ℓ-Invertible Cycles for $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic ($\mathcal{MQ}$) Public Key Cryptography

Jintai Ding[1⋆], Christopher Wolf[2], and Bo-Yin Yang[3⋆⋆]

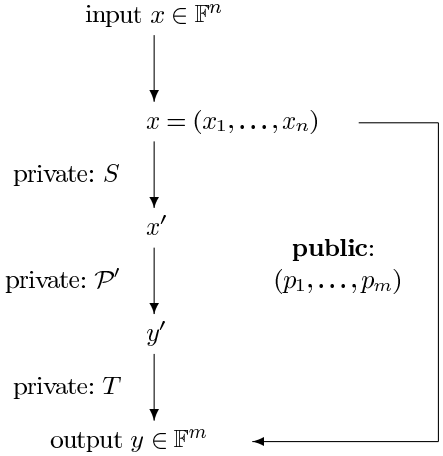
[1] University of Cincinnati and Technische Universität Darmstadt, ding@math.uc.edu
[2] Ecole Normale Superieur, chris@christopher-wolf.de
[3] Institute of Information Science, Academia Sinica and TWISC, by@moscito.org

Abstract. We propose a new basic trapdoor ℓIC (ℓ-Invertible Cycles) of the mixed field type for $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key cryptosystems. This is the first new basic trapdoor since the invention of Unbalanced Oil and Vinegar in 1997. ℓIC 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 ℓIC has very distinctive properties of its own. In practice, ℓIC 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

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



We work over a finite field $\mathbb{F}$ of q elements (the *base field*). $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ is a system of m quadratic polynomials in n variables in $\mathbb{F}$, called the *central map* and its components *central polynomials*. Composition with the affine maps S, T masks the structure of $\mathcal{P}'$ and gives the public map:

$$\mathcal{P} = (p_1, \ldots, p_m) := T \circ \mathcal{P}' \circ S \tag{1}$$

We usually write, for $1 \le i \le m, 1 \le j \le k \le n$,

$p_i(x_1, \ldots, x_n) := \sum_{1 \le j \le k \le n} \gamma_{i,j,k} x_j x_k + \sum_{j=1}^{n} \beta_{i,j} x_j + \alpha_i$

where α_i is usually normalized to zero. The Public key comprise the $mn(n+3)/2$ coefficients $\gamma_{ijk}, \beta_{ij} \in \mathbb{F}$.

$\mathcal{M}$ultivariate $\mathcal{Q}$uadratic ($\mathcal{MQ}$) public-key cryptography first appeared in the English literature in the mid '80s [?,?] as alternatives to traditional PKCs. A

⋆ 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

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 [?]). 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 [?], 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^* ([?], Imai-Matsumoto).
- **HFE:** Hidden Field Equations ([?], Patarin), a generalization of MIA.

Single-Field (or "True"): Works on the individual components of x' and y'.
- **UOV:** Unbalanced Oil and Vinegar ([?,?], Patarin *et al*).
- **STS:** Stepwise Triangular System (lectures in Japanese from '85 – [?], Tsujii; in English, [?]). Generalized later to its present form [?,?].

Some primitives are composite, e.g., Medium Field Encryption (triangular stages [?]) or enTTS/TRMS/Rainbow [?,?,?] (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 (ℓIC)

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" (ℓIC). 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 [?]. A standard example is the map $(A_1, A_2, A_3) \to (A_2A_3, A_3A_1, A_1A_2)$ 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.

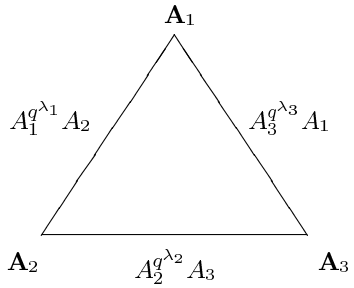


Figure 2. Graphical Representation of 3-Invertible Cycles

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 $\{1, \ldots, \ell\}$ we define

$$\mu : \{1, \ldots, \ell\} \to \{1, \ldots, \ell\} : \mu(i) := \begin{cases} 1 & \text{for } i = \ell \\ i+1 & \textit{otherwise} \end{cases} \tag{2}$$

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 $S, T \in Aff^{-1}(\mathbb{F}^n)$ be two invertible affine mappings and the vector $\Lambda := (\lambda_1, \ldots, \lambda_\ell) \in \{0, \ldots, k-1\}^\ell$. We now have the following mapping:*

$$P : \mathbb{E}^\ell \to \mathbb{E}^\ell : (A_1, \ldots, A_\ell) \to (A_1^{q^{\lambda_1}} A_2, \ldots, A_{\ell-1}^{q^{\lambda_{\ell-1}}} A_\ell, A_\ell^{q^{\lambda_\ell}} A_1) \tag{3}$$

