Secure Variants of the Square Encryption Scheme

Crystal Lee Clough[1] and Jintai Ding[2,3]

[1] Nanyang Technological University, Singapore
clclough@ntu.edu.sg
[2] University of Cincinnati, Cincinnati, OH USA
[3] Southern Chinese University of Technology

Abstract. This paper discusses two encryption schemes to fix the Square scheme. Square+ uses the Plus modification of appending randomly chosen polynomials. Double-Layer Square uses a construction similar to some signature schemes, splitting the variables into two layers, one of which depends on the other.

1 Introduction

Multivariate public-key cryptosystems (MPKCs) are thought to be one of the options for cryptography in a post-quantum setting. Some secure MPKC encryption schmes exist but they are slow and unwieldy in comparison with multivariate signature schemes. There is room for improvement in the realm of MPKCs.

In this paper we will show some new encryption schemes based on Square. The original Square system was broken via a differential attack and we show two different ways to thwart this attack. Square+ is a minor reformulation which differs from Square only by the addition of a few extra polynomials. Double-Layer Square is a more structural renovation, using layers of variables much like the Rainbow and Square-Vinegar signature schemes [1,7]. We make the case that both of these new options are secure against known attacks.

This paper is organized as follows: in Section 2 we describe the Square and HFE cryptosystems and attacks on them, in Section 3 we describe and analyze Square+, in Section 4 we describe and analyze Double-Layer Square, and we conclude in Section 5.

2 Background

The Square system and the variants of it that we will introduce here can be seen as a natural evolution of a sequence of MPKC schemes. Though not the first in this vein[1], the HFE (Hidden Field Equations) system of Patarin is a good starting point for this discussion because it is very general and also extensively analyzed (e.g., [4,8,9,11,12,13,16]).

[1] For example, the C^* scheme of Matsumoto and Imai [14] predates HFE by about 8 years.

N. Sendrier (Ed.): PQCrypto 2010, LNCS 6061, pp. 153–164, 2010.

2.1 HFE

Let k a field of size q and K a degree-n extension of k, say $K \cong k[y]/\langle g(y) \rangle$ for some irreducible g. In the original versions of HFE, k is characteristic 2.

The construction exploits the relationship between the standard vector space k^n and the field K (they are isomorphic as vector spaces but K has additional structure). Plaintext and ciphertext are vectors in k^n and accordingly, the public key is a map $k^n \to k^n$. The private key is a detour through K, using a map of a specific form.

Definition 1. *An HFE polynomial with bound D over K is a univariate polynomial of the form*

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

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

The reason for using HFE polynomials is to guarantee that the components of the public key are quadratic. Explicitly, an HFE system is constructed as follows: the public key is

$$P = L_1 \circ \varphi \circ F \circ \varphi^{-1} \circ L_2, \text{ where}$$

- L_1, L_2: $k^n \to k^n$ are invertible affine maps
- φ: $K \to k^n$ is the vector space isomorphism

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

- F: $K \to K$ is an HFE polynomial of some bound D.

See Figure 1. The private key is the decomposition of P. Since F is a univariate polynomial of bounded degree, preimages under F can be found, using Berlekamp's algorithm for example.

$$\begin{tikzcd}
 & K \arrow[r, "F"] & K \arrow[d, "\varphi"'] & \\
k^n \arrow[r, "S"] \arrow[rrr, bend right, "Public\ Key\ P"'] & k^n \arrow[u, "\varphi^{-1}"'] \arrow[r, "\bar{F}"] & k^n \arrow[r, "T"] & k^n
\end{tikzcd}$$

Fig. 1. The HFE system

Algebraic Attacks. The most straighforward way for an attacker holding a ciphertext $(y_1, \ldots, y_n) \in k^n$ and the public key P is to try to find the corresponding plaintext is to solve $P(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$. This is a system of n quadratic equations in the n variables $x_1, \ldots, x_n$:

$$\begin{aligned} P_1(x_1, \ldots, x_n) - y_1 &= 0 \\ P_2(x_1, \ldots, x_n) - y_2 &= 0 \\ &\vdots \\ P_n(x_1, \ldots, x_n) - y_n &= 0. \end{aligned} \tag{1}$$

Breaking an MPKC by solving these equations directly is known as an algebraic attack. Since solutions to (1) are in the variety of the ideal $\langle P_1 - y_1, \ldots, P_n - y_n \rangle \subset k[x_1, \ldots, x_n]$, a Gröbner basis of this ideal is extremely helpful. For cases of cryptographic interest, the reduced Gröbner basis with respect to lex ordering will usually look like

$$\{f_1(x_n), f_2(x_{n-1}, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n)\},$$

whose zero set can be found, via back-substitution, as easily as n univariate polynomial equations can be solved. One of the best algorithms to compute a Gröbner basis is the F_4 algorithm of Faugère [10].

In fact, using F_4 for find the Gröbner basis of the corresponding ideal seems to be the most effective way of algebraically attacking MPKCs[2] and are particularly effective against characteristic-2 HFE systems. Faugère used F_4 to break several instances of HFE [11], though it is important to note that these are characteristic-2 cases. It was later pointed out that the characteristic has a significant effect on the performance of F_4 , since an attacker can make use of the field equations $x^q - x = 0$ [8].

2.2 Square

Square was proposed in [3]. This attempt at a new MPKC was motivated by observations about the characteristic's effect on F_4 [8], and the then-apparent success in using odd-characteristic HFE as the foundation of a signature scheme [1]. All of the ideas of Square have been seen before; what makes this system novel is that these ideas are combined in a new way.

See Figure 2. Let k be a field of size q, and here we force $q \equiv 3 \mod 4$. Plaintexts will be vectors in k^n. Embed k^n into a larger space k^{n+l} via an injective affine map $L_1 \colon k^n \to k^{n+l}$. We choose n and l so that $n + l$ is odd.

Let K be a degree $n+l$ extension of k. Just as for HFE, we use a vector space isomorphism $\varphi \colon K \to k^{n+l}$ and an invertible affine map $L_2 \colon k^{n+l} \to k^{n+l}$. For the core map $K \to K$, we use

$$F(X) = X^2,$$

[2] Other polynomial solving algorithms exist, in particular the XL algorithm and its improvements [13,15], but at present they outperform F_4 only in contrived cases.

$$\begin{tikzcd}
& K \arrow[r, "F"] & K \arrow[d, "\varphi"] & \\
k^n \arrow[r, "L_2"] \arrow[rrr, bend right, "P"] & k^{n+l} \arrow[u, "\varphi^{-1}"] \arrow[r] & k^{n+l} \arrow[r, "L_1"] & k^{n+l}
\end{tikzcd}$$

Fig. 2. The Square system

hence the name Square. From these we construct the public key

$$P = L_1 \circ \varphi \circ F \circ \varphi^{-1} \circ L_2.$$

P will be an $(n + l)$-tuple of quadratic polynomials in n variables. The Square setup is quite similar to that of HFE and the earlier C^* scheme of [14]; in fact one may think of it as an odd-characteristic, embedded HFE with $D = 2$ and a specifically chosen HFE polynomial.

The decryption process is the real selling point of Square. When $|K| \equiv 3 \mod 4$, we can find preimages under F using the square root formula

$$X = \pm Y^{\frac{q^{n+l}+1}{4}}. \tag{2}$$

This makes decryption fast, especially in comparison to traditional characteristic-2 HFE systems, whose core maps have very high degree.

An Attack on Square. Though Square was shown to be strong against algebraic attacks, it was broken by what may be categorized as a differential attack [2]. Recall that the discrete differential of a function f is

$$Df(A, X) = f(A + X) - f(A) - f(X) + f(0).$$

We will hereafter refer to the below as the "Square attack".

Let us work over K. To emphasize that L_1 and L_2 (and hence their lifts) are affine, let

$$\varphi^{-1} \circ L_1 \circ \varphi = \widehat{L}_1 + \hat{l}_1,$$
$$\varphi^{-1} \circ L_2 \circ \varphi' = \widehat{L}_2 + \hat{l}_2,$$

where $\varphi' \colon \mathbb{F}_{q^n} \to k^n$, $\widehat{L}_i$ linear and $\hat{l}_i \in K$. Also let

$$\widehat{P} = \varphi^{-1} \circ P \circ \varphi',$$

$$X = \varphi^{-1}(\overrightarrow{x}) \text{ and } Y = \varphi^{-1}(\overrightarrow{y}).$$

