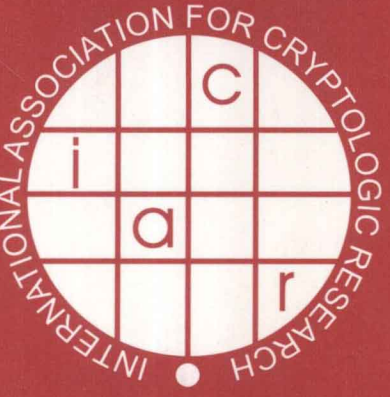
Tatsuaki Okamoto
Xiaoyun Wang (Eds.)

Public Key Cryptography – PKC 2007

LNCS 4450

10th International Conference
on Practice and Theory in Public-Key Cryptography
Beijing, China, April 2007, Proceedings



Springer

Tatsuaki Okamoto Xiaoyun Wang (Eds.)

Public Key Cryptography – PKC 2007

10th International Conference
on Practice and Theory in Public-Key Cryptography
Beijing, China, April 16-20, 2007
Proceedings

Springer

Volume Editors

Tatsuaki Okamoto
NTT Laboratories, Nippon Telegraph and Telephone Corporation
Japan
E-mail: okamoto.tatsuaki@lab.ntt.co.jp

Xiaoyun Wang
Shandong University and Tsinghua University
China
E-mail: xywang@sdu.edu.cn

Library of Congress Control Number: 2007923868

CR Subject Classification (1998): E.3, F.2.1-2, C.2.0, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-71676-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-71676-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12042999 06/3180 5 4 3 2 1 0

Preface

The 10th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2007) was held at Tsinghua University in Beijing, China, April 16–20, 2007. PKC is the premier international conference dedicated to cryptology focusing on all aspects of public-key cryptography. The event is sponsored by the International Association of Cryptologic Research (IACR), and this year it was also sponsored by the National Natural Science Foundation of China (NSFC) and Tsinghua University.

The conference received 118 submissions, and the Program Committee selected 29 of these for presentation. The Program Committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to public-key cryptography. Each paper was anonymously reviewed by at least three Program Committee members.

Extended abstracts of the revised versions of the accepted papers are in these proceedings. The program also included three invited lectures by Rafail Ostrovsky with UCLA, USA, Shige Peng with Shandong University, China and Adi Shamir with the Weizmann Institute of Science, Israel. Two papers regarding the invited lectures are included in these proceedings. The PKC 2007 Program Committee had the pleasure of awarding this year's PKC best paper award to Xavier Boyen and Brent Waters for their paper, entitled "Full-Domain Subgroup Hiding and Constant-Size Group Signatures."

We are extremely grateful to the Program Committee members for their enormous investment of time and effort in the difficult and delicate process of review and selection. We gratefully acknowledge the help of a large number of external reviewers who reviewed submissions in their area of expertise. We also thank the PKC Steering Committee for their support.

Electronic submissions were made possible by the Web Review system, iChair, developed by Thomas Baignéres and Matthieu Finiasz at EPFL, LASEC. We would like to thank Thomas Baignéres and Matthieu Finiasz for their great support.

We deeply thank Andrew C. Yao, the General Chair, for his effort in organizing and making this conference possible. The great scientist was the source of the success of PKC 2007.

We are grateful to all the Organizing Committee members for their volunteer work. In addition, we would like to thank Wei Yu for his enormous support in installing and operating the iChair system in the review process and editing of these proceedings.

We wish to thank all the authors, for submitting papers, and the authors of accepted papers for their cooperation.

February 2007

Tatsuaki Okamoto
Xiaoyun Wang

PKC 2007

The 10th International Conference on Theory and Practice of Public-Key Cryptography

Tsinghua University, Beijing, China, April 16–20, 2007

Sponsored by the *International Association of Cryptologic Research (IACR)*, *National Natural Science Foundation of China* and *Tsinghua University*.

