AN12304

Leakage Resilient Primitive (LRP) Specification

Rev. 1.1 — 13 March 2019 Application note
466011 COMPANY PUBLIC

Document information

Information	Content
Keywords	NXP, Leakage Resilient Primitive, LRP, AES cryptography, enhances side-channel and fault resistance
Abstract	This application note addresses the implementation of an alternative AES-based protocol for authentication and secure messaging using a Leakage Resilient Primitive, LRP. The LRP works as a wrapper around the AES cryptography and enhances side-channel and fault resistance.

Revision history

Revision history

Rev	Date	Description
1.1	20190313	Remove the specific product names in Keywords
1.0	20190131	Initial version

1 Introduction

This document describes NXP's Leakage Resilient Primitive (LRP) and its use for authentication, encryption and CMAC operation. The LRP primitive serves as a drop-in replacement for AES and only uses standard cryptographic constructions based on AES, without any proprietary cryptography. Thus, in this context, LRP can be seen as an alternative for AES which is itself based on AES but comes with better properties w.r.t. implementation security.

1.1 Cryptographic security

The security of LRP is based on the security of the Goldreich-Goldwasser-Micali (GGM) construction of a pseudo-random function [2] from a pseudo-random generator (PRG). The proof of its security can be found in many cryptography textbooks (e.g. [3]). In the case of LRP, the used pseudo-random generator PRG is AES in counter (CTR) mode [1] which itself is a NIST standard.

For encryption, LRP is used in a slight variation of the CTR mode. That is, instead of x-oring the key stream to the message, it is used as keys in electronic code book (ECB) mode. For MACing, the classical CMAC construction is adapted [1] and simply replaced the block cipher by LRP.

1.2 Organization

The remainder of this document is organized in two parts:

- Section 2 specifies the algorithms and how to use them.
- Section 3 provides test vectors.

2 Algorithms

This section describes the algorithms which have to be used to implement LRP and the cryptographic services using LRP.

2.1 Pre-computations

The algorithms in this section usually only need to be executed once per key, independent of the data to process. Basically, they are used to expand the 128-bit key material to 16 secret plaintexts and at least 1 updated key, each of them being vectors of 128-bit length.

2.1.1 Plaintext and key generation

The basic principle of the secret plaintext and updated key generation is depicted in Figure 1. The gray boxes containing the letter 'E' symbolize AES block cipher invocations in encryption direction. Furthermore, the triangle input is the key input and the other one the plaintext input. Finally, whenever a byte value in hexadecimal notation is fed in as a plaintext this has to be understood as feeding in a 128-bit vector containing 16 times this byte. For instance $0x55$ refers to $0x55555555555555555555555555555555$ or $\{0x55\}^{16}$ in short. It can be seen that the first two encryptions serve as a length doubling PRG where the upper output is further used as a seed in the generation of the 2^m secret plaintexts. The lower output is used as a seed for the generation of the q updated keys. Typically, the upper and the lower branches (secret plaintext and updated key generation) are invoked as separate algorithms. These are specified in Algorithms 1 and 2.

The parameter m within these algorithms is 4.

$E_k(p)$ denotes the encryption of p under key k. The parameter q in the context of secure messaging is 2 in order to generate one MACing key k_0 and one encryption key k_1.

Note, that in the context of the NTAG 42x DNA and NTAG 42x DNA TT, k_0 is used as encryption key in case PICCData encryption is applied.

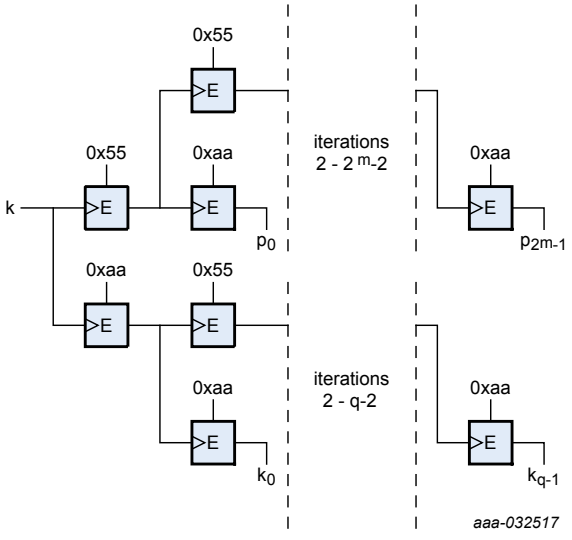

Figure 1. Generation of secret plaintexts and updated keys

2.1.1.1 Algorithm 1

$\{p_0, \ldots, p_{2^m - 1}\}$ = generatePlaintexts(m, k)

Require: Parameter m, key k.

Ensure: Plaintexts $\{p_0, \ldots, p_{2^m - 1}\}$.

$h = k$

$h = E_h(\{0x55\}^{16})$

for $i = 0 \ldots 2^m - 1$ **do**

$p_i = E_h(\{0xaa\}^{16})$

$h = E_h(\{0x55\}^{16})$

end for

return $\{p_0, \ldots, p_{2^m - 1}\}$

2.1.1.2 Algorithm 2

$\{k_0, \ldots, k_{q - 1}\}$ = generateUpdatedKeys(q, k)

Require: Parameter q, key k.

Ensure: Updated keys $\{k_0, \ldots, k_{q - 1}\}$.

$h = k$

$h = E_h(\{0xaa\}^{16})$

for $i = 0 \ldots q - 1$ **do**

$k_i = E_h(\{0xaa\}^{16})$

$h = E_h(\{0x55\}^{16})$

end for

return $\{k_0, \ldots, k_{q - 1}\}$

2.2 LRP function evaluation

LRP itself is defined by Algorithm 3 which takes the precomputed values from Algorithms 1 and 2 as input.

In particular, k' refers to one of the keys from $\{k_0, \ldots, k_{q-1}\}$, where k_0 is used for integrity protection (MAC calculation) and for PICCData encryption in NTAG 424 DNA and k_1 is used for encryption of data in Full Communication mode.

As above, $m = 4$, therefore $len(x, m)$ returns the number of nibbles as in general $len(x, m)$ is defined as $\lceil \log_m(x) \rceil$.

The purpose of the $final$ flag is to allow for caching. Especially, for encryption where x represents a counter and thus most of the most significant bits (MSBits) will stay the same from one invocation of Algorithm 3 to another, caching intermediate values can tremendously increase the performance.

2.2.1 Algorithm 3

$y = \text{evalLRP}\left(m, \{\{p_0, \ldots, p_{2^m-1}\}, \text{k}'\}, l, x, final\right)$

Require: The dimension m, a set of plaintexts $\{p_0, \ldots, p_{2^m-1}\}$, an updated key k', the length $l = len(x, m)$, the input $x = x_0, \ldots, x_{l-1}$ with $x_i \in \mathbb{F}_{2^m}$, an indicator for the final transformation *final*.

Ensure: Result of (partial) LRP evaluation y

$y = k'$

for $i = 0$ to $l - 1$ **do**

$p = p_{x_i}$

$y = E_y(p)$

end for

if $final = true$ **then**

$y = E_y(0^n)$

end if

return y

2.3 LRICB

Encryption and decryption are implemented as operating LRP in CTR mode and then using the resulting key stream as a key for AES in ECB mode. We refer to this mode as Leakage Resilient Indexed Code Book (LRICB) mode. For an w-block plaintext pt, this can be written as

$$ct = \left(r, E_{\text{LRP}_k}(r)\left(pt_0\right), \ldots, E_{\text{LRP}_k}(r+w-1)\left(pt_{w-1}\right)\right),$$
$$pt = \left(r, D_{\text{LRP}_k}(r)\left(pt_0\right), \ldots, D_{\text{LRP}_k}(r+w-1)\left(pt_{w-1}\right)\right)$$

where pt_i and ct_i denote the i^{th} plaintext and ciphertext block, r is the counter value, LRP_k is LRP using key k, E_{LRP_k} and D_{LRP_k} denote the encryption and decryption using the output of the LRP evaluation as key. The message needs to be either a multiple of 16 bytes or padded using Padding Method 2 of ISO/IEC 9797-1 [4], i.e. by adding always 0x80 followed, if required, by zero bytes until a string with a length of a multiple of 16 bytes is obtained. Note that if the plain data is a multiple of 16 bytes already, an additional padding block is added. The only exception is during the authentication itself (AuthenticateLRPFirst and AuthenticateLRPNonFirst), where no padding is applied at all.

Running encryption in counter mode also has the advantage that for a w-block output $c_0, \ldots, c_{w-1}$, $r_0, \ldots, r_{w-1}$ have up to $w^l = len(128, m) - len(w, m)$ equal most significant chunks. This means that the loop in Algorithm 3 can in the first step only be evaluated until depth w^l which takes w^l encryptions. Then for every r_i, the remaining evaluation effort is $len(w, m) + 2$ (2 for the final transformation and the ECB step). Therefore, the effort for encrypting w blocks can be stated as $w^l + (len(w, m) + 2) * w$ encryptions.

To allow such optimizations, the counter is assumed to be in big-endian as it is processed from left to right by evalLRP (see Algorithm 3). However, the optimizations themselves are not included in the depicted algorithm.

2.3.1 Algorithm 4

LRICB encryption: $\{r, ct\} = \text{LRICBenc}\left(m, \left\{\{p_0, \ldots, p_{2^m-1}\}, k'\right\}, w, r, pt, pad\right)$

Require: Parameter m, $\{p_0, \ldots, p_{2^m-1}\}$, an updated key k',
the length $l = len(r, m)$, the least significant l digits
of the counter $r = r_{l-1}, \ldots, r_0$ with $r_i \in \mathbb{F}_{2^m}$, the plaintext pt,
an indicator whether 0x80 padding is used pad.

Ensure: The ciphertext $ct = ct_0 \ldots ct_{w-1}$ and an updated counter r.

if $pad = 1$ **then**
  Apply padding by adding a 0x80 byte and filling up the block with 0x00
else if $len(pt, 8) \bmod 16 \neq 0$ **then**
  return FAIL
else if $len(pt, 8) = 0$ **then**
  return FAIL
end if
$w = len(pt, 128)$
for $i = 0 \ldots w - 1$ **do**
  $y = \text{evalLRP}\left(m, \left\{\{p_0, \ldots, p_{2^m-1}\}, k'\right\}, l, r, true\right)$
  $ct_i = E_y(pt_i)$
  $r = r + 1$
end for
return $\{r, ct\}$

2.3.2 Algorithm 5

LRICB decryption: $\{r, pt\} = \text{LRICBDecs}\left(m, \left\{\left\{p_0, \ldots, p_{2^m-1}\right\}, k'\right\}, w, r, ct, pad\right)$

Require: Parameter m, $\left\{p_0, \ldots, p_{2^m-1}\right\}$, an updated key k', the length $l = len(r, m)$ the least significant l digits of the counter $r = r_{l-1}, \ldots, r_0$ with $r_i \in \mathbb{F}_{2^m}$, the ciphertext ct.

Ensure: The plaintext $ct = ct_0 \ldots ct_{w-1}$ and an updated counter r.