Using this notation,

$$\begin{aligned} \widehat{P}(X) &= \widehat{L}_1(\widehat{L}_2(X)^2) + \widehat{L}_1(\hat{l}_2 \cdot \widehat{L}_2(X)) + \hat{l}_1 \\ &= \text{quadratic} + \text{linear} + \text{constant}. \end{aligned}$$

By fixing some $A \in K$, we can view the differential $D\widehat{P}$ as a univariate function

$$D\widehat{P}_A(X) = D\widehat{P}(X, A) = \widehat{L}_1 \circ M_A \circ \widehat{L}_2(X),$$

where M_A denotes multiplication by a constant which depends on A $\{D\widehat{P}_A \colon A \in K\}$ are all linear maps and they form a vector space over K.

Now, every $D\widehat{P}_A$ is of the form $\widehat{L}_1 \circ M_A \circ \widehat{L}_2$ and the linear part of $\widehat{P}$, $\widehat{L}_1(\hat{l}_2 \cdot \widehat{L}_2(X))$, has a similar form. By picking a basis for these we obtain a set

$$\begin{aligned} \Delta &= \{D\widehat{P}_{A_1} \ldots, D\widehat{P}_{A_n}\} \cup \{\widehat{L}_1(\hat{l}_2 \cdot \widehat{L}_2(X))\} \\ &= \{D_i = \widehat{L}_1 \circ M_{\lambda_i} \circ \widehat{L}_2; M_{\lambda_i}(X) = \lambda_i X, i = 1, \ldots, n+1\} \end{aligned}$$

for some unknown $\lambda_1, \ldots, \lambda_{n+1}$.

The maps of Δ are helpful because they can help us identify $\widehat{L}_1$. This is due to the fact that

$$(\widehat{L}_1 \circ M_\lambda \circ \widehat{L}_1^{-1})(\widehat{L}_1 \circ M_{\lambda_i} \circ \widehat{L}_2) = \widehat{L}_1 \circ M_{\lambda\lambda_i} \circ \widehat{L}_2. \tag{3}$$

We look for solutions L to the system of equations

$$L \circ D_i \in Span\{D_j \colon j > m\}, \quad i \leq m. \tag{4}$$

We are guaranteed by (3) that among the solutions will be some $\widehat{L}_1 \circ M_\lambda \circ \widehat{L}_1^{-1}$.

Once such an L is known, L_1 and L_2 can be recovered and Square is broken.

3 Square+

The Plus modification has been seen before, first by Patarin [17], but was considered useless and did not receive much attention. The real example of its use is to counter differential attacks of a system called Perturbed Matsumoto-Imai [6]. This motivated us to look at a Plus variant of Square.

The modification is simple: for any MPKC, a Plus variant can be constructed by appending some number p of randomly chosen quadratic polynomials to the public key before a final mixing process. Let us describe this specifically for the case of Square.

As usual, let k be a field of size q, where $q \equiv 3 \mod 4$. Plaintexts will be vectors in k^n, we will embed the space of plaintexts into k^{n+l}, and K is a field extension of degree $n + l$. Let $m = n + l + p$. As for Square, we make use of the following maps: the vector space isomorphism $\varphi \colon K \to k^{n+l}$, the core map $F \colon K \to K$ given by

$$F(X) = X^2,$$

and an injective affine map $L_2 \colon k^n \to k^{n+l}$. We also use p quadratic polynomials in $n + l$ variables,

$$g_1, \ldots, g_p \in k[x_1, \ldots, x_{n+l}]$$

and an invertible affine map $L_1 \colon k^m \to k^m$.

Since $\varphi \circ F \circ \varphi^{-1}$ is an $(n+l)$-tuple of quadratic polynomials, by appending $g_1, \dots, g_p$ we can create a map $\overline{F}^+ : k^n \to k^m$. From this we construct the public key

$$P^+ = L_1 \circ \overline{F}^+ \circ L_2.$$

See Figure 3. P^+ will be an m-tuple of quadratic polynomials

$$P^+(x_1, \dots, x_n) = \begin{pmatrix} P_1^+(x_1, \dots, x_n) \\ P_2^+(x_1, \dots, x_n) \\ \vdots \\ P_m^+(x_1, \dots, x_n) \end{pmatrix}.$$

$$\begin{tikzcd}
 & K \arrow[r, "F"] & K \arrow[d, "\varphi"] & & \\
k^n \arrow[r, "L_2"] \arrow[drrrr, bend right=60, "P^+"'] & k^{n+l} \arrow[u, "\varphi^{-1}"] \arrow[r, "\overline{F}"] \arrow[ddr, "g_1,\dots,g_p"'] & k^{n+l} \arrow[dr] & & \\
 & & & * \arrow[r, "L_1"] & k^{n+l+p} \\
 & & k^p \arrow[ur] & &
\end{tikzcd}$$

Fig. 3. Overview of the Square+ system. The * denotes concatenation.

