Exploiting Switching of Transistors in Digital Electronics for RFID Tag Design

Chia-Lin Cheng *Student Member, IEEE*, Luong N. Nguyen *Student Member, IEEE*, Milos Prvulovic *Senior Member, IEEE*, and Alenka Zajić *Senior Member, IEEE*

***Abstract*— Existing analog-signal side-channels, such as EM emanations, are a consequence of current-flow changes that are dependent on activity inside an electronic circuits. In this paper, we introduce a new class of side-channels that is a consequence of impedance changes in switching circuits, and we refer to it as an *impedance-based side-channel*. One example of such a side-channel is when digital logic activity causes incoming EM signals to be modulated as they are reflected (backscattered), at frequencies that depend on both the incoming EM signal and the circuit activity. This can cause EM interference or leakage of sensitive information, but it can also be leveraged for RFID tag design.**

In this paper, we first introduce a new class of side-channels that is a consequence of impedance differences in switching circuits, and we refer to it as an *impedance-based side-channel*. Then, we demonstrate that the impedance difference between transistor gates in the high-state and in the low-state changes the radar cross section (RCS) and modulates the backscattered signal. Furthermore, we have investigated the possibility of implementing the proposed RFID on ASIC for signal enhancement. Finally, we propose a digital circuit that can be used as a semi-passive RFID tag. To illustrate the adaptability of the proposed RFID, we have designed a variety of RFID applications across carrier frequencies at 5.8 GHz, 17.46 GHz, and 26.5 GHz to demonstrate flexible carrier frequency selection and bit configuration.

***Index Terms*— Radio frequency identification, RFID tags, EM side-channels, impedance-based side-channels.**

I. Introduction

Radio-frequency identification (RFID) and near-field communication (NFC) have been widely used in everyday life. Radio-frequency identification is typically used in supply chain management, asset tracking, data exchange, telemetry, access control, etc. [1]–[9] and has market that is worth several billion dollars today and is expected to grow $>$ 10 % per year [10]. On the other hand, near-field communication (NFC), also referred to as inductive-coupled RFID, is extensively used for promotional marketing, smart posters, security, files exchange, contactless payment, etc. [11] and has market that is expected to reach USD 47.43 billion by 2024 [12].

There are two main classes of RFID tags: *chip-based*, which use an integrated circuit (IC) chip to store tag information [8], [13]–[15], and *chipless*, which use the electromagnetic signature of the all-passive tag substrate to store the information [16]–[18]. The RFIDs can also be classified as passive, semi-passive, and active depending on whether the tag uses electromagnetic sources for power and communication, uses battery power for only its IC circuits, or uses battery power for both IC circuits and communication.

In this paper, we first introduce a new class of side-channels that is a consequence of impedance differences in switching circuits, and we refer to it as an *impedance-based side-channel*. Then, we demonstrate that the impedance difference between transistor gates in the high-state and in the low-state changes the radar cross section (RCS) and modulates the backscattered signal and propose a digital circuit that can be used as a semi-passive RFID tag. We implement this RFID tag in FPGA as a proof of concept. Proposed tag can be directly used in state-of-the-art smartphones such as Apple iPhone 7 and Samsung Galaxy S5 [19] that already have a FPGA board as a replacement for near-field communication (NFC) chips. More importantly, this approach opens up new possibilities for RFID designers to experiment with impedances of transistors switching from high-state to low-state and furtherer optimize this transmission mechanism in ASIC designs. We have investigated the possibility of implementing the proposed RFID on ASIC for backscatter signal enhancement. Simulation results show that a 30 dB enhancement can be achieved by optimizing logic gates' impedances.

To illustrate flexibility of this design (circuit can be easily reprogrammed) we have interrogated the proposed RFID tag at the following frequencies: 1) 5.8 GHz, a frequency typically used for RFID communications, 2) 17.46 GHz, a frequency that we have identified to have the highest signal-to-noise ratio (SNR), and 3) 26.5 GHz, a frequency that can be used for 5G wireless communications. Additionally, we have designed a variety of RFID applications to demonstrate flexible bit-configuration. State-of-the-art RFID tags are selected to compare to our RFID applications, which include: *static IDs with 6, 12, and 36 bits*, *multi-bit (4, 8, and 12 bits) dynamic RFID tag*, and *single-bit dynamic RFID tag*.

The proposed static ID configurations can transmit up to 36 bits simultaneously and provide up to 68.7 billion (2^{36}) combinations of unique IDs, whereas existing RFID tags with computational chips [20]–[22] can only transmit 1 bit simultaneously. The number and pattern of bits are fully re-configurable. This flexible bit design does not occupy additional space on the printed circuit board of the FPGA as the number of bits increases.

The proposed dynamic RFID tags with 4 bits, 8 bits, and 12

This work has been supported, in part, by NSF grants 1651273 and 1740962 and ONR grant N00014-17-1-2540. The views and findings in this paper are those of the authors and do not necessarily reflect the views of NSF or ONR.

Chia-Lin Cheng, Luong N. Nguyen, and Alenka Zajić are with the School of Electrical and Computer Engineering, Milos Prvulovic is with the School of Computer Science, Georgia Institute of Technology, Atlanta, GA 30332, USA.

bits were implemented and all bits were successfully detected. This design is meant to be comparable to RFIDs with multi-bit modulations. Our results are comparable with work in [9], where both 16-QAM (quadrature amplitude modulation) and 4-PSK (phase shift keying) RFIDs are designed. We have also tested a single-bit dynamic RFID tag. By transmitting one bit of information at a time to have better SNR, the proposed RFID tag can achieve a data rate of 100 kbits/sec with a bit error rate (BER) of 0.00000183 (10^{-6}), which is comparable to state-of-the-art RFIDs in [23], [24].

The rest of the paper is organized as follows: Section II introduces impedance-based side-channel used for creating backscattering communication channel, investigates the possibility of implementing the proposed RFID on ASIC, and describes digital circuit design for proposed RFID tag. Section III describes measurement setup and tests what is the maximum range at which the tag can operate. Section IV demonstrates applications of the proposed RFID tag across frequencies of 5.8 GHz, 17.46 GHz, and 26.5 GHz. Finally, Section V presents concluding remarks.

II. Impedance-based Side-channel as a Backscattering Communication Channel

Existing analog-signal side-channels, such as EM emanations, are a consequence of current-flow changes that are dependent on activity inside an electronic circuits. In this paper, we introduce a new class of side-channels that is a consequence of impedance changes in switching circuits, and we refer to it as an *impedance-based side-channel*. Our motivation to explore impedance-based side-channels was a hypothesis that the backscatter radio effect should be present in electronic devices. To explain our reasoning, we start with a description of traditional backscatter data communication.

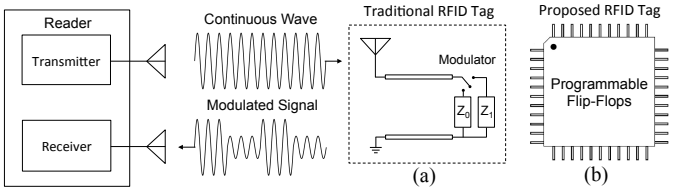


Fig. 1. Comparison between (a) traditional RFID tag and (b) proposed RFID tag.

