          Address Protected Neighbor Discovery for Low-power and Lossy Networks
                        draft-ietf-6lo-ap-nd-11

   Abstract

      This document specifies an extension to 6LoWPAN Neighbor Discovery
      (ND) protocol defined in RFC6775 and updated in RFC8505. The new
      extension is called Address Protected Neighbor Discovery (AP-ND) and
      it protects the owner of an address against address theft and
      impersonation attacks in a low-power and lossy network (LLN). Nodes
      supporting this extension compute a cryptographic identifier (Crypto-
      ID) and use it with one or more of their Registered Addresses. The
      Crypto-ID identifies the owner of the Registered Address and can be
      used to provide proof of ownership of the Registered Addresses. Once
      an address is registered with the Crypto-ID and a proof-of-ownership
      is provided, only the owner of that address can modify the
      registration information, thereby enforcing Source Address
      Validation.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

      Neighbor Discovery Optimizations for 6LoWPAN networks [RFC6775]
      (6LoWPAN ND) adapts the original IPv6 neighbor discovery (NDv6)
      protocols defined in [RFC4861] and [RFC4862] for constrained low-
      power and lossy network (LLN). In particular, 6LoWPAN ND introduces
      a unicast host address registration mechanism that reduces the use of
      multicast. 6LoWPAN ND defines a new Address Registration Option (ARO)
      that is carried in the unicast Neighbor Solicitation (NS) and
      Neighbor Advertisement (NA) messages exchanged between a 6LoWPAN Node
      (6LN) and a 6LoWPAN Router (6LR). It also defines the Duplicate
      Address Request (DAR) and Duplicate Address Confirmation (DAC)
      messages between the 6LR and the 6LoWPAN Border Router (6LBR). In
      LLN networks, the 6LBR is the central repository of all the
      registered addresses in its domain.

      The registration mechanism in 6LoWPAN ND [RFC6775] prevents the use
      of an address if that address is already registered in the subnet
      (first come first serve). In order to validate address ownership,
      the registration mechanism enables the 6LR and 6LBR to validate the
      association between the registered address of a node, and its
      Registration Ownership Verifier (ROVR). ROVR is defined in [RFC8505]
      and it can be derived from the MAC address of the device (using the
      64-bit Extended Unique Identifier EUI-64 address format specified by
      IEEE). However, the EUI-64 can be spoofed, and therefore, any node
      connected to the subnet and aware of a registered-address-to-ROVR
      mapping could effectively fake the ROVR. This would allow the an
      attacker to steal the address and redirect traffic for that address.
      [RFC8505] defines an Extended Address Registration Option (EARO)
      option that allows to transport alternate forms of ROVRs, and is a
      pre-requisite for this specification.

      In this specification, a 6LN generates a cryptographic ID (Crypto-ID)
      and places it in the ROVR field during the registration of one (or
      more) of its addresses with the 6LR(s). Proof of ownership of the
      Crypto-ID is passed with the first registration exchange to a new
      6LR, and enforced at the 6LR. The 6LR validates ownership of the
      cryptographic ID before it creates any new registration state, or
      changes existing information.

      The protected address registration protocol proposed in this document
      enables Source Address Validation (SAVI) [RFC7039]. This ensures

that only the actual owner uses a registered address in the IPv6
source address field. A 6LN can only use a 6LR for forwarding
packets only if it has previously registered the address used in the
source field of the IPv6 packet.

The 6lo adaptation layer in [RFC4944] and [RFC6282] requires a device
to form its IPv6 addresses based on its Layer-2 address to enable a
better compression. This is incompatible with Secure Neighbor
Discovery (SeND) [RFC3971] and Cryptographically Generated Addresses
(CGAs) [RFC3972], since they derive the Interface ID (IID) in IPv6
addresses with cryptographic keys.

2. Terminology

2.1. BCP 14

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in BCP
14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

2.2. References

Terms and concepts from the following documents are used in this
specification:

o "Terms Used in Routing for Low-Power and Lossy Networks (LLNs)"
   [RFC7102],

o "SEcure Neighbor Discovery (SEND)" [RFC3971],

o "Cryptographically Generated Addresses (CGA)" [RFC3972],

o "Neighbor Discovery for IP version 6" [RFC4861] ,

o "IPv6 Stateless Address Autoconfiguration" [RFC4862],

o "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs):
   Overview, Assumptions, Problem Statement, and Goals " [RFC4919],

o "Neighbor Discovery Optimization for Low-power and Lossy Networks"
   [RFC6775], and

o "Registration Extensions for 6LoWPAN Neighbor Discovery"
   [RFC8505].

2.3. Abbreviations

   This document uses the following abbreviations:

   6BBR: 6LoWPAN Backbone Router

   6LBR: 6LoWPAN Border Router

   6LN: 6LoWPAN Node

   6LR: 6LoWPAN Router

   6CIO: Capability Indication Option

   ARO: Address Registration Option

   CIPO: Crypto-ID Parameters Option

   LLN: Low-Power and Lossy Network

   NA: Neighbor Advertisement

   NCE: Neighbor Cache Entry

   ND: Neighbor Discovery

   NDP: Neighbor Discovery Protocol

   NDPSO: NDP Signature Option

   NS: Neighbor Solicitation

   ROVR: Registration Ownership Verifier

   RPL: IPv6 Routing Protocol for LLNs

   RA: Router Advertisement

   RS: Router Solicitation

   RSAO: RSA Signature Option

   TID: Transaction ID

3. Updating RFC 8505

   This specification introduces a new token called a cryptographic
   identifier (Crypto-ID) that is used to prove indirectly the ownership
   of an address that is being registered by means of [RFC8505].

   In order to prove its ownership of a Crypto-ID, the registering node
   needs to supply certain parameters including a nonce and a signature
   that will prove that the node has the private-key corresponding to
   the public-key used to build the Crypto-ID. This specification adds
   the capability to carry new options in the NS(EARO) and the NA(EARO).
   The NS(EARO) carries a variation of the CGA Option (Section 4.3), a
   Nonce option and a variation of the RSA Signature option
   (Section 4.5) in the NS(EARO). The NA(EARO) carries a Nonce option.