Encryption with Square+. A plaintext $(s_1, \dots, s_n) \in k^n$ in encrypted by computing

$$(c_1, \dots, c_m) = P^+(s_1, \dots, s_n).$$

Decryption with Square+. For a ciphertext $(c_1, \dots, c_m) = P^+(s_1, \dots, s_n) \in k^m$, decryption is performed as follows: first, let

$$(y_1, \dots, y_m) = L_1^{-1}(c_1, \dots, c_m)$$

and

$$Y = \varphi^{-1}(y_1, \dots, y_{n+l}) \in K.$$

In other words, we "unmix" the random polynomials and discard them before moving the ciphertext to the big field. Then we solve $X^2 = Y$. Due to our choice of q and $n+l$, we can use the square root formula (2). This gives two solutions. Since L_2 is affine, in general only one of them will be in the image of $\varphi^{-1} \circ L_2$. The preimage of the solution will be $(s_1, \dots, s_n)$. Note that with the Plus polynomials, we have a backup method of deciding between the two square roots. The addition of random polynomials all but ensures that only one of them will actually be a preimage of the ciphertext under P^+.

Security Analysis. The main question regarding the security of Square+ is, How do the Plus polynomials change the potency of attacks against Square? The answer is that some attacks become more successful, some are thwarted, and others are mostly unaffected.

When Square was proposed, justifications were made for its resilience to attacks reliant on invariant subspaces and/or properties of the bilinear forms associated to the public key [3]. The addition of random polynomial information will not increase the probability of linear algebraic properties of the core map. Of course, an attacker could find linear combinations of the public key polynomials and come across a large enough collection (around $n+l$) which are a combination of only the original Square public key components. The chance of an attacker doing so randomly is $q^{-p(n+l)}$ and at present there does not seem to be any way to find these combinations in a more effficient way. So, there is no reason that Plus polynomials will make these attacks suddenly dangerous.

On the other hand, providing more polynomial information about the plaintext-ciphertext relationship *will* make algebraic attacks predictably more effective. See Figures 4 and 5 for a summary of our experiments regarding algebraic attack times for some Square+ systems. Thus it is important to use a small p not only for practicality reasons but also security. Considering the results of our algebraic attack experiments and extrapolating the data, it seems that a Square+ scheme with $q = 31$, $n = 48$, $l = 3$, and $p = 5$ looks promising.

The reason for adding the Plus polynomials is to dodge the Square attack. Since we add quadratic polynomials, the "noise" they create affects the differentials. In particular, if we proceed as in the Square atttack - work in an extension

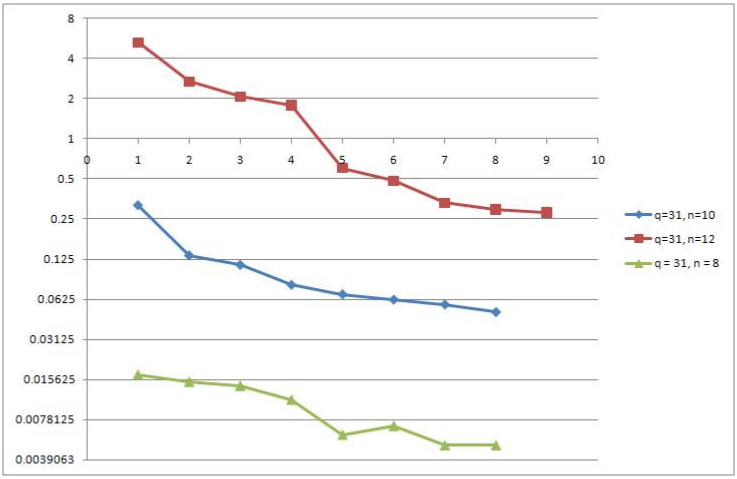

Fig. 4. Algebraic Attack times against Square+ vs p, for various q and n. The value of l is 3 for all tests.

