A note on "a new password-authenticated module learning with rounding-based key exchange protocol: Saber.PAKE"

Zhengjun Cao and Lihua Liu

Abstract. We show the Seyhan-Akleylek key exchange protocol [J. Supercomput., 2023, 79:17859-17896] cannot resist offline dictionary attack and impersonation attack, not as claimed.

Keywords: Key exchange, mutual authentication, offline dictionary attack, impersonation attack

1 Introduction

Recently, Seyhan and Akleylek [1] have presented a new lattice-based password-authenticated three-pass key exchange protocol for the post-quantum era. It is designed to meet many security requirements, such as mutual authentication, session key agreement, perfect forward secrecy, resistent to impersonation attack, dictionary attack, and man-in-the-middle attack [2]. Though the protocol is interesting, we find it is insecure against offline password-guessing attack and impersonation attack.

2 Review of the Seyhan-Akleylek key exchange protocol

In the considered scenario, there are two entities, client $\acute{c}$ and server $\acute{s}$. The involved notations are listed below (see Table 1). The scheme can be depicted as follows (see Table 2).

3 The flaws

The protocol is claimed to be resistant to dictionary attack. It argues: *The four different hash functions are used and the password is selected randomly at the beginning. One of the hashes is used to obtain the password's hash, and the others are used to calculate key and shared key components. These additions provide the independence of messages, keys, and passwords.*

We find the claim is not sound. In fact,

$$k'_{\acute{c}} = H_3(\acute{c}, \acute{s}, \boldsymbol{\alpha}, \boldsymbol{b}_{\acute{s}}, c, \boldsymbol{\gamma}_{\acute{s}}) \tag{1}$$

where $k'_{\acute{c}}, \acute{c}, \boldsymbol{\alpha}, c, \boldsymbol{b}_{\acute{s}}$, transferred via open channels, can be captured by the adversary. Though the server's identifier $\acute{s}$ is not transferred, any other client knows the identifier. That means $\acute{s}$ is not a

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

Table 1: The involved symbols

symbol	description	symbol	description
n	a power of 2	ℓ	rank of the module
$\mathbb{Z}_q$	ring of integers modulo q	$\mathcal{R}_q$	$\mathbb{Z}_q[X]/(X^n+1)$
$\mathcal{R}_q^{\ell\times\ m}$	ring of $\ell\times\ m$ matrices on $\mathcal{R}_q$	$\boldsymbol{a}^T$	transpose of $\boldsymbol{a}$
β_μ	the central binomial distribution with parameter μ		
h	a constant vector over $\mathcal{R}_q^{\ell\times\ 1}$,	h_1	a constant polynomial over $\mathcal{R}_q$, all coefficients equal to $2^{\varepsilon_q-\varepsilon_p-1}$
h_2	a constant polynomial over $\mathcal{R}_q$, all coefficients equal to $2^{\varepsilon_p-2}-2^{\varepsilon_p-\varepsilon_t-2}$	bits()	bits reconciliation function
H_1	$\{0,1\}^*\to\mathcal{R}_q^{\ell\times\ 1}$ a hash function	H_2, H_3, H_4	hash functions

