2023-02-24

Rank AGS Identification Scheme and Signature Scheme

Nagaraja, V

10.3390/math11051139
Mathematics
MDPI AG

mathematics

MDPI

Article

Rank AGS Identification Scheme and Signature Scheme

Vaishnavi Nagaraja [1,†], Muhammad Rezal Kamel Ariffin [1,*,†], Terry Shue Chien Lau [2,†], Nurul Nur Hanisah Adenan [1,†], Ji-Jian Chin [3,†], Sook-Chin Yip [4,†] and Timothy Tzen Vun Yap [2,†]

1 Institute for Mathematical Research, Universiti Putra Malaysia, Serdang 43400, Selangor, Malaysia
2 Faculty of Computing and Informatics, Multimedia University, Cyberjaya 63100, Selangor, Malaysia
3 School of Engineering, Computing and Mathematics (Faculty of Science and Engineering), University of Plymouth, Drake Circus, Plymouth PL 48AA, UK
4 Faculty of Engineering, Multimedia University, Cyberjaya 63100, Selangor, Malaysia
* Correspondence: rezal@upm.edu.my
† These authors contributed equally to this work.

Abstract: The identification protocol is a type of zero-knowledge proof. One party (the prover) needs to prove his identity to another party (the verifier) without revealing the secret key to the verifier. One can apply the Fiat–Shamir transformation to convert an identification scheme into a signature scheme which can be used for achieving security purposes and cryptographic purposes, especially for authentication. In this paper, we recall an identification protocol, namely the RankID scheme, and show that the scheme is incorrect and insecure. Then, we proposed a more natural approach to construct the rank version of the AGS identification protocol and show that our construction overcomes the security flaws in the RankID scheme. Our proposal achieves better results when comparing the public key size, secret key size, and signature size with the existing identification schemes, such as Rank RVDC and Rank CVE schemes. Our proposal also achieves 90%, 50%, and 96% reduction for the signature size, secret key size, and public key size when compared to the Rank CVE signature scheme.

Keywords: public-key cryptography; post-quantum cryptography; code-based cryptography; rank metric; signature scheme; identification scheme

MSC: 11T71

Citation: Nagaraja, V.; Ariffin, M.R.K.; Lau, T.S.C.; Adenan, N.N.H.; Chin, J.-J.; Yip, S.-C.; Yap, T.T.V. Rank AGS Identification Scheme and Signature Scheme. *Mathematics* **2023**, *11*, 1139. https://doi.org/10.3390/math11051139

Academic Editor: Jonathan Blackledge

Received: 25 December 2022
Revised: 27 January 2023
Accepted: 30 January 2023
Published: 24 February 2023

1. Introduction

1.1. Literature Review

Cryptography refers to the secure communication techniques that are derived from mathematical concepts and algorithms to transform messages in ways that mean it is hard to retrieve back the message. There are well-known cryptosystems, such as RSA, which have been used until today. Nevertheless, this cryptosystem suffers from a few weaknesses that might lead to the vulnerability of attacks, as we can read in [1,2]. The hard problem of RSA, which is the factorization of large prime numbers, could turn out to be its weakness if there exists a quantum computer. Therefore, it is necessary for cryptographers to construct other cryptographic primitives that resist attacks by quantum computers, which are often coined as post-quantum cryptosystems. One of the most common candidates for post-quantum cryptosystems is built based on code-based cryptography. McEliece cryptosystem [3] is one of the most well-known and the first motivation initiated in code-based cryptosystems almost 40 years ago. Digital signature schemes (DSS) under code-based cryptography are also secure as they are able to achieve three goals of cryptography, including data integrity, authenticity, and non-repudiation.

One can consider the construction of code-based DSS via the hash-and-sign approach, such as the CFS scheme proposed by Courtois et al. [4]. In this scheme, the document is

repeatedly hashed to the bit-length r until the output becomes a decryptable ciphertext. However, this was one of the weaknesses of this signature apart from having a very large public key size. On the other hand, one can construct a code-based DSS by considering the zero-knowledge protocol approach (ZKP). More specifically, in a zero-knowledge protocol, one party (named Prover $\mathcal{P}$) needs to prove to the other party (named verifier $\mathcal{V}$) that he or she knows the secret key without revealing the value or any information regarding the secret key. Proof of identity as a means of authentication is the most common and secure application of ZKP. One type of ZKP is the identification protocol which can be converted into a signature scheme via the Fiat–Shamir paradigm. Meanwhile, if the person loses his or her data or key, recovery is difficult to be attempted in ZKP. ZKP also has a large signature size due to a large number of repetitions, and it requires a lot of computations since it needs a large number of interactions between the prover and the verifier.

In 1994, Stern designed an identification protocol [5] that worked in the Hamming metric. In this case, let F_{q^m} be a finite field with q^m elements where q is a prime power, and m is an integer. In this scheme, given an error vector e which has weight w and a vector, $s = He^T$ where H is a parity check matrix over $F_2^{(n-k)\times n}$. The prover $\mathcal{P}$ is needed to convince the verifier $\mathcal{V}$ that he or she knows the value of e (the secret key). Stern managed to reduce the cheating probability (the probability where a dishonest prover not knowing e can cheat the verifier in the protocol) from $\frac{2}{3}$ to $\frac{1}{2}$ which led to a reduction in the signature size. Later in 1997, Veron [6] proposed a different formulation of the secret key, $x = mG \oplus e \in F_2^n$ where the matrix $G \in F_2^{k\times n}$ and x are public parameters. Despite the increment of the public key size, Veron succeeded in reducing the communication cost. Since then, various schemes have been invented using different modifications to enhance their schemes from the previous ones. Aguilar, Gaborit, and Schrek [7] proposed a scheme (AGS) utilizing double circulant codes to increase the number of challenges. They also managed to cut down the communication cost in addition to reducing the size of the secret and public keys.

More recently, rank metrics have been considered to construct code-based identification protocols and DSS by extending the constructions from the code-based identification protocols and DSS in the Hamming metric. In 2018, Bellini et al. [8] proposed the rank metric version of the Veron and CVE identification protocols and DSS. However, Lau et al. [9] showed that the rank Veron was insecure, as its secret key could be recovered in polynomial time. Nevertheless, Bellini et al. [10] improved the rank Veron DSS and proposed another scheme, namely the RVDC identification protocol and DSS. Furthermore, in 2019, Ayebie et al. [11] designed a rank metric version of the AGS identification scheme by using random double circulant codes, which is known as the RankID scheme.

1.2. Research Flow

In this paper, we analyzed the RankID scheme. Their construction has errors in correctness, which results in the invalidity of the scheme. The operations defined in the scheme do not ensure the commutativity of the matrices and do not preserve the rank of error vectors. Even if we assume the scheme is correct, we show that the scheme is insecure, as its design leads to the leakage of the secret key. Then, we propose a new rank version of the AGS ID more naturally and show that the new scheme achieves completeness, soundness, and zero-knowledge properties. We also provide parameters achieving 128-bit and 256-bit security levels, the latter is determined by the complexity for solving the Rank Syndrome Decoding (RSD) problem.

1.3. Contribution of This Work

Our Rank AGS scheme parameters can reduce the signature and key size when compared to the Rank CVE [8] and RVDC [10] schemes.

1.4. Paper Organization

This paper is structured as follows: in Section 2, we present the notions and preliminaries that are used throughout the paper. Section 3 provides the analysis of RankID, which

shows the errors in RankID that lead to the insecurity of the scheme. Section 4 introduces the explanations and details of our proposed scheme, Rank AGS. Section 5 shows the achievement of our proposed scheme on zero knowledge protocol security properties such as completeness, soundness, and zero knowledge. Additionally, we also provide the signing and verification algorithm of Rank AGS and the comparison of the sizes of the signature, public, and secret key of Rank AGS with the other existing schemes in this section. Furthermore, we also added the percentage of reduction in the key and signatures sizes of Rank AGS with the reference Rank CVE as the original reference. Finally, we finish with a section for the conclusion (Section 6).

2. Preliminaries

In this section, we recall the background on rank metrics and the hard problem used in this paper. We also introduce the specification for AGS and RankID that have been used in [7,11]. Throughout this paper, we will be using the following notations and definitions.

Let q be a prime power and m be an integer. Then, let F_{q^m} be a finite field with q^m elements.

Definition 1. *An $[n,k]$-linear code C of length n is a linear subspace of $F_{q^m}^n$ with dimension k. A matrix $G \in F_{q^m}^{k\times n}$ is called a generator matrix of code C if its rows form a basis of C. A matrix H is called a parity check matrix of C if $C = \{x \in F_{q^m}^n : H \cdot x^T = 0\}$.*

Definition 2 (Rank Support)**.** *Let $x = (x_1, \cdots, x_n) \in F_{q^m}^n$. The support of x, $Supp(x)$ is an F_q-vector space spanned by elements $x_1, \cdots, x_n$.*

Definition 3 (Rank Metric)**.** *Let $x = (x_1, \cdots, x_n) \in F_{q^m}^n$; the rank weight of x is defined as the dimension of the support of x,*

$$wt_R(x) = dim(Supp(x)).$$

Let $\beta_1, \cdots, \beta_m$ be a basis for F_{q^m}. For each $1 \le i \le n$, we can write x_i as an F_q-linear combination of the basis, i.e., there exists $c_{ji} \in F_q$ such that

$$x_i = \sum_{j=1}^{m} c_{ji}\beta_j .$$

When forming an $m \times n$ matrix $M = (c_{ji}) \in F_q$, and we can rewrite x as:

$$x = (x_1, \cdots, x_n) = (\beta_1, \cdots, \beta_m)M,$$

and the rank weight of x also can be defined as the rank of the matrix M, $wt_R(x) = rk(M)$. Now, let us define a problem that most of the cryptosystem in the rank metric is based on.

Problem 1 (Rank syndrome decoding problem (RSD))**.** *Given a random matrix $G \in F_{q^m}^{k\times n}$, the random vectors $x \in F_{q^m}^n$, $f \in F_{q^m}^k$ and an integer of $r > 0$ can be used as an input. The rank syndrome decoding, $RSD(q,m,n,k,r)$ problem needs to determine the vector $e \in F_{q^m}^n$ such that $rk(e) = r$ and $fG \oplus e = x$.*

Gaborit and Zémor [12] showed that the RSD could be probabilistically reduced to the syndrome decoding problem in the Hamming metric, where the syndrome decoding problem is an NP-complete problem. Therefore, RSD is acceptable as a good candidate for code-based cryptography.

The complexity of solving the rank syndrome decoding problem (RSD) is shown below. We list down the combinatorial and algebraic attacks on $RSD(q,m,n,k,r)$ in Table 1 and Table 2, respectively, from [13] with their corresponding solving complexities.

Table 1. Combinatorial attacks on RSD.

Attacks	Complexity
CS [14]	$O((nr+m)^3 q^{(m-r)(r-1)})$
GRS-I [15]	$O((n-k)^3 m^3 q^{r\, min\{k,\frac{km}{n}\}})$ if $s \neq 0$, $O((n-k)^3 m^3 q^{(r-1) min\{k,\frac{km}{n}\}})$ if $s = 0$
OJ-I [16]	$O(r^3 m^3 q^{(r-1)(k+1)})$
OJ-II [16]	$O((k+r)^3 r^3 q^{(m-r)(r-1)})$
GRS-II [15]	$O((n-k)^3 m^3 q^{(r-1)\, min\{k+1,\frac{(k+1)m}{n}\}})$
AGHT [17]	$O((n-k)^3 m^3 q^{r\frac{(k+1)m}{n}-m})$

We used the following notation in Table 2 below.
The constant linear algebra is $w \approx 2.807$, and the integer is $a \geq 0$,
$p := max\{i : m\binom{n-i-k-1}{r} \geq \binom{n-i}{r} - 1\}$,
$A_t := \sum_{j=1}^{t} \binom{n}{r}\binom{mk+1}{j}$,
$B_t := \sum_{j=1}^{t}(m\binom{n-k-1}{r}\binom{mk+1}{j} + \sum_{i=1}^{j}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{mk+1}{j-i})$,
$b := min\{t \in Z : 0 < t < r+2, A_t \leq B_t\}$,
$d_{n,r,k} = (r+1)(k+1) - (n+1)$,
$C_{n,k} = \binom{n}{k}$, and $v_k = n-k-1$.

Table 2. Algebraic attacks on RSD.

Attacks	Conditions	Complexity
FLP [18]	$m = n, (n-r)^2 = nk$	$O((log\, q)n^{3(n-r)^2})$
CGK [19]	-	$O(k^3 m^3 q^{r\frac{km}{n}})$
GRS [15]	$d_{n,r,k} \leq 0$	$O(((r+1)(k+1)-1)^3)$
	$[\frac{d_{n,r,k}}{r}] \leq k$	$O(r^3 k^3 q^{r[\frac{d_{n,r,k}}{r}]})$
BBB [20]	$mC_{v_k,r} \geq C_{n,r}$	$O((\frac{((m+n)r)^r}{r!})^w)$
	$mC_{v_k,r} < C_{n,r}$	$O((\frac{((m+n)r)^{r+1}}{(r+1)!})^w)$
BBC [21]	$mC_{v_k-p,r} \geq C_{n-p,r} - 1$	$O(mC_{v_k-p,r}C_{n-p,r^{w-1}})$
	$mC_{v_k,r} \geq C_{n-a,r} - 1$	$O(q^{ar}mC_{v_k,r}C_{n-a,r^{w-1}})$
	$A_b - 1 \leq B_b, q = 2$	$O(B_b A_b^{w-1})$

Definition 4 (Circulant matrix). *A $k \times k$ matrix is called a circulant matrix if each row is obtained from the previous one by a cyclic shift from one position to the right. In particular, A is generated by a vector $a = (a_0, \cdots, a_{k-1})$ in the form of:*

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{k-1} \\ a_{k-1} & a_0 & \cdots & a_{k-2} \\ & & \vdots & \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

Definition 5 (Double circulant matrix). *A $[2k, k]$-code over F_{q^m} is a double circulant code if it is generated by a matrix $G = [A|B]$, where A and B are $k \times k$ circulant matrices.*

RankID

In this subsection, we first introduce the definitions and operations that have been used in RankID [11]. Then, we identified the errors found in the RankID scheme.

