A Resistance Deviation-to-Time Interval Converter and its Application to a Passive RFID Tag for Security

Jimann Park, Youngsoo Park, Youngsae Kim, Sungik Jun
Wireless security application research team
ETRI
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-700
KOREA
http://www.etri.re.kr

*Abstract:*A passive RFID tag with security and measurement concepts is presented. The sensor interface module has a resistance deviation-to-time interval converter. The passive RFID tag embedded with a converter is described. A prototype RFID tag using a converter has been built with CMOS 0.35um technology. The experimental results have shown that the tag has an 8 bits resolution and a linearity characteristic when the output pulse is counted by a 3.39 MHz clock. The proposed converter is insensitive to the pulse width change regardless of environment changes. The design principle and the circuit configuration are simple. The proposed converter is expected to find wide applications in the signal processing of various sensors.

Key words – RFID tag, RFID application, security, sensor signal processor, converter, analog circuit.

1 Introduction

The most of Radio frequency identification (RFID) system using a sensor is applied for the instrument and measurement, and the commercial sensor tags are used at the simple work level of measurement parts. An RFID tag including a sensor function has been developed and it is presented a passive RFID tag chip embedded with a sensor interface module without battery.[1]-[2] The RFID tag for their applications can be performed the sensor with the resistance characteristics. Many resistive sensors produce small resistance variations with relatively large fixed offset resistance and sometimes need temperature compensation. The properties of resistive sensors have made resistance deviation-to-digital conversion techniques a very useful approach for implementing interface circuitry. These circuits are implemented a various analog-to-digital (A/D) converter. [3]-[5]

On the other hand, the RFID systems have the security functions in a various parts. Most security RFID systems implement a digital signal processor based on the crypto algorithm. In order to improve the above mentioned function, the RFID system in this paper is realized a sensor interface circuit using a resistance deviation-to- time interval converter and its applications to a security RFID tag. The passive RFID tag in this paper plays a role in security and measurement systems, and resistive sensors can have small or large resistance variations according to applications. This paper describes a simple resistance deviation-to-time interval converter based on continuous-time ramp integration and digital time differentiation. The converter is expected to find wide applications in the signal processing of various sensors for security and measurement RFID tags.

2. Circuit Description and Operation

2.1 Security Method

Fig. 1 shows the block diagram of a passive RFID tag embedded with a crypto and sensor interface module. It consists of an antenna, a radio frequency analog module (RFA), a radio frequency digital (RFD) protocol module, a control module, a crypto module, a sensor interface module, and memory.

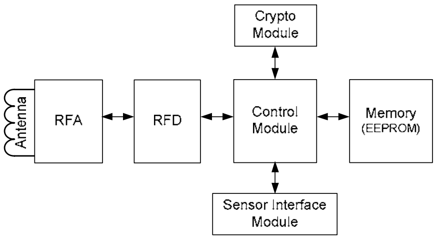
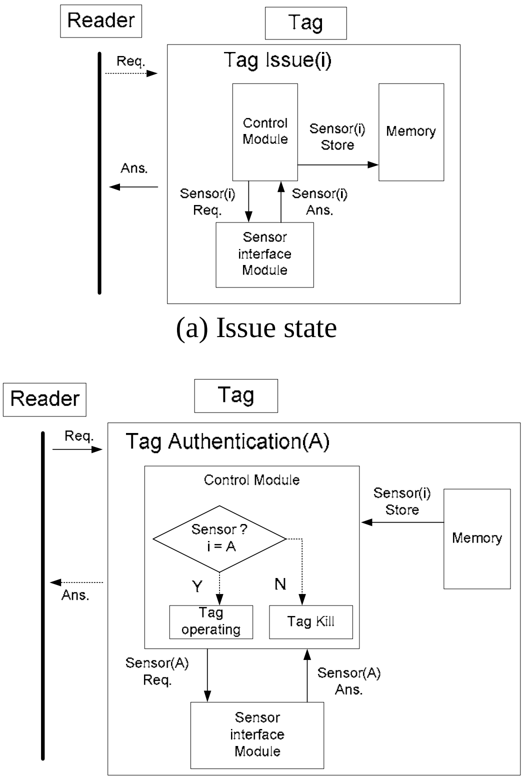


Fig. 1. Block diagram of the proposed RFID tag.

