Article

Continuously Variable-Frequency Energy-Encrypted Wireless Power Transfer

Wei Liu 1, K. T. Chau 1,*, W. H. Lam 1 and Zhen Zhang 1,2

1 Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, China; liuwei@eee.hku.hk (W.L.); whlam@eee.hku.hk (W.H.L.); zhangz@tju.edu.cn (Z.Z.)
2 School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China
* Correspondence: ktcchau@eee.hku.hk; Tel.: +852-2859-2704

Received: 3 March 2019; Accepted: 1 April 2019; Published: 3 April 2019

Abstract: This paper proposes and implements a novel continuously variable-frequency energy-encrypted wireless power transfer (WPT) system for wireless energy security in multi-receiver applications. To prevent wireless energy from being illegally stolen, the proposed chaotic 2-D frequency-and-duration encryption (FDE) technology directly generates well-defended security keys to guarantee energy security. An LCC-compensated transmitter without using a switched-capacitor array is proposed to competently encrypt the wireless energy into burglarproof energy packages, which are decrypted only by authorized receivers. Then, the concept of the static variable capacitor (SVC) is presented to achieve dynamical impedance compensation for wireless energy decryption in authorized receivers with knowledge of security keys. Consequently, the proposed energy-encrypted SVC-based WPT system can flexibly encrypt and decrypt wireless energy packages in a continuous frequency-and-duration adjustment rather than in a discrete way, thus greatly improving energy security performance. Theoretical analysis, computer simulation and experimental results are provided to verify the feasibility of the proposed continuously energy-encrypted SVC-based WPT system.

Keywords: continuous frequency-and-duration adjustment; energy encryption; wireless power transfer; static variable capacitor; LCC-compensated network

1. Introduction

Wireless power transfer (WPT), first proposed by Nikola Tesla, can be traced back to more than one hundred years ago [1]. Recently, the WPT possesses the key advantages of cordless, spark-proof, better convenience and higher flexibility, and thus has re-attracted unprecedented attention of consumers, manufacturers and academic researchers [2–4]. This wireless energy-accessing pattern is gradually improving our conventional plug-in charging pattern and meanwhile alleviating the limitations of current battery techniques. As one of most epoch-making technologies, the WPT shows great talents and potentials in various industrial applications and interdisciplinary areas, such as domestic appliances or medical electronics [5–7], electric vehicle (EV) wireless charging [8–10], wireless motor drive [11,12] and emerging wireless energy security [13,14].

The working principle of magnetic resonant coupling (MRC) was first proposed and experimentally demonstrated as a significant promotion on WPT techniques in 2007 [15]. Due to its high efficiency and high-power capability, the MRC-based WPT has been rapidly identified as one of the most promising implementation ways for near-field power transmission. Although the WPT successfully removes the messy charging wires, it inevitably takes the risks of energy stealing or leakage because of such convenient wireless energy-accessing pattern. Although a selective WPT technology can achieve oriented power transmission to specified receivers among multi-receivers [11,16], the illegal...
receivers may track and lock the fixed operating frequency to steal the wireless power. Accordingly, to guarantee wireless energy security, the concept of energy encryption was proposed to encrypt the wireless energy as the information encryption does, which ensures that only authorized receivers can successfully decrypt and harvest the encrypted wireless energy \[9,13\]. However, these encryption schemes desire switched-capacitor arrays to discretely adjust the operating frequency and matched capacitance, thus suffering from discrete adjustment, finite selections and low flexibility.

Therefore, a practical variable capacitor awaits to be developed for continuously variable-frequency energy-encrypted WPT systems. A transistor-controlled variable capacitor was proposed for stabilizing soft-switching operation \[17,18\], but its tested power level is relatively low. The mechanisms of virtual capacitors \[19\], electric springs \[20\] and single-phase var generators \[21\] can be used to develop a static variable capacitor (SVC) for continuous impedance compensation, and thus wireless energy encryption and decryption. Incorporated with the merits of LCC-compensated transmitter \[22–24\] and the variable-frequency characteristics of a series-to-series (SS) WPT system using fixed compensation \[9,16\], a novel LCC-compensated switched-capacitorless energy-encrypted transmitter is proposed, which tactfully avoids the usage of an extra SVC in the transmitter.

The rest of this paper is organized as follows. Section 2 will discuss the topology and operation principle of the proposed continuously variable-frequency energy-encrypted WPT system. Section 3 will present the directly 2-D frequency-and-duration encryption (FDE) and the SVC decryption. Section 4 will be devoted to the computational simulation of electromagnetic fields and system circuit. In Section 5, an experimental prototype will be constructed and tested to verify the proposed continuously energy-encrypted SVC-based WPT system. A conclusion will be drawn in Section 6.

2. Topology and Operating Principle

2.1. System Topology

By eliminating the messy charging wires, WPT can possess various merits of cleanness, convenience and flexible mobility over conventional plug-in charging pattern, but wireless energy security is gradually recognized as a key concern by consumers and manufacturers. Energy-encrypted WPT systems can prevent transgressors from illegally stealing wireless energy and thus improve energy security performance in the multiple-objective WPT-based applications, such as static park-charging EVs, dynamic roadway-charging EVs and wireless charging consumer or medical electronics.

