sensors

MDPI

Article

Efficient Authentication Protocol and Its Application in Resonant Inductive Coupling Wireless Power Transfer Systems

Emmanuel Ahene [1,*], Mark Ofori-Oduro [2], Frimpong Twum [1], Joojo Walker [3] and Yaw Marfo Missah [1]

[1] Department of Computer Science, Kwame Nkrumah University of Science and Technology, PMB, UPO, KNUST, Kumasi, Ghana; ftwum.cos@knust.edu.gh (F.T.); ymissah@gmail.com (Y.M.M.)

[2] Department of Electrical and Computer Engineering, Concordia University, 1455 De Maisonneuve Blvd, Montreal, QC H3G IM8, Canada; oduromark91@gmail.com

[3] School of Software Engineering, University of Electronic Science and Technology of China, Chengdu 610051, China; joojokojododzi@gmail.com

* Correspondence: aheneemmanuel@knust.edu.gh

Abstract: Chaos theory and its extension into cryptography has generated significant applications in industrial mixing, pulse width modulation and in electric compaction. Likewise, it has merited applications in authentication mechanisms for wireless power transfer systems. Wireless power transfer (WPT) via resonant inductive coupling mechanism enables the charging of electronic devices devoid of cords and wires. In practice, the key to certified charging requires the use of an authentication protocol between a transmitter (charger) and receiver (smartphone/some device). Via the protocol, a safe level and appropriate charging power can be harvested from a charger. Devoid of an efficient authentication protocol, a malicious charger may fry the circuit board of a receiver or cause a permanent damage to the device. In this regard, we first propose a chaos-based key exchange authentication protocol and analyze its robustness in terms of security and computational performance. Secondly, we theoretically demonstrate how the protocol can be applied to WPT systems for the purposes of charger to receiver authentication. Finally, we present insightful research problems that are relevant for future research in this paradigm.

Keywords: chaos-based cryptography; key exchange; authentication protocol; wireless power transfer

check for updates

Citation: Ahene, E.; Ofori-Oduro, M.; Twum, F.; Walker, J.; Missah, Y.M. Efficient Authentication Protocol and Its Application in Resonant Inductive Coupling Wireless Power Transfer Systems. *Sensors* **2021**, *21*, 8245. https://doi.org/10.3390/s21248245

Academic Editor: Jiankun Hu

Received: 30 September 2021
Accepted: 26 November 2021
Published: 9 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In the wireless power transfer (WPT) concept [1], a transmitter device, driven by a source of electric power, produces a time-varying electromagnetic field that transmits power crosswise over space to the receiver device. The receiver device extracts power from the field and then supplies this to an electrical load. Since the emergence of WPT technology, the traditional usage trends of electrical energy have been significantly changing, rendering the use of wires and power cords unattractive and impractical for mobility and large-scale deployments [2]. The diverse forms of WPT are classified as radiative and non-radiative based on their transmission techniques and distance of transmission. In the radiative WPT, power is transmitted over long distances by means of electromagnetic waves such as radio frequency (RF) waves, microwaves or laser beams [3,4]. In contrast, power is transmitted over short distances by means of electromagnetic fields coupling such as inductive, resonant inductive, magnetic or capacitive coupling in the non-radiative WPT [5–7]. Both technologies have useful applications in the transfer of energy with differences in power transfer efficiency (PTE). The scope of this paper is limited to non-radiative WPT systems that exist via resonant inductive coupling techniques.

In earlier applications of WPT using inductive power transfer (IPT), designers were faced with the challenge of reduced energy efficiency since the strength of the induced magnetic field decreased with respect to distance. As a remedy, the concept of WPT using resonant inductive coupling was introduced [5]. The inception of resonators with the same frequency in the sources and receiver coil, respectively, ensures that both systems couples magnetically, hence allowing for higher efficiency in energy transfer. This implies that power transfer occurs over an air gap devoid of metal or any material connection. However, when the two objects are far apart, power transfer is achievable via resonating the two coils at the same frequency. Greater power transfer distance is attainable with resonant repeaters between the two components. Until now, WPT using resonant inductive coupling holds much promise for future technology since its range of transmission is the largest range among the other techniques in the non-radiative WPT systems [8]. It has merited applications in biomedical implants, charging portable devices, electric vehicles and smartcards.

Although the resonant inductive coupling technique has multiple benefits, it is associated with unexpected security vulnerabilities. Firstly, the rate of energy harvesting can enormously change due to the sensitivity of energy transmitters (ET) to the surrounding environment (which is the presence of other energy receivers (ER) beside their targeted ER). Secondly, it is possible for an adversarial ET (such as counterfeit wireless chargers) to initiate a launch or an attack that can cause power surges that can fry the ER device's circuitry [9,10]. The absence of relevant security measures in resonant inductive coupling WPT systems may slow down their rapid adoption in the future. The emphasis of this paper is to provide a key exchange authentication mechanism that can be applied to resonant inductive coupling WPT systems. We leverage the deterministic random-like property of chaos theory to achieve our objective in this paper.

Chaos-based cryptography has generated significant applications in industrial mixing, pulse width modulation and in electric compaction [11,12]. Likewise, it has merited applications in authentication and energy encryption mechanisms [13–15] for wireless power transfer systems. In [13–15], the authors proposed several energy encryption techniques for resonant inductive coupling WPT systems using chaos-based cryptographic techniques. However, in their approaches, they only achieve confidentiality and they lack authentication. We point out that their approaches do not provide perfect forward secrecy and resistance to replay attacks that are essential security requirements for resonant inductive coupling WPT systems.

Perfect forward secrecy assures that an adversarial ET does not compromise session keys, which are relevant to generating switching frequencies for both authorized ET and ER, even at the compromise of one party's private key. Moreover, resistance to replay attack can prevent an unauthorized ER or a malicious device from delaying the process of electric power charging. As a remedy, we propose a key exchange authentication protocol from chaos theory and demonstrate how it can be applied to the realization of a secure WPT system that assures equitable power transfer. Our scheme achieves mutual authentication, perfect forward secrecy, resistance to replay attack and known key security. For simplicity, we redefine "resonant inductive coupling WPT systems" as "WPT systems" and "key exchange authentication protocol" as "authenticated key exchange scheme" in the subsequent sections of the paper.

