MinRank Based Three-Pass Identification Scheme with Half Cheating Probability

Bagus Santoso[1,a)] Yasuhiko Ikematsu[2,b)] Shuhei Nakamura[3,c)]
Takanori Yasuda[4,d)]

Abstract: In Asiacrypt 2001, Courtois proposed the first three-pass zero-knowledge identification (ID) scheme based on the MinRank problem. However, in Courtois' basic ID scheme, the cheating probability, i.e., the success probability of cheating prover, is 2/3, which is larger than half. Although Courtois also proposed a variant scheme which is claimed to have half cheating probability, the security of the variant scheme is not formally proven and it requires another hardness assumption on a specific one-way function and also an additional assumption that verifier always generates challenges according to a specific distribution. In this paper, we propose the first three-pass zero-knowledge ID scheme based on the MinRank problem with the cheating probability of exactly half even with only two-bit challenge space, without any additional assumption. Our proposed ID scheme reduces the necessary number of rounds in order to achieve the targeted security level against impersonation.

Keywords: Minrank Problem, Identification Scheme, Zero-Knowledge

1. Introduction

In 1997, P. Shor [18] showed polynomial-time quantum algorithms to break factoring and discrete logarithm based cryptosystems. Therefore, we need to develop cryptosystems having a resistance to quantum computer attacks. The research area to study such cryptosystems is called post quantum cryptography (PQC) [2]. The most promising candidates for PQC are computational problems based on lattice, isogeny, coding theory, and multivariate polynomials.

In particular, one of computational problems based on multivariate polynomials is *multivariate quadratic* (MQ) problem, which finds a solution to a system of quadratic equations over a finite field. In general, MQ problem is the foundation for constructing multivariate public key cryptosystems (MPKC). There have been a lot of multivariate schemes, HFE [15], UOV [11], Rainbow [6], and so on. Among them, Rainbow gets a lot of attention since it was chosen as a third round candidate [5] in NIST PQC standardization project [14].

On the other hand, many cryptanalysis against multivariate schemes such HFE and Rainbow are not only based on MQ problem, but also another computational problem called MinRank problem. MinRank problem is the problem of finding a linear combination $\sum_{i=1}^{m-1} \alpha_i M_i - M_0$ with a specified rank r from a given set of matrices $\{M_0, \ldots, M_{m-1}\}$. MinRank problem is proven to be NP-complete [3]. Therefore, we can consider cryptographic schemes based on the MinRank problem.

In fact, in Asiacrypt 2001, Courtois [4] proposed the first three-pass zero-knowledge identification (ID) scheme based on the MinRank problem. In Courtois' basic ID scheme, the cheating probability, i.e., the success probability of cheating prover, is 2/3, which is larger than half. As a result, in order to achieve the desired security level against impersonation, Courtois' basic ID scheme needs to be repeated in larger number of rounds compared to the common ID scheme with half cheating probability such as Feige-Fiat-Shamir [9,10] or Schnorr [16,17] ID schemes. This makes the total communication cost of Courtois' basic ID scheme quite high in practice. In the same paper, Courtois also proposed a variant of the basic ID scheme. Courtois claimed that the variant of the basic scheme has cheating probability half (1/2) by employing several additional assumptions: (1) the verifier sends challenge according a certain fixed distribution and (2) a certain special function satisfies one-wayness. However, Courtois did not provide any formal proof that the variant scheme is secure. Moreover, it is not clear how the variant scheme will maintain privacy against an adversary

[1] Department of Computer and Network Engineering, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan.
[2] Institute of Mathematics for Industry, Kyushu University 744, Motooka, Nishi-ku, Fukuoka 819–0395, Japan.
[3] Department of Liberal Arts and Basic Sciences, Nihon University, 1-2-1 Izumi-cho, Narashino, Chiba 275-8575, Japan.
[4] Institute for the Advancement of Higher Education, Okayama University of Science, 1-1 Ridaicho, Kitaku, Okayama 700-0005, Japan.
a) santoso.bagus@uec.ac.jp
b) ikematsu@imi.kyushu-u.ac.jp
c) nakamura.shuhei@nihon-u.ac.jp
d) tyasuda@bme.ous.ac.jp

which acts as a malicious verifier where it sends challenge according to arbitrary distribution.

In this paper, we propose a new three-pass ID scheme based on MinRank problem. By assuming the hardness of decisional MinRank problem and the existence of perfectly hiding and computational binding commitment, without using any additional assumption, we can prove that the probability that an adversary not possessing the valid secret key being accepted by the adversary is at most half (1/2). Hence, the number of rounds which are needed for our proposed scheme to achieve the desired security level is less than Courtois' ID scheme. As a practical result, our estimation on the total communication cost for 128-bit security, 192-bit security and 256-bit security shows that the total communication cost of our proposed scheme is less than Courtois' first ID scheme.

This paper is organized as follows. In Section 2 we provide the definitions of notations and review the definitions of MinRank problem. In Section 3 we describe our proposed scheme and its security properties. In Section 4 we provide the proof of the theorems related to the properties of our scheme. In Section 5 we discuss the selection of practical parameters. Finally, we close our paper with conclusion in Section 6.

2. Preliminaries

In this section, we will show the definition of notations and notions used throughout the paper.

Notations and Consensus.

Unless noted otherwise, let any algorithm in this paper be a probabilistic polynomial time Turing Machine.

Definition 1 (Search Minrank Problem) The search minrank problem is defined as follows. Given a positive integer $r \in \mathbb{N}$ and m random n-square matrices over a finite field $\mathbb{F}$: $M_0, M_1, \ldots, M_{m-1}$, find $\alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in \mathbb{F}^{m-1}$ such that $\mathrm{rank}(M) = r$, where $M = \sum_{i=1}^{m-1} \alpha_i M_i - M_0$.

Decisional Minrank Problem

In this paper, we use the hardness of the decisional version of the minrank problem as the basic assumption of the security since it is much simpler to prove the security based on the decisional version compared to the search version above.

Informally, the decisional minrank problem is as follows: given a positive integer $r \in \mathbb{N}$ and m n-square matrices over a finite field $\mathbb{F}$: $M_0, M_1, \ldots, M_{m-1}$, decide whether there exists $\alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in \mathbb{F}^{m-1}$ such that $\mathrm{rank}(M) = r$, where $M = \sum_{i=1}^{m-1} \alpha_i M_i - M_0$.

Remark 1 Although solving the decisional minrank problem seems easier than solving the search minrank problem, Courtois [4] has proven that the decisional minrank problem is NP-hard.

The formal definition of decisional minrank problem is as follows.