Figure 1 depicts the proposed continuously variable-frequency energy-encrypted WPT system using the SVC in receivers. The whole system mainly comprises of one LCC-compensated switched-capacitorless transmitter and multiple receivers, including the authorized and unauthorized ones. It is worth noting that the LCC-compensated transmitter without using a switched-capacitor array can offer a definite merit of flexibly encrypting the wireless energy by continuously adjusting the operating frequency and its active duration. The concept of the SVC is newly introduced to achieve dynamic impedance compensation in the authorized receiver circuits. With knowledge of security keys, only the authorized receivers can accordingly decrypt the wireless energy packages encrypted by the LCC-compensated switched-capacitorless transmitter. Moreover, a chaotic 2-D FDE technology is directly used to generate a sequence of more defensive security keys for the superior wireless energy encryption.
2.2. Operating Principle

As depicted in Figure 1, $R_t$, $L_t$, $C_t$, $i_t$, $R_{tk}$, $L_{tk}$, $C_{tk}$ and $i_{tk}$ ($k \in Z^+$, and $k = 1, \ldots, m, \ldots, n$) with subscripts $t$ and $r$ denote the coil internal resistances, resonant coil inductances, matched capacitances and currents in the transmitter and receiver circuits in the $k$th energy-encrypted WPT channel, respectively. For example, if $k = m$, $R_{rm}$ and $i_{rm}$ are the coil internal resistances and resonant currents in the receiver circuits in the $m$th energy-encrypted WPT channel as shown in Figure 1. Besides, $L_{tk}$ and $L_{tk,k_2}$ ($k_1, k_2 \in [1, n]$) denote the mutual inductance between the transmitter coil and the $k$th receiver coil and that between the $k_1$th and $k_2$th receiver coils, respectively. The inductor $L_C$, capacitor $C_C$ and capacitor $C_t$ form the LCC-compensated network in the transmitter side. In the circuit of the proposed SVC, $L_{sk}$ is the smoothing inductor, and $C_{DC}$ and $C_{sk}$ represent the capacitors in the DC and AC sides, respectively. Similarly, if $k = m$, $C_{sm}$ is the AC-side capacitor in the $m$th receiver circuits in Figure 1.

To commence with theoretical analysis, some assumptions are made: (i) $L_{tk} = L_t$, $L_{tk,k_2} = L_{tk}$, $R_{tk} = R_{tk}$, and $R_{Lk} = R_L$. (ii) $R_{Lk,eq}$ is the equivalent resistance of load resistance $R_{Lk}$ and $R_{Lk,eq} = 8R_{Lk}/\pi^2$. (iii) $L_{tk,k_2} = \frac{L_{tk}L_{tk,k_2}}{L_{tk} + L_{tk,k_2}}$ can be regarded as zero. In each energy-encrypted WPT channel, the initial operating frequency $f_k$ is given by

$$f_k = \frac{1}{2\pi\sqrt{L_{tk}C_{tk}}}, \quad k = 1, 2, \ldots, n, \quad n \in Z^+$$

where $n$ is the total number of energy-encrypted channels. When the $m$th group of receivers is authorized to decrypt and harvest the wireless energy-encrypted packages, the authorized $m$th receivers will operate at the $m$th operating frequency $f_m$. According to the security keys of the FDE sequences, delivered from the energy-encrypted transmitter, both operating frequency $f_m$ and its duration may chaotically change, and the SVC in the authorized receivers will be rapidly activated for impedance compensation. Meanwhile, the switched-capacitorless energy-encrypted transmitter will operate at the same chaotic FDE sequences to dynamically encrypt the wireless energy. Consequently, both the transmitter and the $m$th group of authorized receivers operates at the chaotic operating frequency $f_m$. In such a way, the general equation can be derived as:
where the total impedance $Z_{\text{ref}}$ reflected from all receiver circuits to the transmitter circuit can be derived as:

$$Z_{\text{ref}} = \sum_{k=1}^{n} \lambda_k Z_{\text{ref} k} = \sum_{k=1, k \neq m}^{n} \lambda_k Z_{\text{ref} k} + \lambda_m \frac{(\omega_m L_{\text{ref}})^2}{R_m + R_{\text{eq}m}} = \lambda_m \frac{(\omega_m L_{\text{eq}})^2}{R_m + R_{\text{eq}m}} + j \cdot \text{Im} \left( \sum_{k=1, k \neq m}^{n} \lambda_k Z_{\text{ref} k} \right)$$

The total impedance $Z_{\text{ref}}$ reflected from all receiver circuits to the transmitter circuit can be derived as:

$$Z_{\text{ref}} = \sum_{k=1}^{n} \lambda_k Z_{\text{ref} k} = \sum_{k=1, k \neq m}^{n} \lambda_k Z_{\text{ref} k} + \lambda_m \frac{(\omega_m L_{\text{ref}})^2}{R_m + R_{\text{eq}m}} = \lambda_m \frac{(\omega_m L_{\text{eq}})^2}{R_m + R_{\text{eq}m}} + j \cdot \text{Im} \left( \sum_{k=1, k \neq m}^{n} \lambda_k Z_{\text{ref} k} \right)$$

where $Z_{\text{ref} k} = \frac{(\omega_m L_{\text{ref} k})^2}{Z_m}$, which is the $k$th impedance $Z_{\text{ref} k}$ reflected from the $k$th receiver circuits. Besides, $\lambda_k$ obeys a random distribution, which represents the number of receivers in the $k$th energy-encrypted WPT channel. Accordingly, in order to guarantee superior energy security performance, the reflected impedances from the authorized and unauthorized receivers, respectively, should satisfy the following inequality:

$$\text{Re}(\cdot) \geq \text{Im}(\cdot) \geq \text{Re}(\cdot)$$

where $\text{Re}(\cdot)$ and $\text{Im}(\cdot)$ are the real and imaginary parts of complex impedance, respectively.

