(prefix + msg)
    R = point_mul(r, G)
    Rs = point_compress(R)
    h = sha512_modq(Rs + A + msg)
    s = (r + h * a) % q
    return Rs + int.to_bytes(s, 32, "little")

```

And finally the verification function.

```
def verify(public, msg, signature):
    if len(public) != 32:
        raise Exception("Bad public-key length")
    if len(signature) != 64:
        Exception("Bad signature length")
    A = point_decompress(public)
    if not A:
        return False
    Rs = signature[:32]
    R = point_decompress(Rs)
    if not R:
        return False
    s = int.from_bytes(signature[32:], "little")
    h = sha512_modq(Rs + public + msg)
    sB = point_mul(s, G)
    hA = point_mul(h, A)
    return point_equal(sB, point_add(R, hA))
```

[7.](#) Test Vectors

This section contains test vectors for Ed25519ph, Ed448ph, Ed25519 and Ed448.

Each section contains sequence of test vectors. The octets are hex encoded and whitespace is inserted for readability. Ed25519 and Ed25519ph private and public keys 32 octets, signatures are 64 octets. Ed448 and Ed448ph private and public keys are 57 octets, signatures are 114 octets. Messages are of arbitrary length.

[7.1.](#) Test Vectors for Ed25519

These test vectors are taken from [[ED25519-TEST-VECTORS](#)] (but we removed the public key as a suffix of the secret key, and removed the message from the signature) and [[ED25519-LIBCRYPT-TEST-VECTORS](#)].

-----TEST 1

ALGORITHM:
Ed25519

SECRET KEY:
9d61b19deffd5a60ba844af492ec2cc4
4449c5697b326919703bac031cae7f60

PUBLIC KEY:
d75a980182b10ab7d54bfed3c964073a
0ee172f3daa62325af021a68f707511a

MESSAGE (length 0 bytes):

SIGNATURE:
e5564300c360ac729086e2cc806e828a
84877f1eb8e5d974d873e06522490155
5fb8821590a33bacc61e39701cf9b46b
d25bf5f0595bbe24655141438e7a100b

-----TEST 2

ALGORITHM:
Ed25519

SECRET KEY:
4ccd089b28ff96da9db6c346ec114e0f
5b8a319f35aba624da8cf6ed4fb8a6fb

PUBLIC KEY:

Josefsson & Liusvaara Expires July 22, 2016

[Page 20]

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

3d4017c3e843895a92b70aa74d1b7ebc
9c982ccf2ec4968cc0cd55f12af4660c

MESSAGE (length 1 byte):
72

SIGNATURE:
92a009a9f0d4cab8720e820b5f642540
a2b27b5416503f8fb3762223ebdb69da
085ac1e43e15996e458f3613d0f11d8c
387b2eae4302aeeb00d291612bb0c00

-----TEST 3

ALGORITHM:
Ed25519

SECRET KEY:
c5aa8df43f9f837bedb7442f31dcb7b1
66d38535076f094b85ce3a2e0b4458f7

PUBLIC KEY:
fc51cd8e6218a1a38da47ed00230f058
0816ed13ba3303ac5deb911548908025

MESSAGE (length 2 bytes):
af82

SIGNATURE:
6291d657deec24024827e69c3abe01a3
0ce548a284743a445e3680d7db5ac3ac
18ff9b538d16f290ae67f760984dc659
4a7c15e9716ed28dc027beceea1ec40a

-----TEST 1024

ALGORITHM:
Ed25519

SECRET KEY:
f5e5767cf153319517630f226876b86c
8160cc583bc013744c6bf255f5cc0ee5

PUBLIC KEY:
278117fc144c72340f67d0f2316e8386
ceffbf2b2428c9c51fef7c597f1d426e

MESSAGE (length 1023 bytes):

08b8b2b733424243760fe426a4b54908
632110a66c2f6591eabd3345e3e4eb98
fa6e264bf09efe12ee50f8f54e9f77b1
e355f6c50544e23fb1433ddf73be84d8
79de7c0046dc4996d9e773f4bc9efe57

38829adb26c81b37c93a1b270b20329d
658675fc6ea534e0810a4432826bf58c
941efb65d57a338bbd2e26640f89ffbc
1a858efcb8550ee3a5e1998bd177e93a
7363c344fe6b199ee5d02e82d522c4fe
ba15452f80288a821a579116ec6dad2b
3b310da903401aa62100ab5d1a36553e
06203b33890cc9b832f79ef80560ccb9
a39ce767967ed628c6ad573cb116dbef
efd75499da96bd68a8a97b928a8bbc10
3b6621fcde2beca1231d206be6cd9ec7
aff6f6c94fcd7204ed3455c68c83f4a4
1da4af2b74ef5c53f1d8ac70bdcb7ed1
85ce81bd84359d44254d95629e9855a9
4a7c1958d1f8ada5d0532ed8a5aa3fb2
d17ba70eb6248e594e1a2297acbbb39d
502f1a8c6eb6f1ce22b3de1a1f40cc24
554119a831a9aad6079cad88425de6bd
e1a9187ebb6092cf67bf2b13fd65f270
88d78b7e883c8759d2c4f5c65adb7553
878ad575f9fad878e80a0c9ba63bcbcc
2732e69485bbc9c90bfbd62481d9089b
eccf80cfe2df16a2cf65bd92dd597b07
07e0917af48bbb75fed413d238f5555a
7a569d80c3414a8d0859dc65a46128ba
b27af87a71314f318c782b23ebfe808b
82b0ce26401d2e22f04d83d1255dc51a
ddd3b75a2b1ae0784504df543af8969b
e3ea7082ff7fc9888c144da2af58429e
c96031dbcad3dad9af0dcbaaaf268cb8
fcffead94f3c7ca495e056a9b47acdb7
51fb73e666c6c655ade8297297d07ad1
ba5e43f1bca32301651339e22904cc8c
42f58c30c04aafdb038dda0847dd988d
cda6f3bfd15c4b4c4525004aa06eeff8
ca61783aaccec57fb3d1f92b0fe2fd1a8
5f6724517b65e614ad6808d6f6ee34df
f7310fdc82aebfd904b01e1dc54b2927
094b2db68d6f903b68401adebf5a7e08
d78ff4ef5d63653a65040cf9bfd4aca7
984a74d37145986780fc0b16ac451649
de6188a7dbdf191f64b5fc5e2ab47b57
