Equivalent Keys in HFE, C*, and Variations

Christopher Wolf and Bart Preneel

K.U.Leuven, ESAT-COSIC,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
{Christopher.Wolf, Bart.Preneel}@esat.kuleuven.ac.be,
chris@Christopher-Wolf.de
http://www.esat.kuleuven.ac.be/cosic/

Abstract. In this article, we investigate the question of equivalent keys for two $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key schemes HFE and C^{*--} and improve over a previously known result, which appeared at PKC 2005. Moreover, we show a new non-trivial extension of these results to the classes HFE-, HFEv, HFEv-, and C^{*--}, which are cryptographically stronger variants of the original HFE and C* schemes. In particular, we are able to reduce the size of the private — and hence the public — key space by at least one order of magnitude and several orders of magnitude on average. While the results are of independent interest themselves as they broaden our understanding of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes, we also see applications both in cryptanalysis and in memory efficient implementations.

Keywords: Multivariate Quadratic Equations, Public Key signature, Hidden Field Equations, HFE, HFE-, HFEv, HFEv-, C*, C^{*--}

1 Introduction

In the last 15 years, several schemes based on the problem of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations have been proposed. The most important ones certainly are C* [9] and Hidden Field Equations (HFE, [13]) plus their variations C^{*--}, HFE-, HFEv, and HFEv- [7,12,13]. Both have been used to construct signature schemes, namely C^{*--} in Sflash [3], and HFEv- in Quartz [2]. As for all systems based on $\mathcal{MQ}$-equations, the public key has the form

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

for $1 \leq i \leq m; 1 \leq j \leq k \leq n$ and $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathbb{F}$ (constant, linear, and quadratic terms). We write the set of all such equations as $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Moreover, the private key consists of the triple $(S, \mathcal{P}', T)$ where $S \in \mathrm{Aff}(\mathbb{F}^n), T \in \mathrm{Aff}(\mathbb{F}^m)$ are affine transformations (cf Sect. 2.2) and $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ is a polynomial-vector $\mathcal{P}' := (p'_1, \ldots, p'_m)$ with m components; each component is a polynomial in n variables $x'_1, \ldots, x'_n$. Throughout this paper, we will denote

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 33–49, 2005.

components of this private vector $\mathcal{P}'$ by a prime $'$. In contrast to the public polynomial vector $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$, the private polynomial vector $\mathcal{P}'$ does allow an efficient computation of $x'_1, \ldots, x'_n$ for given $y'_1, \ldots, y'_m$. Hence, the goal of $\mathcal{MQ}$-schemes is that this inversion should be hard if the public key $\mathcal{P}$ alone is given. The main difference between $\mathcal{MQ}$-schemes lies in their special construction of the central equations $\mathcal{P}'$ and consequently the trapdoor they embed into a specific class of $\mathcal{MQ}$-problems.

In this paper, we investigate the question of equivalent keys for selected $\mathcal{MQ}$-schemes. Due to space limitations, we concentrate on HFE, HFE-, HFEv, HFEv-, C*, and C^{*--}. As outlined above, they are quite important as they have been used in constructions submitted to the NESSIE project [10]. However, we want to point out that the techniques outlined here are quite general and can also be applied to other schemes. The first paper on the topic of equivalent keys is [19]. In this paper, we introduce the Frobenius sustainer and are hence able to improve over the results from [19]. Moreover, this paper is the first to deal with variations of $\mathcal{MQ}$-schemes, cf [20] for the terminology of $\mathcal{MQ}$-trapdoors. To this aim, we needed to develop the reduction sustainer, as we would not have been able to deal with the HFE- and the C^{*--} modification otherwise.

This paper is outlined as follows: after this general introduction, we move on to the necessary mathematical background in Sect. 2. This includes particularly a definition of the term *equivalent keys*. In Sect. 3, we concentrate on a subclass of affine transformations, denoted *sustaining transformations*, which can be used to generate equivalent keys. These transformations are applied to different variations of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations in Sect. 4. This paper concludes with Sect. 5, cf [19] for results on Unbalanced Oil and Vinegar schemes (UOV). A general overview of $\mathcal{MQ}$-schemes can be found in [20].

2 Mathematical Background

In this section, we outline some observations useful in the remainder of this paper.

2.1 Basic Definitions

We start with a formal definition of the term "equivalent private keys":

Definition 1. *We call two private keys*

$$(T, \mathcal{P}', S), (\tilde{T}, \tilde{\mathcal{P}}', \tilde{S}) \in \mathit{Aff}(\mathbb{F}^m) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \mathit{Aff}(\mathbb{F}^n)$$

"equivalent" if they lead to the same public key, i.e., if we have

$$T \circ \mathcal{P}' \circ S = \mathcal{P} = \tilde{T} \circ \tilde{\mathcal{P}}' \circ \tilde{S}\,.$$

In order to find equivalent keys, we consider the following transformations: