# A Decentralized Ciomputationally Lightweight Key Establishment Protocol Over Elliptic Curves

Seyed-Mohsen Ghoreishi, Mohammad Amiri

Department of computer engineering, Technical and Vocational University, Sary, Mazandaran, Iran

Corresponding author: Seyed-Mohsen Ghoreishi, Email: mohsen.gh.crypto@gmail.com

The high cost of performing Bilinear Pairings besides the inherent problems of Traditional and Identity-based protocols, which are in turn in the category of public-key cryptographic ones, led to proposing many pairing-free cryptosystems in the context of Certificateless PKC. This category of cryptographic schemes is defined over lightweight elliptic curves rather than high-expense bilinear pairings. In this document, a pairing-free secret sharing scheme has been proposed over Certificateless PKC infrastructure which utilizes elliptic curve-based group operations. The output of this contribution, with a focus on computational complexity, is a novel scheme that is notably less expensive in comparison with the cost of related proposed ones.

**Keywords**: ECC-Based Cryptography, Secret sharing, Certificateless, Key Agreement.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 489–496. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-50

# 1 Introduction

Pioneered by Al-Riyami and Paterson, the idea of Certificateless Public Key Cryptography[1], were introduced at 2003 [1] to prevail the inherent drawback of Identity-Based PKC, named Key-Escrow. Mentioned problem was resulted by generating the users' secret key by a malicious or even curious Third Party, which has the role of generating private keys assigned to the users. By the use of Private Key Generator[2], considered channel would be prone to eavesdropping or occurrences of other security flaws. The remarkable work of Al-Riyami et al. could solve this problem by transforming the TTP responsibility to only generation of partial keys and named this party Key Generation Center (KGC). Hence, each user would be able to create the assigned private key after obtaining the related partial key, received by KGC.

Afterwards, large variety of cryptosystems were constructed over Certificateless PKC Infrastructure [2-5] such as secret sharing ones in the form of key agreement, key exchange, and key establishment [6-20]. In general, it is possible to classify the Certificateless secret sharing protocols into two categories; pairing-based [6-10] and paring-free [11-21]. By the use of Elliptic Curve, the latter one avoids pairing maps, which is known as a heavy cryptographic function (refer to Table1). As a result, pairing-free protocols are much more efficient than the pairing-based ones.

The output of current work would be a Certificateless secret sharing protocol which eliminates the use of costly pairings. It is apparent from the comparisons given in section five that the proposed scheme would be remarkably more lightweight than other ones. The reminder of this article is following sections. The second one assigns to introduce a road-map allocated to related protocols. Next section emphasizes on our contribution in the proposed protocol. Section four gives the details of our proposed protocol. The fifth section analyzes the performance of our protocol and the related ones. The last part is assigned to the conclusion.

# 2 Related Works

In 2003, Al-Riyami et al. [1] could overcome keyeskrew security flaw. Although their work was notable, the formal security proof was not provided. Following their work, several Certificateless key agreement protocols were proposed also without proving the security [6-9]. Later on, Swanson in [10] could introduce a superior security model. However, all of the schemes suffer from high complexity of computation of Bilinear Pairings.

Hence, in order to avoid such an expensive operation various ECC based protocols have been proposed regarding to eliminating pairing maps [11-19].According to this idea, several pairing-free Key Agreement protocols have been proposed in the context of Identity-Based and Certificateless cryptography [22-29]. The security of pairing-free protocols has been investigated widely. For instance, it has been shown by the authors of [13] that the proposed protocols in [11] and [12] are not secure. Although the proposed protocol in [13] is secure, it consists of nine scalar multiplications which is quite high in compare with other existing works. He et al. in [14] could prove that their proposed protocol is formally secure under eCK model. However, Sun et al. [15] claimed that mentioned protocol is not secure against type1 adversary. Although it is proved that he's protocol in [14] is secure formally, the considered security model is not strong. Although He et al. [16] have proven their proposed protocol under strong eCK model, it has been proven by Sun et al. [17] that the protocol in [16] is not secure against neither type1 adversary, nor type2. Moreover, it suffers from some flaws in the given proof.

Although, Sun et al. [17] had proven the security considering all events. However, the efficiency improvement is not significant and gap assumption is not as strong as computational ones [23].

