INTERNATIONAL STANDARD

ISO/IEC 14443-4

Second edition
2008-07-15

AMENDMENT 4
2014-01-15

Identification cards — Contactless integrated circuit cards — Proximity cards —

Part 4: Transmission protocol

AMENDMENT 4: Frame with error correction

Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité —

Partie 4: Protocole de transmission

AMENDEMENT 4: Trame avec correction d'erreur

Reference number
ISO/IEC 14443-4:2008/Amd.4:2014(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 4 to ISO/IEC 14443-4:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

Identification cards — Contactless integrated circuit cards — Proximity cards —

Part 4: Transmission protocol

AMENDMENT 4: Frame with error correction

Page 2, NOTE in 3.4

Replace NOTE with

“

NOTE The PICC independent from its type may use the frame with error correction defined in clause 10. Alternatively the PICC Type A may use one of the standard frames defined for Type A and the PICC Type B may use the frame defined for Type B. This Type B frame is called standard frame, too, within this specification.

”

Page 2, Clause 4

Add new symbols and abbreviations in alphabetic order

“

A	Hamming control bits generation matrix (6 rows, 56 columns)
CRC_32	Cyclic Redundancy Check error detection code used within enhanced block
c_n	Hamming control bit n
$\underline{d}$	vector containing 56 data bits
d_n	data bit n
H	matrix needed to calculate Hamming syndrome $\underline{s}$ (6 rows, 62 columns)
$h'_{m,n}$	element in row m and column n of matrix ***H'***
H'	matrix needed to get matrix ***A*** (6 rows, 62 columns)
$\underline{h'}_n$	column vector of matrix ***H'***
$\boldsymbol{I_{6x6}}$	6 by 6 Identity matrix
LEN	two bytes LENgth field used within enhanced block
n	column index
m	row index
SYNC	SYNChronization sequence
$\underline{s}$	6-bit vector containing Hamming syndrome

s’ error position code

s error position

$\underline{y}$ 62-bit vector ($\underline{y}$’ with no padding bits)

$\underline{y'}$ 64-bit vector containing received modified Hamming sub-block

y'_n received bit n in each modified Hamming sub-block

“

Page 14, 7.1

Replace first paragraph with

“

The block format depends on the frame format used for its transmission.

The standard block format as specified in Figure 14 shall be used in standard frames as defined in ISO/IEC 14443-3 and consists of:

— a prologue field (mandatory);

— an information field (optional);

— a two-byte epilogue field (mandatory).

The enhanced block format specified in Figure 15 shall be used in frames with error correction as defined in Clause 10 and consists of:

— a length field (mandatory);

— a prologue field (mandatory);

— an information field (optional);

— a four-byte epilogue field (mandatory).

“

Page 15, after Figure 14

Add a new Figure 15, renumber all figures, add new subclause 7.1.1 and renumber all subsequent subclauses.

“

NOTE The items in brackets indicate optional requirements.

