Cryptanalysis of “$2R$” Schemes

Ye Ding-Feng[1], Lam Kwok-Yan[2], and Dai Zong-Duo[3]

[1] Kent Ridge Digital Lab, Singapore 119613
dfye@krdl.org.sg
[2] National University of Singapore, Singapore 119260
lamky@comp.nus.edu.sg
[3] Graduate School, University of Science & Technology of China
yangdai@mimi.cnc.ac.cn

Abstract. The function decomposition problem can be stated as: Given the algebraic expression of the composition of two mappings, how can we identify the two factors? This problem is believed to be in general intractable [1]. Based on this belief, J. Patarin and L. Goubin designed a new family of candidates for public key cryptography, the so called “$2R$–schemes” [10, 11]. The public key of a “$2R$”-scheme is a composition of two *quadratic mappings*, which is given by n polynomials in n variables over a finite field K with q elements. In this paper, we contend that a composition of two quadratic mappings can be decomposed in most cases as long as $q > 4$. Our method is based on heuristic arguments rather than rigorous proofs. However, through computer experiments, we have observed its effectiveness when applied to the example scheme “D^{**}”given in [10].

1 Introduction

Public key cryptography is becoming more and more important in modern computer and communication systems. Many public key cryptosystems (PKCs) have been proposed since Diffie and Hellman initiated this direction in 1976 [2]. Usually the security of a PKC relies on a hard mathematical problem. The most famous such problems are integer factorization and discrete logarithm. PKCs based on these two kinds of problems, such as RSA[13] and ElGamal[3], although mathematically sound, need to perform a large amount of huge arithmetics, so are not very efficient compared to classical symmetric cryptographic algorithms such as DES. Much effort has been paid in seeking more efficient constructions for PKCs. One class of these constructions make use of mapping compositions. The basic idea is as follows: a user chooses several easily-invertible mappings which he keeps secret, computes the algebraic expression of their composition and makes it public; then anyone else can do encryption or verify signatures using the public key, but will be faced with a set of complicated algebraic equations when he tries to decrypt cipher texts or to forge signatures. An obvious advantage of these PKCs is that the private key side computations (decrypting and signing) can be made very efficient and be implemented with very simple

Michael Wiener (Ed.): CRYPTO’99, LNCS 1666, pp. 315-325, 1999.

hardware. There are two main drawbacks however: large public key size and ambiguous security foundations.

The earliest examples of PKCs making use of mapping compositions were proposed by T.Matsumoto and H.Imai [4] in 1985. One of them, called "B", looks like "$t \circ f \circ s$", where t, s are two secret linear mappings over $GF(2)^n$, $f : x \mapsto (x+c) \bmod (2^n-1)+1$, $0 \mapsto 0$, c is also secret, and elements of $GF(2)^n$ is identified with integers naturally. This scheme is still unbroken. Another example is called "C^*" (see also [5]), in which the above f is replaced by a "quadratic polynomial tuple" which will be called *quadratic mapping* in this paper. C^* was broken by Jacques Patarin [7] in 1995.

One-round schemes are generalizations of C^*. They are of the form the "$t \circ f \circ s$", where s, $t : K^n \to K^n$ are affine, $f : K^n \to K^n$ is quadratic, and K is a finite field. J. Patarin and L. Goubin gave several constructions of one-round schemes using algebraic techniques and S-boxes (see [10, 11]), and they also showed that their constructions are insecure. Therefore they proposed two-rounds schemes, abbreviated as "2R", in which the public key is the composition of two secret one-round schemes, based on the assumption that functional decomposition problem is hard.

In this paper, we show that "2R" schemes can be decomposed into separated one-round schemes in most cases as long as the field K has more than 4 elements. However, we were only able to justify this claim by some heuristic arguments and experimental evidences instead of rigorous proofs.

