INTERNATIONAL STANDARD

ISO/IEC 18033-4

First edition
2005-07-15

AMENDMENT 1
2009-12-15

Information technology — Security techniques — Encryption algorithms —

Part 4: Stream ciphers

AMENDMENT 1: Rabbit and Decim

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement —

Partie 4: Chiffrements en flot

AMENDEMENT 1: Rabbit et Decim

Reference number
ISO/IEC 18033-4:2005/Amd.1:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Amendment 1 to ISO/IEC 18033-4:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This Amendment introduces two additional keystream generators for use as stream ciphers: Rabbit and Decim^{v2}.

Rabbit is specified in 7.3, and test vectors are given in A.4.

Decim^{v2} is specified in 7.4, and test vectors are given in A.5.

For all keystream generators, security statements are given in Annex B, and object identifiers are given in Annex C.

Information technology — Security techniques — Encryption algorithms —

Part 4: Stream ciphers

AMENDMENT 1: Rabbit and Decim

Page 4, Clause 4, immediately before b_i

Add the following:

AND Bitwise logical AND operation.

Page 4, Clause 4, line 21

Replace with the following:

OR Bitwise logical OR operation.

Page 5, immediately before 4.1

Add the following note:

NOTE Additional variables and notation specific to a given keystream generator are introduced with the algorithm.

Page 23, after 7.2.7

Add the following new subclauses:

7.3 Rabbit keystream generator

Rabbit is a keystream generator which uses a 128-bit secret key K, a 64-bit initialization vector IV, and a 513-bit internal state variable S_i ($i \geq 0$). It outputs a 128-bit keystream block Z_i at every iteration of the function $Strm$.

The 513 bits of the internal state S_i are divided between eight 32-bit state variables $X_0^{(i)}$, ...,$X_7^{(i)}$, eight 32-bit counter variables $C_0^{(i)}$, ...,$C_7^{(i)}$, and one counter carry bit $b^{(i)}$.

The description uses the notation defined in Section 4 of the standard. In addition, a special notation for bit arrays is used to enhance readability: when labeling the bits of a variable A, the least significant bit is denoted by $A^{[0]}$. The notation $A^{[h..g]}$ represents bits h through g of variable A, where bit position h is more significant than bit position g.

NOTE 1 For Rabbit, the maximum recommended amount of keystream produced from a given key K is 2^{64} keystream blocks. This provides a large security margin against cryptanalysis, while at the same time implying no practical limitations on the applicability of the algorithm.

NOTE 2 We refer to [1] for the original proposal of the cipher and to [2] for an overview of its cryptographic security.

7.3.1 Additional variables and notation

In the specification of the Rabbit keystream generator, the following specific notation is used:

A	Constant for Rabbit
b	Carry bit for Rabbit
C	Counter variable for Rabbit
g	Subfunction used for Rabbit
X	Inner state variable for Rabbit

In addition, a number of other symbols are used for auxiliary local variables in algorithm descriptions. These symbols occur only within a given function specification and do not have a global meaning. They are thus described in the function declaration.

7.3.2 Initialization function *Init*

In the following, the initialization function *Init* of Rabbit is specified.

INPUT: 128-bit key K, 64-bit initialization vector IV.

OUTPUT: Initial value of the state variable $S_0 = (b^{(0)}, X_0^{(0)}, ..., X_7^{(0)}, C_0^{(0)}, ..., C_7^{(0)})$.

Local variables: counters i, j

1. Let $K_0 = K^{[15..0]}$, $K_1 = K^{[31..16]}$, ..., and $K_7 = K^{[127..112]}$.
2. Set S_{-9} as follows:
   - 2.1. Set $b^{(-9)} = 0$.
   - 2.2. For $j = 0, 1, ..., 7$:
     - 2.2.1. If j is even:
       - 2.2.1.1. Set $X_j^{(-9)} = K_{(j+1 \bmod 8)} \| K_j$.
       - 2.2.1.2. Set $C_j^{(-9)} = K_{(j+4 \bmod 8)} \| K_{(j+5 \bmod 8)}$.
     - 2.2.2. Else:
       - 2.2.2.1. Set $X_j^{(-9)} = K_{(j+5 \bmod 8)} \| K_{(j+4 \bmod 8)}$.
       - 2.2.2.2. Set $C_j^{(-9)} = K_j \| K_{(j+1 \bmod 8)}$.
3. Iterate the next-state function *Next* four times:
   - 3.1. For $i = -8, -7, -6, -5$:
     - 3.1.1. $S_i = Next(S_{i-1})$
4. Set S_{-4} as follows:
   - 4.1. Modify the counters as follows:

$$C_0^{(-4)} = C_0^{(-5)} \oplus X_4^{(-5)} \oplus IV^{[31..0]} \qquad C_1^{(-4)} = C_1^{(-5)} \oplus X_5^{(-5)} \oplus (IV^{[63..48]} \| IV^{[31..16]})$$
$$C_2^{(-4)} = C_2^{(-5)} \oplus X_6^{(-5)} \oplus IV^{[63..32]} \qquad C_3^{(-4)} = C_3^{(-5)} \oplus X_7^{(-5)} \oplus (IV^{[47..32]} \| IV^{[15..0]})$$
$$C_4^{(-4)} = C_4^{(-5)} \oplus X_0^{(-5)} \oplus IV^{[31..0]} \qquad C_5^{(-4)} = C_5^{(-5)} \oplus X_1^{(-5)} \oplus (IV^{[63..48]} \| IV^{[31..16]})$$
$$C_6^{(-4)} = C_6^{(-5)} \oplus X_2^{(-5)} \oplus IV^{[63..32]} \qquad C_7^{(-4)} = C_7^{(-5)} \oplus X_3^{(-5)} \oplus (IV^{[47..32]} \| IV^{[15..0]})$$

4.2. Set $X_0^{(-4)} = X_0^{(-5)}$, ..., $X_7^{(-4)} = X_7^{(-5)}$, $b^{(-4)} = b^{(-5)}$.

5. Iterate the next-state function *Next* four times:

   5.1. For i = -3, -2, -1, 0:

      5.1.1. $S_i = Next\ (S_{i-1})$

6. Output $S_0 = (b^{(0)}, X_0^{(0)}, ..., X_7^{(0)}, C_0^{(0)}, ..., C_7^{(0)})$.

NOTE The IV is mixed into the internal state in steps 4 and 5 of the algorithm. If the application requires frequent re-initialization under the same key, it makes sense to store the internal state after step 3 as master state and to perform only steps 4 through 6 for re-initialization.

7.3.3 Next-state function *Next*

The next-state function *Next* of Rabbit is specified as follows:

INPUT: State variable $S_i = (b^{(i)}, X_0^{(i)}, ..., X_7^{(i)}, C_0^{(i)}, ..., C_7^{(i)})$.

OUTPUT: State variable $S_{i+1} = (b^{(i+1)}, X_0^{(i+1)}, ..., X_7^{(i+1)}, C_0^{(i+1)}, ..., C_7^{(i+1)})$.

Local variables: counter j, 33-bit positive integer *temp*

1. Set constants A_0, ..., A_7 as follows:

   A_0 = 0x4D34D34D A_1 = 0xD34D34D3
   A_2 = 0x34D34D34 A_3 = 0x4D34D34D
   A_4 = 0xD34D34D3 A_5 = 0x34D34D34
   A_6 = 0x4D34D34D A_7 = 0xD34D34D3

