Revista Colombiana de Matemáticas

Volumen 45
Número 2
2011

Sociedad Colombiana de Matemáticas

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE BOGOTÁ
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS

Revista Colombiana de Matemáticas
Volumen 45(2011)2, páginas 147-166

New Variants of the Square-Vinegar Signature Scheme

Nuevas variantes del esquema de firmas Square-Vinegar

John B. Baena[1], Crystal Lee Clough[2], Jintai Ding[3]

[1]Universidad Nacional de Colombia, Medellín, Colombia

[2]Thomas More College, Crestview Hills, United States

[3]University of Cincinnati, Cincinnati, United States

Abstract. This paper proposes two ways to fix the broken Square-Vinegar signature scheme. We give heuristic arguments as well as experimental evidence to support the security claims. The first variant, Square-Vinegar with Embedding, uses a simple modification that nonetheless changes the nature of the public key polynomials. The second, 2-Square-Vinegar, is a more significant overhaul of the construction, using a bivariate secret map instead of a univariate one.

Key words and phrases. Multivariate cryptography, Square-vinegar signature scheme, Odd characteristic.

2000 Mathematics Subject Classification. 11T71, 11Y40.

Resumen. Este artículo propone dos maneras de arreglar el esquema de firmas Square-Vinegar, el cual ha sido roto. Suministramos argumentos heurísticos, así como evidencia experimental para apoyar nuestras afirmaciones sobre seguridad. La primera variante, Square-Vinegar con inmersión, a pesar de usar una modificación simple, cambia la naturaleza de los polinomios de la clave pública. La segunda, 2-Square-Vinegar, es una revisión más significativa de la construcción, con una función secreta bivariada en lugar de una univariada.

Palabras y frases clave. Criptografía multivariada, esquema de firmas Square-Vinegar, característica impar.

1. Introduction

Multivariate public-key cryptosystems (MPKCs) are those schemes constructed using multivariate polynomials over a finite field. The study of MPKCs is motivated by the fact that solving a system of multivariate polynomial equations is NP-hard [6]. Unlike integer factorization or the discrete log problem, solving a system of multivariate equations should be no easier to solve for a quantum computer than for any other computer. For this reason, MPKCs stand among the few options for post-quantum cryptography.

Among the proposed MPKCs is HFE, proposed in 1996 by Patarin [9] (see Section 2.1). An HFE scheme could still be secure, but the parameters required would make it so inefficient as to be unusable. Many variants of HFE have been proposed and analyzed. For example, HFEv$^-$ is a signature scheme which combines HFE with another system called Oil-Vinegar and also uses the Minus construction [11]. Particular HFEv$-$ schemes include Quartz, whose improvement Quartz-7m seems secure, and Square-Vinegar which has significantly faster signing times than Quartz [1]. Square-Vinegar was broken in 2009 [2]. In this paper, we introduce some variants of the original Square-Vinegar scheme and some arguments and experimental results suggesting that these variants resist attack.

This paper is organized as follows. In Section 2 we give some relevant background material - a description of the HFE, Oil-Vinegar, and original Square-Vinegar schemes and the attacks against Square-Vinegar. Sections 3 and 4 are devoted to our new versions of Square-Vinegar and their security analysis.

2. Background

We describe the original Square-Vinegar scheme and how it is broken, preceded by a brief description of HFE and Oil-Vinegar schemes for clarity.

2.1. HFE

The cryptosystem HFE, short for Hidden Field Equations, was proposed by Patarin in 1996 [9]. Let k be a field of size q and K a degree n extension. Like many other MPKCs, this scheme relies on the interplay between the field structure and vector space structure of K. For the original versions, k is characteristic 2. We require univariate polynomials over K of a specific form.

Definition 1. An *HFE polynomial with bound D* is a polynomial of q-Hamming weight degree 2 and total degree not more than D. In other words, $G \in K[X]$ is an HFE polynomial if it is of the form

$$G(X) = \sum_{q^i+q^j \leq D} \alpha_{ij} X^{q^i+q^j} + \sum_{q^j \leq D} \beta_j X^{q^j} + \gamma,$$

where $\alpha_{ij},\ \beta_j,\ \gamma \in K$.

To construct an HFE system for a specified D, choose randomly from the collection of HFE polynomials of bound D a secret core map $F : K \to K$. The public key P is the composition of F with invertible affine transformations S and T along with the vector space isomorphism $\varphi : K \to k^n$:

$$P = T \circ \varphi \circ F \circ \varphi^{-1} \circ S.$$

Note that P is a tuple

$$P = \begin{pmatrix} P_1(x_1, \ldots, x_n) \\ \vdots \\ P_n(x_1, \ldots, x_n) \end{pmatrix}$$

where each P_i is a quadratic polynomial. The private key is the decomposition of P, in particular the maps S and T. See Figure 1.

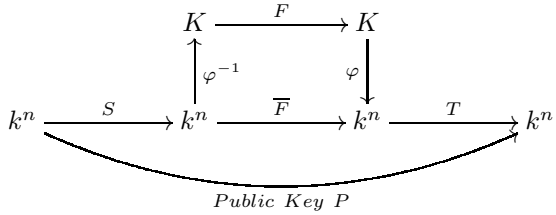

FIGURE 1. The HFE system.

2.2. Oil-Vinegar

Also proposed by Patarin is the Oil-Vinegar signature scheme [10]. Let $o, v \in \mathbb{N}$ and consider the ring $k[x_1, \ldots, x_o, x'_1, \ldots, x'_v]$. We call $x_1, \ldots, x_o$ *oil variables* and $x'_1, \ldots, x'_v$ *vinegar variables*. The scheme is built from polynomials of a certain form.

