Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012

Abstract

The purpose of this document is to make the specifications of the cryptographic algorithms defined by the Russian national standards GOST R 34.10-2012 and GOST R 34.11-2012 available to the Internet community for their implementation in the cryptographic protocols based on the accompanying algorithms.

These specifications define the pseudorandom functions, the key agreement algorithm based on the Diffie-Hellman algorithm and a hash function, the parameters of elliptic curves, the key derivation functions, and the key export functions.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7836.
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.

Table of Contents

1. Introduction ......................................................... 3
2. Conventions Used in This Document ................................. 3
3. Basic Terms, Definitions, and Notations ............................ 3
4. Algorithm Descriptions .............................................. 6
   4.1. HMAC Functions .................................................. 6
   4.2. Pseudorandom Functions .......................................... 7
   4.3. VKO Algorithms for Key Agreement ............................... 8
   4.4. The Key Derivation Function KDF_TREE_GOSTR3411_2012_256 . 10
   4.5. The Key Derivation Function KDF_GOSTR3411_2012_256  ........ 11
   4.6. Key Wrap and Key Unwrap ....................................... 11
5. The Parameters of Elliptic Curves ................................. 12
   5.1. Canonical Form .................................................. 13
   5.2. Twisted Edwards Form ........................................... 14
6. Security Considerations .............................................. 15
7. References ............................................................. 16
   7.1. Normative References ........................................... 16
   7.2. Informative References .......................................... 17
Appendix A. Values of the Parameter Sets .............................. 18
   A.1. Canonical Form Parameters .................................... 18
   A.2. Twisted Edwards Form Parameters ............................... 20
Appendix B. Test Examples ................................................ 22
Appendix C. GOST 28147-89 Parameter Set .............................. 30
Acknowledgments ........................................................ 30
Authors’ Addresses ...................................................... 30
1. Introduction

The accompanying algorithms are intended for the implementation of cryptographic protocols. This memo contains a description of the accompanying algorithms based on the Russian national standards GOST R 34.10-2012 [GOST3410-2012] and GOST R 34.11-2012 [GOST3411-2012]. The English versions of these standards can be found in [RFC7091] and [RFC6986]; the English version of the encryption standard GOST 28147-89 [GOST28147-89] (which is used in the key export functions) can be found in [RFC5830].

The specifications of algorithms and parameters proposed in this memo are provided on the basis of experience in the development of the cryptographic protocols, as described in [RFC4357], [RFC4490], and [RFC4491].

This memo describes the pseudorandom functions, the key agreement algorithm based on the Diffie-Hellman algorithm and a hash function, the parameters of elliptic curves, the key derivation functions, and the key export functions necessary to ensure interoperability of security protocols that make use of the Russian cryptographic standards GOST R 34.10-2012 [GOST3410-2012] digital signature algorithm and GOST R 34.11-2012 [GOST3411-2012] cryptographic hash function.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Basic Terms, Definitions, and Notations

This document uses the following terms and definitions for the sets and operations on the elements of these sets:

- **(xor)**: Exclusive-or of two binary vectors of the same length.

- **V_n**: The finite vector space over GF(2) of dimension n, n >= 0, with the (xor) operation. For n = 0, the V_0 space consists of a single empty element of size 0. If U is an element of V_n, then U = (u_(n-1), u_(n-2), ..., u_1, u_0), where u_i in {0, 1}. 
The set of byte vectors of size \( r, r \geq 0 \), for \( r = 0 \) the \( V_{(8, r)} \) set consists of a single empty element of size 0. If \( W \) is an element of \( V_{(8, r)} \), \( r > 0 \), then \( W = (w^0, w^1, \ldots, w^{(r-1)}) \), where \( w^0, w^1, \ldots, w^{(r-1)} \) are elements of \( V_8 \).

**Bit representation**

The bit representation of the element \( W = (w^0, w^1, \ldots, w^{(r-1)}) \) of \( V_{(8, r)} \) is an element \( (w_{(8r-1)}, w_{(8r-2)}, \ldots, w_1, w_0) \) of \( V_{(8r)} \), where \( w^0 = (w_7, w_6, \ldots, w_0) \), \( w^1 = (w_15, w_14, \ldots, w_8) \), \ldots, \( w^{(r-1)} = (w_{(8r-1)}, w_{(8r-2)}, \ldots, w_{(8r-8)}) \) are elements of \( V_8 \).

**Byte representation**

If \( n \) is a multiple of 8, \( r = n/8 \), then the byte representation of the element \( W = (w_{(n-1)}, w_{(n-2)}, \ldots, w_0) \) of \( V_n \) is a byte vector \( (w^0, w^1, \ldots, w^{(r-1)}) \) of \( V_{(8, r)} \), where \( w^0 = (w_7, w_6, \ldots, w_0) \), \( w^1 = (w_{15}, w_{14}, \ldots, w_8) \), \ldots, \( w^{(r-1)} = (w_{(8r-1)}, w_{(8r-2)}, \ldots, w_{(8r-8)}) \) are elements of \( V_8 \).

**A|B**

Concatenation of byte vectors \( A \) and \( B \), i.e., if \( A \) in \( V_{(8, r1)} \), \( B \) in \( V_{(8, r2)} \), \( A = (a^0, a^1, \ldots, a^{(r1-1)}) \) and \( B = (b^0, b^1, \ldots, b^{(r2-1)}) \), then \( A|B = (a^0, a^1, \ldots, a^{(r1-1)}, b^0, b^1, \ldots, b^{(r2-1)}) \) is an element of \( V_{(8, r1+r2)} \).

