

ℓ -Invertible Cycles for Multivariate Quadratic (\mathcal{MQ}) Public Key Cryptography

Jintai Ding^{1,*}, Christopher Wolf², and Bo-Yin Yang^{3,**}

¹ University of Cincinnati and Technische Universität Darmstadt
ding@math.uc.edu

² Ecole Normale Supérieure
chris@christopher-wolf.de

³ Institute of Information Science, Academia Sinica and TWISC
by@moscito.org

Abstract. We propose a new basic trapdoor ℓ IC (ℓ -Invertible Cycles) of the mixed field type for Multivariate Quadratic public key cryptosystems. This is the first new basic trapdoor since the invention of Unbalanced Oil and Vinegar in 1997. ℓ IC can be considered an extended form of the well-known Matsumoto-Imai Scheme A (also MIA or C^*), and share some features of stagewise triangular systems. However ℓ IC has very distinctive properties of its own. In practice, ℓ IC is much faster than MIA, and can even match the speed of single-field \mathcal{MQ} schemes.

Keywords: Public Key, \mathcal{MQ} , Trapdoor, Encryption, Signing.

1 Introducing \mathcal{MQ} Public Key Cryptosystems

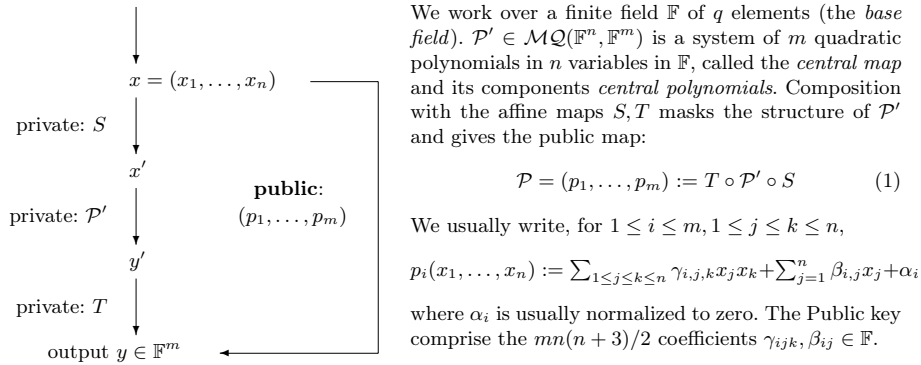


Fig. 1. Illustration of Terminology and Notation for a modern \mathcal{MQ} -trapdoor

Multivariate Quadratic (\mathcal{MQ}) public-key cryptography first appeared in the English literature in the mid '80s [FD85, IM85] as alternatives to traditional

* Also partially sponsored by grants from the Charles Phelps Taft Research Center and the Alexander von Humboldt Foundation.

** Also sponsored by Taiwan's National Science Council project 95-2115-M-001-021 and indirectly via TWISC (Taiwan Information Security Center) @ NTUST.

PKCs. A common excuse given to study them is “for ecological diversity”, inevitably mentioning Quantum Computers that will easily break factoring and discrete-log-based PKCs (Shor’s algorithm [Sho97]). However, we hope to show that there is independent interest in studying \mathcal{MQ} PKCs below.

To construct a PKC, we need to be able to invert \mathcal{P}' efficiently. A simple method to build \mathcal{P}' for consequent inversion is a *basic trapdoor*, which can be combined or modified slightly to create variants. Using the terminology of [WP05b], we have a handful of systemic ways to create new central maps, which we call “Modifiers”, from the following four previously known basic trapdoors:

Mixed-Field (or “Big Field”): Operates over an extension field $\mathbb{E} = \mathbb{F}^k$.

MIA: Matsumoto-Imai Scheme A or C^* ([IM85], Imai-Matsumoto).

HFE: Hidden Field Equations ([Pat96], Patarin), a generalization of MIA.

Single-Field (or “True”): Works on the individual components of x' and y' .

UOV: Unbalanced Oil and Vinegar ([Pat97, KPG99], Patarin *et al*).

STS: Stepwise Triangular System (lectures in Japanese from '85 – [TKI+86], Tsujii; in English, [Sha93]). Generalized later to its present form [GC00, WBP04].

Some primitives are composite, e.g., Medium Field Encryption (triangular stages [WYHL06]) or enTTS/TRMS/Rainbow [DS05b, WHL⁺05, YC05] (UOV stages).

Outline. In the next section, we introduce our new trapdoor and discuss its basic properties. In particular, we show that certain instances can be inverted very quickly. Section 3 give cryptanalytic properties of this basic trapdoor and enumerates possible attacks. Section 4 discusses counter-measures to these attacks, *i.e.*, *modifiers*. We give the practical instances in Section 5. These we verify to withstand known attacks. The main text of the paper concludes with Section 6.

2 ℓ -Invertible Cycles (ℓ IC)

In this section, we will introduce a new basic way to construct central maps for \mathcal{MQ} public key cryptography that does not fit into the above taxonomy and hence can be considered a new basic trapdoor with properties in between that of MIA and STS. It runs much faster than MIA, and hence has practical value especially in resource-limited environments (e.g. smart cards). Due to its structure, we call it “ ℓ -Invertible Cycles” (ℓ IC). We will motivate this name later.

2.1 Basic Trapdoor

A *Cremona Transformation* is a map on the projective plane that is quadratic in the homogeneous coordinates [Ful89]. A standard example is the map $(A_1, A_2, A_3) \rightarrow (A_2A_3, A_3A_1, A_1A_2)$ which easily checks to be well-defined. The map is uniquely and efficiently invertible when $A_1A_2A_3 \neq 0$.

We extend this idea below to any integral cycle length $\ell \geq 2$; we illustrate with the case $\ell = 3$ since (unfortunately) the case $\ell = 2$ is a bit more technical.

