Rebuttal to "Comments on 'Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption'"

Taeho Jung, *Student Member, IEEE*, Xiang-Yang Li, *Senior Member, IEEE*, Zhiguo Wan, and Meng Wan, *Member, IEEE*

***Abstract*—Ma *et al.* recently submitted a comment correspondence which points out a flaw in our paper (a sequel of our earlier paper published in the *Proceedings of IEEE INFOCOM*). The flaw led to the leakage of the system-wide master key; therefore, we improved our own scheme by addressing it.**

I. Summary of the Uncovered Flaw

Our key generation (Section V.B in [1] and IV.B in [2]) let all attribute authorities (*i.e.,* key generators) jointly and securely distribute $D = g^{\sum v_k + \sum d_k}$ to all users where any individual v_k, d_k is kept secret to anyone else but the k-th authority $\mathcal{A}_k$. $g^{\sum v_k}$ works as a system-wide master key which can be composed if and only if all authorities participate in the computation, and it is not supposed to be known to anyone (even the authorities).

However, when $H(att(i))^{r_i} g^{\sum d_k}$ is delivered to the key requester, the authority in charge of the attribute i directly sent out $H(att(i))^{r_i}$, and all single $x_k g^{d_k}$'s where $\prod x_k = 1$. This enabled all key requesters to calculate $g^{\sum d_k} = \prod(x_k g^{d_k})$, and this can recover $g^{\sum v_k}$ from $D = g^{\sum v_k + \sum d_k}$, which allowed attackers to bypass our privilege control by directly using the calculated system-wide master key.[1]

Besides, since x_k is always reused, any valid key requester is able to infer all individual $x_k g^{d_k}$ as well.

II. Addressing the Flaw

It is easy to fix this flaw. All we need to do is to prevent authorities from sending all single $x_k g^{d_k}$'s to key requesters. In order to do so, we let each authority $\mathcal{A}_k$ privately send $H(att(i))^{r_i} \cdot x_k \cdot g^{d_k}$ as a whole to the key requester (*i.e.* kept secret to other authorities) if $\mathcal{A}_k$ is in charge of any attribute of this requester, and he sends only $x_k \cdot g^{d_k}$ if none of the attributes of this requester are under his control.

By doing so, at least one $x_k \cdot g^{d_k}$ remains hidden to the key requesters because authorities do not generate keys for attributes not belonging to the user at all. Then, there must be one authority who sends out $H(att(i))^{r_i} \cdot x_k \cdot g^{d_k}$ instead of $x_k \cdot g^{d_k}$, and key requesters are not able to derive $g^{\sum d_k}$ or $g^{\sum v_k}$.

Also, in order to avoid leakage of individual $x_k g^{d_k}$'s, we simply let all authorities share fresh x_k's for every different attribute. This does not affect the asymptotic complexity of the key generation algorithm since the original complexity is $O(N|\mathbb{A}|)$ where N is the number of authorities and $|\mathbb{A}|$ is the number of attributes in the requested keys for each authority. The extra computation overhead is not noticeable either since it is merely $(N-1)|\mathbb{A}|$ random numbers generation, $2(N-1)|\mathbb{A}|$ multiplications and $|\mathbb{A}|$ exponentiations. The extra communication overhead due to this fix is noticeable since the authority needs to send a large integer (128-256B) to $N-1$ authorities, and it also receives integers from $N-1$ authorities. This is comparable to the original overhead of the key generation algorithm which requires communication of multiple large integers. However, the increment is at most twice of the original communication overhead.

Acknowledgements

The authors express their sincere gratitude to the peer scholars Ma, Hui; Zhang, Rui; and Yuan, Wei from Institute of Information Engineering, Chinese Academy of Sciences, State Key Laboratory of Information Security, who discovered the flaws in their protocols.

References

[1] T. Jung, X. Li, Z. Wan, and M. Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 190–199, Jan. 2014.

[2] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2625–2633.

Manuscript received October 7, 2015; revised November 19, 2015; accepted December 3, 2015. Date of current version February 1, 2016. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Liqun Chen.

T. Jung is with the Department of Computer Science, Illinois Institute of Technology, Chicago, IL 60616 USA (e-mail: tjung@hawk.iit.edu).

X.-Y. Li is with the Department of Computer Science, Illinois Institute of Technology, Chicago, IL 60616 USA, and also with the Department of Computer Science and Technology, TNLIST, Tsinghua University, Beijing 100084, China (e-mail: xli@cs.iit.edu).

Z. Wan is with the Tsinghua National Laboratory for Information Science and Technology, School of Software, Tsinghua University, Beijing 100084, China, and also with the State Key Laboratory of Information Security, Chinese Academy of Sciences, Beijing 100190, China (e-mail: wanzhiguo@tsinghua.edu.cn).

M. Wan is with the Center for Science and Technology Development, Ministry of Education, Beijing 100190, China (e-mail: wanmeng@cutech.edu.cn).

Digital Object Identifier 10.1109/TIFS.2015.2509946

[1] The system-wise master key is not supposed to be known to any user or any authority in the system. This component will exist in valid private key if and only if all authorities jointly generated the private key. All authorities independently perform their key generation tasks, and our scheme does not need a central coordinator for the key generation.