A strongly secure PF-CL-AKA protocol with two-way ID-based authentication in advance for smart IoT devices

Zhishuo Zhang¹, Yu Sun², Wei Zhang¹, Yi Wu¹, Zhiguang Qin¹

¹University of Electronic Science and Technology of China (UESTC), Chengdu, China
²Fujian Normal University, Fujian, China

E-mail: qinzg@uestc.edu.cn

Abstract. With the rapid advancements of semiconductor technologies and wireless communication, Internet-of-Things (IoT) based network has a wider range adoption in the smart city. The Wireless Body Area Network (WBAN) is a representative IoT based network designed to connect various wearable IoT devices, located inside or outside of a human body. The WBAN typically connects itself to the mobile network and Internet via the smartphones. But how to mutually authenticate the entities’ identities and ensure the data confidentiality and integrity during the data transmission over a channel have still been the most prominent challenge in the IoT based networks. To solve the abovementioned challenge, in this paper, we propose a strongly secure pairing-free certificateless authenticated key agreement (PF-CL-AKA) protocol with two-way identity-based authentication before extracting the secure session key for the smartphones and wearable IoT devices. Our protocol is provably secure in the Lippold model, which means our protocol is still secure as long as each party of the channel has at least one uncompromised partial private term.

1. Introduction

With the rapid development of sensor technologies and 5G network, IoT-based computing and communication networks have been recognized as a new wave of information paradigm after cloud computing and mobile communication networks [1], [2]. IoT-based computing and communication networks have a wider spread usage in the modern smart city (e.g. Industrial Internet of Things (IIoT) [3], Internet of Vehicles (IoV) [4] and radio-frequency identification (RFID) networks). Wireless body area network (WBAN) [5] is a predominant and representative application of IoT-based networks, which can collect the real-time vital health data through the wearable IoT devices to provide the timely health services for humans. The attending doctor can monitor the patients’ health state remotely via the WBAN and the mobile networks. The wearable IoT devices on the human bodies can detect the medical signals such as electrocardiogram (ECG), pulse rate, blood flow, temperature, photoplethysmogram (PPG), electroencephalography (EEG) and so on. The smartphones are in charge of collecting and gathering all the significant signals from the wearable IoT devices to a data package. Then the user can send the data package to the attending doctor for real-time treatment. How to ensure the data confidentiality during the data transmission between the devices and guarantee that only the authorized attending doctor can access the sensitive health data have been the prominent open issue in the WBAN and mobile networks. The figure 1 shows the common architecture of a WBAN healthcare system.
So in this paper, to overcome the above obstacle, we propose a strongly secure pairing-free certificateless authenticated key agreement (PF-CL-AKA) protocol with two-way ID-based authentication before extracting the secure session key for the smartphones and wearable IoT devices. And our protocol is provably secure in the Lippold model (Resistent to any types of impersonation attacks; Perfect forward secrecy, including KGC forward secrecy; No key-control), which means our protocol is still secure as long as each party of the channel has at least one uncompromised partial private term. What’s more, besides above, our protocol also perfectly withstand to replay attacks.

2. Related works
Shamir [6] first proposed the concept of identity-based public key cryptography (ID-based PKC) in 1984. In ID-based PKC, no certificate is required since the user’s public key is associated with the user’s identity. However, the traditional ID-based PKC will face to the key escrow problem because all the private terms in user’s private key are generated by the Key Generation Centre (KGC). To solve the key escrow problem in ID-based PKC, Al-Riyami et al. [7] introduced the pioneering work about the certificateless public key cryptosystem (CL-PKC). In CL-PKC, user’s private key is split into two parts, which are generated by the KGC and the user in private separately. Thus, CL-PKC could solve the key escrow problem.

As an important cryptographic mechanism in CL-PKC, certificateless authenticated key agreement (CL-AKA) protocol has been studied widely. By using the CL-AKA protocols, two devices can establish a secure channel to ensure the data security during data transmission over an open network. These works [8]-[14] design the CL-AKA protocols with pairings. The pairing operation is a very complicated operation [15] [16], so the pairing-based CL-AKA (PB-CL-AKA) protocols are not suitable for the resource-constrained IoT devices. Recently some works [17]-[27] build the pairing-free CL-AKA (PF-CL-AKA) protocols to improve the efficiency of the CL-AKA protocols.

