Unique (EM4001) RFID Emulator

Michal Krumnikl
Media Research Lab, Department of Computer Science
VSB – Technical University of Ostrava

August 12, 2007

1 Unique (EM4001) RFID Emulator

Radio Frequency Identification (RFID) systems are widely used to identify, locate and track people, products or animals. These systems consists of the reader unit and a passive tag. The passive tag is composed of an antenna coil and chip with the memory. It is powered by the time varying electromagnetic field generated by the reader. This RF signal is called a carrier signal. The information stored in the tag is transmitted to the reader by altering the electromagnetic field of the reader.

Many companies and organizations are using RFID card to control access to buildings and offices. An employee holds their card near the reader, unique identification read from the card, is checked against the database of persons allowed to enter and then the doors are opened or not.

This article shows the security risks of using one type of RFID chips for such authentication purposes - Unique chips. They are not supposed to be used in such applications, but security features are often overlooked. Security and privacy aspects of RFID systems are described in articles listed by G. Avoine[3]. We will show how easy is to sniff the Unique identification and replicate the identification card.

1.1 Tag operation

The reader is generating an RF carrier sine wave, detecting modulation anomalies. Detected modulation on the field would indicate the presence of a tag.

Inductively coupled transponders are almost always operated passively. When the tag enters the RF field generated by the reader it will charge the inner capacitor from the induced current in the coil. When it has sufficient energy to operate, it divides the carrier and begins clocking its data to an output transistor, which is connected to the coil inputs. Shutting the coil causes field fluctuation, which can be seen as a slight change in amplitude of the carrier. The reader detects these amplitude modulated data and process the resulting bitstream according to the modulation and encoding pattern.

The example of modulation pattern is shown on Figure 1, representing the amplitude modulation (voltage drop) of the signal. In such way, we can intercept the communication with RFID tags by measuring the distortions in electromagnetic field. This can be done by using appropriate tuned LC circuit connected

to the signal recording device. Such device is capable to intercept the RFID communication even behind the wall on that the RFID reader is mounted.

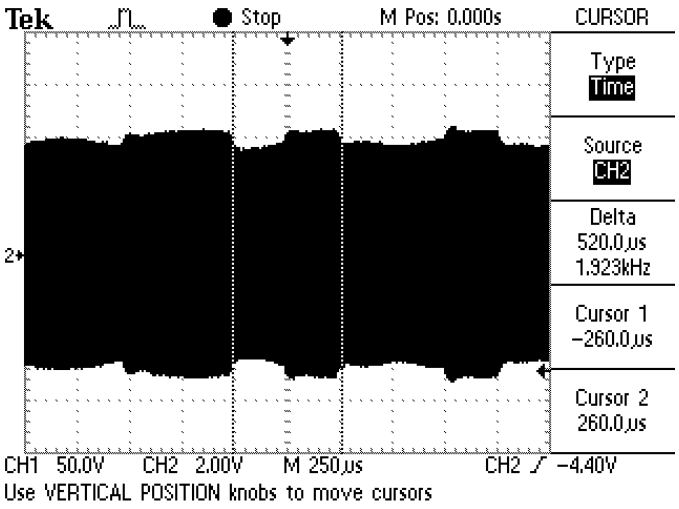

Figure 1: Oscilogram of Voltage on RFID Coil

1.1.1 Unique (EM4001) Tags

Unique is a contactless transponder. The output data contains a 9 bit header, 40 bits of data, 14 parity bits, and a stop bit. The way to modulate the output data uses Manchester coding[1], with a bit rate corresponding to 64 cpb (carrier cycles per bit). General features of Unique cards are :

- 125 kHz carrier,
- ASK modulation,
- Manchester coding,
- 40 bits for ID.

Unique data are encoded in the 64 bits according to the following scheme (see Table 1). The message header consists of nine `1` bits for the header. D0 – D40 are user data bits storing the unique 5 byte id of the chip. PR0 – PR9 are row parity bits, PC0 – PC3 are column parity bits. This system is using even parity. The last bit is the stopbit set to `0`. The chip is transmitting data as long as it is in the range of readers field.

1.2 Emulator design

RFID emulator is based on cheap Atmel microcontroller. The processor used for the tag emulator is ATMega8 operating at 4 MHz. It handles the Manchester encoding and transmits the encoded data to output transistor connected to the

[1]Manchester encoding has a level change at the middle of every bit clock period. This method is used to embed clocking information to help synchronize the reader to the bitstream.