In this paper, the two applications of the RFID tag are described–security and measurement using a sensor interface module. In other words, the RFID tag plays the role in security function of a reuse-prevention and measurement function of a sensor values. This tag for security and measurement applications can be performed using the any sensors or devices with resistance characteristics. To satisfy this tag operation, the RFID tag has to measure the sensor value using a sensor interface module, and then, the value has to process by the security method based on the tag's control module. This sensor interface module has a resistance deviation-to-time interval converter.

Fig. 2 shows the two states for the security method of Fig. 1: One is an issue state and the other an authentication state.



(a) Issue state

(b) Authentication state

Fig. 2. The security method for the RFID tag.

If the RFID reader is commanded to the tag on the issue state, it is processed by the security method of the tag as shown in Fig. 2(a), and the sensor value, sensor (i), of the issue state is stored in the physical temper-resistance memory. Figure 2(b) show that is processed by the same method as Fig. 2(a). To see the authentication state, lets it compare issue sensor value with authentication sensor value. If the compared results of two sensor values are the agreement, the RFID tag is operated by the security method. If they are not agreement, the RFID tag is not operated. It should be noted that the security method using a sensor interface module in this paper apply on the RFID system. The proposed tag shows that it can be made a various functions using the sensor interface module and the RFID system can be realized a security RFID tag with no crypto algorithm.[6]-[7]

2.2 Resistance Deviation-to-Time Interval Converter

Fig. 3 shows the circuit diagram of the resistance deviation-to-time interval converter. It consists of a ramp integrator formed by capacitor (C_R) and current source (I_{RC}), two voltage-sources formed by resistors (R_{s1}, R_{s2}) and current source (I_{RS}), two comparators formed by MOS transistors, and a logic part formed by digital gates.

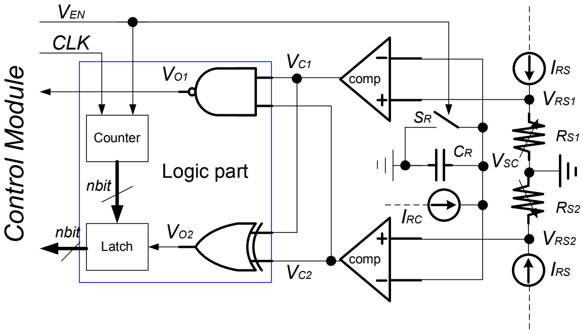


Fig. 3. Circuit diagram of the resistance deviation-to-time interval converter.

A constant-current source I_{RS} and a resistor R_{S1} form a lower flat voltage ($V_{RS1} = I_{RS} R_{S1}$), and I_{RS} and R_{S2} form an upper flat voltage ($V_{RS2} = I_{RS} R_{S2}$). Two resistors, R_{S1} and R_{S2}, can be represented a resistive sensor or fixed device according to the application. In this paper, the resistor R_{S2} represents a resistive sensor whose resistance change is to be detected. The upper flat voltage V_{S2} is identical to the lower one expects that R_{S1} is used instead of R_{S2}. R_{S1} is the reference resistor with which the resistance of the sensor is to be compared. Two comparators together with two flat voltage sources and a ramp integrator form a resistance deviation-to-time interval converter, whose transfer characteristics are shown in Fig. 4. It is noticeable that the input voltage of the comparator can be controlled by dc bias currents I_{RC} and I_{RS}. To see how the resistance deviation-to-time interval converter operates, refer to Fig. 5 which shows the timing diagram of the converter. We assume that both of the comparators are at their positive saturation level V_{dd}, and R_{S2} is greater than R_{S1}. Prior to the start of the conversion cycle, switch S_R is closed, thus discharging the capacitor C_R and setting the negative-input voltage of the comparator V_{SC} to 0.

