TRF79xx/MSP430/Stellaris Mifare Direct Mode 0 Training

Texas Instruments

ERF Systems/Apps Team

12/2011

Mifare Background

- Mifare uses ISO14443A air interface protocol, so TRF79xx is setup for ISO14443A, and Mifare card UID is read and then selected.
- After this point, a three round authentication must take place, and this is where the Mifare deviates from the standard, so the TRF79xx is placed in Direct Mode 0 (Analog Front End Mode)
- For TX, this is the relationship of MOD pin to carrier, as the MCU must modulate the RF according to the ISO14443A air interface and do so in accordance with Mifare protocol.
- For RX, this is the digitized data bit stream from I/O_6, which the MCU must decode, according to the ISO14443A air interface standard.

ISO14443A Standard Important Timings

- 128/fc = 9.435uSec = t_b (106kbps data rate)
- 64/fc = 4.719uSec = t_x time
- 32/fc = 2.359uSec = t_1 time

Figure 10 together with the timing parameters in Table 7 illustrate sequences X, Y and Z.

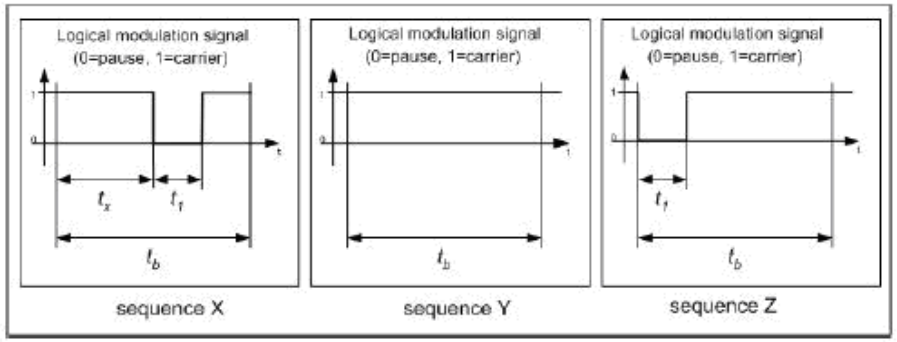


Figure 10 — Sequences for Type A communication PCD to PICC

Table 7 — Parameters for sequences

Parameter	Bit rate			
	fc/128	*fc*/64	*fc*/32	*fc*/16
t_b	128/*fc*	64/*fc*	32/*fc*	16/*fc*
t_x	64/*fc*	32/*fc*	16/*fc*	8/*fc*
t_1	see t_1 of Table 3	see t_1 of Table 5		

The above sequences shall be used to code the following information:

— logic "1": sequence X,

— logic "0": sequence Y with the following two exceptions:

i) If there are two or more contiguous "0"s, sequence Z shall be used from the second "0" on,

ii) If the first bit after a "start of frame" is "0", sequence Z shall be used to represent this and any "0"s which follow directly thereafter,

— start of communication: sequence Z,

— end of communication: logic "0" followed by sequence Y,

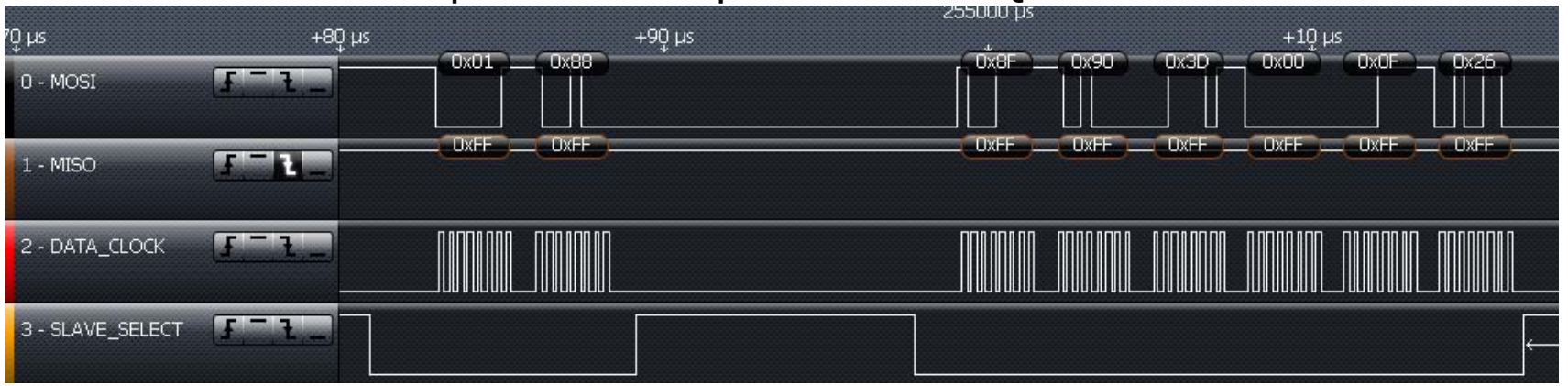
— no information: at least two sequences Y.