The formal security model of the AKA protocols is the extended Canetti-Krawczyk (eCK) model which has been introduced in [28]. And Lippold et al. [8] first applied the eCK model for the CL-AKA protocols. They [8] also proposed a strongly secure PB-CL-AKA protocol which is provably secure in their security model (Lippold model). Though there has been proposed many PF-CL-AKA protocols in the literature [17]-[27]. But most of them [17],[18],[20],[22]-[24],[26],[27] have been pointed out not secure in the Lippold model.
3. Preliminaries

3.1. Background of elliptic curve group

Let the symbol $E_{F_p}/F_p$ denote an elliptic curve $E_{F_p}$ over a prime finite field $F_p$, defined by an equation $y^2 = x^3 + ax + b$, $a, b \in F_p$ and with the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. The points on $E_{F_p}/F_p$ together with an extra point $O$ called the point at infinity form an Abelian Group $G'$ in the point addition of the elliptic curve. Let $P$ is a point over $E_{F_p}/F_p$ with prime order $q$. Then by the point $P$, a cyclic additive subgroup $G$ of $G'$ with prime order $q$ can be generated. The point $P$ is called the generator of $G$.

There are some Diffie-Hellman problems over $G$ described as follows.

3.3.1. Computational diffie-hellman problem (CDHP). For $a, b \in Z_q^*$, given $P, aP, bP$, compute $abP$.

3.3.2. Decisional diffie-hellman problem (DDHP). For $a, b, c \in Z_q^*$, given $P, aP, bP, cP$, decide whether $c \equiv ab \mod q$.

3.3.3. Gap diffie-hellman problem (GDHP)[30]. For $a, b \in Z_q^*$, given $P, aP, bP$, compute $abP$ by accessing a DDH oracle.

3.2. Lippold security model

In this paper, we adopt the Lippold security model for our PF-CL-AKA protocol, but due to lack of space, the full description is omitted. The details of Lippold model can be found in [25],[8]. If a CL-AKA protocol is proved secure in Lippold model. That means even if an adversary corrupts at most two out of three types of secrets per party involved in the test session, the adversary still cannot extract the session key. If a CL-AKA protocol is proved secure in Lippold model, that means the protocol can capture all the basic security properties including ephemeral secrets leakage resistance (ESLR), perfect forward security (PFS), key compromise impersonation resistance (KCIR) and so on.

4. Our proposed PF-CL-AKA protocol with prior two-way ID-based authentication for the smartphones and wearable IoT devices

![Figure 2. The framework and workflow of our protocol.](image-url)
4.1. Protocol detail
In this section, we elaborate our proposed PF-CL-AKA protocol with priorly two-way ID-based authentication for the smartphones and wearable IoT devices. The framework and the workflow of our protocol is shown in Figure 2.

4.1.1 Setup. KGC executes this Setup algorithm by using the given security parameter \( \kappa \).

1. KGC chooses a finite field \( F_p \), where \( p \) is a \( \kappa \)-bit prime. Then KGC defines an elliptic curve \( E(F_p) : y^2 = x^3 + ax + b \) mod \( p \) over \( F_p \), where \( a, b \in F_p \), \( p \geq 3 \), \( 4a^3 + 27b^2 \neq 0 \) mod \( p \). KGC chooses a point \( P \) with prime order \( q \) over \( E(F_p) \) and generates a cyclic additive group \( G \) of prime order \( q \) by \( P \).

2. KGC \( k \leftarrow_{\{\kappa\}} Z_q^* \) where \( \leftarrow_{\{\kappa\}} \) means “randomly choose”. Then KGC computes \( Q = kp \).

3. KGC chooses five one-way collision-resistance hash functions as
   \[
   H_1 : \{0,1\}^* \times G \rightarrow Z_q^* \\
   H_2 : \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \rightarrow Z_q^* \\
   H_3 : G \rightarrow \{0,1\}^* \\
   H_4 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \rightarrow \{0,1\}^* \\
   H_5 : \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \rightarrow \{0,1\}^* 
   \]

4. Finally, KGC outputs the public parameters (PK) and sets the master private key (MK) as
   \[ \text{PK} = \{G, q, P, Q, H_1, H_2, H_3, H_4, H_5\}; \text{MK} = k. \]

4.1.2 Extract ID-based Private/Public Key. A device \( \beta \) sets its MAC address (\( MAC_\beta \)) as its ID (\( ID_\beta = MAC_\beta \)). Then the device \( \beta \) sends \( ID_\beta = MAC_\beta \) to the KGC. KGC extracts the ID-based private/public key for the device with \( ID_\beta = MAC_\beta \) as follows.