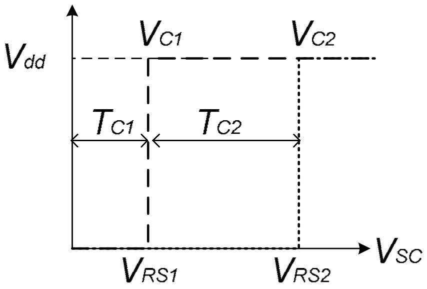


Fig. 4. Transfer characteristics of two comparator.

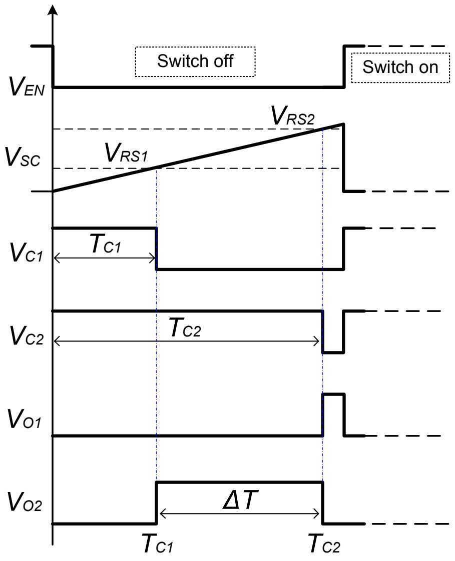


Fig. 5. Timing diagram of the converter.

The conversion cycle begins with opening the switch. Since the reference current I_{RC} for a ramp integrator flows through the capacitor, V_{SC} rises linearly with a slope of I_{RC}/C_R. When V_{SC} reaches a lower flat voltage of the positive input voltage of the comparator V_{RS1} ($=I_{RS}R_{S1}$), the output of the comparator falls to zero, and the output of the EX-OR gate V_{O2} becomes high. Denoting the time duration for which V_{C1} keeps V_{dd}. T_{C1}, we can write

$$T_{C1} = \frac{V_{RS1}}{I_{RC}} C_R \tag{1}$$

The conversion process continues until V_{SC} reaches the upper flat voltage of the positive input voltage of the comparator V_{RS2} ($=I_{RS}R_{S2}$). At this instant the output of the comparator falls to zero, thereby V_{O2} becomes low and the output of NAND gate V_{O1} becomes high. The switch is now closed and thus clamping the voltage V_{SC} to ground. This in turn triggers the comparators, causing their outputs to rise to V_{dd} and V_{O1} to be reduced. The switch is now opened and a new conversion process is started. Denoting the time duration for which V_{C2} keeps V_{dd}. T_{C2}, we can write

$$T_{C2} = \frac{V_{RS2}}{I_{RC}} C_R \tag{2}$$

The time duration of the V_{O2} pulse is given by

$$\Delta T = T_{C2} - T_{C1} \tag{3}$$

Combining (1) and (2) into (3), one can obtain

$$\Delta T = \frac{V_{RS2} - V_{RS1}}{I_{RC}} C_R = \frac{(R_{S2} - R_{S1})}{I_{RC}} I_{RS} C_R \tag{4}$$

Equation (4) also indicates that the sensitivity and the resolution of the converter can be controlled by adjusting the dc current I_{RC} or I_{RS}. This equation shows that it can be canceled e temperature coefficients of the converter and no numerical approximations have been made. It should be noted that the measurement and security of tag apply by the RFID system. The proposed tag shows that it can be made a various applications using the sensor interface module. In this case of the security application, this tag can be performed using any fixed devices with the resistance characteristics.

2.3 Comparator Implementation

A simple implementation of a single power-source comparator for the sensor interface module is shown in Fig. 6. It consists of a differential amplifier M_1~ M_5, a common-source M_6-M_7, an input bias PMOS transistors M_{P1}-M_{P2}, and two cascade current mirrors formed by transistors M_{C1}~M_{C8} and resistors R_1-R_2.

