Three-Pass Identification Scheme Based on MinRank Problem with Half Cheating Probability

Bagus Santoso  
Department of Computer and Network Engineering,  
The University of Electro-Communications,  
Email: santoso.bagus@uec.ac.jp

Shuhei Nakamura  
Department of Liberal Arts and Basic Sciences, Nihon University

Yasuhiko Ikematsu  
Institute of Mathematics for Industry, Kyushu University

Takanori Yasuda  
Institute for the Advancement of Higher Education,  
Okayama University of Science

Abstract—In Asiacrypt 2001, Courtois proposed the first three-pass zero-knowledge identification (ID) scheme based on the MinRank problem. However, in a single round of Courtois’ ID scheme, the cheating probability, i.e., the success probability of the cheating prover, is 2/3, larger than half. Although Courtois also proposed a variant scheme which he claimed to have half cheating probability, its security is not formally proven, and it requires another hardness assumption on a specific one-way function and that verifier always generates challenges according to a specific non-uniform distribution.

This paper proposes the first three-pass zero-knowledge ID scheme based on the MinRank problem with the cheating probability of exactly half for each round, even with only two-bit challenge space, without any additional assumption. The proposed ID scheme requires fewer rounds and less average total communications costs than Courtois’ under the same security level against impersonation.

I. INTRODUCTION

In 1997, P. Shor [15] showed polynomial-time quantum algorithms to break integer factoring and discrete logarithm based cryptosystems. Therefore, we need to develop cryptosystems resistant to quantum computer attacks. The research area to study such cryptosystems is called post quantum cryptography (PQC) [1]. The most promising candidates for PQC are based on lattices, isogeny, coding theory, and multivariate polynomial problems. In particular, one of the computational problems based on multivariate polynomials is the multivariate quadratic (MQ) problem, which finds a solution to a system of quadratic equations over a finite field. The MQ problem is the foundation for constructing multivariate public key cryptosystems (MPKC). There have been a lot of multivariate schemes, HFE [12], UOV [10], Rainbow [8], MQDSS [5], etc. Among them, Rainbow was chosen as a third-round candidate [7] in the NIST PQC standardization project [11].

However, in many multivariate schemes, including Rainbow, the security is based on the hardness of a particular combination of the MQ problem and the MinRank problem, where the MinRank problem is the problem of finding a linear combination with a specified rank from a given finite set of matrices. Unfortunately, due to this kind of combination of MQ and MinRank problems, it is known that those schemes are vulnerable to many attacks. (See Beullens’ works on Rainbow [2], [3].) Since the MQ problem and the MinRank problem are NP-complete, we can consider constructing cryptographic schemes based on only one of the MQ or the MinRank problems. Such construction is very important for the diversity of PQC. Sakumoto et al. proposed an ID scheme [13] purely based on MQ problem, which eventually led to the signature scheme MQDSS [5] which was chosen as a second-round candidate in the NIST PQC project.

In 2001, Courtois [6] proposed the first three-pass zero-knowledge identification (ID) scheme purely based on the MinRank problem. In this ID scheme, the cheating probability, i.e., the success probability of the cheating prover, is 2/3, which is larger than half (=1/2). Thus, to achieve the desired security level against impersonation, Courtois’ ID scheme needs more rounds than the standard ID schemes with a half cheating probability, such as the Feige-Fiat-Shamir ID scheme [9]. As a result, Courtois’ scheme’s total communication cost is relatively high in practice. In the same paper [6], Courtois also proposed a variant of his ID scheme. He further claimed that the variant has half cheating probability by employing the following additional assumptions: (1) the verifier sends the challenge according to a particular fixed distribution, and (2) a specific function satisfies one-wayness. However, Courtois did not provide any formal security proof for the variant scheme, and it is unclear how the variant scheme will maintain privacy against a malicious verifier who sends challenges according to an arbitrary distribution.

