Available online at www.sciencedirect.com
ScienceDirect
ICT Express 7 (2021) 200–204
www.elsevier.com/locate/icte

Cryptanalysis of a Pairing-free Certificateless Signcryption scheme

Philemon Kasyoka[a,b,*], Michael Kimwele[a], Shem Mbandu Angolo[c]

[a] School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya
[b] School of Information and Communication Technology, South Eastern Kenya University, Kitui, Kenya
[c] School of Computing and Mathematics, Co-operative University of Kenya, Karen-Nairobi, Kenya

Received 22 July 2019; received in revised form 20 May 2020; accepted 31 July 2020
Available online 9 August 2020

Abstract

Signcryption is a very useful cryptographic primitive that aims to achieve authentication and confidentiality in an efficient manner. We cryptanalyze the signcryption scheme of Wei and Ma (2019) which is claimed to be secure. Further, we propose a corresponding modification to show how their signcryption scheme can be made more secure in our proposed signcryption scheme. The security analysis is also applicable to other signcryption schemes with similar design.

Keywords: Certificateless; Cryptanalysis; Elliptic curve cryptography; Signcryption scheme

Contents

* Corresponding author at: School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya.
E-mail address: pkasyoka@gmail.com (P. Kasyoka).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2020.07.006
2405-9595/

1. Introduction

A conventional signcryption provides an efficient way to perform signing and encryption in a single logical process making it more efficient than signing a message then later encrypting the same message. Signcryption can come in different forms, that is, public key infrastructure (PKISC) signcryption, identity-based signcryption (IBSC) or certificateless signcryption (CLSC) [1]. The PKI makes use of a certificate authority who is in charge of generating a certificate that binds to the user's public key. Certificate Authority also maintains a certificate revocation list that issues expired or revoked certificates. Due to numerous tasks resource demanding tasks performed by the PKI, it makes PKISC, not suitable for use on resource constrained environments. To eliminate the certificates problem, IBSC notion was proposed [2,3]. The idea is that, the user's public key can be derived from arbitrary strings such as a telephone number or email address and the private keys are generated by a trusted third party called private key generator (PKG). The PKG makes use of a master secret key that is related to the system parameters. [4] noted that, the IBSC suffers from the weakness of key escrow problem where the PKG knows all the users' private keys. To overcome this weakness, the notion of CLSC scheme was proposed by [5]. In the CLSC, the user's full private key is composed of two parts: one comes from the third trust party referred to as key generation center (KGC) and another part of the key is generated by the user.

1.1. Attack model

The scheme by [6] follows a model described in [7]. We look at security from the perspective of two types of adversaries. One the Type-I adversary without possession of KGC's secret key but can replace user's public keys and is usually denoted as A_I. The other adversary is Type II adversary, the adversary represents an insider adversary who is a malicious KGC that has access to the master secret key and is usually denoted as A_{II} under unforgeability [4]. In this paper, we review a certificateless hybrid signcryption scheme proposed by [6] and show how the scheme is existentially forgeable against both Type-I and Type-II adversaries.

2. Wei and Ma signcryption scheme

The Wei and Ma [6] (hereafter called WM) signcryption scheme is comped of six probabilistic polynomial-time algorithms: setup, set secret value, extract partial private key, set private key, signcrypt, and de-signcrypt

2.1. Setup

The algorithm takes parameter λ as input and returns system parameters *params* and master key *msk*. The algorithm is run by the KGC. The setup is performed as follows:

Choose λ -bit prime p and return tuple $\{p, F_p, G_p, P\}$, where G_p is an additive cyclic group consisting point on elliptic curve over F_p and P as the generator of G_p. Choose master key $x \in Z_p^*$ and set master public key as $P_{pub} = xP$, then choose cryptographic hash functions: $H_0\{0,1\}^* XG_p \rightarrow Z_p^*$, $H_1\colon G_pXG_p \rightarrow \{0,1\}^n$, $H_2\colon G_pX\{0,1\}^* X\{0,1\}^* XG_p \rightarrow Z_p^*$ and $H_3\colon G_pX\{0,1\}^* X\{0,1\}^* XG_p \rightarrow Z_p^*$. KGC will publish system $params = \{F_p, G_p, P, P_{pub}, H_0, H_1, H_2, H_3\}$

2.2. Set secret value

The algorithm is run by $user_i$ with identity ID_i, $user_i$ randomly selects value $x_{IDi} \in Z_p^*$ and computes public key s $P_{IDi} = x_{IDi}P$.