Traditional backscattering communication in Fig. 1 (a) refers to a radio channel where a reader sends a continuous carrier wave (CW) signal and retrieves information from a modulated wave scattered back from a tag. During backscatter operation, the input impedance of a tag antenna is intentionally mismatched by two-state RF loads (Z_0 and Z_1) to vary the tag's reflection coefficient and to modulate the incoming CW [25], [26].

Our hypothesis was that inverters in digital electronics also have two-state RF loads and can be designed to reflect the modulated signal. For example, when input voltage is low, NMOS transistors in inverters are off and PMOS transistors are on. A direct path exists between V_{out} and V_{DD}, resulting in a high output state. On the other hand, high input results in a low output state. As shown in Fig. 2 (b), there exists a finite resistance between the output and V_{DD} and between the output and the ground, respectively [27]. The switching between NAND logic's high output state (R_1) and low output state (R_0) creates impedance variation, which is analogous to the variation in antenna terminating impedance in typical RFID tags. The impedance variation creates a difference in the circuit's RCS and thus modulates the electronic backscatter signals.

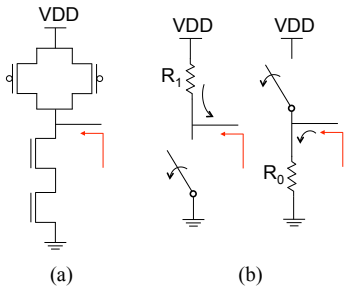


Fig. 2. (a) output circuit of a CMOS-NAND gate, (b) high-state resistance, R_1 (PMOS on resistance) and low-state resistance, R_0 (NMOS on resistance).

To test this hypothesis, we use a Field-Programmable Gate Array (FPGA) and program a cyclical shift register out of flip-flops shown in Fig. 3 that consists of a large number of inverters connected in parallel as shown in Fig. 4. A shift register is a group of flip-flops set up in a linear fashion with their inputs and outputs connected together such that the data is shifted from one device to another when the circuit is active. Here we use linear feedback shift registers (LFSRs), i.e., we connect the most significant bit, MSB (FFN in Fig. 3) back to the least significant bit, LSB (FF1 in Fig. 3) to cause the function to endlessly cycle through a sequence of patterns.

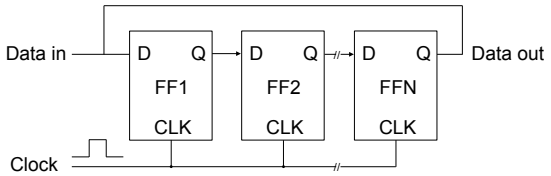


Fig. 3. Toggling circuits (shift registers) that generate hardware switching activity.

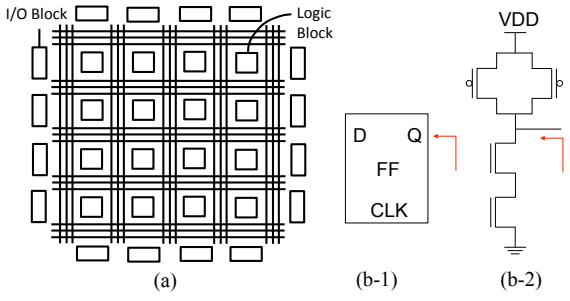


Fig. 4. (a) Simplified internal structure of FPGA, (b-1) programmable flip-flop, (b-2) equivalent output circuit of a CMOS-NAND gate.

A simplified internal structure of an FPGA chip is shown

in Fig. 4 (a), where logic blocks are arranged in a two-dimensional grid and are connected by a programmable-routing interconnect. This symmetrical grid is connected to I/O blocks which make off-chip connections. The "programmable/re-configurable" term in FPGAs indicates their ability to implement a new function on the chip after its fabrication is complete. Logic blocks can be simplified as programmable flip-flops shown in Fig. 4 (b-1). Most flip flops are based on CMOS-NAND gates due to their low latency. An equivalent output circuit of a CMOS-NAND gate is shown in Fig. 4 (b-2). When input voltage is low, NMOS transistors are off and PMOS transistors are on. A direct path exists between V_{out} and V_{DD}, resulting in a high output state. On the other hand, high input results in a low output state. This change between states with different impedance creates a difference in the circuit's RCS and thus modulates the electronic backscatter signals.

In order to modulate CW signal, we have programmed flip-flops to switch in a pattern shown in Fig. 5. Flip-flops continuously switch between high state and low state at a clock frequency (f_{clock}) of 50 MHz for half of clock cycle and stay quiet for the other half of the clock cycle. The switching cycle (modulating frequency, f_m) directly relates to the modulated signal bandwidth, i.e., the first harmonic of the modulated backscatter signal will be located at $f_{carrier} \pm f_m$. By changing f_m, we can easily upshift or downshift the modulated signals, making design very flexible. Note that f_m should be selected to avoid undesired harmonics in higher frequencies, i.e., the highest sideband (f_m) needs to be less than three times of the lowest sideband (f_m), and to comply radio regulations and avoid interference from other radio systems. Please note that in practice, the switching transistors do not produce ideal square pulses but rather pulses that have rising and falling edges, which sometimes leads to appearance of signals at even harmonics of the modulated backscatter signal. To avoid undesired interference, the highest sideband (f_m) should be less than two times of the lowest sideband (f_m).

Digital units that have periodic behavior, such as voltage regulators, typically produce signals in frequency range much lower than a processor clock. One of the reasons for that is to minimize interference between periodic activities that tend to produce multiple harmonics on the board. When designing RFID, knowledge of frequencies of periodic activities on the board will help determine where to position frequencies of RFID modulated sidebands. The potential interfering frequencies caused by other digital units can be found using method proposed in [28].

In addition to the switching pattern, the number of simultaneously-switched elements is another factor that affects electronic backscattering modulation. The more flip-flops are switching in unison, the stronger the backscatter signal is. To control the number of elements that switch simultaneously, we use an N-bit shift register, where N can be used to control the number of simultaneously-toggled flip-flops. Fig. 3 shows a simplified schematic for a 3-bit shift register, created by connecting N=3 flip-flops (FFs). Fig. 6 shows how logic is mapped onto an Altera Cyclone V FPGA chip for different values of N, Dark blue blocks represent utilized resources

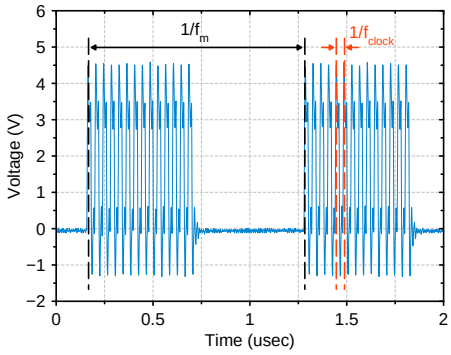


Fig. 5. Flip-flops switching signal pattern at f_m=900 kHz.

(flip-flops and logic) while light blue blocks denote unused resources. This Cyclone V FPGA chip is completely utilized (100% design in Fig. 6) when N=36600, and designs with 50% and 30% utilization use N=18300 and N=10980, respectively. Note that other FPGA chips may contain different numbers of programmable elements (total available N), so the same utilization percentage may require different values of N to be selected when using other FPGA chips.