4. New Fields and Options

   In order to avoid the need for new ND option types, this
   specification reuses and extends options defined in SEND [RFC3971]
   and 6LoWPAN ND [RFC6775] [RFC8505]. This applies in particular to
   the CGA option and the RSA Signature Option. This specification
   provides aliases for the specific variations of those options as used
   in this document. The presence of the EARO option in the NS/NA
   messages indicates that the options are to be processed as specified
   in this document, and not as defined in SEND [RFC3971].

4.1. New Crypto-ID

   The Crypto-ID can be used as a replacement to the MAC address in the
   ROVR field of the EARO option and the EDAR message, and is associated
   with the Registered Address. The ownership of a Crypto-ID can be
   demonstrated by cryptographic mechanisms, and by association, the
   ownership of the Registered Address can be acertained. A node in
   possession of the necessary cryptographic primitives SHOULD use
   Crypto-ID by default as ROVR in its registrations. Whether a ROVR is
   a Crypto-ID is indicated by a new "C" flag in the NS(EARO) message.

   The computation of the Crypto-ID requires the support of Elliptic
   Curve Cryptography (ECC) and that of a hash function as detailed in
   Section 6.2. The elliptic curves and the hash functions that can be
   used with this specification are listed in Table 1 in Section 8.2.
   The signature scheme that specifies which combination is used is
   signaled by a Crypto-Type in a new Crypto-ID Parameters Option (see
   Section 4.3).

4.2. Updated EARO

   This specification updates the EARO option as follows:

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     |    Status     |    Opaque     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Rsvd |C| I |R|T|     TID       |     Registration Lifetime     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   ...           Registration Ownership Verifier (ROVR)         ...
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
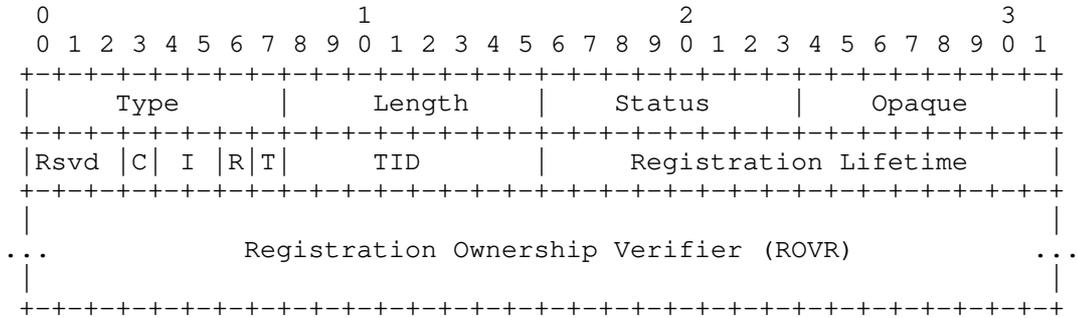
              Figure 1: Enhanced Address Registration Option

   Type: 33

   Length: 8-bit unsigned integer. The length of the option
                  (including the type and length fields) in units of 8
                  bytes.

   Status: 8-bit unsigned integer. Indicates the status of a
                  registration in the NA response. MUST be set to 0 in
                  NS messages.

   Opaque: Defined in [RFC8505].

   Rsvd (Reserved): This field is unused. It MUST be initialized to
                  zero by the sender and MUST be ignored by the
                  receiver.

   C: This "C" flag is set to indicate that the ROVR field
                  contains a Crypto-ID and that the 6LN MAY be
                  challenged for ownership as specified in this
                  document.

   I, R, T, and TID: Defined in [RFC8505].

   Registration Ownership Verifier (ROVR): When the "C" flag is set,
                  this field contains a Crypto-ID.

   This specification uses Status values "Validation Requested" and
   "Validation Failed", which are defined in [RFC8505]. No other new
   Status values are defined.

4.3. Crypto-ID Parameters Option

   This specification defines the Crypto-ID Parameters Option (CIPO), as
   a variation of the CGA Option that carries the parameters used to
   form a Crypto-ID. In order to provide cryptographic agility
   [RFC7696], this specification supports different elliptic curves,
   indicated by a Crypto-Type field. NIST P-256 [FIPS186-4] MUST be
   supported by all implementations. The Edwards-Curve Digital
   Signature Algorithm (EdDSA) curve Ed25519 (PureEdDSA) [RFC8032] MAY
   be supported as an alternate.

   The type of cryptographic algorithm used in the calculation of the
   Crypto-ID is signaled by the Crypto-Type field of the CIPO as
   specified in Table 1 in Section 8.2. Although the different
   signature schemes target similar cryptographic strength, they rely on
   different curves, hash functions, signature algorithms, and/or
   representation conventions.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |    Length     |  Pad Length   |   Reserved    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Crypto-Type  |   Modifier    |           Reserved            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    |                                                               |
    .                                                               .
    .                  Public Key (variable length)                .
    .                                                               .
    |                                                               |
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    .                                                               .
    .                          Padding                              .
    .                                                               .
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
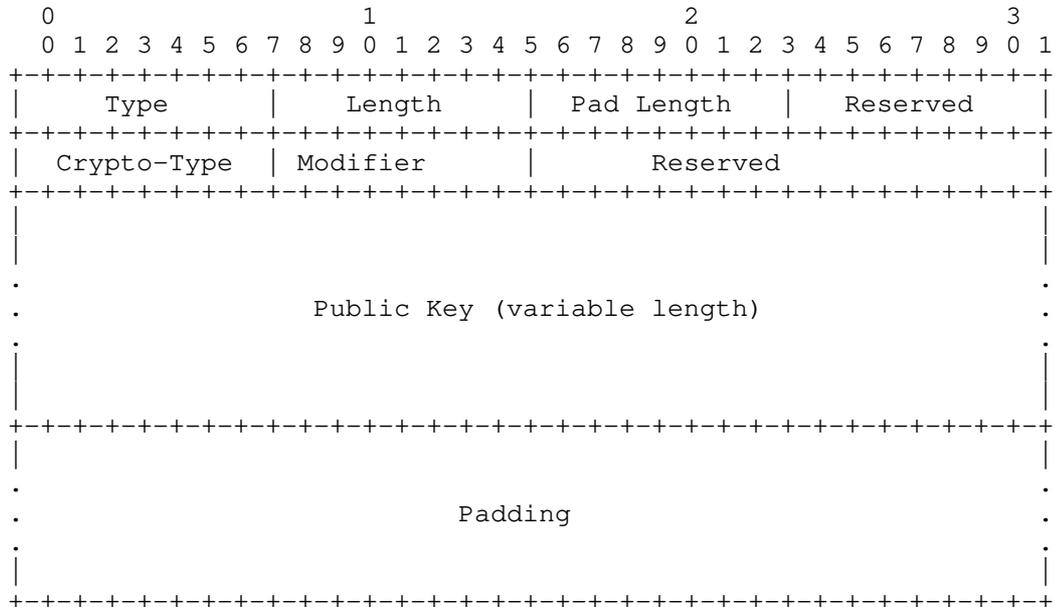
                   Figure 2: Crypto-ID Parameters Option

   Type: 11. This is the same value as the CGA Option, CIPO
                      is a particular case of the CGA option

   Length: 8-bit unsigned integer. The length of the option in
                      units of 8 octets.

