

# Digital implementation of a demodulator for HF RFID reader device

Tilen Svete, Anton Pleteršek

Tehnološki park 21, Ljubljana, Slovenia

**Abstract:** This paper presents a demodulator for high frequency radio frequency identification (HF RFID) signals based on the Costas loop [1]. A description is presented of how correlation between two signals can be simplified in terms of the operations involved and implemented using a digital Costas loop [2, 3]. After carrier direct down conversion and bandpass filtering, the proposed demodulator is used to demodulate the subcarrier signal. A brief description is given of the signal characteristics of HF RFID signals at a carrier frequency of  $f_c = 13.56$  MHz and the operation of the subcarrier demodulator. Packet error rate (PER) measurement results are presented for protocols ISO/IEC 14443 type A and type B at a bitrate  $f_c/128$  (approximately 106 kbit/s), FeliCa at  $f_c/64$  (approximately 212 kbit/s), and ISO/IEC 15693 at  $f_c/512$  (approximately 26.48 kbit/s). A comparison between the measured PER results and the theoretical BPSK PER limit is presented. Also shown is the comparison with a HF RFID reader integrated circuit ST25R3911 [4], where an almost 11 dB improvement in PER performance for ISO/IEC 14443 type B  $f_c/128$  was achieved.

**Keywords:** HF RFID reader; digital demodulator; correlation; Costas loop; packet error rate

## Digitalna implementacija demodulatorja za HF RFID izpraševalnik

**Izveček:** V tem članku predstavimo demodulator za visoko frekvenčno radiofrekvenčno identifikacijo (HF RFID) na osnovi Costas-ove zanke [1]. Opišemo poenostavitev korelacije med dvema signaloma na osnovi vpletenih operacij in implementacijo z uporabo Costas-ove zanke [2, 3]. Po direktnemu mešanju nosilca navzdol in pasovno prepustnem filtriranju uporabimo predstavljen demodulator za demodulacijo podnosilnega signala. Po kratkem pregledu karakteristik signalov na področju HF RFID pri nosilni frekvenci  $f_c = 13,56$  MHz, opišemo delovanje demodulatorja in njegovo delovanje preizkusimo z meritvami pogostosti paketnih napak (angl. packet error rate ali PER). Predstavimo rezultate PER meritev za protokole ISO/IEC 14443 tip A in B pri podatkovni hitrosti  $f_c/128$  (približno 106 kbit/s), FeliCa pri hitrosti  $f_c/64$  (približno 212 kbit/s) in ISO/IEC 15693 pri hitrosti  $f_c/512$  (približno 26,48 kbit/s). Naredimo primerjavo med izmerjenimi vrednostmi in teoretičnimi mejami za kodiranje bitov, ki se uporablja v naštetih protokolih. Prav tako za protokol ISO/IEC 14443 tip B podatkovne hitrosti  $f_c/128$  naredimo primerjavo z integriranim vezjem HF RFID izpraševalnika ST25R3911 [4], kjer smo dosegli skoraj 11 dB izboljšavo v PER zmogljivostih.

**Ključne besede:** HF RFID izpraševalnik; digitalni demodulator; korelacija; Costas-ova zanka; pogostost paketnih napak

\* Corresponding Author's e-mail:tilen.svete@st.com

### 1 Introduction

In HF RFID a reader and a contactless card or tag form a master/slave communication setup. The reader generates the magnetic field required to both power and communicate with the tag. The tag extracts power from its antenna to supply itself and uses antenna load modulation to answer reader commands. The tag modulates the carrier signal with a subcarrier signal, where the subcarrier frequency is defined as the carrier frequency divided by a whole number (e.g. 16, 32 or 64). The changes in the load of the tag antenna can be seen

by the reader as either changes in carrier field amplitude or phase or both, depending on distance, orientation, and other parameters of the reader-tag antenna system (resonance frequencies, quality factors, etc.).

In the reader receiver the carrier is down converted using direct down conversion. After amplification and bandpass filtering to remove DC and higher order components of conversion, only the frequency band which holds the subcarrier signal remains. Bit information is encoded in the phase or the amplitude of the subcar-

rier signal, so a reliable means of extracting the information is required.

In the field of HF RFID, Y.-H. Kim, M.-W. Seo, Y.-C. Choi, and H.-J. Yoo [5] have proposed and implemented a receiver architecture where a comparator with selectable detection threshold is used to digitize the subcarrier signal after carrier direct down conversion and band-pass filtering. The burden of bit recognition thus falls with the decoding circuit following the comparator. This implementation is simple and effective, but suffers from rapidly degrading noise performance. In addition, any damage to the signal by external interferers or effects of the reader-tag antenna system can cause the comparators to output dubious pulses that are hard to interpret correctly by the decoder. Bit duration and subcarrier presence detection can also suffer as a result.

H. Min, Y. Liu, and C. Huang [6] have proposed digital correlation based receivers for RFID, but focused on the ultra-high frequency (UHF) RFID domain (from 860 MHz to 960 MHz). Their implementation consumed a large amount of hardware (12 parallel correlator banks) to tackle the problem of large frequency deviations present in UHF tag replies, due to the nature of tag operation at such frequencies.

In the HF RFID domain, C. Angerer [7] presented a receiver structure that used an integrator as a simple rectangular pulse correlator and algorithm for synchronization. While their results show good performance, their work is based on the EPC global HF standard.

The demodulators in the listed papers are based on classical implementations of correlators as a finite impulse response or FIR filter, where coefficients represent the signal being searched for.

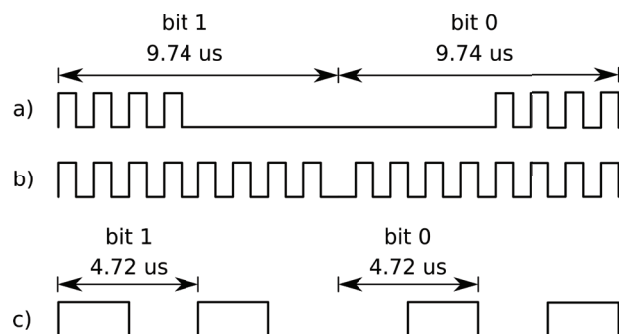
This paper presents a demodulator based on the Costas loop that uses simplified correlation to extract phase and amplitude information from the subcarrier signal. The demodulator was implemented in the digital domain so testing could be done on a field-programmable gate array (FPGA) development board. The output of the demodulator is a bit stream that holds information about the subcarrier phase or amplitude. An additional output is a signal indicating the start of a data packet or presence of signal collisions due to multiple tags responding at the same time. The subcarrier demodulator performs simplified correlation to extract bit information from the phase or amplitude of the subcarrier. An advantage of the demodulator presented in this work over classical implementations using multiplier-accumulators is that reception of HF RFID signals can be made robust against variations in subcarrier frequency or phase (for example due to active

tag transmission). Additional benefits come from the ability of the architecture of the demodulator to support different data rates with the same hardware and easy scalability in terms of desired performance. A brief comment on this is at the end of section 3.

First, a brief overview of the signal characteristics in the HF RFID field is presented in section 2. Next, the demodulator design and operation are described in section 3. The hardware implementation and measurement setup are presented in section 4. In section 5, the theoretical reception limits for HF RFID protocols are defined. The packet error rate measurement results for protocols defined in standards ISO/IEC 14443, ISO/IEC 15693 and JIS X – 6139 (FeliCa) at their base data rates are presented in section 6.

## 2 Signal characteristics

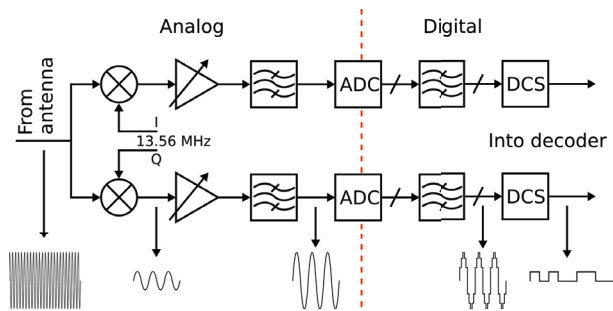
Standards ISO/IEC 14443, ISO/IEC 15693 and JIS X – 6139 (FeliCa) describe protocols used in HF RFID and NFC (Near Field Communications – a rapidly growing subdomain of HF RFID, popular in mobile devices). The protocols share similarities with each other, which can be used in the design of the demodulator.



