The following publication H. Wang, N. Tashakor, W. Jiang, W. Liu, C. Q. Jiang and S. M. Goetz, "Hacking Encrypted Frequency-Varying Wireless Power: Cyber-Security of Dynamic Charging," in IEEE Transactions on Energy Conversion, vol. 39, no. 3, pp. 1947-1957, Sept. 2024 is available at https://doi.org/10.1109/TEC.2024.3355743.

Hacking Encrypted Frequency-Varying Wireless Power: Cyber-Security of Dynamic Charging

Hui Wang, *Member, IEEE*, Nima Tashakor, *Member, IEEE*, Wei Jiang, Wei Liu, *Member, IEEE*, C. Q. Jiang, *Senior Member, IEEE*, Stefan M. Goetz, *Member, IEEE*

***Abstract*—Recently, energy encryption for wireless power transfer (WPT) has been developed for energy safety, which is important in public places to suppress unauthorized energy extraction. Most techniques vary the frequency so that unauthorized receivers cannot extract energy because of non-resonance. However, this strategy is unreliable. To stimulate the progress of energy encryption technology and point out security holes, this paper proposes a decryption method for the fundamental principle of encrypted frequency-varying WPT. The paper uses an auxiliary coil to detect the frequency and a switched-capacitor array to adaptively compensate the receiver for a wide frequency range. The switched-capacitor array contains two capacitors and one semiconductor switch. One capacitor compensates the receiver all the time while the other's active time during one WPT cycle is regulated by the switch. Thus, the proposed hacking receiver controls the equivalent capacitance of the compensation and steals WPT energy. Finally, a simulation model and experimental results prove the effectiveness of the attack on frequency-hopping energy encryption. Although any nonnegligible energy extracted would be problematic, we achieved to steal 78~84% of the energy an authorized receiver could get. When the frequency changes, the interceptor is coarsely tuned very quickly, which can hack fast frequency-varying encrypted system.**

***Index Terms*—Wireless power transfer, cyber security, energy hacking, frequency varying, energy encryption, energy decryption, variable capacitor.**

Manuscript received Aug. 2023; revised Nov. 2023; accepted Jan. 2024. This work was supported by the National Science Foundation (NSF) under Grant #1608929 and the Federal Ministry of Education and Research of Germany in the project "Open6GHub" (grant number: 16KISK004), as well as the TU-Nachwuchsring, Rhineland-Palatinate Technical University (RPTU), Germany, under Grant #FF_2024-1_4. The content is solely the responsibility of the authors and does not necessarily represent the views of the funders. (Corresponding author: Stefan M. Goetz, stefan.goetz@duke.edu.)

H. Wang, Nima Tashakor, and Stefan M. Goetz are with the Department of Electrical and Computer Engineering, Duke University, Durham, NC 27710, USA (e-mail: hui.wang@duke.edu; nima.tashakor@duke.edu; stefan.goetz@duke.edu).

W. Jiang is with the Department of Electrical and Computer Engineering, Rhineland-Palatinate Technical University, Germany (e-mail: jwauto@163.com).

W. Liu is with Research Centre for Electric Vehicles and Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University, 999077, Hong Kong (e-mail: wei.liu@polyu.edu.hk).

C. Q. Jiang is with the Department of Electrical Engineering and the State Key Laboratory of Terahertz and Millimeter Waves, City University of Hong Kong, Hong Kong SAR, China. (e-mail: chjiang@cityu.edu.hk).

I. Introduction

Wireless power transfer (WPT) is a widely known solution in contactless charging [1]. The main practical advantages compared to traditional wired charging are high flexibility through electromagnetic coupling, on-road move-and-charge ability [2] as well as high safety due to the avoidance of any connector and bare contacts [3]. Such features make WPT very popular for charging smartphones [4], electric motors [5], electric vehicles [6], medical devices [7], and implants [8].

However, despite numerous advantages, energy safety is still a major concern. For a public charging service, unauthorized users also can harvest energy in this electromagnetic field [9].

To solve this problem, various energy encryption methods have been proposed. Static wireless charging with magnetic field editing is desired [10], i.e., the transmitter knows the authorized user's position and selectively charges that area accordingly [11]. Thus, unauthorized users should not have access to the magnetic fields and cannot steal energy, as shown in Fig. 1(a). However, in many applications, it is complicated to shield off the field entirely and make it inaccessible to any form of interceptor; this applies particularly if the receiver should have the freedom to move [12]. For roadway charging, for instance, multiple authorized users drive fast on the road [13]; so all transmitter coils should be activated, and unauthorized users are unavoidably involved.

Therefore, in some public places, power suppliers prefer frequency-varying strategies [14], as shown in Fig. 1(b). In principle, only authorized receivers know the WPT frequency (sequence), which may be the key itself as in digital cyphers, most obviously stream cyphers, or exchanged on a separate secure digital communication channel. Thus, only authorized receivers should be able to tune their resonators through a capacitor to compensate the receiver, while unauthorized users cannot harvest energy because of the impedance mismatch of the receiving circuit [15]. A switched-capacitor array is the most popular compensation for frequency-varying encryption [16], as the transceiver can jump between multiple fixed resonance frequencies [17]. In principle, the number of resonant frequency points is equal to the number of parallel capacitors [18]. Recently developed topologies for capacitor compensation [19], such as higher-order compensation [20] or capacitor matrices [21], can offer more resonant frequency points. Moreover, to complicate energy interception, Qi et al.

presented a stepless frequency compensation method, which can control the frequency from 90 kHz to 150 kHz with a variable capacitor [22].

However, we will demonstrate that encryption through frequency-hopping or -varying is not reliable and can be hacked easily. To avoid someone abusing this energy encryption method and to stimulate more researchers to pay attention to energy encryption, this paper demonstrates an energy decryption attack on frequency-varying WPT systems. The ingredients are an auxiliary coil to detect the WPT frequency in time and a continuous switched-capacitor array to compensate the receiver for a wide frequency range.

This paper is organized as follows: Section II will first analyze the system configuration. Next, Section III will present the frequency detection and the stepless frequency compensation. Section IV follows with the system design procedure. A series of computer simulations and experiments verify the approach in Section V and Section VI, respectively. Finally, Section VII summarizes the paper.

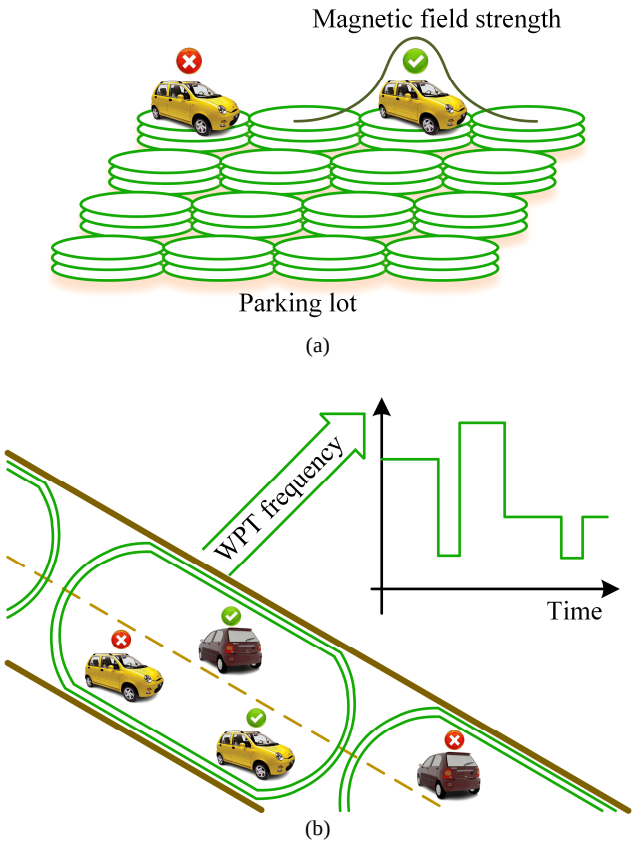


Fig. 1. Current energy protection methods for WPT. (a) Magnetic field editing for static charging. (b) Frequency-variation for dynamic charging.

II. System Configuration

As shown in Fig. 2, both authorized and unauthorized receivers have access to the electromagnetic field created by the transmitter and attempt to harvest energy, where L_T is the inductance of the transmitter, while L_R and L_A denote the inductances of the hacking receiver and auxiliary coil, respectively; I_T and I_R are currents of transmitter and hacking receiver, respectively; M_R denotes the mutual inductance between transmitter and receiver, and M_A denotes the mutual inductance between transmitter and auxiliary coil, while M_{RA} is the mutual inductance between hacking receiver and auxiliary coil; C_{R1} and C_{R2} are the capacitors to compensate L_R for a wide frequency range, and S_R is the switch to control C_{R2}; V_{CR1}, V_{CR2}, V_{SR}, I_{R1}, and I_{R2} are the voltages and currents of corresponding capacitors and switch, respectively; V_{LR} and V_{LA} are the voltages of L_R and L_A, respectively; V_{RL} is the load voltage.

