Feng Bao San Ling
Tatsuaki Okamoto Huaxiong Wang
Chaoping Xing (Eds.)

LNCS 4856

# Cryptology and Network Security

6th International Conference, CANS 2007
Singapore, December 2007
Proceedings

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
i a c r

Springer

Feng Bao   San Ling   Tatsuaki Okamoto
Huaxiong Wang   Chaoping Xing (Eds.)

# Cryptology and Network Security

6th International Conference, CANS 2007
Singapore, December 8-10, 2007
Proceedings



Springer

Volume Editors

Feng Bao
Institute for Infocomm Research
Singapore
E-mail: baofeng@i2r.a-star.edu.sg

San Ling
Nanyang Technological University
Singapore
E-mail: lingsan@ntu.edu.sg

Tatsuaki Okamoto
NTT Laboratories
Japan
E-mail: okamoto.tatsuaki@lab.ntt.co.jp

Huaxiong Wang
Nanyang Technological University
Singapore
E-mail: hxwang@ntu.edu.sg

Chaoping Xing
Nanyang Technological University
Singapore
E-mail: matxcp@nus.edu.sg

Library of Congress Control Number: 2007939802

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-76968-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-76968-2 Springer Berlin Heidelberg New York



Springer is a part of Springer Science+Business Media

springer.com


Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12196395 06/3180 5 4 3 2 1 0

# Preface

The sixth International Conference on Cryptology and Network Security (CANS 2007) was held at the Grand Plaza Park Hotel, Singapore, 8–10 December 2007. The conference was sponsored by *Nanyang Technological University* and the *Lee Foundation*, Singapore.

The goal of CANS is to promote research on all aspects of cryptology and network security, as well as to build a bridge between research on cryptography and network security. The first International Conference on Cryptology and Network Security was held in Taipei, Taiwan, in 2001. The second one was held in San Francisco, California, USA, on September 26–28, 2002, the third in Miami, Florida, USA, on September 24–26, 2003, the fourth in Xiamen, Fujian, China, on December 14–16, 2005 and the fifth in Suzhou, Jiangsu, China, on December 8–10, 2006.

The program committee accepted 17 papers from 68 submissions. The reviewing process took nine weeks, each paper was carefully evaluated by at least three members of the program committee. We appreciate the hard work of the members of the program committee and the external referees who gave many hours of their valuable time.

In addition to the contributed papers, there were six invited talks:

- Artur Ekert: *Quantum Cryptography*
- Christian Kurtsiefer: *Aspects of Practical Quantum Key Distribution Schemes*
- Keith Martin: *A Bird's-Eye View of Recent Research in Secret Sharing*
- Mitsuru Matsui: *The State-of-the-Art Software Optimization of Block Ciphers and Hash Functions*
- Josef Pieprzyk: *Analysis of Modern Stream Ciphers*
- David Pointcheval: *Adaptive Security for Password-Based Authenticated Key Exchange in the Universal-Composability Framework.*

We would like to thank all the people involved in organising this conference. In particular, we would like to thank the organising committee for their time and efforts, and Krystian Matusiewicz for his help with LaTeX.

December 2007

Feng Bao<br>San Ling<br>Tatsuaki Okamoto<br>Huaxiong Wang<br>Chaoping Xing

# 6th International Conference on Cryptology and Network Security (CANS 2007)

Sponsored by

Nanyang Technological University, Singapore
Lee Foundation, Singapore

## CANS Steering Committee

| | |
|---|---|
| Yvo Desmedt | University College London, UK |
| Matt Franklin | UC, David, USA |
| Yi Mu | University of Wollongong, Australia |
| David Pointcheval | CNRS and ENS, France |
| Huaxiong Wang | Nanyang Technological University, Singapore |

## General Chairs

| | |
|---|---|
| San Ling | Nanyang Technological University, Singapore |
| Chaoping Xing | National University of Singapore, Singapore |