   Modifier: 8-bit unsigned integer.

   Pad Length: 8-bit unsigned integer. The length of the Padding
                     field.

   Crypto-Type: The type of cryptographic algorithm used in
                     calculation Crypto-ID (see Table 1 in Section 8.2).

   Public Key: JWK-Encoded Public Key [RFC7517].

   Padding: A variable-length field making the option length a
                     multiple of 8, containing as many octets as specified
                     in the Pad Length field.

   The implementation of multiple hash functions in a constrained
   devices may consume excessive amounts of program memory.
   [I-D.ietf-lwig-curve-representations] provides information on how to
   represent Montgomery curves and (twisted) Edwards curves as curves in
   short-Weierstrass form and illustrates how this can be used to
   implement elliptic curve computations using existing implementations
   that already provide, e.g., ECDSA and ECDH using NIST [FIPS186-4]
   prime curves.

   For more details on representation conventions, we refer to
   Appendix B.

4.4. Nonce Option

   This document reuses the Nonce Option defined in section 5.3.2. of
   SEND [RFC3971] without a change.

4.5. NDP Signature Option

   This document reuses the RSA Signature Option (RSAO) defined in
   section 5.2. of SEND [RFC3971]. Admittedly, the name is ill-chosen
   since the option is extended for non-RSA Signatures and this
   specification defines an alias to avoid the confusion.

   The description of the operation on the option detailed in section
   5.2. of SEND [RFC3971] apply, but for the following changes:

   o The 128-bit CGA Message Type tag [RFC3972] for AP-ND is 0x8701
      55c8 0cca dd32 6ab7 e415 f148 84d0. (The tag value has been
      generated by the editor of this specification on random.org).

   o The signature is computed using the hash algorithm and the digital
      signature indicated in the Crypto-Type field of the CIPO option

using the private-key corresponding the public-key passed in the
CIPO.

o The alias NDP Signature Option (NDPSO) can be used to refer to the
   RSAO when used as described in this specification.

5. Protocol Scope

The scope of the protocol specified here is a 6LoWPAN Low Power Lossy
Network (LLN), typically a stub network connected to a larger IP
network via a Border Router called a 6LBR per [RFC6775]. A 6LBR has
sufficient capability to satisfy the needs of duplicate address
detection.

The 6LBR maintains registration state for all devices in its attached
LLN. Together with the first-hop router (the 6LR), the 6LBR assures
uniqueness and grants ownership of an IPv6 address before it can be
used in the LLN. This is in contrast to a traditional network that
relies on IPv6 address auto-configuration [RFC4862], where there is
no guarantee of ownership from the network, and each IPv6 Neighbor
Discovery packet must be individually secured [RFC3971].

```
             ---+-------- ...........
                |         External Network
                |
          +-----+
          |     | 6LBR
          +-----+
             o     o   o
         o     o   o      o
           o  o LLN   o    o      o
           o   o   o       (6LR)
                o           (6LN)
```
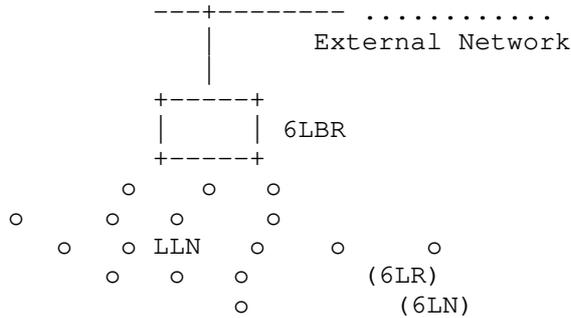
Figure 3: Basic Configuration

In a mesh network, the 6LR is directly connected to the host device.
This specification mandates that the peer-wise layer-2 security is
deployed so that all the packets from a particular host are securely
identifiable by the 6LR. The 6LR may be multiple hops away from the
6LBR. Packets are routed between the 6LR and the 6LBR via other
6LRs. This specification mandates that a chain of trust is
established so that a packet that was validated by the first 6LR can
be safely routed by other on-path 6LRs to the 6LBR.

6. Protocol Flows

   The 6LR/6LBR ensures first-come/first-serve by storing the EARO
   information including the Crypto-ID associated to the node being
   registered. The node can claim any address as long as it is the
   first to make such a claim. After a successful registration, the
   node becomes the owner of the registered address and the address is
   bound to the Crypto-ID in the 6LR/6LBR registry.

   This specification enables the 6LR to verify the ownership of the
   binding at any time assuming that the "C" flag is set. The
   verification prevents other nodes from stealing the address and
   trying to attract traffic for that address or use it as their source
   address.

   A node may use multiple IPv6 addresses at the same time. The node
   may use a same Crypto-ID, to prove the ownership of multiple IPv6
   addresses. The separation of the address and the cryptographic
   material avoids the constrained device to compute multiple keys for
   multiple addresses. The registration process allows the node to use
   the same Crypto-ID for all of its addresses.

6.1. First Exchange with a 6LR

   A 6LN registers to a 6LR that is one hop away from it with the "C"
   flag set in the EARO, indicating that the ROVR field contains a
   Crypto-ID. The Target Address in the NS message indicates the IPv6
   address that the 6LN is trying to register. The on-link (local)
   protocol interactions are shown in Figure 4. If the 6LR does not
   have a state with the 6LN that is consistent with the NS(EARO), then
   it replies with a challenge NA (EARO, status=Validation Requested)
   that contains a Nonce Option (shown as NonceLR in Figure 4). The
   Nonce option MUST contain a random Nonce value that was never used
   with this device.