In the transmitter circuit, the total impedance $Z_{t, \text{total}}$ and the input impedance $Z_{\text{in}}$ in the inverter output side can be respectively calculated as:

$$Z_{t, \text{total}} = Z_{\text{ref}} + Z_t, \quad Z_{\text{in}} = R_C + j \omega_m L_C + \frac{Z_{t, \text{total}} Z_C}{Z_{t, \text{total}} + Z_C}$$

where $R_C$ is the internal resistance of $L_C$.

Accordingly, the input current $i_{\text{in}}$ and the transmitter current $i_t$ can be respectively expressed as:

$$i_{\text{in}} = \frac{U_{\text{in}}}{Z_{\text{in}}}, \quad i_t = \frac{Z_C}{Z_C + Z_{t, \text{total}}} i_{\text{in}}$$

Also, the input impedance angle $\varphi$ and the input power $P_{\text{in}}$ can be respectively written as:

$$\varphi = \arctan \left( \frac{\text{Im}(Z_{\text{in}})}{\text{Re}(Z_{\text{in}})} \right), \quad P_{\text{in}} = U_{\text{in}} |i_{\text{in}}| \cos \varphi$$
The current $i_{rk}$ through the $k$th receiver circuit, the total output power $P_{\text{out}}$ and its corresponding transmission efficiency $\eta_k$ in the $k$th energy-encrypted WPT channel can be respectively expressed as:

$$i_{rk} = \frac{j\omega_m L_{rk} h_i}{Z_{rk}}, \quad P_{\text{out}} = \lambda_k |i_{rk}|^2 R_{\text{rk,eq}}, \quad \eta_k = \frac{P_{\text{out}}}{P_m}$$  

(9)

Thus, the $k$th transmission efficiency $\eta_k$ can be derived as:

$$\eta_k = \frac{\lambda_k R_{\text{rk}} (\omega_m L_{rk})^2}{(\omega_m C_C)^2 R_C \left( R_{tr}^2 + \left( \omega_m L_T - \frac{1}{\omega_m C_C} - \frac{1}{\omega_m C_T} + \text{Im} \left( \sum_{k=1, k \neq m}^{n} \lambda_k Z_{\text{ref}k} \right) \right)^2 \right)} + R_{tr}$$

(10)

where $R_{tr} = \text{Re} \left( \sum_{k=1}^{n} \lambda_k Z_{\text{ref}k} \right) + R_{tr}$, and the key derivation is listed as (A1) in the Appendix A.

According to Equation (10), $\eta_k$ is impervious of $L_C$. Particularly, when the $m$th receivers are authorized, the corresponding transmission efficiency $\eta_m$ of the authorized $m$th receivers can be rewritten as:

$$\eta_m = \frac{\lambda_m R_{\text{lm}} (\omega_m L_{lm})^2}{(\omega_m C_C)^2 R_C \left( \text{Re} \left( \sum_{k=1}^{n} \lambda_k (\omega_m L_{rk})^2 \right) + R_l \right) + \left( \omega_m L_T - \frac{1}{\omega_m C_C} - \frac{1}{\omega_m C_T} + \text{Im} \left( \sum_{k=1, k \neq m}^{n} \lambda_k (\omega_m L_{rk})^2 \right) \right)^2 \right)} + R_{tr}$$

(11)

where resistance coefficients ($T_r$ and $T_{\text{ref}k}$) and conductance coefficients ($T_c$, $T_{\text{lc}k}$, $T_{\text{rc}k}$ and $T_{\text{rr}k}$) in the transmitter and receiver circuits can be respectively defined as:

$$\begin{align*}
&T_r = \text{Re} \left( \sum_{k=1}^{n} \lambda_k (\omega_m L_{rk})^2 \right) + R_p \approx \text{Re} \left( \sum_{k=1}^{n} \lambda_k (\omega_m L_{rk})^2 \right) \approx \lambda_m \frac{(\omega_m L_{lm})^2}{R_{\text{lm,eq}} + R_{\text{lm,eq}}} \\
&T_c = \omega_m L_T - \frac{1}{\omega_m C_C} - \frac{1}{\omega_m C_T} + \sum_{k=1, k \neq m}^{n} \lambda_k (\omega_m L_{rk})^2 > 0 \\
&T_{\text{lc}k} = \omega_m L_T - \frac{1}{\omega_m C_C} - \frac{1}{\omega_m C_T} < 0 \\
&T_{\text{rc}k} = \sum_{k=1, k \neq m}^{n} \lambda_k (\omega_m L_{rk})^2 - T_{\text{rk}} \left( T_{\text{rk}}^2 + T_{\text{ck}}^2 \right) \\
&T_{\text{rr}k} = R_{rk} + R_{\text{lk,eq}} \\
&T_{\text{ck}} = \frac{1}{\omega_m C_T} - \omega_m L_{rk}
\end{align*}$$

(12)

Also, its key derivation is listed as (A2) in the Appendix A.

