INTEGRATION, the VLSI journal 47 (2014) 123–129

Contents lists available at ScienceDirect

INTEGRATION, the VLSI journal

journal homepage: www.elsevier.com/locate/vlsi

Hardware implementation of tag-reader mutual authentication protocol for RFID systems

V.R. Vijaykumar [a,*], S. Elango [b]

[a] Department of Electronics and Communication Engineering, Anna University, Coimbatore, Coimbatore-641047, Tamil Nadu, India
[b] Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode-638401, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 13 September 2012
Received in revised form
24 January 2013
Accepted 6 March 2013
Available online 21 March 2013

Keywords:
Authentication protocol
Field programmable gate array
RFID
Linear feedback shift register
Truncated multiplier

ABSTRACT

Radio-frequency identification (RFID) is a recent technology that utilizes radio frequencies to track the object by transmitting a signal with a unique serial identity. Generally, the drawbacks of RFID technology are high cost and authentication systems between a reader and a tag become weak. In this paper, we proposed a protocol for RFID tag–reader mutual authentication scheme which is hardware efficient and consumes less dynamic power. Truncated multipliers are implemented in RFID tag–reader mutual authentication protocol system due to reduction in hardware cost and dynamic power. Experimental evaluation reveals that the proposed protocol with truncated multipliers provides more security than the earlier schemes. The proposed protocol is described in VHDL and simulated using Altera Quartus II. The functional block is implemented as hardware using an Altera DE2 Cyclone II (EP2C35F672C6) Field-Programmable Gate Array (FPGA).

1. Introduction

An RFID tag stores the information electronically which can be read from several meters away without having contact between tag and reader. Tag consists of an integrated circuit for handling data and an antenna for receiving and transmitting a radio-frequency signal. The RFID system utilizes one of three general band's low frequency (LF) at 125 kHz to 134 kHz, high frequency (HF) at 13.56 MHz, and Ultra HF at 860 MHz to 930 MHz [1,2]. RFID tags contain a unique serial number namely electronic product code (EPC) that can individually identify every single tagged item [3,4]. Electronic product Code Class 1 generation 2 (EPC C1G2) provides only very basic security tools using a 16 bits pseudorandom number generator (PRNG) [5]. The LFSR can be created using the Galois or Fibonacci configuration of gates and registers. Fibonacci implementation, the output from some of the registers is EX-ORed with each other and fed back to the input of the shift register. Fibonacci LFSR is more suitable for hardware implementation than the Galios LFSR [6–8]. A light authentication protocols that use only efficient bitwise operations (such as EX-OR, AND, OR, addition etc.) on tags have been defined in [9]. In [10] Hernandez-Castro et al. proposed an efficient protocol for low cost RFID tags in which number of addition operation reduced compared to [9]. An additional rotation operation is used for authentication protocol in [11]. Konidala et al. [12] proposed a protocol that utilized tag's access and kill passwords for the tag–reader mutual authentication scheme based on EX-OR operation.

In Peris-Lopez et al. [13] uses a MixBits function that require many iterations to complete, which leads to increase the hardware cost. Huang et al. [14] modified the Padgen function proposed by Konidala et al. and implemented a protocol in FPGA. Li et al. [15] proposed a EX-OR scheme for an efficient implementation of protocol. Schulte et al. [16] states that the power dissipation of a truncated multiplier is less compared to a standard multiplier. Wang et al. [17] states that truncated multiplier is used for lossy applications. Ko and Hsiao proposed an efficient array based truncated multiplier, which consume less power and utilized fewer hardware resources [18]. Selwyn discussed a various RFID Mutual authentication protocol in [19,20] in order to identify the vulnerabilities in protocols. In another work Cho et al. [21] analyzed, securing against brute-force attack of a hash function based authentication protocols. All the above protocols are fails in any one of the following aspects such as cost, security, power consumption and possibility of backward processing of the operation or function. In this paper truncated multiplier is used to encode the information during a mutual authentication process, it reduces the hardware cost, strengthening security and consumes less power to perform this multiplication. In addition to that, number of bit processing is fewer which lead to reduction in the bit length and their no possibility of finding the information by performing backward processing. The rest of this paper is organized as follows. In Section 2, we present the background and its related work on the RFID reader-to-tag authentication protocol.

* Corresponding author. Tel.: +919442014139.
E-mail addresses: vr_vijay@hotmail.com (V.R. Vijaykumar), eceelango@gmail.com (S. Elango).

0167-9260/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.vlsi.2013.03.002

The Proposed mutual authentication protocol is discussed in Section 3. Section 4 shows the simulation and implementation results of the mutual authentication scheme. Finally, we conclude the paper in Section 5.