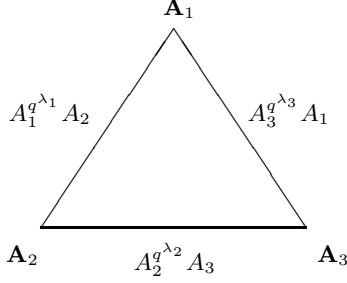


Fig. 2. Graphical Representation of 3-Invertible Cycles

Note that we write \mathbb{N} for the non-negative integers, *i.e.*, we have $\mathbb{N} := \mathbb{Z}^+ \cup \{0\}$. To express properly the successor in $\{1, \dots, \ell\}$ we define

$$\mu : \{1, \dots, \ell\} \rightarrow \{1, \dots, \ell\} : \mu(i) := \begin{cases} 1 & \text{for } i = \ell \\ i + 1 & \text{otherwise} \end{cases} \quad (2)$$

Definition 1. Fix an integer $\ell \geq 2$ as the length of the cycle. Let \mathbb{F} be the base field with $q := |\mathbb{F}|$ elements and $\mathbb{E} := GF(q^k)$ its k^{th} -degree extension for some $k \in \mathbb{Z}^+$. Computations in \mathbb{E} are modulo the irreducible polynomial $\pi(t) \in \mathbb{F}[t]$. We denote $Q := |\mathbb{E}| = q^k$ and have $m = n = \ell k$ for the number of variables and equations over the ground field \mathbb{F} , respectively. In addition, let $S, T \in \text{Aff}^{-1}(\mathbb{F}^n)$ be two invertible affine mappings and the vector $\Lambda := (\lambda_1, \dots, \lambda_\ell) \in \{0, \dots, k - 1\}^\ell$. We now have the following mapping:

$$P : \mathbb{E}^\ell \rightarrow \mathbb{E}^\ell : (A_1, \dots, A_\ell) \rightarrow (A_1^{q^{\lambda_1}} A_2, \dots, A_{\ell-1}^{q^{\lambda_{\ell-1}}} A_\ell, A_\ell^{q^{\lambda_\ell}} A_1) \quad (3)$$

Identifying the corresponding coefficients in the vector spaces \mathbb{F}^n and \mathbb{E}^ℓ , we get a canonical bijection

$$\phi : \mathbb{F}^n \rightarrow \mathbb{E}^\ell : (x_1, \dots, x_n) \rightarrow (x'_1 + x'_2 t + \dots + x'_k t^{k-1}, \dots, x'_{n-k+1} + x'_{n-k+2} t + x'_n t^{k-1}) \quad (4)$$

and its inverse ϕ^{-1} . The public key is computed as the composition

$$\mathcal{P} : \mathbb{F}^n \rightarrow \mathbb{F}^m : \mathcal{P} := T \circ \phi^{-1} \circ P \circ \phi \circ S. \quad (5)$$

We then call such a Multivariate Quadratic public key system of the ℓ IC-type.

The name “invertible cycle” is due to that the variables A_1, \dots, A_ℓ can be drawn in the form of a cycle (cf. Fig. 2 for $\ell = 3$). The variables $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$ are the nodes while each edge stands for a product $A_i^{q^{\lambda_i}} A_{\mu(i)}$ with $i = 1, 2, 3$.

Note that the use of the canonical bijection ϕ is similar for the Matsumoto-Imai Scheme A (MIA) and Hidden Field Equations (HFE). However, we have $\ell = 1$ here, and also a different form of the central mapping $P \in \mathbb{E}[X]$. In the sequel, we denote the output of P by B_1, \dots, B_ℓ , where

$$B_1 := A_1^{q^{\lambda_1}} A_2, \dots, B_{\ell-1} := A_{\ell-1}^{q^{\lambda_{\ell-1}}} A_\ell, B_\ell := A_\ell^{q^{\lambda_\ell}} A_1$$

Remark 1. The mapping $A_i^{q^{\lambda_i}}$ is linear over the ground field \mathbb{F} . Hence, the central equation P can be expressed as quadratic polynomials over \mathbb{F} .

Remark 2. Replacing $A_i^{q^{\lambda_i}} A_{\mu(i)}$ by $A_i^{q^{\lambda_i}} A_{\mu(i)}^{q^{\kappa_i}}$ for $1 \leq i \leq \ell$ and some $\kappa_i \in \mathbb{N}$ does not increase the security of ℓ IC: we can always reduce the second expression to $A_i^{q^{\lambda_i - \kappa_i \pmod{k}}} A_{\mu(i)}$ by using Frobenius transformations. In a nutshell, we exploit that Frobenius transformations are invertible linear mappings over the vector spaces \mathbb{F}^n and \mathbb{F}^k , respectively, and can hence be “absorbed” into the mappings $S, T \in \text{Aff}^{-1}(\mathbb{F}^n)$. For \mathcal{M} ultivariate \mathcal{Q} uadratic systems, this idea has been introduced under the name *Frobenius sustainers* [WP05a].

2.2 Singularities

To use ℓ IC in as an encryption or as a signature scheme, we need to invert the central map P , *i.e.*, we need to find a solution $(A_1, \dots, A_\ell) \in \mathbb{E}^\ell$ for given input $(B_1, \dots, B_\ell) \in \mathbb{E}^\ell$. Unfortunately, this is not possible in all cases; due to its form ℓ IC has the following singularities:

$$\{ (A_1, \dots, A_\ell) \in \mathbb{E}^\ell \mid A_1 = 0 \vee \dots \vee A_\ell = 0 \}$$

Having $Q := |\mathbb{E}|$ and exploiting that Q in comparison with ℓ is usually “big” for practical and secure schemes we can approximate the probability that a singularity occurs by

$$\left(\sum_{i=1}^{\ell} (Q - 1)^{\ell-1} \right) / Q^\ell \approx \frac{\ell}{Q}$$

In the Matsumoto-Imai Scheme A, we do not have this problem as MIA forms a bijection. In comparison, Hidden Field Equations does not allow to compute an inverse in about 40% of all cases for a practical choice of parameters [Pat96, CGP01, WP04]. Our new trapdoor ℓ IC is hence between these two extreme cases. Practical values for Q will be discussed in Sec. 5.