To prevent the unauthorized receivers from stealing wireless energy, the unauthorized receiver currents should be far less than the authorized ones, and it can even be neglected. Thus, the energy-encrypted WPT system should always keep satisfying the following inequality:

$$\frac{j\omega_m L_{\text{lm}} |h_i|}{(R_{\text{lm}} + R_{\text{lm}}) / \lambda_m} \gg \max \left( \frac{j\omega_m L_{\text{rk}} |h_i|}{Z_{rk} / \lambda_k} \right), \ k \neq m$$

(13)

which also indicates that $i_{lm}$ through the $m$th authorized receiver circuit is not less than $\epsilon$ times of the maximum value of $i_{rk}$ ($k \neq m$) through all the unauthorized ones, and thus there is:

$$\begin{align*}
P_{\text{out}} &\geq \epsilon^2 P_{\text{out}} \\
\eta_m &\geq \epsilon^2 \eta_k, \ k \neq m, \ \epsilon \in R^+ \end{align*}$$

(14)
Assuming $L_{trm} = L_{trk} = L_{tr}$, in order to guarantee relatively high transmission efficiency, the impedance in the authorized receiver circuits should be much less than the minimum one in all the unauthorized receiver circuits. Hence, there is a constraint condition:

$$\frac{R_{rm} + R_{Lm}}{\lambda_m} << \min \left( \frac{|Z_{rk}|}{\lambda_k} \right) \Rightarrow \frac{R_{rm} + R_{Lm}}{\lambda_m} << \min \left( \frac{\text{Im}(Z_{rk})}{\lambda_k} \right), \ k \neq m$$

(15)

Accordingly, the transmission efficiencies $\eta_k$ and $\eta_m$ are impervious to the parameter $L_C$ of the LCC compensation network in the transmitter circuit. Although the internal resistance of $L_C$ will lead to extra power loss, the proposed energy encryption scheme takes the advantage of continuous frequency adjustment without using bulky switched-capacitor arrays [13]. Inevitably, the proposed continuously energy-encrypted SVC-based WPT system may suffer from a disadvantage in terms of additional complexity and slightly deteriorated efficiency of the security-enhanced WPT system.

3. Frequency-and-Duration Encryption and Static Variable Capacitor Decryption

3.1. Chaotic 2-D Frequency-and-Duration Encryption

The key of energy encryption mainly relies on the frequency sensitivity in the conventional MRC-based WPT systems. The proposed continuously variable-frequency energy encryption scheme is detailed depicted in Figure 2, where the encryption and decision-making unit generates the defensive chaotic 2-D FDE sequences, namely the security keys. Based on the wireless data interaction between the energy-encrypted transmitter and energy-decrypted receivers, the encryption and decision-making unit will conduct the maximum efficiency band tracking (MEBT) to suppress the wireless energy leakage. Practically, the operating frequencies of the unauthorized receivers always dynamically and randomly change, which will unexpectedly result in an increasing probability of energy stealing or leakage. Thus, the MEBT will dynamically optimize the frequency band of energy encryption for maximizing transmission efficiency. According to the optimized security keys, the LCC-compensated switched-capacitorless transmitter will encrypt the wireless energy into encoded energy packages. This energy encryption is realized by proactively attuning both the switching frequency and its duration to the FDE security keys in a continuous way. After certificating the authorization of specific receivers, the FDE security keys will be secretly delivered to the authorized receivers. With knowledge of the FDE security keys, the authorized receivers will decrypt the encoded energy packages by conducting the proposed SVC-based impedance compaction. Thus, they can effectively harvest wireless energy from the proposed continuously variable-frequency energy-encrypted WPT system. Due to the lack of security keys, the unauthorized receivers can pick up only an insignificant level of encrypted wireless energy.

In Figure 2b, a chaotic 2-D FDE algorithm is directly adopted to dynamically generate the encrypted frequency and its active duration sequences – the security keys. It plays an important role in ensuring wireless energy security. The Hénon map is used to generate a 2-D discrete-time chaotic series [25,26] as given by:

$$\left\{ \begin{array}{l}
\xi_{f,i+1} = \xi_{d,i} + 1 - A_f \xi_{f,i}^2, A_f \in [1.0, 1.5], A_d = 0.3 \\
\xi_{d,i+1} = A_d \xi_{f,i}
\end{array} \right.$$ 

(16)

where $\xi_{f,i}$ and $\xi_{d,i}$ are the chaotic sequences of the energy-encrypted frequency and its duration, respectively, and $A_f$ and $A_d$ are the corresponding bifurcation parameters. To produce the desired random-like but bounded security keys ($\zeta_i$, $\xi_i$) for the proposed continuously energy encryption scheme, $A_f = 1.4$ is selected [26]. Hence, the chaotic security keys $\gamma_i$ and $\beta_i$ can be expressed as:

$$\left\{ \begin{array}{l}
\gamma_i = a_\gamma + b_\gamma \xi_{f,i}, 0 < 1.5 b_\gamma < a_\gamma \\
\beta_i = a_\beta + b_\beta \xi_{d,i}, 0 < 0.4 b_\beta < a_\beta
\end{array} \right.$$ 

(17)
Both the encrypted angular frequency $\omega_m$ and its duration $D_m$ can be respectively expressed as:

\[
\begin{align*}
\omega_m &= \gamma \omega_0 \\
D_{m,q} &= \beta_1 D_0, \quad q \in Z^+
\end{align*}
\]  

(18)

Thus, the encrypted operating angular frequency and its duration can be chaotically varied in the proposed continuously energy-encrypted WPT system. Generally, $\omega_0$ and $D_0$ can be arbitrarily designed based on the power level and transmission distance. Instead of simultaneously regulating switched-capacitor arrays in both the transmitter and the authorized receivers [13], the LCC-compensated switched-capacitorless transmitter can self-adaptively attune the switching frequency to synchronize the FDE security keys. Meanwhile, the authorized receivers just need to activate the SVC for dynamic impedance compensation and energy decryption. Accordingly, the equivalent matched capacitor will be adjusted as:

\[
C_{rb} \left( \sum_{q=1}^{\frac{D_m}{m}} (\beta_1 D_0) \right) = \frac{1}{f_1^2} \frac{1}{\omega_0^2 L_{rb}}
\]  

(19)

Consequently, the encoded energy package can only be decrypted by these authorized receivers with knowledge of security keys.

3.2. Static Variable Capacitor Decryption

The wireless energy decryption can be realized by adjusting the compensated impedance. Since the coupling characteristics are pre-determined by the transmitter and receiver coils, the capacitance is normally chosen as the control objective for the impedance compensation. The capacitor array [27] and the capacitor matrix [28] were reported, but identified as finite capacitance selections. This discrete energy encryption scheme [13] desires to simply increase the alternative capacitors, which will inevitably deteriorate the practicability and applicability of energy-encrypted WPT systems using bulky switched-capacitor arrays. Accordingly, this paper proposes and implements an SVC scheme for impedance compensation by controlling the output current to simulate the voltage-current characteristic of a real capacitor or inductor. Theoretically, the proposed SVC can offer infinite capacitance selections by adjusting the compensated impedance in a continuous way, thus significantly improving the energy security performance for multi-receiver WPT systems.
Generally, receivers usually adopt the series circuit topology in the conventional WPT systems. In the initial resonance state, the receiver current $I_{r(\omega t)}$ leads the transmitter current $I_{t(\omega t)}$ precisely by $\pi/2$ as shown in Figure 3. When the encrypted operating frequency deviates from the inherent resonant frequency, the leading angle $\theta$ obtained by the authorized receiver current may be greater or less than $\pi/2$. Accordingly, the proposed SVC can be activated to implement impedance compensation by controlling the equivalent impedance. Figure 3 shows the phasor diagram of the proposed SVC. When the frequency $f_m$ is increased to encrypt the wireless energy, the receiver circuit enters into the non-resonant state, where the receiver current $I_{r(\omega t)}$ leads the transmitter current $I_{t(\omega t)}$ by $\pi/2 - \alpha_1$, less than $\pi/2$. Since the reactive impedance is greater than the capacitive impedance, the proposed SVC should be activated to decrease the equivalent capacitance by injecting a current phasor as $I_{s(\omega t)}$. Similarly, when the frequency $f_m$ is decreased for encryption, the non-resonant receiver current $I_{r(\omega t)}$ leads the transmitter current $I_{t(\omega t)}$ by $\pi/2 + \alpha_2$, greater than $\pi/2$. Accordingly, the proposed SVC should be activated to increase the equivalent capacitance by injecting a current phasor as $I_{s(\omega t)}$. In such ways, the receiver current $I_{r(\omega t)}$ of $I_{r(\omega t)}$ is pulled back to lead $I_{t(\omega t)}$ by $\pi/2$, which effectively ensures the resonant state, even for a continuously variable-frequency operation. Consequently, the authorized receiver can successfully decrypt the encoded energy packages, thus ensuring the power transmission performance. Besides, the proposed SVC can also control the harvested wireless powers and power distributions by adjusting the impedances of the authorized receiver circuits.

![Figure 3. Phasor diagram of proposed SVC.](image)

As shown in Figure 4, the proposed SVC can offer continuous impedance compensation by adopting an H-bridge inverter. In the proposed SVC, the DC side uses only a capacitor, rather than a power supply. With knowledge of the energy-encrypted frequency, the phase-locked loop is used to track and lock the phases of both the encrypted transmitter current and the receiver current. The phase of the encrypted transmitter current, as well as the FDE security keys, will be secretly delivered to the authorized receiver. According to the phase angle leading the transmitter current by $\pi/2$, the receiver current can be predicted. Finally, the corresponding control signals are generated by a phase correction controller.
4. Computational Simulation

To assess the energy security performance of the proposed continuously energy-encrypted WPT system, finite element analysis (FEA) and system simulation are performed. The key design specifications and parameters are listed in Table 1. Detailed geometries with dimensions of the transmitter and receiver coils are depicted in Figure 5, where the transmitter and receiver coils respectively adopt a two-layer and three-layer configurations to enhance their mutual inductances, hence improving the transmission efficiency. The transmission distance is 130 mm and each receiver coil can be separately authorized to decrypt and pick up the encrypted wireless power.

Table 1. Design specifications and parameters.

