# A Fully Integrated HF-Band Passive RFID Tag IC Using 0.18-$\mu$m CMOS Technology for Low-Cost Security Applications

Jong-Wook Lee, *Senior Member, IEEE*, Duong Huynh Thai Vo, Quoc-Hung Huynh, and Sang Hoon Hong

***Abstract*—We present a fully integrated small-size HF-band passive RF identification (RFID) tag chip with authentication and security functions. The design of the RF transceiver and digital control of the tag IC is based on the International Organization for Standardization-14443 type-B protocol. The design of the key analog part of the tag IC is presented, which includes a robust demodulator for 10% amplitude shift keying envelope detection, a high-quality random number generator, and a voltage regulator that can handle a range of output load currents. To implement the secure data transaction with a reader, a 128-b advanced encryption standard (AES) with a new cyclic key generation is used for the data encryption and decryption. An on-chip 4-kb electrically erasable programmable ROM (EEPROM) is used to support the AES operation, tag identification, and tag self-destruction. The read and write accesses of the EEPROM are performed using a 128-b wide buffer with self-timed bursts. The tag chip is fabricated in a one-poly six-metal low-power 0.18-$\mu$m CMOS process with a $CoSi_2$ Schottky diode and EEPROM process. Using the scaled-down CMOS technology, the size of the tag chip is only $1.1 \times 1$ mm$^2$, providing a cost-effective solution for everyday RFID applications.**

***Index Terms*—CMOS, HF band, radio frequency identification (RFID), Schottky, tag IC.**

## I. Introduction

RADIO FREQUENCY IDENTIFICATION (RFID) is a technology which is widely used in applications such as supply chain management, logistics, building/house access control, and traffic toll collections [1]–[4]. One important advantage of the RFID technology is its inherent security and reliability. By employing the authentication and security functions available from the RFID tag IC, intentional deception and false modification of the product identification are effectively prevented. Utilizing the reliable security measure, the RFID technology is increasingly adopted for high-cost products, such as liquor and jewelry, in order to guarantee the quality of genuine items.

The HF-band RFID technology has inherent advantages in terms of security and reliability due to the close contact operation. Because a barcode identification system is very cheap, low cost is essential in order to extend the use of the RFID technology to everyday low-cost items.

Previously, a few HF-band tag ICs were reported [5]–[8]. These were implemented based on the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)-14443 type-B protocol [9] and ISO/IEC-15693 [10]. The work in [6] had a built-in Digital Encryption Standard block to provide the security functions through authentication and encryption. Previous works were designed using 0.8- and 0.6-$\mu$m CMOS technology in [5] and [6], respectively. The sizes of these tag chips were quite large, i.e., 11 and 8 mm$^2$, respectively, in view of the current CMOS technology. In addition, the power consumptions of these tag chips were more than 2 mW due to high supply voltages. Recently, an RFID tag IC with a ferroelectric random access memory (FeRAM) using 0.35-$\mu$m CMOS technology has been reported [8]. Since the FeRAM has a lower programmable voltage than the electrically erasable programmable ROM (EEPROM), the use of the FeRAM can provide advantages in terms of the operating distance and the tag read/write speed. However, implementing a security function in an RFID tag using the FeRAM is difficult because of its limited endurance and lifetime for data storage.

In this paper, we present a fully integrated RFID tag chip solution for cost-effective applications. Compared to the previously reported tag ICs [5]–[8], our design is based on a scaled-down low-power 0.18-$\mu$m CMOS process. The use of advanced technology and new circuit design techniques has allowed a significant reduction in the chip size. The size of the tag IC is just 1.1 mm$^2$, which is the smallest of all of the HF-band RFID tag ICs reported to date. Furthermore, the power consumption is as low as 360 $\mu$W, which is a factor of five times lower than the previously reported data in [5] and [6]. The low power consumption allows a tag IC to be used with a smaller tag antenna. The ISO-14443 type-B standard uses 10% amplitude shift keying (ASK) modulation for its reader-to-tag communication. The detection of small amplitude changes due to temperature and process variations is challenging. In this paper, a new voltage mode demodulator is proposed, and a detailed design technique is presented for reliable data

Manuscript received February 18, 2010; revised May 19, 2010 and June 13, 2010; accepted July 11, 2010. Date of publication August 3, 2010; date of current version May 13, 2011. This work was supported by the Korean Government (Ministry of Education, Science, and Technology) through the Mid-Career Researcher Program under the National Research Foundation of Korea Grant 2009-0078157.

J.-W. Lee and S. H. Hong are with the School of Electronics and Information, Kyung Hee University, Suwon 446-701, Korea (e-mail: daniel@khu.ac.kr).

D. H. T. Vo and Q.-H. Huynh are with the School of Electronics and Information, Kyung Hee University, Suwon 446-701, Korea, and also with Silicon Design Solutions, Milpitas, CA 95035 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIE.2010.2060460

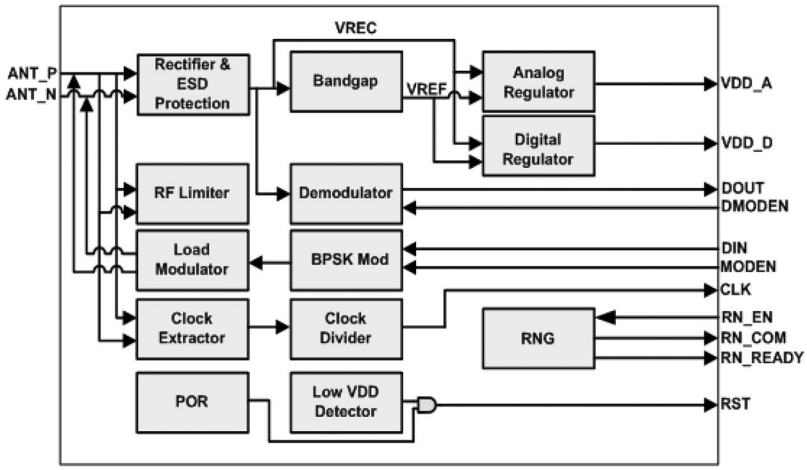



Fig. 1. Functional block diagram of analog part of tag IC.

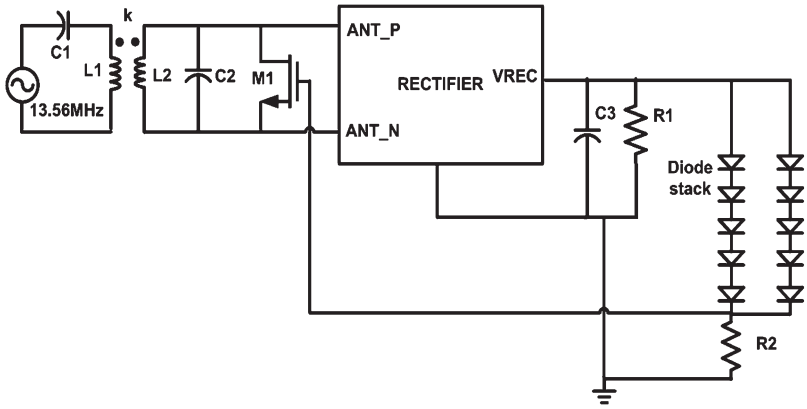



Fig. 2. Circuit schematic of the RF limiter with rectifier and reader-to-tag interface model.

demodulation. A 128-b advanced encryption standard (AES) is used to provide a secure data transaction with a reader. The AES operation is supported by a 4-kb EEPROM. For efficient power generation, $CoSi_2$ Schottky diodes are used, which was realized using a no-mask added process for cost reduction.

