Short Group Signatures Without Random Oracles

Bo Qin\textsuperscript{1,2} (秦 波), Qian-Hong Wu\textsuperscript{3} (伍前红), Willy Susilo\textsuperscript{3}, Yi Mu\textsuperscript{2} (穆 恬), Yu-Min Wang\textsuperscript{1} (王育民) and Zheng-Tao Jiang\textsuperscript{4} (姜正涛)

1 National Key Laboratory of Integrated Service Networks, Xi’an University, Xi’an 710071, China
2 Department of Mathematics, School of Science, Xi’an University of Technology, Xi’an 710048, China
3 Center for Information Security Research, School of Information Technology and Computer Science 
University of Wollongong, NSW, Australia
4 School of Computer Science and Technology, Beihang University, Beijing 100083, China

E-mail: qinbo@xaut.edu.cn; \{qhwxmu, wsusilo\}@uw.edu.au; zzt.jiang@163.com

Received November 22, 2006; revised April 12, 2007.

Abstract We propose short group signature (GS) schemes which are provably secure without random oracles. Our basic scheme is about 14 times shorter than the Boyen-Waters GS scheme at Eurocrypt 2006, and 42\% shorter than the recent GS schemes due to Ateniese et al. The security proofs are provided in the Universally Composable model, which allows the proofs of security valid not only when our scheme is executed in isolation, but also in composition with other secure cryptographic primitives. We also present several new computational assumptions and justify them in the generic group model. These assumptions are useful in the design of high-level protocols and may be of independent interest.

Keywords group signature, information security, standard model, universally composable model

1 Introduction

Group signatures, introduced by Chaum and van Heyst\textsuperscript{[1]}, have many applications such as e-cash and anonymous authentication\textsuperscript{[2,3]}. In this notion, any group member can sign messages on behalf of the group, and the resulting signatures keep the identity of signer secret but a third party can open the signature if required. The early GS schemes were usually analyzed by investigating whether they independently satisfied a number of security properties. Later, Bellare, Micciancio, and Warinschi (BMW)\textsuperscript{[4]} introduced a modern formalism for static groups. As noted by Kiayias and Yung\textsuperscript{[5]}, the BMW definition models a primitive of a relaxed GS as it requires a key-issuing center to generate all keys in the system and distributes them to the group manager and group members. In \textsuperscript{[6]}, Ateniese et al. introduced an alternative definition of GS schemes, which has the advantage to allow the proofs of security valid not only when the protocol is executed in isolation, but also in composition with other secure protocols.

The security of most GS schemes and their variants (e.g., \textsuperscript{[7}~\textsuperscript{11]}) are proven in the random oracle model\textsuperscript{[12]}. These schemes are very efficient and rely on various computational assumptions such as the \(\gamma\)-SDH assumption\textsuperscript{[7,13]}, the Strong RSA assumption\textsuperscript{[8,10]} and the LRSW assumption\textsuperscript{[14,15]}. In this model, the scheme in \textsuperscript{[7]} takes about 1533 bits for achieving an RSA-1024 security level. It is the shortest GS in the random oracle model. Although this methodology leads to the construction of efficient and provably secure schemes, the recent results due to Barak et al.\textsuperscript{[16,17]} showed that there exist signature and encryption schemes that are provably secure in the random oracle model, but any implementation of the random oracle results in insecure schemes. Hence, due to the importance of GS schemes, it is essential to have GS schemes that are secure in the standard model.

In the standard model, there are few known schemes in the literatures. Bellare et al.\textsuperscript{[4]} presented the first construction secure in the standard model. Their construction is a theoretic result rather than a practical one as they use generic Non-Interactive Zero Knowledge (NIZK) techniques, which are very inefficient in practice.

Recently, following the BMW model, the first practical GS secure without random oracles has been proposed at Eurocrypt 2006 by Boneh and Waters\textsuperscript{[18]}. 

\textsuperscript{1} Regular Paper
\textsuperscript{2} This work is supported by the National Natural Science Foundation of China under Grant No. 60473027, ARC Discovery Grant of Australia under Grant No. DP0557493 and China Postdoctoral Science Foundation (Grant No. 2006040095).
They presented this scheme by exploiting the Waters' identity-based signatures\cite{19} and the recent NIZK proofs due to Groth, Ostrovsky and Sahai\cite{20}. The attractive feature of this scheme relies on relatively weak assumptions, namely the well-known CDH assumption and a newly introduced Subgroup Decision assumption\cite{21}. Nonetheless, there are several drawbacks in the scheme. The group public key and signatures are of logarithmic length in the number of users and hence the GS size grows according to the group scale. The situation is deteriorated by the long representation (at least 1025 bits) of group elements as their scheme requires the Subgroup Decision assumption, which is derived from factorizing the composite order of pairing groups. Moreover, due to the weakness of the underlying BN model, the security, especially the culpability (informally, a rogue group manager cannot frame an honest group member) can only be provided via an external trusted third party that generates all group members' keys.