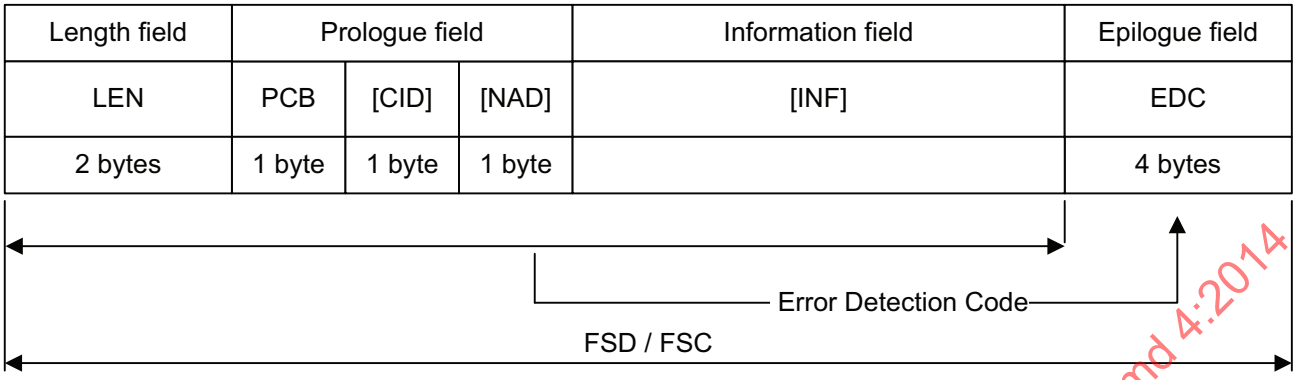

Figure 15 — Enhanced block format

7.1.1 Length field

The two-byte length field shall contain the total number of bytes contained in the following fields:

— Length field;

— Prologue field;

— Information field.

Least significant byte is transmitted first, then most significant byte.

“

Page 18, 7.1.3 (renumbered to 7.1.4)

Replace 7.1.4 with

“

7.1.4 Epilogue field

The epilogue field contains the EDC of the transmitted block. A transmitted block shall be considered correct if it is received with a valid EDC value.

The EDC of standard blocks shall be the CRC defined in ISO/IEC 14443-3. Type A PICCs shall use CRC_A and Type B PICCs shall use CRC_B in both directions.

The EDC of enhanced blocks shall be CRC_32 as defined below.

The CRC_32 uses polynomial = ‘04C11DB7’ with initial value = ‘FFFFFFFF’ and reflected bit order (LSB first). The final CRC value is bit-inverted before transmission and the least significant byte is transmitted first. Refer to ISO/IEC 13239 for further details. A code sample and an example are given in Annex E.

“

Page 23, 7.5.6

Replace first sentence with

“When at least one error is detected (after the optional error recovery mechanism see 10.4.7) the following recovery rules shall be applied.”

Page 25, before Annex A

Add a new clause 10 with the following:

“

10 Frame with error correction

10.1 General

Frames with error correction as specified in 10.2 and 10.3 shall be used after their activation as specified in 10.5. An example is given in Annex F.

10.2 Type A PCD frame format for bit rates up to *fc*/16 and higher than *fc*/2 and Type A PICC frame format for all bit rates

Frames with error correction, as defined in Figure 27, shall be used for data exchange and consist of, in the following order:

— start of communication;

— SYNC;

— enhanced block with error correction (see 10.4);

— end of communication.

SYNC consists of 6 dedicated bytes with the value ‘555574747474’ transmitted in this order.

SYNC and enhanced blocks with error correction shall be transmitted as bytes consisting of 8 bits.

NOTE Parity bits (see ISO/IEC 14443-3, 6.2.3.2) are not used.

S	SYNC	Enhanced block with error correction	E

Figure 27 — Frame with error correction

10.3 Type A PCD frame format for bit rates of *fc*/8, *fc*/4 and *fc*/2 and Type B PCD and PICC frame format for all bit rates

Frames with error correction, as defined in Figure 28, shall be used for data exchange and consist of, in the following order:

— SOF as defined in ISO/IEC 14443-3, 7.1.4;

— SYNC as defined in 10.2 transmitted as characters as defined in ISO/IEC 14443-3, 7.1.1;

— enhanced block with error correction (see 10.4) transmitted as characters as defined in ISO/IEC 14443-3, 7.1.1;

— EOF as defined in ISO/IEC 14443-3, 7.1.5.

No character separation shall be applied in frames with error correction.

SOF, EOF, start bit, stop bit and SYNC may be suppressed in accordance with 10.5.

SOF	SYNC	Enhanced block with error correction	EOF

Figure 28 — Frame with error correction

10.4 Enhanced block with error correction

10.4.1 General

Enhanced block with error correction shall be composed of one or several 8-byte modified Hamming sub-blocks, each of them being calculated from 7-byte sub-blocks from enhanced block (see Figure 29).