## II. Analog Functional Block

Fig. 1 shows the analog part of the HF-band RFID tag IC, which supports the ISO-14443 type-B protocol. The power management block includes a full-wave rectifier, RF limiter, regulator, and low-voltage detector. The Schottky diode is used for the rectifier. Due to its passive operation, the digital switching noise can cause a ripple in the supply voltage, which, in turn, affects the operation of sensitive analog circuits, such as the demodulator. To deal with the voltage ripple, two regulators are used to separately provide the digital and analog supply voltages (VDD_A and VDD_D), respectively.

The signal processing circuitry includes an ASK demodulator, load modulator, binary phase-shift keying (BPSK) modulator, clock generator, analog random number generator (RNG), and a power-on-reset. In the load modulator, a subcarrier of 847.5 kHz is used with the BPSK modulated data to facilitate the separation of the backscatter spectrum from the continuous wave (CW) power emitted by the reader.

## III. Rectifier, RF Limiter, and Load Modulator

For the power generation of the tag IC, a full-wave bridge rectifier is used because it has a higher current driving capability than a half-wave rectifier. Previously, the rectifier based on the diode-connected MOSFET has been used [5]–[8]. The efficiency of a MOSFET rectifier is usually lower than that of a Schottky diode due to its relatively high channel resistance [11]. In our design, we use a low-loss $CoSi_2$ Schottky diode, which has a higher RF-to-dc conversion efficiency than the MOSFET-based rectifier. The size of the diode is selected so that enough power can be delivered to the digital and memory sections of the tag chip. The average power consumption of the digital and memory is about 90 $\mu$W, and the rectifier efficiency under this load condition is 68%.

To protect the internal circuits under a high RF power, an RF limiter is placed between the two terminals of the tag antenna. The RF limiter is designed concurrently with the rectifier, taking into consideration the output range of the rectifier. Fig. 2 shows the schematic of the RF limiter with the rectifier and reader-to-tag interface model. The series $L_1$ and $C_1$ resonator network represents the reader part. The RF limiter consists of two diode stacks, a resistor $R_2$, and a large periphery shunting transistor $M_1$. When the rectified voltage exceeds the turn-on voltage of the diode stack, the shunting device $M_1$ is activated. When the gate voltage of the shunting transistor is turned on,

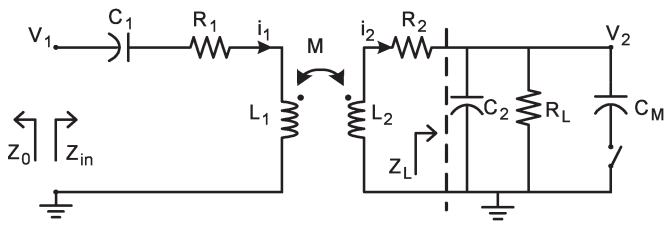



Fig. 3. Coupling model between the reader and tag.

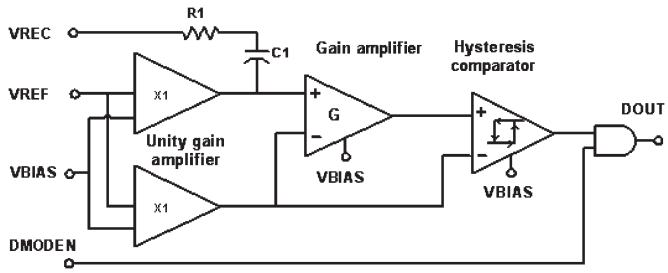



Fig. 4. Circuit schematic of the ASK demodulator.

it causes the capacitance across the tag antenna terminal to change. The resonance frequency of the parallel $L_2$ and $C_2$ network of the tag is then detuned, which results in a lower input power to the rectifier. Careful design is required so that the RF limiter can provide a wide-range operation while ensuring circuit protection.

Fig. 3 shows the coupling model between the reader and tag. The inductances of the reader and tag antennas shown in Fig. 2 are $L_1 = 1.6$ $\mu$H and $L_2 = 2.1$ $\mu$H, respectively, which are estimated using the formula in [12]. The mutual inductance between the reader and tag antenna is $M = k\sqrt{L_1 L_2}$, and the coupling factor $k$ is calculated using

$$k(x) \cong \frac{r_{\text{tag}}^2 \cdot r_{\text{reader}}^2}{\sqrt{r_{\text{tag}} \cdot r_{\text{reader}}} \cdot \left(\sqrt{x^2 + r_{\text{reader}}^2}\right)^3} \tag{1}$$

where $r_{\text{tag}}$ and $r_{\text{reader}}$ are the radii of the tag and reader antennas, respectively [1]. For our system, the dimensions of the antennas are $r_{\text{tag}} \cong 2.2$ cm and $r_{\text{reader}} \cong 7$ cm; then, the coupling factor between the antennas separated by $x = 1$ cm is $k = 0.15$. In Fig. 3, the impedance $Z_{\text{L}}$ at two different switch states is given by

$$Z_{\text{L},0,1} = \frac{R_{\text{L}}}{1 + Q_{0,1}^2} + \frac{1}{j\omega(C_2 + mC_{\text{M}})} \frac{Q_{0,1}^2}{1 + Q_{0,1}^2} \tag{2}$$

where $Q_{0,1} = \omega(C_2 + mC_{\text{M}})R_{\text{L}}$ is the $Q$ factor of the parallel $R$–$C$ circuit modulated by the switch, where $m = 0$ indicates the open switch and $m = 1$ is for the closed switch [13]. Using $i_2 = j\omega M i_1/(j\omega L_2 + R_2 + Z_{\text{L},0,1})$ and assuming $L_1$ and $C_1$ resonate at $\omega_0 = 2\pi f_0$, then the input impedance at the reader is

$$Z_{\text{in},0,1} = \frac{V_1}{i_1} = R_1 + \frac{\omega^2 M^2}{j\omega L_2 + R_2 + Z_{\text{L},0,1}}. \tag{3}$$

The source impedance $Z_0$ is matched to $R_1$, and assuming $Q_{0,1} \gg 1$, the reflection coefficient is obtained as

$$\Gamma_{0,1} = \frac{Z_{\text{in},0,1} - Z_0^*}{Z_{\text{in},0,1} + Z_0} = \left[1 + \frac{2R_1\left[j(\omega L_2 - R_{\text{L}}/Q_{0,1}) + \left(R_2 + R_{\text{L}}/Q_{0,1}^2\right)\right]}{\omega^2 k^2 L_1 L_2}\right]^{-1}. \tag{4}$$

For the BPSK backscatter modulation, the real part of $\Gamma_{0,1}$ is zero for both states in an ideal condition while the imaginary part is equal in magnitude and is opposite in sign as

$$\Gamma_{0,1} \cong \pm j\rho \tag{5}$$

where $0 < \rho < 1$ is the modulation index. Then, the backscattered power $P_{\text{bs}}$ is obtained as

$$P_{\text{bs}} = \rho^2 P_{\text{in,avail}} \tag{6}$$

where $P_{\text{in,avail}} = V_1^2/8R_1$ is the available input power from the reader when not loaded by the tag. For a given separation between the reader and tag, the backscattered power can be estimated using (1), (4), and (6). This power should be larger than the reader sensitivity for the correct demodulation of data received from a tag.

## IV. ASK Demodulator and Modulator

The ISO-14443 type-B HF RFID standard uses the 10% ASK modulation for the reader-to-tag communication. The demodulator should be able to detect a small change in the RF envelope caused by process and temperature variations. Furthermore, the amplitude of the incident signal has a high dynamic range depending on the distance between the tag and reader. Therefore, the design of the demodulator is quite challenging.

Fig. 4 shows the circuit schematic of the proposed ASK demodulator. The demodulator consists of two unity gain buffers, a high gain amplifier, and a hysteresis comparator. The series $R_1$ and $C_1$ branch removes the dc voltage level and differentiates the signal envelope from the rectifier VREC so that the rising and falling edges are maintained. The removal of the dc voltage level allows the detection of the input signal changes independent of the distance between the tag and reader.

The differentiated signal is level-shifted by the VREF and is amplified by the gain amplifier. The VREF is generated by an on-chip bandgap reference. The data level decision of the incoming signal is made by comparing it with the VREF; therefore, the variation of the VREF should be minimized. Another unity gain buffer is employed for both the gain stage amplifier and the hysteresis comparator in order to maintain a stable VREF level. The unity gain buffers are designed for a very low power (2.4-$\mu$A current consumption) to minimize the additional power consumption of the demodulator.

Another important issue in the passive RFID is that the digital circuit switching can modulate the analog supply voltage of the demodulator, which can result in the false data detection of the incoming signal. This problem is solved by two methods:

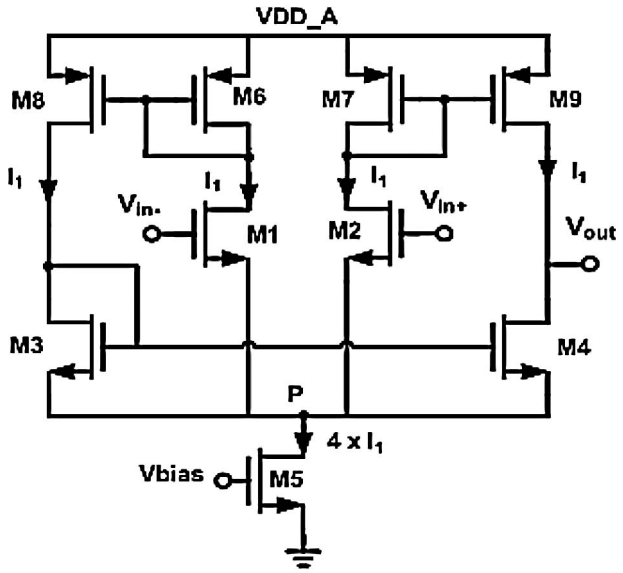



Fig. 5. Operational amplifier used for the gain stage of demodulator.

1) using a hysteresis comparator [14] and 2) reducing the bandwidth of the second stage gain amplifier so that the high-frequency switching noise is not amplified. Because the data level decision is based on the comparison of two signals with only a very small difference, any mismatch between the VREF and the output common-mode voltage in the gain stage of the amplifier results in an error in the demodulator output. To avoid a false data decision, the common mode voltage level at the output of the gain amplifier should closely follow that of the input.

Fig. 5 shows the schematic of the gain amplifier which ensures that the output follows the reference input voltage. The current sink $M_5$ carries $4I_1$, and the current mirrors force an equal current in the four branches. All of the NMOS (PMOS) transistors are of the same size. With the common voltage $V_p$ at node P, we have

$$V_{\text{in}-} = V_p + V_{\text{TH}} + \sqrt{\frac{2I_1}{\mu_n C_{\text{ox}}(W_1/L_1)}} \tag{7}$$

where $\mu_n$ is the electron mobility, $C_{\text{ox}}$ is gate oxide capacitance, $V_{\text{TH}}$ is the threshold voltage, and $W_1/L_1$ is the device width to length ratio of $M_1$. A similar expression for $V_{G3}$ shows that we have $V_{G3} = V_{G1} = V_{\text{in}-}$ if $M_1$ and $M_3$ have the same threshold voltages and process parameters. The voltage at the drain of $M_4$ is expressed as

$$V_{D4} = \frac{1}{\lambda_4}\left(I_1\left[\frac{1}{2}\mu_n C_{\text{ox}}(W_4/L_4)(V_{\text{GS4}} - V_{\text{TH}})\right]^{-1} - 1\right) \tag{8}$$

where $\lambda_4$ is the channel-length modulation parameter of $M_4$. A similar expression for $V_{D3}$ shows that the same current through $M_3$ and $M_4$ forces $V_{D3} = V_{D4}$ if the two transistors have perfect matching. With $V_{\text{GS4}} = V_{\text{GS3}}$, we can maintain the input common-mode voltage equal to the output common-mode level. There always exists a finite mismatch in the transistor. Considering the effect of the mismatch, the common-mode to differential-mode conversion gain $A_{\text{CM-DM}}$ is expressed as

$$\begin{aligned} A_{\text{CM-DM}} &= -\frac{|g_{\text{m1}} - g_{\text{m2}}|\,[(1/g_{\text{m6}})\|r_{o1}\|r_{o6}]}{(g_{\text{m1}} + g_{\text{m2}})r_{o5} + 1} \\ &\approx -\frac{|g_{\text{m1}} - g_{\text{m2}}|}{(g_{\text{m1}} + g_{\text{m2}})r_{o5} + 1}\left(\frac{L_6}{W_6}\right). \end{aligned} \tag{9}$$

The $A_{\text{CM-DM}}$ is caused by the mismatch between $M_1$ and $M_2$ and the finite output impedance $r_{o5}$ of $M_5$. A large $(W_6/L_6)$ ratio is used, and $r_{o5}$ is increased by reducing the dc bias current. To reduce the mismatch between $M_1$ and $M_2$, a common-centroid layout is used to keep the devices matched despite process variations.

## V. Regulator

Separate voltage regulators are used to isolate the power supplies of the analog and digital circuits, so the digital switching noise does not disturb the sensitive analog supply voltage. The voltage regulator shown in Fig. 6 is designed in order to provide a precision supply voltage despite input power variations.

The regulator is based on a folded cascode differential input stage with a current buffer compensation. Compared to a nulling resistor or voltage buffer compensation, the current buffer compensation technique provides a better gain bandwidth and an improved power-supply rejection performance [15]. The load current drawn from the digital circuit and the EEPROM varies significantly for a passive RFID tag IC, particularly when the erase/program operation is performed in the EEPROM. Therefore, the stability of the regulator should be examined over the entire range of load currents.