2.3 Inversion

As we have as many free variables A_i as conditions B_i for $1 \leq i \leq \ell$, we may expect one solution on average when inverting P . Alas, this is not always true, as shown by the obvious counterexample:

$$(B_1, B_2) := P(A_1, A_2) := (A_1 A_2, A_2 A_1) \in \mathbb{E}^2.$$

So some instances of ℓ IC that cannot be inverted usefully. For practical use, we construct below a sequence of specific ℓ IC instances which allows easy inversion.

Lemma 1. *For a fixed $\ell \geq 2$, let our ℓ IC central map $P : (A_1, \dots, A_\ell) \mapsto (B_1, \dots, B_\ell)$ be*

$$B_1 := \begin{cases} A_1 A_2 & \text{for } \ell \text{ odd and} \\ A_1^q A_2 & \text{for } \ell \text{ even} \end{cases}, \quad B_i := A_i A_{\mu(i)} \text{ for } 2 \leq i \leq \ell.$$

Then the inverse image of $(B_1 \dots B_\ell)$, where $B_i \in \mathbb{E}^* := \mathbb{E} \setminus \{0\}$, $\forall i$ is given by

$$A_1 := \begin{cases} \sqrt{\frac{\prod_{i=0}^{(\ell-1)/2} B_{2i+1}}{\prod_{i=1}^{(\ell-1)/2} B_{2i}}} & \text{for } \ell \text{ odd and} \\ q^{-1} \sqrt{\frac{\prod_{i=0}^{\ell/2-1} B_{2i+1}}{\prod_{i=1}^{\ell/2} B_{2i}}} & \text{for } \ell \text{ even} \end{cases} \quad A_i := \frac{B_i}{A_{\mu(i)}} \text{ for } i = 2, \dots, \ell.$$

Proof. Case $\ell = 3$: We have $B_1 := A_1 A_2, B_2 := A_2 A_3, B_3 := A_3 A_1$. Simple computations yield $A_1 := \sqrt{B_1 B_3 / B_2}, A_3 := B_3 / A_1, A_2 := B_2 / A_3$.

Case ℓ odd, $\ell > 3$: We use induction to extend the result from $\ell = 3$ to all odd $\ell > 3$. Therefore we observe that the structure of the central mapping P allows us to write equations of the form $A_i = A_{\mu(\mu(i))} \frac{B_i}{B_{i+1}}$ for $1 < i < \ell$ by eliminating the variable $A_{\mu(i)}$. Hence, the fraction $\frac{B_i}{B_{i+1}}$ can be inserted in the inversion formula for A_1 in the case $(\ell - 2)$.

Case ℓ even: The proof for this case is analogous. We start our induction with $\ell = 2$ and have $B_1 := A_1^q A_2, B_2 := A_2 A_1$ and its inverse $A_1 := q^{-1} \sqrt{B_1 / B_2}, A_2 := B_2 / A_1$.

Bijectivity. For ℓ odd or \mathbb{F} of characteristic 2, the above mapping is a bijection in $(\mathbb{E}^*)^\ell$. For ℓ even, the situation is more difficult as $(q - 1) \mid (q^a - 1)$ for any $a \in \mathbb{Z}^+$, and we lose bijectivity for any $q > 2$. However, for $q = 2$, we obtain a bijection. Moreover, inversion now only costs two divisions in the extension field \mathbb{E} and we need not solve any nontrivial equations.

Special instances. When $\ell = 2$ we say it is a *Binary Invertible Cycle* (2IC) and when $\ell = 3$ a *Delta Invertible Cycle* (3IC) (see Fig. 2).

3 Cryptanalytic Properties of ℓ IC

We herein discuss some basic cryptanalytic properties of the new trapdoor. This serves a dual purpose: We find an easy cryptanalysis for ℓ IC in its basic form. Simultaneously, we effectively put ℓ IC through the same screening process as other \mathcal{MQ} trapdoors, particularly Matsumoto Imai Scheme A. This points us toward ways to build practical, more resilient ℓ IC-based schemes.

One attack is left to a later section because we only heard of it succeeding, and do not even have any details.

3.1 Patarin Relations

We start with an extension of the Patarin relations used to cryptanalyse MIA [Pat95]. This was used by Fouque, Granboulan, and Stern to cryptanalyse the internally perturbed MIA encryption scheme (PMI/MIAi) [FGS05]. As is more customarily employed against symmetric cryptosystems, we examine this multivariate differential :

$$\begin{aligned} P(A_1, \dots, A_\ell) - P(A_1 - \delta_1, \dots, A_\ell - \delta_\ell) + P(\delta_1, \dots, \delta_\ell) \\ = (A_1^{q^{\lambda_1}} \delta_2 + A_2 \delta_1^{q^{\lambda_1}}, \dots, A_\ell^{q^{\lambda_\ell}} \delta_1 + A_1 \delta_\ell^{q^{\lambda_\ell}}) \end{aligned}$$

We observe that the above equations are linear in the unknowns $A_i \in \mathbb{E}$ for any given values $\delta_i \in \mathbb{E}$ and $1 \leq i \leq \ell$. Now we simply pick δ_i at random and compute many differentials of the public key. Soon we recover enough linear relations to invert the public map. This effectively finds an equivalent private key. It may be estimated that the number of linearization equations for $\mathbb{F} = \text{GF}(2)$ is 4ℓ , which we do not have space to describe here.

This resembles MIA and HFE in that the Patarin attack is very efficient against the former, and an extended version of the attack defeats the latter if bijective central maps are used [Pat95, Pat96].

3.2 Rank Attacks

In a *rank attack*, the quadratic parts central and public polynomials of a given Multivariate Quadratic public key system are written as symmetric matrices. We try to recover the private key by finding linear combinations of the public matrices with certain specific ranks. Their initial cryptographical use was by Coppersmith-Stern-Vaudenay to break Birational Permutations [CSV93]. Goubin and Courtois [GC00] have the most straightforward exposition of rank attacks. Later extensions and analysis can be seen in [WBP04, YC05].

There are two distinct types: In one the cryptanalyst randomly tries to hit kernel vectors of a linear combination of the public matrices with the lowest rank R . The running time is proportional to $q^{R\lceil m/n \rceil}$. In the other random linear combinations are taken, hoping to locate a precipitous fall in rank. This takes time $\propto q^u$, where u counts the central equations whose coefficients must vanish.