In this paper, we propose a new three-pass ID scheme based on the MinRank problem. Assuming the hardness of decisional MinRank problem and the existence of perfectly binding commitment, we successfully prove, without using any additional assumption, that in our scheme, the probability that an adversary without a valid secret key is accepted by the verifier is at most half (=1/2). As a result, our scheme needs fewer rounds to achieve the desired security level than Courtois’. Also, our scheme has less average total communication cost than Courtois’ in the actual implementation using random seeds and pseudorandom generators.

This paper is organized as follows. In Section 2 we explain the MinRank problem. In Section 3 we describe our ID scheme...
and its security properties. In Section 4 we prove the theorems related to the properties of our scheme. In Section 5 we discuss the selection of practical parameters. Finally, we conclude our paper in Section 6.

II. PRELIMINARIES

Notations and Consensus: Unless noted otherwise, let any algorithm in this paper be a probabilistic polynomial time Turing Machine. We also define as follows: Let \( F \) be a finite field used throughout this paper, \( M_n(F) \) be the set of \( n \times n \) matrices over \( F \) and \( GL_n(F) \) be the set of \( n \times n \) invertible matrices over \( F \).

Definition 1 (Search MinRank Problem): The search \( \text{MinRank} \) problem is defined as follows. Given a positive integer \( r \in \mathbb{N} \) and \( m \) matrices \( M_0, M_1, \ldots, M_{m-1} \in M_n(F) \), find \( \alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in F^{m-1} \) such that \( \text{rank}(M) = r \), where \( M = \sum_{i=1}^{m-1} \alpha_i M_i - M_0 \).

Decisional \( \text{MinRank} \) Problem

In this paper, we use the hardness of the decisional version of the \( \text{MinRank} \) 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.

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

\[
\left| \Pr \left[ D^\text{Gen}(F, r, m, n) = 1 \right] - \Pr \left[ D^\text{LossyGen}(F, r, m, n) = 1 \right] \right| \geq \varepsilon,
\]

where:

- \( D^\text{Gen} \) denotes that \( D \) receives the input from the oracle \( \text{Igen} \) which generates an instance of \( \text{MinRank} \) problem that has at least one solution, i.e., \( m \) matrices: \( M_0, M_1, \ldots, M_{m-1} \in M_n(F) \), such that there exists \( \alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in F^{m-1} \) satisfying the following:

\[
\text{rank} \left( \sum_{i=1}^{m-1} \alpha_i M_i - M_0 \right) = r,
\]

- \( D^\text{LossyGen} \) denotes that \( D \) receives the input from the oracle \( \text{LossyGen} \) who generates \( m \) random matrices \( M_0, M_1, \ldots, M_{m-1} \in M_n(F) \), which do not necessarily have \( \alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in F^{m-1} \) satisfying Eq. (1).

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

Remark 1: Buss et al. [4] and Courtois [6] have proven that the decisional \( \text{MinRank} \) problem is \( \text{NP-Complete} \).

III. 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-knowledge.

A. 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 \( m \) matrices \( M_0, M_1, \ldots, M_{m-1} \in M_n(F) \). The secret key \( sk \) consists of \( \alpha = (\alpha_1, \ldots, \alpha_{m-1}) \in F^{m-1} \) such that \( \text{rank}(M) = r \), where \( M = \sum_{i=1}^{m-1} \alpha_i M_i - M_0 \).

Interactive Protocol: A single elementary round of interactive protocol between a prover \( P(pk, sk) \) and a verifier \( V(pk) \) is described as follows. Similar to Courtois’ ID scheme [6], we also employ the hash function \( H \) which acts as a commitment with perfectly hiding and computational binding properties.

Step 1: \( P \) randomly generates \( S_0, S_1, T_0, T_1 \in GL_n(F) \) and \( X_0, X_1 \in M_n(F) \). Next, \( P \) generates \( \beta_0 = (\beta_0_1, \ldots, \beta_0_{m-1}) \in F^{m-1} \) and \( \beta_1 = (\beta_1_1, \ldots, \beta_1_{m-1}) \in F^{m-1} \), then computes the following:

\[
N_0 = \sum_{i=1}^{m-1} \beta_0_i M_i \quad N_1 = \sum_{i=1}^{m-1} \beta_1_i M_i
\]

\[
U_{0,0} = T_0 N_0 S_0 + X_0 \quad U_{1,0} = T_1 N_1 S_1 + X_1
\]

\[
U_{0,1} = T_0 M S_0 + U_{0,0} \quad U_{1,1} = T_1 M S_1 + U_{1,0}
\]

\[
R_0 = (S_0, T_0, X_0) \quad R_1 = (S_1, T_1, X_1)
\]