Definition 2 (Decisional Minrank Problem) An algorithm $\mathcal{D}$ is said to (t, ε)-solve the decisional minrank problem associated with the finite field $\mathbb{F}$ and $r, m, n \in \mathbb{N}$ if $\mathcal{D}$ runs in t units of time and the following holds.

$$\left| \Pr\left[\mathcal{D}^{\mathsf{IGen}}(\mathbb{F}, r, m, n) = 1\right] - \Pr\left[\mathcal{D}^{\mathsf{LossyGen}}(\mathbb{F}, r, m, n) = 1\right] \right| \geqq \varepsilon,$$

where:

- $\mathcal{D}^{\mathsf{IGen}}$ denotes that $\mathcal{D}$ receives the input from the oracle IGen which generates an instance of minrank problem that has at least one solution, i.e., m n-square matrices over a finite field $\mathbb{F}$: $M_0, M_1, \ldots, M_{m-1}$, such that there exists $\alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in \mathbb{F}^{m-1}$ satisfying the following:

$$\mathrm{rank}\left(\sum_{i=1}^{m-1} \alpha_i M_i - M_0\right) = r, \tag{1}$$

- $\mathcal{D}^{\mathsf{LossyGen}}$ denotes that $\mathcal{D}$ receives the input from the oracle $\mathsf{LossyGen}$ which generates m arbitrarily random n-square matrices over a finite field $\mathbb{F}$, i.e., $M_0, M_1, \ldots, M_{m-1}$ which do not necessarily have $\alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in \mathbb{F}^{m-1}$ satisfying Eq. (1).

The decisional minrank problem associated with the finite field $\mathbb{F}$ and $r, m, n \in \mathbb{N}$ is said to be (t, ε)-hard if there is no algorithm $\mathcal{D}$ which (t, ε)-solves the problem.

3. Proposed Scheme

In this section, first we describe our proposed identification scheme. Then we show that our proposed scheme satisfies the standard properties such as completeness, soundness, and zero-knowledgeness.

3.1 Construction

Key Generation

Given the security parameter as input, the key generator generates the public pk and the secret key sk which satisfy the following properties. The public key pk consists of a positive integer $r \in \mathbb{N}$ and random m matrices over a finite field $\mathbb{F}$: $M_0, M_1, \ldots, M_{m-1}$. The secret key sk consists of $\alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in \mathbb{F}^{m-1}$ such that $\mathrm{rank}(M) = r$, where $M = \sum_{i=1}^{m-1} \alpha_i M_i - M_0$.

Remark 2 Here, we do not describe the concrete implementation of the key generator. We will describe it in the later section when we discuss about the concrete implementation of the scheme.

Interactive Protocol

A single elementary round of interactive protocol between a prover $P(pk, sk)$ and a verivier $V(pk)$ is described as follows. Similar to Courtois' ID scheme [4], we also employ the hash function H which acts as a commitment with *perfectly hiding* and *computational binding* properties.

Step 1: P generates random non-singular matrices S_0, S_1, T_0, T_1 over $\mathbb{F}$ and random matrices X_0, X_1 over $\mathbb{F}$. Then P randomly generates $\beta_{0,1}$ and $\beta_{1,1}$: $\beta_0 = (\beta_{0,1}, \ldots, \beta_{0,m-1}) \in \mathbb{F}^{m-1}$, $\beta_1 = (\beta_{1,1}, \ldots, \beta_{1,m-1}) \in \mathbb{F}^{m-1}$ and computes the

followings:

$$N_0 = \sum_{i=1}^{m-1} \beta_{0,i} M_i \quad (2) \qquad N_1 = \sum_{i=1}^{m-1} \beta_{1,i} M_i \quad (6)$$

$$U_{0,0} = T_0 N_0 S_0 + X_0 \quad (3) \qquad U_{1,0} = T_1 N_1 S_1 + X_1 \quad (7)$$

$$U_{0,1} = T_0 M S_0 + U_{0,0} \quad (4) \qquad U_{1,1} = T_1 M S_1 + U_{1,0} \quad (8)$$

$$R_0 = (S_0, T_0, X_0) \quad (5) \qquad R_1 = (S_1, T_1, X_1) \quad (9)$$

Finally, P sends $Y = (Y_0, Y_1)$ to V where the followings hold.

$$Y_0 = (H(U_{0,0}), H(U_{0,1}), H(R_0)) \quad (10)$$

$$Y_1 = (H(U_{1,0}), H(U_{1,1}), H(R_1)). \quad (11)$$

Step 2: V parses Y_0 and Y_1 as $Y_0 = (Y_{0,0}, Y_{0,1}, Y_{0,2})$ and $Y_1 = (Y_{1,0}, Y_{1,1}, Y_{1,2})$. Then, V chooses randomly $c \in \{0, 1, 2, 3, 4\}$ and sends c to P.

Step 3: P computes $Z_{0,0}, Z_{0,1}, Z_{1,0}, Z_{1,1}$ according to the value of c as follows.

Case $c = 0$:	$Z_{0,0} = U_{0,0}$,	$Z_{1,0} = R_1$,
	$Z_{0,1} = U_{0,1}$,	$Z_{1,1} = \beta_1$.
Case $c = 1$:	$Z_{0,0} = R_0$,	$Z_{1,0} = R_1$,
	$Z_{0,1} = \beta_0$,	$Z_{1,1} = \beta_1 + \alpha$.
Case $c = 2$:	$Z_{0,0} = R_0$,	$Z_{1,0} = R_1$,
	$Z_{0,1} = \beta_0 + \alpha$	$Z_{1,1} = \beta_1$
Case $c = 3$:	$Z_{0,0} = R_0$,	$Z_{1,0} = U_{1,0}$,
	$Z_{0,1} = \beta_0$,	$Z_{1,1} = U_{1,1}$.

Step 4: V parses $Z = (Z_0, Z_1)$ into $Z_{0,0}, Z_{0,1}, Z_{1,0}, Z_{1,1}$. And then V performs verification procedure according to the value of c as follows.

Case $c = 0$**:** $Z_{1,0}$ is parsed as $Z_{1,0} = (\widetilde{S}, \widetilde{T}, \widetilde{X})$ and $Z_{1,1}$ is parsed as $Z_{1,1} = (\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_{m-1})$.

$H(Z_{0,0}) \stackrel{?}{=} Y_{0,0}$, $H(Z_{0,1}) \stackrel{?}{=} Y_{0,1}$,
$\mathrm{rank}(Z_{0,1} - Z_{0,0}) \stackrel{?}{=} r$,
$H(Z_{1,0}) \stackrel{?}{=} Y_{1,2}$, $H(\widetilde{U}) \stackrel{?}{=} Y_{1,0}$, where

$$\widetilde{U} = \widetilde{T}\left(\sum_{i=1}^{m-1} \widetilde{\gamma}_i M_i\right)\widetilde{S} + \widetilde{X}.$$

$\widetilde{S} \stackrel{?}{\in} \mathbb{GL}$, $\widetilde{T} \stackrel{?}{\in} \mathbb{GL}$.

