An improved authentication scheme for Internet of things

Zhongliang Xie\textsuperscript{1,2} and Lingyun Jiang\textsuperscript{1,2,}\
\textsuperscript{1}Institute of Internet of Things, Nanjing University of Posts and Telecommunications, China\textsuperscript{2}Institute of Communication Technology, Nanjing University of Posts and Telecommunications, China

Abstract. Designing a secure authentication scheme is of great importance to the practical applications of the Internet of Things (IoT). In 2017, Wang et al. proposed an improved mutual authentication scheme for the embedded devices and a server over Kalra et al.’s and Chang et al.’s. And they provided a formal proof for their scheme. However, their scheme is still insecure and cannot resist against key compromise impersonation (KCI) attack. In the paper, we first demonstrate the shortcoming of Wang et al.’s scheme, and then we carry out an improvement over Wang et al.’s scheme to address the revealed issue by using an auxiliary server. Keywords. Authentication, Cryptanalysis, Elliptic curve cryptography, Internet of Things

1. Introduction
The Internet of Things (IoT) is considered to be the technological and economic wave of the global information industry after the Internet \cite{1}. The use of IoT applications \cite{2-5} brings many conveniences to people. In these IoT applications, the things can collect sensitive information from the environment, which is then used to analyze and make decisions \cite{6}. However, the security issues of the IoT are more challenging than that of the traditional Internet \cite{7}. Most of the IoT devices are resource-constrained, and it is difficult to implement complex encryption algorithms on them. If the security issues cannot be addressed, it will hinder the massive use of IoT applications \cite{8}. Therefore, it is important to design a secure and lightweight authentication scheme for the IoT.

Traditional Public Key Cryptosystems (PKC) have to deal with the distribution and management of certificates which are too complex to be utilized for the IoT devices \cite{9}. In 1984, Shamir \cite{10} first introduced the idea of ID-based cryptosystems (IBC). IBC avoid time-consuming and complex certificate mechanisms by using the entity's ID or email address as its public key, which are suitable for IoT scenarios. An ID-based cryptosystem often uses elliptic curve cryptography (ECC \cite{11}) for the reason that ECC can obtain the same security strength with a smaller key size \cite{12}. Truong et al. \cite{13} proposed an ID-based authentication for mobiles on ECC. Liao et al. \cite{14} proposed a secure ECC-based RFID authentication scheme. The scheme is integrated with ID-verifier transfer protocol. Shah et al. \cite{15} used a variant of the three-way authentication mechanism to authenticate the IoT device and the server. They used the secure vault to store keys and change the secure vault according to the data exchanged between the server and the device after every session. Yao et al. \cite{16} proposed a lightweight attribute-based encryption scheme for the IoT on ECC. Aman et al. \cite{17} proposed a mutual authentication scheme for the IoT systems using physical unclonable functions. Hao et al. \cite{18}...
proposed a collaborative PHY(physical-layer)-Aided technique for end-to-end IoT devices. They used the devices’ unique PHY features (carrier frequency offset (CFO), in-phase/quadrature-phase imbalance (IQI)) and the collaboration of several intermediate nodes to achieve an elevated resistance to computation-based attacks.

In 2015, Kalra et al. [19] proposed a lightweight authentication scheme by using elliptic curve cryptography. In their scheme, they implement mutual authentication between the embedded devices and the cloud server. However, Chang et al. [20] found that Kalra et al.’s scheme cannot achieve mutual authentication and the server cannot calculate the session key, so Chang et al. proposed an improved scheme to address these problems. In 2017, Wang et al. [21] found that Chang et al.’s improved scheme is still insecure. The adversary can impersonate the server to communicate with the device and can further obtain session keys which may bring huge damage (Kalra et al.’s scheme cannot withstand this attack as well). Therefore, Wang et al. proposed a modified scheme to solve the problem and gave a formal proof for their improved scheme. However, Wang et al.’s scheme is still not safe. In this paper, we demonstrate that Wang et al.’s scheme cannot resist against key compromise impersonation (KCI) attack [22]. The adversary can impersonate the legitimate device to communicate with the server. And we offer an improved scheme to address the revealed issue without losing the security features and advantages of the Wang et al.’s scheme.

