A Nonvolatile Flip-Flop-Enabled Cryptographic Wireless Authentication Tag With Per-Query Key Update and Power-Glitch Attack Countermeasures

Hyung-Min Lee, *Member, IEEE*, Chiraag S. Juvekar, *Student Member, IEEE*, Joyce Kwong, *Member, IEEE*, and Anantha P. Chandrakasan, *Fellow, IEEE*

***Abstract*— Counterfeiting is a major issue plaguing global supply chains. In order to mitigate this problem, a wireless authentication tag is presented that implements a cryptographically secure pseudorandom number generator and authenticated encryption modes. The tag uses Keccak, the cryptographic core of SHA3, to update keys before each protocol invocation, limiting side-channel leakage. Power-glitch attacks are mitigated through state backup on ferroelectric capacitor-based nonvolatile flip-flops with a fully integrated energy backup storage, which needs a 2.2× smaller area compared with conventional approaches. The 130 nm CMOS tag harvests wireless power through a 433 MHz inductive link and communicates with a reader by a pulse-based modulation that minimizes the wireless power dead time. The proposed regulating voltage multiplier simultaneously rectifies, boosts, and regulates a >0.55 V ac input to a 1.5 V supply voltage with <1.1% line and load regulation while requiring only one on-chip decoupling capacitor. The bidirectional data telemetry operates at 125 kb/s, while requiring 4% (downlink) and 6.25% (uplink) duty cycles. Full system operation including the tag, reader, and server protocol is demonstrated in the presence of worst-case power interruption events.**

***Index Terms*— Authentication tag, cryptographic engine, encryption, energy backup, ferroelectric capacitor (FeCap), inductive link, power-glitch attack, pulse-based wireless telemetry, side-channel attack, wireless power transfer.**

I. Introduction

COUNTERFEITING is a major problem plaguing both the retail sector as well as global supply chains. In the past few years, multimillion dollar losses have been attributed to counterfeit automotive parts, aircraft parts, and pharmaceutical drugs. An electronic tag affixed to these components offers a convincing solution for authenticating them at the time of purchase [1]. Unfortunately, this also has the side effect of making the tags themselves a lucrative target for counterfeiters. Due to the embedded nature of these tagging solutions, protecting them necessitates effective countermeasures against physical attacks [2] such as fault injection [3] and side-channel attacks [4]. This makes the design of a secure authentication tag a challenging and interesting problem.

Recent work on the design of RFID-like authentication tags can be roughly classified into two categories. First, we have simple low-cost organic RFID tags that can be integrated on flexible substrates [5], [6]. These tags typically do not integrate any security features or nonvolatile (NV) memory due to technology limitations [7]. Second, we have CMOS tags that are designed for more complex use cases such as those where security is a concern [8], [9]. Here, cryptographic primitives are implemented to support authenticated modes of operation. Even when secure algorithms are used, the tags may still be vulnerable to implementation-based attacks since the attacker can leverage physical access to the tag [10]. The cost-sensitive RFID systems make deploying circuit-level countermeasures against physical attacks challenging.

Algorithmic countermeasures that use key update to provide physical attack resilience are a viable solution to this problem [11], [12]. Our work builds on these ideas and leverages circuit and technology innovations to enable one of the first physical embodiments of a wireless tagging solution using a low overhead key update protocol. Our key contributions are summarized as follows.

1) A cryptographic challenge–response protocol is implemented to allow a server to securely authenticate the tag.
2) The tag uses Keccak [13], the cryptographic core of SHA3, to update cryptographic keys before each protocol invocation, to prevent side-channel attacks.
3) Power-glitch attacks are mitigated via state backup on ferroelectric capacitor (FeCap)-based NV flip-flops (NVDFFs) [14] using the on-chip energy backup storage.
4) Wireless power and data telemetry (WPDT) circuits are optimized for compact size and robust operation in near-field applications using an inductive link.

Manuscript received April 19, 2016; revised June 25, 2016; accepted September 8, 2016. Date of publication December 26, 2016; date of current version January 4, 2017. This paper was approved by Guest Editor Subhasish Mitra. This work was supported in part by Denso and in part by Texas Instruments.

H.-M. Lee was with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 USA. He is now with the IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA (e-mail: hyungmin@us.ibm.com).

C. S. Juvekar and A. P. Chandrakasan are with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: anantha@mtl.mit.edu).

J. Kwong was with Texas Instruments, Dallas, TX 75243 USA (e-mail: joycekwong@alum.mit.edu).

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/JSSC.2016.2611678

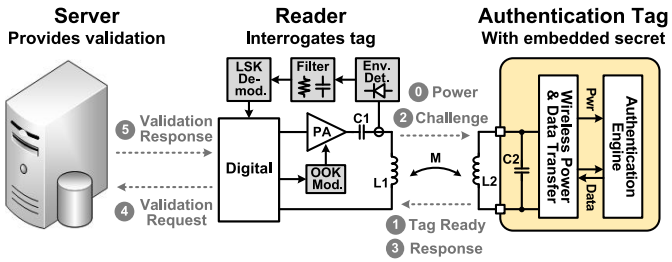

Fig. 1. Authentication system consisting of the tag, the handheld reader, and the back-end server.

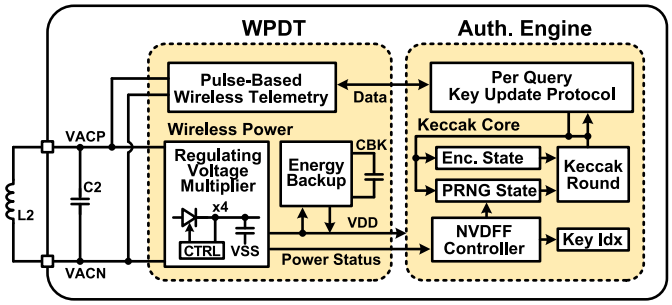

Fig. 2. Overview of the key features implemented on the authentication tag.

The rest of this paper, which is an extended version of [15], focuses on our authentication protocol, detailed circuit techniques, performance analysis, and measurement results that fully describe our authentication tag.

II. System Architecture

A. Authentication System and Tag Overview

Fig. 1 shows the three major components of our authentication system: authentication tags that are affixed to the equipment being protected, a reader to interrogate these tags and verify their authenticity, and a back-end server that seeds the tags with an initial secret during an enrollment step at manufacture and then maintains a database in order to validate tag responses.

The authentication tag consists of an on-chip authentication engine (AE) that supports the required cryptographic protocols and a WPDT frontend that harvests energy from the reader using a 433 MHz near-field inductive link. The AE implements our per-query key update protocol using the Keccak algorithm to provide cryptographically secure pseudorandom number generation (CS-PRNG) and authenticated encryption functionalities. NVDFFs are used to implement all the cryptographic states on the tag. A regulating voltage multiplier (RVM) is implemented for efficient power conversion, and pulse-based modulation is used to reduce wireless power dead time during telemetry. When combined with an on-chip energy backup unit (EBU), the NVDFFs provide robust countermeasures against power-glitch attacks. Fig. 2 presents a block diagram of the tag summarizing these contributions.

B. Threat Model and Implemented Countermeasures

The proposed tags are meant to protect relatively low-cost equipment in the U.S. $10–$500 range. The threat model that we consider in this paper is hence limited to those attacks where the amortized cost of an attack is lower than the cost of the equipment being authenticated, such as follows.

1) *Passive Side-Channel Attacks:* The attacker may passively monitor the power consumed and the electromagnetic (EM) emission radiated by the tag to mount a differential power analysis (DPA) or a differential EM analysis attack.
2) *Active Power Glitch Attacks:* The attacker may introduce overvoltage or undervoltage power supply glitches to leak bits by inducing faults during cryptographic or NV memory operation.
3) *Protocol Attacks on Tag-Reader Communication:* The attacker may capture, corrupt, and replay any transaction between the tag and the reader.

Physical probing and photon emission attacks can potentially be used for extracting secret key material. However, repeating such attacks on a per tag basis would be cost prohibitive for the class of equipment we aim to protect with the proposed tags, and hence are not addressed here.

