Roots of Square: Cryptanalysis of Double-Layer Square and Square+

Full Version

Enrico Thomae, Christopher Wolf

Horst Görtz Institute for IT-security
Faculty of Mathematics
Ruhr-University of Bochum, 44780 Bochum, Germany
http://www.cits.rub.de/
{enrico.thomae, christopher.wolf}@rub.de, chris@christopher-wolf.de

Second Version: **2011-10-04**
First Version: **2011-08-10**

Abstract. Square is a multivariate quadratic encryption scheme proposed in 2009. It is a specialization of Hidden Field Equations by using only odd characteristic fields and also X^2 as its central map. In addition, it uses embedding to reduce the number of variables in the public key. However, the system was broken at Asiacrypt 2009 using a differential attack. At PQCrypto 2010 Clough and Ding proposed two new variants named *Double-Layer Square* and *Square+*. We show how to break Double-Layer Square using a refined *MinRank* attack in 2^{45} field operations. A similar fate awaits Square+ as it will be broken in 2^{32} field operations using a mixed MinRank attack over both the extension and the ground field. Both attacks recover the private key, given access to the public key. We also outline how possible variants such as *Square–* or *multi-Square* can be attacked.

Key words: Multivariate Cryptography, Algebraic Cryptanalysis, Square, Double-Layer Square, Square+, MinRank, Key Recovery

1 Introduction

In the world of Post-Quantum cryptography, $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key schemes have an important place. They were investigated as early as 1985 [16, 14] and have branched out into several systems.

In this article, we deal with the so-called *Square* system, which works both over a ground field $\mathbb{F}_q$ with q elements, as over an extension field $\mathbb{F}_{q^{n+\ell}}$. Its main feature is the operation X^2 over $\mathbb{F}_{q^{n+\ell}}$. Obviously, this is very simple to compute and invert—in particular when compared to the similar system Hidden Field Equations [17]. Inversion of X^2 utilizes the equation $X = \pm Y^{\frac{q^{n+\ell}+1}{4}}$. Hence, we need $q^{n+\ell} \equiv 3 \pmod 4$ and inverting $Y \in \mathbb{F}_q$ requires only one exponentiation in $\mathbb{F}_{q^{n+\ell}}$. Depending on the choice of q, n, the inversion is as efficient as for Sflash [10, 1].

Square itself was proposed 2009 in [7]. It was broken in the same year [4] using a differential attack. At PQCrypto 2010 Clough and Ding [9] proposed two new variants of Square, called *Double-Layer Square* and *Square+* which are claimed to be secure against all known attacks. We will outline below how they differ from the original Square scheme—but can be broken nevertheless.

One thing which has also developed with $\mathcal{MQ}$ schemes is their cryptanalysis. In this article, we will concentrate on attacks from the so-called MinRank family. Idea is to find a linear combination of some matrices, such that the new matrix has a special (minimal) rank. Or more formally: Given k matrices $M_1, \ldots, M_k \in \mathbb{F}_q^{n \times n}$ and a scalar $r \in \mathbb{N}$, find a vector $\lambda \in \mathbb{F}_q^k$ such that

$$\operatorname{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i\right) \leq r.$$

We call this an *MinRank(q, k, r)-problem.* Note that the *general* MinRank problem is NP-complete [5]. We will see later how $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes relate to matrices in general and to MinRank in particular.

A first MinRank attack in the $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic setting was launched against TTM [13]. Informally speaking, the authors exploited the existence of a so-called step-structure in the private key to reveal linear relations between the private and the public key. When enough of these relations were found, the whole private key could be unravelled. A similar approach was followed in [20]. Here, the step-width was made wider: Instead of allowing only rank differences of 1, rank differences up to r were allowed. Finally, [22] gave further ideas on discovering rank structure, in particular "crawling" attacks that exploit that areas of low rank might be close-by. A cryptanalysis of the Rainbow Signature Scheme using MinRank can be found in [3]. Our attack on Double-Layer Square (see sect. 3) will strongly refer to this paper.

Another algorithm to break MinRank-instances in practice is [12]. Here, Gröbner bases are used to actually calculate elements of the kernel and thus derive possible choices of $\lambda \in \mathbb{F}_q^k$. For some parameters this algorithm is much faster than sampling and therefore we use it in sect. 4 to break Square+.

1.1 Achievement and Organisation

In this paper, we describe an efficient cryptanalysis of the two public key schemes Double-Layer Square and Square+. We show how to break Double-Layer Square by a refined MinRank attack that is an extension of Billet and Gilbert [3] attack against Rainbow. The overall attack complexity is 2^{45}. Furthermore we break Square+ using methods from the cryptanalysis of odd characteristic HFE [2] and a MinRank attack [12]. In both cases, the attack is in polynomial time of (nearly) all parameters. In particular, the schemes are completely broken for all possible, practical choices of parameters.

In sect. 2, we introduce the Square cryptosystem and fix some notation. Double-Layer Square and its attack is discussed in sect. 3. We deal with Square+ and the corresponding MinRank problem in sect. 4. This paper concludes with sect. 5. There, we also outline possible extensions to Square– or multi-Square.

2 Notation

In this section we shortly recap the Square encryption scheme [7]. We start by giving some general outline on $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key systems and some notation.

Each $\mathcal{MQ}$-scheme uses a public $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with

$$\mathcal{P} := \begin{pmatrix} p^{(1)}(x_1, \ldots, x_n) \\ \vdots \\ p^{(m)}(x_1, \ldots, x_n) \end{pmatrix}$$

for $1 \leq k \leq m$ and

$$p^{(k)}(x_1, \ldots, x_n) := \sum_{1 \leq i \leq j \leq n} \gamma_{ij}^{(k)} x_i x_j$$

as public key. The trapdoor is given by a structured central map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with

$$\mathcal{F} := \begin{pmatrix} f^{(1)}(x_1, \ldots, x_n) \\ \vdots \\ f^{(m)}(x_1, \ldots, x_n) \end{pmatrix}$$

for $1 \leq k \leq m$ and

$$f^{(k)}(x_1, \ldots, x_n) := \sum_{1 \leq i \leq j \leq n} \tilde{\gamma}_{ij}^{(k)} x_i x_j.$$

In order to hide this trapdoor we choose two secret linear transformations $S \in \mathbb{F}_q^{n \times n}, T \in \mathbb{F}_q^{m \times m}$ and define $\mathcal{P} := T \circ \mathcal{F} \circ S$. Note that some proposals also use a linear and constant part of $p^{(k)}$ and $f^{(k)}$. However, as it is well known that quadratic terms only depend on quadratic terms from the secret map $\mathcal{F}$ and on linear terms from S, T, we can safely ignore the linear and constant parts in our cryptanalysis to ease explanation [19, 15, 3]. Where necessary, the affine case can be added easily.

