Remarks on *"Analysis of One Popular Group Signature Scheme"* in Asiacrypt 2006

Giuseppe Ateniese[1], Jan Camenisch[2], Marc Joye[3], and Gene Tsudik[4]

[1] Department of Computer Science, The Johns Hopkins University
3400 North Charles Street, Baltimore, MD 21218, USA
ateniese@cs.jhu.edu
[2] IBM Research, Zurich Research Laboratory
Säumertrasse 4, CH-8803 Rüschlikon, Switzerland
jca@zurich.ibm.com
[3] Thomson R&D France, Corporate Research, Security Laboratory
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné, France
marc.joye@thomson.net
[4] Department of Information and Computer Science, University of California
Irvine, CA 92697-3425, USA
gts@ics.uci.edu

Abstract. In [2], a framing 'attack' against the ACJT group signature scheme is presented. This note shows that: (i) the attack framework considered in [2] is *invalid*, and (ii) even within the invalid framework, the specific attack in [2] does not work since forged signatures are strongly deniable. We conclude that there is no security weakness in the ACJT group signature scheme when implemented correctly.

Group signature schemes allow a group member to sign messages *anonymously* on behalf of the group. Moreover, in the case of a dispute, the group manager (GM) can recover the identity of the actual signer. In [1], Ateniese, Camenisch, Joye, and Tsudik introduced a provably secure group signature scheme, the so-called ACJT scheme.

In [2], Zhengjun Cao presents a framing 'attack' against the ACJT scheme. However, the attack is based on the assumption that the group manager knows the value $t = \log_{a_0} a$. This assumption is *invalid* in the verifiable setting considered in [1] since the parameters a, a_0 are verifiably random to GM. In a verifiable setting, there is no trusted party involved but evidence that the parameters are well-formed has to be provided. In the case of random parameters this means, in practice, that they are the outputs of any practical constructions based on AES, SHA-1, 2, etc., in order to create an unpredictable and uncontrollable sequence (where no trusted party is needed). In [1], the SETUP phase is assumed to be verifiable; quoted from [1]: *"We note that, in practice, components of $\mathcal{Y}$ must be verifiable to prevent framing attacks"* (where $\mathcal{Y}$ is the group signature public key). This last sentence is general enough to render invalid the assumption underlying the framing attack in [2], although admittedly we did not detail in the original paper how GM selects the values a, a_0 (for instance, as a function of

$h(S)$ and $h(S_0)$ respectively, for a standard hash $h(\cdot)$ and public strings S and S_0, etc.). See, e.g., IEEE P1363 or ANSI X9.62 for standard methods of selecting parameters verifiably at random.

Note that having a verifiable **or** trusted SETUP phase is also the common assumption of any other group signature schemes in the literature. For instance, in the work of Kiayias and Yung [4], which provides a full proof of a variant of the ACJT scheme in a complete security model, the SETUP phase is assumed to be a trusted operation.

However, the work of Cao [2] points out that the ACJT scheme is secure as long as $t = \log_{a_0} a$ is unknown. Indeed, the ACJT signature is nothing else that a proof of knowledge of values u and v such that:

$$(T_1/{T_3}^x)^u = a^v a_0 \pmod{n} ,$$

where $x = \log_g y$. Now, we note that, if $T_1/{T_3}^x = A_i \pmod{n}$ for some user U_i then GM can forge signatures by setting $u = 0$ and $v = -1/t \bmod \phi(n)$. We stress again that these forgeries are easily avoided in a verifiable setting, as in [1], where GM provides evidence that a, a_0 are random, or in a trusted setting, as in [4], where the generation of a, a_0 is trusted.

Remark. For the sake of completeness, we remark that the specific attack described in [2] is invalid even assuming that GM knows the value t. Indeed, Kiayias [3] first noticed that the signatures in [2] are deniable in a strong sense while clearly regular signatures are not. That is, given the values s_1, s_2 as defined in [2], Kiayias noted that the following equation always holds:

$$(a^{s_2 - c2^{\lambda_1}} a_0^{-c})^{e_i} = a_0^{s_1 - c2^{\gamma_1}} \pmod{n} .$$

Thus, signatures so forged by GM can always be detected and denied. Even if group certificates are hidden, a group member can deny those forged signatures and accuse GM by presenting his e_i value.

Acknowledgments. We are grateful to Aggelos Kiayias and Moti Yung for their insightful comments and suggestions. We thank Zhengjun Cao for providing us with a copy of [2] upon our request.

References

1. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In M. Bellare (Ed.), *Advances in Cryptology – CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 255–270, Springer, 2000.
2. Zhengjun Cao. Analysis of one popular group signature scheme. In X. Lai and K. Chen (Eds.), *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 460–466, 2006.
3. A. Kiayias. Personal communication, November 20, 2006.
4. A. Kiayias and M. Yung. Secure scalable group signature with dynamic joins and separable authorities, International Journal of Security and Networks 2006 - Vol. 1, No.1/2 pp. 24-45. (Previous version: ePrint Technical Report 2004/076, available at URL `http://eprint.iacr.org/2004/076/`)