**K (key)**

An arbitrary element of \( V_n \). If \( K \) in \( V_n \), then its size (in bits) is equal to \( n \), where \( n \) can be an arbitrary natural number.
This memo uses the following abbreviations and symbols:

<table>
<thead>
<tr>
<th>Symbols</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>H_256</td>
<td>GOST R 34.11-2012 hash function with 256-bit output</td>
</tr>
<tr>
<td>H_512</td>
<td>GOST R 34.11-2012 hash function with 512-bit output</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed-based Message Authentication Code. A function for calculating a message authentication code, based on a hash function in accordance with [RFC2104]</td>
</tr>
<tr>
<td>PRF</td>
<td>A pseudorandom function, i.e., a transformation that allows generation of a pseudorandom sequence of bytes</td>
</tr>
<tr>
<td>KDF</td>
<td>A key derivation function, i.e., a transformation that allows keys and keying material to be derived from the root key and additional input using a pseudorandom function</td>
</tr>
<tr>
<td>VKO</td>
<td>A key agreement algorithm based on the Diffie-Hellman algorithm and a hash function</td>
</tr>
</tbody>
</table>

To generate a byte sequence of the size $r$ with functions that give a longer output, the output is truncated to the first $r$ bytes. This remark applies to the following functions:

- the functions described in Section 4.2;
- KDF_TREE_GOSTR3411_2012_256 described in Section 4.4;
- KDF_GOSTR3411_2012_256 described in Section 4.5.

Hereinafter, all data are provided in byte representation unless otherwise specified.

If a function is defined outside this document (e.g., H_256) and its definition requires arguments in bit representation, it is assumed that the bit representations of the arguments are formed immediately before the calculation of the function (in particular, immediately after the application of the operation (|) to the byte representation of the arguments).

If the output of another function defined outside of this document is used as an argument of the functions defined below and it has the bit representation, then it is assumed that an output MUST have a length
that is a multiple of 8 and that it will be translated into the byte representation in advance.

When a point on an elliptic curve is given to an input of a hash function, affine coordinates for short Weierstrass form are used (see Section 5): an x coordinate value is fed first, a y coordinate value is fed second, both in little-endian format.

4. Algorithm Descriptions

4.1. HMAC Functions

This section defines the HMAC transformations based on the GOST R 34.11-2012 [GOST3411-2012] algorithm.

4.1.1. HMAC_GOSTR3411_2012_256

This HMAC transformation is based on the GOST R 34.11-2012 [GOST3411-2012] hash function with 256-bit output. The object identifier of this transformation is shown below:

id-tc26-hmac-gost-3411-12-256::= {iso(1) member-body(2) ru(643) rosstandart(7) tc26(1) algorithms(1) mac(4) hmac-gost-3411-12-256(1)}.

This algorithm uses H_256 as a hash function for HMAC, described in [RFC2104]. The method of forming the values of ipad and opad is also specified in [RFC2104]. The size of HMAC_GOSTR3411_2012_256 output is equal to 32 bytes, the block size of the iterative procedure for the H_256 compression function is equal to 64 bytes (in the notation of [RFC2104], L = 32 and B = 64, respectively).

4.1.2. HMAC_GOSTR3411_2012_512

This HMAC transformation is based on the GOST R 34.11-2012 [GOST3411-2012] hash function with 512-bit output. The object identifier of this transformation is shown below:

id-tc26-hmac-gost-3411-12-512::= {iso(1) member-body(2) ru(643) rosstandart(7) tc26(1) algorithms(1) mac(4) hmac-gost-3411-12-512(2)}.

This algorithm uses H_512 as a hash function for HMAC, described in [RFC2104]. The method of forming the values of ipad and opad is also specified in [RFC2104]. The size of HMAC_GOSTR3411_2012_512 output is equal to 64 bytes, the block size of the iterative procedure for the H_512 compression function is equal to 64 bytes (in the notation of [RFC2104], L = 64 and B = 64, respectively).
4.2. Pseudorandom Functions

This section defines four HMAC-based PRF transformations recommended for usage. Two of them are designed for the Transport Layer Security (TLS) protocol and two are designed for the IPsec protocol.

4.2.1. PRFs for the TLS Protocol

4.2.1.1. PRF_TLS_GOSTR3411_2012_256

This is the transformation providing the pseudorandom function for the TLS protocol (1.0 and higher versions) in accordance with GOST R 34.11-2012 [GOST3411-2012]. It uses the P_GOSTR3411_2012_256 function that is similar to the P_hash function defined in Section 5 of [RFC5246], where the HMAC_GOSTR3411_2012_256 function (defined in Section 4.1.1 of this document) is used as the HMAC_hash function.

\[
\text{PRF_TLS_GOSTR3411_2012_256} (\text{secret}, \text{label}, \text{seed}) = \text{P_GOSTR3411_2012_256} (\text{secret}, \text{label} \mid \text{seed}).
\]

Label and seed values MUST be assigned by a protocol, their lengths SHOULD be fixed by a protocol in order to avoid possible collisions.

4.2.1.2. PRF_TLS_GOSTR3411_2012_512

This is the transformation providing the pseudorandom function for the TLS protocol (1.0 and higher versions) in accordance with GOST R 34.11-2012 [GOST3411-2012]. It uses the P_GOSTR3411_2012_512 function that is similar to the P_hash function defined in Section 5 of [RFC5246], where the HMAC_GOSTR3411_2012_512 function (defined in Section 4.1.2 of this document) is used as the HMAC_hash function.

\[
\text{PRF_TLS_GOSTR3411_2012_512} (\text{secret}, \text{label}, \text{seed}) = \text{P_GOSTR3411_2012_512} (\text{secret}, \text{label} \mid \text{seed}).
\]

Label and seed values MUST be assigned by a protocol, their lengths SHOULD be fixed by a protocol in order to avoid possible collisions.

4.2.2. PRFs for the IKEv2 Protocol Based on GOST R 34.11-2012

The specification for the Internet Key Exchange protocol version 2 (IKEv2) [RFC7296] defines the usage of PRFs in various parts of the protocol for the purposes of generating and authenticating keying material.

IKEv2 has no default PRF. This document specifies that HMAC_GOSTR3411_2012_256 may be used as the "prf" function in the "prf+" function for the IKEv2 protocol.
Also, this document specifies that HMAC_GOSTR3411_2012_512 may be used as the "prf" function in the "prf+" function for the IKEv2 protocol (PRF_IPSEC_PRFPLUS_GOSTR3411_2012_512).  

4.3. VKO Algorithms for Key Agreement

This section specifies the key agreement algorithms based on GOST R 34.10-2012 [GOST3410-2012].

4.3.1. VKO_GOSTR3410_2012_256

The VKO_GOSTR3410_2012_256 transformation is used for agreement of 256-bit keys and is based on the 256-bit version of GOST R 34.11-2012 [GOST3411-2012]. This algorithm can be applied for a key agreement using GOST R 34.10-2012 [GOST3410-2012] with 256-bit or 512-bit private keys.