Definition 6. *Let vector* $x = (x_1, \cdots, x_n) \in F_{q^m}^n$ *and* $M = (c_{ji}) \in F_q$, *as defined in Equation (2). We defined the function* Φ_β *map from* $F_q^{m\times n}$ *to* $F_{q^m}^n$ *as* $\Phi_\beta(M) = x$. *The inverse function,* Φ_β^{-1} *was defined as the mapping for* $F_{q^m}^n$ *to* $F_q^{m\times n}$ *and we can rewrite it as* $\Phi_\beta^{-1}(x) = (M)$.

Definition 7 (Asterisk Product)**.** *Let* $Q \in F_q^{m\times m}$, $x \in F_{q^m}^n$, $M = (c_{ji}) \in F_q$ *and* β *be a basis of* F_{q^m} *over* F_q. *We define the product* $Q * x$ *by*

$$Q * x = \Phi_\beta(QM).$$

Let k be an integer such that $k > 1$, to any $\alpha \in F_{q^m}^*$ we associate the symmetric matrix $\tilde{\alpha}_k \in F_{q_m}^{k\times k}$ such that:

$$\tilde{\alpha}_k = \begin{pmatrix} \alpha & & & \\ & \alpha^2 & & \\ & & \ddots & \\ & & & \alpha^k \end{pmatrix} \tag{1}$$

Definition 8 (Bullet Product)**.** *Let* α *be an element of* $F_{q^m}^*$, k *be an integer such that* $k > 1$, *and* $v = (v_1||v_2)$ *(where* $||$ *is the concatenation symbol) be a vector of* $F_{q^m}^n$ *such that* $v_1, v_2 \in F_{q^m}^k$. *We define the product* $v \bullet \alpha$ *as follows:*

$$v \bullet \alpha = v_1\tilde{\alpha}_k||v_2\tilde{\alpha}_k.$$

where $\tilde{\alpha}_k$ *is as defined in Equation (1).*

The RankID scheme [11] utilizes the double circulant matrix from the AGS ID scheme [7] to generate the generator matrix, G as a public key. The hard problem on which the RankID is based is the RSD problem. They introduced the special multiplication law that has been used in their protocol, as we explained in the previous section in definitions (7) and (8).

Their protocol uses a public $k \times n$ (with $n = 2k$) random double circulant matrix G over F_{q^m}. This matrix G generates an $[n, k]$-linear code over F_{q^m}. They considered the matrix of type $G = (I_k, G_1)$ where G_1 is a $k \times k$ circulant matrix over F_{q^m} and I_k is the $k \times k$ identity matrix.

Private key: (e, f) with $e \in F_{q^m}^{2k}$ with $rk(e) = r$ and $f \in F_{q^m}^k$.

Public key: (G, x, r) with $G \in F_{q^m}^{k\times 2k}$, $x = fG \oplus e$.

3. Analysis of RankID

Here, we provide more details regarding the errors that we encountered in the RankID (Table 3). The authors in [11] claimed that RankID achieved completeness by the following argument.

When $g = 0$, then the verifier can compute:

$$\begin{aligned} (u \oplus f\tilde{\alpha}_k)G \oplus x \bullet \alpha &= uG \oplus f\tilde{\alpha}_k G \oplus (fG \oplus e) \bullet \alpha \\ &= uG \oplus f\tilde{\alpha}_k G \oplus fG \bullet \alpha \oplus e \bullet \alpha \\ &= uG \oplus f\tilde{\alpha}_k G \oplus (f\tilde{\alpha}_k||fG_1\tilde{\alpha}_k) \oplus e \bullet \alpha \\ &= uG \oplus f\tilde{\alpha}_k G \oplus (f\tilde{\alpha}_k||f\tilde{\alpha}_k G_1) \oplus e \bullet \alpha \\ &= uG \oplus f\tilde{\alpha}_k G \oplus f\tilde{\alpha}_k G \oplus e \bullet \alpha \\ &= uG \oplus e \bullet \alpha. \end{aligned} \tag{2}$$

Equation (2) is incorrect because $\tilde{\alpha}_k$ and G_1 are not commutative. Although $\tilde{\alpha}_k$ is symmetric: it does not commute with the matrix G_1. Therefore, $fG_1\tilde{\alpha}_k \neq f\tilde{\alpha}_k G_1$.

The second error in the scheme is when $g = 1$, then we obtain $rk(Q * (e \bullet \alpha)P) \neq r$. To illustrate $rk(e \bullet \alpha) \neq r$, we provide a counterexample here. Since P and Q are invertible over F_q, they preserve the rank of the vector. Therefore, we only require showing that $rk(e \bullet \alpha) \neq r$.

Table 3. The identification protocol (RankID).

Prover, $\mathcal{P}$		Verifier, $\mathcal{V}$
$u \in F_{q^m}^k$		
$P \in GL_{2k}(F_q)$		
$Q \in GL_m(F_q)$		
	$c_1 = h(P\|\|Q\|\|(uG_1 \oplus f))$, $c_2 = h(Q * (uG)P)$ $\longrightarrow$	
	$\alpha \in F_{q^m}$ $\longleftarrow$	
	$c_3 = h(Q*(uG \oplus (e \bullet \alpha))P)$ $\longrightarrow$	
	$g \in \{0,1\}$ $\longleftarrow$	
if $g = 0$,		
	$u + f\tilde{\alpha}_k$, $uG_1 \oplus f$, $(P\|\|Q)$ $\longrightarrow$	verify: $c_1 = h(P\|\|Q\|\|(uG_1 \oplus f))$, $c_3 = h(Q * (uG \oplus (e \bullet \alpha))P)$
if $g = 1$,		
	$Q * (uG)P$, $Q * (e \bullet \alpha)P$ $\longrightarrow$	verify: $c_2 = h(Q * (uG)P)$, $c_3 = h(Q * (uG \oplus (e \bullet \alpha))P)$ $rk(Q * (e \bullet \alpha)P) \leq r$

Proof. Let z be a primitive element in F_{q^m} and $\{1, z, z^2, \cdots, z^{m-1}\}$ be a basis of F_{q^m} over F_q. Let $q = 2$, $k = 4$, $m = 11$, $\alpha = z^2$, $e = (e_1||e_2) \in F_{q^m}^{2k}$ where $e_1 = (1, z, z^2, z)$ and $e_2 = (z, z^2, z, z^2)$ with $rk(e) = 3$.

$$\begin{aligned} rk(e \bullet \alpha) &= rk(e_1\tilde{\alpha}_k||e_2\tilde{\alpha}_k) \\ &= rk(1, z, z^2, z)\begin{pmatrix} z^2 & & & \\ & z^4 & & \\ & & z^6 & \\ & & & z^8 \end{pmatrix} \\ &\quad ||(z, z^2, z, z^2)\begin{pmatrix} z^2 & & & \\ & z^4 & & \\ & & z^6 & \\ & & & z^8 \end{pmatrix} \\ &= rk(z^2, z^5, z^8, z^9||z^3, z^6, z^7, z^{10}) \\ &= 8. \end{aligned}$$

□

From the above counterexample, we obtain $rk(e \bullet \alpha) = 8$ which is greater than $rk(e) = r = 3$. Therefore, $rk(Q * (e \bullet \alpha)P) \neq r$.