2.3. Extract partial private key

KGC computes $d_{IDi} = xH_0(ID_i, P_{IDi})\, mod\ p$ as the partial private key and forwards d_{IDi} to user through a secure channel. When user receives d_{IDi}, $user_i$ can verify d_{IDi} by checking if $d_{IDi}P = xH_0(ID_i, P_{IDi})\, P_{pub}$ holds.

2.4. Set private key

The full private key is set as $sk_{ID} = (d_{IDi}, x_{IDi})$.

2.5. Signcrypt

A $user_i$ with identity ID_s and τ as timestamp, will execute the algorithm as follows:

Choose a random $l_{ID} \in Z_P^*$; $S_{ID} = l_{ID}P$; $H = H_2(S_{IDs}, \tau, ID_r, P_{IDs})$; $H' = H_3(S_{ID}, \tau, ID_r, P_{IDr})$; $W_{IDs} = d_{IDi} + l_{IDs} \cdot H + x_{IDs} \cdot H' mod\ p$; $T_{IDS} = l_{IDs} \cdot H_0(ID_r, P_{IDr})\, P_{pub}$; $K = H_1(T_{IDS}, l_{IDs} \cdot P_{IDr})$ and outputs $\varphi ID_s = (s_{IDs}, W_{IDs})$ and K

2.6. De-signcrypt

Given φID_s, K, signer identity ID_s and public key P_{IDs}. The decryption process proceeds as follows: $H = H_2(S_{IDs}, \tau, ID_r, P_{IDs})$, $H' = H_3(S_{IDs}, \tau, ID_r, P_{IDr})$

If $W_{IDs}P = H_0(ID_s, P_{IDs})\, P_{pub} + H \cdot S_{IDs} + H'P_{IDs}$ then the signature is valid, the receiver recover ID_r is used to compute $T_{IDS} = d_{IDr} \cdot S_{IDs}$

3. Security analysis

3.1. Unforgeability

WM [6] have claimed their scheme is existentially unforgeable against both Type-I and Type-II attacks with proof similar to Bartino [7]. We show that their scheme is insecure against both Type-I and Type-II attacks. In EUF-CMA-I and EUF-CMA-II games, A_I and A_{II} forgers have access to full private key of the receiver, A_I is not allowed to query partial private key of the sender and A_{II} is not allowed to replace public key or extract the user private key.

Type-I attack: The adversary interacts with challenger C in the training phase similar to WM [6]. A_I cannot query the private key for sender. However, A_I has access to receiver's full private key. Adversary A_I makes signcryption queries with ID_s, ID_r and arbitrary value τ. C responds to A_I with $\varphi_{IDs} = (S_{ID}, W_{IDs})$ and symmetric key $K^* = H_1(T_{IDS}, x_{IDr} \cdot S_{ID})$. Adversary obtains a forged $\varphi^*_{ID_s} = (S_{ID}, W_{IDs})$ during the training phase for the same arbitrary value τ by performing the following steps. A_I selects $x^*_A, d^*_A \in_R Z^*_P$ and replaces sender public key P_{ID_s} with $P^*_{ID_A} = x^*_A P$. The adversary will proceed to compute the master public key computed as $P^*_{pub} = H_0^{-1}(d^*_A P)$ such that $d^*_A P = H_0(ID_s, P^*_{ID_A})$ holds. A_I selects $l_{ID} \in_R Z^*_P$ and proceeds by computing $S_{ID} = l_{ID}P$; $H = H_2\left(S_{ID}, \tau, ID_s, P^*_{ID_A}\right)$; $H' = H_3(S_{ID}, \tau, ID_r, P_{IDr})$; $W_{IDs} = d^*_A + l_{ID} \cdot H + x^*_A \cdot H' mod\, p$; $T_{IDS} = d_{IDr} \cdot S_{ID}$. Finally, it will output signature $\varphi^*_{ID_s} = (S_{ID}, W_{IDs})$ and symmetric key $K^* = H_1(T_{IDS}, l_{IDs} \cdot P_{IDr})$. The signature will pass verification because $W_{IDs}P = H_0\left(ID_s, P^*_{ID_A}\right) P^*_{pub} + H \cdot S_{ID} + H' \cdot P^*_{ID_A}$ will hold. It is also noted that WM [6] scheme has a security flaw that can allow an adversary to access to KGC's master secret key x by computing $x' = d_{IDi} H_0(ID_i, P_{IDi})^{-1}$. This makes it possible to compute partial private key for a given user as $d^*_i = x' H_0(ID_i, P_{IDi})\, mod\, p$. The partial private key can be verified by checking if equation $d^*_i P = H_0(ID_i, P_{IDi})\, P_{pub}$ holds.