TABLE I
State-Dependent NVDFF Energy Consumption

Initial State	Final State	Regular Mode Energy/bit (fJ)	Backup-Restore Energy/bit (pJ)
0	0	7.660	2.501
	1	52.454	-
1	0	30.344	-
	1	7.365	1.402

The NVDFFs used in this paper exhibit state-dependent power consumption during both regular operation and backup modes as shown in Table I, and side-channel countermeasures are necessary. Simple power analysis (SPA) attempts to recover key material based on direct inspection of single traces. These attacks are most effective on small data paths where the power trace information can be correlated with the Hamming weight of an intermediate result [16] or when control flow of the algorithm depends on intermediate values [17]. Our AE implementation is constant time with no-state-dependent control flow. In both regular as well as backup modes of operation, all 400 NVDFFs are simultaneously updated. Running an SPA on such a large intermediate state seems challenging.

DPA-style attacks that involve the collection of multiple power traces with varying plaintexts for the same key [18] are still a potential attacker vector. These attacks work because specific points on the power trace are well correlated with a subset of key bits. By trying various guesses for those key bits and correlating them with measured data, we observe that the correct guess correlates more strongly with the measured power after a certain threshold number of traces is reached. We protect against these attacks by deploying a protocol that ensures that the same key is never used twice for any cryptographic operation. Thus multiple power traces with the same key cannot be collected.

In practice, the implementation of such a key update mechanism is complicated by the fact that the tags are passively

powered by a reader, which may be hostile. An attacker may interrupt the power supply during the key update operation hoping that the tag will either revert to using the old key or repeat the key update. If this happens, the tag performs multiple cryptographic computations using the same key making side-channel attacks possible. Similar attacks have been demonstrated in the context of secure EEPROM memories [19]. We mitigate these classes of attacks using NVDFFs to store both the cryptographic state as well as the relevant control registers on the tag. In case power is interrupted, all computation is simply paused, and the state is backed up to the NV memory [14]. On the next power-up, the state is restored, and computation continues seamlessly without repeating even a single cycle of cryptographic computation. Careful codesign of the controller sequencing these operations and the EBU enables to handle all corner cases as described in Section V-C.

C. Protocol Details

The server initializes each tag with a 64 b public chip ID and a unique 256 b secret seed. Ideally, after this seed is written into the NVDFFs, a single-bit fuse could be burned indicating that seeding is disabled. In order to reduce design complexity, the corresponding fuse is not implemented in our test chip. At a high level, an iteration of the challenge–response protocol consists of the following steps. On receiving power from the reader, the tag first charges its backup energy storage before the AE is activated. Next, the AE wakes up and updates its key using the Keccak-based CS-PRNG, increments the key index, and indicates to the reader that it is ready for the next challenge. The reader then sends the tag a random challenge to which the tag responds using an authenticated encryption with associated data (AEAD) mode of operation [20]. The reader then sends this challenge–response pair to a trusted server for validation. Fig. 3 depicts our per-query key update protocol.

Given the initial seed values, it is possible to clone tags, and hence it is crucial that the server verification database is kept secret. The use of a CS-PRNG to generate fresh keys mitigates side channel and replay attacks. AEAD allows us to support both tag authentication as well as support future tag versions where the tag can transmit secret information, such as the state of on-chip sensors, back to the server. Both the CS-PRNG and AEAD modes use the Keccak algorithm [20], [21], and are implemented by sharing common hardware on the tag. Both protocol and NVDFF controllers are implemented as finite state machines on chip. The AEAD authentication message is computed using the chip ID, key index, and challenge as associated data. Using the public chip ID and the current key index in the associated data also mitigates any desynchronization attempts. Another advantage of sending the authenticated key index back to the server is that the server can verify that the key indices used in subsequent transactions form a monotonically increasing sequence. Thus, even if an attacker clones a tag, he must ensure that key indices across all the cloned copies are synchronized to prevent detection. On the other hand, the use of the chip ID and key index as associated data also implies that the protocol is no longer privacy preserving. A privacy-preserving protocol that supports key update on the tag without the need for server involvement in the key update is an interesting direction for future work. Finally, we note that the use of a 64 b counter and a minimum time interval of 200 μs between two power-cycle events (imposed by the speed of the save–restore circuits) imply that counter-overflow-based denial-of-service attacks are infeasible.

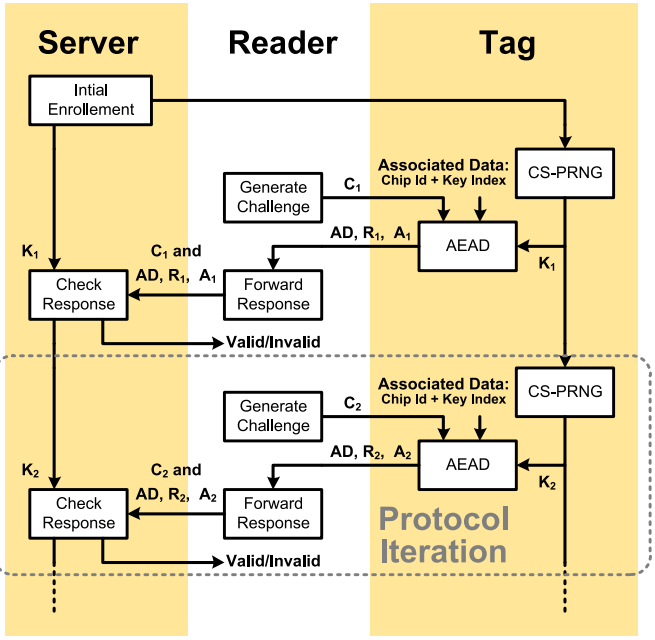

Fig. 3. Block diagram showing our update protocol. K_i are the per-query keys. C_i, AD, R_i, and A_i are the challenge, associated data, response, and authentication message, respectively (see Fig. 6).

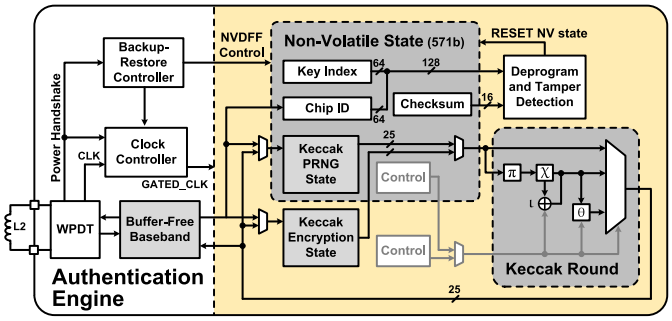

Fig. 4. Overall architecture of the AE circuits.

III. Authentication Engine

A. Overall Architecture

Fig. 4 shows the overall architecture of the AE. The AE includes the Keccak cryptographic core consisting of the state for the CS-PRNG and AEAD modes as well as shared logic implementing the rounds of the Keccak algorithm. The state elements for the CS-PRNG mode, the chip ID, and the key-index are all implemented using a total of 571 NVDFFs. The backup-restore and clock controllers interface these NVDFFs with the WPDT block and implement power-glitch attack countermeasures. A separate deprogramming and tamper detection block computes a checksum over all the

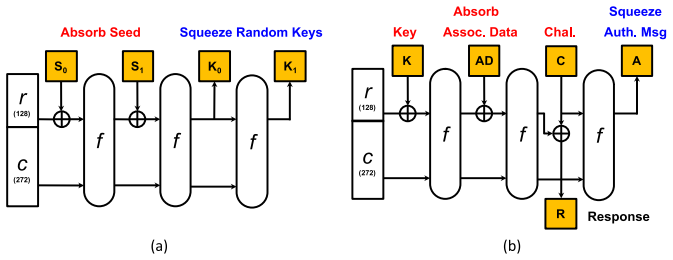

Fig. 5. (a) CS-PRNG mode and (b) AEAD mode of the Keccak algorithm implemented on the AE (r, c, and f represent the rate, capacity, and permutation function, respectively).

NVDFF data and erases all the state in case any mismatch is detected. The AE no longer contains any cryptographic material and must be reseeded by the server before it can respond to any future challenges. The AE, including the NVDFFs, occupies a total of 17.9k NAND gates. Operating at a 125 kHz clock frequency, it consumes 3.6 μW in standby and 8.6 μW when running the authentication protocol.