<table>
<thead>
<tr>
<th>Items</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital signal processor</td>
<td>TMS320F28335</td>
</tr>
<tr>
<td>Transmitter compensated inductance</td>
<td>150 µH</td>
</tr>
<tr>
<td>Transmitter compensated capacitance</td>
<td>250 nF</td>
</tr>
<tr>
<td>Transmitter capacitance</td>
<td>1.00 nF</td>
</tr>
<tr>
<td>Transmitter coil inductance</td>
<td>5.668 µH</td>
</tr>
<tr>
<td>Transmitter coil turns</td>
<td>20 (2 layers)</td>
</tr>
<tr>
<td>Transmitter coil internal resistance</td>
<td>0.3 Ω</td>
</tr>
<tr>
<td>Receiver capacitances</td>
<td>81.43, 185.23, 850.00 mF</td>
</tr>
<tr>
<td>Receiver coil inductances (L1, L2,</td>
<td>345.66, 355.30, 348.63 μH</td>
</tr>
<tr>
<td>Receiver coil internal resistance</td>
<td>0.2 Ω</td>
</tr>
<tr>
<td>Mutual inductances (L1, L2, L3)</td>
<td>26.72, 33.11, 28.59 μH</td>
</tr>
<tr>
<td>SVC AC inductance</td>
<td>10 μH</td>
</tr>
<tr>
<td>SVC AC capacitance</td>
<td>2 μF</td>
</tr>
<tr>
<td>Output filter capacitance</td>
<td>2000 μF</td>
</tr>
</tbody>
</table>

By using FEA, Figure 6 shows the decreasing trend of coupling coefficient with the increasing vertical transfer distance between the transmitter and central (or lateral) authorized receiver. Also, the magnetic field distributions are shown in Figure 7 in which only the central receiver coil is authorized, or only the right lateral receiver coil is authorized. As shown in Figure 7a,b, the magnetic flux pipe can be effectively built up by using the energy encryption scheme. It can be observed that the vast majority of magnetic flux lines are bundled up through the authorized receiver coil, and only insignificant ones are dispersed through the unauthorized receiver coils. Figure 7a,b also demonstrate that the current densities in the authorized receiver coil are much larger than those in the unauthorized ones. Therefore, only the authorized receiver can successfully decrypt and harvest the encrypted wireless energy, thus inducing large current. Along the vertical plane, the contour plots of the magnetic flux densities are plotted in Figure 7c,d, where the magnetic flux densities around the authorized
receivers are far higher than those around the unauthorized ones. Along the middle parallel plane, the 3-D magnetic flux densities are plotted in Figure 7e,f, where the saddle-shape magnetic flux densities under the authorized receiver coil can reach up to 3.044 mT and 2.619 mT, respectively. By applying the proposed continuously energy encryption scheme, Figure 8a shows that both the authorized receiver current and output voltage (23.82 V) are much larger than the unauthorized receiver currents and output voltages (2.01 V and 3.26 V). Figure 8b shows that both the operating frequency and its active duration are simultaneously encrypted in a 2-D scale to improve the energy security performance. With knowledge of security keys, the authorized receiver can always successfully decrypt and pick up the encrypted wireless power, thus generating an average output voltage of 22.75 V, while the unauthorized receivers fail to decrypt and harvest from the proposed energy-encrypted WPT system, hence only generating insignificant values of 2.27 V and 3.28 V. Correspondingly, the wireless power harvested by the authorized receiver is 104.57 W, far greater than those (0.83 W and 2.16 W) harvested by the unauthorized ones. During the first 0.08 s, an energy of 8.37 J is transferred to the authorized receiver, whereas only 0.239 J is transferred to the unauthorized ones, corresponding to 2.78% of the total energy transfer.

Figure 5. Geometries of transmitter and receiver coils. (a) Transmitter coil; (b) receiver coil; and (c) displacement between transmitter and receiver coils.

Figure 6. Coupling coefficients versus vertical transfer distance between transmitter and receivers.
Figure 5. Geometries of transmitter and receiver coils. (a) Transmitter coil; (b) receiver coil; and (c) displacement between transmitter and receiver coils.

Figure 6. Coupling coefficients versus vertical transfer distance between transmitter and receivers. (a) and (b) show the effect of the vertical distance on the coupling coefficients for central and lateral authorized receivers, respectively. The coupling coefficients decrease with the increase of the vertical transfer distance. (c) and (d) show the effect of the vertical distance on the coupling coefficients for central and lateral unauthorized receivers, respectively. The coupling coefficients are lower than those for the authorized receivers.

Figure 7. Magnetic field distributions. (a) Flux lines and current densities (central coil authorized); (b) flux lines and current densities (lateral coil authorized); (c) flux densities along vertical plane (central coil authorized); (d) flux densities along vertical plane (lateral coil authorized); (e) 3-D flux densities (central coil authorized); and (f) 3-D flux densities (lateral coil authorized).