   The 6LN replies to the challenge with an NS(EARO) that includes a new
   Nonce option (shown as NonceLN in Figure 4), the CIPO (Section 4.3),
   and the NDPSO containing the signature. The information associated
   to a Crypto-ID stored by the 6LR on the first NS exchange where it
   appears. The 6LR MUST store the CIPO parameters associated with the
   Crypto-ID so it can be used for more than one address.

```
  6LN                                                           6LR
   |                                                             |
   |<---------------------- RA ----------------------|          |
   |                                                 |          ^
   |-------------- NS with EARO (Crypto-ID) ------------>|       |
   |                                                 |        option
   |<- NA with EARO (status=Validation Requested), NonceLR-|   |
   |                                                 |          v
   |------- NS with EARO, CIPO, NonceLN and NDPSO -------->|     |
   |                                                             |
   |<----------------- NA with EARO --------------------|        |
   |                                                             |
   |                          ...                                |
   |                                                             |
   |-------------- NS with EARO (Crypto-ID) ------------->|       |
   |                                                             |
   |<----------------- NA with EARO --------------------|        |
   |                                                             |
   |                          ...                                |
   |                                                             |
   |-------------- NS with EARO (Crypto-ID) ------------->|       |
   |                                                             |
   |<----------------- NA with EARO --------------------|        |
   |                                                             |
```
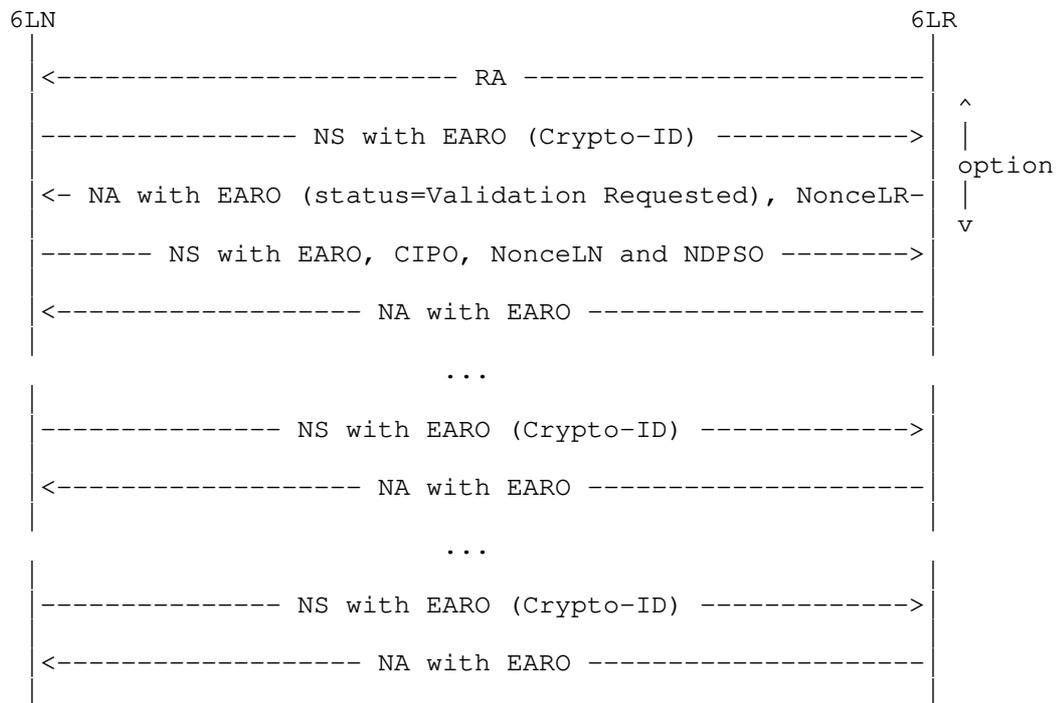
               Figure 4: On-link Protocol Operation

   The steps for the registration to the 6LR are as follows:

   o Upon the first exchange with a 6LR, a 6LN will be challenged to
      prove ownership of the Crypto-ID and the Target Address being
      registered in the Neighbor Solicitation message. When a 6LR
      receives a NS(EARO) registration with a new Crypto-ID as a ROVR,
      it SHOULD challenge by responding with a NA(EARO) with a status of
      "Validation Requested".

   o The challenge is triggered when the registration for a Source
      Link-Layer Address is not verifiable either at the 6LR or the
      6LBR. In the latter case, the 6LBR returns a status of
      "Validation Requested" in the DAR/DAC exchange, which is echoed by
      the 6LR in the NA (EARO) back to the registering node. The
      challenge MUST NOT alter a valid registration in the 6LR or the
      6LBR.

   o Upon receiving a NA(EARO) with a status of "Validation Requested",
      the registering node SHOULD retry its registration with a Crypto-
      ID Parameters Option (CIPO) (Section 4.3) that contains all the
      necessary material for building the Crypto-ID, the NonceLN that it

generated, and the NDP signature (Section 4.5) option that proves
its ownership of the Crypto-ID and intent of registering the
Target Address.

o In order to validate the ownership, the 6LR performs the same
   steps as the 6LN and rebuilds the Crypto-ID based on the
   parameters in the CIPO. It also verifies the signature contained
   in the NDPSO option. If the Crypto-ID does not match with the
   public-key in the CIPO option, or if the signature in the NDPSO
   option cannot be verified, the validation fails.

o If the 6LR fails to validate the signed NS(EARO), it responds with
   a status of "Validation Failed". After receiving a NA(EARO) with
   a status of "Validation Failed", the registering node SHOULD try
   to register an alternate target address in the NS message.

6.2. NDPSO generation and verification

   The signature generated by the 6LN to provide proof-of-ownership of
   the private-key is carried in the NDP Signature Option (NDPSO). It
   is generated by the 6LN in a fashion that depends on the Crypto-Type
   (see Table 1 in Section 8.2) chosen by the 6LN as follows:

   o Concatenate the following in the order listed:

      1. 128-bit type tag (in network byte order)

      2. JWK-encoded public key

      3. the 16-byte Target Address (in network byte order) sent in the
          Neighbor Solicitation (NS) message. It is the address which
          the 6LN is registering with the 6LR and 6LBR.

