IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE CONSUMER TECHNOLOGY SOCIETY SECTION

Received 5 May 2022, accepted 22 June 2022, date of publication 4 July 2022, date of current version 11 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3188316

RESEARCH ARTICLE

Efficient Extended Chaotic Map-Based IBE for Industrial Environment

TIAN-FU LEE AND YI-CHIEN HUANG
Department of Medical Informatics, Tzu Chi University, Hualien 97004, Taiwan
Corresponding author: Tian-Fu Lee (jackytflee@mail.tcu.edu.tw)

This work was supported by the Ministry of Science and Technology of the Republic of China, Taiwan, under Contract MOST 106-2221-E-320-001, Contract MOST 108-2221-E-320-001, and Contract MOST 110-2221-E-320-005-MY2.

ABSTRACT Identity-based encryption is a public key-based method of encryption that enables communicating identities to use some individual and unique information, such as their physical IP addresses and MAC addresses, to identify them and as public keys. The scheme does not require the extra device to store long-term public keys. So, it is convenient for use in practical applications, including smart industry and smart manufacturing. This study develops a novel, efficient, and secure identity-based encryption scheme using an extended Chebyshev chaotic map that has recently been demonstrated to outperform traditional cryptography, including modular exponential computations or scalar multiplications on elliptic curves. Besides demonstrating that the proposed scheme satisfies the security requirements of identity-based encryption, the simulation results of this study show that the proposed scheme requires less response time than related identity-based encryption schemes. Due to hardware limitations, not all industrial devices can load heavy computations. Therefore, the proposed identity-based encryption scheme outperforms related identity-based encryption approaches, and is suitable for industrial environment.

INDEX TERMS Public key infrastructure, chaotic map, identity-based encryption, industry, information security.

I. INTRODUCTION

In the concept of public key infrastructure (PKI), a certificate authority (CA) is responsible for binding a public key to an entity's corresponding identity. Bindings are established through the process of enrolling and issuing certificates. The CA may delegate the responsibility of a Registration Authority (RA) to handle the certificate issuance process, including the authenticity of the identity information contained in certificates signed by the certificate authority, to ensure valid and correct registrations. For industrial or smart manufacturing PKI, RA needs to be able to model and re-model production processes while maintaining the level of security required creating trusted device identities directly on the production floor, and thus requires greater flexibility and robustness. Additionally, the RA must be located directly on the production line and perform authentication and certificate issuance during the production process, as shown in Fig.1. This requires registries to adopt new security approaches in terms of hardware requirements, separation of network interfaces, management functions that support the life cycle of production lines and maintenance services [1], [2].

Shamir introduced the concept of the identity-based cryptosystem in [3]. The system is an implementation of an email address-based PKI that allows entities to verify digital signatures using only public information, such as the entity's identifier. Therefore, it only instantiates identity-based signatures (IBS). Identity-based encryption (IBE) is a kind of public-key encryption, which enables entities to use some individual and unique information to identify them and as their public keys. This information may be their physical IP addresses and MAC addresses. The entities do not need equipment to store long-term public keys.

In Maurer [4] did some of the research that led to IBE scheme. In Boneh and Franklin [5] proposed an IBE scheme using Weil pairing. In the same year, Cocks [6] developed

The associate editor coordinating the review of this manuscript and approving it for publication was Saif Al Zahir.

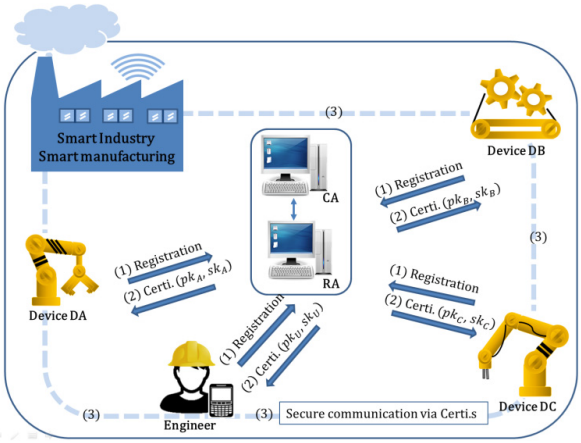

FIGURE 1. CA delegates RA to handle the certificate issuance process. Then RA is located directly on the production line and perform authentication and certificate issuance during the production process for industrial or smart manufacturing PKI.