## Program Chairs

| | |
|---|---|
| Feng Bao | Institute for Infocomm Research, Singapore |
| Tatsuaki Okamoto | NTT Labs, Japan |

## Program Committee

| | |
|---|---|
| Michel Abdalla | École Normale Supérieure, France |
| Colin Boyd | QUT, Australia |
| Mike Burmester | Florida State University, USA |
| Hao Chen | Fudan University, China |
| Liqun Chen | HP Bristol Labs, UK |
| Robert Deng | SMU, Singapore |
| Alex Dent | Royal Holloway, UK |
| Eiichiro Fujisaki | NTT Labs, Japan |
| Jun Furukawa | NEC, Japan |
| David Galindo | École Normale Supérieure, France |
| Aline Gouget | Gemalto, France |
| Amir Herzberg | Bar Ilan University, Israel |

| | |
|---|---|
| Atsuo Inomata | JST, Japan |
| Akinori Kawachi | Titech, Japan |
| Angelos Keromytis | Columbia University |
| Aggelos Kiayias | University of Connecticut, USA |
| Hiroaki Kikuchi | Tokai University, Japan |
| Eike Kiltz | CWI, Netherlands |
| Kwangjo Kim | Info. and Comm. University, Korea |
| Arjen Lenstra | EPFL, Switzerland |
| Peng Chor Leong | NTU, Singapore |
| Javier Lopez | University of Malaga, Spain |
| Mitsuru Matsui | Mitsubishi Electric, Japan |
| Yi Mu | University of Wollongong, Australia |
| Joern Mueller-Quade | University of Karlsruhe, Germany |
| Antonio Nicolosi | NYU & Stanford University, USA |
| Kenny Paterson | Royal Holloway, UK |
| Olivier Pereira | UCL, Belgium |
| Giuseppe Persiano | Università di Salerno, Italy |
| Josef Pieprzyk | Macquarie University, Australia |
| C. Pandu Rangan | IIT, India |
| Frederic Rousseau | EADS, France |
| Rei Safavi-Naini | University of Calgary, Canada |
| Berry Schoenmakers | TU Eindhoven, Netherlands |
| Jorge Villar | Universitat Politècnica de Catalunya, Spain |
| Xiaoyun Wang | Shandong University, China |
| Duncan Wong | City University of Hong Kong, China |
| Sung-Ming Yen | National Central University, Taiwan |
| Yiqun Lisa Yin | Security Consultant, USA |
| Yunlei Zhao | Fudan University, China |
| Jianying Zhou | $I^2R$, Singapore |

## Organising Committee

| | |
|---|---|
| Huaxiong Wang | Nanyang Technological University, Singapore |
| Eiji Okamoto | Tsukuba, Japan |
| Guat Tin Goh | Nanyang Technological University, Singapore |
| Hwee Jin Soh | Nanyang Technological University, Singapore |
| Sen How Chia | Nanyang Technological University, Singapore |

## External Referees

| | | |
|---|---|---|
| Frederik Armknecht | Scott Contini | Eiichiro Fujisaki |
| Sébastien Canard | Cunsheng Ding | Steven Galbraith |
| Kai Yuen Cheong | Gerardo Fernandez | Clemente Galdi |
| Benoit Chevallier-Mames | Pierre-Alain Fouque | Paul Hoffman |

Qiong Huang
Tetsu Iwata
Shaoquan Jiang
Marcelo Kaihara
Tomi Klein
David Lacour
Byoungcheon Lee
Homin K. Lee
Wei-Chih Lien
Benoit Libert
Krystian Matusiewicz
Cedric Ng
Juan Gonzalez Nieto
Christopher Portmann
Geraint Price
M-R Reyhanitabar
Stefan Röhrich
Ryo Sakaguchi
Siamak F. Shahandashti
Tom Shrimpton
Martijn Stam
Kohtaro Tadaki
Qian Tang
Jheng-Hong Tu
Marion Videau
Nguyen Vo
Martin Vuagnoux
Bo-Ching Wu
Chi-Dian Wu
Qianhong Wu
Chih-Hung Wang
Guomin Yang
Kan Yasuda
Hong-Sheng Zhou