Table 2: The Seyhan-Akleylek key exchange protocol

Client $\acute{c}:\{pw, seed_A\}$		Server $\acute{s}:\{pw, seed_A\}$
Input $\acute{s}, pw$. Compute $\boldsymbol{A}\leftarrow \text{gen}(seed_A)\in\boldsymbol{\mathcal{R}}_q^{\ell\times\ell}$, $\boldsymbol{s}_{\acute{c}}\leftarrow\beta_\mu(\boldsymbol{\mathcal{R}}_q^{\ell\times 1})$, $\boldsymbol{b}_{\acute{c}}=\text{bits}(\boldsymbol{A}\boldsymbol{s}_{\acute{c}}+h,\varepsilon_q,\varepsilon_p)\in\boldsymbol{\mathcal{R}}_p^{\ell\times 1}$, $\boldsymbol{\gamma}_{\acute{c}}=H_1(pw)$, $\boldsymbol{\alpha}=\boldsymbol{b}_{\acute{c}}+\boldsymbol{\gamma}_{\acute{c}}$.	$\xrightarrow{\acute{c},\ \boldsymbol{\alpha}}$	Abort if $\boldsymbol{\alpha}\notin\boldsymbol{\mathcal{R}}_p^{\ell\times 1}$. Compute $\boldsymbol{A}\leftarrow\text{gen}(seed_A)\in\boldsymbol{\mathcal{R}}_q^{\ell\times\ell}$, $s_{\acute{s}}\leftarrow\beta_\mu(\boldsymbol{\mathcal{R}}_q^{\ell\times\ 1})$, $\boldsymbol{b}_{\acute{s}}=\text{bits}(\boldsymbol{A}^T\boldsymbol{s}_{\acute{s}}+h,\varepsilon_q,\varepsilon_p)\in\boldsymbol{\mathcal{R}}_p^{\ell\times 1}$, $\boldsymbol{\gamma}_{\acute{s}}=-H_1(pw)$, $\boldsymbol{b}'_{\acute{c}}=\boldsymbol{\alpha}+\boldsymbol{\gamma}_{\acute{s}}$. Abort if $\boldsymbol{b}'_{\acute{c}}\neq\boldsymbol{b}_{\acute{c}}$.
	$\xleftarrow{c,\ \boldsymbol{b}_{\acute{s}},\ k'_{\acute{s}}}$	$v_{\acute{s}}=\text{bits}(\boldsymbol{s}_{\acute{s}}^T,\varepsilon_q,\varepsilon_p)\boldsymbol{b}'_{\acute{c}}+h_1\in\boldsymbol{\mathcal{R}}_p$, $c=\text{bits}(v_{\acute{s}},\varepsilon_p-1,\varepsilon_t)\in\boldsymbol{\mathcal{R}}_t$, $k_{\acute{s}}=\text{bits}(v_{\acute{s}},\varepsilon_p,1)$, $k'_{\acute{s}}=H_2(\acute{c},\acute{s},\boldsymbol{\alpha},\boldsymbol{b}_{\acute{s}},c,\boldsymbol{\gamma}_{\acute{s}})$, $k''_{\acute{s}}=H_3(\acute{c},\acute{s},\boldsymbol{\alpha},\boldsymbol{b}_{\acute{s}},c,\boldsymbol{\gamma}_{\acute{s}})$
Abort if $\boldsymbol{b}_{\acute{s}}\notin\boldsymbol{\mathcal{R}}_p^{\ell\times 1}$. Compute $v_{\acute{c}}=\boldsymbol{b}_{\acute{s}}^T\text{bits}(\boldsymbol{s}_{\acute{c}},\varepsilon_q,\varepsilon_p)+h_1\in\boldsymbol{\mathcal{R}}_p$, $k_{\acute{c}}=\text{bits}(v_{\acute{c}}-2^{\varepsilon_p-\varepsilon_t-1}c+h_2,\varepsilon_p,1)$, $\boldsymbol{\gamma}_{\acute{s}}=-\boldsymbol{\gamma}_{\acute{c}}$. Abort if $k'_{\acute{s}}\neq H_2(\acute{c},\acute{s},\boldsymbol{\alpha},\boldsymbol{b}_{\acute{s}},c,\boldsymbol{\gamma}_{\acute{s}})$. Compute $k'_{\acute{c}}=H_3(\acute{c},\acute{s},\boldsymbol{\alpha},\boldsymbol{b}_{\acute{s}},c,\boldsymbol{\gamma}_{\acute{s}})$, $sk_{\acute{c}\acute{s}}=H_4(\acute{c},\acute{s},\boldsymbol{\alpha},\boldsymbol{b}_{\acute{s}},c,\boldsymbol{\gamma}_{\acute{s}})$.	$\xrightarrow{k'_{\acute{c}}}$	
		Abort if $k'_{\acute{c}}\neq k''_{\acute{s}}$. Compute $sk_{\acute{s}\acute{c}}=H_4(\acute{c},\acute{s},\boldsymbol{\alpha},\boldsymbol{b}_{\acute{s}},c,\boldsymbol{\gamma}_{\acute{s}})$.

confidential parameter. The adversary (any legitimate client) can obtain it. Now only the parameter $\boldsymbol{\gamma}_{\acute{s}}$ in Eq.(1) is not known to the adversary. Notice that

$$\boldsymbol{\gamma}_{\acute{s}} = -H_1(pw) \tag{2}$$

The adversary can test any password λ in the dictionary Dict to check if

$$k'_{\acute{c}} = H_3(\acute{c}, \acute{s}, \boldsymbol{\alpha}, \boldsymbol{b}_{\acute{s}}, c, -H_1(\lambda)), \quad \lambda \in \text{Dict} \tag{3}$$

Once the challenging equation holds for some λ, the adversary can find the target password $pw = \lambda$ or its equivalent password $pw' = \lambda$.

After the adversary retrieves the target password or an equivalent password, he can compute the session key $H_4(\acute{c}, \acute{s}, \boldsymbol{\alpha}, \boldsymbol{b}_{\acute{s}}, c, -H_1(\lambda))$ and launch impersonation attack successfully. By the way, the parameter $seed_A$ is also shared by the client and the server, which is actually used as a secret key.

4 Conclusion

We show the Seyhan-Akleylek key exchange protocol is insecure against offline dictionary attack and impersonation attack. We hope the findings in this note could be helpful for the future work on designing such schemes.

References

[1] Seyhan, K., Akleylek, S.: A new password-authenticated module learning with rounding-based key exchange protocol: Saber.pake. J. Supercomput. 79(16), 17859-17896 (2023)

[2] Menezes, A., Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, USA (1996)