1. KGC \( r_\beta \leftarrow_{\{\kappa\}} Z_q^* \) and computes the ID-based public/private keys for the device with \( ID_\beta \) as
   \[ R_\beta = r_\beta P \]
   \[ s_\beta = r_\beta + H_1(ID_\beta, R_\beta) k \]

2. Finally, KGC sends the ID-based public/private keys \( \{R_\beta, s_\beta\} \) to the device with \( ID_\beta = MAC_\beta \) via a secure channel. The device \( \beta \) does the discriminant \( s_\beta P = R_\beta + H_1(ID_\beta, R_\beta) Q \) to check whether the ID-based private/public keys are valid.

4.1.3 Set self-based private/public key. Device with \( ID_\beta = MAC_\beta \) \( x_\beta \leftarrow_{\{\kappa\}} Z_q^* \) and computes \( X_\beta = x_\beta P \). Device with \( ID_\beta = MAC_\beta \) sets \( x_\beta \) as its self-based private key and outputs \( X_\beta \) as its self-based public key.

4.1.4 Key agreement with priorly two-way ID-based authentication. Device A with \( ID_A = MAC_A \) and Device B with \( ID_B = MAC_B \) interact as follows to authenticate each other and negotiate the session key. Device A owns \( \{R_A, ID_A, X_A, x_A, s_A\} \) and device B owns \( \{R_B, ID_B, X_B, x_B, s_B\} \). Suppose the key-value term \( \{ID_A; \{R_A, X_A\}\} \) is in the device B’s storage and the key-value term \( \{ID_B; \{R_B, X_B\}\} \) is in the device A’s storage.

1. Device A \( \{Y_A, e_A\} \leftarrow_{\{\kappa\}} Z_q^* \). Next exports a timestamp \( \text{Timestamp}_A \) from its OS and chooses a authentication message \( M_A \in \{0,1\}^l \). Then computes
   \[ E_A = e_A P \]
   \[ h_A = H_2(\text{Timestamp}_A, ID_A, E_A, R_A, X_A) \]
   \[ \alpha_A = \frac{Y_A}{s_A + h_A X_A} \]
   \[ K_A = Y_A(X_B + R_B + H_3(ID_B, R_B) Q) \]
\( C_A = M_A \oplus H_3(K_A) \)

\( V_A = H_4(\text{Timestamp}_A, M_A, ID_A, C_A, E_A, R_A, X_A) \)

Device A sends \( \{E_A, \text{Timestamp}_A, ID_A, \alpha_A, C_A, V_A\} \) to the device B.

(2) If \( \text{Timestamp}_A \) is valid and fresh, device B computes as follows.

\[
h'_A = H_2(\text{Timestamp}_A, ID_A, E_A, R_A, X_A) \\
K'_A = (s_B + x_B)\alpha_A (R_A + H_1(ID_A, R_A)Q + h'_A X_A) \\
M'_A = C_A \oplus H_3(K'_A)
\]

Then device B checks whether \( V_A = H_4(\text{Timestamp}_A, M'_A, ID_A, C_A, E_A, R_A, X_A) \) holds or not. If the equation holds, that means device A passes the authentication. Otherwise, device B breaks the connection to the device A.

(3) Device B \( \{y_B, e_B\} \leftarrow (R) Z^*_q \). Next exports a timestamp \( \text{Timestamp}_B \) from its OS and chooses an authentication message \( M_B \in \{0,1\}^l \). Then computes

\[
E_B = e_B^P \\
h_B = H_2(\text{Timestamp}_B, ID_B, E_B, R_B, X_B) \\
\alpha_B = \frac{s_B + h_B x_B}{y_B} \\
K_B = y_B (X_A + R_A + H_1(ID_A, R_A)Q) \\
C_B = M_B \oplus H_3(K_B) \\
V_B = H_4(\text{Timestamp}_B, M_B, ID_B, C_B, E_B, R_B, X_B)
\]

Device B sends \( \{E_B, \text{Timestamp}_B, ID_B, \alpha_B, C_B, V_B\} \) to the device A.

(4) If \( \text{Timestamp}_B \) is valid and fresh, device A computes as follows.

\[
h'_B = H_2(\text{Timestamp}_B, ID_B, E_B, R_B, X_B) \\
K'_B = (s_A + x_A)\alpha_B (R_B + H_1(ID_B, R_B)Q + h'_B X_B) \\
M'_B = C_B \oplus H_3(K'_B)
\]

Then device A check whether \( V_B = H_4(\text{Timestamp}_B, M'_B, ID_B, C_B, E_B, R_B, X_B) \) holds or not. If the equation holds, that means device B passes the authentication. Otherwise, device A breaks the connection to device B.