Security Analysis of RankID

Now, we assumed that RankID was correct even though we found some errors in this scheme. We showed that, based on the information sent through the channels, one could recover the secret of the scheme.

As we know, the adversary can have the public key, which is (G, r, x) and other elements from the scheme such as $(\alpha, G_1, x, u + f\tilde{\alpha_k}, uG_1 \oplus f, P||Q)$ as the adversary can look over the communication channel.

Now, we show how the secret key f was retrieved as follows:

Let $w = u + f\tilde{\alpha}_k$ and $v = uG_1 \oplus f$,

$$\begin{aligned} y &= wG_1 - v \\ &= uG_1 + f\tilde{\alpha}_k G_1 - uG_1 - f \\ &= f\tilde{\alpha}_k G_1 - f \\ &= f[\tilde{\alpha}_k G_1 - I]. \end{aligned}$$

Now, let $\delta = \tilde{\alpha}_k G_1 - I$ and δ look random with the random matrix minus the identity matrix. Therefore, we can have the inverse of the matrix, δ, so that f can be retrieved.

$$f = y\,[\delta]^{-1}.$$

Then, we can also computed the secret u.

$$\begin{aligned} u &= w - f\tilde{\alpha}_k \\ &= w - y[\delta]^{-1}\tilde{\alpha}_k. \end{aligned}$$

Since we identified (f, u), we could successfully retrieve the error vector, e. Therefore, RankID is insecure to be used.

4. New Rank AGS Identification Protocol

In this section, we describe our new zero-lnowledge identification protocol, namely the Rank AGS identification protocol. Our technique implements the double circulant structure in the public matrix, G. Our public key is still the same as (G, r, x). Our secret key is (f, e). We modified the secret α that would be sent by the verifier to the prover into $\alpha = \gamma Cir(v)$ where $\gamma \in F_{q^m}$ and $Cir(v)$ is a circulant matrix generated by a vector $v \in F_q^k$.

We introduced a new definition of the product, which is defined below.

Definition 9 (Dot Product,$\cdot$)**.** *Let $e = (e_1||e_2) \in F_{q^m}^{2k}$ where $e_1, e_2 \in F_{q^m}^k$ and let $\alpha \in F_{q^m}^{k \times k}$. We define the product of $e \cdot \alpha$ as follows:*

$$e \cdot \alpha = (e_1\alpha||e_2\alpha).$$

4.1. Key Generation

We used the same notation and the same keys as in the scheme of RankID. Our zero-knowledge protocol uses a public $k \times n$ ($n = 2k$) random double circulant matrix G over F_{q^m}.

4.1.1. Key Generation

Choose k, m, q, and r.

$G \xleftarrow{\$} F_{q^m}^{k \times 2k}$

$e \xleftarrow{\$} F_{q^m}^{2k}$ with $rk(e) = r$.

$f \xleftarrow{\$} F_{q^m}^k$
$x \leftarrow fG \oplus e$
Public Key = $pk \leftarrow (G, r, x)$, Secret Key = $sk \leftarrow (f, e)$.

4.1.2. Rank AGS ID

In our zero-knowledge protocol, to prove its identity, a prover must prove the knowledge of the secret key (e, f) by using two blinding techniques. The first one is to Xor a random vector to the secret key f, and the second blinding technique uses the "$*$" and "$\cdot$" products to multiply the secret e to random values. Moreover, the security of our protocol relies on the hardness of the rank syndrome decoding problem (RSD). We modify the α that has been distributed by the verifier to the prover where $\alpha = \gamma Cir(v)$, where $v \in F_q^k$ and $\gamma \in F_{q^m}$. Notice that the RankID scheme is insecure due to the extra information $uG_1 + f$ sent by the prover to the verifier. As a result, we considered the original AGS scheme in the Hamming metric and constructed the Rank AGS more naturally. Therefore, the key generation and the algorithm of the Rank AGS are still the same except for the commit, $c_1 = h(P||Q)$, and we removed the response $uG_1 \oplus f$ when the challenge $g = 0$ was received. The repaired new scheme is shown in Table 4 below:

Table 4. The identification protocol (Rank AGS).

Prover, P		Verifier, V
$u \in F_{q^m}^k$ $P \in GL_{2k}(F_q)$ $Q \in GL_m(F_q)$		
	$c_1 = h(P\|\|Q)$ $c_2 = h(Q * (uG)P)$ $\longrightarrow$	
	$\alpha \in F_{q^m}^{k \times k}$ $\longleftarrow$	
	$c_3 = h(Q * (uG \oplus (e \cdot \alpha))P)$ $\longrightarrow$	
	$g \in \{0,1\}$ $\longleftarrow$	
if $g = 0$,		
	$u + f\alpha$, $P\|\|Q$ $\longrightarrow$	verify: $c_1 = h(P\|\|Q)$, $c_3 = h(Q * (uG \oplus (e \cdot \alpha))P)$
if $g = 1$,		
	$Q * (uG)P$, $Q * (e \cdot \alpha)P$ $\longrightarrow$	verify: $c_2 = h(Q * (uG)P)$, $c_3 = h(Q * (uG \oplus (e \cdot \alpha))P)$, $rk(Q * (e \cdot \alpha)P) \leq r$

4.1.3. Algorithm of Rank AGS ID

1. A prover $\mathcal{P}$ randomly chooses $u \in F_{q^m}^k$, $P \in GL_{2k}(F_q)$, $Q \in GL_m(F_q)$. Then, $\mathcal{P}$ sends to a verifier $\mathcal{V}$ the commitments c_1 and c_2 such that: $c_1 = h(P||Q)$ and $c_2 = h(Q * (uG)P)$. Here, h is a hash function.
2. A verifier $\mathcal{V}$ sends $\alpha \in F_{q^m}^{k \times k}$ to $\mathcal{P}$.
3. A prover $\mathcal{P}$ builds $c_3 = h(Q * (uG \oplus (e \cdot \alpha))P)$ and sends to $\mathcal{V}$.
4. A verifier $\mathcal{V}$ sends $g \in \{0, 1\}$ to $\mathcal{P}$.
5. Two possibilities:

- If $g = 0$: $\mathcal{P}$ reveals $u + f\alpha$ and $P||Q$.
- If $g = 1$: $\mathcal{P}$ reveals $Q * (uG)P$ and $Q * (e \cdot \alpha)P$.

6. Verification step, two possibilities:
   - If $g = 0$: $\mathcal{V}$ verifies that $c_1 = h(P||Q), c_3 = h(Q * (uG \oplus (e \cdot \alpha))P)$ have been honestly computed;
   - If $g = 1$: $\mathcal{V}$ verifies that $c_2 = h(Q * (uG)P), c_3 = h(Q * (uG \oplus (e \cdot \alpha))P)$ have been honestly computed and $rk(Q * (e \cdot \alpha)P) \leq r$.

Now, we provide a simple toy example of the Rank AGS scheme as in Table 5 below. Let $q = 2$, $k = 4$, $m = 3$. Let z be the primitive element in F_{2^3} and $1, z, z^2$ be the basis of F_{2^3} over F_2.