1.1. Related Work

In a concise manner, we present related works pertinent to the WPT system paradigm and the authenticated key exchange scheme (AKE) paradigm.

On WPT systems, Kurs et al. [2] primarily introduced the notion of wireless transmission of power through strongly coupled magnetic resonance. In their work, they experimentally demonstrated the efficiency of non-radiative power transfer over distances up to eight times the radius of a coil with a 40% efficiency in the transfer of 60 watts. Wang et al. [11] accordingly worked on the system structure authorization and principle explanation of WPT by way of strongly coupled magnetic resonances (SCMR). In general, their work analyzes the characters of the multicoil system of SCMR and emphasizes the instructions for designing practical WPT system structures. In [12], Rajiv et al. significantly contributed to the WPT paradigm by proposing the resonant coupling analysis for a two-coil wireless power transfer system. On the other hand, Lee et al. [16] proposed that wireless transmission can be done using a different approach by presenting reflexive field containment in dynamic inductive power transfer systems. In 2009, Cannon et al. [17] proposed magnetic resonant coupling as a potential means for wireless power transfer to multiple small receivers. In summary, these related works and others such as [7,18] focus on the efficiency mode of transfer, the working principles and the circuit topology of WPT systems. Few existing works attempt to address the security issues of WPT systems. In [13] and [14], Zhen et al. proposed the energy encryption technique for wireless power transfer. However, their work does not assure perfect forward secrecy and resistance to replay attack. In [19], genuine chargers are authenticated using public key authentication mechanisms such as elliptic curve cryptography. This approach is meant to overcome the challenge of skewness in received power between ERs and secure the ERs from perceived attacks by counterfeit ETs. By extension, a generic mechanism [20] based on certificateless cryptography has been designed for improving secure WPT systems. However, according to [21], it may be a computationally expensive approach for encrypting the resonant frequency.

AKE schemes allow for two entities to securely communicate over insecure channels with shared keys. After its inception [22] by Diffie and Hellman, several useful AKE schemes [23–26] have been developed with diverse application perspectives. The adoption of chaos theory into AKE is due to its suitable properties of extreme sensitivity to initial conditions, pseudo-randomness, low computational cost, unpredictability and non-periodicity [27–29]. Essentially, the concept of chaos-based AKE [30,31] has shown merit in secure smartcard transactions [32], Internet of Things [33], smart grids [34] and WPT systems [13–15]. Several chaos-based AKE schemes [24,35–38] have been developed over the years. However, most of them may not be directly applicable to achieve a secure WPT system. For instance, the schemes in [35,38] are computationally expensive and may not be fitting for WPT devices. In contrast, recent works such as [13–15] are applicable to WPT systems but they do not provide perfect forward secrecy and resistance to replay attack. In this perspective, we put forward an efficient chaos-based AKE (CBAKE) scheme that can be applied to WPT systems by extension and can assure secure and equitable power transfer.

1.2. Organization

The rest of the paper is organized as follows: In Section 2, preliminary concepts employed in the paper are presented. In Section 3, the concrete construction of the proposed scheme and its security analysis are presented. We evaluate the performance of our scheme and compare it to other chaos-based AKE schemes in Section 4. In Section 5, we show how our scheme can be applied to realize a secure WPT system and also compare our proposed scheme to other existing WPT schemes in terms of functionality. In Section 6, we present the open research questions that can extend research in this domain. Finally, we conclude this paper in Section 7.

2. Preliminaries

2.1. Wireless Power Transfer Scenario

Transfer of energy from the transmitter to the receiver is achieved by ensuring that both systems are resonating at the same frequency [39–41]. We give a further explanation using Figure 1. According to Figure 1, it is obvious that the basic circuit of a WPT system is made up of three fundamental units, namely the transmitter, resonator and receiver. We denote V_S as the source voltage, R_{ET} as the resistance, C_{ET} as the capacitance and L_{ET} as the inductance of the transmitter. C_D, R_D, and L_{D1}/L_{D2} are the capacitance, resistance and inductance of the resonator, respectively, while C_{ER}, R_{ER} and L_{ER} are the capacitance, resistance and inductance of the receiver. Finally, R_l is identified as the load resistance. The switching frequencies [42,43] of the transmitter ω_{ET} resonator ω_D and receiver ω_{ER} are mathematically defined as; $\omega_{ET} = \frac{1}{\sqrt{C_{ET}L_{ET}}}$, $\omega_D = \frac{1}{\sqrt{C_D L_D}}$, $\omega_{ER} = \frac{1}{\sqrt{C_{ER}L_{ER}}}$.

Hence, to obtain maximum power transfer from the transmitter to the receiver, all units of the circuit must reach the same frequency of resonance as shown in Equation (1).

This can be achieved by simultaneously adjusting the capacitance on the transmitter's side as well as the receiver's side. The resonance coil is necessary for the increase of the transmission distance between the transmitter and the receiver:

$$\omega_{ET} = \omega_{ER} = \omega_{ED} \tag{1}$$

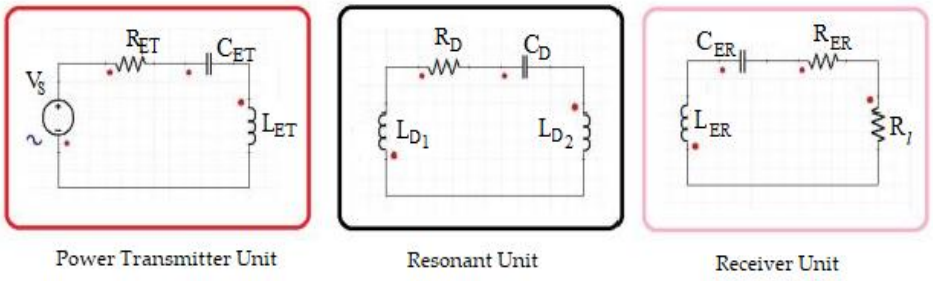

Figure 1. Wireless power transfer (WPT) system basic circuit.

