An Actively Detuned Wireless Power Receiver With Public Key Cryptographic Authentication and Dynamic Power Allocation

Nachiket Desai, *Student Member, IEEE*, Chiraag Juvekar, *Student Member, IEEE*, Shubham Chandak, and Anantha P. Chandrakasan, *Fellow, IEEE*

***Abstract*— This paper presents a CMOS resonant wireless charging receiver with an active detuning mechanism for controlling the received power, without using any passive components being switched in and out. This detuning mechanism is first combined with an on-chip elliptic curve accelerator that achieves 0.77-μJ/elliptic curve scalar multiplication and in-band telemetry for authenticating a wireless charger using elliptic curve cryptography, with up to 16× rejection at the output of the receiver. Second, equitable power distribution between two receivers coupled to the same charger is demonstrated by controlled detuning of the closer receiver. The system can overcome up to a 4:1 asymmetry in distance to the charger between two receivers. Implemented in 0.18-μm CMOS, the receiver IC delivers 520-mW peak output power and 74% peak end-to-end efficiency in the tuned mode.**

***Index Terms*— Active rectification, authentication, elliptic curve cryptography, security, wireless power transfer.**

I. Introduction

THE rapid growth of Internet of Things (IoT) devices has led to a corresponding growth in the adoption of near-field wireless charging for various applications [1]–[6]. However, as the number of wireless power receivers grows, so will the number of chargers that might be counterfeit or not strictly standards compliant [7], [8]. Given the critical nature of the tasks performed by IoT devices, protecting them from harsh transients imposed by counterfeit wireless chargers [9] is important. These transients could have potentially destructive impacts on both the receiver's electronics and the battery being charged [10], [11]. This problem is made more challenging by the fact that the underdamped LC resonant tanks used by most resonant wireless power transmission (WPT) systems [12], [13] tend to cause overvoltage or overcurrent conditions in response to the transients imposed by the charger.

Manuscript received April 21, 2017; revised June 30, 2017; accepted July 25, 2017. Date of publication September 7, 2017; date of current version December 26, 2017. This paper was approved by Guest Editor Pui-In Mak. This work was supported in part by the MIT Lincoln Laboratory and in part by Texas Instruments. *(Corresponding author: Nachiket Desai.)*

N. Desai is with Intel Labs, Hillsboro, OR 97124 USA (e-mail: nvdesai@alum.mit.edu).

C. Juvekar and A. P. Chandrakasan are with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 USA.

S. Chandak is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305 USA.

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

Digital Object Identifier 10.1109/JSSC.2017.2737562

A number of examples in the literature [14]–[18] deal with authenticating a wired charger for the reasons of battery safety. Secure hash algorithm (SHA)-based cryptographic authentication protocols have been implemented commercially [19] for the same purpose. These solutions use a cryptographic element attached to the receiver that generates a challenge using a predetermined key. A genuine charger that has the appropriate key can then decrypt and respond to that challenge. The receiver is open circuited until it receives the correct response, upon which it begins drawing energy from the charger. While a similar challenge-response protocol for charger authentication could be employed for incorporating secure charging into WPT, the projected scale of IoT wireless power receivers in the near future would make authentication based on a pre-shared secret (symmetric key), which is well suited for one-charger one-receiver scenarios, unsustainable. Symmetric key authentication between the receiver and the charger requires that the receiver either be pre-programmed with the private keys of all possible chargers or be capable of exchanging a new key upon encountering a new charger. The former is clearly not scalable, while the latter requires all chargers and receivers share a master key that facilitates the key exchange over the same communication channel, thus introducing a new weak point in the system [20]. Both approaches require a secure memory on the receiver, which cannot be read by an attacker; otherwise, an attacker could extract these keys and impersonate a valid charger.

Instead, public key authentication uses two separate keys—a publicly known key used by the receiver for generating the challenge (public key) and its associated private key that is known only to the charger and is used for generating the response. The distribution of the charger public keys can be handled by issuing certificates signed by a trusted certificate authority, in a way similar to the key-exchange handshake implemented in the transport layer security (TLS) protocol. This avoids the need for implementing both secure key exchange and storage.

In a scenario where multiple receivers are coupled to the same charger, the power delivered to a receiver is a strong function of its proximity and orientation (which is related to the magnetic coupling coefficient) with respect to the charger coil [21], [22], with more power going to the closer receiver. This physically imposed constraint might not necessarily reflect the actual energy requirements of the

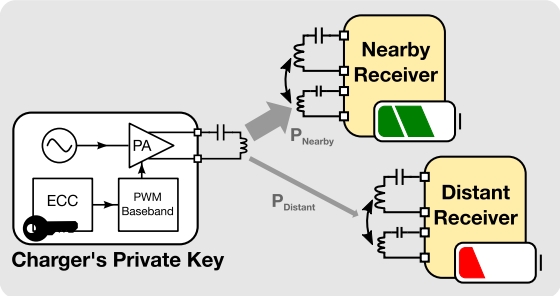


Fig. 1. System architecture of a WPT system with multiple receivers connected to a single authenticated charger.

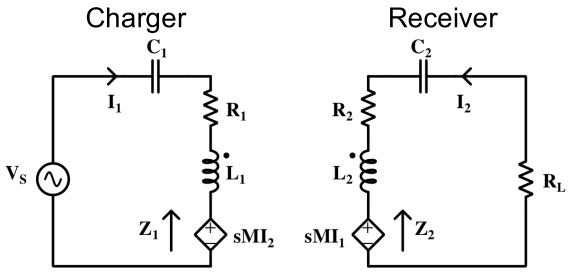


Fig. 2. Equivalent circuit of WPT system.

various receivers. This can be seen in the system-level diagram shown in Fig. 1. In order to address these two disparate issues, two capabilities are required on the receiver side—the ability to: 1) safely block power transmitted by a counterfeit wireless charger and 2) be invisible to the charger so that more power can be delivered to a more distant receiver that might need it.

Section II describes a technique to accomplish both these requirements in a resonant WPT system without the use of any switched passive component (inductor or capacitor) arrays. Section III describes the implementation of the receiver in a CMOS IC. Section IV describes a public key-based scheme for charger authentication for scalability and to avoid the need for secure key storage on the receiver. Measurement results for the complete system are presented in Section V.

II. Dual-Coil Resonant Frequency Modulation for Receiver Detuning

A generic equivalent circuit of a resonant WPT system is shown in Fig. 2, along with the dependent voltage sources induced by the mutual coupling of the two inductors. Both coils are tuned with series capacitors C_1 and C_2, respectively. Open-circuiting the load to block power from the charger makes it invisible to the charger, since the back electromotive force (EMF) generated at the charger, sMI_2, is zero. However, since the LC tanks used by resonant WPT systems typically operate with a large intrinsic quality factor (Q) for good efficiency, this makes the charger coil current, I_1, large and the forward EMF, sMI_1, unsafe. On the other hand, short-circuiting R_L in Fig. 2 ensures a large back EMF and safe operation, but receiver invisibility is lost. The third option—detuning the receiver by a small fraction can dramatically reduce the current through the receive coil due to the large Q, which makes the receiver less visible at the transmitter by

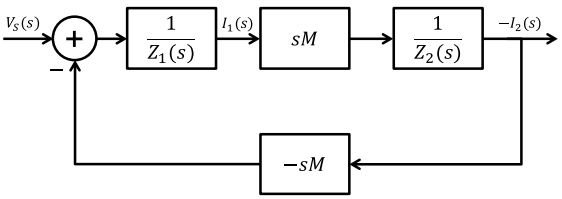


Fig. 3. Feedback block diagram for the two-coil inductively coupled circuit in Fig. 2.

inducing a smaller back EMF on the charging coil. The large forward EMF generated as a consequence is dropped across the residual reactance of the tank. At typical near-field operating frequencies (<40 MHz), both the receiver coil L_2 and its series capacitor C_2 are off-chip, and can easily tolerate the large induced voltage.

A trivial implementation of receiver detuning, using either an array of capacitors or inductors that can be switched in or out, is not well suited for resonant WPT systems. To maintain the high Q (~10) needed for good efficiency [12], [13], a passive element array needs either series switches with very low R_{ON} or parallel switches that can tolerate large open-circuit voltages. Neither of these are suitable for low-area implementation on a standard CMOS process. Instead, we have implemented an alternative approach for detuning the receiver without using any switched passives, as described further in this section.

A. Pole-Splitting in Coupled Second-Order Systems

The feedback signal flow diagram for the coupled system in Fig. 2 is shown in Fig. 3.

The feedback loop transfer function of the signal flow diagram in Fig. 3 is

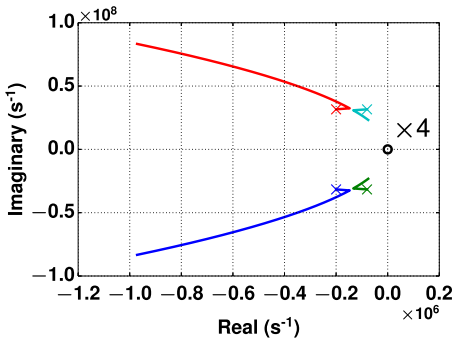
$$L(s) = \frac{-s^2M^2}{Z_1(s)Z_2(s)} \tag{1}$$

where

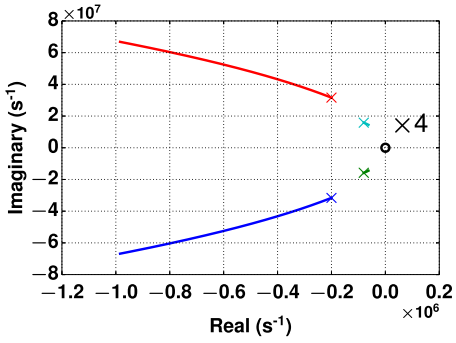
$$Z_1(s) = sL_1 + R_1 + \frac{1}{sC_1}$$
$$Z_2(s) = sL_2 + R_2 + \frac{1}{sC_2} + R_L \tag{2}$$

are the impedances seen by the dependent voltage sources on each side. M is the mutual inductance between the two coils and the coupling coefficient k is defined as $k = M/(L_1L_2)^{1/2}$. The loop transfer function gain can be directly modulated by k.

From (1) and (2), the two-coil system has four open-loop zeros at the origin and four open-loop poles. For a well-designed system that operates at medium to strong coupling between the coils ($kQ > 1$), the open-loop poles are complex at both the maximum power-point and the maximum efficiency-point of the system [13], [23]. A root locus plot for an example of the system in Fig. 3 is shown in Fig. 4(a), with both LC tanks tuned to the same resonant frequency but with different quality factors. As the coupling coefficient increases, the closed-loop system poles first move toward each other along a circle centered at the origin (with the same resonant frequency). Upon increasing k further, they split, leading to the formation of two separate natural modes in



(a)



(b)

Fig. 4. Root locus plots for system in Fig. 3. (a) Same resonant frequency. (b) Different resonant frequencies.

the system, which move further and further apart. If instead, the two LC tanks are tuned at separate frequencies, as shown in Fig. 4(b), both the closed-loop poles and their associated resonant frequencies immediately begin to move apart as k is increased.

B. Receiver Architecture for Detuning

The movement of the poles of two second-order systems under strong coupling can be used to implement detuning. Instead of having a single LC tank, the receiver can have two coils, and thus two LC tanks, as shown in Fig. 5. If the two coils on the receiver are coupled, the amount of receiver detuning can be controlled by controlling the value of the feedback transfer function between them. The shift in the resonant frequency caused by the interaction between two resonant, single-coil receivers coupled to the same charging coil and being in close proximity to each other has been investigated in [24], with a focus on the reduced output power and efficiency as both the receivers detune from the operating frequency. Here, we can make use of the same effect to our advantage instead, by having controlled detuning between two LC tanks on the same receiver.

The receiver in Fig. 5 has two coils: a main coil that receives the bulk of the power when the receiver is tuned to the charger, and an auxiliary coil that detunes the system when required. However, modulating the coupling between the main and auxiliary coils on the receiver to implement detuning in a similar fashion to the root locus plots in Fig. 4 implies physically modifying the coils' geometry and/or their relative placement, making it unsuitable for a practical system.

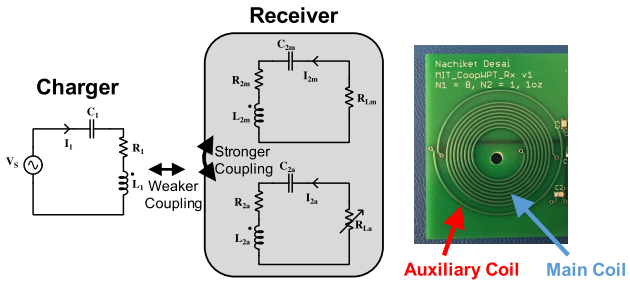


Fig. 5. Receiver with two coils in order to implement detuning—the two coils on the receiver are implemented in a concentric fashion to improve their mutual coupling for larger feedback loop gain.

Instead, the value of the feedback transfer function can be changed by manipulating the value of the load connected to the auxiliary coil, R_{L2a}, albeit without direct proportionality to the loop transfer function. The zero-coupling condition can be replicated by open-circuiting the auxiliary coil, which allows the main coil to receive power from a charger tuned to the L_{2m}–C_{2m} resonant frequency. Maximizing the magnitude of the feedback transfer function by short-circuiting the auxiliary coil leads to maximal detuning.

Setting the LC resonances of the two coils at separate frequencies leads to better detuning response, as shown in Fig. 4(b). The L_{2a}–C_{2a} tank is chosen to have a lower resonant frequency than the L_{2m}–C_{2m} tank. This has many advantages—since the charger is tuned to the L_{2m}–C_{2m} tank when the receiver is receiving power, any harmonics generated by the power amplifier (PA) at the charger should not excite the L_{2a}–C_{2a} tank at its resonant frequency and lead to a loss in the power transfer efficiency. Second, as shown in Fig. 4(b), the higher frequency poles move farther from the original positions than the lower frequency ones, and hence should correspond to the poles of the L_{2m}–C_{2m} tank, which receives power in the tuned state. Finally, choosing the L_{2a}–C_{2a} tank resonance at a higher frequency could cause issues with it being too close to the self-resonance frequency of the auxiliary coil, beyond which the auxiliary coil behaves as a capacitor.

The resonant frequency of the receiver changes in the region, where the auxiliary coil load resistance R_{L2a} is comparable to the reactance of the auxiliary coil inductance. As the auxiliary load resistance increases, the resonant frequency decreases. Under the limit where R_{L2a} approaches infinity, the effect of the auxiliary coil begins to disappear and the receiver's resonant frequency approaches $(2\pi(L_{2m}C_{2m})^{1/2})^{-1}$, which is the natural oscillation frequency of the main coil L_{2m}–C_{2m} tank.