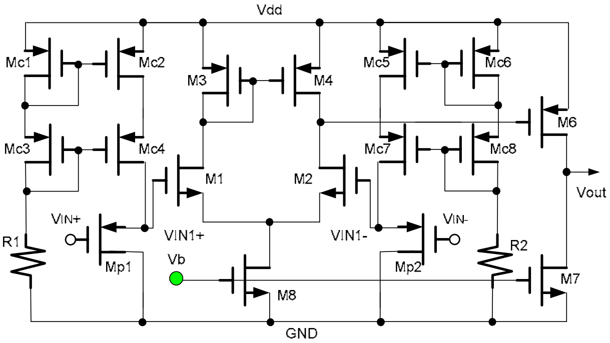


Fig. 6. The proposed comparator.

In this paper, the presented comparator with a simple and single power-source for the passive RFID tag is designed. To achieve this operation, the input bias circuit is to be used two PMOS input bias transistors, M_{P1} and M_{P2}. The driving circuits for a PMOS, M_{P1} consist of a cascade current-mirror formed by transistors M_{C1}~M_{C4} and a resistors R_1, and is designed to make the input bias voltage with dc level shift about Vdd/2 voltage. For simplicity, assume that all the transistors are ideal and identical. Summing the input bias voltages, V_{IN1+} and V_{IN1-}around the loop consisting of the input voltages of V_{IN+}, V_{IN-} and the source-gate junctions of V_{SG1}, V_{SG2}, respectively, we obtain

$$V_{IN1+} = V_{IN+} + V_{SG1} = V_{IN+} + \left(\sqrt{\frac{I_D}{K_P}} + V_t \right) \qquad (6a)$$

$$V_{IN1-} = V_{IN-} + V_{SG2} = V_{IN-} + \left(\sqrt{\frac{I_D}{K_P}} + V_t \right) \qquad (6b)$$

The input bias voltage, V_{IN1+}, V_{IN1-} of a differential amplifier in the comparator from Esq. (6a) and (6b) is determined by input voltage and V_{SG}. Since the operation of the comparator is given by open loop gain, we can obtain the transfer function of the comparator expressed as follows:

$$V_{IN+} > V_{IN-}, V_{IN1+} > V_{IN1-},\ V_{out} = V_{dd} \qquad (7a)$$

$$V_{IN+} < V_{IN-},\ V_{IN1+} < V_{IN1-},\quad V_{out} = 0 \qquad (7b)$$

The proposed comparator shows that it can be made a simple and input bias circuit using the PMOS.

3. Experiment Results and Discussion

A block diagram shown in Fig. 1 using a resistance deviation-to-time interval converter was built using 0.35um processor and designed by the CMOS circuit. The prototype RFID tag chip die area is 2mm x 2mm and is shown in Fig. 7.

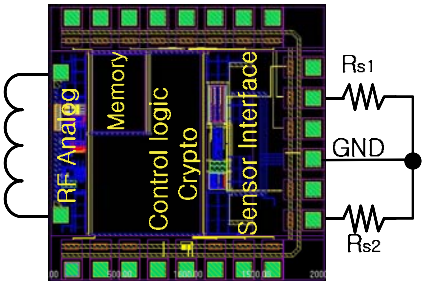


Fig. 7. The prototype RFID tag chip.

The generated voltage at the RFA of the RFID tag was 3V, and this voltage was driven supply power for the RFID tag. The maximum power consumption of the sensor interface module is about 180uW. The constant current, I_{RS} for the flat voltage was set at 1uA, and I_{RC} for the ramp integrator was set at 0.5uA, whose it is a cascode current mirror. To confirm the principles of a security and measurement operation in this paper, the resistors with the fixed or the variable resistor were used for R_{S1}, R_{S2}. On the other hand, to measure the precise resistor values, the variable resistor can be used for R_{S2} and fixed resistor can be used for R_{S1} with the corresponding R_{S2}. In order to make the signal processing independent of temperature and other environmental variations, two matched resistors were used: an active sensor resistor with a large change values was used for R_{S2} and a dummy sensor protected from physical contact is used for R_{S1}. Fig. 8 shows the plot of the measured time interval against resistance deviation, and the linearity line of the conversion characteristic show close agreement between predicted behavior and experimental performance, which is adequate for most applications. The temperature stability of the converter was measured by varying temperature from 10℃ to 50℃, and the time interval against the temperature change has not a change. The maximum conversion time was about 75.52us when the resistance deviation was 1MΩ. Counting the output pulse with a 3.39 MHz clock generated at RFID tag, the resolution of 8 bits was obtainable. A higher resolution could be achieved by using a higher speed clock signal.