General Chair

Andrew C. Yao, Tsinghua University, China

Program Co-chairs

Tatsuaki Okamoto, NTT, Japan
Xiaoyun Wang, Tsinghua University, China

Organizing Committee

Andrew C. Yao ..... Tsinghua University, China
Xiaoyun Wang ..... Tsinghua University, China
Yuexuan Wang ..... Tsinghua University, China
Xiaoming Sun ..... Tsinghua University, China
Hongbo Yu ..... Tsinghua University, China
Qi Feng ..... Tsinghua University, China
Meiqin Wang ..... Shandong University,China

Program Committee

Feng Bao ..... I2R, Singapore
Jung Hee Cheon ..... Seoul National University, Korea
Alfredo De Santis ..... University of Salerno, Italy
Yvo Desmedt ..... UCL, UK
Giovanni Di Crescenzo ..... Telcordia Tech., USA
Steven Galbraith ..... Royal Holloway University of London, UK
Juan Garay ..... Bell labs, USA
Jonathan Katz ..... University of Maryland, USA
Kwangjo Kim ..... ICU, Korea
Hugo Krawczyk ..... IBM, USA
Arjen Lenstra ..... Lucent, USA
Anna Lysyanskaya ..... Brown University, USA
Alfred Menezes ..... University of Waterloo, Canada
Kazuo Ohta ..... University of Electro-Communications, Japan

Rafail Ostrovsky ..... UCLA, USA
Dingyi Pei ..... Guangzhou University, China
David Pointcheval ..... ENS, France
C. Pandu Rangan ..... IIT Madras, India
Hovav Shacham ..... Weizmann Institute, Israel
Igor Shparlinski ..... Macquarie University, Australia
Serge Vaudenay ..... EPFL, Switzerland
Frances Yao ..... City University of Hong Kong, Hong Kong, China
Moti Yung ..... Columbia University, USA
Yuliang Zheng ..... University of North Carolina at Charlotte, USA

Steering Committee

Ronald Cramer ..... CWI and Leiden University, The Netherlands
Yvo Desmedt ..... University College London, UK
Hideki Imai (Chair) ..... AIST and Chuo University, Japan
Kwangjo Kim ..... Information and Communications University, Korea
David Naccache ..... ENS, France
Tatsuaki Okamoto ..... NTT, Japan
Jacques Stern ..... ENS, France
Moti Yung ..... RSA Laboratories and Columbia University, USA
Yuliang Zheng (Secretary) .... University of North Carolina at Charlotte, USA

External Reviewers

Michel Abdalla
Patrick Amon
Paolo D Arco
Joonsang Baek
Thomas Baigneres
Caroline Belrose
Olivier Billet
Colin Boyd
Dan Brown
Qingjun Cai
Sebastien Canard
Melissa Chase
Carlos Cid
Scott Contini
Cecile Delerablee
Alex Dent
Konidala M. Divyan
Junwu Dong
Dang Nguyen Duc
Ratna Dutta
Yuichiro Esaki
Serge Fehr
Anna Lisa Ferrara
Matthieu Finiasz
Pierre-Alain Fouque
Rosario Gennaro
Nick Howgrave Graham
Jens Groth
Shai Halevi
Safuat Hamdy
Yoshikazu Hanatani
Darrel Hankerson
Jason Hinek
Qiong Huang
James Hughes
Sebastien Kunz Jacques
Ellen Jochemsz
Pascal Junod
Marcelo Kaihara
Alexandre Karlov
Yutaka Kawai
Aggelos Kiayias
Eike Kilt
Woo-Hwan Kim
Thorsten Kleinjung
Yuichi Kokubun
Vlad Kolesnikov
Yuichi Komano
Takahiro Kondo
Chiu-Yuen Koo
Noboru Kunihiro
Kaoru Kurosawa
Taekyoung Kwon
Rob Lambert
Kristin Lauter
Munkyu Lee
Jin Li
Yong Li
Vo Duc Liem
Seongan Lim