III. Receiver Implementation

As described in Section II-B, receiver-side detuning is implemented by varying the load resistance connected to the auxiliary coil in Fig. 5. The rectifier connected to the main coil rectifies the induced ac voltage and delivers energy to an external voltage source, which could be a battery in parallel with a filter capacitor with low ESR. A separate rectifier connected to the auxiliary coil acts as its load and has the same external dc voltage source at its output. Changing the resistance looking into the ac input terminals of the auxiliary

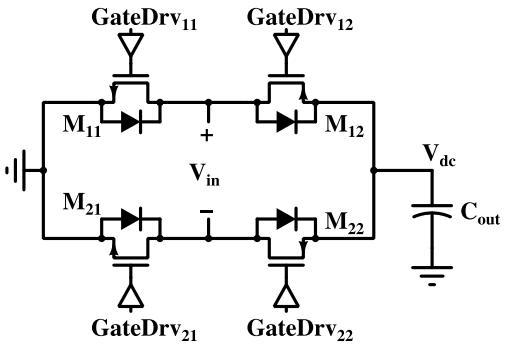


Fig. 6. Basic building block of the main and auxiliary rectifiers.

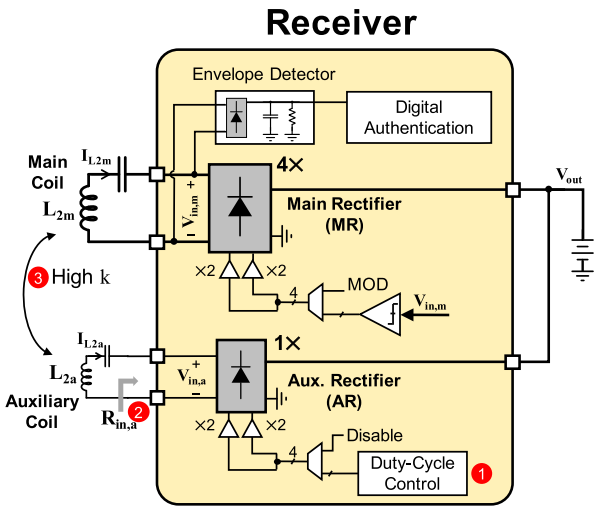


Fig. 7. Block diagram of receiver with detuning mechanism—1: duty cycle changes. 2: AR input resistance changes. 3: high k causes poles to move.

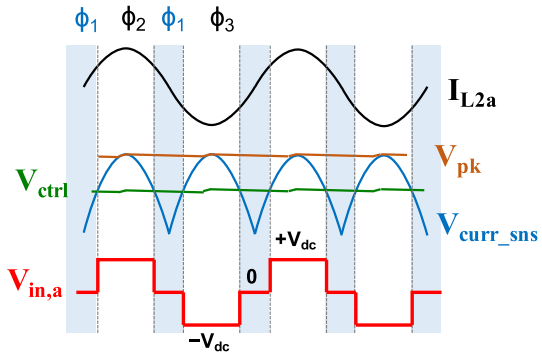


Fig. 8. Current sense-based rectifier control.

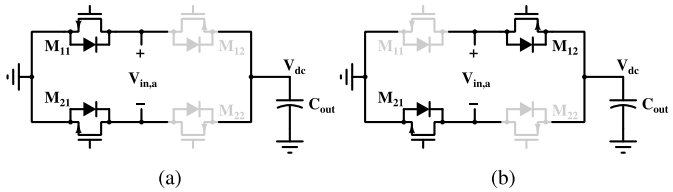


Fig. 9. Phases of the operation of current-sense-based duty-cycled rectifier control. Phase ϕ_3 is similar to ϕ_2, but with the opposite set of transistors ON/OFF. (a) ϕ_1, ($V_{\text{curr\_sns}} < V_{\text{ctrl}}$). (b) ϕ_2, ($I_{L2a} > 0$, $V_{\text{curr\_sns}} > V_{\text{ctrl}}$).

rectifier can emulate the variable load R_{L2a} in Fig. 5. This will be discussed in detail in Section III-A.

The basic building block of the rectifiers in the proposed wireless power receiver is shown in Fig. 6. It is a synchronously driven full-bridge rectifier made of low-side NMOS and high-side PMOS devices. The body diodes of all the switches are shown in Fig. 6 as well. The gate drivers driving the MOS switches have an in-built, statically configured dead time to prevent a short circuit path forming from the output to ground.

A block diagram of the receiver is shown in Fig. 7. The main coil resonance frequency $(2\pi\,(L_{2a}C_{2a})^{1/2})^{-1}$, i.e., the frequency at which the charger transmits power, is set to 6.78 MHz (f_{op}). The auxiliary coil resonance frequency $(2\pi\,(L_{2a}C_{2a})^{1/2})^{-1}$ is set at $f_{\text{op}}/2$. When the receiver is configured to accept power, the main rectifier delivers energy to the dc output. In this mode, the input resistance of the auxiliary rectifier (which emulates R_{L2a} in Fig. 5) is made large by disabling its switch gate drive. The main rectifier is controlled by a synchronous gate driver that uses comparators to detect the turning on of the body diodes in order to turn the field-effect transistor on.

An envelope detector made up of a passive, diode-based rectifier followed by an *RC* low-pass filter demodulates the forward telemetry messages, which appear as an ON–OFF keying (OOK)-modulated current waveform induced by the charger. For backward telemetry, the receiver uses load-shift keying on the main coil, i.e., shorting the main coil or connecting it to the load in order to signal bits. The short circuit functionality is implemented by using the two low-side switches on the main rectifier instead of adding a separate switch in parallel to the rectifier. This reduces the parasitic capacitance across ac input of the main rectifier by up to 30%.

A. Current Sense-Based Rectifier Control

Duty cycle control of the auxiliary rectifier's ac input resistance is obtained using a current sense-based approach. The voltage $V_{\text{curr\_sns}}$ in Fig. 8 is obtained by sensing the currents in the active low-side switch using a 400× smaller replica-biased transistor whose current is passed through an on-chip resistor [25].

A peak detector circuit retrieves the local peak voltage of $V_{\text{curr\_sns}}$, which is shown as V_{peak} in Fig. 8. The duty cycle of the rectifier is set by a dc control voltage V_{ctrl}, which is obtained from the peak voltage V_{peak} using a DAC-based resistor divider. When $V_{\text{curr\_sns}} < V_{\text{ctrl}}$, the auxiliary coil is shorted by turning both the low-side switches on and both the high-side switches off. When $V_{\text{curr\_sns}} > V_{\text{ctrl}}$, the appropriate low- and high-side switches are turned on based on the sign of I_{L2a} to deliver power to the output. By changing the settings of the resistor DAC, the value of V_{ctrl} relative to V_{peak} can be changed. This controls the fraction of the cycle for which the rectifier delivers power to the load. The switch configurations for two of the three phases of the rectifier in Fig. 8 are shown in Fig. 9.

From Fig. 7, the output of the auxiliary rectifier can be considered as a dc voltage. Hence, across its ac input terminals, the auxiliary rectifier can be modeled with an ac voltage source in phase with its input current and a series resistor that models

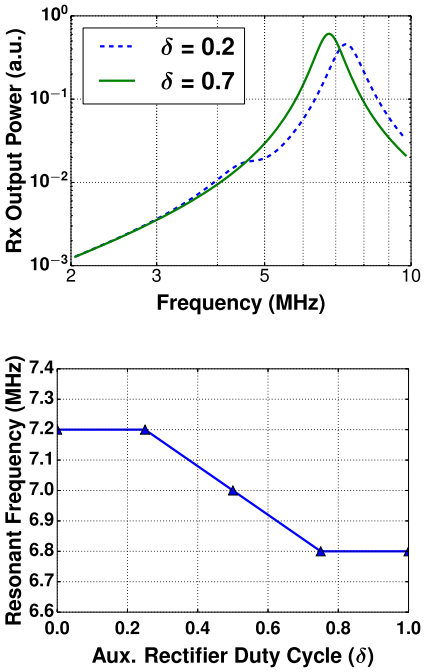


Fig. 10. Frequency response of receiver to auxiliary rectifier-based detuning.

the on resistance of its switches. Even though the rectifier cannot be modeled solely as a load resistor of fixed value, the two-coil receiver system still has two complex conjugate open loop pole pairs and its root locus plot still resembles the plot shown in Fig. 4. The duty cycle of the auxiliary rectifier, δ, can be defined as the fraction of the *total* oscillation period during which the auxiliary rectifier is connected to its output. The control voltage is related to the duty cycle as $V_{\text{ctrl}} = V_{\text{peak}} \cdot \cos(\pi\delta/2)$. The first harmonic of the input voltage of the auxiliary rectifier, $V_{\text{in},a}$, is proportional to $\sin(\pi\delta/2)$. Modulating $V_{\text{in},a}$ (and hence the effective input resistance of the rectifier) controls the auxiliary coil current (I_{L2a}) relative to the main coil current I_{L2m}, causing the system poles to move away from f_{op} as described in Section II.