f7f7276cd419c17a3ca8e1b939ae49e4

88acba6b965610b5480109c8b17b80e1
b7b750dfc7598d5d5011fd2dcc5600a3
2ef5b52a1ecc820e308aa342721aac09
43bf6686b64b2579376504ccc493d97e
6aed3fb0f9cd71a43dd497f01f17c0e2
cb3797aa2a2f256656168e6c496afc5f
b93246f6b1116398a346f1a641f3b041
e989f7914f90cc2c7fff357876e506b5
0d334ba77c225bc307ba537152f3f161
0e4eafe595f6d9d90d11faa933a15ef1
369546868a7f3a45a96768d40fd9d034
12c091c6315cf4fde7cb68606937380d
b2eaaa707b4c4185c32eddcdd306705e
4dc1ffc872eeee475a64dfac86aba41c
0618983f8741c5ef68d3a101e8a3b8ca
c60c905c15fc910840b94c00a0b9d0

SIGNATURE:

0aab4c900501b3e24d7cdf4663326a3a
87df5e4843b2cbdb67cbf6e460fec350
aa5371b1508f9f4528ecea23c436d94b
5e8fcd4f681e30a6ac00a9704a188a03

-----TEST SHA(abc)

ALGORITHM:

Ed25519

SECRET KEY:

833fe62409237b9d62ec77587520911e
9a759cec1d19755b7da901b96dca3d42

PUBLIC KEY:

ec172b93ad5e563bf4932c70e1245034
c35467ef2efd4d64ebf819683467e2bf

MESSAGE (length 64 bytes):

ddaf35a193617abacc417349ae204131
12e6fa4e89a97ea20a9eeee64b55d39a
2192992a274fc1a836ba3c23a3feebbd
454d4423643ce80e2a9ac94fa54ca49f

SIGNATURE:

dc2a4459e7369633a52b1bf277839a00
201009a3efbf3ecb69bea2186c26b589
09351fc9ac90b3ecfd7c66431e030
3dca179c138ac17ad9bef1177331a704

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

[7.2.](#) Test Vectors for Ed25519ph

-----TEST abc

ALGORITHM:
Ed25519ph

SECRET KEY:
833fe62409237b9d62ec77587520911e
9a759cec1d19755b7da901b96dca3d42

PUBLIC KEY:
ec172b93ad5e563bf4932c70e1245034
c35467ef2efd4d64ebf819683467e2bf

MESSAGE (length 3 bytes):
616263

SIGNATURE:
dc2a4459e7369633a52b1bf277839a00
201009a3efbf3ecb69bea2186c26b589
09351fc9ac90b3ecfd7bc7c66431e030
3dca179c138ac17ad9bef1177331a704

[7.3.](#) Test Vectors for Ed448

-----Blank

ALGORITHM:
Ed448

SECRET KEY:
6c82a562cb808d10d632be89c8513ebf
6c929f34ddfa8c9f63c9960ef6e348a3
528c8a3fcc2f044e39a3fc5b94492f8f
032e7549a20098f95b

PUBLIC KEY:
5fd7449b59b461fd2ce787ec616ad46a
1da1342485a70e1f8a0ea75d80e96778
edf124769b46c7061bd6783df1e50f6c

d1fa1abeafe8256180

MESSAGE (length 0 bytes):

SIGNATURE:

533a37f6bbe457251f023c0d88f976ae

Josefsson & Liusvaara

Expires July 22, 2016

[Page 24]

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

2dfb504a843e34d2074fd823d41a591f
2b233f034f628281f2fd7a22ddd47d78
28c59bd0a21bfd3980ff0d2028d4b18a
9df63e006c5d1c2d345b925d8dc00b41
04852db99ac5c7cdda8530a113a0f4db
b61149f05a7363268c71d95808ff2e65
2600

-----1 octet

ALGORITHM:

Ed448

SECRET KEY:

c4eab05d357007c632f3dbb48489924d
552b08fe0c353a0d4a1f00acda2c463a
fbea67c5e8d2877c5e3bc397a659949e
f8021e954e0a12274e

PUBLIC KEY:

43ba28f430cdff456ae531545f7ecd0a
c834a55d9358c0372bfa0c6c6798c086
6aea01eb00742802b8438ea4cb82169c
235160627b4c3a9480

MESSAGE (length 1 byte):

03

SIGNATURE:

26b8f91727bd62897af15e41eb43c377
efb9c610d48f2335cb0bd0087810f435
2541b143c4b981b7e18f62de8ccdf633
fc1bf037ab7cd779805e0dbcc0aae1cb
cee1afb2e027df36bc04dcecbf154336
c19f0af7e0a6472905e799f1953d2a0f

f3348ab21aa4adafd1d234441cf807c0
3a00

-----1 octet (with context)

ALGORITHM:
Ed448

SECRET KEY:
c4eab05d357007c632f3dbb48489924d
552b08fe0c353a0d4a1f00acda2c463a
fbea67c5e8d2877c5e3bc397a659949e
f8021e954e0a12274e

Josefsson & Liusvaara

Expires July 22, 2016

[Page 25]

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

PUBLIC KEY:
43ba28f430cdff456ae531545f7ecd0a
c834a55d9358c0372bfa0c6c6798c086
6aea01eb00742802b8438ea4cb82169c
235160627b4c3a9480

MESSAGE (length 1 byte):
03

CONTEXT:
666f6f

SIGNATURE:
d4f8f6131770dd46f40867d6fd5d5055
de43541f8c5e35abbcd001b32a89f7d2
151f7647f11d8ca2ae279fb842d60721
7fce6e042f6815ea000c85741de5c8da
1144a6a1aba7f96de42505d7a7298524
fda538fccbbb754f578c1cad10d54d0d
5428407e85dcbc98a49155c13764e66c
3c00

-----11 octets

ALGORITHM:
Ed448

SECRET KEY:

cd23d24f714274e744343237b93290f5
11f6425f98e64459ff203e8985083ffd
f60500553abc0e05cd02184bdb89c4cc
d67e187951267eb328

PUBLIC KEY:

dcea9e78f35a1bf3499a831b10b86c90
aac01cd84b67a0109b55a36e9328b1e3
65fce161d71ce7131a543ea4cb5f7e9f
1d8b00696447001400

MESSAGE (length 11 bytes):

0c3e544074ec63b0265e0c

SIGNATURE:

1f0a8888ce25e8d458a21130879b840a
9089d999aaba039eaf3e3afa090a09d3
89dba82c4ff2ae8ac5cdfb7c55e94d5d
961a29fe0109941e00b8dbdeea6d3b05
1068df7254c0cdc129cbe62db2dc957d

Josefsson & Liusvaara

Expires July 22, 2016

[Page 26]

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

bb47b51fd3f213fb8698f064774250a5
028961c9bf8ffd973fe5d5c206492b14
0e00

-----12 octets