Briefly stated, our method is as follows. Suppose $\pi = f \circ g : K^n \to K^n$ be the composition of two quadratic mappings. We have n output polynomials of π in n variables of degree 4. The partial derivatives of all these polynomials with respect to all the n input variables give n^2 cubic polynomials, spanning a linear space $\tilde{V}$. This space is contained in the space V of cubic polynomials spanned by products of the n input variables X_i and the n intermediate output polynomials of g, provided that K has more than 4 elements. Since both $\tilde{V}$ and V tend to have dimension n^2 for random choices, we hope they are equal (or at least the the codimension is small). For a linear combination F of input variables, we can use linear algebra to compute $(V : F)$, the space of quadratic polynomials r such that $rF \in V$. When $n > 2$, the intersection of these spaces is a candidate for the space $\mathcal{L}(g)$ spanned by the n output polynomials of g. This last statement needs the assumption that the factorization of π is unique, that is, if we write $\pi = f' \circ g'$ for quadratic f', g', then g and g' differ only by a linear factor.

We have applied this method to a concrete example D^{**} in the "2R" family. D^{**} is a composition of two D^*s, and a D^* is a mapping of the form $t \circ \phi \circ s$", where ϕ is the squaring in the extension field $K^{(n)}$. In the example, $K = \mathrm{GF}(251)$ and $n = 9$. In our experiments, the above method has never failed to find the linear class of the inner D^*, by which we mean the set of mappings which differ from each other by a linear bijection.

The rest of this paper is organized as follows: Section 2 gives a brief review of "2R" schemes and some notations and definitions. Section 3 describes the steps in decomposing compositions of quadratic mappings. Section 4 gives some experiment reports. Section 5 is the conclusion of this paper.

2 "2R" Schemes and "D^{**}": A Brief Review

Through out this paper K denotes a finite field of q elements, and K^n denotes the vector space over K of dimension n. Any polynomial $P = P(X_1, X_2, \cdots, X_n)$ can be seen as a mapping $K^n \to K : (x_1, x_2, \cdots, x_n) \mapsto P(x_1, x_2, \cdots, x_n)$. Similarly, any n polynomials $(P_1, P_2, \cdots, P_n)$ can be regarded as a mapping $K^n \to K^n$:

$$(x_1, x_2, \cdots, x_n) \mapsto (P_1(x_1, x_2, \cdots, x_n), P_2(x_1, x_2, \cdots, x_n), \cdots, P_n(x_1, x_2, \cdots, x_n).$$

Conversely, any mapping $K^n \to K^n$ can be expressed as n polynomials as above, these polynomials are called its component polynomials. A mapping is called *linear*, if its component polynomials are all homogeneous of degree 1; *affine*, if constant terms are allowed; *quadratic*, if the total degree ≤ 2.

"2R" schemes ("2R" stands for 2 rounds) were introduced by Jacques Patarin and Louis Goubin in [11]. The private key consists of

1. Three affine bijections r, s, t from K^n to K^n.
2. Two quadratic mappings ψ, ϕ : $K^n \to K^n$ (in fact, these two mappings can also be made public).

The public items are:

1. The field K and dimension n.
2. The n polynomials of the composed mapping $\pi = t \circ \psi \circ s \circ \phi \circ r$ which are of total degree 4.

The public-key side computation is just an application of the mapping π (both message blocks and signatures belong to K^n). To explain decryption and signing, we need more words. The designers of these schemes do not require the private mappings ψ, ϕ be bijections. To achieve the uniqueness of decryption, we should introduce enough redundancy in message blocks. Similarly, to compute a signature, we should keep enough redundancy-bits so that for any message m, we can find a redundant tail R making $m||R$ lie in the range of π. The non-injectiveness of ψ, ϕ will in general greatly reduce the efficiency in private-key side computations. In the scheme D^{**}, these drawbacks are overcomed by a clever choice of the message-block space, see [10]. The essence of decryption is to find the full preimage $\pi^{-1}(c)$ for any given c, and that of signing is to find a single element belonging to $\pi^{-1}(c)$. When the private keys are known, this can be reduced to inverting ψ and ϕ.

As the authors of [11] point out, the security of "2R" schemes can be affected by the choices of ψ, ϕ. Since ψ and ϕ should be easy to construct and invert, currently only the following constructions are known:

1. "C^*-functions": monomials over an extension of degree n over K: $a \mapsto a^{1+q^\theta}$.