**Figure 1:** Bit coding of HF RFID protocols

Figure 1 shows the bit coding for a) ISO/IEC 14443 type A  $f_c/128$  and b) ISO/IEC 14443 type B  $f_c/128$ , where the subcarrier frequency is 847.5 kHz. At the bottom of figure 1, c) shows FeliCa  $f_c/64$ , where the subcarrier frequency is 211.875 kHz. Not shown is the bit coding for ISO/IEC 15693  $f_c/512$ , which uses Manchester coded subcarrier, like in a), but with 8 periods of 423.75 kHz subcarrier followed by 8 periods of no subcarrier for bit 1, for a total bit length of approximately 37.76 μs. One can notice that there are two types of coding schemes, Manchester and BPSK. The demodulator design is accordingly divided into two parts: reception of BPSK coded subcarrier and reception of Manchester coded subcarrier. Both use the same hardware, but with different settings.

### 3 Demodulator design and operation



**Figure 2:** Block schematic of a HF RFID reader receiver

Figure 2 shows the reception path of a HF RFID reader. The carrier signal from the antenna is first directly down converted. The conversion result is then amplified and bandpass filtered to remove the DC component and to remove high frequency components. The end result are I and Q channels with a subcarrier signal, ready to be converted to digital signals by analog to digital converters (ADCs). The digital signals are further bandpass filtered to remove unwanted spectral images and to more accurately define the bandwidth (BW). At this stage in the reception chain, there is a digitized subcarrier signal with a bandwidth of twice the data rate, in case of BPSK, or four times the data rate, in case of Manchester code. The proposed demodulator (digital correlation system or DCS) is used at this stage to convert the subcarrier signal into a baseband signal, to provide filtering (as ideal correlation does), and to perform symbol and packet start recognition.

$$(f * u)(\tau) = \int_{-\infty}^{\infty} f^*(\tau) u(t + \tau) dt \quad (1)$$

Equation 1 describes correlation between two signals, where  $f$  is a signal in which the pattern  $u$  is searched for. In the above equation,  $f^*$  is the complex conjugate of signal  $f$ . In our case,  $f^*$  is the digitized subcarrier signal that is compared to a known sample  $u$ . A local subcarrier clock can be used as signal  $u$ . In this way the subcarrier signal, or more accurately its frequency or phase, can be compared with the local subcarrier clock's frequency or phase. The operation of correlation can be divided into three main parts: multiplication, time or phase adjustment, and integration or averaging.

The subcarrier signal is mixed with two local subcarrier clocks in 90 degree phase relation between them, effectively performing direct quadrature conversion. The I channel subcarrier signal is thus split into I and Q sub-channel baseband signals. The same operation is performed on the Q channel subcarrier signal. Because the clocks are single-bit signals and the digitized subcarrier is a multi-bit signal, the operation of multiplication can

be reduced to an operation of inversion and addition (sign change in a number represented in two's complement representation). When the clock is '1' the subcarrier amplitude is unchanged and when the clock is '0' the sign of the subcarrier amplitude is inverted.