The algorithm is designed to produce an encryption key or a keying material of size 256 bits to be used in various cryptographic protocols. A key or a keying material KEK_VKO (x, y, UKM) is produced from the private key x of one side, the public key y*P of the opposite side and the User Keying Material (UKM) value.

The algorithm can be used for static and ephemeral keys with the public key size n >= 512 bits including the case where one side uses a static key and the other uses an ephemeral one.

The UKM parameter is optional (the default UKM = 1) and can take any integer value from 1 to 2^((n/2)-1). It is allowed to use a non-zero UKM of an arbitrary size that does not exceed n/2 bits. If at least one of the parties uses static keys, the RECOMMENDED length of UKM is 64 bits or more.

KEK_VKO (x, y, UKM) is calculated using the formulas:

\[
\text{KEK}_\text{VKO} (x, y, \text{UKM}) = H_{256} \left( K (x, y, \text{UKM}) \right),
\]

\[
K (x, y, \text{UKM}) = (m/q*\text{UKM}*x \mod q)^* (y*P),
\]

where m and q are the parameters of an elliptic curve defined in the GOST R 34.10-2012 [GOST3410-2012] standard (m is an elliptic curve points group order, q is an order of a cyclic subgroup), P is a non-zero point of the subgroup; P is defined by a protocol.

This algorithm is defined similar to the one specified in Section 5.2 of [RFC4357], but applies the hash function H_256 instead of the hash function GOST R 34.11-94 [GOST3411-94] (referred to as "gostR3411").
In addition, \( K(x, y, \text{UKM}) \) is calculated with public key size \( n \geq 512 \) bits and UKM has a size up to \( n/2 \) bits.

4.3.2. VKO_GOSTR3410_2012_512

The VKO_GOSTR3410_2012_512 transformation is used for agreement of 512-bit keys and is based on the 512-bit version of GOST R 34.11-2012 [GOST3411-2012]. This algorithm can be applied for a key agreement using GOST R 34.10-2012 [GOST3410-2012] with 512-bit private keys.

The algorithm is designed to produce an encryption key or a keying material of size 512 bits to be used in various cryptographic protocols. A key or a keying material \( KEK_{VKO} (x, y, \text{UKM}) \) is produced from the private key \( x \) of one side, the public key \( y*P \) of the opposite side and the UKM value, considered as an integer.

The algorithm can be used for static and ephemeral keys with the public key size \( n \geq 1024 \) bits including the case where one side uses a static key and the other uses an ephemeral one.

The UKM parameter is optional (the default \( \text{UKM} = 1 \)) and can take any integer value from 1 to \( 2^{(n/2)}-1 \). It is allowed to use a non-zero UKM of an arbitrary size that does not exceed \( n/2 \) bits. If at least one of the parties uses static keys, the RECOMMENDED length of UKM is 128 bits or more.

\( KEK_{VKO} (x, y, \text{UKM}) \) is calculated using the formulas:

\[
KEK_{VKO} (x, y, \text{UKM}) = H_{512} (K (x, y, \text{UKM}))
\]

\[
K (x, y, \text{UKM}) = (m/q*\text{UKM}x \mod q)*(y*P),
\]

where \( m \) and \( q \) are the parameters of an elliptic curve defined in the GOST R 34.10-2012 [GOST3410-2012] standard (\( m \) is an elliptic curve points group order, \( q \) is an order of a cyclic subgroup), \( P \) is a non-zero point of the subgroup; \( P \) is defined by a protocol.

This algorithm is defined similar to the one specified in Section 5.2 of [RFC4357], but applies the hash function \( H_{512} \) instead of the hash function GOST R 34.11-94 [GOST3411-94] (referred to as "gostR3411"). In addition, \( K(x, y, \text{UKM}) \) is calculated with public key size \( n \geq 1024 \) bits and UKM has a size up to \( n/2 \) bits.
4.4. The Key Derivation Function KDF_TREE_GOSTR3411_2012_256

The key derivation function KDF_TREE_GOSTR3411_2012_256 based on the HMAC_GOSTR3411_2012_256 function is given by:

\[ KDF_{\text{TREE-GOSTR3411-2012-256}}(K_{\text{in}}, \text{label}, \text{seed}, R) = K(1) \mid K(2) \mid K(3) \mid K(4) \mid \ldots, \]

\[ K(i) = \text{HMAC}_{\text{GOSTR3411-2012-256}}(K_{\text{in}}, [i]_b \mid \text{label} \mid 0x00 \mid \text{seed} \mid [L]_b), \ i \geq 1, \]

where:

- **K_in** Derivation key.
- **label**, **seed** The parameters that MUST be assigned by a protocol; their lengths SHOULD be fixed by a protocol.
- **R** A fixed external parameter, with possible values of 1, 2, 3, or 4.
- **i** Iteration counter.
- **[i]_b** Byte representation of the iteration counter (in the network byte order); the number of bytes in the representation [i]_b is equal to R (no more than 4 bytes).
- **L** The required size (in bits) of the generated keying material (an integer, not exceeding 256*(2^(8*R)-1)).
- **[L]_b** Byte representation of L, in network byte order (variable length: no leading zero bytes added).

The key derivation function KDF_TREE_GOSTR3411_2012_256 is intended for generating a keying material of size L, not exceeding 256*(2^(8*R)-1) bits, and utilizing general principles of the input and output for the key derivation function outlined in Section 5.1 of NIST SP 800-108 [NISTSP800-108]. The HMAC_GOSTR3411_2012_256 algorithm described in Section 4.1.1 is selected as a pseudorandom function.

Each key derived from the keying material formed using the derivation key K_in (0-level key) may be a 1-level derivation key and may be used to generate a new keying material. The keying material derived from the first level derivation key can be split down into the second level derivation keys. The application of this procedure leads to the construction of the key tree with the root key and the formation...
of the keying material to the hierarchy of the levels, as described in Section 6 of NIST SP 800-108 [NISTSP800-108]. The partitioning procedure for keying material at each level is defined in accordance with a specific protocol.