2.2. Chebyshev Chaotic Map

The Chebyshev polynomial [44,45] of degree n is defined as:

$$T_n(x) = cos(n^* arccos\,(x))(-1 \le x \le 1)$$

The recurrent formulas are:

$$T_0(x) = 1,\ T_1(x) = x,\ T_2(x) = 2x^2 - 1,\ \ldots,$$

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x),\ n = 1,\ 2, \ldots.$$

Chebyshev polynomial also exhibits the following properties:
(1) Semi-group property

$$\begin{aligned} T_r(T_s(x)) &= cos(r^* arccos(cos(s^* arccos(x)))) \\ &= cos(rs^* arccos(x)) \\ &= T_{sr}(x) \\ &= T_s(T_r(x)) \\ &\therefore\ T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x)) \forall\, s, r \in Z^+ \end{aligned}$$

(2) Chaotic property when $n > 1$, Chebyshev polynomial map $T_n : [-1,\ 1] \to [-1,\ 1]$ of degree n is a chaotic map with its invariant density:

$$f^*(x) = \frac{1}{\sqrt[\pi]{1 - x^2}}$$

For the Lyapunov exponent, $\lambda = \ln n > 0$.

2.3. Hard Problem

Our scheme is based on three hard problems, namely: the hardness of the quadratic residue assumption and the two hard problems associated with the semi-group property of the Chebyshev polynomial, namely the chaotic-based discrete logarithm (CDL) problem and the chaotic-based Diffie–Hellman (CDH) problem. These hard problems are assumed to be infeasible to solve if one is not aware of some specific parameters. In other words, no polynomial time algorithm has been found to solve such problems. We give the details of the problems as follows:

(1) Quadratic Residue Assumption: Given p and q as two large primes and $n = p * q$. Let the symbol QR_n denote the set of all quadratic residues in $[1, n-1]$. If $y = x^2 \ mod\ n$ has a solution, i.e., $\exists$ a square root for y, then y is named as a quadratic residue modulo

n where $y \in QR_n$. To find x satisfying $y = x^2 \ mod \ n$ when p and q are unknown is computationally intractable since no polynomial algorithm has been found to solve the factoring problem.

(2) Chaotic-based Discrete Logarithm (CDL) Problem: Given the variable x and the result y, it is infeasible to find the integer n, such that $T_n(x) \equiv y \ mod \ p$

(3) Chaotic-based Diffie–Hellman (CDH) Problem: Given the variable x, $T_n(x) \ mod \ p$ and $T_m(x) \ mod \ p$, it is infeasible to compute $T_{nm}(x) \ mod \ p$ without knowing n or m.

3. A Chaos-Based Authentication Key Exchange Scheme

In this section, we outline the concrete construction of the CBAKE scheme.

Phase 1: System Initialization

With a security parameter λ, the energy transmitter ET first generates large primes p and q and computes $n = p * q$. Here, p and q are kept as secret keys, whereas n is published by the ET. Additionally, the ET publishes two hash functions H_1: $\{0,1\}^* \rightarrow \{0,1\}^\lambda$ and $H_2 : \{0,1\}^* \rightarrow (-\infty, +\infty)$.

Phase 2: Authentication and Key Exchange

- First, the ER chooses integers r and y at random and computes $x = H_1(y)$, $T_r(x) = r_{pub,} k = y * r_{pub}$, $\mu = (k||PW)$, $r = \mu^2 \ mod \ n$, $EID_{ER} = U_{ER} \oplus H_2(\mu)$ and $UAuth_{ER} = H_2(\mu,\ T_r(x),\ T_1,\ EID_{ER})$. Here, T_1 is the initial timestamp. The ER sends $C_1 = \{UAuth_{ER},\ r,\ T_r(x),\ T_1,\ EID_{ER}\}$ to the ET.
- Given C_1, the ET validates whether $T_2 - T_1 \leq \triangle T$ is true or not. Here, T_2 is the ET's current timestamp. Upon successful verification, the Chinese remainder theorem is used to solve R using p and q to get $\mu_1,\ \mu_2,\ \mu_3,\ \mu_4$ and then the ET determines whether $\mu' = (k'||PW'\ )$ by verifying whether $UAuth_{ER} = H_2(\mu_i,\ T_r(x),\ T_2,\ EID_{ER})$ for i = 1, 2, 3, 4. Subsequently, the ET computes $U_{ER} = EID_{ER} \oplus H_2(\mu')$ and validates whether $PW' = PW$ is right or not. If true, the ET successfully authenticates the ER and selects a random integer s and computes $x = H_1(y')$, $T_s(x)$, $\gamma = H_2(T_r(x), T_s(x), T_{sr}(x))$, $UAuth_{ET} = H_2(\gamma,\ PW, U_{ET}, U_{ER}, T_2)$. The ET then sends $C_2 = \{UAuth_{ET}, U_{ET}, T_s(x), T_2\}$ to the ER.
- It is verified whether $T_3 - T_2 \leq \triangle T$ is true or not once C_2 is received by the ER. Note that T_3 is the current timestamp here. The ER then computes $\gamma' = H_2(T_r(x), T_s(x), T_{sr}(x))$ and validates the rightness of $UAuth_{ET} = H_2(\gamma', PW, U_{ET}, U_{ER}, T_2\Big)$. Once verified as right, the ER successfully authenticates the ET; otherwise, the ER aborts this request. Now, the ER and the ET possess $\gamma = H_2(T_r(x), T_s(x), T_{rs}(x))$. Thus, γ is the shared session key, which is relevant for computing the switching frequency.