The paper is organized as follows. Section II reviews Wang et al.’s scheme. Section III shows the insecurity of Wang et al.’s scheme. Section IV is our improved scheme and the analysis of it. Section V compares our scheme with relevant schemes. Section VI presents the conclusion.

2. Review Wang et al.’s scheme

In this section, we review the scheme proposed by Wang et al. Some intuitive notations are listed in table 1.

| Notations and descriptions |
|-----------------------------|
| $D_i$ | $i$ th device |
| $S$ | the server |
| $A$ | the adversary |
| $ID_i$ | identity of device $D_i$ |
| $H(.)$ | A one-way hash function maps any string to a $l_H$-bit long string. (i.e., $H: \{1\}^* \rightarrow \{1\}^{l_H}$) |
| $h(.)$ | A one-way hash function maps any string to a $l_h$-bit long string. (i.e., $h: \{1\}^* \rightarrow \{1\}^{l_h}$) |
| $O$ | point at infinity |
| $G$ | generator point of order $n$, (i.e., $n \cdot G = O$) |
| EXP_Time | expiration time for a specific device |
| $X$ | secret key of the server |
| $SK$ | session key |

2.1. System initialization phase

Before the system begins, the server $S$ selects a secret key $X$ with $l_h$-bit long, a one-way hash function $H(.)$, an elliptic curve $E$ and a generator $G$ on $E$. And then $S$ publishes $(H(.), E, G)$ as system parameters and keeps the key $X$ secret.

2.2. Registration phase

In this phase, the embedded device $D_i$ is registered with the server $S$. $D_i$ sends its $ID_i$ to $S$. Then $S$ calculates
\[
CK = h(R_i \| X \| EXP\_Time \| ID_i)
\]
(1)
\[
CK' = CK \times G
\]
(2)
\[
T_i = R_i \oplus H(X)
\]
(3)
\[
A_i = h(R_i \oplus H(X) \| CK')
\]
(4)
\[
A_i' = A_i \times G
\]
(5)

where \(R_i\) is a random \(l_H\)-bit string generated by \(S\). \(S\) stores \(\{A_i', T_i, ID_i, EXP\_Time\}\) in its database and sends \(CK'\) back to the device via a secure channel. Upon receiving \(CK'\) from \(S\), the device \(D_i\) securely stores \(ID_i\) and \(CK'\).

### 2.3. Login and authentication phase

| Embedded Device | Server |
|-----------------|--------|
| Registration    | \(ID_i\) | Generate a random \(l_H\)-bit string \(R_i\) and Compute |
|                 |         | CK = h(R_i \| X \| EXP\_Time \| ID_i) |
|                 |         | CK' = CK \times G |
|                 |         | \(T_i = R_i \oplus H(X)\) |
|                 |         | \(A_i = h(R_i \oplus H(X) \| CK')\) |
|                 |         | \(A_i' = A_i \times G\) |
| Securely store   | \(CK'\) | Store \(\{A_i', T_i, ID_i, EXP\_Time\}\) in a database |

#### Login and Authentication

Choose a random \(N_1 \in [2, 2^H]\) and Compute

\[
P_1 = N_1 \times G
\]
(6)
\[
P_2 = H(P_1 \| N_1 \times CK')
\]
(7)
Compute \(P_1 = T_i \oplus H(X)\). \(S\) searches its database to get the record of \(D_i\) by exploiting \(ID_i\). \(S\) reconstructs \(CK\) with the help of \(T_i\), \(EXP\_Time\), \(X\) and calculates \(P_1' = H(P_1 \| CK \times P_i)\), and rejects if \(P_1' \neq P_1\).