Case $c = 1$**:** $Z_{0,0}$ is parsed as $Z_{0,0} = (\widehat{S}, \widehat{T}, \widehat{X})$ and $Z_{0,1}$ is parsed as $Z_{0,1} = (\widehat{\gamma}_1, \ldots \widehat{\gamma}_{m-1})$. $Z_{1,0}$ is parsed as $Z_{1,0} = (\widetilde{S}, \widetilde{T}, \widetilde{X})$ and $Z_{1,1}$ is parsed as $Z_{1,1} = (\widetilde{\mu}_1, \ldots \widetilde{\mu}_{m-1})$.

$H(Z_{0,0}) \stackrel{?}{=} Y_{0,2}$, $H(\widehat{U}) \stackrel{?}{=} Y_{0,0}$, where

$$\widehat{U} = \widehat{T}\left(\sum_{i=1}^{m-1} \widehat{\gamma}_i M_i\right)\widehat{S} + \widehat{X}. \quad (12)$$

$\widehat{S} \stackrel{?}{\in} \mathbb{GL}$, $\widehat{T} \stackrel{?}{\in} \mathbb{GL}$.
$H(Z_{1,0}) \stackrel{?}{=} Y_{1,2}$, $H(\widetilde{W} - \widetilde{T} M_0 \widetilde{S}) \stackrel{?}{=} Y_{1,1}$, where

$$\widetilde{W} = \widetilde{T}\left(\sum_{i=1}^{m-1} \widetilde{\mu}_i M_i\right)\widetilde{S} + \widetilde{X}. \quad (13)$$

$\widetilde{S} \stackrel{?}{\in} \mathbb{GL}$, $\widetilde{T} \stackrel{?}{\in} \mathbb{GL}$.

Case $c = 2$**:** $Z_{0,0}$ is parsed as $Z_{0,0} = (\widehat{S}, \widehat{T}, \widehat{X})$ and $Z_{0,1}$ is parsed as $Z_{0,1} = (\widehat{\mu}_1, \ldots \widehat{\mu}_{m-1})$. $Z_{1,0}$ is parsed as $Z_{1,0} = (\widetilde{S}, \widetilde{T}, \widetilde{X})$ and $Z_{1,1}$ is parsed as $Z_{1,1} = (\widetilde{\gamma}_1, \ldots \widetilde{\gamma}_{m-1})$.

$H(Z_{0,0}) \stackrel{?}{=} Y_{0,2}$, $H(\widehat{W} - \widehat{T} M_0 \widehat{S}) \stackrel{?}{=} Y_{0,1}$, where

$$\widehat{W} = \widehat{T}\left(\sum_{i=1}^{m-1} \widehat{\mu}_i M_i\right)\widehat{S} + \widehat{X}. \quad (14)$$

$\widehat{S} \stackrel{?}{\in} \mathbb{GL}$, $\widehat{T} \stackrel{?}{\in} \mathbb{GL}$.
$H(Z_{1,0}) \stackrel{?}{=} Y_{1,2}$, $H(\widetilde{U}) \stackrel{?}{=} Y_{1,0}$, where

$$\widetilde{U} = \widetilde{T}\left(\sum_{i=1}^{m-1} \widetilde{\gamma}_i M_i\right)\widetilde{S} + \widetilde{X}. \quad (15)$$

$\widetilde{S} \stackrel{?}{\in} \mathbb{GL}$, $\widetilde{T} \stackrel{?}{\in} \mathbb{GL}$.

Case $c = 3$**:** $Z_{0,0}$ is parsed as $Z_{0,0} = (\widehat{S}, \widehat{T}, \widehat{X})$ and $Z_{0,1}$ is parsed as $Z_{0,1} = (\widehat{\gamma}, \ldots \widehat{\gamma}_{m-1})$.

$H(Z_{0,0}) \stackrel{?}{=} Y_{0,2}$, $H(\widehat{U}) \stackrel{?}{=} Y_{0,0}$, where

$$\widehat{U} = \widehat{T}\left(\sum_{i=1}^{m-1} \widehat{\gamma}_i M_i\right)\widehat{S} + \widehat{X}.$$

$\widehat{S} \stackrel{?}{\in} \mathbb{GL}$, $\widehat{T} \stackrel{?}{\in} \mathbb{GL}$.
$H(Z_{1,0}) \stackrel{?}{=} Y_{1,0}$, $H(Z_{1,1}) \stackrel{?}{=} Y_{1,1}$, $\mathrm{rank}(Z_{1,1} - Z_{1,0}) \stackrel{?}{=} r$,

If all corresponding checking equations hold, V outputs 1 (accept), otherwise V outputs 0 (reject).

Remark 3 We said that the response Z is a valid response w.r.t. challenge c if all checking equations in the verifier side corresponding to the value of c hold.

Remark 4 A full identification scheme consists of ℓ repetitions of the single elementary round of interactive protocol and the verifier will accept the prover if and only if V outputs 1 in all ℓ rounds.

Remark 5 Here we assume that the length of the input into the hash function H is larger than that of the output, that is why we can assume that H acts as a perfectly hiding commitment. We also assume that H is collision resistant, i.e., for any i polynomial algorithm, it is hard to find two distinct inputs with the same output. That is why we can assume that H acts a computational binding commitment. Any common standard hash functions such as SHA-128, SHA-256, SHA-512 is assumed to have these properties.

3.2 Completeness

Here we show that any prover who possesses the secret key and follows the procedure of the honest prover will always be accepted by the verifier.

Theorem 1 (Completeness) Let P be a prover who

possesses the secret key sk corresponding the the public key pk of our proposed identification scheme. Let P generate Y in Step 1 according to the described procedure and send it to the verifier. Then for any received challenge $c \in \{0,1,2,3\}$ from the verifier, if P computes Z according to described procedure, Z is a valid response w.r.t. challenge c.

In order to prove the above theorem, it is sufficient to show that for each challenge $c \in \{0,1,2,3\}$, Z which is generated accordingly in the procedure of the prover will satisfy all the corresponding checking equations on the verifier side. See Section 4.1 for the detailed proof.

3.3 Soundness

In order to prove the soundness of our proposed scheme, we will use the following proposition.

Proposition 1 Let Y denote the value sent by the prover in the Step 1 to the verifier and let $Z^{(c)}$ denote the valid response w.r.t. challenge c for any $c \in \{0,1,2,3\}$. Then, from Y and any three combinations of elements from the set $\{Z^{(0)}, Z^{(1)}, Z^{(2)}, Z^{(3)}\}$ we can efficiently compute the solution of search minrank problem represented by the public key.

We describe the detailed proof of above proposition in Section 4.2. Based on above proposition, we can easily see that the following corollary holds.