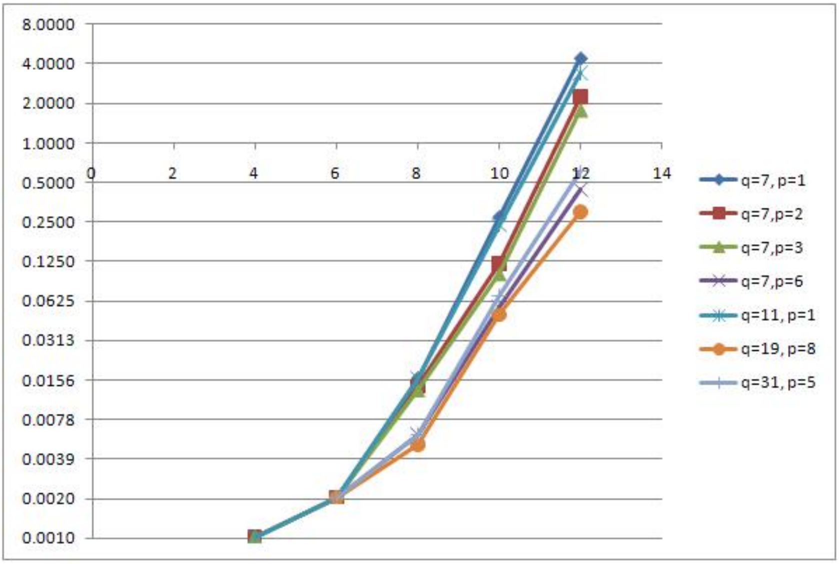

Fig. 5. Algebraic Attack times against Square+ vs n, for various q and p. The value of l is 3 for all tests.

field and fix one input of the differential as in (2.2), we see that

$$D\widehat{P}_A = \widehat{L}_1 \circ M_A \circ \widehat{L}_2 + L,$$

for some linear map L which comes from the randomly-chosen Plus polynomials and thus should also be random. So the differentials of teh Square+ public key cannot be used in the same way as in 3 to identify the secret transformation. Plus was effectively used to protect the Perturbed Matsumoto-Imai system from differential attack in [6].

4 Double-Layer Square

The Plus variant of Square uses “cosmetic” changes to the structure of the system to obstruct an attacker’s access to the nice differential properties of Square. Another approach is to destroy the properties altogether by complicating the core map. This is the main idea behind Double-Layer Square.

Construction. The construction takes cues from the Rainbow signature scheme [7]. The variables are split into two “layers”; some of the input components determine the polynomial into which other components are fed. We will discuss below why an attacker should not be able to separate the layers.

Again $|k| = q \equiv 3 \mod 4$. Plaintexts are vectors in k^{2n}, n odd. Let $L_2 \colon k^{2n} \to k^{2n+l}$ be an affine transformation of rank $2n$.

Remark. Here, we would like to note that this map L_2 uses the idea of embedding proposed to enhance the security of Sflash in [5]. The application of this embedding is critical in ensuring the security of our new scheme.

The first layer: Let $K \cong k^{n+l}$ via vector space isomorphism φ and $F\colon K \to K$ be given by $F(X) = X^2$. The map

$$\overline{F} = \varphi \circ F \circ \varphi^{-1}$$

is an $(n+l)$-tuple of quadratic polynomials in $n+l$ variables.

The second layer: Let $K' \cong k^n$ via the vector space isomorphism φ'. Consider the map $G\colon k^{n+l} \times K' \to K'$ given by

$$G((x_1, \dots, x_{n+l}), X) = \alpha X^2 + \beta(x_1, \dots, x_{n+l})X + \gamma(x_1, \dots, x_{n+l}),$$

where $\alpha \in K'$, β is affine and γ is quadratic[3]. The map

$$\overline{G} = \varphi' \circ G \circ (id \times \varphi'^{-1}),$$

is an n-tuple of quadratic polynomials in $2n+l$ variables.