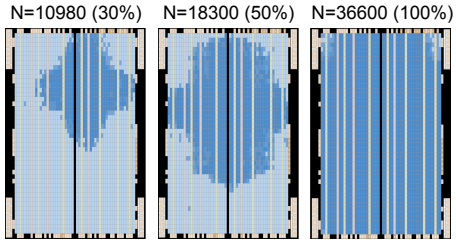


Fig. 6. Logic utilization mapping of an ALTERA Cyclone V FPGA chip.

The proposed RFID operates the same as traditional RFID when only one inverter is used to create two impedance states, i.e., only a single-bit single-sideband transmission is created. However, when higher data-rate is needed, traditional RFID uses multiple amplitude and/or phase levels and multi-bit modulation schemes to transmit the message in a single-sideband transmission. With dedicated ASIC, the proposed RFID can be designed in a similar fashion. However, it is also possible to have multiple inverters in the FPGA that switch at different frequencies, allowing for dynamic or static multi-bit designs using frequency modulation. The advantage of multi-frequency design is that receiver design is much simpler. For example, it does not require channel equalization and synchronization and detection is much simpler. To generate multiple bits as demonstrated in Section IV, multiple shift registers in Fig. 7 are used to switch at different f_m. Parameter M' represents the number of total shift registers. Parameter $N_{M'}$ denotes the number of total configured flip-flops in the M'^{th} shift register. The more flip-flops are configured, the higher SNR can be achieved. Parameter $f_{mM'}$ is the modulating frequency of the M'^{th} shift register, which affects the location of each side band and corresponding bandwidth for the communications.

Next, we demonstrate that backscattered sidebands are actually created by changing switching frequency of the FPGA

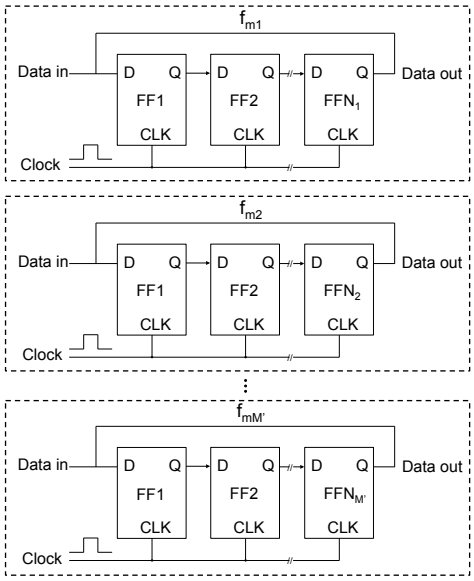


Fig. 7. Building blocks of the multi-bit RFID tag. M' is the number of total shift registers (bits). $N_{M'}$ is the number of total configured flip-flops in the M'^{th} shift register. $f_{mM'}$ is the modulating frequency of the M'^{th} shift register.

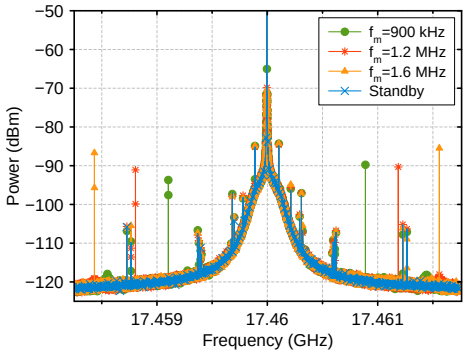


Fig. 8. Measured backscatter power with $f_{carrier}$=17.46 GHz and f_m=900 kHz (green), 1.2 MHz (red), and 1.6 MHz (yellow), respectively. The standby curve (blue) is the measured backscatter signal when FPGA board is turned on but not switching. A low noise amplifier (GNA-130F) is applied in this measurement.

circuits. The switching frequencies of the flip-flops in the FPGA board are varied from f_m=900 kHz, to 1.2 MHz, and to 1.6 MHz with logic utilization of 100 %. Measurement setup is presented in Fig. 12 (c). A low noise amplifier, GNA-130F from RF Bay Inc [29] is used and P_t is 15 dBm. Fig. 8 shows the measurement results with f_m=900 kHz (green), 1.2 MHz (red), and 1.6 MHz (yellow). The standby curve (blue) is the measured backscattered signal when FPGA board is turned on but not switching. Distinct modulated sidebands are observed at 17.46 GHz ± 900 kHz, 17.46 GHz ± 1.2 MHz, and 17.46 GHz ± 1.6 MHz. Signal strength of the modulated sidebands reaches up to -85 dBm, which is sufficient for commercial-available RFID readers in [30] and [31] with sensitivity of -120 dBm and -125 dBm to detect. This result shows that our proposed RFID technology can be used for commercial applications. In the standby mode, other sidebands around 17.46 GHz are also observed. Since the measurement is conducted in an indoor office environment, these sidebands are results from surrounding interference, e.g., measurement instruments, LCD monitors, mobile phones, WiFi routers, etc. **Note that conductive traces on an FPGA board that connect the FPGA chip to GPIO pins may act as antennas and radiate the backscatter signal. We disconnect these traces to verify that the signal is coming from the FPGA chip itself and not from the board. When turned on, GPIO pins can still operate correctly but will produce stronger RFID signal**. Our experiment results in Fig. 8 verify that switching electronics can establish backscattering channels without any antennas and RF front-end circuits.

We note here that the proposed tag does not have to be implemented in FPGA. Specialized circuits, e.g., ASIC, can be fabricated and the impedance difference between NAND logic's high output and low output state can be further optimized. Here we investigate the possibility of implementing the proposed RFID on ASIC to enhance backscatter signal strength. ASIC's NMOS/PMOS transistors with unbalanced on-state impedances can lead to larger RCS and thus increase the backscatter signal. In order to design ASIC that can effectively enhance the backscatter signal, first we need to understand the impedance model of the proposed RFID tag. Output impedance of a power supply network in integrated circuits is the parallel combination of output impedances of individual power-supply connections of all flip-flops [15]. The more flip-flops are connected, the more individual power supplies are connected in parallel, which reduces impedance. That is, the total input impedance of the proposed RFID tag is inversely related to the logic utilization N. Given this relationship between logic utilization and input impedance, we introduce a modulation loss factor, M, which relates the total tag's modulation loss to transistors' impedance variation. M can be expressed as,

$$M(x\%) = \frac{1}{4}\left|\frac{R_1(x\%) - 377^*}{R_1(x\%) + 377} - \frac{R_0(x\%) - 377^*}{R_0(x\%) + 377}\right|^2 \quad (1)$$

where $R_1(x\%)$ and $R_0(x\%)$ are the estimated high state (1s) resistance and low state (0s) resistance of the FPGA chip. Parameter x represents the percentage of total logic resources being configured. $R_1(x\%)$ and $R_0(x\%)$ are defined as,