2. "Triangular-functions":
$$(a_1, \cdots, a_n) \mapsto (a_1, a_2 + q_1(a_1), \cdots, a_n + q_{n-1}(a_1, \cdots, a_{n-1}))$$
where each q_i is quadratic.
3. "S-boxes-functions": $(a_1, \cdots, a_n) \mapsto$
$$(S_1(a_1, \cdots a_{n_1}), S_2(a_{n_1+1}, \cdots, a_{n_1+n_2}), \cdots, S_d(a_{n_1+\cdots+n_{d-1}}, \cdots, a_n))$$
where $n = \sum n_i$, and S_i is a quadratic mapping $K^{n_i} \to K^{n_i}$.
4. techniques by combining "S-boxes" with "triangular-functions".
5. D^*-functions: squaring in extension of K of degree n, denoted as $K^{(n)}$, where $q^n \equiv -1 \pmod 4$.

Previous researches [11, 8] have shown that, when ψ is in the first two classes, the resulted scheme is weak. Note that if we drop t and ψ in above description of "2R", we get the so called one-round schemes. A "2R" scheme is just a composition of two one-round schemes. All one-round schemes from the above constructions have been shown to be insecure [8, 9, 7, 10, 11].

"D^{**}" is a special instance of "2R". It is defined as:

1. $q^n \equiv -1 \pmod 4$, and q is about of the size 2^8. (For example, $q = 251$, $n = 9$ [10].)
2. r, s, t are linear bijections.
3. $\psi = \phi$ is the squaring in $K^{(n)}$, where $K^{(n)}$ denotes the extension of K of degree n.
4. The message block space is chosen in such a way [10] that the restriction of π on it is an injection. (This is irrelevant to the purpose of this paper.)

Note that the public polynomials in D^{**} are all homogeneous of degree 4.

3 Decomposing "2R" Schemes

A basic assumption behind "2R" schemes is that the functional decomposition problem for a composition of two quadratic mappings from K^n to K^n is hard. In this section we will give evidences which indicate that this assumption is not realistic provided $q > 4$.

As in the previous section, let $\pi = t \circ \psi \circ s \circ \phi \circ r$ be the public key. If for any quadratic f, g, satisfying $\pi = f \circ g$, we have $f = t \circ \psi \circ s_1$, $g = s_2 \circ \phi \circ r$, for some affine bijections s_1, s_2 satisfying $s = s_1 \circ s_2$, we say that π has unique factorization. If the factorization of π is not unique, even we can decompose it into two quadratic mappings, we are not sure if these two mappings are one-round functions which can be attacked by known methods. Therefore we need to assume this uniqueness of decomposition. It seems difficult to justify this assumption theoretically, but we believe that most compositions of quadratic mappings do have unique factorizations.

Note that if we can find a $g = s_2 \circ \phi \circ r$, then f may be obtained by solving linear equations arising from coefficients-comparing. Note also that s_2 is not important, what we really care is the *affine class* $\{s \circ \phi \circ r$: for all affine bijection $s\}$ (similarly, the *linear class* of a mapping g is $\{s \circ g$: for all linear bijection $s\}$), and this class is uniquely determined by the vector space generated by component polynomials of g and 1. In the following we will describe how to obtain this space when given the component polynomials of π.

To ease the discussion, we assume all the mappings r, s, t, ϕ, ψ are homogeneous. In this case, we only need $q > 3$. The general case can be reduced to the homogeneous case when $q > 4$, by a standard algebraic procedure which is called homogenization, see Appendix 1.

3.1 A Linear-Algebra Problem on Polynomials

Now we assume f, g be two homogeneous quadratic mappings from K^n to K^n. Given the composition $f \circ g$, which is a homogeneous mapping of degree 4, we want to determine the linear class of g, this is equivalent to determine the linear space $\mathcal{L}(g)$ generated by component polynomials of g. This linear space may not be directly obtained, but later we will show that the linear space $V(g) = \sum_{1 \leq i \leq n} X_i \mathcal{L}(g)$ can in most cases be obtained from the component polynomials of $f \circ g$. So we are faced with the following problem of linear algebra.

