Remarks on "Analysis of one popular group signature scheme" in Asiacrypt 2006

Giuseppe Ateniese
Department of Computer Science, The Johns Hopkins University
3400 North Charles Street, Baltimore, MD 21218, USA
E-mail: ateniese@cs.jhu.edu

Jan Camenisch
IBM Research, Zurich Research Laboratory
Säumertrasse 4, CH-8803 Rüschlikon, Switzerland
E-mail: jca@zurich.ibm.com

Marc Joye*
Thomson R&D France, Corporate Research, Security Laboratory
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
E-mail: marc.joye@thomson.net
* Corresponding author

Gene Tsudik
Department of Information and Computer Science, University of California
Irvine, CA 92697-3425, USA
E-mail: gts@ics.uci.edu

Abstract: At Asiacrypt 2006, Cao presented a putative framing 'attack' against the ACJT group signature scheme by Ateniese et al. This paper shows that the attack framework considered by Cao is *invalid*. As we clearly illustrate, there is *no security weakness* in the ACJT group signature scheme as long as all the detailed specifications of the original paper are being followed.

Keywords: Public-key cryptography; group signatures; ACJT scheme.

Reference to this paper should be made as follows: Ateniese, G., Camenisch, J., Joye, M. and Tsudik, G., 'Remarks on "Analysis of one popular group signature scheme" in Asiacrypt 2006', Int. J. Applied Cryptography, Vol. 1, No. 4, pp. 320–322.

Biographical notes: Giuseppe Ateniese is an Associate Professor of Computer Science at the Johns Hopkins University. His main research areas are applied cryptography and system security. He has recently worked on group signatures, RFID privacy, secure storage systems (provable data possession, secure versioning), and proxy re-cryptography.

Jan Camenisch received his Ph.D. in 1998 ("Group Signatures Schemes and Payment Systems Based on the Discrete Logarithm Problem"). In 1998–1999, he was a Research Assistant Professor in Computer Science, University of Aarhus, Denmark. Since 1999, he is a Research Staff Member at IBM Zurich and working on cryptography and network security.

Marc Joye is a Technical Advisor for Thomson R&D, France. He received his Ph.D. in Applied Sciences (Cryptography) from the Université Catholique de Louvain in 1997. In 1998 and 1999, he was a post-doctoral fellow of the National Science Council, Republic of China. From 1999 to 2006, he was with the Card Security Group, Gemplus (now Gemalto), France.

Gene Tsudik is a Professor of Computer Science at the University of California, Irvine (UCI). His research interests are: computer/network security & privacy as well as applied cryptography. He obtained his PhD in Computer Science from the University of Southern California (USC) in 1991. Before coming to UCI in 2000, he was at the IBM Zurich Research Laboratory (1991–1996) and USC Information Sciences Institute (1996–2000).

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 Ateniese et al. (2000), Ateniese, Camenisch, Joye, and Tsudik introduced a provably secure group signature scheme, the so-called ACJT scheme.

In a recent paper, Cao (2006) 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 Ateniese et al. (2000) 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 Ateniese et al. (2000) is assumed to be verifiable. We quote directly from Ateniese et al. (2000):

> "... 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 Cao (2006). However, we admit that our original paper 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 (2006), (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 Ateniese et al. (2000), 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 (2006)). 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 Ateniese et al. (2000), 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),[1] we can conclude that computing a v satisfying $a^v a_0 \equiv 1 \pmod{n}$ (i.e., $v = -1/t \bmod p'q'$)[2] 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 $u \not\equiv 0 \pmod{p'}$. 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 as shown in Brands (1993) 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 Ateniese et al. (2000), where GM provides evidence that a and a_0 are indeed random. It is similarly unknown in a trusted setting, as in Kiayias and Yung (2006), 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 his paper upon our request.

References

Ateniese, G., Camenisch, J., Joye, M., and Tsudik, G. (2000). A practical and provably secure coalition-resistant group signature scheme. In Bellare, M., editor, *Advances in Cryptology – CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 255–270. Springer.

Brands, S. (1993). An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, Centrum voor Wiskunde en Informatica (CWI), The Nederlands.

Cao, Z. (2006). Analysis of one popular group signature scheme. In Lai, X. and Chen, K., editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 460–466. Springer.

Kiayias, A. and Yung, M. (2006). Secure scalable group signature with dynamic joins and separable authorities. *International Journal of Security and Networks*, 1(1/2):24–45. Previous version: Cryptology ePrint Archive, Report 2004/076, available at URL `http://eprint.iacr.org/2004/076/`.

Notes

[1]We remind the reader that e_i is chosen by GM as a (large) prime in a prescribed interval Γ so that this condition is automatically satisfied; further checking that e_i is a prime in Γ can be verified at any time (e.g., in case of disputes).

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