an IBE scheme that was based on quadratic residue. In Lee *et al.* [7] proposed a new IBE scheme in which a private key is issued by a key generation center (KGC) and multiple key privacy authorities protect its privacy. Their scheme provides a secure channel in which a simple blinding technique is used for pairing-based cryptography. Such identity-based public-key cryptosystems do not require extra equipment to store long-term public keys, and so are more convenient than traditional public-key and symmetric cryptosystems for in everyday life. However, currently available IBE schemes require time-consuming modular exponential computations or scalar multiplications on elliptic curves. However, due to hardware limitations, not all industrial devices can load heavy operations. Therefore, developing an IBE scheme suitable for industrial environments is a very important research issue.

Recent research has shown that cryptosystems using operations based on Chebyshev chaotic maps are more efficient than traditional cryptosystems using modular exponential computation and scalar multiplication on elliptic curves [8]–[10]. However, Bergamo *et al.* [11] showed that public-key cryptosystems based on Chebyshev polynomials fail to exhibit the contributory property of key agreements. In Zhang [12] resolved this security weakness by enhancing the Chebyshev polynomials, and showed that enhanced Chebyshev chaotic maps have similar properties to non-enhanced ones and have the discrete logarithm, and Diffie-Hellman problems. Thus, to enhance the efficiency, many extended chaotic map-based approaches [13]–[21] have been developed for communicating protocols and use in user authentication schemes, telecare medicine information systems and other cryptosystems.

To provide a more suitable IBE solution for industrial environment, this investigation presents a novel IBE scheme by using extended Chebyshev chaotic map assumptions. The contributions of this paper are described as follows.

1) The proposed extended chaotic map-based IBE scheme does not require time-consuming modulo exponential computations or scalar multiplications on elliptic curves.
2) This investigation demonstrates that the proposed scheme satisfies the security requirements of IBE, including correctness, semantic security, and the ability to protect against privileged insider attacks.
3) The simulation results of this study show that the proposed scheme requires less response time than related IBE schemes.
4) Compared with other related schemes, the proposed IBE scheme not only retains the security requirements of identity-based encryption, but also has higher efficiency.

TABLE 1. Notation.

Notation	Description
PKG	The Private Key Generator (PKG) is a trusted third party and is responsible for generating the corresponding private keys.
pk_U/sk_U	The public/ private key pair of device U
p	A large prime number
l	A security parameter
$H(.)$	A secure one-way function and $H(\cdot):(-\infty,+\infty)\rightarrow\{0,1\}^l$
$h(.)$	A secure one-way hash function and $h(\cdot):\{0,1\}^*\rightarrow\{0,1\}^l$
$\oplus$	The exclusive-or (XOR) operation

The remainder of this investigation is organized as follows. Section II briefly reviews concepts associated with identity-based public-key cryptosystems and extended chaotic maps. Section III presents the proposed identity-based public-key cryptosystem, which uses extended chaotic maps. Section IV analyzes security and performance of the proposed IBE scheme. Final section draws conclusions.

II. PRELIMINARIES

This section introduces the relevant notation and describes the underlying primitives used in this study, including keyed hash function, enhanced Chebyshev chaotic maps, the extended chaotic map-based discrete logarithm, Diffie-Hellman problems, and the inverse assumption.

A. NOTATION

Table 1 lists the notations used in the proposed IBE scheme.

B. KEYED HASH FUNCTION

A family of keyed hash functions $H := \{H_k\}_{k\in K}$, where each H_k is a function that maps G to $\{0, 1\}^l$. Let D be an algorithm that has as inputs an element of k and an element of $\{0, 1\}^l$, and outputs a bit. The ES-advantage of D is defined as

$$|\Pr[k \in K, r \in Z_R : D(r, H_k(r)) = 1] - \Pr[h \in Z_R, r_A \in Z_R : D(r, h) = 1]|$$

and is denoted as Adv_{es}. Then, the hash H is entropy smoothing if the ES-advantage Adv_{es} of every efficient algorithm is negligible. [22]

C. ENHANCED CHEBYSHEV CHAOTIC MAPS

In Lee [10] enhanced Chebyshev polynomials and proved that the semi-group property and the commutative under composition hold on the interval $(-\infty, +\infty)$. Accordingly,

$$T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) \bmod p,$$

where $n \geq 2$, $x \in (-\infty, +\infty)$ and p is a large prime number. Then,

$$T_r(T_s(x)) \equiv T_{rs}(x) \equiv T_s(T_r(x)) \bmod p$$

holds.