The extent to which detuning occurs can be seen from the simulation plots in Fig. 10. As the duty cycle, and hence, the input resistance, of the auxiliary rectifier are reduced, the receiver begins to detune. This causes both I_{L2m} and the induced back EMF on the charging coil to decrease. Lowering the input resistance of the auxiliary rectifier, $R_{\text{in},a}$, leads to a higher resonant frequency at the receiver.

B. Coil Design

Appropriate sizing of the auxiliary coil is necessary to ensure good detuning performance as well as high efficiency and output power in tuned operation. If the auxiliary coil inductance L_{2a} is made large by having a large area or a large number of turns on it, the mutual inductance from the charging coil to the auxiliary coil increases, and so does the induced voltage from the charger. In this case, when the receiver is configured to receive power from the charger, the large induced voltage on the auxiliary coil can inadvertently turn on the passive rectifier formed by its body diodes even when the gate drive is turned off. This could lead to detuning when it is not desired and lower the overall received power

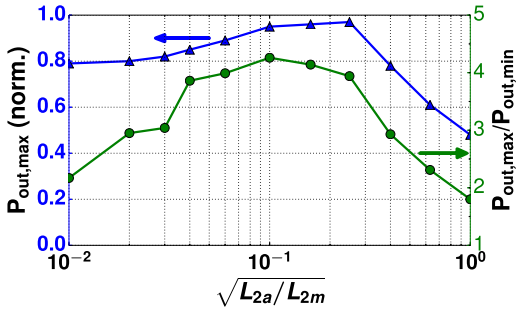


Fig. 11. Degree of detuning and blocking versus effective turns ratio between main and auxiliary coils.

and power transfer efficiency. On the other hand, making L_{2a} small reduces the feedback loop gain and the amount of detuning achievable when the receiver is configured to block the charger.

This can be seen in Fig. 11, which is obtained from simulation. If the effective turns' ratio between the main coil and the auxiliary coil on the receiver, $N_{\text{rx}} = (L_{2a}/L_{2m})^{1/2}$, is large, the maximum output power goes down, since the receiver is fairly detuned even with the auxiliary rectifier gate drive disabled. When the turns' ratio is small, the power blocking capability goes down when the auxiliary rectifier is enabled. The power blocking capability is measured as the ratio of the output power when the auxiliary rectifier is fully disabled to the output power when the auxiliary rectifier is fully shorted. A turns' ratio $N_{\text{rx}} = 0.28$ was chosen to achieve reasonable detuning while preventing inadvertent detuning during resonant power transfer. Since the auxiliary coil is smaller than the main coil, it has a smaller induced voltage from the charger coil. The currents in the auxiliary coil are also smaller, since it is tuned at $f_{\text{op}}/2$. Hence, the switches on the main and the auxiliary rectifiers can be scaled in a 4:1 size ratio to reflect this, as shown in Fig. 7.

The picture of the two coils on the receiver shown in Fig. 5 achieves the desired N_{rx}. The coils are implemented in a concentric fashion for better coupling. The addition of the auxiliary coil leads to a 15% larger total coil area on the receiver, which corresponds to a 32% area penalty over having just the main coil. The auxiliary coil also requires an additional ceramic capacitor on the printed circuit board (PCB), whose footprint is negligible to the total coil area. The inductance values at 6.78 MHz obtained from a finite-element simulation are $L_{2m} = 1.781\ \mu$H and $L_{2a} = 144.4$ nH and the coupling coefficient between the two coils is 0.304. The measured value of L_{2m} at the operating frequency is 1.847 μH.

IV. Authentication Block

The receiver authentication block (shown in Fig. 12) decides whether to accept or block power from the charger based on the result of a challenge-response authentication protocol it executes with the charger. The authentication block consists of a baseband pulse width modulation (PWM) modem for communication with the charger, an serial peripheral interface core for initial configuration and two-cryptographic accelerators: a Keccak-based sponge-PRNG similar to [1] that is used to generate random challenges and an NIST

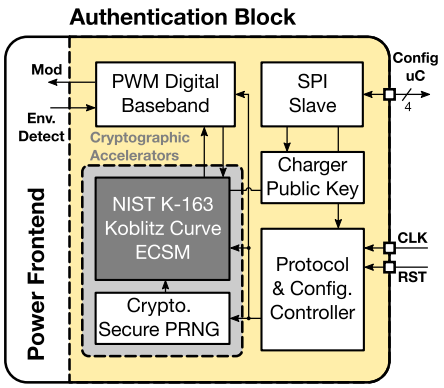


Fig. 12. Overview of the authentication engine.

K-163 elliptic curve scalar multiplier (ECSM) that is used to verify the received responses using the charger's public key stored on the device. At startup, a fresh seed is used to configure the PRNG to ensure that no challenges are repeated.

The receiver communicates with the charger over the inductive link. Packets from the charger are modulated using OOK, while packets from the receiver use load-shift keying, both using the PWM baseband waveforms at 20 kb/s. The use of PWM bits makes clock recovery unnecessary and simplifies demodulation at both ends.

A. Authentication Protocol

The challenge-response protocol employs a Diffie–Hellman-based scheme, where the receiver generates a random scalar c and sends the point $C = c \cdot G$ (where G is the generator of the curve) as the challenge. The charger then uses its private key, p to compute the response $R = p \cdot C$. The receiver then uses the charger's public key $P = p \cdot G$ to check whether $R = c \cdot P$. Thus, the receiver needs to perform two scalar multiplications in order to authenticate the charger: first to generate the challenge and then to verify the response. Since scalar multiplications are a relatively costly operation, a dedicated ECSM unit is used to accelerate them.

B. ECSM Architecture Selection

From an implementation perspective, an ECSM designer must make many choices such as the choice of the curve, form of the coordinates, the field representation, and the field operation implementation. Our ECSM implements scalar multiplication on the NIST K-163 curve [26], which is specified over the binary field $\mathbb{F}_{2^{163}}$ and provides an 80-bit security level. Koblitz curves were chosen, because they allow for efficient scalar multiplication by using the Frobenius endomorphism (τ) as detailed in [27]. Scalar multiplication is commonly computed using a double and add ladder, but on Koblitz curves, one can recode the scalar to its τ-adic representation and replace the doubling by more efficient $\tau(P) = \tau(x, y) = (x^2, y^2)$ operations. We use a normal representation for the binary field as this makes raising to a power of 2, i.e., x^{2^n} a left shift by n-bits, thus making the τ operation essentially free. This is the main source of the efficiency of Koblitz curves, making it a very popular for low resource implementations [28], [29]. Typically one needs to implement additional hardware for converting the scalar to the tauadic form. However, since we are only interested in ECSM for Diffie–Hellman operations, we can simply interpret the CS-PRNG output as the recoded scalar and thus avoid the need for a separate converter.