$w = len\left(ct, 128\right)$
for $i = 0 \ldots w - 1$ **do**
  $y = \text{evalLRP}\left(m, \left\{\left\{p_0, \ldots, p_{2^m-1}, k'\right\}\right\}, l, r, true\right)$
  $pt_i = D_y(ct_i)$
  $r = r + 1$
end for
if $pad = 1$ **then**
  if isPaddingValid(pt) **then**
    pt = removePadding(pt)
  else
    return FAIL
  end if
end if
return $\{r, pt\}$

2.4 LRP-CMAC

LRP-CMAC is obtained by just replacing AES in CMAC by LRP. The CMAC keys K_1 and K_2 are therefore generated as follows:

$$K_0 = \text{evalLRB}\left(m, \left\{\left\{p_0, \ldots, p_{2^m-1}\right\}, k'\right\}, l, \{0\text{x}00\}^{16}, final\right),$$
$$K_1 = K_0 \cdot x \mod x^{128} + x^7 + x^2 + x + 1,$$
$$K_2 = K_0 \cdot x^2 \mod x^{128} + x^7 + x^2 + x + 1.$$

2.4.1 Algorithm 6

$y = \text{CMAC\_LRP}\left(m, \left\{\left\{p_0, \ldots, p_{2^m-1}\right\}, k', K_1, K_2\right\}, l, x\right)$

Require: Parameter m, the plaintexts $\left\{p_0, \ldots, p_{2^m-1}\right\}$, an updated key k', the byte length $l = len(x, 8)$, the input $x = x_0, \ldots, x_{l-1}$, the CMAC keys K_1 and K_2.

Ensure: The CMAC result y.

$y = \{0x00\}^{16}$
$i = 0$
while $l > 16$ **do**
  $y = y \oplus x_i \ldots x_{i+16-1}$
  $y = \text{evalLRP}\left(m, \left\{\left\{p_0, \ldots, p_{2^m-1}\right\}, k'\right\}, y, true\right)$
  $l = l - 16$
  $i = i + 16$
end while
$y = y \oplus x_i \ldots x_{i+l-1}\{0x00\}^{16-l}$
if $l = 16$ **then**
  $y = y \oplus K_1$
else
  $x_{i+l} = 0x80$
  $y = y \oplus K_2$
end if
$y = \text{evalLRP}\left(m, \left\{\left\{p_0, \ldots, p_{2^m-1}\right\}, k'\right\}, y, true\right)$
return y

