**From:** (b) (6)
**To:** Moody, Dustin (Fed)
**Cc:** Perlner, Ray A. (Fed)
**Subject:** Re: revising our PQC paper
**Date:** Monday, April 17, 2017 11:59:53 AM
**Attachments:** IAC2PCABCSMMES5.pdf
IAC2PCABCSMMES5.tex
References.bib

Hi, guys,

Here are my revisions.  Please take a look.

Cheers,
Daniel

On Fri, Apr 14, 2017 at 8:28 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> Daniel,
>
> I've attached the files for you to add to.
>
> I'd be up for exploring the ideas you mentioned about the break even point.  It'd be really good to involve Albrecht as well.  Hope you are feeling better.
>
> Dustin
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Thursday, April 13, 2017 5:27:10 PM
> **To:** Moody, Dustin (Fed)
> **Cc:** Perlner, Ray (Fed)
> **Subject:** Re: revising our PQC paper
>
> Hi, Dustin,
>
> Can you make the changes you mentioned and send me the revised source?  I can address 3 fairly well by simply adding a paragraph on why minors modeling doesn't work.  The reviewer doesn't know what s/he is talking about though, because KS makes no sense here.  I do think, however, that there are many in the intended audience who would be interested in a comparison between the linear algebra technique here and the minors modeling minrank approach.  It is interesting to see why the minors modeling approach is so much worse in this case.
>
> On the other hand, finding the break-even point on linear algebra search versus minors modeling is itself a very interesting question that we should study for another paper

> (independent of any particular scheme). Let's work on this for another submission this year... say SAC again? The idea is this, we take systems of formulae with a low minrank and attack it with linear algebra search and minors modeling and determine the complexity. Then we vary things like number of variables/equations, the minrank, or the field size. (My understanding is that the French team says that minors is always more efficient for these cases.) Then we study the case of differential invariants with interlaced kernels and vary along the same parameters. We already know that the linear algebra search is better for the parameters we attack, but as q increases there will be a breakeven point. As the minrank increases there is likely a breakeven point as well. This could be important work for the establishment of parameters for small field multivariate schemes in the future, so it's definitely worth a try. Let's bring Albrecht on board with this project as well.
>
> Cheers,
> Daniel
>
> On Thu, Apr 13, 2017 at 3:15 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:
>
> > Daniel,
> >
> > The only comments that we possibly need to address came from one reviewer. I talked with Ray about them. He’ll be on annual leave after today, so it’s up to you and me to finish any revisions we decide to to do. Here’s a few thoughts on the comments:
> >
> > 1) “- The authors argue that this approach allows for the same complexity regardless of the characteristic of the field, which notably is the motivation of the paper, and was not the case in [18]. However, very little space is devoted to this important question.
> >
> > In particular, it is not clear why Eq. 1 has always a single solution over all characteristics except 3.
> >
> > Char. 2 is especially important, and the authors should argue more rigorously why there are no linear dependencies (in a form of a proposition or similar).
> >
> > This will emphasize the novelty of the approach. Even more, I suggest to discuss the difference compared to [18] in the introduction. “
> >
> > We don’t think we really need to do anything in regard to comment 1, because we think the paper already does a good job at explaining everything. Perhaps this comment was caused by not being able to read [18]. We could do some revision, but we didn’t think we really had to.
> >
> > 2) “- The description of the MinRank attack (Sec. 4) is somehow in the wrong order or perhaps a part is missing.

First it should be shown that a tensor H(E)(w) will have a rank 2s provided E is in the band and w is in the band kernel."

We'll add "(see Figure 2)" after "at rank at most 2s" at the top of p7. I think Figure 2 shows pretty simply that the rank of H(E)(w) will be 2s.

3)"- It should be commented briefly on the difference of using the Kipnis-Shamir or minors modeling, and why it was chosen not to."

We defer to you on what (if anything) should be mentioned regarding Kipnis-Shamir or minors modeling.

- The paper should be checked for typos and the use of vector notation.

I'll run a spell checker on it. Not sure of any vector notation problems.

Thanks,

Dustin

```
\documentclass[runningheads]{llncs}
\usepackage[margin=1.35in]{geometry}
\usepackage{amssymb,amsmath,authblk}
\setcounter{tocdepth}{3}
\usepackage{graphicx}
\usepackage{tikz}
\usepackage{mathtools}
\usepackage{color}

\usepackage{url}
\urldef{\mailsa}\path|daniel.smith@nist.gov|
\urldef{\mailsb}\path|ray.perlner@nist.gov|
\urldef{\mailsc}\path|dustin.moody@nist.gov|
\newcommand{\keywords}[1]{\par\addvspace\baselineskip
\noindent\keywordname\enspace\ignorespaces#1}


%===============Definitions===========================


\newcommand{\bdf}{\begin{definition}}
\newcommand{\edf}{\end{definition}}
\newcommand{\beq}{\begin{equation}}
\newcommand{\eeq}{\end{equation}}
\newcommand{\bsp}{\begin{split}}
\newcommand{\esp}{\end{split}}
\newtheorem{Thm}{Theorem}
\newtheorem{Lem}{Lemma}
\newtheorem{Cor}{Corollary}
\newtheorem{Prop}{Proposition}[chapter]
\newtheorem{Def}{Definition}
\newtheorem{Rem}{Remark}
\newcommand{\Z}{\mathbb{Z}}
\newcommand{\dc}{\textcolor{red}}
\def\mathbi#1{\textbf{\em #1}}


%===================End Definitions=======================

%===============Perspective Definitions======================

%\def\xa{108}
%\def\ya{-106}
%\def\za{80}

\def\xdirx{-0.996}
\def\xdiry{0.087}
\def\ydirx{0.614}
\def\ydiry{0.43}
\def\zdirx{0.0}
\def\zdiry{1}
```

```latex
%=============End Perspective Definitions====================

%==============Color Definitions=======================

\definecolor{lightgray}{rgb}{0.85,0.85,0.85}
\definecolor{mediumgray}{rgb}{0.75,0.75,0.75}
\definecolor{darkgray}{rgb}{0.45,0.45,0.45}

%============End Color Definitions======================

%===============Notation Macros=====================

\newcommand\restr[2]{{% we make the whole thing an ordinary symbol
  \left.\kern-\nulldelimiterspace % automatically resize the bar with \right
  #1 % the function
  \vphantom{\big|} % pretend it's a little taller at normal size
  \right|_{#2} % this is the delimiter
  }}

%=============End Notation Macros====================


\begin{document}

\mainmatter

\title{Improved Attacks for Characteristic-2 Parameters of the Cubic ABC Simple Matrix Encryption Scheme}

\titlerunning{Improved Attacks on Cubic Simple Matrix Encryption}

\author[1]{Dustin Moody}
\author[1]{Ray Perlner}
\author[1,2]{Daniel Smith-Tone}
\affil[1]{National Institute of Standards and Technology,

Gaithersburg, Maryland, USA}
\affil[2]{Department of Mathematics, University of Louisville,

Louisville, Kentucky, USA}
\authorrunning{D Moody, R Perlner, \& D Smith-Tone}

\institute{\mailsc, \mailsb, \mailsa}


\toctitle{Lecture Notes in Computer Science}
\tocauthor{Authors' Instructions}
\maketitle

\begin{abstract}
In the last few years multivariate public key cryptography has experienced an infusion of new ideas for encryption.
Among these new strategies is the ABC Simple Matrix family of encryption schemes which utilize the structure of a
large matrix algebra to construct effectively invertible systems of nonlinear equations hidden by an isomorphism of
polynomials. One promising approach to cryptanalyzing these schemes has been structural cryptanalysis, based on
applying a strategy similar to MinRank attacks to the discrete differential. These attacks however have been
```