The formulae for point addition on the curve are closely coupled with the chosen point representation. If we represent the field inversions and multiplication by I and M, respectively, then the affine formulae require $2M$ and $1I$, while the projective Lopez–Dahab (LD) coordinates require $8M$ for mixed point addition [30]. For $\mathbb{F}_{2^{163}}$, we can use Itoh–Tsujii (IT) inversion and perform an inversion using $9M$. Thus, it seems that the LD coordinates offer lower complexity when compared with the affine ($8M$ versus $11M$) at the cost of increased storage of one extra field element. Field multiplication in the normal basis is typically more complicated than the one in the polynomial basis and from the point of compact implementation, we use the bit-level serial input parallel output (SIPO) and parallel input parallel output (PIPO) multipliers from [31] and [32], respectively.

In order to better understand the impact of these design choices, we implemented an affine SIPO ECSM and LD coordinate ECSMs using both the SIPO and PIPO multipliers. The various architectures are shown in detail in Fig. 13. We implemented the affine PIPO architecture from [29] as a baseline in order to allow a fair comparison in our technology.

In all designs, the input point P is stored in x and y and is never disturbed. The input scalar is stored in p and the output point is retrieved from x_1 and y_1. We perform left-to-right double-and-add and store the intermediate points in x_1 and y_1. z_1 is used in LD coordinates for the third coordinate of the intermediate points. The field addition of any two registers is performed over two cycles: first write to z by XORing with 0 and then XOR z with the second argument. The inputs to the multiplier are always fixed to avoid any mux overhead. We first copy one argument to t, and then, we can multiply it with either x_1 or z_1 while accumulating the result in z in a serial fashion.

An analysis of both the affine and LD formulae shows that we can implement the necessary field operations using a single accumulator z. Our affine design strategically stores the intermediate results in t itself in order to reduce the register count. IT inversion additionally requires the multiplication of t by shifted versions of itself. This would require an additional register or a barrel shifter. We resolve this issue by using an SIPO multiplier. Hence, we only need a 1-bit-wide multiplexer that taps the appropriate bits from t instead of a full barrel shifter. This also reduces the multiplexer complexity compared with the baseline design. When using LD coordinates, we only need to perform a single final inversion of z_1. We can copy z_1 to t and use z_1 for the shifted versions, thus avoiding an additional register for both the PIPO and SIPO multipliers.

C. ECSM Implementation and Performance

All the above-mentioned architectures were synthesized in a 0.18-μm CMOS technology at a frequency of 200 MHz using regular V_t standard cells with a nominal supply voltage of 1.8 V. Table I compares these synthesized designs.

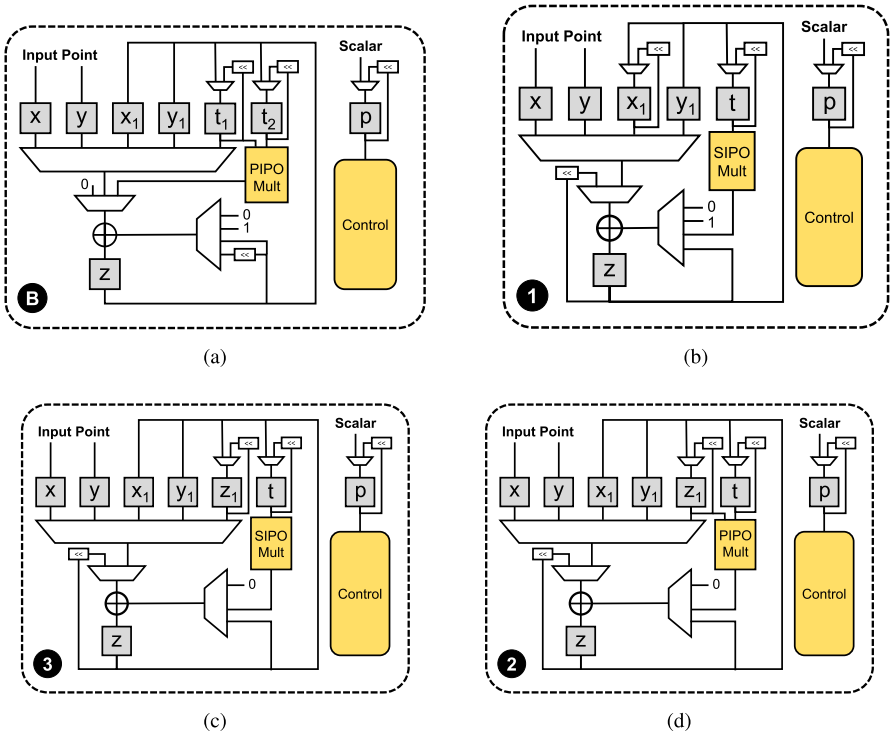


Fig. 13. Comparison of K-163 ECSM architectures. (a) Baseline (affine PIPO) [29]. (b) Affine SIPO. (c) LD SIPO. (d) LD PIPO.

TABLE I
COMPARISON OF LOW-RESOURCE ECSM ARCHITECTURES

	Baseline [29]	**Affine SIPO**	LD SIPO	LD PIPO
Area (GE)	11340	**11100**	12350	11990
Latency (kcycles)	106.7	**98**	73.5	73.5
Gate Efficiency (ECSM/s/GE)	0.165	**0.184**	0.220	0.227
Power (mW)	15.8	**12.7**	21.07	19.35
Energy (µJ/ECSM)	8.42	**6.22**	7.75	7.11

From our results, we observe that the LD formulae (using $8M$) when compared with the affine ($11M$) formulae result in better latency and gate efficiency for the LD implementations. However, surprisingly, this does not translate to better energy efficiency due to the larger mux overhead and higher load seen by z. The SIPO multiplier is larger than the PIPO multiplier, and hence, the LD SIPO implementation is worse on all metrics when compared with the LD PIPO implementation. For the affine implementations, we observe that although the SIPO multiplier is larger the reduction in the register count and mux complexity results in the overall smallest implementation with roughly 27% lower energy when compared with the baseline implementation. Based on this analysis, the affine SIPO architecture was chosen for our implementation.

Since the overall authentication protocol requires just two ECSMs at the verifier, we can use aggressive voltage scaling to improve the energy efficiency while maintaining real-time operation. Fig. 14 reports the performance of the ECSM as function of the supply voltage. We observe that at the minimal energy point (0.475 V), the ECSM requires 0.77 μJ per ECSM.

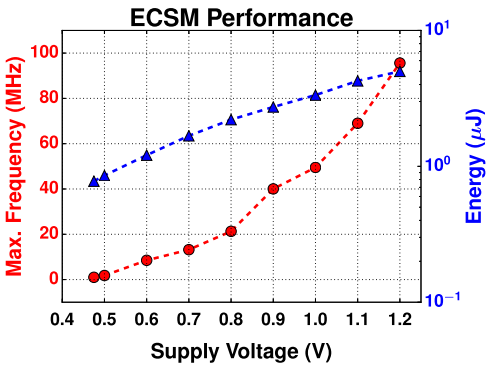


Fig. 14. Performance summary of the ECSM unit.

A comparison of the implemented ECSM versus recently reported works is presented in Table II.

V. MEASUREMENT RESULTS

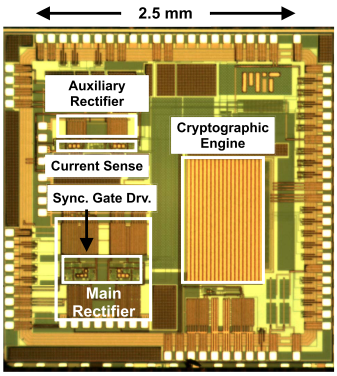
A. Test Setup

The receiver was fabricated in a 0.18-μm CMOS process with 5-V transistors and occupies 2.8-mm^2 active area. The addition of the auxiliary rectifier and its associated control circuits increases the active area of the IC by approximately 35%. The charger was implemented using an H-bridge push–pull PA made up of off-the-shelf components integrated on a PCB and driven at f_{op} (6.78 MHz). The charger coil is an 8-turn, 3 in $\times$ 2 in rectangular spiral made of PCB traces with 4.3-μH measured inductance. The PA drives a series LC tank comprising the transmit coil and its series capacitor tuned at f_{op}. The digital baseband functionality on the charger that

TABLE II
COMPARISON OF RECENT LOW-RESOURCE ECSM IMPLEMENTATIONS

	This work	Roy et al. [28][a]	Azarderakhsh et al. [29][a]	Lee et al. [33]	Pessl et al. [34][a,c]	Wenger et al. [35][a]
Technology	**0.18 µm**	0.13 µm	65 nm	90 nm	0.13 µm	0.13 µm
Curve type	**Koblitz**	Koblitz	Koblitz	Binary	Prime	Binary
Curve size	**163**	283	163	160	160	163
Latency (k-cycles)	**98**	1566	106.7	62.5	139.9	341.8
Frequency (MHz)	**1**	16	13.5	204	1	1
Area (GE)	**11471**	10204[b]	11571	98000	12448	11778
Power (µW)	**7.93**	97.70	77.2	-	42.42	63.3
Energy (µJ/ECSM)	**0.77**	9.56	0.61	9.3	-	21.6

[a] Only post-synthesis results available
[b] Including RAM for storing point coordinates
[c] ECSM core including 823-GE hash engine, exact ECSM energy unavailable



Overall System	
Technology	0.18µm CMOS (5V)
V_{DD}	4V (Power Control) 0.475V (Digital)
Active Area	2.8mm²
Wireless Power/Data Transfer	
L_{2m}/L_{2a}	1.8µH/140nH
Efficiency	74% (peak)
$P_{out,dc}$	520mW (peak)
Uplink/Downlink	20kbps PWM OOK
Cryptographic Engine	
Elliptic Curve	NIST K-163
ECSM Power	7.9uW (@ 1MHz)
CS-PRNG	Keccak-f[200]
Power Blocking	
$P_{out,max}/P_{out,min}$	3.5× – 16×
Power Balancing	
Max. Tuning	1350×

Fig. 15. Die micrograph and performance summary of implemented receiver.

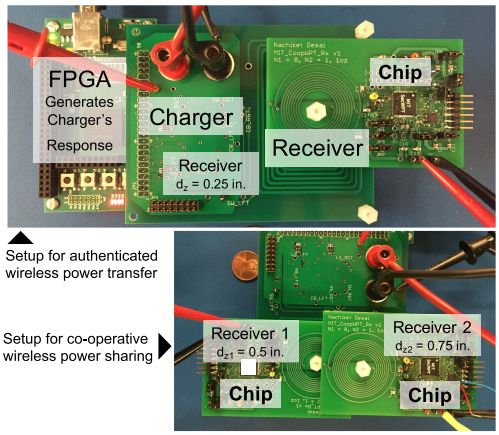


Fig. 16. Measurement setup for charger authentication and power balancing.

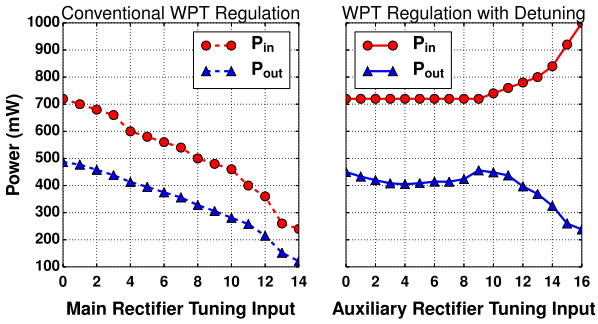


Fig. 17. Power regulation with and without detuning.

generates responses to the challenges sent by the receivers is implemented on an FPGA.

The peak dc output power in the tuned mode is 520 mW and the peak end-to-end efficiency ($P_{\text{out,dc}}/P_{\text{in,dc}}$) is 74%. The control circuits on the receiver consume 32 mW of power. This is with the charger operating from a 4-V supply and the receiver delivering power to a 4-V dc voltage source (both consistent with cell voltages of a standard Li-ion battery). The charger and the receiver are aligned center-to-center with a vertical distance of 0.5 in. between them. A die micrograph and performance summary of the implemented receiver is shown in Fig. 15. The measurement setup for testing both charger authentication and cooperative power balancing is shown in Fig. 16. For the power balancing measurement setup, the two receivers are held at different distances from the same charger by using nylon board spacers of different lengths.

B. Power Blocking and Charger Authentication

An example of power regulation with and without detuning is shown in Fig. 17. The plot on the left shows a more conventional style of regulation with a current-sense-based duty cycle control on the main rectifier, with the auxiliary rectifier disabled. A larger tuning input to the DAC leads to a larger control voltage relative to the peak in Fig. 8. This leads to a lower duty cycle and lower input resistance. As the main rectifier tuning input is increased, the main coil current goes up and so does the back EMF. This leads to the charger drawing lower input dc power. Thus, the receiver is more visible at the transmitter and is susceptible to transients imposed by it.

The plot on the right side of Fig. 17 shows the effect of regulation with controlling the auxiliary rectifier tuning input. As the tuning input is increased, the auxiliary rectifier input resistance $R_{\text{in},a}$ decreases and the auxiliary coil current increases. As the receiver detunes due to this effect, the main coil current is expected to go down, reducing the dc output power of the receiver. In this case, detuning is evident from an increase in the charger input dc power ($P_{\text{in,dc}}$) due to the lower

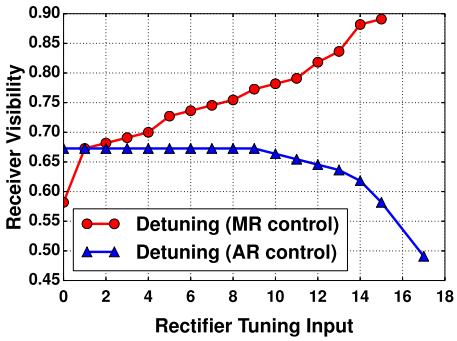


Fig. 18. Receiver visibility at charger.

TABLE III
COMPARISON OF RECENT WIRELESS CHARGING RECEIVERS WITH ACTIVE POWER CONTROL

	This work	Choi et al. [3] ISSCC 2016	Hwang et al. [4] ISSCC 2016	Li et al. [6] ISSCC 2015
Frequency	**6.78 MHz**	50 kHz	100-300 kHz/ 6.78 MHz	13.56 MHz
Total eff. (Peak at dist.)	**74% at 6.35 mm**	N/A	84% at N/A	62.4% at N/A
Output power	**520 mW**	20 mW	6 W	234 mW
Switched passives	**No**	Yes	Yes	No
Compensation technique	**Auxiliary coil**	Resonant cycle tracking	Multi-coil resonance	Primary equalization

back EMF from the lower main coil current. The amount of detuning can also be expressed in terms of the visibility of the receiver at the charger, which can be defined as the difference between charger's input dc power and the input power when there is no receiver present as a fraction of the latter (3). A plot of the receiver visibility at the charger is shown in Fig. 18

$$\text{Rx Visibility} \triangleq \frac{P_{\text{in,No Rx}} - P_{\text{in}}}{P_{\text{in,No Rx}}}. \tag{3}$$

A comparison of the wireless power receiver with other recently reported receivers that apply an active compensation technique to control the amount of power delivered is shown in Table III. To the best of our knowledge, authentication has not been implemented in any of the recently reported wireless charging works.