Perret Ludovic
Daegun Ma
Benoit Chevallier Mames
Barbara Masucci
Alex May
Alexander May
Maria Meyerovich
Anton Mityagin
Satoshi Miyagawa
Payman Mohassel
David Molnar
Jean Monnerat
Siguna Mueller
Phong Nguyen
Phong Q. Nguyen
Takashi Nishide
Haruki Ota
Duong Hieu PHAN
Sylvain Pasini
Kenny Paterson
Manas Patra
Ludovic Perret
Benny Pinkas
Tal Rabin
Leonid Rayzin
Pankaj Rohatgi
Bagus Santoso
Benjamin Smith
Martijn Stam
Ron Steinfeld
Rene Struik
Willy Susilo
Chunming Tang
Emmanuel Thome
Xiaojian Tian
Jacques Traore
Berkant Ustaoglu
Jose Villegas
Ivan Visconti
Martin Vuagnoux
Shabsi Walfish
Brent Waters
Christopher Wolf
Duncan S. Wong
David Woodruff
Yongdong Wu
Guomin Yang
Jeong Hyun Yi
Kazuki Yoneyama
Hyojin Yoon
Xiaolai Zhang

Table of Contents

Signatures I

Invited Talk I

Cryptanalysis

Protocols I

Signatures II

Multivariate Cryptosystems

Encryption

Protocols II

Invited Talk II

Number Theoretic Techniques

Public-Key Infrastructure

Full-Domain Subgroup Hiding and Constant-Size Group Signatures

Xavier Boyen[1] and Brent Waters[2,*]

[1] Voltage Inc., Palo Alto
xb@boyen.org
[2] SRI International
bwaters@csl.sri.com

Abstract. We give a short constant-size group signature scheme, which we prove fully secure under reasonable assumptions in bilinear groups, in the standard model. We achieve this result by using a new NIZK proof technique, related to the BGN cryptosystem and the GOS proof system, but that allows us to hide integers from the full domain rather than individual bits.

1 Introduction

Group signatures, introduced by Chaum and van Heyst [19], allow any member of a certain group to sign a message on behalf of the group, but the signer remains anonymous within the group. However, in certain extenuating circumstances an authority will have the ability to revoke the anonymity of a signer and trace the signature. One of the primary motivating use scenarios of group signatures is in anonymous attestation, which has practical applications such as in building Trusted Platform Modules (TPMs). Group signatures have also attracted much attention in the research community where several constructions have been proposed [1,2,3,5,6,9,12,13,14,15,16,25,27,29].

The most efficient group signature constructions given only have a proof of security in the random oracles model and either are based on the Strong-RSA assumption in Z_n [2,3,16] or use bilinear groups [9,11,17]. Solutions in the standard model can be derived from general assumptions as first shown by Bellare et. al. [5].

Recently, two efficient group signature schemes were respectively proposed both by Boyen and Waters [13] and Ateniese et al. [1] that did not use random oracles. The two solutions took different approaches and have different features.

The Boyen-Waters construction used a two-level hierarchical signature, where the first level corresponds to the signer's identity and the second level is the message to be signed. The scheme hides the actual identity in the first level by using bilinear groups of composite order and applying a mechanism from the recent Non-Interactive Zero-Knowledge (NIZK) result of Groth, Ostrovsky, and

* Supported by NSF CNS-0524252 and the US Army Research Office under the CyberTA Grant No. W911NF-06-1-0316.

T. Okamoto and X. Wang (Eds.): PKC 2007, LNCS 4450, pp. 1–15, 2007.

Sahai [23]. The two drawbacks of the Boyen-Waters result are that the number of group elements in the signature are logarithmic in the number of signers in the group and that the anonymity property is only secure against chosen-plaintext attacks, as opposed to chosen-ciphertext attacks. The need for a logarithmic number of group elements results from the fact that a signer must prove that the blinded first level identity was computed correctly. The authors needed to use the model for CPA attacks because the tracing authority used the knowledge of the factorization of the order to trace members.