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

\[
Y_0 = (H(U_{0,0}), H(U_{0,1}), H(R_0))
\]

\[
Y_1 = (H(U_{1,0}), H(U_{1,1}), H(R_1))
\]

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 \( c \in \{0, 1, 2, 3\} \) 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 \( c \) | \( Z_{0,0} \) | \( Z_{0,1} \) | \( Z_{1,0} \) | \( Z_{1,1} \) |
|----------|----------|----------|----------|----------|
| \( c = 0 \) | \( U_{0,0} \) | \( U_{0,1} \) | \( U_{1,0} \) | \( U_{1,1} \) |
| \( c = 1 \) | \( U_{0,0} \) | \( U_{0,1} \) | \( U_{1,0} \) | \( U_{1,1} \) |
| \( c = 2 \) | \( U_{0,0} \) | \( U_{0,1} \) | \( U_{1,0} \) | \( U_{1,1} \) |
| \( c = 3 \) | \( U_{0,0} \) | \( U_{0,1} \) | \( U_{1,0} \) | \( U_{1,1} \) |

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

Remark 2: The response \( Z \) is said to be a valid response with respect to challenge \( c \) if all checking equations in the verifier side corresponding to the value of \( c \) hold.

Remark 3: A full identification scheme consists of \( \ell \) repetitions of the single elementary round above and the verifier will accept the prove if and only if \( V \) outputs 1 in all \( \ell \) rounds.
B. 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 to 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 with respect to 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 our full paper in [14] for the detailed proof.

C. 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 with respect to the challenge \( c \in \{0, 1, 2, 3\} \). 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 the search MinRank problem represented by the public key.

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

**Corollary 1:** If the public key has no corresponding secret key, the success probability of any prover to be accepted by the verifier in all \( \ell \) 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 \( A \) be an algorithm such that given the public key \( pk \), it is accepted in all \( \ell \) rounds of the full identification protocol with probability \( \varepsilon_A \geq \frac{1}{2^\ell} \), where the probability is taken over the random coins of \( A \), the key generator, and the verifier. Assume that \( H \) is a random oracle. Then, we can construct an algorithm which \((t, \varepsilon)\)-solves the decisional MinRank problem associated with the finite field \( \mathbb{F} \) and \( r, m, n \in \mathbb{N} \) such that the following holds.

\[ \varepsilon = \varepsilon_A - \frac{1}{2^\ell}, \quad t = t_A, \]

where \( t_A \) is the maximum total time of \( A \) interacting in one full identification protocol.

**Corollary 2:** If the decisional MinRank problem is \((t, \varepsilon)\)-hard, then the success probability of any adversary attempting to impersonate a prover in the random oracle model without secret key within \( t \) time units is upper-bounded by \( \varepsilon + 1/2^\ell \).

D. Zero-Knowledgeness

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

**Theorem 3 (Zero-Knowledgeness):** Assume that \( H \) is a random oracle. 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 \( sk \).

IV. PROOFS OF MAIN THEOREMS

A. 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
rank \( \sum_{i=1}^{m-1} \alpha_i M_i - M_0 \) = \( r \) holds, where \( r \) and \( M_0, \ldots, M_{m-1} \) are generated by the key generation algorithm as elements of the public key.