ALGORITHM:

Ed448

SECRET KEY:

258cdd4ada32ed9c9ff54e63756ae582
fb8fab2ac721f2c8e676a72768513d93
9f63dddb55609133f29adf86ec9929dc
cb52c1c5fd2ff7e21b

PUBLIC KEY:

3ba16da0c6f2cc1f30187740756f5e79
8d6bc5fc015d7c63cc9510ee3fd44adc
24d8e968b6e46e6f94d19b945361726b
d75e149ef09817f580

MESSAGE (length 12 bytes):

64a65f3cdedcdd66811e2915

SIGNATURE:

7eeeab7c4e50fb799b418ee5e3197ff6
bf15d43a14c34389b59dd1a7b1b85b4a
e90438aca634bea45e3a2695f1270f07
fdcdf7c62b8efeaf00b45c2c96ba457e
b1a8bf075a3db28e5c24f6b923ed4ad7
47c3c9e03c7079efb87cb110d3a99861
e72003cbae6d6b8b827e4e6c143064ff
3c00

-----13 octets

ALGORITHM:

Ed448

SECRET KEY:

7ef4e84544236752fbb56b8f31a23a10
e42814f5f55ca037cdcc11c64c9a3b29
49c1bb60700314611732a6c2fea98eeb
c0266a11a93970100e

PUBLIC KEY:

b3da079b0aa493a5772029f0467baebe
e5a8112d9d3a22532361da294f7bb381

5c5dc59e176b4d9f381ca0938e13c6c0
7b174be65dfa578e80

MESSAGE (length 13 bytes):

64a65f3cdedcdd66811e2915e7

SIGNATURE:

6a12066f55331b6c22acd5d5bfc5d712
28fbda80ae8dec26bdd306743c5027cb
4890810c162c027468675ecf645a8317
6c0d7323a2ccde2d80efe5a1268e8aca
1d6fbc194d3f77c44986eb4ab4177919
ad8bec33eb47bbb5fc6e28196fd1caf5
6b4e7e0ba5519234d047155ac727a105

3100

-----64 octets

ALGORITHM:
Ed448

SECRET KEY:
d65df341ad13e008567688baedda8e9d
cdc17dc024974ea5b4227b6530e339bf
f21f99e68ca6968f3cca6dfe0fb9f4fa
b4fa135d5542ea3f01

PUBLIC KEY:
df9705f58edbab802c7f8363cfe5560a
b1c6132c20a9f1dd163483a26f8ac53a
39d6808bf4a1dfbd261b099bb03b3fb5
0906cb28bd8a081f00

MESSAGE (length 64 bytes):
bd0f6a3747cd561bddd4640a332461a
4a30a12a434cd0bf40d766d9c6d458e5
512204a30c17d1f50b5079631f64eb31
12182da3005835461113718d1a5ef944

SIGNATURE:
554bc2480860b49eab8532d2a533b7d5
78ef473eeb58c98bb2d0e1ce488a98b1
8dfde9b9b90775e67f47d4a1c3482058
efc9f40d2ca033a0801b63d45b3b722e
f552bad3b4ccb667da350192b61c508c
f7b6b5adadc2c8d9a446ef003fb05cba
5f30e88e36ec2703b349ca229c267083
3900

-----256 octets

ALGORITHM:
Ed448

SECRET KEY:
2ec5fe3c17045abdb136a5e6a913e32a

b75ae68b53d2fc149b77e504132d3756
9b7e766ba74a19bd6162343a21c8590a
a9cebca9014c636df5

PUBLIC KEY:

79756f014dcfe2079f5dd9e718be4171
e2ef2486a08f25186f6bffa43a9936b9b
fe12402b08ae65798a3d81e22e9ec80e
7690862ef3d4ed3a00

MESSAGE (length 256 bytes):

15777532b0bdd0d1389f636c5f6b9ba7
34c90af572877e2d272dd078aa1e567c
fa80e12928bb542330e8409f31745041
07ecd5efac61ae7504dabe2a602ede89
e5cca6257a7c77e27a702b3ae39fc769
fc54f2395ae6a1178cab4738e543072f
c1c177fe71e92e25bf03e4ecb72f47b6
4d0465aaea4c7fad372536c8ba516a60
39c3c2a39f0e4d832be432dfa9a706a6
e5c7e19f397964ca4258002f7c0541b5
90316dbc5622b6b2a6fe7a4abffd9610
5eca76ea7b98816af0748c10df048ce0
12d901015a51f189f3888145c03650aa
23ce894c3bd889e030d565071c59f409
a9981b51878fd6fc110624dcbcd0bf7
a69cccce38fabdf86f3bef6044819de11

SIGNATURE:

c650ddbb0601c19ca11439e1640dd931
f43c518ea5bea70d3dcde5f4191fe53f
00cf966546b72bcc7d58be2b9badef28
743954e3a44a23f880e8d4f1cfce2d7a
61452d26da05896f0a50da66a239a8a1
88b6d825b3305ad77b73fbac0836ecc6
0987fd08527c1a8e80d5823e65cafe2a
3d00

-----1023 octets

ALGORITHM:

Ed448

SECRET KEY:

872d093780f5d3730df7c212664b37b8
a0f24f56810daa8382cd4fa3f77634ec
44dc54f1c2ed9bea86fafb7632d8be19
9ea165f5ad55dd9ce8

PUBLIC KEY:

a81b2e8a70a5ac94ffdbcc9badfc3feb
0801f258578bb114ad44ece1ec0e799d
a08effb81c5d685c0c56f64eecaef8cd
f11cc38737838cf400

MESSAGE (length 1023 bytes):

6ddf802e1aae4986935f7f981ba3f035
1d6273c0a0c22c9c0e8339168e675412
a3debfa435ed651558007db4384b650
fcc07e3b586a27a4f7a00ac8a6fec2cd
86ae4bf1570c41e6a40c931db27b2faa
15a8cedd52cff7362c4e6e23daec0fbc
3a79b6806e316efcc7b68119bf46bc76
a26067a53f296dafdbdc11c77f7777e9
72660cf4b6a9b369a6665f02e0cc9b6e
dfad136b4fabe723d2813db3136cfde9
b6d044322fee2947952e031b73ab5c60
3349b307bdc27bc6cb8b8bbd7bd32321
9b8033a581b59eadebb09b3c4f3d2277
d4f0343624acc817804728b25ab79717
2b4c5c21a22f9c7839d64300232eb66e
53f31c723fa37fe387c7d3e50bdf9813
a30e5bb12cf4cd930c40cfb4e1fc6225
92a49588794494d56d24ea4b40c89fc0
596cc9ebb961c8cb10adde976a5d602b
1c3f85b9b9a001ed3c6a4d3b1437f520
96cd1956d042a597d561a596ecd3d173
5a8d570ea0ec27225a2c4aaff26306d1
526c1af3ca6d9cf5a2c98f47e1c46db9
a33234cfd4d81f2c98538a09ebe76998
d0d8fd25997c7d255c6d66ece6fa56f1
1144950f027795e653008f4bd7ca2dee
85d8e90f3dc315130ce2a00375a318c7
c3d97be2c8ce5b6db41a6254ff264fa6
155baee3b0773c0f497c573f19bb4f42
40281f0b1f4f7be857a4e59d416c06b4
c50fa09e1810ddc6b1467baeac5a3668
d11b6ecaa901440016f389f80acc4db9