Sometimes, as for Square, the trapdoor does not reveal itself over $\mathbb{F}_q^n$ but over the extension field $\mathbb{F}_{q^{n+\ell}}$. Let $\varphi : \mathbb{F}_q^{n+\ell} \to \mathbb{F}_{q^{n+\ell}}$ be the standard isomorphism between the vector space and the extension field and $\mathcal{F}' = \varphi \circ \mathcal{F} \circ \varphi^{-1}$. As outlined above, Square is defined for $q^{n+\ell} \equiv 3 \pmod 4$ and uses $\mathcal{F}' = X^2$ over $\mathbb{F}_{q^{n+\ell}}$. This can be easily inverted by the square root formula

$$X = \pm Y^{\frac{q^{n+\ell}+1}{4}}. \tag{1}$$

To make their scheme more resistant, the authors of Square have chosen S as a $(n + \ell) \times n$ matrix of rank n. This is equivalent to deleting ℓ variables from the secret map $\mathcal{F}$ in the public map $\mathcal{P}$. See figure 1 for an overall illustration of Square. The original parameters of the scheme are $n = 34, q = 31$ and $\ell = 3$ [7].

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}"] \arrow[d, "S"'] & \mathbb{F}_q^{n+\ell} \\
\mathbb{F}_q^{n+\ell} \arrow[r, "\mathcal{F}"] \arrow[d, "\varphi"'] & \mathbb{F}_q^{n+\ell} \arrow[u, "T"'] \\
\mathbb{F}_{q^{n+\ell}} \arrow[r, "\mathcal{F}'"] & \mathbb{F}_{q^{n+\ell}} \arrow[u, "\varphi^{-1}"']
\end{tikzcd}$$

Fig. 1. The Square Scheme.

In the sequel, we will make heavy use of the matrix representation of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic polynomials. As described above, we assume all polynomials $p^{(k)}$ and $f^{(k)}$ for $1 \leq k \leq n + \ell$ to be homogenized. As explained, we can do so as the linear and constant parts of the $p^{(k)}$ and $f^{(k)}$ do not carry any cryptographically relevant information. Let $\underline{x} = (x_1, \ldots, x_n)^\intercal$ respectively $\underline{\tilde{x}} = (\tilde{x}_1, \ldots, \tilde{x}_{n+\ell})^\intercal$ be a column vector and $\mathfrak{P}^{(k)} \in \mathbb{F}^{n \times n}$ respectively $\mathfrak{F}^{(k)} \in \mathbb{F}^{n+\ell \times n+\ell}$ the matrix describing the quadratic form of $p^{(k)} = \underline{x}^\intercal \mathfrak{P}^{(k)} \underline{x}$ respectively $f^{(k)} = \underline{\tilde{x}}^\intercal \mathfrak{F}^{(k)} \underline{\tilde{x}}$. We restrict to symmetric matrices (see figure 2). Using a minor twist, we can also represent univariate polynomials over the extension field $\mathbb{F}_{q^n}$ this way. By a slight abuse of notation, we obtain the same figure 2 for the univariate polynomial $P^{(k)}(X) = \sum\limits_{0 \leq i \leq j < n} \gamma_{i,j}^{(k)} X^{q^i + q^j}$ over the extension field $\mathbb{F}_{q^n}$ for $\underline{x} = (X, X^q, \ldots, X^{n-1})^\intercal$.

$$\mathfrak{P}^{(k)} = \begin{pmatrix} \gamma_{1,1}^{(k)} & \gamma_{1,2}^{(k)}/2 & \cdots & \cdots & \gamma_{1,n}^{(k)}/2 \\ \gamma_{1,2}^{(k)}/2 & \gamma_{2,2}^{(k)} & & & \gamma_{2,n}^{(k)}/2 \\ \vdots & \vdots & \ddots & & \vdots \\ \gamma_{1,n-1}^{(k)}/2 & \gamma_{2,n-1}^{(k)}/2 & & \gamma_{n-1,n-1}^{(k)} & \gamma_{n-1,n}^{(k)}/2 \\ \gamma_{1,n}^{(k)}/2 & \gamma_{2,n}^{(k)}/2 & \cdots & \gamma_{n-1,n}^{(k)}/2 & \gamma_{n,n}^{(k)} \end{pmatrix}$$

Fig. 2. Matrix representation $\mathfrak{P}^{(k)}$ of the public key polynomial $p^{(k)}$.

3 Double-Layer Square

Double-Layer Square as proposed in [9] uses the idea of Rainbow [11] to split the central map into two layers and thus destroy the differential properties in the public map that where used to break Square. The first layer is just the same mapping $\mathcal{F}$ as for Square. The second layer is defined by $\mathcal{G} : \mathbb{F}_q^{2n+\ell} \to \mathbb{F}_q^n$ with $\mathcal{G} = \varphi'^{-1} \circ G \circ (id \times \varphi')$ and $\varphi' : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ the standard isomorphism. It is explicitly given by

$$G((x_1,\ldots,x_{n+\ell}),X) = \alpha X^2 + \beta(x_1,\ldots,x_{n+\ell})X + \gamma(x_1,\ldots,x_{n+\ell}) \tag{2}$$

where $\alpha \in \mathbb{F}_{q^n}$, β is affine and γ is quadratic over $\mathbb{F}_{q^n}$. The whole central map over the vector space is thus given by

$$\mathcal{F}||\mathcal{G} = \begin{pmatrix} f^{(1)}(x_1,\ldots,x_{n+\ell}) \\ \vdots \\ f^{(n+\ell)}(x_1,\ldots,x_{n+\ell}) \\ g^{(1)}(x_1,\ldots,x_{2n+\ell}) \\ \vdots \\ g^{(n)}(x_1,\ldots,x_{2n+\ell}) \end{pmatrix}.$$

With $||$ we denote concatenation of two vectors and $g^{(i)} = x^\intercal \mathfrak{G}^{(i)} x$ with $\mathfrak{G}^{(i)} \in \mathbb{F}_q^{2n+\ell \times 2n+\ell}$. By construction, we have $\text{rank}(f^{(i)}) \leq n+\ell$ and $\text{rank}(g^{(i)}) \leq 2n+\ell$, cf. fig. 3 for the overall structure of the two layers. In order to invert the central map we first use the square root formula (1) to determine $x_1,\ldots,x_{n+\ell}$. This solution is plugged into (2) which is then solved, *e.g.* by the school book root finding for quadratic equations or by Berlekamp's algorithm. See fig. 4 for an illustration of the whole scheme.

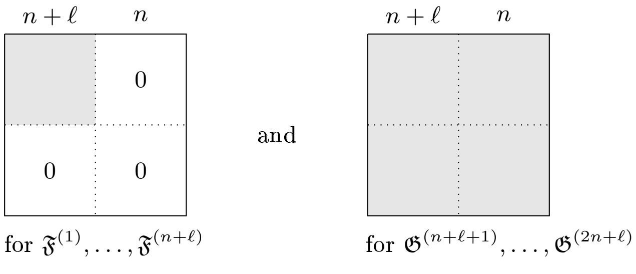
$n+\ell$
n
0
0
0
for $\mathfrak{F}^{(1)},\ldots,\mathfrak{F}^{(n+\ell)}$
and
$n+\ell$
n
for $\mathfrak{G}^{(n+\ell+1)},\ldots,\mathfrak{G}^{(2n+\ell)}$

Fig. 3. Central maps of Double-Layer Square.

$$\begin{tikzcd}
\mathbb{F}_q^{2n} \arrow[r, "\mathcal{P}"] \arrow[d, "S"'] & \mathbb{F}_q^{2n+\ell} \\
\mathbb{F}_q^{2n+\ell} \arrow[r, "\mathcal{F}||\mathcal{G}"] & \mathbb{F}_q^{2n+\ell} \arrow[u, "T"']
\end{tikzcd}$$

Fig. 4. The DoubleLayer Square Scheme. $||$ denotes concatenation of vectors.