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

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

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

$$\mathcal{P} : \mathbb{F}^n \to \mathbb{F}^m : \mathcal{P} := T \circ \phi^{-1} \circ P \circ \phi \circ S\,. \tag{5}$$

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

The name "invertible cycle" is due to that the variables $A_1, \ldots, A_\ell$ 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 $B_1, \ldots, B_\ell$, where

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

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 ℓIC: 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 $S, T \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$. For $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems, this idea has been introduced under the name *Frobenius sustainers* [?].

2.2 Singularities

To use ℓIC 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 $(A_1, \ldots, A_\ell) \in \mathbb{E}^\ell$ for given input $(B_1, \ldots, B_\ell) \in \mathbb{E}^\ell$. Unfortunately, this is not possible in all cases; due to its form ℓIC has the following singularities:

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

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 [?,?,?]. Our new trapdoor ℓIC 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 ℓIC that cannot be inverted usefully. For practical use, we construct below a sequence of specific ℓIC instances which allows easy inversion.

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

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

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

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

Proof. **Case** $\ell = 3$**:** We have $B_1 := A_1A_2, B_2 := A_2A_3, B_3 := A_3A_1$. Simple computations yield $A_1 := \sqrt{B_1B_3/B_2}, A_3 := B_3/A_1, A_2 := B_2/A_3$.

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 $B_1 := A_1^q A_2, B_2 := A_2A_1$ and its inverse $A_1 := \sqrt[q-1]{B_1/B_2}, A_2 := B_2/A_1$.

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 loose 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 ℓIC

We herein discuss some basic cryptanalytic properties of the new trapdoor. This serves a dual purpose: We find an easy cryptanalysis for ℓIC in its basic form. Simultaneously, we effectively put ℓIC 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 ℓIC-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 [?]. This was used by Fouque, Granboulan, and Stern to cryptanalyse the internally perturbed MIA encryption scheme (PMI/MIAi) [?]. As is more customarily

employed against symmetric cryptosystems, we examine this multivariate differential :

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

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 $\mathbb{F} = \mathrm{GF}(2)$ 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 [?,?].

3.2 Rank Attacks

In a *rank attack*, the quadratic parts central and public polynomials of a given $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic 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 [?]. Goubin and Courtois [?] have the most straightforward exposition of rank attacks. Later extensions and analysis can be seen in [?,?].

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 $q^{R\lfloor m/n \rfloor}$. 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 ℓIC, we want to write matrices in blocks corresponding to pairs of variables in the larger field $\mathbb{E}$. Express central matrices as $H_1,\ldots,H_\ell \in \mathbb{E}^{\ell\times\ell}$ and their $\mathbb{E}$-blocks as $\eta_{i,j,k} \in \mathbb{E}$ for $1 \leq i,j,k \leq \ell$.

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

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

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

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 [?]), 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 ℓIC and modified ℓIC 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 [?]. 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 [?,?,?] 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 ℓIC, we expect a similar behaviour here. This is in line small scale experiments using Magma [?], 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* [?,?,?,?]. E.g., we tested 3IC– systems with MAGMA v2.12-8 on a 2GB machine using $\mathbb{E} = (\mathrm{GF}(256))^4$ or $(\mathrm{GF}(256))^5$. If we removed at least 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 [?] 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 2ICi+ that we will investigate later is not susceptible.

3.5 Further Attacks

There is a special attack from Felke [?] 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 ℓIC.

A different class from XL are algorithms from [?] 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 [?, 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 (ℓIC-)

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 ℓIC, 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 [?] also increases by at least q^r.

Like with MIA, we cannot use ℓIC- 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 (ℓICi+)

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 ℓIC 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 perturbated modification. Here, it also prevents a UOV attack.

Internal perturbation has been introduced for MIA and HFE as PMI ("Perturbated Matsumoto-Imai") and ipHFE respectively [?,?]. We can also call them MIAi and HFEi. As PMI/MIAi has been broken in [?], a new variant PMI+/MIAi+ has been proposed [?]. Due to space limitations we do not go into details, but we believe PMI+ unaffected by the attack from [?]. 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 $S^i \in \mathrm{Aff}^{-1}(\mathbb{F}^n, \mathbb{F}^w)$ the so-called "perturbation space". Note that the perturbation space has the same input variables $x_1, \ldots, x_n$ as the affine transformation $S \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$. However, it has only dimension w. Hence we can write $(z'_1, \ldots, z'_w) := S^i(x_1, \ldots, x_n)$ for the perturbation variables $z'_1, \ldots, z'_w$. As for the plus modification, we denote with $\mathcal{P}^* := \phi^{-1} \circ P \circ \phi$ the ℓIC mapping over the ground field $\mathbb{F}$.