To analyze the stability of the designed regulator, a small signal equivalent circuit shown in Fig. 7 is used to derive the loop gain $LG = T_{\text{out}}/T_{\text{in}}$ by cutting node "X" in Fig. 6. The $g_{\text{m1}}$ and $g_{\text{mp}}$ represent the transconductances of the input differential stage $M_1/M_2$ and the pass device $M_{\text{P}}$, respectively. The $R_{\text{eq}}$ is the equivalent output resistance, $C_{\text{L}}$ is the output load capacitance, $C_{\text{g}}$ and $r_{01}$ are the equivalent capacitance and resistance at the output of the error amplifier, and $\beta$ is the feedback factor given by $R_2/(R_1 + R_2)$.

The input impedance looking into the source terminal of the current buffer compensation transistor $M_9$ is $(g_{\text{m9}}^{-1}\|r_{09}) \cong g_{\text{m9}}^{-1}$. When the output resistance of $M_{11}$ is neglected, $V_{\text{g}}$, $i_{\text{fb}}$, and $V_{\text{out}}$ are expressed, respectively, as

$$i_{\text{fb}} \cong \frac{V_{\text{out}}}{g_{\text{m9}}^{-1} + (sC_{\text{C}})^{-1}} \tag{10}$$

$$V_{\text{g}} = \left(r_{01}\left\|\frac{1}{sC_{\text{g}}}\right.\right)(i_{\text{fb}} + g_{\text{m1}}T_{\text{in}}) \tag{11}$$

$$\begin{aligned} T_{\text{out}} &= \beta \cdot V_{\text{out}} \\ &= -\beta \cdot \left[R_{\text{eq}}\left\|\frac{1}{sC_{\text{L}}}\right.\right\|\left(\frac{1}{g_{\text{m9}}} + \frac{1}{sC_{\text{C}}}\right)\Bigg] g_{\text{mp}}V_{\text{g}}. \end{aligned} \tag{12}$$

Because the load current through $C_{\text{L}}$ is much bigger than the current flowing through $C_{\text{C}}$, we can neglect the current

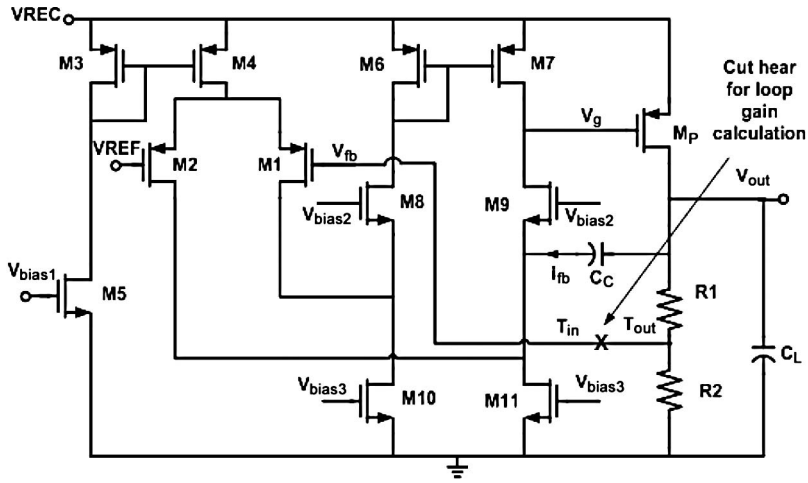



Fig. 6. Circuit schematic of the regulator.

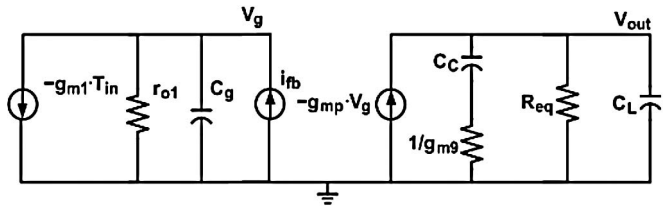



Fig. 7. Simplified small-signal equivalent circuit of the regulator.

through $C_{\rm C}$. Using the condition of $C_{\rm C} \ll C_{\rm L}$ and $g_{\rm m9}^{-1} \ll R_{\rm eq}$, the loop gain $LG$ is approximated as

$$LG = -\frac{\beta \cdot g_{\rm m1} g_{\rm mp} R_{\rm eq} r_{01} \left(1 + \frac{sC_{\rm C}}{g_{\rm m9}}\right)}{1 + as + bs^2 + cs^3} \tag{13}$$

where

$$a = C_{\rm C} g_{\rm m9}^{-1} + C_{\rm g} r_{01} + C_{\rm L} R_{\rm eq} + C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp} \tag{14}$$

$$b = (C_{\rm C} C_{\rm L} R_{\rm eq} + C_{\rm C} C_{\rm g} r_{01}) g_{\rm m9}^{-1} + C_{\rm g} C_{\rm L} R_{\rm eq} r_{01} \tag{15}$$

$$c = C_{\rm C} C_{\rm g} C_{\rm L} R_{\rm eq} r_{01} g_{\rm m9}^{-1}. \tag{16}$$

In the transfer function of (13), there are one zero and three poles. The locations of the poles vary under different load currents due to $R_{\rm eq}$ and $g_{\rm mp}$. As a result, the loop gain is analyzed for different load current conditions.

When the load current is small, the current drained from the pass transistor is reduced to $V_{\rm out}/(R_1 + R_2)$. Because $g_{\rm mp}$ is at its minimum, we can use the approximation $C_{\rm L} R_{\rm eq} \gg C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp}$ and neglect $C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp}$ in (14). Then, the term $(1 + sC_{\rm C}/g_{\rm m9})$ is formed in the denominator and cancels out the zero, so $LG$ can be approximated as

$$\begin{aligned} LG &\cong -\frac{\beta * g_{\rm m1} g_{\rm mp} R_{\rm eq} r_{01} \left(1 + \frac{sC_{\rm C}}{g_{\rm m9}}\right)}{(1 + C_{\rm L} R_{\rm eq} s + C_{\rm g} r_{01} s + C_{\rm g} C_{\rm L} r_{01} R_{\rm eq} s^2)\left(1 + \frac{sC_{\rm C}}{g_{\rm m9}}\right)} \\ &= -\frac{\beta * g_{\rm m1} g_{\rm mp} R_{\rm eq} r_{01}}{(1 + C_{\rm g} r_{01} s)(1 + C_{\rm L} R_{\rm eq} s)} \end{aligned} \tag{17}$$

where $p_1 = (C_{\rm L} R_{\rm eq})^{-1}$ and $p_2 = (C_{\rm g} r_{01})^{-1}$ are the dominant and nondominant poles, respectively. For a large load current, $g_{\rm mp}$ is increased, so we can use the approximations in (14): $C_{\rm L} R_{\rm eq} \ll C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp}$ and $C_{\rm g} r_{01} \ll C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp}$. In (15), the term $(C_{\rm C} C_{\rm L} R_{\rm eq} + C_{\rm C} C_{\rm g} r_{01}) g_{\rm m9}^{-1}$ is smaller than $C_{\rm g} C_{\rm L} R_{\rm eq} r_{01}$ and can be neglected. Using the condition of $C_{\rm C} \ll C_{\rm L}$, the loop gain $LG$ is then approximated as

$$LG \cong -\frac{\beta * g_{\rm m1} g_{\rm mp} R_{\rm eq} r_{01} \left(1 + \frac{sC_{\rm C}}{g_{\rm m9}}\right)}{(1 + C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp} s + C_{\rm g} C_{\rm L} R_{\rm eq} r_{01} s^2)\left(1 + \frac{sC_{\rm C}}{g_{\rm m9}}\right)}. \tag{18}$$