      4. NonceLR received from the 6LR (in network byte order) in the
          Neighbor Advertisement (NA) message. The random nonce is at
          least 6 bytes long as defined in [RFC3971].

      5. NonceLN sent from the 6LN (in network byte order). The random
          nonce is at least 6 bytes long as defined in [RFC3971].

      6. The length of the ROVR field in the NS message containing the
          Crypto-ID that was sent.

      7. 1-byte (in network byte order) Crypto-Type value sent in the
          CIPO option.

   o Depending on the Crypto-Type, apply the hash function on this
      concatenation.

o Depending on the Crypto-Type, sign the hash output with ECDSA (if
   curve P-256 is used) or sign the hash with EdDSA (if curve Ed25519
   (PureEdDSA)).

The 6LR on receiving the NDPSO and CIPO options first hashes the JWK
encoded public-key in the CIPO option to make sure that the leftmost
bits up to the size of the ROVR match. Only if the check is
successful, it tries to verify the signature in the NDPSO option
using the following.

o Concatenate the following in the order listed:

   1. 128-bit type tag (in network byte order)

   2. JWK-encoded public key received in the CIPO option

   3. the 16-byte Target Address (in network byte order) received in
       the Neighbor Solicitation (NS) message. It is the address
       which the 6LN is registering with the 6LR and 6LBR.

   4. NonceLR sent in the Neighbor Advertisement (NA) message. The
       random nonce is at least 6 bytes long as defined in [RFC3971].

   5. NonceLN received from the 6LN (in network byte order) in the
       NS message. The random nonce is at least 6 bytes long as
       defined in [RFC3971].

   6. The length of the ROVR field in the NS message containing the
       Crypto-ID that was received.

   7. 1-byte (in network byte order) Crypto-Type value received in
       the CIPO option.

o Depending on the Crypto-Type indicated by the (6LN) in the CIPO,
   apply the hash function on this concatenation.

o Verify the signature with the public-key received and the locally
   computed values. If the verification succeeds, the 6LR and 6LBR
   add the state information about the Crypto-ID, public-key and
   Target Address being registered to their database.

6.3. Multihop Operation

In a multihop 6LoWPAN, the registration with Crypto-ID is propagated
to 6LBR as described in this section. If the 6LR and the 6LBR
maintain a security association, then there is no need to propagate
the proof of ownership to the 6LBR.

A new device that joins the network auto-configures an address and
performs an initial registration to a neighboring 6LR with an NS
message that carries an Address Registration Option (EARO) [RFC8505].
The 6LR validates the address with an 6LBR using a DAR/DAC exchange,
and the 6LR confirms (or denies) the address ownership with an NA
message that also carries an Address Registration Option.

Figure 5 illustrates a registration flow all the way to a 6LowPAN
Backbone Router (6BBR) [I-D.ietf-6lo-backbone-router].

```
       6LN               6LR               6LBR              6BBR
        |                 |                 |                 |
        |    NS(EARO)     |                 |                 |
        |---------------->|                 |                 |
        |                 |  Extended DAR   |                 |
        |                 |---------------->|                 |
        |                 |                 |                 |
        |                 |                 | proxy NS(EARO)  |
        |                 |                 |---------------->|
        |                 |                 |                 |   NS(DAD)
        |                 |                 |                 |   ------>
        |                 |                 |                 |
        |                 |                 |                 |   <wait>
        |                 |                 |                 |
        |                 |                 | proxy NA(EARO)  |
        |                 |                 |<----------------|
        |                 |  Extended DAC   |                 |
        |                 |<----------------|                 |
        |    NA(EARO)     |                 |                 |
        |<----------------|                 |                 |
        |                 |                 |                 |
```
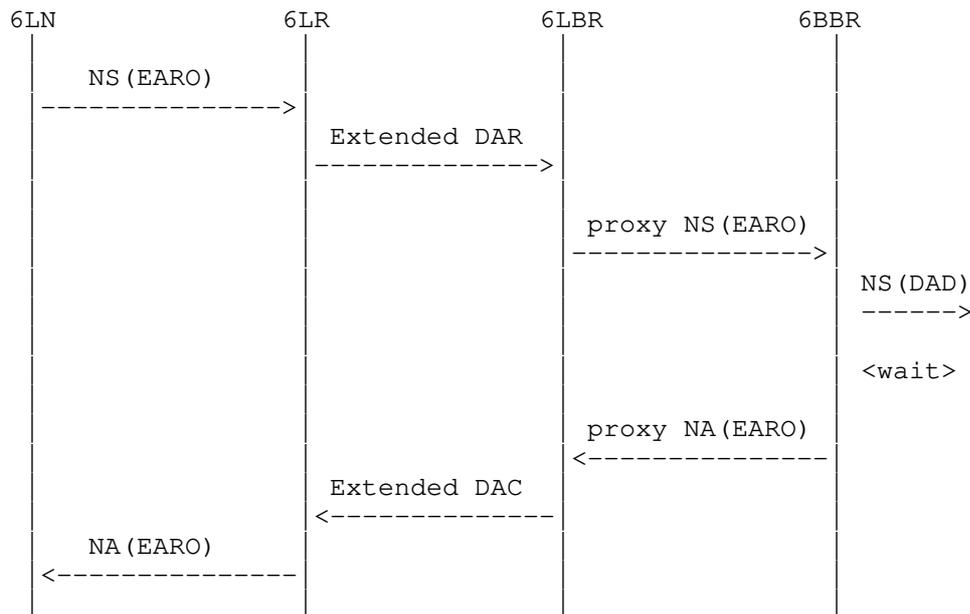
                   Figure 5: (Re-)Registration Flow

In a multihop 6LoWPAN, a 6LBR sends RAs with prefixes downstream and
the 6LR receives and relays them to the nodes. 6LR and 6LBR
communicate using ICMPv6 Duplicate Address Request (DAR) and
Duplicate Address Confirmation (DAC) messages. The DAR and DAC use
the same message format as NS and NA, but have different ICMPv6 type
values.

In AP-ND we extend DAR/DAC messages to carry cryptographically
generated ROVR. In a multihop 6LoWPAN, the node exchanges the
messages shown in Figure 5. The 6LBR must identify who owns an
address (EUI-64) to defend it, if there is an attacker on another
6LR.