$$R_1(x\%) = \frac{R_1(10\%)}{\frac{x\%}{10\%}} + R_{pkg} \quad (2)$$

$$R_0(x\%) = \frac{R_0(10\%)}{\frac{x\%}{10\%}} + R_{pkg}. \quad (3)$$

$R_1(10\%)$ and $R_0(10\%)$ are the estimated high state (1s) and low state (0s) resistances of an FPGA chip where 10 % of total resources are utilized. R_{pkg} is the estimated resistance contributed by the package of the IC chip, e.g., wire bonds inside the chip case. The input impedance of the tag is equal to free space impedance, 377 Ω, since there is no antenna but only air at the interface between the carrier signal and FPGA chip. Note that total impedance may also be affected by GPIO pins. For all the RFID designs proposed in this paper, we disconnect the traces that connect the chip and GPIO pins, and thus, GPIO pins do not affect the impedance variation created by the switching transistors. As a result,

the proposed impedance model in (1) does not include the influence from GPIO pins. According to [27], typical values of R_0 and R_1 are in k$Omega$ range and the values of R_0 and R_1 are inversely proportional to the W/L ratio of the device (ratio of width and length). **Therefore, by tuning transistor's W/L ratio, we can control the values of R_0 and R_1, M, and the corresponding backscatter power.** In order to estimate $R_0(10\%)$, and $R_1(10\%)$, we first configure the FPGA with a modulating frequency f_m= 900 kHz and logic utilization varying from 10 % to 100 %, and measure the corresponding backscattered power at 17.46 GHz + 900 kHz. We then perform curve fitting to estimate the optimal value of ($R_0(10\%)$, $R_1(10\%)$) as (18.8 kΩ, 20.4 kΩ), which is within reasonable range [27]. The estimated value of R_{pkg} is found to be in the range of several Ohms based on the dimensions of the wire bonds provided by [32] and the formulae in [33]. It is found that R_{pkg} has very minor impact to the total resistance since R_{pkg} is in the range of several ohms while R_0 and R_1 are in the kilo-Ohm range. Next, by using (1), we can estimate the value of M for the FPGA processor as -39.1 dB. We have designed an ASIC with (R_0, R_1)=(6 kΩ, 100 kΩ), and M=-9.1 dB. Comparison of M between the current FPGA processor and the proposed ASIC design is summarized in Table I. We can observe that by increasing the difference between ASICs' two impedance states R_0 and R_1, M and the backscatter power can be effectively enhanced by 30 dB. Next, we conducted simulation of MOSFET transistors with

TABLE I

COMPARISON OF MODULATION LOSS FACTOR (M)

Designs	(R0, R1) (kΩ)	Logic Utilization	M	Enhancement of M
Current FPGA	(18.8, 20.4)	100 %	-39.1 dB	+0 dB
ASIC	(6, 100)	100 %	-9.1 dB	+30 dB

Keysight Advanced Design System to demonstrate that the proposed ASIC design in Table I can be achieved by tuning transistors' W/L ratios. Schematic design of the simulation is presented in Fig. 9. BSIM4 NMOS and PMOS transistor

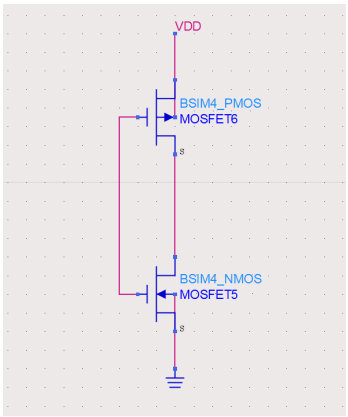


Fig. 9. Schematic design for simulation of a CMOS driver based on BSIM4 NMOS and PMOS transistor models.

models [34], [35] we use are based on 0.16 um process, i.e., the minimum length of gate (L) of a transistor is 0.16 um. Figs. 10 and 11 present the simulation results of the R_0 of NMOS transistor and R_1 of PMOS transistor with different W/L ratios as the drain voltage (V_{DD}) sweeps from 0 V to 3 V. Results show that the proposed ASIC design (third row in Table I) with (R_0, R_1)=(6 kΩ, 100 kΩ) can be achieved by using $(W/L)_{NMOS}$=3, $(W/L)_{PMOS}$=1, and V_{DD}=1.5 V.

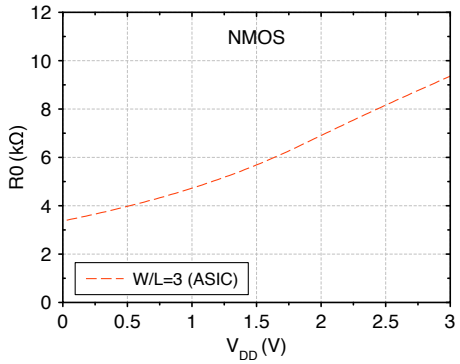


Fig. 10. Simulation results of the on-resistance of ASIC's NMOS transistor with (W, L)=(0.48 um, 0.16 um) as V_{DD} sweeps from 0 V to 3 V.

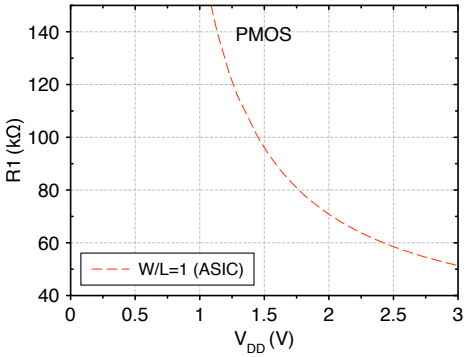
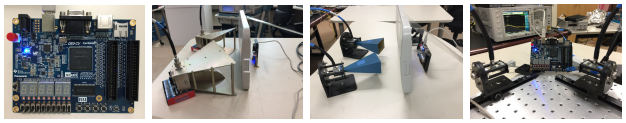


Fig. 11. Simulation results of the on-resistance of ASIC's PMOS transistor with (W, L)=(0.16 um, 0.16 um) as V_{DD} sweeps from 0 V to 3 V.

III. MEASUREMENT SETUP

An Agilent MXG N5183A Signal Generator with input power of 15 dBm (31.6 mW) is used as a signal source and an Agilent MXA N9020A Vector Signal Analyzer is used to record the signals. An Altera DE0-Cyclone V FPGA board is used as the RFID tag as shown in Fig. 12 (a). For interrogation, we use double ridge horn antennas (Com-Power AH-118) shown in Fig. 12 (b) for 5.8 GHz measurements. Double ridge horn antenna operates from 0.7 GHz to 18 GHz with average isotropic gain of 10 dBi. Fig. 12 (c) shows measurement setup with WR-62 standard gain horn antennas (PE9854/SF-20) that operate from 12.4 GHz to 18 GHz with average isotropic gain of 20 dBi. Finally, Fig. 12 (d) shows measurement setup with horn antennas (A-INFO LB-28-10) operating from 26.5 GHz to 40 GHz with average isotropic gain of 10 dBi. Note that in Figs. 12 (b) and (c), a 3-mm thick plastic case is placed between the T_x/R_x and the FPGA board to demonstrate that the proposed RFID tag can be potentially integrated into electronic devices with plastic enclosures, e.g., laptops, smartphones, tablets, etc. Note that we use different horn antennas because none of them cover all frequencies of interest, i.e. 5.8 GHz, 17.46 GHz, and 26.5 GHz.