To form a standard two-pole system, we apply a further approximation using $C_{\rm L} C_{\rm g} (C_{\rm C} g_{\rm mp})^{-1} \ll C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp}$ so that $LG$ can be simplified to

$$LG \cong -\frac{\beta * g_{\rm m1} g_{\rm mp} R_{\rm eq} r_{01}}{(1 + C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp} s)\left(1 + \frac{C_{\rm L} C_{\rm g}}{C_{\rm C} g_{\rm mp}} s\right)} \tag{19}$$

where $p_1 = (C_{\rm C} R_{\rm eq} r_{01} g_{\rm mp})^{-1}$ and $p_2 = C_{\rm C} g_{\rm mp} (C_{\rm L} C_{\rm g})^{-1}$ are the dominant and nondominant poles for a high-load current.

Fig. 8 shows the loop gain transfer functions of the regulator with $C_{\rm C} = 2$ pF and $C_{\rm L} = 100$ pF under the no-load and full-load (500 $\mu$A) conditions. A good phase margin of approximately 89° is achieved under both conditions, indicating that good stability can be obtained using the folded cascode operational amplifier.

## VI. Digital Control Block

The digital control block of the RFID tag is designed in accordance with the ISO-14443 type-B standard. As shown in Fig. 9, the digital block consists of three blocks which are the MODEM, 128-b AES block, and 4-kb (256 b × 16 b) EEPROM. Inside the MODEM block, there are five subblocks which include the Encoder, Decoder, proximity IC card state (PICC-state), Active-control, and cyclic redundancy check 16 (CRC16).

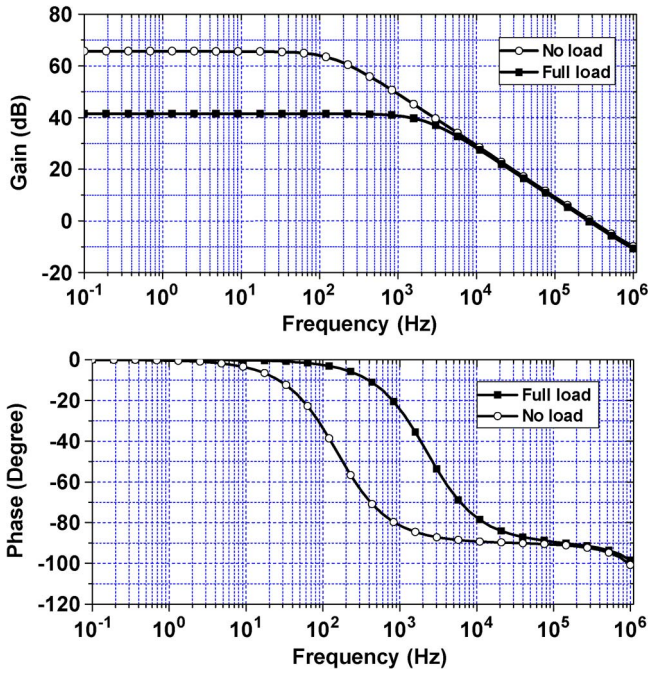



Fig. 8. Gain and phase of the regulator.

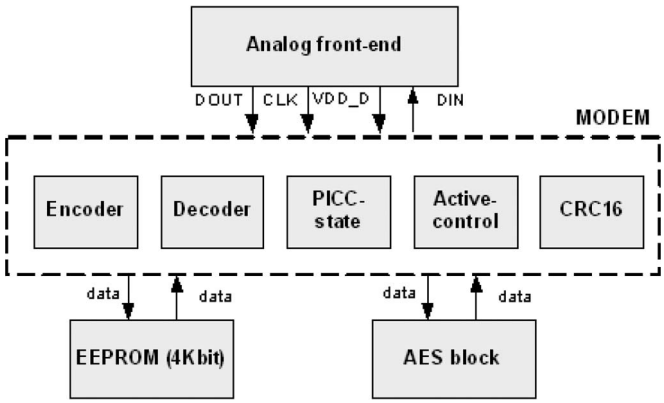



Fig. 9. Architecture of the digital control block with interfaces for analog, EEPROM, and AES block.

The MODEM includes three interfaces: the MODEM interface that interacts with the analog front end, the memory controller that interacts with the EEPROM, and the 128-b AES interface circuit that interacts with the AES block. The Encoder block in conjunction with the CRC16 block encodes the response to the reader and generates a serial bit stream output. The Decoder block in conjunction with the same CRC16 block decodes the incoming serial bit stream sent by the reader. The PICC-state block is a state machine that controls the tag search and anticollision portion of the protocol. The EEPROM and AES interface logic are activated only during the active state of the implemented standard, and the Active-control block in the MODEM incorporates these interfaces.

To implement the security function, the Active-control block takes a slightly different approach from the one used in [6] and [16]. Instead of the tag sending the random data to be encrypted by the reader, the tag transmits several base keys upon request from the reader. Both the reader and the tag hold the same two copies of the reader certification data (RCD) and the tag certification data. The reader uses the keys to generate the current session key to encrypt the RCD and requests the tag to certify the reader. The tag decrypts the received RCD using the tag-generated session key. The session key on both the reader and the tag is synchronized and updated at some specific events. The tag compares the decrypted RCD with the RCD stored in the EEPROM. If the reader is authenticated, the same procedure is used to authenticate the tag. The advantage of this approach is the ability to change the base keys for the same tag product without reconfiguring the reader. The self-destruct mode in the tag provides an additional security measure. The tag renders itself obsolete when it enters the active mode more than four times. Therefore, the ability to reuse the tag for illegal purposes is effectively eliminated.

The EEPROM has an asynchronous interface. Both the program and erase times require approximately 2.5 ms. Since the memory can only be accessed 16 b at a time, the data write is performed using a 128-b buffer within the MODEM using a timer and an address generator. Depending on the data size, the timer and the address generator are set appropriately for the self-timed automatic write operations. Multiple accesses between the reader and the tag are used for larger data sizes. For each access, the reader provides the starting address and the command. The tag uses the address and the command information to perform self-timed writes. Therefore, a large interval of up to 40 ms is required between consecutive data writes from the reader.

The AES function requires a 128-b key and 128 b of data in its register before the encryption or decryption operation. The encrypted or decrypted 128-b output is generated in a nonpredetermined number of computation cycles. The output computation is both data and key dependent. Therefore, the interface logic requires the monitoring of the output status at every clock cycle for an efficient operation.