The Ateniese et. al. scheme works in asymmetric bilinear groups. Their scheme has signatures with a constant number of group elements and has chosen-ciphertext security. However, its proofs of security rely on interactive assumptions where the adversary has access to an oracle; therefore, these assumptions are inherently non-falsifiable [28]. In addition, the scheme has the drawback that if a user's private key is compromised then it can be used to revoke the anonymity of that user's past signatures. Although, it should be pointed out that some schemes have used this property as an advantage in Verifier-Local Group signatures [11].

Groth [21] also gave a recent group signature scheme that was proven CCA-secure in the standard model under the decisional Linear assumption [9]. Signatures in his scheme technically consist of a constant number of group elements, however, as noted by the author the constant is too large for real systems and in practice his constant will be much more than $\lg(n)$ for any reasonable number of n signers. The result does though, give a feasibility result under a relatively mild assumption.

In this paper we give a new construction of a group signature scheme that addresses some of the drawbacks of the Boyen-Waters [13] solution. Following their scheme we use a two-level hierarchical signature as the basis for our signatures, where the first level specifies the identity. However, we use a new signature on the first level based off an assumption related to Strong Diffie-Hellman (SDH) [8] that we call the Hidden Strong Diffie-Hellman, which like SDH and Strong-RSA has the property that the adversary has flexibility in what he is allowed to return to the challenger. The signature has the property that if the signer gives a signature on an arbitrary group element this can be used to break our assumption. We provide efficient proofs of well-formmess that use techniques beyond those given in [23], including proofs of encrypted Diffie-Hellman tuples. One disadvantage of this approach is that it uses a stronger assumption for unforgeability than CDH, which was used in the Boyen-Waters [13] scheme. However, we emphasize that this assumption is falsifiable.

2 Preliminaries

We review a number of useful notions from the recent literature on pairing-based cryptography, which we shall need in later sections. First, we briefly review the properties that constitute a group signature scheme and define its security.

We take this opportunity to clarify once and for all that, in this paper, the word "group" by default assumes its algebraic meaning, except in contexts such

as "group signature" and "group manager" where it designates a collection of users. There should be no ambiguity from context.

2.1 Group Signatures

A group signature scheme consists of a pentuple of PPT algorithms:

- A group setup algorithm, *Setup*, that takes as input a security parameter 1^λ (in unary) and the size of the group, 2^k, and outputs a public key PK for verifying signatures, a master key MK for enrolling group members, and a tracing key TK for identifying signers.
- An enrollment algorithm, *Enroll*, that takes the master key MK and an identity ID, and outputs a unique identifier s_{ID} and a private signing key K_{ID} which is to be given to the user.
- A signing algorithm, *Sign*, that takes a group member's private signing key K_{ID} and a message M, and outputs a signature σ.
- A (usually deterministic) verification algorithm, *Verify*, that takes a message M, a signature σ, and a group verification key PK, and outputs either `valid` or `invalid`.
- A (usually deterministic) tracing algorithm, *Trace*, that takes a valid signature σ and a tracing key TK, and outputs an identifier s_{ID} or the failure symbol $\perp$.

There are four types of entities one must consider:

- The group master, which sets up the group and issues private keys to the users. Often, the group master is an ephemeral entity, and the master key MK is destroyed once the group is set up. Alternatively, techniques from distributed cryptography can be used to realize the group master functionality without any real party becoming in possession of the master key.
- The group manager, which is given the ability to identify signers using the tracing key TK, but not to enroll users or create new signing keys.
- Regular member users, or signers, which are each given a distinct private signing key K_{ID}.
- Outsiders, or verifiers, who can only verify signatures using the public key PK.

We require the following correctness and security properties.