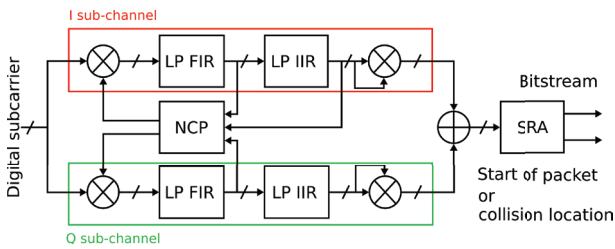
The phase of the I sub-channel clock is corrected to match the phase of the subcarrier signal. Naturally, the phase relationship between I and Q sub-channel clocks is kept constant. When phase lock between the subcarrier signal and I sub-channel clock is achieved, mixing is effectively reduced to full wave rectification of the subcarrier signal. The I sub-channel holds all the information about the phase of the subcarrier, while the combination of I and Q sub-channels determines in which way to correct the phase. To remove noise and higher order components of mixing, the signal is filtered with both a finite impulse response (FIR) and infinite impulse response (IIR) digital filters. Decimation can be employed before the IIR filter to reduce its size. The FIR filter removes the exact higher order frequencies of mixing, while the IIR filter removes noise and provides a frequency characteristic that closely follows the spectrum of the data in the base band. In this setup, classical correlation is replaced by mixing, phase correction and filtering (a Costas loop). The added benefit over classical correlation is being able to control the phase and frequency of the local subcarrier clock (signal  $u$ ) and thus use the same structure to demodulate signals with varying subcarrier phase or frequency throughout the data packet.

Another advantage is the ability to be able to freely set the cutoff frequency of the IIR low pass filters to match the spectrum of the data packet without the need to change the structure of the demodulator. ISO/IEC 14443 type A and B high bitrates have identical bit coding (BPSK coded  $f_c/16$  or 847.5 kHz subcarrier), but slightly different data packet structure. At  $f_c/64$  kbit/s 4 subcarrier periods are used to represent a bit, 2 subcarrier periods are used at  $f_c/32$  kbit/s and 1 subcarrier period at  $f_c/16$  kbit/s. The spectrum of the input subcarrier signal changes with data rate, so the cutoff frequency of the IIR filters can be adjusted accordingly while using the same topology and hardware.

The disadvantage is the need for a pilot tone in the subcarrier signal, so the loop has time to achieve phase lock. However, all HF RFID BPSK protocols have long pilot tones (>20 subcarrier periods).

Figure 3 shows the basic structure of the proposed subcarrier demodulator. The symbol recognition algorithm (SRA) block tracks the demodulator output signal and performs symbol recognition and start of packet detection for BPSK coded protocols or collision detec-

tion for Manchester coded protocols. The numerically controlled phase (NCP) block controls the phase of the I and Q subcarrier clocks. Only the signs of the multi-bit signals from the filter outputs are used, as only one phase correction of fixed size is possible per subcarrier period. As such, the time in subcarrier periods the loop takes to achieve phase lock (or approximate phase lock), depends on the phase correction resolution. In the case of ISO/IEC 14443 type B  $f_c/128$  kbit/s, a main clock frequency of  $f_c=13.56$  MHz is used. The subcarrier frequency is  $f_c/16$  or 847.5 kHz. This means that there are 16 samples for every subcarrier period. The size of the phase correction is one sample, or 1/16 of the subcarrier period, which means that the phase corrections are coarse, but sufficient for successful demodulation of the subcarrier signal. Ideally, it takes 4 phase corrections at most to align the I subcarrier clock phase to the input subcarrier phase. With excessive noise it can take longer. Phase corrections are disabled when a phase change is occurring on the subcarrier signal so a false phase correction does not occur.

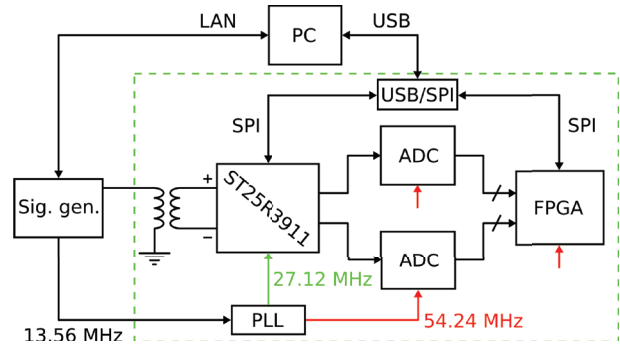


**Figure 3:** Block diagram of the proposed demodulator

The architecture can easily be scaled if size is a limitation, at the cost of performance. For example, the area of the IIR low pass filters can be reduced by reducing the filter order or increasing the ratio between the filter sampling frequency and cutoff frequency. The cost for this is worse noise attenuation and, as a result, worse noise performance.

