An argument for rank metric

Vadym Fedyukovych

August 16, 2008

Abstract

A protocol is introduced to show an upper bound for rank of a square matrix.

1 Introduction

Prover shows his knowledge of matrix elements committed, as well as a statement regarding the matrix with a protocol introduced in this report. He shows that rank of the matrix is at most a threshold with responses of a variant of Schnorr protocol [Oka92, Sch89]. Condition tested is root multiplicity of characteristic function of another matrix with elements that are Prover responses. Responses are validated with commitments to matrix elements. Pedersen commitment scheme [Ped91] is used with this protocol.

An upper bound for error in a damaged codeword of Goppa code (in Hamming metric) can be shown with a related protocol [Fed08]. Set approximate matching can be shown with another related protocol [Fed07].

2 Preliminaries

Let F_q be a finite field with q elements. Let $\mathbb{E} = \{e_{ij}\}$ be a square matrix of size n with elements from $\mathbb{F}_q$, and let $\Lambda = \{\lambda_{ij}\}$ be an identity matrix: $\lambda_{ii} = 1, \lambda_{ij} = 0, j \neq i$. Notation $|\mathbb{E}|$ is used for matrix determinant.

Definition 1. *Matrix characteristic function* is a mapping from all square matrices to the ring of polynomials:

$$f(x; \mathbb{E}) = |x\Lambda - \mathbb{E}| \tag{1}$$

Commitment scheme it a tuple of algorithms $Gen(), Commit(), Open()$ such that *binding* and *hiding* holds. With *homomorphic commitment scheme* one can open a linear combination of values committed. Some commitment schemes also have protocols to show knowledge of values committed. Pedersen commitment scheme is computationally binding and unconditionally hiding, is additively homomorphic, and have an argument of knowledge protocol.

Interactive protocol is an interactive pair of algorithms such that *completeness* and *soundness* holds. Soundness is unconditional for a proof, and depends on hardness of a problem for an argument. *Extractor algorithm* exists for some protocols that can produce auxiliary input of Prover machine from Prover responses given oracle access to Prover. A protocol with an extractor is *of knowledge*. *Simulator algorithm* exists for some protocols that produces simulated transcript indistinguishable from protocol transcript with a Prover. A protocol with a simulator is *zero knowledge*. A protocol with a simulator producing transcripts indistinguishable from all protocol transcripts with the same challenges is *honest verifier zero knowledge*.

Schwartz-Zippel lemma [Sch80] is the core of our verification technique and soundness proof.

3 Protocol

Lemma 1. *For a square matrix $\mathbb{E}$ of rank k and size n*

$$f(x; \mathbb{E}) = x^{n-k} f_k(x) \tag{2}$$

where $f_k(x)$ is a monic polynomial of power k.

We show $x^{-(n-T)} f(x; \mathbb{E})$ is a polynomial with a protocol introduced in this report such that $rank(\mathbb{E}) \leq T$.

Let $\{W_{ij}\}$ be a set of commitments, and $\{R_{ij}\}$ be a set of responses of Chaum-Pedersen protocol with a challenge $c \in \mathbb{F}_q$:

$$W_{ij} = g^{e_{ij}} h^{\zeta_{ij}} \tag{3}$$

$$R_{ij} = r_{ij}(c), \qquad r_{ij}(y) = y e_{ij} + \alpha_{ij} \tag{4}$$

Consider a matrix of polynomials: $\mathbb{B}(y) = \{r_{ij}(y)\}$. It is clear that

$$f(xy; \mathbb{B}(y)) = \sum_{l=0}^{n} a_l(x) y^l, \qquad a_n(x) \equiv f(x; \mathbb{E}) \tag{5}$$

Verifier tests that

$$f(xy; \mathbb{B}(y)) \equiv y^n x^{n-T} \sum_{s=0}^{T} x^s b_s + \sum_{l=0}^{n-1} a_l(x) y^l$$

for $x = d$ and $y = c$ chosen at random, and for some $\{a_l(x)\}$, $\{b_s\}$. Protocol is shown on Figure 1.

Lemma 2 (Soundness). *Probability for a honest Verifier to accept while running protocol shown on Figure 1 for any polynomial Prover and any matrix $\mathbb{E}$ of rank more than T is at most $\frac{2n}{q}$.*

Proof. (Concise) Any Prover producing a pair of responses R_{ij}, Θ_{ij} other than estimates of linear polynomials

$$f_R(y) = ye_{ij} + \alpha_{ij}, \qquad f_\Theta(y) = y\zeta_{ij} + \beta_{ij} \tag{6}$$

at $y = c$ that fit (16) for some $\alpha_{ij}, \beta_{ij}, \zeta_{ij}$

$$R_{ij} \neq f_R(c), \qquad \Theta_{ij} \neq f_\Theta(c) \tag{7}$$

will also produce a solution to DL problem:

$$log_h(g) = -\frac{R_{ij} - f_R(c)}{\Theta_{ij} - f_\Theta(c)} \tag{8}$$

In the following we consider all responses R_{ij} to be estimates of polynomials linear in challenge. Any Prover running protocol shown on Figure 1 with any square matrix of rank more than T will result in estimating a non-zero polynomial

$$F(y, x) = -f(xy; \mathbb{B}(y)) + y^n x^{n-T} \sum_{s=0}^{T} x^s b_s + \sum_{l=0}^{n-1} a_l(x) y^l \tag{9}$$