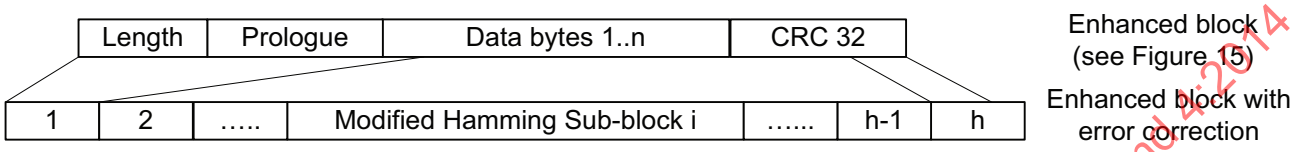

Figure 29 — Enhanced block with error correction

10.4.2 Modified Hamming Sub-block format

Each modified Hamming sub-block shall consist of 7 bytes from enhanced block, followed by one Hamming control byte used to correct one single-bit error on the Hamming sub-block.

Modified Hamming sub-blocks shall always be complete. If necessary, 'FF' bytes shall be added to complete the last bytes from enhanced block to get 7 bytes.

10.4.3 Hamming control byte

The Hamming control byte shall contain the Hamming control bits c_n and logical "1" padding bits in the following order:

— 1 logical "1" padding bit;

— 6 Hamming control bits c_n in the order c_1, c_2, c_3, c_4, c_5, c_6;

— 1 logical "1" padding bit.

An example for Hamming control byte calculation in C language is given in Annex F.2.

10.4.4 Hamming control generation matrix *A*

Hamming control bits generation matrix ***A*** (see Figure 32) shall be generated by following steps:

— generate Matrix ***H'*** (see Figure 31) using equation in Figure 30;

— remove column vectors $\underline{h}'_n$, with n = 1, 2, 4, 8, 16 and 32, of ***H'***.

$$h'_{m,n} = \begin{cases} 1 \text{ for } (n \wedge 2^{m-1}) \neq 0 \\ 0 \text{ otherwise} \end{cases} \quad \text{with } 1 \leq m \leq 6 \text{ and } 1 \leq n \leq 62$$

Figure 30 — Matrix *H'* generation

NOTE ^ stands for a bitwise AND operation.

$$H' = \begin{pmatrix} 1 & 0 & 1 & 0 & \dots & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 & 1 \end{pmatrix}$$

Figure 31 — Matrix *H'*

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 & \dots & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 & 1 \end{pmatrix}$$

Figure 32 — Hamming control generation matrix *A*

10.4.5 Hamming control bits calculation

Hamming control bits c_m (m = 1..6) shall be calculated over data d_n (n = 1..56) using equation in Figure 33. d_1 is bit b1 of the first byte and d_{56} is bit b8 of the seventh byte of any 7-byte sub-block from enhanced block.

$$\underline{c} = A \times \underline{d}$$

Figure 33 — Hamming control bits generation

10.4.6 Hamming control check matrix *H*

The Hamming control check matrix ***H*** (illustrated in Figure 34) is a concatenation of matrix ***A*** and matrix I_{6x6}.

$$H = A \,|\, I_{6,6} \begin{pmatrix} 1 & 1 & 0 & 1 & \dots & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & 1 & & 0 & 0 & 1 & 0 & 1 & & 0 & 0 \\ 0 & 1 & 1 & 1 & & 1 & 1 & 1 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & & 1 & 1 & 1 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & & 1 & 1 & 1 & 0 & 0 & & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 & 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Figure 34 — Hamming control check matrix *H*

10.4.7 Error correction

Hamming control bits shall be used to detect and correct any single bit error in modified Hamming sub-blocks.