Remark 4: 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 \( Z^{(1)}_{0,0} \) be parsed as \( Z^{(1)}_{0,0} = (\tilde{S}^{(1)}, \tilde{T}^{(1)}, \tilde{X}^{(1)}) \) and \( Z^{(1)}_{0,1} \) be parsed as \( Z^{(1)}_{0,1} = (\tilde{S}_{1,\ldots,1}, \tilde{X}_{m-1}^{(1)}) \). Also let \( Z^{(2)}_{0,0} \) be parsed as \( Z^{(2)}_{0,0} = (\tilde{S}^{(2)}, \tilde{T}^{(2)}, \tilde{X}^{(2)}) \) and \( Z^{(2)}_{0,1} \) be parsed as \( Z^{(2)}_{0,1} = (\tilde{\mu}_1, \ldots, \tilde{\mu}_{m-1}) \). Since the following holds:

\[
H \left( \tilde{S}^{(1)}, \tilde{T}^{(1)}, \tilde{X}^{(1)} \right) = H \left( \tilde{S}^{(2)}, \tilde{T}^{(2)}, \tilde{X}^{(2)} \right) = Y_{0,2},
\]

we can define as follows: \( (\tilde{S}, \tilde{T}, \tilde{X}) := (\tilde{S}^{(1)}, \tilde{T}^{(1)}, \tilde{X}^{(1)}) = (\tilde{S}^{(2)}, \tilde{T}^{(2)}, \tilde{X}^{(2)}) \). From \( H(Z^{(0)}_{0,0}) = Y_{0,0} \) and Eq. (4), we obtain as follows.

\[
Y_{0,0} = H(Z^{(0)}_{0,0}) = H \left( \tilde{T} \left( \sum_{i=1}^{m-1} \tilde{\gamma}_i M_i \right) \tilde{S} + \tilde{X} \right) \quad (8)
\]

\[
\Rightarrow Z^{(0)}_{0,0} = \tilde{T} \left( \sum_{i=1}^{m-1} \tilde{\gamma}_i M_i \right) \tilde{S} + \tilde{X}.
\]

Similarly, from \( H(Z^{(0)}_{0,1}) = Y_{0,1} \) and Eq. (6), we also have the followings hold.

\[
Y_{0,1} = H(Z^{(0)}_{0,1}) = H \left( \tilde{T} \left( \sum_{i=1}^{m-1} \tilde{\mu}_i M_i \right) \tilde{S} + \tilde{X} \right) \quad (9)
\]

\[
\Rightarrow Z^{(0)}_{0,1} = \tilde{T} \left( \sum_{i=1}^{m-1} \tilde{\mu}_i M_i \right) \tilde{S} + \tilde{X} - \tilde{T} M_0 \tilde{S}.
\]

Finally, we have the followings hold.

\[
\text{rank}(Z^{(0)}_{0,1} - Z^{(0)}_{0,0}) = \text{rank} \left( \tilde{T} \left( \sum_{i=1}^{m-1} (\tilde{\mu}_i - \tilde{\gamma}_i) M_i - M_0 \right) \tilde{S} \right) \quad (a)
\]

\[
= \text{rank} \left( \sum_{i=1}^{m-1} (\tilde{\mu}_i - \tilde{\gamma}_i) M_i - M_0 \right),
\]

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

Case 2: \( Y \) and \( (Z^{(0)}, Z^{(1)}, Z^{(2)}) \): Similar to Case 1. The only difference is that all relations and components of \( Z^{(1)} \) in Case 1 are substituted by those of \( Z^{(2)} \).

Case 3: \( Y \) and \( (Z^{(1)}, Z^{(2)}, Z^{(3)}) \): Let \( Z^{(2)}_{1,0} \) be parsed as \( Z^{(2)}_{1,0} = (\tilde{S}^{(2)}, \tilde{T}^{(2)}, \tilde{X}^{(2)}) \) and \( Z^{(2)}_{1,1} \) be parsed as \( Z^{(2)}_{1,1} = (\tilde{\gamma}_1, \ldots, \tilde{\gamma}_{m-1}) \). Also let \( Z^{(1)}_{1,0} \) be parsed as \( Z^{(1)}_{1,0} = (\tilde{S}^{(1)}, \tilde{T}^{(1)}, \tilde{X}^{(1)}) \) and \( Z^{(1)}_{1,1} \) be parsed as \( Z^{(1)}_{1,1} = (\tilde{\mu}_1, \ldots, \tilde{\mu}_{m-1}) \). Since the following holds:

\[
H \left( \tilde{S}^{(1)}, \tilde{T}^{(1)}, \tilde{X}^{(1)} \right) = H \left( \tilde{S}^{(2)}, \tilde{T}^{(2)}, \tilde{X}^{(2)} \right) = Y_{1,2},
\]

we can define as follows: \( (\tilde{S}, \tilde{T}, \tilde{X}) := (\tilde{S}^{(1)}, \tilde{T}^{(1)}, \tilde{X}^{(1)}) = (\tilde{S}^{(2)}, \tilde{T}^{(2)}, \tilde{X}^{(2)}) \). From \( H(Z^{(3)}_{1,0}) = Y_{1,0} \) and Eq. (7), we obtain as follows.