3.1 MinRank attack against Double-Layer Square

In this section we adapt the MinRank attack of Billet and Gilbert [3] to Double-Layer Square. In order to reconstruct T we have to solve the problem of finding a linear combination $\sum_{i=1}^{2n+\ell} \lambda_i \mathfrak{P}^{(i)}$ for $\lambda_i \in \mathbb{F}_q$ with minimal rank. In general this is a difficult problem, as Buss *et al.* [5] showed that the decisional version of MinRank over $\mathbb{F}_q$ is NP-complete.

The idea of [3] to calculate a solution of the MinRank problem is to sample a vector $\omega \in_R \mathbb{F}_q^{2n}$ and hope that it lies in the kernel of a linear combination of low-rank matrices. If this is the case solving the linear system of equations

$$\sum_{i=1}^{2n+\ell} \lambda_i \mathfrak{P}^{(i)} \omega = 0 \text{ for } \omega \in_R \mathbb{F}_q^{2n}, \lambda_i \in \mathbb{F}_q, \mathfrak{P}^{(i)} \in \mathbb{F}_q^{2n \times 2n} \tag{3}$$

reveals a part of the secret transformation T. The crucial point is to calculate the probability over all ω that there exist values $\lambda_1, \ldots, \lambda_{n+\ell} \in \mathbb{F}_q$ such that

$$\omega \in \ker \left(\sum_{i=1}^{n+\ell} \lambda_i S^\intercal \mathfrak{F}^{(i)} S \right) . \tag{4}$$

For S being an $(2n+\ell) \times (2n+\ell)$ matrix of full rank and $\omega \in_R \mathbb{F}_q^{2n+\ell}$ this probability equals the likelihood of

$$S\omega \in \ker \left(\sum_{i=1}^{n+\ell} \lambda_i \mathfrak{F}^{(i)} \right) . \tag{5}$$

While the general idea is the same for Double-Layer Square, we need to be careful as S is a $(2n+\ell) \times 2n$ matrix of rank $2n$. We will tackle this problem after having calculated the probability that there exists $\lambda_i \in \mathbb{F}_q$ fulfilling (5).

It is well known that the probability of a random $(m \times n)$ matrix over $\mathbb{F}_q$ being regular is given by

$$\prod_{i=0}^{m-1} \left(1 - \frac{q^i}{q^n} \right) < 1 - \frac{1}{q^{n-m+1}} . \tag{6}$$

This implies that the probability of a random $(m \times n)$ matrix over $\mathbb{F}_q$ to be singular is bounded below by $1/(q^{n-m+1})$. In Fig. 5 we illustrate the coefficient matrix of the linear system

$$\left(\sum_{i=1}^{n+\ell} \lambda_i \mathfrak{F}^{(i)} + \sum_{i=n+\ell+1}^{2n+\ell} \lambda_i \mathfrak{G}^{(i)} \right) S\omega = 0 \tag{7}$$

for a random but fixed $\omega \in \mathbb{F}^{2n+\ell}$ and for $g^{(i)} = x^\intercal \mathfrak{G}^{(i)} x$ the associated matrix for a given secret polynomial $g^{(i)}$.

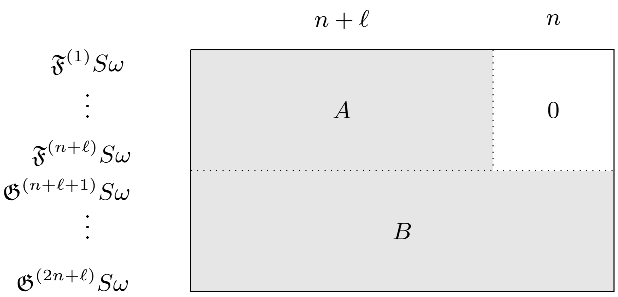
$n+\ell$
n
$\mathfrak{F}^{(1)}S\omega$
$\vdots$
$\mathfrak{F}^{(n+\ell)}S\omega$
$\mathfrak{G}^{(n+\ell+1)}S\omega$
$\vdots$
$\mathfrak{G}^{(2n+\ell)}S\omega$
A
0
B

Fig. 5. Coefficient matrix of linear system (7).

The probability that there exist $\lambda_1, \ldots, \lambda_{n+\ell} \in \mathbb{F}_q$ such that (5) holds is the probability of matrix A in figure 5 to be singular, *i.e.* $1/q$. Note that it is not enough for our attack that such a linear combination exists. In order to *efficiently* obtain this solution using (3) we also need the rank of the whole matrix from fig. 5 to be $\operatorname{rank}(A) + n$. This is true with overwhelming probability in our case. Otherwise we would obtain parasitic solutions by (3).

Up to this point, the overall complexity of the MinRank attack is

$$q(n+\ell)(2n+\ell)^3$$

as we expect to sample q vectors $\omega \in \mathbb{F}_q^{2n}$ until A becomes singular. We need to repeat this sampling until we have recovered $(n+\ell)$ linearly independent equations of small rank. Solving (3) requires Gaussian elimination in $(2n+\ell)$ variables.

Now we have to deal with the problem that S is not a $(2n+\ell) \times (2n+\ell)$ square matrix but a rectangular $(2n+\ell) \times 2n$ matrix. Obviously equation (4) and (5) are not equivalent any longer, but it holds

$$\sum_{i=1}^{n+\ell} \lambda_i \mathfrak{F}^{(i)} S\omega + \sum_{i=n+\ell+1}^{2n+\ell} \lambda_i \mathfrak{G}^{(i)} S\omega = 0 \Rightarrow \sum_{i=1}^{n+\ell} \lambda_i S^\intercal \mathfrak{F}^{(i)} S\omega + \sum_{i=n+\ell+1}^{2n+\ell} \lambda_i S^\intercal \mathfrak{G}^{(i)} S\omega = 0.$$