77025e7f5924388c7e340a732e554440

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

e76570f8dd71b7d640b3450d1fd5f041
0a18f9a3494f707c717b79b4bf75c984
00b096b21653b5d217cf3565c9597456
f70703497a078763829bc01bb1cbc8fa
04eadc9a6e3f6699587a9e75c94e5bab
0036e0b2e711392cff0047d0d6b05bd2
a588bc109718954259f1d86678a579a3
120f19cfb2963f177aeb70f2d4844826
262e51b80271272068ef5b3856fa8535
aa2a88b2d41f2a0e2fda7624c2850272
ac4a2f561f8f2f7a318bfd5caf969614
9e4ac824ad3460538fdc25421beec2cc
6818162d06bbbed0c40a387192349db67
a118bada6cd5ab0140ee273204f628aa
d1c135f770279a651e24d8c14d75a605
9d76b96a6fd857def5e0b354b27ab937
a5815d16b5fae407ff18222c6d1ed263
be68c95f32d908bd895cd76207ae7264
87567f9a67dad79abec316f683b17f2d
02bf07e0ac8b5bc6162cf94697b3c27c
d1fea49b27f23ba2901871962506520c
392da8b6ad0d99f7013fbc06c2c17a56
9500c8a7696481c1cd33e9b14e40b82e
79a5f5db82571ba97bae3ad3e0479515
bb0e2b0f3bfcd1fd33034efc6245eddd
7ee2086ddae2600d8ca73e214e8c2b0b
db2b047c6a464a562ed77b73d2d841c4
b34973551257713b753632efba348169
abc90a68f42611a40126d7cb21b58695
568186f7e569d2ff0f9e745d0487dd2e
b997cafc5abf9dd102e62ff66cba87

SIGNATURE:

e301345a41a39a4d72fff8df69c98075
a0cc082b802fc9b2b6bc503f926b65bd
df7f4c8f1cb49f6396afc8a70abe6d8a
ef0db478d4c6b2970076c6a0484fe76d
76b3a97625d79f1ce240e7c576750d29
5528286f719b413de9ada3e8eb78ed57
3603ce30d8bb761785dc30dbc320869e
1a00

[7.4.](#) Test Vectors for Ed448ph

-----TEST abc

ALGORITHM:

Ed448ph

SECRET KEY:

833fe62409237b9d62ec77587520911e
9a759cec1d19755b7da901b96dca3d42

PUBLIC KEY:

55ab69e205b6c7b344711f9576dfe48e
963e39e03f0fc0374465ff6b7eaa1d7d
0c95c1c36c1f4a7dc89e74fdd0dc9b34
187e1ee702b303f000

MESSAGE (length 3 bytes):

616263

SIGNATURE:

c61f474654ce82432a6cc5c43f295b49
b5a8a256047f1edc09fe69588f75cc3b
c8bee6eaf6dc52ecac585583780fa238
2059416759a11d938079e3d0a7ed873d
4f99cdde00a35a6698e9e1763071e698
5eee73682dc91448b9058e31c1483719
f44a0d59b7d398c82c6db48c32d60db2
3e00

-----TEST abc (with context)

ALGORITHM:

Ed448ph

SECRET KEY:

833fe62409237b9d62ec77587520911e
9a759cec1d19755b7da901b96dca3d42

PUBLIC KEY:

55ab69e205b6c7b344711f9576dfe48e

963e39e03f0fc0374465ff6b7eaa1d7d
0c95c1c36c1f4a7dc89e74fdd0dc9b34
187e1ee702b303f000

MESSAGE (length 3 bytes):
616263

CONTEXT:
666f6f

SIGNATURE:
b0820f1ea13b9118d41c59de9637e92d

Josefsson & Liusvaara

Expires July 22, 2016

[Page 32]

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

45878b88c72fc813a42468d90f2f323b
130e3104c9fb4746fcace1b0454cffaa
a420a405474fae5180f43b5d975e579c
059ecece8c6cbbc621baf0586db0747f
0b2a7728a6606dc86d0f157b5628e20d
e93c98afa9d5b1d4b6ba6994690db4fc
2f00

[8.](#) Acknowledgements

EdDSA and Ed25519 was initially described in a paper due to Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe and Bo-Yin Yang. The Ed448 curves is due to Mike Hamburg.

This draft is based on an earlier draft co-authored by Niels Moeller.

Feedback on this document was received from Werner Koch, Damien Miller, Bob Bradley, Franck Rondepierre, Alexey Melnikov, Kenny Paterson, and Robert Edmonds.

The Ed25519 test vectors were double checked by Bob Bradley using 3 separate implementations (one based on TweetNaCl and 2 different implementations based on code from SUPERCOP).

[9.](#) IANA Considerations

None.

[10.](#) Security Considerations

[10.1.](#) Side-channel leaks

For implementations performing signatures, secrecy of the key is fundamental. It is possible to protect against some side-channel attacks by ensuring that the implementation executes exactly the same sequence of instructions and performs exactly the same memory accesses, for any value of the secret key.

To make an implementation side-channel silent in this way, the modulo p arithmetic must not use any data-dependent branches, e.g., related to carry propagation. Side channel-silent point addition is straight-forward, thanks to the unified formulas.

Scalar multiplication, multiplying a point by an integer, needs some additional effort to implement in a side-channel silent manner. One simple approach is to implement a side-channel silent conditional

assignment, and use together with the binary algorithm to examine one bit of the integer at a time.

Note that the example implementations in this document do not attempt to be side-channel silent.

[10.2.](#) Use of contexts