By using FEA, Figure 6 shows the decreasing trend of coupling coefficient with the increasing vertical transfer distance between the transmitter and central (or lateral) authorized receiver. Also, the magnetic field distributions are shown in Figure 7 in which only the central receiver coil is authorized, or only the right lateral receiver coil is authorized. As shown in Figures 7a and b, the magnetic flux pipe can be effectively built up by using the energy encryption scheme. It can be observed that the vast majority of magnetic flux lines are bundled up through the authorized receiver coil, and only insignificant ones are dispersed through the unauthorized receiver coils. Figures 7a and b also demonstrate that the current densities in the authorized receiver coil are much larger than those in the unauthorized ones. Therefore, only the authorized receiver can successfully decrypt and harvest the encrypted wireless energy, thus inducing large current. Along the vertical plane, the contour plots of the magnetic flux densities are plotted in Figures 7c and d, where the magnetic flux densities around the authorized receivers are far higher than those around the unauthorized ones. Along the middle parallel plane, the 3-D magnetic flux densities are plotted in Figures 7e and f, where the saddle-shape magnetic flux densities under the authorized receiver coil can reach up to 3.044 mT.
and 2.619 mT, respectively. By applying the proposed continuously energy encryption scheme, Figure 8a shows that both the authorized receiver current and output voltage (23.82 V) are much larger than the unauthorized receiver currents and output voltages (2.01 V and 3.26 V). Figure 8b shows that both the operating frequency and its active duration are simultaneously encrypted in a 2-D scale to improve the energy security performance. With knowledge of security keys, the authorized receiver can always successfully decrypt and pick up the encrypted wireless power, thus generating an average output voltage of 22.75 V, while the unauthorized receivers fail to decrypt and harvest from the proposed energy-encrypted WPT system, hence only generating insignificant values of 2.27 V and 3.28 V. Correspondingly, the wireless power harvested by the authorized receiver is 104.57 W, far greater than those (0.83 W and 2.16 W) harvested by the unauthorized ones. During the first 0.08 s, an energy of 8.37 J is transferred to the authorized receiver, whereas only 0.239 J is transferred to the unauthorized ones, corresponding to 2.78% of the total energy transfer.

![Figure 8a](image1.png)

**Figure 8a.** Authorized and unauthorized receiver currents.

![Figure 8b](image2.png)

**Figure 8b.** Authorized and unauthorized output voltages.

5. Experimental Verification

To verify the feasibility of the proposed continuously energy-encrypted SVC-based WPT system, an exemplified prototype is built for experimental tests as shown in Figure 9. When the encrypted operating frequency deviates the resonant frequency, Figure 10a shows the measured waveforms of the transmitter current $i_t$, SVC inactive current $i_{sm}$, authorized receiver current $i_{rm}$ and output voltage $u_{om}$ in the state of inactivating SVC. It can be observed that the leading angle $\theta$ does not exactly equal $\pi/2$, and the output voltage $u_{om}$ of the authorized receiver, as well as its harvested wireless power, is low. After activating the SVC in Figure 10b, the leading angle $\theta$ is pulled back to $\pi/2$, and both the output voltage $u_{om}$ and the harvested wireless power of the authorized receiver are effectively increased. Thus, the energy-encrypted WPT system reenters into a resonance state by adjusting the SVC-based impedance compensation. To demonstrate the dynamic response of the proposed SVC-based decryption, Figure 10c shows the measured waveforms of the proposed energy-encrypted...
WPT system operating from the inactivation to the activation of SVC. The increased output voltage of the authorized receiver effectively verifies the feasibility of the proposed SVC.

![Experimental setup.](image)

After activating the proposed SVC for energy decryption, Figure 11a shows measured waveforms of the input voltage $u_{in}$, encrypted transmitter current $i_r$, authorized receiver current $i_{on}$, and unauthorized receiver current $i_{on}$. It can be observed that the authorized receiver current $i_{on}$ (5.43 A) is much larger than the unauthorized one (0.601 A). As shown in Figure 11b, the output voltage $u_{on}$ (25.57 V) of the authorized receiver is far larger than the output voltages $u_{on}$ (3.71 V and 1.30 V) of the unauthorized ones. Thus, the wireless power harvested by the authorized receiver can reach up to 130.76 W, while those harvested by the unauthorized receivers are suppressed to insignificant values of 2.75 W and 0.39 W, corresponding to 2.35% of the total power transfer. By directly introducing the chaotic 2-D FDE technology, Figure 11c shows the encryption performance of the proposed continuously energy-encrypted SVC-based WPT system. Notedly, both the fluctuations and their widths on the output voltages indicate that the proposed 2-D FDE scheme is effective by flexibly encrypting the operating frequency and its duration in a 2-D scale. It can be found that the average output voltage $u_{on}$ of the authorized receiver can achieve 22.49 V, whereas the output voltages $u_{on}$ and $u_{on}$ of the unauthorized ones are insignificant, only 2.98 V and 1.50 V, respectively. Correspondingly, the authorized receiver can decrypt and pick up the encrypted wireless power of 101.16 W, while the unauthorized receiver’s performance is greatly suppressed with harvested wireless powers of 1.78 W and 0.45 W, respectively. Thus, the authorized receiver can successfully harvest 97.84% of wireless powers among all the receivers. It confirms that the MEBT and chaotic 2-D FDE can generate a sequence of dynamic security keys to guarantee energy security. Thus, the proposed continuously energy-encrypted SVC-based WPT system is well verified to improve the energy security performance for multi-receiver WPT systems.
The proposed continuously energy-encrypted SVC-based WPT system is well verified to improve the energy security performance for multi-receiver WPT systems.