4.5. The Key Derivation Function KDF_GOSTR3411_2012_256

The KDF_GOSTR3411_2012_256 function is equivalent to the function KDF_TREE_GOSTR3411_2012_256, when R = 1, L = 256, and is given by:

\[ \text{KDF}_\text{GOSTR3411}_\text{2012}_\text{256} \left( \text{K}_\text{in}, \text{label}, \text{seed} \right) = \text{HMAC}_\text{GOSTR3411}_\text{2012}_\text{256} \left( \text{K}_\text{in}, 0x01 | \text{label} | 0x00 | \text{seed} | 0x01 | 0x00 \right), \]

where:

- \( \text{K}_\text{in} \): Derivation key.
- \( \text{label}, \text{seed} \): The parameters that MUST be assigned by a protocol; their lengths SHOULD be fixed by a protocol.

4.6. Key Wrap and Key Unwrap

Wrapped representation of a secret key K (256-bit GOST 28147-89 [GOST28147-89] key, 256-bit or 512-bit GOST R 34.10-2012 [GOST3410-2012] private key) is formed as follows by using a given export key K_e (GOST 28147-89 [GOST28147-89] key) and a random seed vector:

1. Generate a random seed vector from 8 up to 16 bytes.
2. With the key derivation function, using an export key K_e as a derivation key, produce a key KEK_e (K_e, seed), where:

\[ \text{KEK}_\text{e} \left( \text{K}_\text{e}, \text{seed} \right) = \text{KDF}_\text{GOSTR3411}_\text{2012}_\text{256} \left( \text{K}_\text{e}, \text{label}, \text{seed} \right), \]

where the KDF_GOSTR3411_2012_256 function (see Section 4.5) is used as a key derivation function for the fixed label value

\[ \text{label} = \left( 0x26 | 0xBD | 0xB8 | 0x78 \right). \]

3. GOST 28147-89 [GOST28147-89] Message Authentication Code (MAC) value (4-byte) for the data K and the key KEK_e (K_e, seed) is calculated; the initialization vector (IV) in this case is equal to the first 8 bytes of seed. The resulting value is denoted as CEK_MAC.
4. The key $K$ is encrypted with the GOST 28147-89 [GOST28147-89] algorithm in the Electronic Codebook (ECB) mode with the key $KEK_e (K_e, seed)$. The result is denoted as $CEK_ENC$.

5. The wrapped representation of the key is $(seed \mid CEK_ENC \mid CEK_MAC)$.

The value of key $K$ is restored from the wrapped representation of the key and the export key $K_e$ as follows:

1. Obtain the seed, $CEK_ENC$ and $CEK_MAC$ values from the wrapped representation of the key.

2. With the key derivation function, using the export key $K_e$ as a derivation key, produce a key $KEK_e(K_e, seed)$, where:

$$KEK_e(K_e, seed) = KDF_GOSTR3411_2012_256(K_e, label, seed),$$

where the $KDF_GOSTR3411_2012_256$ function (see Section 4.5) is used as a key derivation function for the fixed label value

$$label = (0x26 \mid 0xBD \mid 0xB8 \mid 0x78).$$

3. The $CEK_ENC$ field is decrypted with the GOST 28147-89 [GOST28147-89] algorithm in the Electronic Codebook (ECB) mode with the key $KEK_e(K_e, seed)$. The unwrapped key $K$ is assumed to be equal to the result of decryption.

4. GOST 28147-89 [GOST28147-89] MAC value (4-byte) for the data $K$ and the key $KEK_e(K_e, seed)$ is calculated; the initialization vector (IV) in this case is equal to the first 8 bytes of seed. If the result is not equal to $CEK_MAC$, an error is returned.

The GOST 28147-89 [GOST28147-89] algorithm is used with the parameter set defined in Appendix C of this document.

5. The Parameters of Elliptic Curves

This section defines the elliptic curves parameters and object identifiers that are RECOMMENDED for usage with the signature and verification algorithms of the digital signature in accordance with the GOST R 34.10-2012 [GOST3410-2012] standard and with the key agreement algorithms VKO_GOSTR3410_2012_256 and VKO_GOSTR3410_2012_512.

This document does not negate the use of other parameters of elliptic curves.
5.1. Canonical Form

This section defines the elliptic curves parameters of the GOST R 34.10-2012 [GOST3410-2012] standard for the case of elliptic curves with prime 512-bit moduli in canonical (short Weierstrass) form, that is given by the following equation defined in GOST R 34.10-2012 [GOST3410-2012]:

\[ y^2 = x^3 + ax + b \pmod{p}. \]

In case of elliptic curves with 256-bit prime moduli, the parameters defined in [RFC4357] are proposed for use.

5.1.1. Parameters and Object Identifiers

The parameters for each elliptic curve are represented by the following values, which are defined in GOST R 34.10-2012 [GOST3410-2012]:

\[ p \] the characteristic of the underlying prime field;
\[ a, b \] the coefficients of the equation of the elliptic curve in the canonical form;
\[ m \] the elliptic curve group order;
\[ q \] the elliptic curve subgroup order;
\[ (x, y) \] the coordinates of the point P (generator of the subgroup of order q) of the elliptic curve in the canonical form.

Both sets of the parameters are presented as structures of the form:

\[
\text{SEQUENCE} \{ \\
\text{p INTEGER,} \\
\text{a INTEGER,} \\
\text{b INTEGER,} \\
\text{m INTEGER,} \\
\text{q INTEGER,} \\
\text{x INTEGER,} \\
\text{y INTEGER} \\
\}
\]

The parameter sets have the following object identifiers:

1. \text{id-tc26-gost-3410-12-512-paramSetA} := \{iso(1) member-body(2) ru(643) rostandart(7) tc26(1) constants(2) sign-constants(1) gost-3410-12-512-constants(2) paramSetA(1)\);
2.  id-tc26-gost-3410-12-512-paramSetB::= {iso(1) member-body(2)
ru(643) rosstandart(7) tc26(1) constants(2) sign-constants(1)
gost-3410-12-512-constants(2) paramSetB(2)}.

The corresponding values of the parameter sets can be found in Appendix A.1.

5.2.  Twisted Edwards Form

This section defines the elliptic curves parameters and object identifiers of the GOST R 34.10-2012 [GOST3410-2012] standard for the case of elliptic curves that have a representation in the twisted Edwards form with prime 256-bit and 512-bit moduli.