The so called syndrome $\underline{s}$ shall be calculated using equation in Figure 35. To get $\underline{y}$ from $\underline{y'}$, the padding bits of the received data y'_n on position 57 and 64 shall be removed. y'_1 is bit b1 of the first received byte and y'_{64} is bit b8 of the eighth received byte of any 8-byte sub-block from enhanced block with error correction.

$$\underline{s} = H \times \underline{y}$$

Figure 35 — Syndrome calculation

The numerical interpretation s' of the syndrome $\underline{s}$ shall be used for error correction:

— if s' = 0, 1, 2, 4, 8, 16, 32 or 63 no change in received bits y'_1 to y'_{56}

— else

  — calculate error position s by reducing s' by the amount of powers of 2 (1, 2, 4, 8, 16, 32) which are smaller than s'

  — invert the received bit y'_s

NOTE More than one bit error cannot be corrected by this method. EDC will detect these multiple errors with very high probability.

10.5 Activation of frame with error correction in the PROTOCOL state

S(PARAMETERS) blocks shall be used to negotiate the used frame and communication parameters in PROTOCOL state. The following rules shall be applied to negotiate those parameters:

— The information field shall contain tags and values as defined in Tables 4 and 6 and Figures 36 and 37.

— The PCD shall send an S(PARAMETERS) block to request frame format parameters.

— If the PICC supports S(PARAMETERS) blocks, the PICC shall respond with an S(PARAMETERS) block containing values for all supported frame format parameters. If the PICC does not support S(PARAMETERS) it shall stay mute. The PICC shall always indicate the same framing options independent of which tag is used.

After the PICC has sent its response and has indicated its parameters the PCD may activate the desired options for each communication direction with following rules:

— The information field shall contain tags and values as defined in Tables 4 and 6 and Figures 36 and 37.

— The PCD shall send an S(PARAMETERS) block to activate selected frame format parameters.

— The PICC shall acknowledge the activated frame format parameters with an S(PARAMETERS) block and then shall activate the negotiated frame format parameters.

— The PCD shall activate the negotiated frame format parameters.

NOTE 1 S(PARAMETERS) block is defined in ISO/IEC 14443-4:2008/Amd.1:2012.

Table 6 — Frame format function tags identifier definition

Tags (Hex)	Description	Length (Hex)	Value		
'A5'	Frame Format Request	0	-		
'A6'	Frame Format Indication	L	Tags (Hex)	Length (Hex)	Value
			'80'	'01'	List of supported frames PCD to PICC (see Figure 36) [a]
			'81'	'01'	List of supported frames PICC to PCD (see Figure 36) [a]
			'82'	'01'	Supported framing options PCD to PICC (see Figure 37) [b]
			'83'	'01'	Supported framing options PICC to PCD (see Figure 37) [c]
'A7'	Frame Format Activation	L	Tags (Hex)	Length (Hex)	Value
			'84'	'01'	Selected frame PCD to PICC (see Figure 36) [d]
			'85'	'01'	Selected frame PICC to PCD (see Figure 36) [d]
			'86'	'01'	Selected framing options from PCD to PICC (see Figure 37) [b e]
			'87'	'01'	Selected framing options from PICC to PCD (see Figure 37) [c e f]
'A8'	Frame Format Acknowledgement	0	-		

[a] Bit 8 shall be set to the same value in both communication directions

[b] Shall be omitted for Type A PICCs for bit rates up to *fc*/16

[c] Shall be omitted for Type A PICCs

[d] Bit 8 shall be set to (0)b and only one bit out of b1 and b2 shall be set to (1)b.

[e] When SYNC is suppressed the PCD shall not select both start bit and stop bit suppression and SOF and EOF suppression. If start bit and stop bit suppression is selected, SOF and EOF low time of 10 etu and SOF high time of 2 etu shall be used.

[f] When tag '87' is used, the corresponding tag of bit rates > *fc*/16 shall not be used and vice versa.

NOTE The length field is in accordance with the full range of BER-TLV (see ISO/IEC 7816-4:2013).