Type-II attack: The adversary interacts with challenger C in the training phase similar to WM [6]. A_{II} cannot query private key for sender. However, A_{II} has access to receiver's full private key. Adversary A_{II} makes signcryption queries with ID_s, ID_r and arbitrary value τ. C responds to A_{II} with $\varphi^*_{IDs} = (S_{ID}, W_{IDs})$ and symmetric key K^*. Now A_{II} has forged signature φ^*_{IDs} for arbitrary value τ obtained as follows.A_{II} computes a new key $K^* = H_1(T_{IDS}, x_{IDr} \cdot S_{ID})$ where $T_{IDS} = d_{IDr} \cdot S_{ID}$. Therefore, $\varphi^*_{IDs} = (S_{ID}, W_{IDs})$ is a valid signature of key K^* from sender ID_s and receiver ID_r. Computation of $H = H_2(S_{ID}, \tau, ID_s, P_{IDs})$ will yield the same value for signature φ^*_{IDs} or φ_{IDs}. The validity check $W_{IDs}P = H_0(ID_s, P_{IDs})\, P_{pub} + H \cdot S_{ID} + H' \cdot P_{IDs}$ will hold.

4. Proposed modification signcryption scheme

In this section we are proposing a secure and efficient scheme which is a modification of the signcryption scheme by WM [6].

4.1. Setup

Our setup is similar to WM [6] except for a change in cryptographic $H_0\{0,1\}^* XG_pXG_p \to Z^*_p$; $H_1: G_pXG_pXG_p \to \{0,1\}^n$, $H_2: G_pXG_pX\{0,1\}^* X\{0,1\}^* XG_p \to Z^*_p$ and $H_3: G_pXG_pX\{0,1\}^* X\{0,1\}^* XG_p \to Z^*_p$. KGC will publish the system $params = \{F_p, G_p, P, P_{pub}, H_0, H_1, H_2, H_3\}$

4.2. Set secret value

The algorithm is run by $user_i$ with identity ID_i, $user_i$ randomly selects value $x_{IDi} \in Z^*_p$ and computes public key s $P_{IDi} = x_{IDi}P$.

4.3. Extract partial private key

KGC will randomly select value $r_{IDi} \in Z^*_p$ and set $R_{IDi} = r_{IDi}P$ then compute partial private key as $d_{IDi} = r_{IDi} + x \cdot h_0\, mod\, p$ where h_0 is $H_0(ID_i, R_{IDi}, P_{IDi})$ as the partial private key. KGC computes value $Q_{IDi} = R_{IDi} + H_0(ID_i, R_{IDi}, P_{IDi})\, P_{pub}$ and forwards $(d_{IDi}, Q_{IDi}, R_{IDi})$ to user through a secure channel. When user receives d_{IDi}, $user_i$ can verify d_{IDi} by checking if $d_{IDi}P = R_{IDi} + H_0(ID_i, R_{IDi}, P_{IDi})\, P_{pub}$ holds.

4.4. Set private key

The full private key is set as $sk_{ID} = (d_{IDi}, x_{IDi})$.