Private key: $e = (1, z, z^2, z||z, z^2, z, z^2)$ with $e \in F_{2^3}^8$ with $rk(e) = 3$ and $f = (1, z, z, z^2)$ with $f \in F_{2^3}^4$.

Public key: $G = \begin{pmatrix} 1 & z & z & z^2 & z & 1 & z^2 & z \\ z^2 & 1 & z & z & z & z & 1 & z^2 \\ z & z^2 & 1 & z & z^2 & z & z & 1 \\ z & z & z^2 & 1 & 1 & z^2 & z & z \end{pmatrix}$ with $G \in F_{2^3}^{4\times 8}$, $r = 3$ and $x = fG \oplus e = (1 + z + z^2, z, z, z, z + z^2, 1 + z + z^2, z + z^2, z^2)$.

Table 5. Example of identification protocol (Rank AGS).

Prover, P		Verifier, V
$u = (1, z, z^2, z) \in F_{2^3}^4$ $P \in GL_8(F_2)$ $P = \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 1&0&0&1&0&1&0&0 \\ 1&1&1&1&0&1&0&1 \\ 1&0&1&0&0&1&1&0 \\ 1&0&0&1&1&1&0&0 \\ 1&1&0&1&1&1&0&0 \\ 0&1&0&0&0&0&1&1 \\ 0&1&1&1&0&0&1&1 \end{pmatrix}$ $Q = \begin{pmatrix} 1&0&1 \\ 0&1&0 \\ 1&0&0 \end{pmatrix} \in GL_3(F_2)$		
	$c_1 = h(P\|\|Q)$ $= 10101011100011100011000001$ $c_2 = h(Q * (uG)P)$ $= 11010000100111010011111101$	
	$\longrightarrow$	
	$\alpha = \begin{pmatrix} 1&0&1&0 \\ 0&1&0&1 \\ 1&0&1&0 \\ 0&1&0&1 \end{pmatrix} \in F_{2^3}^{4\times 4}$	
	$\longleftarrow$	
	$c_3 = h(Q * (uG \oplus (e \cdot \alpha))P)$ $= 10101010110110010010011011$	
	$\longrightarrow$	
	$g \in \{0, 1\}$	
	$\longleftarrow$	

Table 5. *Cont.*

if $g = 0$,	$\xrightarrow{\substack{u + f\alpha \\ = (z, z^2, 1 + z + z^2, z^2), \\ P\|\|Q}}$	Assume can be verified as we can receive back: $c_1 = h(P\|\|Q) = 10101011100011100011000001$, $c_3 = h(Q * (uG \oplus (e \cdot \alpha))P) = 10101010110110010010011011$
if $g = 1$,	$\xrightarrow{\substack{Q * (uG)P = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \\ Q * (e \cdot \alpha)P = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}}$	Assume can be verified as we can receive back: $c_2 = h(Q * (uG)P) = 11010000100111010011111101$, $c_3 = h(Q * (uG \oplus (e \cdot \alpha))P) = 10101010110110010010011011$, $rk(Q * (e \cdot \alpha)P) = 2 \leq 3$

From the above Rank AGS example, we were able to prove that our Rank AGS scheme works efficiently.

5. Properties and Security of the Rank AGS ID

In this section, we prove the ZK security of our scheme by using the usual zero-knowledge arguments and also consider security properties such as completeness, zero knowledge, and soundness. We also showed that this protocol is zero-knowledge with a cheating probability of around $\frac{1}{2}$.

5.1. Completeness

We obtained the completeness of Rank AGS that has been described in (Table 4) by showing that if an honest prover $\mathcal{P}$ and an honest verifier $\mathcal{V}$ execute our protocol, it always succeeds.

Theorem 1. *If a prover and a verifier honestly execute Rank AGS, we have for any round*

$$Pr[RankAGSId_{P,V} = Accept] = 1.$$

Proof. $\mathcal{P}$ and $\mathcal{V}$ are supposed to be honest. We can verify c_3 in the case that $g = 0$, $\mathcal{V}$ can compute:

$$\begin{aligned}
(u \oplus f\alpha)G \oplus x \cdot \alpha &= uG \oplus f\alpha G \oplus (fG \oplus e) \cdot \alpha \\
&= uG \oplus f\alpha G \oplus fG \cdot \alpha \oplus e \cdot \alpha \\
&= uG \oplus f\alpha G \oplus (f||fG_1) \cdot \alpha \oplus e \cdot \alpha \\
&= uG \oplus f\alpha G \oplus (f\alpha||fG_1\alpha) \oplus e \cdot \alpha \\
&= uG \oplus f\alpha G \oplus (f\alpha||f\alpha G_1) \oplus e \cdot \alpha \\
&= uG \oplus f\alpha G \oplus f\alpha G \oplus e \cdot \alpha \\
&= uG \oplus e \cdot \alpha.
\end{aligned}$$

□

In the case $g = 1$, we can check that $rk(Q * (e \cdot \alpha)P) = r$. The proof is as below when we consider $rk(e \cdot \alpha) = rk(e)$.

Proof. Let $(\beta_1, \cdots, \beta_m)$ be the basis for F_{q^m}. Let M_{e_1} and M_{e_2} be the support matrices for e_1 and e_2 respectively.

$$\begin{aligned} e \cdot \alpha &= e_1\gamma Cir(v)||e_2\gamma Cir(v) \\ &= (\beta_1, \cdots, \beta_n)M_{e_1}\gamma Cir(v)||(\beta_1, \cdots, \beta_n)M_{e_2}\gamma Cir(v) \\ &= \gamma(\beta_1, \cdots, \beta_n)M_{e_1}Cir(v)||\gamma(\beta_1, \cdots, \beta_n)M_{e_2}Cir(v). \end{aligned}$$

Now, we can determine $rk(e \cdot \alpha)$. Let $M_1' = M_{e_1}Cir(v)$ and $M_2' = M_{e_2}Cir(v)$.

$$\begin{aligned} rk(e \cdot \alpha) &= rk(M_1'||M_2') \\ &= rk(M_{e_1}Cir(v)||M_{e_2}Cir(v)) \\ &= rk([M_{e_1}||M_{e_2}]\begin{pmatrix} Cir(v) & 0 \\ 0 & Cir(v) \end{pmatrix}) \\ &\leq \min\left\{ rk(M_{e_1}||M_{e_2}),\ rk\begin{pmatrix} Cir(v) & 0 \\ 0 & Cir(v) \end{pmatrix} \right\} \\ &\leq rk(M_{e_1}||M_{e_2}) \\ &\leq rk(e) = r. \end{aligned}$$

□

Therefore, $rk(Q * (e \cdot \alpha)P) \leq r$. The verifier, $\mathcal{V}$ can execute the protocol correctly.

5.2. Zero Knowledge

We used the classical idea of simulation as presented in [22] to ensure zero knowledge. We need to prove that no information can be deduced in polynomial time from the execution of the Rank AGS protocol.