Altogether by concatenating the first and second layers, we obtain a map $k^{2n+l} \to k^{2n+l}$ given by

$$\overline{F} * \overline{G} = \begin{pmatrix} \overline{F}_1(x_1, \dots, x_{n+l}) \\ \overline{F}_2(x_1, \dots, x_{n+l}) \\ \vdots \\ \overline{F}_{n+l}(x_1, \dots, x_{n+l}) \\ \overline{G}_1(x_1, \dots, x_{2n+l}) \\ \overline{G}_2(x_1, \dots, x_{2n+l}) \\ \vdots \\ \overline{G}_n(x_1, \dots, x_{2n+l}) \end{pmatrix}.$$

Using with the embedding L_2 and a final invertible transformation $L_1\colon k^{2n+l} \to k^{2n+l}$ we get a public key $P\colon k^{2n} \to k^{2n+l}$

$$P = L_1 \circ (\overline{F} * \overline{G}) \circ L_2.$$

Encryption. To encrypt a message $(m_1, \dots, m_{2n}) \in k^{2n}$, simply compute

$$(c_1, \dots, c_{2n+l}) = P(m_1, \dots, m_{2n}).$$

[3] More precisely the maps β_i and γ are of the form

$$\beta_i(x_1, \dots, x_{n+l}) = \sum_{1 \le j \le n+l} \xi_{ij} x_j + \nu_i,$$

$$\gamma(x_1, \dots, x_{n+l}) = \sum_{1 \le j < l \le n+l} \eta_{jk} x_j x_k + \sum_{1 \le j \le n+l} \sigma_j x_j + \tau,$$

where ξ_{ij}, ν_i, η_{jl}, σ_j and τ are randomly chosen from K'.

Decryption. Given a ciphertext $(c_1, \ldots, c_{2n+l})$ we must first compute

$$(c'_1, \ldots, c'_{2n+l}) = L_1^{-1}(c_1, \ldots, c_{2n+l}) \in k^{2n+l}.$$

We know that $\overline{F}(x_1 \ldots, x_{n+l}) = (c'_1, \ldots, c'_{n+l})$. We can easily find preimages under $\overline{F}$ by going back to the "big field" K and using the square root formula in K:

$$\sqrt{Y} = \pm Y^{\frac{q^{n+l}+1}{4}} \tag{5}$$

Suppose $(z_1^{(1)}, \ldots, z_{n+l}^{(1)})$ and $(z_1^{(2)}, \ldots, z_{n+l}^{(2)})$ are the two preimages under $\overline{F}$. Now we find a preimage under $\overline{G}$ using each as vinegar variables. We solve

$$G((z_1^{(i)}, \ldots, z_{n+l}^{(i)}), X) = \varphi'^{-1}(c_{n+l+1}, \ldots, c_{2n+l}).$$

With the $z_j^{(i)}$s plugged in, this is just a univariate polynomial equation over K'. We can solve it either by Berlekamp's algorithm or via the quadratic formula, again using the square root formula (5).

Now there are up to four preimages of $\overline{F} * \overline{G}$. However, the correct preimage must lie in $L_2(k^n)$; in general only one will do so and that preimage is the plaintext. We work under the assumption that we are trying to decrypt an encrypted message, so at least one of the possibilities will lie in this space.

Remark 1. There is no reason why we cannot use more than two layers in this construction. However, each layer will increase by a factor of 2 the number of preimages to be checked in the final stage of the decryption process. Since two layers seem to be enough to stymie attacks, there is no reason to slow the decryption process with added layers.

Security Analysis. First we observe that algebraic attacks against Double-Layer Square systems perform about as well as against Square systems with the same number of variables. Thus we believe that Double-Layer Square is safe from algebraic attacks.

Many successful attacks on MPKCs exploit the simplicity of private maps when viewed as univariate polynomials, and this gives Double-Layer Square an advantage. The univariate polynomial which corresponds to $\overline{F} * \overline{G}$ is an HFE polynomial over a degree $2n + l$ extension, but in general it will have maximum degree $(2q^{n+l-1})$ and many terms. The Square attack relies on the differential property $DF(A, X) = 2AX$ which is not true for most HFE polynomials.