Definition 2. A polynomial $f \in k[x_1, \ldots, x_o, x'_1, \ldots, x'_v]$ is called an *oil-vinegar polynomial* if it is of the form

$$f(x_1, \ldots, x_o, x'_1, \ldots, x'_v) = \sum_{i=0}^{o} \sum_{j=0}^{v} a_{ij} x_i x'_j + \sum_{i=0}^{v} \sum_{j=0}^{v} b_{ij} x'_i x'_j + \sum_{i=0}^{o} c_i x_i + \sum_{j=0}^{v} d_j x'_j + e.$$

In other words, an oil-vinegar polynomial is a quadratic polynomial of the oil and vinegar variables which has no monomials of the form oil·oil.

The public key of an Oil-Vinegar scheme is $P = F \circ L : k^{o+v} \to k^o$, where L is an invertible affine transformation $k^{o+v} \to k^{o+v}$ and $F : k^{o+v} \to k^o$ (the decomposition of P is the private key). The components F_i of F are oil-vinegar polynomials.

Signing a document $(y_1, \ldots, y_o) \in k^o$ is easy because once the vinegar variables are given values, say $w_1, \ldots, w_v \in k$, then the system on the oil variables

$$F(x_1, \ldots, x_o, w_1, \ldots, w_v) = \begin{pmatrix} F_1(x_1, \ldots, x_o, w_1, \ldots, w_v) \\ \vdots \\ F_0(x_1, \ldots, x_o, w_1, \ldots, w_v) \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_o \end{pmatrix}$$

is simply a linear system of equations. The signer has the freedom to choose the vinegar values at random.

The drawback of the Oil-Vinegar system is that v must be large; i.e., the signature must be more than twice as long as the document.

2.3. HFEv− and Square-Vinegar

We now outline one way to make a signature scheme from the HFE idea: Square-Vinegar, a special case of HFEv−.

Let $k \cong \mathbb{F}_q$ with q odd and $n, v \in \mathbb{N}$. The field K is an extension of degree n and $\phi : K \to k^n$ is the usual vector space isomorphism, defined by

$$\phi(a_1 + a_2 y + \cdots + a_n y^{n-1}) = (a_1, a_2, \ldots, a_n).$$

To construct a public key, we will use as a secret core map $G : K \times k^v \to K$. Let $X_v = (x'_1, \ldots, x'_v) \in k^v$ and refer to these as "vinegar variables"; then G is given by

$$G(X, X_v) = AX^2 + \beta(X_v)X + \gamma(X_v), \tag{1}$$

where A is a nonzero element of K. The maps β and γ, both maps $k^v \to K$, are as follows:

$$\beta(X_v) = \sum_{1 \le j \le v} B_j x'_j + C, \tag{2}$$

and

$$\gamma(X_v) = \sum_{1 \le j \le i \le v} D_{ij} x'_i x'_j + \sum_{1 \le j \le v} E_j x'_j + H, \tag{3}$$

where B_j, C, D_{ij}, E_j, H are randomly chosen elements of K. Note that β is linear in the components of X_v and γ is quadratic. The connection to HFE is that once the vinegar variables are fixed, G becomes a polynomial in X and is an HFE polynomial of bound 2.

By combining the map G with the vector space isomorphism and the identity map $id : k^v \to k^v$, we construct a quadratic map $\overline{G} : k^n \times k^v \to k^n$,

$$\overline{G}(x_1, \ldots, x_n, x'_1, \ldots, x'_v) = \phi \circ G \circ (\phi^{-1} \times id)(x_1, \ldots, x_n, x'_1, \ldots, x'_v).$$

We also use two invertible affine transformations $T : k^n \to k^n$, $S : k^{n+v} \to k^{n+v}$, and a projection map $\pi : k^n \to k^{n-r}$ given by $\pi(z_1, \ldots, z_n) = (z_1, \ldots, z_{n-r})$. This projection describes the "$-$" action of removing components of the public key.

The public key P is a composition of these maps in the order $P = \pi \circ T \circ \overline{G} \circ S$, see Figure 2. The private key is the decomposition of P, i.e., the map G along with S and T.

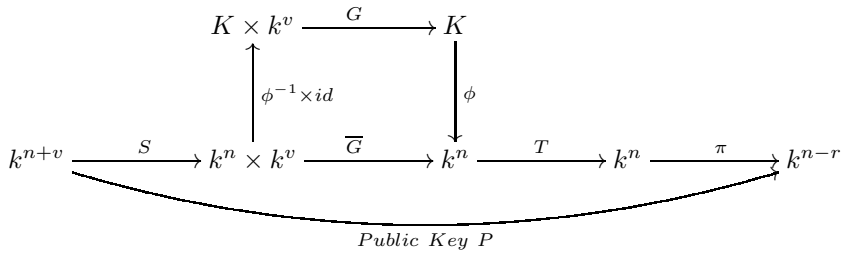

FIGURE 2. The Square-Vinegar System.

Using this construction for a signature scheme is very similar to using the first proposed variant, Square-Vinegar with Embedding, so we omit those details here.

Note that here we described Square-Vinegar, but and HFEv$-$ scheme has the same structure. In general, q need not be odd and the degree bound of G is not necessarily 2. In fact, Quartz-7m has $q = 2$ and $D = 129$ [12].

2.4. Attacks on Square-Vinegar

For simplicity, we will assume that $A = 1$ in (1). Before describing two different attacks on Square-Vinegar, we make the following important observation. While the core map G is defined as

$$G(X, X_v) = X^2 + \beta(X_v)X + \gamma(X_v),$$

where β is linear and γ quadratic, we may in fact assume that β is constant, in other words that there are no oil-vinegar cross terms. This is because

$$\begin{aligned} G &= \widetilde{G} \circ L, \quad \text{where} \\ \widetilde{G}(X, X_v) &= X^2 + \gamma(X_v) - \frac{1}{4}\beta(X_v)^2, \\ L(X, X_v) &= \left(X + \frac{1}{2}\beta(X_v), X_v\right). \end{aligned}$$

The map L is invertible, and may be absorbed by S.