7. Security Considerations

7.1. Inheriting from RFC 3971

   Observations regarding the following threats to the local network in
   [RFC3971] also apply to this specification.

   Neighbor Solicitation/Advertisement Spoofing

      Threats in section 9.2.1 of RFC3971 apply. AP-ND counters the
      threats on NS(EARO) messages by requiring that the NDP Signature
      and CIPO options be present in these solicitations.

   Duplicate Address Detection DoS Attack

      Inside the LLN, Duplicate Addresses are sorted out using the ROVR,
      which differentiates it from a movement. DAD coming from the
      backbone are not forwarded over the LLN, which provides some
      protection against DoS attacks inside the resource-constrained
      part of the network. Over the backbone, the EARO option is
      present in NS/NA messages. This protects against misinterpreting
      a movement for a duplication, and enables the backbone routers to
      determine which one has the freshest registration and is thus the
      best candidate to validate the registration for the device
      attached to it. But this specification does not guarantee that
      the backbone router claiming an address over the backbone is not
      an attacker.

   Router Solicitation and Advertisement Attacks

      This specification does not change the protection of RS and RA
      which can still be protected by SEND.

   Replay Attacks

      Nonces (NonceLR and NonceLN) generated by the 6LR and 6LN
      guarantees against replay attacks of the NS(EARO).

   Neighbor Discovery DoS Attack

      A rogue node that managed to access the L2 network may form many
      addresses and register them using AP-ND. The perimeter of the
      attack is all the 6LRs in range of the attacker. The 6LR must
      protect itself against overflows and reject excessive registration
      with a status 2 "Neighbor Cache Full". This effectively blocks
      another (honest) 6LN from registering to the same 6LR, but the 6LN
      may register to other 6LRs that are in its range but not in that
      of the rogue.

7.2. Related to 6LoWPAN ND

   The threats discussed in 6LoWPAN ND [RFC6775][RFC8505] also apply
   here. Compared with SeND, this specification saves about 1Kbyte in
   every NS/NA message. Also, this specification separates the
   cryptographic identifier from the registered IPv6 address so that a
   node can have more than one IPv6 address protected by the same
   cryptographic identifier. SeND forces the IPv6 address to be
   cryptographic since it integrates the CGA as the IID in the IPv6
   address. This specification frees the device to form its addresses
   in any fashion, thereby enabling not only 6LoWPAN compression which
   derives IPv6 addresses from Layer-2 addresses but also privacy
   addresses.

7.3. ROVR Collisions

   A collision of Registration Ownership Verifiers (ROVR) (i.e., the
   Crypto-ID in this specification) is possible, but it is a rare event.
   The formula for calculating the probability of a collision is $1 - e^{-k^2/(2n)}$ where n is the maximum population size (2^{64} here,
   1.84E19) and K is the actual population (number of nodes). If the
   Crypto-ID is 64-bits (the least possible size allowed), the chance of
   a collision is 0.01% when the network contains 66 million nodes.
   Moreover, the collision is only relevant when this happens within one
   stub network (6LBR). In the case of such a collision, an attacker
   may be able to claim the registered address of an another legitimate
   node. However for this to happen, the attacker would also need to
   know the address which was registered by the legitimate node. This
   registered address is never broadcasted on the network and therefore
   providing an additional 64-bits that an attacker must correctly
   guess. To prevent address disclosure, it is RECOMMENDED that nodes
   derive the address being registered independently of the ROVR.

7.4. Implementation Attacks

   The signature schemes referenced in this specification comply with
   NIST [FIPS186-4] or Crypto Forum Research Group (CFRG) standards
   [RFC8032] and offer strong algorithmic security at roughly 128-bit
   security level. These signature schemes use elliptic curves that
   were either specifically designed with exception-free and constant-
   time arithmetic in mind [RFC7748] or where one has extensive
   implementation experience of resistance to timing attacks
   [FIPS186-4]. However, careless implementations of the signing
   operations could nevertheless leak information on private keys. For
   example, there are micro-architectural side channel attacks that
   implementors should be aware of [breaking-ed25519]. Implementors
   should be particularly aware that a secure implementation of Ed25519
   requires a protected implementation of the hash function SHA-512,

   whereas this is not required with implementations of SHA-256 used
   with ECDSA.

7.5. Cross-Protocol Attacks

   The same private key MUST NOT be reused with more than one signature
   scheme in this specification.

8. IANA considerations

8.1. CGA Message Type

   This document defines a new 128-bit value under the CGA Message Type
   [RFC3972] name space: 0x8701 55c8 0cca dd32 6ab7 e415 f148 84d0.

8.2. Crypto-Type Subregistry

   IANA is requested to create a new subregistry "Crypto-Type
   Subregistry" in the "Internet Control Message Protocol version 6
   (ICMPv6) Parameters". The registry is indexed by an integer in the
   interval 0..255 and contains an Elliptic Curve, a Hash Function, a
   Signature Algorithm, and Representation Conventions, as shown in
   Table 1, which together specify a signature scheme. The following
   Crypto-Type values are defined in this document:

Crypto-Type value	0 (ECDSA256)	1 (Ed25519)	2 (ECDSA25519)
Elliptic curve	NIST P-256 [FIPS186-4]	Curve25519 [RFC7748]	Curve25519 [RFC7748]
Hash function	SHA-256 [RFC6234]	SHA-512 [RFC6234]	SHA-256 [RFC6234]
Signature algorithm	ECDSA [FIPS186-4]	Ed25519 [RFC8032]	ECDSA [FIPS186-4]
Representation conventions	Weierstrass, (un)compressed, MSB/msb first	Edwards, compressed, LSB/lsb first	Weierstrass, (un)compressed, MSB/msb first
Defining specification	RFC THIS	RFC THIS	RFC THIS

                        Table 1: Crypto-Types

   New Crypto-Type values providing similar or better security (with
   less code) may be defined in the future.

   Assignment of new values for new Crypto-Type MUST be done through
   IANA with "Specification Required" and "IESG Approval" as defined in
   [RFC8126].

9. Acknowledgments

   Many thanks to Charlie Perkins for his in-depth review and
   constructive suggestions. We are also especially grateful to Robert
   Moskowitz for his comments that led to many improvements.