# 3 Our Contributions

Considering all events to support the security concerns [15], a Certificateless ECC based secret sharing protocol is proposed with several interesting features. First of all, due to the use of Certificateless cryptography, it does not suffer from complex management of certificates issued by Certificate Authority (CA). Secondly, Key Escrow problem is avoided as the Trusted Third Party only generates partial keys and the actual private key is unknown to it. Thirdly, beside of using group operations over elliptic curves, the proposed protocol has been designed in such a way that requires minimal computations. Finally, the proposed protocol supports all necessary security requirements for secret sharing protocols.

# 4 The Recommended Protocol

This part introduces mentioned Certificateless secret sharing protocol. Proposed protocol consists of following phases.

**Setup**: the input would be security parameter, the output are hidden Master-key($s$) and public tuple Params:

$$s \in \mathbb{Z}_q^* \quad (1)$$

$$\text{Params:} < q, \mathbb{F}_q, E/\mathbb{F}_q, G, P, P_{Pub}, H_1, H_2 > \quad (2)$$

Here:

$$H_1: \{0,1\}^* \times G \rightarrow \mathbb{Z}_q^* \quad (3)$$

$$H_2: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \rightarrow \mathbb{Z}_q^*. \quad (4)$$

**Partial-Private-Extract:** in this phase, KGC retunes backpartial-private-key($s_i$ for any entity such as $i$) after required computations:

$$r_i \in_r \mathbb{Z}_q^* \quad (5)$$

$$R_i = r_i P \quad (6)$$

$$h_i = H_1(ID_i, R_i) \quad (7)$$

$$s_i = r_i + h_i s (mod\ q). \quad (8)$$

**Set-Public-Private Keys:** in this phase, any entity such as $i$ computhes its assigned final public/private key pair ($SK_i, PK_i/S_i$) after required computations:

$$l_i \in_r \mathbb{Z}_q^* \quad (9)$$

$$L_i = l_i P \quad (10)$$

$$u_i = l_i + h_i' s_i (mod\ q) \quad (11)$$

$$U_i = u_i P \quad (22)$$

$$h_i' = H_1(ID_i, L_i) \quad (33)$$

$$SK_i = (s_i, l_i, u_i) \quad (44)$$

$$PK_i = (R_i, S_i, X_i, U_i) \quad (55)$$

$$S_i = \left(R_i + h_i P_{pub}\right) = s_i P \quad (66)$$

**Exchange**: Participants A and B, compute the key tokens $T_A$ and $T_B$, respectively. Then, transfer the computed value to the other participant.

(1) Participant A computes as followed:

$$t_A \in_r \mathbb{Z}_q^* \quad (77)$$

$$T_A = \left((t_A l_A)(s_A + u_A)\right)[S_B + U_B] \quad (88)$$

(2) Participant B computes the key token similar to what participant A does:

$$t_B \in_r \mathbb{Z}_q^* \quad (99)$$

$$T_B = \left((t_B l_B)(s_B + u_B)\right)[S_A + U_A] \quad (20)$$

**Computation**: The shared secret must be computed by communicated parties, separately:

$$K_{AB} = (t_A l_A) T_B \quad (21)$$

$$K_{BA} = (t_B l_B) T_A \quad (22)$$

The equation (23) indicates that computed values are equivalent:

$$K_{AB} = (t_A l_A)\left((t_B l_B)(s_B + u_B)\right)[S_A + U_A] = \left((t_A l_A)(t_B l_B)(s_A + u_A)(s_B + u_B)\right)P$$
$$= (t_B l_B)\left((t_A l_A)(s_A + u_A)\right)[S_B + U_B] = K_{BA} \quad (23)$$

In order to acquire the session key, parties drive the final value, $k_s$, according to the equation (24).

$$k_s = H_2(ID_A, ID_B, T_A, T_B, K_{AB}) = H_2(ID_A, ID_B, T_A, T_B, K_{BA}) \quad (24)$$

# 5 Results and Discussion

This section presents a comprehensive comparison of the proposed protocol and a subset of related works from the computational cost perspective. As noted earlier, recent Certificateless protocols utilize elliptic curve based group operations which are much more lightweight than Pairings operation [31,32]. As acclaimed in [32] Table1 illustrates that computation of scalar multiplication operation over elliptic curves would be considerably less time consuming than computation of Bilinear Pairings. As a result, the given comparison excludes pairing-based secret sharing protocols.