2. Let $b_0^{(i+1)} = b^{(i)}$

3. For j = 0, 1, ..., 7:

   3.1. Let $temp = C_j^{(i)} + A_j + b_j^{(i+1)}$; this results in a 33-bit value.

   3.2. Let $b_{j+1}^{(i+1)} = temp^{[32]}$.

   3.3. Let $C_j^{(i+1)} = temp^{[31..0]}$.

4. Let $b^{(i+1)} = b_8^{(i+1)}$

5. For j = 0, 1, ..., 7:

   5.1. Let $G_j = g(X_j^{(i)}, C_j^{(i+1)})$. The detailed description of the function g is given in 7.3.5.

6. Modify internal state as follows:

$$
\begin{aligned}
X_0^{(i+1)} &= G_0 +_{32} (G_7 <<<_{32} 16) +_{32} (G_6 <<<_{32} 16)\\
X_1^{(i+1)} &= G_1 +_{32} (G_0 <<<_{32} 8) +_{32} G_7\\
X_2^{(i+1)} &= G_2 +_{32} (G_1 <<<_{32} 16) +_{32} (G_0 <<<_{32} 16)\\
X_3^{(i+1)} &= G_3 +_{32} (G_2 <<<_{32} 8) +_{32} G_1\\
X_4^{(i+1)} &= G_4 +_{32} (G_3 <<<_{32} 16) +_{32} (G_2 <<<_{32} 16)\\
X_5^{(i+1)} &= G_5 +_{32} (G_4 <<<_{32} 8) +_{32} G_3\\
X_6^{(i+1)} &= G_6 +_{32} (G_5 <<<_{32} 16) +_{32} (G_4 <<<_{32} 16)\\
X_7^{(i+1)} &= G_7 +_{32} (G_6 <<<_{32} 8) +_{32} G_5
\end{aligned}
$$

7. Output $S_{i+1} = (b^{(i+1)}, X_0^{(i+1)}, ..., X_7^{(i+1)}, C_0^{(i+1)}, ..., C_7^{(i+1)})$.

7.3.4 Keystream function *Strm*

The keystream function *Strm* of Rabbit is specified as follows:

INPUT: State variable $S_i = (b^{(i)}, X_0^{(i)}, ..., X_7^{(i)}, C_0^{(i)}, ..., C_7^{(i)})$.

OUTPUT: Keystream block Z_i.

1. Set Z_i as follows:

$$
\begin{aligned}
Z_i^{[15..0]} &= X_0^{(i)}[15..0] \oplus X_5^{(i)}[31..16] \\
Z_i^{[31..16]} &= X_0^{(i)}[31..16] \oplus X_3^{(i)}[15..0] \\
Z_i^{[47..32]} &= X_2^{(i)}[15..0] \oplus X_7^{(i)}[31..16] \\
Z_i^{[63..48]} &= X_2^{(i)}[31..16] \oplus X_5^{(i)}[15..0] \\
Z_i^{[79..64]} &= X_4^{(i)}[15..0] \oplus X_1^{(i)}[31..16] \\
Z_i^{[95..80]} &= X_4^{(i)}[31..16] \oplus X_7^{(i)}[15..0] \\
Z_i^{[111..96]} &= X_6^{(i)}[15..0] \oplus X_3^{(i)}[31..16] \\
Z_i^{[127..112]} &= X_6^{(i)}[31..16] \oplus X_1^{(i)}[15..0]
\end{aligned}
$$

2. Output Z_i.

7.3.5 Function *g*

The function *g* is specified as follows:

INPUT: Two 32-bit parameters *u* and *v*.

OUTPUT: 32-bit result $g(u,v)$.

Local variables: 64-bit positive integer *temp*

1. Let $temp = (u +_{32} v)^2$; this results in a 64-bit value.

2. Let $g(u,v) = temp^{[31..0]} \oplus temp^{[63..32]}$.

3. Output $g(u,v)$.

7.4 Decim^{v2} keystream generator

Decim^{v2} is a keystream generator which uses an 80-bit secret key *K* and a 64-bit initialization vector *IV*. Decim^{v2} is composed of a 192-bit maximum length linear feedback shift register *A*, filtered by a 14-variable Boolean function *F*. In keystream generation mode, the output of *F* is used to feed a compression block which is a function called *ABSG*, whose output finally passes through a 32-bit long buffer *B* to regulate the keystream output rate.

NOTE 1 See Reference [3] for the theoretical background on the design rationale of Decim^{v2}.

The state variable S_i of Decim^{v2} consists of the 192-bit value $a^{(i)} = (a_0^{(i)}, a_1^{(i)}, ..., a_{191}^{(i)})$ of register *A*, a 3-bit variable $T^{(i)}$ which corresponds to the state of the compression function *ABSG*, the 32 bits $b^{(i)} = (b_0^{(i)}, b_1^{(i)}, ..., b_{31}^{(i)})$ in buffer *B*, and the number $l^{(i)}$ of bits in buffer *B* that are ready to be output.

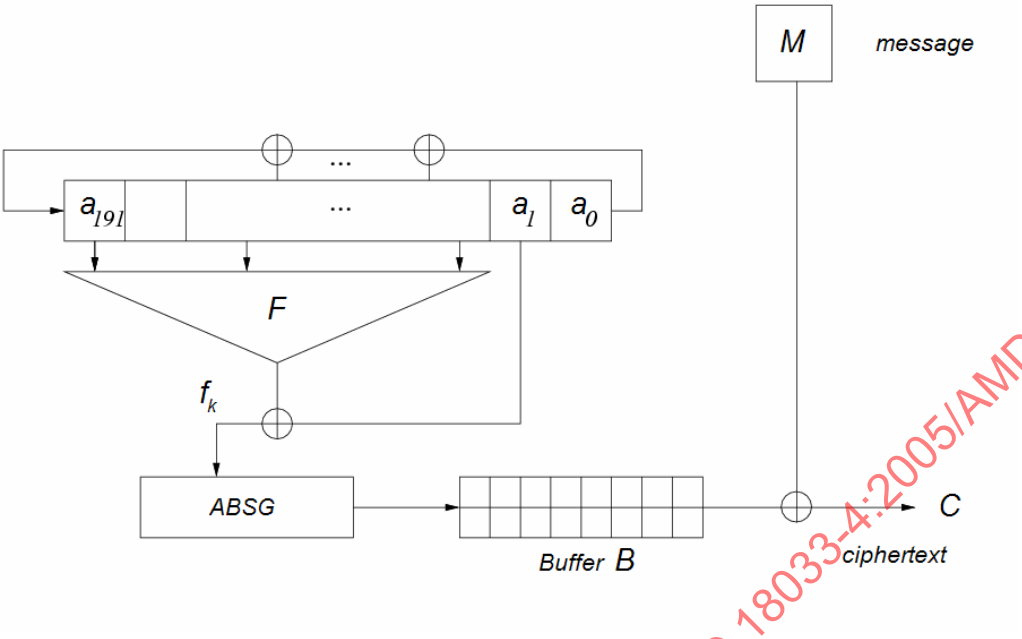

Figure 10 — Schematic drawing of Decim^{v2}.

The *Init* function, defined in detail in 7.4.2, takes as input the 80-bit key K and the 64-bit initialization vector IV, and produces the initial value of the state variable $S_0 = (a^{(0)}, T^{(0)}, b^{(0)}, I^{(0)})$.

The *Next* function, defined in detail in 7.4.4, takes as an input the value of the state variable $S_i = (a^{(i)}, T^{(i)}, b^{(i)}, I^{(i)})$ and produces as output the next value of the state variable $S_{i+1} = (a^{(i+1)}, T^{(i+1)}, b^{(i+1)}, I^{(i+1)})$. The *Next* function can operate in any of three different modes, depending on whether the iteration performed is part of the initialization of the register, the initialization of the buffer, or the subsequent keystream generation.

The *Strm* function, defined in detail in 7.4.5, takes as an input the value of the state variable $S_i = (a^{(i)}, T^{(i)}, b^{(i)}, I^{(i)})$, and produces as output a keystream bit Z_i.

NOTE 2 The standard output rate of Decim^{v2} is 1/4. Therefore, in order to synchronize the state variable and the keystream output, the *Next* function performs four standard iterations of Decim^{v2} as specified in [3].

NOTE 3 The compression function of Decim^{v2} has a variable output rate, equal to 1/3 on average. Therefore, a buffer mechanism is used to ensure a constant output rate. The differences between the buffer output rate and the compression function output rate, as well as the buffer length, have been chosen to ensure that the buffer always functions as expected with overwhelming probability, as described in Section 7.4.2.

7.4.1 Additional variables and notation

In the specification of the Decim^{v2} keystream generator, the following specific notation is used:

a	Inner state variable for Decim^{v2}
ABSG	Compression function used for Decim^{v2}
b, b'	Inner state variables for Decim^{v2}
B	Buffering function used for Decim^{v2}
F	Linear feedback function used for Decim^{v2}

I, I'	Inner state variables for Decim^{v2}
L	Filtering function used for Decim^{v2}
T, T'	Inner state variables for Decim^{v2}
Y	Boolean function used for Decim^{v2}

In addition, a number of other symbols are used for auxiliary local variables in algorithm descriptions. These symbols occur only within a given function specification and do not have a global meaning. They are thus described in the function declaration.