I.e. the probability of choosing ω in the kernel of low-rank matrices is still $1/q$. This argument hides a slight heuristic. If we choose $\omega \in_R \mathbb{F}_q^{2n}$, $S\omega$ is not a random element in $\mathbb{F}_q^{2n+\ell}$ any longer and thus the rows of the matrix in fig. 5 are not randomly chosen. Nevertheless they are independent and thus formula (6) should be a good approximation. Our experiments in table 1 confirm this. The backward direction is not true, as $2n+\ell$ vectors of lenght $2n$ are always linearly dependent and thus we obtain q^ℓ parasitic solutions. The overall attack cost is therefore

$$(n+\ell)q^{\ell+1}(2n+\ell)^3\,.$$

Unfortunately, the authors of [9] did not provide concrete security parameters. However, using their security analysis, we derived $q = 31, n = 17, \ell = 4$ for a claimed security level of 2^{80}. Using our attack, this reduces to 2^{45} to separate the upper from the lower level. We have broken this set of parameters in about 1 day, see Table 1. Moreover, we can ignore the embedding modifier, as explained in [2, Sect. 5]. In a nutshell, we work on the maximal rank of the corresponding matrices. However, the embedding modifier will only *decrease* the rank and hence not increase its maximum. Hence, the difference from fig. 3 still holds. Once we have separated these layers, the rest of the attack is equal to Billet/Macario-Rat [4], although we have to take the Double-Layer structure into account. First, we separate out the two layers $\mathfrak{F}$ and $\mathfrak{G}$. Using the algorithm of Billet/Macario-Rat, we can separate the variables of the $\mathfrak{F}$-layer into $x_1, \ldots, x_{n+\ell}$ (output of Billet/Macario-Rat) and $x_{n+\ell+1}, \ldots, x_{2n+\ell}$ (others). Using these, we have the variable mixing S,

Table 1. Time to recover the hidden vector space T for fixed field size $q = 31$, field extension $n = 17$ and variable embedding degree ℓ. The number of samples from the vector space ($\#\omega$) is independent from ℓ, but close to qn. Each line is based on 11 independent experiments. The line with previously secure parameters is **highlighted in bold**.

					time [sec]		
q	n	ℓ	$\#\omega$	$\#\omega/n$	min	avg	max
31	17	1	500	29.41	129	170	219
		2	460	27.06	210	268	375
		3	568	33.41	2416	3069	3903
		4	**567**	**33.35**	**55595**	**83334**	**126587**

the equation mixing T, and the inner layer X^2 for the *first layer* $\mathfrak{F}$. For the second, *i.e.* the $\mathfrak{G}$-layer, it is a bit more complicated as we are dealing with

$$\alpha X^2 + \beta(x_1, \ldots, x_{n+\ell})X + \gamma(x_1, \ldots, x_{n+\ell})\,.$$

here, so Billet/Macario-Rat does not apply directly. However, we see by inspection that all monomials depending on $x_1, \ldots, x_{n+\ell}$ come from the term γ, all monomials depending both on $x_1, \ldots, x_{n+\ell}$ and $x_{n+\ell+1}, \ldots, x_{2n+\ell}$ come from βX; and the rest comes from αX^2. Applying Billet/Macario-Rat to these gives us the complete variable change S and equation change T (up to equivalences, [21]). Hence, we have reconstructed the private key and are therefore in the same position as the legitimate user when computing $y = \mathcal{P}(x)$ for given $y \in \mathbb{F}_q^{2n+\ell}$.

3.2 Experimental Results

We have implemented attack in Sage [18]. In particular, we needed to verify if the probability computations for obtaining a separation into the two layers is correct. To this aim, we have implemented full Double-Layer Square, including embedding modifier and the layer structure.

Table 2. Time to recover the hidden vector space T for varying field size q, but fixed field extension $n = 17$ and embedding degree $\ell = 4$. The number of samples from the vector space ($\#\omega$) is independent from ℓ, but close to qn. Each line is based on 11 independent experiments. The line with previously secure parameters is **highlighted in bold**.

					time [sec]		
n	ℓ	q	$\#\omega$	$\#\omega/q$	min	avg	max
17	4	3	47	15.55	15	18	21
		5	85	17.04	35	53	62
		7	148	21.12	96	180	225
		11	230	20.89	717	963	1094
		13	244	18.74	1310	1730	2159
		17	319	18.76	4164	5590	6895
		19	385	20.26	7260	9941	14489
		23	448	19.47	16102	22734	27614
		29	577	19.89	45687	67172	93908
		31	**567**	**18.28**	**55595**	**83334**	**126587**

We have used the parameters derived from [9] and varied one of the three, *i.e.* the number of variables n, the embedding degree ℓ and the field size q. The results can be found in tables 1–3. In particular, we have verified that the relation $\#\omega = qn$ holds, *i.e.* if the number of samples only depends on q times the dimension of T. Except for small values of ℓ (cf. table 3), we have

Table 3. Time to recover the hidden vector space T for fixed field size $q = 31$, embedding degree ℓ, and variable field extension n. The number of samples from the vector space ($\#\omega$) is independent from ℓ, but close to qn. As the values for n are rather small, there were some parasitic solutions, *i.e.* more vectors ω needed to be sampled. Each line is based on 11 independent experiments.

					time [sec]		
q	ℓ	n	$\#\omega$	$\#\omega/n$	min	avg	max
31	4	7	305	43.52	20333	35763	51591
		8	409	51.07	30592	49048	72719
		9	388	43.08	27830	47124	79685
		10	471	47.15	38412	58527	77266
		11	408	37.05	35559	51443	63089

found a good correlation. However, as for small dimensions, the ranks become small, too, so we expect that a random matrix is far more likely to exhibit such a small rank. Hence, the number of parasitic solutions increases, too. The derived parameters of Double-Layer Square were broken in just under an hour on average (3100s $\approx$ 50min), cf. tables 2–3.
All computations were carried out on a Intel(R) Xeon(R) CPU X3350 with 2.66GHz, 4 cores, and 8GB physical RAM. For each tuple (q, n, ℓ), we have carried out 11 independent experiments. Each of them took up to 2 hours.

4 Square+

Another version of the Square cryptosystem is called Square+. It was also suggested in the very same paper as Double-Layer Square by Clough and Ding [9]. As Square, it uses X^2 over the extension field $\mathbb{F}_{q^{n+\ell}}$ as its central monomial. In addition, we have $p \in \mathbb{N}$ random equations that blind the differential structure of X^2 in the public key. In total, we obtain $m := n + \ell + p$ equations for Square+. Obviously, Square+ is overdetermined—both due to the embedding of ℓ variables and the p extra polynomials. In order to prevent Gröbner based attacks, $(\ell + p)$ has to be chosen relatively small compared to n. In the original Square+ paper, proposed parameters are $q = 31, n = 48, \ell = 3, p = 5$ [9].
Let $\varphi : \mathbb{F}_q^{n+\ell} \to \mathbb{F}_{q^{n+\ell}}$ be the standard isomorphism between the vector space $\mathbb{F}_q^{n+\ell}$ and the finite field $\mathbb{F}_{q^{n+\ell}}$. Denote with $a_1, \ldots, a_p$ a total of p random, quadratic polynomials over $\mathbb{F}_q$, the so-called *plus-polynomials*. The mixing of the equations is realized by a full-rank matrix $T \in \mathbb{F}_q^{(n+\ell+p)\times(n+\ell+p)}$. The embedding modifier is realized via a matrix $S \in \mathbb{F}_q^{(n+\ell)\times n}$ with $\operatorname{rank}(S) = n$. The Square part is expressed over the ground field as $\mathcal{C}$, the plus polynomials are given in $\mathcal{A}$, see

$$\begin{aligned}
\mathcal{C} : \mathbb{F}^{n+\ell} \to \mathbb{F}^{n+\ell} : (u_1, \ldots, u_{n+\ell}) &\to \varphi^{-1} \circ X^2 \circ \varphi(u_1, \ldots, u_{n+\ell}) \\
&= (v_1, \ldots, v_{n+\ell}), \\
\mathcal{A} : \mathbb{F}^{n+\ell} \to \mathbb{F}^{p} : (u_1, \ldots, u_{n+\ell}) &\to (a_1(u_1, \ldots, u_{n+\ell}), \ldots, a_p(u_1, \ldots, u_{n+\ell})) \\
&= (v_{n+\ell+1}, \ldots, v_{n+\ell+p})
\end{aligned}$$