The extended Chebyshev chaotic maps exhibit the discrete logarithm, and Diffie-Hellman problems [12], [15]–[18], and are described as follows.

1) EXTENDED CHAOTIC MAP-BASED DISCRETE LOGARITHM PROBLEM (DLP)

Given y, $T(\cdot)$, x and p, where $x \in (-\infty, +\infty)$ and p is a large prime number, finding an integer r that satisfies $y \equiv T_r(x) \bmod p$ is computationally infeasible. The advantage that is gained by an attacker who solves the extended chaotic map-based discrete logarithm problem is given by Adv_{dlp}, which is negligible.

2) EXTENDED CHAOTIC MAP-BASED DIFFIE-HELLMAN PROBLEM (DHP)

Given $T_r(x)$, $T_s(x)$, $T(\cdot)$, x and p, where $r, s \geq 2$, $x \in (-\infty, +\infty)$ and p is a large prime number, calculating

$$T_{rs}(x) \equiv T_r(T_s(x)) \equiv T_s(T_r(x)) \bmod p$$

is computationally infeasible.

3) EXTENDED CHAOTIC MAP-BASED INVERSE ASSUMPTION

Since the Chebyshev polynomial satisfies the semi-group property (closure and associative), given u, v, $T(\cdot)$, x and p, where $u, v \geq 2$, $x \in (-\infty, +\infty)$ and p is a large prime number, finding an integer u^{-1} that satisfies

$$T_{u^{-1}}(T_{u\cdot v}(x)) \equiv T_{u^{-1}\cdot u\cdot v}(x) \equiv T_v(x) \bmod p$$

is computationally infeasible. The advantage that is gained by an attacker who violates the extended chaotic map-based inverse assumption is given by Adv_{inv}, and which is negligible.

III. PROPOSED ID-BASED ENCRYPTION SCHEME USING EXTENDED CHAOTIC MAPS FOR INDUSTRIAL ENVIROMENT

This section presents the proposed efficient IBE scheme that is based on extended chaotic maps. Figure 2 depicts the proposed scheme, which consists of setup, extraction, encryption and decryption phases, as follows.

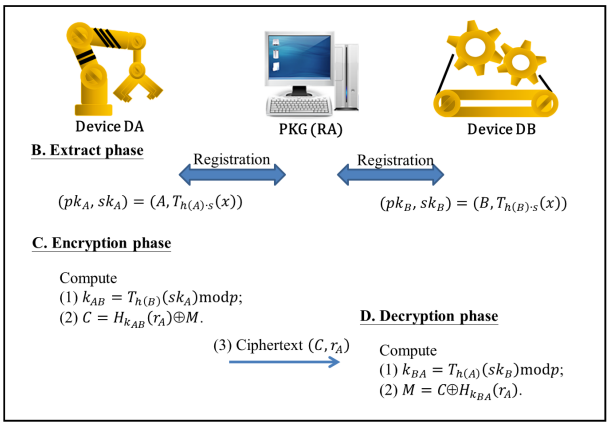

FIGURE 2. The encryption and decryption processes of the proposed IBE scheme for Industrial Environments.

A. SETUP PHASE

(1) The PKG randomly specifies a random number s as its master key and the Chebyshev chaotic maps $T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) \bmod p$, where $n \geq 2$, $x \in (-\infty, +\infty)$ and p is a large prime number.

(2) The PKG also specifies two hash functions $h(\cdot) : \{0,1\}^* \rightarrow \{0,1\}^l$ and $H(\cdot) : (-\infty, +\infty) \rightarrow \{0,1\}^l$, where l is security parameter.