4.5. Signcrypt

A $user_i$ with identity ID_s and τ as timestamp, will execute the algorithm as follows:

Choose a random $l_{ID} \in Z^*_P$; $S_{ID} = l_{ID}P$; $T_{IDS} = l_{IDs} \cdot Q_{IDr}$; $H = H_2(S_{ID}, T_{IDS}, \tau, ID_r, P_{IDs})$; $H' = H_3(S_{ID}, T_{IDS}, \tau, ID_r, P_{IDr})$; $W_{IDs} = d_{IDs} + l_{IDs} \cdot H + x_{IDs}$; $H' mod\, p$; $K = H_1(T_{IDS}, S_{ID}, Q_{IDr}, ID_r)$ Output $\varphi ID_s = (S_{IDs}, W_{IDs})$ and K

4.6. De-signcrypt

Given φID_s, K, signer identity ID_s and public key (Q_{IDs}, P_{IDs}). The decryption process proceeds as follows: $T_{IDS} = d_{IDr} \cdot S_{IDs}$; $H = H_2(S_{ID}, T_{IDS}, \tau, ID_r, P_{IDs})$, $H' = H_3(S_{ID}, T_{IDS}, \tau, ID_r, P_{IDr})$ If $W_{IDs}P = Q_{IDs} + H \cdot S_{IDs} + H' \cdot P_{IDs}$ then the signature is valid, the receiver computes $K = H_1(d_{IDr} \cdot S_{IDs}, Q_{IDr}, ID_r)$

Correctness

The correctness of our scheme is as follows: $T_{IDr} = l_{ID}Q_{IDr} = l_{ID}(R_{IDr} + h_0 P_{pub})$ while T_{IDr} can also be computed as $T_{IDr} = d_{IDr}S_{IDs} = l_{ID}P(r_r + xh_0) = l_{ID}\left(R_{IDr} + h_0 P_{pub}\right)$.

5. Security analysis of the proposed scheme

The security of our improved scheme is based on Elliptic Curve Discrete Logarithm (ECDL) problem. We provide a formal security proof that our proposed signcryption scheme is UF-CMA secure against Type-I and Type-II attacker in the random oracle model under ECDL assumption.

5.1. Proof of unforgeability

Theorem 2. *Our scheme is EUF-CMA secure in the random oracle model under ECDLP assumption*

Proof. We provide the proof for this theorem in Lemmas 1 and 2.

Lemma 1. *Our scheme is EUF-CMA secure under DLP assumption in random oracle model. If there exists adversary A_I with a non-negligible advantage ε that can compromise authenticity property of our scheme, then there exists algorithm C that can solve the DLP problem with advantage*

$$\Pr[C] \geq \varepsilon \frac{1}{qH_0}\left(1 - \frac{q_s(qH_2 + qH_3)}{2^k}\right).$$

Here, qH_0, qH_2 and qH_3 are the maximum number of queries to H_0, H_2 and H_3 queries respectively, while q_s and q_u represent signcryption and unsigncrypt queries respectively.

Initial After running $Setup(1^k)$, the challenger C gives the system params to adversary A_I. Value $b \in_R Z_q^*$ will be used to simulate the partial private key of the sender, therefore challenger C must solve $P = dP$ for $(Q_A = dP)$ which is an instance of DL problem. C maintains lists $L_i (i = 0, 1, 2, 3)$ for random oracles H_0, H_1, H_2 and H_3. A list L_K can be used to store private and public keys.

Training phase. In this phase hash queries are similar to theorem 1 in [8] except for H_1 query where C checks whether tuple $(T_{IDS}, S_{ID}, Q_{IDr}, ID_r, K)$ exists in L_1. If it exists, C returns K to A_I. Otherwise, it chooses $K \in \{0, 1\}^n$ return is to A_I and adds tuple $(T_{IDS}, S_{ID}, Q_{IDr}, ID_r, K)$ to list L_1.

Forgery At the end of training phase, *adversary A_I* outputs ciphertext $\sigma^* = \left(S^*_{IDs}, W^*_{IDs}, K^*\right)$ with ID^*_s and ID^*_r as sender and receiver respectively. If $ID_s \neq ID^*$ C aborts the session. Otherwise, C submits an H_2 query on $\left(S^*_{ID}, T = d_r S^*_{IDs}, ID^*_r, P^*_r\right)$ and H_3 query on $\left(S^*_{ID}, R_s, H^*, ID^*_r\right)$ to obtain another H^* and H'^* respectively. A_I will fail if any of the hash values H^* and H'^* or both are already defined in the corresponding list. The validity of ciphertext φID^*_s will determine if the adversary A_I wins the game or not.