7.4.2 Initialization function *Init*

The Initialization function *Init* is defined as follows.

INPUT: 80-bit key K, 64-bit initialization vector IV.

OUTPUT: Initial value of the state variable $S_0 = (a^{(0)}, T^{(0)}, b^{(0)}, I^{(0)})$.

Local variables: counters i, j

a) Initialize the register with the key K and the initialization vector IV.

   1) Set $a_j^{(-256)} = K_j$ for j =0,1,…,79.

   2) Set $a_j^{(-256)} = K_{j-80} \oplus IV_{j-80}$ for j =80,81,…,143.

   3) Set $a_j^{(-256)} = K_{j-80} \oplus IV_{j-144} \oplus IV_{j-128} \oplus IV_{j-112} \oplus IV_{j-96}$ for j =144,145,…,159.

   4) Set $a_j^{(-256)} = IV_{j-160} \oplus IV_{j-128} \oplus 1$ for j =160,161,…,191.

b) Initialize the buffer and the compression function:

   1) Set $T^{(-256)} = 000$.

   2) Set $b_j^{(-256)} = 0$ for j =0,1,…,31.

   3) Set $I^{(-256)} = 0$.

c) Set $S_{-64} = InitNext^{192}$ (S_{-256}, LFSR).

d) Set i = -64.

e) While $I^{(i)} < 32$ and $i<0$:

   1) Set $S_{i+1} = InitNext(S_i, \text{BUFF})$.

   2) Set $i=i+1$.

f) Set $S_0 = S_i$.

g) Output S_0.

NOTE Steps d), e) and f) of the Decim^{v2} initialization involve filling the buffer before starting the keystream output. As the output rate of the compression function varies, the number of steps required to fill the buffer may vary. In step e), the *InitNext*(BUFF) function is iterated 64 times at most, which guarantees that the buffer is full with probability more than $1-2^{-97}$. On average, the buffer is full after 24 iterations. If a fixed, constant number of steps in the Init function is needed for implementation, the test $I^{(i)} < 32$ in step e) can be removed.

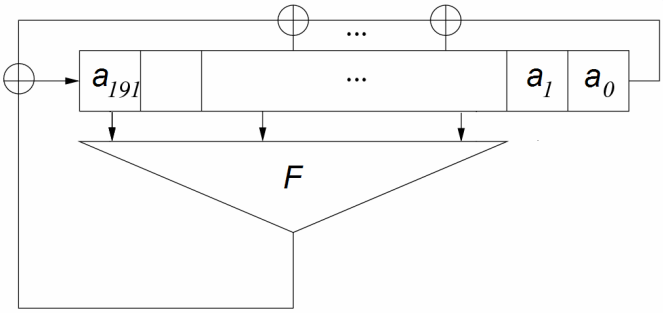

Figure 11 — Initialization mechanism.

7.4.3 Initialization Next-state function *InitNext*

Decim^{v2} has two modes for the *InitNext* function: one mode is used during the initialization of the register A and the second during the initial filling of the buffer.

INPUT: State variable $S_i = (a^{(i)}, T^{(i)}, b^{(i)}, l^{(i)})$, *mode* $\in$ {LFSR, BUFF}.

OUTPUT: Next value of the state variable $S_{i+1} = (a^{(i+1)}, T^{(i+1)}, b^{(i+1)}, l^{(i+1)})$.

Local variables: counters j, k, buffers f_k, r, c,
state buffers $\alpha^{(0)}, ..., \alpha^{(4)}, \tau^{(0)}, ..., \tau^{(4)}, \beta^{(0)}, ..., \beta^{(4)}, \iota^{(0)}, ..., \iota^{(4)}$.

LFSR mode (execute if mode = LFSR)**:**

a) Update the state of the register A with the following steps:

1) Set $\alpha^{(0)} = a^{(i)}$.

2) For $k = 0, 1, 2, 3$:

i) Set $f_k = F(\alpha^{(k)})$ and $r = L(\alpha^{(k)}) \oplus f_k$.

ii) For $j = 0,1,\ldots,190$ set $\alpha_j^{(k+1)} = \alpha_{j+1}^{(k)}$.

iii) Set $\alpha_{191}^{(k+1)} = r$.

3) Set $a^{(i+1)} = \alpha^{(4)}$.

BUFF mode (execute if mode = BUFF)**:**

a) Update the state of the register A with the following steps:

1) Set $\alpha^{(0)} = a^{(i)}$.

2) For $k = 0, 1, 2, 3$:

i) Set $f_k = \alpha_1^{(k)} \oplus F(\alpha^{(k)})$ and $r = L(\alpha^{(k)})$.

ii) For $j = 0,1,\ldots,190$ set $\alpha_j^{(k+1)} = \alpha_{j+1}^{(k)}$.

iii) Set $\alpha_{191}^{(k+1)} = r$.

3) Set $a^{(i+1)} = \alpha^{(4)}$.

b) Set $\tau^{(0)} = T^{(i)}$, $\beta^{(0)} = b^{(i)}$, $\iota^{(0)} = l^{(i)}$.

c) For k = 0, 1, 2, 3:

1) Update the state of the compression block with the following steps:

i) Set $c = f_k \oplus \tau_0^{(k)}$.

ii) Set $\tau^{(k+1)} = ABSG(\tau^{(k)}, f_k)$.

iii) If $\tau_0^{(k+1)} = 0$, set *output* = TRUE , otherwise set *output* = FALSE.

2) Update the state of the buffer by $(\beta^{(k+1)}, \iota^{(k+1)}) = B(\beta^{(k)}, \iota^{(k)}, output, c)$.

d) Set $T^{(i+1)} = \tau^{(4)}$.

e) Set $b^{(i+1)} = \beta^{(4)}$ and $l^{(i+1)} = \iota^{(4)}$.

7.4.4 Next-state function *Next*

INPUT: State variable $S_i = (a^{(i)}, T^{(i)}, b^{(i)}, l^{(i)})$.

OUTPUT: Next value of the state variable $S_{i+1} = (a^{(i+1)}, T^{(i+1)}, b^{(i+1)}, l^{(i+1)})$.

Local variables: counters j, k, buffers f_k, r, c,
state buffers $\alpha^{(0)}, ..., \alpha^{(4)}, \tau^{(0)}, ..., \tau^{(4)}, \beta^{(0)}, ..., \beta^{(4)}, \iota^{(0)}, ..., \iota^{(4)}$.

a) Update the state of the register A with the following steps:

1) Set $\alpha^{(0)} = a^{(i)}$.

2) For k = 0, 1, 2, 3:

i) Set $f_k = \alpha_1^{(k)} \oplus F(\alpha^{(k)})$ and $r = L(\alpha^{(k)})$.

ii) For j = 0, 1, …,190 set $\alpha_j^{(k+1)} = \alpha_{j+1}^{(k)}$.

iii) Set $\alpha_{191}^{(k+1)} = r$.

3) Set $a^{(i+1)} = \alpha^{(4)}$.

b) Set $\tau^{(0)} = T^{(i)}$, $\beta^{(0)} = b^{(i)}$, $\iota^{(0)} = l^{(i)}$-1.

c) For j = 0, 1, …, $\iota^{(0)}$-1 , set $\beta_j^{(0)} = b_{j+1}^{(i)}$

d) For k = 0, 1, 2, 3:

1) If $\iota^{(0)} = 0$, set $\tau^{(k+1)} = \tau^{(k)}$, *output* = TRUE and $c = f_k$, otherwise update the state of the compression block with the following steps:

i) Set $c = f_k \oplus \tau_0^{(k)}$.

ii) Set $\tau^{(k+1)} = ABSG(\tau^{(k)}, f_k)$.

iii) If $\tau_0^{(k+1)} = 0$, set *output* = TRUE , otherwise set *output* = FALSE.

2) Update the state of the buffer by $(\beta^{(k+1)}, \iota^{(k+1)}) = B(\beta^{(k)}, \iota^{(k)}, output, c)$.

e) Set $T^{(i+1)} = \tau^{(4)}$, $b^{(i+1)} = \beta^{(4)}$ and $l^{(i+1)} = \iota^{(4)}$.