B. Keccak Algorithm and Implementation

The Keccak algorithm implemented on the tag consists of two major components: an internal state and a permutation function that iteratively operates on that state. It supports two operations: absorb and squeeze and is commonly referred to as a sponge construction [13]. The CS-PRNG and AEAD modes for our authentication protocol can be implemented by combining these operations as shown in Fig. 5. Keccak state can be divided into rate and capacity components with the former determining throughput while the latter determines the security level. The permutation function consists of multiple rounds where each round includes five subrounds, θ, ρ, π, χ, and ι.

We implement the Keccak-f[400] variant of the permutation function which uses a 400 b internal state, compared with the 1600 b state used in SHA3, in order to save area and backup energy as shown in Section V-C. The rate and capacity sizes are set to 128 and 272 b, respectively (compared to 1024 and 576 in SHA3). Although the reduction in rate reduces the throughput, we are still able to scan an average of 30 tags/s. Since the tag can only be seeded once at initialization, we need to only consider the passive state-recovery attack analysis [20]. This results in 272 b security up to 2^{64} iterations of the protocol. Thus the best attack on the CS-PRNG is to instead guess the initial 256 b seed. Use of 128 b keys and authentication messages for AEAD results in 128 b security against key and plaintext recovery as well as authentication forgery [21]. Thus even with a reduced capacity, 128 b security is guaranteed.

The number of rounds used in the permutation function is set to 20 for both the modes following the conservative guidelines used in SHA3 as opposed to the reduced round counts suggested in [21]. Since the internal state of the CS-PRNG must be persisted when the AEAD mode responds to the reader challenges, a separate 400 b state-array is used for the AEAD state. Each array is organized as 25 16 b lane

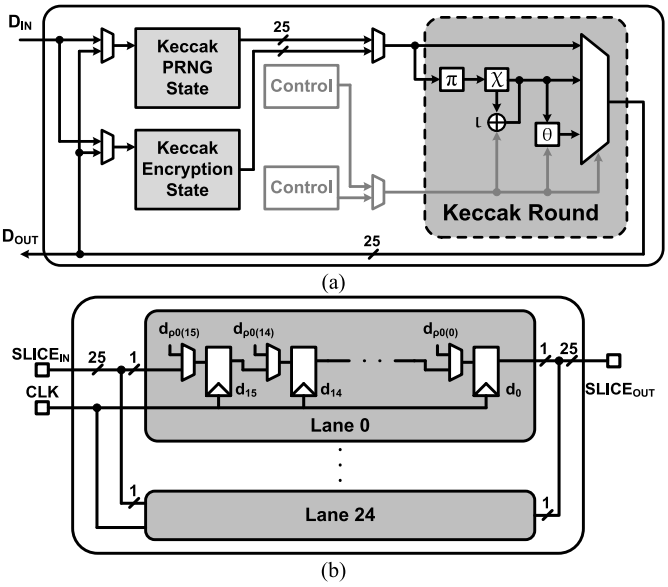

Fig. 6. Keccak architecture sharing a common combinational round implementation across the CS-PRNG and AEAD state. (a) Keccak architecture. (b) Shift register-based Keccak state.

shift registers allowing us to access the state one slice at a time over 16 cycles. Of the five subrounds used in the permutation, four (θ, π, χ, and ι) act on the full slice and hence are they are regrouped and implemented in a common combinational block shared by both the modes. The ρ operation acts on lanes and is implemented with lane-specific hard-coded multiplexers. The Keccak architecture and the state array are presented in Fig. 6. Since most of the literature cites performance metrics for only the core hashing functionality of Keccak, a comparison of our architecture when resynthesized to perform only hashing (and state implemented with regular flip-flops) is presented in Table II.

C. Selective NVDFF Storage

The proposed tag requires low-power NV memory for the save–restore operation and large on-chip capacitors for energy backup storage (described in Section V). To address these design constraints, the tag was implemented in a 130 nm process that offers ferroelectric RAM and capacitor options. The AE uses a standard-cell based design, and the set of cells is augmented with an NVDFF cell. The NVDFF cell consumes 3.2× area of a conventional flip-flop and requires 3.4 pJ of energy for the save–restore operation. This energy must be stored on-chip for security since it is used to mitigate power-glitch attacks. Thus, reducing the number of NVDFFs allows us to reduce the area occupied by both the AE as well as the backup capacitors. Fortunately, only the chip ID, key index counter, the CS-PRNG mode state, and associated control registers need to be saved to recover from a power glitch event. In particular, if a glitch occurs when a response is being generated, all the states associated with the current challenge can be safely erased. When power is restored the tag can update its key and simply respond to a new challenge. Hence the AEAD state and other miscellaneous state elements are

TABLE II
KECCAK CORE BENCHMARKING FOR 400 AND 1600 b STATE SIZES

State Size	Reference	Tech. (nm)	Cycles	Gates (GE)	Power (μW/MHz)	Throughput (kb/s)	Energy/bit (pJ/bit)	Gate Efficiency (kbps/kGE)
400	**This Work**	**130**	**356**	**2421**	**13**	**404.49**	**32.14**	**167.08**
	[22]	250	1000	3113	-	144	-	46.26
	[23]	130	1000	5090	11.5	144	79.87	28.29
1600	**This Work**	**130**	**1624**	**7537**	**41.2**	**827.59**	**49.78**	**109.8**
	[23]	130	1200	20790	44.9	1120	40.09	53.87
	[24]	130	15427	5898	13.7	87.12	157.25	14.77

TABLE III
IMPACT OF KECCAK STATE SIZE AND SELECTIVE NVDFF INSTANTIATION ON AE AREA AND BACKUP ENERGY (ALL AREA IN GE)

	Keccak 400			Keccak 800			Keccak 1600		
	FF Count	All NV Area	Selective Area[A]	FF Count	All NV Area	Selective Area[A]	FF Count	All NV Area	Selective Area[A]
CS-PRNG State	427	6027	6027	828	11639	11639	1629	22851	22851
AEAD State	427	6027	1831	828	11639	3532	1629	22851	6897
Volatile State	144	1728	1728	144	1728	1728	144	1728	1728
AE (Misc.)	334	11219	8362	334	11219	8362	334	11219	8362
Total	**1332**	**25001**	**17948**	**2134**	**36225**	**25261**	**3736**	**58649**	**39838**
NVDFF Count	-	**1332**	**571**	-	**2134**	**972**	-	**3736**	**1773**

[A] Selective architecture uses regular flip-flops for AEAD and misc. AE state.

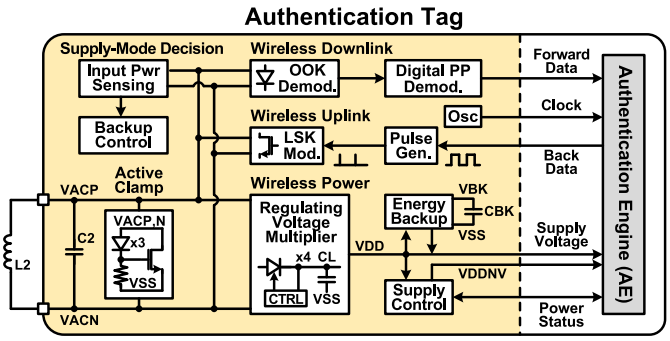

Fig. 7. Overall architecture of the WPDT circuits.

only implemented using regular flip-flops. Table III describes the impact of the reduction in the CS-PRNG state size (400 versus 1600 b in SHA3) and selective NVDFF instantiation on the backup energy and AE area.

IV. WIRELESS POWER AND DATA TELEMETRY

A. Overall Architecture

Fig. 7 shows the overall architecture of the WPDT circuits in the authentication tag. The WPDT circuits use an inductive link with loosely coupled magnetic coils (L_1, L_2) to implement energy harvesting and bidirectional data communication with the reader. Operation in the 433 MHz ISM band enables a small tag form factor using a millimeter-size off-chip L_2 and an on-chip resonant capacitor C_2. A power amplifier (PA) on the reader (Fig. 1) drives the primary coil and induces an ac voltage (V_{ACP} and V_{ACN}) across the secondary. The proposed RVM then converts this into a dc voltage and stores it on an on-chip decoupling capacitor C_L to power the AE. Since the input ac amplitude depends on the coupling coefficient (k), it can vary greatly. The proposed RVM is designed to generate the regulated system supply voltage V_{DD} (=1.5 V) from an input amplitude higher than 550 mV. If the input amplitude becomes too high, an active clamp circuit limits it below 1.2 V by shorting V_{ACP} and V_{ACN} to ground. In addition, pulse-based modulation of the power carrier signal is implemented for bidirectional data telemetry, thus sharing the inductive link and minimizing wireless power interruption. The wireless downlink to the tag employs on–off keying (OOK) and the uplink back to the reader employs load-shift keying (LSK).