# Table of Contents

## Public Key Encryption



## Intrusion Detection



## Email Security



## Denial of Service Attacks



## Authentication

# Mutative Identity-Based Signatures or Dynamic Credentials Without Random Oracles

Fuchun Guo[1], Yi Mu[2,⋆], and Zhide Chen[1,⋆⋆]

[1] Key Lab of Network Security and Cryptology
School of Mathematics and Computer Science
Fujian Normal University, Fuzhou, China
fuchunguo1982@gmail.com,
zhidechen@fjnu.edu.cn

[2] Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong, Wollongong NSW 2522, Australia
ymu@uow.edu.au

**Abstract.** We introduce a new identity-based signature scheme that possesses the feature of mutability in terms of its mutable signer identity. We name this new signature scheme *Mutative Identity-Based Signature* (MIBS). The merit of this proposed scheme lies in the novel property on protection of private information such as birthdate, social security number, credit card number, etc. that have to be employed as part of a user identity served as a public key. In MIBS, we allow all these private information to serve as a user identity, while only one of these information (along with the user name, as non-secret part of a user identity) is revealed to the verifier. For example, when using a signature to a legitimate merchant, only the credit card number and the user name are revealed without leaking other private information. This signature scheme is naturally associated with a *dynamic* credential system, where a signature accommodates the feature of a secret credential. We provide a security model and then prove its security based on the $q$-Strong Diffie-Hellman ($q$-SDH) problem and the Computational Diffie-Hellman (CDH) problem in the standard model.

**Keywords:** ID-based Signature, Mutative Identity.

## 1 Introduction

In 1984, Shamir [11] first introduced the idea of Identity-Based (or ID-based) Signature (IBS), aimed to create a signature on a message where any user can verify the signature using the signer's public information such as email address, ID numbers or telephone numbers instead of a conventional public key in order to simply the certificate management. Since Boneh and Franklin [2] introduced the first ID-Based Encryption (IBE) from pairings in 2001, several novel IBS

⋆ This project was partially supported by the UoW Near Miss grant.
⋆⋆ Partially supported by Science and Technology of Fujian Province (2006F5036).

F. Bao et al. (Eds.): CANS 2007, LNCS 4856, pp. 1–14, 2007.

schemes have been proposed (e.g., in the random oracle model [6,9,5] and in the standard model [10]).

An ID-based system requires a constant identity of a user. This identity must be fixed as the unique public key. We are motivated by the following scenario.

A normal identity such as a user name or an email address is not sufficient to identify a user. For instance, two users could have the exactly same name. Because of this, a compound identity accommodating multiple information about a user identity such as name, birthdate, tax number, driver's licence number, credit card number, etc. is used. However, some information in this compound identity are private to some parties but non-private to some others. For example, a client can provide his name along with his credit card number to a legitimate merchant, while his birthdate should not be revealed.

A clumsy solution to the privacy of compound identity is to allow the private key generator to create a number of private keys for a user. Each private key is associated with a piece of the compound identity, i.e., the public key is composed of a general identity (e.g. a user's name) and an extra identity (e.g. a credit card number). A signature is created in terms of the piece of identity that can be revealed to the verifier. This approach is obviously problematic due to difficulty in key management.

Motivated by the above scenario, in this paper, we present a new notion of IBS: *Mutative Identity-Based Signature* (MIBS). In MIBS, a public key (the compound identity) is composed of the basic public information (non-private identity) and extra information (private identities). A compound identity maps a single private signing key. When a signature is formed, the signer can choose which piece of the compound identity should be revealed to the verifier. Our scheme can be considered as a private credential scheme with dynamic and selective private contents. In this scenario, The private key generator can be considered as a credential issuer. A credential can be *dynamically* generated (signed) by the private key holder. Furthermore, our scheme can also be applied to multi-identity-based access control. That is, a user has a number of identities that form an unique compound identity. An identity in the compound identity is associated with a key for accessing an entity.