For ℓ IC, we want to write matrices in blocks corresponding to pairs of variables in the larger field \mathbb{E} . Express central matrices as $H_1, \dots, H_\ell \in \mathbb{E}^{\ell \times \ell}$ and their \mathbb{E} -blocks as $\eta_{i,j,k} \in \mathbb{E}$ for $1 \leq i, j, k \leq \ell$.

$$\eta_{i,j,k} := \begin{cases} M_{\lambda_i} & \text{if } i = j, k = \mu(i), \\ M_{\lambda_i}^T & \text{if } i = k, j = \mu(i), \\ 0 & \text{otherwise,} \end{cases}$$

where M_r is the matrix in $\mathbb{F}^{k \times k}$ that correspond to the Frobenius map $A \mapsto A^{q^r}$. Note that these matrices are symmetric. In the case of 3IC, *i.e.*, $\ell = 3$, they effectively specialize to

$$H_1 := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad H_2 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad H_3 := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

All these matrices have essentially rank 2 over the extension field \mathbb{E} . For the actual attack, we would need to transfer $M \in \mathbb{E}^{\ell \times \ell}$ to $\mathbb{F}^{n \times n}$. However the overall attack complexity is not affected by this change of vector space. Just as in other schemes using extension fields (e.g. cf. Medium Field Encryption [WYHL06]), when performed in \mathbb{F} we have a rank of $2k$ for all these matrices. We may see that the running time of the both the above algorithms are $Q^2 = q^{2k}$ times some polynomial factor in n and m , which is cubic in the practical range.

Note that there are instances in which one or the other rank attack simply fails to work. One example is the case of 2IC, *i.e.*, for $\ell = 2$. Here rank attacks will not apply as any nontrivial linear combination of the private polynomials (matrices) has the maximum rank $n = 2k$. The above discussion of rank attacks are in line with results of tests on ℓ IC and modified ℓ IC schemes with blocks of 24 and 32 bits (which are admittedly very small).

3.3 Gröbner Basis Computations

Another important type of attack are Gröbner attacks as in the cryptanalysis of HFE [FJ03]. The most powerful algorithms known are of the Faugère-Lazard type. These essentially run eliminations on an extended Macaulay matrix, and include $\mathbf{F}_4/\mathbf{F}_5$ and what is known as XL [CKPS00, Fau99, Fau02] plus variations.

We know from the cryptanalysis of MIA and HFE that their easy algebraic structure leads to a low running time of the corresponding Gröbner bases algorithm. Due to the very easy structure of ℓ IC, we expect a similar behaviour here. This is in line small scale experiments using Magma [MAG], so we must disrupt the regular structure. In general, when the structure of the system is sufficiently perturbed, the behavior is as in generic systems studied by Bardet, Faugère *et al* [BFS04, BFSY05, YC04b, YC04a]. E.g., we tested 3IC⁻ systems with MAGMA v2.12-8 on a 2GB machine using $\mathbb{E} = (\text{GF}(256))^4$ or $(\text{GF}(256))^5$. If we removed at least two components, the resulting system resolved in exactly the amount of time as a generic one (including segfaulting on 13-variable systems). With only one component removed, it resolved nearly instantly.

3.4 Separation of Oil and Vinegar

In the original 3IC, we see that variables corresponding to the components of A_1 are only multiplied with those of A_2 and A_3 . This makes for a UOV type of attack [KPG99] which has a complexity roughly proportional to $n^4 q^d$, where d is the difference between the size of the oil and vinegar sets. We can proceed similarly for other choices of ℓ . We see that the UOV attack has time complexity $\sim Q$ for odd ℓ and very small complexity for even ℓ . Since the minus modifier does not change the complexity of the UOV attack, 3IC⁻ as a signature scheme is ok if we use large enough Q . The plus modifier disrupts the UOV attack so the 2IC⁺ that we will investigate later is not susceptible.

3.5 Further Attacks

There is a special attack from Felke [Fel04] to defeat the technique called “branching” as used in the original C^* . We have investigated this matter and concluded that the attacks against branching do not apply against ℓ IC.

A different class from XL are algorithms from [CGMT02] which deal with the case $n \gg m$. As we usually have $m = n$, or $n \approx m$ for the embedding modification (cf Sec. 4.3), these algorithms are not applicable to our setting.

4 Modified Versions

Due to the effectiveness of the attacks considered above, we need to apply modifiers [WP05b, Sec. 4] to the basic trapdoor to obtain secure schemes. This is the same situation as for MIA and HFE. To the best of our knowledge every published attack against a system of this type is covered by this paper.

4.1 ℓ -Invertible Cycles Minus (ℓ IC-)

The first modification is the so-called “minus” modification. Here, Let R be the projection from $\mathbb{F}^n \mapsto \mathbb{F}^m$ that simply discards the final parameters. $r := n - m$ as “reduction parameter”. The public key is now $\mathcal{P} := R \circ T \circ \phi^{-1} \circ P \circ \phi \circ S$. In contrast to (5), we have inserted the reduction R after the affine transformation T . When inverting ℓ IC, we assign random values to these missing r coordinates over \mathbb{F} . Hence, we have q^r possible inputs for each message $y \in \mathbb{F}^m$.

As for MIA and HFE, the minus modifier increases the complexity of the Patarin attack (Sec. 3.1) by a factor of q^r , since instead of one possible solution, the attacker is now faced with an r -dimensional vector space over \mathbb{F} of possible solutions. To our current knowledge, picking the right one requires brute force and hence at least q^r operations. In addition, the attack complexity of the Faugère-Joux attack [FJ03] also increases by at least q^r .

Like with MIA, we cannot use ℓ IC- for encryption, only for signature schemes: as there are r equations missing, the legitimate user must work equally hard to recover the correct solution $x \in \mathbb{F}^n$. As our security assumption is that q^r computations are not possible, we reached a contradiction if we assume that the legitimate user can obtain the message x while the attacker cannot. As for Stepwise-Triangular, rank attacks are unaffected by the minus modification.