significantly more expensive when applied to parameters using fields of characteristic 2, which have been the most common choice for published parameters. This disparity is especially great for the cubic version of the Simple Matrix Encryption Scheme.

In this work, we demonstrate a technique that can be used to implement a structural attack which is as efficient against parameters of characteristic 2 as are attacks against analogous parameters over higher characteristic fields. This attack demonstrates that, not only is the cubic simple matrix scheme susceptible to structural attacks, but that the published parameters claiming 80 bits of security are less secure than claimed (albeit only slightly.) Similar techniques can also be applied to improve structural attacks against the original Simple Matrix Encryption scheme, but they represent only a modest improvement over previous structural attacks. This work therefore demonstrates that choosing a field of characteristic 2 for the Simple Matrix Encryption Scheme or its cubic variant will not provide any additional security value.
\keywords{multivariate public key cryptography, differential invariant, MinRank, encryption}
\end{abstract}

\section{Introduction}

The National Institute of Standards and Technology (NIST) is currently engaged in an effort to update the public key infrastructure, providing alternatives to the classical public key schemes based on arithmetic constructions. The discovery by Peter Shor in the 1990s of efficient algorithms for factoring and computing discrete logarithms, see \cite{Shor}, accelerated research towards building the necessary class of computers, those that Feynman famously suggested in \cite{Feynman:1981tf}: quantum computers. There has been growing interest among scientists in our discipline in the years since, to provide protocols and algorithms that are post-quantum, that is, secure in the quantum model of computing. The recent publication by (NIST), see \cite{CFP}, of a call for proposals for post-quantum standards directly addresses the challenge of migration towards a more diverse collection of tools for our public key infrastructure.

Public key schemes based on the difficulty of inverting nonlinear systems of equations provide one possibility for post-quantum security. Multivariate Public Key Cryptography (MPKC) is a reasonable option because the problem of solving systems of nonlinear equations, even if only quadratic, is known to be NP-complete; thus, the generic problem is likely beyond the reach of quantum adversaries. Furthermore, there are a variety of standard techniques to metamorphosize multivariate schemes, to introduce new properties, to enhance security, to reduce power consumption, to resist side-channel analysis, etc. %One possible candidate for practical, efficient, and nonconforming solutions to some of the most consequential public key applications is Multivariate Public Key Cryptography(MPKC). Multivariate schemes are attractive in certain applications because of the maleability of the schemes. Different modifications of similar ideas can make a scheme more suited to lightweight architectures, enhance security, or parametrize various aspects of performance.

%In addition, MPKC is one among a few serious candidates to have risen to prominence as post-quantum options. The fundamental problem of solving a system of quadratic equations is known to be NP-hard, and so in the worst case, solving a system of generic quadratic equations is unfeasible for a classical computer; neither is there any indication that the task is easier in the quantum computing paradigm. % Furthermore, experience indicates that this problem is hard even in the average case; thus multivariate cryptosystems at least have a chance of being difficult to break. Secondly, multivariate cryptosystems are often very efficient, see \cite{boyin,boyin2,boyin3}. Finally, such cryptosystems can be very amenable to the user demands, with multiple parameters hidden within the system which can be altered by the user to achieve different performance goals.

There are numerous long-lived multivariate digital signature schemes. All of UOV \cite{uov}, HFE- \cite{Patarin2}, and HFEv- \cite{DBLP:conf/ctrsa/PatarinCG01} have been studied for around two decades. Moreover, some of the above schemes have optimizations which have strong theoretical support or have stood unbroken in the literature for some time. Notable among these are UOV, which has a cyclic variant \cite{DBLP:conf/indocrypt/PetzoldtBB10} that dramatically reduces the key size, and Gui \cite{DBLP:conf/asiacrypt/PetzoldtCYTD15}, an HFEv- scheme, that, due to tighter bounds on the complexity of algebraically solving the underlying system of equations, see \cite{DBLP:conf/pqcrypto/DingY13}, has much more aggressive parameters than QUARTZ, see

\cite{DBLP:conf/ctrsa/PatarinCG01}.