### 4 Hardware implementation

The demodulator was implemented on a field-programmable gate array (FPGA) development board for debugging and testing purposes. Since only the digital part of the receiver could be implemented on a FPGA, the analog front end (AFE) and ADCs were implemented with separate ICs, as shown in figure 4. For the AFE, the reader IC ST25R3911 was used. The IC was configured into a test mode, where the AFE outputs were available on its output pins. ADCs were used to sample the AFE outputs and relay their data to the FPGA. This way, a direct comparison between the proposed demodulator and ST25R3911 was possible.



**Figure 4:** Measurement setup block diagram

### 5 Packet error rate theoretical limits

To have an absolute benchmark to compare with measurement results a theoretical limit of the bit error rate (BER) or packet error rate (PER) for HF RFID protocols is needed. We derive the theoretical limit from [8].

$$E_b = V_{Srms}^2 T_b \tag{2}$$

$$N_0 = \frac{V_{Nrms}^2}{BW} \tag{3}$$

$$BER_{BPSK} = \frac{1}{2} \operatorname{erfc} \left( \sqrt{\frac{E_b}{N_0}} \right) \tag{4}$$

$$PER = 1 - (1 - BER)^l \tag{5}$$

Equation 2 describes the energy per bit  $E_b$  in relation to the signal *rms* voltage  $V_{Srms}$  and the bit duration  $T_b$ . Equation 3 describes the noise power spectral density  $N_0$  in relation to the noise *rms* voltage  $V_{Nrms}$  and the bandwidth of the noise  $BW$ . Equation 4 shows the ideal performance of BPSK coded protocols, such as ISO/IEC 14443 type B. Equation 5 shows the relation between the bit error rate and packet error rate for a given packet length of  $l$  bits. Bit length  $l$  needs to hold the number of all bits that need to be received successfully in order for the packet to be received successfully, as standard HF RFID data packets do not include error correcting codes. Special symbols, start, stop, parity, and CRC bits all need to be included. The longer the data packet, the less likely it will be received correctly in its entirety in a noisy environment.

This limit only takes into account the errors that arise from bit errors in the presence of noise, but not the errors that occur when packet start or end are not detected due to noise. However, the limit is very useful since it represents an absolute marker unrelated to demodulator architecture, against which demodulator

performance can be compared. The smaller the difference between the measured and the theoretical limit, the better the performance of the demodulator is.

A similar formula can be written for Manchester coded protocols:

$$BER_{Manchester} = \frac{1}{2} \operatorname{erfc} \left( \sqrt{\frac{E_b}{8N_0}} \right) \quad (6)$$

Equation 6 describes the ideal performance of Manchester coded protocols, such as ISO/IEC 14443 type A for a data rate of  $f_c/128$  kbit/s. Compared to equation 4, we have a factor of 8 present in the denominator of the fraction inside the square root. This factor is the result of differences between Manchester code and BPSK. It stems from the need to correctly recognize both bit halves and a smaller distance between bit symbols in the constellation diagram for Manchester coded signals. Interestingly, ISO/IEC 14443 type A  $f_c/128$  kbit/s has the same theoretical PER as type A  $f_c/16$  kbit/s (type A data rates larger than  $f_c/128$  kbit/s are BPSK coded), which demonstrates the superior robustness of BPSK compared to Manchester code with regards to noise.

Table 1 shows the  $E_b/N_0$  (energy per bit to noise power spectral density ratio or SNR per bit) values in dB for 10 % PER for all protocols and data rates for data packets 10 bytes long (8 data and 2 CRC bytes).