Converted dc power is additionally stored on an on-chip backup capacitor C_{BK} to maintain the system operation in the presence of power glitches. When the input power sensing unit detects interruption of inductive power, a backup controller switches the EBU to supply the AE and deactivates the RVM and telemetry circuits to save static power. A supply control unit is implemented to synchronize startup and shutdown timing between the WPDT block and the AE. Correct NVDFF

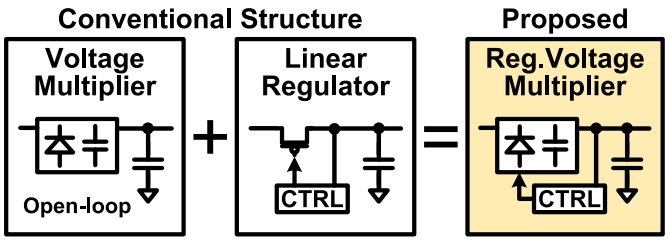

Fig. 8. Conceptual diagram of the RVM.

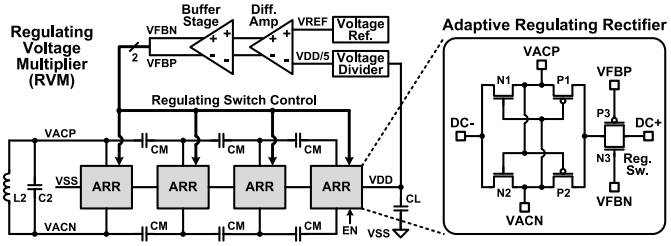

Fig. 9. Schematic of the RVM and its ARR.

operation requires a separate supply rail V_{DDNV} [14] that supports a fast discharge (<5 μs). The supply control unit trickle charges this rail to 1.5 V at startup before connecting it to V_{DD} to avoid supply disruption due to charge sharing.

B. Regulating Voltage Multiplier

Conventional RF frontends implement an ac–dc voltage multiplier to rectify and boost the ac input voltage and generate the required dc output. However, this open-loop output voltage depends on the input ac amplitude and varies based on the link geometry parameters such as coil separation and alignment, necessitating an additional regulator to supply the system [25]. Fig. 8 shows a conceptual diagram of our proposed RVM that combines the voltage multiplier and regulator into a single structure to simultaneously rectify, boost, and regulate a small ac coil voltage to the desired supply voltage. The RVM needs only one decoupling capacitor compared with the conventional voltage multiplier, which typically needs an additional regulator and two decoupling capacitors, requiring larger on-chip area.

Fig. 9 shows the schematic of the RVM utilizing four ac-coupled adaptive regulating rectifiers (ARRs), connected in series to charge-multiplier capacitors C_M (=8 pF) in order to boost V_{DD}. Each ARR consists of cross-coupled NMOS and PMOS transistors, $N_{1,2}$ and $P_{1,2}$, to deliver forward current during the peak of ac inputs without using additional gate-drive circuits [26]. Unlike an open-loop rectifier as in [26], where the dc output level varies depending on the ac input amplitude, the proposed ARR utilizes regulating switches N_3 and P_3 to adjust a dc output level through negative feedback signals V_{FBN} and V_{FBP} regardless of the ac input amplitude. The V_{DD} is divided and compared with a reference voltage V_{REF} (=300 mV) through a differential amplifier and a buffer. Then, V_{FBN} and V_{FBP} adaptively control dropout voltages across regulating switches in ARRs to regulate V_{DD} to 1.5 V.

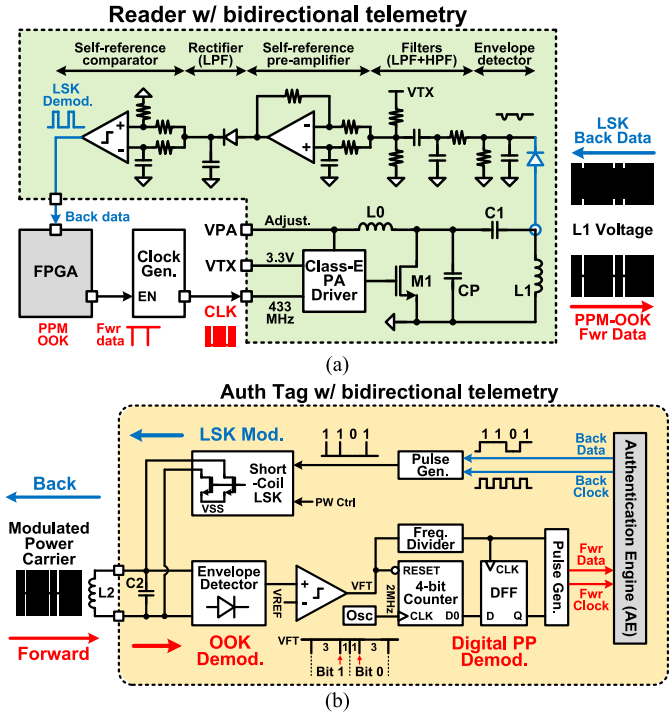

Fig. 10. Block diagram of (a) reader and (b) authentication tag with emphasis on pulse-based bidirectional data telemetry.

Additionally, this built-in regulation also limits each ARR dc output below V_{DD} for overvoltage self-protection, thus alleviating the need for high-voltage transistors in the RVM.

While a dominant pole results from the V_{DD} node due to a large C_L, a source–follower buffer stage on the feedback loop ensures stable regulation by moving nondominant poles to higher frequencies. Since the RVM generates the system V_{DD}, it must have self-startup capability. During startup, both V_{FBN} and V_{FBP} initially stay at 0 V, and V_{ACP} or V_{ACN} can be connected to the ARR output dc+ through the transistor P_1 or P_2 and the regulating switch P_3 to charge C_M and boost V_{DD}. Therefore, as long as the $V_{ACP,N}$ amplitude is greater than 550 mV, this system can start up.

C. Pulse-Based Data Telemetry

Wireless data telemetry through modulation of the power carrier signal enables bidirectional communication between the tag and the reader through the same inductive link. Among various modulation schemes, OOK, which turns on and off the carrier signal, offers robust data transfer against coil coupling variations and allows simple data recovery circuits in the tag. However, the 50% duty-cycled pulsewidth modulated OOK sacrifices half of the wireless power time by turning off the carrier signal for a low data bit, limiting the power delivered to the tag [26]. To ensure high average power delivered to the tag, we utilize a pulse-position modulation (PPM) scheme with short off-times to minimize the wireless power dead time.

Fig. 10 shows the block diagram of the reader and the tag with emphasis on the pulse-based data telemetry. During forward telemetry, a field-programmable gate array (FPGA) on the reader controls a clock generator to provide

a 433 MHz PPM clock to a class-E PA, leading to PPM-OOK power carrier signals across L_1. Then, an envelope detector on the tag rectifies and OOK demodulates the envelope of the power carrier received by L_2, and a comparator recovers the PPM forward telemetry signal V_{FT}. The PPM signal has two pulse positioning ratios among three pulses, 3:1 for high data bit and 1:3 for low data bit, and each pulsewidth can be as low as 0.16 μs. An all-digital PP demodulator, which uses a 2 MHz counter to count the number of clock cycles for $V_{\mathrm{FT}} = 0$ and 1, distinguishes PPs and extracts 125 kb/s data from V_{FT}, without consuming static power.

Back telemetry uses LSK by closing switches across L_2 for 0.5 μs (per high bit) to generate voltage variations across L_1. In the tag, the 50% duty-cycle back data at 125 kb/s from the AE is simply converted into 0.5 μs pulse trains instead of using an additional PP modulator in the tag. The pulse trains drive switches connected between L_2 nodes and V_{SS}, resulting in load changes reflected to the L_2C_2-tank. Then, the voltage changes across L_1 are detected, filtered, amplified, and digitized to generate the LSK-demodulated signal, which is oversampled in the FPGA to recover the data bits. A diode rectifier after the amplifier operates as a low-pass filter to broaden the pulsewidth. An inverter-based ring oscillator is used to generate the on-chip clock, and the reader performs clock recovery to compensate for tag reader clock drift and set the appropriate downlink clock bit period.