Corollary 1 If the public key does not have any corresponding secret key, the success probability of any prover to be accepted by the verifier in all ℓ rounds of a full identification at most $1/2^{\ell}$.

The security of our scheme against key-only impersonation attack, i.e., soundness, is based on the hardness of decisional minrank problem, as stated by the following theorem.

Theorem 2 Let $\mathcal{A}$ be an algorithm such that given the public key pk, it is accepted in all ℓ rounds of the full identification protocol with probability $\varepsilon_{\mathcal{A}} \geqq \frac{1}{2^{\ell}}$, where the probability is taken over the random coins of $\mathcal{A}$, the key generator, and the verifier. Then, we can construct an algorithm which (t,ε)-solves the decisional minrank problem associated with the finite field $\mathbb{F}$ and $r,m,n \in \mathbb{N}$ such that the following holds.

$$\varepsilon = \varepsilon_{\mathcal{A}} - \frac{1}{2^{\ell}}, \quad t = t_{\mathcal{A}},$$

where $t_{\mathcal{A}}$ is the maximum total time of $\mathcal{A}$ interacting in one full identification protocol.

Corollary 2 If decisional minrank problem is (t,ε)-hard, then the success probability of any adversary attempting to impersonate a prover without secret key within t time units is upper-bounded by $\varepsilon + 1/2^{\ell}$.

3.4 Zero-Knowledgeness

The following theorem is to guarantee that no knowledge on the secret leaked by communication with the prover.

Theorem 3 (Zero-Knowledgenes) For any verifier V, there exists an algorithm M which given input the public key pk, perfectly simulates the view of verifier with the same distribution as the view of V engaging with the prover possessing pk and the secret key sk.

4. Proofs of Main Theorems

4.1 Proof of Theorem 1

It is sufficient to show that for each challenge $c \in \{0,1,2,3\}$, Z which is generated accordingly in the procedure of the prover will satisfy all the corresponding checking equations on the verifier side. Let us check for each case of challenge.

Case $c = 0$: Since $Z_{0,0} = U_{0,0}$ and $Y_{0,0} = H(U_{0,0})$, it is obvious that $H(Z_{0,0}) = H(U_{0,0}) = Y_{0,0}$ holds. Similarly, since $Z_{0,1} = U_{0,1}$ and $Y_{0,1} = H(U_{0,1})$ holds, it is obvious that $H(Z_{0,1}) = H(U_{0,1}) = Y_{0,1}$. Since $Z_{0,0} = U_{0,0}$ and $Z_{0,1} = U_{0,1}$, the followings hold.

$$\begin{aligned}\operatorname{rank}(Z_{0,1} - Z_{0,0}) &= \operatorname{rank}(U_{0,1} - U_{0,0}) \\ &= \operatorname{rank}(T_0 M S_0) \\ &\overset{(a)}{=} \operatorname{rank}(M) = r.\end{aligned}$$

Eq. (a) holds since T_0 and S_0 are invertible matrices. Since $Z_{1,0} = R_1$ and $Y_{1,2} = H(R_1)$, it is obvious that $H(Z_{1,0}) = H(R_1) = Y_{1,2}$ holds. Also, we can easily see that $(\widetilde{S}, \widetilde{T}, \widetilde{X}) = (S_1, T_1, X_1)$. Since S_1, T_1 are invertible matrices, so are $\widetilde{S}, \widetilde{T}$. Since $Z_{1,1} = \beta_1$, it is obvious that $(\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_{m-1}) = (\beta_{1,1}, \ldots, \beta_{1,m-1}.)$ Thus, the followings hold.

$$\begin{aligned}\widetilde{U} &= \widetilde{T}\left(\sum_{i=1}^{m-1} \widetilde{\gamma}_i M_i\right)\widetilde{S} + \widetilde{X} \\ &= T_1\left(\sum_{i=1}^{m-1} \beta_{1,i} M_i\right) S_1 + X_1 \\ &= T_1 N_1 S_1 + X_1 = U_{1,0}.\end{aligned}$$

Hence, since $Y_{1,0} = H(U_{1,0})$, $H(\widetilde{U}) = H(U_{1,0}) = Y_{1,0}$ holds.

Case $c = 1$: Since $Z_{0,0} = R_0$ and $Y_{0,2} = H(R_0)$, it is obvious that $H(Z_{0,0}) = Y_{0,2}$ holds. Hence, one can see that $(\widehat{S}, \widehat{T}, \widehat{X}) = (S_0, T_0, X_0)$ holds. Since $Z_{0,1} = \beta_0$, it is obvious that $(\widehat{\gamma}_1, \ldots, \widehat{\gamma}_{m-1}) = (\beta_{0,1}, \ldots, \beta_{0,m-1})$ holds. Thus, the following holds.

$$\begin{aligned}\widehat{U} &= \widehat{T}\left(\sum_{i=1}^{m-1} \widehat{\gamma}_i M_i\right)\widehat{S} + \widehat{X} \\ &= T_0\left(\sum_{i=1}^{m-1} \beta_{0,i} M_i\right) S_0 + X_0 \\ &= T_0 N_0 S_0 + X_0 = U_{0,0}.\end{aligned}$$

Hence, since $Y_{0,0} = H(U_{0,0})$, automatically $H(\widehat{U}) = H(U_{0,0}) = Y_{0,0}$ holds. Next, since $Z_{1,0} = R_1$ and $Y_{1,2} = H(R_1)$, it is obvious that $H(Z_{1,0}) = Y_{1,2}$ holds. Hence, one can see that $(\widetilde{S}, \widetilde{T}, \widetilde{X}) = (S_1, T_1, X_1)$ holds. Since $Z_{1,1} = \beta_1 + \alpha$, it is obvious that $(\widetilde{\mu}_1, \ldots, \widetilde{\mu}_{m-1}) =$

$(\beta_{1,1}+\alpha_1,\ldots,\beta_{1,m-1}+\alpha_{m-1})$ holds. Thus, the following holds.

$$\begin{aligned}\widetilde{W}-\widetilde{T}M_0\widetilde{S} &= \widetilde{T}\left(\sum_{i=1}^{m-1}\widetilde{\mu}_i M_i\right)\widetilde{S}+\widetilde{X}-\widetilde{T}M_0\widetilde{S}\\ &= T_1\left(\sum_{i=1}^{m-1}(\beta_{1,i}+\alpha_i)M_i\right)S_1+X_1\\ &\quad -T_1M_0S_1\\ &= T_1N_1S_1+T_1MS_1+T_1M_0S_1+X_1\\ &\quad -T_1M_0S_1\\ &= T_1N_1S_1+X_1=U_{1,0}\end{aligned}$$

Hence, since $Y_{1,0}=H(U_{1,0})$, automatically $H(\widetilde{W}-\widetilde{T}M_0\widetilde{S})=H(U_{1,0})=Y_{1,0}$ holds.