Technical Information

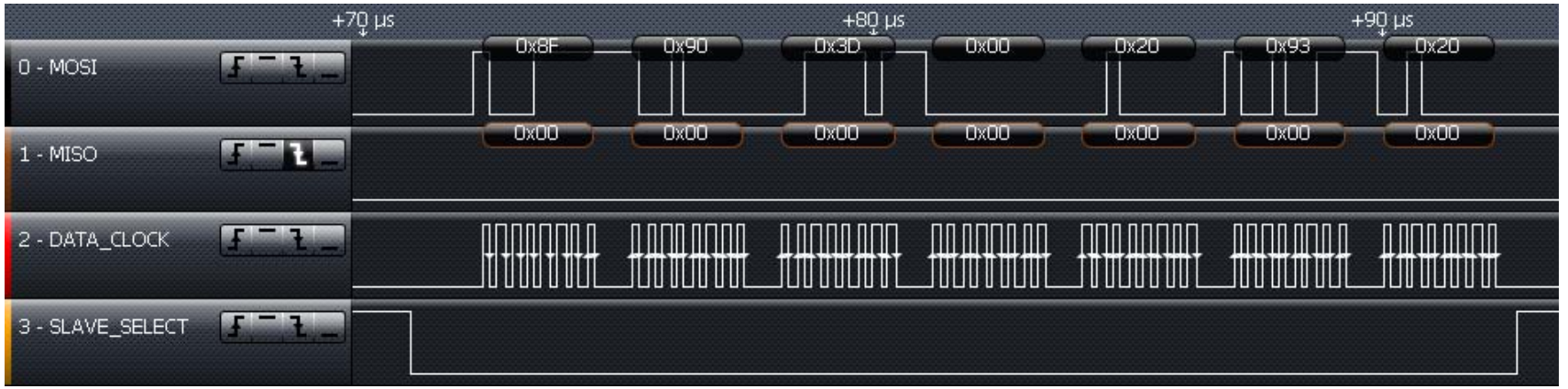
- The following several slides go into the details of using the TRF79xx devices first in Direct Mode 2 to read the card and select it, then in Direct Mode 0 during Mifare Card specific operations.
  - Note: subsequent slides do not show all register configurations, but this has been done beforehand, per the TRF79xx datasheets.

Reading and Selecting the Mifare Card in Direct Mode 2

- TRF79xx is configured for ISO14443A operations, ISO Control Register is set for RX w/no CRC present in response and REQA is issued.

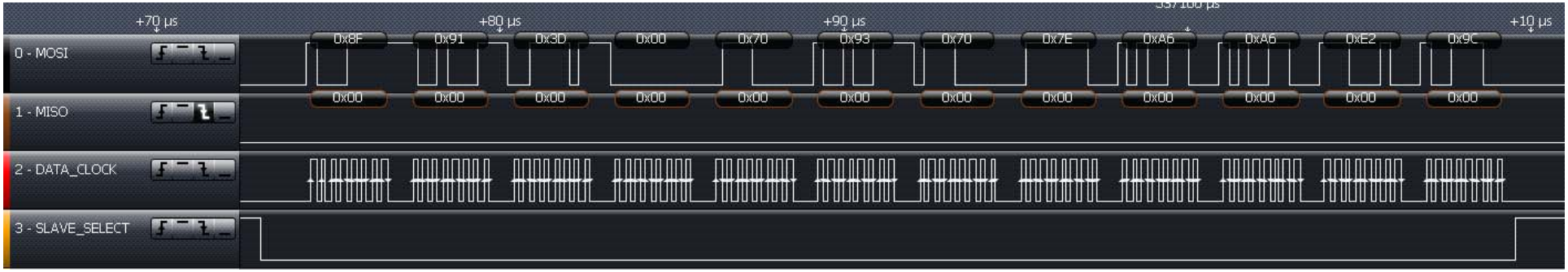


- ATQA is received, and then anti-collision sequence is started.

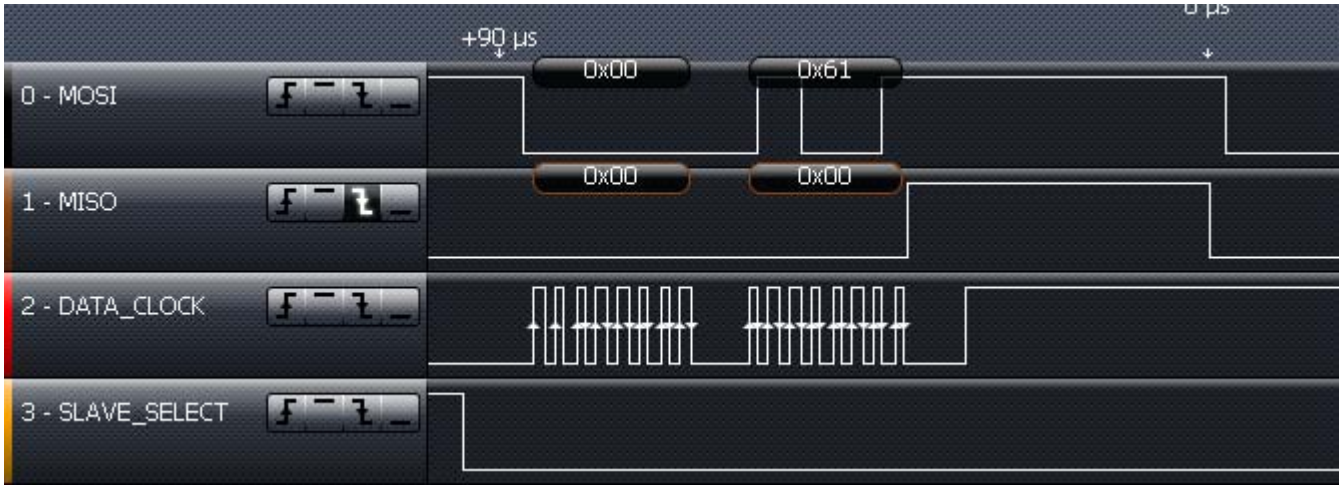


Reading and Selecting the Mifare Card in Direct Mode 2

- We receive the UID CLn, and then transmit the SELECT Command.