B. EXTRACT PHASE

A device DA registers its identity A to the PKG and gets its public/ private key pair

$$(pk_A, sk_A) = (A, T_{h(A)\cdot s}(x) \bmod p).$$

Similarly, a device DB registers its identity B to the PKG and gets his public/ private key pair

$$(pk_B, sk_B) = (B, T_{h(B)\cdot s}(x) \bmod p).$$

C. ENCRYPTION PHASE

The device DA now encrypts the plaintext M by performing the following steps.

(1) DA computes $k_{AB} = T_{h(B)}(sk_A) \bmod p$ by using its private key sk_A and B's identity B.

(2) DA computes $C = H_{k_{AB}}(r_A) \oplus M$, where r_A is a random number or a timestamp.

(3) The resulting ciphertext (C, r_A) is sent to the device DB.

D. DECRYPTION PHASDE

The receiver DB decrypts the ciphertext (C, r_A) and gets the plaintext M by using the following steps.

(1) DB computes $k_{BA} = T_{h(A)}(sk_B) \bmod p$ by using its private key sk_B and and DA's identity A.

(2) DB obtains M by computing $M = C \oplus H_{k_{BA}}(r_A)$.

E. EXAMPLE

1) SETUP PHASE

(1) The PKG specifies its master key $s = 35$ and the Chebyshev chaotic maps

$$T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) \bmod p,$$

where $n \geq 2$, $x = 65$ and $p = 101$.

(2) The PKG also specifies two hash functions $h(\cdot)$ and $H(\cdot)$.

2) EXTRACTION PHASE

Device DA registers its identity $A =$ "192.168.22.1" to the PKG. Then PKG computes $h(A) = h(\text{"192.168.22.1''}) = 29$ and $sk_A = T_{h(A)}(T_s(x)) \bmod p = T_{29}(10) \bmod 101 = 88$, where $T_s(x) \equiv T_{35}(65) \bmod 101 = 10$, and sends key pair $(pk_A, sk_A) = (A, 88)$ to DA through a secure channel. Similarly, DB registers its identity $B =$ "192.168.22.2" to the PKG. PKG computes $h(B) = h(\text{"192.168.22.2"}) = 53$ and $sk_B = T_{h(B)}(T_s(x)) \bmod p = T_{53}(10) \bmod 101 = 98$, and sends key pair $(pk_B, sk_B) = (B, 98)$ to DB through a secure channel.

3) ENCRYPTION PHASE

The sender DA can now encrypt the plaintext $M = 87$ by performing the following steps.

(1) Device DA computes $k_{AB} = T_{h(B)}(sk_A) \bmod p = T_{53}(88) \bmod 101 = 34$ by using her private key $sk_A = 88$ and DB's identity B.

(2) DA computes

$$\begin{aligned} C &= H_{k_{AB}}(r_A) \oplus M = H_{34}(20180908) \oplus 87 = 69 \oplus 87 \\ &= 01000101_2 \oplus 01010111_2 = 00010010_2 \\ &= 18, \end{aligned}$$

where $r_A = 20180908$ is the timestamp.

(3) The resulting ciphertext $(C, r_A) = (18, 20180908)$ is sent to DB.

4) DECRYPTION PHASE

The receiver DB decrypts the ciphertext (C, r_A) and obtains the plaintext M by performing the following steps.

(1) DB computes $k_{BA} = T_{h(A)}(sk_B) \bmod p = T_{29}(98) \bmod 101 = 34$ by using his private key $sk_B = 98$ and DA's identity A.

(2) DB obtains M = 87 by computing

$$\begin{aligned} M &= C \oplus H_{k_{BA}}(r_A) = 0010010_2 \oplus H_{34}(20180908) \\ &= 00010010_2 \oplus 01000101_2 = 01010111_2 \\ &= 87. \end{aligned}$$

IV. SECURITY AND PERFORMANCE ANALYSES

This section provides security analyses of the proposed scheme, in terms of correctness and the semantic security, and the ability to protect against privileged insider attacks, and compares its performance with that of other related schemes.