Case $c=2$: This case is similar to the case $c=1$ with additional notes as follows:

- any variable in the form of $\widehat{*}$ notation switches with the resembling variable in the form of $\widetilde{*}$ notation,
- any variable in the form of $*_0$ notation switches with the resembling variable in the form of $*_1$ notation,
- for any numeric j, any variable in the form of $*_{0,j}$ notation switches with the resembling variable in the form of $*_{1,j}$ notation.

Case $c=3$: This case is similar to the case $c=0$ with the same additional notes as in the case $c=2$.

4.2 Proof of Proposition 1

It is sufficient to show that from Y and any combination of three elements from the set of the valid responses $\{Z^{(0)},Z^{(1)},Z^{(2)},Z^{(3)}\}$, we can compute $\alpha=(\alpha_1,\ldots,\alpha_{m-1})\in\mathbb{F}^{m-1}$ such that $\mathrm{rank}\left(\sum_{i=1}^{m-1}\alpha_iM_i-M_0\right)=r$ holds, where r and $M_0,\ldots,M_{m-1}$ are generated by the key generation algorithm as elements of the public key.

Remark 6 Note that in our proposed scheme, we assume that H has computational binding property. Hence, we can assume that for any polynomial time algorithm, if $H(a)=H(b)$, then $a=b$ must hold except with negligible probability.

Case 1: Y and $(Z^{(0)},Z^{(1)},Z^{(2)})$.

Let $Z_{0,0}^{(1)}$ be parsed as $Z_{0,0}^{(1)}=(\widehat{S}^{(1)},\widehat{T}^{(1)},\widehat{X}^{(1)})$ and $Z_{0,1}^{(1)}$ be parsed as $Z_{0,1}^{(1)}=(\widehat{\gamma}_1,\ldots\widehat{\gamma}_{m-1})$. Also let $Z_{0,0}^{(2)}$ be parsed as $Z_{0,0}^{(2)}=(\widehat{S}^{(2)},\widehat{T}^{(2)},\widehat{X}^{(2)})$ and $Z_{0,1}^{(2)}$ be parsed as $Z_{0,1}^{(2)}=(\widehat{\mu}_1,\ldots\widehat{\mu}_{m-1})$. Since the following holds:

$$H\left(\widehat{S}^{(1)},\widehat{T}^{(1)},\widehat{X}^{(1)}\right)=H\left(\widehat{S}^{(2)},\widehat{T}^{(2)},\widehat{X}^{(2)}\right)=Y_{0,2},$$

we can define as follows: $(\widehat{S},\widehat{T},\widehat{X}):=(\widehat{S}^{(1)},\widehat{T}^{(1)},\widehat{X}^{(1)})=(\widehat{S}^{(2)},\widehat{T}^{(2)},\widehat{X}^{(2)})$. From $H(Z_{0,0}^{(0)})=Y_{0,0}$ and Eq. (12), we obtain as follows.

$$\begin{aligned}Y_{0,0}=H(Z_{0,0}^{(0)})&=H\left(\widehat{T}\left(\sum_{i=1}^{m-1}\widehat{\gamma}_iM_i\right)\widehat{S}+\widehat{X}\right)\qquad(16)\\ \Rightarrow Z_{0,0}^{(0)}&=\widehat{T}\left(\sum_{i=1}^{m-1}\widehat{\gamma}_iM_i\right)\widehat{S}+\widehat{X},\end{aligned}$$

Similarly, from $H(Z_{0,1}^{(0)})=Y_{0,1}$ and Eq. (14), we also have the followings hold.

$$\begin{aligned}Y_{0,1}=H(Z_{0,1}^{(0)})&=H\left(\widehat{T}\left(\sum_{i=1}^{m-1}\widehat{\mu}_iM_i\right)\widehat{S}+\widehat{X}-\widehat{T}M_0\widehat{S}\right)\qquad(17)\\ \Rightarrow Z_{0,1}^{(0)}&=\widehat{T}\left(\sum_{i=1}^{m-1}\widehat{\mu}_iM_i\right)\widehat{S}+\widehat{X}-\widehat{T}M_0\widehat{S}\end{aligned}$$

Finally, we have the followings hold.

$$\begin{aligned}\mathrm{rank}(Z_{0,1}^{(0)}-Z_{0,0}^{(0)})&=\mathrm{rank}\left(\widehat{T}\left(\sum_{i=1}^{m-1}(\widehat{\mu}_i-\widehat{\gamma}_i)M_i-M_0\right)\widehat{S}\right)\\ &\overset{(a)}{=}\mathrm{rank}\left(\sum_{i=1}^{m-1}(\widehat{\mu}_i-\widehat{\gamma}_i)M_i-M_0\right),\end{aligned}$$

where Eq. (a) holds since $\widehat{S},\widehat{T}$ are non-singular. Therefore, we can set $\alpha_i=\widehat{\mu}_i-\widehat{\gamma}_i$ for $i\in[1,m-1]$, since $\mathrm{rank}(Z_{0,1}^{(0)}-Z_{0,0}^{(0)})=r$ holds.

Case 2: Y and $(Z^{(0)},Z^{(2)},Z^{(3)})$.

Similar to Case 1. The only diffference is that all relations and components of $Z^{(1)}$ in Case 1 are substituted by those of $Z^{(3)}$.

Case 3: Y and $(Z^{(1)},Z^{(2)},Z^{(3)})$.

Let $Z_{1,0}^{(2)}$ be parsed as $Z_{1,0}^{(2)}=(\widetilde{S}^{(2)},\widetilde{T}^{(2)},\widetilde{X}^{(2)})$ and $Z_{1,1}^{(2)}$ be parsed as $Z_{1,1}^{(2)}=(\widetilde{\gamma}_1,\ldots\widetilde{\gamma}_{m-1})$. Also let $Z_{1,0}^{(1)}$ be parsed as $Z_{1,0}^{(1)}=(\widetilde{S}^{(1)},\widetilde{T}^{(1)},\widetilde{X}^{(1)})$ and $Z_{1,1}^{(1)}$ be parsed as $Z_{1,1}^{(1)}=(\widetilde{\mu}_1,\ldots\widetilde{\mu}_{m-1})$. Since the following holds:

$$H\left(\widetilde{S}^{(1)},\widetilde{T}^{(1)},\widetilde{X}^{(1)}\right)=H\left(\widetilde{S}^{(2)},\widetilde{T}^{(2)},\widetilde{X}^{(2)}\right)=Y_{1,2},$$

we can define as follows: $(\widetilde{S},\widetilde{T},\widetilde{X}):=(\widetilde{S}^{(1)},\widetilde{T}^{(1)},\widetilde{X}^{(1)})=(\widetilde{S}^{(2)},\widetilde{T}^{(2)},\widetilde{X}^{(2)})$. From $H(Z_{1,0}^{(3)})=Y_{1,0}$ and Eq. (15), we obtain as follows.