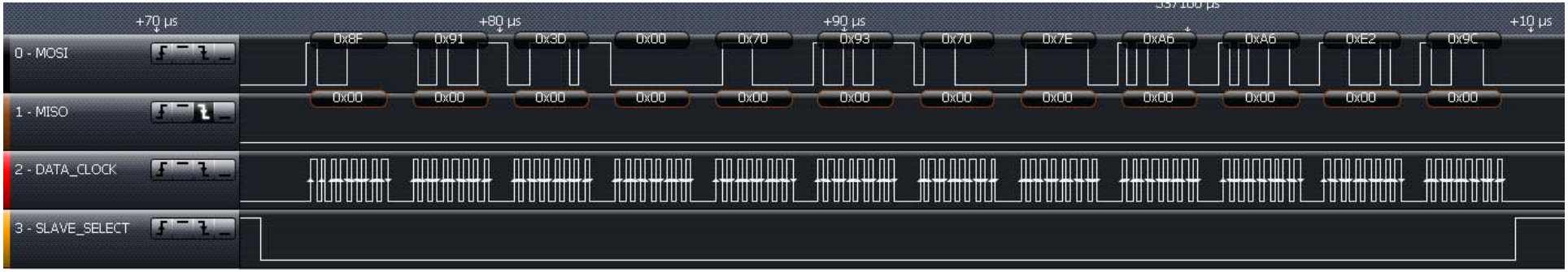
- We receive the SAK, and then the TRF7960/-60A is placed into Direct Mode 0.



Reading and Selecting the Mifare Card in Direct Mode 2

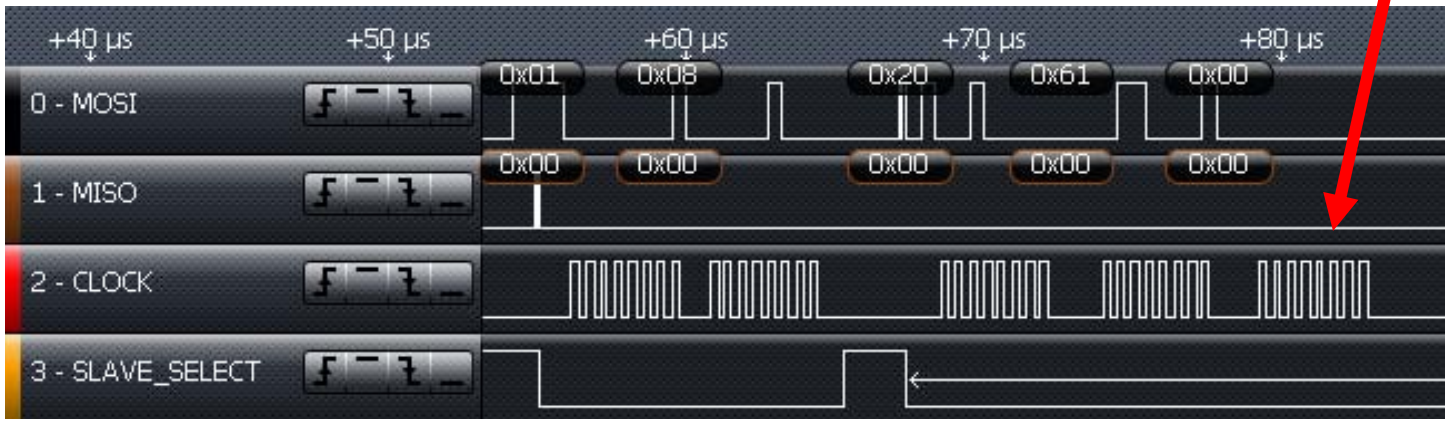
(cont., **TRF7970A** DM0 specific)

- We receive the UID CLn, and then transmit the SELECT Command.