A. SECURITY ANALYSES

1) CORRECTNESS

In the encryption phase of the proposed scheme, DA computes k_{AB} by using his/her private key sk_A and DB's identity B, where

$$\begin{aligned} k_{AB} &\equiv T_{h(B)}(sk_A) \equiv T_{h(B)}(T_{h(A)\cdot s}(x)) \\ &\equiv T_{h(B)\cdot h(A)\cdot s}(x) \bmod p. \end{aligned}$$

Next, DA sends (C, r_A) to DB, where $C = H_{k_{AB}}(r_A) \oplus M$. In the decryption phase, DB computes k_{BA} by using its private key sk_B and DA's identity A, where

$$\begin{aligned} k_{BA} &\equiv T_{h(A)}(sk_B) \equiv T_{h(A)}(T_{h(B)\cdot s}(x)) \\ &\equiv T_{h(A)\cdot h(B)\cdot s}(x) \bmod p. \end{aligned}$$

Thus, $k_{BA} = k_{AB}$ holds.

Additionally,

$$\begin{aligned} C \oplus H_{k_{BA}}(r_A) &= (H_{k_{AB}}(r_A) \oplus M) \oplus H_{k_{BA}}(r_A) \\ &= H_{k_{AB}}(r_A) \oplus H_{k_{BA}}(r_A) \oplus M \\ &= M. \end{aligned}$$

Therefore, the DB can get the correct plaintext M by using its private key.

2) PROVIDING SEMANTIC SECURITY

The following theorem establishes that the proposed encryption scheme has semantic security if the used keyed hash is entropy-smoothing and the extended chaotic map-based discrete logarithm and inverse assumptions hold.

Theorem 1: Let Adv_{es} be the advantage that is gained by an adversary who breaks the keyed hash function; let Adv_{dlp} denote the advantage that is gained by an adversary who solves the extended chaotic map-based DL problem; and let Adv_{inv} be the advantage that is gained by an adversary who violates the extended chaotic map-based inverse assumption. The advantage that is gained by an adversary who breaks the semantic security of the proposed encryption scheme is,

$$Adv^{sem}_{id\_encrption} \leq 2 \cdot Adv_{dlp} + 2 \cdot Adv_{inv} + 2 \cdot Adv_{es} + \frac{1}{2^{l-1}}.$$

Proof: Assume that game G_i is the probability of the event $\boldsymbol{E_i}$ that the adversary wins this game. Game $\mathbf{G}_3$ is the terminal game and concludes with the adversary's having a negligible advantage in breaking the semantic security of the proposed IBE scheme.

Game $\mathbf{G}_0$: This game corresponds to the real attack against the proposed IBE scheme. E_0 is defined as the event that $b = \hat{b}$ in game $\mathbf{G}_0$.

Game $\mathbf{G}_1$: $\mathbf{G}_0$ is transformed into game $\mathbf{G}_1$ by computing $h(B)$ by simply random selection h_B, rather than using a hash. Then, games $\mathbf{G}_0$ and $\mathbf{G}_1$ are mutually indistinguishable except with respect to collisions of the used hash functions. According to the birthday paradox [22] and the Difference Lemma [23],

$$|\Pr[E_0] - \Pr[E_1]| \leq \frac{1}{2^l}. \tag{1}$$

Game $\mathbf{G}_2$: $\mathbf{G}_1$ is transformed into game $\mathbf{G}_2$ by computing $T_s(x) \bmod p$ by simply random selection R_S, rather than as a series of extended chaotic maps. Accordingly,

$$|\Pr[E_1] - \Pr[E_2]| \leq Adv_{dlp}, \tag{2}$$

where Adv_{dlp} is the advantage that is provided by some efficient algorithms and is negligible under the extended chaotic map-based DL.

Game $\mathbf{G}_3$: $\mathbf{G}_2$ is transformed into game $\mathbf{G}_3$ by simply random selection k_{AB} rather than as a series of extended chaotic maps. Accordingly,

$$|\Pr[E_2] - \Pr[E_3]| \leq Adv_{inv}, \tag{3}$$

where Adv_{inv} is the advantage that is provided by some efficient algorithms and is negligible under the extended chaotic map-based inverse assumption.

Game $\mathbf{G}_4$: Game$\mathbf{G}_3$ is transformed into game$\mathbf{G}_4$ by simply choosing H at random rather than as a key hash. Then,

$$|\Pr[E_3] - \Pr[E_4]| \leq Adv_{es}, \tag{4}$$

where Adv_{es} is the ES-advantage that is provided by some efficient algorithms and is negligible if H is assumed to be entropy-smoothing.