Consistency. The consistency requirements are such that, whenever, (for a group of 2^k users)

$$(\mathsf{PK}, \mathsf{MK}, \mathsf{TK}) \leftarrow \mathit{Setup}(1^\lambda, 2^k),$$
$$(s_{\mathsf{ID}}, K_{\mathsf{ID}}) \leftarrow \mathit{Enroll}(\mathsf{MK}, \mathsf{ID}), \qquad \sigma \leftarrow \mathit{Sign}(K_{\mathsf{ID}}, M),$$

we have, (except with negligible probability over the random bits used in *Verify* and *Trace*)

$$\mathit{Verify}(M, \sigma, \mathsf{PK}) = \mathtt{valid}, \qquad \text{and} \qquad \mathit{Trace}(\sigma, \mathsf{TK}) = s_{\mathsf{ID}}.$$

The unique identifier s_{ID} can be used to assist in determining the user ID from the transcript of the *Enroll* algorithm; s_{ID} may but need not be disclosed to the user; it may be the same as ID.

Security. Bellare, Micciancio, and Warinschi [5] characterize the fundamental properties of group signatures in terms of two crucial security properties from which a number of other properties follow. The two important properties are:

Full Anonymity which requires that no PPT adversary be able to decide (with non-negligible probability over one half) whether a challenge signature σ on a message M emanates from user ID_1 or ID_2, where ID_1, ID_2, and M are chosen by the adversary. In the original definition of [5], the adversary is given access to a tracing oracle, which it may query before and after being given the challenge σ, much in the fashion of IND-CCA2 security for encryption.

Boneh, Boyen, and Shacham [9] relax this definition by withholding access to the tracing oracle, thus mirroring the notion of IND-CPA security for encryption. We follow [9] and speak of *CCA2-full anonymity* and *CPA-full anonymity* for the respective notions.

Full Traceability which requires that no coalition of users be able to generate, in polynomial time, a signature that passes the *Verify* algorithm but fails to trace to a member of the coalition under the *Trace* algorithm. According to this notion, the adversary is allowed to ask for the private keys of any user of its choice, adaptively, and is also given the secret key TK to be used for tracing—but of course not the enrollment master key MK.

It is noted in [5] that this property implies that of *exculpability* [4], which is the requirement that no party should be able to frame a honest group member as the signer of a signature he did not make, not even the group manager. However, the model of [5] does not consider the possibility of a (long-lived) group master, which leaves it as a potential framer. To address this problem and achieve the notion of *strong exculpability*, introduced in [2] and formalized in [26,6], one would need an interactive enrollment protocol, call *Join*, at the end of which only the user himself knows his full private key; the same mechanism may also enable concurrent dynamic group enrollment [6,27].

We refer the reader mainly to [5] for more precise definitions of these and related notions.

2.2 Bilinear Groups of Composite Order

We review some general notions about bilinear maps and groups, with an emphasis on groups of *composite order* which will be used in most of our constructions. We follow [10] in which composite order bilinear groups were first introduced in cryptography.

Consider two finite cyclic groups G and G_T having the same order n, in which the respective group operation is efficiently computable and denoted multiplicatively. Assume that there exists an efficiently computable function $e : G \times G \to G_T$, called a bilinear map or pairing, with the following properties:

- (Bilinearity) $\forall u, v \in G$, $\forall a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$, where the product in the exponent is defined modulo n;

– (Non-degeneracy) $\exists g \in G$ such that $e(g, g)$ has order n in G_T. In other words, $e(g, g)$ is a generator of G_T, whereas g generates G.

If such a bilinear map can be computed efficiently, the group G is called a bilinear group. We remark that the vast majority of cryptosystems based on pairings assume for simplicity that bilinear groups have prime order. In our case, it is important that the pairing be defined over a group G containing $|G| = n$ elements, where $n = pq$ has a (ostensibly hidden) factorization in two large primes, $p \neq q$.

2.3 Complexity Assumptions

We make use of a few complexity assumptions: computational Diffie-Hellman (CDH) in the prime-order bilinear subgroup G_p, Subgroup Decision in the group G of composite order $n = pq$, and a new assumption in G_p related to Strong Diffie-Hellman (SDH) that we call HSDH.

