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 [3], a putative framing "attack" against the ACJT group signature scheme [1] is presented. This note shows that the attack framework considered in [3] is *invalid*. As we clearly illustrate, there is **no security weakness** in the ACJT group signature scheme as long as all the detailed specifications in [1] are being followed.

Group signature schemes allow a group member to sign messages *anonymously* on behalf of the group. In 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 an upcoming paper [3], Cao presents an alleged framing attack against the ACJT scheme. This attack is based on the assumption that the GM knows the value $t = \log_{a_0} a$. This assumption is clearly *invalid* in the verifiable setting considered in [1] since the parameters a and a_0 are verifiably random to GM. Although a verifiable setting involves no trusted party, evidence that the parameters are well-formed must be provided. For random parameters this means that they are generated as the outputs of *practical* pseudo-random functions (PRFs) or pseudo-random permutations (PRPs), such as those based on SHA or AES. This is needed in order to generate an unpredictable output sequence. The SETUP phase in [1] is assumed to be verifiable. We quote directly 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).

The above is general enough to completely invalidate the assumption underlying the alleged framing attack in [3]. However, we admit that the original paper [1] does not describe exactly how GM selects the values a and a_0 (e.g., as a function of $h(S)$ and $h(S_0)$, respectively, for a standard hash function $h(\cdot)$ and public strings S and S_0). Refer to IEEE P1363 and ANSI X9.62 standards for prominent examples of methods used to generate verifiably random parameters.

We further note that a verifiable **or** trusted SETUP phase is a common assumption among many group signature schemes in the literature. For instance, the work of Kiayias and Yung [4], (which provides a full proof of a variant of the ACJT scheme in a complete security model) assumes the SETUP phase to be a trusted operation.

However, we stress that the ACJT scheme is secure as long as $t = \log_{a_0} a$ is unknown. As the proof that GM cannot frame users was rather condensed in [1], we expand it here. Indeed, it is not hard to see that an ACJT group signature amounts to a proof of knowledge of values u and v such that:

$$(T_1/{T_2}^x)^u \equiv a^v a_0 \pmod{n},$$

where $x = \log_g y$ (one of GM's secret keys). Now, we note that, if $T_1/{T_2}^x \equiv A_i \pmod{n}$ for some user U_i, it follows that:

$${A_i}^u \equiv a^v a_0 \pmod{n} \ .$$

In other words, the party who generated a group signature must know values u and v such that this equation holds. A group member, U_i, is able to do so using $u = e_i$ and $v = x_i$ as witnesses.

GM might be able to do so as well, —*provided that it knows $t = \log_{a_0} a$ (and can thus frame any user U_i)*— by setting $u = k(p'q')$, for some k such that u lies in the required range (and thus $u \equiv 0 \pmod{p'q'}$), and $v = -1/t \bmod p'q'$ (cf. Cao [3]). We now show that, if GM does *not* know $\log_{a_0} a$, it is unable to frame a user U_i, i.e., to compute a group signature with $T_1/{T_2}^x \equiv A_i \pmod{n}$.

For the sake of the argument, let us assume that factorization of $n = pq = (2p'+1)(2q'+1)$ is known. We argue that, if GM can produce a group signature with $T_1/{T_2}^x \equiv A_i \pmod{n}$ then it can compute either $\log_{a_0} a$ or a representation of C_2 w.r.t. random bases a and a_0, where C_2 is computed as $a^{x_i} \pmod{n}$ during the JOIN protocol by the user corresponding to U_i.

From the JOIN protocol in [1], we know that ${A_i}^{e_i} \equiv C_2 a_0 \pmod{n}$ holds. Therefore, we conclude that u and v must satisfy:

$${C_2}^u \equiv ({A_i}^u)^{e_i}\, {a_0}^{-u} \equiv a^{ve_i}\, {a_0}^{e_i - u} \pmod{n} \ .$$

First, we assume that $u \equiv 0 \pmod{p'q'}$. Then, we have $1 \equiv (a^v a_0)^{e_i} \pmod{n}$. Now, provided that $\gcd(e_i, p'q') = 1$ (otherwise, GM would leak the factorization of n in the JOIN protocol and it can be verified by U_i), we can conclude that computing a v satisfying $a^v a_0 \equiv 1 \pmod{n}$ (i.e., $v = -1/t \bmod p'q')$[‡] is infeasible under the discrete logarithm assumption. Thus, we get a contradiction and can rule out that $u \equiv 0 \pmod{p'q'}$. W.l.o.g., we now assume that $u \not\equiv 0$

[‡] Note that $\gcd(t, p'q') = 1$ since a is of order $p'q'$.

(mod p'). In this case — since we assume that p' is known — $e_i/u \bmod p'$ can be computed and thus:

$$C_2 \equiv a^{ve_i/u} a_0^{e_i/u-1} \pmod{p},$$

i.e., a representation of C_2 w.r.t. random bases a_0 and a in a group of order a (known) prime, which is infeasible under the discrete logarithm assumption [2] since C_2 was chosen randomly by U_i.

In all cases, we have a contradiction. □

In conclusion, provided that the discrete logarithm problem is hard and that $\log_{a_0} a$ is unknown, the ACJT group signature scheme is provably secure against framing by GM. We point out, once again, that $\log_{a_0} a$ is unknown in the verifiable setting, as in [1], where GM provides evidence that a and a_0 are indeed random. It is similarly unknown in a trusted setting, as in [4], where the generation of a, a_0 is trusted.

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 [3] 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. S. Brands. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, Centrum voor Wiskunde en Informatica (CWI), The Nederlands, April 1993.
3. 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.
4. A. Kiayias and M. Yung. Secure scalable group signature with dynamic joins and separable authorities, International Journal of Security and Networks, volume 1, no. 1/2, pages 24–45, 2006. (Previous version: Cryptology ePrint Archive, Report 2004/076, available at URL `http://eprint.iacr.org/2004/076/`)