Choose a random \(N_2 \in [2, 2^H]\) and Compute

\[
P_3 = N_2 \times G
\]
\[
P_4 = H(P_2 \| N_2 \times A_i')
\]
Compute \(T_i, P_1, P_2\)

\[
A_i = h(T_i \| CK')
\]
\[
P_1' = H(P_1 \| A_i \times P_i)
\]
Rejects if \(P_1' \neq P_1\)

\[
V_1 = H(P_1' \| N_1 \times P_1)
\]
SK = \(H(P_2 \| N_2 \times P_1)\)
Rejects if \(V_1 \neq V_1\) and calculates

### Figure 1. The scheme of Wang et al.

When \(D_i\) wants to login to \(S\), it chooses a random number \(N_1\) with \(l_H\)-bit long. It then computes

\[
P_1 = N_1 \times G
\]
(6)
\[
P_2 = H(P_1 \| N_1 \times CK').
\]
(7)

\(D_i\) sends \(P_1\) and \(P_2\) to \(S\) along with its ID \(ID_i\). \(S\) searches its database to get the record of \(D_i\) by exploiting \(ID_i\). \(S\) reconstructs \(CK\) with the help of \(T_i\), \(EXP\_Time\), \(X\) and calculates \(P_2' = H(P_1 \| CK \times P_i)\), and rejects if \(P_2' \neq P_2\). Then, \(S\) chooses a random number \(N_2\) with \(l_H\)-bit long and calculates
\[ P_3 = N_2 \times G \]  
\[ P_4 = H(P'_2 \| N_2 \times A'_i) \]  
\{ T_i, P_3, P_4 \} are delivered to \( D_i \). \( D_i \) computes \( A_i = h(T_i \| C K') \) and \( P'_4 = H(P_2 \| A_i \times P_3) \) and rejects if \( P_4 \neq P'_4 \). Then \( D_i \) computes

\[ V_i = H(P'_4 \| N_1 \times P_3) \]  
\[ SK = H(P'_3 \| N_1 \times P_3) \]  
\( V_i \) is transmitted to \( S \). \( S \) computes \( V'_i = H(P_i \| N_2 \times P_1) \) and compares \( V'_i \) with the received \( V_i \). If \( V'_i = V_i \), \( S \) accepts the device \( D_i \)'s login request and keeps the session key \( SK = H(P_3 \| N_2 \times P_1) \), otherwise rejects. The specific scheme of Wang et al. is shown in figure 1.

3. Analysis of the Wang et al.'s scheme

In this section, we demonstrate Wang et al.'s scheme cannot withstand a realistic attack, namely key compromise impersonation (KCI) attack. In the case of KCI attack [22], if the adversary \( A \) gets the key of a communicating party, it can impersonate the compromised party to communicate with the other parties, or impersonates the other parties to communicate with the compromised party. A scheme that free from this form of "reverse impersonation" is said to resist against KCI attack, that is, in the scheme, the adversary \( A \) can only use the key to impersonate the compromised party.

Here, we show the damages of KCI attack. If the adversary \( A \) impersonates the device \( D \) to communicate with the server, it may send some false information to the server, causing the server to fail to make the right decisions (e.g., temperature alarms, etc.). At the same time, according to the access control policy, the data (such as some sensitive medical data) stored on the server by the device \( D \) is only accessible by the device \( D \) itself, and the server has no access rights, which is very common in practical applications. If the server is compromised, the adversary \( A \) may not be able to get the device's data, but if the adversary \( A \) impersonates the device \( D \) to communicate with the server as well as gets the session key, the adversary \( A \) will get the data that the device \( D \) stored on the server.