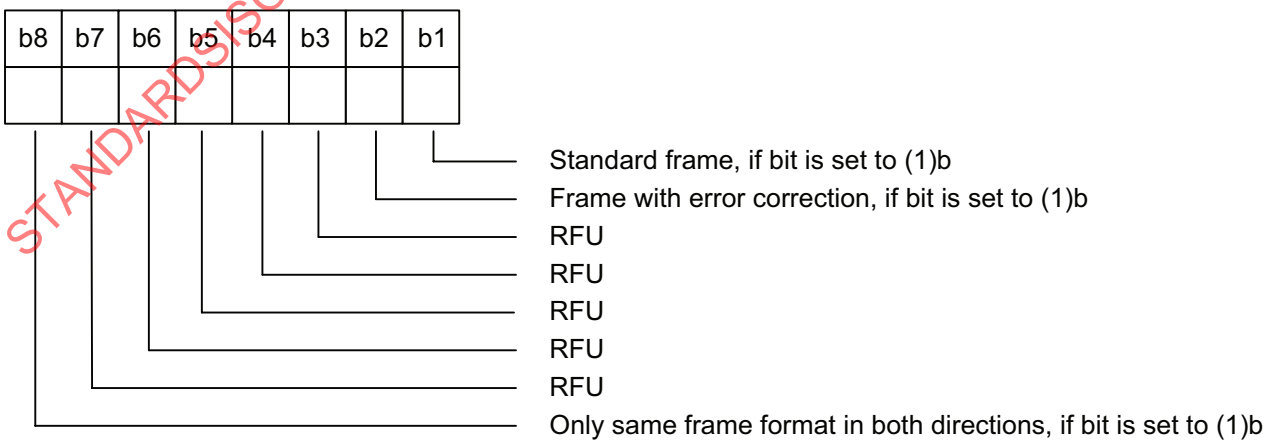

Figure 36 — Frame formats

NOTE 2 Standard frame support is mandatory.

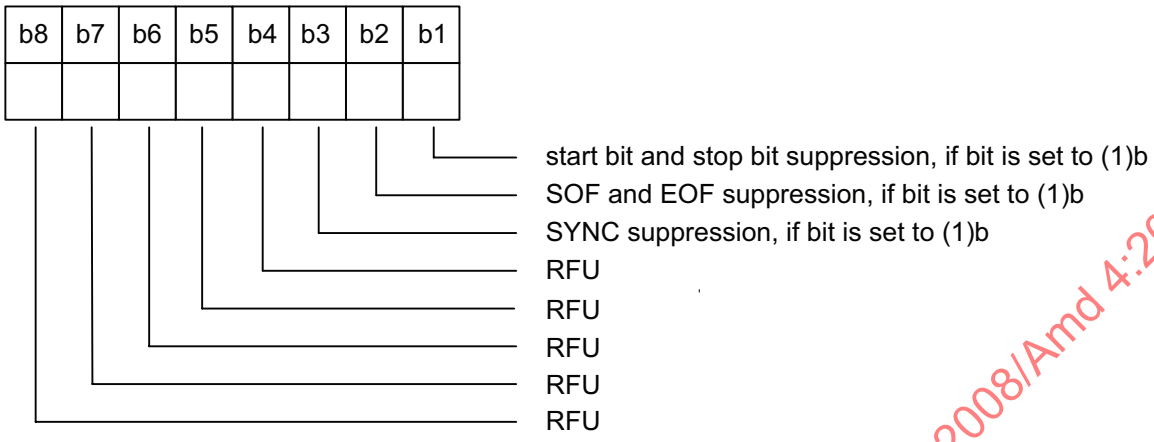

Figure 37 — Framing options

NOTE 3 Framing options depend on PICC Type, frame format, bit rate and communication direction. An overview is given in Annex G.