Multivariate public key encryption, however, has a much rockier history. Several attempts at multivariate encryption, see \cite{DBLP:conf/asiacrypt/GoubinC00,DBLP:conf/pqcrypto/TsujiiGTF10} for example, have been shown to be weak based on rank or differential weaknesses. Recently, a new framework for developing secure multivariate encryption schemes has surfaces, drawing on the idea that it may impose sufficiently few restrictions on a multivariate map to be merely an injective map into a much larger codomain instead of being essentially a permutation. A few interesting attempts to achieve multivariate encryption have originated from this thought. ZHFE, see \cite{DBLP:conf/pqcrypto/PorrasBD14}, the quadratic and cubic variants of the ABC Simple Matrix Scheme, see \cite{DBLP:conf/pqcrypto/TaoDTD13} and \cite{DBLP:conf/pqcrypto/DingPW14}, and Extension Field Cancellation, see \cite{DBLP:conf/pqcrypto/SzepieniecDP16}, all use fundamentally new structures for the derivation of an encryption system.

A few of the above schemes have already suffered some setbacks. A questionable rank property in the public key of ZHFE presented in \cite{DBLP:conf/pqcrypto/PerlnerS16} makes this scheme appear dubious, while it was shown that the quadratic Simple Matrix structure leaves the signature of a differential invariant in the public key which is exploited in \cite{DBLP:conf/pqcrypto/MoodyPS14} to effect an attack.

The case of the Cubic Simple Matrix encryption scheme is more interesting; the authors in \cite{DBLP:conf/pqcrypto/DingPW14} present a heuristic argument for security and suggest the possibility of provable security for the scheme. These provable security claims were undermined in \cite{conf/sac/MoodyPS16}, however, with the presentation of a key recovery attack on a full scale version of the Cubic Simple Matrix encryption scheme. The complexity of the attack was on the order of $q^{s+2}$ for characteristic $p>3$, $q^{s+3}$ for characteristic $3$, and $q^{2s+6}$ for characteristic $2$. Here $s$ is the dimension of the matrices in the scheme, and $q$ is the cardinality of the finite field used. This technique was an extension and augmentation of the technique of \cite{DBLP:conf/pqcrypto/MoodyPS14}, and similarly exploited a differential invariant property of the core map to perform a key recovery attack. Nonetheless, the much higher complexity of this attack for characteristic $2$ left open the possibility that there may be some security advantage to using a cubic ABC map over a field with characteristic 2.

In this paper, we present an attack whose complexity is on the order of $q^{s+2}$ for all characteristics. Similar techniques can also improve the complexity of attacks against characteristic $2$ parameters for the original quadratic version of the ABC cryptosystem, from $q^{s+4}$ (reported in \cite{DBLP:conf/pqcrypto/MoodyPS14}) to $q^{s+2}$. %\dc{Ray has commented out how the attack works on the 80-bit and 100-bit parameters. We may wish to include this as many people will only read the intro, and not the whole paper.}

Specifically, our technique improves the complexity of attacking CubicABC($q=2^8$,$s=7$), designed for $80$-bit security, from the horrendous value of $2^{177}$ in \cite{conf/sac/MoodyPS16} to approximately $2^{88}$ operations, the same as the direct algebraic attack complexity reported in \cite{DBLP:conf/pqcrypto/DingPW14}. More convincing is our attack on CubicABC($q=2^8$,$s=8$), designed for $100$-bit security. We break the scheme in approximately $2^{98}$ operations. Furthermore, the attack is fully parallelizable and requires very little memory; hence, our technique is asymptotically far more efficient than algebraic attacks, the basis for the original security estimation. Thus, the security claims in \cite{DBLP:conf/pqcrypto/DingPW14} not only fail to hold in the odd characteristic case, they fail to hold in characteristic two as well.

%In light of NIST's recommendation to migrate to 112 bit security, see \cite{SP800-131A}, and the fact that the attack is more effective with larger values of $s$, we are forced to conclude that the CubicABC is broken.

The paper is organized as follows. In the next section, we present the structure of the Cubic ABC Simple Matrix encryption scheme. In the following section, the fingerprint of the matrix algebra used in the construction of the ABC scheme is exposed. In the subsequent section, the effect of this structure on minrank calculations is determined. We then calculate the complexity of the full attack including the linear algebra steps required for full key recovery. Finally, we review these results and discuss the security of the Cubic ABC scheme and its quadratic counterpart moving forward.

\section{The Cubic ABC Matrix Encryption Scheme}

In \cite{DBLP:conf/pqcrypto/DingPW14}, the Cubic ABC Matrix encryption scheme is proposed. The motivation behind the scheme is to use a large matrix algebra over a finite field to construct an easily invertible cubic map. The construction uses matrix multiplication to combine random linear and quadratic formulae into cubic formulae in a way that allows a user with knowledge of the structure of the matrix algebra and the polynomial isomorphism used to compose the scheme to invert the map.

Let $k=\mathbb{F}_q$ be a finite field. Linear forms and variables over $k$ will be denoted with lower case letters. Vectors of any dimension over $k$ will be denoted with bold font, $\mathbf{v}$. Fix $s\in\mathbb{N}$ and set $n=s^2$ and $m=2s^2$. An element of a matrix ring $M_d(k)$ or the linear transformations they represent, will be denoted by upper case letters, such as $M$. When the entries of the matrix are being considered functions of a variable, the matrix will be denoted $M(\mathbf{x})$. Let $\phi:M_{s\times 2s}(k)\rightarrow k^{2s^2}$ represent the vector space isomorphism sending a matrix to the column vector consisting of the concatenation of its rows. The output of this map, being a vector, will be written with bold font; however, to indicate the relationship to its matrix preimage, it will be denoted with an upper case letter, such as $\mathbf{M}$.

The scheme utilizes an isomorphism of polynomials to hide the internal structure. Let $\mathbf{x}=\left[\begin{matrix}x_1,x_2,\ldots,x_n\end{matrix}\right]^{\top}\in k^n$ denote plaintext while $\mathbf{y}=\left[\begin{matrix}y_1,\ldots,y_m\end{matrix}\right]\in k^m$ denotes ciphertext. Fix two invertible linear transformations $T\in M_m(k)$ and $U\in M_n(k)$. (One may use affine transformations, but there is no security or performance benefit in doing so.) Denote the input and output of the central map by $\mathbf{u}=U\mathbf{x}$ and $\mathbf{v}=T^{-1}(\mathbf{y})$.