3 Test Vectors

3.1 LRP Eval in detail

1. **Test Vectors**
   a. **LRP Eval in detail**

Here, Base key refers to *k* in Algorithms 1 and 2. `P[i]` maps to p_i in Algorithm 1 and `UK[i]` maps to k_i in Algorithm 2.

```
Generating Secret Plaintexts and Updated Keys
Base key: 56-78-26-B8-DA-8E-76-84-32-A9-54-8D-BE-4A-A3-A0
    AES block key: 56-78-26-B8-DA-8E-76-84-32-A9-54-8D-BE-4A-A3-A0
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 3A-92-AA-06-40-F2-6A-E9-2F-81-99-36-52-F0-05-18
    AES block key: 56-78-26-B8-DA-8E-76-84-32-A9-54-8D-BE-4A-A3-A0
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 22-DA-7A-8A-2F-4A-72-1D-43-EC-1C-97-02-FE-77-BE
```

```
Generating Secret Plaintexts
Plaintext base key: 3A-92-AA-06-40-F2-6A-E9-2F-81-99-36-52-F0-05-18
    AES block key: 3A-92-AA-06-40-F2-6A-E9-2F-81-99-36-52-F0-05-18
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: AC-20-D3-9F-53-41-FE-98-DF-CA-21-DA-86-BA-79-14
```

```
P[0]: AC-20-D3-9F-53-41-FE-98-DF-CA-21-DA-86-BA-79-14
    AES block key: 3A-92-AA-06-40-F2-6A-E9-2F-81-99-36-52-F0-05-18
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 10-79-E9-6B-0E-24-61-C2-DE-AB-00-30-59-56-54-9A
```

```
Key for next secret plaintext generation: 10-79-E9-6B-0E-24-61-C2-DE-AB-00-30-59-56-54-9A
    AES block key: 10-79-E9-6B-0E-24-61-C2-DE-AB-00-30-59-56-54-9A
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 90-7D-A0-3D-67-24-49-16-69-15-E4-56-3E-08-9D-6D
```

```
P[1]: 90-7D-A0-3D-67-24-49-16-69-15-E4-56-3E-08-9D-6D
    AES block key: 10-79-E9-6B-0E-24-61-C2-DE-AB-00-30-59-56-54-9A
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: F9-A0-89-7A-D9-D3-76-BA-F7-88-6C-62-C8-E8-97-15
```

```
Key for next secret plaintext generation: F9-A0-89-7A-D9-D3-76-BA-F7-88-6C-62-C8-E8-97-15
    AES block key: F9-A0-89-7A-D9-D3-76-BA-F7-88-6C-62-C8-E8-97-15
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 92-FA-A8-B8-78-CC-D5-0C-63-13-DB-59-09-9D-CC-E8
```

```
P[2]: 92-FA-A8-B8-78-CC-D5-0C-63-13-DB-59-09-9D-CC-E8
    AES block key: F9-A0-89-7A-D9-D3-76-BA-F7-88-6C-62-C8-E8-97-15
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 84-B8-14-14-BE-98-AD-7F-12-EE-F0-DD-1B-17-DF-FF
```

```
Key for next secret plaintext generation: 84-B8-14-14-BE-98-AD-7F-12-EE-F0-DD-1B-17-DF-FF
    AES block key: 84-B8-14-14-BE-98-AD-7F-12-EE-F0-DD-1B-17-DF-FF
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 37-2F-A1-3D-D4-3E-FD-41-98-59-DC-BC-FC-EF-FB-F8
```

```
P[3]: 37-2F-A1-3D-D4-3E-FD-41-98-59-DC-BC-FC-EF-FB-F8
    AES block key: 84-B8-14-14-BE-98-AD-7F-12-EE-F0-DD-1B-17-DF-FF
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 02-0C-87-DA-40-8C-3C-8D-E2-C1-58-86-2B-09-B6-3D
```

```
Key for next secret plaintext generation: 02-0C-87-DA-40-8C-3C-8D-E2-C1-58-86-2B-09-B6-3D
    AES block key: 02-0C-87-DA-40-8C-3C-8D-E2-C1-58-86-2B-09-B6-3D
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 5F-E2-E4-68-95-8B-6B-05-C8-A0-34-F3-38-23-CF-1B
```

```
P[4]: 5F-E2-E4-68-95-8B-6B-05-C8-A0-34-F3-38-23-CF-1B
```

```
    AES block key: 02-0C-87-DA-40-8C-3C-8D-E2-C1-58-86-2B-09-B6-3D
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 95-38-28-9A-9A-AC-5B-2D-B4-BB-76-F8-0F-B8-E8-5B
```

```
Key for next secret plaintext generation: 95-38-28-9A-9A-AC-5B-2D-B4-BB-76-F8-0F-B8-E8-5B
    AES block key: 95-38-28-9A-9A-AC-5B-2D-B4-BB-76-F8-0F-B8-E8-5B
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: AB-75-E2-FA-6D-CC-BA-A0-4E-85-D0-7F-B9-4E-ED-28
```

```
P[5]: AB-75-E2-FA-6D-CC-BA-A0-4E-85-D0-7F-B9-4E-ED-28
    AES block key: 95-38-28-9A-9A-AC-5B-2D-B4-BB-76-F8-0F-B8-E8-5B
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: A9-ED-2B-3A-93-C5-07-D1-3C-28-C5-58-2F-C3-5E-12
```

```
Key for next secret plaintext generation: A9-ED-2B-3A-93-C5-07-D1-3C-28-C5-58-2F-C3-5E-12
    AES block key: A9-ED-2B-3A-93-C5-07-D1-3C-28-C5-58-2F-C3-5E-12
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: AC-05-BC-DA-C4-4B-14-BF-FD-F8-90-74-98-69-53-89
```

```
P[6]: AC-05-BC-DA-C4-4B-14-BF-FD-F8-90-74-98-69-53-89
    AES block key: A9-ED-2B-3A-93-C5-07-D1-3C-28-C5-58-2F-C3-5E-12
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 3E-52-A9-EC-91-92-2C-9A-0B-53-E7-9A-44-BE-88-2E
```

```
Key for next secret plaintext generation: 3E-52-A9-EC-91-92-2C-9A-0B-53-E7-9A-44-BE-88-2E
    AES block key: 3E-52-A9-EC-91-92-2C-9A-0B-53-E7-9A-44-BE-88-2E
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 0A-F9-75-ED-75-29-42-D7-56-A8-A9-7C-78-C0-9C-D8
```

```
P[7]: 0A-F9-75-ED-75-29-42-D7-56-A8-A9-7C-78-C0-9C-D8
    AES block key: 3E-52-A9-EC-91-92-2C-9A-0B-53-E7-9A-44-BE-88-2E
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: AF-DA-9A-87-2B-A6-A7-59-CC-9E-AC-6E-A3-24-D9-E4
```

```
Key for next secret plaintext generation: AF-DA-9A-87-2B-A6-A7-59-CC-9E-AC-6E-A3-24-D9-E4
    AES block key: AF-DA-9A-87-2B-A6-A7-59-CC-9E-AC-6E-A3-24-D9-E4
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 4F-58-AF-B5-7C-AD-5F-E1-6C-03-3F-9D-F5-B5-B3-FE
```

```
P[8]: 4F-58-AF-B5-7C-AD-5F-E1-6C-03-3F-9D-F5-B5-B3-FE
    AES block key: AF-DA-9A-87-2B-A6-A7-59-CC-9E-AC-6E-A3-24-D9-E4
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 78-FB-A2-45-D5-AA-8D-0C-F7-3D-EA-EF-B2-5F-19-87
```

```
Key for next secret plaintext generation: 78-FB-A2-45-D5-AA-8D-0C-F7-3D-EA-EF-B2-5F-19-87
    AES block key: 78-FB-A2-45-D5-AA-8D-0C-F7-3D-EA-EF-B2-5F-19-87
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 56-98-D7-B5-F5-95-66-14-D5-7B-5A-18-B9-B8-81-0E
```

```
P[9]: 56-98-D7-B5-F5-95-66-14-D5-7B-5A-18-B9-B8-81-0E
    AES block key: 78-FB-A2-45-D5-AA-8D-0C-F7-3D-EA-EF-B2-5F-19-87
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 0E-E5-92-0E-07-49-07-BB-AE-D5-E5-20-46-CF-09-82
```

```
Key for next secret plaintext generation: 0E-E5-92-0E-07-49-07-BB-AE-D5-E5-20-46-CF-09-82
    AES block key: 0E-E5-92-0E-07-49-07-BB-AE-D5-E5-20-46-CF-09-82
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 5A-C8-CF-BA-77-F7-C6-A6-13-48-AF-B9-2B-11-95-CA
```

```
P[10]: 5A-C8-CF-BA-77-F7-C6-A6-13-48-AF-B9-2B-11-95-CA
    AES block key: 0E-E5-92-0E-07-49-07-BB-AE-D5-E5-20-46-CF-09-82
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 78-59-E9-ED-31-7C-EF-35-AF-37-25-D3-AC-24-9D-CE
```

```
Key for next secret plaintext generation: 78-59-E9-ED-31-7C-EF-35-AF-37-25-D3-AC-24-9D-CE
    AES block key: 78-59-E9-ED-31-7C-EF-35-AF-37-25-D3-AC-24-9D-CE
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
```

```
    AES block ciphertext: 01-2D-66-10-89-16-E2-9A-86-E8-81-46-A1-04-7D-3A