We provide a security model and then prove its security based on the $n$-Strong Diffie-Hellman ($n$-SDH, known as $q$-SDH) problem and the Computational Diffie-Hellman (CDH) problem in the standard model.

**Road Map:** In Section 2, we provide the definitions of MIBS, including the security model and the complexity assumption. In Section 3, we review the accumulator technique from Nguyen's construction. In Section 4, we propose our MIBS scheme and its security proof against chosen message attacks. In Section 5, we give some discussions. We conclude our paper in Section 6.

## 2 Definition

A Mutative Identity-Based Signature (MIBS) can be described as the following algorithms:

Setup: This algorithm is run by the Private Key Generator (PKG). On input a security parameter $1^k$, it outputs master public parameters *params* and master secret key. The PKG publishes *params* and keeps the master secret key.

KeyGen: This algorithm is run by the PKG. On input *params*, the master secret key and a compound identity $U = \langle ID, A_1, A_2, \cdots, A_t \rangle$ $(1 \leq t \leq n)$, it outputs the signing key $d_u$ of $U$, where $ID$ is the basic non-private information and $A_i$ are private information.

Sign: This algorithm is run by the signer. On input the signing key $d_U$, a compound identity $U$, a verification identity $V_u = \langle ID, A_i \rangle$, a message $M$ and *params*, it outputs the verification key $v_k$ (only the verification identity $V_u$ exposes to the verifier) and the signature $\sigma$, where $A_i \in \langle A_1, A_2, \cdots, A_t \rangle$ is decided by the original signer.

Verify: This algorithm is run by any verifier. On input the signature $(M, v_k, \sigma)$ and *params*, it outputs **accept** if the signature is valid on $M$ for verification identity $V_u$; otherwise outputs **reject**.

### 2.1 Security Model

Mutative Identity-Based Signature (MIBS) is unforgeable against the chosen message attack, denoted by UF-MIBS-CMA, where the game between a challenger and an adversary is described as follows:

**Setup:** The challenger runs the algorithm Setup of the MIBS scheme and gives the master public *paramas* to the adversary.

**Queries:** The adversary adaptively makes a number of different queries to the challenger. Each query can be one of the following.

- Signing Key Queries. The adversary makes queries on the signing key of $U = \langle ID, A_1, A_2, \cdots, A_t \rangle$. The challenger responds by running the algorithm KenGen and forwarding the signing key $d_u$ to the adversary.
- Signature Queries. The adversary makes queries on the signature of $(U, V_u, M)$ of compound identity $U = \langle ID, A_1, A_2, \cdots, A_t \rangle$, where $V_u = \langle ID, A_i \rangle$. The challenger responds by first running algorithm KeyGen to generate the signing key $d_u$ and then running the algorithm Sign to obtain a signature $\sigma$, which is forwarded to the adversary.

**Forgery:** The adversary outputs a signature $(M^*, v_k^*, \sigma^*)$ of compound identity $U^*$ and verification identity $V_u^*$. The adversary succeeds if the following hold true:

- $\sigma^*$ is a valid signature on $M^*$ for verification identity $V_u^*$;
- No signing key query on $U^*$. No signature query on $(U^*, V_u', M^*)$ for any $V_u'$.

The advantage of an adversary in the above game is defined as

$$Adv_{\mathcal{A}} = \Pr[\mathcal{A} \ succeeds]$$

**Definition 1.** *An adversary $\mathcal{A}$ is said to be an $(\epsilon, t, q_k, q_s)$-forger of a MIBS if $\mathcal{A}$ has at least $\epsilon$ advantage in the above game, runs in time at most $t$ and makes at most $q_k$ and $q_s$ queries on the signing key and the signature. A MIBS scheme is said to be $(\epsilon, t, q_k, q_s)$-secure if no $(\epsilon, t, q_k, q_s)$-forger exists.*

### 2.2 Bilinear Pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of prime order $p$. Let $g$ be a generator of $\mathbb{G}$. A map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is called a bilinear pairing (map) if this map satisfies the following properties:

- Bilinear: for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$;
- Non-degeneracy: $e(g, g) \neq 1$. In other words, if $g$ be a generator of $\mathbb{G}$, then $e(g, g)$ generates $\mathbb{G}_T$;
- Computability: There is an efficient algorithm to compute $e(u, v)$ for all $u, v \in \mathbb{G}$.

### 2.3 Complexity Assumption

The security of our MIBS scheme will be reduced to the hardness of $n$-Strong Diffie-Hellman ($n$-SDH) problem and the Computational Diffie-Hellman (CDH) problem in the group in which the signature is constructed. So, We briefly review the definition of the $n$-SDH problem and the CDH problem [7,10]:

**Definition 2.** *Let $\mathbb{G}$ be the group defined as above with a generator $g$ and elements $g^s, g^{s^2}, \cdots, g^{s^n} \in \mathbb{G}$ where $s$ is selected uniformly at random from $\mathbb{Z}_p$, the $n$-SDH problem in $\mathbb{G}$ is to compute $\langle c, g^{1/c+s}\rangle$ for any $c \in \mathbb{Z}_p/\{-s\}$.*

**Definition 3.** *We say that the $(\epsilon_A, t_A)$ $n$-SDH assumption holds in the group of $\mathbb{G}$ if there is no algorithm running in time $t_A$ at most can solve the $n$-SDH problem in $\mathbb{G}$ with the probability at least $\epsilon_A$.*

**Definition 4.** *Let $\mathbb{G}$ be the group defined as above with a generator $g$ and elements $g^a, g^b \in \mathbb{G}$ where $a, b$ are selected uniformly at random from $\mathbb{Z}_p$, the CDH problem in $\mathbb{G}$ is to compute $g^{ab}$.*

**Definition 5.** *We say that the $(\epsilon, t)$-CDH assumption holds in the group of $\mathbb{G}$ if there is no algorithm running in time $t$ at most can solve the CDH problem in $\mathbb{G}$ with the probability at least $\epsilon$.*

## 3 Accumulator Overview

The idea of accumulator was first introduced by Benaloh and de Mare [1] and further developed in [3]. Basically, an accumulator scheme is an algorithm where we can combine a large set of elements into one short one. For a given element, if it was included into the accumulator, then there must be a corresponding witness; otherwise it is impossible to find such a witness. Camenisch and Lysyanskaya introduced dynamic accumulators [4], which allow us to dynamically delete and add elements from/into the original set. Recently, Nguyen [8] presented a dynamic accumulator scheme from bilinear pairings and used it to construct an ID-based ring signature. Accumulators is a useful technique that has a number of applications.

### 3.1 Definition

A secure accumulator $f : X \times Y \rightarrow X$ for a family inputs $\{y_i\}$ is a function with the following properties:

- Efficient evaluation: On input $(u, y_i) \in X \times Y$, outputs a value $v \in X$, where $X$ is an accumulator domain for the function $f$ and $Y$ is the domain whose elements are to be accumulated;
- Quasi-commutative: $f(f(u, y_1), y_2) = f(f(u, y_2), y_1)$, i.e. the communication is independent of the order of $y_i$ for all accumulated elements;
- Witnesses: Let $v \in X$ and $x \in X$. A value $w \in X$ is called a witness for $x$ in $v$ under $f$ if $f(w, x) = v$;
- Security(Collision Resistant): Let $\mathbf{A} = f(u, Y^*)$ be the accumulator of $Y^* = \{y_i\}$. It is hard for all adversaries to forge an accumulator value $y' \notin Y^*$ and a witness $w'$ such that $\mathbf{A} = f(w', y')$.

