FFM Cryptosystem - Finite Field Matrix Cryptosystem - a public-key cryptosystem with encryption and signature schemes based on the hardness of finite field polynomial factorization

Yuri S Villas Boas

January 15, 2024

Abstract

We introduce a cryptosystem based on the difficulty of factorizing polynomials over finite fields. Public key is given by a full-rank Matrix over this field, and private key by its eigenvector decomposition. Cryptosystem allows for encryption and signature schemes, which are covered in the document, as well as preliminary cryptanalysis.

keywords: finite field polynomial factorization, linear algebra over finite field, characteristic polynomial, eigenvector decomposition, public-key cryptosystem, encryption scheme, signature scheme, cryptanalysis.

1 Algebra

Our proposed cryptosystem can be defined by the table below:

Component	**Formula**	**Definition**
Private Key	(R, A, R^{-1})	$R = (\mathbf{r_1}, \cdots, \mathbf{r_n})$ full-rank, with $n \geq 4$, even $A = (a_1\mathbf{e_1}, \cdots, a_n\mathbf{e_n})$, with $B\mathbf{r_i} = a_i\mathbf{r_i} \neq \mathbf{0}$
Public Key	B	$B = RAR^{-1}$
Plaintext	P	$P \in \mathbb{F}_p^{n\times n}$ represent an ordered basis over $\mathbb{F}_p^n$
Ciphertext	C	$C = PBP^{-1}$
Decription	VR^{-1}	$V = (\mathbf{v_1}, \cdots, \mathbf{v_n})$, where $C\mathbf{v_i} = a_i\mathbf{v_i}$
Document	d	$d \in \mathbb{F}_p$
Signature	s	$s = \Pi_{i=1}^{n/2}(x - a_{\pi(i)}^d) \in \mathbb{F}_p[x]$, where $\pi(\cdot) \in S_n$
Verification	$s \vert b_d$	$b_d = det\left(B^d - xI\right) \in \mathbb{F}_p[x]$

where,

$\mathbb{F}_p$	refers to the finite field of order p;
$\mathbb{F}_p[x]$	refers to the set of polynomials over $\mathbb{F}_p$;
$(\mathbf{m_1}, \cdots, \mathbf{m_n})$	signifies a matrix having $\mathbf{m_i}$ as its ith column vector;
$\mathbf{e_i}$	refers to the ith canonical vector of $\mathbb{F}_p$;
$p \vert q$	means 'p divides q';
S_n	is the symmetric group of n elements;

2 Computability

Throughout this session we will analyse the **polynomial-reducibility** of objects defined in the previous session. We are particularly concerned about the asymptotic complexity of factorizing elements of $\mathbb{F}_p[x]$ as function of the number of bits of p.

Throughout this session, we will have

$$n \geq 2 \tag{1}$$

$$f(x) = \Pi_{i=1}^{n}(x - a_i) = c_0x^0 + \cdots + c_{n-1}x^{n-1} + x^n : a_1, \cdots, a_n \in \mathbb{F}_p \tag{2}$$

$$f, g, h \in \mathbb{F}_p[x] : f = g * h \wedge deg(g), deg(h) \geq 1 \tag{3}$$

In other words, f is an n-degree monic polynomial over a finite field with $n \geq 2$, having c_i as the coefficient to ith power, and roots $a_1, \cdots, a_n$ in the field; and g, h non-trivial factors of f.

Definition 2.1. We define[1] the **non-strict preorder** $a \leq_p b$ as: *"b is polynomially reducible to a."* namely *"There exists a polynomial-time complexity algorithm to compute b from a."* That definition ensues the following **strict preorder** $a <_p b$ given by $a \leq_p b \wedge a \not\geq_p b$, and the **equivalence relation** $a \equiv_p b$ given by $a \leq_p b \wedge a \geq_p b$.

The bases of **asymmetric** cryptosystems are $<_p$ relations (which are **asymmetric**). We will now enunciate a few of them component-wise ($\leq_p$ and $\not\geq_p$). The first is the general objects in which the cryptosystem is based, and the following are the objects of the cryptosystem, and how they exactly or approximately replicate the $<_p$ relation. Here (as typically happens), $\not\geq_p$ relations are ultimately based on a conjecture — **in**existence of polynomial time algorithms with certain characteristics — while $\leq_p$ are constructively proven by the definition of the cryptosystem's algorithms.

Lemma 2.2 (Easiness of Polynomial Multiplication)**.**

$$(g, h) \leq_p g * h$$

Conjectured Lemma 2.3 (Hardness of Polynomial Factorization)**.**

$$(g, h) \not\geq_p g * h$$

Lemma 2.4 (eigen value-eigen vector equivalence)**.** $(B, R) \equiv_p (B, A)$

Proof.

($\leq_p$)**:** Compute $a_i \coloneqq (\mathbf{e_{j(i)}}^T B\mathbf{r_i}) * (\mathbf{e_{j(i)}}^T\mathbf{r_i})^{-1}$, for each $0 \leq i \leq n$ and any $j(\cdot)$ for which $\mathbf{e_{j(i)}}^T\mathbf{r_i} \neq 0$ — which is guaranteed to exist by R being full-rank. Namely, use the definition of eigenvectors to calculate each eigenvalues by taking one non-zero entry of $B\mathbf{r_i}$ and finding the 'ratio' of it to the same (non-null) entry of $\mathbf{r_i}$ (meaning, multiply the former by the later's multiplicative inverse in $\mathbb{F}_p$).

[1] 'p' in $\leq_p$ stands for *polynomial time*, while 'P' in the plaintext object stands, in fact, for *plaintext*, and 'p' in $\mathbb{F}_p$ is an incognate *prime* number. Those are three totally different concepts and they sharing the same letter is just a notation coincidence. Another two things not to be confused are the 'polynomials' of the asymptotic complexity of algorithms and the 'polynomials' that some of the described algorithms operate on.