```

```
P[11]: 01-2D-66-10-89-16-E2-9A-86-E8-81-46-A1-04-7D-3A
    AES block key: 78-59-E9-ED-31-7C-EF-35-AF-37-25-D3-AC-24-9D-CE
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 3F-13-F3-72-7B-EC-89-42-3E-B8-6A-96-79-F8-0F-96
```

```
Key for next secret plaintext generation: 3F-13-F3-72-7B-EC-89-42-3E-B8-6A-96-79-F8-0F-96
    AES block key: 3F-13-F3-72-7B-EC-89-42-3E-B8-6A-96-79-F8-0F-96
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 25-F8-F9-25-46-DB-A8-65-11-91-46-FC-9B-26-0B-CA
```

```
P[12]: 25-F8-F9-25-46-DB-A8-65-11-91-46-FC-9B-26-0B-CA
    AES block key: 3F-13-F3-72-7B-EC-89-42-3E-B8-6A-96-79-F8-0F-96
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 92-8A-AD-02-C3-99-8D-AE-13-4C-0D-0E-8B-41-E5-E3
```

```
Key for next secret plaintext generation: 92-8A-AD-02-C3-99-8D-AE-13-4C-0D-0E-8B-41-E5-E3
    AES block key: 92-8A-AD-02-C3-99-8D-AE-13-4C-0D-0E-8B-41-E5-E3
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: BE-9E-E4-4F-C4-2D-8C-73-C6-5E-2B-6D-0B-24-54-EB
```

```
P[13]: BE-9E-E4-4F-C4-2D-8C-73-C6-5E-2B-6D-0B-24-54-EB
    AES block key: 92-8A-AD-02-C3-99-8D-AE-13-4C-0D-0E-8B-41-E5-E3
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: D1-C2-4E-76-35-2E-2F-CE-88-11-B2-82-43-02-CE-79
```

```
Key for next secret plaintext generation: D1-C2-4E-76-35-2E-2F-CE-88-11-B2-82-43-02-CE-79
    AES block key: D1-C2-4E-76-35-2E-2F-CE-88-11-B2-82-43-02-CE-79
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 37-D7-34-A5-1C-07-6E-B8-03-BD-53-0E-17-EB-87-DC
```

```
P[14]: 37-D7-34-A5-1C-07-6E-B8-03-BD-53-0E-17-EB-87-DC
    AES block key: D1-C2-4E-76-35-2E-2F-CE-88-11-B2-82-43-02-CE-79
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 98-BB-7F-E4-92-79-DC-29-B4-FA-9E-02-CA-5D-A2-E0
```

```
Key for next secret plaintext generation: 98-BB-7F-E4-92-79-DC-29-B4-FA-9E-02-CA-5D-A2-E0
    AES block key: 98-BB-7F-E4-92-79-DC-29-B4-FA-9E-02-CA-5D-A2-E0
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 71-B4-44-AF-25-7A-93-21-53-11-D7-58-DD-33-32-47
```

```
P[15]: 71-B4-44-AF-25-7A-93-21-53-11-D7-58-DD-33-32-47
    AES block key: 98-BB-7F-E4-92-79-DC-29-B4-FA-9E-02-CA-5D-A2-E0
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: 1F-6A-A5-2B-46-DF-E0-4E-CB-29-A3-D6-88-47-F0-24
```

```
Key for next secret plaintext generation: 1F-6A-A5-2B-46-DF-E0-4E-CB-29-A3-D6-88-47-F0-24
Updated key base key: 1F-6A-A5-2B-46-DF-E0-4E-CB-29-A3-D6-88-47-F0-24
    AES block key: 22-DA-7A-8A-2F-4A-72-1D-43-EC-1C-97-02-FE-77-BE
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 16-3D-14-ED-24-ED-93-53-73-56-8E-C5-21-E9-6C-F4
```

```
UK[0]: 16-3D-14-ED-24-ED-93-53-73-56-8E-C5-21-E9-6C-F4
    AES block key: 22-DA-7A-8A-2F-4A-72-1D-43-EC-1C-97-02-FE-77-BE
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: E2-39-B7-DA-97-EE-06-02-07-8C-BF-09-BF-59-F2-38
```

```
Key for next updated key generation: 1F-6A-A5-2B-46-DF-E0-4E-CB-29-A3-D6-88-47-F0-24
    AES block key: E2-39-B7-DA-97-EE-06-02-07-8C-BF-09-BF-59-F2-38
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: 1C-51-9C-00-02-08-B9-5A-39-A6-5D-B0-58-32-71-88
```

```
UK[1]: 1C-51-9C-00-02-08-B9-5A-39-A6-5D-B0-58-32-71-88
    AES block key: E2-39-B7-DA-97-EE-06-02-07-8C-BF-09-BF-59-F2-38
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
```

```
    AES block ciphertext: FB-96-9B-27-C1-9B-E2-77-D9-3C-AC-BF-7B-15-F1-A0
```

```
Key for next updated key generation: 1F-6A-A5-2B-46-DF-E0-4E-CB-29-A3-D6-88-47-F0-24
    AES block key: FB-96-9B-27-C1-9B-E2-77-D9-3C-AC-BF-7B-15-F1-A0
    AES block plaintext: AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA-AA
    AES block ciphertext: FE-30-AB-50-46-7E-61-78-3B-FE-6B-5E-05-60-16-0E
```

```
UK[2]: FE-30-AB-50-46-7E-61-78-3B-FE-6B-5E-05-60-16-0E
    AES block key: FB-96-9B-27-C1-9B-E2-77-D9-3C-AC-BF-7B-15-F1-A0
    AES block plaintext: 55-55-55-55-55-55-55-55-55-55-55-55-55-55-55-55
    AES block ciphertext: F1-18-50-83-33-63-A2-62-51-99-74-DB-82-1D-DA-60
```

```
Key for next updated key generation: 1F-6A-A5-2B-46-DF-E0-4E-CB-29-A3-D6-88-47-F0-24
LRP_Eval IV: 13-59
ivNumNibbles: 4
Key: FE-30-AB-50-46-7E-61-78-3B-FE-6B-5E-05-60-16-0E
    Processing IV nibble 0 (1):
    Secret Plaintext to use: 90-7D-A0-3D-67-24-49-16-69-15-E4-56-3E-08-9D-6D
    Key to use: FE-30-AB-50-46-7E-61-78-3B-FE-6B-5E-05-60-16-0E
        AES block key: FE-30-AB-50-46-7E-61-78-3B-FE-6B-5E-05-60-16-0E
        AES block plaintext: 90-7D-A0-3D-67-24-49-16-69-15-E4-56-3E-08-9D-6D
        AES block ciphertext: F5-06-C1-D4-FC-71-27-6C-6C-60-72-E4-AD-EE-38-E5
    intermediate result: F5-06-C1-D4-FC-71-27-6C-6C-60-72-E4-AD-EE-38-E5
    Processing IV nibble 1 (3):
    Secret Plaintext to use: 37-2F-A1-3D-D4-3E-FD-41-98-59-DC-BC-FC-EF-FB-F8
    Key to use: F5-06-C1-D4-FC-71-27-6C-6C-60-72-E4-AD-EE-38-E5
        AES block key: F5-06-C1-D4-FC-71-27-6C-6C-60-72-E4-AD-EE-38-E5
        AES block plaintext: 37-2F-A1-3D-D4-3E-FD-41-98-59-DC-BC-FC-EF-FB-F8
        AES block ciphertext: 44-33-EF-60-7D-7B-44-FD-0A-AD-67-BC-CF-4E-CF-3E
    intermediate result: 44-33-EF-60-7D-7B-44-FD-0A-AD-67-BC-CF-4E-CF-3E
    Processing IV nibble 2 (5):
    Secret Plaintext to use: AB-75-E2-FA-6D-CC-BA-A0-4E-85-D0-7F-B9-4E-ED-28
    Key to use: 44-33-EF-60-7D-7B-44-FD-0A-AD-67-BC-CF-4E-CF-3E
        AES block key: 44-33-EF-60-7D-7B-44-FD-0A-AD-67-BC-CF-4E-CF-3E
        AES block plaintext: AB-75-E2-FA-6D-CC-BA-A0-4E-85-D0-7F-B9-4E-ED-28
        AES block ciphertext: 1F-B2-81-E1-AA-3A-2D-EB-FD-EF-F4-5D-11-89-FC-E4
    intermediate result: 1F-B2-81-E1-AA-3A-2D-EB-FD-EF-F4-5D-11-89-FC-E4
    Processing IV nibble 3 (9):
    Secret Plaintext to use: 56-98-D7-B5-F5-95-66-14-D5-7B-5A-18-B9-B8-81-0E
    Key to use: 1F-B2-81-E1-AA-3A-2D-EB-FD-EF-F4-5D-11-89-FC-E4
        AES block key: 1F-B2-81-E1-AA-3A-2D-EB-FD-EF-F4-5D-11-89-FC-E4
        AES block plaintext: 56-98-D7-B5-F5-95-66-14-D5-7B-5A-18-B9-B8-81-0E
        AES block ciphertext: 2A-20-C7-B6-F5-C8-C2-02-7C-44-70-74-4A-6F-52-D3
    intermediate result: 2A-20-C7-B6-F5-C8-C2-02-7C-44-70-74-4A-6F-52-D3
whitening
Key to use: 2A-20-C7-B6-F5-C8-C2-02-7C-44-70-74-4A-6F-52-D3
    AES block key: 2A-20-C7-B6-F5-C8-C2-02-7C-44-70-74-4A-6F-52-D3
    AES block plaintext: 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
    AES block ciphertext: 1B-A2-C0-C5-78-99-6B-C4-97-DD-18-1C-68-85-A9-DD
result of whitening: 1B-A2-C0-C5-78-99-6B-C4-97-DD-18-1C-68-85-A9-DD
Result: 1B-A2-C0-C5-78-99-6B-C4-97-DD-18-1C-68-85-A9-DD
```