### 3.2 Accumulator from Bilinear Pairing

We make use of Nguyen's accumulator scheme from Bilinear Pairing [8] defined as follows: Let $T = (g, g^s, g^{s^2}, \cdots, g^{s^n})$ be the tuple of elements from $\mathbb{G}$ and $u = g^z$ for some known $z$ randomly from $\mathbb{Z}_p$. The secure accumulator based on the number of elements in $T$ is defined as:

$$f(u, y_i) = u^{y_i+s} = g^{z(y_i+s)}$$

which satisfies the requirements of a secure accumulator.

- Efficient evaluation: For $u \in \mathbb{G}$ and $Y^* = \{y_1, y_2, \cdots, y_t\} \in \mathbb{Z}_p \setminus \{-s\}$, where $n$ elements in $Y^*$ at most, the accumulator value is

$$f(u, Y^*) = g^{z(y_1+s)(y_2+s)\cdots(y_t+s)}$$

  can be computed in time polynomial in $t$ from $T, z$ and $\{y_1, y_2, \cdots, y_t\}$ without the knowledge of the auxiliary information $s$.
- Quasi-commutative:

$$f(f(u, y_1), y_2) = g^{z(y_1+s)(y_2+s)} = f(f(u, y_2), y_1).$$

- Witness: The witness for $y_t$ in $f(u, Y^*)$ are two elements $\mathrm{W}_0, \mathrm{W}_1 \in \mathbb{G}$, where

$$\mathrm{W}_0 = g^{z(y_1+s)(y_2+s)\cdots(y_{t-1}+s)}, \quad \mathrm{W}_1 = g^{zs(y_1+s)(y_2+s)\cdots(y_{t-1}+s)}$$

which can be verified by

$$e\Big(\mathrm{W}_0, g^s\Big) = e\Big(g^{z(y_1+s)(y_2+s)\cdots(y_{t-1}+s)}, g^s\Big) = e\Big(\mathrm{W}_1, g\Big)$$

$$\mathbf{A} = (\mathrm{W}_0)^{y_t}\mathrm{W}_1 = g^{z(y_1+s)(y_2+s)\cdots(y_t+s)}.$$

- Security (Collision Resistant): It holds according to the following theorem.

**Theorem 1.** *The accumulator is Collision Resistant if the n-SDH assumption holds, where n is the upper bound on the number of elements to be accumulated by the accumulator.*

Proof. [8]. □

# 4 The MIBS Scheme

## 4.1 Construction

Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be the bilinear map, $\mathbb{G}, \mathbb{G}_T$ be two cyclic groups of order $p$ and $g$ be the corresponding generator in $\mathbb{G}$. We set $z \equiv 1$ of the accumulator scheme in our MIBS scheme.

**Setup:** The system parameters are generated as follow: Select two secrets $\alpha, \beta \in \mathbb{Z}_p$ at random, choose $g, g_2, u_0, m_0$ randomly from $\mathbb{G}$, and set the value $g_1 = g^\alpha, k_i = g^{\beta^i}$ for all $i \in \{1, 2, \cdots, n\}$. Choose one vector $\boldsymbol{u} = (u_i)$ of length $n_u$ and one vector $\boldsymbol{m} = (m_i)$ of length $n_m$, where $u_i, m_i \in \mathbb{G}$. A collision-resistant hash functions $H : \{0,1\}^* \to \{0,1\}^{n_u}$. The master public *params* and the master secret key are

$$params = (g, g_1, g_2, k_1, k_2, \cdots, k_q, u_0, \boldsymbol{u}, m_0, \boldsymbol{m}, H), \quad \text{secret key} = \alpha, \beta.$$

