A Note on " Provably Secure and Lightweight Authentication Key Agreement Scheme for Smart Meters"

Zhengjun Cao, Lihua Liu

Abstract. We show that the authentication key agreement scheme [IEEE Trans. Smart Grid, 2023, 14(5), 3816-3827] is flawed due to its inconsistent computations. We also show that the scheme fails to keep anonymity, not as claimed.

Keywords: Authentication, anonymity, key agreement, elliptic curve, point at infinity.

1 Introduction

In a smart grid, smart meters should be responsible for the information exchange between consumers and service providers. To authenticate each other and securely transmit information, they need to establish secure session keys via open channels. Recently, Chai et al. [1] have presented a key agreement scheme for smart meters. It is designed to meet many security requirements, including mutual authentication, session key security, identity anonymity, resistent against replay attack, impersonation attack, denial of service attack, etc. In this note, we show that the scheme is not correctly presented, and should be revised. We also find the scheme cannot provide anonymity.

2 Review of the Chai et al.'s scheme

In the considered scenario, there are three parities: Certificate Authority (CA), smart meters, and an NAN gateway. The involved notations and their descriptions are listed below (see Table 1).

Initialisation Phase. The CA chooses a prime p and $a, b \in \mathbb{Z}_p^*$ to define the elliptic curve E as $y^2 = x^3 + ax + b \bmod p$, where $4a^3 + 27b^2 \neq 0$. Choose a generator G of a cyclic subgroup of the elliptic curve group $E(F_p)$, with the prime order n. Choose two hash functions $H_1 : \{0,1\}^* \to \{0,1\}^v, H_2 : \{0,1\}^* \to \{0,1\}^l$, where v, l are two positive integers. Publish the system parameters $p, a, b, G, n, H_1, H_2, v, l$ and h, where $h = \sharp E(F_p)/n$.

Registration Phase. A smart meter (A) and NAN gateway (B) will register with CA. A sends its identifier ID_A to CA. CA checks the uniqueness of ID_A. Then CA generates a public-private key pair for A: it selects a random number $d_A \in \mathbb{Z}_n^*$ and calculates

$$P_A = [d_A]G, \quad Z_A = H_1(ID_A \| a \| b \| G \| P_A).$$

Send the private key d_A to A via a secure channel. Similarly, CA generates a public-private key pair for B and sends the private key d_B to B via a secure channel.

Z. Cao is with Department of Mathematics, Shanghai University, China. L. Liu is with Department of Mathematics, Shanghai Maritime University, Shanghai, China. Email: liulh@shmtu.edu.cn

Table 1: Notations and descriptions

F_p	finite field containing p elements
$E(F_p)$	the set of all rational points of the elliptic curve E over F_p (including the infinity point O)
G	a generator of an elliptic curve group with the prime order n
$\sharp E(F_p)$	the cardinality of group $E(F_p)$
h	cofactor, $h = \sharp E(F_p)/n$
ID_A, ID_B	identifiers of user A and B
RID_u	pseudonym identifier of user u
d_u	private key of user u
P_u	public key of user u
$x\|\|y$	the concatenation of x and y
$\oplus$	bitwise XOR
$H_1(\cdot), H_2(\cdot)$	hash functions
$KDF(\cdot)$	key derivation function

Authentication Phase. The phase can be depicted as below (see Table 2).

Table 2: The Chai et al.'s key agreement scheme

Smart meter (A)	Gateway (B)
Pick a nonce r_A and a timestamp T_A to compute $u_A = r_A + d_A$, $RID_A = ID_A \oplus H(Z_B\|\|u_A)$.	
$\xrightarrow{RID_A, T_A, u_A}$	
	Check T_A. Then check if $ID_A \stackrel{?}{=} RID_A \oplus H(Z_B\|\|u_A)$. Pick a nonce r_B to compute $R_B = [r_B]G = (x_2, y_2)$, $R_A = [u_A]G - P_A = (x_1, y_1)$. Pick the timestamp T_B. Compute $s = H_2(R_A\|\|P_B\|\|T_A\|\|T_B)$, $e = H_2(R_B\|\|P_A\|\|T_A\|\|T_B)$, $t_B = (d_B + e \times r_B) \bmod n$, $V = [h \times t_B](P_A + [s]R_A) = (x_V, y_V)$. Verify $V \stackrel{?}{=} O$. If so, compute $S_B = H_1(0x02\|\|y_V \|\|H_1(x_V\|\|Z_A\|\|Z_B\|\|x_1\|\|y_1\|\|x_2\|\|y_2)$.
	$\xleftarrow{T_B, R_A, R_B, S_B}$
Check T_B. Then compute $s = H_2(R_A\|\|P_B\|\|T_A\|\|T_B)$, $e = H_2(R_B\|\|P_A\|\|T_A\|\|T_B)$, $t_A = (d_A + s \times r_A) \bmod n$, $U = [h \times t_A](P_B + [e]R_B) = (x_U, y_U)$. Verify $U \stackrel{?}{=} O$. If so, compute $S_1 = H_1(0x02\|\|y_U \|\|H_1(x_U\|\|Z_A\|\|Z_B\|\|x_1\|\|y_1\|\|x_2\|\|y_2)$. Check if $S_1 = S_B$. If so, compute $S_A = H_1(0x03\|\|y_U \|\|H_1(x_U\|\|Z_A\|\|Z_B\|\|x_1\|\|y_1\|\|x_2\|\|y_2)$, $K_A = KDF(x_U\|\|y_U \|\|Z_A\|\|Z_B, klen)$.	
$\xrightarrow{S_A}$	
	Compute $S_2 = H_1(0x03\|\|y_V \|\|H_1(x_V\|\|Z_A\|\|Z_B\|\|x_1\|\|y_1\|\|x_2\|\|y_2)$. Verify $S_2 \stackrel{?}{=} S_A$. If so, compute $K_B = KDF(x_V\|\|y_V \|\|Z_A\|\|Z_B, klen)$.