Under the scheme of Wang et al., if the adversary \( A \) breaks into the server (e.g., using zero-day attacks like Heartbleed [23, 24]), and gets the server's secret key \( X \) and stored database information \( \{ A'_i, T_i, ID_i, EXP\_Time \} \). The adversary \( A \) can impersonate \( D_i \) as follows:

**Step 1:** The adversary \( A \) chooses a random \( N_1 \in [2, 2^h] \) and computes \( P_i = N_1 \times G \), \( P_2 = H(P'_2 \| N_1 \times C K) \), where \( C K = h(T_i \oplus H(X) \| X \| EXP\_Time \| ID_i) \times G \). Then \( A \) sends \( \{ ID_i, P_1, P_2 \} \) to the server.

**Step 2:** Upon receiving \( \{ ID_i, P_1, P_2 \} \) from \( A \), the server will find no abnormalities and sends \( \{ T_i, P_3, P_4 \} \) back to \( A \).

**Step 3:** \( A \) then computes \( A_i = h(T_i \| C K') \), \( P'_4 = H(P_2 \| A_i \times P_3) \), \( V_i = H(P'_4 \| N_1 \times P_3) \), \( SK = H(P'_3 \| N_1 \times P_3) \) and sends \( V_i \) to the server.

**Step 4:** After receiving \( V_i \), the server computes \( V'_i \) and will find \( V'_i \) equal to the received \( V_i \). So the server will accept the adversary \( A \)'s login request and computes the session key \( SK = H(P'_3 \| N_2 \times P_1) \), which is equal to the session key that \( A \) holds.

Therefore, Wang et al.'s scheme is insecure. In the KCI attack scenario, it assumes that the server was compromised, but it was discovered a long time later. This exists in real-world. For example, JPMorgan Chase's server was found to be attacked a few months later after it was compromised [25].

4. The proposed scheme
As stated in [26], when an authentication server also acts as a registry, it is impossible for the authentication server to withstand KCI attack. Inspired by the study of Camenisch et al. [27] and Wang et al. [12], we use one more server (i.e., an auxiliary server) to solve the insecure problem of Wang et al.'s scheme.

![Figure 2. A secure way to deploy servers.](image)

For security reasons, we can deploy two servers (e.g., A and B) on the same Local Area Network (LAN). Therefore, both A and B have an IP address on the LAN. In addition, one (assumed A) is also deployed on the Internet, so A also has a public IP address, and others can access A through the Internet. A firewall inside the LAN can be used to implement an access policy that only A's LAN internal IP is allowed to access B. In this way, it is impossible to access B through the Internet. As a result, it is a good choice to store important or sensitive data on B. Details can be seen in figure 2.

### 4.1. Details of the improvement

![Figure 3. Our improved scheme. The bottom of the place we modified was marked with a solid line.](image)
Figure 3 shows our improved scheme, the bottom of the place we modified was marked with a solid line. Based on the above analysis, we decided to deploy the auxiliary server $AS$ and server $S$ on the same LAN. The server $S$ has both a public IP address and a LAN IP address. We set the policy to only allow the server $S$’s LAN IP address to access the auxiliary server $AS$, and the server $S$ is restricted to only send the ID to the auxiliary server $AS$.

In the device registration phase, the server $S$ does not store $T_i$ anymore, instead, it sends $T_i$ through a secure channel to the auxiliary server $AS$ for storage together with the device’s ID $ID_i$. Besides, the server will not only send $CK'$ to the device $D_i$ over the secure channel but also send $T_i$ to the device $D_i$.

In the login and authentication phase, the server $S$ extracts the device's ID $ID_i$ from the login request and sends it to the auxiliary server $AS$ by using its LAN IP address. The auxiliary server $AS$ queries the database to get the corresponding $T_i$ based on the ID $ID_i$ and sends $ID_i,T_i$ back to the server $S$. The message that the server $S$ responds to the device $D_i$ is only $P_3,P_4$, and there will be no more $T_i$.