The public key for ℓICi 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 ℓIC-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 $(z'_1, \ldots, z'_w) \in \mathbb{F}^w$ — 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 [?].

4.3 ℓ-Invertible Cycles Embedded (ℓIC↗) without Singularities

Here we introduce the new modifier embedding (↗), motivated by the practical need to avoid singularities in trapdoors of the ℓIC-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 ℓIC 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 [?]. In fact, it is a new generic modifier and can be used in any $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic construction.

For our new embedding modifier we embedding the following translation from $\mathbb{F}^{k-1} \to \mathbb{F}^k$ that takes $(x_1, \ldots, x_{k-1})$ to $(x_1, \ldots, x_{k-1}, 1)$. 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 $(x_1, \ldots, x_{k-1}) \in \mathbb{F}$. 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 $A_1, \ldots, A_\ell \in \mathbb{E}$. Calling the corresponding transformation $\nu : \mathbb{F}^n \to \mathbb{F}^{n-\ell}$ 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 $\nu^{-1} : (y_1, \ldots, y_{k-1}, 1) \to (y_1, \ldots, y_{k-1})$ needs to be inserted between the affine transformation T and the ℓIC 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 $B_1, \ldots, B_\ell \in \mathbb{E}$.

5 Practical Instances

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

5.1 Signature

To obtain a secure signature scheme, we use ℓIC–, 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 ℓIC– 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 ℓIC- is orders of magnitude faster than MIA-; further data will be posted if we can avoid the differential attack on ℓIC-.

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

Claimed Security	Input [bits]	Output [bits]	n	m	Parameters ℓ	k	r	Attack Complexity Gröbner	Rank/UOV	Key Size [kBytes] 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

[?] 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 ℓIC, if SFLASH (MIA-) cannot be patched, ℓIC- will likely suffer the same fate, so now we do not recommend ℓIC- unless this can be circumvented.

5.3 Encryption

We base our proposed encryption scheme on 2ICi+$\nearrow$, *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 [?]. Due to space limitations in this paper we do not repeat their arguments but point to [?]. 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 [?]. 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 [?]. Computing direct division in finite fields is given in [?]. Counting operations for the inversion formula in Lemma 1 over $\mathbb{E} = \mathrm{GF}(q^k)$, 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 $\mathrm{GF}(q^n)$ but in a much smaller extension field $\mathrm{GF}(q^k)$. 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 $\mathbb{E} = \mathrm{GF}(q^a)$ over the ground field $\mathbb{F} = \mathrm{GF}(q)$. 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 [?]. In a nutshell, this translates to n squaring operations and $1/2n$ multiplications in $\mathrm{GF}(q^n)$. Therefore, we obtain an overall workload of $O(n^3)$. Tricks to speed this operation up can be found in [?]. 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 [?]. Its running time is estimated to be in $O(n^3 d^2 + n^2 d^3)$ for d the total degree of the central mapping [?]. In practice, we have $d = 129, \ldots, 257$.

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 $Y \in \mathrm{GF}(q^n)$ 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 $q = 128$, $n = 37$ [?]. For HFE, we have $q = 2$, $n = 103$ in Quartz [?]. 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 [?]. 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 [?] which means it is much faster than SFLASH.

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

ℓIC i+ implementations we compare simple runs of ℓIC 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. ℓIC i+ is clearly quite a bit faster.

6 Conclusions

In this article, we have constructed a new basic $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic trapdoor called ℓ-invertible cycles (ℓIC). 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 $\mathbb{E} = \mathrm{GF}(q^n)$ for $q := |\mathbb{F}|$ and n the number of variables, we compute in the much smaller extension field $\mathbb{E} = \mathrm{GF}(q^k)$ 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 ℓIC-type schemes without decryption failure. Apart from ℓIC, constructions like [?] 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 *ℓIC* 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 ℓIC 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)	$O(n^3d^2 + n^2d^3)$	$q = 2$, $n = 103$, $d = 129$	71	3
MIA (Sflash)	$O(n^3)$	$q = 128$ $n = 37$	15.4	2.45
ℓIC, $\ell = 3$	$O(\ell k^3 + \ell k^2)$	$q = 256$, $k = 10$	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 ℓIC 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