\[
Y_{1,0} = H(Z^{(3)}_{1,0}) = H \left( \tilde{T} \left( \sum_{i=1}^{m-1} \tilde{\gamma}_i M_i \right) \tilde{S} + \tilde{X} \right) \quad (10)
\]

\[
\Rightarrow Z^{(3)}_{1,0} = \tilde{T} \left( \sum_{i=1}^{m-1} \tilde{\gamma}_i M_i \right) \tilde{S} + \tilde{X}.
\]

Similarly, from \( H(Z^{(3)}_{1,1}) = Y_{1,1} \) and Eq. (5), we also have the followings hold.

\[
Y_{1,1} = H(Z^{(3)}_{1,1}) = H \left( \tilde{T} \left( \sum_{i=1}^{m-1} \tilde{\mu}_i M_i \right) \tilde{S} + \tilde{X} - \tilde{T} M_0 \tilde{S} \right) \quad (11)
\]

\[
\Rightarrow Z^{(3)}_{1,1} = \tilde{T} \left( \sum_{i=1}^{m-1} \tilde{\mu}_i M_i \right) \tilde{S} + \tilde{X} - \tilde{T} M_0 \tilde{S}.
\]

Finally, we have the followings hold.

\[
\text{rank}(Z^{(3)}_{1,1} - Z^{(3)}_{1,0}) = \text{rank} \left( \tilde{T} \left( \sum_{i=1}^{m-1} (\tilde{\mu}_i - \tilde{\gamma}_i) M_i - M_0 \right) \tilde{S} \right) \quad (a)
\]

\[
= \text{rank} \left( \sum_{i=1}^{m-1} (\tilde{\mu}_i - \tilde{\gamma}_i) M_i - M_0 \right),
\]

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

Case 4: \( Y \) and \( (Z^{(0)}, Z^{(1)}, Z^{(3)}) \): Similar to Case 3. The only difference is that all relations and components of \( Z^{(2)} \) in Case 1 are substituted by those of \( Z^{(0)} \).

B. 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.

C. Proof Sketch of Theorem 2

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

$$\left| \Pr[D^{\text{IGen}}(\text{par}) = 1] - \Pr[D^{\text{LossyGen}}(\text{par}) = 1] \right| \leq \varepsilon_A - \frac{1}{2^q}.$$ 

This proves Theorem 2.

D. 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 generated by a honest prover who possesses valid secret key. Note that we can put the responses and commitment in Courtois’ ID scheme [6]. It is easy to see that we can apply the proof of zero-knowledge for Courtois’ ID scheme into our proposed scheme.

V. PARAMETER SELECTIONS

A. 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 $Z^{(0)}$ denote the valid response of the prover with respect to challenge $c$ for any $c \in \{0, 1, 2, 3\}$. For simplicity, here we assume that all matrices are $n$-square matrices and $E = E_q$, where $q$ is a power of some prime. Thus, we have:

$$|Z^{(0)}| = |Z^{(3)}| \approx 2n^2 \log_2 q + \underline{\text{seed}_{\text{STX}}} + |\text{seed}_b|,$$

$$|Z^{(1)}| = |Z^{(2)}| \approx 2|\underline{\text{seed}_{\text{STX}}} + |\text{seed}_b| + (m - 1) \log_2 q,$$

where $\underline{\text{seed}_{\text{STX}}}$ is the seed for generating $(S_0, T_0, X_0)$ or $(S_1, T_1, X_1)$ and $\text{seed}_b$ is the seed for generating $\beta_0$ or $\beta_1$.