Problem 1 *Let $\mathcal{W}$ be a linear space of dimension $\leq n$ consisting of quadratic forms in n variables $X_1, \cdots, X_n$. Given $V = \sum_{1 \leq i \leq n} X_i \mathcal{W}$, is it possible (and how) to uniquely determine $\mathcal{W}$?*

For any subspace $\mathcal{L}'$ of the linear space $\mathcal{L}$ generated by $X_1, \cdots, X_n$, let

$$(V : \mathcal{L}') \overset{\text{def}}{=\!=} \{r \in K[X_1, X_2, \cdots, X_n] : \; r\mathcal{L}' \subseteq V\}.$$

When $\mathcal{L}'$ has dimension 1, say, generated by F, we also write $(V : F) = (V : \mathcal{L}')$. We have the following conjecture.

Conjecture 1 *Notations and assumptions as above, then for randomly chosen $\mathcal{W}$, the probability ρ that $(V : \mathcal{L}) = \mathcal{W}$ are very close to 1 when $n > 2$.*

Note that $(V : \mathcal{L}')$ can be computed using linear algebra for any V and $\mathcal{L}'$, so the above conjecture says that in general the answer to the above problem is positive.

Although we can not prove the above conjecture or give a reasonable estimation on ρ, in the following we will justify this conjecture with some heuristic arguments based on some standard facts from linear algebra.

Let $\mathcal{Q}$ denote the total space of all quadratic forms. We have $\dim(\mathcal{Q}) = n(n+1)/2$. In the application at hand we may assume $\dim(\mathcal{W}) = n$, so $\dim(\mathcal{Q}/\mathcal{W}) = n(n+1)/2 - n = n(n-1)/2$, where $\mathcal{Q}/\mathcal{W}$ means quotient space. Now we wish to estimate $\dim((V : \mathcal{L})/\mathcal{W})$. Note that $(V : \mathcal{L})/\mathcal{W} = \cap_i (V : X_i)/\mathcal{W}$. It is not easy to characterize this intersection because of the complex relations between the spaces $(V : X_i)$. To simplify things, we regard the n spaces $(V : X_i)/\mathcal{W}$ as n independent random variables. This is neither supported or disapproved by any theoretical results we know. By linear algebra (see Appendix 2), two random subspaces of dimension n_1, n_2 of a n-dimension space tend to have intersection of dimension $n_1 + n_2 - n$, so we need that $\sum_i \dim((V : X_i)/\mathcal{W})$ exceeds $(n-1)n(n-1)/2$ to expect a nonzero intersection $\cap_i (V : X_i)/\mathcal{W}$.

Now let us see the dimension of the subspaces $(V : X_i)/\mathcal{W}$. Since every coordinate X_i plays the same role, we only need to consider $(V : X_1)/\mathcal{W}$. Let $(g_1, g_2, \cdots, g_n)$ be a basis of $\mathcal{W}$, any element in $(V : X_1)/\mathcal{W}$ can be written in form $(\sum g_i F_i)/X_1$, where F_i are linear forms in $X_2, \cdots, X_n$, and satisfying $\sum g_i(0, X_2, \cdots, X_n)F_i = 0$. Let σ be the linear map from $\mathcal{L}'^n$, where $\mathcal{L}'$ be the space of linear forms in $X_2, \cdots X_n$, to the space of cubic polynomials:

$$(F_1, \cdots, F_n) \mapsto \sum g_i(0, X_2, \cdots, X_n)F_i.$$

Then we see $\dim((V : X_1)/\mathcal{W}) \leq \dim(\ker(\sigma))$. Again we regard σ as a random linear mapping between spaces of dimensions $n(n-1)$, $(n-1)n(n+1)/6$ respectively, so we may expect $\dim(\sigma) = n(n-1) - (n-1)n(n+1)/6$ ($\dim(\ker(\sigma)) = 0$, if the r.h.s is negative). This number is: 2, when $n = 3$, 4; and 0, when $n > 5$.

Therefore we can not expect $\sum_i \dim((V : X_i)/\mathcal{W}) > (n-1)n(n-1)/2$ when $n \geq 3$, which suggests we have good chance to have $(V : \mathcal{L}) = \mathcal{W}$. Note that this conclusion would be more credible if q or n gets larger.