3.2 LRP Eval

Here, IV maps to x in Algorithm 3 whereas KEY is the key used to generate $\{p_0, \ldots, p_{2m-1}\}$ and k^1. UPDATEDKEY refers to the index i of the updated key k_i which is used as k^1. Finally, FINALIZE defines whether the output whitening step is performed.

```
KEY             = 567826B8DA8E768432A9548DBE4AA3A0
IV              = 1359
FINALIZE        = 1
UPDATEDKEY      = 2
RES             = 1BA2C0C578996BC497DD181C6885A9DD
```

```
KEY             = B65557CE0E9B4C5886F232200113562B
IV              = BB4FCF27C94076F756AB030D
FINALIZE        = 0
UPDATEDKEY      = 1
```

```
RES             = 6FDFA8D2A6AA8476BF94E71F25637F96
```

```
KEY             = 88B95581002057A93E421EFE4076338B
IV              = 77299D
FINALIZE        = 1
UPDATEDKEY      = 2
RES             = E9C04556A214AC3297B83E4BDF46F142
```

```
KEY             = C48A8E8B16571645A1557825AA66AC91
IV              = 1F0B7C0DB12889CA436CABB78BE42F9
FINALIZE        = 1
UPDATEDKEY      = 3
RES             = 51296B5E6D3B8DB8A1A7399760A19189
```

```
KEY             = CAF3750AFF93F9A0C8861BCCCCDF1A9D
IV              = 9273B7
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = 468C2BFCF993E7F112E150C17298A968
```

```
KEY             = 65024B14AA99E9CA93F51172E19EE000
IV              = 826CE8A26DFE768D91
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = A3830865D52EAEBC6471CDBD3DFC0A89
```

```
KEY             = 1EDB9D253DF18D72BEEAE960B6FDF325
IV              = FD7BBC6CE819F04AF0C3944C9E
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = B73B50D4BA439DF9D4AFB79FF10F1446
```

```
KEY             = 08CFACB758EB34F0106D42358F22B5EB
IV              = 431B8F155EB1F28334F201CADD7
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = 40C01FC5DF4C142D9C9721F74A373BA5
```

```
KEY             = CC57E7503BCCCF260D6B4E2AB38ACE94
IV              = 4D09838DF371FAC5D5B641EE45
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = C1A465936A097FF76FCAF18166E8DF60
```

```
KEY             = D0E9C3CACE9A747A74F582AA0F873FF9
IV              = FCB69068C83E64765676F718E41E25
FINALIZE        = 1
UPDATEDKEY      = 2
RES             = A944D5A19C5B86392CC3CFC58F57C321
```

```
KEY             = 59C9C703C66A9FD2948E0A48617285DC
IV              = F28EFF672184665744FD835B106484
FINALIZE        = 1
```

```
UPDATEDKEY      = 0
RES             = F078390B345FC6E22EE9A75B3D8BF490
```

```
KEY             = 2E763263979117BED33A331B15E3F01B
IV              = 2B96BFF1A8429C6E
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = 9193DA3870AA345EB4FDFB5EE4A35E61
```

```
KEY             = A14E397DA6C410440FA9EC4C61774094
IV              = 4B42600D
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = 21C0B442BF41B7DDD80D4A99CD7B7B81
```

```
KEY             = 921038ED913CCEEFC6286B756F9ABC8D
IV              = 9FE171DCB4CA1F7E5
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = 9FF1DBB5E8528E56370EB55919642AC0
```

```
KEY             = F2512BC694E7A66D6ED67E0841BA2523
IV              = D0F92AC3F33EC12CF5B65C6ECE12DE0
FINALIZE        = 1
UPDATEDKEY      = 3
RES             = 6271F38386E7399D7FA1709A72B4F585
```

```
KEY             = 75FCA5E188F44F1E808597A0B7B690D4
IV              = 64962F5DED0468F1
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = EBD6F32ED75566E6756A14EC16715CBD
```

```
KEY             = 1000076C2934BDB02750204704DAA472
IV              = 8C3E0
FINALIZE        = 1
UPDATEDKEY      = 2
RES             = 581C3B057F9312FECF4A7B8070C83B8C
```

```
KEY             = 99B1647A76CD170EA07997043E1E7919
IV              = F
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = BA5F895E8B57F7753EE5C7276E60B37F
```

```
KEY             = 6983FC665FBB8BEA35DADBB2EF446656
IV              = BDF09818B0A7AFFF9C8
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = E0A4144033A1CACD1DBCE30F9883A1DB
```

```
KEY             = 9FBC2045FA6215B4FD1ABA412DD9C59D
IV              = F9B72310BDAE086C51D354B65F1F05F1
```

```
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = 3F410411D5ED704572D06EDE6AB45CA2
```

```
KEY             = 1EBB6DF4E251A10B9503AE6B3EEB0ACA
IV              = CDD68EFF713C8
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = 28740D45D92737D6CF8F05D05B961424
```

```
KEY             = 415F46BA9A3C3C44A7E1782117668105
IV              = 590012E84AEC7
FINALIZE        = 0
UPDATEDKEY      = 2
RES             = 9852EFC35E53F2A4E8DA55770123C99D
```

```
KEY             = 371A061E4A3065D00F41C4DA68722FFA
IV              = 52C78A675488D
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = FD2BDCC3EA26AF2069A4C536E3D6B33B
```

```
KEY             = E28DFE591559441D04213D889747BC46
IV              = 414E42E7
FINALIZE        = 1
UPDATEDKEY      = 2
RES             = 5E8BF483C2D6DA906EC58D1B63AC9887
```

```
KEY             = 18A4209AAEF2CFC67E48834ED7D2B62B
IV              = 4B6E0EBCBB920A0B441114478
FINALIZE        = 0
UPDATEDKEY      = 0
RES             = D054F91224DAC4C9E46EDF7EFAB6D179
```

```
KEY             = FBBCE5B5F4BF962A345BBF3F13F9E474
IV              = D6B8F778C25
FINALIZE        = 1
UPDATEDKEY      = 2
RES             = 73C265CD18C9F909784DCFC4CAA5109D
```

```
KEY             = 8E90A2AEBEB136C000521AEC0037ACFF
IV              = B3FD7B7F1026CF70FF71CF8
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = 7F519F9B9EAB01EF8DED79520C46770E
```

```
KEY             = FA89CC662EF47C75A9887F12A6C9879F
IV              = B9
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = 4973ECE66EEE903D4761EF3960210735
```

```
KEY             = 3F0E5E6D0F7F7BDE4DB2C4F074D02062
```

```
IV              = 7D0AA4C30A75FC6C6A5D47D12247
FINALIZE        = 1
UPDATEDKEY      = 3
RES             = 87F43A64DAF93DF744F54FECE1A480AB
```

```
KEY             = B443EC2B5E56AF789D27F6C38F9DD6A9
IV              = 0CACAE327B04E870A3151E967
FINALIZE        = 0
UPDATEDKEY      = 0
RES             = 795553EBFA89AD541C0ED2E5F3C4611F
```

```
KEY             = 7DD9BF8D3337D57ACD92069B13B16CCE
IV              = 2266169A6882C7E84
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = 49F4FFFEA580EC96D5DCACC9E10AA95E
```

```
KEY             = B39A5A07AB6746B5DE4875ED9492DF1B
IV              = F03704D4806A731
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = 635E39AEF94D050B5424E1D967027594
```

```
KEY             = E2703DC54BF4E7C63337FFF0AB6BB6F0
IV              = 35D183BB4C56E8F70B
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = 3E537D77DE31EA05C33CE70B4ECE65FA
```

```
KEY             = DF19EF9394EE6344A0832AF8ADCBABE4
IV              = 44CB4DE4352D3E45F5
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = 80F1A5169142107FF0873BC4222E8173
```

```
KEY             = 24E6DD53E9FEE719486C5CBD07714FC8
IV              = 24B80F682AF9B33
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = 4FA0477728E34E1408D98643F8124035
```

```
KEY             = FAE4C2544FF93C20BAA6D60FAFE4919B
IV              = 87C4DB
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = FD2847D87ADC24C27FA042D1DCA1459B
```

```
KEY             = 6D1902203D17BCBCE3A0A961EC358517
IV              = CA5195213C2C75D37DCC6A67
FINALIZE        = 1
UPDATEDKEY      = 3
```

```
RES             = 2EADE5706A4BCD7CAF844DE01B127CE0
```

```
KEY             = 7BC16676A8522EBC2564FEC235654DF8
IV              = A885
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = 9819FE9556933E1CFC4E99C8BF64ACFA
```

```
KEY             = F989FF4BDDD5AB6999EF517B742EA085
IV              = C4DE07A5E
FINALIZE        = 0
UPDATEDKEY      = 0
RES             = D6FEE60DBC8BA533E320ED1D18076D82
```

```
KEY             = 5F07C727DA21B6C1E2688237672BCB7D
IV              = 8C74AC47C037AD729D38E3A
FINALIZE        = 0
UPDATEDKEY      = 0
RES             = 6021FC212F818102027C61FCE28D382C
```

```
KEY             = 549C67ECD60E848F773990990CAC681E
IV              = 475BB41878EB17468F7A68847DDD3BAC
FINALIZE        = 1
UPDATEDKEY      = 3
RES             = C3B5EE74A722E784887C4C9FDB497855
```

```
KEY             = 9AFF3EF56FFEC3153B1CADB48B445409
IV              = 4B073B247CD48F7E0A
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = 909415E5C8BE77563050F2227E17C0E4
```

```
KEY             = F2BBB25D607ECD1E551CD75CF0033CCE
IV              = 0335137B5641EFA4F176836A65F0F49
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = 87832A9AF79C6CE436EA4DB6CAB18203
```

```
KEY             = 806A50530D7735B40AC4EF1638E8AD6A
IV              = D4137764716DBC8C579BEAB7E76754E
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = CF991392F0369350A7E21BE52F748821
```

```
KEY             = 64193EF6BDDDC74C7C008DB98ED5FF67
IV              = 89AB
FINALIZE        = 1
UPDATEDKEY      = 3
RES             = 4A828E35DBADF6A465321363717D0D27
```

```
KEY             = F9E29780209AC952DD87C2572C4950BF
IV              = 35AF18F46C2FD3C8C6EB507147CA35A
FINALIZE        = 1
```

```
UPDATEDKEY      = 1
RES             = 51F3482AB8880850390F4F6D775F5C1F
```

```
KEY             = 37A6769D43FEFA9F79CA61628BAFA7F1
IV              = FB
FINALIZE        = 1
UPDATEDKEY      = 0
RES             = 81C84283D18071F08DE72AD51B5826B6
```

```
KEY             = 047568AC57D4DE026C40F7228BDD1819
IV              = F1B11
FINALIZE        = 0
UPDATEDKEY      = 3
RES             = 9CE6BEC0F80FDF7D78B1C219130102E7
```

```
KEY             = F36472663A3BA87F3E76399C66C23EC9
IV              = 1FF73338D23ED6AE968
FINALIZE        = 1
UPDATEDKEY      = 1
RES             = 36DA0902796F4682034DB07D0FF58E28
```

```
KEY             = 906249E5AF810339F199A25AEC0281E8
IV              = 56DA443282912622BB92338F8CA
FINALIZE        = 1
UPDATEDKEY      = 2
RES             = 317600A76B5A7984A681D1D8855F86FC
```