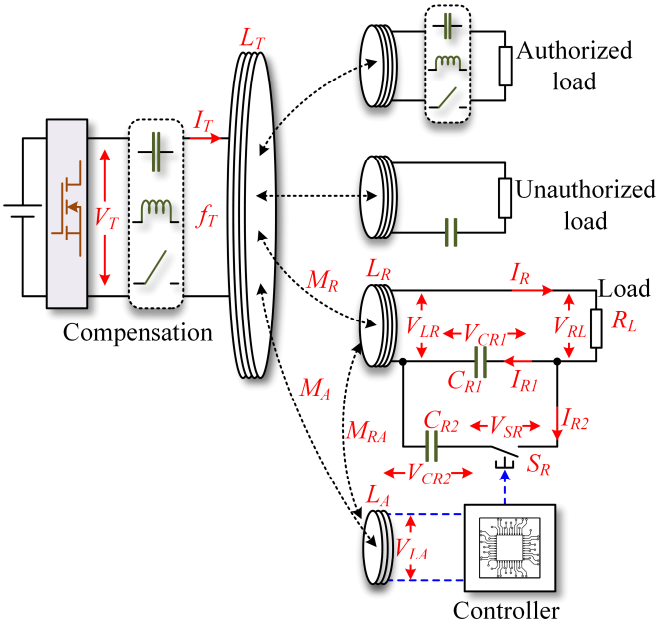


Fig. 2. Common wireless charging system and the proposed hacking receiver.

It should be mentioned that, although the compensation settings of the transmitter and authorized receivers are unknown, the transmitter frequency f_T should be able to vary throughout a wide range [16].

The interceptor coil L_R serves as the receiver to steal wireless power, while the auxiliary coil L_A is a small open-loop sensor coil to detect the phase and frequency of the transmitter current I_T.

Besides, it should be mentioned that the compensation network only contains one switch and two capacitors, which is sufficient to compensate the receiver L_R for a wide frequency range. The key is controlling the turn-on time of the switch and adjusting the duty cycle of the controlled capacitor during one cycle. Therefore, the equivalent capacitance of the compensation network can be continuously controlled over a wide range. Also, the compensation network retains the merit of being simple and robust when compared with high-order or capacitor-matrix compensation networks.

III. System Decryption Operation Strategy

A. Frequency and Phase Detection

For the proposed energy decryption method, the detection

of WPT frequency f_T and phase is the first step in wireless power decryption.

Based on the most basic electromagnetic induction principle of WPT, voltages V_{LR} and V_{LA} can be expressed as [23]

$$\begin{cases} V_{LR} = 2\pi f_T M_R I_T - 2\pi f_R L_R I_R \\ V_{LA} = 2\pi f_T M_A I_T + 2\pi f_R M_{RA} I_R \end{cases}. \tag{1}$$

Obviously, both V_{LR} and V_{LA} contain the frequency and phase information of I_T. However, V_{LR} is much easier to be affected by the receiver's current I_R, as L_R is much larger than M_{RA}. When the receiving circuit of the variable-capacitor compensation is not resonant, I_R is not sinusoidal and strongly distorted. Thus, V_{LR} is disturbed, which would deteriorate any estimation of the phase.

The simple auxiliary coil as a sensor is practically a Kelvin-connected field detection and allows rapid undistorted estimation of field properties [24]. The frequency f_T is narrowed down already after the first zero crossings through simple counting. Also, the voltage upward zero crossings can be detected and treated as zero phase, which will be used for capacitance regulation in the next section.

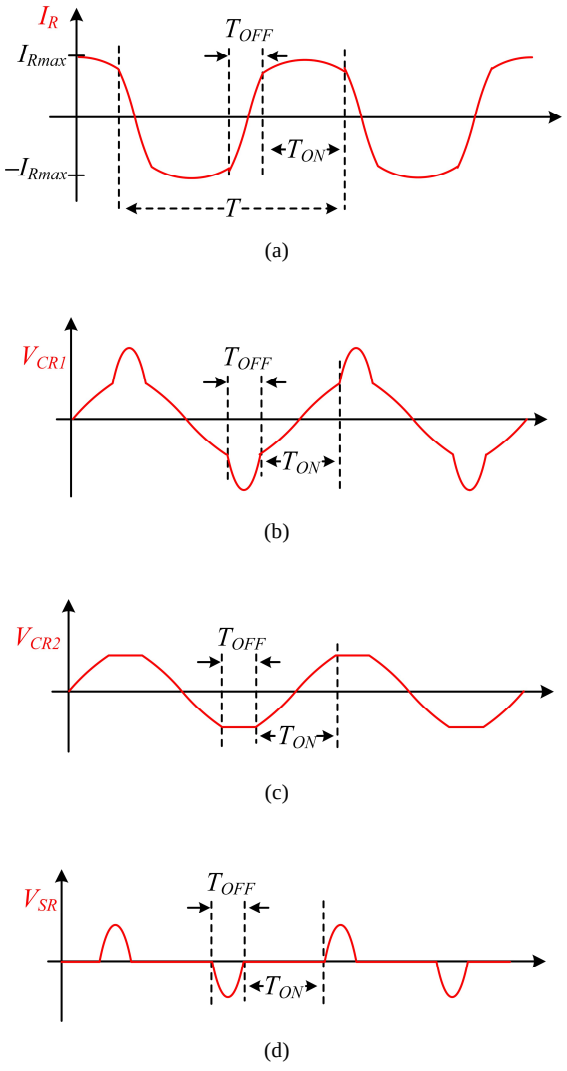


Fig. 3. Waveforms of system voltage and current with the time-division switched-capacitor array. (a) Receiver current. (b) The voltage of the capacitor C_{R1}. (c) The voltage of the capacitor C_{R2}. (d) The voltage of the switch S_R.

B. Compensation Capacitance Regulation with Time-Division Method

To regulate the equivalent capacitance of the compensation, this paper adopts a time-division regulation method [25], which controls the switch S_R on and off twice during one WPT cycle. As shown in Fig. 3, the capacitor C_{R1} is actively compensating the entire time, while C_{R2} only participates temporarily for T_{ON}, twice in one period. Therefore, the effective equivalent capacitance of the compensation C_{RE} can be controlled by switching S_R. To be more specific, when the capacitor voltage V_{CR1} increases from 0 to the maximum value, the equivalent capacitance C_{RE} can be expressed as

$$\frac{\int_0^{\frac{T}{4}} I_R dt}{C_{RE}} = \frac{\int_0^{\frac{T_{ON}}{2}} I_R dt}{C_{R1}+C_{R2}} + \frac{\int_{\frac{T_{ON}}{2}}^{\frac{T}{4}} I_R dt}{C_{R1}} \tag{2}$$

where T is the period of one WPT cycle, and T_{ON} is the switch-on time of switch S_R during one control cycle.

As aforementioned, the switch S_R will turn on and off twice. Thus, the control period is half of one WPT period, and T_{OFF} can be expressed as

$$T_{ON} + T_{OFF} = \frac{T}{2}. \tag{3}$$

As the compensation varies, the current I_R in (2) is a piecewise function and can be expressed as

$$I_R = \begin{cases} I_{Rmax1} \sin\left(2\pi f_{T1} t + \dfrac{\pi}{2}\right) & \left(t \le \dfrac{T_{ON}}{2}\right) \\ I_{Rmax2} \sin\left(2\pi f_{T2} t + \dfrac{\pi}{2} + \theta_T\right) + K_T & \left(\dfrac{T_{ON}}{2} \le t \le \dfrac{T}{4}\right) \end{cases} \tag{4}$$

where f_{T1} and f_{T2} are unknown frequencies; θ_T and K_T are offsets unknown yet; I_{Rmax1} and I_{Rmax2} are the maximum currents of the transmitter compensated through paralleled $C_{R1}||C_{R2}$ and the single capacitor C_{R1}, respectively.

For simplification, the current I_R is considered a sinuous waveform and expressed as

$$I_R = I_{Rmax} \sin\left(2\pi f_T t + \frac{\pi}{2}\right) \quad \left(0 \le t \le \frac{T}{4}\right). \tag{5}$$

Therefore, an approximate analytical solution for C_{RE} can be obtained as

$$C_{RE} = \frac{1}{\dfrac{1-\sin\left(\pi f_T T_{ON}\right)}{C_{R1}} + \dfrac{\sin\left(\pi f_T T_{ON}\right)}{C_{R1}+C_{R2}}}. \tag{6}$$

Also, the desired equivalent capacitance can be calculated from [26]

$$C_{RE} = \frac{1}{\left(2\pi f_T\right)^2 L_R}. \tag{7}$$

In consequence, with the acknowledged inductance, capacitance, and detected frequency, the switch-on time T_{ON} follows

$$T_{ON}=\frac{1}{\pi f_T}\arcsin\left(\frac{C_{R1}+C_{R2}}{C_{R2}}-\left(2\pi f_T\right)^2 L_R\frac{C_{R1}\left(C_{R1}+C_{R2}\right)}{C_{R2}}\right). \quad (8)$$

After getting the theoretical calculation value of T_{ON}, the primary side needs to tune this value because of the difference between (4) and (5). Also, considering the signal V_{LA} may be affected by external electromagnetic interference, the zero-phase point is imprecise. Moreover, if the transmitter current is not constant or load-independent, I_T is generally positively related to the impedance of the receiving circuits $\sum Z_i$, and their relationship can be expressed as [27]

$$I_T \propto \frac{V_T}{\sum_1^n Z_i'}=\frac{V_T}{\left(2\pi f_T\right)^2}\sum_1^n\frac{Z_i}{M_i^2} \quad (9)$$

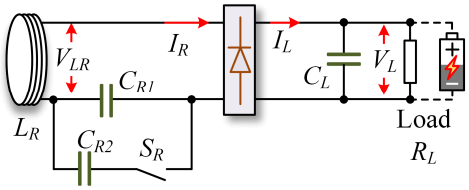


Fig. 4. Receiving circuit with rectifier bridge and load battery.