Security Analysis of the CBAKE Scheme

In this subsection, we analyze the proposed chaos-based authenticated key exchange scheme in terms of its security and performance. Our proposed scheme is secured in terms of mutual authentication, contribution property of key agreement, private key security, perfect forward secrecy, resistance to password guessing attack, user anonymity, known key security and resistance to replay attack.

1. Mutual Authentication: In the proposed scheme, the ET authenticates the ER by verifying $H_2(EID_{ER},\ \mu_i,\ T_r(x),\ T_1) = UAuth_{ER}$ and $PW' = PW$. Subsequently, the ER authenticates the ET by verifying $H_2(\gamma', PW, U_{ET}, U_{ER}) = UAuth_{ET}$ as stated in the third step, where $\gamma' = H_2(T_r(x), T_s(x), T_s(T_r(x)))$. Hence, the proposed scheme has mutual authentication capability.
2. Resistance to Replay Attack: The proposed scheme guarantees the freshness of the key due to the timestamps being utilized. These can be seen as follows: T_1 in C_1, T_2 in C_2 and T_3 in C_3. Therefore, our proposed scheme prevents replaying attacks.
3. Contribution Property of Key Agreement: In the proposed scheme, the chaotic session key is $\gamma = H_2(T_r(x), T_s(x), T_{rs}(x))$. In the process, no party is able to determine the session key alone since s and r are random numbers secretly generated by the power

transmitter and the receiver, respectively. Notably, the proposed scheme satisfies the contribution feature of the key agreement.

4. Private Key Security: Given $T(\cdot)$, $T_r(x)$ and $T_s(x)$. $T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$, the session key $\gamma = H_2(T_r(x), T_s(x), T_{rs}(x))$ cannot be calculated if r, s and x remain unknown, due to the chaotic maps Diffie–Hellman problem [46]. Therefore, the session key cannot be derived by an unauthorized user in our proposed CBAKE scheme.
5. Known Key Security: The session key $\gamma = H_2(T_r(x), T_s(x), T_{rs}(x))$ generated in distinct rounds are not dependent on each other due to the fact that r, s and x are chosen randomly by the ER and the ET, respectively, and, in the scheme executions, they are independent of each other. Hence, the proposed scheme achieves the known-key security.
6. Perfect Forward Secrecy: In our scheme, a false password PW will not result in any previous session key $\gamma = H_2(T_r(x), T_s(x), T_{rs}(x))$ since the short-lived numbers r, s and x are picked randomly and independent among the executions of the scheme's algorithms. More specifically, the proposed scheme has perfect forward secrecy. However, an attacker can use the strategy of Bergamo et al. [44] to realize the secret key y and derive previous session keys $\gamma = H_2(T_r(x), T_s(x), T_{rs}(x))$, where $x = H_1(y)$ if the private keys p and q of T are known.
7. Resistance to Password Guessing Attack: For $V = H_2(EID_{ER},\ \mu,\ T_r(x))$, where $\mu = (k||PW)$, $UAuth_{ET}= H_2(\gamma, PW, U_{ET}, U_{ER})$ involve password related information. Even though some of the messages are revealed, PW cannot be obtained due to the hash function $H_2(\cdot)$, which has a one-way property. Moreover, PW is protected by the secret value k. Additionally, there exists no information that can aid an attacker to directly confirm the authenticity of the guessed passwords. In this way, offline password guessing attacks fail with respect to our proposed scheme.
8. User Anonymity: The temporary identity $EID_{ER}= U_{ER} \oplus H_2(\mu)$, where $\mu = (k||PW)$ and k represent a random secret generated by the ER is not dependent on scheme executions. Therefore, ID_{ER} cannot be obtained from EID_{ER} when k, PW and likewise ID_{ET} are unknown. Moreover, due to the quadratic residue assumption, one cannot decipher μ from R if the power transmitter's secret keys p and q are not known, where $R = \mu^2 \ mod\ n$. In addition, U_{ER} and U_{ET} cannot be generated from $UAuth_{ER}= H_2(\gamma,\ U_{ER}, U_{ET})$, $UAuth_{ET}= H_2(\gamma, PW\ U_{ER}, U_{ET})$ because of the inherent one-way property of the hash function. Hence, our proposed CBAKE scheme achieves the user anonymity feature.

4. Performance Analysis

In this section, we present a performance analysis of our proposed CBAKE scheme in relation to other chaos-based schemes. We highlight the computation cost of each of the schemes and also compare some of the significant properties that these schemes possess. The results from our analysis and the corresponding notations used for the analysis with their meanings are presented in Tables 1 and 2, respectively. In Table 1, we follow the experimental results in [35] as a standard to evaluate all the schemes under comparison. Researchers in [35] report that when using the PBC library on an Ubuntu 12.04.1 32 bit operating system, with 2.4 GHz CPU and 2.0 GB RAM, the estimated running times for various cryptographic operations are as follows: the time of the hash-based operation is 0.00058 s, the symmetric encryption or decryption is 0.0086 s, the modular squaring operation, modular square root operation, elliptic curve scalar multiplication and Chebyshev polynomial operation are 0.01018 s, 0.00987 s, 0.063165 s and 0.02104 s, respectively. They considered the XOR operation cost as negligible in their analysis. As shown in Table 1, we begin our comparison with the various computational cost evaluated.

Table 1. Performance evaluation.