NOTE 1 The condition $t^{(0)} = 0$ in step 1) should never be satisfied; if it is, this means that the buffer has become empty during the keystream generation. This happens with probability less than 2^{-80} at every state update, see [3] for details. Also, this probability is higher if the buffer is not full after the *Init* function, but, as mentioned in 7.4.2 (NOTE), this also happens with negligible probability.

NOTE 2 The *InitNext* function and the *Next* function share many computations steps. Indeed, the LFSR mode of the *InitNext* function mainly consists of the LFSR update of the BUFF mode and of the *Next* function, the only difference being that the Boolean function output is added to the feedback bit. The BUFF mode of the *InitNext* function and the *Next* function differ only in that the buffer B is shifted only in the latter.

7.4.5 Keystream function *Strm*

INPUT: State variable $S_i = (a^{(i)}, T^{(i)}, b^{(i)}, I^{(i)})$.

OUTPUT: Keystream bit Z_i.

a) Set $Z_i = b_0^{(i)}$.

b) Output Z_i.

7.4.6 Linear feedback function *L*

INPUT: 192-bit tuple $w = (w_0, w_1, \ldots, w_{191})$.

OUTPUT: Bit $q=L(w)$.

Set $q=w_0 \oplus w_3 \oplus w_4 \oplus w_{23} \oplus w_{36} \oplus w_{37} \oplus w_{60} \oplus w_{61} \oplus w_{98} \oplus w_{115} \oplus w_{146} \oplus w_{175} \oplus w_{176} \oplus w_{187}$.

7.4.7 Filtering function *F*

INPUT: 192-bit tuple $w = (w_0, w_1, \ldots, w_{191})$.

OUTPUT: Bit $q=F(w)$.

Set $q = Y((w_{13}, w_{28}, w_{45}, w_{54}, w_{65}, w_{104}, w_{111}, w_{144}, w_{162}, w_{172}, w_{178}, w_{186}, w_{191}))$.

7.4.8 Boolean function *Y*

INPUT: 13-bit tuple $w = (w_0, w_1, \ldots, w_{12})$.

OUTPUT: Bit $q=Y(w)$.

Set $q = (\oplus_{0 \le j \le 12} w_j) \oplus (\oplus_{0 \le j < k \le 12} w_j w_k)$.

NOTE Equivalently, q is given by $q = 0$ if $X = 0$ or $X = 3$, and $q = 1$ otherwise, with $X = w_0 + w_1 + \ldots + w_{12} \bmod 4$.

7.4.9 Compression function *ABSG*

INPUT: 3-bit state T, input bit c.

OUTPUT: 3-bit state $T'=ABSG(T,c)$.

a) If $T_0 = 1$, set $T'_1=T_1$, otherwise set $T'_1= c$.

b) Set $T'_2 = T_0$ AND $(T_1 \oplus c)$.

c) Set $T'_0 = (T_0 \oplus 1)$ OR T'_2.

7.4.10 Buffering function *B*

INPUT: 32-bit tuple $b = (b_0, b_1, \ldots, b_{31})$, index I , Boolean *output*, input bit c.

OUTPUT: 32-bit tuple $b' = (b'_0, b'_1, \ldots, b'_{31})$, index I'.

a) Set $I' = I$, $b' = b$.

b) If *output* = TRUE and $I' < 32$, do the following:

1) Set $b'_{I'} = c$.

2) Set $I' = I' + 1$.

c) Output $B(b, I, output, c) = (b', I')$.

Page 38, after A.3.2.2

Insert the following new subclauses:

A.4 Examples for Rabbit

All test vectors for Rabbit are given in little-endian notation, i.e. for multi-byte numbers, the most significant bytes are stored at the highest memory addresses.

A.4.1 Key, initialization vector and keystream triplets

```
K = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IV= 00 00 00 00 00 00 00 00
Z = ED B7 05 67 37 5D CD 7C D8 95 54 F8 5E 27 A7 C6 8D 4A DC 70 32 29 8F 7B D4 EF F5 04 AC A6 29 5F
    66 8F BF 47 8A DB 2B E5 1E 6C DE 29 2B 82 DE 2A B4 8D 2A C6 56 59 79 22 0E C9 09 A7 E7 57 60 98

K = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IV= 00 01 02 03 04 05 06 07
Z = 98 71 C7 BA 4E A3 08 07 CD AA 49 64 66 39 2D 2F 4A FF 43 55 EF 90 69 56 10 9B 96 65 97 8D AC ED
    9B 7C 6F 7F C8 2C 67 D2 73 22 CB DE 9D B0 16 45 8C 38 2C 9C 7D 30 44 E6 52 0B B9 2A 13 53 C0 FF

K = 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
IV= 00 00 00 00 00 00 00 00
Z = A8 F7 E6 9B 69 40 A7 8D 13 6A 5C 15 4A 15 79 52 A6 E4 23 58 59 E3 02 20 EA 68 64 36 BB 38 EF 53
    9C 29 40 55 6B 09 EC D7 FE A2 B0 AC 83 07 F1 69 62 65 A3 D6 44 28 1C 39 C9 CD 5E 1E 2F 9B E4 D0

K = 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
IV= 00 01 02 03 04 05 06 07
Z = F2 89 19 DD A1 28 F8 F9 0A 30 34 6E 97 94 D2 B7 4C 69 A2 D9 91 37 27 BC 5A 30 18 E6 33 2A F7 F3
    BE 3A C3 EF B3 68 F4 3A 4C B8 58 67 B8 1C 91 F9 24 29 0C 81 6B 8B 57 88 98 C5 7F B4 C0 BA 05 BD
```