3.3 LRP LRICB

Here, IV refers to the counter value *r* and USEPADDING refers to *pad* in Algorithm 4. For k^1 the test vectors always use k_0.

```
KEY             = E0C4935FF0C254CD2CEF8FDDC32460CF
IV              = C3315DBF
USEPADDING      = 1
PT              = 012D7F1653CAF6503C6AB0C1010E8CB0
CT              = FCBBACAA4F29182464F99DE41085266F
                  480E863E487BAAF687B43ED1ECE0D623
```

```
KEY             = EFA5B7429CD153BF0086DEF900C0F235
IV              = 9036FFFF
USEPADDING      = 0
PT              = E7F61E012F4F3255312BA68B1D2FDABF
CT              = EA6E09AC2FB97E102D8CA64C1CBC0C0C
```

```
KEY             = 15CDECFC507C777B31CA4D6562D809F2
IV              = 5B29FFFF
USEPADDING      = 0
PT              = AA8EC68E0519914D8F00CFD8EA226B7E
CT              = C8FBD3842E69C8E2EBCA96CE28AB02F0
```

```
KEY             = A2D06401CDF35822B430F4457D1D1775
IV              = 5C35A6ED
```

```
USEPADDING      = 1
PT              = D2D83A1971077EDDFE2DF28DF9B736A4
                  D9D4244BCF72E9597CB47B7DCDB5A4B2
                  45B52080E79BBFEDC69F1EE983CE
CT              = 73B1BED57B59090BC496799FA9BFE9F5
                  252A88350A8F48A4FF252B8E813F6D96
                  CA8BA7C8162E4CB2DFE0D53800FF01DA
```

```
KEY             = 3CEEB70C13578D714860EEE19DBC8B01
IV              = 104988FF
USEPADDING      = 0
PT              = 3E1537842F53FFD5AD788DC6C0A14D25
CT              = 0EFEEAE6249011EF6CD2D28980B93766
```

```
KEY             = D36CC09105FD0261C58FD5604486F757
IV              = 01FFFFFF
USEPADDING      = 0
PT              = EF44FE3B50A73B1974D7D624B74012D5
                  BEA07D9F91278035C470CD0BD0E753B2
                  A2F90DBE638A3F2E252A112081DC9894
                  2F802D788F4F7AC8C3C876DFDA30498D
                  842382BD32537134614F7A671660B4E8
                  D738DB50B9DA23527F45FA9B145F54F4
                  E0839C5D5ADA61DC0EF91740D513B263
                  148E08A155F9D4A9002F3EED58D62002
                  FA858692C3578DFDD7FE41BFC2E27D6C
CT              = F72471266DE22E2C66A6B89F20CA0085
                  9B63A41E396A592EF6673E3A5220DF70
                  B9E0D3EFF3503F81F203573871CD5006
                  679A10071B861C3A71B02B86C766576F
                  35DE0790913E7A429C28DB6C398FEA5F
                  9E140F92F5C6729F7FFAD38DE456F1D6
                  222569B461568091B305AB69F19930BC
                  489D18B8C3D6FA7B3D37467E4F3A6C95
                  77E8C285C375A0B73970016BDB288AE4
```

```
KEY             = 9397878556B29FE7AFF25C2A9C748338
IV              = D9154550
USEPADDING      = 1
PT              = CA56B814E61EB2D25AC14E9AAB48E59F
                  E3D0FB6360637B09E6
CT              = E1D03C38C92DDF5A7C5A3FC1AA52E746
                  27192A01143D26E8F592EE5D3C335168
```

```
KEY             = AD9C2DDF73F7CA844BE8492F9A0C3D77
IV              = C9FFFFFF
USEPADDING      = 0
PT              = CEC19DAA67DAAE2E398185F2E6CA8415
                  5F5F9C7048C4BDEB9649B920A7429FC3
                  F2372809E7A1816E806BD2BCF2D732F7
                  64290B9ECE7CF30A04B1131D218E87F6
                  E2C2FFAFA17A2DBDDD2DF0DCF101F8BF
CT              = AA8D27EFC3D3ABF80A487C6C3577B2AB
                  6B2FAA4317C0B3EFBB8C9A301F21C5FD
                  2FE0E2E27B6516B8678121091A411D8A
                  08B7E1111E9DB13DB169B2D305200767
```

```
                  9E84BE742D4AEABD11FAE5624D49EDE0
```

```
KEY             = 16C1BB7D3701F476431E05368D634DF2
IV              = E4DCDA30
USEPADDING      = 0
PT              = 4DC0A08C161803B9540760D209BFE1CD
                  896C8375F72F79E0FEF81527C8E8936B
                  D182E94054EA2D05027D395CED1FDA1C
                  F8634D16D274031E46C08E1D03DCF06C
                  74F40187D6A0789F3F7D737AF51DF3DE
                  1EF92E649A7C985D7ECAFA945C0F0226
                  8CCDE8F81D524558EAAED75500892829
                  CCAFFF09AD8CD1F75CA4090CA5E4422F
                  7B4DEE2835FAC0CBB3D579EBA4435CF5
                  A1D1C7AC0FF878FFFCF09B794939B206
                  6BA7D9B39A00F3D1EE3356D812E55219
                  47146AD41D961F83D5EE2B445F47827A
                  227380FD69A85AA1DDF5BEDBA29FED16
CT              = B1CF729E877227D606F104827ED07334
                  FBF1AA7782341C77BBEB31EFAB36B963
                  44431098AB2658A5D7F7ADA4B60680C5
                  727F418037DEF71DA1A12AD4C621C74C
                  CD0C3923769798BF7B401C91AA23B060
                  358B7BB3FA831B1D06A85ED5EA8B0A8B
                  1747BCC6D64D3639F8D1B8EBB633C4A0
                  2279B59C7E250113080B0240C2947E73
                  BC774B8A1A981F85FE9C18D1C9BA0259
                  54E803C08756FC1FD9B83E0CF56C41EC
                  6D32C0EE1946CD6E80E541CC9A0A407C
                  6D171855D0793080A0FE423A0D1B63C4
                  5C03F7789552F28E72849DCC42F31F91
```

```
KEY             = 9D813134CFDEE9D58755DEACD4AF72A7
IV              = FFFFFFFF
USEPADDING      = 1
PT              = 27
CT              = F5833FC397356EA3D9ECADBB9F6FE440
```

```
KEY             = D744E1350115A7DD154DAA448AAA7513
IV              = CAAECC2D
USEPADDING      = 0
PT              = E94EB047D1927A06E6C1FE4374A8AABE
CT              = 5A00BAA47E1753668D605A1998843DC8
```

```
KEY             = 08949164317113BBE09CD40CFCC9A4C0
IV              = 191B4BB2
USEPADDING      = 1
PT              = 5EC9AC319F21030D25EE85C595783BF5
                  6635BE6E0A1C1D3E2A585CF859A8880E
                  918C134A0EAFFCB208EEA3B53A5386D3
CT              = AE617C37C4F55FD711DFD2E3025524C7
                  CA08571CC556A3C85C3BFC9652916070
                  D1CEF452A089F65BE4A981EA9694CCF1
```

```
                  133087AB70D7FCC7EC9496F4F83ADEA5
```

```
KEY             = 7770F8D6C4639941AB6E0746C40AB47C
IV              = 65773408
USEPADDING      = 0
PT              = 0B651B786704D6D28981E9B0B24A2EF2
                  D19EA0A7B5EDFE3A274FC31F7E6D8689
                  409DB8FD7EC8446A31743B89CBCCB32C
CT              = 55BEB785703EDE175B4EA69054023EB3
                  CF3996C55D3D0FD5D8ED757C397E066C
                  1453ADC6879FF2F501765524CAE5AA27
```

```
KEY             = 061593514510831E67E1511741B6541C
IV              = FA5F6F15
USEPADDING      = 1
PT              = 7641B2746F5A9C961968DA3544301999
                  969C762C297A1F1E8F6C5D9E9AD5A089
                  F60F99416BF372F77BAA9DEB42C51B3E
                  FBF899D7932E0DFB2193E502FCFEFB43
                  C7503E3497D82EA32A7EB17EDD34DCC9
                  511EA2A23CC9F6C8029D20D80D6FFA7C
                  AE5923F187E6A723C9F6AC14
CT              = B3CB99514F0AFE7151C3743FAF7DB17E
                  622529CE16F3BB9203BA7DBE45DC89CB
                  3AFDEF19F47CA9BEB54B46F0AB3347FC
                  80BCE7BDF21A2DDB4EB6A425923977FD
                  201A8163865E9BD73B4384702BAF33E7
                  D693DE4D8F6DA00097133E3AA77E25BD
                  5277A24DF1361B5F4725C9FE4CF89145
```

```
KEY             = 7C8E1EEDB71BB1DE5B5907FE5A7532F9
IV              = B85695BB
USEPADDING      = 1
PT              = 426A777FD8451CE14C737F3221F1BD1C
CT              = 9B5C42B96086FB2A9A9AC0B280F020B4
                  B4734EBAD2D6A73BE758B9C8CC7226E5
```

```
KEY             = 215551249711B3AE6B7361F19048BF9A
IV              = DCCCFFFF
USEPADDING      = 0
PT              = 7929BF798535A3FE67127A32EC5330B7
CT              = 6C4D5A30B3102D627721D19EDDCEC534
```

```
KEY             = C91464E42B5004B4E556541876B546D4
IV              = 8F421EFF
USEPADDING      = 1
PT              = 354467EF78A8909DC61CDEB628250A94
CT              = 0ADA577B841FC5CB112230336B33CDA7
```

```
                  2E17D303D05EC66CAECF892B0C282DF5
```

```
KEY             = 2EE08B87B1CCA5A2A93548C2952E2526
IV              = 3827CF6F
USEPADDING      = 1
PT              = B8B18B
CT              = 29E99882A0DCED4E55FB3E61303DE275
```

```
KEY             = F5C3E99FB75E316B76689FC5464260CD
IV              = 0797F6B7
USEPADDING      = 1
PT              =
CT              = 93DC3EE14B612BE6A3E9E2E8040CDFCB
```

```
KEY             = C7031CA1994DECF01D4084D8F577C6F5
IV              = CDB066D0
USEPADDING      = 1
PT              =
CT              = 3B1DAAC45010793FD592FB76827796A5
```

```
KEY             = 10E7C2FA0DF36D4E89F05B15C9DD1BB2
IV              = D42802DB
USEPADDING      = 0
PT              = B150EFCB5EA66A0D8888652AF6104C17
CT              = ACA71BCE7E9057EA8B834B37BF028D1C
```

```
KEY             = 896B876BDF03D34B1DE3F8973323FDC7
IV              = FFFFFFFF
USEPADDING      = 0
PT              = 4054B588DE18B6C46BA699C3E2AD7DA3
                  AD7AADD3DA658A9D97BDB3A99805403D
                  7BD7C27E959405E0E16EB7572ECF55AE
                  25DBD5B09C1D2EDACA18F120640C2C66
                  665C480BEAFF0D1975CDF26BAD336FC7
CT              = 60801EEFA4D5506A73753F826F82EFE6
                  B02E6579BB654256BAC5C7ED81E16A19
                  0BF8953A056FB869A9C5C10C87AE3FDE
                  28CE32730B290F4EB0062E96AB29B40F
                  764AD5D8ACE61997EC515BB69B24E6C0
```

```
KEY             = 680583BD2F90A05DA9E8B37DA2E47CD4
IV              = 4151F0D2
USEPADDING      = 1
PT              = 3BCE2BC22D96A92AB85E896F36D6BBEA
                  6102
CT              = 82A7917C5D9B16C8B01277F3E4FF6BD1
```

```
                  4BF404176F344188F7F8AB2D072C0F99
```

```
KEY             = 4B8F7691511E2A5C429C401D415CEE73
IV              = 55D131FF
USEPADDING      = 1
PT              = D2
CT              = 83FF5F0382BC7EA5C795122C83D3B0C2
```

```
KEY             = 1B1A179CE9C0DB3E45A97D0D98D0530C
IV              = E9FFFFFF
USEPADDING      = 0
PT              = 472DBAFE6434D357402785A3348081B0
                  2EAB54244EE9C9C88E91001C5158992D
                  E36E79AD8446454939940902C8746669B
CT              = 397C9EFFD28C560411B934895C8DF60F
                  082B9560778F8571B5C31A057B34C235
                  2F11B5634788623499C6BDD5C490F5CB
```

```
KEY             = ABD094D694942C5E64F26FD333B705E7
IV              = 8E57BFC6
USEPADDING      = 1
PT              =
CT              = C96E153DDBEC9B8CE23A142A34230CD1
```

```
KEY             = EA0D599D41482A647081C4C3994F411A
IV              = 48FFFFFF
USEPADDING      = 0
PT              = 86A093D7A4AC7089A91E04C7B127A8CE
                  468423CABE6F84ED8B9A10F4F568D3B1
                  FF11C18AD099DC18530FA6231681E0AF
                  C8473CB585D371161CA64C0A9C7B9441
                  4B53C79F661EFDADA80B76AEC960D609
                  B9602CAE2B1D2B2CA0AA6E2A4CD27BD8