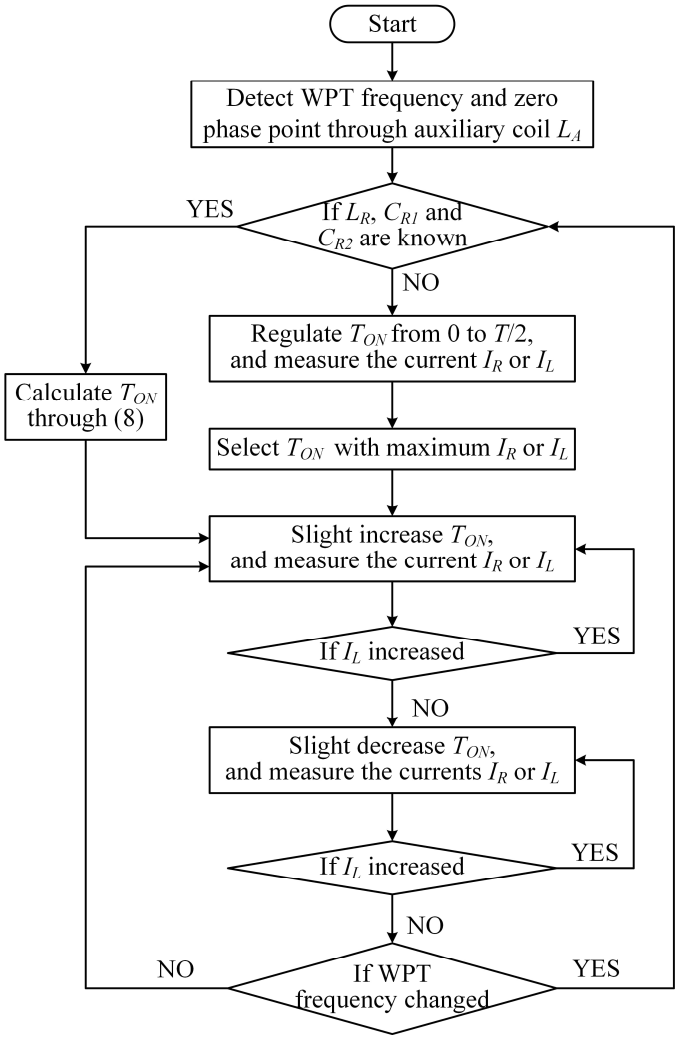


Fig. 5. Flowchart of energy decryption based on time counting and comparison.

where V_T is the primary converter's output voltage, and $\sum Z'_i$ is the impedance of all receivers' impedance referred to the transmitter side.

Thus, with larger I_T, the V_{LR} may also increase according to (1). In other words, when the current I_T is not load-independent, the maximum power transfer frequency point may drift from the resonant frequency point, and it is very difficult to calculate through equations.

The most applicable way for tuning T_{ON}/T_{OFF} is by detecting the load current or voltage. By increasing or decreasing T_{ON}, the load power changes accordingly. Thus, the T_{ON} that relates to the maximum load current or voltage V_L is the desired switching time. It should be mentioned that a large voltage stabilizing capacitor C_L may connect in parallel to the DC-load in some applications, and it will stabilize the voltage and current of the load, as shown in Fig. 4. Also, if the load is a battery, V_L is always increasing during the hacking process. Therefore, it is difficult to detect any V_L variation when changing T_{ON}, while the receiver current I_R and the current I_L for both R_L and C_L are the desired reference signals for tuning T_{ON}.

To illustrate the proposed energy decryption method better, the flowchart of the whole process is shown in Fig. 5.

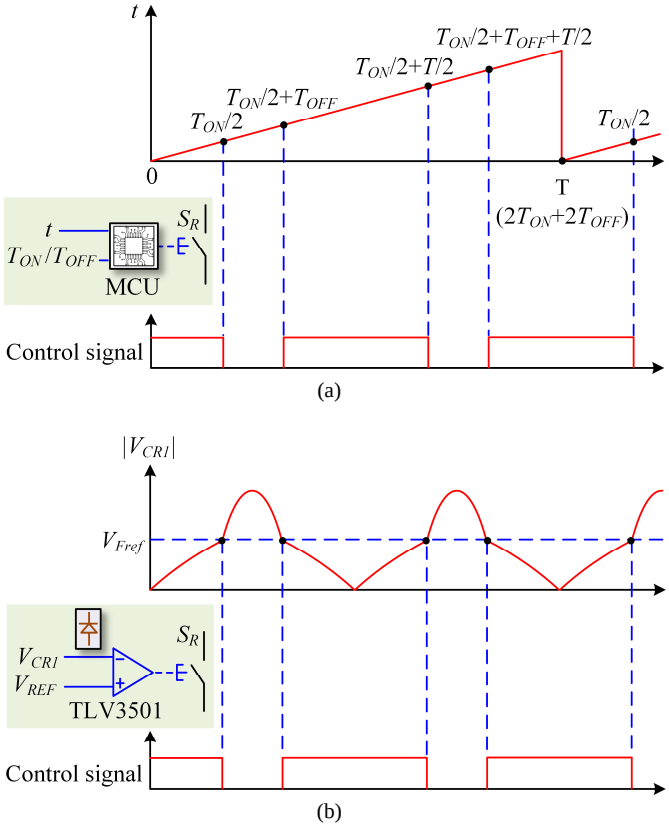


Fig. 6. Control strategy for switch S_R. (a) Extract control signal from temporal comparison. (b) Extract control signal from voltage comparison.

IV. System Design

A. Control Signal Source for Time-Division Switched-Capacitor

There are two possible control strategies for switch S_R to regulate the equivalent capacitance C_{RE}: one is based on time counting and comparing with switching time T_{ON}, while the other one is based on measuring capacitor voltage V_{CR1} and comparing with voltage threshold V_{REF}, as shown in Fig. 6. The one offering higher reliability and possessing better performance will be employed.

For the voltage comparison strategy, the desired voltage threshold V_{REF} can be acquired through negative feedback regulation, as shown in Fig. 7. The largest advantage is that there is no need to detect the WPT frequency or zero-phase point. Also, the voltage comparison can be conducted by a zero-crossing detector (comparator chip). Thus, the controller does not need to measure the high-frequency AC voltage V_{CR1}.

However, the feedback control of V_{REF} in Fig. 7 is time-consuming, as V_{CR1} is generally thousands of volts under resonant conditions. Once the reference V_{REF} increases too much and is larger than the maximum value of V_{CR1}, S_R will be on all the time; thus, we need to regulate V_{REF} from the beginning. Moreover, if the transmitter current I_T, the mutual inductance M_R, or the load R_L change, I_R and V_{CR1} follow accordingly. As a result, the intercepting receiver needs to re-regulate the threshold V_{REF}.

Therefore, we selected the temporal comparison strategy. Although WPT frequency and zero-phase detection are required, the desired switching time can be acquired faster to deal with variable frequency encryption strategy. Also, if I_T is load-independent, the switching time T_{ON}/T_{OFF} is only related to frequency f according to (8), and there is no need to regulate the switching time when the load changes.

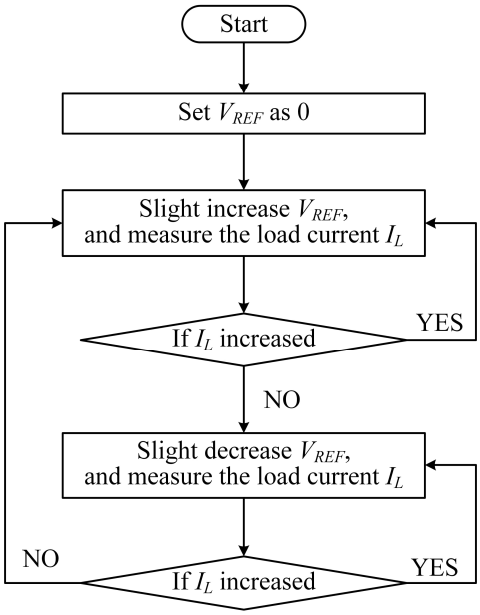


Fig. 7. Flowchart of energy decryption based on voltage measuring and comparison.