### 4.2. Analysis of our improved scheme

**Theorem 1:** Our improved scheme retains the security features and advantages of Wang et al.’s scheme.

**Proof:** In our proposed scheme, only the storage location of $T_i$ has been changed, that is, $T_i$ is stored in the device and the auxiliary server separately. Other than that, no change has been made elsewhere. Therefore, our scheme inherits the security features and advantages of Wang et al.’s scheme. Details of the security features and advantages of the Wang et al.’s scheme can be seen in [21].

**Theorem 2:** Our improved scheme can resist against KCI attack.

**Proof:** Now if the adversary $A$ breaks into the server $S$ and gets the server’s secret key $X$ as well as database information, but because of lacking of $T_i$, and the adversary $A$ cannot intercept $T_i$ (only $P_3,P_4$ are sent by the server $S$, no more $T_i$) from the channel, so the adversary $A$ will not be able to reconstruct $CK$, which means $A$ cannot calculate $CK'$, let alone $P_3$ and $V_i$. As a result, the adversary $A$ cannot impersonate the device $D_i$ to communicate with the server $S$, which means that the adversary $A$ will not be able to conduct KCI attack unless $A$ breaks into the auxiliary server $AS$ as well. In fact, it is almost impossible to break into two servers with different protection measures at the same time. Further, when we adopt the above deployment or other methods to ensure the security of the auxiliary server $AS$, it is impossible for the adversary $A$ to carry out KCI attack, which means that our scheme can resist against KCI attack.

### 5. Efficiency and comparison

| Schemes       | Computation overhead | Communication cost | Storage cost |
|---------------|----------------------|--------------------|--------------|
|               | Device               | Server             | Device       | Server       | Device       | Server       |
| Chang et al. [20] | $5T_p+4T_H$          | $5T_p+5T_H$        | $4L$         | $3L$         | $3L$         | $4L$         |
| Wang et al. [21]  | $5T_p+5T_H$          | $5T_p+6T_H$        | $4L$         | $3L$         | $2L$         | $4L$         |
| Ours           | $5T_p+5T_H$          | $5T_p+6T_H$        | $4L$         | $2L$         | $3L$         | $5L$         |

In this section, we compare our scheme with relevant [20] and [21]. Without loss of generality, for the sake of simplicity, here we assume that all values (device ID, the output of hash functions, points on
an ECC curve, etc.) have the same length $L$. Let $T_p$ and $T_H$ denote the time required for the ECC point multiplication and the hash operation, respectively. Other lightweight operations are ignored. Table 2 shows the results of the comparison.

As can be seen from the table, the efficiency of our scheme is slightly lower than that of Chang et al. [20] and Wang et al. [21]. But considering that our scheme solves the security flaws of their schemes, the loss of efficiency is worthwhile.

6. Conclusion
In this paper, we prove that Wang et al.'s scheme is insecure and unable to resist against KCI attack. The adversary can impersonate a legitimate device to communicate with the server, which may bring many security risks. Using an auxiliary server successfully solves the defects of Wang et al.'s scheme while retaining the security features and advantages of the Wang et al.'s scheme. In general, our improved scheme can provide greater security for the embedded devices and the server.

Acknowledgments
This work was supported by the Natural Science Foundation of China under Grant 61871446.