V. Energy Backup and Power Glitch Countermeasures

A. Area-Optimal Energy Backup Design

In the case wireless power is interrupted, the energy backup storage provides the energy required for both the NVDFF save–restore as well as key update. The following three constraints need to be satisfied for safe operation: total backup energy of 3.5 nJ must be supplied, V_{DD} droop must be regulated within 10%, and finally the on-chip decoupling capacitor C_L must store 0.5 nJ to support the instantaneous current resulting from the parallel save–restore of all 571 NVDFFs. One approach is to size C_L to also meet the first two constraints, according to the following equation:

$$E_{\mathrm{CL}} = \frac{1}{2} \times C_{\mathrm{LVF}} \times A_{\mathrm{CL}} \times \left(V_{\mathrm{DD}}^2 - V_{\mathrm{DD(MIN)}}^2\right) \quad (1)$$

where E_{CL} is the required energy (3.5 nJ), C_{LVF} is the capacitance per unit area, A_{CL} is the on-chip area of C_L, and $V_{\mathrm{DD(MIN)}}$ is set to 1.35 V (10% maximum droop). Even when using high-density low-voltage FeCaps (1.5 LV FeCaps), this approach consumes 0.8 mm^2 silicon area.

A more area-efficient approach is to separate the decoupling (instantaneous energy) and backup (total energy) requirements. In this approach, we continue to use the LV FeCaps for decoupling but use high-voltage FeCaps (3.3 V HV FeCaps) for backup. The main advantage is that although the HV FeCaps have a lower capacitance per unit area C_{HVF}, they allow higher energy densities as they can be charged to a higher voltage compared with C_L.

Fig. 11 describes the design methodology for area-optimal energy backup design. At startup the EBU charges

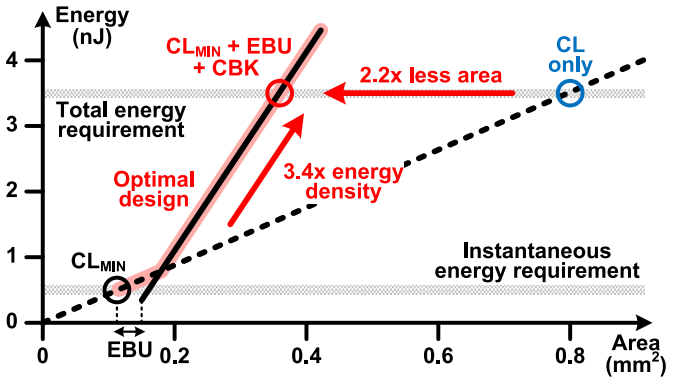

Fig. 11. Area-optimal energy backup storage design using the backup capacitor (C_{BK}) and the EBU.

C_{BK} to 2.75 V. On interruption of wireless power, energy stored in C_{BK} is supplied to the AE through a linear regulator. The EBU details are described in Section V-B. C_{BK} and C_L are sized to satisfy the following equations:

$$\begin{aligned} E_{\mathrm{TOTAL}} &= E_{\mathrm{CL}} - E_{\mathrm{EBU}} + [E_{\mathrm{CBK}} \times \eta_{\mathrm{REG}}] \\ &= E_{\mathrm{CL}} - E_{\mathrm{EBU}} + \left[\frac{1}{2} \times C_{\mathrm{HVF}} \times A_{\mathrm{CBK}} \times \left(V_{\mathrm{BK}}^2 - V_{\mathrm{DD(MIN)}}^2\right) \times \eta_{\mathrm{REG}}\right] \end{aligned} \quad (2)$$

where E_{Total} is the required energy (3.5 nJ), E_{CL} is the decoupling energy (0.5 nJ), E_{EBU} is the energy consumption of the EBU, E_{CBK} is the available energy from C_{BK}, η_{REG} is the efficiency of the EBU regulator, and A_{CBK} is the on-chip area of C_{BK}. η_{REG} can be averaged to 79% when C_{BK} is discharged from V_{BK} (2.75 V) to $V_{\mathrm{DD(MIN)}}$ (1.35 V). E_{EBU} was simulated to be 0.2 nJ, the EBU area A_{EBU} was found to be 0.04 mm^2 from postlayout, and C_L is sized to 0.11 mm^2 to supply 0.5 nJ. By solving (2), we find that C_{BK} must be sized at 0.21 mm^2. Thus, the total area for energy backup including C_L, C_{BK}, and the EBU is just 0.36 mm^2, which is 2.2× lower than the conventional approach of using a single high-density LV FeCap.

B. Energy Backup Unit

Fig. 12 shows the block diagram of the EBU and its clock-controlled voltage doubler. The EBU has three operation modes: charging, standby, and backup. In the charging mode, the EBU uses wireless power to charge C_{BK} to 2.75 V through a voltage doubler supplied by the RVM at 1.5 V. In the standby mode, the EBU holds the charging voltage of C_{BK} to 2.75 V by automatically refreshing through the same voltage doubler, while the AE is powered through the RVM. If the input power sensing circuit in Fig. 7 detects loss of wireless power, the EBU disables the voltage doubler and enters the backup mode. Then, C_{BK} powers V_{DD} through a linear regulator until the AE completes key update and safe shutdown.

The clock-controlled voltage doubler uses a strong-arm comparator to compare a divided V_{BK} with a reference voltage V_{REF} and generate a clock output signal when V_{BK} is below 2.75 V. Then, the inverted comparator output V_{CB} is

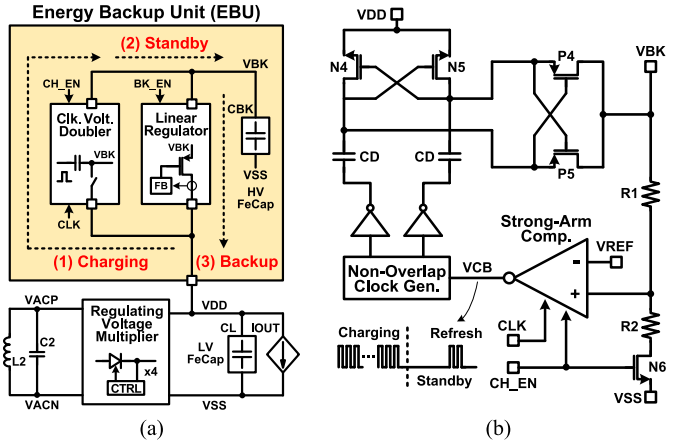

Fig. 12. Block diagram of (a) EBU and (b) its clock-controlled voltage doubler.

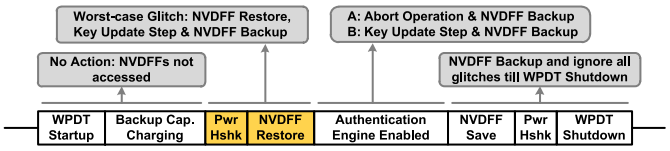

Fig. 13. Power-glitch response as a function of the tag state.

fed into a nonoverlapped clock generator, whose output clocks operate a cross-coupled switched-capacitor (SC) voltage doubler to charge C_{BK}. Once V_{BK} exceeds 2.75 V, V_{CB} is held at 0 V and the SC voltage doubler is deactivated. When V_{BK} eventually falls below 2.75 V due to the small power consumption (<1.5 μW for monitoring V_{BK}) of the EBU, the voltage doubler automatically refreshes C_{BK} to maintain $V_{BK} = 2.75$ V.

C. Energy Control During Power Glitches

The RVM regulates power glitches overshoot within 10% of V_{DD} (Section VI-B). The AE was designed and experimentally verified to tolerate this level of V_{DD} overshoot. An undervoltage glitch shorter than 0.5 μs is interpreted as a spurious bit by the telemetry circuit and ignored since it is not a part of a well-formed packet. The power glitch response to a longer undervoltage glitch depends on the exact state of the tag when power is lost as shown in Fig. 13. Initially, the AE is first held during the EBU charging mode. After this the AE requests trickle charging of V_{DDNV} before NVDFF restore. If power is lost before this completes, no action needs to be taken, as the NVDFFs have not been accessed yet. Once V_{DDNV} reaches 1.5 V, and NVDFF restore is started, any power loss necessitates that the restore, a key-update cycle, and save-all be performed from C_{BK}. After the NVDFFs are restored, the AE tries to complete the key update before running the challenge–response protocol. Power loss at this point is handled separately based on whether the AE was running in the CS-PRNG mode or AEAD mode. The former indicates that a key update was in progress and must be resumed later, while the latter indicates that the previous challenge was aborted and a new key update must be started.