Schemes	Computation Cost	Computation Time in Seconds	F1	F2	F3	F4
[35]	$49T_H + 10T_C + 2T_S$	0.25602	No	Yes	Strong	Yes
[38]	$43T_H + 10T_C$	0.23534	No	Yes	Weak	Yes
[47]	$18T_H + 10T_C$	0.22084	No	No	Weak	Yes
[48]	$7T_H + 4T_C$	0.0882	Yes	No	Weak	Yes
[49]	$5T_H + 6T_C + 5T_S$	0.17214	No	No	Weak	Yes
[50]	$12T_H + 4T_C$	0.09112	No	No	Weak	Yes
[51]	$5T_H + 4T_C + 5T_S$	0.13006	No	No	Weak	No
[53]	$21T_H + 6T_C$	0.13842	No	Yes	Strong	Yes
[54]	$9T_H + 4T_C$	0.08938	No	Yes	Strong	Yes
Ours	$13T_H + 4T_C + T_{SQ} + T_{SR}$	0.20337	Yes	Yes	Strong	Yes

The schemes presented in [35,38,47] are computationally expensive compared to our proposed CBAKE scheme and the other schemes making them inefficient for practical applications. Moreover, we point out that scheme [38] exhibits some weaknesses with regards to resisting possible attacks. On the other hand, chaotic maps-based schemes [48–51] exhibit low computations and are therefore ideal for practical applications. However, due to the fact that they do not support user anonymity and are also weak in resisting possible attacks, they will not be expedient to use in applications such as WPT systems. All the schemes presented in Table 1 except [51] support perfect forward secrecy, which is an important feature for practical applications such as WPT systems. The researchers in [52] revealed that scheme [51] lacks this important feature of perfect forward secrecy. Again, schemes [53,54] have lower computational cost than our proposed scheme. This is mainly due to the fact that quadratic residues are employed in protecting a user's password in our proposed CBAKE scheme. In our scheme, one modular squaring operation is needed by an ER, while the ET needs one squaring root solving operation. Conversely, it has been shown in [55,56] that a modular squaring operation is equivalent to a few hundred gates. The implementation of SHA-1, MD5 and the universal hash function requires 20 K gates, 16 K gates and 1.7 K gates, respectively.

Table 2. Meanings of symbols used for performance evaluation.

Notation	Meaning
F1	Non-usage of extra device such as smartcard
F2	Supports user anonymity
F3	Resistance to possible attacks
F4	Supports perfect forward secrecy
TH	Time for executing a hash function
TC	Time for executing a chaotic map operation
TS	Time for executing a symmetric encryption or decryption operation
TSQ	Time for executing a squaring operation
TSR	Time for executing a square root operation

Hence, it is worth mentioning that the ET's efficiency in CBAKE is unaffected by the modular squaring operation. Additionally, no symmetric encryption/decryption operations are carried out by schemes [40,48,50–54] and CBAKE so they achieve lower computational costs from a user perspective. Moreover, CBAKE [has significant security properties than other related schemes. Furthermore, to protect a weak password, most related schemes employ extra devices, such as smartcards, to store their long-term secret key; only our CBAKE scheme and [48] do not employ smartcards. In our proposed CBAKE scheme, a party only stores their own password and does not need an extra device for storing a long-term secret key.

5. Application to WPT System

In this section, we only demonstrate theoretically the application of CBAKE scheme to a WPT system. Rigorous implementation of the system is out of the scope of the paper.

As shown in Figure 2, the system comprises a transmitter device whose source of power is obtained from the main power line. The transmitter device (ET) converts the power to an electromagnetic field, which can be received by one or more receiver devices via resonant inductive coupling. The receiver device (ER) receives power and then converts it back to a direct electric current (DC), which is utilized by the electrical load. Both the transmitter and receiver circuit comprise a resistor, inductor, variable capacitor and a processing entity or node. Essentially, a judicious regulation of the working frequency in the energy transmitter and energy receiver circuits determines the performance of power flow. In other words, power transfer is efficient based on the optimal switching frequency. Subsequently, we refer to the transmitter device as a wireless charger pad (WCP) and the receiver device as a mobile phone. To ensure an efficient and secured wireless power flow, the wireless charger pad establishes trust with the mobile phone by running the CBAKE scheme. The WCP controls the variable capacitor using its obtained chaotic session key. In this way, the frequency of the WCP is also regulated. The mobile phone can only receive power, when, accordingly, its frequency is simultaneously regulated by the same chaotic session key. It is obvious that, once the ephemeral session key is unknown, the usage of the transferred wireless power would be undesirable to other unauthorized receiving devices. We define the process whereby the wireless charger pad and the mobile phone undertakes internal computations and regulations to resonate at the same frequency using their ephemeral chaotic session keys as energy encryption and decryption, respectively. The detailed process for the encryption and decryption is depicted in the flowchart in Figure 3 and mathematically deduced as follows.

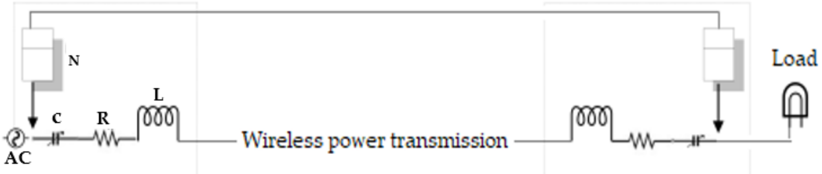

Figure 2. System energy encryption architecture.

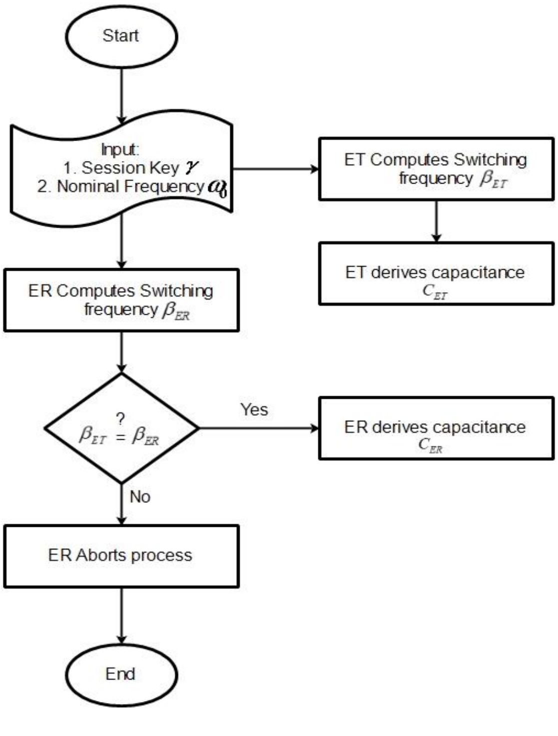
Start
Input:
1. Session Key γ
2. Nominal Frequency ω_0
ET Computes Switching frequency β_{ET}
ET derives capacitance C_{ET}
ER Computes Switching frequency β_{ER}
$\beta_{ET} \overset{?}{=} \beta_{ER}$
Yes
ER derives capacitance C_{ER}
No
ER Aborts process
End

Figure 3. Illustration of the process of encryption and decryption.