1	1	1	1	1	1	1	1	1
				D0	D1	D2	D3	**PR0**
				D4	D5	D6	D7	**PR1**
				D8	D9	D10	D11	**PR2**
				D12	D13	D14	D15	**PR3**
				D16	D17	D18	D19	**PR4**
				D20	D21	D22	D23	**PR5**
				D24	D25	D26	D27	**PR6**
				D28	D29	D30	D31	**PR7**
				D32	D33	D34	D35	**PR8**
				D36	D37	D38	D39	**PR9**
				PC0	**PC1**	**PC2**	**PC3**	0

Table 1: Unique Chip Memory Organization

LC circuit tuned to 125 kHz. The circuit diagram as shown in Figure 2 is simple, LC circuit consists of $162\mu H$ coil and $10nF$ capacitor chosen according to the equation

$$f = \frac{1}{2\pi}\sqrt{\frac{1}{LC}}. \tag{1}$$

In case of values mentioned above, the frequency of the LC circuit is approximately 124 kHz. When the transistor is off, the circuit is tuned and when it is on, the circuit is detuned, interfering the carrier frequency.

The coil used during the experiments was N–turn multilayer circular coil. Its inductance can by calculated by

$$L = \frac{0.31(aN)^2}{6a + 9h + 10b}(\mu H), \tag{2}$$

where a is average radius of the coil in cm, N is number of turns, b is winding thickness in cm and h is winding height in cm. Antennas designs are described in Microchip application notes[2].

In order to emulate 64 cpb Manchester tag we need to generate $256\mu s$ pulses[2] according to Manchester encoding scheme. The proper switching is maintained by internal counter every $256\mu s$, the data bits are shifted in $512\mu s$ intervals (twice the counter time, because of Manchester encoding).

Microcontroller transmits 64 bits of RFID data in infinite loop.

1.3 Conclusion

Building an Unique RFID transponder is not complicated and even not expensive. The circuit presented here makes possible to store several RFIDs and switch them according the need or make a series generator that will try all possible combinations. One RFID is transmitted in $32.768ms$, in order to transmit all possible combinations we would need 1142 years. But in case we know the first three bytes (which is not improbable, because cards are usually issued in

[2] 125 kHz carrier has a cycle $8\mu s$ in length, so 64 cpb means $64 * 8 = 512\mu s$ per bit.

big series with incremented ids) we will need 152 hours. In such situations it is unacceptable to have security based on such simple RFID chips. More secure types of RFIDs are needed to ensure higher safety level.

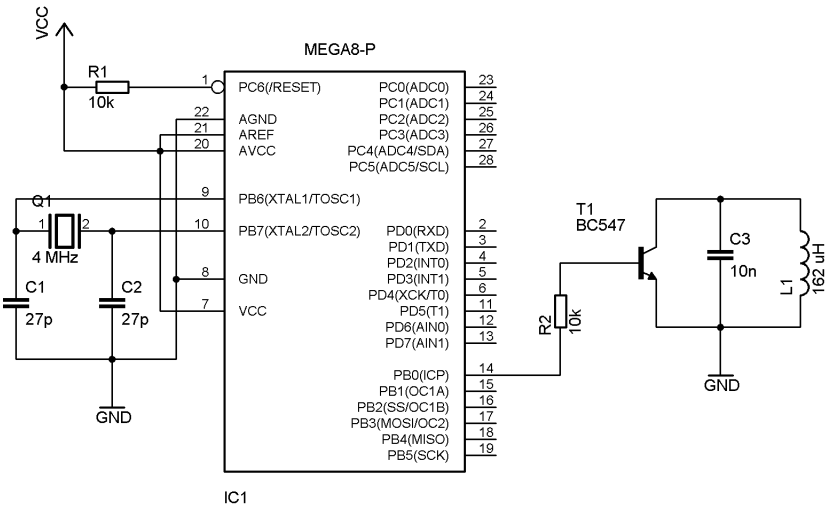

Figure 2: RFID Unique Tag Emulator Diagram

References

[1] P. Sorrells, *Passive RFID Basics (AN680)*, Microchip Technology Inc.

[2] Y. Lee, *Antenna Circuit Design (AN710)*, Microchip Technology Inc.

[3] G. Avoine, *Security and Privacy in RFID Systems*, http://lasecwww.epfl.ch/ gavoine/rfid/index.html

[4] J. Westhues, *Proximity Cards*, http://cq.cx/prox.pl

[5] *EM9928 125 KHz Desktop Card Reader Datasheet*