                  7A65D8C3BA4149A9498F0D7A5CC24DBB
CT              = 557D92979767DF003FAC2D865C5650FB
                  00936AE565D4413A506E82DA0BADED4C
                  CA98E0F82A602893AE2C8122F2757E3F
                  20AB6AB5D66EED94F2C7908E3AB0F03F
                  1B6FD87DF5FB347C0A8A8F8C8334B4A8
                  9D66D4ACA4D5E1AC398F9198723A54EA
                  E62E52A331D18E2F252C2737DDA6A950
```

```
KEY             = D042503B4FE6152D279BFFBBB0D360D5
IV              = 8F9E3364
USEPADDING      = 1
PT              = 649C0FB1CFDD5CB2590A814089944FAA
CT              = 7BB7E3DA21CBCCEAAEDB71798114656C
                  331C7D2DCD661C43F679FC50FA0239E5
```

```
KEY             = 9B1E418DF9752F37EBBD8EE833BDF2D7
```

```
IV              = 24FFFFFF
USEPADDING      = 1
PT              = 55534E159F14DD7731368988EE6DD7C6
                  114E747F9C17A91BBC12D68C26531F2F
                  FCFC
CT              = 158B3B9C6136FB715CCF435CA4CADE80
                  8D1F98431327061A9A64D52A5FE7B274
                  6D7F5A633FC0CFE7855656AD3C6B94CF
```

```
KEY             = D9E39CA8EFD45645C1A19B44920B46AE
IV              = B9D3EA7D
USEPADDING      = 1
PT              = 3D5050DD16598BF294F32A695F9F2956
                  560880787FCB4677994C447F1F9B3969
                  4F629605F5E38A41B8A077528450734A
                  5486E7A1B2E00D7209D943CA150CD3F9
                  BAC119FD092361727E3FBFDF53F4F249
CT              = 0241258DBBC6395735FE6F8B81BB958A
                  3758FD7C772F801EA689A1B3DB83D711
                  CC0E16CF08AEFB39E3DF50551AAB8293
                  E16085B0B7805C2CCFB9A0D2E8FC7354
                  2C844A35A9B352F750F8E9344591E2BE
                  C55C87E4AFDE1FA5FAB6AF09357EF28C
```

```
KEY             = D9F92A98B398B76E5523FC1B9FC02CAB
IV              = CC7E98C3
USEPADDING      = 0
PT              = 752273212D1F14E6FAF01BE13A452109
                  ABA7E52646D2BE121313D55C2F1262B8
                  F9743D76434D2704E735A5CF10CA9138
                  76B98BCE5B0ADEA263600D1A49B7B6E7
                  8D63E7C607AAC65D7FE13E112DEF0249
                  819CE57687945CEF959B13E33F0DBA30
                  7EBD41ADE2CA30CCF32D4E7ACBCD7574
                  5EC498ADD14060F906F8316C97E21E72
                  260E936FAD5466B66B19825A45E224C8
                  259E847B740D5E3D5D48A7EA99C33410
                  0EDC54BC3A06C60A5DE141B8BE06B323
                  D36847F85DA3FD18B0551265AC7C1DA7
                  E4714B698E678E1ED87A1E92CCA67E57
CT              = 6CF4254823B6A182B155A4280F5DD9B8
                  6F83968BCA07ABB552077647446C5AE4
                  1584B964CB69C03B84BBA9CD181AF608
                  48488B355B058FBEC74FFF11F5A4F05A
                  D15138FA2C4C71BA0AB15C35EDEA9958
                  F6C1904CEC673936554611A47BEDEC46
                  7387B99E4D3415C716AECA75039F4FBD
                  B19BE15E042E81522CD819122D3B9D00
                  7B9D5DF4A11AFC4FEB58DE24821CE507
                  B2B2B720355E3B23275B05AC543C61EC
                  3905B01B1B3704A86577FE7B4204FC84
                  8AF94E612C2A168568D4F44326113AEB
                  7F767E5B43A4B3B2987EDDBD279A8E37
```

```
KEY             = 948316307C3CB26BDE3B0CE4F4605DE0
```

```
IV              = C4FFFFFF
USEPADDING      = 0
PT              = 20E3846A4C09D7BAD12965EC2BA8BFDF

CT              = BB1942D3E6F866ADD796B7EA85755D57
```

```
KEY             = 8A525AA92A771D3DCE32D2329C49EEAA
IV              = 5653FFFF
USEPADDING      = 1
PT              = 33
CT              = 352BBE318443FB9A095621256F9FB523
```

```
KEY             = 7BD86E2B8DDBBF431130FDA8C5479C19
IV              = 37A41E87
USEPADDING      = 1
PT              = 1762579CF1E8E9C1F6C4A7A5C089AB99
                  2555740A9FD7D5CB681A07F9C042969F
                  9EE3A8E0B9940CC0DB85A5558FFF5EFE
                  8F21708117E459408C8B33D7E0F001B4
                  2D0807DDE0CADF9149B32E1931803C69
                  BC09699ED11587B98968532D6035DFEB
                  84F12787F8801DC442DE3864B63F0F0C
                  4FCA1AD78763E218814D537877B13114
                  D443953F58B5703BEBA45BF2DD230349
                  5946DE951A0763200E0F06AA2DA44D90
                  AD238F72
CT              = C1A48806D8F8A135B7A68636A21203D4
                  A414AEEC663557BA029DB5665EB7BEB6
                  9A93E7812277279B501A8EB96EEC64E6
                  6874AE7EE33A80CD5D2C3C65B02BF125
                  B989E6BB72BFBC6266A915EDFE05D12B
                  967E8B5C29D37A8B5A4DEB0DB7CC3206
                  4EA95C802377C4C22AE5AECAE61EADB9
                  062B8E88382A194ECEB7F08B211FA9E3
                  B1A69D9B37C243D47C9AA56C969C3BA8
                  E2ED668E83BC369CB5C423EBF9A226E7
                  AF00721AFFEB7AE544C9BABD84E4EE3E
```

```
KEY             = AACFB49A5ADFECE208EF3B5D4A091F30
IV              = D3FFFFFF
USEPADDING      = 1
PT              = 4657CA45B993909F8992433B3B1B8118
                  1ED4A85F23851CBD112AC292369E6BEB
                  93D0A58A3DAA82C9BA6A959E8F60BDB1
                  5E5C12740667EAC13B0C338ED1FE69EB
                  2758A76A75F7DA7452DEA5B9EF7D2EB1
                  6C1034D98BF7E42CE6E44E3076F3F7BB
                  01A97636B8533B67819E2127C130D1BD
                  DE8222C1CA8F6030737B8391A8AAFD5F
                  E6E9B84606F7F819D4CD58EDD5BD6AB6
                  129051F4D136F1714946C33DCFAABED7
                  A0C240D7778AB7E78A09EDFD37725AB6
                  10CD7E1758088DB0F846FCBF33BA492A
                  0E
CT              = E55B18F8DF0546749E5637BDFB11460B
```

```
                  AF0BAB9F8CF2D2344335BE43E4F624D4
                  34EA724407C9CCA1CB0719C0D508B2A7
                  9D9B2AD6552AF40412E1D835707542AF
                  A91C764C32DBC18272C9E88BB2763974
                  FF9C6AF1888459589FC4CF86157F311C
                  3E96C252396FD0CA5E43F8746ABF6501
                  A7141806A82B57BEB506EB9B6D0D6977
                  C0F5859B4A5BB15484F350B6DB8ED144
                  E3D9368B39E2295A180536D4AAC5D180
                  02E277E9EF4D9E0D408CB0FE7D08F612
                  92C2554E9AC18B1F94538E8904F66D2B
                  7002231D3FB984365D4013061D963F63

KEY             = 814C137C933E88D96A69C849F43AD6EC
IV              = 0DFFFFFF
USEPADDING      = 0
PT              = 308EF7B3CFBFC2EEB62647397D8FF63D
CT              = B5D3F8560A4577820D2E839D8EF122A5

KEY             = EE9FC566040C26D3268D47FE6602B4DF
IV              = FFFFFFFF
USEPADDING      = 1
PT              = B0A5D3AF72356A90F86E29
CT              = 38D1239AF8949B43101EF67CB1C6F211

KEY             = DB2467238C4278C488B371684DC981FC
IV              = 5A3705BD
USEPADDING      = 0
PT              = 53DED4C9FB71BB70C2D8E992BF2A5790
CT              = 77813088C92EE813F90A7F7FCC42F88C

KEY             = C17CD03E3D85E5F0380F59F3B149DC9C
IV              = F2F53964
USEPADDING      = 1
PT              = 8BF1986A9B0CAD2C1E81B736F1CEF8E3
CT              = 5AD8ACC4AF8AFD1F5A5E269D53B592DF
                  3E9965397F2CE7005BF6AECE35D1D39D

KEY             = 90EC18C8BF78FB4C9FC9F1F3EDC6F08F
IV              = 8845F9F4
USEPADDING      = 1
PT              = 2A5AE4BB036B6BBF6AA029ED3812F64B
                  CAD11BB93F589127AEABD4048BC278CB
                  813A4EA067E4C586872E5B4F669A0DE6
CT              = 0EBF6D014252EA52C077B67AA2BEFAD2
                  0847A449B450B8CB1FDC3649E2C20FAD
                  168A0F40D8982FEB2FB1A8CDE5504A1B
                  FD4BE3A732272E049ECD5B78BEE385F9

KEY             = FD0C03A1318C45D2C8BD0D58966733A8
```

```
IV              = 275D6CFE
USEPADDING      = 1
PT              = 31
CT              = A126BB809FBA89EA9F656104F449BED6
```

```
KEY             = 10FC41C1139DED067FBED69AF5F47CD7
IV              = AAD66DEF
USEPADDING      = 1
PT              = 0F22A828
CT              = D47A868705A125678D9B1B8FF67978B7
```

```
KEY             = 1D959B5A35D586FBFABAA961B4EA50C2
IV              = 760948FF
USEPADDING      = 0
PT              = 4A19B8E48ECB5E56A040FF9ABFA650AF
                  DCB246BE46C8D746B705DA2AEF0EF7F5
                  481F8B6D42152CDE035E490FC3DC4AA1
                  2D8932EB6052CF8241722C88F0336692
                  490951A01BE36DC68667BBE77EC883DB
CT              = D9339BB44320E9A58113E928753A441C
                  499E17B4289C7FA1ECF6F640C42618BE
                  599A3C70E475325C3123FEA5E2C2B2C2
                  E17046EA3610EBF3DD50FEC8EC131B9E
                  52021A8A4B5826CD599C05C38E190358
```

```
KEY             = BB38FD66DB0B95F54F092BD0E9A3EDCF
IV              = F7B7C5B9
USEPADDING      = 0
PT              = 6B65F897E80379EF50CDB836FFB63E74
CT              = 800B79783988A4B9C38B580DBD43B29F
```

```
KEY             = 5C5112B79CDDE37AECEFC602C95110B2
IV              = B24A6FA6
USEPADDING      = 1
PT              = 98D5
CT              = 98B5D3CAE67A2AE3C05455E5EC5FBFEB
```

```
KEY             = 3498F80187442E5974927F8E827DABF8
IV              = 3D7725FF
USEPADDING      = 1
PT              = D7
CT              = CE6ECAEC9FBEAAF74C2AD5AFBE66B697
```

```
KEY             = FDEA0C05BB450D4553F7C47A8423B73D
IV              = 20CBE124
USEPADDING      = 1
PT              = 98192E1443BBEF6D306F678DC3487437
CT              = B473762E32201AD37E60A64945A7D312
```

```
                  3912F4280283876BD1672F62062A9254
```

```
KEY             = 570079FCA0DC05C863E96473B8497B45
IV              = CAFFADF3
USEPADDING      = 1
PT              =
CT              = B23F34E57538504915DDA4479CFCA3FE
```

```
KEY             = 17F248D6920799AFE75B6E4E3E1BBC14
IV              = FFFFFFFF
USEPADDING      = 1
PT              = 9B8020184B707288E9BCF1D1E2CBC4D0
                  ED0DF78CE4F1DFB18D5BB20E630B54B5
                  CF43FE2EC74222DECB93D25774E0768B
CT              = 8C8F3AB5C6863E45D1DE3DBEB1CFF992
                  510ABB95B44188B71EEBAA3E86655BA9
                  A3F59795337F7E2299AE771D3428EC7C
                  01AAB4432B046526A9641FB580613CBD
```

```
KEY             = B7E4F9E62A37DFAAA16F8BF0BD6325DE
IV              = 683C01FF
USEPADDING      = 1
PT              = 511E883CADE426577E126D8A9864548D
                  58B73220686DF3EF37DED8BF20DC4EFB
                  11768E8B1932DE0B970BA7CCFAB2693A
                  7809B0F3B8F857E32B9904CE0C6736A2
CT              = AE43CEB7586F6BB2848C623E01E26CE2
                  575CE57EC97AB064E498A5D0D8831399
                  E7D40471B5F7E984F679E0D8183D831D
                  4230679D24A21FA47F8D9E6775B16C08
                  B5367247F68ABDD4E6CF6196213BFA1F
```