A twisted Edwards curve $E$ over a finite prime field $F_p$, $p > 3$, is an elliptic curve defined by the equation:

\[ e*u^2 + v^2 = 1 + d*u^2*v^2 \pmod{p}, \]

where $e, d$ are in $F_p$, $ed(e-d) \neq 0$.

A twisted Edwards curve has an equivalent representation in the short Weierstrass form defined by parameters $a, b$. The parameters $a, b, e,$ and $d$ are related as follows:

\[
\begin{align*}
a &= s^2 - 3*t^2 \pmod{p}, \\
b &= 2*t^3 - t*s^2 \pmod{p}, \\
s &= (e - d)/4 \pmod{p}, \\
t &= (e + d)/6 \pmod{p}.
\end{align*}
\]

Coordinate transformations are defined as follows:

\[
\begin{align*}
(u,v) &\rightarrow (x,y) = (s(1 + v)/(1 - v) + t, s(1 + v)/(1 - v)u)), \\
(x,y) &\rightarrow (u,v) = ((x - t)/y, (x - t - s)/(x - t + s)).
\end{align*}
\]

5.2.1. Parameters and Object Identifiers

The parameters for each elliptic curve are represented by the following values, which are defined in GOST R 34.10-2012 [GOST3410-2012]:

- $p$ The characteristic of the underlying prime field.
- $a, b$ The coefficients of the equation of the elliptic curve in the canonical form.
e, d  The coefficients of the equation of the elliptic curve in the
twisted Edwards form.

m      The elliptic curve group order.

q      The elliptic curve subgroup order.

(x, y)  The coordinates of the point P (generator of the subgroup of
        order q) of the elliptic curve in the canonical form.

(u, v)  The coordinates of the point P (generator of the subgroup of
        order q) of the elliptic curve in the twisted Edwards form.

Both sets of the parameters are presented as ASN structures of the
form:

SEQUENCE {
  p      INTEGER,
  a      INTEGER,
  b      INTEGER,
  e      INTEGER,
  d      INTEGER,
  m      INTEGER,
  q      INTEGER,
  x      INTEGER,
  y      INTEGER,
  u      INTEGER,
  v      INTEGER
}

The parameter sets have the following object identifiers:

1. id-tc26-gost-3410-2012-256-paramSetA ::= {iso(1) member-body(2)
 ru(643) rostandart(7) tc26(1) constants(2) sign-constants(1)
 gost-3410-12-256-constants(1) paramSetA(1)};

2. id-tc26-gost-3410-2012-512-paramSetC ::= {iso(1) member-body(2)
 ru(643) rostandart(7) tc26(1) constants(2) sign-constants(1)
 gost-3410-12-512-constants(2) paramSetC(3)}.

The corresponding values of the parameter sets can be found in
Appendix A.2.

6. Security Considerations

This entire document is about security considerations.
7. References

7.1. Normative References


Smyshlyaev, et al. Informational [Page 16]
7.2. Informative References

[GOST3411-94]

[NISTSP800-108]


Appendix A. Values of the Parameter Sets

A.1. Canonical Form Parameters

Parameter set: id-tc26-gost-3410-12-512-paramSetA

SEQUENCE
{

  OBJECT IDENTIFIER
  id-tc26-gost-3410-12-512-paramSetA
  SEQUENCE
  {
    INTEGER
    00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
    C7
    INTEGER
    00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
    C4
    INTEGER
    00 E8 C2 50 5D ED FC 86 DD C1 BD 0B 2B 66 67 F1
    DA 34 B8 25 74 76 1C B0 E8 79 BD 08 1C FD 0B 62
    65 EE 3C B0 90 F3 0D 27 61 4C B4 57 40 10 DA 90
    DD 86 2E F9 D4 EB EE 47 61 50 31 90 78 5A 71 C7
    60
    INTEGER
    00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF 27 E6 95 32 F4 8D 89 11 6F F2 2B 8D 4E 05 60
    60 9B 4B 38 AB FA D2 B8 5D CA CD B1 41 1F 10 B2
    75
    INTEGER
    00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF 27 E6 95 32 F4 8D 89 11 6F F2 2B 8D 4E 05 60
    60 9B 4B 38 AB FA D2 B8 5D CA CD B1 41 1F 10 B2
    75
    INTEGER
    03

    Smyshlyaev, et al.   Informational   [Page 18]
Parameter set: id-tc26-gost-3410-12-512-paramSetB

SEQUENCE

{  
  OBJECT IDENTIFIER
  id-tc26-gost-3410-12-512-paramSetB
  SEQUENCE
  {
    INTEGER
    00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    6F
    INTEGER
    00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    6C
    INTEGER
    68 7D 1B 45 9D C8 41 45 7E 3E 06 CF 6F 5E 25 17
    B9 7C 7D 61 4A F1 38 BC BF 85 DC 80 6C 4B 28 9F
    3E 96 5D 2D B1 41 6D 21 7F 8B 27 6F AD 1A B6 9C
    50 F7 8B EE 1F A3 10 6E FB 8C CB C7 C5 14 01 16
    INTEGER
    00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    01 49 A1 EC 14 25 65 A5 45 AC FD B7 7B D9 D4 0C
    FA 8B 99 67 12 10 1B EA 0E C6 34 6C 54 37 4F 25
    BD
    INTEGER
    00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    01 49 A1 EC 14 25 65 A5 45 AC FD B7 7B D9 D4 0C
    FA 8B 99 67 12 10 1B EA 0E C6 34 6C 54 37 4F 25
    BD
    INTEGER
    02
  }
}

Smyshlyaev, et al.            Informational                    [Page 19]
A.2. Twisted Edwards Form Parameters