A.4.2 Sample internal states

```
K = 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
IV= 00 01 02 03 04 05 06 07
Z = F2 89 19 DD A1 28 F8 F9 0A 30 34 6E 97 94 D2 B7 4C 69 A2 D9 91 37 27 BC 5A 30 18 E6 33 2A F7 F3
    BE 3A C3 EF B3 68 F4 3A 4C B8 58 67 B8 1C 91 F9 24 29 0C 81 6B 8B 57 88 98 C5 7F B4 C0 BA 05 BD
```

```
After key expansion (Internal state S(-9))
x0:03020100 x1:0D0C0B0A x2:07060504 x3:01000F0E x4:0B0A0908 x5:05040302 x6:0F0E0D0C x7:09080706
c0:09080B0A c1:03020504 c2:0D0C0F0E c3:07060908 c4:01000302 c5:0B0A0D0C c6:05040706 c7:0F0E0100
carry:0

After key setup iteration 1 (Internal state S(-8))
x0:05783933 x1:162113C0 x2:B38F168E x3:F08A919E x4:7F2CDA94 x5:ACBEB878 x6:0D5257A9 x7:4FF46B46
c0:563CDE57 c1:D64F39D7 c2:41DF5C42 c3:543ADC55 c4:D44D37D5 c5:3FDD5A40 c6:5238DA53 c7:E25B35D3
carry:0

After key setup iteration 2 (Internal state S(-7))
x0:798C2CEC x1:CC05FFD4 x2:50D68324 x3:2C306745 x4:AD519559 x5:81595E7A x6:29A589E2 x7:15212B97
c0:A371B1A4 c1:A99C6EAA c2:76B2A977 c3:A16FAFA2 c4:A79A6CA8 c5:74B0A775 c6:9F6DADA0 c7:B5A86AA6
carry:1

After key setup iteration 3 (Internal state S(-6))
x0:CD328957 x1:66D5AB1F x2:0D115824 x3:FCCEB784 x4:12E900D7 x5:36A46997 x6:9F40C5BC x7:AB1C8A08
c0:F0A684F2 c1:7CE9A37D c2:AB85F6AC c3:EEA482EF c4:7AE7A17B c5:A983F4AA c6:ECA280ED c7:88F59F79
carry:1

After key setup iteration 4 (Internal state S(-5))
x0:A31515F8 x1:5DFD3AC6 x2:33CD6AD2 x3:4BD778E5 x4:89708269 x5:D93095C1 x6:5E495F60 x7:C197863A
c0:3DDB5840 c1:5036D851 c2:E05943E1 c3:3BD9563C c4:4E34D64F c5:DE5741DF c6:39D7543A c7:5C42D44D
carry:1

After counter modification / IV setup (Internal state S(-4))
x0:A31515F8 x1:5DFD3AC6 x2:33CD6AD2 x3:4BD778E5 x4:89708269 x5:D93095C1 x6:5E495F60 x7:C197863A
c0:B7A9DB29 c1:8E004E92 c2:B9161985 c3:FF4AD106 c4:EE23C2B7 c5:84AC781B c6:0D1C3BEC c7:1291ADA8
carry:1

After IV setup iteration 1 (Internal state S(-3))
x0:054A3F2F x1:BE444CDE x2:573425A4 x3:9347FAD1 x4:29036A2F x5:DD3C6B50 x6:12CC3803 x7:6F7847C0
c0:04DEAE77 c1:614D8366 c2:EDE966BA c3:4C7FA453 c4:C170F78B c5:B97FC550 c6:5A510F39 c7:E5DEE27B
carry:0

After IV setup iteration 2 (Internal state S(-2))
x0:0FDB9A3A x1:334807E8 x2:E68BCC98 x3:0FDA371C x4:9C3E3036 x5:7774E657 x6:C6FCBB4C x7:A8D1AC4F
c0:521381C4 c1:349AB839 c2:22DCB3EF c3:99B477A1 c4:94BE2C5E c5:EE531285 c6:A785E286 c7:B92C174E
carry:1

After IV setup iteration 3 (Internal state S(-1))
x0:1A2EF77E x1:FDEEE287 x2:A918F5A1 x3:D6414F76 x4:4848D473 x5:BCE9BD30 x6:3E524094 x7:16242C51
c0:9F485512 c1:07E7ED0C c2:57900124 c3:E6E94AEE c4:680B6131 c5:23265FBA c6:F4BAB5D4 c7:8C794C21
carry:1

After IV setup iteration 4 (Internal state S(0))
x0:98A651C2 x1:FF5F0007 x2:5C48C79E x3:661B3E75 x4:49247B9A x5:3C7AA744 x6:4AEF3F40 x7:D117584E
c0:EC7D2860 c1:DB3521DF c2:8C634E58 c3:341E1E3B c4:3B589605 c5:57F9ACEF c6:41EF8921 c7:5FC680F5
carry:1

After keystream iteration 1 (Internal state S(1))
x0:2A158BE4 x1:D93EC5A4 x2:298B7C1B x3:01F4F70C x4:E241E934 x5:0216D073 x6:72769563 x7:54BA8C75
c0:39B1FBAE c1:AE8256B3 c2:C1369B8D c3:8152F188 c4:0EA5CAD8 c5:8CCCFA24 c6:8F245C6E c7:3313B5C8
carry:1
output F2 89 19 DD A1 28 F8 F9 0A 30 34 6E 97 94 D2 B7

After keystream iteration 2 (Internal state S(2))
x0:46EC0492 x1:A4B5D46E x2:7B374C9E x3:93249F4E x4:E93894EF x5:6DDEC710 x6:2799B917 x7:7B0F0F20
c0:86E6CEFC c1:81CF8B86 c2:F609E8C2 c3:CE87C4D5 c4:E1F2FFAB c5:C1A04758 c6:DC592FBB c7:0660EA9B
carry:1
```

```
output 4C 69 A2 D9 91 37 27 BC 5A 30 18 E6 33 2A F7 F3

After keystream iteration 3 (Internal state S(3))
x0:98C27422 x1:0D5B5EC2 x2:FEEC9F8D x3:423F7701 x4:E22AB517 x5:4E9CC418 x6:A7535E87 x7:F73E8572
c0:D41BA24A c1:551CC059 c2:2ADD35F7 c3:1BBC9823 c4:B540347F c5:F673948D c6:298E0308 c7:D9AE1F6F
carry:0
output BE 3A C3 EF B3 68 F4 3A 4C B8 58 67 B8 1C 91 F9

After keystream iteration 4 (Internal state S(4))
x0:3B844C36 x1:AF5CD78B x2:2619A0AC x3:774FBA88 x4:D16C6AC4 x5:6512AE4E x6:6A8ECD8F x7:2BC76513
c0:21507597 c1:2869F52D c2:5FB0832C c3:68F16B70 c4:888D6952 c5:2B46E1C2 c6:76C2D656 c7:ACFB5442
carry:1
output 24 29 0C 81 6B 8B 57 88 98 C5 7F B4 C0 BA 05 BD
```

A.5 Examples for Decim^{v2}

The byte-values and binary decomposition of bytes follow the big-endian notation, i.e. for multi-byte numbers, the most significant bytes are stored at the lowest memory addresses. In particular, this holds for the key, IV, keystream, register and buffer byte- and binary values given below.

Thus, we write

$K = K_{79} \ldots K_0$
$IV = IV_{63} \ldots IV_0$
$Z = Z_n \ldots Z_0$
$a = a_{191} \ldots a_0$
$b = b_{31} \ldots b_0$
$T = T_2T_1T_0$

and, for instance, given the key

K = de aa 00 40 00 30 00 0f 08 80,

we have

$K_{79}\ldots K_{72}]$=de, $[K_{71}\ldots K_{64}]$=aa … $[K_7\ldots K_0]$=80,

with bit-decomposition as follows:

$K_{79} \ldots K_0$ = 11011110 10101010 00000000 01000000 00000000
00110000 00000000 00001111 00001000 10000000

A.5.1 Key, initialization vector and keystream triplets

```
K = 00 00 00 00 00 00 00 00 00 80
IV= 00 00 00 00 00 00 00 00
Z = 76 e3 89 be 1b fb ad d5 3c ce a0 fe 43 b8 c8 fb d3 92 b8 0b 52 94 60 f8

K = 00 00 00 00 00 00 00 00 00 00
IV= 00 00 00 00 00 00 00 80
Z = 4c ec bd b3 0e cd c9 c0 8b 41 8f 7f 28 ff 83 48 75 40 ff c5 cb 0a 33 da

K = 09 09 09 09 09 09 09 09 09 09
IV= 00 00 00 00 00 00 00 00
Z = 43 9b ba f8 a7 84 dc f9 e6 d2 90 1d 12 4d 43 09 22 33 f2 47 60 19 70 53

K = 09 08 07 06 05 04 03 02 01 00
IV= 00 00 00 00 00 00 00 00
Z = 52 b1 73 10 01 2a cd 3a d2 20 4f e2 b2 2a 5d 21 64 41 f6 3d d3 b4 43 6a

K = eb 98 45 f2 9f 4c f9 a6 53 00
IV= de 77 10 a9 42 db 74 0d
Z = 62 ff c9 cc 21 0e 07 ea 6e 50 f0 fb 1b 60 36 7f 88 a6 a5 27 9b 18 cb b8
```

```
K = fa a7 54 01 ae 5b 08 b5 62 0f
IV= f9 92 2b c4 5d f6 8f 28
Z = f0 af 66 52 2a 23 8b 29 63 37 8b 18 ec 1f 4c a8 27 91 3d 2c f0 ad 94 d9
```

A.5.2 Sample internal states

We provide the binary equivalents of the internal states for key stages, namely at time -256, time -64, time 0 and time 193.

```
K = 00 00 00 00 00 00 00 00 00 80
IV= 00 00 00 00 00 00 00 00
Z = 76 e3 89 be 1b fb ad d5 3c ce a0 fe 43 b8 c8 fb d3 92 b8 0b 52 94 60 f8
```