3.4 LRP CMAC

Here, MSG refers to the input x and MAC refers to y in Algorithm 6. For k^1 the test vectors always use k_0. Finally, Kx refers to the subkeys (K1 or K2) used in CMAC.

```
KEY         = 63A0169B4D9FE42C72B2784C806EAC21
Kx          = 84F2F5E532EF011BE4E122C3CF215FC1
MSG         =
MAC         = 0E07C601970814A4176FDA633C6FC3DE
```

```
KEY         = 8195088CE6C393708EBBE6C7914ECB0B
Kx          = 2D22571A33B2965A9B49FF4395A43046
MSG         = BBD5B85772C7
MAC         = AD8595E0B49C5C0DB18E77355F5AAFF6
```

```
KEY         = 59242F9365E79E5F155B1430D8BA2E56
Kx          = 785B8545675572C4262A9801B1559947
MSG         =
```

```
MAC         = B8306666C22F9FF3B53A074C6004ABB5
```

```
KEY         = E7FEB463C2498E04EFC5BF503473FC3A
Kx          = EC31EA82E247DB1AAE486AE404C5D252
MSG         = F3EFB6B0D4A7
MAC         = C17AA38420EE2AA13087578CFBB0B7F3
```

```
KEY         = 7860B864632C6C8BC9A4C06D49D7E2AE
Kx          = C3D55306E216D704D6FFDB120D56B990
MSG         = DC7F
MAC         = 59D3D3A4307A3BBD8E8E5F4B8E75510D
```

```
KEY         = E2F84A0B0AF40EFEB3EEA215A436605C
Kx          = 6843C8FDC5C7AEABDF473D186A42EDA3
MSG         = 8BF1DDA9FE445560A4F4EB9CE0
MAC         = D04382DF71BC293FEC4BB10BDB13805F
```

```
KEY         = D66C19216297BAA60D7EA7C13E7839F9
Kx          = 3E97953DA78AEF240AD537372C51D471
MSG         = 56076C610CAFB99D0EFAB679C360F342
              02655178EE7E7236E8BFCC1C66BDDA17
              F2F67F65ADBF55E70009FE84F0477B18
              45B7E5B48231FBD89436794CE39D3651
              1F9F86CCE08E95430F6977E57FEE45A0
              44B3D7AFD72694C1FAA6D07645080363
              D2AC6451C1AE37B621A1
MAC         = EFFA1488A73FDBCE5B91BBF9B8D51775
```

```
KEY         = A418BA1658A6F0D90830C58679F80AC4
Kx          = 43033791EEA9FF04B189958D562C6A5C
MSG         = 06
MAC         = FF9561CC6E45FFFD4388003AA5F61233
```

```
KEY         = 651312D289F4DE957C208D35827C07E4
Kx          = 3854A163527454454441B1B4C7D3B835
MSG         = D39E4B336C46FCDCFDF803A49EB3A603
              851CFCFA72B3A5F843768EBDEDEB9398
              91059275C79F1DADE2B97E288A91E3
MAC         = 9B1530F1AD35213EB8903D5610BFD7C4
```

```
KEY         = C960E0C80D89728D1FF952EFF5B83FEE
Kx          = C0E47345C0AABE83D0BE0CE2624D9097
MSG         = 21
MAC         = 4EBEE65E5DD0C30F89C8ED49A3D2BF32
```

```
KEY         = 313CE6FF4F18B9357C6EB292C55C0D22
Kx          = 4CDA79316AA8E3545DD4673189902BEC
MSG         = 7C74AF27F5A2CA6BC4207E4AA82FA3E2
              0D3A59D4E97CE43D62F2E2E1EFDD5AF4
              20AEB5C836D85975EECAB84D33481D2D
              694078D5C5A388FF9072C402C0E97CE6
              C6892AF97ADBAC35E0E4E61FC497091A
              D5B577AF64842F7D26B538C31357B504
              4ED187AA1D24B38E9343F5E0BC683BF8
```

```
                68A92D0B71CC81415AADD2C4A3E82189
                2FE1D1F2105FFDB101E91B21
MAC         = 74637ECB978422D4426F8F876A70E721
```

```
KEY         = 8F4EC0BE7A3F5B6A2AAA92814F454F70
Kx          = 0EE5492230A06FA5A2F89D767923B58D
MSG         = 6CB1DB9648E809AC7B0988B160B20BED
                144A648DB75E854E50A2CA0F8D5F13FE
                70FF229CE427315651BD
MAC         = CFF39D67CB2B1987DDE2841E4C7F6225
```

```
KEY         = AEA00AD0EF9243833DA4861D6A0D2C8C
Kx          = 50368F14FF9E0252897F46B2D4C92142
MSG         =
MAC         = 954230A72692BAB4CE1A44473D081376
```

```
KEY         = F91F1CF58941608F6F08ED190D3BF9B0
Kx          = 125544328737911A0A9415C9CFA07712
MSG         = CB09216F785295157058E08B38579E91
                AB808E8E02D47A508A78E1705D4847C6
                F3E52E15FA8611EECB7AFEAF0C8ED5E4
                5A1E38C4F02335F68ED1E4FF7024B728
                101997522989972 46EA0C387D6CB43FC
                A3FD153E0F83D6CFB0378629A1127EA6
                C3D69EF3F683BAD18714565060AD20C3
                8DE75C720F79188D43C8A1F2026E825B
                211CC4FF2C50061F4343B7FB2C856E02
                16C29BB9B60B9749BD11AF2DE1C7CF19
                91FA2F43E820973DE13C2FCBC11D60BE
                599FDB3FD2C9A516857A411BA0D93E7B
                749E6A32552B19F52B5ED879DBCC88A0
                B0F1D342EC8F46C85418BE6EDF7C9C08
                FEB45623B22E682E85E61474F02C3AB8
                F2A16AAF05FC8FE5
MAC         = 5D5E7B4182EBD50B31FFE52DE4AB5C11
```

```
KEY         = 57A2DD3D6DAB16AFC1D07B277664ED82
Kx          = 7F2FCD9F8E4A8E3725F0071B9C8743B4
MSG         = D2D728DE057B3E
MAC         = DBDEC069CF2B46450CEFB34FFD80D840
```

```
KEY         = 11ED02022570CB10502BC1DACF64B21F
Kx          = B6BB0A6CC3CA379226EFDB9D6C457EDC
MSG         = E825603F896A85CAB45E6730D89DD4CE
                78010599
MAC         = 4A1577C366D53080D0DFD1CC47EE3CC7
```

```
KEY         = DD315EE3E236161FB777CAC2EC8A29C7
Kx          = 1AD7728D6A4A0520114B130B9D55BD81
MSG         = 469CCC
MAC         = E45A7903A8B9B0366309BB11A451E244
```

```
KEY         = 5AA9F6C6DE5138113DF5D6B6C77D5D52
Kx          = 2AE0EBD376BCD4A27B1CD406D2431CF9
MSG         = A4434D740C2CB665FE5396959189383F
```

```
MAC         = 8B43ADF767E46B692E8F24E837CB5EFC
```

```
KEY         = 4F41663FB985F7B47200246449B3DF33
Kx          = 80AEF0373782D05177726FFB0FA4F3C2
MSG         = 52D12581AC3FA13F2135F325130424AC
MAC         = D21C5F1F7881C84540373E4AF9C01714
```

```
KEY         = FDDA1F4B99010C07521C4B74633559D3
Kx          = FCB9B67395C53881D443449302C0D47D
MSG         = BE
MAC         = D3C4EE477F4FA5092B1FE726C18C3D01
```

```
KEY         = 0D46557550CB313F36AFBA87625D961A
Kx          = 3273289C6F7DBD9140A3AC11AB96F495
MSG         = 90
MAC         = F7C8553DED574829E6EE68112CB3817B
```

```
KEY         = F32DDBECDB1F527C06B46B3FCDD8F623
Kx          = D2957F516B0DF1971B6B2147C68213B2
MSG         = 9CB9DCD3FB3DB886ACAB218F7D522899
              64EF11ECBAA8051B2290BD23EC9F8448
              1CAA5773FF18E0E299F55A094AB05086
              CD894D51C3252BF4B3C0
MAC         = 9E1107B058A7C310F41AFEDB3C0E58CA
```

```
KEY         = B06A7F949A0D26D872D2FAB4994B0E2F
Kx          = 3A805DB26699EBE2A3CA749A9888E06F
MSG         = 7240375662513285F67F63C03E677562
MAC         = 4249F423B3137D3C5EF9A315C4BFD1D3
```

```
KEY         = 055A4CE2713D7D8B18EF014394D266A6
Kx          = 359AE1AA196387EC39F9E8E608FDC826
MSG         =
MAC         = 8D8FDCF864C745DF8ABAAFADA00F5074
```

```
KEY         = 2A473E38BBF4537C5397F45AE498CD4D
Kx          = 5D5F27EC92608C0712D3878A83F7B0E4
MSG         = C2AC3D7250EEF02318BC084F294B1AC7
              2291EE1DC02AF424941CAAC685FCA59D
              9008679B00C56A0562583BDAEC0BBA
MAC         = 66DC2BCE269B793B4ACA1A4D04DDD668
```

```
KEY         = 4DB286486F2B417498B819DD33442A9E
Kx          = D41D109EA30E10E137CAE834B59F8B14
MSG         = E37EC65C26E8BA67EF193889625C13FE
              B436724E93CFE3E7E836C138BA1EC381
              4C996A34C0EB4943860CA99EE154D1E7
              169F67E1F8708D149ADE74EF2782ADD0
              56B63CC8F2DF3EC8EC2EC78725450693
              65D9221BB7E188DC0C5599E177591C04
              5FD9472A1809F536609FF4CAA806EE55
              D8E08A4D5F911875
```

```
MAC         = 39D04705396D2ABD4CA96B693FC20B04
```

```
KEY         = 2E5FBC9C465D509212C3274CFEDC7B5C
Kx          = 77A89510033CEBFFD5EB02AC2DC518B3
MSG         = BE
MAC         = BE0A9F7E4F4C9C55A35D0F90DC0FF866
```

```
KEY         = 340567430897CFCEA4CEC0D2FBB84C58
Kx          = 2A22AC48EFA945339B22E335464B4B96
MSG         = E5DEA257FC642D6A74D60187702BB635
MAC         = B9A019E7BB4A84929365B6414D84B849
```

```
KEY         = 0254B8C2431E598C2BE0C20F8AFBB8C7
Kx          = E880EF06E1A19AF718B35E80D32E45AA
MSG         = EC
MAC         = CC6D34A67B2E3F08221F1F23C498F3B8
```

```
KEY         = 0C32A26430F8BE4A8B8D9523EEAE969F
Kx          = 0A0D8002F377B0C00F7AF0F5A9E71753
MSG         = 1BA21EDF781D39FC69DC8F6F15488520
              DFEE60CDE1553579670D0A31EC9288A0
              AFC1F1908385B7DA854D21B106B3D866
              107E94D8254849C66CA4776B130810D7
              53EEC05456F59C5936864893338473B3
              34A3206DFDB07B66772A23DF0D4CC67C
              3D4A5D17F2840F1BE13AA19E00B693E8
              30C4376FE8A2D9A2735ADC2CD2BD4CE9
              C0CB56E8265BC0AF94058CC20E
MAC         = 0C4222286E02A484217881644CD11A7E
```

```
KEY         = DD65C1973AAE481556949A70BBA498A8
Kx          = AD46B292A44636C9935DAC161263AB3C
MSG         = DE3560AAC2D50387DBE216179395F41B
MAC         = E19DA6375B7D44AC7EF2DC379E496775
```

```
KEY         = 94970E03D46936BB786BB72807B1BB67
Kx          = 200B7BB09B59E00D4561DA915298BDA5
MSG         = ED78D9458D
MAC         = E9779A2E7A2F713C3692E71D1704AA00
```

```
KEY         = 7BB18459270EA38C4EB115EAE374FEA4
Kx          = 10CD915058439C89AE22B6CB9712804B
MSG         = 2927AE423C96C4BAA61E34BE46EE8436
MAC         = B342A9697FC469EC29D554E24742936E
```

```
KEY         = 1E44A8857A620951EA738A31BBBB21BC
Kx          = C4921E131FCC7E2B35A78860AF480902
MSG         = 17EA78DED1A793E12B9C86796D131274
              5605C71D5D58C90B92FEEBFC7855389C
              FA61075930A6A8BA7670BED604B84DA7
              0F4713088A6D78BE20
```

```
MAC         = FF3D98D31F457AE0D957601ED44F3777
```

```
KEY         = 6D4BD3BC9668D663E97F0C0CB844AF5C
Kx          = E37C71B522A797C67EFC6F5B54683C10
MSG         = 06DAB144ED31412F118CE94838C25AD5
              FEE008E8721B
MAC         = 6BE23B4AFE1F608BCA215E94D7AADA51
```

```
KEY         = 38419B570263AC7EC78B252E66712277
Kx          = ADAB17D7BCCA53117BA64E2E553F88FE
MSG         = F323C37F8255860DC6E4B07FEBA16FA9
MAC         = C2D8DAC25EDC2FB9E9F2DCD010AFF945
```

```
KEY         = 952FDE8393C45D230A5BE9B38636D154
Kx          = 6F97C6586DED928DEFFEFCBB7C71C643
MSG         = D7800E257001A774AE7BCFB2CE1307B5
              B044
MAC         = 05F1CE30451A03A6E468B3A59033A554
```

```
KEY         = 2EC5A074266CD3868F125C40A85C51D2
Kx          = D5A7EBFC1FA31D74ADA27815426746F8
MSG         = C3B6AE5BE019
MAC         = 003EB550D462D3E9A2ED9BD4B798C87F
```

```
KEY         = 01B823CA9E8EFE175836625AA152E972
Kx          = A38CD6F22953DB258CB5ABBB508EF884
MSG         = 61
MAC         = 32A2D28599066AA0DDCD1DFB6C3373B0
```

```
KEY         = FC5558E552206A0FF2194552D1CE6B48
Kx          = 7035246DCE824EE244DE68B5BA8C0324
MSG         = 9B5B542E0A39512195ED0EA6A0BCCE71
MAC         = 2797A78D54BE757328F7A00C4B522B2C
```

```
KEY         = B93BDEAD484349154F801B064C5BBB29
Kx          = A53A9086733E606616E5AB6C956B07CC
MSG         = B647
MAC         = 0C808D5AE0364B41B122EDB487397BB9
```

```
KEY         = E718EE5C2C37AC31129DD60377CB97AF
Kx          = C1A134D29738702C49E2A03DF3C8E13E
MSG         = 1E4BD43A31
MAC         = 7D45F28E5FAA0C2FA7379A3BBA4B2A6E
```

```
KEY         = E477385CD36D02F3F6945AE61DDDA24F
Kx          = 78AC2C1CC2DE88761BDB54687FDE79B1
MSG         = 5D96B808E8C5D7BDC8CD1922FA5234F9
              B5C9690184D4035571F3613C3A15E25F
              E2ED87E17F53EAA82A352EC7
MAC         = B7F4DB09E5C5A9133D60AAFC283D270D
```

```
KEY         = 41C4238B6E55539E0B55C089936396F5
Kx          = 5E5CA473E94481320189974EC5108FDA
```

```
MSG       =
MAC       = AA7032ED436E7B52808E2E703F8781A1
```

```
KEY       = B2EABA3F0CCB537962DEC1D64EA63B13
Kx        = 17A233E56C5B8C1660D7849D41745971
MSG       = C243538D2DFD4D1CBCF54490B27BDD87
            8416C01ADCF0C0
MAC       = 0BC42ECAC57934BC09899693664C2FF5
```

```
KEY       = 4A7F71E3574FEA248ECC9EF0A667B2DF
Kx        = 5D3F47D30189B1EA1502BDA01D0B9D66
MSG       = 7D469C2A5E8C28BA15B308D183080DBB
            1AF6CDD2D1B6C3148B3620D236F2147F
            4BD7
MAC       = 82B9D1AF7643DE20A65117D1FBA48C7C
```

```
KEY       = CD38D5B8F8C3C26A7818951E225EA424
Kx        = 7E064526AF6D0804C37BB5D2B5D0DA35
MSG       = C682889F28
MAC       = 093C98AFB1CA352477A296D97611BC72
```

```
KEY       = 6C5683229E8985AC3BD5E661FD0A1066
Kx        = A1878860BE9382E82E2B55FF12466D17
MSG       = C1
MAC       = 9F65E3937D6C9140FF9B02857ADAFB5B
```

```
KEY       = 2D113F05F079BF06B54D19D0566BE656
Kx        = E54ABD326A766100B7F7F15407601DB8
MSG       = CF
MAC       = 25938AC2F0F78B21416D5BA1D3642B63
```

```
KEY       = 3E521285C1B089D7083214AA2871E299
Kx        = C506FC8DC3D9E0179913B9866A3622AD
MSG       = 99472DB3A480E63173D39E9F5D
MAC       = 132A1027AD89A5F26C200966D581554B
```

4 Abbreviations

Table 1. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher Block Chain, one mode of operation for block ciphers
CMAC	Cipher-based Message Authentication Code
CTR	Counter Mode
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
ECB	Electronic Code Book Mode
IV	Initialization Vector
LRICB	LRP Indexed Code Book mode
LRP	Leakage Resilient Primitive
LSBit	Least Significant Bit
MAC	Message Authentication Code
MSBit	Most Significant Bit
PRG	Pseudo-Random Generator

5 References

1. Morris J. Dworkin. SP 800-38a 2001 edition. recommendation for block cipher modes of operation: Methods and techniques. Technical report, Gaithersburg, MD, United States, 2001.
2. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, August 1986.
3. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapan & Hall/CRC, 2014.
4. **ISO/IEC 9797-1:1999**
   Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.

6 Legal information

6.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

6.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

MIFARE — is a trademark of NXP B.V.

DESFire — is a trademark of NXP B.V.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 13 March 2019
Document identifier: AN12304
Document number: 466011