CDH in Bilinear Groups. The CDH assumption states that there is no probabilistic polynomial time (PPT) algorithm that, given a triple $(g, g^a, g^b) \in G_p^3$ for random exponents $a, b \in \mathbb{Z}_p$, computes $g^{ab} \in G_p$ with non-negligible probability. Because of the pairing, CDH in G_p implies a "Gap DH" assumption [24] and should not be confused with the vanilla CDH assumption in usual non-pairing groups. It is also subsumed by the HSDH assumption we describe later.

The Subgroup Decision Assumption. Our second tool is the Subgroup Decision assumption introduced in [10]. It combines features of bilinear pairings with the hardness of factoring, which is the reason for working with bilinear groups of composite order.

Informally, the Subgroup Decision assumption posits that for a bilinear group G of composite order $n = pq$, the uniform distribution on G is computationally indistinguishable from the uniform distribution on a subgroup of G (say, G_q, the subgroup of order q). The precise definition is based on the subgroup decision problem, which we now define.

Consider an "instance generator" algorithm $\mathcal{GG}$ that, on input a security parameter 1^λ, outputs a tuple (p, q, G, G_T, e), in which p and q are independent uniform random λ-bit primes, G and G_T are cyclic groups of order $n = pq$ with efficiently computable group operations (over their respective elements, which must have a polynomial size representation in λ), and $e : G \times G \to G_T$ is a bilinear map. Let $G_q \subset G$ denote the subgroup of G of order q. The subgroup decision problem is:

> On input a tuple $(n = pq, G, G_T, e)$ derived from a random execution of $\mathcal{GG}(1^\lambda)$, and an element w selected at random either from G or from G_q, decide whether $w \in G_q$.

The advantage of an algorithm $\mathcal{A}$ solving the subgroup decision problem is defined as $\mathcal{A}$'s excess probability, beyond $\frac{1}{2}$, of outputting the correct solution. The probability is defined over the random choice of instance and the random bits used by $\mathcal{A}$.

The HSDH Assumption. Last, we need to introduce a new assumption we call Hidden SDH by analogy to the SDH assumption [8] from which it descends. We present it in the next section.

3 The Hidden Strong Diffie-Hellman Assumption

We introduce a new assumption in the prime-order bilinear group G_p. It is a variant of the Strong Diffie-Hellman (SDH) assumption proposed in [8]. It is slightly stronger, but retains the attributes of the original assumption of being non-interactive, falsifiable, and provably true in the generic bilinear group model.

The Strong Diffie-Hellman assumption in bilinear groups states that there is no probabilistic polynomial time (PPT) adversary that, given a $(\ell+1)$-tuple $(g, g^{\omega}, g^{\omega^2}, \ldots, g^{\omega^{\ell}}) \in G_p^{\ell+1}$ for a random exponent $\omega \in \mathbb{Z}_p^*$, outputs a pair $(c, g^{1/(\omega+c)}) \in \mathbb{Z}_p^* \times G_p$ with non-negligible probability. (The parameter ℓ is defined externally.) What makes the SDH assumption useful is that it implies the hardness of the following problem:

> On input two generators $g, g^{\omega} \in G_p$, and $\ell-1$ distinct pairs $(c_i, g^{1/(\omega+c_i)}) \in \mathbb{Z}_p^* \times G_p$, output an additional pair $(c, g^{1/(\omega+c)}) \in \mathbb{Z}_p^* \times G_p$ such that $c \neq c_i$ for all $i = 1, \ldots, \ell-1$.

This argument was used by Boneh and Boyen [8] as the basis of their secure signature constructions. In particular, Boneh and Boyen's primordial "weakly secure signature" on a message c is nothing more than the group element $g^{1/(\omega+c)}$. Much of their paper is concerned with securing these signatures against *adaptive* chosen message attacks, but for our purposes this is unnecessary.