Parameter set: id-tc26-gost-3410-2012-256-paramSetA

SEQUENCE
{
    OBJECT IDENTIFIER
    id-tc26-gost-3410-2012-256-paramSetA
    SEQUENCE
    {
        INTEGER
        00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD 97
        INTEGER
        00 C2 17 3F 15 13 98 16 73 AF 48 92 C2 30 35 A2 7C E2 5E 20 13 BF 95 AA 33 B2 2C 65 6F 27 7E 73 35
        INTEGER
        29 5F 9B AE 74 28 ED 9C CC 20 E7 C3 59 A9 D4 1A 22 FC CD 91 08 E1 7B F7 BA 93 37 A6 F8 AE 95 13
        INTEGER
        01
        INTEGER
        06 05 F6 B7 C1 83 FA 81 57 8B C3 9C FA D5 18 13 2B 9D F6 28 97 00 9A F7 E5 22 C3 2D 6D C7 BF FB
        INTEGER
        01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3F 63 37 7F 21 ED 98 D7 04 56 BD 55 B0 D8 31 9C
        INTEGER
        40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0F D8 CD DF C8 7B 66 35 C1 15 AF 55 6C 36 0C 67
        INTEGER
        00 91 E3 84 43 A5 E8 2C 0D 88 09 23 42 57 12 B2 BB 65 8B 91 96 93 2E 02 C7 8B 25 82 FE 74 2D AA 28
Parameter set: id-tc26-gost-3410-2012-512-paramSetC

`SEQUENCE`{
  `OBJECT IDENTIFIER` id-tc26-gost-3410-2012-512-paramSetC
  `SEQUENCE`
  {
    `INTEGER` 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF F

Appendix B. Test Examples

1) HMAC_GOSTR3411_2012_256

Key K:

00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f

T:

01 26 bd b8 78 00 af 21 43 41 45 65 63 78 01 00
HMAC_GOSTR3411_2012_256 (K, T) value:

```
a1 aa 5f 7d e4 02 d7 b3 d3 23 f2 99 1c 8d 45 34
01 31 37 01 0a 83 75 4f d0 af 6d 7c d4 92 2e d9
```

2) HMAC_GOSTR3411_2012_512

Key K:

```
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f
```

T:

```
01 26 bd b8 78 00 af 21 43 41 45 65 63 78 01 00
```

HMAC_GOSTR3411_2012_512 (K, T) value:

```
a5 9b ab 22 ec ae 19 c6 5f bd e6 e5 f4 e9 f5 d8
54 9d 31 f0 37 f9 df 9b 90 55 00 e1 71 92 3a 77
3d 5f 15 30 f2 ed 7e 96 4c b2 ee dc 29 e9 ad 2f
3a fe 93 b2 81 4f 79 f5 00 0f fc 03 66 c2 51 e6
```

3) PRF_TLS_GOSTR3411_2012_256

Key K:

```
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f
```

Seed:

```
18 47 1d 62 2d c6 55 c4 d2 d2 26 96 91 ca 4a 56
0b 50 ab a6 63 55 3a f2 41 f1 ad a8 82 c9 f2 9a
```

Label:

```
11 22 33 44 55
```

Output T1:

```
ff 09 66 4a 44 74 58 65 94 4f 83 9e bb 48 96 5f
15 44 ff 1c c8 e8 f1 6f 24 7e e5 f8 a9 eb e9 7f
```
 Output T2:

c4 e3 c7 90 0e 46 ca d3 db 6a 01 64 30 63 04 0e
c6 7f c0 fd 5c d9 f9 04 65 23 52 37 bd ff 2c 02

4) PRF_TLS_GOSTR3411_2012_512

Key K:
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f

Seed:
18 47 1d 62 2d c6 55 c4 d2 d2 26 96 91 ca 4a 56
0b 50 ab a6 63 55 3a f2 41 f1 ad a8 82 c9 f2 9a

Label:
11 22 33 44 55

Output T1:

f3 51 87 a3 dc 96 55 11 3a 0e 84 d0 6f d7 52 6c
5f c1 fb de c1 a0 e4 67 3d d6 d7 9d 0b 92 0e 65
ad 1b c4 7b b0 83 b3 85 1c b7 cd 8e 7e 6a 91 1a
62 6c f0 2b 29 e9 e4 a5 8e d7 66 a4 49 a7 29 6d

Output T2:

e6 1a 7a 26 c4 d1 ca ee cf d8 0c ca 65 c7 1f 0f
88 c1 f8 22 c0 e8 c0 ad 94 9d 03 fe e1 39 57 9f
72 ba 0c 3d 32 c5 f9 54 f1 cc cd 54 08 1f c7 44
02 78 cb a1 fe 7b 7a 17 a9 86 fd ff 5b d1 5d 1f

5) PRF_IPSEC_PRFPLUS_GOSTR3411_2012_256

Key K:

c9 a9 a7 73 20 e2 cc 55 9e d7 2d ce 6f 47 e2 19
2c ce a9 5f a6 48 67 05 82 c0 54 c0 ef 36 c2 21

Data S:

01 26 bd b8 78 00 1d 80 60 3c 85 44 c7 27 01 00
Output T1:
2d e5 ee 84 e1 3d 7b e5 36 16 67 39 13 37 0a b0
54 c0 74 b7 9b 69 a8 a8 46 82 a9 f0 4f ec d5 87

Output T2:
29 f6 0d da 45 7b f2 19 aa 2e f9 5d 7a 59 be 95
4d e0 08 f4 a5 0d 50 4d bd b6 90 be 68 06 01 53

6) PRF_IPSEC_PRFPLUS_GOSTR3411_2012_512

Key K:
c9 a9 a7 73 20 e2 cc 55 9e d7 2d ce 6f 47 e2 19
2c ce a9 5f a6 48 67 05 82 c0 54 c0 ef 36 c2 21

Data S:
01 26 bd b8 78 00 1d 80 60 3c 85 44 c7 27 01 00

Output T1:
5d a6 71 43 a5 f1 2a 6d 6e 47 42 59 6f 39 24 3f
cc 61 57 45 91 5b 32 59 10 06 ff 78 a2 08 63 d5
f8 8e 4a fc 17 fb be 70 b9 50 95 73 db 00 5e 96
26 36 98 46 cb 86 19 99 71 6c 16 5d d0 6a 15 85

Output T2:
48 34 49 5a 43 74 6c b5 3f 0a ba 3b c4 6e bc f8
77 3c a6 4a d3 43 c1 22 ee 2a 57 75 57 03 81 57
ee 9c 38 8d 96 ef 71 d5 8b e5 c1 ef a1 af a9 5e
be 83 e3 9d 00 e1 9a 5d 03 dc d6 0a 01 bc a8 e3