For time -256 until -64 (executions of *InitNext* (*S*,LFSR)), internal state variables *T*, *b* and *I* have the following values:

```
T: 000
b: 00 00 00 00
I: 0
```

```
Decim v2 Internal State at time -256
a: ff ff ff ff 00 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00 80

Decim v2 Binary Internal State at time -256 (Binary notation)
a: 11111111 11111111 11111111 11111111 00000000 00000000 00000000 00000000
   00000000 00000000 00000000 00000000 00000000 10000000 00000000 00000000
   00000000 00000000 00000000 00000000 00000000 00000000 00000000 10000000

Executions of InitNext(S,LFSR)

Decim v2 Internal State at time -255
a: 2f ff ff ff f0 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 08

Decim v2 Internal State at time -254
a: 42 ff ff ff ff 00 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00

Decim v2 Internal State at time -253
a: 84 2f ff ff ff f0 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00

Decim v2 Internal State at time -252
a: 98 42 ff ff ff ff 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00

Decim v2 Internal State at time -251
a: 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00

Decim v2 Internal State at time -250
a: 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00

Decim v2 Internal State at time -249
a: e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 08 00 00 00 00 00 00

Decim v2 Internal State at time -248
a: 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 80 00 00 00 00 00 00

Decim v2 Internal State at time -247
a: 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 08 00 00 00 00 00

Decim v2 Internal State at time -246
a: 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 80 00 00 00 00 00

Decim v2 Internal State at time -245
a: d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 08 00 00 00 00

Decim v2 Internal State at time -244
a: 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 80 00 00 00 00

Decim v2 Internal State at time -243
a: 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 08 00 00 00
```

```
Decim v2 Internal State at time -242
a: d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 00 80 00 00 00

Decim v2 Internal State at time -241
a: fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 00 08 00 00 00

Decim v2 Internal State at time -240
a: df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 00 00 80 00 00

Decim v2 Internal State at time -239
a: ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 00 08 00 00

Decim v2 Internal State at time -238
a: fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 00 80 00

Decim v2 Internal State at time -237
a: ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 00 08 00

Decim v2 Internal State at time -236
a: ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 00 00 80

Decim v2 Internal State at time -235
a: ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 00 08

Decim v2 Internal State at time -234
a: 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 00 00

Decim v2 Internal State at time -233
a: 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00 00

Decim v2 Internal State at time -232
a: 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00 00

Decim v2 Internal State at time -231
a: b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00 00

Decim v2 Internal State at time -230
a: 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00 00

Decim v2 Internal State at time -229
a: c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00 00

Decim v2 Internal State at time -228
a: bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00 00

Decim v2 Internal State at time -227
a: 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00 00

Decim v2 Internal State at time -226
a: d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00 00

Decim v2 Internal State at time -225
a: bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00 00

Decim v2 Internal State at time -224
a: 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00 00

Decim v2 Internal State at time -223
a: 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00 00

Decim v2 Internal State at time -222
a: b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00 00

Decim v2 Internal State at time -221
a: fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00 00

Decim v2 Internal State at time -220
a: 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00 00

Decim v2 Internal State at time -219
a: 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0 00

Decim v2 Internal State at time -218
a: 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff 00
```

```
Decim v2 Internal State at time -217
a: 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff f0

Decim v2 Internal State at time -216
a: f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff ff

Decim v2 Internal State at time -215
a: 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff ff

Decim v2 Internal State at time -214
a: e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff ff

Decim v2 Internal State at time -213
a: 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff ff

Decim v2 Internal State at time -212
a: f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff ff

Decim v2 Internal State at time -211
a: 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f ff

Decim v2 Internal State at time -210
a: 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42 ff

Decim v2 Internal State at time -209
a: 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84 2f

Decim v2 Internal State at time -208
a: 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98 42

Decim v2 Internal State at time -207
a: d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99 84

Decim v2 Internal State at time -206
a: 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89 98

Decim v2 Internal State at time -205
a: 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8 99

Decim v2 Internal State at time -204
a: 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e 89

Decim v2 Internal State at time -203
a: 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04 e8

Decim v2 Internal State at time -202
a: 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00 4e

Decim v2 Internal State at time -201
a: c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0 04

Decim v2 Internal State at time -200
a: 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d 00

Decim v2 Internal State at time -199
a: 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16 d0

Decim v2 Internal State at time -198
a: 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1 6d

Decim v2 Internal State at time -197
a: 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd 16

Decim v2 Internal State at time -196
a: 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df d1

Decim v2 Internal State at time -195
a: 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed fd

Decim v2 Internal State at time -194
a: c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe df

Decim v2 Internal State at time -193
a: bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef ed
```

```
Decim v2 Internal State at time -192
a: 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee fe

Decim v2 Internal State at time -191
a: c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce ef

Decim v2 Internal State at time -190
a: 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c ee

Decim v2 Internal State at time -189
a: 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60 ce

Decim v2 Internal State at time -188
a: 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06 0c

Decim v2 Internal State at time -187
a: a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0 60

Decim v2 Internal State at time -186
a: ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b 06

Decim v2 Internal State at time -185
a: fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5 b0

Decim v2 Internal State at time -184
a: 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc 5b

Decim v2 Internal State at time -183
a: 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b c5

Decim v2 Internal State at time -182
a: f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6 bc

Decim v2 Internal State at time -181
a: af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd 6b

Decim v2 Internal State at time -180
a: 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b d6

Decim v2 Internal State at time -179
a: 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38 bd

Decim v2 Internal State at time -178
a: b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3 8b

Decim v2 Internal State at time -177
a: 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb 38

Decim v2 Internal State at time -176
a: 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f b3

Decim v2 Internal State at time -175
a: e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84 fb

Decim v2 Internal State at time -174
a: 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18 4f

Decim v2 Internal State at time -173
a: d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21 84

Decim v2 Internal State at time -172
a: 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2 18

Decim v2 Internal State at time -171
a: f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f 21

Decim v2 Internal State at time -170
a: 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9 f2

Decim v2 Internal State at time -169
a: d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e 9f

Decim v2 Internal State at time -168
a: cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6 e9
```

```
Decim v2 Internal State at time -167
a: dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f 6e

Decim v2 Internal State at time -166
a: ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45 f6

Decim v2 Internal State at time -165
a: fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04 5f

Decim v2 Internal State at time -164
a: 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10 45

Decim v2 Internal State at time -163
a: 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1 04

Decim v2 Internal State at time -162
a: 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d 10

Decim v2 Internal State at time -161
a: d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31 d1

Decim v2 Internal State at time -160
a: 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13 1d

Decim v2 Internal State at time -159
a: 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81 31

Decim v2 Internal State at time -158
a: 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88 13

Decim v2 Internal State at time -157
a: d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8 81

Decim v2 Internal State at time -156
a: ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c 88

Decim v2 Internal State at time -155
a: 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77 c8

Decim v2 Internal State at time -154
a: 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17 7c

Decim v2 Internal State at time -153
a: b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91 77

Decim v2 Internal State at time -152
a: 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49 17

Decim v2 Internal State at time -151
a: 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44 91

Decim v2 Internal State at time -150
a: e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4 49

Decim v2 Internal State at time -149
a: fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc 44

Decim v2 Internal State at time -148
a: cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b c4

Decim v2 Internal State at time -147
a: 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5 bc

Decim v2 Internal State at time -146
a: 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c 5b

Decim v2 Internal State at time -145
a: 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25 c5

Decim v2 Internal State at time -144