10. References

10.1. Normative References

   [FIPS186-4]
              FIPS 186-4, "Digital Signature Standard (DSS), Federal
              Information Processing Standards Publication 186-4", US
              Department of Commerce/National Institute of Standards and
              Technology , July 2013.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

   [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander,
              "SEcure Neighbor Discovery (SEND)", RFC 3971,
              DOI 10.17487/RFC3971, March 2005,
              <https://www.rfc-editor.org/info/rfc3971>.

   [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)",
              RFC 3972, DOI 10.17487/RFC3972, March 2005,
              <https://www.rfc-editor.org/info/rfc3972>.

   [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
              "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
              DOI 10.17487/RFC4861, September 2007,
              <https://www.rfc-editor.org/info/rfc4861>.

   [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
              Address Autoconfiguration", RFC 4862,
              DOI 10.17487/RFC4862, September 2007,
              <https://www.rfc-editor.org/info/rfc4862>.

   [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C.
              Bormann, "Neighbor Discovery Optimization for IPv6 over
              Low-Power Wireless Personal Area Networks (6LoWPANs)",
              RFC 6775, DOI 10.17487/RFC6775, November 2012,
              <https://www.rfc-editor.org/info/rfc6775>.

   [RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517,
              DOI 10.17487/RFC7517, May 2015,
              <https://www.rfc-editor.org/info/rfc7517>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

   [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C.
              Perkins, "Registration Extensions for IPv6 over Low-Power
              Wireless Personal Area Network (6LoWPAN) Neighbor
              Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018,
              <https://www.rfc-editor.org/info/rfc8505>.

   [SEC1]   SEC1, "SEC 1: Elliptic Curve Cryptography, Version 2.0",
              Standards for Efficient Cryptography , June 2009.

10.2. Informative references

   [breaking-ed25519]
              Samwel, N., Batina, L., Bertoni, G., Daemen, J., and R.
              Susella, "Breaking Ed25519 in WolfSSL", Cryptographers'
              Track at the RSA Conference , 2018,
              <https://link.springer.com/
              chapter/10.1007/978-3-319-76953-0_1>.

   [I-D.ietf-6lo-backbone-router]
              Thubert, P., Perkins, C., and E. Levy-Abegnoli, "IPv6
              Backbone Router", draft-ietf-6lo-backbone-router-11 (work
              in progress), February 2019.

   [I-D.ietf-lwig-curve-representations]
              Struik, R., "Alternative Elliptic Curve Representations",
              draft-ietf-lwig-curve-representations-01 (work in
              progress), November 2018.

   [RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6
              over Low-Power Wireless Personal Area Networks (6LoWPANs):
              Overview, Assumptions, Problem Statement, and Goals",
              RFC 4919, DOI 10.17487/RFC4919, August 2007,
              <https://www.rfc-editor.org/info/rfc4919>.

   [RFC4944]   Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler,
               "Transmission of IPv6 Packets over IEEE 802.15.4
               Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007,
               <https://www.rfc-editor.org/info/rfc4944>.

   [RFC6234]   Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms
               (SHA and SHA-based HMAC and HKDF)", RFC 6234,
               DOI 10.17487/RFC6234, May 2011,
               <https://www.rfc-editor.org/info/rfc6234>.

   [RFC6282]   Hui, J., Ed. and P. Thubert, "Compression Format for IPv6
               Datagrams over IEEE 802.15.4-Based Networks", RFC 6282,
               DOI 10.17487/RFC6282, September 2011,
               <https://www.rfc-editor.org/info/rfc6282>.

   [RFC7039]   Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed.,
               "Source Address Validation Improvement (SAVI) Framework",
               RFC 7039, DOI 10.17487/RFC7039, October 2013,
               <https://www.rfc-editor.org/info/rfc7039>.

   [RFC7102]   Vasseur, JP., "Terms Used in Routing for Low-Power and
               Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January
               2014, <https://www.rfc-editor.org/info/rfc7102>.

   [RFC7217]   Gont, F., "A Method for Generating Semantically Opaque
               Interface Identifiers with IPv6 Stateless Address
               Autoconfiguration (SLAAC)", RFC 7217,
               DOI 10.17487/RFC7217, April 2014,
               <https://www.rfc-editor.org/info/rfc7217>.

   [RFC7696]   Housley, R., "Guidelines for Cryptographic Algorithm
               Agility and Selecting Mandatory-to-Implement Algorithms",
               BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015,
               <https://www.rfc-editor.org/info/rfc7696>.

   [RFC7748]   Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves
               for Security", RFC 7748, DOI 10.17487/RFC7748, January
               2016, <https://www.rfc-editor.org/info/rfc7748>.

   [RFC8032]   Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital
               Signature Algorithm (EdDSA)", RFC 8032,
               DOI 10.17487/RFC8032, January 2017,
               <https://www.rfc-editor.org/info/rfc8032>.

   [RFC8126]   Cotton, M., Leiba, B., and T. Narten, "Guidelines for
               Writing an IANA Considerations Section in RFCs", BCP 26,
               RFC 8126, DOI 10.17487/RFC8126, June 2017,
               <https://www.rfc-editor.org/info/rfc8126>.

Appendix A.   Requirements Addressed in this Document

   In this section we state requirements of a secure neighbor discovery
   protocol for low-power and lossy networks.

   o The protocol MUST be based on the Neighbor Discovery Optimization
      for Low-power and Lossy Networks protocol defined in [RFC6775].
      RFC6775 utilizes optimizations such as host-initiated interactions
      for sleeping resource-constrained hosts and elimination of
      multicast address resolution.

   o New options to be added to Neighbor Solicitation messages MUST
      lead to small packet sizes, especially compared with existing
      protocols such as SEcure Neighbor Discovery (SEND). Smaller
      packet sizes facilitate low-power transmission by resource-
      constrained nodes on lossy links.

   o The support for this registration mechanism SHOULD be extensible
      to more LLN links than IEEE 802.15.4 only. Support for at least
      the LLN links for which a 6lo "IPv6 over foo" specification
      exists, as well as Low-Power Wi-Fi SHOULD be possible.

   o As part of this extension, a mechanism to compute a unique
      Identifier should be provided with the capability to form a Link
      Local Address that SHOULD be unique at least within the LLN
      connected to a 6LBR.

   o The Address Registration Option used in the ND registration SHOULD
      be extended to carry the relevant forms of Unique Interface
      Identifier.

   o The Neighbor Discovery should specify the formation of a site-
      local address that follows the security recommendations from
      [RFC7217].