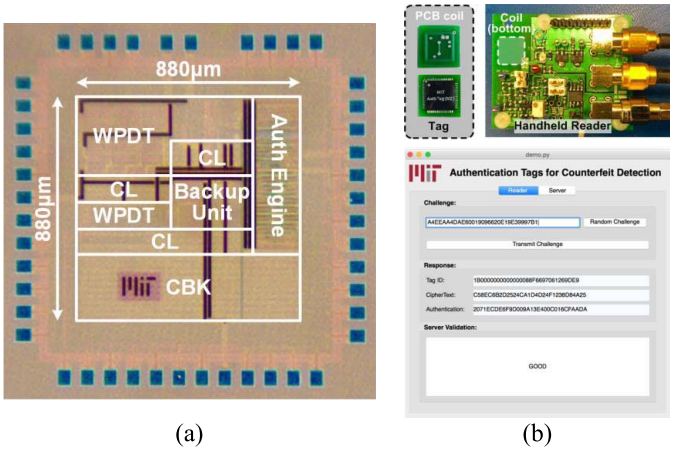

Fig. 14. (a) Chip micrograph and floorplan of the authentication tag. (b) Test setup with the tag and reader (top) controlled by a back-end server software (bottom).

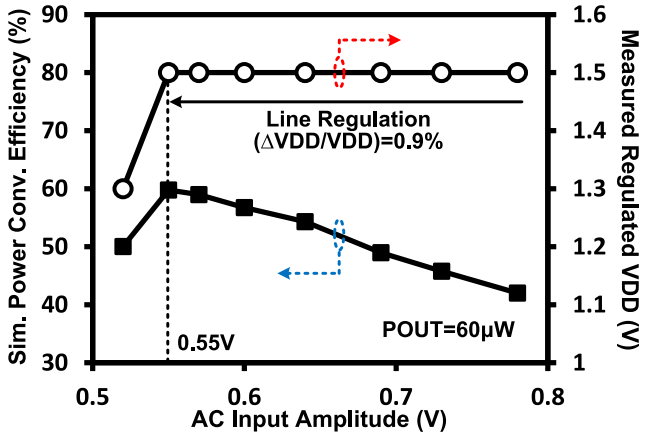

Fig. 15. Power/voltage conversion efficiency and regulation capability of the RVM.

Finally, glitches during the save operation are ignored, as the ongoing save can be completed from the decoupling capacitor.

VI. Measurement Results

A. Chip Micrograph and Test Setup

The authentication tag was fabricated in a 130 nm CMOS process and occupies 0.77 mm^2 area. Fig. 14(a) shows the chip micrograph and floorplan including the WPDT circuits, EBU, AE, and on-chip capacitor C_L and C_{BK}. Fig. 14(b) shows the test setup with the tag and the reader controlled by the backend server software. The tag is attached to an 8 mm printed circuit board PCB coil ($L_2 = 35$ nH) and wirelessly scanned by a discrete handheld reader with a 10 mm power coil ($L_1 = 23.5$ nH). The reader is controlled by an Opal Kelly XEM6001 FPGA board and transfers wireless power and data to scan the tag over a 433 MHz inductive link across a 5 mm separation. The backend server runs on a laptop connected to the reader to demonstrate tag enrollment and authentication.

B. Wireless Power and Data Telemetry

Fig. 15 shows the power/voltage conversion efficiency and regulation capability of the RVM. The RVM generated

TABLE IV
WIRELESS POWER CONVERSION CIRCUIT BENCHMARKING

Publication		2014 [25]	2015 [27]	2015 [28]	**This work**
Technology		180nm CMOS	65nm CMOS	180nm CMOS	**130nm CMOS**
Structure		Voltage Multiplier + Regulator	Rectifier + Regulator	Regulating Rectifier	**Regulating Voltage Multiplier**
Frequency (MHz)		915	300	144	**433**
$V_{AC(PEAK)}$ (V)		-	0.6 [A]	1.2	**0.55**
V_{DD} (V) [B]		1.8	0.5	1	**1.5**
I_{LOAD} (μA)		350	315	100	**40**
VCR		-	0.83	0.92	**2.73**
PCE (%)	AC-DC [C]	52	84	54	**60**
	Regulator	82	82.5	-	**-**
	Total	43	70	54	**60**
Load regulation (%)		-	-	1.87	**1.1** [D]

[A] Estimated from provided data, [B] Regulated, [C] Simulated,
[D] Load change between 10 μA and 200 μA with settling time < 2 μs

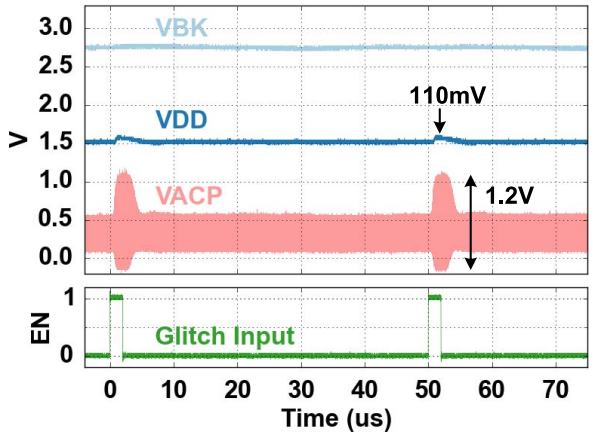

Fig. 16. Measured waveforms of the RVM with overvoltage power-glitch inputs showing an ac input voltage (V_{ACP}) and a dc output voltage (V_{DD}) of the RVM and a backup capacitor voltage (V_{BK}).

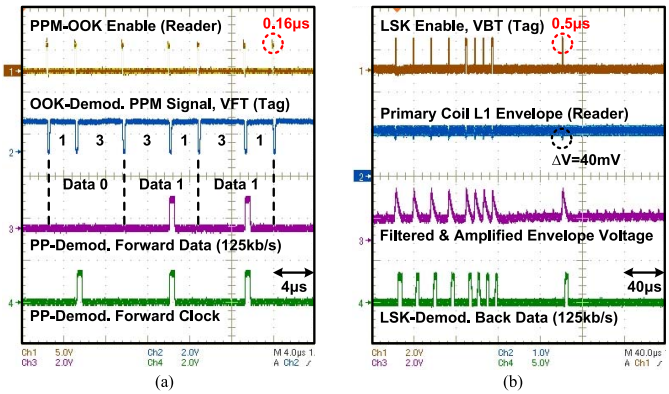

Fig. 17. Measured waveforms of (a) forward telemetry with PPM-OOK and (b) back telemetry with LSK.

the 1.5 V V_{DD} to supply output power (P_{OUT}) of 60 μW from ac input peak amplitudes [$V_{AC(PEAK)}$] higher than 550 mV at 433 MHz, leading to voltage conversion ratio [VCR = $V_{DD}/V_{AC(PEAK)}$] up to 2.73. The RVM also achieved simulated power conversion efficiency [PCE = $P_{OUT}/P_{AC(IN)}$] up to 60%, while a higher $V_{AC(PEAK)}$ resulted in a PCE decrease due to larger voltage drops across regulating switches in the RVM. Static line and load regulation ($=\Delta V_{DD}/V_{DD}$) of 0.9% and 1.1% were measured with $V_{AC(PEAK)}$ variation (0.55–1.2 V) and load current variation (10–200 μA), respectively. Measured waveforms of an RVM response to a transient overvoltage power glitch are shown in Fig. 16. The RVM limits transient overshoot on V_{DD} to 110 mV within a safe margin (10% of V_{DD}) for the AE. The active clamp further limits $V_{AC(PEAK)}$ to below 1.2 V. Table IV benchmarks the RVM against recent wireless power circuits.