$$\begin{aligned}Y_{1,0}=H(Z_{1,0}^{(3)})&=H\left(\widetilde{T}\left(\sum_{i=1}^{m-1}\widetilde{\gamma}_iM_i\right)\widetilde{S}+\widetilde{X}\right)\qquad(18)\\ \Rightarrow Z_{1,0}^{(3)}&=\widetilde{T}\left(\sum_{i=1}^{m-1}\widetilde{\gamma}_iM_i\right)\widetilde{S}+\widetilde{X},\end{aligned}$$

Similarly, from $H(Z_{1,1}^{(3)})=Y_{1,1}$ and Eq. (13), we also have the followings hold.

$$\begin{aligned}Y_{1,1}=H(Z_{1,1}^{(3)})&=H\left(\widetilde{T}\left(\sum_{i=1}^{m-1}\widetilde{\mu}_iM_i\right)\widetilde{S}+\widetilde{X}-\widetilde{T}M_0\widetilde{S}\right)\qquad(19)\\ \Rightarrow Z_{1,1}^{(3)}&=\widetilde{T}\left(\sum_{i=1}^{m-1}\widetilde{\mu}_iM_i\right)\widetilde{S}+\widetilde{X}-\widetilde{T}M_0\widetilde{S}\end{aligned}$$

Finally, we have the followings hold.

$$\begin{aligned}\mathrm{rank}(Z^{(3)}_{1,1} - Z^{(3)}_{1,0}) &= \mathrm{rank}\left(\widetilde{T}\left(\sum_{i=1}^{m-1}(\widetilde{\mu}_i - \widetilde{\gamma}_i)M_i - M_0\right)\widetilde{S}\right)\\ &\overset{(a)}{=} \mathrm{rank}\left(\sum_{i=1}^{m-1}(\widetilde{\mu}_i - \widetilde{\gamma}_i)M_i - M_0\right),\end{aligned}$$

where Eq. (a) holds since $\widetilde{S}, \widetilde{T}$ are non-singular. Therefore, we can set $\alpha_i = \widetilde{\mu}_i - \widetilde{\gamma}_i$ for $i \in [1, m-1]$, since $\mathrm{rank}(Z^{(3)}_{1,1} - Z^{(3)}_{1,0}) = r$ holds.

Case 4: Y and $(Z^{(0)}, Z^{(1)}, Z^{(3)})$.

Similar to Case 3. The only diffference is that all relations and components of $Z^{(2)}$ in Case 1 are substituted by those of $Z^{(0)}$.

4.3 Proof Sketch of Corollary 1

Recall that based on Proposition 1, we know that in any single round, if the prover can answer correctly three out of four possible challenges from the verifier, it means that the prover knows the secret key corresponding public key. Thus, in the case that the public key has no corresponding valid secret key, even a prover with unbounded resources must not be able to answer correctly more than two out of four possible challenges in any single round. Otherwise, it will contradict with the assumption that the public key that the public key has no corresponding secret key.

4.4 Proof Sketch of Theorem 2

Let define algorithm $\mathcal{D}^{\mathsf{InputGen}}(\mathbb{F}, r, m, n)$ as follows. First, $\mathcal{D}$ retrieves inputs from the oracle $\mathsf{InputGen}$ in the form of m n-square matrices over the finite field $\mathbb{F}$: $M_0, \ldots, M_{m-1}$. Then, $\mathcal{D}$ simulates the key generation algorithm of the identification scheme by setting the public key pk as r and $M_0, \ldots, M_{m-1}$. Next, $\mathcal{D}$ inputs pk to $\mathcal{A}$ and runs $\mathcal{A}$ as the prover and $\mathcal{D}$ acts as the honest verifier. If $\mathcal{A}$ successfully gives valid responses in all ℓ rounds of the full identification protocol, $\mathcal{D}$ outputs 1, otherwise, $\mathcal{D}$ outputs 0. Note that if $\mathsf{InputGen}$ is IGen, the probability of $\mathcal{D}$ outputs 1 is exactly $\varepsilon_{\mathcal{A}}$. Meanwhile, when $\mathsf{InputGen}$ is $\mathsf{LossyGen}$, based on Corollary 1, the probability of D outputs 1 is at most $1/2^{\ell}$. Thus, denoting the system parameters $(\mathbb{F}, r, m, n)$ as par, we obtain as follows.

$$\left|\Pr[\mathcal{D}^{\mathsf{IGen}}(\mathrm{par}) = 1] - \Pr[\mathcal{D}^{\mathsf{LossyGen}}(\mathrm{par}) = 1]\right| \geqq \varepsilon_{\mathcal{A}} - \frac{1}{2^{\ell}}.$$

This proves the Theorem 2.

4.5 Proof Idea of Theorem 3

It is sufficient to prove that given any $c \in \{0, 1, 2, 3\}$, we can create valid response $Z_{0,0}, Z_{0,1}, Z_{1,0}, Z_{1,1}$ and the commitment Y_0, Y_1 without using secret key such that their distribution is the same as the distribution of the response and commitment generated by a honest prover who possesses valid secret key. Note that we can put the responses and commitment into two independent groups: $(Y_0, Z_{0,0}, Z_{0,1})$ and $(Y_1, Z_{1,0}, Z_{1,1})$, such that each group is corresponding to the set of responses and commitment in Courtois' basic ID scheme [4]. Hence, it is easy to see that we can apply the proof of zero-knowledge for Courtois' basic ID scheme into our proposed scheme.

5. Parameter Selections

5.1 Complexity of MinRank Problem

In this subsection, we review known attacks against MinRank Problem to select some practical parameters.

There are two types of attack. First one is to mainly use linear algebra and second one is to reduce the MinRank problem into an MP problem. Set $\mathbb{F} = \mathbb{F}_q$.

Linear algebra type

There exist 4 attacks in this type. Our review for this type mainly follows the Subsection 4.2 in [4].

(i) **Exhaustive search attack**: This attack is to find $M := \sum_{i=1}^{m-1}\alpha_i M_i - M_0$ or a matrix with rank $\leq r$ from the linear combinations of $M_0, \ldots, M_{m-1}$. The complexity to find M from $M_0, \ldots, M_{m-1}$ is given by

$$q^{m-1}(r+1)^{\omega},$$

where $2 < \omega \leq 3$ is a linear algebra constant.

