EM4100 RFID Cloner Kit

This kit contains everything needed to build a low-frequency (125 kHz) EM4100 compatible device capable of cloning and replaying RFID tags. All of the documentation, hardware, and software is available on github: https://github.com/kbembedded/EM4100_Cloner
The whole device is controlled by a PIC16F684 microcontroller, which is pre-programmed. The software currently supports cloning of read-only LF RFID tags, a manual input of arbitrary IDs, and replaying the stored IDs to standard RFID transceivers. There are a total of 16 locations available to save IDs to or replay from.
If you have any issues, are missing parts, or just have questions, ask in the Hardware Hacking Village at DEF CON, or send an email to support@kbembedded.com

See the schematic and layout PDFs, located in the doc/ directory for more information about the circuit

Label	Description
R1	25 Ohm
R2, R3	100 Ohm
R4, R5, R6, R7	33 kOhm
R8, R10	7.87 kOhm
R9	1M Ohm
R11, R12, R13	130 kOhm
IC1	PIC16F684
IC2	LM258/LM358
S2	Slide Switch (mislabeled on PCB)
D1	1N4148 Signal Diode
C2, C4, C6, C9, C11	1 nF Ceramic
C3, C5, C10	4.7 nF Ceramic
C1, C8, C12, C13	10 nF Ceramic
C7	100 uF Aluminum, lay flat
BT1	CR2032 Battery Holder
S1	Push Switch
S3	DIP Switch
Q1	N-Chan. MOSFET (2106)
Q2, Q3	P-Chan. MOSFET (2104)
GRN	Green LED
RED	Red LED
J1	6-pin RA header (optional)

Notes about assembly:

IC1, IC2, S2, S3, C7, D1, GRN, RED, BT1 and Q1-Q3

- IC1 and IC2 have notches on the chip and the PCB that should match up
- S2 has the slider tab marked on the PCB to note orientation.
- S3 has a white dot on the upper-right corner and lines up with "S3"
- C7 has a white stripe on the negative (cathode) side of the capacitor. The capacitor must be mounted with the stripe opposite the "+" symbol.
- D1 must have the stripe on the component match the stripe on the PCB
- GRN & RED both have one leg shorter than the other; the shorter leg is the negative (cathode) leg and needs to line up with the flat side printed on the PCB.
- BT1 must be mounted with the concave circle closest to the edge of the PCB.
- Q1-Q3 must be mounted facing the same was as the silkscreen on the PCB

J1 is optional and can be used to reprogram the PIC

The backside of the PCB has 16 blocks of silkscreen that can be used to make notes about what IDs are saved in each of the save locations. Wet-erase and permanent markers work well in these blocks.

For S3, switch down is a binary 0, and switch up is a binary 1

Operation instructions:

The EM4100 cloner kit has three modes of operation: clone, replay, and manual input. The DIP switch is used as a way to select the location to save to, or read from. While the DIP switch has numbers on it, the numbers listed next to the "BIT" designator under the DIP switch are used to represent the bit values, i.e. leftmost switch is bit 3, and rightmost switch is bit 0.

Clone an RFID tag:

Slide S2 in to the "Clone" position and set the save location on the DIP switch. Warning! If an ID is successfully cloned, it will be written to this save location and will destroy the ID that was saved there previously! Hold down the button S1 and the red LED will light up. Bring the device near a 125 kHz RFID tag and when the tag is successfully read and saved, the red LED will turn off and the green one will turn on. You can now release the button and the cloner will go back to sleep.

Replay an RFID tag:

Slide S2 in to the "Replay" position and set the location on the DIP switch. This will replay the ID stored at the selected location. This mode is passive and the microcontroller will only wake up when another transceiver sends a 125 kHz carrier signal. Once a valid carrier signal is detected, the cloner will synchronize to it and continuously replay the ID in the selected location. Note that the PIC (and LF RFID in general) is extremely low power, and a device may still be able to be read while in "Replay" mode even with the battery removed.

Manually input a tag ID:

Slide S2 in to the "Replay" position and set the save location on the DIP switch. Warning! If an ID is successfully entered, it will be written to this save location and will destroy the ID that was saved there previously! Press and hold down the button S1 for 5 seconds and both LEDs will turn on. Release the switch and the green LED will turn off. The new ID to be saved is now input using the DIP switch, one nibble at a time, starting with the most significant nibble of the ID and moving right. Input the nibble to the DIP switch, press and release S1, and the LED will toggle from red to green when depressed, and back to red when released. This process is repeated 9 times for all 10 nibbles. If at any time while in this mode S1 is not depressed for 20 seconds, the cloner will go back to sleep and no changes will be made to the selected ID location.
For example, to input an ID of ABCDEF0123 to location 4:
Slide S2 to "Replay", set 4 on the DIP switch (0100), hold the button for 5 seconds until the LEDs turn on then release the button.
Set 0xA (1010) on the DIP switch, depress and release the button S1.
Set 0xB (1011) on the DIP switch, depress and release the button S1.
Set 0xC (1100) on the DIP switch, depress and release the button S1.
Repeat for all 10 nibbles of the ID

No touchy zone:

The analog signal detector circuit is capacitively sensitive and the additional capacitance that the body has will affect performance of the circuit if touched. The back of the PCB has a section that is outlined called the "No touchy zone." Be sure to not come in to contact with this section of the PCB on the back while operating the cloner as it will have an adverse affect.