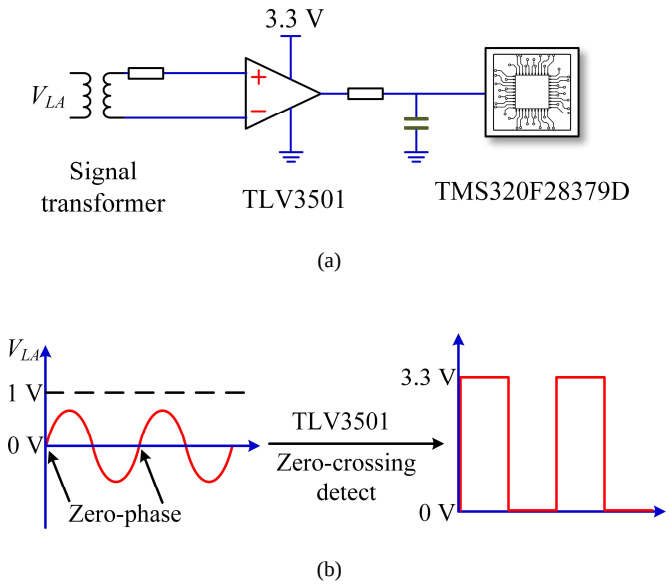


Fig. 8. Frequency and phase detection. (a) Detection circuit. (b) Signal processing.

B. Signal Processing Circuit

As the energy we are aiming to hack is generally tens to hundreds of kilohertz, phase detection should be timely and effective.

First, we employed a small signal transformer to isolate the signal V_{LA}. Then, considering the signal V_{LA} from coil L_A may be too small to be detected by any signal processor, the TLV3501 thresholds, quantifies, and amplifies V_{LA} with minimum phase lag, as shown in Fig. 8.

C. Switch for Compensation Capacitor

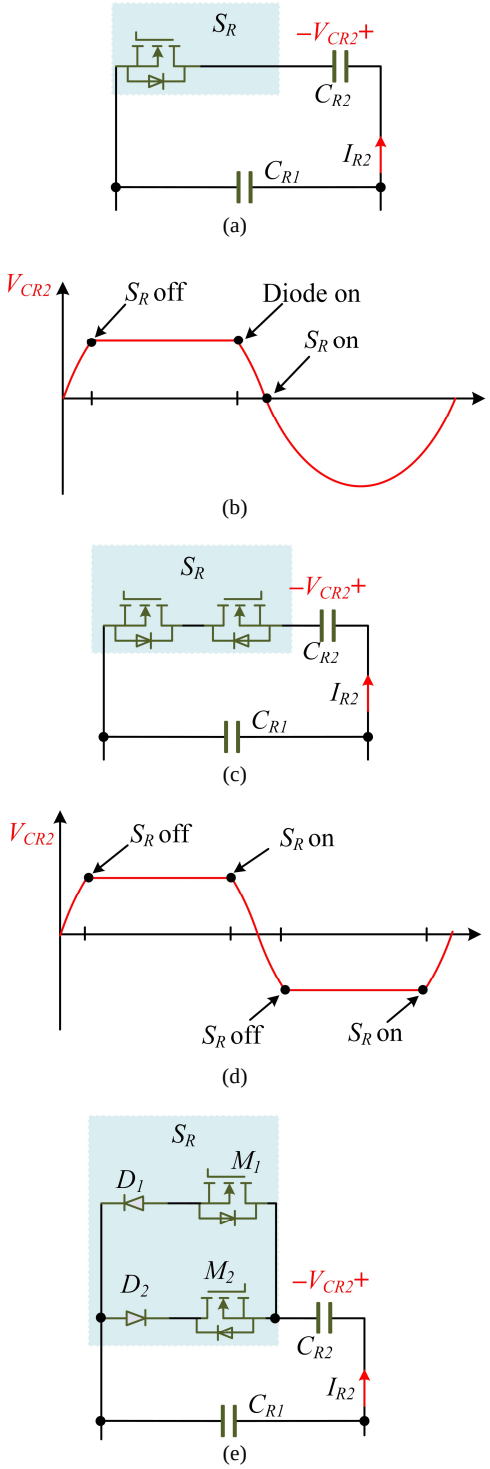
Previous work with variable capacitors uses only a single MOSFET for switch S_R [28], as shown in Fig. 9(a). However, the capacitor current I_{R2} is AC, while the MOSFET contains a body diode. Thus, the high-frequency capacitor current is only under control during half a period, while the body diode of the MOSFET continuously conducts during the other half-cycle, as shown in Fig. 9(b). Therefore, the adjustment effect is only half of the idea condition, and the fundamental component decreases in this asymmetric voltage waveform.

A pair of reverse-series-connected MOSFETs can solve the problem, as shown in Fig. 9(c). Thus, both the higher and lower half-cycle of the capacitor current can be controlled, as shown in Fig. 9(d).

However, the controller needs to compare the time with four switching times in one cycle, as shown in Fig. 6(a). Especially, if the switch S_R delays turn-on at the second or fourth comparison, the capacitor voltages V_{CR1} and V_{CR2} should be different. Thus, S_R does not turn on at zero voltage, and a large current loop is formed between two capacitors.

Therefore, to avoid the current loop between capacitors and reduce switch-on losses of S_R, we employ two MOSFETs and two diodes as S_R, as shown in Fig. 9(e) and (f). At the first switching time $T_{ON}/2$, we turn off the first MOSFET, namely

M_1, and turn on the second MOSFET, namely M_2. No current flows through M_2 until V_{CR2} is higher than V_{CR1} because of D_2. Hence, S_R will be on automatically and preciously at the second switching time $T_{ON}/2+T_{OFF}$. It should be mentioned that both D_2 and M_2 switch on at zero voltage, just like shown in Fig. 3(d), so they are well protected. Similarly, at the third switching time $T_{ON}/2+T/2$, M_2 is off and M_1 is on. Then, S_R will be on automatically and preciously at the fourth switching time, and both D_1 and M_1 switch on at zero voltage.



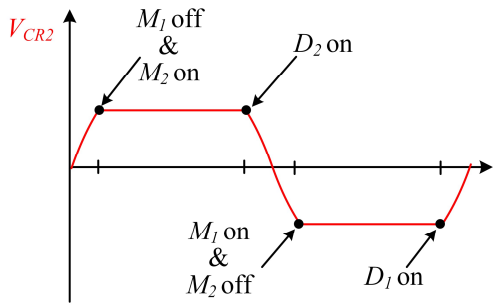


Fig. 9. Various circuits for adaptive capacitor compensation. (a) Single transistor for the capacitor. (b) Asymmetric capacitor voltage. (c) Double transistor as the bidirectional switch for the capacitor. (d) Symmetrical capacitor voltage with four control points. (e) Parallel-transistor-and-diode circuit for switch S_R. (f) Symmetrical capacitor voltage with two control points.

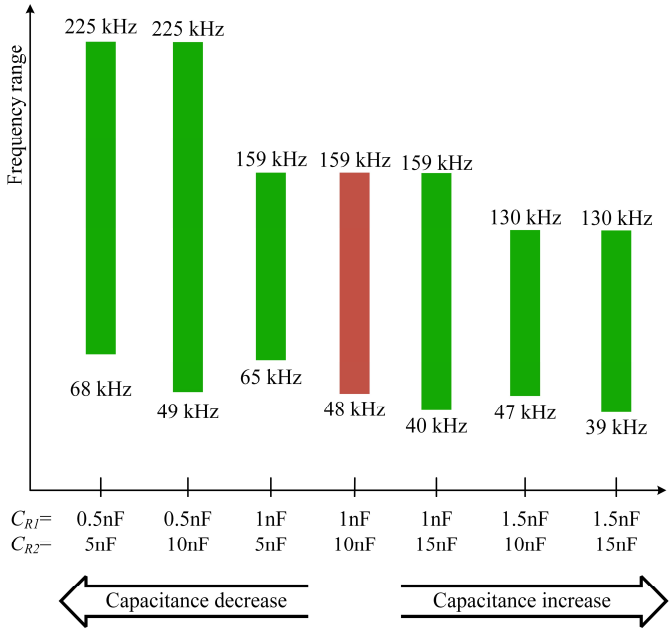


Fig. 10. Relationship between the hacking frequency range and capacitance variation.

D. Capacitance Selection

The switched-capacitor array allows changing the equivalent capacitance C_{RE} in the range of $[C_{R1}, C_{R1}+C_{R2}]$. Thus, the hacking frequency range reaches

$$\frac{1}{2\pi\sqrt{L_R\left(C_{R1}+C_{R2}\right)}} \le f_R \le \frac{1}{2\pi\sqrt{L_R C_{R1}}}. \tag{10}$$

Therefore, C_{R1} should be low enough to compensate the receiver at the highest frequency f_H, while $C_{R1}+C_{R2}$ should be large enough to compensate L_R at the lowest frequency f_L.