The construction of the central map is as follows. Define three $s\times s$ matrices $A$, $B$, and $C$ in the following way:
\[
A=\left[\begin{matrix}
p_1 & p_2 & \cdots & p_s\\
p_{s+1}& p_{s+2} & \cdots & p_{2s}\\
\vdots & \vdots & \ddots & \vdots\\
p_{s^2-s+1} & p_{s^2-s+2} & \cdots & p_{s^2}\\\end{matrix}\right], B=\left[\begin{matrix}b_1 & b_2 & \cdots & b_s\\
b_{s+1}& b_{s+2} & \cdots & b_{2s}\\
\vdots & \vdots & \ddots & \vdots\\
b_{s^2-s+1} & b_{s^2-s+2} & \cdots & b_{s^2}\\\end{matrix}\right],
\]
and
\[
C=\left[\begin{matrix}
c_1 & c_2 & \cdots & c_s\\
c_{s+1}& c_{s+2} & \cdots & c_{2s}\\
\vdots & \vdots & \ddots & \vdots\\
c_{s^2-s+1} & c_{s^2-s+2} & \cdots & c_{s^2}\\\end{matrix}\right].
\]
Here the $p_i$ are quadratic forms on $\mathbf{u}$ chosen independently and uniformly at random from among all quadratic forms and the $b_i$ and $c_i$ are linear forms on $\mathbf{u}$ chosen independently and uniformly at random from among all linear forms.

We define two $s\times s$ matrices $E_1=AB$ and $E_2=AC$. Since $A$ is quadratic and $B$ and $C$ are linear in $u_i$, $E_1$ and $E_2$ are cubic in the $u_i$. The central map $\mathcal{E}$ is defined by
\[
\mathcal{E}=\phi\circ(E_1||E_2).
\]

Thus $\mathcal{E}$ is an $m$ dimensional vector of cubic forms in $\mathbf{u}$. Finally, the public key is given by $\mathcal{F}=T\circ\mathcal{E}\circ U$.

Encryption with this system is standard: given a plaintext $(x_1,\ldots,x_n)$, compute $(y_1,\ldots,y_m)=\mathcal{F}(x_1,\ldots,x_n)$. Decryption is somewhat more complicated.

To decrypt, one inverts each of the private maps in turn: apply $T^{-1}$, invert $\mathcal{E}$, and apply $U^{-1}$.
To ``invert'' $\mathcal{E}$, one assumes that $A(\mathbf{u})$ is invertible, and forms a matrix
\[
A^{-1}(\mathbf{u})=\left[\begin{matrix}
w_1 & w_2 & \cdots & w_s\\
w_{s+1}& w_{s+2} & \cdots & w_{2s}\\
\vdots & \vdots & \ddots & \vdots\\
w_{s^2-s+1} & w_{s^2-s+2} & \cdots & w_{s^2}\\\end{matrix}\right],
\]
where the $w_i$ are indeterminants. Then collectinging the relations $A^{-1}(\mathbf{u})E_1(\mathbf{u})=B(\mathbf{u})$ and $A^{-1}(\mathbf{u})E_2(\mathbf{u})=C(\mathbf{u})$, we have $m=2s^2$ linear equations in $2n=2s^2$ unknowns $w_i$ and $u_i$. %(We note here that it would be more correct to say $A^{-1}(\bar{u})E_1(\bar{u})=B(\bar{u})$ and $A^{-1}(\bar{u})E_2(\bar{u})=C(\bar{u})$, since the values of these matrices depend on $\bar{u}$.)
Using, for example, Gaussian elimination one can eliminate all of the variables $w_i$ and most of the $u_i$. The resulting relations can be substituted back into $E_1(\mathbf{u})$ and $E_2(\mathbf{u})$ to obtain a large system of equations in very few variables which can be solved efficiently in a variety of ways.

\section{The Structure of the Cubic ABC scheme} \label{sec:diffstructcubic}

\subsection{Column Band Spaces}\label{sec:bandspace}

Each component of the central $\mathcal{E}(\mathbf{u})=E_1(\mathbf{u})||E_2(\mathbf{u})$ map may be written as:
$$
%\label{E1comp}
\mathcal{E}_{(i-1)s+j}=\sum_{l=1}^{s}p_{(i-1)s+l}b_{(l-1)s+j},
$$
for the $E_1$ equations, and likewise, for the $E_2$ equations:
$$
%\beq\label{E2comp}
\mathcal{E}_{s^2+(i-1)s+j}=\sum_{l=1}^{s}p_{(i-1)s+l}c_{(l-1)s+j}
$$
where $i$ and $j$ run from 1 to $s$.

Consider the $s$ sets of $s$ polynomials that form the columns of $E_1$, i.e. for each $j\in\{1,\ldots,s\}$ consider $(\mathcal{E}_{ j}, \mathcal{E}_{s+j}, \ldots , \mathcal{E}_{s^2-s+ j})$. With high probability, the linear forms $b_{ j}, b_{s+j}, \ldots , b_{s^2-s+ j}$ are linearly independent, and if so the polynomials may be re-expressed, using a linear change of variables to $(u'_1, \ldots u'_{s^2})$ where
$u'_i = b_{(i-1)s+j}$ for $i = 1, \ldots, s$. After the change of variables, the only cubic monomials contained in $(\mathcal{E}_{ j}, \mathcal{E}_{s+j}, \ldots , \mathcal{E}_{s^2-s+ j})$ will be those containing at least one factor of $u'_1, \ldots, u'_s$. We can make a similar change of variables to reveal structure in the $s$ sets of $s$ polynomials that form the columns of $E_2$: Setting $u'_i = c_{(i-1)s+j}$ for $i = 1, \ldots, s$ and a fixed $j$, the only cubic monomials contained in $(\mathcal{E}_{s^2+ j}, \mathcal{E}_{s^2+s+j}, \ldots , \mathcal{E}_{2s^2-s+ j})$ will be those containing at least one factor of $u'_1, \ldots, u'_s$.