4.2 ℓ -Invertible Cycles Internally Perturbed Plus (ℓ ICi+)

The generic plus modifier adds $a \in \mathbb{Z}^+$ random equations in n input variables each to the private key. This is applicable to encryption only, as the extra equations (without trapdoor) slow down signature generation by q^a — it takes that many tries to find one output of the ℓ IC mapping P to meet those conditions.

Patarin relations and Gröbner attacks are not affected by the plus modification. However, it is still useful to build an encryption scheme. In the case of MIA because the “plus” helps to overcome some attacks against the internally perturbed modification. Here, it also prevents a UOV attack.

Internal perturbation has been introduced for MIA and HFE as PMI (“Perturbed Matsumoto-Imai”) and ipHFE respectively [Din04, DS05a]. We can also call them MIAi and HFEi. As PMI/MIAi has been broken in [FGS05], a new variant PMI+/MIAi+ has been proposed [DG06]. Due to space limitations we do not go into details, but we believe PMI+ unaffected by the attack from [FGS05]. Hence, combining the two modifications *internal perturbation* and *plus* allows the construction of an efficient encryption scheme. However, the central

mapping \mathcal{P}' and all its components need to have full rank. In our setting, this means that we cannot use any other cycle length but $\ell = 2$, *i.e.*, 2IC.

After talking about the impact of the internal perturbation modification, we now properly introduce it: Let $w \in \mathbb{Z}^+$ for $w < n$ be the perturbation dimension, $\mathcal{P}^i \in_R \mathcal{MQ}(\mathbb{F}^w, \mathbb{F}^n)$ a uniformly randomly chosen system in w input variables and n equations, and $S^i \in \text{Aff}^{-1}(\mathbb{F}^n, \mathbb{F}^w)$ the so-called “perturbation space”. Note that the perturbation space has the same input variables x_1, \dots, x_n as the affine transformation $S \in \text{Aff}^{-1}(\mathbb{F}^n)$. However, it has only dimension w . Hence we can write $(z'_1, \dots, z'_w) := S^i(x_1, \dots, x_n)$ for the perturbation variables z'_1, \dots, z'_w . As for the plus modification, we denote with $\mathcal{P}^* := \phi^{-1} \circ P \circ \phi$ the ℓ IC mapping over the ground field \mathbb{F} .

The public key for ℓ ICi is now composed as

$$\mathcal{P} := T \circ [(\mathcal{P}^* \circ S) + (\mathcal{P}^i \circ S^i)],$$

i.e., we add the perturbation polynomials to the original ℓ IC-polynomials. To invert this modified trapdoor, *i.e.*, to compute $x \in \mathbb{F}^n$ for given $y \in \mathbb{F}^m$, we need to guess correctly the values of the perturbation variables $(z'_1, \dots, z'_w) \in \mathbb{F}^w$ — which translates to a workload proportional to q^w . As the number of equations and the number of variables matches, we expect one solution on average for any given input $y \in \mathbb{F}^m$. However, when used as an encryption scheme, there is at least one valid output $x \in \mathbb{F}^n$. We know that the i modifier by itself is not secure, and it must be combined with the $+$ modifier as shown by the Fouque-Granboulan-Stern differential attack [FGS05].

4.3 ℓ -Invertible Cycles Embedded (ℓ IC \nearrow) Without Singularities

Here we introduce the new modifier embedding (\nearrow), motivated by the practical need to avoid singularities in trapdoors of the ℓ IC-type.

With the minus modification, singularities are of no concern: they are too few and we can always change the input in the missing equations to obtain a possible signature. However, when ℓ IC is used in the context of an encryption scheme, its singularities pose a problem as they lead to decryption failures. The modification described in this section can also be used in other schemes which suffer from a decryption failure such as [WYHL06]. In fact, it is a new generic modifier and can be used in any Multivariate Quadratic construction.

For our new embedding modifier we embed the following translation from $\mathbb{F}^{k-1} \rightarrow \mathbb{F}^k$ that takes (x_1, \dots, x_{k-1}) to $(x_1, \dots, x_{k-1}, 1)$. In effect, we have eliminated the zero-point from the vector space \mathbb{F}^k . As we used the canonical bijection ϕ between the vector space \mathbb{F}^k and the extension field \mathbb{E} , the zero of \mathbb{E} cannot be reached anymore for any given input $(x_1, \dots, x_{k-1}) \in \mathbb{F}$. The price we pay are fewer input variables, *i.e.*, we now obtain an overdetermined system of polynomials. We can do the same to all ℓ variables $A_1, \dots, A_\ell \in \mathbb{E}$. Calling the corresponding transformation $\nu : \mathbb{F}^n \rightarrow \mathbb{F}^{n-\ell}$ and setting $k := (n - \ell)/\ell$ for $k \in \mathbb{N}$ we obtain the following construction for the public key

$$\mathcal{P} = T \circ \phi^{-1} \circ P \circ \nu \circ S. \tag{6}$$

To do signing, the “inverse” transformation $\nu^{-1} : (y_1, \dots, y_{k-1}, 1) \rightarrow (y_1, \dots, y_{k-1})$ needs to be inserted between the affine transformation T and the ℓ IC mapping P . To the same effect, we could have used the construction of (6). However, this would have slowed down signature generation by a factor of q^ℓ as we have ℓ additional equations over \mathbb{F} to satisfy for any given input $B_1, \dots, B_\ell \in \mathbb{E}$.

5 Practical Instances

We use the previous section to develop practical instances of ℓ IC. Main purpose is to see how variations on ℓ IC scales up for different security levels.

5.1 Signature

To obtain a secure signature scheme, we use ℓ IC-, in particular 3IC-, as this seems the most suitable modification for our purpose. In particular, the security of the minus modification is well understood; we are therefore able to give instances of ℓ IC- for several security levels. Different choice of parameters are possible, 3IC- with $q = 256$ seems most suitable(cf. Sec. 3), and still allows efficient implementation on 8-bit microprocessors which are still dominant in low-end smart cards. We summarize optimal choices in Table 1. Preliminary tests show that ℓ IC- is orders of magnitude faster than MIA-; further data will be posted if we can avoid the differential attack on ℓ IC-.