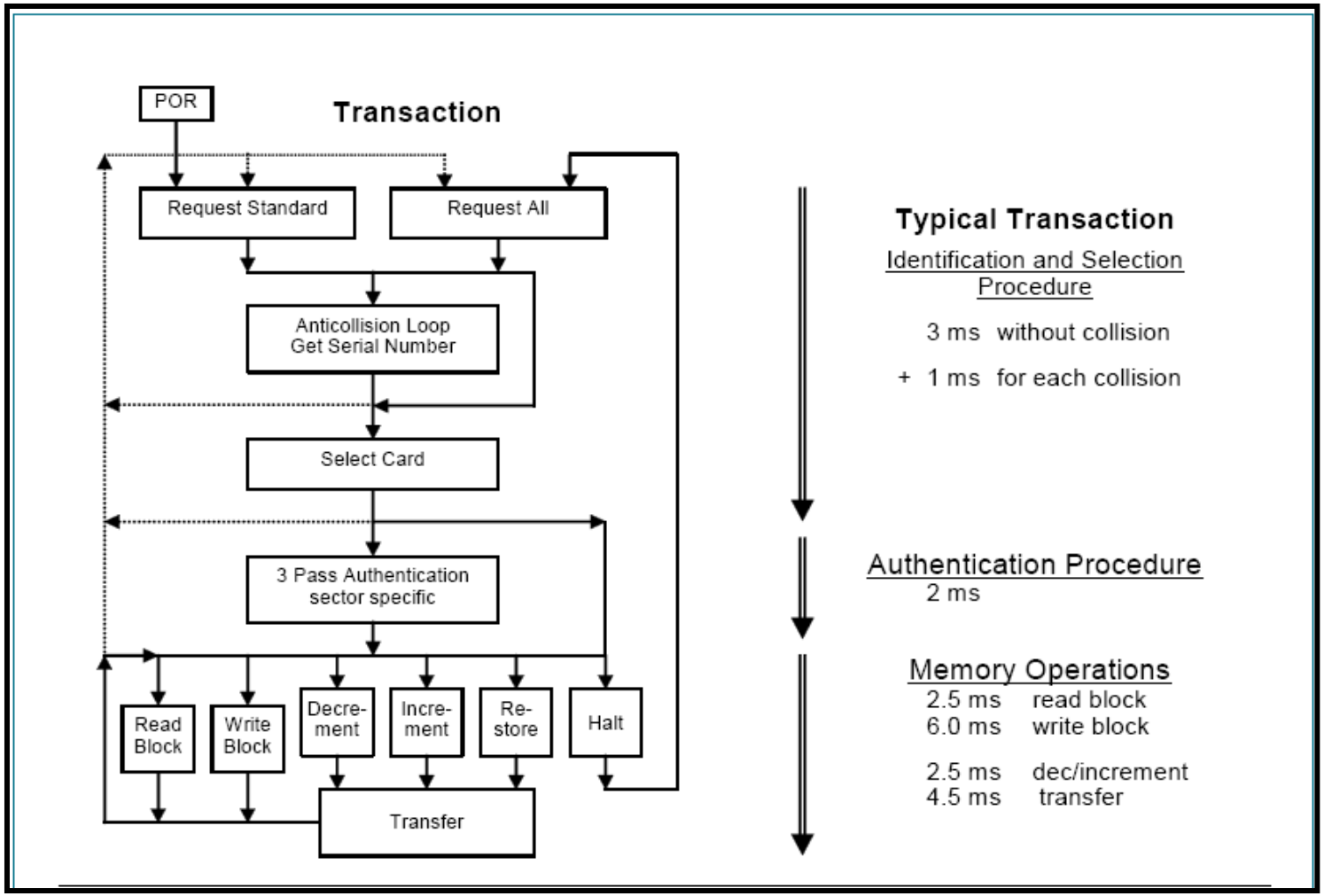
- We receive the SAK, and then the TRF7970A is placed into Direct Mode 0.

NOTE : see extra 8 clocks after sending 0x61 to Chip Status Control Register (Direct Mode 0) setting



Mifare Card Interaction Flow

(from NXP MF1ICS50 Data Sheet, marked public document)



Three pass authentication sequence

1. The reader specifies the sector to be accessed and chooses key A or B.
2. The card reads the secret key and the access conditions from the sector trailer. Then the card sends a random number as the challenge to the reader (pass one).
3. The reader calculates the response using the secret key and additional input. The response, together with a random challenge from the reader, is then transmitted to the card (pass two).
4. The card verifies the response of the reader by comparing it with its own challenge and then it calculates the response to the challenge and transmits it (pass three).
5. The reader verifies the response of the card by comparing it to its own challenge.

NOTE: **After transmission of the first random challenge the communication between card and reader is encrypted.**

Three pass authentication sequence (cont.)

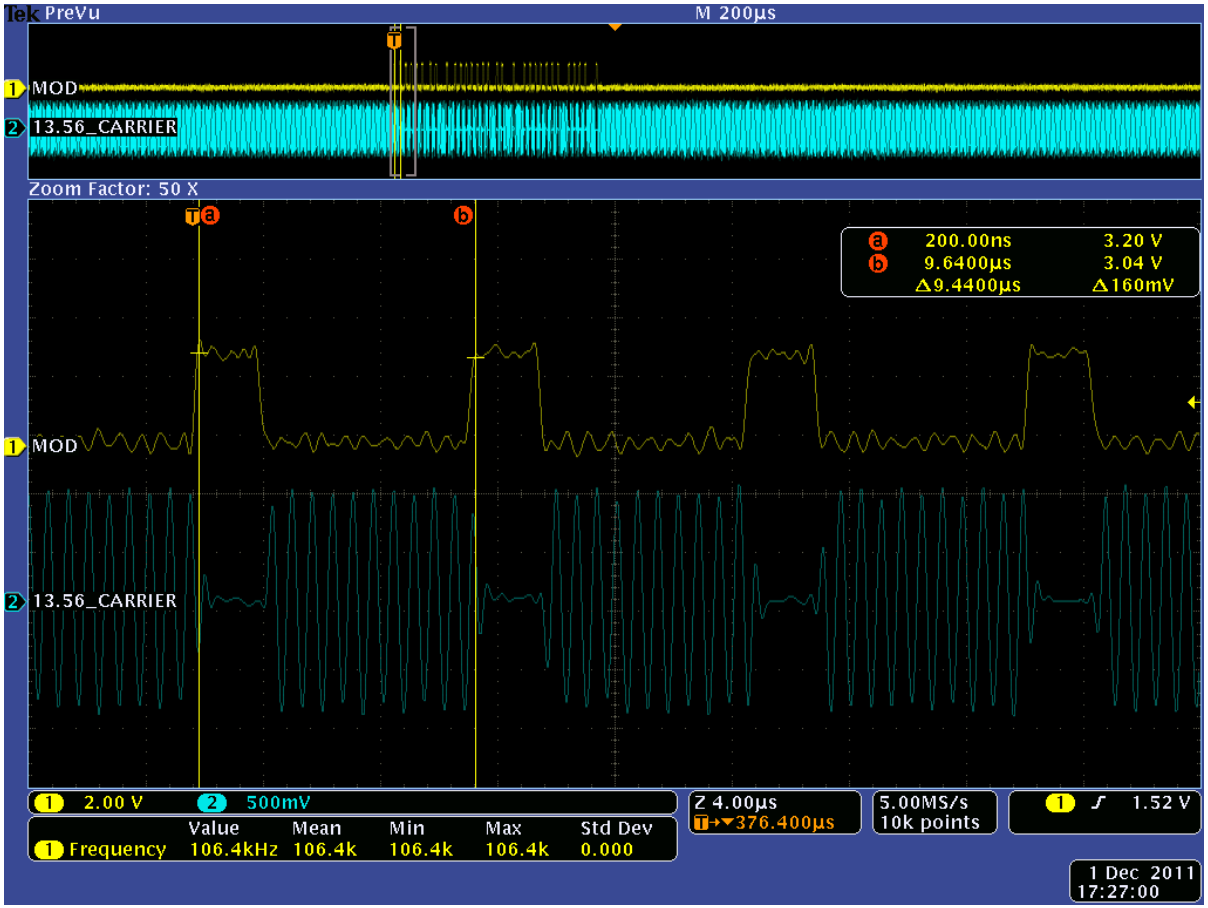
- The AUTH protocol does:
  - Reader sends 32 bit random number (+ error correction)
  - Card responds with 32 bit key stream XOR a derivative of the reader random number XOR its own random number
  - Reader responds with 32 bit key stream XOR the card random number
- **NOTE: None of this information can really be checked for plausibility without the secret keys, as it's either random or encrypted (or both mixed). This is why you will see later in the slides that 38 bits are sent out instead of the 80 bits that one might expect from reading publicly available NXP documents.**