As a result, capacitances C_{R1} and C_{R2} can be expressed as

$$\begin{cases} C_{R1} \le \dfrac{1}{\left(2\pi\times f_H\right)^2 L_R} \\ C_{R2} \ge \dfrac{1}{\left(2\pi\times f_L\right)^2 L_R} - C_{R1} \end{cases}. \tag{11}$$

Generally, the international standard of automotive wireless electricity transmission of SAE is 85 kHz [29]. Thus, the

decryption frequency range should include at least 80~100 kHz. Then, the capacitances can be selected through (11).

As various capacitor types have aging problems and capacitances tend to decrease, it is desired to select a larger capacitance of C_{R2}. Otherwise, the lower limit of the hacking frequency may increase over time. To be more specific, if the inductance L_R is constant as 1 mH, while capacitances C_{R1} and C_{R2} change from 50% to 150%, the hacking frequency range will change as shown in Fig. 10. Also, this figure illustrates that if C_{R1} is too large, the upper limit f_H may not be high enough. Thus, it is desired to select a smaller capacitance of C_{R1} to avoid an insufficient upper limit f_H.

Meanwhile, C_{R2} cannot be infinitely large, otherwise, the equivalent capacitance C_{RE} will be too sensitive to T_{ON}/T_{OFF}. Also, C_{R1} cannot be infinitesimal. Otherwise, the peak voltage of V_{CR1} would be too high. In consequence, the peak voltage may exceed the limits of switch S_R and break it.

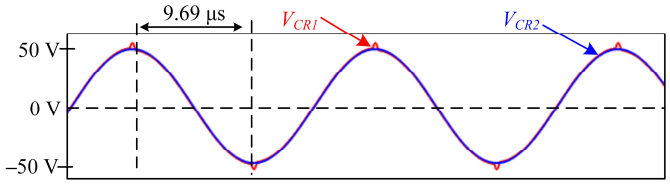
TABLE I
SIMULATION PARAMETERS

Item	Value/Type	Unit
WPT frequency range (f_T)	50~300	kHz
Transmitter coil inductances (L_T)	150	μH
Receiver coil inductances (L_R, L_{R50}, L_{R300})	80, 80, 80	μH
Compensation capacitances (C_{R1}, C_{R2})	3, 130	nF
Load resistance (R_L)	25	Ω

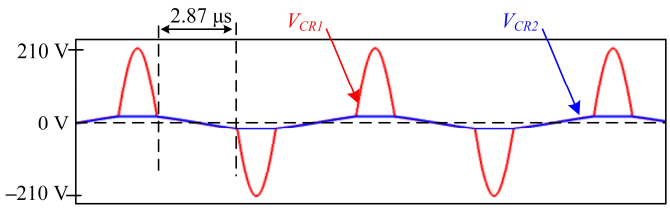
V. SIMULATION

For verification, a series of computational simulations in MATLAB/Simulink provided verification. Transmitter L_T offers load-independent current I_T from 50~300 kHz. In addition to the transmitter and hacking receiver, two more receivers L_{R50} and L_{R300} serve for comparison. The resonant frequencies for low-frequency receiver L_{R50} and high-frequency receiver L_{R300} were 50 kHz and 300 kHz, respectively, and other key parameters are given in Table I.

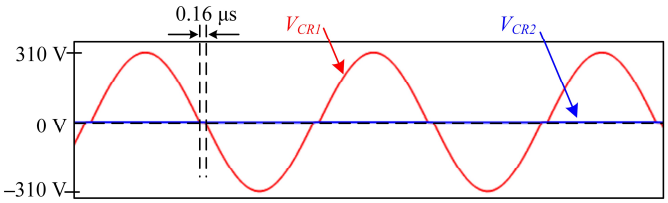
When the transmitter provides I_T at 50 kHz, 120 kHz, and 300 kHz, the hacking controller calculates T_{ON} as 9.69 μs, 2.87 μs, and 0.16 μs respectively, as shown in Fig. 11.



(a)



(b)



(c)

Fig. 11. Voltages of the capacitors for the hacking receiver (a) at 50 kHz, (b) at 120 kHz, and (c) at 300 kHz.

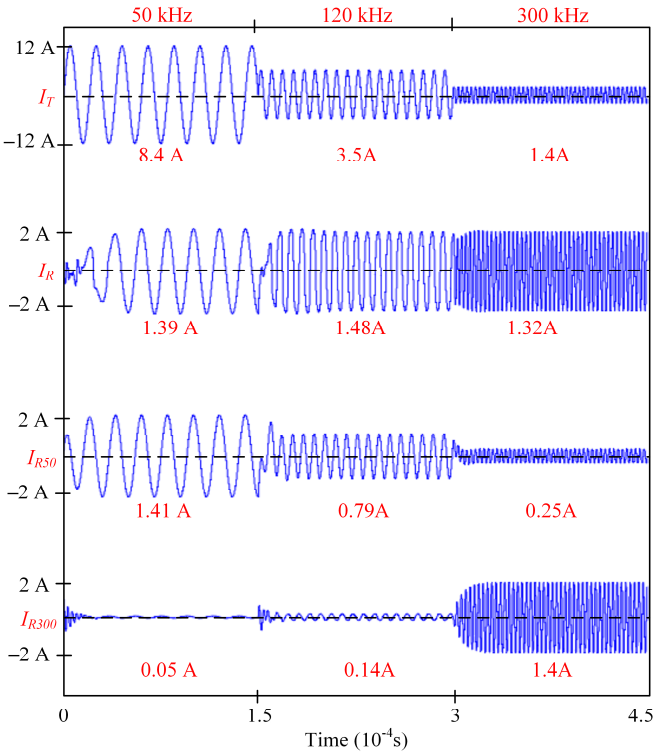


Fig. 12. Currents of the transceiver and the three receivers at different frequencies: from top to bottom (1) the transmitter, (2) the unauthorized interceptor, (3) the receiver with fixed resonance at 50 kHz, and (4) the receiver with fixed resonance at 300 kHz.

For a comparison, Fig. 12 shows currents of L_R, L_{R50}, and L_{R300}, namely I_R, I_{R50}, and I_{R300}, at different frequencies. The frequency detection and feedback control processes are omitted, and T_{ON} is directly acquired from (8) to put three-frequency stages into one figure. It proves that, even only employing coarse tuning, the current of the hacking receiver current is only slightly smaller than the full-resonant receiver current and much larger than the un-resonant receiver current. Moreover, the ratio of the loads' power, namely P_R: P_{R50}: P_{R300}, is 0.97: 1: 0.001, 1: 0.28: 0.01, and 0.88: 0.03: 1, at 50 kHz, 120 kHz, and 300 kHz, respectively.

Therefore, the hacking receiver can steal substantial amounts of energy from the transmitter for a wide frequency range with the calculated T_{ON} from (8).

TABLE II
EXPERIMENT PARAMETERS

Item	Value/Type	Unit

WPT frequency range (f_T)	79~161	kHz
Transmitter coil inductances (L_T)	150	μH
Receiver coil inductances (L_R, L_{R79}, L_{R161})	80, 80, 80	μH
Auxiliary coil inductances (L_A)	10	μH
Mutual inductances among transmitter and receivers and auxiliary coil (M_R, M_A, M_{RA})	15, 3, 2	μH
Compensation capacitances (C_{R1}, C_{R2})	10, 44	nF
Load resistances (R_L, R_{79}, R_{161})	25, 25, 25	Ω
Transmission distance	40	mm
Diameter of the transmitter coil	19	cm
Diameter of the receiver coil	9	cm