As an example the sequence for an activation of frame with error correction in both directions with

— no SYNC suppression in both directions

— no SOF and EOF suppression in both directions

— start bit and stop bit suppression in both directions and

with a PICC indicating to support

— standard and frame with error correction in both directions independent of each direction

— SYNC suppression in both directions

— SOF and EOF suppression in both directions and

— start bit and stop bit suppression in both directions

is illustrated in Figure 38. An overview on allowed suppressions of framing options is given in Annex G.

Step	PCD		PICC
1	S(PARAMETERS)('A0 02 A5 00' CRC)	⟶	
2		⟵	S(PARAMETERS) ('A0 0E' 'A6 0C' '80 01 03' '81 01 03' '82 01 07' '83 01 07' CRC)
3	S(PARAMETERS) ('A0 0E' 'A7 0C' '84 01 02' '85 01 02' '86 01 01' '87 01 01' CRC)	⟶	
4		⟵	S(PARAMETERS)('A0 02 A8 00' CRC)

Figure 38 — Frame activation example

NOTE 4 For Type A PICCs, tags '82' and '86' are omitted in certain cases (see table footnote b in Table 6) and tags '83' and '87' are always omitted (see table footnote c in Table 6).

"

Page 36, after Annex D

Add a new Annex E, Annex F and Annex G with the following:

Annex E
(informative)

CRC_32 encoding

E.1 CRC_32 encoding

This Annex is provided for explanatory purposes and indicates the bit patterns in enhanced block. It is included for the purpose of checking a CRC_32 encoding.

Initial Value = 'FFFFFFFF'.

EXAMPLE In Figure E.1 transmission of first byte = '06', second byte = '00', third byte = '0A', fourth byte = '01', fifth byte = '01', sixth byte = '02', and appended CRC_32 is illustrated. Calculated CRC_32 = '8098F1FE'.

1st byte	2nd byte	3rd byte	4th byte	5th byte	6th byte	CRC_32			
'06'	'00'	'0A'	'01'	'01'	'02'	80	98	F1	FE

Figure E.1 — Enhanced frame including CRC_32

E.2 Code sample written in C language for CRC_32 calculation

```
// ComputeCrc32.cpp : Defines the entry point for the console application

#include <stdio.h>

unsigned long ComputeCrc32(unsigned char *Data) {

  unsigned long c;
  unsigned char d, e, f;

  unsigned int i;

  unsigned int Length = 6;
  // initial value
  c = 0xffffffff;
  // compute CRC
  for (i = 0; i < Length; i++) {
    d = Data[i];

    e = c ^ d;
    f = e ^ (e << 6);
    c = (c >>  8) ^ (f << 24) ^ (f << 23) ^ (f << 22) ^
        (f << 20) ^ (f << 19) ^ (f << 17) ^ (f << 16) ^
        (f << 14) ^ (f << 13) ^ (f << 12) ^ (f <<  8) ^
        (f <<  2) ^ (f <<  1) ^ (f >>  2);
  }
  // invert result
  c = c ^ 0xffffffff;

  return c;
}


int main(void)
{
  unsigned char BuffCRC_32[6] = {0x06, 0x00, 0x0A, 0x01, 0x01, 0x02};
  unsigned int Crc32;
  int i;
```

```
  printf("\n");
  printf("CRC-32 reference results ISO/IEC 14443-4\n");
  printf("Crc-32 G(x) = x^32 + x^26 + x^23 + x^22 + x^16 + x^12 + x^11 +
                        x^10 + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1\n\n");
    printf("CRC_32 of [ ");
    for(i=0; i<6; i++) printf("%02X ",BuffCRC_32[i]);
    Crc32 = ComputeCrc32(BuffCRC_32);

  // revert byte order to get least significant byte first
    printf("] Transmitted: %02X then %02X then %02X then %02X.\n",
    (Crc32 & 0xFF), ((Crc32 >> 8) & 0xFF), ((Crc32 >> 16) & 0xFF), ((Crc32 >> 24) &
0xFF));

    return 0;
}
```