Now we can write the public key $\mathcal{P}$ of Square+ as $\mathcal{P} := T \circ (\mathcal{C} \circ S, \mathcal{A} \circ S)$. See figure 6 for a graphical representation. Note that all intermediate operations are quadratic over $\mathbb{F}_q$, as is $\mathcal{P}$. If we leave out the embedding modifier for a moment (transformation S), there are two parts of Square+, namely the invertible, but "soft" part X^2, represented by transformation $\mathcal{C}$, and the not-invertible "hard" part $a_1, \ldots, a_p$, represented by transformation $\mathcal{A}$. If we manage to separate them, we are done as there is an efficient attack against Square [2].

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}"] \arrow[d, "S"'] & \mathbb{F}_q^{n+\ell+p} \\
\mathbb{F}_q^{n+\ell} \arrow[r, "\mathcal{C} \parallel \mathcal{A}"] & \mathbb{F}_q^{n+\ell+p} \arrow[u, "T"']
\end{tikzcd}$$

Fig. 6. The Double-Layer Square Scheme.

4.1 Odd-Characteristic HFE Attack against Square+

To this aim, we have a closer look at "odd Characteristic HFE" (or odd-HFE) and its cryptanalysis [6, 2]. In particular we notice that the central map of odd-HFE is

$$\sum_{(i,j)\in\Delta(D)} \gamma_{i,j} X^{q^i+q^j}$$

for a set of admissible degrees $\Delta(D) := \{(i,j) \in \mathbb{N}^2 : i \leq j, q^i + q^j \leq D\}$, $\mathbb{N}$ the set of non-negative integers and $\gamma_{i,j} \in \mathbb{F}_{q^n}$ the coefficients of the corresponding private key. Setting $D = 2$ and $\gamma_{(0,0)} = 1$, we obtain $\Delta(2) = (0,0)$ and the central map of odd-HFE coincides with the one of Square+. As a result, we can apply the cryptanalysis of Bettale *et al.* [2] against odd-HFE also against Square+. Alas, this cryptanalysis does not include the case odd-HFE+, so we need to investigate this question closely to determine if we can break Square+ within this framework. As we will see below, it works but there are subtle changes to be made.

As for the original attack against odd-HFE, the key point is the observation that we can write X^2 as a matrix of small rank over the *extension* field. More to the point, we have $X^2 = \underline{x}^\intercal \mathfrak{F} \underline{x}$ over $\mathbb{F}_{q^{n+\ell}}$ for $\underline{x} = (X, X^q, X^{q^2}, \ldots, X^{q^{n-1}})^\intercal$ with $\mathfrak{F}_{1,1} = 1$ but $\mathfrak{F}_{i,j} = 0$ otherwise. As only $\mathfrak{F}_{1,1}$ is non-zero, we obviously have $\operatorname{rank}(\mathfrak{F}) = 1$. A similar observation for a MinRank attack against HFE was already used by Kipnis-Shamir [15]. Note that expressing X^2 over the ground field yields a much higher rank, in practice close to $(n+\ell)$.

To ease notation and to mount the attack, we follow the approach of [2] and start with the vector $(\theta_1, \ldots, \theta_{n+\ell}) \in \mathbb{F}_{q^{n+\ell}}^{n+\ell}$. Note that this vector has a double function: First, it fixes a basis of the vector space $\mathbb{F}_q^{n+\ell}$, *i.e.* over the ground field, and second, the elements $\theta_1, \ldots, \theta_{n+\ell}$ are simultaneously interpreted over the extension field $\mathbb{F}_{q^{n+\ell}}$. This way we can apply the homomorphism $\mathbb{F}_{q^{n+\ell}} \to \mathbb{F}_{q^{n+\ell}} : x \mapsto x^{q^k}$ for $k = 0, \ldots, (n+\ell-1)$ within the extension field. Finally, this is used to construct a matrix $M_{n+\ell}$.

$$M_{n+\ell} := \begin{pmatrix} \theta_1 & \theta_1^q & \ldots \theta_1^{q^{n+\ell-1}} \\ \theta_2 & \theta_2^q & \ldots \theta_2^{q^{n+\ell-1}} \\ \vdots & & \ddots \quad \vdots \\ \theta_{n+\ell} & \theta_{n+\ell}^q & \ldots \theta_{n+\ell}^{q^{n+\ell-1}} \end{pmatrix}$$

More precisely, for a vector $v := (v_1, \ldots, v_{n+l}) \in \mathbb{F}_q^{n+\ell}$ we have the mapping $\phi : \mathbb{F}_q^{n+\ell} \mapsto \mathbb{F}_{q^{n+\ell}}$ with

$$\phi(v) \mapsto V_1 : (v_1, \ldots, v_{n+\ell}) M_{n+\ell} =: (V_1, \ldots, V_{n+\ell}) .$$

Note that this mapping only uses the first component of the vector $(V_1, \ldots, V_{n+\ell})$. Moreover, the first column of $M_{n+\ell}$ consists only of base elements of $\mathbb{F}_q^{n+\ell}$. Hence, two values $V_1, \tilde{V_1} \in \mathbb{F}_{q^n}$ will only be equal if the corresponding vectors $v, \tilde{v} \in \mathbb{F}_q^n$ are the same. The inverse mapping needs to make use of the special structure of the matrix $M_{n+\ell}$ to map elements back into the ground field. We have $\phi^{-1} : \mathbb{F}_{q^{n+\ell}} \mapsto \mathbb{F}_q^{n+\ell}$ for

$$\phi^{-1}(V) \mapsto (v_1, \dots, v_{n+\ell}) : (V, V^q, \dots, V^{q^{n+\ell-1}})M_{n+\ell}^{-1} =: (v_1, \dots, v_{n+\ell})\,.$$

Using the matrix $M_{n+\ell}$, we can now go back and forth between the two vector spaces $\mathbb{F}_q^{n+\ell}$ (ground field) and $\mathbb{F}_{q^{n+\ell}}^{n+\ell}$ (extension field). The latter is a very redundant version of the former as we could use any component of the vector $\underline{V} = (V, V^q, \dots, V^{q^{n+\ell-1}})$ to reconstruct all other $(n+\ell-1)$ elements. However, we will see below how it will help us to express the rank condition on $\mathfrak{F}$ using only publicly available information.