Table 1. ℓ IC- over GF(256) with Different Security Levels for Signing

Claimed Security	Input [bits]	Output [bits]	n		Parameters			Attack Complexity		Key Size [kBytes]	
			m	ℓ	k	r	Gröbner	Rank/UOV	Public	Private	
2^{80}	160	240	30	20	3	10	20	2^{80}	2^{85}	9.92	1.86
2^{96}	192	288	36	24	3	12	24	2^{96}	2^{104}	16.8	2.59
2^{128}	256	384	48	32	3	16	32	2^{130}	2^{137}	39.20	4.70

5.2 More on Differential Attacks

[FGS05] was a differential attack in the classical sense – take differentials and try to find a distinguisher. It was announced at the rump session of Asiacrypt 2006 that SFLASH (MIA-) was finally broken on the extension of such an attack. This is so far an unpublished attack, because the details are very sketchy. However, due to the extreme similarity between MIA and ℓ IC, if SFLASH (MIA-) cannot be patched, ℓ IC- will likely suffer the same fate, so now we do not recommend ℓ IC- unless this can be circumvented.

5.3 Encryption

We base our proposed encryption scheme on 2ICi+↗, *i.e.*, 2-Invertible Cycles with internal perturbation, added equations, and embedding (to avoid decryption

errors). With this choice of scheme, we suggest the following parameters: $q = 2, n = 132, m = 146, \ell = 2, k = 67, w = 6, a = 12$. This leads to a public key of 160.2 kBytes and a private key of 5.7 kBytes, respectively. The claimed security level is 2^{80} . Our choice of parameters is based on [DG06]. Due to space limitations in this paper we do not repeat their arguments but point to [DG06]. However, we want to stress that at present, our understanding of the security of the internal perturbation modification is limited although there some results on Gröbner bases in [DGS⁺05]. This means in particular that we do not have precise security estimations for higher security levels.

5.4 Implementation and Speed

A good overview on implementing finite field operations can be found in [LD00]. Computing direct division in finite fields is given in [FW02]. Counting operations for the inversion formula in Lemma 1 over $\mathbb{E} = \text{GF}(q^k)$, we see that we need ℓ divisions, $(\ell - 2)$ multiplications, and one root. Note that the operations do not take place in a big field $\text{GF}(q^n)$ but in a much smaller extension field $\text{GF}(q^k)$. It is difficult to give a closed formula for the speed of basic arithmetic operations as they largely depend on the model used, *e.g.*, hardware vs. software, operations on bits vs. operations on processor words. Nevertheless, when counting our costs in operations in the ground field \mathbb{F} , we can roughly say that we have $O(a^2)$ for squaring/multiplying and $O(a^3)$ for division/exponentiation. Here we have $l \in \mathbb{Z}^+$ the extension degree of the corresponding field $\mathbb{E} = \text{GF}(q^a)$ over the ground field $\mathbb{F} = \text{GF}(q)$. We have to keep this in mind when comparing ℓIC with the other two mixed field schemes MIA and HFE.

Comparison with MIA and HFE. Inverting the mixed field scheme MIA costs one exponentiation with large exponent [CGP02]. In a nutshell, this translates to n squaring operations and $1/2n$ multiplications in $\text{GF}(q^n)$. Therefore, we obtain an overall workload of $O(n^3)$. Tricks to speed this operation up can be found in [ACDG03]. In the case of HFE, the situation is even worse as we need to execute a complete root finding algorithm to invert the central mapping [CGP01]. Its running time is estimated to be in $O(n^3d^2 + n^2d^3)$ for d the total degree of the central mapping [Pat96]. In practice, we have $d = 129, \dots, 257$.

We can summarize our results for the three maps MIA, HFE, and ℓIC as follows: the first needs $O(n^3)$ operations in the ground field \mathbb{F} for n the extension degree as it needs to compute Y^h for given $Y \in \text{GF}(q^n)$ and $h \in \mathbb{Z}^+$, *i.e.*, an exponentiation. The second needs to solve a univariate polynomial equation $P(X) = Y$ for P being a polynomial of fixed degree $d \in \mathbb{Z}^+$. The corresponding running time is about $O(n^3d^2 + n^2d^3)$ operations in the ground field \mathbb{F} . Finally, ℓIC needs $O(\ell k^3 + \ell k^2)$ operations over the ground field \mathbb{F} .

A choice for MIA is SFLASH^{v2} with $q = 128, n = 37$ [CGP02]. For HFE, we have $q = 2, n = 103$ in Quartz [CGP01]. Choices for ℓIC are given in Sec. 5.3 and Table 1, respectively. Both trapdoors have a claimed security level of 2^{80} 3DES computations as required in NESSIE [NES]. Note that Quartz uses the underlying trapdoor four times to achieve very short signatures of 128 bit. This

special construction is called a “Chained Patarin Construction” (CPC). We summarize our comparison in Table 2. Preliminary runs to sign with $m = 24, n = 36$ matches the speed enTTS [YC05] which means it is much faster than SFLASH.

Further Speed up. ℓ IC is amenable to parallelizing on multiple arithmetic units.

ℓ IC i+ implementations. We compare simple runs of ℓ IC i+ on a 10MHz 8052 simulator with $q = 2, n = 134, m = 146, \ell = 2, k = 67, w = 6, a = 12$ (public key 160.2 kBytes, private key 5.7 kBytes), and per transmission time 1.4 seconds. Our PMI+ program has $n = 84, m = 96, q = 2$, and a transmission time of 2.5 seconds per block. ℓ IC i+ is clearly quite a bit faster.