(a) (b) (c) (d)

Fig. 12. (a) Altera Cyclone V FPGA board; measurement setup for the (b) 5.8 GHz, (c) 17.46 GHz, (d) 26.5 GHz measurements.

A. Interrogation Frequency, Distance, and Power Consumption

In this section, we have investigated the optimal carrier frequency to interrogate the proposed RFID tag and the maximum distance at which the signal can be received.

We use the measurement setup in Fig. 12 (b) with P_t=15 dBm and f_m=900 kHz. After sweeping carrier frequencies from 1 GHz to 18 GHz, we have found that the highest SNR is around 40 dB in the frequency range between 17 and 18 GHz.

To test how far away we can receive backscattered signal, we have configured an 1 bit RFID with 100 % logic utilization in order to maximize the SNR and to achieve longer distance. The FPGA board is placed at 2 m away from the T_x and R_x. The $f_{carrier}$ is set at 17.46 GHz with P_t=15 dBm and f_m=900 kHz. Fig. 13 shows the measured backscatter signal at a distance of 2 m. It is observed that the sideband appears at $f_{carrier}$ + 900 kHz with SNR around 5 dB. Empirically,

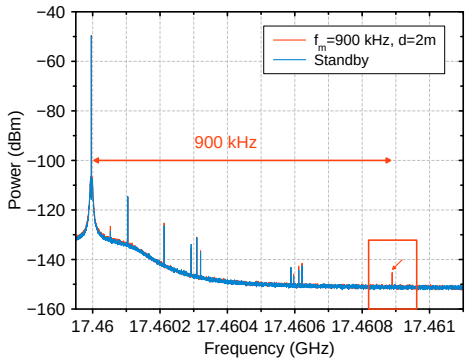


Fig. 13. Measurement results of the proposed 1-bit RFID with 100 % logic resources. Distance is set at 2 m. $f_{carrier}$ is set at 17.46 GHz and f_m is set at 900 kHz.

we have determined that a minimum 2.7 % of total logic resources is needed to provide one observable sideband (bit) with SNR around 3 dB at T_x/R_x-to-tag distance=20 cm. This implies that an FPGA chip can be used for multiple tasks, i.e., enable RFID tag without interrupting normal function of the FPGA chip. For example, if an FPGA is configured for intense data processing, we can reduce the number of bits and logic utilization of each bit, e.g., an 1-bit RFID allocated with 8 % of total logic resources, leaving 92 % of free logic resources for data processing; if an FPGA chip is mainly idle, we can increase the number of bits and logic utilization of each bit, e.g., an 8-bit RFID with each bit assigned with 10 % of total logic resources for higher SNR and data rate, leaving 20 % of free logic resources for non-RFID activities, e.g., computing, DSP, etc. Therefore, there is great design flexibility while still supporting normal functionality of an FPGA-based system. Regarding power consumption, given an Altera Cyclone V FPGA configured at 100 % logic utilization, a typical DC current consumption is 8.1 mA with a supply voltage of 1.1 V, which leads to a maximum power consumption of 9.5 dBm (8.91 mW) [36].

IV. RFID Applications

In this section, we illustrate how the proposed RFID tag can be used for several different applications: 1) static IDs with 6, 12, and 36 bits; 2) dynamic multi-bit communications; 3) high data rate communications.

A. 6-Bit, 12-Bit, and 36-Bit Static IDs

The first application is static ID with 6 bits, 12 bits, and 36 bits, respectively. The "static" term means that the designed bit pattern does not change over time. Information stored on the tag depends on total number of bits. We use multiple shift registers design described in Fig. 7 to configure multi-bit RFID design.

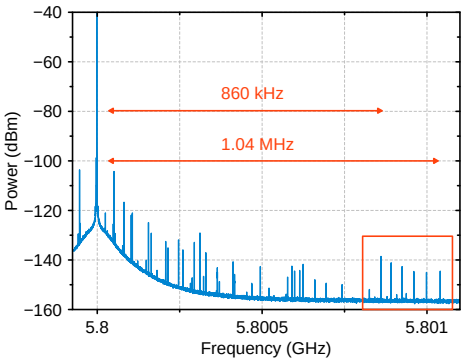


Fig. 14. Measurement results of 5.8 GHz 6 bits static ID with 16 % of logic resources assigned to each bit. f_m ranges from 860 kHz to 1.04 MHz.

For the 6 bit, 12 bit, and 36 bit RFIDs, f_m is set in a range of 860 kHz–1.04 MHz, 700 kHz–1.04 MHz, and 300 kHz–1.04 MHz and 15 %, 8.3 %, and 2.7 % of logic resources are assigned to each bit, which contributes a total logic utilization of 90 %, 99.7 %, and 97.2 % and a corresponding power consumption of 9.04 dBm (8.02 mW), 9.49 dBm (8.88 mW), and 9.38 dBm (8.66 mW), respectively. Each bit can be turned on and off individually to generate binary signals 1s and 0s with up to 68.7 billion (2^{36}) combinations of unique IDs. We demonstrate 6 bits and 12 bits static IDs at both 5.8 GHz and 26.5 GHz. The more bits are configured, the less logic resources are assigned to each bit, which requires higher antenna gain to accommodate lower SNR. As a result, we were able to observe signals for a 36 bits static ID only at 17.46 GHz because it had the highest SNR. Measurement results are shown in Figs. 14–18. It can be observed that all bits are clearly identified and separated at least 15 kHz apart with SNRs ranging from 6 dB to 20 dB, providing sufficient margins for signal detection. Our designs demonstrate flexible carrier frequency selection and bits configuration. Note that in Fig. 18, due to attenuation, harmonics of lower sidebands do not cause observable interference to the higher sidebands. For the measurement setup, P_t is 15 dBm, T_x/R_x–tag distance is 20 cm. Note that the plastic enclosure as obstruction between the tag and the T_x/R_x can cause extra 1 to 2 dB attenuation. The measurement results shown in Figs. 14–18 is without obstruction for better SNR demonstration.

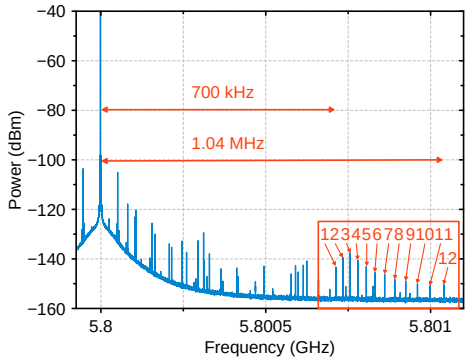


Fig. 15. Measurement results of 5.8 GHz 12 bits static ID with 8 % of logic resources assigned to each bit. f_m ranges from 700 kHz to 1.04 MHz.

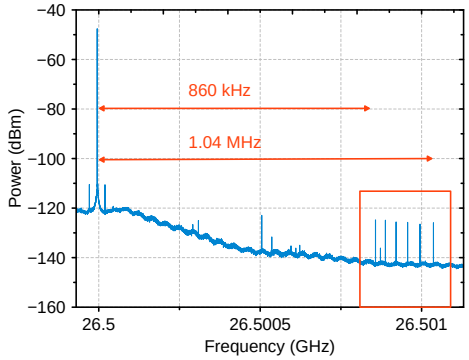


Fig. 16. Measurement results of 26.5 GHz 6 bits static ID with 16 % of logic resources assigned to each bit. f_m ranges from 860 kHz to 1.04 MHz.