2.4.1. Invariant Subspace Attack

One method of attacking the Square-Vinegar scheme is related to an attack on the Oil-Vinegar system [7]. For any homogeneous quadratic polynomial, i.e. a quadratic form, we may associate a unique symmetric matrix. Specifically, if $\vec{x} = (x_1 \cdots x_m)^T$ and $f(x_1, \ldots, x_m) \in k[x_1, \ldots, x_m]$ is homogeneous degree 2, then there exists a unique $M \in \mathcal{M}_{m\times m}(k)$ such that $f(x_1, \ldots, x_m) = \vec{x}^T M \vec{x}$. We will refer to such an M as the *matrix associated to f*. Also, we may speak of the matrix associated to a nonhomogeneous quadratic, meaning the matrix associated to its homogenous part.

As discussed above, without loss of generality let us assume that G has no oil-vinegar cross terms. Then the components of the map $\overline{G} = (\overline{G}_1, \ldots, \overline{G}_n)$ will also have limited mixing of the variables, in particular they have the form

$$\overline{G}_t(z_1, \ldots, z_{n+v}) = \sum_{j\leq i=1}^{n} a_{tij} z_i z_j + \sum_{j\leq i=1}^{v} b_{tij} z_{n+i} z_{n+j}.$$

This means that the matrix $\mathcal{G}_t$ associated to $\overline{G}_t$ looks like

$$\mathcal{G}_t = \begin{pmatrix} \mathcal{G}_{t1} & 0 \\ 0 & \mathcal{G}_{t2} \end{pmatrix},$$

with $\mathcal{G}_{t1} \in \mathcal{M}_{n\times n}(k)$, $\mathcal{G}_{t2} \in \mathcal{M}_{v\times v}(k)$ symmetric.

Among the useful properties of these matrices are their invariant subspaces. Let $k^n \times \{(0, \ldots, 0)\} \subset k^{n+v}$ be the "oil space" $\mathcal{O}$ and $\{(0, \ldots, 0)\} \times k^v \subset k^{n+v}$ be the "vinegar space" $\mathcal{V}$. Note that $\mathcal{G}_t(\mathcal{O}) \subseteq \mathcal{O}$ and $\mathcal{G}_t(\mathcal{V}) \subseteq \mathcal{V}$. In fact, if $\mathcal{G}_t$ is invertible this holds for $\mathcal{G}_t^{-1}$ as well.

The $\mathcal{G}_t$ are not directly accessible to an attacker; he has only the public key P. However, each component P_i of P is a quadratic polynomial and thus has an associated matrix $\mathcal{P}_i$. The $\mathcal{P}_i$ do not have $\mathcal{O}$ and $\mathcal{V}$ as invariant subspaces, but it turns out that $S^{-1}(\mathcal{O})$ *is a common invariant subspace of all matrices of the form* $\mathcal{P}_i^{-1}\mathcal{P}_j$. Moreover, $S^{-1}(\mathcal{O})$ is a common invariant subspace of all matrices in the k-linear space Ω spanned by the matrices $\mathcal{P}_i^{-1}\mathcal{P}_j$.

If the characteristic polynomial of a randomly selected matrix $\Delta \in \Omega$ factors into two distinct irreducible polynomials, then we can recover the subspace $S^{-1}(\mathcal{O})$ as the kernel of $C(\Delta)$, where C is the degree n irreducible polynomial of such factorization. In this way we can get rid of the vinegar variables X_v from the core map G, being left with a new core map of the form

$$\begin{aligned} \widehat{G} : K &\longrightarrow K \\ X &\longmapsto \widehat{G}(X) = X^2 + E, \end{aligned}$$

where E is a constant element in K. After this we can use the attack on SFlash [5], to recover the r polynomials that were removed from the public key (minus

part of Square-Vinegar). Then we use the Kipnis-Shamir attack on HFE [8], to recover invertible linear transformations $\widehat{S} : k^n \to k^n$ and $\widehat{T} : k^n \to k^n$ such that the remaining public key is equivalent to the map $\widehat{T} \circ \widehat{G} \circ \widehat{S}$, thus breaking the system.

2.4.2. Differential Attack

Another attack on Square-Vinegar was presented in [2]. The authors found an equivalent secret key by taking advantage of properties of the differential of the core map G. By differential of a map $f(x)$ we mean $Df(a, x) = f(a + x) - f(a) - f(x) + f(0)$.

As in the invariant subspace attack, without loss of generality assume that oil and vinegar do not mix, i.e., the β term of G is constant.

They note that usually, an L satisfying

$$DP\big(L(X, X_v), (Y, Y_v)\big) + DP\big((X, X_v), L(Y, Y_v)\big) = 0, \tag{4}$$

where P is the Square-Vinegar public key, is of the form

$$L = S^{-1} \circ (\phi \times id) \circ \Lambda_{uc} \circ (\phi^{-1} \times id) \circ S,$$

where $\Lambda_{uc} : K \times k^v \to K \times k^v$, with $u \in K$ and $c \in k$, given by

$$\Lambda_{uc}(X, X_v) = (uX, cX_v).$$

This L satisfy (4) because

$$P \circ L = \pi \circ T \circ \phi \circ G \circ \Lambda_{uc} \circ (\phi^{-1} \times id) \circ S.$$

Such L can be found by an attacker since they satisfy a linear equation derived from the public key. Since the characteristic polynomial of L is the characteristic polynomial of Λ_{uc}, one can find the corresponding c and u^{q^i} for some i. Once u^{q^i} is known, one can find a map $\widetilde{S}$ which plays the role of S in the equivalent private key. From here, Square-Vinegar is dead.