A highly uniform distribution of random numbers is necessary for implementing the anticollision and security functions. Fig. 10 shows the schematic of the RNG. In this circuit, the outputs from both the analog and digital RNGs are combined. To further increase the quality of the random numbers, the outputs of the analog and digital random numbers are selected in a multiplexer which is clocked by a clock generator with large jitter. The analog RNG uses a low-frequency ring-type oscillator (13 kHz) with random jitter on the rising edge to sample the extracted system clock running at 13.56 MHz. Higher quality random numbers are obtained with a bigger root-mean-square jitter value or a faster high-frequency oscillator. The digital RNG is a 5-b pseudo-RNG which has a random sequence repeating after 32 cycles.

Fig. 11 shows the waveform timing description of the RNG operation. After receiving a request to generate a random number (EN goes high), the low-frequency clock output (S_CLK) with high jitter is used as the clock of a D-type flip-flop to sample the fast clock F_CLK. The S_CLK is also used as the clock for the digital pseudo-RNG and a multiplexer. OUT_RN is the output obtained from multiplexing the analog and digital random numbers. OUT_READY rises at the first rising edge of the S_CLK to indicate that the random sequence is ready after

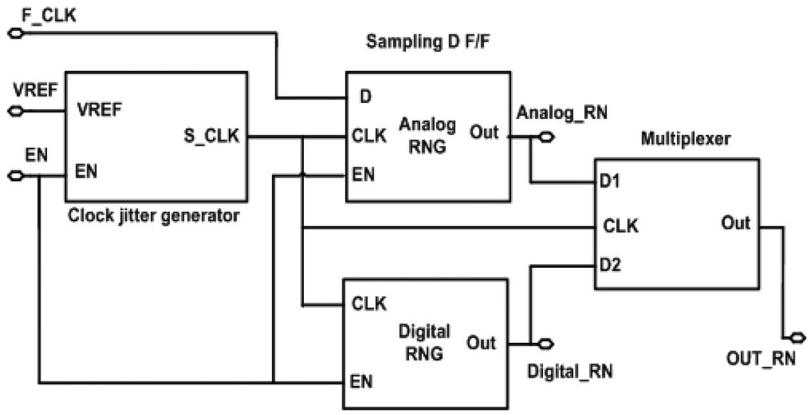



Fig. 10. Schematic of RNG.

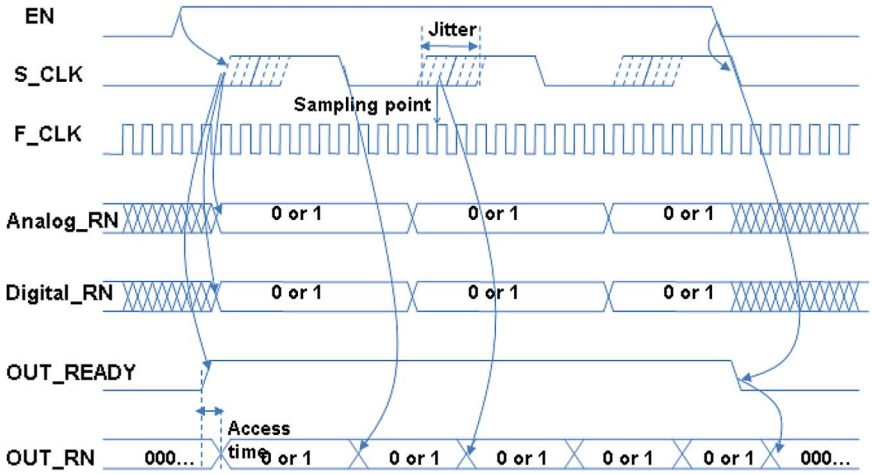



Fig. 11. Waveform timing description of the RNG.

a finite access time. It still stays at a high level until EN goes low so that the final output of the RNG is valid during the pulse high period of the OUT_READY signal.

## VII. Measured Results

Fig. 12 shows a microphotograph of the fabricated tag chip using a 0.18-$\mu$m one-poly six-metal CMOS process. The 250-pF storage capacitor is realized on top of the digital part in order to reduce the size of the chip. The chip size is $1.1 \times 1$ mm$^2$, which is more than seven times smaller than the size of the implementations in [5]–[7]. Separate test pins are added to the designed tag chip to verify the chip functionality.

The fabricated tag is tested in a wireless condition using a custom RFID reader conforming to the ISO-14443 type-B protocol [17], and the data are measured by probing the pins located in the test board using an oscilloscope with a 1-M$\Omega$ load impedance. The sensitivity of the tag (or minimum input power) is about 0 dBm.

Fig. 13 shows the measured results for the reader command REQB [9]. To verify the demodulator function, the data output from the reader is also shown. The modulation depth of the ASK signal from the reader is 10%. The results show a correct demodulator output. The output level is 1.8 V, which

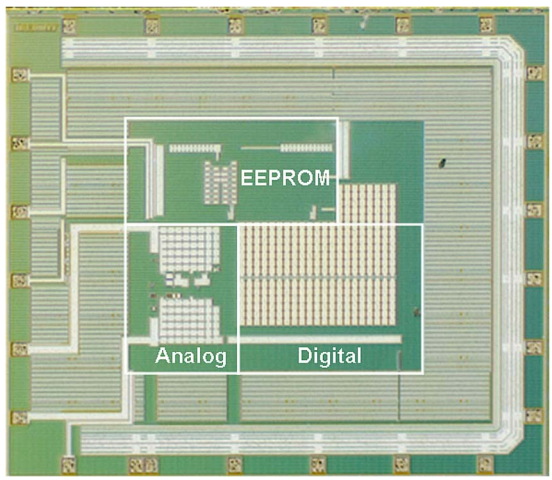



Fig. 12. Microphotograph of the fabricated tag chip including test pads. Core chip size is $1.1 \times 1$ mm$^2$.

is generated by the on-chip regulator from the rectifier output VREC shown in the figure. Fig. 14 shows the measured results of the response ATQB generated by the tag when receiving the REQB command from the reader. Separate testing of the digital part showed that the tag responds with an ATA command

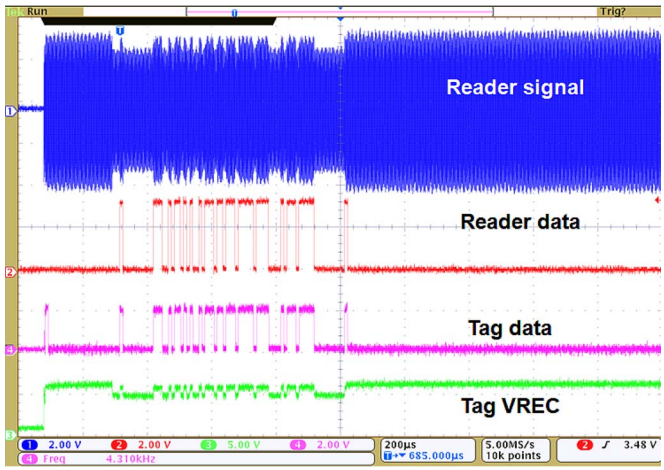



Fig. 13. Measured results of the RFID tag for REQB command. Results are (from the top) signal from reader, data from reader, demodulated data, and rectified voltage.