More generally, we can make a similar change of variables to reveal structure in any of a large family of $s$ dimensional subspaces of the span of the component polynomials of $E_1$ and $E_2$, which we will call column band spaces in analogy to the band spaces used to analyze the quadratic ABC cryptosystem in

\cite{DBLP:conf/pqcrypto/MoodyPS14}. Each family is defined by a fixed linear combination, $(\beta, \gamma)$, of the columns of $E_1$ and $E_2$:

\begin{Def}\label{bandspacedef}
The column band space defined by the $2s$-dimensional linear form $(\beta, \gamma)$ is the space of cubic maps, $\mathcal{B}_{\beta, \gamma}$ , given by:
\[
\mathcal{B}_{\beta, \gamma}=\mbox{Span} (\mathcal{E}_{\beta, \gamma,1}, \ldots, \mathcal{E}_{\beta, \gamma,s}),
\]
where
\[
\mathcal{E}_{\beta, \gamma, i} = \sum_{j=1}^s (\beta_j \mathcal{E}_{(i-1)s+j}+ \gamma_j \mathcal{E}_{s^2+(i-1)s+j})\]
\[
=\sum_{l=1}^s\left(p_{(i-1)s+ l}\sum_{j=1}^s \left(\beta_j b_{(l-1)s+j}+ \gamma_j c_{(l-1)s+j}\right)\right).
\]
\end{Def}

Note that under a change of variables
\[
(x_1,\ldots,x_{s^2})\xmapsto{M}(u'_1, \ldots u'_{s^2})\mbox{, where }u'_i = \sum_{j=1}^s\left(\beta_j b_{(i-1)s+j}+ \gamma_j c_{(i-1)s+j}\right)\mbox{ for }i = 1, \ldots, s,
\]
the only cubic monomials contained in the elements of $\mathcal{B}_{\beta, \gamma}$ will be those containing at least one factor of  $u'_1, \ldots, u'_s$.

In such a basis, the third formal derivative, or the $3$-tensor of third partial derivatives
\[
D^3\mathcal{E}=\sum_{i,j,k}\frac{\partial^3\mathcal{E}}{\partial u'_i\partial u'_j\partial u'_k}du'_i\otimes du'_j\otimes du'_k,
\]
of any map $\mathcal{E}\in\mathcal{B}_{\beta,\gamma}$ has a special block form, see Figure \ref{fig:bsd}. This tensor is the same as the one used for the attack in \cite{conf/sac/MoodyPS16}, although in that case it was computed using the discrete differential. There are, however, a number of disadvantages to using this 3-tensor to represent the structural features of cubic ABC. In particular, when defined over a field of characteristic 2, the symmetry of the 3-tensor results in the loss of any information about coefficients for monomials of the form $x_i^2x_j$, since the 3rd derivatave of such a monomial is always 0. We will therefore use a different tool to express the structure of cubic ABC.

Using the same $u'$ basis as above, we see that the gradient $\nabla_{u'}\mathcal{E}$ produces a covector of quadratic forms, which can be though of as a quadratic map that takes any vector $w$ of the form
\[
(0, \ldots, 0, u'_{s+1}(\mathbf{w}), \ldots, u'_{s^2}(\mathbf{w}))^{\top},
\]
to a covector of the form
\[
(y(u'_1), \ldots, y(u'_s), 0, \ldots, 0).
\]
Note that, by the chain rule, we can relate $\nabla_{u'}\mathcal{E}=\left[\frac{\partial\mathcal{E}}{\partial u'_1},\ldots,\frac{\partial\mathcal{E}}{\partial u'_{s^2}}\right]$ to the formal derivative defined over the public basis:
\[
\nabla\mathcal{E} = \left[\frac{\partial\mathcal{E}}{\partial x_1},\ldots,\frac{\partial\mathcal{E}}{\partial x_{s^2}}\right] = \nabla_{u'}\mathcal{E}\left[\frac{du'_j}{dx_i}\right]_{i,j}
\]

using the nonsingular change of basis matrix whose entries are $\frac{du'_j}{dx_i}.$ We can therefore conclude that even defined over the public basis, the first formal derivative of any map $\mathcal{E}\in\mathcal{B}_{\beta,\gamma}$ is a quadratic map that takes an $s^2-s$ dimensional space of vectors to an $s$ dimensional space of covectors.

We will define the term ``band kernel" to describe this $s^2-s$ dimensional space of vectors (including $\mathbf{w}$) which are mapped to an $s$ dimensonal image space by the first formal derivative of $\mathcal{E}$.