3. Square-Vinegar with Embedding

In light of these attacks on Square-Vinegar, we propose some new variants of this idea, which resist known attacks. Square-Vinegar with Embedding is a simple modification - we have only altered the transformation S.

3.1. Description

Again, let $k \cong \mathbb{F}_q$ with q odd and $n, l, v \in \mathbb{N}$. Consider the extension field K of degree $n + l$ and $\phi : K \to k^{n+1}$ the usual vector space isomorphism.

As with Square-Vinegar, the secret core map $G : K \times k^v \to K$ is given by

$$G(X, X_v) = AX^2 + \beta(X_v)X + \gamma(X_v),$$

where A is a nonzero element of K. The maps β and γ are defined exactly as for Square-Vinegar.

By combining G with the vector space isomorphism, we build a quadratic map $\overline{G} : k^{n+1} \times k^v \to k^{n+1}$,

$$\overline{G} = \phi \circ G \circ (\phi^{-1} \times id).$$

We also make use of a full rank affine transformation (an embedding) $S : k^{n+v} \to k^{n+1} \times k^v$, an invertible affine transformation $T : k^{n+1} \to k^{n+1}$, and a projection map $\pi : k^{n+1} \to k^{n+l-r}$ given by $\pi(z_1, \ldots, z_{n+l}) = (z_1, \ldots, z_{n+l-r})$.

The public key P is a composition of these maps in the following order:

$$P = \pi \circ T \circ \overline{G} \circ S.$$

See Figure 3. The private key is the decomposition of P, i.e., the map G along with S and T.

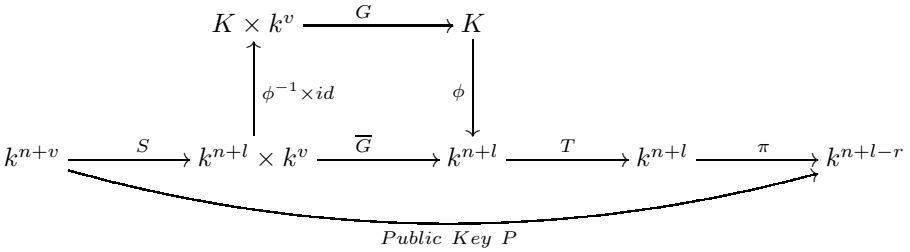

FIGURE 3. The Square-Vinegar with embedding system.

What makes this scheme different from the Square-Vinegar is that S is an embedding. The intention of this change is to destroy the connection between the space of signatures k^{n+v} and the field structure of K. We will discuss this further in the security analysis, Section 3.2.

To use this setup for digital signatures, documents will be elements of k^{n+l-r}. To sign a document $(y_1, \ldots, y_{n+l-r})$, we perform the following steps:

- Randomly "complete" the document with $y_{n+l-r+1}, \ldots, y_{n+l} \in k$.
- Choose values $w_1, \ldots, w_v$ for the vinegar variables X_v (at random).
- Solve over K the quadratic equation in X

$$G\big(X, (w_1, \ldots, w_v)\big) = \phi^{-1} \circ T^{-1}(y_1, \ldots, y_{n+l}). \tag{5}$$

- If the equation has no solutions in K, make a new choice of vinegar variables and try again.

- Once we have an equation of the form (5) with solutions in K, say $\widetilde{X}_1$ and $\widetilde{X}_2$, check if $\big(\widetilde{X}_i, (w_1, \ldots, w_v)\big)$ has a preimage under $(\phi^{-1} \times id) \circ S$. If not, try again with new vinegar variables.

- Suppose $\widetilde{X}_i$ is a solution to (5) and the set $S^{-1}\big(\phi(\widetilde{X}_i), w_1, \ldots, w_v\big) \neq \varnothing$. Since S is injective, $S^{-1}\big(\phi(\widetilde{X}_i), w_1, \ldots, w_v\big)$ is a singleton. This element of k^{n+l+v} is a signature of the document.

Since the signing process involves choosing values and poor choices are possible, extensive testing was done to see how many tries were required to obtain a signature. The results are summarized in Table 1; one sees that roughly q tries are required to sign when $l = 1$.

TABLE 1. Signing times for Square-Vinegar with embedding systems, for $r = 3$.

q	n	$n+l$	v	Average time to sign [s]	Average # of tries to sign [s]
19	30	31	4	0.045956	20.931
19	32	33	4	0.086812	19.404
19	30	31	6	0.042304	17.867
19	32	33	6	0.096156	20.904
23	30	31	4	0.055344	24.823
23	32	33	4	0.117324	24.064
23	32	33	6	0.118104	23.700
23	34	35	6	0.126204	23.988
31	30	31	4	0.076880	32.083
31	32	33	4	0.156300	31.276
31	30	31	6	0.082756	32.739
31	32	33	6	0.158768	30.840

Note that these average signing times are much faster than when using Quartz parameters: $t \approx 2.6$ s, when $q = 2$, $D = 129$, $n = 103$, $v = 4$ and $r = 3$; see [1].

We used MAGMA 2.14 on a Vaio Computer with Windows Vista which has an Intel(R) Core(TM)2 Duo CPU 2.00GHz processor with 2.00 GB of memory installed, to run the computer experiments. In each case 100 different random documents were tried.

3.2. Security Analysis

3.2.1. Invariant Subspace Attacks

As in the case of Square-Vinegar, the matrices associated to the core map $\overline{G}$ have a nice block-diagonal shape. However, the fact that S is an embedding prevents the public key polynomials' associated matrices from sharing these invariant subspaces.

