병렬 순환 잉여 검사를 이용한 발전된 무선인식 시스템에 관한 연구
A study on the advanced RFID system using the parallel cyclic redundancy check

강태규*	윤상문*	신석균**	강민수***	이기서****
Kang, Tai-Kyu	Yoon, Sang-Mun	Shin, Seok-kyun	Kang, Min-Soo	Lee, Key-Seo

ABSTRACT

This paper has presented the parallel cyclic redundancy check (CRC) technique that performs CRC computation in parallel superior to the conventional CRC technique that processes data bits serially. Also, it has showed that the implemented parallel CRC circuit had been successfully applied to the inductively coupled passive RFID system working at a frequency of 13.56MHz in order to process the detection of logical faults more fast and the system had been verified experimentally. In comparison with previous works, the proposed RFID system using the parallel CRC technique has been shown to reduce the latency and increase the data processing rates in the results. Therefore, it seems reasonable to conclude that the parallel CRC realization in the RFID system offers a means of maintaining the integrity of data in the high speed RFID system.

I. INTRODUCTION

In communication systems, data integrity is ensured by the addition of a frame check sequence (FCS) at the end of a message so it can be checked at its destination for correct transmission. CRC can be employed to generate the FCS at the source of the message, and check the integrity of the entire message (data plus FCS) at the destination. Current RFID systems employ CRC to validate message integrity. CRC calculation can be performed in hardware or software. The common hardware solution is the linear feedback shift register (LFSR), which is a simple bit-serial architecture for both encoding and decoding messages. The bit-serial approach lacks efficiency for processing a parallel data stream, since every n-bit data word needs n-clock cycles to calculate the check sum. This approach is not efficient at high bit rates. The basic bit-serial algorithm can be accelerated by parallel processing a number of bits. Such a case demands the parallel CRC solution. The parallel CRC implementation can perform the necessary logic operations much faster than conventional CRC implementation and allows one circuit to be shared by several transmission lines.

This paper is structured as follows. In Section 2, gives a short summary of the RFID technology as the background information of RFID systems. In Section 3, illustrates the key elements of the parallel CRC technique and derives the logic equations of parallel CRC technique and presents the parallel CRC circuit. In Section 4, designs the inductively coupled passive RFID system using the implemented parallel CRC circuit. Finally, in Section 5, evaluates the experiment results and presents the conclusions of this paper.

* 광운대학교대학원 제어계측공학과, 석사 과정

** (주)마이크로트랙, RAMS 팀장

*** 한양대학교 정보통신공학과, 교수

**** 광운대학교대학원 제어계측공학과, 정교수, 정회원

II. RF IDentification

RFID denotes Radio-Frequency Identification. It provides a quick, flexible and reliable way to electronically detect, track and control a variety of items. RFID systems use radio transmissions to send energy to a transponder which in turn emits a unique identification code back to data collection reader linked to an information management system. RFID systems effectively utilize two separate antennas one on the transponder, and one on the reader to accomplish the task of data transfer by radio signals back to the data management system. The data collected from the transponder can be sent either directly to a host computer through standard interfaces, or it can be stored in a portable reader and up-loaded later to a computer for data processing.

An RFID system is always made up of two components: The transponder, which is located on the object to be identified. The interrogator or reader, which, depending upon the design and the technology used, may be a read or write/read device. A reader typically contains a radio frequency module, a control unit and a coupling element to the transponder. In addition, many readers are fitted with an additional interface to enable them to forward the data received to another system. On the reader side, modulator modulates the binary sequences from the memory unit into analog waveform, here proper coding (Manchester) and modulation (ASK, FSK) schemes will be selected by the modulator. The oscillator adds a carrier frequency to the analog waveform and the amplifier will amplify the signals and send them out through the antenna. The transponder, which represents the actual data-carrying device of an RFID system, normally consists of a coupling element and an electronic microchip. On the transponder side works almost the same as on the reader side. The clock module provides clocks to the digital circuits and the power module provides enough energy to drive the circuit. Demodulators on both sides will convert the transmitted signal to binary sequences for the digital circuits. When the transponder, which does not usually posses its own voltage supply (battery), is not within the interrogation zone of a reader it is totally passive. The transponder is only activated when it is within the interrogation zone of a reader. The power required to activate the transponder is supplied to the transponder through the coupling unit (contactless), as are the timing pulse and data.