7) VKO_GOSTR3410_2012_256 with 256-bit output on the GOST
R 34.10-2012 512-bit keys with id-tc26-gost-3410-12-512-paramSetA

UKM value:
1d 80 60 3c 85 44 c7 27

Private key x of A:
c9 90 ec d9 72 fc e8 4e c4 db 02 27 78 f5 0f ca
c7 26 f4 67 08 38 4b 8d 45 83 04 96 2d 71 47 f8
c2 db 41 ce f2 2c 90 b1 02 f2 96 84 04 f9 b9 be
c6 47 c7 96 92 d8 18 26 b3 2b 8d ac a4 3c b6 67
Public key $x^*P$ of A (curve point $(X, Y)$):

```
aa b0 ed a4 ab ff 21 20 8d 18 79 9f b9 a8 55 66
54 ba 78 30 70 eb a1 0c b9 ab b2 53 ec 56 dc f5
d3 cc ba 61 92 e4 64 e5 bc b6 de a1 37 79 2f
24 31 f6 c8 97 eb 1b 3c 0c c1 43 27 b1 ad c0 a7
91 46 13 a3 07 4e 3e 3a ed b2 04 d3 8d 35 63 97
1b d8 75 8e 8c 9d b1 14 03 72 1b 48 00 2d 38
46 1f 92 47 2d 40 ea 92 f9 95 8c 0f fa 4c 93 75
64 01 b9 7f 89 fd be 0b 5e 46 e4 a4 63 1c db 5a
```

Private key $y$ of part B:

```
48 c8 59 f7 b6 f1 15 85 88 7c c0 5e c6 ef 13 90
cf ea 73 9b 1a 18 c0 d4 66 22 93 ef 63 b7 9e 3b
80 14 07 0b 44 91 85 90 b4 b9 96 ac fe a4 ed fb
bb cc cc 8c 06 ed d8 bf 5b da 92 a5 13 92 d0 db
```

Public key $y^*P$ of B (curve point $(X, Y)$):

```
19 2f e1 83 b9 71 3a 07 72 53 c7 2c 87 35 de 2e
a4 2a 3d bc 66 ea 31 78 38 b6 5f a3 25 23 cd 5e
fc a9 74 ed a7 c8 63 f4 95 4d 11 47 f1 f2 b2 5c
39 5f ce lc 12 91 75 e8 76 d1 32 e9 4e d5 a6 51
04 88 3b 41 4c 9b 59 2e c4 dc 84 82 6f 07 d0 b6
d9 00 6d da 17 6c e4 8c 39 6e 1e 3f 97 d1 02 e0 3b
b5 98 bf 13 2a 22 8a 45 f7 20 1a ba 08 fc 52 4a
2d 77 e4 3a 36 2a b0 22 ad 40 28 f7 5b de 3b 79
```

KEK_VKO value:

```
c9 a9 a7 73 20 e2 cc 55 9e d7 2d ce 6f 47 e2 19
2c ce a9 5f a6 48 67 05 82 c0 54 c0 ef 36 c2 21
```

8)VKO_GOSTR3410_2012_512 with 512-bit output on the GOST
R 34.10-2012 512-bit keys with id-tc26-gost-3410-12-512-paramSetA

UKM value:

```
1d 80 60 3c 85 44 c7 27
```

Private key $x$ of A:

```
c9 90 ec d9 72 fc e8 4e c4 db 02 27 78 f5 0f ca
c7 26 f4 67 08 38 4b 8d 45 83 04 96 2d 71 47 f8
c2 db 41 ce f2 2c 90 b1 02 f2 96 84 04 f9 b9 be
6d 47 c7 96 92 d8 18 26 b3 2b 8d ac a4 3c b6 67
```
Public key $x^*P$ of A (curve point $(X, Y)$):

aa b0 ed a4 ab ff 21 20 8d 18 79 9f b9 a8 55 66
54 ba 78 30 70 eb a1 0c b9 ab b2 53 ec 56 dc f5
d3 cc ba 61 92 e4 64 e6 e5 b6 de a1 37 79 2f
24 31 f6 c8 97 eb 1b 3c 0c c1 43 27 b1 ad c0 a7
91 46 13 a3 07 4e 36 3a ed b2 04 d3 8d 35 63 97
1b d8 75 8e 8c 9d b1 14 03 72 1b 48 00 2d 38
46 1f 92 47 2d 40 ea 92 f9 95 8c 0f fa 4c 93 75
64 01 b9 7f 89 fd be 0b 5e 46 e4 a4 63 1c db 5a

Private key $y$ of B:

48 c8 59 f7 b6 f1 15 85 88 7c c0 5e c6 ef 13 90
cf ea 73 9b 1a 18 c0 d4 66 22 93 ef 63 b7 9e 3b
80 14 07 b0 44 91 85 90 b4 b9 96 ac fe a4 ed fb
bb cc cc 8c 06 ed d8 bf 5b da 92 a5 13 92 d0 db

Public key $y^*P$ of B (curve point $(X, Y)$):

19 2f e1 83 b9 71 3a 07 72 53 c7 2c 87 35 de 2e
a4 2a 3d bc 66 ea 31 78 38 b6 5f a3 25 23 cd 5e
fc a9 74 ed a7 c8 63 f4 95 4d 11 47 f1 f2 b2 5c
39 5f ce 1c 12 91 75 e8 76 d1 32 e9 4e d5 a6 51
04 88 3b 41 4c 9b 59 2e c4 dc 84 82 6f 07 d0 b6
d9 00 6d da 17 6c e4 8c 39 1e 3f 97 d1 02 e0 3b
b5 98 bf 13 2a 22 8a 45 f7 20 1a ba 08 fc 52 4a
2d 77 e4 3a 36 2a b0 22 ad 40 28 f7 5b de 3b 79

KEK_VKO value:

79 f0 02 a9 69 40 ce 7b de 32 59 a5 2e 01 52 97
ad aa d8 45 97 a0 d2 05 b5 0e 3e 17 19 f9 7b fa
7e e1 d2 66 1f a9 97 9a 5a a2 35 b5 58 a7 e6 d9
f8 8f 98 2d d6 3f c3 5a 8e c0 dd 5e 24 2d 3b df