6 Conclusions

In this article, we have constructed a new basic Multivariate Quadratic trapdoor called ℓ -invertible cycles (ℓ IC). It is the first time since nearly a decade that a basic trapdoor has been found. The main motivation for this new trapdoor is speed: instead of computing operations in the big finite field $\mathbb{E} = \text{GF}(q^n)$ for $q := |\mathbb{F}|$ and n the number of variables, we compute in the much smaller extension field $\mathbb{E} = \text{GF}(q^k)$ for $n = \ell k$ for some cycle length ℓ . Typical choices of ℓ are 2 and 3. Depending on the architecture, finite field arithmetic costs up to $O(n^3)$. Hence, decreasing the size of the extension field \mathbb{E} results in a significant speed-up in practice. In particular, our implementation is expected to outperform the previously fastest trapdoor Matsumoto-Imai Scheme A (MIA). In addition, we have formally introduced the new embedding modifier (\nearrow). It is motivated by the practical need to achieve ℓ IC-type schemes without decryption failure. Apart from ℓ IC, constructions like [WYHL06] suffer from this problem.

Table 2 shows the different complexities, parameters and public key sizes for trapdoors of the mixed field types with a claimed security level of 2^{80} . Unfortunately, we do not have exact estimations on their inherent complexity but asymptotic ones. Nevertheless, we see that ℓ IC for a similar security level is expected to perform significantly better than the two other basic trapdoors HFE (using parameters from Quartz) and MIA (parameters from SFLASH^{v2}). Apart from this, we have shown that ℓ IC can be used both in signature schemes of various security levels as well as in an encryption scheme. We want to stress

Table 2. Mixed Field Trapdoors with Claimed Security Level 2^{80}

Trapdoor	Complexity to Invert Trapdoor	Parameters	Key Size [kBytes]	
			Public	Private
HFE (Quartz)	$O(n^3 d^2 + n^2 d^3)$	$q = 2, n = 103, d = 129$	71	3
MIA (Sflash)	$O(n^3)$	$q = 128, n = 37$	15.4	2.45
ℓ IC, $\ell = 3$	$O(\ell k^3 + \ell k^2)$	$q = 256, k = 10$	9.92	1.86

here that trapdoors from the single field class, *i.e.*, Unbalanced Oil and Vinegar (UOV) and Stepwise-Triangular Schemes (STS) do *not* allow constructions leading to encryption schemes.

So as an overall conclusion, we have presented a new trapdoor which is both interesting from a theoretical point of view and also has advantages over previously known schemes. At present we have to leave it as an open question exactly which forms of ℓ IC than these given in Lemma 1 allow efficient inversion.

We stress that it is still an original sin that no list of possible attacks can be exhaustive. Multivariate Quadratic schemes are still in need of some provable security results. But we hope to have shown that the variety available in the genre keeps it in play and interesting.

Acknowledgements

The authors would like to thank TWISC (Taiwan Information Security Center) for sponsoring a series of lectures on \mathcal{MQ} cryptosystems at Nat'l Taiwan U. of Sci. and Tech. in January 2006, the discussions following which led to this work.

Note: An updated version will be made available online either at the authors' website or at ePrint archive after more details are known about the new attacks.

References

- [ACDG03] Mehdi-Laurent Akkar, Nicolas T. Courtois, Romain Duteuil, and Louis 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.
- [ACN05] *Conference on Applied Cryptography and Network Security — ACNS 2005*, volume 3531 of *Lecture Notes in Computer Science*. Springer, 2005. ISBN 3-540-26223-7.
- [BFS04] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004. Previously appeared as INRIA report RR-5049.
- [BFSY05] M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. In P. Gianni, editor, *MEGA 2005 Sardinia (Italy)*, 2005.
- [CGMT02] Nicolas Courtois, Louis Goubin, Willi Meier, and Jean-Daniel Tacier. Solving underdefined systems of multivariate quadratic equations. In *Public Key Cryptography — PKC 2002*, volume 2274 of *Lecture Notes in Computer Science*, pages 211–227. David Naccache and Pascal Paillier, editors, Springer, 2002.
- [CGP01] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Quartz: Primitive specification (second revised version)*, October 2001. <https://www.cosic.esat.kuleuven.be/nessie> Submissions, Quartz, 18 pages.

- [CGP02] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Sflash: Primitive specification (second revised version)*, 2002. <https://www.cosic.esat.kuleuven.be/nessie>, Submissions, Sflash, 11 pages.
- [CKPS00] Nicolas T. Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 392–407. Bart Preneel, editor, Springer, 2000. Extended Version: <http://www.minrank.org/xlfull.pdf>.
- [Cry93] Douglas R. Stinson, editor. *Advances in Cryptology — CRYPTO 1993*, volume 773 of *Lecture Notes in Computer Science*. Springer, 1993. ISBN 3-540-57766-1.
- [CSV93] Don Coppersmith, Jacques Stern, and Serge Vaudenay. Attacks on the birational permutation signature schemes. In *Crypto [Cry93]*, pages 435–443.
- [DG06] Jintai Ding and Jason Gower. Inoculating multivariate schemes against differential attacks. In *PKC*, volume 3958 of *LNCS*. Springer, April 2006. Also available at <http://eprint.iacr.org/2005/255>.
- [DGS⁺05] Jintai Ding, Jason E. Gower, Dieter Schmidt, Christopher Wolf, and Z. Yin. Complexity estimates for the F_4 attack on the perturbed Matsumoto-Imai cryptosystem. In *CCC*, volume 3796 of *LNCS*, pages 262–277. Springer, 2005.
- [Din04] Jintai Ding. A new variant of the Matsumoto-Imai cryptosystem through perturbation. In *Public Key Cryptography — PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 305–318. Feng Bao, Robert H. Deng, and Jianying Zhou (editors), Springer, 2004.
- [DS05a] Jintai Ding and Dieter Schmidt. Cryptanalysis of HFEv and internal perturbation of HFE. In *PKC [PKC05]*, pages 288–301.
- [DS05b] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *ACNS [ACN05]*, pages 164–175.
- [Fau99] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139:61–88, June 1999.
- [Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *International Symposium on Symbolic and Algebraic Computation — ISSAC 2002*, pages 75–83. ACM Press, July 2002.
- [FD85] Harriet Fell and Whitfield Diffie. Analysis of public key approach based on polynomial substitution. In *Advances in Cryptology — CRYPTO 1985*, volume 218 of *Lecture Notes in Computer Science*, pages 340–349. Hugh C. Williams, editor, Springer, 1985.
- [Fel04] Patrick Felke. On the affine transformations of HFE-cryptosystems and systems with branches. *Cryptology ePrint Archive*, Report 2004/367, 2004. <http://eprint.iacr.org/2004/367>, version from 2004-12-17, 10 pages.
- [FGS05] Pierre-Alain Fouque, Louis Granboulan, and Jacques Stern. Differential cryptanalysis for multivariate schemes. In *Advances in Cryptology — EUROCRYPT 2005*, *Lecture Notes in Computer Science*. Ronald Cramer, editor, Springer, 2005. 341–353.

- [FJ03] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equations (HFE) using Gröbner bases. In *Advances in Cryptology — CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Dan Boneh, editor, Springer, 2003.
- [Ful89] William Fulton. *Algebraic curves. An introduction to algebraic geometry, a Reprint of 1969 original in Advanced Book Classics*. Addison-Wesley Publishing Company, Redwood City, CA, 1989. ISBN: 0-201-51010-3.
- [FW02] Patrick Fitzpatrick and Christopher Wolf. Direct division in factor rings. *Electronic Letters*, 38(21):1253–1254, October 2002. Extended version: <http://eprint.iacr.org/2004/353>, 7 pages.
- [GC00] Louis Goubin and Nicolas 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.
- [IM85] Hideki Imai and Tsutomu 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.
- [KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar signature schemes. In *Advances in Cryptology — EUROCRYPT 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Jacques Stern, editor, Springer, 1999.
- [LD00] Julio López and Ricardo Dahab. An overview of elliptic curve cryptography. Technical report, Institute of Computing, State University of Campinas, Brazil, 22nd of May 2000. <http://citeseer.nj.nec.com/333066.html> or <http://www.dcc.unicamp.br/ic-tr-ftp/2000/00-14.ps.gz>.
- [MAG] Computational Algebra Group, University of Sydney. *The MAGMA Computational Algebra System for Algebra, Number Theory and Geometry*. <http://magma.maths.usyd.edu.au/magma/>.
- [NES] NESSIE: New European Schemes for Signatures, Integrity, and Encryption. Information Society Technologies programme of the European commission (IST-1999-12324). <http://www.cryptonessie.org/>.
- [Pat95] Jacques Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt’88. In *Advances in Cryptology — CRYPTO 1995*, volume 963 of *Lecture Notes in Computer Science*, pages 248–261. Don Coppersmith, editor, Springer, 1995.
- [Pat96] Jacques 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>.
- [Pat97] Jacques Patarin. The oil and vinegar signature scheme. presented at the Dagstuhl Workshop on Cryptography, September 1997. transparencies.
- [PKC05] Serge Vaudenay, editor. *Public Key Cryptography — PKC 2005*, volume 3386 of *Lecture Notes in Computer Science*. Springer, 2005. ISBN 3-540-24454-9.
- [RSA05] David Pointcheval, editor. *The Cryptographer’s Track at RSA Conference 2005*, volume 3860 of *Lecture Notes in Computer Science*. Springer, 2005. ISBN 3-540-31033-9.

- [Sha93] Adi Shamir. Efficient signature schemes based on birational permutations. In *Crypto* [Cry93], pages 1–12.
- [Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.
- [TKI⁺86] S. Tsujii, K. Kurosawa, T. Itoh, A. Fujioka, and T. Matsumoto. A public key cryptosystem based on the difficulty of solving a system of nonlinear equations. *ICICE Transactions (D) J69-D*, 12:1963–1970, 1986.
- [WBP04] Christopher Wolf, An Braeken, and Bart 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, September 8–10 2004. Extended version: <http://eprint.iacr.org/2004/237>.
- [WHL⁺05] Lih-Chung Wang, Yuh-Hua Hu, Feipei Lai, Chun yen Chou, and Bo-Yin Yang. Tractable rational map signature. In *PKC* [PKC05], pages 244–257. ISBN 3-540-24454-9.
- [WP04] Christopher Wolf and Bart Preneel. Asymmetric cryptography: Hidden Field Equations. In *European Congress on Computational Methods in Applied Sciences and Engineering 2004*. P. Neittaanmäki, T. Rossi, S. Korotov, E. Oñate, J. Périaux, and D. Knörzer, editors, Jyväskylä University, 2004. 20 pages, extended version: <http://eprint.iacr.org/2004/072/>.
- [WP05a] Christopher Wolf and Bart Preneel. Equivalent keys in HFE, C^* , and variations. In *Proceedings of Mycrypt 2005*, volume 3715 of *Lecture Notes in Computer Science*, pages 33–49. Serge Vaudenay, editor, Springer, 2005. Extended version <http://eprint.iacr.org/2004/360/>, 15 pages.
- [WP05b] Christopher Wolf and Bart Preneel. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. *Cryptology ePrint Archive*, Report 2005/077, 12th of May 2005. <http://eprint.iacr.org/2005/077/>, 64 pages.
- [WYHL06] Lih-Chung Wang, Bo-Yin Yang, Yuh-Hua Hu, and Feipei Lai. A “medium-field” multivariate public-key encryption scheme. In *RSA* [RSA05], pages 132–149. ISBN 3-540-31033-9.
- [YC04a] Bo-Yin Yang and Jiun-Ming Chen. All in the XL family: Theory and practice. In *ICISC 2004*, volume 3506 of *Lecture Notes in Computer Science*, pages 67–86. Springer, 2004.
- [YC04b] Bo-Yin Yang and Jiun-Ming Chen. Theoretical analysis of XL over small fields. In *ACISP 2004*, volume 3108 of *Lecture Notes in Computer Science*, pages 277–288. Springer, 2004.
- [YC05] Bo-Yin Yang and Jiun-Ming Chen. Building secure tame-like multivariate public-key cryptosystems: The new TTS. In *ACISP 2005*, volume 3574 of *Lecture Notes in Computer Science*, pages 518–531. Springer, July 2005.