Theoretical Computer Science 520 (2014) 51–61

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Identity based identification from algebraic coding theory

Guomin Yang [a,*,1], Chik How Tan [b], Yi Mu [a], Willy Susilo [a,2], Duncan S. Wong [c,2]

[a] School of Computer Science and Software Engineering, University of Wollongong, Australia
[b] Temasek Laboratories, National University of Singapore, Singapore
[c] Department of Computer Science, City University of Hong Kong, Hong Kong

ARTICLE INFO

Article history:
Received 19 October 2012
Received in revised form 17 April 2013
Accepted 8 September 2013
Communicated by X. Deng

Keywords:
Identity based cryptography
Identification
Error-correcting codes
Syndrome decoding

ABSTRACT

Cryptographic identification schemes allow a remote user to prove his/her identity to a verifier who holds some public information of the user, such as the user public key or identity. Most of the existing cryptographic identification schemes are based on number-theoretic hard problems such as Discrete Log and Factorization. This paper focuses on the design and analysis of identity based identification (IBI) schemes based on algebraic coding theory. We first revisit an existing code-based IBI scheme which is derived by combining the Courtois–Finiasz–Sendrier signature scheme and the Stern zero-knowledge identification scheme. Previous results have shown that this IBI scheme is secure under passive attacks. In this paper, we prove that the scheme in fact can resist active attacks. However, whether the scheme can be proven secure under concurrent attacks (the most powerful attacks against identification schemes) remains open. In addition, we show that it is difficult to apply the conventional OR-proof approach to this particular IBI scheme in order to obtain concurrent security. We then construct a special OR-proof variant of this scheme and prove that the resulting IBI scheme is secure under concurrent attacks.

1. Introduction

Remote user identification is one of the fundamental research topics in cryptography, and is very useful in practice. We can separate public key user identification schemes into two categories: standard identification (SI), and identity based identification (IBI). In a standard identification scheme, the verifier has the public key of the prover and uses this public key to verify the genuineness of the remote user, while in an identity based identification scheme, the verifier can perform the verification just based on the prover's identity.

Most of the existing identification schemes follow a three-move (or Σ-type) structure: the prover P initiates an identification protocol by sending a *commitment* Cmt, then the verifier V replies with a *challenge* Ch, and finally P generates a *response* Rsp and sends it to V who makes a final *decision* which is either 'accept' or 'reject'. In [1], Bellare et al. called identification schemes following such a structure *canonical* identification schemes. Many canonical SI and IBI schemes have been proposed in the literature (e.g. [1,11,5,10,14,19,21,20]). The security of these schemes are based on the intractability of several number-theoretic problems such as factorization, discrete log, and RSA. One important application of canonical

* Corresponding author.
E-mail addresses: gyang@uow.edu.au (G. Yang), tsltch@nus.edu.sg (C.H. Tan), ymu@uow.edu.au (Y. Mu), wsusilo@uow.edu.au (W. Susilo), duncan@cityu.edu.hk (D.S. Wong).

[1] Part of the work was done when G. Yang was with Temasek Laboratories, National University of Singapore.

[2] W. Susilo is supported by the ARC Future Fellowship (FT0991397). D.S. Wong is supported by a grant from the RGC of the HKSAR, China (Project No. CityU 121512).

0304-3975/$ – see front matter
http://dx.doi.org/10.1016/j.tcs.2013.09.008

identification schemes is that we can derive a standard signature (SS) (or identity based signature (IBS), resp.) scheme from an SI (or IBI, resp.) scheme via the Fiat–Shamir transformation [11].

From SI/SS to IBI. In [1], Bellare, Namprempre and Neven presented a generic framework to transform any SI scheme satisfying certain conditions into an IBI scheme. The derived IBI scheme will inherit the security of the underlying SI scheme. Independent to Bellare et al.'s work, in [15], Kurosawa and Heng proposed another generic framework that transforms any standard signature scheme, which is existentially unforgeable under adaptive chosen message attacks [13], into an IBI scheme secure against passive adversaries. In [24], Yang et al. further showed that in order to achieve passive security, a standard signature scheme secure under *known* message attacks suffices.