Next, consider the complexity to find a matrix with rank $\leq r$. The probability that a square matrix with size n is of rank ℓ is given by

$$P(n, \ell) := \frac{(q^n - 1)^2(q^n - q)^2 \cdots (q^n - q^{\ell-1})^2}{(q^{\ell} - 1) \cdots (q^{\ell} - q^{\ell-1}) \cdot q^{n^2}}.$$

We assume that the probability that a linear combination of $M_0, \cdots, M_{m-1}$ is of rank ℓ is $P(n, \ell)$. Then the complexity to find a matrix with rank $\leq r$ from the linear combinations of $M_0, \ldots, M_{m-1}$ is given by

$$\left(\sum_{\ell=1}^{r} P(n, \ell)\right)^{-1}(r+1)^{\omega}.$$

(ii) **Kernel attack**: This attack is to find an element of the kernel of M. The complexity is given by

$$\mathrm{Min}\left(q^{\lceil \frac{m}{n} \rceil r}, q^{\lfloor \frac{m}{n} \rfloor r + (m \mod n))}\right) m^{\omega}.$$

(iii) **"Big m" attack**: This attack is valid for $m \gg n$. The complexity is given by

$$q^{\mathrm{Max}(0, n(n-r)-m)} \cdot (n(n-r))^{\omega}.$$

(iv) **Syndrome attack**: This attack is valid for $m \gg n$. The complexity is given by

$$q^{\mathrm{Max}(\frac{n^2-m-1}{2}, nr-m-\frac{r^2}{4})} \cdot \mathcal{O}(n^2 r).$$

There is another attack using submatrices that works under $r \ll n$ (see also [4]). However, in our setting, we will choose the rank r to be about $n/2$. Therefore, we skip such an attack.

MP type

The MinRank problem can be reduced to the problem that solves a system of polynomial equations (namely, MP problem). There exist three attacks in this type: (v) Kipnis-Shamir attack, (vi) Minors modeling attack, and (vii) Support minors modeling attack.

(v) **Kipnis-Shamir attack** [12]: Let c be an integer such that $\lceil m/(n-r) \rceil \leq c \leq n-r$. By considering $\alpha_1, \ldots, \alpha_m$ and kernel basis vectors $\{\mathbf{y}_1, \ldots, \mathbf{y}_c\}$ of $\sum_{i=1}^m \alpha_i M_i - M_0$ as variables, Kipnis-Shamir attack solves the quadratic system consisting of $\mathbf{y}_i \cdot \left(\sum_{i=1}^m \alpha_i M_i - M_0\right) = 0$. The complexity estimations of this attack are given as Table 1. Here, for each estimation, we take c giving the minimum value in Table 1.

Table 1 Complexity estimations for the Kipnis-Shamir attack

Faugere et al. [8]	Verbel et al. [19]	Nakamura et al. [13]
$\log_2(q)\binom{n}{r}^{\omega(n-r)}$	$\left(m\binom{cr+D_{KS}-1}{D_{KS}}\right)^{\omega}$	$\binom{m+cr+D_{mgd}}{D_{mgd}}^{\omega}$

Here, D_{KS} is defined as follows. Let $d_{KS} = \min_{1 \leq d \leq r}\{d : \binom{r}{d} n > \binom{r}{d+1} m\}$. Then $D_{KS} = d_{KS} + 2$. Moreover, D_{mgd} is defined as follows. Set

$$\sum_{(e_0,e_1,\ldots,e_c)\in\mathbb{Z}^{c+1}} a_{(e_0,e_1,\ldots,e_c)} t_0^{e_0} t_1^{e_1} \cdots t_c^{e_c} := \frac{\prod_{i=1}^c (1-t_0 t_i)^n}{(1-t_0)^m (1-t_1)^r \cdots (1-t_c)^r}.$$

Then define $D_{mgd} = \min\left\{\sum_{i=1}^c e_i : a_{(e_0,e_1,\ldots,e_c)} < 0\right\}$.

(vi) **Minors modeling attack** [7]: This attack solves the system consisting of the $(r+1)$-minors of $\sum_{i=1}^m \alpha_i M_i - M_0$, whose variables are $\alpha_1, \ldots, \alpha_m$. The complexity is estimated by $\binom{m+r}{r}^{\omega}$.

(vii) **Support Minors modeling attack** [1]: This attack solves a quadratic system whose variables are $\alpha_1, \ldots, \alpha_m$ and r-minors, and its complexity is estimated by

$$3\binom{m+D_{Spp}}{D_{Spp}}^2 \binom{n}{r}^2 (r+1)m.$$

Here, D_{Spp} is defined as follows. For $b \geq 1$, set $R_{m,n,r}(b) = \sum_{i=1}^b (-1)^{i+1}\binom{n}{r+i}\binom{n+i-1}{i}\binom{m+b-i-1}{b-i}$ and $\mathcal{M}(b,1) = \binom{m+b}{b}\binom{n}{r}$. Then define $D_{Spp} = \min\{b \mid R_{m,n,r}(b) > \mathcal{M}(b,1) - 1\}$.

5.2 Communication Costs

We will estimate the communication costs based on the assumption that we use random seed and pseudorandom generator to generates $S_0, S_1, T_0, T_1, X_0, X_1, \beta_0, \beta_1$. Let $Z^{(c)}$ denote the valid response of the prover w.r.t. challenge c for any $c \in \{0,1,2,3\}$. For simplicity, here we assume that all matrices are n-square matrices, and $\mathbb{F} = \mathbb{Z}_p$ for some prime p. Thus, we have as follows.

$$|Z^{(0)}| = |Z^{(3)}| \approx 2n^2 \log_2 p + |\mathrm{seed}_{\overline{STX}}| + |\mathrm{seed}_\beta|,$$
$$|Z^{(1)}| = |Z^{(2)}| \approx 2|\mathrm{seed}_{\overline{STX}}| + |\mathrm{seed}_\beta| + (m-1)\log_2 p,$$

where $\mathrm{seed}_{\overline{STX}}$ is the seed for generating (S_0, T_0, X_0) or (S_1, T_1, X_1) and seed_β is the seed for generating β_0 or β_1.