References
[1] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china perspective,” IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.
[2] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–43, 2014.
[3] S. Li, T. Tryfonas, and H. Li, “The internet of things: a security point of view,” Internet Research, vol. 26, no. 2, pp. 337–359, 2016.
[4] A. GhaffarianHoseini, N. D. Dahlan, U. Berardi, A. GhaffarianHoseini, and N. Makarem, “The essence of future smart houses: From embedding ict to adapting to sustainability principles,” Renewable and Sustainable Energy Reviews, vol. 24, pp. 593–607, 2013.
[5] Y. Yuehong, Y. Zeng, X. Chen, and Y. Fan, “The internet of things in healthcare: An overview,” Journal of Industrial Information Integration, vol. 1, pp. 3–13, 2016.
[6] N. Li, D. Liu, and S. Nepal, “Lightweight mutual authentication for iot and its applications,” IEEE Transactions on Sustainable Computing, vol. 2, no. 4, pp. 359–370, 2017.
[7] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “Internet of things security: a top-down survey,” Computer Networks, 2018.
[8] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, “On security challenges and open issues in internet of things,” Future Generation Computer Systems, vol. 83, pp. 326–337, 2018.
[9] D. Wang, B. Da, J. Li, and R. Li, “Ibs enabled authentication for iot in ion framework,” in Global Internet of Things Summit (GloTS), 2017. IEEE, 2017, pp. 1–6.
[10] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Workshop on the theory and application of cryptographic techniques. Springer, 1984, pp. 47–53.
[11] N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of computation, vol. 48, no. 177, pp. 203–209, 1987.
[12] D. Wang, H. Cheng, D. He, and P. Wang, “On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices,” IEEE Systems Journal, vol. 12, no. 1, pp. 916–925, 2018.
[13] T.-T. Truong, M.-T. Tran, and A.-D. Duong, “Improvement of the more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on ecc,” in 2012 26th International Conference on Advanced Information Networking and Applications Workshops. IEEE, 2012, pp. 698–703.
[14] Y.-P. Liao and C.-M. Hsiao, “A secure ecc-based rfid authentication scheme integrated with id-verifier transfer protocol,” Ad Hoc Networks, vol. 18, pp. 133–146, 2014.
[15] T. Shah and S. Venkatesan, “Authentication of iot device and iot server using secure vaults,” in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018, pp. 819–824.

[16] X. Yao, Z. Chen, and Y. Tian, “A lightweight attribute-based encryption scheme for the internet of things,” Future Generation Computer Systems, vol. 49, pp. 104–112, 2015.

[17] M. N. Aman, K. C. Chua, and B. Sikdar, “Mutual authentication in iot systems using physical unclonable functions,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1327–1340, 2017.

[18] P. Hao, X. Wang, and W. Shen, “A collaborative phy-aided technique for end-to-end iot device authentication,” IEEE Access, vol. 6, pp. 42279–93, 2018.

[19] S. Kalra and S. K. Sood, “Secure authentication scheme for iot and cloud servers,” Pervasive and Mobile Computing, vol. 24, pp. 210–223, 2015.

[20] C.-C. Chang, H.-L. Wu, and C.-Y. Sun, “Notes on secure authentication scheme for iot and cloud servers,” Pervasive and Mobile Computing, vol. 38, pp. 275–278, 2017.

[21] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, “A secure authentication scheme for internet of things,” Pervasive and Mobile Computing, vol. 42, pp. 15–26, 2017.

[22] H. Krawczyk, “Hmqv: A high-performance secure diffie-hellman protocol,” in Annual International Cryptology Conference. Springer, 2005, pp. 546–566.

[23] C. Lee, L. Yi, L.-H. Tan, W. Goh, B.-S. Lee, and C.-K. Yeo, “A wavelet entropy-based change point detection on network traffic: a case study of heartbleed vulnerability,” in Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on. IEEE, 2014, pp. 995–1000.

[24] Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey et al., “The matter of heartbleed,” in Proceedings of the 2014 conference on internet measurement conference. ACM, 2014, pp. 475–488.

[25] M. Goldstein, N. Perlroth, and D. Sanger, “Hackers’ attach cracked 10 financial firms in major assault,” The New York Times, 2014.

[26] D. Wang, N. Wang, P. Wang, and S. Qing, “Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity,” Information Sciences, vol. 321, pp. 162–178, 2015.

[27] J. Camenisch, R. R. Enderlein, and G. Neven, “Two-server password-authenticated secret sharing uc-secure against transient corruptions,” in IACR International Workshop on Public Key Cryptography. Springer, 2015, pp. 283–307.