The authentication flow and the corresponding measured waveforms are shown in Fig. 19. The receiver starts up in the fully detuned state with the auxiliary rectifier enabled and waits for a charger to come in range. When the envelope detector detects a charger, the authentication block on the receiver generates a challenge. Upon receiving the challenge, the charger uses its private key to generate a response, which is then checked by the receiver. Upon successful authentication, the receiver disables the auxiliary rectifier to commence resonant power transfer. This causes $P_{\text{out,dc}}$ to rise to 128 mW from the 8-mW detuned value for the case shown in Fig. 19.

C. Dynamic Power Balancing

Fig. 20 shows the system performance when two receivers are coupled to the same charging coil with different coupling coefficients. If the receivers individually try to maximize their

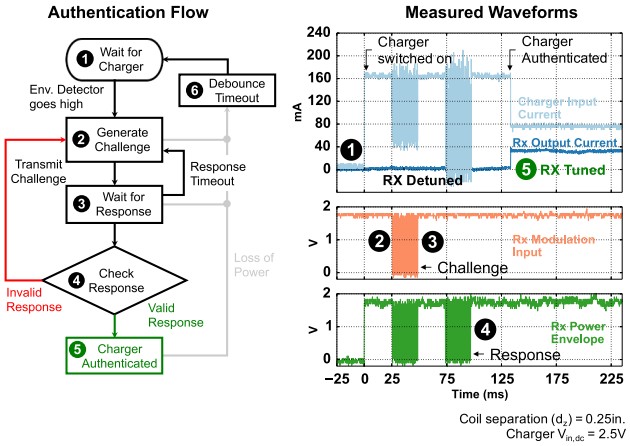


Fig. 19. Authentication flowchart and transmitter and receiver traces during authentication.

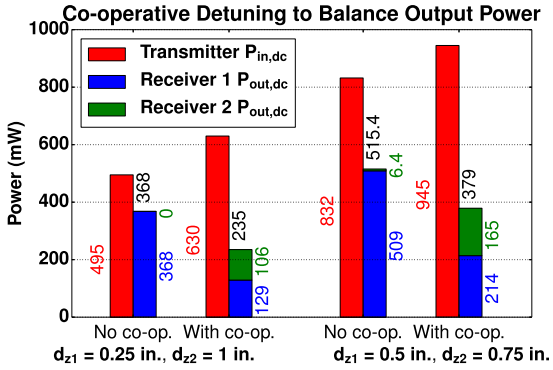


Fig. 20. Cooperative power sharing by receivers at different distances from the charger (d_{z1} and d_{z2} are the distances to the closer and farther receivers, respectively).

output powers, the power delivered is skewed heavily in favor of the nearby receiver. Detuning the nearby receiver can reduce or even reverse the physically imposed asymmetry in the delivered power, and distribute power based on the relative needs of both receivers. Since the charging coil current is limited by the nearby receiver, detuning it allows the charger output power to rise, as shown in Fig. 17. This induces a larger EMF on the farther receiver and allows more power to be delivered to it. Fig. 20 shows power numbers for two distance configurations when the receivers do not cooperate and when they cooperate with the goal of equalizing their individual dc output powers for two separate levels of coupling asymmetry.

Fig. 21 shows that maximally detuning the closer receiver allows the asymmetry in power delivery to be reversed even when the two receivers are at distances in a 4:1 ratio away from the charger. In both cases, the total efficiency (η_{total}) is highest when the receivers do not cooperate, because most of the power goes to the closer receiver at higher efficiency. By detuning the closer receiver, a more significant fraction of the power can be delivered to the farther receiver at lower η_{total}. Thus, detuning allows for a tradeoff between η_{total} and balanced power delivery.

From Fig. 21, it can also be seen that partially detuning the closer receiver using duty cycle control described

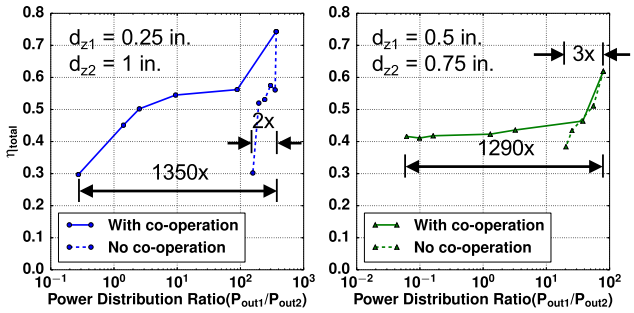


Fig. 21. Range of power ratios obtainable by cooperative action by the receivers.

in Section III-A allows the system to achieve intermediate power distribution ratios. This can offer an overall efficiency benefit when compared against time multiplexing the system between the closer receiver being maximally detuned and fully tuned. For example, in the 4:1 asymmetric case shown in Fig. 21, the overall efficiency in achieving a 50–50 energy split between the two receivers is about 42% with partial detuning of the closer receiver. If instead, time multiplexing is chosen to achieve the same energy split, the system must spend 82% of its time with the closer receiver maximally detuned (a state with lower overall efficiency). This leads to a time-averaged overall efficiency of 37%.

VI. Conclusion

IoT devices with wireless charging capability need to be protected from damaging transients imposed by counterfeit chargers to ensure safe operation. Moreover, with multiple receivers coupled to the same charging coil with different coupling coefficients, the amount of received power is heavily dictated by the physical constraints instead of the actual power requirements of the receivers. This paper presented an active control technique for a wireless power receiver that addresses both these issues by controlling the amount by which the receiver is detuned from the frequency at which the charger transmits power. Detuning is achieved without the use of any switched passive components, which typically need to be implemented with switches capable of tolerating large amounts of current and/or voltage stress. The charger is authenticated using a public key-based authentication scheme that is scalable and avoids the need for the receiver to securely store a private key. The receiver detuning technique achieves up to 16× power blocking and is capable of completely inverting the power distribution profile in a one-charger two-receiver scenario with 4:1 distance asymmetry between the receivers.

Acknowledgment

The authors would like to thank the TSMC University Shuttle Program for chip fabrication.

References

[1] 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*, Jan./Feb. 2016, pp. 290–291.

[2] L. Cheng, W.-H. Ki, T.-T. Wong, T.-S. Yim, and C.-Y. Tsui, "A 6.78 MHz 6 W wireless power receiver with a 3-level $1\times/1/2\times/0\times$ reconfigurable resonant regulating rectifier," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Jan./Feb. 2016, pp. 376–377.

[3] M. Choi, T. Jang, J. Jeong, S. Jeong, D. Blaauw, and D. Sylvester, "A current-mode wireless power receiver with optimal resonant cycle tracking for implantable systems," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Jan./Feb. 2016, pp. 372–373.

[4] J. T. Hwang *et al.*, "An all-in-one (Qi, PMA and A4WP) 2.5 W fully integrated wireless battery charger IC for wearable applications," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Jan./Feb. 2016, pp. 378–379.

[5] K.-G. Moh *et al.*, "A fully integrated 6 W wireless power receiver operating at 6.78 MHz with magnetic resonance coupling," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 230–231.

[6] X. Li, C.-Y. Chui, and W.-H. Ki, "Wireless power transfer system using primary equalizer for coupling- and load-range extension in bio-implant applications," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 228–229.

[7] *AirFuel Wireless Power Transfer System Baseline System Specification V1.3*, AirFuel Alliance, Shenzhen, China, 2016.

[8] *Wireless Power Transfer System Description Version 1.1.2*, Wireless Power Consortium, Piscataway, NJ, USA, 2013.

[9] W. Furtner, S. Schächer, M. Littow, L. Cimaz, and P. E. Leinonen, "BIF—Battery interface standard for mobile devices," in *Proc. Custom Integr. Circuits Conf. (CICC)*, Sep. 2013, pp. 1–8.