Figure 10. Measured waveforms of proposed SVC-based energy-encrypted WPT system. (a) Inactivate SVC ($\theta > 90^\circ$); (b) activate SVC ($\theta = 90^\circ$); and (c) dynamic response.
5. Conclusions

A novel continuously variable-frequency energy-encrypted WPT system using SVC has been proposed and then implemented, which can significantly improve the wireless energy security. The proposed LCC-compensated switched-capacitorless transmitter can continuously encrypt the wireless energy into theft-proof energy packages, while the presented SVC successfully facilitates only authorized receivers to decrypt and harvest the encoded energy packages. By directly introducing a chaotic 2-D FDE technology, a sequence of highly defensive security keys is generated to greatly enhance energy security performance. With knowledge of security keys, the authorized receiver can successfully harvest 97.84% of wireless powers among all the receivers, while the unauthorized ones pick up only insignificant wireless powers from the proposed energy-encrypted WPT system.

The feasibility of the proposed continuously variable-frequency energy-encrypted WPT system...
using LCC-compensated switched-capacitorless transmitter and SVC has been effectively verified by theoretical analysis, simulation and experimentation.

**Author Contributions:** W.L., K.T.C. and W.H.L. developed the idea, carried out the analysis, performed the verification and wrote this paper. Z.Z. made important suggestions.

**Funding:** This research was funded by the Hong Kong Research Grants Council, Hong Kong Special Administrative Region, China, grant number 17204317.

**Conflicts of Interest:** The authors declare no conflict of interest.

**Appendix A**

\[ \eta_k = \frac{\lambda_1 |\eta_k|^2 |\eta_{k,eq}|}{|Z_{k,eq}|} = \left( \frac{\lambda_1 (|\omega_n L_C|)^2 R_{k,eq} |\eta_{k,eq}|}{|Z_{k,eq}|} \right)^2 = \frac{\lambda_1 R_{k,eq} (|\omega_n L_C|)^2}{|Z_{k,eq}|} \]

\[ \eta_C = \left( \frac{\lambda_1 R_{k,eq} (|\omega_n L_C|)^2}{|Z_{k,eq}|} \right)^2 \]

\[ \begin{align*} & \left( \frac{R_C + \text{Re} \left( \sum_{k=1}^{n} \lambda_k Z_{k,eq} \right) + j \text{Im} \left( \sum_{k=1}^{n} \lambda_k Z_{k,eq} \right)}{|Z_C|} \right)^2 \\ & = \left( \frac{R_C + \text{Re} \left( \sum_{k=1}^{n} \lambda_k Z_{k,eq} \right) + j \text{Im} \left( \sum_{k=1}^{n} \lambda_k Z_{k,eq} \right)}{|Z_C|} \right)^2 \end{align*} \]
\[
\eta_m = \frac{\lambda_m R_{eq} (\omega_m L_m)^2}{ \left( R_{eq} + R_m \right)^2} \left( R_{eq} \left( \prod_{k=1}^m \left( \frac{\lambda_k (\omega_m L_{tk})^2}{\omega_m R_{eq} + \omega_m C} \right) \right) + R_t \right) + \frac{\lambda_m R_{eq} (\omega_m L_{m1})^2}{ \left( R_{eq} + R_m \right)^2} \left( \frac{\lambda_m (\omega_m L_{m1})^2}{ \left( \omega_m \omega_m C + \frac{1}{\omega_m C} \right)} \right) + R_t \]
\]

\[
\eta_m = \frac{\lambda_m R_{eq} (\omega_m L_m)^2}{ \left( R_{eq} + R_m \right)^2} \left( R_{eq} \left( \prod_{k=1}^m \left( \frac{\lambda_k (\omega_m L_{tk})^2}{\omega_m R_{eq} + \omega_m C} \right) \right) + R_t \right) + \frac{\lambda_m R_{eq} (\omega_m L_{m1})^2}{ \left( R_{eq} + R_m \right)^2} \left( \frac{\lambda_m (\omega_m L_{m1})^2}{ \left( \omega_m \omega_m C + \frac{1}{\omega_m C} \right)} \right) + R_t \]

\(Z_1 = \omega_m L_{m1} - \frac{1}{\omega_m C} + \frac{\lambda_m (\omega_m L_{m1})^2}{ \left( \omega_m \omega_m C + \frac{1}{\omega_m C} \right)} + \frac{\lambda_m \omega_m L_{m1}}{ \left( \omega_m \omega_m C + \frac{1}{\omega_m C} \right)}\)

\(Z_2 = \omega_m L_{m1} - \frac{1}{\omega_m C} + \frac{\lambda_m (\omega_m L_{m1})^2}{ \left( \omega_m \omega_m C + \frac{1}{\omega_m C} \right)} + \frac{\lambda_m \omega_m L_{m1}}{ \left( \omega_m \omega_m C + \frac{1}{\omega_m C} \right)}\)

References


23. Yan, Z.; Zhang, Y.; Song, B.; Zhang, K.; Kan, T.; Mi, C. An LCC-P compensated wireless power transfer system with a constant current output and reduced receiver size. *Energies* 2019, 12, 172. [CrossRef]

24. Liu, X.; Clare, L.; Yuan, X.; Wang, C.; Liu, J. A design method for making an LCC compensation two-coil wireless power transfer system more energy efficient than an SS counterpart. *Energies* 2017, 10, 1346. [CrossRef]