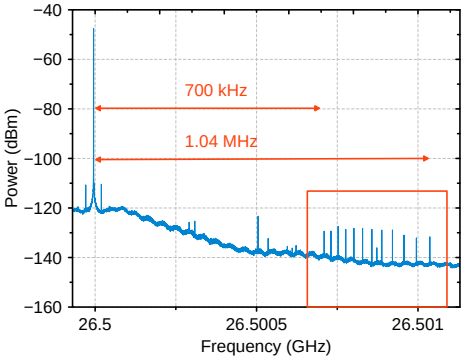


Fig. 17. Measurement results of 26.5 GHz 12 bits static ID with 8 % of logic resources assigned to each bit. f_m ranges from 700 kHz to 1.04 MHz.

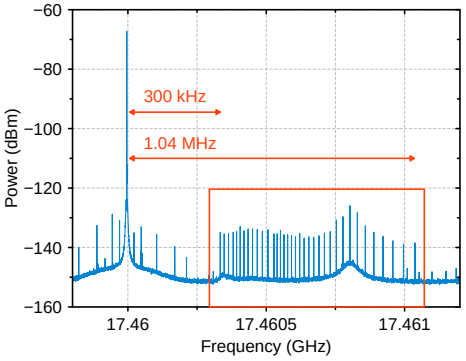


Fig. 18. Measurement results of 17.46 GHz 36 bits static ID with 2.7 % of logic resources assigned to each bit. f_m ranges from 300 kHz to 1.04 MHz.

B. Dynamic Multi-Bit Communications

The second application is dynamic multi-bit communications. The "dynamic" term means the designed bit pattern changes over time. Compared to the static IDs in Section IV-A, here individual bit is turned on and off over time at a switching frequency (f_s) to transmit information. As a result, information stored on the tag is not limited by total number of bits but depends on f_s and total transmitting time.

We design 4-bit, 8-bit, and 12-bit RFID tags to transmit specific symbols and successfully detect the symbols at the receiver. Each bit is allocated with 8 % of logic resources and f_s is set at 100 kHz. Consequently, the 4, 8, and 12 bits designs have a total logic utilization of 32 %, 64 %, and 96 %, a corresponding data rate of 400 bits/sec, 800 bits/sec, and 1.2 kbits/sec, and a corresponding power consumption of 4.55 dBm (2.85 mW), 7.56 dBm (5.7 mW), and 9.32 dBm (8.55 mW), respectively. Fig. 19 presents symbol patterns measured at the receiver for the 4 bits design. Data symbols are designed in the following patterns: (1111), (1000), (1010), (0101), (0011), (0111). The f_m ranges from 1 MHz to 1.14 MHz to accommodate all 4 bits. Measurement results show that all the symbols are successfully detected and match the designed signal patterns. In the 8 bits and 12 bits designs, the f_m ranges from 1 MHz to 1.39 MHz and from 1 MHz to 1.79 MHz, respectively. The 8 bits design has symbol patterns of (11111111), (00000000), (10011100), (10000011) and the 12 bits design has symbol patterns of (111111111111), (000000000000), (100000011100), (100000000011). Similarly, all symbols of the 8 bits and 12 bits RFID are successfully detected as shown in Figs. 20 and 21. For the measurement setup, P_t is 15 dBm, T_x/R_x–tag distance is 20 cm, interrogation frequency is 17.46 GHz. Note that the plastic enclosure as obstruction between the tag and the T_x/R_x can cause extra 1 to 2 dB attenuation. The measurement results shown in Figs. 19–21 is without obstruction for better SNR demonstration.

C. Dynamic Single-Bit Communications with Maximum Data Rate

The third application is focused on providing high data rate communication between the interrogator and the tag. We have designed an 1-bit RFID with 100 % logic utilization and maximum power consumption of 9.5 dBm (8.91 mW) to maximize SNR. The f_m is set at 1.92 MHz and the f_s is set at 100 kHz, providing a data rate of 100 kbits/sec. In order to estimate the bit error rate (BER), we use the VSA with a sampling rate of 2.56 MHz to record more than 1 million transmitting bits (1091227 bits) for around 11 seconds. The RFID tag modulates the carrier signals with a testing symbol pattern of (111010). Fig. 22 presents the measured signal strength of the transmitted symbols. Solid curve is the modulated backscatter signals measured by the VSA, while red circles are post-measurement signal processing sampled signals. In order to detect bit 0 and bit 1, a threshold value of -81 dBm is chosen since it provides the lowest BER. Our signal processing results show that only 2 errors are detected among all 1091227 transmitted bits, that is, our proposed RFID tag achieves a BER of 0.00000183 (10^{-6}) at a data rate of 100 kbits/sec. For the measurement setup, P_t is 15 dBm, T_x/R_x–tag distance is 20 cm, interrogation frequency is 17.46 GHz.

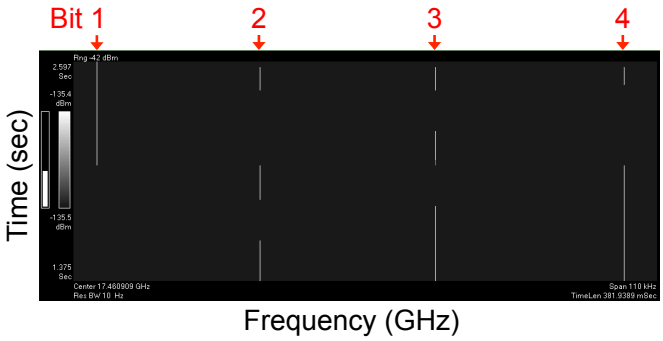


Fig. 19. Measurement results of 17.46 GHz 4 bits RFID for dynamic communications. f_m ranges from 1 MHz to 1.14 MHz. Symbol patterns: (1111), (1000), (1010), (0101), (0011), (0111).

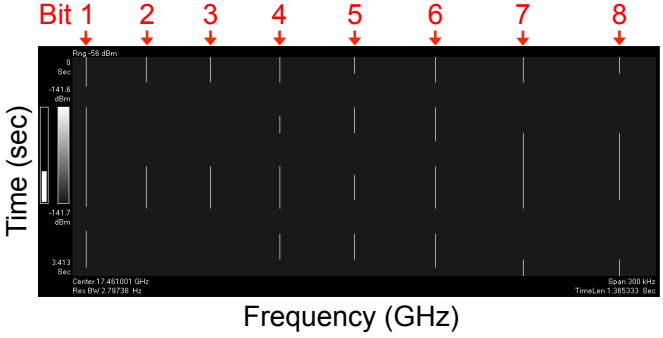


Fig. 20. Measurement results of 17.46 GHz 8 bits RFID for dynamic communications. f_m ranges from 1 MHz to 1.39 MHz. Symbol patterns: (11111111), (00000000), (10011100), (10000011).