3 Inconsistent computations

The correctness of this scheme is not well verified. It only shows $U = V$, and immediately claims that *"A and B successfully negotiate the same session key"* (see page 3819, Ref.[1]).

According to its original description, A and B should verify that $U = O$ or $V = O$, respectively, where O is the zero point. But it is easy to find that

$$\begin{aligned} U &= [h \times t_A](P_B + [e]R_B) \\ &= [h \times (d_A + s \times r_A)(d_B + e \times r_B)]G \end{aligned}$$

To ensure $U = O$, it requires that

$$(d_A + s \times r_A)(d_B + e \times r_B) \equiv 0 \bmod n \tag{1}$$

In view of that n is a prime, we have

$$d_A + s \times r_A \equiv 0 \bmod n, \text{ or } d_B + e \times r_B \equiv 0 \bmod n,$$

i.e.,

$$d_A + H_2(R_A \| P_B \| T_A \| T_B) \times r_A \equiv 0 \bmod n,$$

or

$$d_B + H_2(R_B \| P_A \| T_A \| T_B) \times r_B \equiv 0 \bmod n.$$

It leads to

$$H_2(R_A \| P_B \| T_A \| T_B) \equiv -d_A \times r_A^{-1} \bmod n, \tag{2}$$

$$H_2(R_B \| P_A \| T_A \| T_B) \equiv -d_B \times r_B^{-1} \bmod n. \tag{3}$$

Since d_A is randomly chosen by the CA, it is impossible to choose such a number r_A for the party A so that the hash value satisfies Eq.(2), due to the unpredictability of hash function H_2. Likewise, it is impossible to choose such a number r_B for the party B so that the other hash value satisfies Eq.(3). That means A and B will fail to verify that $U = O$ or $V = O$, respectively.

We would like to stress that the point at infinity is an extra element added to the elliptic curve and the rules of point addition, such that for all P on the curve (including the point at infinity O), it holds $P + O = P = O + P$.

For the Weierstrass equation $y = x^3 + ax + b \bmod p$, the point at infinity, O, can have different values according to the underlying coordinate system, which has no a fixed representation in affine coordinates, instead a unique representation $(0, 1, 0)$ in projective coordinates [2]. But the Chai et al.'s scheme is just presented using affine coordinates. In this case, the zero point is only a virtual point, and the verification that a point equals to zero point cannot be practically implemented.

We also find the verifications have no relation to the later processes, and never been discussed in the whole scheme. Therefore, both verifications can be removed. By the way, the strings $0x02$, $0x03$ have no relation to the security of resulting key (see the later security argument, §V, Ref.[1]). The parameter *klen* is not specified. These typos can be reasonably fixed.

4 The loss of anonymity

As for the anonymity, it argues: "*In the authentication stage, the smart meter establishes the session key through pseudonym identifier RID, and the attacker cannot obtain the real identity. After the pseudonym expires, the attacker cannot overhear the user. Thus, identity anonymity is guaranteed*" (see page 3822, Ref.[1]). We find the simple argument is not sound.

Notice that $RID_A = ID_A \oplus H(Z_B \| u_A)$, where RID_A, u_A are directly sent to B via the open channel. An adversary can retrieve RID_A, u_A by eavesdropping the channel. The other parameter is

$$Z_B = H_1(ID_B \| a \| b \| G \| P_B) \tag{4}$$

where a, b, G are public system parameters, and P_B is the public key of the gateway B. Since the identifier ID_B is used to distinguish the gateway from others, ID_B is also a publicly available parameter, not a confidential parameter. Otherwise, such an identifier losses its signification. So, the adversary can obtain Z_B (in the same system, any smart meter knows Z_B). Therefore, the adversary can compute

$$ID_A = RID_A \oplus H(Z_B \| u_A) \tag{5}$$

to reveal the target smart meter's identity.

5 Conclusion

We show that the Chai et al.'s authentication key agreement scheme should be revised due to some inconsistent computations. We find the structure of an elliptic curve group is still unfamiliar to some newcomers. We also show that the scheme cannot provide anonymity. The findings in this note could be helpful for the future work on designing such schemes.

References

[1] S. Chai, et al., Provably Secure and Lightweight Authentication Key Agreement Scheme for Smart Meters, *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 3816-3827, 2023.

[2] D. Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, USA, 2003.