**Table 1.** Processing time of computing pairing and ECC-based scalar MUL [32]

| Operation | Time (m. sec.) |
|---|---|
| Pairing | 20.01 |
| ECC-based scalar multiplication | 0.83 |

Table2 shows the required time complexity for executing group operations by considering Modular Multiplication as a unit [33].

**Table 2.** Group operations complexity of computation [33]

| Notation | Definition and conversion |
|---|---|
| $T_{MM}$ | Time complexity for executing the modular multiplication |
| $T_{SM}$ | Time complexity for executing the elliptic curve scalar multiplication$1T_{SM} \approx 29T_{MM}$ |
| $T_{PA}$ | Time complexity for executing the elliptic curve point addition,$1T_{PA} \approx 0.12T_{MM}$ |
| $T_{IN}$ | Time complexity for executing the modular inversion operation,$1T_{IN} \approx 11.6T_{MM}$ |

Based on the given information, computational cost of the related works is compared versus our proposed one. The details are illustrated in Table3.

**Table 3.** Comparison of the proposed protocol and related work from computational complexity viewpoint

| Authors | Required computations for Exchange and Computation phases from A's perspective | Computed exponentiation(Scalar Multiplication) | Computed point addition | Computed modular multiplication |
|---|---|---|---|---|
| He et al. [14] | $T_{a=}aP$<br>$K_{AB}^1 = (a + s_A)[T_B + S_B]$<br>$K_{AB}^2 = (a + x_A)[T_B + X_B]$<br>$K_{AB}^3 = aT_B$ | $aP, (a + s_A)[T_B + S_B],$<br>$(a + x_A)[T_B + X_B], aT_B$ | $[T_B + S_B],$<br>$[T_B + X_B]$ | o |
| Sun et al. [15] | $T_{A=}aP$<br>$K_{AB}^1 = (a + s_A + x_A)[T_B + S_B + X_B]$<br>$K_{AB}^2 = (a + 2s_A - x_A)[T_B + 2s_B - X_B]$<br>$K_{AB}^3 = (a - s_A - 2x_A)(T_B - S_B + 2X_B)$ | $aP,$<br>$(a + s_A + x_A)[T_B + S_B + X_B],$<br>$(a + 2s_A - x_A)[T_B + 2s_B - X_B],$<br>$(a - s_A - 2x_A)(T_B - S_B + 2X_B)$ | $T_B + S_B + X_B,$<br>$T_B + 2s_B,$<br>$S_B + 2X_B$ | o |
| He et al. [16] | $T_A = a(X_B + S_B)$<br>$K_{AB}^1 = (a + s_A)^{-1}T_B + aP$<br>$K_{AB}^2 = a(x_A + s_A)^{-1}T_B$ | $a(X_B + S_B),$<br>$(a + s_A)^{-1}T_B, aP,$<br>$a(x_A + s_A)^{-1},$<br>$a(x_A + s_A)^{-1}T_B$ | $X_B + S_B$<br>$(a + s_A)^{-1}T_B + aP$ | $a[(x_A + s_A)^{-1}]$ |
| Deng [20] | $T_{A=}aP$<br>$Z_B = T_B + R_B + h_B P_{pub} + kP_B$<br>$K_{AB}^1 = (s_A + kx_A + a)Z_B$<br>$K_{AB}^2 = aT_B$ | $aP, (h_B P_{pub}), kP_B, uZ_B, a$ï<br>where<br>$u = (s_A + kx_A + a)$ | $T_B + R_B + h_B P_{pub} + kP_B$ | $kx_A$ |
| Deng Gao [21] | $T_{A=}aP$<br>$K_{ij=}(l_{ij}a + t_i + d)(l_{ij}T_B + T_j + R_j + h_j P_{pub})$ | $aP, (l_{ij}T_B), (h_j P_{pub}), uV$<br>where<br>$u = (l_{ij}a + t_i + d)$ | $(l_{ij}T_B) + T_j + R_j + (h_j P_{pub})$ | $(l_{ij}a)$ |