Measured waveforms of the pulse-based data telemetry are shown in Fig. 17. The PPM-OOK forward telemetry in Fig. 17(a) transmits data to the tag at 125 kb/s, with a minimum pulsewidth of 0.16 μs, leading to a 4% duty cycle (=2 × 0.16/8 μs). Thus, PPM-OOK results in 12.5× lower dead-time energy loss compared with 50% duty cycle pulsewidth modulation [26]. Then, the PP demodulator generates synchronized forward data and clock provided to the AE at 125 kb/s. The LSK back telemetry in Fig. 17(b) shorts the L_2C_2-tank for 0.5 μs per high bit at 125 kb/s, leading to a 6.25% duty cycle. The small voltage variation (=40 mV) across L_1 in the reader is filtered and amplified to demodulate the back data at 125 kb/s.

C. Energy Backup Storage

Safe shutdown operation with the energy backup storage was verified through a worst case power interruption event. Fig. 18 shows the measured waveforms for safe shutdown when wireless power is interrupted just after V_{DDNV} reaches 1.5 V, but before NVDFF restore starts. In response, the WPDT circuits enter a sleep mode, and the energy from C_{BK} supplied the AE to restore states runs a key update step and completes the save to the NVDFFs within 70 μs. The V_{BK} decreases from 2.75 V as these operations are performed,

TABLE V
AUTHENTICATION TAG SPECIFICATION

Overall System		Authentication Engine	
Process	130 nm CMOS	Modes	PRNG + Auth-encryption
V_{DD} / V_{BK} / P_{SB}	1.5V / 2.75V / 7.5µW [A]	Throughput	30 Tags/sec
Die area [B]	0.77mm^2	Algorithm	Keccak (400 bit permutation)
Wireless Power & Data Telemetry		Power	3.6µW standby / 8.6µW auth
Source	433-MHz inductive link	Area	17.9k GE (incl. 571 NVDFFs)
L_1 / L_2	23.5nH / 35nH	**Attack Mitigation**	
Downlink	0.16-µs PPM-OOK, 125kb/s	Side-channel	Per-query key update
Uplink	0.5-µs PW LSK, 125kb/s	Power glitch	NVDFF + Energy backup

[A] Static standby power, [B] Including on-chip decoupling capacitors, C_L and C_{BK}.

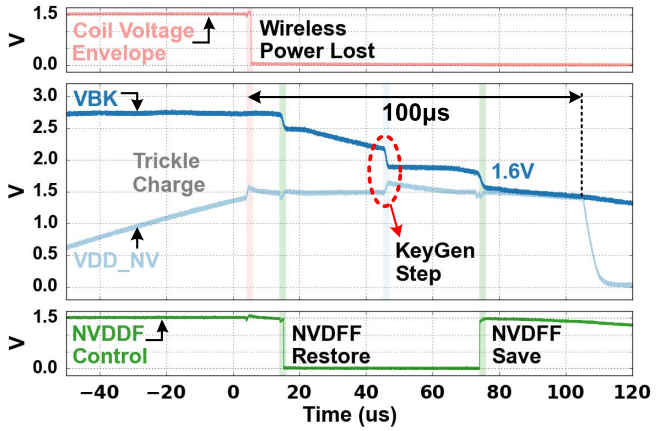

Fig. 18. Measured waveforms showing safe shutdown with the EBU during a worst case power interruption event.

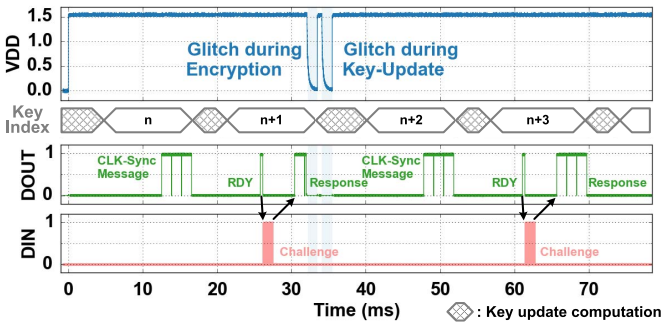

Fig. 19. Measured waveforms showing safe system response to two successive power glitch events.

but V_{BK} does not drop below 1.5 V, indicating that the energy backup storage was sufficient to complete the safe shutdown. Then, the supply control unit in Fig. 7 initiates the V_{DDNV} fast discharge for correct NVDFF operation.

D. Power-Glitch System Response

Successful operation in the presence of two successive power-glitch events is shown in the measured waveforms of Fig. 19. The first glitch is inserted during the AEAD mode, and the current response is aborted. The power is restored, and then a second glitch is inserted when the CS-PRNG is updating the key. The key update is paused and completed the next time the tag powers up. The tag then indicates that it is ready for a new challenge and successfully completes a challenge response iteration verifying that it can be recovered from the two glitches. Table V summarizes the specifications of the wireless authentication tag.

TABLE VI
EFFECT OF TEMPERATURE ON TAG SPECIFICATIONS

Temperature (°C)	V_{DD} (V)	V_{BK} (V)	Tag Clock Period (µs)	Backup-Energy[A] (pJ/Bit)
-20	1.465	2.660	10.13	2.30
20	1.496	2.716	8.38	2.48
40	1.508	2.732	7.72	2.52
80	1.530	2.754	7.02	2.58

[A] Simulated energy for backup-restore of 1 NVDFF

In simulation, the backup energy for a single NVDFF varies by ∼10% over temperature from −20 °C to 80 °C. Thus, it is expected that the available energy margin (+40%) on the backup capacitor is sufficient for correct operation. Full system operation was experimentally verified in a thermal chamber. Correct system glitch responses were verified, and the measurement results of the V_{DD}, V_{BK}, and the on-chip ring-oscillator clock period are presented in Table VI. The clock recovery algorithm on the reader was adjusted to accept a wider range to account for the temperature drift of the oscillator.

VII. CONCLUSION

We developed a wireless authentication tag using FeCap NVDFFs for security applications and demonstrated mitigation techniques against passive and active threat models. The tag performs per-query key updates before each protocol invocation to prevent side-channel attacks. Also, the NVDFF key storage and FeCap-based energy backup solution enable complete NVDFF save–restore for safe shutdown against power-glitch attacks. The RVM and pulse-based telemetry ensure an energy-efficient wireless interface between the tag and the reader. The proposed authentication tag can provide a secure proof of origin in a highly globalized supply chain.

ACKNOWLEDGMENT

The authors would like to thank Texas Instruments for fabrication and S. Chakraborty for technical discussions.

REFERENCES

[1] P. Tuyls and L. Batina, "RFID-Tags for Anti-counterfeiting," in *Topics in Cryptology*, D. Pointcheval, Ed. Berlin, Germany: Springer, 2006, pp. 115–131.

[2] I. Verbauwhede, J. Balasch, S. S. Roy, and A. Van Herrewege, "Circuit challenges from cryptography," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 428–429.

[3] K. Gomina, J.-B. Rigaud, P. Gendrier, P. Candelier, and A. Tria, "Power supply glitch attacks: Design and evaluation of detection circuits," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 136–141.

[4] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2009, pp. 64–65.

[5] K. Myny *et al.*, "An inductively-coupled 64b organic RFID tag operating at 13.56 MHz with a data rate of 787b/s," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2008, pp. 290–291.

[6] V. Fiore *et al.*, "A 13.56 MHz RFID tag with active envelope detection in an organic complementary TFT technology," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2014, pp. 492–493.

[7] K. Myny *et al.*, "Organic RFID tags," in *Radio Frequency Identification Fundamentals and Applications Design Methods and Solutions*, C. Turcu, Ed. Rijeka, Croatia: InTech, 2010.

[8] H. Kim, T.-H. Ki, S. Lee, and H.-S. Lee, "CMOS security-enhanced passive (SEP) tag supporting to mutual authentication," *IEEE Trans. Ind. Electron.*, vol. 61, no. 9, pp. 4920–4930, Sep. 2014.

[9] J. Ertl, T. Plos, M. Feldhofer, N. Felber, and L. Henzen, "A security-enhanced UHF RFID tag chip," in *Proc. Euromicro Conf. Digit. Syst. Design (DSD)*, Sep. 2013, pp. 705–712.

[10] D. Oswald and C. Paar, "Breaking Mifare DESFire MF3ICD40: Power analysis and templates in the real world," in *Cryptographic Hardware and Embedded Systems*, B. Preneel and T. Takagi, Eds. Berlin, Germany: Springer, 2011, pp. 207–222.