a: 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92 5c

Decim v2 Internal State at time -143
a: d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9 25
```

```
Decim v2 Internal State at time -142
a: 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca 92

Decim v2 Internal State at time -141
a: b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc a9

Decim v2 Internal State at time -140
a: 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f ca

Decim v2 Internal State at time -139
a: f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89 fc

Decim v2 Internal State at time -138
a: 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8 9f

Decim v2 Internal State at time -137
a: 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af 89

Decim v2 Internal State at time -136
a: 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a f8

Decim v2 Internal State at time -135
a: 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46 af

Decim v2 Internal State at time -134
a: e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4 6a

Decim v2 Internal State at time -133
a: 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b 46

Decim v2 Internal State at time -132
a: f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76 b4

Decim v2 Internal State at time -131
a: 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7 6b

Decim v2 Internal State at time -130
a: 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e 76

Decim v2 Internal State at time -129
a: c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2 e7

Decim v2 Internal State at time -128
a: 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d 2e

Decim v2 Internal State at time -127
a: 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8 d2

Decim v2 Internal State at time -126
a: 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f 8d

Decim v2 Internal State at time -125
a: 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6 f8

Decim v2 Internal State at time -124
a: 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd 6f

Decim v2 Internal State at time -123
a: 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc d6

Decim v2 Internal State at time -122
a: 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed cd

Decim v2 Internal State at time -121
a: 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe dc

Decim v2 Internal State at time -120
a: f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f ed

Decim v2 Internal State at time -119
a: 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21 fe

Decim v2 Internal State at time -118
a: d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22 1f
```

```
Decim v2 Internal State at time -117
a: 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2 21

Decim v2 Internal State at time -116
a: 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d 22

Decim v2 Internal State at time -115
a: 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53 d2

Decim v2 Internal State at time -114
a: 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45 3d

Decim v2 Internal State at time -113
a: 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4 53

Decim v2 Internal State at time -112
a: 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed 45

Decim v2 Internal State at time -111
a: 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e d4

Decim v2 Internal State at time -110
a: b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23 ed

Decim v2 Internal State at time -109
a: 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2 3e

Decim v2 Internal State at time -108
a: 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b 23

Decim v2 Internal State at time -107
a: 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91 b2

Decim v2 Internal State at time -106
a: a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9 1b

Decim v2 Internal State at time -105
a: ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe 91

Decim v2 Internal State at time -104
a: bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf e9

Decim v2 Internal State at time -103
a: 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c fe

Decim v2 Internal State at time -102
a: 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64 cf

Decim v2 Internal State at time -101
a: 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46 4c

Decim v2 Internal State at time -100
a: a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94 64

Decim v2 Internal State at time -99
a: 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9 46

Decim v2 Internal State at time -98
a: 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d 94

Decim v2 Internal State at time -97
a: 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6 d9

Decim v2 Internal State at time -96
a: d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b 6d

Decim v2 Internal State at time -95
a: 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9 b6

Decim v2 Internal State at time -94
a: 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f 9b

Decim v2 Internal State at time -93
a: 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51 f9
```

```
Decim v2 Internal State at time -92
a: 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85 1f

Decim v2 Internal State at time -91
a: 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18 51

Decim v2 Internal State at time -90
a: a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1 85

Decim v2 Internal State at time -89
a: 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e 18

Decim v2 Internal State at time -88
a: a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6 e1

Decim v2 Internal State at time -87
a: da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f 6e

Decim v2 Internal State at time -86
a: 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39 f6

Decim v2 Internal State at time -85
a: d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3 9f

Decim v2 Internal State at time -84
a: ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c 39

Decim v2 Internal State at time -83
a: 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38 c3

Decim v2 Internal State at time -82
a: 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53 8c

Decim v2 Internal State at time -81
a: 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55 38

Decim v2 Internal State at time -80
a: a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75 53

Decim v2 Internal State at time -79
a: 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77 55

Decim v2 Internal State at time -78
a: 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07 75

Decim v2 Internal State at time -77
a: c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10 77

Decim v2 Internal State at time -76
a: 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1 07

Decim v2 Internal State at time -75
a: 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f 10

Decim v2 Internal State at time -74
a: 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8 f1

Decim v2 Internal State at time -73
a: 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d 8f

Decim v2 Internal State at time -72
a: 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69 d8

Decim v2 Internal State at time -71
a: 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86 9d

Decim v2 Internal State at time -70
a: 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48 69

Decim v2 Internal State at time -69
a: 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64 86

Decim v2 Internal State at time -68
a: f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06 48
```

```
Decim v2 Internal State at time -67
a: 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60 64

Decim v2 Internal State at time -66
a: 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6 06

Decim v2 Internal State at time -65
a: 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b 60


Decim v2 Internal State at time -64
a: 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71 b6

Decim v2 Internal State at time -64 (Binary notation)
a: 00111000 00100011 11111001 01010100 10010100 01100011 01011000 11010001
   01101001 01010111 10101101 10001101 10100101 10100001 01001001 10100111
   10000111 01001100 10100011 01010101 10111011 10100100 01110001 10110110
T: 000        b: 00000000 00000000 00000000 00000000        I: 0

Executions of InitNext(S,BUFF)

Decim v2 Internal State at time -63
a: 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47 1b
T: 111        b: 00 00 00 00        I: 1

Decim v2 Internal State at time -62
a: a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4 71
T: 111        b: 00 00 00 00        I: 2

Decim v2 Internal State at time -61
a: 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba 47
T: 101        b: 00 00 00 00        I: 3

Decim v2 Internal State at time -60
a: 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb a4
T: 101        b: 00 00 00 08        I: 4

Decim v2 Internal State at time -59
a: b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b ba
T: 101        b: 00 00 00 18        I: 5

Decim v2 Internal State at time -58
a: 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55 bb
T: 001        b: 00 00 00 38        I: 6

Decim v2 Internal State at time -57
a: 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35 5b
T: 101        b: 00 00 00 78        I: 7

Decim v2 Internal State at time -56
a: 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3 55
T: 001        b: 00 00 00 f8        I: 9

Decim v2 Internal State at time -55
a: 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a 35
T: 001        b: 00 00 00 f8        I: 11

Decim v2 Internal State at time -54
a: 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58 a3
T: 010        b: 00 00 00 f8        I: 13

Decim v2 Internal State at time -53
a: a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15 8a
T: 010        b: 00 00 60 f8        I: 15

Decim v2 Internal State at time -52
a: 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1 58
T: 011        b: 00 00 60 f8        I: 16

Decim v2 Internal State at time -51
a: 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d 15
T: 011        b: 00 00 60 f8        I: 17

Decim v2 Internal State at time -50
a: d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69 d1
T: 010        b: 00 00 60 f8        I: 18
```

```
Decim v2 Internal State at time -49
a: 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96 9d
T: 001        b: 00 04 60 f8        I: 19

Decim v2 Internal State at time -48
a: 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49 69
T: 001        b: 00 14 60 f8        I: 21

Decim v2 Internal State at time -47
a: 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14 96
T: 001        b: 00 14 60 f8        I: 23

Decim v2 Internal State at time -46
a: 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1 49
T: 000        b: 00 94 60 f8        I: 25

Decim v2 Internal State at time -45
a: 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a 14
T: 000        b: 02 94 60 f8        I: 27

Decim v2 Internal State at time -44
a: e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5 a1
T: 010        b: 12 94 60 f8        I: 29

Decim v2 Internal State at time -43
a: 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da 5a
T: 010        b: 12 94 60 f8        I: 30

Decim v2 Internal State at time -42
a: 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5
T: 000        b: 52 94 60 f8        I: 32

Decim v2 Internal State at time 0
a: 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d a5
T: 000        b: 52 94 60 f8        I: 32

Decim v2 Internal State at time 0 (Binary notation)
a: 00000111 11100100 01010110 01000010 11011001 00111010 01001100 01100011
   10010100 00000111 10100010 00111000 00100011 11111001 01010100 00111011
   01010011 00100000 10000111 10100111 01010111 10001101 10001101 10100101
T: 000        b: 01010010 10010100 01100000 11111000        I: 32
```