III. PARALLEL CRC

Parallel Cyclic Redundancy Check(CRC) implementations simultaneously process multiple bits of data in parallel, increasing the data processing rate, with only a relatively small increase in the hardware complexity of serial CRC implementations that process data bits serially. The bit-serial approach lacks efficiency for processing a parallel data stream, since every n bit data word needs n clock cycles to calculate the checksum. Such a case demands a parallel CRC circuit solution. Parallel CRC hardware is attractive because, by processing the message in blocks of w bits each, it is possible to reach a speed-up of w with respect to the time needed by the serial implementation.

Starting from the circuit represented in [Figure 3.1], the parallel CRC has been implemented. In the following, we assume that the degree of polynomial generator (m) and the length of the message to be processed (k) are both multiples of the number of bits to be processed in parallel

(w). This is typical in data transmission where a message consists of many bytes and the polynomial generator, as desired parallelism, consists of a few nibbles. In the final circuit that we will obtain, the sequence S_1 plus the zeros are sent to the circuit in blocks of $w$bits each. After $\frac{k+m}{w}$ clock periods, the FFs outputs give the desired FCS. From linear systems theory, we know that a discrete time, time-invariant linear system can be expressed as follows.

$$\begin{cases} X(i+1)=FX(i)+GU(i) \\ Y(i) \quad\; =HX(i)+JU(i) \end{cases} \qquad (1)$$

where $X$is the state of the system, $U$the input, and $Y$the output. We use $F\,G\,H\,J$to denote matrices and use $X\,Y$ and $U$to denote column vectors. The solution of the first equation of the system (1) is:

$$X(i)=F^{i}X(0)+[F^{i-1}G\ldots FGG][U(0)\ldots U(i-1)]^{T}. \qquad (2)$$

We can apply (2) to the LFSR circuit [Figure 3.1]. From this consideration, the solution of the system (1) (expressed by (2)) is valid even if we replace multiplication and addition with the AND and XCR operators, respectively. In order to point out that the AND and XCR operators must be also used in the product of matrices, we will denote their product by $\otimes$ Let us consider the circuit shown in [Figure 3.1]. It is just a discrete-time, time-invariant linear system for which the input $U(i)$ is the ith bit of the input sequence; the state Xrepresents the FFs output and the vector Ycoincides with X i.e., $H$and $J$are the identity and zero matrices, respectively. Matrix $F$and $G$are chosen according to the equations of serial LFSR, So, we have:

$$X=[x_{m-1}\ldots x_1x_0]^T$$

$$H=I_m$$

The identity matrix of size $m\times m$

$$H=[00\ldots0]^T$$

$$L=d$$

$$G=[00\ldots1]^T$$

$$F=\left[\begin{array}{ccccc} p_{m-1} & 1 & 0 & \ldots & 0 \\ p_{m-2} & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ p_1 & 0 & 0 & \ldots & 1 \\ p_0 & & 0 & \ldots & 0 \end{array}\right.$$

where p_i are the bits of the divisor P(i.e., the coefficients of the generator polynomial). When i coincides with w the solution derived from (2) with substitution of the operators is:

$$X(u)=F^{u}\otimes X(0)[0\ldots0|d(0)\ldots d(w-1)]^{T}. \qquad (3)$$

where $X(0)$ is the initial state of the FFs. Considering that the system is time-invariant, we obtain a recursive formula:

$$X^{'}=F^{w}\otimes X\oplus D \qquad (4)$$

where, for clarity, we have indicated with $X^{'}$ and X respectively, the next state and the present state of the system, and $D=[d_{m-1}\ldots d_1 d_0]^T$ assumes the following values: $[0\ldots 0 b_0 \ldots b_{w-1}]$, $[0\ldots 0 b_w \ldots b_{2w-1}]^T$, etc., where b_i are the bits of the sequence S_1 followed by a sequence of m zeros. This result implies that it is possible to calculate the m bits of the FCS by sending the $k+m$ bits of the message S_1 plus the zeros, in blocks of w bits each. So, after $\frac{k+m}{w}$ clock periods, X is the desired FCS. Now it is important to evaluate the matrix F^w. There are several options, but it is easy to show that the matrix can be constructed recursively when i ranges from 2 to w

$$F^i = \left[F^{i-1} \begin{bmatrix} p_{m-1} \\ \cdots \\ p_1 \\ p_0 \end{bmatrix} \middle| \begin{matrix} \textit{the first } m-1 \\ \textit{columns of } F^{i-1} \end{matrix} \right]. \qquad (5)$$

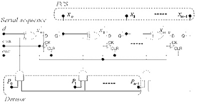
From (5), we can obtain F^w when F^m is already available. If we indicate with P' the vector $[p_{m-1}\ldots p_1 p_0]^T$, we have:

$$F^w = \left[F^{w-1} \otimes P' \ldots F \otimes P' \, P' \middle| \begin{matrix} I_{m-w} \\ 0 \end{matrix} \right], \qquad (6)$$

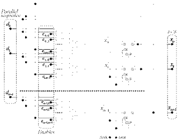
where I_{m-w} is the identical matrix of order $m-w$. Furthermore, we have:

$$F^m = [F^{m-1} \otimes P' | \ldots | F \otimes P' | P']. \qquad (7)$$

So, F^w may be obtained from F^m as follows: The first w columns of F^w are the last w columns of F^m. The upper right part of F^w is I_{m-w} and the lower right part must be filled with zeros.



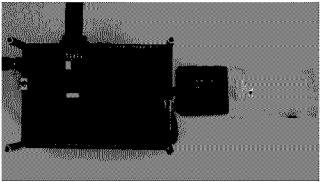
[Figure 3.1] One of the possible LFSR architectures



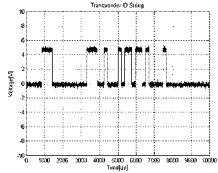
[Figure 3.2] Parallel CRC architecture

IV. EXPERIMENT

As the [Figure 4.1] indicates, the proposed RFID system using the parallel CRC technique is made of the following parts: the microcontroller, the Programmable Logic Device (PLD), the reader and the transponder. The microcontroller has been used to control the reader with the antenna and matching circuit and to perform the data exchange between the reader and the external application software. The parallel CRC circuit has been implemented by VHDL codes in the PLD according to the ISO/IEC 13239 (polynomial: $x^{16}+x^{12}+x^{5}+1$=0x8408, reverse, start value 0xFF, 1's complement). The inductively coupled passive RFID system has been operated in the 13.56MHz ISM band with a range of up to 1m according to the ISO standard 15693 that describes the method of functioning and operating parameters of contactless vicinity coupling smart cards.

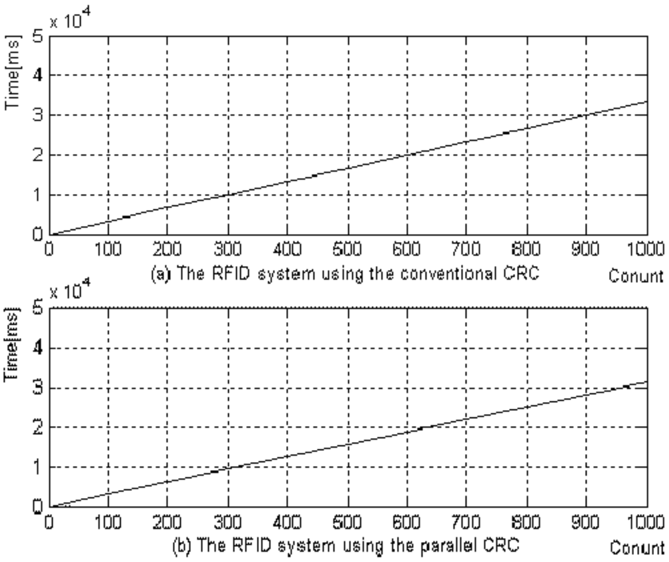


[Figure 4.1] RFID System using the Parallel CRC



[Figure 4.2] Waveform of Transponder ID

Having clarified the objectives of the experiment, the procedure will be explained in sequence. First, the data communications between the reader and the transponder have been performed by the ISO 15693 standards protocols and the conventional CRC codes implemented in the firmware. As the result, [Figure 4.2] indicates the waveform of the transponder ID string. Second, we have complied the VHDL codes concerning the presented parallel CRC circuit and simulated them using the Altera's Maxplus+II. What has to be noticed is that it is focused on implementing the parallel CRC circuit using the VHDL codes in the PLD because there are many dissertations that have already proved that the parallel CRC technique is much faster than the conventional CRC technique in a view of speed. Third, the conventional CRC codes in the firmware of the RFID system had been eliminated and the PLD implementing the parallel CRC circuit has been connected to the RFID system to apply the parallel CRC technique instead of the conventional CRC technique. Finally, the data transferred between the reader and the transponder has been successfully observed in the external application software. Also, the time of the data communications has been measured and compared approximately between the existing RFID system and the proposed RFID system by using the timer and counter of the external application program on the limited conditions. [Figure 4.3] shows comparatively the line graph of the time of processing the data regarding the transponder ID between the existing RFID system and the proposed RFID system.



(a) The RFID system using the conventional CRC

(b) The RFID system using the parallel CRC

[Figure 4.3] The line graph of the time of processing the data

V. CONCLUSIONS AND FUTURE WORK

The presented parallel CRC technique has been successfully implemented by the VHDL codes in the PLD and verified experimentally in the simulation using the Altera's MAX+ plus II software tool. Furthermore, the implemented parallel CRC circuit has been applied to the inductively coupled passive RFID system working at a frequency of 13.56MHz and the data communications between the reader and the transponder have been correctly observed in the external application program. Although the speed of data exchanged in the RFID system has not been investigated precisely, the RFID system using the parallel CRC technique has been shown to reduce the latency and increase the data processing rates in the result of [Figure 4.3]. Therefore, it seems reasonable to conclude that the parallel CRC realization in the RFID system offers a means of maintaining the integrity of data in the high speed RFID system.

A further direction of this study will be to provide more evidence for this result in detail and, from now on, a more prescriptive approach will be needed to solve the mentioned issue. Finally, the result of this paper will change the direction of the entire study of the RFID system.

REFERENCES

[1] W.W.Peterson and D.T. Brown, "Cyclic Codes for Error Detection", Proc. IRE, Jan. 1961.

[2] A.S. Tanenebaum, "Computer Networks", Prentice Hall, 1981.

[3] W. Stallings, "Data and Computer Communications", Prentice Hall, 2000.

[4] T.V. Ramabadran and S.S. Gaitonde, "A Tutorial on CRC Computations", IEEE, Aug. 1988.

[5] N.R. Saxena and E.J. McCluskey, "Analysis of Checksums, Extended Precision Checksums and Cyclic Redundancy Checks", IEEE Trans. Computer, July. 1990.

[6] K. Finkenzeller, "RFID Handbook Second Edition", John Wiley and Sons Ltd., 2003.

[7] Min-Soo, Kang, "A Study on Prevention of Collision and Data Loss of the RFID system using a Full-Length Instruction Code Method", 2002.