Theorem 2. *The protocol defined in (Table 4) is a prover-verifier zero-knowledge protocol.*

Proof. Let S and δ be a simulator using a dishonest verifier and the number of rounds that are taken by an honest identification process to be executed, respectively. We needed to construct a polynomial-time simulator S of the protocol that, by interacting with the verifier V, could provide a transcript indistinguishable from the original protocol. The simulator S should perform the following steps:

If $g = 0$:

S randomly chooses $u' \in F_{q^m}^k$, $P' \in F_q^{2k \times 2k}$ and $Q' \in F_q^{m \times m}$ and solves the equation $x = fG \oplus e$ without necessarily satisfying the condition $rk(e) = r$. Then, the computed $c_1 = h(P'||Q')$ and c_2 is taken as a random value. S simulates the verifier by applying (c_1, c_2) to obtain $\alpha \in F_{q^m}^{k \times k}$. Then, S can compute $c_3 = h(Q' * (u'G \oplus (e \cdot \alpha))P')$. Note that P', Q', and u' are indistinguishable from P, Q, and $u + f\alpha$.

If $g = 1$:

S randomly chooses $u' \in F_{q^m}^k$, $P' \in F_q^{2k \times 2k}$ and $Q' \in F_q^{m \times m}$. Now, he randomly chooses $f' \in F_{q^m}^k$ and $e' \in F_{q^m}^{2k}$ such that $rk(e') = r$. Then, he computes $c_2 = h(Q' * (u'G)P')$ and c_1 is taken as a random value. S simulates the verifier by applying (c_1, c_2) to obtain $\alpha \in F_{q^m}^{k \times k}$ and then S can compute $c_3 = h(Q' * (u'G \oplus (e' \cdot \alpha))P')$. Note that P', Q', u', f' and e' are indistinguishable from $Q^*(uG)P$ and $Q * (e \cdot \alpha)P$. □

Therefore, S generates a communication transcript that is indistinguishable from another communication transcript which exactly looks similar to an honest identification process execution in 2δ rounds.

5.3. Soundness

The soundness of our scheme can be proven by starting to show that for each round, a dishonest prover can cheat with a probability that does not exceed $\frac{q^{m+k}-q^m-q^k+2}{2(q^{m+k}-q^m-q^k+1)}$. The finite field used is F_{q^m}.

St_1: He or she randomly chooses u', P', Q', and solves the equation $x = f'G \oplus e'$ without necessary satisfying the condition $rk(e') = r$ where $f' \in F_{q^m}^k$ and $e' \in F_{q^m}^{2k}$ when receiving $g = 0$ as a challenge. Then, he or she computes $c_1 = h(P'||Q')$ and sets c_2 at random data. Thus, the dishonest prover is able to answer the challenge $g = 0$ regardless of the value of α chosen by the verifier.

St_2: He or she randomly chooses u', P', Q', and generates the couple (f', e') randomly such that $rk(e') = r$ when receiving $g = 1$ as a challenge. Then, he or she can compute $c_2 = h(Q' * (u'G)P')$ and set c_1 at random data. In this case, the rank of e' is valid. Thus, the dishonest prover can correctly answer the challenge $g = 1$ regardless of the value of α.

By trying to guess α, the above two strategies can be improved. Let α' be the guessed value of α. Thus, the dishonest prover can compute $h(x)$ where $x = Q * (uG \oplus (e \cdot \alpha'))P$.

Since there are only two strategies (St_1, St_2), we have $P(St = St_i) = \frac{1}{2}$. Next, we only have two possibilities of being challenged which are $g \in 0, 1$. Therefore, $P(g = i) = \frac{1}{2}$. Meanwhile, the probability of guessing the correct value of α depends on its size. We know that $\alpha = \gamma Cir(v)$ where $\gamma \in F_{q^m}$ and $v \in F_q^k$. Thus, excluding 0, the size of α is $(q^m - 1)(q^k - 1)$ and the probability of guessing the correct α is $\frac{1}{(q^m-1)(q^k-1)}$.

Therefore, the success cheating probability of a strategy for one round is given by:

$$\begin{aligned}
P &= \sum_{i=0}^{1} P(St = St_i)P(b = i) + P(St = St_i)P(b = 1 - i)P(\alpha = v') \\
&= P(St = St_0)P(b = 0) + P(St = St_0)P(b = 1)P(\alpha = v') \\
&\quad + P(St = St_1)P(b = 1) + P(St = St_1)P(b = 0)P(\alpha = v') \\
&= (\frac{1}{2})(\frac{1}{2}) + (\frac{1}{2})(\frac{1}{2})(\frac{1}{q^{m+k} - q^m - q^k + 1}) \\
&\quad + (\frac{1}{2})(\frac{1}{2}) + (\frac{1}{2})(\frac{1}{2})(\frac{1}{q^{m+k} - q^m - q^k + 1}) \\
&= (\frac{1}{4}) + (\frac{1}{4})(\frac{1}{q^{m+k} - q^m - q^k + 1}) + (\frac{1}{4}) \\
&\quad + (\frac{1}{4})(\frac{1}{q^{m+k} - q^m - q^k + 1}) \\
&= \frac{1}{2} + (\frac{1}{2(q^{m+k} - q^m - q^k + 1)}) \\
&= \frac{q^{m+k} - q^m - q^k + 2}{2(q^{m+k} - q^m - q^k + 1)}.
\end{aligned}$$

If a dishonest prover succeeds in cheating with a probability higher than $\left(\frac{q^{m+k}-q^m-q^k+2}{2(q^{m+k}-q^m-q^k+1)}\right)^{\delta}$ where δ is the number of rounds, then he or she can solve the rank syndrome decoding problem (RSD).

5.4. Rank AGS Signature Scheme

After this, we investigated the signature scheme based on the Rank AGS ID. As mentioned in the introduction, the Fiat–Shamir transform [23] can turn any zero-knowledge identification scheme into a signature scheme by considering the cryptographic hash functions known as the commit-and-challenge approach. The key generation of our signature scheme is the same as in Rank AGS ID. Now, we present the Rank AGS signing and verification algorithm as shown in the following Algorithms 1 and 2 respectively.

Algorithm 1 rank AGS signing algorithm

Input: msg, message, δ, number of rounds, sk=(f,e)$\leftarrow KGen$, pk=(G,r,x)$\leftarrow KGen$.
Output: Sign(sk,pk,msg,δ)

Step 1:
for $i = 1$ to δ **do**
  $u_i \in F_{q^m}^k$
  $P_i \in F_q^{2k\times 2k}$
  $Q_i \in F_q^{m\times m}$
  $c_{i,0} \leftarrow h(P_i||Q_i)$
  $c_{i,1} \leftarrow h(Q_i * (u_i G)P_i)$
end for
$cmt_0 \leftarrow c_{1,0}||c_{1,1}||\cdots||c_{\delta,0}||c_{\delta,1}$
Step 2:
$ch_1 \leftarrow h(cmt_0||msg)$
Step 3:
for $i = 1$ to δ **do**
  $\gamma_i = (ch_{1,(i-1)m+(i-1)k+1}, \cdots, ch_{1,im+(i-1)k})$
  $v_i = (ch_{1,im+(i-1)k+1}, \cdots, ch_{1,im+ik})$
  $\alpha_i = \gamma_i Cir(v_i)$
  $cmt_{1,i} \leftarrow h(Q_i * (u_i G \oplus (e \cdot \alpha_i))P_i)$
end for
Step 4:
$ch_2 \leftarrow h((cmt_1||1)||\cdots||(cmt_1||\ell))$
Step 5:
for $i = 1$ to δ **do**
  if $ch_{2,i} = 0$, **then**
    $rsp_i \leftarrow [u_i + f_i\alpha_i, (P_i||Q_i)]$
  end if
  if $ch_{2,i} = 1$, **then**
    $rsp_i \leftarrow [(Q_i * (u_i G)P_i), (Q_i * (e \cdot \alpha_i)P_i)]$
  end if
end for
sgn$\leftarrow [cmt_0, ch_1, cmt_1, ch_2, rsp]$
return sgn

Impersonation attack. An attacker executes the Rank AGS with a prover, $\mathcal{P}$, and tries to give answers that the verifier, $\mathcal{V}$, will accept. It is impossible to give commitments that can be opened for two values of g. Without the knowledge of the secret key, e, the probability of success is at most $Pr_{imp} = \frac{1}{2}$.