Assume that the challenger A_{chao} attempts to violate the extended chaotic map-based discrete logarithm assumption or the extended chaotic map-based inverse assumption, and the adversary A is constructed to break the semantic security of the proposed encryption scheme. A_{chao} flips an unbiased coin $b \in \{0, 1\}$ and returns the encryption of M_b to the adversary A. Then A outputs its guess bit b' and wins if $b' = b$. If A outputs b, then A_{chao} outputs 1; otherwise, it outputs 0.

Since all r_A and $H_{kAB}(r_A)$ are random and independent, and no knowledge about b is leaked,

$$\Pr[E_4] = \frac{1}{2}. \tag{5}$$

Merging Eqs. (1), (2), (3), (4) and (5) and applying the Difference Lemma [22] yields,

$$\Pr[E_0] \leq 2 \cdot Adv_{dlp} + 2 \cdot Adv_{inv} + 2 \cdot Adv_{es} + \frac{1}{2^{l-1}}. \tag{6}$$

The proof is thereby concluded. □

3) PROTECTING AGAINST INSIDER ATTACKS

The following theorem indicates that the proposed encryption scheme withstands attacks by privileged insiders if the extended chaotic map-based DL and inverse assumptions hold.

Theorem 2: The proposed scheme withstands attacks by privileged insiders.

Proof: Assume that a legitimate adversary A_E whose identity is E has the public/ private key pair $(pk_E, sk_E) = (E, T_{h(E)\cdot s}(x) \bmod p)$, and attempts to derive the plaintext M from the ciphertext (C, r_A) that was encrypted by Alice, the public/ private key pair (pk_E, sk_E) and public information, where $k_{AB} \equiv T_{h(B)}(sk_A) \equiv T_{h(A)}(sk_B) \equiv T_{h(A)\cdot h(B)\cdot s}(x) \bmod p$, $C = H_{k_{AB}}(r_A) \oplus M$ and r_A is a random number or a timestamp. Then A_E must have the secret k_{AB}. Since A_E has no the knowledge of sk_A, sk_B and the PKG's secret key s, he/she has s or $T_s(x) \bmod p$.

(1) A_E endeavors to derive the PKG's secret key s from the public/ private key pair (pk_E, sk_E) and public information $T(\cdot)$, x and p. Let x_0 be $T_{h(E)}(x) \bmod p$. Now, $sk_E \equiv T_{h(E)\cdot s}(x) \equiv T_s(T_{h(E)}(x)) \equiv T_s(x_0) \bmod p$. Given $sk_E \equiv T_s(x_0) \bmod p$, $T(\cdot)$, x_0 and p, finding an integer s' that satisfies $sk_E \equiv T_{s'}(x_0) \bmod p$ is computationally infeasible owing to the extended chaotic map-based DL assumption. The advantage that is gained by an attacker who derives the PKG's secret key s is bounded by a negligible probability: Adv_{dlp}.

(2) A_E endeavors to derive $T_s(x) \bmod p$ from the public/ private key pair (pk_E, sk_E) and public information $T(\cdot)$, x and p. Finding an integer $h(E)^{-1}$ that satisfies $T_{h(E)^{-1}}(T_{h(E)\cdot s}(x)) \equiv T_{h(E)^{-1}\cdot h(E)\cdot s}(x) \equiv T_s(x) \bmod p$ is computationally infeasible on account of the extended chaotic map-based inverse assumption. The advantage that is gained by an attacker who derives $T_s(x) \bmod p$ is bounded by a negligible probability Adv_{inv}.

Accordingly, A_E fails to have s and $T_s(x) \bmod p$ because both Adv_{dlp} and Adv_{inv} are negligible. Hence, A_E cannot obtain the secret k_{AB} or the plaintext M. The advantage that is gained by an adversary who decrypts the ciphertext (C, r_A) and gets the plaintext M from (pk_E, sk_E) and public information is bounded by $(Adv_{dlp} + Adv_{inv})$, and is therefore negligible. □

TABLE 2. Computational comparison.