Using the TRF79xx in Direct Mode 0 for Authentication

- At this point, the MOD pin is being driven by the MCU, which in turn is driving the TRF79xx transmitter, in accordance with the ISO14443A air interface specifications. For example, below is a logic analyzer capture showing the TRF79xx being put into Direct Mode 0, and also shown below is exact same thing, but on oscilloscope, so that the RF output can be correlated to how MOD pin is being driven. (next slide shows full size of the RF screen shot)

ISO14443A SOF (in Direct Mode 0)

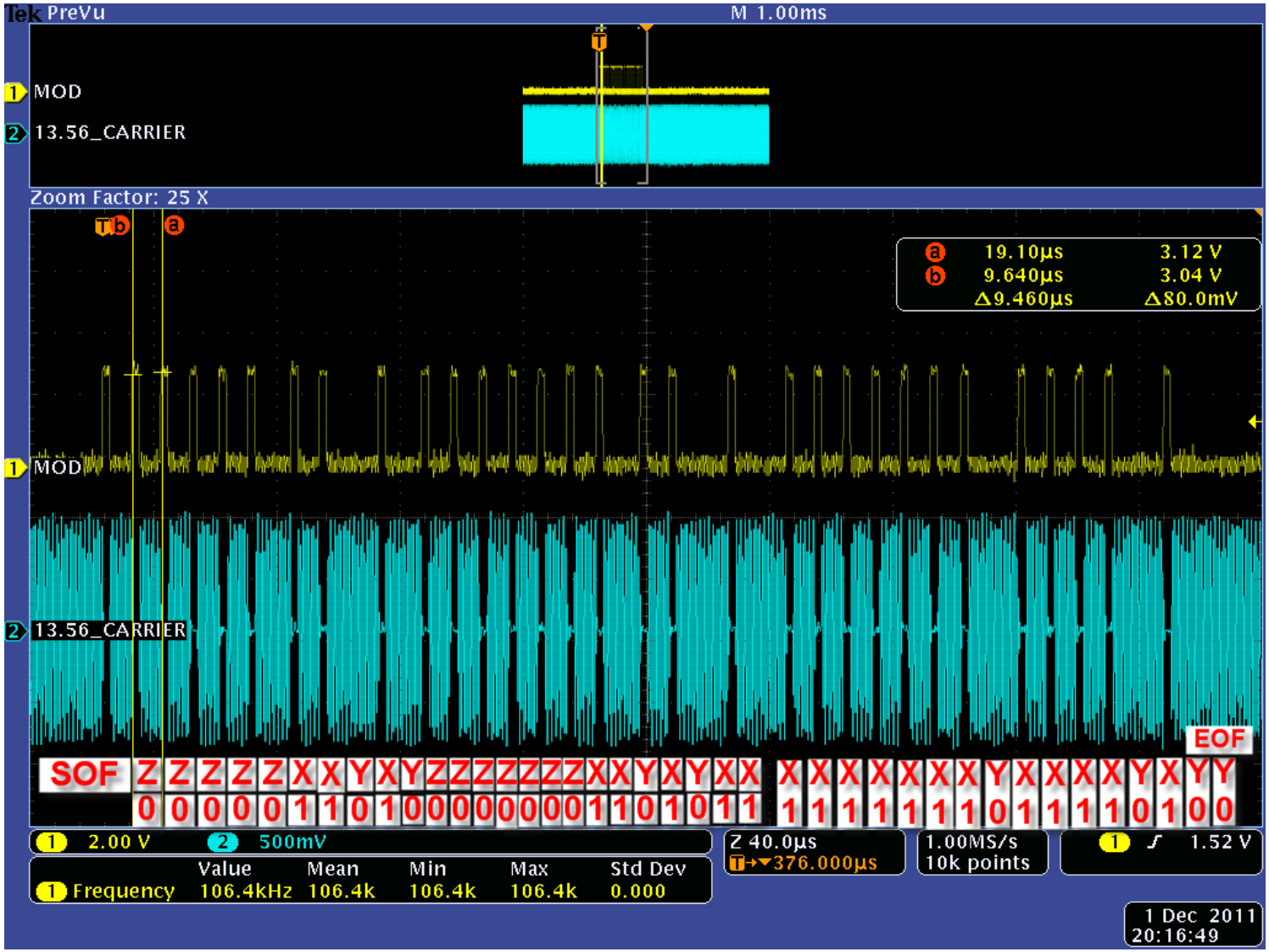
- Per the ISO14443A Standard, this is sequence Z, which is used for the PCD to PICC Start of Communication (SOF)



MSP430 Code Snippet

- * First stage of mutual authentication given a card's UID.
- * card_challenge is the card nonce as an integer
- */
- void crypto1_mutual_1(crypto1_state *state, uint32_t uid, uint32_t card_challenge)
- {
- 	state->ops->mutual_1(state, uid, card_challenge);
- }

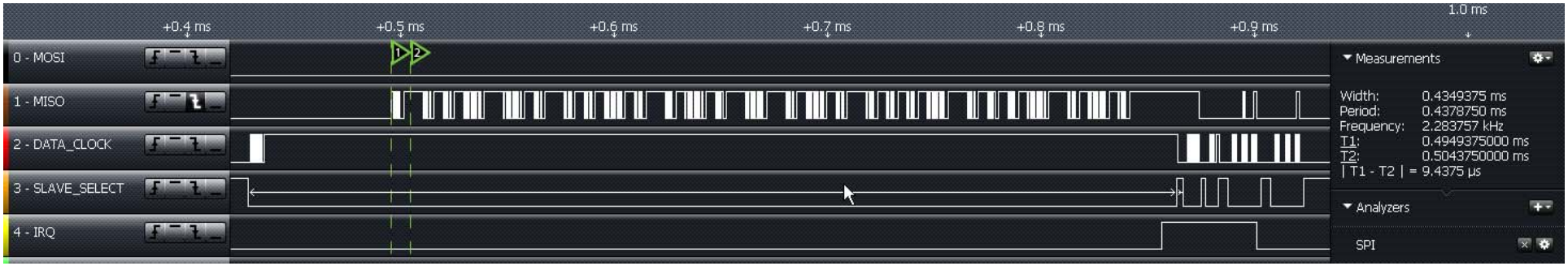
First TRF79xx TX Sequence Out in DM0 for Mifare Authentication



First TRF79xx RX Sequence on I/O_6 in DM0 for Mifare Authentication (Analog Capture)

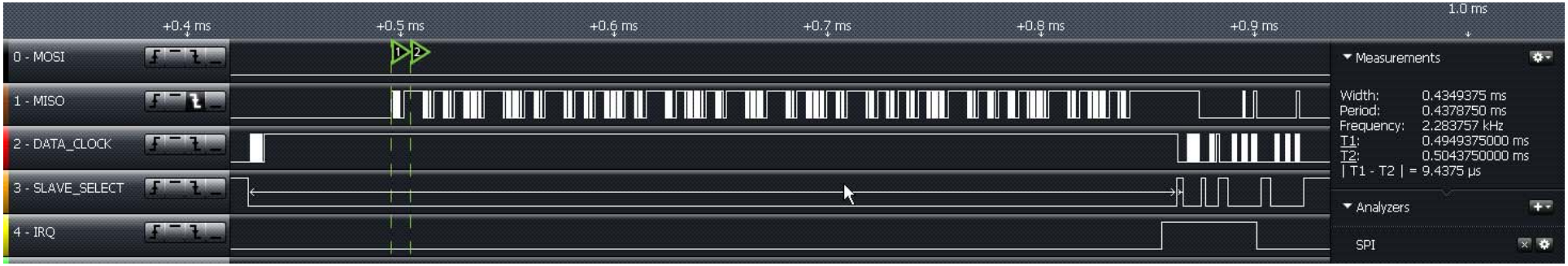
First TRF79xx RX Sequence on I/O_6 in DM0 for Mifare Authentication (cont., digital capture of previous slide)

- PICC is communicating back @ 106kbps (fc/128), so:
  - The following sequences are defined:
    - Sequence D: the carrier shall be modulated with the subcarrier for the first half (50 %) of the bit duration,
    - Sequence E: the carrier shall be modulated with the subcarrier for the second half (50 %) of the bit duration,
    - Sequence F: the carrier is not modulated with the subcarrier for one bit duration.
  - Bit coding shall be Manchester with the following definitions:
    - logic "1": Sequence D
    - logic "0": Sequence E
    - Start of Communication: Sequence D
    - End of Communication: Sequence F
    - No Information: No Subcarrier.
- T1:T2 cursors are ISO14443A PICC to PCD SOF (Sequence D)



First TRF79xx RX Sequence on I/O_6 in DM0 for Mifare Authentication (cont., digital capture of previous slide)

- Data is encrypted:

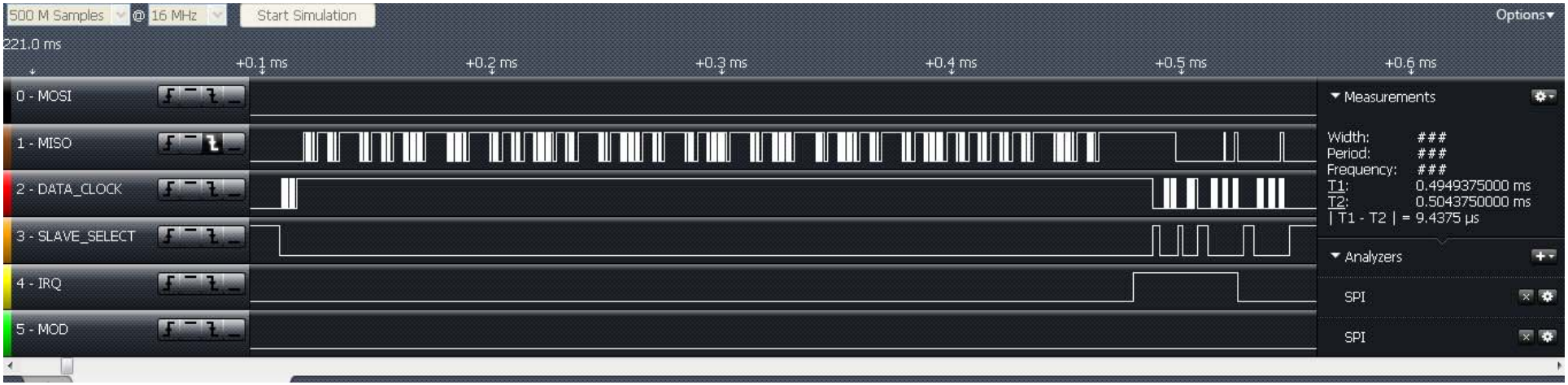


Second TRF79xx TX Sequence Out in DM0 for Mifare Authentication (analog)

- This is encrypted TX out.

Second TRF79xx RX Sequence on I/O_6 in DM0 for Mifare Authentication (cont., digital dapture of previous slide)