9) Key derivation function KDF_GOSTR3411_2012_256

K_in key:

00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f

Label:

26 bd b8 78
Seed:
af 21 43 41 45 65 63 78

KDF(K_in, label, seed) value:
a1 aa 5f 7d e4 02 d7 b3 d3 23 f2 99 1c 8d 45 34
01 31 37 01 0a 83 75 4f d0 af 6d 7c d4 92 2e d9

10) Key derivation function KDF_TREE_GOSTR3411_2012_256

Output size of L:
512

K_in key:
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f

Label:
26 bd b8 78

Seed:
av 21 43 41 45 65 63 78

K1:
22 b6 83 78 45 c6 be f6 5e a7 16 72 b2 65 83 10
86 d3 c7 6a eb e6 da e9 1c ad 51 d8 3f 79 d1 6b

K2:
07 4c 93 30 59 9d 7f 8d 71 2f ca 54 39 2f 4d dd
e9 37 51 20 6b 35 84 c8 f4 3f 9e 6d c5 15 31 f9

R:
1
11) Key wrap and unwrap with the szOID_Gost28147_89_TC26_Z_ParamSet parameters

Key K_e:
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f

Key K:
20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f
30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f

Seed:
af 21 43 41 45 65 63 78

Label:
26 bd b8 78

KEK_e(seed) = KDF_GOSTR3411_2012_256(K_e, label, seed):
a1 aa 5f 7d e4 02 d7 b3 d3 23 f2 99 1c 8d 45 34
01 31 37 01 0a 83 75 4f d0 af 6d 7c d4 92 2e d9

CEK_MAC:
be 33 f0 52

CEK_ENC:
d1 55 47 f8 ee 85 12 1b c8 7d 4b 10 27 d2 60 27
e0 c0 71 bb a6 e7 2f 3f ec 6f 62 0f 56 83 4c 5a
Appendix C.  GOST 28147-89 Parameter Set

The parameter set has the following object identifier:

\[ id-tc26-gost-28147-param-Z::= \{iso(1) member-body(2) ru(643) rostandart(7) tc26(1) constants(2) cipher-constants(5) gost-28147-constants(1) param-Z(1)\} \]

The parameter set is defined below:

<table>
<thead>
<tr>
<th>x</th>
<th>K1(x)</th>
<th>K2(x)</th>
<th>K3(x)</th>
<th>K4(x)</th>
<th>K5(x)</th>
<th>K6(x)</th>
<th>K7(x)</th>
<th>K8(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>c</td>
<td>6</td>
<td>b</td>
<td>c</td>
<td>7</td>
<td>5</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>8</td>
<td>f</td>
<td>d</td>
<td>e</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>f</td>
<td>2</td>
<td>e</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
<td>8</td>
<td>1</td>
<td>a</td>
<td>6</td>
<td>5</td>
<td>d</td>
</tr>
<tr>
<td>4</td>
<td>a</td>
<td>9</td>
<td>2</td>
<td>d</td>
<td>8</td>
<td>9</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>a</td>
<td>f</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>b</td>
<td>5</td>
<td>a</td>
<td>f</td>
<td>6</td>
<td>c</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>9</td>
<td>c</td>
<td>d</td>
<td>6</td>
<td>d</td>
<td>a</td>
<td>c</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>e</td>
<td>1</td>
<td>e</td>
<td>7</td>
<td>0</td>
<td>b</td>
<td>f</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
<td>e</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>7</td>
<td>4</td>
<td>f</td>
</tr>
<tr>
<td>a</td>
<td>d</td>
<td>4</td>
<td>7</td>
<td>a</td>
<td>3</td>
<td>8</td>
<td>b</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>7</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>e</td>
<td>1</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>b</td>
<td>c</td>
<td>3</td>
<td>b</td>
<td>4</td>
<td>d</td>
<td>9</td>
</tr>
<tr>
<td>d</td>
<td>3</td>
<td>d</td>
<td>9</td>
<td>e</td>
<td>4</td>
<td>3</td>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td>e</td>
<td>f</td>
<td>0</td>
<td>6</td>
<td>9</td>
<td>2</td>
<td>e</td>
<td>3</td>
<td>b</td>
</tr>
<tr>
<td>f</td>
<td>1</td>
<td>f</td>
<td>0</td>
<td>b</td>
<td>c</td>
<td>0</td>
<td>7</td>
<td>2</td>
</tr>
</tbody>
</table>

Acknowledgments

We thank Valery Smyslov, Igor Ustinov, Basil Dolmatov, Russ Housley, Dmitry Khovratovich, Oleksandr Kazymyrov, Ekaterina Smyshlyaeva, Vasily Nikolaev, and Lolita Sonina for their careful readings and useful comments.

Authors’ Addresses

Stanislav Smyshlyaev (editor)
CRYPTO-PRO
18, Suschevsky val
Moscow 127018
Russian Federation

Phone: +7 (495) 995-48-20
Email: svs@cryptopro.ru
Evgeny Alekseev  
CRYPTO-PRO  
18, Suschevsky val  
Moscow  127018  
Russian Federation

Phone: +7 (495) 995-48-20  
Email: alekseev@cryptopro.ru

Igor Oshkin  
CRYPTO-PRO  
18, Suschevsky val  
Moscow  127018  
Russian Federation

Phone: +7 (495) 995-48-20  
Email: oshkin@cryptopro.ru

Vladimir Popov  
CRYPTO-PRO  
18, Suschevsky val  
Moscow  127018  
Russian Federation

Phone: +7 (495) 995-48-20  
Email: vpopov@cryptopro.ru

Serguei Leontiev  
CRYPTO-PRO  
18, Suschevsky val  
Moscow  127018  
Russian Federation

Phone: +7 (495) 995-48-20  
Email: lse@cryptopro.ru

Vladimir Podobaev  
FACTOR-TS  
11A, 1st Magistralny proezd  
Moscow  123290  
Russian Federation

Phone: +7 (495) 644-31-30  
Email: v_podobaev@factor-ts.ru
Dmitry Belyavsky
TCI
8, Zoologicheskaya st
Moscow 117218
Russian Federation

Phone: +7 (499) 254-24-50
Email: beldmit@gmail.com