A note on "LAKAF: lightweight authentication and key agreement framework for smart grid network"

Zhengjun Cao[1], Lihua Liu[2]

Abstract. We show that the key agreement scheme [J. Syst. Archit., 116: 102053, 2021] is flawed. It makes use of a symmetric key encryption to transfer data between the user and server. But the symmetric key is easily retrieved by an adversary, which results in the loss of data confidentiality, and makes it vulnerable to impersonation attack.

Keywords: Authentication, Key agreement, Impersonation attack, Symmetric key encryption, Smart grid

1 Introduction

Recently, Khan *et al.* [1] have presented a key agreement scheme for smart grid network, in which there are three entities: user U, server S, and a trust authority (TA). The TA is responsible for initialization. U and S register with TA via secure communication channels, respectively. Then U and S will mutually authenticate with each other by using key agreement through public channel.

The scheme only involves lightweight operations, such as hashing, string concatenation, bit-wise XOR, and elliptic curve based operations [2]. Though the scheme is interesting, we find it flawed because it fails to keep data confidentiality.

2 Review of the scheme

Let $\mathbb{G}$ be a group defined on an elliptic curve $\mathcal{E}$, with respective to a finite prime field $\mathbb{Z}_q^*$. $g \in \mathbb{G}$ is a base point. $h(\cdot)$ is a hash function. The biometric authentication is performed using the fuzzy extractor, where $Gen(\cdot)$ and $Rep(\cdot)$ procedures are used during login phase.

TA picks $x \in \mathbb{Z}_q^*$, sets the public key as $P_{pub} = xg$, with respect to the secret key x. The scheme can be described as follows (see Table 1).

3 Insecure against external attack

In the key agreement phase, the server S needs to compute

$$K_2 = h(I_1 \oplus (h(t_1) \oplus t_1)\|h(t_1 \oplus r_S g)\|t_1) \tag{1}$$

---

[1] Department of Mathematics, Shanghai University, Shanghai, 200444, China

[2] Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.

Email: liulh@shmtu.edu.cn

Table 1: The Khan *et al.*'s key agreement scheme

User U: $\{ID_U, PW_U\}$	TA: $\{x\}$	Server S: $\{ID_S\}$
Input identity ID_U, password PW_U. Imprint the biometric key B_U.		
Pick $r_U \in Z_q^*$, compute $(\sigma_U, \tau_U) = Gen(B_U)$. $\gamma_U = h(PW_U \| \sigma_U) \oplus r_U$.	Assign a registration counter C_U. Compute $A = h(ID_U \| x \| C_U)$, $\beta = A \oplus \gamma_U$.	
$\xRightarrow[\text{[secure channel]}]{ID_U, \gamma_U}$	Store $\{ID_U, C_U, \beta\}$.	
	$\xLeftarrow{\beta,\ C_U}$	
Compute $\beta_1 = \beta \oplus \sigma_U$, $\beta_2 = h(ID_U \| PW_U \| \beta_1)$. Store $\{\beta, \beta_1, \beta_2, \tau_U, C_U\}$.		
	Assign a counter C_S.	$\xLeftarrow{ID_S}$
	Compute $\xi = h(ID_S \| x \| C_S)$. Store $\{ID_S, \xi, C_S\}$.	Pick $r_S \in Z_q^*$, compute public key $PK_S = r_S g$.
	$\xRightarrow{\xi,\ C_S}$	Store $\{\xi, C_S\}$.
User U: $\{ID_U, PW_U, \beta, \beta_1, \beta_2, \tau_U, C_U\}$	$\boxed{\text{Key Agreement}}$	Server S: $\{ID_S, \xi, C_S\}$
Login with ID_U^*, PW_U^*, B_U^* to get $\sigma_U^* = Rep(B_U^*, \tau_U^*)$. Compute $\beta_1^* = \beta \oplus \sigma_U^*$, $\beta_2^* = h(ID_U^* \| PW_U^* \| \beta_1^*)$. Check $\beta_2^* = \beta_2$. If so, pick $a \in Z_q^*$, compute		Check $t_2 - t_1 \leq \triangle t$. If so, compute $I_2 = I_1 \oplus (h(t_1) \oplus t_1)$, $K_2 = h(I_2 \| h(t_1 \oplus r_S g) \| t_1)$. Check $ID_U^* = I_2$.
$S_1 = h(ID_U \| a \| C_U)$,	$\xrightarrow[\text{[public channel]}]{M_1 = \{E_1, I_1, t_1\}}$	Decrypt $D_{K_2}(E_1) = (a, S_1, C_U)$.
$I_1 = ID_U \oplus (h(t_1) \oplus t_1)$, $K_1 = h(ID_U \| h(t_1 \oplus PK_S) \| t_1)$. Encrypt $E_1 = E_{K_1}(a, S_1, C_U)$.		Check $S_1^* = h(ID_U^* \| a \| C_U)$. Pick $b \in Z_g^*$, compute $SK_S = h(ID_U^* \| ID_S \| C_U \| C_S \| abg \| t_3)$ $S_2 = h(ID_S \| ID_U^* \| S_1^* \| \xi \| SK_S \| t_1)$, $\xi_1 = \xi \oplus h(C_U \| ID_U^* \| K_2)$,
Check $t_4 - t_3 \leq \triangle t$.		$\eta = ID_S \oplus h(b \| C_S \| C_U)$,
Compute $K_4 = h(ID_U \| S_1 \| a \| C_U \| t_3)$.	$\xleftarrow{M_2 = \{E_2, t_3\}}$	$K_3 = h(ID_U^* \| S_1^* \| a \| C_U \| t_3)$.
Decrypt $D_{K_4}(E_2) = (\eta, \xi_1, C_S, b)$. Check $ID_S^* = \eta \oplus h(b \| C_S \| C_U)$. Compute $SK_U = h(ID_U \| ID_S^* \| C_U \| C_S \| abg \| t_3)$, $\xi^* = \xi_1 \oplus h(C_U \| ID_U \| K_1)$. Check $S_2^* = h(ID_S^* \| ID_U \| S_1 \| \xi^* \| SK_U \| t_1)$.		Encrypt $E_2 = E_{K_3}(\eta, \xi_1, C_S, b)$.

for a symmetric key encryption, where $PK_S = r_S g$ is the public key of the server S, which is publicly available to an external adversary.

The message $M_1 = \{E_1, I_1, t_1\}$ is transferred via a public channel, which means the adversary can capture it. Therefore, the time stamp t_1 and the parameter I_1 are also exposed to the adversary. Thus, the adversary can recover K_2 by using Eq.(1). With the recovered key and captured ciphertext E_1, the adversary can decrypt it, i.e.,

$$D_{K_2}(E_1) = (a, S_1, C_U) \tag{2}$$

to obtain the plaintext $\{a, S_1, C_U\}$. Besides, the adversary can recover the user's identity

$$ID_U = I_1 \oplus (h(t_1) \oplus t_1) \tag{3}$$

Now, the other key

$$K_4 = h(ID_U \| S_1 \| a \| C_U \| t_3) \tag{4}$$

is also retrieved by the adversary, using the captured time stamp t_3. Therefore, the adversary can decrypt the ciphertext E_2, i.e.,

$$D_{K_4}(E_2) = (\eta, \xi_1, C_S, b) \tag{5}$$

to obtain the plaintext η, ξ_1, C_S, b. Finally, the adversary can recover the server's identity

$$ID_S = \eta \oplus h(b \| C_S \| C_U) \tag{6}$$

and the parameter

$$\xi = \xi_1 \oplus h(C_U \| ID_U \| K_2) \tag{7}$$

With the retrieved $\{ID_S, \xi, C_S\}$, the adversary can impersonate the server S to cheat any user.

4 Insecure against internal attack

Notice that the server's secret key r_S is not actually invoked, instead only the public key $r_S g$ is invoked once. Since a legitimate user U needs to compute

$$\begin{aligned}
&(\eta, \xi_1, C_S, b) \leftarrow D_{K_4}(E_2),\\
&ID_S = \eta \oplus h(b \| C_S \| C_U),\\
&\xi = \xi_1 \oplus h(C_U \| ID_U \| K_1),
\end{aligned}$$

i.e., C_S, ID_S, ξ are directly exposed to U, we find that a corrupted user can impersonate the server to cheat other users.

5 Conclusion

In this note, we show that the Khan *et al.*'s key agreement scheme is flawed because it is not explicitly organized. The findings in this note could be helpful for the future work on designing such key agreement schemes.

References

[1] A. Khan, *et al.*, LAKAF: lightweight authentication and key agreement framework for smart grid network. J. Syst. Archit., 116: 102053 (2021)

[2] D. Hankerson, S. Vanstone, A. Menezes, *Guide to Elliptic Curve Cryptography.* Springer New York, USA (2006)