| | | | | |
|---|---|---|---|---|
| | | $V = (l_{ij}T_B + T_j + R_j + h_j P_{pub})$ | | |
| Xie et al. [22] | $T_{A=}aP$<br>$K_{AB}^1 = (s_A + x_A + a)(T_B + R_B + h_B P_{pub} + P_B)$<br>$K_{AB}^2 = aT_B$ | $aP, aT_B, (h_B P_{pub}), uV$<br>where<br>$u = (s_A + x_A + a)$<br>$V = (T_B + R_B + h_B P_{pub} + P_B)$ | $T_B + R_B + h_B P_{pub} + P_B$ | o |
| Our proposed Protocol | $T_A = \big((t_A l_A)(s_A + u_A)\big)[S_B + U_B]$<br>$K_{AB} = (t_A l_A)T_B$ | $uV, wT_B$<br>where<br>$u = \big((t_A l_A)(s_A + u_A)\big)$<br>$V = [S_B + U_B]$<br>$w = (t_A l_A)$ | $S_B + U_B$ | $t_A l_A$ |

Finally, the given data in Table4 is deducted from Table2 and Table3. In this table, superiority of the proposed protocol from performance perspective is considerably notable.

**Table 4. C**omparison of computational performance

| protocols | Required operations | Overall computational cost |
|---|---|---|
| He et al. [14] | $4\ T_{SM} + 2T_{PA}$ | 116.24 |
| Sun et al. [15] | $4\ T_{SM} + 4T_{PA}$ | 116.48 |
| He et al. [16] | $5\ T_{SM} + 2T_{PA} + 2T_{IN} + T_{MM}$ | 169.44 |
| Deng [18] | $5\ T_{SM} + 3T_{PA} + T_{MM}$ | 146.36 |
| Deng , Gao [19] | $4\ T_{SM} + 3T_{PA} + T_{MM}$ | 117.36 |
| Xie et al. [20] | $4\ T_{SM} + 3T_{PA}$ | 116.36 |
| Our proposed Protocol | $2\ T_{SM} + T_{PA} + T_{MM}$ | 59.12 |

It is deductible from Table4that the proposed protocol is notably more lightweight than the others. The rightmost column indicates overall computational cost of the compared protocols.

# 6 Conclusion

The low computational complexity in pairing-free cryptosystems attracted many researchers to propose lightweight protocols in this style. Recently proposed Certificateless secret sharing protocols, which eliminated pairing maps, still are not as cost effective as expected. The results of this paper deduce that the current proposed secret sharing protocol is remarkably more lightweight than current related ones.

# References


[1] Al-Riyami, S. S. and Paterson, K. G. (2003). Certificateless public key cryptography. In *International conference on the theory and application of cryptology and information security*, 2003: 452-473.

[2] Zhang, Z. and Wong, D. (2006). Certificateless Public-Key Signature: Security Model and Efficient Construction. In *Applied Cryptography and Network Security*, 293-308.

[3] Li, X., Chen, K. and Sun, L. (2005). Certificateless Signature and Proxy Signature Schemes from Bilinear Pairings. *Lithuanian Mathematical Journal*, 45: 76-83.

[4] Liu, J.K., Au, M.H. and Susilo, W. (2007). Self-Generated-Certificate Public Key Cryptography and Certificateless Signature/Encryption Scheme in the Standard Model. In *7 ACM Symposium on InformAtion, Computer and Communications Security*.

[5] Yum, D. H. and Lee, P. J. (2004). Generic Construction of Certificateless Encryption. In *Computational Science and Its Applications*, 802-811.

[6] Wang, S., Cao, Z. and Dong, X. (2006). Certificateless authenticated key agreement based on the MTI/CO protocol. *Journal of Information and computational science*, 3(3): 575-581.

[7] Mandt, T. K. and Tan, C.H. (2006). Certificateless authenticated two-party key agreement protocols. In *Annual Asian Computing Science Conference*, 37-44.

[8] Shi, Y. and Li, J. (2007). Two-party authenticated key agreement in Certificateless public key cryptography. *Wuhan University Journal of Natural Sciences*, 12(1): 71-74.

[9] Lippold, G., Boyd, C. and Nieto, J. G. (2009). Strongly secure Certificateless key agreement. In *International conference on pairing-based cryptography*, 206-230.

[10] Hou, M. and Xu, Q. (2009). A two-party certificateless authenticated key agreement protocol without pairing. In *2nd IEEE International Conference on Computer Science and Information Technology*, 2009:412-416.