\ IBE schemes Computations\	Boneh&Franklin [5]	Al-Riyami&Paterson [24]	Proposed IBE
Extract phase	$1T_{ecc}$+$1T_{hash}$	$4T_{ecc}$+$1T_{hash}$	$1T_{chao}$+$1T_{hash}$
Required time	52 ms.	193 ms.	18 ms.
Encrypt phase	$1T_{pairing}$+$1T_{ecc}$ +$1T_{hash}$ +$1T_{xor}$	$1T_{pairing}$+$1T_{ecc}$ +$2T_{hash}$ +$1T_{xor}$	$1T_{chao}$+$2T_{hash}$ +$1T_{xor}$
Required time	98 ms.	103 ms.	23 ms.
Decrypt phase	$1T_{pairing}$+$1T_{hash}$ +$1T_{xor}$	$1T_{pairing}$+$1T_{hash}$ +$1T_{xor}$	$1T_{chao}$+$2T_{hash}$ +$1T_{xor}$
Required time	51 ms.	51 ms.	23 ms.

TABLE 3. Simulation environment.

Hardware/ Software specification
Intel CPU i7 CPU 3.2GHz
8G Memory
Windows 10
Scala programming language
Used Algorithms
Asymmetric en/decryption algorithm: ECC, Pairing
Symmetric en/decryption algorithm: AES
Extended Chebyshev chaotic maps
Hash function: SHA-1

B. PERFORMANCE ANALYSES

Table 2 compares the related IBE schemes and the proposed IBE schemes with respect to performance, where T_{ecc} is the time of execution of a scalar multiplication operation on an elliptic curve; $T_{pairing}$ is the time of execution of a Weil pairing operation; T_{hash} is the time of execution of a hash operation; T_{chao} is the time of execution of a Chebyshev chaotic map operation and T_{xor} is the time of execution of an exclusive-OR operation. Table 3 presents the simulation environment which includes used hardware/software specifications and algorithms.

The IBE schemes of Boneh and Franklin [5] and Al-Riyami and Paterson [24] require time-consuming scalar

multiplication operations on elliptic curves and Weil pairing operations. Only the proposed IBE scheme is developed using lightweight computations, including hash, Chebyshev chaotic map and exclusive-OR operations, and so it requires less computational time and is thus more efficient than the other approaches.

V. CONCLUSION

This investigation proposes an efficient and secure IBE scheme for industrial environment. The proposed IBE scheme is developed by using extended Chebyshev chaotic maps, and does not involve a time-consuming modular exponential operation or elliptic curve point multiplication. Thus, it is more efficient than related IBE approaches, and improves upon the current identity-based cryptosystem in terms of both convenience and computing performance. Since not all industrial devices can load heavy computations, the proposed IBE scheme is more suitable for industrial environment.

The future work will extend the proposed IBE scheme to the practical industrial environments, and generalize it to related applications, including medical information systems, smart homes, transportation systems, Internet of Things, etc.

ACKNOWLEDGMENT

The authors would like to appreciate Ted Knoy for his editorial assistance.

REFERENCES

[1] A. Philipp. *PKI in Manufacturing—Creating an Industrial PKI Registration Authority*. Accessed: Apr. 14, 2020. [Online]. Available: https://www.primekey.com/resources/pki-in-manufacturing-creating-an-industrial-pki-registration-authority/

[2] K. M. Brisch and M. M. Jung. (Jul. 2017). *Industry 4.0: The Authentication of Things Within the Internet of Things—PKI as a Solution Approach*. Dotmagazine. [Online]. Available: https://www.dotmagazine.online/issues/digital-production/blockchain-and-Iot/industry-4-0-the-authentication-of-things-within-the-internet-of-things-pki-as-a-solution-approach

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology (CRYPTO)* (Lecture Notes in Computer Science), vol. 196, CA, USA, 1984, pp. 47–53.

[4] U. M. Maurer, "Protocols for secret key agreement by public discussion based on common information," in *Advances in Cryptology (CRYPTO)*, CA, USA, 1992, pp. 461–470.

[5] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology (CRYPTO)*. 2001, pp. 213–229.

[6] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Proc. 8th IMA Int. Conf. Cryptogr. Coding*, 2001, pp. 360–363.