Contexts can be used to separate uses of the protocol between different protocols (which is very hard to reliably do otherwise) and between different uses within the same protocol. However, the following SHOULD be kept in mind when using this facility:

The context should be a constant string specified by the protocol using it. It SHOULD NOT incorporate variable elements from the message itself.

Most signing functions do not support contexts, so those SHOULD NOT be relied to perform security-critical separations.

Contexts are an extra input, which percolates out of APIs, as such, even if signature scheme supports contexts, those may not be

available for use. This problem is compounded by the fact that many times the application is not invoking the signing and verification functions directly, but via some other protocol.

10.3. Mixing different prehashes

Using the same key with different prehashes is a bad idea. The most obvious problem is that identity transform can produce message values colliding with hashes of interesting messages (or vice versa). Additionally, even if it is infeasible to find collisions in two hash functions, there is nothing guaranteeing that finding collisions between hashes is infeasible.

For these reasons, the same private key **MUST NOT** be used for multiple algorithms (including prehashes) without protocol preventing messages output by different prehash algorithms from colliding.

10.4. Signing large amounts of data at once

Avoid signing large amounts of data at once (where "large" depends on expected verifier). In particular, unless the underlying protocol does not require it, the receiver **MUST** buffer the entire message (or enough information to reconstruct it, e.g. compressed or encrypted version) to be verified.

This is needed because most of the time, it is unsafe to process unverified data, and verifying the signature makes a pass through whole message, causing ultimately at least two passes through.

As API consideration, this means that any IUF verification interface is prone to misuse.

11. References

11.1. Normative References

[RFC4634] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", [RFC 4634](#), July 2006.

[I-D.irtf-cfrg-curves]

Langley, A. and M. Hamburg, "Elliptic Curves for Security", [draft-irtf-cfrg-curves-10](#) (work in progress), October 2015.

- [FIPS202] National Institute of Standards and Technology, U.S. Department of Commerce, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", FIPS 202, August 2015.

[11.2.](#) Informative References

- [RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", [BCP 106](#), [RFC 4086](#), June 2005.
- [EDDSA] Bernstein, D., Duif, N., Lange, T., Schwabe, P., and B. Yang, "High-speed high-security signatures", WWW <http://ed25519.cr.yp.to/ed25519-20110926.pdf>, September 2011.
- [EDDSA2] Bernstein, D., Josefsson, S., Lange, T., Schwabe, P., and B. Yang, "EdDSA for more curves", WWW <http://ed25519.cr.yp.to/eddsa-20150704.pdf>, July 2015.
- [Faster-ECC] Bernstein, D. and T. Lange, "Faster addition and doubling on elliptic curves", WWW <http://eprint.iacr.org/2007/286>, July 2007.
- [Edwards-revisited] Hisil, H., Wong, K., Carter, G., and E. Dawson, "Twisted Edwards Curves Revisited", WWW <http://eprint.iacr.org/2008/522>, December 2008.

Josefsson & Liusvaara Expires July 22, 2016 [Page 35]

Internet-Draft EdDSA: Ed25519 and Ed448 January 2016

- [CURVE25519] Bernstein, D., "Curve25519: new Diffie-Hellman speed records", WWW <http://cr.yp.to/ecdh.html>, February 2006.
- [ED448] Hamburg, M., "Ed448-Goldilocks, a new elliptic curve", WWW <http://eprint.iacr.org/2015/625>, June 2015.
- [ED25519-TEST-VECTORS]

Bernstein, D., Duif, N., Lange, T., Schwabe, P., and B. Yang, "Ed25519 test vectors", WWW
<http://ed25519.cr.yp.to/python/sign.input>, July 2011.

[ED25519-LIBCRYPT-TEST-VECTORS]

Koch, W., "Ed25519 Libcrypt test vectors", WWW
<http://git.gnupg.org/cgi-bin/gitweb.cgi?p=libgcrypt.git;a=blob;f=tests/t-ed25519.in;p=h=e13566f826321eece65e02c593bc7d885b3dbe23;hb=refs/heads/master>, July 2014.

[Appendix A](#). Ed25519/Ed448 Python Library

Below is an example implementation of Ed25519/Ed448 written in Python, version 3.2 or higher is required.

[A note to RFC-Editor: Please don't change the relative indentations here: This code is written in programming language where relative indentations are meaningful, so changing those changes program meaning (authors: check this still works in AUTH48). Remove this note before publication.]