Executions of *Next*(*S*)

```
Decim v2 Internal State at time 1
a: a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8 da
T: 101   b: a9 4a 30 7c   I: 32

Decim v2 Internal State at time 2
a: 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad 8d
T: 111   b: d4 a5 18 3e   I: 32

Decim v2 Internal State at time 3
a: b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a d8
T: 010   b: 6a 52 8c 1f   I: 32

Decim v2 Internal State at time 4
a: bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57 ad
T: 111   b: b5 29 46 0f   I: 32

Decim v2 Internal State at time 5
a: eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75 7a
T: 111   b: 5a 94 a3 07   I: 32

Decim v2 Internal State at time 6
a: ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7 57
T: 111   b: 2d 4a 51 83   I: 31

Decim v2 Internal State at time 7
a: fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a 75
T: 110   b: 16 a5 28 c1   I: 32

Decim v2 Internal State at time 8
a: 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87 a7
T: 111   b: 0b 52 94 60   I: 32
```

```
Decim v2 Internal State at time 9
a: f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8 7a
T: 010   b: 05 a9 4a 30   I: 32

Decim v2 Internal State at time 10
a: 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c 87
T: 010   b: 02 d4 a5 18   I: 32

Decim v2 Internal State at time 11
a: f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34 c8
T: 101   b: 01 6a 52 8c   I: 32

Decim v2 Internal State at time 12
a: 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63 4c
T: 100   b: 80 b5 29 46   I: 32

Decim v2 Internal State at time 13
a: 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46 34
T: 101   b: c0 5a 94 a3   I: 31

Decim v2 Internal State at time 14
a: 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94 63
T: 110   b: e0 2d 4a 51   I: 31

Decim v2 Internal State at time 15
a: 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49 46
T: 110   b: 70 16 a5 28   I: 32

Decim v2 Internal State at time 16
a: f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54 94
T: 000   b: b8 0b 52 94   I: 32

Decim v2 Internal State at time 17
a: 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95 49
T: 111   b: dc 05 a9 4a   I: 31

Decim v2 Internal State at time 18
a: 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9 54
T: 100   b: ae 02 d4 a5   I: 32

Decim v2 Internal State at time 19
a: 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f 95
T: 010   b: 57 01 6a 52   I: 32

Decim v2 Internal State at time 20
a: b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23 f9
T: 101   b: 2b 80 b5 29   I: 32

Decim v2 Internal State at time 21
a: eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82 3f
T: 101   b: 15 c0 5a 94   I: 31

Decim v2 Internal State at time 22
a: be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38 23
T: 110   b: 4a e0 2d 4a   I: 31

Decim v2 Internal State at time 23
a: 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23 82
T: 000   b: 25 70 16 a5   I: 32

Decim v2 Internal State at time 24
a: 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2 38
T: 100   b: 92 b8 0b 52   I: 32

Decim v2 Internal State at time 25
a: 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a 23
T: 101   b: c9 5c 05 a9   I: 32

Decim v2 Internal State at time 26
a: 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07 a2
T: 010   b: e4 ae 02 d4   I: 32

Decim v2 Internal State at time 27
a: 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0 7a
T: 111   b: 72 57 01 6a   I: 32
```

```
Decim v2 Internal State at time 28
a: b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b 07
T: 100   b: 39 2b 80 b5   I: 32

Decim v2 Internal State at time 29
a: 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33 b0
T: 101   b: 1c 95 c0 5a   I: 31

Decim v2 Internal State at time 30
a: d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53 3b
T: 000   b: 4e 4a e0 2d   I: 32

Decim v2 Internal State at time 31
a: bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05 33
T: 010   b: a7 25 70 16   I: 32

Decim v2 Internal State at time 32
a: 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20 53
T: 110   b: d3 92 b8 0b   I: 32

Decim v2 Internal State at time 33
a: c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2 05
T: 110   b: e9 c9 5c 05   I: 32

Decim v2 Internal State at time 34
a: 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a 20
T: 111   b: f4 e4 ae 02   I: 32

Decim v2 Internal State at time 35
a: c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93 a2
T: 101   b: 7a 72 57 01   I: 32

Decim v2 Internal State at time 36
a: dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9 3a
T: 110   b: bd 39 2b 80   I: 32

Decim v2 Internal State at time 37
a: fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d 93
T: 110   b: de 9c 95 c0   I: 32

Decim v2 Internal State at time 38
a: af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42 d9
T: 110   b: ef 4e 4a e0   I: 32

Decim v2 Internal State at time 39
a: 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64 2d
T: 010   b: f7 a7 25 70   I: 32

Decim v2 Internal State at time 40
a: e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56 42
T: 000   b: fb d3 92 b8   I: 32

Decim v2 Internal State at time 41
a: fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45 64
T: 111   b: 7d e9 c9 5c   I: 32

Decim v2 Internal State at time 42
a: 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4 56
T: 000   b: 3e f4 e4 ae   I: 32

Decim v2 Internal State at time 43
a: 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e 45
T: 010   b: 1f 7a 72 57   I: 32

Decim v2 Internal State at time 44
a: 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07 e4
T: 000   b: 8f bd 39 2b   I: 32

Decim v2 Internal State at time 45
a: d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0 7e
T: 111   b: 47 de 9c 95   I: 32

Decim v2 Internal State at time 46
a: 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a 07
T: 000   b: 23 ef 4e 4a   I: 32
```

```
Decim v2 Internal State at time 47
a: 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0 a0
T: 101   b: 11 f7 a7 25   I: 31

Decim v2 Internal State at time 48
a: f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb 0a
T: 101   b: 48 fb d3 92   I: 31

Decim v2 Internal State at time 49
a: 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb b0
T: 110   b: 64 7d e9 c9   I: 32

Decim v2 Internal State at time 50
a: 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce bb
T: 111   b: 32 3e f4 e4   I: 32

Decim v2 Internal State at time 51
a: e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc eb
T: 111   b: 19 1f 7a 72   I: 31

Decim v2 Internal State at time 52
a: fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f ce
T: 101   b: 0c 8f bd 39   I: 31

Decim v2 Internal State at time 53
a: 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3 fc
T: 000   b: 46 47 de 9c   I: 31

Decim v2 Internal State at time 54
a: 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f 3f
T: 100   b: 63 23 ef 4e   I: 31

Decim v2 Internal State at time 55
a: 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3 f3
T: 111   b: 71 91 f7 a7   I: 31

Decim v2 Internal State at time 56
a: 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f 3f
T: 100   b: b8 c8 fb d3   I: 32

Decim v2 Internal State at time 57
a: 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76 f3
T: 100   b: dc 64 7d e9   I: 32

Decim v2 Internal State at time 58
a: 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37 6f
T: 111   b: ee 32 3e f4   I: 32

Decim v2 Internal State at time 59
a: b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53 76
T: 000   b: 77 19 1f 7a   I: 32

Decim v2 Internal State at time 60
a: 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5 37
T: 010   b: 3b 8c 8f bd   I: 32

Decim v2 Internal State at time 61
a: 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f 53
T: 100   b: 1d c6 47 de   I: 32

Decim v2 Internal State at time 62
a: f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48 f5
T: 101   b: 0e e3 23 ef   I: 32

Decim v2 Internal State at time 63
a: af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74 8f
T: 111   b: 87 71 91 f7   I: 32

Decim v2 Internal State at time 64
a: ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7 48
T: 111   b: 43 b8 c8 fb   I: 32

Decim v2 Internal State at time 65
a: bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb 74
T: 010   b: 21 dc 64 7d   I: 32
```

```
Decim v2 Internal State at time 66
a: eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be b7
T: 000   b: 90 ee 32 3e   I: 32

Decim v2 Internal State at time 67
a: 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b eb
T: 110   b: c8 77 19 1f   I: 32

Decim v2 Internal State at time 68
a: f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39 be
T: 100   b: e4 3b 8c 8f   I: 32

Decim v2 Internal State at time 69
a: cf 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43 9b
T: 101   b: f2 1d c6 47   I: 32

Decim v2 Internal State at time 70
a: bc f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24 39
T: 000   b: f9 0e e3 23   I: 32

Decim v2 Internal State at time 71
a: ab cf 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52 43
T: 000   b: fc 87 71 91   I: 32

Decim v2 Internal State at time 72
a: ea bc f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5 24
T: 101   b: fe 43 b8 c8   I: 31

Decim v2 Internal State at time 73
a: ce ab cf 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b 52
T: 010   b: 7f 21 dc 64   I: 32

Decim v2 Internal State at time 74
a: 6c ea bc f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6 b5
T: 010   b: 3f 90 ee 32   I: 32

Decim v2 Internal State at time 75
a: 36 ce ab cf 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd 6b
T: 110   b: 1f c8 77 19   I: 32

Decim v2 Internal State at time 76
a: 63 6c ea bc f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b d6
T: 110   b: 0f e4 3b 8c   I: 32

Decim v2 Internal State at time 77
a: b6 36 ce ab cf 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4 bd
T: 000   b: 07 f2 1d c6   I: 32

Decim v2 Internal State at time 78
a: 3b 63 6c ea bc f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c 4b
T: 100   b: 83 f9 0e e3   I: 32

Decim v2 Internal State at time 79
a: a3 b6 36 ce ab cf 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3 c4
T: 101   b: 41 fc 87 71   I: 32

Decim v2 Internal State at time 80
a: aa 3b 63 6c ea bc f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc 3c
T: 010   b: a0 fe 43 b8   I: 32

Decim v2 Internal State at time 81
a: 8a a3 b6 36 ce ab cf 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd c3
T: 111   b: d0 7f 21 dc   I: 31

Decim v2 Internal State at time 82
a: 68 aa 3b 63 6c ea bc f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af dc
T: 010   b: a8 3f 90 ee   I: 31

Decim v2 Internal State at time 83
a: f6 8a a3 b6 36 ce ab cf 2e bb af 50 b4 73 27 0f e8 6f 81 d3 59 fe 2a fd
T: 110   b: d4 1f c8 77   I: 31

Decim v2 Internal State at time 84
a: df 68 aa 3b 63 6c ea bc f2 eb ba f5 0b 47 32 70 fe 86 f8 1d 35 9f e2 af
T: 110   b: ea 0f e4 3b   I: 32
```