Encrypt $(\gamma,\ \omega_0) \rightarrow (\beta_{ET},\ C_{ET}):$ The encrypt algorithm is run by the ET. The ET takes as input the chaotic session key $\gamma = H_2(T_r(x), T_s(x), T_{rs}(x))$ and the nominal frequency ω_0 and outputs a switching frequency $\beta_{ET}= \gamma\omega_0$ and capacitance C_{ET}. C_{ET} is computed as follows: if the chaotic session key for both parties is the Chebyshev polynomial $\gamma = H_2(T_r(x), T_s(x), T_{rs}(x))$ then the ET can compute a switching frequency as $\beta_{ET}= \gamma_i\ \omega_0, \forall\ i\ >\ 0$. Assuming $\omega_{ET} = \beta_{ET}$ then the ET can compute C_{ET} as:

$$\omega_{ET} = \frac{1}{\sqrt{L_{ET}C_{ET}}};\ \gamma\omega_0 = \frac{1}{\sqrt{L_{ET}C_{ET}}};\ C_{ET} = \frac{1}{\sqrt{\gamma^2\omega_0^2 L_{ET}}} \tag{2}$$

Decrypt $(\gamma,\ \omega_0,\ C_{ET}) \rightarrow (\beta_{ER}, C_D,\ C_{ET},):$ The receptor ER computes the switching frequency β_{ER} using their chaotic session key and a nominal frequency ω_0 as input. Assuming $\omega_{ER} = \beta_{ER}$ and, if $\beta_{ER}= \beta_{ET}$, then the ER can derive its capacitance as C_{ER}. C_{ER} is computed as follows:

$$C_D = \frac{1}{\gamma^2\omega_0^2 L_D}\ ;\ C_{ER} = \frac{1}{\gamma^2\omega_0^2 L_{ER}};. \tag{3}$$

The continuous variation of the capacitance value enhances the security performance of the WPT system. In this work, we achieve the continuous variation using the ephemeral session key. Since both ends can obtain the optimal switching frequency, a secure power transfer is assured.

Functionality Comparison

Now, to point out the significance of our work, we compare the basic properties of the following encryption schemes [13–15] for WPT systems to our proposed CBAKE scheme. The CBAKE scheme supports mutual authentication but [13–15] do not achieve mutual authentication. This property prevents an adversarial ER from harnessing power. Moreover, our scheme is resistant to replay attack. This important property is missing in schemes [13–15]. Additionally, we indicate that a WPT system supporting perfect forward secrecy can ensure that an adversarial ET does not compromise session keys. This is significant when generating switching frequencies for both authorized ET and ER even in instances where one party's session key is compromised. Yet again, the perfect forward secrecy feature is absent in schemes [13–15].

6. Open Research Problems

In this section, we enumerate some open research questions that are targeted at ensuring the expansion of this research field. To begin with, considering the resource constrained devices involved in secure WPT systems, a desirable requirement would be to develop and deploy encryption schemes that are lightweight. It is therefore significant to design schemes that have a low computational cost. Furthermore, it is important to design schemes that ensure that there is low power consumption at the nodes in each circuit system. Additionally, since it is significant to achieve fast, stable and secure wireless power transfers, it would be expedient for this research community to investigate the time scale over which the switching frequency varies. It is worth noting that an intelligent attacker unaware of the key can employ small and slow manipulations to the frequency to extract significant amounts of energy. They achieve this by dynamically changing the frequency so as to maximize received energy. Frequency changes that are fast and heavy can result in secondary effects such as differences in frequency ranges of signal components. More research can be carried out on the effects of these factors and more significantly into building a trade-off between them. Finally, it would be interesting to consider how protocols supporting standard wireless communication technologies such as Bluetooth Low Energy and near-field communication can be adapted into the application of resonant inductive coupling WPT systems.

7. Conclusions

In this paper, we have proposed a new chaos-based authenticated key exchange scheme. We have further demonstrated how the scheme can be applied to WPT systems. The proposed scheme primarily establishes trust and exchanges a common session key via an authenticated key exchange protocol, between the energy transmitter and energy receiver. In spite of the fact that our scheme requires extra computation compared to some existing schemes, we point out that our scheme does not need additional devices such as a smartcard for storing long-term passwords, a feature which is pertinent to WPT systems. Our proposed scheme is highly feasible for other practical applications.

Author Contributions: Conceptualization, E.A. and M.O.-O.; methodology, E.A. and M.O.-O.; validation, E.A., F.T., Y.M.M. and J.W.; formal analysis, J.W. and F.T.; writing—original draft preparation, E.A.; writing—review and editing, F.T. and Y.M.M.; supervision, E.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