(5) If all the authentication passes, that means \( h'_A = h_A, h'_B = h_B, M'_A = M_A, M'_B = M_B \), devices A computes the session key as

\[
S_B = R_B + H_1(ID_B, R_B)Q \\
K_{A,1} = (x_B + h_A s_A + e_A)(X_B + h_B s_B + E_B) \\
K_{A,2} = (e_A + 2s_A - x_A)(E_B + 2s_B - X_B) \\
K_{A,3} = (e_A - s_A + 2x_B)(E_B - s_B + 2X_B) \\
\text{SeKey}_A = H_5(M_A, M_B, K_{A,1}, K_{A,2}, K_{A,3})
\]

Device B computes the session key as

\[
S_A = R_A + H_1(ID_A, R_A)Q \\
K_{B,1} = (x_B + h_A s_B + e_B)(X_A + h_A s_A + E_A) \\
K_{B,2} = (e_B + 2s_A - x_A)(E_A + 2s_B - X_A) \\
K_{B,3} = (e_B - s_B + 2x_A)(E_A - s_A + 2X_A) \\
\text{SeKey}_B = H_5(M_A, M_B, K_{B,1}, K_{B,2}, K_{B,3})
\]

It is easy to verify that \( K_{A,1} = K_{B,1}, K_{A,2} = K_{B,2}, K_{A,3} = K_{B,3} \). So \( \text{SeKey}_{AB} = \text{SeKey}_A = \text{SeKey}_B \).

4.2. Security analysis

Refer to [25], our protocol can be easily reduced to the CDHP and GDHP in the Lippold model. Due to this, our protocol can fulfill all the basic security properties. What’s more, in the process of the
priorly two-way ID-based authentication, the freshness of the two parties’ timestamp is required and the timestamps are also embedded in the session key. So our protocol can perfectly withstand the replay attacks. Due to lack of space and the similarity to [9], the full proof is omitted.

4.3. Actual performance evaluation
We use the cryptographic library MIRACL [29] to implement our protocol. The hardware for the simulation experiment is the i5-1135G7 2.4Ghz with 16GB 3200MHz RAM and OS is Windows 10 1903. To achieve the security level of 80 bits, we adopt an cyclic additive $G$ with prime order $q$ (160bits) generated by the generator point $P$ in a non-singular elliptic curve over the field $F_p$, where $p$ is also 160 bits length. We implement our protocol for five times, and we calculate the average consumption time. The average times consumed by the three processings in our protocol are listed as follows. (1) Generate the authentication message: 3.13ms, (2) Verify the authentication message to authenticate the identity of the other party: 3.23ms (3) Extract the secure session key: 4.99ms. We can easily detect that our pairing-free protocol is efficient.

![Actual Performance of Our Protocol](image)

**Figure 3.** The experiment results of our protocol.

5. Conclusion
In this paper, to overcome the security issues in WBAN and mobile networks, we propose a strongly secure PF-CL-AKA protocol with two-way ID-based authentication in advance (before extracting the secure session key) for the smartphones and wearable IoT devices. Our protocol can be proved secure in the Lippold model, which means our protocol is still secure as long as each party of the channel has at least one uncompromised partial private term. What’s more, besides above, our protocol also perfectly withstand to replay attacks. So our protocol is applicable for the WBAN and mobile networks.

Acknowledgments
This work was supported in part by NSFC with No. 61520106007, the Natural Science Foundation of China under Grant U1936101 and the 13th Five-Year Plan of National Cryptography Development Fund for Cryptographic Theory of China under Grant MMJJ20170204.
References

[1] T.-Y. Wu, Z. Lee, M. S. Obaidat, S. Kumari, S. Kumar, and C.-M. Chen, “An authenticated key exchange protocol for multi-server architecture in 5g networks,” IEEE Access, vol. 8, pp. 28 096–28 108, 2020.

[2] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, “On the security of a new ultra-lightweight authentication protocol in iot environment for rfid tags,” The Journal of Supercomputing, vol. 74, no. 1, pp. 65–70, 2018.

[3] H. Xiong, Y. Wu, C. Jin, and S. Kumari, “Efficient and privacy-preserving authentication protocol for heterogeneous systems in iot,” IEEE Internet of Things Journal, 2020.

[4] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, “Efficient certificateless aggregate signature with conditional privacy preservation in iov,” IEEE Systems Journal, 2020.

[5] J. Y. Khan, M. R. Yuce, G. Bulger, and B. Harding, “Wireless body area network (wban) design techniques and performance evaluation,” Journal of medical systems, vol. 36, no. 3, pp. 1441–1457, 2012.

[6] Shamir A (1984) Identity-based cryptosystems and signature protocols. Proc. CRYPTO1984, LNCS, Vol. 196, pp 47–53.