3.2 Recovering $V(g)$

In the previous section we have indicated that $f \circ g$ can likely be factored as long as $V(g)$ can be obtained. Now we will show how to get $V(g)$ from the component polynomials, $h_1, \cdots, h_n$, of $f \circ g$.

Let $\tilde{V}$ denote the linear space generated by

$$\frac{\partial h_j}{\partial X_i} \in V(g), \text{ for all } i, j.$$

Lemma 1. *$\tilde{V} \subset V(g)$ if $q > 3$.*

Proof. When $q > 3$, the expression for each h_j as a homogeneous polynomial of degree 4 is unique. We can write h_j in form $\sum a_{k,l} g_k g_l$, so we have

$$\frac{\partial h_j}{\partial X_i} = \sum a_{k,l}\left(\frac{\partial g_k}{\partial X_i} g_l + \frac{\partial g_l}{\partial X_i} g_k\right) \in V(g).$$

□

Since $\dim(V(g)) \leq n^2$, if we regard the n^2 partial derivatives as random vectors in $V(g)$, then with probability greater than $\prod_{i>0}(1 - q^{-i})$, which is close to $1 - 1/q$ when q is not too small, we will have $\tilde{V} = V(g)$. In general, the probability that $\dim(V(g)/\tilde{V}) \geq \delta$ is approximately $q^{-\delta^2}$. So when $\tilde{V} \neq V(g)$, we can expect that $\dim(V(g)/\tilde{V})$ be very small, say $< n$.

When $\tilde{V} \neq V(g)$, $V(g)$ may be recovered from $\tilde{V}$ as follows. Randomly choose a subspace $\mathcal{L}'$ of $\mathcal{L}$ and compute $(\tilde{V} : \mathcal{L}')$, if we can be assured that $(\tilde{V} : \mathcal{L}') \subset \mathcal{L}(g)$, then we can add $(\tilde{V} : \mathcal{L}')\mathcal{L}$ to $\tilde{V}$, and hope this will enlarge $\tilde{V}$ and by repeating the process to finally get $\tilde{V} = V(g)$. The problem is that it is hard to decide whether $(\tilde{V} : \mathcal{L}') \subset \mathcal{L}(g)$. In the following we will give a solution to this problem for $n > 4$.

Assume $0 < \delta = \dim(V(g)/\tilde{V}) < n$ and $n > 4$. By arguments in the previous subsection, we have seen that $(V(g) : F) = \mathcal{L}(g)$ holds with high probability for a randomly-chosen linear form F. On the other hand, $\dim((F\mathcal{L}(g)) \cap \tilde{V}) \geq n - \delta$, and the equality also holds with high probability. $(V(g) : F) = \mathcal{L}(g)$ implies that

$$(\tilde{V} : F) = ((F\mathcal{L}(g)) \cap \tilde{V})/F.$$

So we could expect that $\dim((\tilde{V} : F)) = n - \delta$ occur frequently. Moreover δ can be detected from the fact that

$$\delta = n - \min\{\dim((\tilde{V} : F)) : \text{for sufficiently many random } F\}$$

. Now it is easy to conclude that $(\tilde{V} : F) \subset \mathcal{L}(g)$ for those F satisfying $\dim((\tilde{V} : F)) = n - \delta$.

4 An Example

In this section, the methods of the previous section are applied to a concrete example, D^{**} with $q = 251$, $n = 9$, which is suggested in [10]. The irreducible polynomial for definition of $K^{(9)}$ is chosen as $t^9 + t + 8$(the choice is irrelevant to the analysis of the scheme). Let ϕ denote the squaring in $K^{(9)}$. Let $g_s = \phi \circ s$ for any linear bijection s. The property that $(V(g_s) : \mathcal{L}) = \mathcal{L}(g_s)$ is independent of s. So are the distribution of dimension of $(V(g_s) : \mathcal{L}')$ while $\mathcal{L}'$ ranging over subspaces of $\mathcal{L}$. Therefore in order to verify the properties of $V(g_s)$ as predicted by the heuristic arguments in the previous section, we may assume $g = \phi$. The component polynomials of ϕ is given in appendix, where indexes for variables start with 0. It can be verified that $\dim(V(g)) = n^2 = 81$. We did not find any linear form F, such that $(V(g) : F) \neq \mathcal{L}(g)$, among 1000 randomly chosen F. So $\mathcal{L}(g)$ has much stronger properties than that stated in Conjecture 1. This also suggests that, if the inner factor of a "2R" scheme is a one-round scheme of type D^*, the attack described in the previous section would likely be successful.