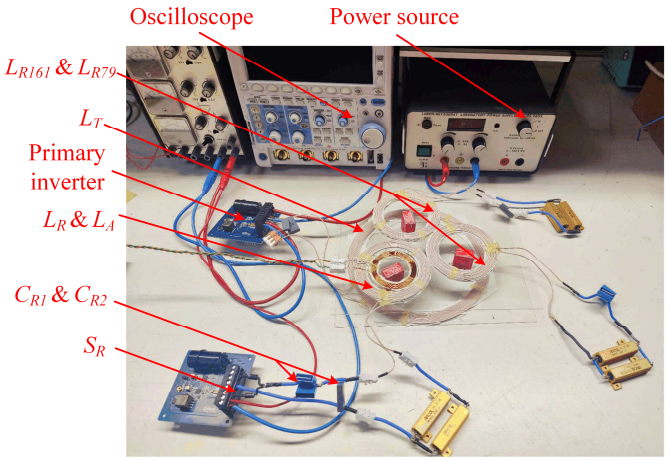


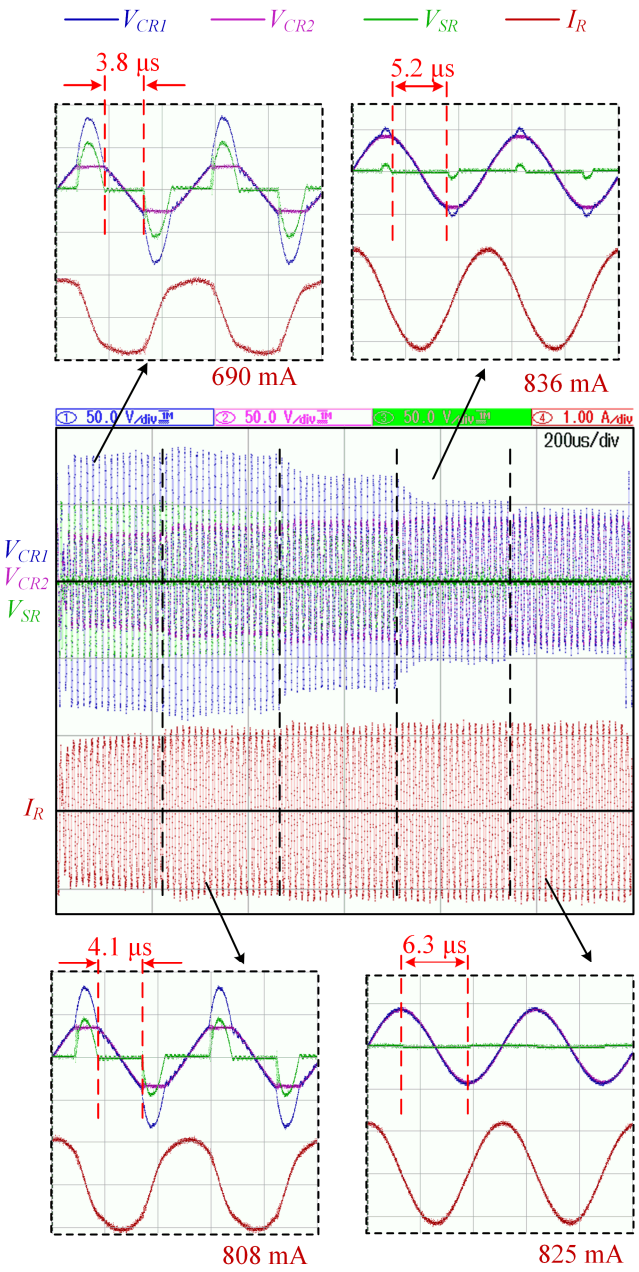
Fig. 13. Experimental setup.

VI. Experiment

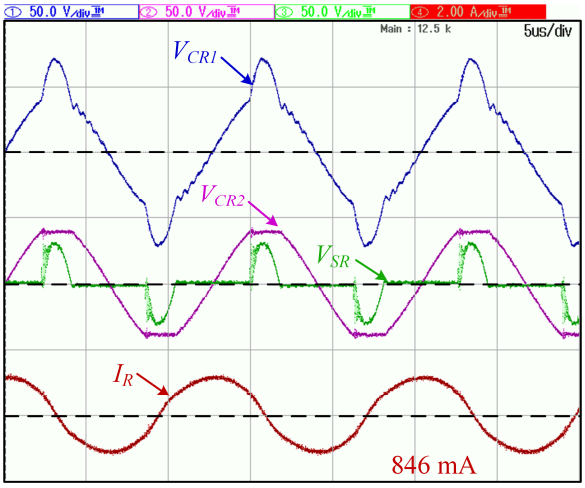
We performed experiments to verify the effectiveness of the proposed energy decryption strategy, as shown in Fig. 13. The experimental setup contains one transmitter, three receivers, and one auxiliary coil, and key parameters are given in Table II. The hacking receiver L_R can harvest energy from 79 kHz to 161 kHz, while the other two receivers L_{R79} and L_{R161} are resonant at 79 kHz and 161 kHz, respectively.

When the transmitter provides 3.4 A current at 79 kHz, the auxiliary coil detects and transfers the frequency and zero-phase points to the controller. Then, the hacking controller calculates T_{ON} as 4.3 μs according to (5) and (8), and controls the shutdown time of the switch S_R to de-active C_{R2}, as shown in Fig. 14.

To avoid the potential error, the hacking receiver needs to tune T_{ON} around the calculated result and detect the corresponding I_R. When increasing T_{ON} from 3.8 to 6.3 μs, the rated value of I_R increases from 690 to 846 mA, and then decreases to 830 mA, as shown in Fig. 14 (a). Thus, 4.7 μs is finally adopted as the best T_{ON} for the current magnetic field, and the corresponding voltages of compensation capacitors and switch are shown in Fig. 14 (b).



(a)



(b)

Fig. 14. Voltages and current of the hacking receiver under 79 kHz. (a) Tuning T_{ON}. (b) With the desired T_{ON}.

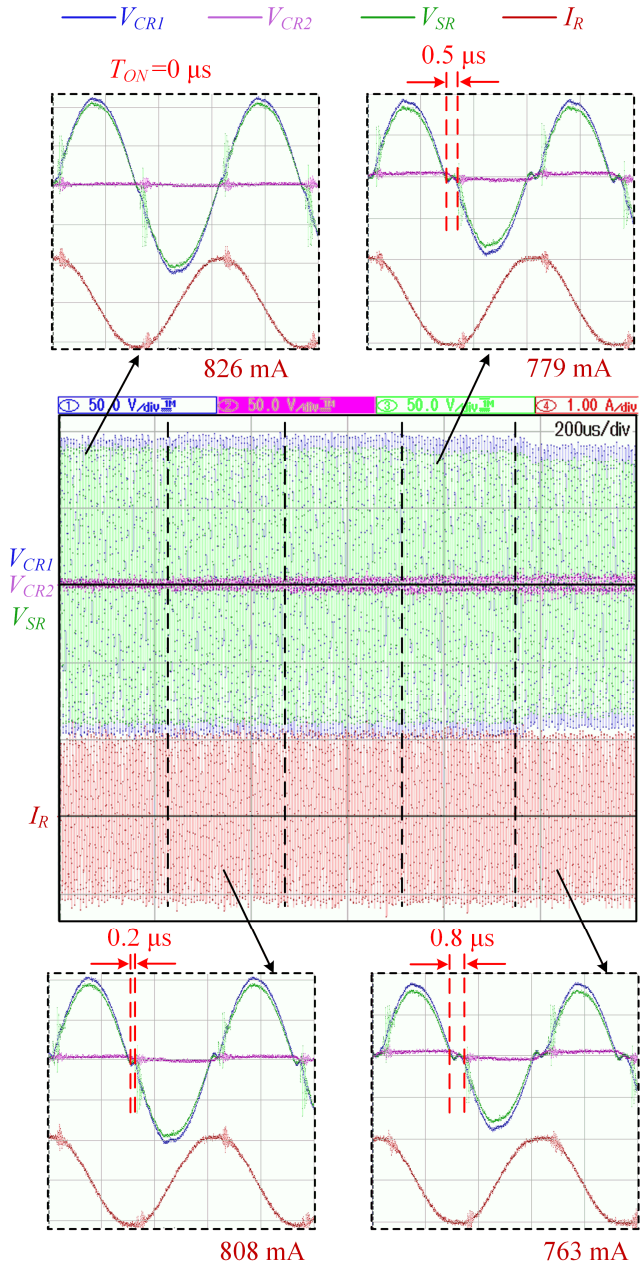


Fig. 15. Voltages and current of the hacking receiver under 161 kHz.

However, when the transmitter provides 1.7 A I_T at 161 kHz, C_{R2} only participates in the compensation for a short time to achieve a low C_{RE}, as shown in Fig. 15. Since the calculated result is 0.22 μs according to (8), the controller detects I_R when regulating T_{ON} from 0 to 0.8 μs. The results show 0 μs is the optimized result for T_{ON} under 160 kHz. It should be mentioned that all MOSFETs and diodes suffer from leakage current. Thus, even when S_R is off all the time, C_{R2} still participates in the compensation; the real compensation C_{RE} would therefore be slightly higher than C_{R1}.

For comparison, the load voltage V_{RL} and load power P_{RL} are compared with peers of low and high-frequency receivers, namely, V_{R79}, V_{R161}, P_{R79}, and P_{R161}, respectively. As shown in Fig. 16, when the transmitter frequency is 79 kHz, the rated values of V_{RL}, V_{R79}, and V_{R161} are 21.7 V, 23.7 V, and 4.1 V, respectively. Thus, the ratio of receiving power among the hacking receiver, low-frequency receiver, and high-frequency receiver should be 0.84: 1: 0.03. However, when the transmitter changes the frequency f to 161 kHz. The rated values of V_{RL}, V_{R79}, and V_{R161} become 19.7 V, 7.6 V, and 22.3 V, respectively, and the power ratio P_{RL}: P_{R79}: P_{R161} becomes 0.78: 0.12: 1.

Moreover, Fig. 17 illustrates the proportion of energy received by each receiver to the total received energy from 79 kHz to 161 kHz. It proves that the proposed energy decryption method can steal substantially more energy than non-resonant receivers.