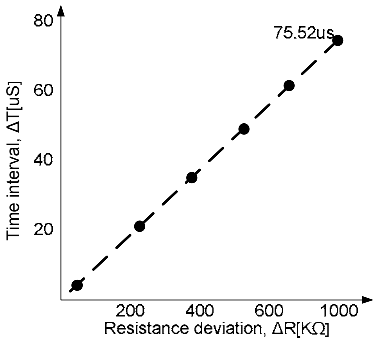


Fig. 8. Plots of measured time interval against resistance deviation.

From the results, we can be obtained a stable pulse width (time interval). Time interval is, so to speak, the resistance difference. The digital code of the time interval was stored in the EEPROM. The digital code value of both the issue and authentication states individually is compared with the one on the authentication state in a control module of the RFID tag. If their digital codes agree, the tag is to operate by the security method, and if it does not agree with this value, the tag is not operated: in other words, the RFID tag plays a role of the reuse-prevention. The proposed RFID tag shows that the security RFID tag can be performed using any devices with resistance characteristics and can be realized using the sensor interface mode. It should be noted that the RFID tag using a resistance deviation-to-time interval converter can be obtained a precision measurement for a various sensors or devices.

4. Conclusion

A novel time interval converter for the RFID tag with the security and measurement concepts is presented. A sensor interface module circuit for the RFID has been described which converts a resistance change into its equivalent pulse width change. The changed digital codes are performed by the RFID tag for the security or measurement. The presented converter is insensitive to the pulse width change regardless of environment change. The design principle and the circuit configuration are simple. Moreover, the converter features a high resolution and a good linearity over the wide resistance or capacitance range. Because of these advantages, the proposed converter is expected to find wide application in the signal processing of various sensors for security and measurement RFID tags. Therefore, passive RFID tag with an embedded with a resistance deviation-to-time interval converter is particularly suitable for the on-chip.

References

[1] K. Opasjumruskit, T. Thanthipwan, O. Sathusen, P. Sirinamarattana, P. Gadmanee, P. Pootarapan, N.Wongkomet, *Rs* A. Thanachayanont, and M. Thamsirianunt, "*Self-Powered Wireless Temperature Sensors Exploit RFID Technology*," *IEEE Pervasive Computing, IEEE vol.5, no. 1*, Jan.-March 2006, pp. 54-61.

[2] Kohvakka, M.; Hannikainen, M.; Hamalainen, T.D., "*Wireless sensor prototype platform*" *Industrial Electronics Society, 2003. IECON '03.*, pp.1499 – 1504, Nov. 2003

[3] J.M. Park and W.S. Chung, "*A Capacitance Deviation-to-Time Interval Converter Based on Ramp-Integration and its Application to a Digital Humidity Controller*," *IEEK*, vol. 37SD, Dec. 2000, pp. 70-78.

[4] Y. Cao and G. C. Temes, "*High-accuracy circuits for on-chip capacitance ratio testing or sensor readout*," *IEEE Trans. Circuits Syst.*, vol. 41, pp. 637-639, Sept.1994

[5] Kaliyugavaradan, S., "*A linear resistance-to-time converter with high resolution*" *Instrumentation and Measurement, IEEE Transactions onVolume 49, Issue 1,* pp.151 – 153, Feb. 2000

[6] D.C.; Engels, D.W.; Cole, P.H., "*Security and privacy solutions for low-cost RFID systems*", *IEEE* CNF, *Intelligent Sensors, Sensor Networks and Information Processing Conference,* 14-17 pp.337 – 342, Dec. 2004

[7] Mooseop Kim, et al, "*Low Power AES Hardware Architecture for Radio Frequency Identification*", *IWSEC 2006, LNCS4266*, pp. 357-368, 2006