[11] M. Medwed, F.-X. Standaert, J. Großschädl, and F. Regazzoni, "Fresh re-keying: Security against side-channel and fault attacks for low-cost devices," in *Progress in Cryptology*, D. J. Bernstein and T. Lange, Eds. Berlin, Germany: Springer, 2010, pp. 279–296.

[12] K. Pietrzak, "A leakage-resilient mode of operation," in *Advances in Cryptology*, A. Joux, Ed. Berlin, Germany: Springer, 2009, pp. 462–482.

[13] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche. (Jan. 2011). *The Keccak Reference*. [Online]. Available: http://keccak.noekeon.org/Keccak-reference-3.0.pdf

[14] M. Qazi, A. Amerasekera, and A. P. Chandrakasan, "A 3.4-pJ FeRAM-enabled D flip-flop in 0.13-μm CMOS for nonvolatile processing in digital systems," *IEEE J. Solid-State Circuits*, vol. 49, no. 1, pp. 202–211, Jan. 2014.

[15] C. S. Juvekar, H.-M. Lee, J. Kwong, and A. P. Chandrakasan, "A Keccak-based wireless authentication tag with per-query key update and power-glitch attack countermeasures," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2016, pp. 290–291.

[16] S. Mangard, "A simple power-analysis (SPA) attack on implementations of the AES key expansion," in *Information Security and Cryptology*, P. J. Lee and C. H. Lim, Eds. Berlin, Germany: Springer, 2002, pp. 343–358.

[17] J. Fan and I. Verbauwhede, "An updated survey on secure ECC implementations: Attacks, countermeasures and cost," in *Cryptography and Security: From Theory to Applications*, D. Naccache, Ed. Berlin, Germany: Springer, 2012, pp. 265–282.

[18] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology*, M. Wiener, Ed. Berlin, Germany: Springer, 1999, pp. 388–397.

[19] J. Balasch, B. Gierlichs, R. Verdult, L. Batina, and I. Verbauwhede, "Power analysis of Atmel CryptoMemory—Recovering keys from secure EEPROMs," in *Topics in Cryptology*, O. Dunkelman, Ed. Berlin, Germany: Springer, 2012, pp. 19–34.

[20] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Sponge-based pseudo-random number generators," in *Cryptographic Hardware and Embedded Systems*, S. Mangard and F.-X. Standaert, Eds. Berlin, Germany: Springer, 2010, pp. 33–47.

[21] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Permutation-based encryption, authentication and authenticated encryption," in *Proc. Directions Authenticated Ciphers (DIAC)*, Jul. 2012, pp. 159–170.

[22] Q. Dong, J. Zhang, and L. Wei, "A SHA-3 based RFID mutual authentication protocol and its implementation," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC)*, Aug. 2013, pp. 1–5.

[23] E. B. Kavun and T. Yalcin, "A lightweight implementation of Keccak hash function for radio-frequency identification applications," in *Radio Frequency Identification: Security and Privacy Issues*, S. B. O. Yalcin, Ed. Berlin, Germany: Springer, 2010, pp. 258–269.

[24] P. Pessl and M. Hutter, "Pushing the limits of SHA-3 hardware implementations to fit on RFID," in *Cryptographic Hardware and Embedded Systems*, G. Bertoni and J.-S. Coron, Eds. Berlin, Germany: Springer, 2013, pp. 126–141.

[25] H.-G. Rhew, J. Jeong, J. A. Fredenburg, S. Dodani, P. G. Patil, and M. P. Flynn, "A fully self-contained logarithmic closed-loop deep brain stimulation SoC with wireless telemetry and wireless power management," *IEEE J. Solid-State Circuits*, vol. 49, no. 10, pp. 2213–2227, Oct. 2014.

[26] N. Desai, J. Yoo, and A. P. Chandrakasan, "A scalable, 2.9 mW, 1 Mb/s e-textiles body area network transceiver with remotely-powered nodes and bi-directional data communication," *IEEE J. Solid-State Circuits*, vol. 49, no. 9, pp. 1995–2004, Sep. 2014.

[27] R. Muller *et al.*, "A minimally invasive 64-channel wireless μECoG implant," *IEEE J. Solid-State Circuits*, vol. 50, no. 1, pp. 344–359, Jan. 2015.

[28] C. Kim, S. Ha, J. Park, A. Akinin, P. P. Mercier, and G. Cauwenberghs, "A 144 MHz integrated resonant regulating rectifier with hybrid pulse modulation," in *Proc. Symp. VLSI Circuits (VLSI Circuits)*, Jun. 2015, pp. C284–C285.

Hyung-Min Lee (S'06–M'14) received the B.S. degree in electrical engineering (*summa cum laude*) from Korea University, Seoul, South Korea, in 2006, the M.S. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2008, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2014.

From 2014 to 2015, he was a Post-Doctoral Associate with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA. In 2015, he joined the IBM T. J. Watson Research Center, Yorktown Heights, NY, USA as a Research Staff Member. His current research interests include analog/mixed-signal/power-management integrated circuit and system design for biomedical and Internet of Things applications.

Dr. Lee was a recipient of Silver Prizes in the 16th and 18th Human-Tech Thesis Prize Contest from Samsung Electronics, South Korea, in 2010 and 2012, respectively, and the Commendation Award in the Fourth Outstanding Student Research Award from TSMC, Taiwan, in 2010.

Chiraag S. Juvekar (S'12) received the B.Tech. and M.Tech. degrees in electrical engineering from IIT Bombay, Mumbai, India, in 2012, and the M.S. degree in electrical engineering and computer science from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2014, where he is currently pursuing the Ph.D. degree.

In 2014, he was with the Embedded Processing Laboratories, Texas Instruments Incorporated, Dallas, TX, USA, designing authentication circuits using emerging memories. His current research interests include low power system design and hardware security.

Mr. Juvekar was a recipient of the MIT Presidential Fellowship in 2012 and the Qualcomm Innovation Fellowship in 2016.

Joyce Kwong (M'04) received the bachelor's degree from the University of Waterloo, Waterloo, ON, USA, in 2004, and the M.S. and Ph.D. degrees in electrical engineering from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2006 and 2010, respectively.

From 2010 to 2015, she was a Technical Staff Member with the Embedded Processing Systems Laboratories, Texas Instruments Incorporated, Dallas, TX, USA. Her current research interests include low power circuits and signal processing architectures.

Dr. Kwong was a co-recipient of the Jack Kilby Outstanding Student Paper Award at the 2008 International Solid-State Circuits Conference. She was a recipient of the Texas Instruments Graduate Woman's Fellowship for Leadership in Microelectronics in 2007 and the NSERC Postgraduate Fellowship from 2007 to 2010. From 2014 to 2015, she has served on the Technical Advisory Board of the SRC's Trustworthy and Secure Semiconductors and Systems Research Program.

Anantha P. Chandrakasan (M'95–SM'01–F'04) received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer sciences from the University of California at Berkeley, Berkeley, CA, USA, in 1989, 1990, and 1994, respectively.

Since 1994, he has been with the Massachusetts Institute of Technology, Cambridge, MA, USA, where he is currently the Vannevar Bush Professor of Electrical Engineering and Computer Science. He has co-authored the books *Low Power Digital CMOS Design* (Kluwer Academic Publishers, 1995), *Digital Integrated Circuits, Second Edition* (Pearson Prentice-Hall, 2003), and *Sub-threshold Design for Ultra-Low Power Systems* (Springer, 2006). His current research interests include ultralow-power circuit and system design, energy harvesting, energy efficient RF circuits, and hardware security.

Dr. Chandrakasan has served as various roles for the IEEE ISSCC including the Program Chair, the Signal Processing Sub-Committee Chair, and the Technology Directions Sub-Committee Chair. He was the Director with the MIT Microsystems Technology Laboratories from 2006 to 2011. He has been the Conference Chair of ISSCC since 2010. Since 2011, he has been the Head of the MIT Electrical Engineering and Computer Science Department. He was a co-recipient of several awards including the 2007 ISSCC Beatrice Winner Award for Editorial Excellence and the ISSCC Jack Kilby Award for Outstanding Student Paper in 2007, 2008, and 2009. He was a recipient of the 2009 Semiconductor Industry Association University Researcher Award and the 2013 IEEE Donald O. Pederson Award in Solid-State Circuits. In 2015, he was elected to the National Academy of Engineering.