\begin{Def}\label{bandkerneldef}
The band kernel of $\mathcal{B}_{\beta, \gamma}$, denoted $\mathcal{BK}_{\beta, \gamma}$, is the space of vectors $x$, such that
\[u'_i = \sum_{j=1}^s\left(\beta_j b_{(i-1)s+j}(x)+ \gamma_j c_{(i-1)s+j}(x)\right) =0,\]
for $i=1, \ldots, s$.
\end{Def}

```
\begin{figure}[!ht]
	\centering
	\begin{tikzpicture}
		\foreach \d in {4}{%
				\pgfmathsetmacro\xxa{0}
				\pgfmathsetmacro\yya{0}
				\pgfmathsetmacro\zza{0}
				\pgfmathsetmacro\xxb{\d}
				\pgfmathsetmacro\yyb{0}
				\pgfmathsetmacro\zzb{0}
				\pgfmathsetmacro\xxc{\d}
				\pgfmathsetmacro\yyc{0}
				\pgfmathsetmacro\zzc{\d}
				\pgfmathsetmacro\xxd{\d-1}
				\pgfmathsetmacro\yyd{0}
				\pgfmathsetmacro\zzd{\d}
				\pgfmathsetmacro\xxe{\d-1}
				\pgfmathsetmacro\yye{0}
				\pgfmathsetmacro\zze{1}
				\pgfmathsetmacro\xxf{0}
				\pgfmathsetmacro\yyf{0}
				\pgfmathsetmacro\zzf{1}
				\pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
				\pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
				\pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
				\pgfmathsetmacro\fourthx{\xxd*\xdirx+\yyd*\ydirx+\zzd*\zdirx}
				\pgfmathsetmacro\fifthx{\xxe*\xdirx+\yye*\ydirx+\zze*\zdirx}
				\pgfmathsetmacro\sixthx{\xxf*\xdirx+\yyf*\ydirx+\zzf*\zdirx}
				\pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
				\pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
				\pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
				\pgfmathsetmacro\fourthy{\xxd*\xdiry+\yyd*\ydiry+\zzd*\zdiry}
				\pgfmathsetmacro\fifthy{\xxe*\xdiry+\yye*\ydiry+\zze*\zdiry}
				\pgfmathsetmacro\sixthy{\xxf*\xdiry+\yyf*\ydiry+\zzf*\zdiry}
				\fill [fill=mediumgray] (\firstx,\firsty) -- (\secondx,\secondy) -- (\thirdx,\thirdy) -- (\fourthx,\fourthy)
-- (\fifthx,\fifthy) -- (\sixthx,\sixthy) -- (\firstx,\firsty);
		}
		\foreach \d in {4}{%
				\pgfmathsetmacro\xxa{\d-1}
```

```
        \pgfmathsetmacro\yya{0}
        \pgfmathsetmacro\zza{\d}
        \pgfmathsetmacro\xxb{\d}
        \pgfmathsetmacro\yyb{0}
        \pgfmathsetmacro\zzb{\d}
        \pgfmathsetmacro\xxc{\d}
        \pgfmathsetmacro\yyc{\d}
        \pgfmathsetmacro\zzc{\d}
        \pgfmathsetmacro\xxd{0}
        \pgfmathsetmacro\yyd{\d}
        \pgfmathsetmacro\zzd{\d}
        \pgfmathsetmacro\xxe{0}
        \pgfmathsetmacro\yye{\d-1}
        \pgfmathsetmacro\zze{\d}
        \pgfmathsetmacro\xxf{\d-1}
        \pgfmathsetmacro\yyf{\d-1}
        \pgfmathsetmacro\zzf{\d}
        \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
        \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
        \pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
        \pgfmathsetmacro\fourthx{\xxd*\xdirx+\yyd*\ydirx+\zzd*\zdirx}
        \pgfmathsetmacro\fifthx{\xxe*\xdirx+\yye*\ydirx+\zze*\zdirx}
        \pgfmathsetmacro\sixthx{\xxf*\xdirx+\yyf*\ydirx+\zzf*\zdirx}
        \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
        \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
        \pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
        \pgfmathsetmacro\fourthy{\xxd*\xdiry+\yyd*\ydiry+\zzd*\zdiry}
        \pgfmathsetmacro\fifthy{\xxe*\xdiry+\yye*\ydiry+\zze*\zdiry}
        \pgfmathsetmacro\sixthy{\xxf*\xdiry+\yyf*\ydiry+\zzf*\zdiry}
        \fill [fill=lightgray] (\firstx,\firsty) -- (\secondx,\secondy) -- (\thirdx,\thirdy) -- (\fourthx,\fourthy) -- (\fifthx,\fifthy) -- (\sixthx,\sixthy) -- (\firstx,\firsty);
    }
    \foreach \d in {4}{%
        \pgfmathsetmacro\xxa{0}
        \pgfmathsetmacro\yya{0}
        \pgfmathsetmacro\zza{0}
        \pgfmathsetmacro\xxb{0}
        \pgfmathsetmacro\yyb{0}
        \pgfmathsetmacro\zzb{1}
        \pgfmathsetmacro\xxc{0}
        \pgfmathsetmacro\yyc{\d-1}
        \pgfmathsetmacro\zzc{1}
        \pgfmathsetmacro\xxd{0}
        \pgfmathsetmacro\yyd{\d-1}
        \pgfmathsetmacro\zzd{\d}
        \pgfmathsetmacro\xxe{0}
        \pgfmathsetmacro\yye{\d}
        \pgfmathsetmacro\zze{\d}
        \pgfmathsetmacro\xxf{0}
        \pgfmathsetmacro\yyf{\d}
        \pgfmathsetmacro\zzf{0}
        \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
        \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
        \pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
```

```
		\pgfmathsetmacro\fourthx{\xxd*\xdirx+\yyd*\ydirx+\zzd*\zdirx}
		\pgfmathsetmacro\fifthx{\xxe*\xdirx+\yye*\ydirx+\zze*\zdirx}
		\pgfmathsetmacro\sixthx{\xxf*\xdirx+\yyf*\ydirx+\zzf*\zdirx}
		\pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
		\pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
		\pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
		\pgfmathsetmacro\fourthy{\xxd*\xdiry+\yyd*\ydiry+\zzd*\zdiry}
		\pgfmathsetmacro\fifthy{\xxe*\xdiry+\yye*\ydiry+\zze*\zdiry}
		\pgfmathsetmacro\sixthy{\xxf*\xdiry+\yyf*\ydiry+\zzf*\zdiry}
		\fill [fill=darkgray] (\firstx,\firsty) -- (\secondx,\secondy) -- (\thirdx,\thirdy) -- (\fourthx,\fourthy) --
(\fifthx,\fifthy) -- (\sixthx,\sixthy) -- (\firstx,\firsty);
	}
	\foreach \d in {3}{%
		\pgfmathsetmacro\xxa{0}
		\pgfmathsetmacro\yya{0}
		\pgfmathsetmacro\zza{1}
		\pgfmathsetmacro\xxb{\d}
		\pgfmathsetmacro\yyb{0}
		\pgfmathsetmacro\zzb{1}
		\pgfmathsetmacro\xxc{\d}
		\pgfmathsetmacro\yyc{\d}
		\pgfmathsetmacro\zzc{1}
		\pgfmathsetmacro\xxd{0}
		\pgfmathsetmacro\yyd{\d}
		\pgfmathsetmacro\zzd{1}
		\pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
		\pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
		\pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
		\pgfmathsetmacro\fourthx{\xxd*\xdirx+\yyd*\ydirx+\zzd*\zdirx}
		\pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
		\pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
		\pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
		\pgfmathsetmacro\fourthy{\xxd*\xdiry+\yyd*\ydiry+\zzd*\zdiry}
		\fill [fill=lightgray] (\firstx,\firsty) -- (\secondx,\secondy) -- (\thirdx,\thirdy) -- (\fourthx,\fourthy) --
(\firstx,\firsty);
	}
	\foreach \d in {3}{%
		\pgfmathsetmacro\xxa{0}
		\pgfmathsetmacro\yya{\d}
		\pgfmathsetmacro\zza{1}
		\pgfmathsetmacro\xxb{\d}
		\pgfmathsetmacro\yyb{\d}
		\pgfmathsetmacro\zzb{1}
		\pgfmathsetmacro\xxc{\d}