```
import hashlib;
import os;

#Compute candidate square root of x modulo p, with p = 3 (mod 4).
def sqrt4k3(x,p): return pow(x,(p + 1)//4,p)

#Compute candidate square root of x modulo p, with p = 5 (mod 8).
def sqrt8k5(x,p):
    y = pow(x,(p+3)//8,p)
    #If the square root exists, it is either y, or y*2^(p-1)/4.
    if (y * y) % p == x % p: return y
    else:
        z = pow(2,(p - 1)//4,p)
        return (y * z) % p

#Decode a hexadecimal string representation of integer.
def hexi(s): return int.from_bytes(bytes.fromhex(s),byteorder="big")
```

#Rotate a word x by b places to the left.

```

def rol(x,b): return ((x << b) | (x >> (64 - b))) & (2**64-1)

#From little-endian.
def from_le(s): return int.from_bytes(s, byteorder="little")

#Do the SHA-3 state transform on state s.
def sha3_transform(s):
    ROTATIONS = [0,1,62,28,27,36,44,6,55,20,3,10,43,25,39,41,45,15,\
                  21,8,18,2,61,56,14]
    PERMUTATION = [1,6,9,22,14,20,2,12,13,19,23,15,4,24,21,8,16,5,3,\
                   18,17,11,7,10]
    RC = [0x0000000000000001,0x0000000000000802,0x800000000000080a,\
          0x8000000008000800,0x000000000000080b,0x0000000008000001,\
          0x8000000008000801,0x8000000000000809,0x000000000000008a,\
          0x0000000000000088,0x0000000008000809,0x000000000800000a,\
          0x000000000800080b,0x800000000000008b,0x8000000000000809,\
          0x8000000000000803,0x8000000000000802,0x8000000000000080,\
          0x000000000000080a,0x800000000800000a,0x8000000008000801,\
          0x8000000000000808,0x0000000008000001,0x8000000008000808]
    for rnd in range(0,24):
        #AddColumnParity (Theta)
        c = [0]*5;
        d = [0]*5;
        for i in range(0,25): c[i%5]^=s[i]
        for i in range(0,5): d[i]=c[(i+4)%5]^rol(c[(i+1)%5],1)
        for i in range(0,25): s[i]^=d[i%5]
        #RotateWords (Rho).
        for i in range(0,25): s[i]=rol(s[i],ROTATIONS[i])
        #PermuteWords (Pi)
        t = s[PERMUTATION[0]]
        for i in range(0,len(PERMUTATION)-1):
            s[PERMUTATION[i]]=s[PERMUTATION[i+1]]
        s[PERMUTATION[-1]]=t;
        #NonlinearMixRows (Chi)
        for i in range(0,25,5):
            t=[s[i],s[i+1],s[i+2],s[i+3],s[i+4],s[i],s[i+1]]
            for j in range(0,5): s[i+j]=t[j]^((~t[j+1])&(t[j+2]))
        #AddRoundConstant (Iota)
        s[0]^=RC[rnd]

#Reinterpret octet array b to word array and XOR it to state s.
def reinterpret_to_words_and_xor(s,b):
    for j in range(0,len(b)//8):
        s[j]^=from_le(b[8*j:][:8])

#Reinterpret word array w to octet array and return it.
def reinterpret_to_octets(w):

```

```
    mp=bytearray()
    for j in range(0,len(w)):
        mp+=w[j].to_bytes(8,byteorder="little")
    return mp

#(semi-)generic SHA-3 implementation
def sha3_raw(msg,r_w,o_p,e_b):
    r_b=8*r_w
    s=[0]*25
    #Handle whole blocks.
    idx=0
    blocks=len(msg)//r_b
    for i in range(0,blocks):
        reinterpret_to_words_and_xor(s,msg[idx:][:r_b])
        idx+=r_b
        sha3_transform(s)
    #Handle last block padding.
    m=bytearray(msg[idx:])
    m.append(o_p)
    while len(m) < r_b: m.append(0)
    m[len(m)-1]|=128
    #Handle padded last block.
    reinterpret_to_words_and_xor(s,m)
    sha3_transform(s)
    #Output.
    out = bytearray()
    while len(out)<e_b:
        out+=reinterpret_to_octets(s[:r_w])
        sha3_transform(s)
    return out[:e_b]

#Implementations of actual SHA-3 functions.
def sha3_224(msg): return sha3_raw(msg,18,6,28)
def sha3_256(msg): return sha3_raw(msg,17,6,32)
def sha3_384(msg): return sha3_raw(msg,13,6,48)
def sha3_512(msg): return sha3_raw(msg,9,6,64)
def shake128(msg,olen): return sha3_raw(msg,21,31,olen)
def shake256(msg,olen): return sha3_raw(msg,17,31,olen)

#A (prime) field element.
class Field:
    #Construct number x (mod p).
    def __init__(self,x,p):
        self.__x=x%p
        self.__p=p
```

```
#Check that fields of self and y are the same.
def __check_fields(self,y):
```

```
    if type(y) is not Field or self.__p!=y.__p:
        raise ValueError("Fields don't match")
#Field addition. The fields must match.
def __add__(self,y):
    self.__check_fields(y)
    return Field(self.__x+y.__x,self.__p)
#Field subtraction. The fields must match.
def __sub__(self,y):
    self.__check_fields(y)
    return Field(self.__p+self.__x-y.__x,self.__p)
#Field negation.
def __neg__(self):
    return Field(self.__p-self.__x,self.__p)
#Field muptiplication. The fields must match.
def __mul__(self,y):
    self.__check_fields(y)
    return Field(self.__x*y.__x,self.__p)
#Field divsion. The fields must match.
def __truediv__(self,y):
    return self*y.inv()
#Field inverse (inverse of 0 is 0).
def inv(self):
    return Field(pow(self.__x,self.__p-2,self.__p),self.__p)
#Field square root. Returns none if square root does not exist.
#Note: not presently implemented for p mod 8 = 1 case.
def sqrt(self):
    #Compute candidate square root.
    if self.__p%4==3: y=sqrt4k3(self.__x,self.__p)
    elif self.__p%8==5: y=sqrt8k5(self.__x,self.__p)
    else: raise NotImplementedError("sqrt(_,8k+1)")
    _y=Field(y,self.__p);
    #Check square root candidate valid.
    return _y if _y*_y==self else None
#Make Field element with the same field as this, but different
#value.
def make(self,ival): return Field(ival,self.__p)
#Is field element the additive identity?
def iszero(self): return self.__x==0
#Are field elements equal?
```