When S is invertible, the matrices $\mathcal{P}_i$ of the public key have the property that $\mathcal{P}_i^{-1}\mathcal{P}_j$ all have $S^{-1}(\mathcal{O})$ as an invariant subspace. This is because

$$\mathcal{P}_j = S^T \widetilde{\mathcal{G}}_j S,$$

where $\widetilde{\mathcal{G}}_j$ is a linear combination of the core map's matrices $\mathcal{G}_1, \ldots, \mathcal{G}_n$; the specific combination is determined by T. Thus $\mathcal{P}_j^{-1} = S^{-1}\widetilde{\mathcal{G}}_j(S^T)^{-1}$. However, when S is just an embedding, we cannot obtain similar expressions that guarantee that $S^{-1}(\mathcal{O})$ is a common invariant subspace of the matrices $\mathcal{P}_i^{-1}\mathcal{P}_j$.

Recall that if $S^{-1}(\mathcal{O})$ were a common invariant subspace of the matrices $\mathcal{P}_i^{-1}\mathcal{P}_j$, then it would also be a common invariant subspace of all matrices in the k-linear space Ω spanned by the matrices $\mathcal{P}_i^{-1}\mathcal{P}_j$.

If the characteristic polynomial of at least one matrix $\Delta \in \Omega$ is irreducible, then there would not be invariant subspaces different from the trivial ones. We were able to confirm this absence by extensive computer experiments; see Table 2 for a summary of these results. We conclude that Square-Vinegar with embedding systems are resistant to this kind of attack.

TABLE 2. Number of irreducible characteristic polynomials.

q	n	l	$n+l$	v	r	Number of irreducible characteristic polynomials
19	32	1	33	4	3	15
19	34	1	35	4	3	10
19	32	1	33	6	3	13
19	34	1	35	6	3	15
23	32	1	33	4	3	16
23	34	1	35	4	3	18
23	32	1	33	6	3	16
23	34	1	35	6	3	17
31	32	1	33	4	3	14
31	34	1	35	4	3	9
31	32	1	33	6	3	12
31	34	1	35	6	3	13

3.2.2. Algebraic Attacks

Algebraic attacks can be employed against any MPKC. Suppose that someone, who does not know the private key, wants to recover the plaintext from a ciphertext $(y_1, \ldots, y_m) \in k^m$. This attacker only has access to the public key $P : k^t \to k^m$, $P = (P_1, \ldots, P_m)$. The most straightforward way to attack is to solve the system of equations

$$\begin{aligned} P_1(x_1, \ldots, x_t) - y_1 &= 0 \\ P_2(x_1, \ldots, x_t) - y_2 &= 0 \\ &\vdots \\ P_m(x_1, \ldots, x_t) - y_m &= 0. \end{aligned} \tag{6}$$

Solving these equations directly is known as the algebraic attack. This can be done with the help of a Gröbner basis. We used the F_4 function of MAGMA, which is the most efficient implementation of the Gröbner basis F_4 algorithm that is currently available. All the computer experiments of this section were run on an Intel(R) Core(TM)2 2.40 GHz processor with 1.99 GB of memory installed.

Because of the vinegar variables, the system (6) is underdetermined. Since we only need to find a solution for this system, we can guess values for some of the variables yielding a system with the same number of equations as variables, as was done in [3]. This speeds up the attack significantly.

The benefits of using fields of odd characteristic for MPKCs against the Gröbner basis attack are discussed in [4]. Our experiments suggest that any prime integer $q \geq 19$ provides a strong defense against an algebraic attack via Gröbner bases. Table 3 and Figure 4 contain a summary of results for $q = 19$. Also, in Figure 5 we can observe how the maximum degree of the polynomials used by F_4 grows as n increases, for different values of q.

We observe that the average time used to solve the system of equations grows exponentially in n. This behavior can also be seen in the memory used. We generated random polynomial equations of the same dimensions (same q, l, n, v and r) and found that the time needed to solve such a system using Gröbner bases is essentially the same that is needed to break Square-Vinegar with embedding with our choices of parameters. Table 4 shows these times for different values of n.

From the information gathered with our experiments it appears that under our choices of parameters, F_4 is no more efficient in solving the public key equations of a Square-Vinegar with embedding scheme than a system of random equations. Extrapolating our data, we think that for any $q \in \{19, 23, 31\}$, the

TABLE 3. Gröbner basis attack for $q = 19$, $l = 1$, $v = 4$ and $r = 3$, for several values of n.

n	$n+l$	Average time [s]	Minimum time [s]	Maximum time [s]	Memory used [MB]
6	7	0.001	0	0.016	6
7	8	0.003	0	0.016	6
8	9	0.016	0.015	0.032	6
9	10	0.085	0.078	0.094	7
10	11	0.593	0.578	0.641	11
11	12	4.036	3.890	4.375	28
12	13	30.055	29.641	32.062	103
13	14	224.705	219.016	240.687	403

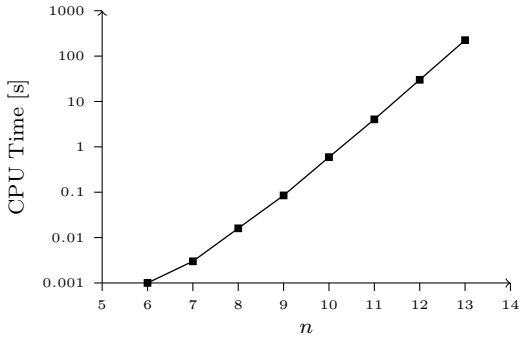

FIGURE 4. Running time under Gröbner basis attack for $q = 19$, $l = 1$, $v = 4$ and $r = 3$, for several values of n.

TABLE 4. Time comparison of some Square-Vinegar with embedding systems and random equations under GB attack. $q = 19$, $l = 1$, $v = 4$, and $r = 3$.

n	Square-Vinegar with embedding	Random equations
6	0.001	0.001
7	0.003	0.003
8	0.016	0.016
9	0.085	0.088
10	0.593	0.611
11	4.036	4.011
12	30.055	30.456
13	224.705	223.988

parameters $n = 30$, $l = 1$, $v = 4$, and $r = 3$, make Square-Vinegar with embedding secure against algebraic attacks (more than 2^{80} computations).

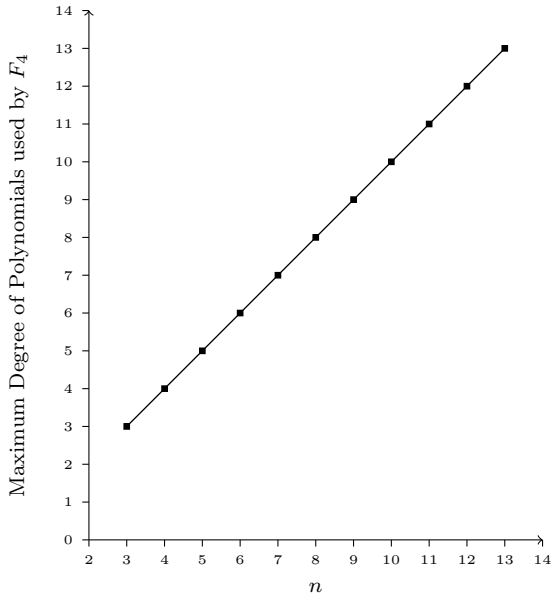

FIGURE 5. Maximum Degree of Polynomial used by F_4 for Square-Vinegar with embedding, $q \in \{19, 23, 31\}$, $l = 1$, $v = 4$, and $r = 3$.

3.2.3. Differential Attacks

Let us now show how the embedding renders the differential attack of [2] ineffective and discuss resistance to other differential-style attacks. Recall that the differential attack on Square-Vinegar makes use of mappings $\Lambda_{uc} : K \times k^v \to K \times k^v$ given by

$$\Lambda_{uc}(X, X_v) = (uX, cX_v).$$

In the attack on Square-Vinegar, one is able to find matrices of the form

$$L = S^{-1} \circ (\phi \times id) \circ \Lambda_{uc} \circ (\phi^{-1} \times id) \circ S.$$

In the new case, S^{-1} does not exist; however, S is injective, so an attacker may find an analogous matrix with the right-inverse of S, i.e., something of the form

$$\widetilde{L} = S^T(SS^T)^{-1} \circ (\phi \times id) \circ \Lambda_{uc} \circ (\phi^{-1} \times id) \circ S.$$

We may find $\widetilde{L}$ in the embedding case as easily as one may find L in the Square-Vinegar case. This is because $\widetilde{L}$ acts as L in the sense that

$$P \circ \widetilde{L} = \pi \circ T \circ \phi \circ G \circ \Lambda_{uc} \circ (\phi^{-1} \times id) \circ S.$$

The vital fact is that the characteristic polynomials of L and $\widetilde{L}$ do not have the same behavior. The characteristic polynomial of L is that of Λ_{uc} but for $\widetilde{L}$ the characteristic polynomial is different. Thus, we cannot discover information about u from this matrix as we can in the Square-Vinegar situation. Without this ability, the attack is dead.

Note also, that being able to find $\widetilde{L}$ puts an attacker in a position similar to that of an attacker of SFlash [5], and a priori it is possible that the "missing" polynomials omitted from the public key could be recovered. However, in the case of SFlash, the knowledge of these hidden multiplication maps is enough to break the system due to the simplicity of the core map. For Square-Vinegar with Embedding, the design of G ensures that $G \circ \Lambda_{uc}$ cannot be $M \circ G$ for any linear map M. So, even though such matrices can be found they are of no use to an attacker.

In light of the above security analysis, we belive that Square-Vinegar with Embedding is a viable signature scheme under reasonable parameter choices.

4. 2-Square-Vinegar

4.1. Description

Again, we use the field $k \cong \mathbb{F}_q$ with q odd, $n, v, r \in \mathbb{N}$, $K \cong \mathbb{F}_{q^n}$, $\phi : K \to k^n$. Documents are vectors in k^{2n-r}, and signatures are vectors in k^{2n+v}. This time we use a core map $G : (K \times K) \times k^v \to K \times K$, the components given by

$$G_1(X, Y, X_v) = X^2 + \beta_1(X_v)Y + \gamma_1(X_v)$$

$$G_2(X, Y, X_v) = Y^2 + \beta_2(X_v)X + \gamma_2(X_v),$$

where $\beta_i : k^v \to K$ are linear as in (2) and $\gamma_i : k^v \to K$ are quadratic as in (3). The affine maps are $S : k^{2n+v} \to k^n \times k^n \times k^v$ and $T : k^n \times k^n \to k^{2n}$. The public key is $P : k^{2n+v} \to k^{2n-r}$ and is given by (see Figure 6)

$$P = \pi \circ T \circ (\phi \times \phi) \circ G \circ (\phi^{-1} \times \phi^{-1} \times id) \circ S.$$

To sign a document $(y_1, \ldots, y_{2n-r}) \in k^{2n-r}$ with 2-Square-Vinegar, we perform the following steps:

- Randomly "complete" the document with $y_{2n-r+1}, \ldots, y_{2n} \in k$.
- Compute $(z_1, \ldots, z_{2n}) = T^{-1}(y_1, \ldots, y_{2n})$ and let
$$(Z_1, Z_2) = \phi^{-1} \times \phi^{-1}(z_1, \ldots, z_{2n}).$$
- Choose values $w_1, \ldots, w_v$ for the vinegar variables, let $W_v = (w_1, \ldots, w_v)$.