So, lifting to a large field and working with a univariate polynomial does not seem to help an attacker. Let us consider the differential of the core map as it is given. Let

$$(a_1, \ldots, a_{2n+l}), (x_1, \ldots, x_{2n+l}) \in k^{2n+l},$$

$$\boldsymbol{a} = (a_1, \ldots, a_{n+l}) \in k^{n+l},$$

$$A = \varphi^{-1}(\boldsymbol{a}) \in K,$$

$$A' = \varphi^{-1'}(a_{n+l+1}, \ldots, a_{2n+l}) \in K'.$$

(Analogous $\boldsymbol{x}$, X and X'.) Then the differentials are

$$DF(A, X) = 2AX \tag{6}$$

$$DG((\boldsymbol{a}, A'), (\boldsymbol{x}, X')) = 2\alpha A'X"' + \beta(\boldsymbol{a})X' + \beta(\boldsymbol{x})A' + D\gamma(\boldsymbol{a}, \boldsymbol{x}). \tag{7}$$

It is true that DF is the same as for Square. However $\boldsymbol{a}$ and $\boldsymbol{x}$ appear in both (6) and (7), and γ is randomly chosen so we cannot expect $D\gamma$ to have any nice properties. Once $\overline{F}$ and $\overline{G}$ are mixed together by L_1, it seems highly unlikely that an attacker can untangle the two differentials to access the simpler one (6).

5 Conclusions

In this paper, we proposed two new encryption schemes based on the Square system. Square+ evades differential attacks by adding noise to the differentials by way of Plus polynomials; Double-Layer Square achieves the same end by using a more complicated core map structure. We explained the new constructions and gave arguments and evidence suggesting that both are secure options.

Acknowledgments. The authors would like to thank Dr. John Baena Giraldo for his help designing the experiments. Thanks also go to the Singapore MoE Tier 2 grant T208B2206, the NSF, NSF China and the Charles Phelps Taft Foundation.

References

1. Baena, J., Clough, C., Ding, J.: Square-Vinegar Signature Scheme. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 17–30. Springer, Heidelberg (2008)
2. Billet, O., Gilles, M.-R.: Cryptanalysis of the Square Cryptosystems. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 451–468. Springer, Heidelberg (2009)
3. Clough, C., Baena, J., Ding, J., Yang, B.-Y., Chen, M.: Square, a new multivariate encryption scheme. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 252–264. Springer, Heidelberg (2009)
4. Courtois, N.: The security of hidden field equations (HFE). In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 266–281. Springer, Heidelberg (2001)
5. Ding, J., Dubois, V., Yang, B.-Y., Owen Chen, C.-H., Cheng Could, C.-M.: Could SFLASH be Repaired? In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part II. LNCS, vol. 5126, pp. 691–701. Springer, Heidelberg (2008)
6. Ding, J., Gower, J.E., et al.: Inoculating Multivariate Schemes against differential attacks. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 290–301. Springer, Heidelberg (2006)
7. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 164–175. Springer, Heidelberg (2005)

8. Ding, J., Schmidt, D., Werner, F.: Algebraic attack on HFE revisited. In: Wu, T.-C., Lei, C.-L., Rijmen, V., Lee, D.-T. (eds.) ISC 2008. LNCS, vol. 5222, pp. 215–227. Springer, Heidelberg (2008)
9. Dubois, V., Granboulan, L., Stern, J.: An efficient provable distinguisher for HFE. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 156–167. Springer, Heidelberg (2006)
10. Faugére, J.-C.: A new efficient algorithm for computing Gröbner bases (F_4). J. Pure Appl. Algebra 139(1-3), 61–88 (1999); Effective methods in algebraic geometry (Saint-Malo, 1998)
11. Faugère, J.-C., Joux, A.: Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
12. Jiang, X., Ding, J., Hu, L.: Public Key Analysis-Kipnis-Shamir Attack on HFE Revisited. In: Pei, D., Yung, M., Lin, D., Wu, C. (eds.) Inscrypt 2007. LNCS, vol. 4990, pp. 399–411. Springer, Heidelberg (2008)
13. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999)
14. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)
15. Mohamed, M.S.E., Mohamed, W., Ding, J., Buchmann, J.: MXL2: Solving Polynomial Equations over GF (2) Using an Improved Mutant Strategy. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 203–215. Springer, Heidelberg (2008)
16. Patarin, J.: Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996)
17. Patarin, J., Goubin, L., Courtois, N.: C*-+ and HM: Variations around two schemes of T. Matsumoto and H. Imai. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 35–50. Springer, Heidelberg (1998)