We have also done experiments to verify that, the linear space $V(g)$ can indeed be recovered by the method described in previous section. For $\pi = t \circ \phi \circ s \circ \phi \circ r$, define $\tilde{V}_\pi$ to be the linear space generated by partial derivatives of component polynomials of π. It is easy to prove that $\dim(\tilde{V}_\pi)$ does not depend on t and r. So we let $t = r = 1$. Again we have tried 1000 randomly chosen s, and we always get $\dim(\tilde{V}_\pi) = n^2 = 81$.

The programs (see Appendix 3) for these experiments are written in Mathematica 3.0, where "test1" tests the properties related to Conjecture 1, and "test2" test the distribution of $\dim(\tilde{V}_\pi)$.

5 Conclusion

In this paper, we have showed that the functional decomposition problem for compositions of quadratic mappings is not hard provided the field of coefficients has more than 4 elements. As a consequence, the base field for "2R" schemes has only 3 choices: $GF(2)$, $GF(3)$, $GF(4)$. However, in these cases, the dimension n should be large to guarantee a reasonable block size (say, $\geq$ 64 bits); since the public key size is at the order of n^5, one can easily see that the resulted schemes are simply impractical. This concludes that the idea of "2R" schemes is not interesting. One possible cure is to replace a few of the component polynomials with random polynomials before composing the last affine bijection, using ideas in [12]. Again, this will greatly reduce the efficiency of private-key side computations, hence lower the practical value of the original designs.

It remains open if the corresponding functional decomposition problem is really hard when $q \leq 4$.

References

1. M. Dickerson, The Functional Decomposition of Polynomials, Ph.D Thesis, TR89-1023, Dept. of Computer Science, Cornell University, Ithaca, NY, July 1989.
2. W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, IT-22(6) 644-654, 1976.
3. T.Elgamal, A Public Key Cryptosystem and a Signature Schemes Based on Discrete Logarithms, IEEE Trans. Inform. Theory, Vol. IT-31(1985), 469-472.
4. T. Matsumoto and H. Imai, Algebraic Methods for Constructing Asymmetric Cryptosystems, AAECC-3, Grenoble, 1985.
5. T. Matsumoto and H. Imai, Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption, Advances in Cryptology, Proceedings of EUROCRYPT'88, Springer Verlag, pp 419-453;
6. W.B. Muller, Polynomial Functions in Modern Cryptology, Contributions to General Algebra 3: Proceedings of the Vienna Conference, Vienna: Verlag Holder-Picher-Tempsky, 1985, pp. 7-32.
7. J. Patarin, Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypto'88, Advances in Cryptology, Proceedings of CRYPTO'95, Springer Verlag, pp 248-261;
8. J. Patarin, Asymmetric Cryptography with a Hidden Monomial, Advances in Cryptology, Proceedings of CRYPTO'96, Springer Verlag, pp 45-60;
9. J. Patarin, Hidden Fields Equations and Isomorphisms of Polynomials: Two New Families of Asymmetric Algorithms, Advances in Cryptology, Proceedings of EUROCRYPT'96, Springer Verlag, pp 33-48;
10. J. Patarin and L. Goubin, Trapdoor one-way permutations and multivariate polynomials, Proceedings of ICICS'97, Lecture Notes in Computer Science, Vol. 1334, Springer, 1997.
11. J. Patarin and L.Goubin, Asymmetric cryptography with S-boxes, Proceedings of ICICS'97, Lecture Notes in Computer Science, Vol. 1334, Springer, 1997.
12. J. Patarin and L.Goubin, C^*_{-+} and HM: Variations Around Two Schemes of T.Matsumoto and H. Imai, Advances in Cryptology, Proceedings of ASIACRYPT'98, Lecture Notes in Computer Science 1514, Springer Verlag, pp 35-49.