[7] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, "Secure key issuing in ID-based cryptography," in *Proc. ACSW Frontiers 2nd Workshop Australas. Inf. Secur., Data Mining Web Intell., Softw. Internationalisation*, vol. 32, 2004, pp. 69–74.

[8] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps," in *Proc. Int. Symp. Circuits Syst.*, vol. 3, May 2003, pp. III-28–III-31.

[9] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*. Boca Raton, FL, USA: CRC Press, 2003.

[10] T. F. Lee, "Efficient three-party authenticated key agreements based on Chebyshev chaotic map-based Diffie–Hellman assumption," *Nonlinear Dyn.*, vol. 81, no. 4, pp. 2071–2078, Aug. 2015.

[11] P. Bergamo, P. D'Arco, A. de Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 7, pp. 1382–1393, Jul. 2005.

[12] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos Soliton Fract.*, vol. 37, no. 3, pp. 669–674, 2008.

[13] Y. Niu and X. Wang, "An anonymous key agreement protocol based on chaotic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 4, pp. 1986–1992, Apr. 2011.

[14] C. Guo and C.-C. Chang, "Chaotic maps-based password-authenticated key agreement using smart cards," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 6, pp. 1433–1440, Jun. 2013.

[15] C.-C. Lee, C.-L. Chen, C.-Y. Wu, and S.-Y. Huang, "An extended chaotic maps-based key agreement protocol with user anonymity," *Nonlinear Dyn.*, vol. 69, nos. 1–2, pp. 79–87, Jul. 2012.

[16] C.-C. Lee and C.-W. Hsu, "A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps," *Nonlinear Dyn.*, vol. 71, nos. 1–2, pp. 201–211, Jan. 2013.

[17] M. S. Farash and M. A. Attari, "An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps," *Nonlinear Dyn.*, vol. 77, nos. 1–2, pp. 399–411, Jul. 2014.

[18] T.-F. Lee, C.-Y. Lin, C.-L. Lin, and T. Hwang, "Provably secure extended chaotic map-based three-party key agreement protocols using password authentication," *Nonlinear Dyn.*, vol. 82, nos. 1–2, pp. 29–38, Oct. 2015.

[19] D.-C. Lou, T.-F. Lee, and T.-H. Lin, "Efficient biometric authenticated key agreements based on extended chaotic maps for telecare medicine information systems," *J. Med. Syst.*, vol. 39, no. 5, p. 58, Mar. 2015.

[20] T. F. Lee, "Efficient and secure temporal credential-based authenticated key agreement using extended chaotic maps for wireless sensor networks," *Sensors*, vol. 15, no. 7, pp. 14960–14980, Jun. 2015.

[21] A. Irshad, M. Sher, S. A. Chaudhary, H. Naqvi, and M. S. Farash, "An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging registration centre," *J. Supercomput.*, vol. 72, no. 4, pp. 1623–1644, Apr. 2016.

[22] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password-based authenticated key exchange protocols using Diffie-Hellman," in *Advances in Cryptology (Eurocrypt)*, Bruges, Belgium, 2000, pp. 156–171.

[23] V. Shoup. (2005). *Sequences of Games: A Tool for Taming Complexity in Security Proofs*. [Online]. Available: http://www.shoup.net

[24] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology (ASIACRYPT)*, Taipei, Taiwan, 2003, pp. 452–473.

TIAN-FU LEE received the B.S. degree in applied mathematics from the National Chung Hsing University, Taiwan, in 1992, the M.S. degree in computer science and information engineering from the National Chung Cheng University, Taiwan, in 1998, and the Ph.D. degree from the Department of Computer Science and Information Engineering, National Cheng Kung University, Taiwan, in 2008. He is currently a Professor with the Department of Medical Informatics, Institute of Medical Sciences, Tzu Chi University. His research interests include cryptography, network security, medical information security, wireless networks, sensor networks, and HIPAA privacy/security regulations.

YI-CHIEN HUANG received the M.S. degree from the Department of Medical Informatics, Tzu Chi University. He is currently a Research Assistant with the College of Medicine, Tzu Chi University. His research interests include network security, medical information security, and HIPAA privacy/security regulations.