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

References

1. Tesla, N. Experiments with Alternate Currents of Very High Frequency and their Application to Methods of Artificial Illumination. *Trans. Am. Inst. Electr. Eng.* **1891**, *VIII*, 266–319. [CrossRef]
2. Kurs, A.; Karalis, A.; Moffatt, R.; Joannopoulos, J.D.; Fisher, P.; Soljačic, M. Wireless Power Transfer via Strongly Coupled Magnetic Resonances. *Science* **2007**, *317*, 83–86. [CrossRef]
3. Das, S.; Wasif, A.; Kumar, N.; Karim, E. Wireless powering by magnetic resonant coupling: Recent trends in wireless power transfer system and its applications. *Renew. Sustain. Energy Rev.* **2015**, *51*, 1525–1552.
4. Liu, Q.; Yildirim, K.S.; Pawełczak, P.; Warnier, M. Safe and secure wireless power transfer networks: Challenges and opportunities in RF-based systems. *IEEE Commun. Mag.* **2016**, *54*, 74–79. [CrossRef]
5. Shinohara, N. *Wireless Power Transfer via Radiowaves*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2014.
6. Lee, C.K.; Zhong, W.X.; Hui, S.Y.R. Recent progress in mid-range wireless power transfer. In Proceedings of the 2012 IEEE Energy Conversion Congress and Exposition, ECCE 2012, Raleigh, NC, USA, 15–20 September 2012.
7. Huh, J.; Lee, S.W.; Lee, W.Y.; Cho, G.H.; Rim, C.T. Narrow-Width Inductive Power Transfer System for Online Electrical Vehicles. *IEEE Trans. Power Electron.* **2011**, *26*, 3666–3679. [CrossRef]
8. Jawad, A.M.; Nordin, R.; Gharghan, S.K.; Jawad, H.M.; Ismail, M. Opportunities and Challenges for Near-Field Wireless Power Transfer: A Review. *Energies* **2017**, *10*, 1022. [CrossRef]
9. Zhang, Z.; Chau, K.T.; Wang, Z.; Li, W. Improvement of Electromagnetic Compatibility of Motor Drives Using Hybrid Chaotic Pulse Width Modulation. *IEEE Trans. Magn.* **2011**, *47*, 4018–4021. [CrossRef]
10. Ye, S.; Chau, K.T. Chaoization of DC Motors for Industrial Mixing. *IEEE Trans. Ind. Electron.* **2007**, *54*, 2024–2032. [CrossRef]
11. Budhia, M.; Boys, J.T.; Covic, G.A.; Huang, C.-Y. Development of a Single-Sided Flux Magnetic Coupler for Electric Vehicle IPT Charging Systems. *IEEE Trans. Ind. Electron.* **2013**, *60*, 318–328. [CrossRef]
12. Lee, W.Y.; Huh, J.; Choi, S.Y.; Thai, X.V.; Kim, J.H.; Al-Ammar, E.; El-Kady, M.A.; Rim, C.T. Finite-Width Magnetic Mirror Models of Mono and Dual Coils for Wireless Electric Vehicles. *IEEE Trans. Power Electron.* **2013**, *28*, 1413–1428. [CrossRef]
13. Zhang, Z.; Chau, K.T.; Qiu, C.; Liu, C. Energy Encryption for Wireless Power Transfer. *IEEE Trans. Power Electron.* **2015**, *30*, 5237–5246. [CrossRef]
14. Zhang, Z.; Chau, K.T.; Liu, C.; Qiu, C. Energy-security-based contactless battery charging system for roadway-powered electric vehicles. In Proceedings of the 2015 IEEE PELS Workshop on Emerging Technologies: Wireless Power (2015 WoW), Daejeon, Korea, 5–6 June 2015.
15. Liu, W.; Chau, K.T.; Lee, C.H.T.; Jiang, C.; Han, W. A Switched-Capacitorless Energy-Encrypted Transmitter for Roadway-Charging Electric Vehicles. *IEEE Trans. Magn.* **2018**, *54*, 1–6. [CrossRef]
16. Lee, K.; Pantic, Z.; Lukic, S. Reflexive Field Containment in Dynamic Inductive Power Transfer Systems. *IEEE Trans. Power Electron.* **2014**, *29*, 4592–4602. [CrossRef]
17. Cannon, B.L.; Hoburg, J.F.; Stancil, D.D.; Goldstein, S.C. Magnetic Resonant Coupling as a Potential Means for Wireless Power Transfer to Multiple Small Receivers. *IEEE Trans. Power Electron.* **2009**, *24*, 1819–1825. [CrossRef]