**KeyGen:** To generate a signing key for $U = \langle ID, A_1, A_2, \cdots, A_n\rangle$, where all $A_i \in \mathbb{Z}_p$, PKG does the following:

- Compute the accumulator value $\mathbf{A}_U = g^{(A_1+\beta)(A_2+\beta)\cdots(A_n+\beta)} \in \mathbb{G}$;
- Compute the hash value $h_U = H(ID, \mathbf{A}_U) \in \{0,1\}^{n_u}$;
- Let $h_U[i]$ be the $i$th bit of $h_U$. Define $\mathcal{H}_U \subset \{1, 2, \cdots, n_u\}$, the set of indices, such that $h_U[i] = 1$. Pick a random $r$ and outputs $d_U$, where

$$d_U = (d_1, d_2) = \Big(g_2^\alpha(u_0 \prod_{i\in\mathcal{H}_U} u_i)^r, g^r\Big)$$

Note that there are two ways for the PKG to compute the accumulator: using $g, A_i$ and the master secret key $\beta$ and using $g, A_i$ and all $k_i$ in the master *params* without the master secret key $\beta$. However, the computational cost of the second way is higher.

**Sign:** To generate a signature $\sigma$ on $M \in \{0,1\}^{n_m}$ of identity $\langle ID, A_i\rangle$ with $d_U$, the signer does the following:

- Compute the two witnesses

$$\mathbf{W}_0 = g^{(A_1+\beta)\cdots(A_{i-1}+\beta)(A_{i+1}+\beta)\cdots(A_n+\beta)},$$

$$\mathbf{W}_1 = g^{\beta(A_1+\beta)\cdots(A_{i-1}+\beta)(A_{i+1}+\beta)\cdots(A_n+\beta)},$$

from $U$ and $k_1, k_2, \cdots, k_n$.
- Output the verification key

$$v_k = \Big(\langle ID, A_i\rangle, \mathbf{W}_1, \mathbf{W}_2\Big) \equiv (\langle ID, A_i\rangle, \sigma_1, \sigma_2).$$

- Let $M[j]$ be the $j$th bit of $M$. Define $\mathcal{M} \subset \{1, 2, \cdots, n_m\}$, the set of indices, such that $M[j] = 1$. Pick a random $s$ and outputs the signature:

$$\sigma_{A_i} = \Big(g_2^{\alpha}(u_0 \prod_{i\in\mathcal{H}_U} u_i)^r (m_0 \prod_{j\in\mathcal{M}} m_j)^s, g^r, g^s\Big) \equiv (\sigma_3, \sigma_4, \sigma_5).$$

**Verify:** Let $(v_k, \sigma_{A_i}) = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ be a valid signature for $(\langle ID, A_i\rangle, M)$. A verifier does the following:

- Check if the following equation holds:

$$e(\sigma_1, k_1) = e(\sigma_2, g).$$

- Compute $\mathbf{A}_U = \sigma_1^{A_i}\sigma_2$ and its hash value $h_U = H(ID, \mathbf{A}_U)$.
- Accept the signature $\sigma$ if the following equation holds

$$e\Big(\sigma_3, g\Big) = e\Big(g_2, g_1\Big) \cdot e\Big(u_0 \prod_{i\in\mathcal{H}_U} u_i, \sigma_4\Big) \cdot e\Big(m_0 \prod_{j\in\mathcal{M}} m_j, \sigma_5\Big).$$