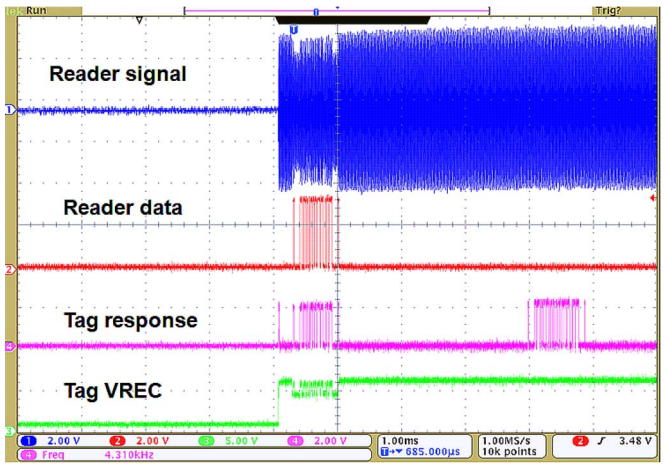



Fig. 14. Measured results of the RFID tag for ATQB response. Results are (from the top) signal from reader, data from reader, demodulated data and tag response, and rectifier output.

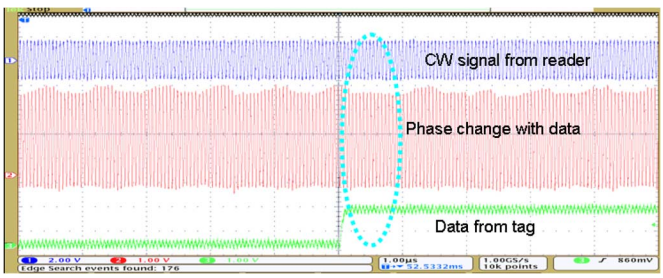



Fig. 15. Measured phase change in the subcarrier with data level.

when receiving an ATTRIB command from the reader. After the tag responds with the ATA command, the tag is put into the active state, wherein the proprietary encryption and decryption operations take over.

Fig. 15 shows the measured backscattering waveform in the time domain to check the phase change in the subcarrier with the data level confirming the correct backscatter modulator operation. Fig. 16 shows the measured backscattering spectrum

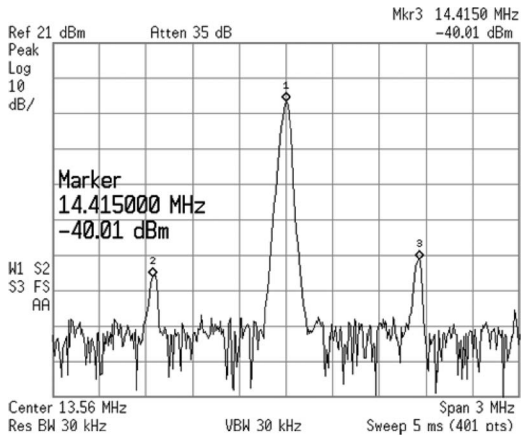



Fig. 16. Backscatter waveform measured at the reader antenna.

TABLE I
MEASURED PERFORMANCE SUMMARY OF THE RFID TAG IC

| | |
|---|---|
| Carrier frequency | 13.56 MHz +/- 10 kHz |
| Modulation type index (reader-to-tag) | ASK 10%, NRZ |
| Data rate (reader-to-tag) | 106 kbps |
| Modulation type index (tag-to-reader) | BPSK, NRZ |
| Backscatter modulation | Capacitive load switching |
| Data rate (tag-to-reader) | 106 kbps |
| Subcarrier frequency (tag-to-reader) | 847.5 kHz |

at the reader antenna separated from the tag antenna by about 1 cm. The spectrum at 13.56 MHz (main lobe) is part of the reader CW signal, and the two sidebands are due to the BPSK *backscatter* load modulation, as explained in Section III. The backscattered signal is 45 dB below the carrier, and its power level is −40 dBm which can be easily detected by a reader. When the distance between the reader and tag antenna changed from 0.7, 1, 1.2, and 2 cm, the backscatter power levels are −38.7, −40.0, −45.2, and −64.6 dBm, respectively. The subcarrier frequency is 847.5 kHz, and the input data rate is 106 kb/s.

Table I gives the measured performance summary of the tag IC meeting the ISO-14443 type-B standard. Table II shows the cost and performance comparison with the previous RFID tag ICs. The overall cost for fabricating the RFID tags ICs in a 300-mm wafer is $12 143 per wafer, and the cost of a 1-mm$^2$ die is 1.28 cents [18]. The number of dies available from a wafer can be obtained from [19] using a calculator. The resultant cost, computed with the wafer price divided by the die count, shows the cost effectiveness of our approach. For fair comparison, the different process technologies should be considered. We use the wafer cost correction factor for different technologies to normalize the cost for the 0.25-$\mu$m technology [20]. Even with the normalized cost, our approach exhibits the lowest cost among the published reports.

TABLE II
COMPARISON WITH PREVIOUS RFID TAG IC

| | This work | [5] | [6] | [7] | [8] |
|---|---|---|---|---|---|
| CMOS process | 0.18 μm | 0.8 μm | 0.6 μm | 0.25 μm | 0.35 μm |
| Power consumed (μW) | 360 | <2000 | 2500 | 28000 | 43 |
| Security algorithm | Yes | No | Yes | No | No |
| Non volatile memory | 4Kb | 24Kb | 8Kb | No | 16Kb |
| Size($mm^2$) | 1.1 | 11 | 8.1 | 16 | N.A |
| Number of die* | 586870 | 57450 | 78190 | 39170 | N.A |
| Estimate cost** (Cent/tag) | 2.1 | 21.1 | 15.5 | 31.0 | N.A |
| Estimate cost*** (Cent/tag) | 2.9 | 7.1 | 10.4 | 31.0 | N.A |

* based on 300mm wafer.
** Estimated price using the number of die available for a 300mm wafer
** Estimated price considering different fabrication cost for different technology

## VIII. CONCLUSION

A fully integrated 13.56-MHz passive RFID tag IC in conformance with the ISO/IEC 14443 type-B protocol has been presented in this paper. The tag IC fabricated using the scaled-down 0.18-$\mu$m CMOS technology achieves the lowest power consumption and the smallest size among previously reported tag ICs. Moreover, a robust demodulator design technique has been presented, which is suitable for detecting the small RF envelope changes required by the ISO/IEC 14443 type-B protocol. For a secure data transaction, a 128-b AES function is employed for the data encryption and decryption, and the function is supported by an on-chip 4-kb EEPROM. The wireless measurement of the designed RFID tag using an HF-band RFID reader has shown successful data demodulation, backscatter modulation, command decoding, and encoding. The result will be useful for item-level RFID tagging applications.

## ACKNOWLEDGMENT

The authors would like to thank Hynix Semiconductor, Ichon, Korea, for the chip fabrication and Ucommtech, Inc., Anyang, Korea, for the technical support. The computer-aided design tools used in this paper were supported by the IC Design Education Center, Korea. The authors would like to thank Q. T. Duong for the regulator simulation.