- This is encrypted RX in



Backup

EVM Screen Captures

- These captures illustrate sequence X, as taken from the TRF7960EVM

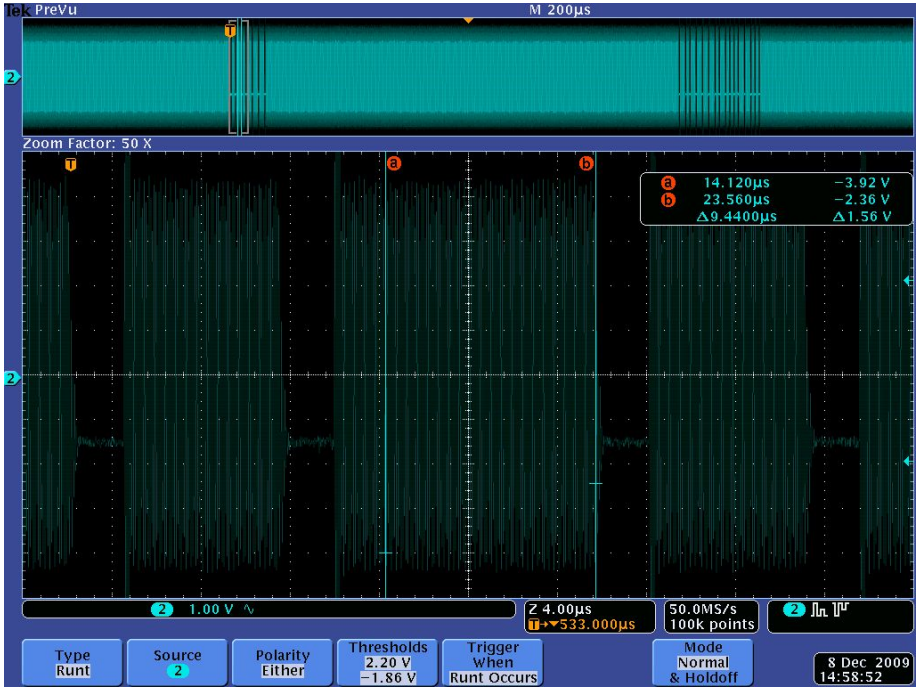
t_b = 9.44uSec

t_x = 4.72uSec

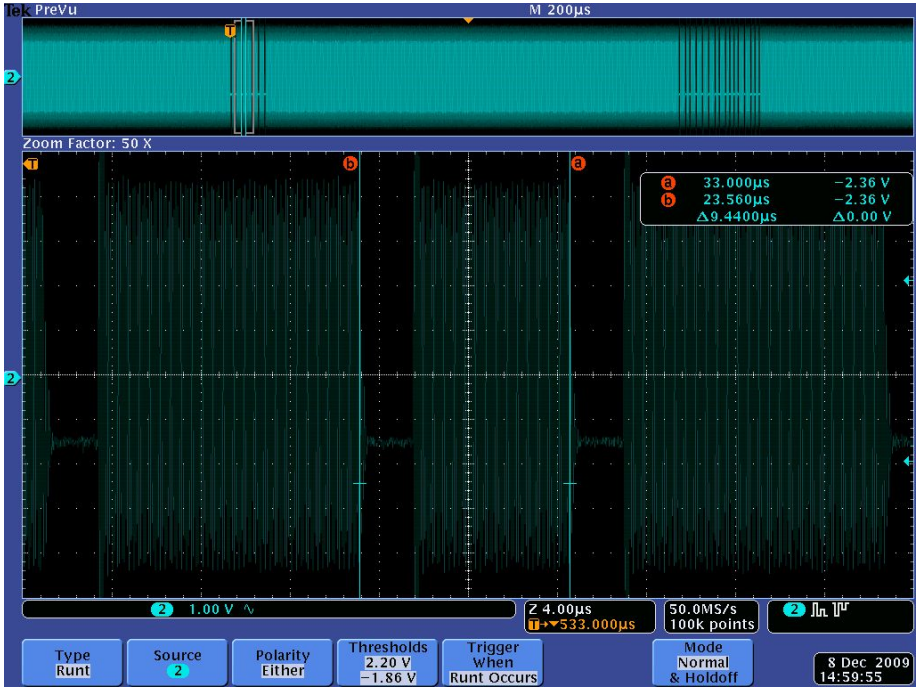
t_1 = 2.48uSec

EVM Screen Captures

- These captures illustrate Sequences Y and Z, as taken from the TRF7960EVM

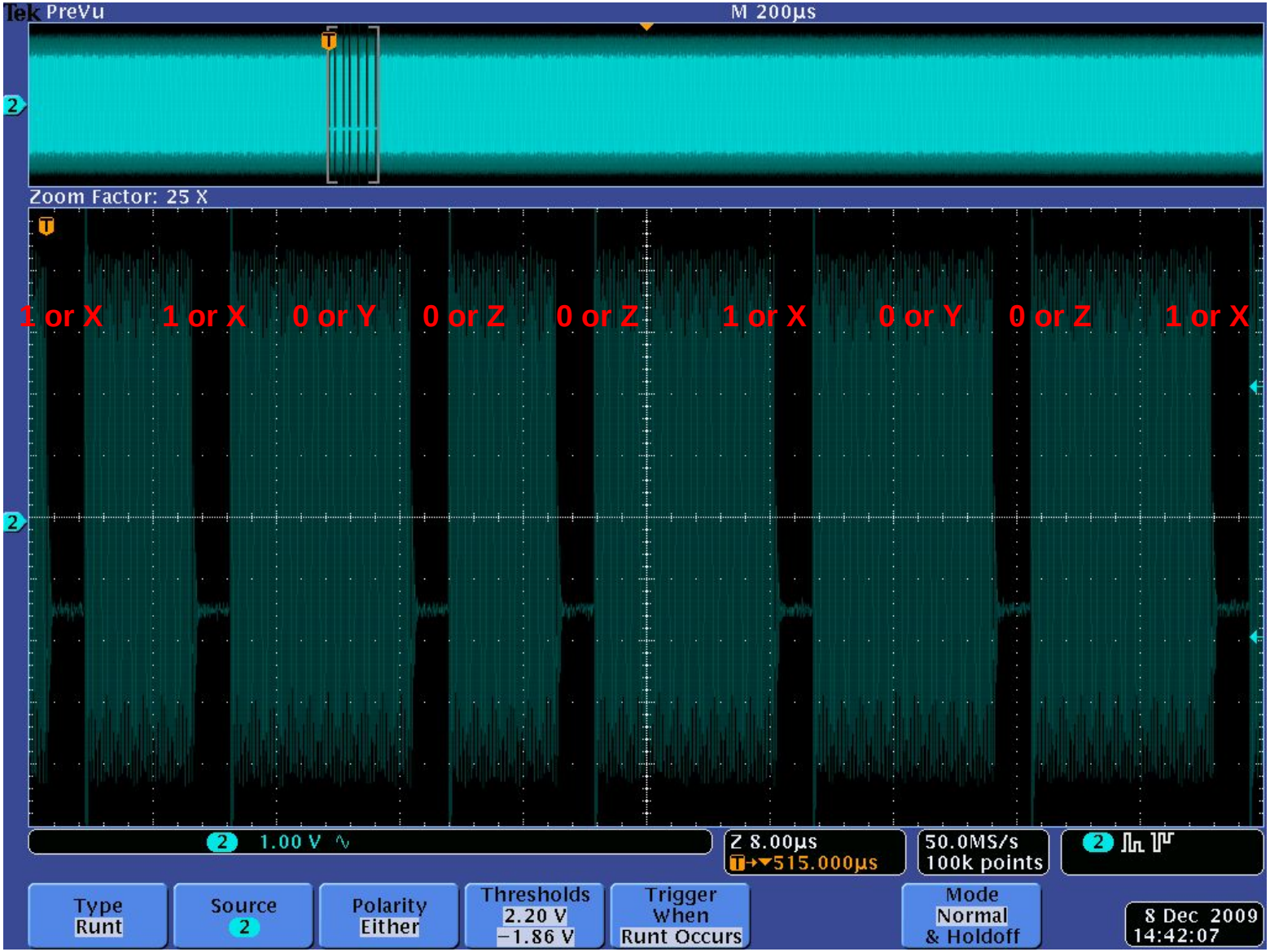


Sequence Y = Carrier for 9.44uSec



Sequence Z = Pause for 2uSec-3uSec, Carrier for Remainder of 9.44uSec

EVM Screen Capture Decoded



Data from GUI for Mifare Authentication

- 19:45:04.452--> 010E000304C0FFFFFFFFFFFF0000
- 19:45:04.749<-- 010E000304C0FFFFFFFFFFFF0000
- Crypto1 set key.
- Initialization ok

- 19:45:04.812--> 010F000304C160007EA6A6E29C0000
- 19:45:05.015<-- 010F000304C160007EA6A6E29C0000
- Crypto1 authentication step 1.
- Card nonce: D06530F3. Success

- 19:45:05.077--> 010C000304C2112233440000
- 19:45:05.312<-- 010C000304C2112233440000
- Crypto1 authentication step 2.
- Authentication ok. Success