More recently, Ateniese, Camenisch, Hohenberger and Medeiros (ACHM) strengthened the security models for GS by incorporating the Universally Composable/Reactive framework. Under their definition, they presented rather efficient GS schemes secure without random oracles\cite{6}. Their construction is based on a variation of the Camenisch-Lysyanskaya signature\cite{15,22}, which is directly obtained from the LRSW assumption\cite{15}. The realization of the scheme is achieved using the bilinear pairings, and an adapted version of the Boneh-Boyen signature\cite{7}. Compared with the Boyen-Waters scheme, the ACHM construction relies on stronger assumptions, namely the Strong LRSW assumption\cite{22} and their newly introduced Strong SXDH assumption\cite{6,22,23}. Their basic GS requires about 2052 bits for an RSA-1024 security level. It is the most efficient GS without random oracles proposed in the literature so far.

**Our Contributions.** We propose short GS schemes without random oracles. The security is proven in the strengthened definition of GS schemes due to Ateniese et al.\cite{6}. Our basic scheme is about 14 times shorter than the BW GS at Eurocrypt 2006\cite{18} for a middle-scale group of 128 members, and 42% shorter than the recent ACHM GS scheme\cite{6}. The scheme is proven secure in the Universally Composable/Reactive framework, which allows the proofs of security valid not only when our scheme is executed in isolation, but also in composition with other secure cryptographic primitives. We also presented several new computational assumptions and justify them in the generic group model. These assumptions are useful in the design of high-level protocol and may be of independent interest.

**Organization of the Paper.** In the next section, we review the security definition of GS schemes. Section 3 presents the underlying computational assumptions related to our constructions. We propose our short GS schemes in Section 4. The security is proven in Section 5. We justify the underlying computational assumptions of our schemes in Section 6, followed with conclusions in the last section.

## 2 Security Definition of GS Schemes

We follow the definition in \cite{6} as it is composable. The definition is based on the ideal/real world model\cite{24-26}. In the real world, there are a number of parties who together execute a GS scheme $\mathcal{G}S$. A number of these parties may be corrupted by the adversary $\mathcal{A}$ (all the corrupted parties are combined into this single adversary). Each party receives its input and reports its output to the environment $\mathcal{E}$. $\mathcal{A}$ and $\mathcal{E}$ may arbitrarily interact. In the ideal world, there are the same parties and each party receives its input and reports its output to $\mathcal{E}$. However, instead of running the real $\mathcal{G}S$, the parties provide its inputs to and receive their outputs from a trusted party $\mathcal{F}_{\mathcal{G}S}$ as an ideal GS functionality.

Let $(\mathcal{A}(a), \mathcal{B}(b)) \leftarrow P(A(x), B(y))$ denote an interactive protocol between $\mathcal{A}$ and $\mathcal{B}$ in which $\mathcal{A}$ and $\mathcal{B}$ have respective inputs $x, y$, and respective outputs $a, b$. We now describe $\mathcal{G}S$ in the real world and $\mathcal{F}_{\mathcal{G}S}$ in the ideal world.

**Real World.** A GS scheme $\mathcal{G}S$ has the usual types of players: a group manager $\mathcal{G}M$, a number of users $U_i$ and a verifier $V$. $\mathcal{G}S$ consists of the algorithms $\mathcal{G}Gen, \mathcal{U}Gen, Join, GSgn, VSgn, Open, VOpen$ defined as follows.

- $(PK, SK) \leftarrow \mathcal{G}Gen(1^\lambda)$ is a probabilistic polynomial time (PPT) algorithm which, on input a security parameter $\lambda$, outputs the group manager $\mathcal{G}M$’s public/private key pair $(PK, SK)$.
- $(pk_{U_i}, sk_{U_i}) \leftarrow \mathcal{U}Gen(1^\lambda)$ is a PPT algorithm which, on input a security parameter $\lambda$, outputs a group member $U_i$’s public/private key pair $(pk_{U_i}, sk_{U_i})$.
- $(\mathcal{G}M(T_{U_i}), U_i(C_{U_i})) \leftarrow \mathcal{Join}(\mathcal{G}M(pk_{U_i}, SK), (PK, sk_{U_i}))$ enables a user $U_i$ joins the signatory group managed by $\mathcal{G}M$. $U_i$’s output is a personalized group signing credential $C_{U_i}$, or an error message. $\mathcal{G}M$’s output is some tracing information $T_{U_i}$ which allows $\mathcal{G}M$ to revoke the anonymity of any signature generated by $U_i$. $\mathcal{G}M$ adds the record $(pk_{U_i}, T_{U_i})$ to its local database $\mathcal{D}_{tr}$.
- $\sigma \leftarrow \mathcal{GSgn}(sk_{U_i}, C_{U_i}, m)$ is a PPT algorithm which, on input a group member $U_i$’s private key $sk_{U_i}$, its signing credential $C_{U_i}$, and a message string $m$, outputs a GS $\sigma$. 