Let $\#R_{1/2}$ and $\#R_{2/3}$ denote the necessary number of rounds to achieve $\ell$-bit security for our scheme and Courtois’ respectively. It is easy to see that $\#R_{1/2} = \ell$ and $\#R_{2/3} = 2/3[\ell/(\log_2 3 - 1)]$. Assuming that the seeds for $\ell$-bit security are $\ell$ bits, we have the following equations for estimating the average total communication costs for $\ell$-bit security.

$$\#Z_{1/2} \approx \frac{\ell}{2} \left( (n^2 + (m - 1)) \log_2 q + \frac{5\ell}{2} \right),$$

$$\#Z_{2/3} \approx \frac{2}{3} \left[ \frac{\ell}{\log_2 3 - 1} \left( (n^2 + (m - 1)) \log_2 q + \frac{3\ell}{2} \right) \right],$$

where $\#Z_{1/2}$ and $\#Z_{2/3}$ denote the average total communication costs of our scheme and that of Courtois’ respectively.

B. SECURITY PARAMETERS

Based on various attacks on the MinRank problem which we review in our full paper [14], we recommend parameters for 128, 192 and 256-bit security with $q = 2$ as follows. Here we denote bytes as B.

| bit security | $(n, m, r)$ | $#R_{1/2}$ | $#R_{2/3}$ | $#Z_{1/2}$ | $#Z_{2/3}$ |
|--------------|------------|------------|------------|------------|------------|
| 128          | (26, 209, 13) | 128 | 146 | 19264 B | 19637 B |
| 192          | (33, 331, 17) | 192 | 220 | 45576 B | 46800 B |
| 256          | (39, 409, 20) | 256 | 292 | 84128 B | 86614 B |

VI. CONCLUSION

In this paper, we have shown a construction of a new three-pass ID scheme with half cheating probability. In practice, compared to Curtois’ ID scheme [6], our scheme requires less number of repetitions to achieve the desired security level and has less average total communication cost. By combining the soundness and the zero-knowledgeness, we may obtain the security against passive-attack. As a future work, we aim to construct a digital signature scheme based on our proposed ID scheme and prove its security against quantum adversaries.

Acknowledgements This work was supported by JST CREST Grant Number JPMJCR2113, JSPS KAKENHI Grant Number JP19K20266, JP20K19802, JP20K03741, JP18H01438, and JP18K11292.

REFERENCES

[1] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. Post-quantum cryptography. Springer, 2009.
[2] Ward Beullens. Improved cryptanalysis of UOV and rainbow. In EUROCRYPT 2021, pages 348–373. Springer, 2021.
[3] Ward Beullens. Breaking rainbow takes a weekend on a laptop. IACR Cryptol. ePrint Arch., (214), 2022.
[4] 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.
[5] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. From 5-pass MQ-based identification to MQ-based signatures. In ASIACRYPT 2016, pages 135–165, 2016.
[6] Nicolas T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem minrank. In ASIACRYPT ’01, pages 402–421. Springer, 2001.
[7] 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.
[8] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In ACNS 2005, pages 164–175, 2005.
[9] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-knowledge proofs of identity. J. Cryptology, 1:77–94, 1988.
[10] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In EUROCRYPT ’99, pages 206–222. Springer, 1999.
[11] National Institute of Standards and Technology. Report on post quantum cryptography. Nistir draft 8105, https://csrc.nist.gov/csrc/media/publications/nistir /8105/ni nal/documents/nistir 8105 draft.pdf, 2019.
[12] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In EUROCRYPT ’96, pages 33–48. Springer, 1996.
[13] Koichi Sakumoto, Taizou Shiraib, and Harumasa Hiwatai. Public-key identification schemes based on multivariate quadratic polynomials. In CRYPTO 2011, pages 706–723, 2011.
[14] Bagus Santoso, Yusuhiko Ikematsu, Shuhei Nakamura, and Takanori Yasuda. Three-pass identification scheme based on minrank problem with half cheating probability. CoRR, arXiv:2205.03255, 2022.
[15] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26(5):1484–1509, 1997.