The identification of the new frequency requires several milliseconds, and then the unauthorized interceptor finishes the whole tuning process within 100 ms, which is only slightly slower than a fixed compensation to build up the oscillation after a frequency change.

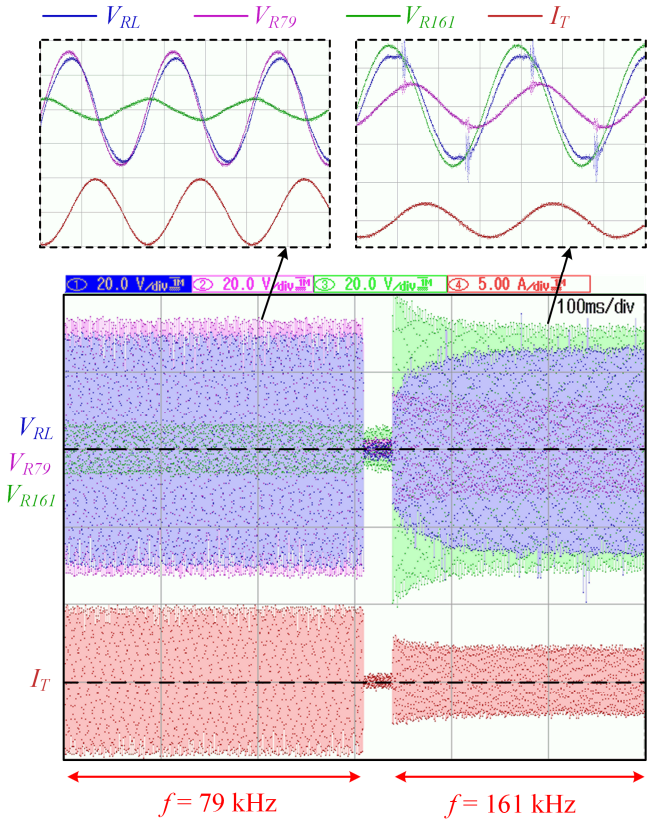


Fig. 16. Load voltages under different frequencies.

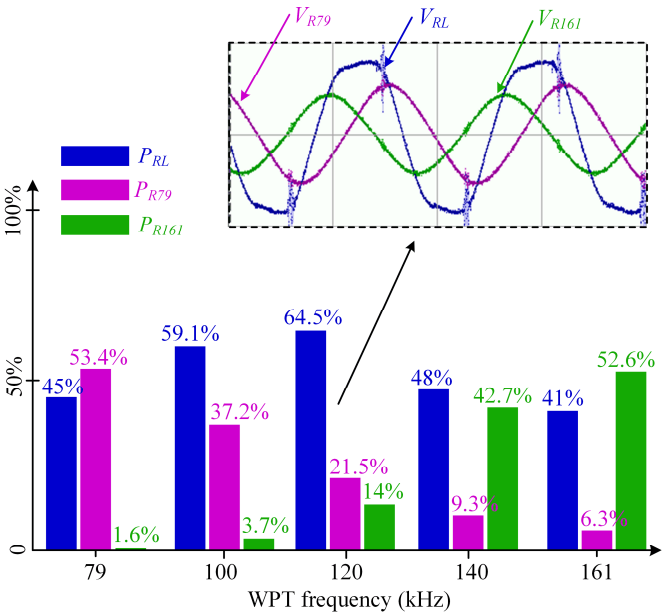


Fig. 17. Percent of energy received by each receiver under different frequencies.

VII. Conclusion

This paper proposes an energy decryption method for frequency-varying encrypted WPT systems. Prominently, only two capacitors and one high-frequency switch are required. The key to adaptive resonance and impedance is controlling the duty cycle of C_{R2} in one cycle in the compensation to achieve a desired equivalent capacitance for different and variable WPT frequencies. Both simulation and experiments prove that the proposed method works well from 79 kHz to 161 kHz, and the hacking receiver can successfully harvest about 78–84% energy of the full-resonant receiver under the same condition. It should be mentioned that even eventually hacking very little energy is already a serious problem. The presented hacking system, however, can even continuously and massively steal energy. Significantly, this energy decryption method can provide a general way to design an energy harvester and energy capturer from electromagnetic fields of WPT systems.

Future research may study high-order LC and LCC compensation to protect the transceiver from sudden over-load through load-independent load current [30, 31]. Dynamically changing LCC compensation would require control methods for two switched-capacitor arrays. Furthermore, strong harmonics and interference may affect the hacking transceiver if they are on a similar amplitude order of magnitude as the main signal, which future attacks may consider to increase the stability of energy theft in such cases.

References

[1] M. Vandeputte, L. Dupre, and G. Crevecoeur, "Quasi-static torque profile expressions for magnetic resonance-based remote actuation," *IEEE Trans. Energy Convers.*, vol. 34, no. 3, pp. 1255-1263, Sep. 2019.

[2] A. Babaki, S. Vaez-Zadeh, A. Zakerian, and G. A. Covic, "Variable-frequency retuned WPT system for power transfer and efficiency improvement in dynamic EV charging with fixed voltage characteristic," *IEEE Trans. Energy Convers.*, vol. 36, no. 3, pp. 2141-2151, Sept. 2021.

[3] N. X. Wang, H.-W. Wang, J. Mei, et. al., "Robust 3-D wireless power transfer system based on rotating fields for multi-user charging," *IEEE Trans. Energy Convers.*, vol. 36, no. 2, pp. 693-702, Jun. 2021.

[4] J. Perzow, "Ranking Qi wireless power transmitters by efficiency," *IEEE Power Electron. Mag.*, vol. 9, no. 3, pp. 56-64, Sept. 2022.

[5] H. Wang, K. T. Chau, W. Liu, and S. M. Goetz, "Design and control of wireless permanent-magnet brushless DC motors," *IEEE Trans. Energy Convers.*, to be published.

[6] X. Zhang, Y. M. Zhang, Z. M. Zhang, and M. Y. Li, "Mode conversion and structure optimization of quadrature coils for electric vehicles wireless power transfer," *IEEE Trans. Energy Convers.*, vol. 35, no. 2, pp. 575-590, Jun. 2020.

[7] J. C. Chen, P. Kan, Z. Yu, et. al., "A wireless millimetric magnetoelectric implant for the endovascular stimulation of peripheral nerves," *Nat. Biomed. Eng*, vol. 6, no. 6, pp. 706-716, Mar. 2022.

[8] C. Sebesta, D. Torres Hinojosa, B. Wang, et. al., "Subsecond multichannel magnetic control of select neural circuits in freely moving flies," *Nat. Mater.*, vol. 21, no. 8, pp. 951-958, Aug. 2022.

[9] M. M. Islam, M. Shahjalal, M. K. Hasan, and Y. Min, "Wireless power transfer with receiver authentication using ECC," *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), pp. 515-518, 2019.

[10] X. Tian, K. T. Chau, W. Liu, H. Pang, and C. H. T. Lee, "Maximum power tracking for magnetic field editing-based omnidirectional wireless power transfer," *IEEE Trans. Power Electron.*, vol. 37, no. 10, pp. 12901-12912, Oct. 2022.

[11] C. Y. Xia, R. H. Jia, Y. T. Shi, A. P. Hu, and Y. Zhou, "Simultaneous wireless power and information transfer based on phase-shift modulation in ICPT system," *IEEE Trans. Energy Convers.*, vol. 36, no. 2, pp. 629-639, Jun. 2021.

[12] Y. J. Jang, S. Jeong, and M. S. Lee, "Initial energy logistics cost analysis for stationary, quasi-dynamic, and dynamic wireless charging public transportation systems," *Energies*, vol. 9, no. 7, Jun. 2016.

[13] A. D. Brovont, D. Aliprantis, S. D. Pekarek, C. J. Vickers, and V. Mehar, "Magnetic design for three-phase dynamic wireless power transfer with constant output power," *IEEE Trans. Energy Convers.*, vol. 38, no. 2, pp. 1481-1484, Jun. 2023.

[14] W. Liu, K. T. Chau, C. H. T. Lee, C. Jiang, and W. Han, "A switched-capacitorless energy-encrypted transmitter for roadway-charging electric vehicles," *IEEE Trans. Magn.*, vol. 54, no. 11, pp. 1-6, Nov. 2018.

[15] W. Liu, K. T. Chau, X. Tian, H. Wang, and Z. Hua, "Smart wireless power transfer – opportunities and challenges," *Renew. Sust. Energ. Rev.*, vol. 180, Jul. 2023.

[16] Z. Zhang, K. T. Chau, C. Qiu, and C. Liu, "Energy encryption for wireless power transfer," *IEEE Trans. Power Electron.*, vol. 30, no. 9, pp. 5237-5246, Sept. 2015.

[17] Z. Zhang, K. T. Chau, C. Liu, and C. Qiu, "Energy-security-based contactless battery charging system for roadway-powered electric vehicles," *2015 IEEE PELS Workshop on Emerging Technologies: Wireless Power (2015 WoW)*, Daejeon, Korea (South), pp. 1-6, 2015.