**Table 1:** Theoretical 10 % PER limits for a 10 byte long data packet for various HF RFID protocols and data rates.

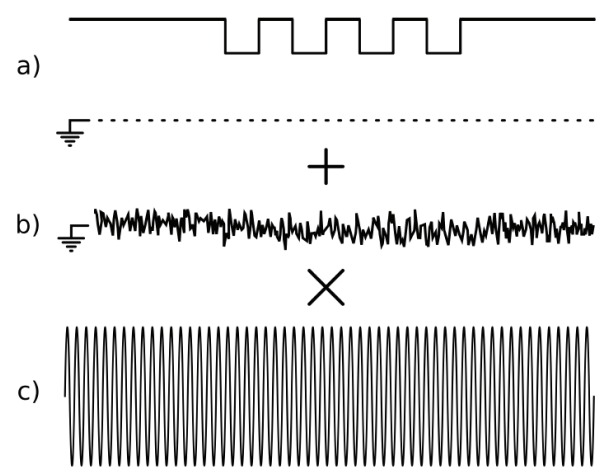
Protocol	Data rate [kbit/s]	10 % PER $E_b/N_0$ [dB]
ISO/IEC 14443 type A*	$f_c/128$	12.69
ISO/IEC 14443 type A	$f_c/64$	6.67
ISO/IEC 14443 type A	$f_c/32$	6.67
ISO/IEC 14443 type A	$f_c/16$	6.67
ISO/IEC 14443 type B	$f_c/128$	6.91
ISO/IEC 14443 type B	$f_c/64$	6.91
ISO/IEC 14443 type B	$f_c/32$	6.91
ISO/IEC 14443 type B	$f_c/16$	6.91
ISO/IEC 15693*	$f_c/2048$	12.68
ISO/IEC 15693*	$f_c/512$	12.68
FeliCa	$f_c/64$	6.78
FeliCa	$f_c/32$	6.78

When comparing different protocols from table 1, one can observe the difference in  $E_b/N_0$  the data structure and bit coding make. Protocols marked with an asterisk \* have Manchester coded bits, whereas the rest are BPSK coded. The difference between Manchester

code and BPSK result is 6.02 dB, as can be seen when comparing ISO/IEC 14443 type A  $f_c/128$  kbit/s and  $f_c/64$  kbit/s (same data structure, different bit coding).

## 6 Measurement results

The testing of the performance of the demodulator was done with PER measurements. For each SNR value a number of noisy packets were sent and the success rate of reception measured.

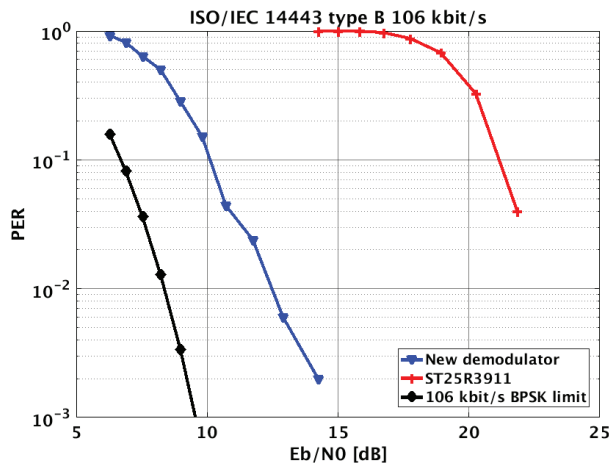


**Figure 5:** Sketch of the test pattern generation procedure.

Figure 5 shows the three steps in test pattern generation. First, a modulation signal with the correct packet structure was created, as shown in a). Then, band limited additive white Gaussian noise (AWGN) was added, as shown in b). The noise BW was 5 MHz while  $N_0$  was determined by the desired SNR value (equation 3). The noise BW was selected so it encompassed the entire BW of the data spectrum and usable frequency range of the AFE. The noisy modulation signal was then scaled and used to modulate a 13.56 MHz carrier, as shown in c). The test pattern generation was done in a Python script and uploaded to the signal generator to be fed into the device under test.