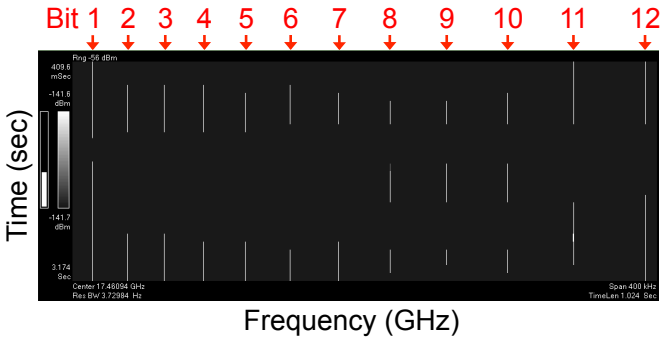


Fig. 21. Measurement results of 17.46 GHz 12 bits RFID for dynamic communications. f_m ranges from 1 MHz to 1.79 MHz. Symbol patterns: (111111111111), (000000000000), (100000011100), (100000000011).

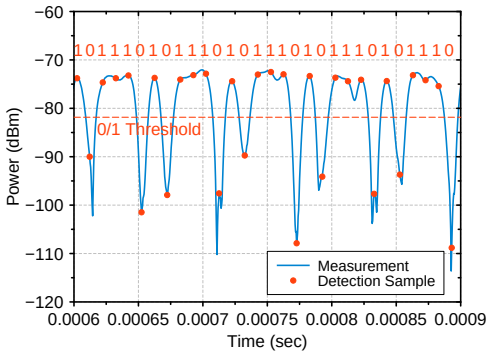


Fig. 22. Measured signal strength of the transmitted symbols. Solid curve is the modulated backscatter signals while red circles are the post-measurement signal processing sampled signals. A threshold value is set at -81 dBm to detect a symbol pattern of (111010).

Note that the plastic enclosure as obstruction between the tag and the T_x/R_x can cause extra 1 to 2 dB attenuation. The measurement results shown in Fig. 22 is without obstruction for better SNR demonstration.

V. Conclusions

In this paper, we have introduced a new class of side-channels that is a consequence of impedance changes in switching circuits, and we refer to it as an *impedance-based side-channel*. One example of such a side-channel is when digital logic activity causes incoming EM signals to be modulated as they are reflected (backscattered), at frequencies that depend on both the incoming EM signal and the circuit activity. This can cause EM interference or leakage of sensitive information, but it also can be leveraged for RFID tag design.

This paper first discuss how an impedance-based backscatter channel is created by switching activity of transistors in digital electronic circuitry. Then, we demonstrate that the impedance difference between transistor gates in the high-state and in the low-state changes the radar cross section (RCS) and modulates the backscattered signal. Simulation results show that the proposed RFID can be implemented on ASIC with a 30 dB signal enhancement. Based on this new backscattering channel, we have proposed a novel semi-passive RFID tag, which can reach a distance up to 2 m and can be interrogated at various frequencies between 1 GHz and 26 GHz. Finally, we have illustrated how this design can be adapted for variety of RFID applications across carrier frequencies at 5.8 GHz, 17.46 GHz, and 26.5 GHz. These applications demonstrate flexible carrier frequency selection and bits configuration, such as static IDs with 6, 12, and 36 bits, which provide up to 68.7 billion (2^{36}) combinations of unique IDs, and multi-bit (4, 8, and 12 bits) dynamic RFIDs for communications. A maximum data rate of 100 kbits/sec with a bit error rate (BER) of 0.00000183 (10^{-6}) is achieved.

References

[1] A. Costanzo, S. Bartolini, L. Benini, E. Farella, D. Masotti, B. Milosevic, L. D. Stefano, A. Franchi, T. S. Cinotti, S. Mattarozzi, and V. Nannini, "Merging rfid, visual and gesture recognition technologies to generate and manage smart environments," in *2011 IEEE International Conference on RFID-Technologies and Applications*, Sept 2011, pp. 521–526.

[2] L. Yang, A. Rida, R. Vyas, and M. M. Tentzeris, "Rfid tag and rf structures on a paper substrate using inkjet-printing technology," *IEEE Transactions on Microwave Theory and Techniques*, vol. 55, no. 12, pp. 2894–2901, Dec 2007.

[3] S.-J. Wu and T.-G. Ma, "A passive uhf rfid meandered tag antenna with tuning stubs," in *2006 Asia-Pacific Microwave Conference*, Dec 2006, pp. 1486–1492.

[4] P. Pursula, T. Vaha-Heikkila, A. Muller, D. Neculoiu, G. Konstantinidis, A. Oja, and J. Tuovinen, "Millimeter-wave identification–a new short-range radio system for low-power high data-rate applications," *IEEE Transactions on Microwave Theory and Techniques*, vol. 56, no. 10, pp. 2221–2228, Oct 2008.

[5] S. Lemey, S. Agneessens, P. V. Torre, K. Baes, J. Vanfleteren, and H. Rogier, "Wearable flexible lightweight modular rfid tag with integrated energy harvester," *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, no. 7, pp. 2304–2314, July 2016.

[6] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications In Contactless Smart Cards and Identification*, 3rd ed. Hobeken, NJ, USA: John Wiley and Sons, 2005.

[7] F. Pebay-Peyroula, J. Reverdy, E. Crochon, and T. Thomas, "Very high data rate contactless air interface: An innovative solution for card to reader link," in *2010 IEEE International Conference on RFID (IEEE RFID 2010)*, April 2010, pp. 203–209.

[8] N. Pillin, N. Joehl, C. Dehollain, and M. J. Declercq, "High data rate rfid tag/reader architecture using wireless voltage regulation," in *2008 IEEE International Conference on RFID*, April 2008, pp. 141–149.

[9] J. Besnoff, M. Abbasi, and D. S. Ricketts, "High data-rate communication in near-field rfid and wireless power using higher order modulation," *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, no. 2, pp. 401–413, Feb 2016.

[10] S. Tedjini, N. Karmakar, E. Perret, A. Vena, R. Koswatta, and R. E-Azim, "Hold the chips: Chipless technology, an alternative technique for rfid," *IEEE Microwave Magazine*, vol. 14, no. 5, pp. 56–65, July 2013.

[11] V. Coskun, K. Ok, and B. Ozdenizci, *Developing NFC Applications*. Wiley Telecom, 2012. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=8044008

[12] [Online]. Available: https://www.grandviewresearch.com/industry-analysis/near-field-communication-nfc-market

[13] P. Chan and V. Fusco, "Bi-static 5.8ghz rfid range enhancement using retrodirective techniques," in *2011 41st European Microwave Conference*, Oct 2011, pp. 976–979.

[14] W. G. Yeoh, Y. B. Choi, L. H. Guo, A. P. Popov, K. Y. Tham, B. Zhao, and X. Chen, "A 2.45-ghz rfid tag with on-chip antenna," in *IEEE Radio Frequency Integrated Circuits (RFIC) Symposium, 2006*, June 2006, pp. 4 pp.–.

[15] I. Vaisband and E. G. Friedman, "Stability of distributed power delivery systems with multiple parallel on-chip ldo regulators," *IEEE Transactions on Power Electronics*, vol. 31, no. 8, pp. 5625–5634, Aug 2016.