**Correctness**

$$\begin{aligned} e(\sigma_1, k_1) &= e\Big(g^{(A_1+\beta)\cdots(A_{i-1}+\beta)(A_{i+1}+\beta)\cdots(A_n+\beta)}, g^{\beta}\Big) \\ &= e\Big(g^{\beta(A_1+\beta)\cdots(A_{i-1}+\beta)(A_{i+1}+\beta)\cdots(A_n+\beta)}, g\Big) \\ &= e(\sigma_2, g). \end{aligned}$$

$$\begin{aligned} e(\sigma_3, g) &= e\Big(g_2^{\alpha}(u_0 \prod_{i\in\mathcal{H}_U} u_i)^r (m_0 \prod_{j\in\mathcal{M}} m_j)^s, g\Big) \\ &= e\Big(g_2^{\alpha}, g\Big)\ e\Big((u_0 \prod_{i\in\mathcal{H}_U} u_i)^r, g\Big)\ e\Big((m_0 \prod_{j\in\mathcal{M}} m_j)^s, g\Big) \\ &= e\Big(g_2, g_1\Big) e\Big(u_0 \prod_{i\in\mathcal{H}_U} u_i, \sigma_4\Big) e\Big(m_0 \prod_{j\in\mathcal{M}} m_j, \sigma_5\Big). \end{aligned}$$

### 4.2 Analysis

In both Waters identity-based encryption scheme [12] and Paterson and Schuldt identity-based signature scheme [10], the identity space is $\{0,1\}^{n_u}$ for a fixed $n_u$ and can be extended to an arbitrary string using a collision-resistant hash function such that a hash value can only represent an "identity," where the extension can achieve the same level of security.

In our MIBS scheme, the verification key is the triple $(V_u, \mathbf{W}_0, \mathbf{W}_1)$ and the signer, knowing the full compound identity, can change the verifying key in terms of the actual application. The extra information in a compound identity is hidden in the witness, while the verifier can only know one of $\{A_i\}$. However, the final accumulated value for a compound identity is the same, i.e. the final "public key" of $H(ID, \mathbf{A}_U)$ is constant in each signing. So, when the security of accumulator holds and collision-resistant hash function holds, the hash value of $H(ID, \mathbf{A}_U)$ represents the "identity" of $U = \langle ID, A_1, A_2, \cdots, A_t\rangle$. I.e. All adversaries cannot find $U' \neq U$ and $U' = \langle ID', A_1', A_2', \cdots, A_t'\rangle$ such that $H(ID, \mathbf{A}_U) = H(ID', \mathbf{A}_{U'})$.

According to the definition of the security model and our construction, we know that the success of forging a valid signature on $V_u^*$ by the adversary actually is on $H(ID^*, \mathbf{A}_U^*)$ of $U^*$ that cannot be queried. So, with the same idea of both Waters and Paterson-Schuldt, we can only prove the security in the identity space of $\{0,1\}^{n_u}$, i.e., we define that the adversary is successful in forging a valid signature of an identity $H(ID^*, \mathbf{A}_U^*)$ even if it knows nothing about the actually identity in $H(ID^*, \mathbf{A}_U^*)$. The interaction between a challenger and an adversary are described as follows:

**Setup:** The challenger runs the algorithm Setup of the MIBS scheme and gives the master public *paramas* to the adversary.

**Queries:** The adversary adaptively makes a number of different queries to the challenger. Each query can be one of the following.

- Signing Key Queries. The adversary makes an query on a bit string of $h_U = \{0,1\}^{n_u}$. The challenger responds by running the algorithm KenGen and forwarding the signing key $d_u$ to the adversary. Note that, the challenger can just run the last step of algorithm KeyGen.
- Signature Queries. The adversary makes query on the signature of $(h_U, M)$. The challenger responds by first running algorithm KeyGen to generate the signing key $d_u$ and then running the algorithm Sign to obtain a signature $\sigma$ without $\mathbf{W}_0, \mathbf{W}_1$, which is forwarded to the adversary.

**Forgery:** The adversary outputs a signature $(M^*, h_U^*, \sigma^*)$ of string $h_U^*$. The adversary succeeds if the following hold true:

- $\sigma^*$ is a valid signature on $M^*$ for $h_U^*$;
- No signing key query on $h_U^*$ and no signature query on $(h_U^*, M^*)$.