[7] Al-Riyami S, Paterson KG (2003) Certificateless public key cryptography. In: Proc. of ASIACRYPT 2003, LNCS 2894, Springer-Verlag, pp 452–473.

[8] Lippold G, Boyd C, Nieto J (2009) Strongly secure certificateless key agreement. In: Pairing 2009, pp 206–230.

[9] Mandt T, Tan C (2008) Certificateless authenticated two-party key agreement protocols. In: Proc. of the ASIAN 2006, LNCS, Springer-Verlag, Vol. 4435, pp 37–44.

[10] Shao Z (2005) Efficient authenticated key agreement protocol using self-certified public keys from pairings. Wuhan Univ J Nat Sci 10(1):267–270.

[11] Shi Y, Li J (2007) Two-party authenticated key agreement in certificateless public key cryptography. Wuhan Univ J Nat Sci 12(1):71–74.

[12] Swanson C (2008) Security in key agreement: Two-party certificateless protocols, Master Thesis, University of Waterloo.

[13] Wang S, Cao Z, Dong X (2006) Certificateless authenticated key agreement based on the MTI/CO protocol. J Inf Comput Sci 3:575–581.

[14] Zhang L, Zhang F, Wua Q, Domingo-Ferrer J (2010) Simulatable certificateless two-party authenticated key agreement protocol. Inf Sci 180:1020–1030.

[15] Chen L, Cheng Z, Smart NP (2007) Identity-based key agreement protocols from pairings. Int J Inf Secur 6: 213–241.

[16] Cao X, Kou W (2010) A pairing-free identity-based authenticated key agreement scheme with minimal message exchanges. Inf Sci 180:2895–2903.

[17] M. Geng and F. Zhang, “Provably secure certificateless two-party authenticated key agreement protocol without pairing,” in 2009 International Conference on Computational Intelligence and Security, vol. 2. IEEE, 2009, pp. 208–212.

[18] M. Hou and Q. Xu, “A two-party certificateless authenticated key agreement protocol without pairing,” in 2009 2nd IEEE International Conference on Computer Science and Information Technology. IEEE, 2009, pp. 412–416.

[19] G. Yang and C.-H. Tan, “Strongly secure certificateless key exchange without pairing,” in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, 2011, pp. 71–79.

[20] H. Xiong, Q. Wu, and Z. Chen, “Toward pairing-free certificateless authenticated key exchanges,” in International Conference on Information Security. Springer, 2011, pp. 79–94.

[21] S. Haiyan, W. Qiaoyan, Z. Hua, and J. Zhengping, “A strongly secure pairing-free certificateless authenticated key agreement protocol for lowpower devices,” Information Technology and Control, vol. 42, no. 2, pp. 191–204, 2013.
[22] D. He, J. Chen, and J. Hu, “A pairing-free certificateless authenticated key agreement protocol,” International Journal of Communication Systems, vol. 25, no. 2, pp. 221–230, 2012.

[23] D. He, Y. Chen, J. Chen, R. Zhang, and W. Han, “A new two-round certificateless authenticated key agreement protocol without bilinear pairings,” Mathematical and Computer Modelling, vol. 54, no. 11-12, pp. 3143–3152, 2011.

[24] D. He, S. Padhye, and J. Chen, “An efficient certificateless two-party authenticated key agreement protocol,” Computers & Mathematics with Applications, vol. 64, no. 6, pp. 1914–1926, 2012.

[25] H. Sun, Q. Wen, H. Zhang, and Z. Jin, “A novel pairing-free certificateless authenticated key agreement protocol with provable security,” Frontiers of Computer Science, vol. 7, no. 4, pp. 544–557, 2013.

[26] D. Tong, J. Liu, K. Mao, and L. Zhang, “Certificateless and pairing-free key agreement scheme for satellite network,” 2014.

[27] H. Tu, N. Kumar, J. Kim, and J. Seo, “A strongly secure pairing-free certificateless authenticated key agreement protocol suitable for smart media and mobile environments,” Multimedia Tools and Applications, vol. 74, no. 16, pp. 6365–6377, 2015.

[28] LaMacchia BA, Lauter K, Mityagin A (2007) Stronger security of authenticated key exchange. In: Proc. of the ProvSection 2007. LNCS, Springer-Verlag, Vol. 4784, pp 1–16.

[29] Shamus Software Ltd. MIRACL Library. [Online]. Available: http://www.shamus.ie/index.php?page=home, accessed May 1, 2015.

[30] D. Boneh, C. Gentry, B. Lynn, H. Shacham et al., “A survey of two signature aggregation techniques,” 2003.