		\pgfmathsetmacro\yyc{\d}
		\pgfmathsetmacro\zzc{\d+1}
		\pgfmathsetmacro\xxd{0}
		\pgfmathsetmacro\yyd{\d}
		\pgfmathsetmacro\zzd{\d+1}
		\pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
		\pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
		\pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
		\pgfmathsetmacro\fourthx{\xxd*\xdirx+\yyd*\ydirx+\zzd*\zdirx}
		\pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
```

```
        \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
        \pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
        \pgfmathsetmacro\fourthy{\xxd*\xdiry+\yyd*\ydiry+\zzd*\zdiry}
        \fill [fill=mediumgray] (\firstx,\firsty) -- (\secondx,\secondy) -- (\thirdx,\thirdy) -- (\fourthx,\fourthy) -- (\firstx,\firsty);
    }
    \foreach \d in {3}{%
        \pgfmathsetmacro\xxa{\d}
        \pgfmathsetmacro\yya{0}
        \pgfmathsetmacro\zza{1}
        \pgfmathsetmacro\xxb{\d}
        \pgfmathsetmacro\yyb{0}
        \pgfmathsetmacro\zzb{\d+1}
        \pgfmathsetmacro\xxc{\d}
        \pgfmathsetmacro\yyc{\d}
        \pgfmathsetmacro\zzc{\d+1}
        \pgfmathsetmacro\xxd{\d}
        \pgfmathsetmacro\yyd{\d}
        \pgfmathsetmacro\zzd{1}
        \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
        \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
        \pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
        \pgfmathsetmacro\fourthx{\xxd*\xdirx+\yyd*\ydirx+\zzd*\zdirx}
        \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
        \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
        \pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
        \pgfmathsetmacro\fourthy{\xxd*\xdiry+\yyd*\ydiry+\zzd*\zdiry}
        \fill [fill=darkgray] (\firstx,\firsty) -- (\secondx,\secondy) -- (\thirdx,\thirdy) -- (\fourthx,\fourthy) -- (\firstx,\firsty);
    }
    \foreach \e in {0,1}{%
        \foreach \d in {4}{%
        \pgfmathsetmacro\xxa{0}
        \pgfmathsetmacro\yya{0}
        \pgfmathsetmacro\zza{\e}
        \pgfmathsetmacro\xxb{\d}
        \pgfmathsetmacro\yyb{0}
        \pgfmathsetmacro\zzb{\e}
        \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
        \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
        \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
        \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
        \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
        }
    }
    \foreach \e in {0,1}{%
        \foreach \d in {4}{%
        \pgfmathsetmacro\xxa{0}
        \pgfmathsetmacro\yya{0}
        \pgfmathsetmacro\zza{\e}
        \pgfmathsetmacro\xxb{0}
        \pgfmathsetmacro\yyb{\d}
        \pgfmathsetmacro\zzb{\e}
        \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
```

```
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
                }
        }
        \foreach \e in {3,4}{%
                \foreach \d in {3}{%
                \pgfmathsetmacro\xxa{\e}
                \pgfmathsetmacro\yya{0}
                \pgfmathsetmacro\zza{1}
                \pgfmathsetmacro\xxb{\e}
                \pgfmathsetmacro\yyb{0}
                \pgfmathsetmacro\zzb{1+\d}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
                }
        }
        \foreach \e in {3,4}{%
                \foreach \d in {3}{%
                \pgfmathsetmacro\xxa{0}
                \pgfmathsetmacro\yya{\e}
                \pgfmathsetmacro\zza{1}
                \pgfmathsetmacro\xxb{0}
                \pgfmathsetmacro\yyb{\e}
                \pgfmathsetmacro\zzb{1+\d}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
                }
        }
        \foreach \e in {3,4}{%
                \foreach \d in {3}{%
                \pgfmathsetmacro\xxa{\e}
                \pgfmathsetmacro\yya{0}
                \pgfmathsetmacro\zza{4}
                \pgfmathsetmacro\xxb{\e}
                \pgfmathsetmacro\yyb{4}
                \pgfmathsetmacro\zzb{4}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
                }
        }
        \foreach \e in {3,4}{%
                \foreach \d in {3}{%
                \pgfmathsetmacro\xxa{0}
                \pgfmathsetmacro\yya{\e}
                \pgfmathsetmacro\zza{4}
                \pgfmathsetmacro\xxb{4}
                \pgfmathsetmacro\yyb{\e}
                \pgfmathsetmacro\zzb{4}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
                }
        }
        \foreach \e in {1,2,3}{%
                \foreach \d in {1,2,3}{%
                \pgfmathsetmacro\xxa{3}
                \pgfmathsetmacro\yya{\e}
                \pgfmathsetmacro\zza{\d}
                \pgfmathsetmacro\xxb{3}
                \pgfmathsetmacro\yyb{\e-1}
                \pgfmathsetmacro\zzb{\d}
                \pgfmathsetmacro\xxc{3}
                \pgfmathsetmacro\yyc{\e}
                \pgfmathsetmacro\zzc{\d+1}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
                \draw [thick] (\thirdx,\thirdy) -- (\firstx, \firsty) -- (\secondx, \secondy);
                }
        }
        \foreach \e in {1,2}{%
                \foreach \d in {1,2,3}{%
                \pgfmathsetmacro\xxa{\e}
                \pgfmathsetmacro\yya{3}
                \pgfmathsetmacro\zza{\d}
                \pgfmathsetmacro\xxb{\e-1}
                \pgfmathsetmacro\yyb{3}
                \pgfmathsetmacro\zzb{\d}
                \pgfmathsetmacro\xxc{\e}
                \pgfmathsetmacro\yyc{3}
                \pgfmathsetmacro\zzc{\d+1}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
                \draw [thick] (\thirdx,\thirdy) -- (\firstx, \firsty) -- (\secondx, \secondy);
                }
        }
        \foreach \d in {1,2,3}{%
                \pgfmathsetmacro\xxa{2}
                \pgfmathsetmacro\yya{3}
                \pgfmathsetmacro\zza{\d}
                \pgfmathsetmacro\xxb{3}
                \pgfmathsetmacro\yyb{3}
                \pgfmathsetmacro\zzb{\d}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
        }
        \foreach \e in {1,2}{%
                \foreach \d in {1,2}{%
                \pgfmathsetmacro\xxa{\e}