Appendix B.   Representation Conventions

B.1. Signature Schemes

   The signature scheme ECDSA256 corresponding to Crypto-Type 0 is
   ECDSA, as specified in [FIPS186-4], instantiated with the NIST prime
   curve P-256, as specified in Appendix B of [FIPS186-4], and the hash
   function SHA-256, as specified in [RFC6234], where points of this
   NIST curve are represented as points of a short-Weierstrass curve
   (see [FIPS186-4]) and are encoded as octet strings in most-
   significant-bit first (msb) and most-significant-byte first (MSB)
   order. The signature itself consists of two integers (r and s),
   which are each encoded as fixed-size octet strings in most-

significant-bit first and most-significant-byte first order. For
details on ECDSA, see [FIPS186-4]; for details on the integer
encoding, see Appendix B.2.

The signature scheme Ed25519 corresponding to Crypto-Type 1 is EdDSA,
as specified in [RFC8032], instantiated with the Montgomery curve
Curve25519, as specified in [RFC7748], and the hash function SHA-512,
as specified in [RFC6234], where points of this Montgomery curve are
represented as points of the corresponding twisted Edwards curve (see
Appendix B.3) and are encoded as octet strings in least-significant-
bit first (lsb) and least-significant-byte first (LSB) order. The
signature itself consists of a bit string that encodes a point of
this twisted Edwards curve, in compressed format, and an integer
encoded in least-significant-bit first and least-significant-byte
first order. For details on EdDSA and on the encoding conversions,
see the specification of pure Ed25519 in . [RFC8032]

The signature scheme ECDSA25519 corresponding to Crypto-Type 2 is
ECDSA, as specified in [FIPS186-4], instantiated with the Montgomery
curve Curve25519, as specified in [RFC7748], and the hash function
SHA-256, as specified in [RFC6234], where points of this Montgomery
curve are represented as points of a corresponding curve in short-
Weierstrass form (see Appendix B.3) and are encoded as octet strings
in most-significant-bit first and most-significant-byte first order.
The signature itself consists of a bit string that encodes two
integers, each encoded as fixed-size octet strings in most-
significant-bit first and most-significant-byte first order. For
details on ECDSA, see [FIPS186-4]; for details on the integer
encoding, see Appendix B.2

B.2. Integer Representation for ECDSA signatures

With ECDSA, each signature is a pair (r, s) of integers [FIPS186-4].
Each integer is encoded as a fixed-size 256-bit bit string, where
each integer is represented according to the Field Element to Octet
String and Octet String to Bit String conversion rules in [SEC1] and
where the ordered pair of integers is represented as the
rightconcatenation of the resulting representation values. The
inverse operation follows the corresponding Bit String to Octet
String and Octet String to Field Element conversion rules of [SEC1].

B.3. Alternative Representations of Curve25519

The elliptic curve Curve25519, as specified in [RFC7748], is a so-
called Montgomery curve. Each point of this curve can also be
represented as a point of a twisted Edwards curve or as a point of an
elliptic curve in short-Weierstrass form, via a coordinate
transformation (a so-called isomorphic mapping). The parameters of

the Montgomery curve and the corresponding isomorphic curves in
twisted Edwards curve and short-Weierstrass form are as indicated
below. Here, the domain parameters of the Montgomery curve
Curve25519 and of the twisted Edwards curve Edwards25519 are as
specified in [RFC7748]; the domain parameters of the elliptic curve
Wei25519 in short-Weierstrass curve comply with Section 6.1.1 of
[FIPS186-4]. For details of the coordinate transformation referenced
above, see [RFC7748] and [I-D.ietf-lwig-curve-representations].

General parameters (for all curve models):

p $2^{255}-19$

    (=0x7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff
    ffffffff ffffffed)

h   8

n   72370055773322622139731865630429942408571163593799076060019509382
    85454250989

    (=2^{252} + 0x14def9de a2f79cd6 5812631a 5cf5d3ed)

Montgomery curve-specific parameters (for Curve25519):

A   486662

B   1

Gu 9 (=0x9)

Gv 14781619447589544791020593568409986887264606134616475288964881837
    755586237401

    (=0x20ae19a1 b8a086b4 e01edd2c 7748d14c 923d4d7e 6d7c61b2
    29e9c5a2 7eced3d9)

Twisted Edwards curve-specific parameters (for Edwards25519):

a   -1 (-0x01)

d   -121665/121666

    (=370957059346694393431380835087545651895421138798432190163887855
    33085940283555)

    (=0x52036cee 2b6ffe73 8cc74079 7779e898 00700a4d 4141d8ab
    75eb4dca 135978a3)

Gx   1511222134953540077250115140958853151145401269304185720604611328
     3949847762202

     (=0x216936d3 cd6e53fe c0a4e231 fdd6dc5c 692cc760 9525a7b2
     c9562d60 8f25d51a)

Gy   4/5

     (=4631683569492647816942839400347516314130799386625622561578303360
     3165251855960)

     (=0x66666666 66666666 66666666 66666666 66666666 66666666
     66666666 66666658)

Weierstrass curve-specific parameters (for Wei25519):

a   1929868153955269923726183083478131797554499744427342733990959733
     4573241639236

     (=0x2aaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa
     aaaaaa98 4914a144)

b   5575174666981890890764528907825714081824110372790101231529440083
     7956729358436

     (=0x7b425ed0 97b425ed 097b425e d097b425 ed097b42 5ed097b4
     260b5e9c 7710c864)

GX   1929868153955269923726183083478131797554499744427342733990959733
     4652188435546

     (=0x2aaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa
     aaaaaaaa aaad245a)

GY   1478161944758954479102059356840998688726460613461647528896488183
     7755586237401

     (=0x20ae19a1 b8a086b4 e01edd2c 7748d14c 923d4d7e 6d7c61b2
     29e9c5a2 7eced3d9)

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis 06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Behcet Sarikaya

Email: sarikaya@ieee.org

Mohit Sethi
Ericsson
Jorvas 02420
Finland

Email: mohit@piuha.net

Rene Struik
Struik Security Consultancy

Email: rstruik.ext@gmail.com