However, an inherent trait of the general notion of signature is that verification requires knowledge of the message. Since in our group signature the first-level "message" is the identity of the user, we would like to keep it as hidden as possible, since at the end of the day we need to blind it. To facilitate this task, we build a modified version of the Boneh-Boyen "weak signature" above that does not require knowledge of c in order to verify. It is based on the Hidden SDH assumption, a straightforward extension to the SDH assumption where the "message" c is not given in the clear.

The Hidden Strong Diffie-Hellman Problem. We first define the ℓ-HSDH problem as follows:

> On input three generators $g, h, g^{\omega} \in G_p$, and $\ell-1$ distinct triples $(g^{1/(\omega+c_i)}, g^{c_i}, h^{c_i}) \in G_p^3$ where $c_i \in \mathbb{Z}_p$, output another such triple $(g^{1/(\omega+c)}, g^c, h^c) \in G_p^3$ distinct of all the others.

Observe that the well-formedness of a triple $(A, B, C) = (g^{1/(\omega+c)}, g^c, h^c)$ can be ascertained without knowing c by verifying that $e(A, g^{\omega}B) = e(g, g)$ and that $e(B, h) = e(C, g)$. In these verifications, the Diffie-Hellman relationship

(g, h, g^c, h^c) serves as a discrete-log NIZK proof of knowledge of c. Notice that contrary to the SDH problem statement [8], here we allow c or some c_i to be zero.

We define the advantage of an HSDH adversary $\mathcal{A}$ as its probability of outputting a valid triple. The probability is taken over the random choice of instance and the random bits used by $\mathcal{A}$.

Definition 1. *We say that the ℓ-HSDH assumption holds in a family of prime order bilinear groups generated by $\mathcal{GG}$, if there is no PPT algorithm that, for sufficiently large $\lambda \in \mathbb{N}$, solves the HSDH problem in the bilinear group $(p, G_p, e) \leftarrow \mathcal{GG}(1^\lambda)$ with non-negligible probability. Here, ℓ may be either an explicit parameter to the assumption, or some polynomially bounded function of the security parameter λ.*

It is easy to see that for any $\ell \geq 1$, hardness of the ℓ-HSDH problem implies hardness of the ℓ-SDH problem in the same group, which itself requires the CDH problem to be hard in that group. To bolster our confidence in the new complexity assumption, we can prove an $\Omega(\sqrt{p/\ell})$ lower bound on the complexity of solving the HSDH problem in generic bilinear groups, provided that $\ell < \sqrt[3]{p}$. Notice that HSDH does not rely on the composite order n, so the generic group model can apply. The proof will appear in the full paper.

4 Anonymous Hierarchical Signatures

As our first step toward short group signatures, we build a hierarchical signature with the signer identity at the first level and the message being signed at the second level, such that the whole signature can be verified without revealing the identity.

In a hierarchical signature, a message is a tuple comprising several atomic message components. The crucial property is that a signature on a message $(m_1, \ldots, m_i)$, also acts as a restricted private key that enables the signing of any message extension $(m_1, \ldots, m_i, \ldots, m_j)$ of which the original message is a prefix. In some schemes, the hierarchy has a maximum depth d, in which case we must have $i \leq j \leq d$. Here, we shall only consider 2-level hierarchical signatures, in which the first level is concerned with user identities, and the second level with messages proper. Notice that 2-level hierarchical signatures and identity-based signatures are equivalent notions: the identity-based key is just a fancy name for a signature on a first-level atomic component.

We use the HSDH assumption to construct a short two-level hierarchical signature that can be verified without knowing the user identity at the first level. Our construction makes a hybrid of two schemes, one at each level.

First Level. At the first level, we devise a variant of the "primary" deterministic Boneh-Boyen signatures from [8, §3.2]. Recall that Boneh-Boyen signatures are constructed in two stages, beginning with a primary "weak" deterministic signature, which is subsequently hardened with a sprinkle of randomness. The