18. Madawala, U.K.; Thrimawithana, D.J. A Bidirectional Inductive Power Interface for Electric Vehicles in V2G Systems. *IEEE Trans. Ind. Electron.* **2011**, *58*, 4789–4796. [CrossRef]
19. Nadeau, P.; Mimee, M.; Carim, S.; Lu, T.K.; Chandrakasan, A.P. 21.1 Nanowatt Circuit Interface to Whole-Cell Bacterial. In *ISSCC 2017/Session 21/Smart SoCs for Innovative Applications*; IEEE: Piscataway, NJ, USA, 2017; pp. 352–354.
20. Ahene, E.; Ofori-Oduro, M.; Agyemang, B. Secure Energy Encryption for Wireless Power Transfer. In Proceedings of the 2017 IEEE 7th International Advance Computing Conference (IACC), Hyderabad, India, 5–7 January 2017; pp. 199–204.
21. Cai, C.; Yang, M.; Qin, M.; Wu, S. High Transmission Capacity P.U.A Wireless Power Transfer for AUV Using an Optimized Magnetic Coupler. In Proceedings of the 2018 IEEE International Magnetics Conference (INTERMAG), Singapore, 23–27 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–2.
22. Diffie, W.; Hellman, M.E. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
23. Lee, C.-C.; Hsu, C.-W. A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. *Nonlinear Dyn.* **2012**, *71*, 201–211. [CrossRef]
24. Tan, Z. A chaotic maps-based authenticated key agreement protocol with strong anonymity. *Nonlinear Dyn.* **2013**, *72*, 311–320. [CrossRef]
25. Xiang, T.; Wong, K.-W.; Liao, X. On the security of a novel key agreement protocol based on chaotic maps. *Chaos Solitons Fractals* **2009**, *40*, 672–675. [CrossRef]
26. Lee, C.-C.; Chen, C.-L.; Wu, C.-Y.; Huang, S.-Y. An extended chaotic maps-based key agreement protocol with user anonymity. *Nonlinear Dyn.* **2012**, *69*, 79–87. [CrossRef]
27. Alvarez, E.; Fernández, A.; Garcia, P.; Jiménez, J.; Marcano, A. New approach to chaotic encryption. *Phys. Lett. A* **1999**, *263*, 373–375. [CrossRef]
28. Baptista, M. Cryptography with chaos. *Phys. Lett. A* **1998**, *240*, 50–54. [CrossRef]
29. Wong, K. A fast chaotic cryptographic scheme with dynamic look-up table. *Phys. Lett. A* **2002**, *298*, 238–242. [CrossRef]
30. Zhao, G.; Wang, J.; Lu, F. Analysis of Some Recently Proposed Chaos-based Public Key Encryption Algorithms. In Proceedings of the 2006 International Conference on Communications, Circuits and Systems, Guilin, China, 25–28 June 2006.
31. Xiao, D.; Liao, X.; Deng, S. A novel key agreement protocol based on chaotic maps. *Inf. Sci.* **2007**, *177*, 1136–1142. [CrossRef]
32. Zhu, H.; Hao, X. A provable authenticated key agreement protocol with privacy protection using smart card based on chaotic maps. *Nonlinear Dyn.* **2015**, *81*, 311–321. [CrossRef]
33. Srinivas, J.; Das, A.K.; Wazid, M.; Kumar, N. Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 1133–1146. [CrossRef]
34. Mood, D.A.; Nikooghadam, M. Efficient Anonymous Password-Authenticated Key Exchange Protocol to Read Isolated Smart Meters by Utilization of Extended Chebyshev Chaotic Maps. *IEEE Trans. Ind. Inform.* **2018**, *14*, 1. [CrossRef]
35. Irshad, A.; Sher, M.; Chaudhry, S.A.; Xie, Q.; Kumari, S.; Wu, F. An improved and secure chaotic map based authenticated key agreement in multi-server architecture. *Multimed. Tools Appl.* **2018**, *77*, 1167–1204. [CrossRef]
36. Wang, X.; Zhao, J. An improved key agreement protocol based on chaos. *Commun. Nonlinear Sci. Numer. Simul.* **2010**, *15*, 4052–4057. [CrossRef]
37. Irshad, A.; Ahmad, H.F.; Alzahrani, B.A.; Sher, M.; Chaudhry, S.A. An efficient and anonymous Chaotic Map based authenticated key agreement for multi-server architecture. *KSII Trans. Internet Inf. Syst.* **2016**, *10*, 5572–5595. [CrossRef]
38. Tan, Z. A privacy-preserving multi-server authenticated key-agreement scheme based on Chebyshev chaotic maps. *Secur. Commun. Networks* **2016**, *9*, 1384–1397. [CrossRef]
39. Li, J.L. Wireless Power Transmission: State-of-the-Arts in Technologies and Potential Applications. In Proceedings of the Asia-Pacific Microwave Conference 2011, Melbourne, VIC, Australia, 5–8 December 2011.
40. Wu, K.; Choudhury, D.; Matsumoto, H. Wireless Power Transmission, Technology, and Applications [Scanning the Issue]. *Proc. IEEE* **2013**, *101*, 1271–1275. [CrossRef]
41. Mou, X.; Sun, H. Wireless Power Transfer: Survey and Roadmap. In Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015.
42. Mohammed, S.S.; Ramasamy, K.; Shanmuganantham, T. Wireless Power Transmission—A Next Generation Power Transmission System. *Int. J. Comput. Appl.* **2010**, *1*, 102–105. [CrossRef]
43. Geiser, J. *Coupled Systems: Theory, Models, and Applications in Engineering*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2014.
44. Kocarev, L.; Tasev, Z. Public-key encryption based on Chebyshev maps. In Proceedings of the 2003 International Symposium on Circuits and Systems, Bangkok, Thailand, 25–28 May 2003; pp. 28–31.
45. Zhang, L. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos Solitons Fractals* **2008**, *37*, 669–674. [CrossRef]
46. Shoup, V.A. *Computational Introduction to Number Theory and Algebra*; Cambridge University Press: Cambridge, UK, 2015.
47. Lima, J.; De Souza, R.M.C.; Panario, D. Security of public-key cryptosystems based on Chebyshev polynomials over prime finite fields. In Proceedings of the 2008 IEEE International Symposium on Information Theory, Toronto, ON, Canada, 6–11 July 2008.
48. Gong, P.; Li, P.; Shi, W. A secure chaotic maps-based key agreement protocol without using smart cards. *Nonlinear Dyn.* **2012**, *70*, 2401–2406. [CrossRef]
49. Islam, S.K.H. Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps. *Nonlinear Dyn.* **2014**, *78*, 2261–2276. [CrossRef]

50. Jiang, Q.; Wei, F.; Fu, S.; Ma, J.; Li, G.; Alelaiwi, A. Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy. *Nonlinear Dyn.* **2015**, *83*, 2085–2101. [CrossRef]
51. Lin, H.-Y. Improved chaotic maps-based password-authenticated key agreement using smart cards. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *20*, 482–488. [CrossRef]
52. Zhu, H.; Hao, X.; Liu, H. An Efficient Authenticated Key Agreement Protocol Based on Chaotic Maps with Privacy Protection using Smart Card. *J. Inf. Hiding Multimed. Signal Process.* **2015**, *6*, 500–510.
53. Cheng, G.; Chin-Chen, C. Chaotic maps-based password-authenticated key agreement using smart cards. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 1433–1440. [CrossRef]
54. Chang, Y.-F.; Tai, W.-L.; Wu, W.-N.; Li, W.-H.; Chen, Y.-C. Comments on Chaotic Maps-Based Password-Authenticated Key Agreement Using Smart Cards. In Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2014, Kitakyushu, Japan, 27–29 August 2014.
55. Burmester, M.; de Medeiros, B.; Motta, R. Robust, anonymous RFID authentication with constant key-lookup. In Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008, Tokyo, Japan, 18–20 March 2008.
56. Chen, Y.; Chou, J.-S.; Sun, H.-M. A novel mutual authentication scheme based on quadratic residues for RFID systems. *Comput. Netw.* **2008**, *52*, 2373–2380. [CrossRef]