5.5. Key Size and Signature Size

Here, we report the key and signature bit size for our Rank AGS ID and Rank AGS Signature scheme, respectively. First, we investigate the key size that we need for Rank AGS ID.

1. Our public keys are (G, x, r). $G \in F_{q^m}^{k \times 2k}$ is a systematic double circulant matrix, which requires only a vector to represent it, $2km\,log_2(q)$. $x \in F_{q^m}^{2k}$ has a size of $km\,log_2(q)$. Therefore, the public key size is $3km\,log_2(q)$.
2. The secret keys are (f, e) where $f \in F_{q^m}^{k}$ and $e \in F_{q^m}^{2k}$. If we have f, then we can compute e from $e = x + fG$. Therefore, it suffices for us to store only f as a secret key, which contributes to $km\,log_2(q)$.
3. Based on the Rank AGS signature scheme, we can construct the signature size of our signature scheme. The signature consists of two commitments which are cmt_0 and $cmt_{1,i}$, and have a total length of $3h\delta$. Then, the challenge, ch_1 is having size of $\delta(k+m)log_2(q)$ and ch_2 is having size of δ. The total size of the response, rsp_i for the commit-challenge, is based on the value of the challenge, which is 0 or 1. The size of rsp_i is $\frac{1}{2}\delta(5km + 4k^2 + m^2)log_2(q)$. The signature size is based on the total size of the commitment, challenge, and response which is $3h\delta + \delta + \delta(k+m)log_2(q) + \frac{1}{2}\delta(5km + 4k^2 + m^2)log_2(q)$.

Algorithm 2 rank AGS verification algorithm

Input: msg, message, δ, number of rounds, $sgn = [cmt_0, ch_1, cmt_1, ch_2, rsp]$, pk=(G,r,x)$\leftarrow KGen$.
Output: Verify(pk,msg,δ,sgn)

for $i = 1$ to δ **do**
  $\gamma_i = (ch_{1,(i-1)m+(i-1)k+1}, \cdots, ch_{1,im+(i-1)k})$
  $v_i = (ch_{1,im+(i-1)k+1}, \cdots, ch_{1,im+ik})$
  $\alpha_i = \gamma_i Cir(v_i)$
  if $ch_{2,i} = 0$ **then**
    $c_{i,0} \leftarrow cmt_{0,2h(i-1)+1}, \cdots, cmt_{0,2h(i-1)+h}$
    if $c_{i,0} \neq h(rsp_{i,2}) \vee$ **then**
      $cmt_{1,i} \neq h(rsp_{i,2(2)} * (rsp_{i,1}G \oplus (x \cdot \alpha_i))rsp_{i,2(1)})$
      return false
    end if
  end if
  if $ch_{2,i} = 1$, **then**
    $c_{i,1} \leftarrow cmt_{0,(2h(i-1)+h)+1}, \cdots, cmt_{0,2hi}$
    if $c_{i,1} \neq h(rsp_{i,1}) \vee cmt_{1,i} \neq h(rsp_{i,1} \oplus rsp_{i,2}) \vee rk(rsp_{i,2}) \neq r$ **then**
      return false
    end if
  end if
end for
return true

Now, we provide the parameter sets achieving 128-bit and 256-bit security levels as shown in Table 6. These security levels are computed based on the complexity of existing known combinatorial and algebraic attacks on the RSD problem. We set $q = 2$, m to be a prime number, and $n = 2k$. The number of rounds needed to decrease the impersonation probability to our needs. Therefore, we fixed the number of rounds, $\delta = 129$ and $\delta = 257$ to reach the desired impersonation probability (2^{-129} and 2^{-257}) to achieve the security level of 128-bits and 256-bits respectively. The hash value, h, is the same as the δ value according to the Rank AGS signature scheme.

We could achieve the desired security level to solve the rank syndrome decoding problem (RSD) based on the sets of small parameters.

Then, we looked at the key and signature bit sizes for other signature schemes, which are based on rank metrics such as Rank CVE [8] and the double circulant version of Veron (Rank RVDC) [10] identification schemes. Then, we compared the size of public, secret, and signature keys with our Rank AGS as shown in Tables 7 and 8.

Table 6. Public, secret keys and signature bit sizes for 128-bit and 256-bit security levels.

Parameters $(q, m, n, k, r, \delta, h)$	Security Level	Signature Size	Secret Key	Public Key
$(2, 43, 38, 19, 8, 129, 129)$	128 bit	533,931	817	2451
$(2, 37, 34, 17, 8, 129, 129)$	128 bit	422,733	629	1887
$(2, 47, 46, 23, 11, 257, 257)$	256 bit	1,466,699	1081	3243
$(2, 53, 46, 23, 11, 257, 257)$	256 bit	1,634,006	1219	3657

Table 7. Comparison of keys and signature bit sizes with CVE and RVDC schemes for 128 security level.

Scheme	Parameters $(q, m, n, k, r, \delta, h)$	Signature Size	Secret Key	Public Key
Rank CVE	$(2, 43, 38, 19, 8, 128, 256)$	3,313,662	1258	33,969
Rank RVDC	$(2, 43, 38, 19, 8, 129, 256)$	574,953	2451	2454
Rank AGS	$(2, 43, 38, 19, 8, 129, 129)$	533,931	817	2451

Table 8. Comparison of keys and signature bit sizes with CVE and RVDC schemes for 256 security level.

Scheme	Parameters $(q, m, n, k, r, \delta, h)$	Signature Size	Secret Key	Public Key
Rank CVE	$(2, 47, 46, 23, 11, 256, 512)$	14,161,547	2162	75,673
Rank RVDC	$(2, 47, 46, 23, 11, 257, 512)$	1,645,057	3243	3247
Rank AGS	$(2, 47, 46, 23, 11, 257, 257)$	1,466,699	1081	3243

Based on the comparison above, we could observe that all our public, secret key size, and signature sizes were smaller than other schemes. The percentage of the size reduction in the keys or signature is given below in Tables 9 and 10 as we consider Rank CVE as the original reference for 128 and 256 security levels.

Table 9. Percentage of size reduction as we consider Rank CVE as the original reference for the 128 security level.

Scheme	Percentage (%)		
	Signature Size	Secret Key	Public Key
Rank RVDC	83	−95	93
Rank AGS	84	35	93

We used the notation of "- %" to indicate that the key size was, in fact, larger than the ones in Rank CVE. In particular, rank RVDC had a larger secret key size compared to Rank CVE. Moreover, Rank AGS reduces drastically in the size of the signature, public key, and secret key compared to Rank CVE.