```

def __eq__(self,y): return self.__x==y.__x and self.__p==y.__p
#Are field elements not equal?
def __ne__(self,y): return not (self==y)
#Serialize number to b-1 bits.
def tobytes(self,b):
    return self.__x.to_bytes(b//8,byteorder="little")
#Unserialize number from bits.
def frombytes(self,x,b):
    rv=from_le(x)%(2**(b-1))

```

```

    return Field(rv,self.__p) if rv<self.__p else None
#Compute sign of number, 0 or 1. The sign function
#has the following property:
#sign(x) = 1 - sign(-x) if x != 0.
def sign(self): return self.__x%2

#A point on (twisted) Edwards curve.
class EdwardsPoint:
    #base_field = None
    #x = None
    #y = None
    #z = None
    def initpoint(self, x, y):
        self.x=x
        self.y=y
        self.z=self.base_field.make(1)
    def decode_base(self,s,b):
        #Check that point encoding is of correct length.
        if len(s)!=b//8: return (None,None)
        #Extract signbit.
        xs=s[(b-1)//8]>>((b-1)&7)
        #Decode y. If this fails, fail.
        y = self.base_field.frombytes(s,b)
        if y is None: return (None,None)
        #Try to recover x. If it does not exist, or is zero and xs is
        #wrong, fail.
        x=self.solve_x2(y).sqrt()
        if x is None or (x.iszero() and xs!=x.sign()):
            return (None,None)
        #If sign of x isn't correct, flip it.
        if x.sign()!=xs: x=-x
        # Return the constructed point.

```

[illegible]

```

@staticmethod
def stdbase():
    return Edwards25519Point(Edwards25519Point.xb,\
        Edwards25519Point.yb)
def __init__(self,x,y):
    #Check the point is actually on the curve.
    if y*y-x*x!=self.f1+self.d*x*x*y*y:
        raise ValueError("Invalid point")
    self.initpoint(x, y)
    self.t=x*y
#Decode a point representation.
def decode(self,s):
    x,y=self.decode_base(s,256);
    return Edwards25519Point(x, y) if x is not None else None
#Encode a point representation
def encode(self):
    return self.encode_base(256)
#Construct neutral point on this curve.
def zero_elem(self):
    return Edwards25519Point(self.f0,self.f1)
#Solve for x^2.
def solve_x2(self,y):
    return ((y*y-self.f1)/(self.d*y*y+self.f1))

```

```

#Point addition.
def __add__(self,y):
    #The formulas are from EFD.
    tmp=self.zero_elem()
    zcp=self.z*y.z
    A=(self.y-self.x)*(y.y-y.x)
    B=(self.y+self.x)*(y.y+y.x)
    C=(self.d+self.d)*self.t*y.t
    D=zcp+zcp
    E,H=B-A,B+A
    F,G=D-C,D+C
    tmp.x,tmp.y,tmp.z,tmp.t=E*F,G*H,F*G,E*H
    return tmp
#Point doubling.
def double(self):
    #The formulas are from EFD.
    tmp=self.zero_elem()
    x1s,y1s,z1s=self.x*self.x,self.y*self.y,self.z*self.z

```



```

#Decode a point representation.
def decode(self,s):
    x,y=self.decode_base(s,456);
    return Edwards448Point(x, y) if x is not None else None
#Encode a point representation
def encode(self):
    return self.encode_base(456)
#Construct neutral point on this curve.
def zero_elem(self):
    return Edwards448Point(self.f0,self.f1)
#Solve for x^2.
def solve_x2(self,y):
    return ((y*y-self.f1)/(self.d*y*y-self.f1))
#Point addition.
def __add__(self,y):
    #The formulas are from EFD.
    tmp=self.zero_elem()
    xcp,ycp,zcp=self.x*y.x,self.y*y.y,self.z*y.z
    B=zcp*zcp
    E=self.d*xcp*ycp
    F,G=B-E,B+E
    tmp.x=zcp*F*((self.x+self.y)*(y.x+y.y)-xcp-ycp)
    tmp.y,tmp.z=zcp*G*(ycp-xcp),F*G
    return tmp
#Point doubling.
def double(self):
    #The formulas are from EFD.
    tmp=self.zero_elem()
    x1s,y1s,z1s=self.x*self.x,self.y*self.y,self.z*self.z
    xys=self.x+self.y
    F=x1s+y1s
    J=F-(z1s+z1s)
    tmp.x,tmp.y,tmp.z=(xys*xys-x1s-y1s)*J,F*(x1s-y1s),F*J
    return tmp
#Order of basepoint.
def l(self):
    return hexi("3fffffffffffffffffffffffffffffffffffffffffffffffff"+\

```

```

    "fffffffff7cca23e9c44edb49aed63690216cc2728dc58f552378c2"+\
    "92ab5844f3")
#The logarithm of cofactor.
def c(self): return 2

```

```

#The highest set bit
def n(self): return 447
#The coding length
def b(self): return 456

#PureEdDSA scheme.
#Limitation: Only  $b \bmod 8 = 0$  is handled.
class PureEdDSA:
    #Create a new object.
    def __init__(self,properties):
        self.B=properties["B"]
        self.H=properties["H"]
        self.l=self.B.l()
        self.n=self.B.n()
        self.b=self.B.b()
        self.c=self.B.c()
    #Clamp a private scalar.
    def __clamp(self,a):
        _a = bytearray(a)
        for i in range(0,self.c): _a[i//8]&=~(1<<(i%8))
        _a[self.n//8]|=1<<(self.n%8)
        for i in range(self.n+1,self.b): _a[i//8]&=~(1<<(i%8))
        return _a
    #Generate a key. If privkey is None, random one is generated.
    #In any case, privkey, pubkey pair is returned.
    def keygen(self,privkey):
        #If no private key data given, generate random.
        if privkey is None: privkey=os.urandom(self.b//8)
        #Expand key.
        khash=self.H(privkey,None,None)
        a=from_le(self.__clamp(khash[:self.b//8]))
        #Return the keypair (public key is  $A=Enc(aB)$ ).
        return privkey,(self.B*a).encode()
    #Sign with keypair.
    def sign(self,privkey,pubkey,msg,ctx,hflag):
        #Expand key.
        khash=self.H(privkey,None,None)
        a=from_le(self.__clamp(khash[:self.b//8]))
        seed=khash[self.b//8:]
        #Calculate r and R (R only used in encoded form)
        r=from_le(self.H(seed+msg,ctx,hflag))%self.l
        R=(self.B*r).encode()
        #Calculate h.
        h=from_le(self.H(R+pubkey+msg,ctx,hflag))%self.l

```