($\geq_p$)**:** For each $1 \leq i \leq n$, solve $(B - a_i I)\mathbf{x_i} = \mathbf{0}$ on $\mathbf{x_i}$ to find the eigenspace of $\mathbf{r_i}$. Arbitrate any member of that space as $\mathbf{r_i}$. The resulting R and R^{-1} will satisfy $RAR^{-1} = B$.

QED

In other words, either component of the private key, A and R suffice to easily calculate the other (R and R^{-1} obviously are, in the same sense, equivalent too). That allows us to, henceforward refer to the private key as just A, for short.

Lemma 2.5. $f \equiv_p M$, where M is any matrix having $a_1, \cdots, a_n \in \mathbb{F}_p$ as eigenvalues. In other words:

Factorizing a monic polynomial of degree n known to have all roots in the field, is as hard as finding the eigenvalues of a matrix of order n, known to have full eigenvalue decomposition.

Proof. We have to prove that there are ($\leq_p$) an easy computation of a matrix M as a function of a given polynomial f with all roots in the field, so that M has full eigenvalue decomposition with the roots of f as eigenvalues; and conversely ($\geq_p$) an easy computation of a polynomial f as function of a given M known to have full eigenvalue decomposition that makes f have M's eigenvalues as roots.

($\leq_p$)**:** Take

$$M \coloneqq C(f) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -c_0 & -c_1 & -c_2 & \dots & -c_{n-1} \end{bmatrix}$$

the so called **companion matrix** of f.

($\geq_p$)**:** Compute

$$f(x) \coloneqq \det(xI - M)$$

through **Gaussian elimination**.

QED

Now, we will apply the same discussion to each component of the cryptosystem:

Theorem 2.6 (Completeness of Key Pair)**.**

$$(R, A(, R^{-1})) \leq_p B$$

Proof. Matrix (inversion and) multiplications $B \coloneqq RAR^{-1}$ totalling $\mathcal{O}(n^3)$ scalar multiplications and sums in $\mathbb{F}_p$. QED

Conjectured Theorem 2.7 (Soundness of Key Pair)**.**

$$(R, A(, R^{-1})) \not\geq_p B$$

Proof. From 2.4, ascertaining either component of the private key A or R is sufficient to ascertain the other. From 2.5, this is as hard as factorizing B's characteristic polynomial, which, by 2.3, is conjectured to be, in fact, hard. QED

Theorem 2.8 (Completeness of Signature)**.**

$$(A, d) \leq_p s$$

that is, ***issuing*** *a signature is easy, and*

$$(B, s', d') \leq_p (s'|B^{d'}), \forall s', d' \in \mathbb{F}_p[x]$$

that is, ***verifying*** *that a signature, corresponds to a documents and a public key is easy.*

Proof.

issuing: s is given by

$$s \coloneqq \Pi_{i=1}^{n/2}(x - a_{\pi(i)}^{d})$$

which has polynomial comple as a direct application of lemma 2.2.

verification: Computation of $B^{d'}$, its characteristic polynomial $b_{d'}$ and division of it by s, yielding:

$$\texttt{s\_is\_valid} \coloneqq ((det(B^{d'} - xI)\%s) == 0)$$

where % represents the remainer operation == is an equality test. All components are of polynomial time complexity.

QED

Conjectured Theorem 2.9 (Soundness of Signature)**.**

$$s \not\geq_p (B, d)$$

Meaning, a signature cannot be easily forged, that is, computed without A.

Proof. In order to forge a valid signature s for document d and public key B, an adversary would have to partially factorize $b^d = det(B^d - xI)$, which is conjectured to be hard in 2.3. In this case, adversary has a polynomial $det(B - xI)$ whose roots are known to be dth roots of those of $det(B^d - xI)$. This additional knowledge is not known to ensue lower time-complex cryptanaly, but is suspected to allow for statistical attacks. QED

Theorem 2.10 (Completeness of Encryption)**.**

$$(B, P) \leq_p C$$

that is, ***encrypting*** *a plaintext message is easy, and*

$$(A, C) \leq_p P$$

that is, ***decrypting*** *a ciphertext message is easy.*

Proof.

encrypting: Matrix inversion and multiplications $C \coloneqq PBP^{-1}$ totalling $\mathcal{O}(n^3)$ scalar multiplications and sums in $\mathbb{F}_p$.

decrypting: We use the algorithm described in ($\geq_p$) session of lemma 2.4, and the fact that C is known to have a full eigenvalue decomposition given by $C = VAV^{-1}$ with (privately) known A to ascertain a valid V, then proceed to compute a $P \coloneqq VR^{-1}$. By construction, the obtained P will satisfy $C = PBP^{-1}$ and therefore represents the same basis meant by the sender of the plaintext. All components are of polynomial time complexity.

QED

Conjecture 2.11 (Soundness of Encryption)**.**

$$P \not\geq_p (B, C)$$

that is, deciphering a ciphertext is hard.

Argument. The apparent hardness of ascertaining P from $C = PBP^{-1}$ seems to be analogous to that of eigenvalue decomposition, proven to be equivalent to the conjectured (2.3) hardness of polynomial factorization.

3 Complexity

4 Cryptanalysis

5 Dedication

This work is dedicated to Dr. Hans-Christian Herbig, a noble, honorable man who kept unswerving virile dignity in face of calumny, persecution, malatie and death. His standing by truth, righteousness and to the personal defense of myself, then, a complete stranger, when nobody else would, at peril to his very career, and without any prospective gain whatsoever will never be forgotten.