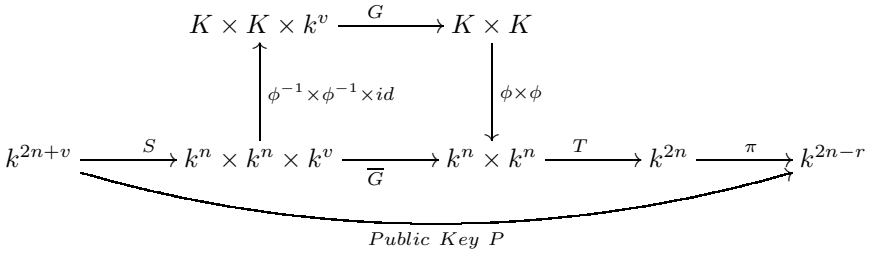

FIGURE 6. The 2-Square-Vinegar System.

- Solve the system of equations

$$X^2 + \beta_1(W_v)Y + \gamma_1(W_v) = Z_1 \tag{7}$$
$$Y^2 + \beta_2(W_v)X + \gamma_2(W_v) = Z_2. \tag{8}$$

  This can be done by solving (7) for Y (or (8) for X) and substituting into the other equation. The resulting univariate quartic equation can be solved using Berlekamp's algorithm, for example.

- If a solution in K cannot be found, make a new choice of vinegar variables and try again. Otherwise, if $(X, Y) \in K \times K$ is a solution to (7) and (8); the signature is

$$S^{-1}(\phi(X), \phi(Y), w_1, \ldots, w_v) \in k^{2n+v}.$$

We present some results when Berlekamp's algorithm is used in Table 5. In each case 100 different random documents were signed for 10 different keys[1].

TABLE 5. Signing times for 2-Square-Vinegar systems, for $r = 3$.

q	n	$2n$	v	$2n+v$	Average time to sign [s]	Average # of tries to sign
19	15	30	4	34	0.014123	1.579
19	16	32	4	36	0.015273	1.567
19	15	30	6	36	0.014104	1.610
19	16	32	6	38	0.015337	1.630
23	15	30	4	34	0.014971	1.623
23	16	32	4	36	0.016902	1.587
23	15	30	6	36	0.015758	1.609
23	16	32	6	38	0.017144	1.628

[1]On an Intel(R) Core(TM)2 Duo CPU 2.00GHz processor with 2.00 GB of memory installed.

Notice again that these signing times are much faster than those when using Quartz parameters: $t \approx 2.6$ s, when $q = 2$, $D = 129$, $n = 103$, $v = 4$ and $r = 3$ [1].

4.2. Security Analysis

4.2.1. Algebraic Attacks

See Section 3.2.2 for a general description of algebraic attacks. For 2-Square-Vinegar, a summary of our experimental results[2] are shown in Table 6 and Figure 7. We can see how the average time and memory used by F_4 to solve the system of equations grow exponentially in n.

TABLE 6. Algebraic attack for 2-Square-Vinegar, with $q = 19$, $v = 4$ and $r = 3$, for several values of n.

n	$2n$	Average time [s]	Minimum time [s]	Maximum time [s]	Memory used [MB]
4	8	0.003	0	0.016	6
5	10	0.086	0.062	0.109	7
6	12	4.002	3.890	4.328	28
7	14	221.886	218.078	240.531	403

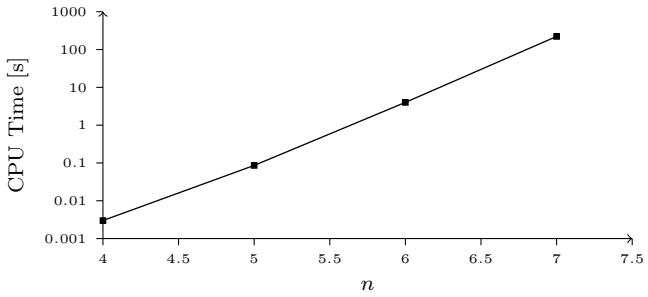

FIGURE 7. Running time under GB attack for 2-Square-Vinegar, with $q = 19$, $v = 4$ and $r = 3$, for several values of n.

As in the case of Square-Vinegar with Embedding, the results suggest that with reasonable parameter choices, an algebraic attack against 2-Square-Vinegar is infeasible.

[2]On an Intel(R) Core(TM)2 2.40 GHz processor with 1.99 GB of memory installed.

4.2.2. Invariant Subspace Attacks

In short, 2-Square-Vinegar resists the invariant subspace attack on Square-Vinegar because the properties that a univariate core map grants to its associated matrices are not granted by the bivariate version.

Let us consider the map $\overline{G}_1 : k^{2n+v} \to k^n$ given by

$$\overline{G}_1 = \phi \circ G_1 \circ (\phi^{-1} \times \phi^{-1} \times id).$$

This map has components

$$\overline{G}_1(x_1, \ldots, x_n, y_1, \ldots, y_n, x'_1, \ldots, x'_v) = \begin{pmatrix} \overline{G}_{11}(x_1, \ldots, x_n, y_1, \ldots, y_n, x'_1, \ldots, x'_v) \\ \vdots \\ \overline{G}_{1n}(x_1, \ldots, x_n, y_1, \ldots, y_n, x'_1, \ldots, x'_v) \end{pmatrix}.$$

These components are quadratic polynomials and due to the structure of G_1, terms of the form $x_i y_j$, $x_i x'_j$, and $y_i y_j$ do not appear. Thus the matrices associated to the $\overline{G}_{1i}$ are all of the form

$$\begin{pmatrix} * & 0 & 0 \\ 0 & 0 & * \\ 0 & * & * \end{pmatrix} \text{ (the 0 and } * \text{ represent blocks)},$$

which does have $k^n \times \{(0, \ldots, 0)\} \subset k^{2n+v}$ as an invariant subspace. However, a similar analysis of G_2 and the analogous $\overline{G}_{2i}$ reveals that the matrices associated to these will be of the form

$$\begin{pmatrix} 0 & 0 & * \\ 0 & * & 0 \\ * & 0 & * \end{pmatrix},$$

with $\{(0, \ldots, 0)\} \times k^n \times \{(0, \ldots, 0)\} \subset k^{2n+v}$ as an invariant subspace. The public key polynomials' associated matrices are linear combinations of both types. So we cannot expect a common invariant subspace to exist.