An external clock source supplied a clock signal synchronous to the carrier field. The gain of the AFE was reduced to avoid adding more noise to the packets by any other noise sources (thermal and 1/f noise in the receiver, oscillator phase noise in the waveform generator). This was done to ensure the artificially generated noise was indeed the dominant noise source. The modulation signal was appropriately scaled, so that the signal levels at the ADC inputs were at nominal levels. Each packet had length of 8 data bytes, 2 cyclic redundancy

check (CRC) bytes, and packet structure as defined in ISO/IEC 14443 for type B at a data rate of  $f_c/128$  kbit/s. Two sets of measurements were done, first on the FPGA development board with the proposed demodulator and later on the HF RFID reader IC ST25R3911.



**Figure 6:** Packet error rate measurement results and the theoretical 106 kbit/s BPSK PER limit.

Figure 6 shows the PER versus the  $E_b/N_0$  value in dB for both sets of measurements. For each data point 500 packets were sent. Figure 6 also shows a 3.1 dB difference between the theoretical limit and measured results at the 0.1 PER mark (10 % fail rate). Also shown is an almost 11 dB improvement compared to the HF RFID reader IC ST25R3911.

Similar results were obtained with other protocols at their base data rates as shown in table 2.

**Table 2:** PER measurement comparison for various protocols.

Protocol	Data rate [kbit/s]	10 % PER $E_b/N_0$ [dB]	Diff. to limit [dB]
ISO/IEC 14443 type A	$f_c/128$	15.7	3.0
ISO/IEC 14443 type B	$f_c/128$	10.2	3.1
ISO/IEC 15693	$f_c/512$	19.1	6.4
FeliCa	$f_c/64$	9.2	2.4

## 7 Conclusion

This paper presented a HF RFID demodulator based on a Costas loop for reception of protocols defined in ISO/IEC 14443, ISO/IEC 15693 and JIS X 6139. Demodulator design and operation were described. PER measurement results for ISO/IEC 14443 type A and B  $f_c/128$

kbit/s, FeliCa  $f_c/64$  kbit/s, and ISO/IEC 15693 single subcarrier  $f_c/512$  kbit/s along with theoretical limits were presented. PER measurement results for ISO/IEC 14443 type B  $f_c/128$  kbit/s showed good performance in noisy environment compared to theoretical  $f_c/128$  kbit/s BPSK PER limit, where a 3.1 dB difference was observed. The difference between the theoretical limit and measurement results can be explained by the fact that the theoretical limit does not include the probability of errors in packet start or end detection, but only the probability of bit errors. Improvements in demodulator design reduce this difference. The theoretical limit serves as an absolute marker against which demodulator performance can be compared. Additionally, an almost 11 dB improvement was observed compared to HF RFID reader ST25R3911 for protocol ISO/IEC 14443 type B  $f_c/128$  kbit/s.

## 8 References

1. J. Costas, "Synchronous Communications," *Proceedings of the IEEE*, vol. 44, p. 1713-1718, 1956.
2. B. Shamla, K. G. Gayathri Devi, "Design and Implementation of Costas loop for BPSK Demodulator," *India Conference (INDICON), 2012 Annual IEEE*, Kochi, 2012.
3. P. Shachi, Rahul Mishra, Ravi Kumar Jatoth, "Coherent BPSK Demodulator using Costas Loop and Early-Late Gate Synchronizer," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, 2013.
4. STMicroelectronics, "ST25R3911 NFC/HF Reader IC." Available: <http://www.st.com/en/nfc/st25r3911.html>.
5. Y.-H. Kim, M.-W. Seo, Y.-C. Choi, H.-J. Yoo, "A 13.56 MHz Receiver SoC for Multi-Standard RFID Reader," *Electron Devices and Solid-State Circuits*, 2008.
6. H. Min, Y. Liu, C. Huang, "Digital Correlation Demodulator Design for RFID Reader Receiver," *Wireless Communications and Networking Conference*, 2007.
7. C. Angerer, "A Digital Receiver Architecture for RFID Readers," *Symposium on Industrial Embedded Systems*, 2008.
8. John G. Proakis, M. Salehi, *Digital Communications*, Fifth edition. McGraw-Hill, 2008.

Arrived: 31. 05. 2018

Accepted: 26. 06. 2018