Adversary A_I will win the game if Eq. (1) holds

$$wP = Q_{ID} + H^* S_{ID} + H'^* P_{IDs} \tag{1}$$

Using forking lemma [9] we can obtain another equation

$$wP = Q_{ID} + HS_{ID} + H' P_{IDs} \tag{2}$$

And subtract it from Eq. (1) to obtain

$$\frac{w^* - wP}{H^* - H + H'^* - H'} = (b + l_i + x_s)\, P \tag{3}$$

We can now recover value b as follows

$$b = \frac{w^* - w}{H^* - H + H'^* - H'} - (l_i + x_s)$$

The value b is a solution to our DL problem, this means C can use adversary A_I as a subroutine to obtain b from $Q_A = bP$. It is possible for C to obtain x_s from public key query and can therefore solve l_i.

Analysis The analysis is focused in the likelihood of the following independent events:

E_1: Adversary A_I does not choose to be challenged on ID^*

E_2: Adversary A_I did ask private key query on ID^*

E_3: Adversary A_I did replace public key and issued a partial private key query on ID^*

E_4: Challenger C aborts in unsigncrypt query due to rejection of a valid ciphertext.

The probability that Challenger C does not abort during this game is

$$\Pr[\neg E_1 \wedge \neg E_4] = \frac{1}{qH_0}\left(1 - \frac{q_s(qH_2 + qH_3)}{2^k}\right).$$

Therefore,

$$\Pr[C] \geq \varepsilon \frac{1}{qH_0}\left(1 - \frac{q_s(qH_2 + qH_3)}{2^k}\right).$$

Lemma 2. *Our scheme is EUF-CMA secure under ECDL assumption in random oracle model. If there exists adversary A_{II} with a non-negligible advantage ε that can compromise authenticity property of our scheme, then there exists algorithm C that can solve the ECDL problem with advantage*

$$\Pr[C] \geq \varepsilon \frac{1}{qH_0}\left(1 - \frac{q_s(qH_2 + qH_3)}{2^k}\right).$$

Here, qH_0, qH_2 and qH_3 are the maximum number of queries to H_0, H_2 and H_3 queries respectively, while q_s and q_u represent signcryption and unsigncrypt queries respectively.

Challenger C will use adversary A_{II} to solve (P, bP) which is an instance of ECDL problem. Our adversary has access to master secret key. C provides system params to our adversary including $P_{pub} = aP$ and $P_i = \lambda P$ where value λ is unknown to C. Value a is the master secret key.

Training phase. This phase is similar to Theorem 2 Lemma 1.

Forgery At the end of training phase, adversary A_{II} outputs ciphertext $\sigma^* = \left(S^*_{IDs}, W^*_{IDs}, K^*\right)$ on with ID^*_s and ID^*_r not generated by Signcrypt query. If $ID_A \neq ID^*$, challenger C aborts the session. Otherwise, C submits H_2 query on tuple $\left(S^*_{ID}, T = d_r S^*_{IDs}, ID^*_r, P^*_r\right)$ to recover value H and H_3 query on $\left(S^*_{ID}, R_s, H^*, ID^*_r\right)$ to obtain another H'. Adversary A_{II} will fail if both H and H' values already exist in the respective list.

Analysis The analysis is focused in the likelihood of the following independent events:

E_1: Adversary A_{II} does not choose to be challenged on ID^*

E_2: Adversary A_{II} did ask private key query on ID^*

E_3: Adversary A_{II} aborts during the unsigncryption query as a result of a rejected valid ciphertext during the simulation.

The rest of the analysis is similar to that of the analysis section of Lemma 1.