[18] Z. Zhang and H. Pang, "Continuously adjustable capacitor for multiple-pickup wireless power transfer under single-power-induced energy field," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6418-6427, Aug. 2020.

[19] W. Liu, K. T. Chau, W. H. Lam, and Z. Zhang, "Continuously variable-frequency energy-encrypted wireless power transfer," *Energies*, vol. 12, no. 7, pp. 1-18, 2019.

[20] L. Ji, L. Wang, and C. Liao, "A new method of encryption wireless energy transmission for EV in the smart grid," *CES Trans. Electr. Mach. Syst.*, vol. 1, no. 4, pp. 405-410, Dec. 2017.

[21] Z. Zhang, W. Ai, Z. Liang, and J. Wang, "Topology-reconfigurable capacitor matrix for encrypted dynamic wireless charging of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9284-9293, Oct. 2018.

[22] C. Qi, H. Micio, and X. Chen, "A 90~150 kHz dual-side tuning encrypted wireless power transfer system based on steplessly variable switch-controlled capacitor," *2022 IEEE 5th International Electrical and Energy Conference (CIEEC)*, Nangjing, China, pp. 2984-2989, 2022.

[23] A. Abdolkhani, A. P. Hu, and N. K. C. Nair, "A double stator through-hole type contactless slipring for rotary wireless power transfer applications," *IEEE Trans. Energy Convers.*, vol. 29, no. 2, pp. 426-434, Jun 2014.

[24] R. Mai, Y. Liu, Y. Li, P. Yue, G. Cao, and Z. He, "An active-rectifier-based maximum efficiency tracking method using an additional measurement coil for wireless power transfer," *IEEE Trans. Power Electron.*, vol. 33, no. 1, pp. 716-728, Jan. 2018.
[25] R. W. Porto, V. J. Brusamarello, L. A. Pereira, and F. R. d. Sousa, "Fine tuning of an inductive link through a voltage-controlled capacitance," *IEEE Trans. Power Electron.*, vol. 32, no. 5, pp. 4115-4124, May 2017.
[26] M. Liu, K. W. Chan, J. F. Hu, Q. F. Lin, J. W. Liu, and W. Z. Xu, "Design and realization of a coreless and magnetless electric motor using magnetic resonant coupling technology," *IEEE Trans. Energy Convers.*, vol. 34, no. 3, pp. 1200-1212, Sept. 2019.
[27] M. Vandeputte, D. Bozalakov, L. Dupré, and G. Crevecoeur, "Improving torque in a magnetic resonance based motoring system by detuning from resonance," *IEEE Trans. Energy Convers.*, vol. 36, no. 2, pp. 1188-1196, Jun. 2021.
[28] D.-H. Kim and D. Ahn, "Self-tuning LCC inverter using PWM-controlled switched capacitor for inductive wireless power transfer," *IEEE Trans. Ind. Electron.*, vol. 66, no. 5, pp. 3983-3992, May 2019.
[29] Society of Automotive Engineers. Wireless Power Transfer for Light-Duty Plug-in/Electric Vehicles and Alignment Methodology. SAE J2954 2022. [Online] Available: https://www.sae.org/standards/content/j2954_202208/.
[30] H. Wang, K. T. Chau, W. Liu, Y. Tang, C. Jiang, and S. M. Goetz, "Stepless frequency regulation for load-independent wireless power transfer with time-division switched capacitors," *IECON 2023- 49th Annual Conference of the IEEE Industrial Electronics Society*, Singapore, pp. 01-06, 2023.
[31] Y. Wu, L. Zhou, S. Liu, R. Mai, J. Tian, and S. Goetz, "A highly-efficient and cost-effective reconfigurable IPT topology for constant-current and constant-voltage battery charging," *2021 IEEE Applied Power Electronics Conference and Exposition (APEC)*, Phoenix, AZ, USA, pp. 451-455, 2021.

Hui Wang (Member, IEEE) received the B.Eng. degree in electrical and electronic engineering from Shandong University of Science and Technology, Qingdao, China, in 2014, and the M.Eng. degree in electrical and electronic engineering from Tianjin University, Tianjin, China, in 2017. In 2022, he received the Ph.D. degree in electrical and electronic engineering in the University of Hong Kong, Pokfulam, Hong Kong, China.

He is currently a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, Duke University, USA, and also with the Electrical and Computer Engineering, Rhineland-Palatinate Technical University, Kaiserslautern, Germany. Before that, he worked as a Postdoctoral Fellow with the Department of Electrical and Electronic Engineering, HKU. His research interests include electric machines and wireless power transfer technologies.

Nima Tashakor (Member, IEEE) earned his B.Sc. degree in Electrical Power Engineering from Isfahan University in Isfahan, Iran, in 2013, followed by his M.Sc. degree in the same field from Shiraz University in Shiraz, Iran, in 2015. In 2022, he completed his Ph.D. with distinction at the Technical University of Kaiserslautern, Germany.

Tashakor's primary research interests lie in power electronics and energy storage systems, focusing on the development, control, and monitoring of modular energy storage and conversion systems. Additionally, he explores the applications of machine learning within the field of power electronics.

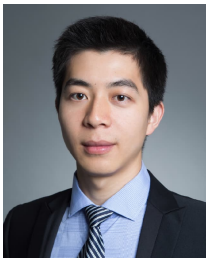
Wei Jiang received the Bachelor and Master degrees from Anhui University of Science and Technology, Huainan, China, in 2004 and 2007 respectively. He is currently an Associate Professor with the Department of Intelligent Engineering, Bozhou Vocational and Technical College. He is also working as a Visiting Researcher with the Electrical and Computer Engineering, Rhineland-Palatinate Technical University, Kaiserslautern, Germany.

His research interests include modular multilevel converters, photovoltaic and energy storage systems, and AC/DC hybrid microgrids.

Wei Liu (Member, IEEE) received the B.Eng. and M.Eng. degrees in electrical engineering from China University of Petroleum, Qingdao, China, and a Ph.D. degree in electrical and electronic engineering from The University of Hong Kong (HKU), Hong Kong, China, in 2014, 2017, and 2021, respectively.

He is currently an Assistant Professor at the Research Centre for Electric Vehicles and Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University (PolyU). He is also an Honorary Assistant Professor at the Department of Electrical and Electronic Engineering, HKU, since 2023. Dr. Liu served as a Postdoctoral Fellow and then was promoted to a Research Assistant Professor from 2021 to 2023, and he is now an Honorary Assistant Professor at the Department of Electrical and Electronic Engineering, HKU. He also worked as a Visiting Researcher with Nanyang Technological University, Singapore (NTU), in 2019. His research interests include wireless power transfer, power electronics, biomedical power electronics, and electric vehicle technologies.

Dr. Liu was the recipient of the Power Engineering Prize from HKU, the Excellent Paper Award, and the Best Presentation Award from international conferences in the area of Electric Vehicles and Transportation Electrification. He is also a Guest Associate Editor of *IEEE Journal of Emerging and Selected Topics in Power Electronics (JESTPE)*, Guest Editor of international journals, and Session Chair of international conferences.



C. Q. Jiang (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees (First Class Honours) in Electrical Engineering and Automation from Wuhan University, Wuhan, China, in 2012 and 2015, respectively, and the Ph.D. degree in Electrical and Electronic Engineering from The University of Hong Kong, Hong Kong SAR, China, in 2019.

He is currently an Assistant Professor with the Department of Electrical Engineering, faculty member in the State Key Laboratory of Terahertz and Millimeter Waves, City University of Hong Kong, Hong Kong SAR, China. From 2019 to 2021, he was a Postdoctoral Research Associate at the University of Cambridge, U.K. Also, he is affiliated with Clare Hall, University of Cambridge since 2021. In 2019, he was a Visiting Researcher at the Nanyang Technological University, Singapore. His research interests include power electronics, wireless power transfer, electric machines and drives, and electric vehicle (EV) technologies.

Dr. Jiang was the recipient of Winner, CAPE Acorn Blue Sky Research Award at the University of Cambridge, Gold Medal in 3rd Asia Exhibition of Innovations and Inventions, Silver Award and Bronze Award in Shenzhen Qianhai Youth Innovation & Entrepreneurship Competition, and First Prize in the Interdisciplinary Research Competition at the University of Hong Kong. He is currently an Associate Editor of *IET Renewable Power Generation*, Guest Editor of Energies, *Electronics*, *Wireless Power Transfer*, *IEEE Open Journal of Vehicular Technology*.

Stefan M. Goetz (Member, IEEE) received the undergraduate and graduate degrees from TU Muenchen, Munich, Germany, and his Ph.D. training at TU Muenchen and Columbia University, New York, NY, USA. He has worked for various companies, after his Ph.D. mostly in the automotive industry.

His research interests include drives, modular power electronics concepts, battery electronics, precise high-power inverters and pulse synthesizers, medical power electronics and instrumentation, as well as integrative power electronics solutions for microgrids and electric vehicle applications.