[10] D. H. Doughty and E. P. Roth, "A general discussion of Li ion battery safety," *Electrochem. Soc. Interface*, vol. 21, no. 2, pp. 37–44, 2012.

[11] K. Zaghib *et al.*, "Safe and fast-charging Li-ion battery with long shelf life for power applications," *J. Power Sources*, vol. 196, no. 8, pp. 3949–3954, Apr. 2011.

[12] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljačić, "Wireless power transfer via strongly coupled magnetic resonances," *Science*, vol. 317, no. 5834, pp. 83–86, Jul. 2007.

[13] M. W. Baker and R. Sarpeshkar, "Feedback analysis and design of RF power links for low-power bionic systems," *IEEE Trans. Biomed. Circuits Syst.*, vol. 1, no. 1, pp. 28–38, Mar. 2007.

[14] Y. Xing, E. W. M. Ma, K. L. Tsui, and M. Pecht, "Battery management systems in electric and hybrid vehicles," *Energies*, vol. 4, no. 11, pp. 1840–1857, 2011.

[15] K. Dietz, "Battery authentication for portable power supplies," *Power Electron. Technol.*, vol. 32, no. 4, pp. 34–39, Apr. 2006.

[16] H. Iwashita *et al.*, "Registration-based vehicle battery charging system," U.S. Patent 8,290,649, Oct. 16, 2012. [Online]. Available: https://www.google.com/patents/US8290649

[17] L. G. Edington and J. E. Dailey, "Encrypted response smart battery," U.S. Patent 6,975,092, Dec. 13, 2005. [Online]. Available: https://www.google.com/patents/US6975092

[18] N. R. C. Rybeck, M. Hansson, and P. Holmqvist, "Rechargeable battery pack with identification circuit, real time clock and authentication capability," U.S. Patent 5,608,306, Mar. 4, 1997. [Online]. Available: https://www.google.com/patents/US5608306

[19] *BQ26100 SHA-1/HMAC Based Security and Authentication IC With SDQ Interface*. Accessed Jan. 29, 2016. [Online]. Available: http://www.ti.com/lit/ds/symlink/bq26100.pdf

[20] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "An elliptic curve processor suitable for RFID tags," in *Proc. IACR Cryptol. ePrint Arch.*, Nov. 2006, pp. 1–14.

[21] B. L. Cannon, J. F. Hoburg, D. D. Stancil, and S. C. Goldstein, "Magnetic resonant coupling as a potential means for wireless power transfer to multiple small receivers," *IEEE Trans. Power Electron.*, vol. 24, no. 7, pp. 1819–1825, Jul. 2009.

[22] J. J. Casanova, Z. N. Low, and J. Lin, "A loosely coupled planar wireless power system for multiple receivers," *IEEE Trans. Ind. Electron.*, vol. 56, no. 8, pp. 3060–3068, Aug. 2009.

[23] N. Desai and A. P. Chandrakasan, "A ZVS resonant receiver with maximum efficiency tracking for device-to-device wireless charging," in *Proc. 42nd Eur. Solid-State Circuits Conf. (ESSCIRC)*, Sep. 2016, pp. 313–316.

[24] D. Ahn and S. Hong, "Effect of coupling between multiple transmitters or multiple receivers on wireless power transfer," *IEEE Trans. Ind. Electron.*, vol. 60, no. 7, pp. 2602–2613, Jul. 2013.

[25] N. V. Desai, "Circuits for efficient and secure power delivery in distributed applications," Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2017.
[26] *Digital Signature Standard (DSS)*, document FIPS PUB 186-4, NIST, Jul. 2013.
[27] J. A. Solinas, "Efficient arithmetic on koblitz curves," in *Towards 702 a Quarter-Century Public Key Cryptography*. Boston, MA, USA: Springer, 2000, pp. 125–179.
[28] S. S. Roy, K. Järvinen, and I. Verbauwhede, "Lightweight coprocessor for Koblitz curves: 283-Bit ECC including scalar conversion with only 4300 gates," in *Proc. Cryptogr. Hardw. Embedded Syst.*, Sep. 2015, pp. 102–122.
[29] R. Azarderakhsh, K. U. Järvinen, and M. Mozaffari-Kermani, "Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 4, pp. 1144–1155, Apr. 2014.
[30] D. J. Bernstein and T. Lange, "Analysis and optimization of elliptic-curve single-scalar multiplication," *Contemp. Math.*, vol. 461, no. 461, pp. 1–20, 2008.
[31] T. Beth and D. Gollman, "Algorithm engineering for public key algorithms," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 4, pp. 458–466, May 1989.
[32] A. Reyhani-Masoleh, "Efficient algorithms and architectures for field multiplication using Gaussian normal bases," *IEEE Trans. Comput.*, vol. 55, no. 1, pp. 34–47, Jan. 2006.
[33] J.-W. Lee, S.-C. Chung, H.-C. Chang, and C.-Y. Lee, "Efficient power-analysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 1, pp. 49–61, Jan. 2014.
[34] P. Pessl and M. Hutter, "Curved tags—A low-resource ECDSA implementation tailored for RFID," in *Proc. Int. Workshop Radio Freq. Identificat., Secur. Privacy Issues (RFIDSec)*, 2014, pp. 156–172.
[35] E. Wenger, "Hardware architectures for MSP430-based wireless sensor nodes performing elliptic curve cryptography," in *Proc. Int. Conf. Appl. Cryptograph. Netw. Secur.*, Jun. 2013, pp. 290–306.

Nachiket Desai (S'10) received the B.Tech. degree in electronics and electrical communication engineering from IIT Kharagpur, Kharagpur, India, in 2010, and the M.S. and Ph.D. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2012 and 2017, respectively.

In 2012, he was with Kilby Labs, Texas Instruments Incorporated, Dallas, TX, USA, where he was involved in designing power converters for energy harvesting applications. In 2014, he was with Kilby Labs, Texas Instruments Incorporated, Santa Clara, CA, USA, where he was involved in designing adaptive rectifier control circuits for wireless charging. He is currently a Research Scientist with Intel Labs, Hillsboro, OR, USA. His current research interests include power converter design for integrated dc–dc converters, energy harvesting, and wireless power transfer.

Chiraag 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 Laboratory, Texas Instruments Incorporated, Dallas, TX, USA, where he was involved in 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.

Shubham Chandak received the B.Tech. degree in electrical engineering from IIT Bombay, Mumbai, India, in 2016. He is currently pursuing the M.S. and Ph.D. degrees in electrical engineering with Stanford University, Stanford, CA, USA.

In 2015, he was with the Massachusetts Institute of Technology, Cambridge, MA, USA, where he was involved in designing hardware for elliptic curve cryptography. His current research interests include information theory, cryptography, and machine learning.

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 September 1994, he has been with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, where he is currently the Vannevar Bush Professor of Electrical Engineering and Computer Science. He was the Director of the MIT Microsystems Technology Laboratories from 2006 to 2011. From 2011 to 2017, he was the Head of the MIT Department of Electrical Engineering and Computer Science. Since 2017, he has been the Dean of the MIT School of Engineering. He has co-authored the books *Low Power Digital CMOS Design* (Kluwer Academic Publishers, 1995), *Digital Integrated Circuits* (Pearson Prentice-Hall, 2003, 2nd edition), and *Sub-threshold Design for Ultra-Low Power Systems* (Springer, 2006). His current research interests include ultra-low-power circuit and system design, energy harvesting, energy efficient RF circuits, and hardware security.

Dr. Chandrakasan 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 received 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. He has served in various roles for the IEEE ISSCC, including the Program Chair, the Signal Processing Subcommittee Chair, and the Technology Directions Subcommittee Chair. He has been the Conference Chair of ISSCC since 2010.