Code-based Cryptography. The first code-based public key cryptosystem was proposed by McEliece [17] in 1978. A variant of the McEliece cryptosystem was later proposed by Niederreiter in [18]. In Asiacrypt 2001, Courtois, Finiasz and Sendrier [8] proposed the first practical code-based digital signature scheme by applying the Full Domain Hash [2,3] to the Niederreiter cryptosystem. The advantage of using algebraic coding theory to construct cryptographic schemes is that these schemes may remain secure even in the post-quantum age.

SI/IBI Based on Algebraic Coding Theory. In [23], Stern proposed a standard identification scheme based on the syndrome decoding problem from algebraic coding theory. However, the Stern identification scheme is not canonical. It requires $3r$ communications rounds between the prover and the verifier where r is a system parameter. Several variants of the scheme are also introduced in [23], including an identity based one. However, no formal security proof was provided for this IBI scheme. In [7,6], Cayrel et al. proposed a new IBI scheme which can be regarded as the combination of a modified version of the Courtois–Finiasz–Sendrier (CFS) digital signature scheme [9] and the Stern identification scheme [23]. In this paper, we refer to this IBI scheme as mCFS-Stern-IBI. In [6], Cayrel et al. proved that mCFS-Stern-IBI is secure under *passive* attacks.

Our contributions. In this paper, we revisit several existing identification schemes based on algebraic coding theory, including the Stern identification scheme and the mCFS-Stern-IBI scheme. We also provide a new security analysis for the mCFS-Stern-IBI scheme by showing that it can in fact achieve *active* security. However, we show that it is difficult to extend the proof to obtain the *concurrent* security (i.e. the highest level of security) of the scheme.

One widely used approach to transform a passive secure IBI scheme into a concurrent secure one is to use the OR-proof technique. However, due to the special design of the mCFS-Stern-IBI scheme, the conventional OR-proof transformation does not work. We then design a new OR-proof system for this particular IBI and obtain a new scheme which is proven secure under concurrent attacks.

2. Preliminaries

In this section, we review the definition and security model for identity based identification schemes. We follow the IBI definition and security model in [1].

2.1. IBI definition

Definition 1. An identity based identification (IBI) scheme consists of four probabilistic polynomial-time (PPT) algorithms $(\mathsf{MKGen}, \mathsf{UKGen}, \mathsf{P}, \mathsf{V})$.

1. MKGen: On input 1^k, where $k \in \mathbb{N}$ is a security parameter, it generates a master public/secret key pair (mpk, msk).
2. UKGen: On input msk and some identity $I \in \{0,1\}^*$, it outputs a user secret key $usk[I]$.
3. (P, V) – User Identification Protocol: The prover with identity I runs algorithm P with initial state $usk[I]$, and the verifier runs V with initial state (mpk, I). The first and last messages of the protocol belong to the prover. The protocol ends when V outputs either 'accept' or 'reject'.

Completeness: For all $k \in \mathbb{N}$, $I \in \{0,1\}^*$, $(mpk, msk) \leftarrow \mathsf{MKGen}(1^k)$, and $usk[I] \leftarrow \mathsf{UKGen}(msk, I)$, an honest V who is initialized with (mpk, I) always outputs 'accept' at the end of the identification protocol after communicating with P who is honest and initialized with $usk[I]$.

2.2. IBI security model

There are three security notions for IBI schemes: impersonation under passive (id-imp-pa), active (id-imp-aa) and concurrent (id-imp-ca) attacks.

Definition 2 *(id-imp-pa).* For an IBI scheme $(\mathsf{MKGen}, \mathsf{UKGen}, \mathsf{P}, \mathsf{V})$, consider the following game between a simulator $\mathcal{S}$ and an adversary $\mathcal{A}$.

1. $\mathcal{S}$ generates a master key pair $(mpk, msk) \leftarrow \mathsf{MKGen}(1^k)$ and gives mpk to $\mathcal{A}$. $\mathcal{S}$ also maintains two user sets: HU and CU, which stand for Honest Users and Corrupted Users, respectively. Initially, both HU and CU are empty.