Estimation for 128-bit security

For achieving 128-bit security, we need to have 128 repetitions of the elementary round. Let $\#Z_{1/2}$ denote the average of the total cost of sending all responses in our proposed identification scheme. Thus, we can estimate $\#Z_{1/2}$ as follows.

$$\begin{aligned}\#Z_{1/2} &= \frac{128}{4}(|Z^{(0)}| + |Z^{(1)}| + |Z^{(2)}| + |Z^{(3)}|) \\ &= \frac{128}{4}(2|Z^{(0)}| + 2|Z^{(1)}|) = 64(|Z^{(0)}| + |Z^{(1)}|) \\ &\approx 64(2n^2 \log_2 p + |\mathrm{seed}_{\overline{STX}}| + |\mathrm{seed}_\beta| \\ &\quad + 2|\mathrm{seed}_{\overline{STX}}| + |\mathrm{seed}_\beta| + (m-1)\log_2 p)\end{aligned}$$

In Courtois' identification scheme [4], for achieving 128-bit security, we need to have 219 repetitions of the elementary round since the cheating probability for each elementary round is 2/3.[*1] In Courtois' identification scheme, we have $c \in \{0,1,2\}$. Based on the same assumption as above on the matrices, the field, and the random seeds, we have as follows.

$$|Z^{(0)}| \approx 2n^2, |Z^{(1)}| \approx |\mathrm{seed}_{\overline{STX}}| + |\mathrm{seed}_\beta|,$$
$$|Z^{(2)}| \approx |\mathrm{seed}_{\overline{STX}}| + (m-1)\log_2 p.$$

Let $\#Z_{2/3}$ denote the average of the total cost of sending all responses in Courtois' identification scheme. Thus, we can estimate $\#Z_{2/3}$ as follows.

$$\begin{aligned}\#Z_{2/3} &= \frac{219}{3}(|Z^{(0)}| + |Z^{(1)}| + |Z^{(2)}|) \\ &= 73(|Z^{(0)}| + |Z^{(1)}| + |Z^{(2)}|) \\ &\approx 73(2n^2 \log_2 p + |\mathrm{seed}_{\overline{STX}}| + |\mathrm{seed}_\beta| \\ &\quad + |\mathrm{seed}_{\overline{STX}}| + (m-1)\log_2 p)\end{aligned}$$

For 128-bit security, it is common to assume that all random seeds have 128 bit length. Thus, we can finalize our estimation as follows.

$$\begin{aligned}\#Z_{1/2} &\approx 128\left(n^2 + \frac{1}{2}(m-1)\right)\log_2 p + 64 \times 5 \times 128 \\ &= 128\left(n^2 + \frac{1}{2}(m-1)\right)\log_2 p + 40960, \\ \#Z_{2/3} &\approx 146\left(n^2 + \frac{1}{2}(m-1)\right)\log_2 p + 73 \times 3 \times 128 \\ &= 146\left(n^2 + \frac{1}{2}(m-1)\right)\log_2 p + 28032.\end{aligned}$$

[*1] This number 219 is based on the fact that $\ell = 219$ is the least integer such that $(2/3)^\ell \leqq 2^{-128}$ holds.

Estimation for General Case

Assuming that the seeds for ℓ-bit security are ℓ bits, we can have the following general equations for estimating the total communication costs for ℓ-bit security.

$$\#Z_{1/2} \approx \ell \times \left(\left(n^2 + (m-1) \right) \log_2 p + \frac{\ell}{2} \times 5 \right) \quad (20)$$

$$\#Z_{2/3} \approx \frac{2}{3} \left\lceil \frac{\ell}{\log_2 3 - 1} \right\rceil \times \left(\left(n^2 + (m-1) \right) \log_2 p + \frac{\ell}{2} \times 3 \right) \quad (21)$$

5.3 Security Parameters

Following the known attacks in Subsection 5.1, we pick three parameters for 128, 192 and 256-bit security as follows.

(i) 128-bit security parameter: $n = 26$, $m = 209$, $r = 13$, $p = 2$.

$$\#Z_{1/2} \approx 19264 \text{ bytes},$$
$$\#Z_{2/3} \approx 19637 \text{ bytes}.$$

(ii) 192-bit security parameter: $n = 33$, $m = 331$, $r = 17$, $p = 2$.

$$\#Z_{1/2} \approx 45576 \text{ bytes},$$
$$\#Z_{2/3} \approx 46800 \text{ bytes}.$$

(iii) 256-bit security parameter: $n = 39$, $m = 469$, $r = 20$, $p = 2$.

$$\#Z_{1/2} \approx 84128 \text{ bytes},$$
$$\#Z_{2/3} \approx 86614 \text{ bytes}.$$

6. Conclusion

Courtois [4] proposed the first three-pass ID scheme based on the MinRank problem, which is an NP-complete problem. However, the cheating probability in Courtois' scheme is 2/3, which is larger than half. In this paper, we have shown a construction of a new three-pass ID scheme with half cheating probability. In practice, our scheme requires less number of repetitions to achieve the desired security level, and thus reduce the total communication costs. As a future work, we aim to construct a digital signature based on our proposed ID scheme and prove its security against quantum adversaries.

Acknowledgements This work was supported by JST CREST Grant Number JPMJCR14D6, JSPS KAKENHI Grant Number JP19K20266, JP20K19802, JP20K03741, JP18H01438, and JP18K11292.

References

[1] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier A. Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In *Advances in Cryptology - ASIACRYPT 2020*, volume 12491 of *Lecture Notes in Computer Science*, pages 507–536. Springer, 2020.

[2] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. Post-quantum cryptography. Springer, 2009.

[3] Jonathan F. Buss, Gudmund Skovbjerg Frandsen, and Jeffrey O. Shallit. The computational complexity of some problems of linear algebra. *J. Comput. Syst. Sci.*, 58(3):572–596, 1999.

[4] Nicolas T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem minrank. In *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 402–421. Springer, 2001.

[5] Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, and Bo-Yin Yang. Rainbow, technical report, national institute of standards and technology, https://csrc.nist.gov/projects/post-quantum-cryptography/round-3- submissions. 2020.

[6] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *Applied Cryptography and Network Security, Third International Conference, ACNS 2005*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175, 2005.

[7] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In *ISSAC 2010, Proceedings*, pages 257–264. ACM, 2010.

[8] Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret. Cryptanalysis of minrank. In *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 280–296. Springer, 2008.

[9] Uriel Feige, Amos Fiat, and Adi Shamir. Zero knowledge proofs of identity. In *STOC*, pages 210–217. ACM, 1987.

[10] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-knowledge proofs of identity. *J. Cryptology*, 1:77–94, 1988.

[11] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *Advances in Cryptology - EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer, 1999.

[12] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in Cryptology - CRYPTO 1999*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

[13] Shuhei Nakamura, Yacheng Wang, and Yasuhiko Ikematsu. Analysis on the minrank attack using kipnis-shamir method against rainbow. *IACR Cryptol. ePrint Arch.*, 2020:908, 2020.

[14] National Institute of Standards and Technology. Report on post quantum cryptography. nistir draft 8105, https://csrc.nist.gov/csrc/media/publications/nistir /8105/final/documents/nistir 8105 draft.pdf. 2019.

[15] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology - EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

[16] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer, 1989.

[17] Claus-Peter Schnorr. Efficient signature generation by smart cards. *J. Cryptol.*, 4(3):161–174, 1991.

[18] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[19] Javier A. Verbel, John Baena, Daniel Cabarcas, Ray A. Perlner, and Daniel Smith-Tone. On the complexity of "superdetermined" minrank instances. In *PQCrypto 2019*, volume 11505 of *Lecture Notes in Computer Science*, pages 167–186. Springer, 2019.