Table 10. Percentage of size reduction as we consider Rank CVE as the original reference for the 256 security level.

Scheme	Percentage (%)		
	Signature Size	**Secret Key**	**Public Key**
Rank RVDC	88	−50	96
Rank AGS	90	50	96

6. Conclusions

In this paper, we studied and identified the errors in RankID [11]. The operations chosen in the RankID construction did not ensure the commutativity of the matrix multiplication and preserved the rank of the error vector. Furthermore, even if we assume that RankID is correct, it is still insecure because the secret key can be recovered. Therefore, we propose a new scheme: Rank AGS ID based on the hardness of the rank syndrome decoding problem (RSD) by considering the original AGS ID in hamming metric. We provided the correctness of our Rank AGS ID and proved that the rank of the error vector was preserved. Our scheme also achieved zero-knowledge security properties such as completeness, soundness, and zero knowledge. Finally, we showed how that our scheme has a smaller public, secret, and signature key size when compared with other identification schemes=-based signatures, such as Rank CVE and Rank RVDC, for 128-bit and 256-bit security levels.

Author Contributions: Conceptualization and Methodology, T.S.C.L., V.N. and N.N.H.A.; Formal analysis, V.N., T.S.C.L., N.N.H.A., M.R.K.A., J.-J.C., T.T.V.Y. and S.-C.Y.; Funding acquisition, T.S.C.L., J.-J.C., T.T.V.Y., and S.-C.Y.; Investigation, T.S.C.L., V.N., N.N.H.A. and M.R.K.A.; Writing-original draft preparation, V.N.; Writing-review and editing, T.S.C.L., M.R.K.A., J.-J.C., T.T.V.Y. and S.-C.Y.; Supervision, T.S.C.L. and M.R.K.A.; Validation, M.R.K.A., T.S.C.L. and J.-J.C.; Project administration, M.R.K.A. All authors have read and agreed to the published version of the manuscript.

Funding: The research was supported by the Ministry of Higher Education of Malaysia's FRGS (FRGS/1/2019/ICT04/MMU/02/5) and the MMU Postdoc (MMUI/220141).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This paper and the research behind it would not have been possible without the exceptional support from the Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia (UPM) in allowing this research to be conducted. We also extend our endless gratitude to the MYBRAINSC scholarship scheme from the Ministry of Higher Education of Malaysia. Finally, the authors sincerely appreciate the editor and anonymous referees for their careful reading and helpful comments to improve this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bufalo, M.; Bufalo, D.; Orlando, G. A note on the computation of the modular inverse for cryptography. *Axioms* **2021**, *10*, 116. [CrossRef]
2. Zhang, Y. Bounded gaps between primes. *Ann. Math.* **2014**, *179*, 1121–1174. [CrossRef]
3. McEliece, R.J. A public-key cryptosystem based on algebraic. *Coding Thv* **1978**, *4244*, 114–116.
4. Courtois, N.T.; Finiasz, M.; Sendrier, N. How to achieve a McEliece-based digital signature scheme. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 9–13 December 2001; pp. 157–174.
5. Stern, J. Designing Identification schemes with keys of short size. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 21–25 August 1994; pp. 164–173.

6. Véron, P. Improved Identification schemes based on error-correcting codes. *Appl. Algebra Eng. Commun. Comput.* **1997**, *8*, 57–69. [CrossRef]
7. Aguilar, C.; Gaborit, P.; Schrek, J. A new zero-knowledge code based Identification scheme with reduced communication. In Proceedings of the IEEE Information Theory Workshop, Paraty, Brazil, 16–20 October 2011; pp. 648–652.
8. Bellini, E.; Caullery, F.; Hasikos, A.; Manzano, M.; Mateu, V. Code-based signature schemes from Identification Protocols in the rank metric. In *Cryptology and Network Security. CANS 2018*; Springer: Cham, Switzerland, 2018; pp. 277–298.
9. Lau, T.S.C.; Tan, C.H.; Prabowo, T.F. Key recovery attacks on some rank metric code-based signatures. In Proceedings of the IMA International Conference on Cryptography and Coding, Oxford, UK, 16–18 December 2019; pp. 215–235.
10. Bellini, E.; Caullery, F.; Gaborit, P.;Manzano, M.; Mateu, V. Improved Veron Identification and signature schemes in the rank metric. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; pp. 1872–1876.
11. Ayebie, E.B.; Assidi, H.; Souidi, E.M. An efficient Identification scheme based on rank metric. In Proceedings of the International Symposium on Foundations and Practice of Security, Toulouse, France, 5–7 November 2019; pp. 273–289.
12. Gaborit, P.; Zémor, G. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Trans. Inf. Theory* **2016**, *62*, 7245–7252. [CrossRef]
13. Lau, T.S.C.; Tan, C.H. MURAVE: A new rank code-based signature with multiple rank verification. In Proceedings of the Code-Based Cryptography Workshop, Zagreb, Croatia, 9–10 May 2020; pp. 94–116.
14. Chabaud, F.; Stern, J. The cryptographic security of the syndrome decoding problem for rank distance codes. In *Advances in Cryptology—ASIACRYPT '96*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 368–381.
15. Gaborit, P.; Ruatta, O.; Schrek, J. On the complexity of the rank syndrome decoding problem. *IEEE Trans. Inf. Theory* **2016**, *62*, 106–109. [CrossRef]
16. Ourivski, A.V.; Johansson, T. New technique for decoding codes in the rank metric and its cryptography applications. *Probl. Inf. Transm.* **2002**, *38*, 237–246. [CrossRef]
17. Aragon, A.; Gaborit, P.; Hauteville, A.; Tillich, J.-P. A new algorithm for solving the rank syndrome decoding problem. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; pp. 2421–2425.
18. Faugere, J.-C.; Levy-dit-Vehel, F.; Perret, L. Cryptanalysis of Minrank. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2008; pp. 280–296.
19. Goubin, L.; Courtois, N.T. Cryptanalysis of the TTM cryptosystem. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, 3–7 December 2000; pp. 44–57.
20. Bardet, M.; Briaud, P.; Bros, M.; Gaborit, P.; Neiger, V.; Ruatta, O.; Tillich, J.-P. An algebraic attack on rank metric code-based cryptosystems. In Proceedings of the In Advances in Cryptology (EUROCRYPT 2020), Zagreb, Croatia, 10–14 May 2020; pp. 64–93.
21. Bardet, M.; Bros, M.; Cabarcas, D.; Gaborit, P.; Perlner, R.; Smith-Tone, D.; Tillich, J.-P.; Verbel, J. Algebraic Attacks for Solving the Rank Decoding and MinRank Problems without Gröbner Basis. 2020. Available online: https://hal.inria.fr/hal-03133479 (accessed on 6 February 2021).
22. Goldreich, O. Zero-knowledge twenty years after its invention. *IACR Cryptol. EPrint Arch.* **2002**, *2002*, 186.
23. Fiat, A.; Shamir, A. How to prove yourself: Practical solutions to Identification and signature problems. In *Advances in Cryptology—CRYPTO '86*; Springer: Berlin/Heidelberg, Germany, 1986; pp. 186–194.