4.2.3. Differential Attacks

Before looking at the differential of the core map, we note the following: for the univariate case, we were able to assume that the core polynomial G had no oil-vinegar cross terms, since the proposed core map is equivalent to such a map via a change of variables. This fact was crucial to the differential attack. But a change of variables cannot yield the same simplification in the bivariate case. The oil and vinegar variables are irrevocably intertwined.

Now let us take a closer look at the differentials of G_1 and G_2.

$$DG_1\big((X,Y,X_v),(A,B,A_v)\big) = 2AX + \beta_1(X_v)B + \beta_1(A_v)Y + D\gamma_1(X_v,A_v),$$

and

$$DG_2\big((X,Y,X_v),(A,B,A_v)\big) = 2BY + \beta_2(X_v)A + \beta_2(A_v)X + D\gamma_2(X_v,A_v).$$

This means that for $a, b \in K$, $c \in k$,

$$DG_1\big((aX,bY,cX_v),(A,B,A_v)\big) - DG_1\big((X,Y,X_v),(aA,bB,cA_v)\big) = (b-c)[\beta_1(A_v)Y - \beta_1(X_v)B,$$

and

$$DG_2\big((aX,bY,cX_v),(A,B,A_v)\big) - DG_2\big((X,Y,X_v),(aA,bB,cA_v)\big) = (a-c)[\beta_2(A_v)X - \beta_2(X_v)A.$$

The important point is that the right hand sides here are nonzero; they are precisely the differentials of the terms that mix oil and vinegar. Given this observation, it seems that an investigation of the differentials of the public key will not give an attacker information about field multiplications.

5. Conclusions

In this paper we describe two new signature schemes, Square-Vinegar with Embedding and 2-Square-Vinegar. For Square-Vinegar with Embedding, we show how signatures could be computed when an embedding is used, how the dangerous property of the related characteristic polynomials is destroyed, and how the threat of algebraic attacks can be managed by informed parameter choices. Similarly, for 2-Square-Vinegar, we give the construction and show that the scheme is secure against known attacks.

References

[1] J. Baena, C. Clough, and J. Ding, *Square-Vinegar Signature Scheme*, Proceedings of the 2nd International Workshop on Post-Quantum Cryptography - PQCrypto2008, Lecture Notes in Computer Science, Springer, 2008, pp. 17–30.

[2] Olivier Billet and Gilles Macario-Rat, *Cryptanalysis of the Square Cryptosystems*, ASIACRYPT, 2009, pp. 451–468.

[3] Nicolas T. Courtois, Magnus Daum, and Patrick Felke, *On the security of HFE, HFEv- and Quartz*, Public key cryptography—PKC 2003 (Berlin, Germany), vol. 2567, Lecture Notes in Comput. Sci., Springer, 2002, pp. 337–350.

[4] Jintai Ding, Dieter Schmidt, and Fabian Werner, *Algebraic Attack on HFE Revisited*, ISC Information Security, 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18, 2008. Proceedings (Tzong-Chen Wu, Chin-Laung Lei, Vincent Rijmen, and Der-Tsai Lee, eds.), Lecture Notes in Computer Science, vol. 5222, Springer, 2008, pp. 215–227.

[5] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern, *Practical Cryptanalysis of SFLASH*, CRYPTO, 2007, pp. 1–12.

[6] M. R. Garey, D. S. Johnson, et al., *Computers and Intractability: A Guide to the Theory of NP-completeness*, WH Freeman San Francisco, 1979.

[7] Aviad Kipnis and Adi Shamir, *Cryptanalysis of the Oil and Vinegar Signature Scheme*, Advances in Cryptology—CRYPTO '98 (Santa Barbara, CA, 1998), Lecture Notes in Comput. Sci., vol. 1462, Springer, Berlin, Germany, 1998, pp. 257–266.

[8] ———, *Cryptanalysis of the HFE Public key Cryptosystem by Relinearization*, Advances in Cryptology—CRYPTO '99 (Santa Barbara, CA), Lecture Notes in Comput. Sci., vol. 1666, Springer, Berlin, Germany, 1999, pp. 19–30.

[9] Jacques Patarin, *Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, Advances in Cryptology—EUROCRYPT 96 (Ueli Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 33–48.

[10] ———, *Oil and Vinegar Signature Scheme*, Dagstuhl Workshop on Cryptography (1997).

[11] Jacques Patarin, Nicolas Courtois, and Louis Goubin, *QUARTZ, 128-bit Long Digital Signatures*, Topics in cryptology—CT-RSA 2001 (San Francisco, CA), Lecture Notes in Comput. Sci., vol. 2020, Springer, Berlin, Germany, 2001, pp. 282–297.

[12] C. Wolf and B. Preneel, *Asymmetric Cryptography: Hidden Field Equations*, European Congress on Computational Methods in Applied Sciences and Engineering, 2004.

(Recibido en febrero de 2011. Aceptado en octubre de 2011)

Departamento de Matemáticas
Universidad Nacional de Colombia
Facultad de Ciencias
Calle 59A No 63-20 - Núcleo El Volador
Medellín, Colombia
e-mail: jbbaena@unal.edu.co

Department of Mathematical Sciences
Thomas More College
Crestview Hills, Kentucky, USA
e-mail: crystal.clough@gmail.com

Department of Mathematical Sciences
University of Cincinnati
839 Old Chem
Cincinnati, OH 45221, USA
e-mail: jintai.ding@uc.edu