It can be shown there is at most $\frac{2n}{q}$ probability for a honest Verifier to choose roots of (9) at random. For all other cases it follows that either $F(y, x) \equiv 0$ holds, or Prover can get $log_h(g)$ from his responses. From $F(y, x) \equiv 0$ it follows (2) holds such that rank of the matrix is at most T. □

Lemma 3 (Zero knowledge). *Protocol shown of Figure 1 is honest verifier zero knowledge.*

Proof. Simulator algorithm is shown of Figure 2. It is clear A has flat distribution over group, and A has flat distribution over $\mathbb{F}_q$, such that simulated transcript is identical to any protocol transcript with a Prover with the same challenges c, d. □

4 Discussion

Protocol introduced may be useful with rank codes [Gab85, GL08]. Namely, an error in a corrupted codeword may be shown to be of a low enough weight, without disclosure of the codeword and the weight, and in zero knowledge. To show a statement regarding rank of a non-square matrix, Prover introduces additional rows chosen by Verifier at random to produce a square matrix.

References

[Fed07] Vadym Fedyukovych. A signature scheme with approximate key matching (in Russian). In *Information Security conference, Kiev*, 2007. Presentation available.

[Fed08] Vadym Fedyukovych. Argument of knowledge of a bounded error. In *(submitted)*, 2008. Presentation available.

[Gab85] Ernst M. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–12, 1985.

[GL08] Ernst M. Gabidulin and Pierre Loidreau. Properties of subspace subcodes of optimum codes in rank metric. *AMC*, 2(2):147–157, 2008.

[Oka92] Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *CRYPTO*, pages 31–53, 1992.

[Ped91] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *CRYPTO*, pages 129–140, 1991.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[Sch89] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In *CRYPTO*, pages 239–252, 1989.

Common input is group elements, commitments and a threshold: $g, h \in \mathbb{G}$, $\{W_{ij}\} \subset \mathbb{G}$, $T \in N$.
Auxiliary input of Prover is a square matrix committed: $\mathbb{E} = \{e_{ij}\}$, $\{\zeta_{ij}\}$ such that $W_{ij} = g^{e_{ij}} h^{\zeta_{ij}}$.
Prover shows $rank(\mathbb{E}) \leq T$ as follows:

1. Prover produces $\{b_s\}$, chooses $\{\gamma_s\}$ at random, produces and sends $\{B_s\}$:
$$|x\Lambda - \mathbb{E}| = x^{n-T} \sum_{s=0}^{T} b_s x^s, \qquad B_s = g^{b_s} h^{\gamma_s} \tag{10}$$
2. Verifier chooses at random and sends $d \in \mathbb{F}_q$
3. Prover chooses $\{\alpha_{ij}\}$, $\{\beta_{ij}\}$, $\{\delta_l\}$ at random from $\mathbb{F}_q$, produces $\{a_l\}$, produces and sends $\{Q_{ij}\}$, $\{A_l\}$:
$$Q_{ij} = g^{\alpha_{ij}} h^{\beta_{ij}} \quad i, j \in [1 \dots n] \tag{11}$$
$$|dy\Lambda - \mathbb{B}(y)| = \sum_{l=0}^{n} a_l y^l, \qquad A_l = g^{a_l} h^{\delta_l} \quad l \in [1 \dots n-1] \tag{12}$$
4. Verifier chooses at random and sends $c \in \mathbb{F}_q$
5. Prover produces responses
$$R_{ij} = ce_{ij} + \alpha_{ij}, \qquad \Theta_{ij} = c\zeta_{ij} + \beta_{ij} \tag{13}$$
$$\Psi = c^n d^{n-T} \sum_{s=0}^{T} \gamma_s d^s + \sum_{l=0}^{n-1} \delta_l c^l \tag{14}$$
6. Verifier produces
$$\mathbb{B}(c) = \{R_{ij}\}, \qquad f_B = \left|dc\lambda_{ij} - \mathbb{B}(c)\right| \tag{15}$$
   Verifier accepts if
$$g^{R_{ij}} h^{\Theta_{ij}} W_{ij}^{-c} = Q_{ij} \tag{16}$$
$$g^{-f_B} h^{-\Psi} \left(\prod_{s=0}^{T} B_s^{d^s} \right)^{c^n d^{n-T}} \prod_{l=0}^{n-1} A_l^{c^l} = 1 \tag{17}$$

Figure 1: Protocol for matrix rank upper bound

1. Verifier chooses

$$\{R_{ij}\}, \{\Theta_{ij}\}, \Psi \qquad i, j \in [1 \dots n] \tag{18}$$

at random from $\mathbb{F}_q$.

2. Verifier chooses

$$\{A_l\}, \{B_s\} \qquad l \in [1 \dots n-1] \quad s \in [0 \dots T] \tag{19}$$

at random from $\mathbb{G}$.

3. Verifier produces

$$\mathbb{B} = \{R_{ij}\}, \quad f_B = \left| dc\lambda_{ij} - \mathbb{B} \right| \tag{20}$$

$$Q_{ij} = g^{R_{ij}} h^{\Theta_{ij}} W_{ij}^{-c} \tag{21}$$

$$A_0 = g^{f_B} h^{\Psi} \left(\prod_{s=0}^{T} B_s^{-d^s} \right)^{c^n d^{n-T}} \prod_{l=1}^{n-1} A_l^{-c^l} \tag{22}$$

Figure 2: Simulator for matrix rank protocol