13. R.L. Rivest, A. Shamir, L.M. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of ACM, v.21, n.2, 1978, pp.120-126.

Appendix 1: Homogenlization

For any polynomial $P(X_1, X_2, \cdots, X_n)$ of supposed degree $d \geq \deg(P)$, define its homogenization as $\tilde{P} = X_0^d P(X_1/X_0, X_2/X_0, \cdots, X_n/X_0)$, where X_0 is a new variable. The supposed degree of the component polynomials of a quadratic mapping is 2, and so on. For any mapping $f : K^n \mapsto K^n$ with component polynomials $(f_1, \cdots, f_n)$, define its homogenization as $\tilde{f} = (X_0^{\deg f}, \tilde{f}_1, \cdots, \tilde{f}_n)$. Conversely, for any $\tilde{f}$ of this form, define its dehomogenization to be $f = (\tilde{f}_1(1, X_1, \cdots, X_n), \cdots, \tilde{f}_n(1, X_1, \cdots, X_n))$.

Lemma 2. *Let the f, g be two mappings $K^n \to K^n$. If $q > \deg f \times \deg g$, then $\widetilde{f \circ g} = \tilde{f} \circ \tilde{g}$.*

Proof. In this case, composition of mappings is equivalent to composition of polynomials, and the lemma follows from the fact that homogenization commutes with polynomial composition. □

Suppose we are given a "2R" public key π, if we can decompose $\tilde{\pi} = \tilde{f} \circ \tilde{g}$, then the decomposition $\pi = f \circ g$ can be obtained simply by dehomogenization. The above lemma guarantees the existence of such a decomposition of $\tilde{\pi}$. In decomposing $\tilde{\pi}$ using the method of this paper, we should add the n polynomials $X_0^2 X_1, \cdots, X_0^2 X_n$ to $\tilde{V}$, the space of partial derivatives.

Appendix 2: Some Basic Facts of Linear Algebra

1. The number of subspaces of dimension k in a space of dimension $n > k$ is:

$$\mu(k, n) = \prod_{0 \leq i < k} (q^n - q^i) / \prod_{0 \leq i < k} (q^k - q^i) \approx q^{(n-k)k}$$

2. The number of $n \times N$ matrices with rank $\leq k < \min(n, N)$ is less than

$$q^{kN} \mu(k, n) \approx q^{k(n+N-k)}$$

3. The probability that the intersection of two random subspaces of dimension n_1, n_2 in a space of dimension n has dimension $n_1 + n_2 - n + \delta \geq 0$ ($\delta \geq 0$) is

$$\mu(n - n_2 - \delta, 2n - n_1 - n_2 - \delta)\mu(n - n_1 - \delta, 2n - n_1 - n_2 - \delta)$$
$$\mu(n_1 + n_2 - n + \delta, n)\mu(n_1, n)^{-1}\mu(n_2, n)^{-1} \approx q^{-\delta(n_1+n_2-n+\delta)}$$

4. The probability that a random linear mapping $\sigma : K^{n_1} \to K^{n_2}$ has a kernel of dimension $e = \max(n_1 - n_2, 0) + \delta$ ($\delta \geq 0$) is

$$q^{-n_1 n_2} \mu(e, n_1) \mu(n_1 - e, n_2) \prod_{0 \leq i < n_1 - e} (q^{n_1 - e} - q^i) \approx q^{-e(e+n_2-n_1)}$$