6. Performance evaluation of the modified scheme

In this section, we analyze the performance of our proposed access control scheme in comparison with schemes by WM [6] . As in [10] we adopt running time and energy consumption on MICA2 mote equipped with ATmega128 8-bit processor clocked at 7.3728 MHz, 4 kB RAM and 128 kB ROM. In our quantitative analysis, we will only consider operations with high computation cost such point multiplication in G_1 denoted as PM. From [11] , we know that a PM operation takes 0.81 s on an elliptic curve with 160 bits p. The signcryption algorithm of WM [6] performs 3 PM and 6 PM in the un-signcryption algorithm while our scheme takes 2 PM and 3 PM in signcryption and un-signcryption respectively. Therefore, the computational time of our modified scheme compared to the scheme by WM [6] is as follows:

- Computation time for ciphertext generation and unsigncryption in WM [6] are $3 * 0.81 = 2.43$ s and $6 * 0.81 = 4.86$ s
- The computation time for ciphertext generation and un-signcryption in our scheme is $2 * 0.81 = 1.62$ s and $3 * 0.81 = 2.43$ s respectively.

The computational time of our scheme is 33% more efficient in signcryption and 50% more efficient in un-signcryption compared to the scheme by WM [6] .

We have adopted the approach used in [12] and [11] to compute energy consumption. Given the power level of MICA2 is 3.0 V and the data rate is 12.4 kbps, we assume that the current draw in active mode is 8.0 mA, the transmitting mode is 27 mA and the current draw for receiving mode is 10 mA [12] . According to [13] a point multiplication operation consumes $3.0 * 8.0 * 0.81 = 19.44$ mJ. The overall energy computation cost of both signcryption and un-signcryption in the schemes by WM [6] and our scheme is computed as $(3 + 6) * 19.44 = 174.96$ mJ and $(2 + 3) * 19.44 = 97.2$ mJ respectively. Therefore, our scheme has reduced the energy computation cost by $(174.96 - 97.2)/174.96 = 44\%$.

7. Conclusion

In this paper, we have demonstrated that certificateless signcryption scheme proposed recently by [6] can be compromised through public key replacement and further, we have proposed how the scheme can be improved to prevent such kind attack and presented a modified and efficient signcryption scheme. We conclude that any other pairing-free signcryption scheme with similar design will be vulnerable to the same attack.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M.E. Saeed, Q. Liu, G. Tian, B. Gao, F. Li, HOOSC: heterogeneous online/offline signcryption for the internet of things, Wirel. Netw. (2017).

[2] L. Chen, J. Malone-Lee, Improved identity-based signcryption, in: Public Key Cryptography-PKC, Springer, Berlin, 2005, pp. 362–379.

[3] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, SIAM J. Comput. 32 (2003) 586–615.

[4] Y. Huifang, Y. Bo, Pairing-free and secure certificateless signcryption scheme, Comput. J. 60 (8) (2016) 1187–1196.

[5] S.S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography, Adv. Cryptol.-ASIACRYPT (2003) 452–473.

[6] L. Wei, W. Ma, Secure and efficient data sharing scheme based on certificateless hybrid signcryption for cloud storage, MDPI-Electron. 8 (590) (2019).

[7] S. Seo, E. Bertino, Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing, in: CERIAS TR 2013-10:CERIAS, West Lafayette, USA, 2013.

[8] A.A. Omala, A.S. Mbandu, K.D. Muturi, C. Jin, Provably secure heterogeneous access control scheme for wireless body area network, J. Med. Syst. 41 (108) (2018).

[9] D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, J. Cryptol. 13 (2000) 361–396.

[10] K.-A. Shim, Y.-R. Lee, C.-M. Park, EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks, Ad-Hoc Netw. 11 (2013) 182–189.

[11] K.A. Shim, S2drp secure implementations of distributed reprogramming, Ad Hoc Netw. 19 (2014) 1–8.

[12] X. Cao, W. Kou, L. Dang, B. Zhao, IMBAS: identity-based multiuser broadcast authentication in wireless sensor networks, Comput. Commun. 31 (4) (2008) 659–667.

[13] C. Ma, K. Xue, P. Hong, Distributed access control with adaptive privacy preserving property for wireless sensor networks, Secur. Commun. Netw. 7 (4) (2014) 759–773.