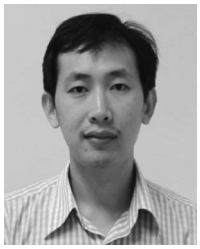
## REFERENCES

[1] K. Finkenzeller, *RFID Handbook*. New York: Wiley, 2003.
[2] EPCglobal, *EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Air Interface Version 1.0.9*, 2005.
[3] P. V. Nikitin and K. V. S. Rao, "LabVIEW-based UHF RFID tag test and measurement system," *IEEE Trans. Ind. Electron.*, vol. 56, no. 7, pp. 2374–2381, Jul. 2009.
[4] J.-W. Lee and B. Lee, "A long range UHF-band passive RFID tag IC based on high-Q design approach," *IEEE Trans. Ind. Electron.*, vol. 56, no. 7, pp. 2308–2316, Jul. 2009.
[5] S. Masui, E. Ishii, T. Iwawaki, Y. Sugawara, and K. Sawada, "A 13.56 MHz CMOS RF identification transponder integrated circuit with a dedicated CPU," in *Proc. ISSCC*, Feb. 1999, pp. 162–163.
[6] P. Rakers, L. Connel, T. Collins, and D. Russel, "Secure contactless smartcard ASIC with DPA protection," *IEEE J. Solid-State Circuits*, vol. 36, no. 3, pp. 559–565, Mar. 2001.
[7] A. Abrial, J. Bouvier, M. Renaudin, P. Senn, and P. Vivet, "A new contactless smart card IC using an on-chip antenna and an asynchronous microcontroller," *IEEE J. Solid-State Circuits*, vol. 36, no. 7, pp. 1101–1106, Jul. 2001.
[8] S. Masui and T. Teramoto, "A 13.56 MHz CMOS RF identification passive tag LSI with ferroelectric random access memory," *IEICE Trans. Electron.*, vol. E88-C, no. 4, pp. 601–606, Apr. 2005.
[9] *Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards, Part 2: Radio Frequency Power and Signals Interface*, ISO/IEC 14443-2, Dec. 1999. Final Committee Draft.
[10] *Identification Cards—Contactless Integrated Circuit Cards—Vicinity Cards—Part 2: Air Interface and Initialization*, ISO/IEC 15693-2, 2000.
[11] Y.-S. Hwang and H.-C. Lin, "A new CMOS analog frontend for RFID tags," *IEEE Trans. Ind. Electron.*, vol. 56, no. 7, pp. 2299–2307, Jul. 2009.
[12] D. Paret, *RFID and Contactless Smart Card Applications*. New York: Wiley, 2005.
[13] X. Chen, W. G. Yeoh, Y. B. Choi, H. Li, and R. Singh, "A 2.45 GHz near-field RFID systems with passive on-chip antenna tags," *IEEE Trans. Microw. Theory Tech.*, vol. 56, no. 6, pp. 1397–1403, Jun. 2008.
[14] G. Palmisano and G. Palumbo, "A compensation strategy for two-stage CMOS opamps based on current buffer," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 44, no. 3, pp. 257–262, Mar. 1997.
[15] B. K. Ahuja, "An improved compensation techniques for CMMOS operational amplifiers," *IEEE J. Solid-State Circuits*, vol. SC-18, no. 6, pp. 629–663, Dec. 1983.
[16] Y.-J. Huang, C.-C. Yuan, M.-K. Chen, W.-C. Lin, and H.-C. Teng, "Hardware implementation of RFID mutual authentication protocol," *IEEE Trans. Ind. Electron.*, vol. 57, no. 5, pp. 1573–1582, May 2010.
[17] Y.-H. Kim, Y.-C. Choi, M.-W. Seo, S.-S. Yoo, and H.-J. Yoo, "A CMOS transceiver for a multi-standard 13.56-MHz RFID reader SoC," *IEEE Trans. Ind. Electron.*, vol. 57, no. 5, pp. 1563–1572, May 2010.
[18] G. Swamy and S. Sarma, White Paper: Manufacturing Cost Simulations for Low Cost RFID Systems, May 2003. [Online]. Available: http://www.audioidlabs.org/uploads/media/MIT_AUTOID-WH017.pdf
[19] M. Hackerott, Die per Wafer Calculator. [Online]. Available: http: / / mrhackerott. org / semiconductor - informatics / informatics / toolz/ DPWCalculator/Input.html
[20] T. Roz, "The chip: Heart of an RFID tag," *EM Microelectronic*, Mar. 2009.

**Jong-Wook Lee** (S'02–M'06–SM'10) was born in Korea on April 6, 1970. He received the B.S. and M.S. degrees in electrical engineering from the Seoul National University, Seoul, Korea, in 1993 and 1997, respectively.

From 1994 to 1996, he was with the military. From 1998 to 2002, he was a Research Assistant with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN. From 2003 to 2004, he was a Postdoctoral Research Associate with the University of Illinois at Urbana–Champaign, Urbana. Since 2004, he has been a Member of the faculty with the School of Electronics and Information, Kyung Hee University, Suwon, Korea. His research interests include the area of millimeter-wave circuit design, radio frequency identification tag chip, and power management IC design.

Mr. Lee was the recipient of the 1997 Korean Government Overseas Scholarship.



**Duong Huynh Thai Vo** was born in Vietnam on October 12, 1981. He received the B.S. degree in electrical engineering from the Polytechnic University, Ho Chi Minh, Vietnam, in 2004. Since 2008, he has been working toward the M.S. degree in the School of Electronics and Information, Kyung Hee University, Suwon, Korea.

From 2004 to 2008, he was a Circuit Design Engineer with Silicon Design Solutions, Milpitas, CA, where he worked on memory compilers and built-in self-test solutions for embedded memories. His research interests include the area of radio frequency identification tag chip, power management IC design, and embedded memory design and test solutions.

**Quoc-Hung Huynh** was born in Vietnam on February 16, 1983. He received the B.S. degree in electrical engineering from the University of Natural Sciences, Ho Chi Minh, Vietnam, in 2006. He is currently working toward the M.S. degree in the School of Electronics and Information, Kyung Hee University, Suwon, Korea.

From 2006 to 2008, he was with the Circuit Design Group, Silicon Design Solutions, Milpitas, CA. His research interests include high-speed and low-power memory circuit design, low-power circuit design techniques for radio frequency identification (RFID), analog front end for passive/semipassive RFID tags, and bandgap reference design.

**Sang Hoon Hong** received the B.S. degree in electronic engineering from Yonsei University, Seoul, Korea, in 1993, and the S.M. and Ph.D. degrees in electrical engineering from Harvard University, Cambridge, MA, in 1998 and 2001, respectively.

From 1998 to 2005, he was a Senior Member of the technical staff with R&D Laboratory, Hynix Semiconductor, Ichon, Korea, where he designed high-performance memory circuits. Since 2006, he has been a Member of the faculty with Kyung Hee University, Suwon, Korea. His research interests include embedded memory interface, low-power circuits, and mixed signal design.