[16] E. Perret, M. Hamdi, G. E. P. Tourtollet, R. Nair, F. Garet, A. Delattre, A. Vena, L. Duvillaret, P. Martinez, S. Tedjini, and Y. Boutant, "Thid, the next step of chipless rfid," in *2013 IEEE International Conference on RFID (RFID)*, April 2013, pp. 261–268.

[17] S. Preradovic and N. C. Karmakar, "Design of fully printable planar chipless rfid transponder with 35-bit data capacity," in *2009 European Microwave Conference (EuMC)*, Sept 2009, pp. 013–016.

[18] M. Ppperl, J. Adametz, and M. Vossiek, "Polarimetric radar barcode: A novel chipless rfid concept with high data capacity and ultimate tag robustness," *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, no. 11, pp. 3686–3694, Nov 2016.

[19] [Online]. Available: https://www.ifixit.com/Teardown

[20] D. Wu, M. J. Hussain, S. Li, and L. Lu, "R2: Over-the-air reprogramming on computational rfids," in *2016 IEEE International Conference on RFID (RFID)*, May 2016, pp. 1–8.

[21] D. D. Donno, L. Catarinucci, A. D. Serio, and L. Tarricone, "A long-range computational rfid tag for temperature and acceleration sensing applications," in *Progress In Electromagnetics Research C*, vol. 45, 2013, pp. 223–235.

[22] R. Colella, D. D. Donno, L. Tarricone, and L. Catarinucci, "Unconventional uhf rfid tags with sensing and computing capabilities," in *Journal of Communications Software and Systems*, vol. 10, 2014, pp. 83–89.

[23] T. Bjorninen, M. Lauri, L. Ukkonen, R. Ritala, A. Z. Elsherbeni, and L. Sydanheimo, "Wireless measurement of rfid ic impedance," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 9, pp. 3194–3206, Sept 2011.

[24] M. S. Reynolds, "A $500^o c$ tolerant ultra-high temperature 2.4 ghz 32 bit chipless rfid tag with a mechanical bpsk modulator," in *2017 IEEE International Conference on RFID (RFID)*, May 2017, pp. 144–148.

[25] H. Stockman, "Communication by means of reflected power," *Proceedings of the IRE*, vol. 36, no. 10, pp. 1196–1204, Oct 1948.

[26] J. D. Griffin and G. D. Durgin, "Complete link budgets for backscatter-radio and rfid systems," *IEEE Antennas and Propagation Magazine*, vol. 51, no. 2, pp. 11–25, April 2009.

[27] J. M. Rabaey, A. Chandrakasan, and B. Nikolic, *Digital Integrated Circuits*, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2008.

[28] M. Prvulovic, A. Zaji, R. L. Callan, and C. J. Wang, "A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems," *IEEE Transactions on Electromagnetic Compatibility*, vol. 59, no. 1, pp. 34–42, Feb 2017.

[29] [Online]. Available: http://rfbayinc.com/products_pdf/product_2_520.pdf

[30] [Online]. Available: https://fccid.io/VBLFMR-6000/User-Manual/Users-Manual-1393998

[31] [Online]. Available: http://www.rfidmarket.com.tr/Data/EditorFiles/CMR-6100.pdf

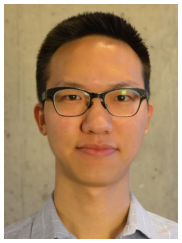
[32] [Online]. Available: http://www.scanditron.com/sites/default/files/material/heraeus_bondingwire_brochure.pdf

[33] [Online]. Available: https://chemandy.com/calculators/round-wire-ac-resistance-calculator.htm

[34] [Online]. Available: http://edadocs.software.keysight.com/pages/viewpage.action?pageId=5512312

[35] [Online]. Available: http://edadocs.software.keysight.com/pages/viewpage.action?pageId=5512639

[36] *Cyclone V Device Datasheet*, CV-51002. Altera Corporation (Intel Programmable Solutions Group), 12 2016.



Chia-Lin Cheng (S'17) received the B.Sc. degree in electrical engineering from the National Taiwan University in 2013 and the M.Sc. degree in electrical engineering from the Georgia Institute of Technology in 2017, respectively. He is currently pursuing his PhD in the Electromagnetic Measurements in Communications and Computing (EMC^2) Lab at the Georgia Institute of Technology focusing on mm-wave and THz wireless channel measurements and modeling. Previously, he worked on signal integrity and non-linear circuits I/O modeling by using machine learning techniques. His research interests span areas of electromagnetics, wireless channel measurements and modeling. He was the recipient of the Best Poster Award at the IEEE International Conference on RFID 2018.

Luong N. Nguyen received the B.Sc. degree in Electrical and Computer Engineering from the Hanoi University of Science and Technology in 2013 and the M.Sc. degree in Electrical and Computer Engineering from the Seoul National University in 2016. Since 2016, he has been a Graduate Research Assistant in the Electromagnetic Measurements in Communications and Computing (EMC^2) Lab, pursuing the Ph.D. degree in the School of Electrical and Computer Engineering, Georgia Institute of Technology focusing on digital circuit design, software and hardware security, and embedded system. His current research interests span areas of ASIC design, computer architecture, and electrical engineering.

He is a past recipient of the Korean Government Scholarship Program, and the best paper award from the 2014 Korean SoC conference.

Milos Prvulovic (S97-M03-SM09) received the B.Sc. degree in electrical engineering from the University of Belgrade in 1998, and the M.Sc. and Ph.D. degrees in computer science from the University of Illinois at Urbana-Champaign in 2001 and 2003, respectively. He is an Associate Professor in the School of Computer Science at the Georgia Institute of Technology, where he joined in 2003. His research interests are in computer architecture, especially hardware support for software monitoring, debugging, and security. He is a past recipient of the NSF CAREER award, and a senior member of the ACM, the IEEE, and the IEEE Computer Society.

Alenka Zajić (S99-M09-SM13) received the B.Sc. and M.Sc. degrees form the School of Electrical Engineering, University of Belgrade, in 2001 and 2003, respectively. She received her Ph.D. degree in Electrical and Computer Engineering from the Georgia Institute of Technology in 2008. Currently, she is an Associate Professor in the School of Electrical and Computer Engineering at Georgia Institute of Technology. Prior to that, she was a visiting faculty member in the School of Computer Science at Georgia Institute of Technology, a post-doctoral fellow in the Naval Research Laboratory, and a design engineer at Skyworks Solutions Inc. Her research interests span areas of electromagnetic, wireless communications, signal processing, and computer engineering. Dr. Zajic was the recipient of the 2017 NSF CAREER award, the Best Paper Award at MICRO 2016, 2012 Neal Shepherd Memorial Best Propagation Paper Award, the Best Student Paper Award at the IEEE International Conference on Communications and Electronics 2014, the Best Paper Award at the International Conference on Telecommunications 2008, the Best Student Paper Award at the 2007 Wireless Communications and Networking Conference, and the Dan Noble Fellowship in 2004, which was awarded by Motorola Inc. and the IEEE Vehicular Technology Society for quality impact in the area of vehicular technology.