```

        #Calculate s.
        S=((r+h*a)%self.l).to_bytes(self.b//8,byteorder="little")
        #The final signature is concatenation of R and S.
        return R+S
#Verify signature with public key.
def verify(self, pubkey, msg, sig, ctx, hflag):
    #Sanity-check sizes.
    if len(sig)!=self.b//4: return False
    if len(pubkey)!=self.b//8: return False
    #Split signature into R and S, and parse.
    Rraw, Sraw=sig[:self.b//8], sig[self.b//8:]
    R, S=self.B.decode(Rraw), from_le(Sraw)
    #Parse public key.
    A=self.B.decode(pubkey)
    #Check parse results.
    if (R is None) or (A is None) or S>=self.l: return False
    #Calculate h.
    h=from_le(self.H(Rraw+pubkey+msg, ctx, hflag))%self.l
    #Calculate left and right sides of check eq.
    rhs=R+(A*h)
    lhs=self.B*S
    for i in range(0, self.c):
        lhs = lhs.double()
        rhs = rhs.double()
    #Check eq. holds?
    return lhs==rhs

#The base PureEdDSA schemes.
pEd25519=PureEdDSA({\
    "B":Edwards25519Point.stdbase(),\
    "H":lambda x,y,z:hashlib.sha512(x).digest()\
})

def Ed448_inthash(data, ctx, hflag):
    dompfx = b""
    if ctx is not None:
        dompfx=b"SigEd448"+bytes([1 if hflag else 0, len(ctx)])+ctx
    return shake256(dompfx+data, 114)

pEd448 = PureEdDSA({\
    "B":Edwards448Point.stdbase(),\
    "H":Ed448_inthash\
})

#EdDSA scheme.
class EdDSA:
    #Create a new scheme object, with specified PureEdDSA base scheme

```

#and specified prehash.

```
def __init__(self,pure_scheme,prehash):
    self.__pflag = True
    self.__pure=pure_scheme
    self.__prehash=prehash
    if self.__prehash is None:
        self.__prehash = lambda x,y:x
        self.__pflag = False
    # Generate a key. If privkey is none, generates a random
    # privkey key, otherwise uses specified private key.
    # Returns pair (privkey, pubkey).
    def keygen(self,privkey): return self.__pure.keygen(privkey)
    # Sign message msg usign specified keypair.
    def sign(self,privkey,pubkey,msg,ctx=None):
        if ctx is None: ctx=b"";
        return self.__pure.sign(privkey,pubkey,self.__prehash(msg,ctx),\
            ctx,self.__pflag)
    # Verify signature sig on message msg using public key pubkey.
    def verify(self,pubkey,msg,sig,ctx=None):
        if ctx is None: ctx=b"";
        return self.__pure.verify(pubkey,self.__prehash(msg,ctx),sig,\
            ctx,self.__pflag)

def Ed448ph_prehash(data,ctx):
    dompfx=b"SigEd448"+bytes([2,len(ctx)])+ctx
    return shake256(dompfx+data,64)

#Our signature schemes.
Ed25519 = EdDSA(pEd25519,None)
Ed25519ph = EdDSA(pEd25519,lambda x,y:hashlib.sha512(x).digest())
Ed448 = EdDSA(pEd448,None)
Ed448ph = EdDSA(pEd448,Ed448ph_prehash)

def eddsa_obj(name):
    if name == "Ed25519": return Ed25519
    if name == "Ed25519ph": return Ed25519ph
    if name == "Ed448": return Ed448
    if name == "Ed448ph": return Ed448ph
    raise NotImplementedError("Algorithm not implemented")
```

Below is a command-line tool that uses the library above to perform computations, for interactive use or for self-checking.

[A note to RFC-Editor: Please don't change the relative indentations here: This code is written in programming language where relative indentations are meaningful, so changing those changes program

meaning (authors: check this still works in AUTH48). Remove this note before publication.]

```
import sys
import binascii
```

```
from eddsa2 import Ed25519
```

```
def munge_string(s, pos, change):
    return (s[:pos] +
            int.to_bytes(s[pos] ^ change, 1, "little") +
            s[pos+1:])
```

```
# Read a file in the format of
# http://ed25519.cr.yp.to/python/sign.input
lineno = 0
while True:
    line = sys.stdin.readline()
    if not line:
        break
    lineno = lineno + 1
    print(lineno)
    fields = line.split(":")
    secret = (binascii.unhexlify(fields[0]))[:32]
    public = binascii.unhexlify(fields[1])
    msg = binascii.unhexlify(fields[2])
    signature = binascii.unhexlify(fields[3])[:64]

    privkey, pubkey = Ed25519.keygen(secret)
    assert public == pubkey
    assert signature == Ed25519.sign(privkey, pubkey, msg)
    assert Ed25519.verify(public, msg, signature)
```

```
if len(msg) == 0:
    bad_msg = b"x"
else:
    bad_msg = munge_string(msg, len(msg) // 3, 4)
    assert not Ed25519.verify(public, bad_msg, signature)
    bad_signature = munge_string(signature, 20, 8)
    assert not Ed25519.verify(public, msg, bad_signature)
    bad_signature = munge_string(signature, 40, 16)
    assert not Ed25519.verify(public, msg, bad_signature)
```

Authors' Addresses

Josefsson & Liusvaara

Expires July 22, 2016

[Page 47]

Internet-Draft

EdDSA: Ed25519 and Ed448

January 2016

Simon Josefsson
SJD AB

Email: simon@josefsson.org
URI: <http://josefsson.org/>

Ilari Liusvaara
Independent

Email: ilariliusvaara@welho.com