Appendix 3

The following is the source code for our experiments written in Mathematica 3.0.

```
p=251; n=9;
phi={
  x[0]^2 + 235x[4]x[5] + 235x[3]x[6] + 235x[2]x[7] + 235x[1]x[8],
  2x[0]x[1] + 249x[4]x[5] + 243x[5]^2 + 249x[3]x[6] + 235x[4]x[6]
  + 249x[2]x[7] + 235x[3]x[7] + 249x[1]x[8] + 235x[2]x[8],
  x[1]^2 + 2x[0]x[2] + 250x[5]^2 + 249x[4]x[6] + 235x[5]x[6] +
  249x[3]x[7] + 235x[4]x[7] + 249x[2]x[8] + 235x[3]x[8],
  2x[1]x[2] + 2x[0]x[3] + 249x[5]x[6] + 243x[6]^2 + 249x[4]x[7] +
  235x[5]x[7] + 249x[3]x[8] + 235x[4]x[8],
  x[2]^2 + 2x[1]x[3] + 2x[0]x[4] + 250x[6]^2 + 249x[5]x[7] +
  235x[6]x[7] + 249x[4]x[8] + 235x[5]x[8],
  2x[2]x[3] + 2x[1]x[4] + 2x[0]x[5] + 249x[6]x[7] + 243x[7]^2 +
  249x[5]x[8] + 235x[6]x[8],
  x[3]^2 + 2x[2]x[4] + 2x[1]x[5] + 2x[0]x[6] + 250x[7]^2 +
  249x[6]x[8] + 235x[7]x[8],
  2x[3]x[4] + 2x[2]x[5] + 2x[1]x[6] + 2x[0]x[7] + 249x[7]x[8] +
  243x[8]^2, x[4]^2 + 2x[3]x[5] + 2x[2]x[6] + 2x[1]x[7] +
  2x[0]x[8] + 250x[8]^2
  };

tovector2[f_]:=Flatten[Table[Coefficient[f, x[i]x[j]],
                             {i,0,n-1},{j,i,n-1}]];

id=IdentityMatrix[n(n+1)(n+2)/6];
mu[i_,j_,k_]:=Block[{i1,j1,k1},
              If[i<=j, i1=i;j1=j;k1=k, i1=j;
              If[i<=k, j1=i; k1=k, j1=k; k1=i]];
              Return[n(n+1)(n+2)/6-(n-i1)(n-i1+1)(n-i1+2)/6
                     +(n-i1)(n-i1+1)/2-(n-j1)(n-j1+1)/2+k1-j1+1]];

Do[M[i]=id[[Flatten[Table[mu[i,j,k] ,{j, 0, n-1},{k, j, n-1}]]]],
  {i, 0, n-1}];

H=NullSpace[Table[tovector2[phi[[i]]].M[i], {i,0, n-1}],
           Modulus->p];

Do[check[i]=Transpose[M[i].Transpose[H]], {i,0, n-1}];

rank[L_]:=Length[NullSpace[Sum[L[[i+1]]check[i],{i,0, n-1}],
                           Modulus->p]]-n;
```

```
test1[count_]:=Block[{i,L, r}, i=1;
                 While[i<=count,
                    L=Table[Random[Integer,p-1], {j,n}];
                    r=rank[L];
                    If[r>0, Save["result.mat", {i, r, L}]];
                    i++] ];

psi=phi/.Table[x[i]->y[i],{i,0,n-1}];

d[f_, i_]:=Sum[j Coefficient[Collect[f,x[i]],
             x[i]^j]x[i]^(j-1), {j,4}];

tovector3[f_]:=Flatten[Flatten[
                  Table[Coefficient[f,x[i]x[j]x[k]],
                        {i,0,n-1},{j,i,n-1},{k,j,n-1}]]]];

test2[count_]:=Block[{A, f, n0, n1, n2, i, S,r,h},
                 i=1; n0=n1=n2=0;
                 While[i<=count,
                 A=Table[Random[Integer,p-1], {k,n}, {j,n}];
                 f=phi.A ; g=Expand[f, Modulus->p]; S={};
                 h=Expand[psi/.Table[y[j]->g[[j+1]],
                         {j,0,n-1}], Modulus->p];
                 Do[AppendTo[S, tovector3[d[h[[k]], j]]],
                        {k,n}, {j,n}];
                 r=n^2-n(n+1)(n+2)/6+Length[NullSpace[S,
                                             Modulus->p]];
                 Switch[r, 0, n0++, 1, n1++, 2, n2++]; i++];
                 Print[n0]; Print[n1]; Print[n2];];
```