2. Background and related works

RFID systems work, whenever a reader antenna emits a radio frequency signal. Tag pick up that radio signal and respond to a reader. Reader reads the signal which is responded by tag. The reader is act as a transceiver (i.e., a combination of transmitter and receiver) because their usual role is to request a tag and receive information from tag. The antenna can be a separate device, or it can be an integrated within a reader [1].

2.1. EPC class-1generation-2 standard

The access password is a 32-bit value stored in the tag's reserved memory if this password is set, then data transfer will be established between tag and reader. Initially reader requests a random number from the tag. Tag generates a random number and sends to reader. The reader cover codes the password by performing a bitwise EX-OR between password and random number. The generated EX-OR output is transmits to the tag. The tag decodes the coded password by performing a bitwise EX-OR of the received cover-coded string with the original as shown in Fig. 1 [5].

In this scheme, both the random number sends un-encrypted form. Man in middle attack is possible to happen by carrying out EX-OR operation between the cover coded passwords with random number, which provides access password and their by malicious reader to illegally access the tag's data [12].

2.2. Konidala mutual authentication scheme

In Konidala et al. [12] proposed a scheme where the server, reader, and the tag follows a multi-step tag–reader mutual authentication procedure as shown in Fig. 2. It uses the tag's 32 bit access and kill passwords in order to perform tag–reader mutual authentication. This protocol uses two rounds of Pad generation function (Padgen) to compute a cover-coding pad. The first round of Padgen function performs over the access password, while the second round of Padgen function performs over the kill password. The Padgen function is used to generate a 16 bit pads for "cover coding" the access password. The main drawbacks of this scheme, it is not implemented as hardware. To perform a single Padgen function it requires much more logical operation also its leads to increase the hardware cost and consume much dynamic power due to increase in the number of transition. To overcome the drawbacks of the above scheme Huang et al. [14] implemented a protocol in FPGA with modified Padgen function, but it increases the hardware cost.

3. Proposed mutual authentication scheme

3.1. Proposed protocol

The protocol consists of three main component's tag, reader and server or database. In the proposed protocol, each tag has an individual EPC, Password (PWD) and a common architecture (truncated multiplier function) provided by manufacturer to encrypt PWD. The database has the information about EPC and PWD of all tags. It also has a common protocol architecture which is embedded in all tags.

Fig. 3. describes the proposed protocol communication step between a reader and a tag. The detailed description of the proposed protocol is as follows:

Step 1: Initially, reader sends a request message to a tag.
Step 2: The tag responds by generating a new random number RTI.
Step 3: The EPC, RT1 information is sent to the server through the reader.
Step 4: The server then computes a CCPWDRT (cover coded password computed by reader from RT1) from truncated multiplier function and generates a new random number RM1 and transmitted to the tag.
Step 5: The tag performs a truncated multiplier function with RT1 and PWD to compute CCPWDTT (cover coded password computed by tag from RT1).

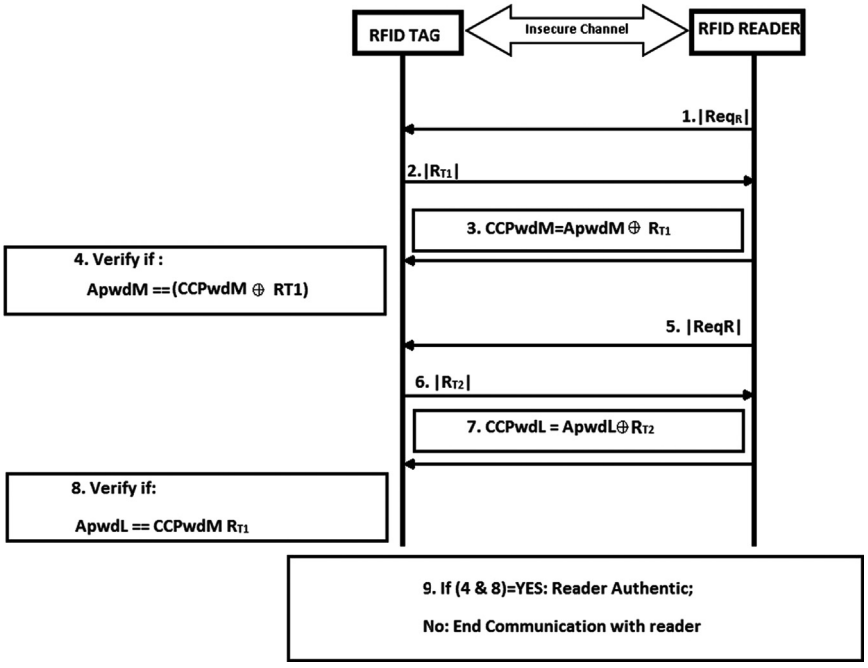

Fig. 1. Authentication scheme proposed by EPC global [5].