[11] Baek, J., Safavi-Naini, R. and Susilo, W. (2005). Certificateless public key encryption without pairing. In *International Conference on Information Security*, 134-148.

[12] Geng, M. and Zhang, F. (2009). Provably secure certificateless two-party authenticated key agreement protocol without pairing. In *International Conference on Computational Intelligence and Security*, 2: 208-212.

[13] Yang, G. and Tan, C. H. (2011). Strongly secure certificateless key exchange without pairing. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 71-79.

[14] He, D., Padhye, S. and Chen, J. (2012). An efficient certificateless two-party authenticated key agreement protocol. *Computers & Mathematics with Applications,* 64(6): 1914-1926.

[15] Sun, H. et al. (2013). A novel pairing-free certificateless authenticated key agreement protocol with provable security. *Frontiers of Computer Science*, 7(4): 544-557.

[16] He, D., Chen, J. and Hu, J. (2012). A pairing-free certificateless authenticated key agreement protocol. *International Journal of Communication Systems,* 25(2): 221-230.

[17] Chen, L., Cheng, Z. and Smart, N.P. (2007). Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6(4): 213-241.

[18] Ghoreishi, S. M. et al. (2014). Security evaluation over lightweight cryptographic protocols. In *International Symposium on Biometrics and Security Technologies*.

[19] Ghoreishi, S. M. et al. (2017). A Secure Identity Based Key Agreement Protocol Without Key-Escrow. *Journal of Engineering and Applied Science*, doi:10.36478/jeasci.2017.4809.4813

[20] Deng, L. (2020). An improved certificateless two-party authenticated key agreement protocol for wireless sensor networks. *International Journal of Ad Hoc and Ubiquitous Computing*, 34(4): 208-215.

[21] Deng, L. and Gao, R. (2021). Certificateless two-party authenticated key agreement scheme for smart grid. *Information Sciences*, 543: 143-156.

[22] Xie, Y. et al. (2019). Efficient two-party certificateless authenticated key agreement protocol under GDH assumption. *International Journal of Ad Hoc and Ubiquitous Computing*, 30(1): 11-25.

[23] Ghoreishi, S.M. and Isnin, I.F. (2013). Secure lightweight pairing-based key-agreement cryptosystems: Issues and Challenges. *International Journal of Engineering and Technology*, 5(2): 320.

[24] Ghoreishi, S.M. et al. (2014). New secure identity-based and certificateless authenticated Key Agreement protocols without pairings. In *International Symposium on Biometrics and Security Technologies*, 188-192.

[25] Ghoreishi, S.M. et al. (2015). A novel secure two-party identity-based authenticated key agreement protocol without bilinear pairings. In *Pattern Analysis, Intelligent Security and the Internet of Things*, 287-294.

[26] Ghoreishi, S.M. et al. (2015). An Efficient Pairing-Free Certificateless Authenticated Two-Party Key Agreement Protocol Over Elliptic Curves. In *Pattern Analysis, Intelligent Security and the Internet of Things*, 295-302.

[27] Ghoreishi, S.M. et al. (2015). Secure and Authenticated Key Agreement protocol with minimal complexity of operations in the context of identity-based cryptosystems. In *International Conference on Computer, Communications, and Control Technology*, 299-303.

[28] Ghoreishi, S.M. et al. (2015). A performance improved certificateless key agreement scheme over elliptic curve based algebraic groups. *Jurnal Teknologi, 77*(20).

[29] Ghoreishi, S., et al. (2016). TWO SECURE NON-SYMMETRIC ROLE KEY-AGREEMENT PROTOCOLS.

[30] Ghoreishi, Seyed-Mohsen, et al. (2014). Rushing attack against routing protocols in Mobile Ad-Hoc Networks. In *International Symposium on Biometrics and Security Technologies*.

[31] Zhang, F., Safavi-Naini, R. and Susilo, W. (2004). An efficient signature scheme from bilinear pairings and its applications. In *International Workshop on Public Key Cryptography*, 277-290.

[32] Cao, X., Kou, W. and Du, X. (2010). A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Information Sciences*, 180(15): 2895-2903.

[33] Islam, S.H. and Biswas, G. (2012). PA pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. *Annals of télécommunications-annales des telecommunications*, 67(11): 547-558.