There are two minor ingredients missing before we can formulate the full attack. The first is the quadratic form of the plus polynomials $a_1, \dots, a_p$. As for Double-Layer Square, we write them as symmetric matrices $A^{(i)} \in \mathbb{F}_q^{(n+\ell)\times(n+\ell)}$ with $x = (x_1, \dots, x_{n+\ell})$ and $a_i = \underline{x}A^{(i)}\underline{x}^\intercal$ for $1 \le i \le p$. Hence, we work over the ground field here. Second, we define matrices $\mathfrak{F}^{(i)} \in \mathbb{F}_{q^{n+\ell}}^{(n+\ell)\times(n+\ell)}$ similar to $\mathfrak{F}$ from above as $\mathfrak{F}^{(i)}_{k,k} := 1$ but $\mathfrak{F}^{(i)}_{a,b} = 0$ for $k := (1-i) \pmod{n+\ell} + 1$, $1 \le a, b \le k$. Or to rephrase this, we have the all-zero matrix with the a single 1, the matrix $\mathfrak{F}^{(1)}$ coincides with the originally defined matrix $\mathcal{F}$, and the 1 is traveling backwards on the main diagonal for each consecutive matrix $\mathfrak{F}^{(i)}$. Note that evaluating $M_{n+\ell}\mathfrak{F}^{(k)}M_{n+\ell}^\intercal$ yields exactly X^2 for each matrix $\mathfrak{F}^{(k)}$.

We now express the private key in terms of $S, T, A, \mathfrak{F}$ and study their corresponding ranks

$$\begin{aligned} P &= T \circ F \circ S \\ &= (\mathcal{C} \circ S, \mathcal{A} \circ S)T \end{aligned}$$

Replacing P on the left hand side with the public key matrices $\mathfrak{P}^{(k)}$ for $1 \le k \le (n+\ell+p)$, plugging in the definitions of $\mathcal{C}, \mathcal{A}$, and bringing the matrix T to the left we obtain

$$\begin{aligned} (\mathfrak{P}^{(1)}, \dots, \mathfrak{P}^{(n+\ell+p)})T^{-1} = [&(SM_{n+\ell}\mathfrak{F}^{(1)}M_{n+\ell}^\intercal S^\intercal, \dots, SM_{n+\ell}\mathfrak{F}^{(n+\ell)}M_{n+\ell}^\intercal S^\intercal)M_{n+\ell}^{-1} \\ &||(SA^{(1)}S^\intercal, \dots, SA^{(p)}S^\intercal)] \end{aligned}$$

Again, "||" denotes the concatenation of vectors. Note that the *overall* equation is over the ground field $\mathbb{F}_q$, while the matrices $\mathfrak{F}^{(i)}$ are over the extension field $\mathbb{F}_q^{n+\ell}$. There are two important remarks to be made: First, the matrices $A^{(i)}$ are with overwhelming probability of high rank, both over the ground field and the extension field $\mathbb{F}_{q^{n+\ell}}$. In contrast, each column $SM_{n+\ell}\mathfrak{F}^{(1)}M_{n+\ell}^\intercal S^\intercal$ has at most rank 1 over the extension field $\mathbb{F}_{q^{n+\ell}}$. Note that the embedding modifier does *not* change the latter rank property as the rank will only decrease, not increase by the embedding modifier, cf. [2, Sect. 5] for a more detailed explanation of this fact. Second, we are only interested in separating out the first $(n+\ell)$ columns of the right hand side from the last p ones. So we do not look for the full matrix T^{-1}, but only its first $(n+\ell)$ columns. We denote them by $\tilde{T} \in \mathbb{F}_q^{(n+\ell+p)\times(n+\ell)}$ and have rank $n+\ell$. Combining these two observations, our equation simplifies to

$$(\mathfrak{P}^{(1)}, \dots, \mathfrak{P}^{(n+\ell+p)})\tilde{T}M_{n+\ell} = (SM_{n+\ell}\mathfrak{F}^{(1)}M_{n+\ell}^\intercal S^\intercal, \dots, SM_{n+\ell}\mathfrak{F}^{(n+\ell)}M_{n+\ell}^\intercal S^\intercal)$$

Note that the *whole* equation is now over the extension field while the coefficients of the matrices $\mathfrak{P}^{(i)}$ come from the ground field. For simplicity, write $U := \tilde{T}M_{n+\ell}$. By construction of $M_{n+\ell}$ we have $u_{i,j} = u_{i,j-1}^q$ and $u_{i,1} = u_{i,n+\ell}^q$ for $1 \le i \le n+\ell, 1 < j \le n+\ell$, so the knowledge of *one* column of U is enough to determine the whole matrix. Hence we only concentrate on the first column of U and obtain

$$\sum_{i=1}^{n+\ell+p} \mathfrak{P}^{(i)} u_{i,1} = S M_{n+\ell} \mathfrak{F}^{(1)} M_{n+\ell}^{\intercal} S^{\intercal} =: H \text{ with } H \in \mathbb{F}_{q^{n+\ell}}^{n \times n}$$

for unknown S. As our final equation is over $\mathbb{F}_q^{n+\ell}$ we clearly have $\operatorname{rank}(H) \leq 1$ and can thus use a similar technique as in section 3 to determine values $\lambda_i \in \mathbb{F}_{q^{n+\ell}}$ such that

$$\operatorname{rank}(\sum_{i=1}^{n+\ell+p} \lambda_i \mathfrak{P}^{(i)}) \leq 1$$

by solving the corresponding MinRank$(q, n+\ell+p, 1)$ problem, *i.e.* for rank $r = 1$.

Table 4. Time to solve the MinRank problem for Square+ for varying embedding degree ℓ, but fixed field size $q = 31$, field extension $n = 17$, and plus equations $p = 5$. Each line is based on 11 independent experiments. We see that the running time does not depend on the embedding degree ℓ.

					time [sec]	
q	n	p	ℓ	min	avg	max
31	17	5	0	1590.59	1610.13	1630.91
			1	1580.85	1605.42	1624.17
			2	1563.80	1600.54	1616.89
			3	1587.97	1603.67	1628.78
			4	1557.96	1604.47	1626.03
			5	1567.56	1610.80	1636.44
			6	1584.20	1606.61	1622.34
			7	1573.56	1604.07	1621.94
			8	1583.91	1609.04	1629.97
			9	1575.46	1603.57	1624.08
			10	1565.71	1597.58	1618.23

4.2 Solving MinRank for Square+

All in all, there are two methods available. The first is credited to Schnorr and works on determinants for $(r+1) \times (r+1)$ submatrices while the other was developed by Levy-dit-Vehel *et al.* [12] and uses Gröbner bases.

We start with Schorr's method. It uses the following observation: For given rank r, each submatrix of size $(r+1) \times (r+1)$ must have determinant zero. Hence, each such determinant gives rise to one equation of degree $(r+1)$. For a $(\tau \times \tau)$-matrix, we can form $\binom{\tau}{r+1}^2$ sub-matrices (selecting $r+1$ rows and columns, respectively) and hence equations. Assuming that a sufficiently high proportion of them is linearly independent, we are able to solve the corresponding system of equations by linearization. In our case, we have $r = 1$ and $\tau := (n+\ell+p)$ free variables, leading to a total of $\binom{n+\ell+p}{2}$ degree 2 monomials. For $\ell + p < n$, this allows to compute a solution in $\binom{n+\ell+p}{2}^3 \in O(n^6)$ computations over $\mathbb{F}_{q^{n+\ell}}$ and is hence polynomial in all security parameters. For the proposed parameters $n = 48, \ell = 3, p = 5$ we obtain a total workload of $\approx 2^{31.77}$ and have hence broken the scheme.

For the second method, we inspect the kernel of the matrix H. Remember that each kernel element $\omega \in \mathbb{F}_{q^{n+\ell}}^n$ has the form $\omega := S M_{n+\ell}(0, \tilde{\omega}_2, \ldots, \tilde{\omega}_{n+\ell})$ for $\tilde{\omega}_i \in \mathbb{F}_{q^{n+\ell}}$ and $2 \leq i \leq (n+\ell)$.

Table 5. Time to solve the MinRank problem for Square+ for varying extension degree n, but fixed field size $q = 31$, embedding degree $\ell = 3$ and plus equations $p = 5$. Each line is based on 11 independent experiments. We see that the running time increses with n, but that this increase is polynomial in n.

				time [sec]		
q	ℓ	p	n	min	avg	max
31	3	5	6	17.51	19.42	22.28
			7	35.67	37.73	39.06
			8	62.21	64.72	67.94
			9	100.10	103.84	106.66
			10	157.60	160.98	164.36
			11	223.90	229.27	234.75
			12	353.21	359.82	365.34
			13	456.14	464.08	472.65
			14	693.66	701.91	709.00
			15	943.38	949.51	958.05
			16	1279.68	1288.73	1302.35
			17	1601.64	1616.49	1631.36
			18	2291.12	2305.78	2329.30
			19	2666.34	2722.55	2752.76
			20	3922.29	3955.14	3980.28
			21	5071.11	5286.55	6969.38
			22	6387.73	6469.96	6513.20
			23	6915.21	6983.90	7085.33
			24	10037.24	11676.78	18159.85
			25	11054.98	11180.87	11254.37
			26	15264.25	15430.23	15528.12

So randomly sampling vectors $\omega \in_R \mathbb{F}^n_{q^{n+\ell}}$ needs $q^{n+\ell}$ trials on average to find a kernel element of H and is hence exponential in the security parameters n, ℓ. It is also impractical for the proposed parameters. Thus we use the more refined technique from Levy-dit-Vehel *et al.* [12] to solve instances of the MinRank problem. In a nutshell, they do not sample vectors ω but *calculate* them. This is done by generating an overdetermined $\mathcal{MQ}$-system and then solving it with Gröbner base techniques. Note that the attack complexity grows exponentially with the rank of the target matrix. However, as this rank is fixed to 1 in our case, we are not concerned by this.

The dimension of the kernel of H is $(n-1)$ in the extension field and thus we can fix all but one coefficient of ω at random and still expect a solution. The corresponding vector therefore becomes $(\omega_1, \ldots, \omega_{n-1}, x)$ with $\omega_i \in \mathbb{F}_{q^{n+\ell}}$ fixed values and x a free variable living over the extension field $\mathbb{F}_{q^{n+\ell}}$. Using this notation, we can formulate the following system of quadratic equations over the vector space $\mathbb{F}^n_{q^{n+\ell}}$:

$$\left(\sum_{i=1}^{n+\ell+p} \lambda_i \mathfrak{P}^{(i)}\right) \omega = 0^n$$

For rank 1, we can sample a total of $(n-1)$ linearly independent values $\omega^{(1)}, \ldots, \omega^{(n-1)}$ from the kernel and hence obtain $(n-1)n$ linearly independent equations in a total of $(n-1)+(n+\ell+p) = 2n+\ell+p-1$ unknowns. According to [12], we expect an overall complexity of $\binom{N+r+1}{r+2}^3$ for N the number of unknowns. For the proposed parameters $n = 48, \ell = 3, p = 5$ we obtain a workload of $\binom{2n+\ell+p+1}{3}^3 \approx 2^{52.55}$. This is clearly worse than Schnorr's method. However, the Gröbner method can exploit computing all intermediate steps in the ground field, so the authors of [2] report a substantial speed-up here. Moreover, for variations of Square+, we might be able to formulate side-conditions easier than for Schnorr's method.

Table 6. Time to solve the MinRank problem for Square+ for varying number of plus polynomials p, but fixed field size $q = 31$, extension degree $n = 17$, and embedding degree $\ell = 3$. Each line is based on 11 independent experiments. We see that the running time increses with p, but that this increase is polynomial in p.

				time [sec]		
q	n	ℓ	p	min	avg	max
31	17	3	1	445.00	463.68	486.29
			2	673.89	691.55	710.60
			3	922.74	953.12	969.35
			4	1252.06	1271.33	1304.54
			5	1645.86	1664.79	1682.80
			6	2133.76	2152.02	2180.77
			7	2723.46	2752.11	2769.51
			8	3437.09	3480.57	3516.38
			9	4344.27	4371.97	4422.50
			10	5374.37	5409.62	5455.11

Table 7. Time to solve the MinRank problem for Square+ for varying size of the ground field q, but fixed extension degree $n = 17$, embedding degree $\ell = 3$, and plus polynomials $p = 5$. Each line is based on 11 independent experiments. We see that the running time increses with p, but that this increase is polynomial in p.

				time [sec]		
n	ℓ	p	q	min	avg	max
17	3	5	5	1620.20	1632.99	1647.49
			7	1623.13	1644.97	1667.52
			11	1656.97	1672.01	1696.61
			13	1676.45	1697.23	1712.70
			29	1666.75	1685.57	1712.05
			31	1650.53	1682.56	1714.89
			37	1646.03	1669.35	1711.87
			41	1663.81	1680.39	1700.42
			127	1617.03	1628.94	1644.85
			131	1625.35	1641.86	1655.91
			251	1614.91	1637.76	1670.60
			257	1615.56	1633.81	1655.00

Executing either the algorithm of Schnorr or of Levi-dit-Vehel *et al.*, we can reconstruct the initial Square system and are in the same position as a legitimate user.

We have implemented the attack of Schnorr and found the theory in line with the practical experiments. In particular, the matrices $\mathfrak{F}^{(i)}$ for $1 \leq i \leq (n + \ell)$ have rank 1 over the extension field and we can reconstruct the matrix H for public key matrices $\mathfrak{P}^{(k)}$ for $1 \leq k \leq (n + \ell + p)$ alone. As for our experiments with Double-Layer Square, we used Sage [18] on a Intel(R) Xeon(R) CPU X3350 with 2.66GHz, 4 cores, and 8GB physical RAM. Moreover, as shown in tables 4–7, no parameter has exponential influence on the running time of the key recovery algorithm.

When implementing the attack a slight problem was memory consumption as Sage proved to be rather inefficient here. Hence, we could not break the proposed parameters although they should be in reach for a memory optimized version of the attack.

5 Conclusion

In this paper we have presented the first cryptanalysis of the two twin schemes Double-Layer Square and Square+. Both attacks relied heavily on the rank properties of the public key equations over the ground field (Double-Layer) or the extension field (Square+). In either case, each scheme is fully broken for any reasonable choice of parameters: For Double-Layer Square, the attack is exponential in the security parameter ℓ. However, as $\ell = 4$ and cannot be increased too much due to generic attacks against $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes, it is efficient in practice. For Square+, the attack is fully polynomial in all security parameters q, ℓ, p.

Table 8. Summary of the complexity of the attacks given in this paper. In both cases, we measure the number of computations over the corresponding field with q being the size of the ground field, n an intermediate extension degree, and ℓ the embedding degree.

Algorithm	Attack	Complexity	over
Double-Layer Square	Key Recovery	$(n+\ell)q^{\ell+1}(2n+\ell)^3$	$\mathbb{F}_q$
Square+	Key Recovery	$\binom{n+\ell+p}{2}^3$	$\mathbb{F}_{q^{n+\ell}}$

As we have established a strong link between odd characteristic Hidden Field Equations and Square, we know that any cryptanalytic result for the former can be exploited for the latter. So the relation between Square and odd-HFE is the same as for MIA/C* and HFE. All attacks to the latter (odd-HFE, HFE) will inevitable apply to the former (Square, MIA/C*). Hence, any strategy to repair Square will need to take these similarities into account. In addition, we have to remember that Square will always be much weaker than odd-HFE—for reasons similar to the pair MIA/C* and HFE. Moreover, we expect that any successful cryptanalysis of odd-HFE can be turned easily in a cryptanalysis of Square—maybe even *without* any further modification. For example, transferring Square to the equivalent of “multi-HFE” [6] does not seem to be a good idea. It was already established that this variant actually leads to a *weaker* version of the original odd-HFE. Similarly, we can conclude that Square- is broken, as is MIA-. Both variations were suggested in [8], the first as “bivariate Square", the other as Square-. On the other hand, a secure version of Square will most certainly give rise to a secure version of MIA.
In particular, Square has exactly the same big advantage over odd-HFE that MIA/C* has over HFE: *Speed.* When it comes to signing/decrypting, both will outperform the more secure variants by orders of magnitudes. Hence, it seems to be too early to call the overall game “Square” being over but it seems a fair guess that some further modifications will be tried. If they will stand the test of time is a different question altogether.

Acknowledgments

We want to thank Gottfried Herold (Bochum) for fruitful discussions and helpful remarks. Furthermore we thank the reviewers for helpful comments.
The authors were supported by the German Science Foundation (DFG) through an Emmy Noether grant where the second author is principal investigator. All authors were in part supported by the European Commission through the IST Programme under contract *ICT-2007-216676 Ecrypt II.*

Bibliography

[1] M.-L. Akkar, N. T. Courtois, R. Duteuil, and L. Goubin. A fast and secure implementation of SFlash. In *Public Key Cryptography — PKC 2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 267–278. Y. Desmedt, editor, Springer, 2002.

[2] L. Bettale, J.-C. Faugère, and L. Perret. Cryptanalysis of multivariate and odd-characteristic hfe variants. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 441–458. Springer, 2011.

[3] O. Billet and H. Gilbert. Cryptanalysis of rainbow. In *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 336–347. Springer, 2006.

[4] O. Billet and G. Macario-Rat. Cryptanalysis of the square cryptosystems. In M. Matsui, editor, *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 451–468. Springer, 2009.

[5] J. F. Buss, G. S. Frandsen, and J. O. Shallit. The computational complexity of some problems of linear algebra. Research Series RS-96-33, BRICS, Department of Computer Science, University of Aarhus, Sept. 1996. `http://www.brics.dk/RS/96/33/`, 39 pages.

[6] C.-H. O. Chen, M.-S. Chen, J. Ding, F. Werner, and B.-Y. Yang. Odd-char multivariate hidden field equations. Cryptology ePrint Archive, Report 2008/543, 2008. `http://eprint.iacr.org/`.

[7] C. Clough, J. Baena, J. Ding, B.-Y. Yang, and M.-S. Chen. Square, a new multivariate encryption scheme. In *Proceedings of the The Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology*, CT-RSA '09, pages 252–264, Berlin, Heidelberg, 2009. Springer-Verlag.

[8] C. L. Clough. *Square: A New Family of Multivariate Encryption Schemes.* PhD thesis, University of Cincinnati, 2009.

[9] C. L. Clough and J. Ding. Secure variants of the square encryption scheme. In N. Sendrier, editor, *PQCrypto*, volume 6061 of *Lecture Notes in Computer Science*, pages 153–164. Springer, 2010.

[10] N. Courtois, L. Goubin, and J. Patarin. *Sflash: Primitive specification (second revised version)*, 2002. `https://www.cosic.esat.kuleuven.be/nessie`, Submissions, Sflash, 11 pages.

[11] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *Conference on Applied Cryptography and Network Security — ACNS 2005*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175. Springer, 2005.

[12] J.-C. Faugère, F. L. dit Vehel, and L. Perret. Cryptanalysis of minrank. In D. Wagner, editor, *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 280–296. Springer, 2008.

[13] L. Goubin and N. T. Courtois. Cryptanalysis of the TTM cryptosystem. In *Advances in Cryptology — ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 44–57. Tatsuaki Okamoto, editor, Springer, 2000.

[14] H. Imai and T. Matsumoto. Algebraic methods for constructing asymmetric cryptosystems. In *Algebraic Algorithms and Error-Correcting Codes, 3rd International Conference, AAECC-3, Grenoble, France, July 15-19, 1985, Proceedings*, volume 229 of *Lecture Notes in Computer Science*, pages 108–119. Jacques Calmet, editor, Springer, 1985.

[15] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem. In *Advances in Cryptology — CRYPTO 1999*, volume 1666 of *Lecture Notes in Computer Science*, pages

19–30. Michael Wiener, editor, Springer, 1999. http://www.minrank.org/hfesubreg.ps or http://citeseer.nj.nec.com/kipnis99cryptanalysis.html.

[16] T. Matsumoto, H. Imai, H. Harashima, and H. Miyakawa. A cryptographically useful theorem on the connection between uni and multivariate polynomials. *Transactions of the IECE of Japan*, 68(3):139–146, Mar. 1985.

[17] J. Patarin. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology — EUROCRYPT 1996*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Ueli Maurer, editor, Springer, 1996. Extended Version: http://www.minrank.org/hfe.pdf.

[18] W. Stein et al. *Sage Mathematics Software (Version 4.6).* The Sage Development Team, 2010. http://www.sagemath.org.

[19] C. Wolf, A. Braeken, and B. Preneel. Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC. In *Conference on Security in Communication Networks — SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 294–309. Springer, Sept. 8–10 2004. Extended version: http://eprint.iacr.org/2004/237.

[20] C. Wolf, A. Braeken, and B. Preneel. On the security of stepwise triangular systems. *Designes, Codes and Cryptography*, 40(3), 2006. 285–302.

[21] C. Wolf and B. Preneel. Equivalent keys in multivariate quadratic public key systems. *Journal of Mathematical Cryptology*, 4(4):375–415, 2011.

[22] B.-Y. Yang and J.-M. Chen. Rank attacks and defence in Tame-like multivariate PKC's. Cryptology ePrint Archive, Report 2004/061, 29$^{\text{rd}}$ September 2004. http://eprint.iacr.org/, 21 pages.