                \pgfmathsetmacro\yya{\d}
                \pgfmathsetmacro\zza{1}
                \pgfmathsetmacro\xxb{\e-1}
                \pgfmathsetmacro\yyb{\d}
                \pgfmathsetmacro\zzb{1}
                \pgfmathsetmacro\xxc{\e}
                \pgfmathsetmacro\yyc{\d-1}
                \pgfmathsetmacro\zzc{1}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
                \draw [thick] (\thirdx,\thirdy) -- (\firstx, \firsty) -- (\secondx, \secondy);
                }
        }
        \foreach \d in {1,2,3}{%
                \pgfmathsetmacro\xxa{\d}
                \pgfmathsetmacro\yya{2}
                \pgfmathsetmacro\zza{1}
                \pgfmathsetmacro\xxb{\d}
                \pgfmathsetmacro\yyb{3}
                \pgfmathsetmacro\zzb{1}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
        }
        \foreach \d in {1,2}{%
                \pgfmathsetmacro\xxa{2}
                \pgfmathsetmacro\yya{\d}
                \pgfmathsetmacro\zza{1}
                \pgfmathsetmacro\xxb{3}
                \pgfmathsetmacro\yyb{\d}
                \pgfmathsetmacro\zzb{1}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
```

```
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
        }
        \foreach \d in {0,1,2,3,4}{%
            \pgfmathsetmacro\xxa{0+\d}
            \pgfmathsetmacro\yya{0}
            \pgfmathsetmacro\zza{0}
            \pgfmathsetmacro\xxb{0+\d}
            \pgfmathsetmacro\yyb{0}
            \pgfmathsetmacro\zzb{1}
            \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
            \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
            \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
            \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
            \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
        }
        \foreach \d in {0,1,2,3,4}{%
            \pgfmathsetmacro\xxa{0}
            \pgfmathsetmacro\yya{0+\d}
            \pgfmathsetmacro\zza{0}
            \pgfmathsetmacro\xxb{0}
            \pgfmathsetmacro\yyb{0+\d}
            \pgfmathsetmacro\zzb{1}
            \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
            \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
            \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
            \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
            \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
        }
        \foreach \d in {2,3,4}{%
            \pgfmathsetmacro\xxa{3}
            \pgfmathsetmacro\yya{0}
            \pgfmathsetmacro\zza{\d}
            \pgfmathsetmacro\xxb{4}
            \pgfmathsetmacro\yyb{0}
            \pgfmathsetmacro\zzb{\d}
            \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
            \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
            \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
            \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
            \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
        }
        \foreach \d in {2,3,4}{%
            \pgfmathsetmacro\xxa{0}
            \pgfmathsetmacro\yya{3}
            \pgfmathsetmacro\zza{\d}
            \pgfmathsetmacro\xxb{0}
            \pgfmathsetmacro\yyb{4}
            \pgfmathsetmacro\zzb{\d}
            \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
            \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
            \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
            \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
            \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
```

```
}
\foreach \d in {1,2}{%
    \pgfmathsetmacro\xxa{3}
    \pgfmathsetmacro\yya{\d}
    \pgfmathsetmacro\zza{4}
    \pgfmathsetmacro\xxb{4}
    \pgfmathsetmacro\yyb{\d}
    \pgfmathsetmacro\zzb{4}
    \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
    \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
    \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
    \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
    \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
}
\foreach \d in {1,2}{%
    \pgfmathsetmacro\xxa{\d}
    \pgfmathsetmacro\yya{3}
    \pgfmathsetmacro\zza{4}
    \pgfmathsetmacro\xxb{\d}
    \pgfmathsetmacro\yyb{4}
    \pgfmathsetmacro\zzb{4}
    \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
    \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
    \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
    \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
    \draw [thick] (\firstx, \firsty) -- (\secondx, \secondy);
}
\foreach \d in {3}{%
        \pgfmathsetmacro\xxa{0}
        \pgfmathsetmacro\yya{0}
        \pgfmathsetmacro\zza{1}
        \pgfmathsetmacro\xxb{0}
        \pgfmathsetmacro\yyb{0}
        \pgfmathsetmacro\zzb{\d+1}
        \pgfmathsetmacro\xxc{\d}
        \pgfmathsetmacro\yyc{0}
        \pgfmathsetmacro\zzc{\d+1}
        \pgfmathsetmacro\xxd{0}
        \pgfmathsetmacro\yyd{\d}
        \pgfmathsetmacro\zzd{\d+1}
        \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
        \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
        \pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
        \pgfmathsetmacro\fourthx{\xxd*\xdirx+\yyd*\ydirx+\zzd*\zdirx}
        \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
        \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
        \pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
        \pgfmathsetmacro\fourthy{\xxd*\xdiry+\yyd*\ydiry+\zzd*\zdiry}
        \draw [thick, dashed] (\firstx,\firsty) -- (\secondx,\secondy) -- (\thirdx,\thirdy);
        \draw [thick, dashed] (\secondx,\secondy) -- (\fourthx,\fourthy);
}
\foreach \d in {4}{%
        \pgfmathsetmacro\xxa{0}
        \pgfmathsetmacro\yya{0}
```

```
                \pgfmathsetmacro\zza{0}
                \pgfmathsetmacro\xxb{0}
                \pgfmathsetmacro\yyb{0}
                \pgfmathsetmacro\zzb{-1}
                \pgfmathsetmacro\xxc{\d}
                \pgfmathsetmacro\yyc{0}
                \pgfmathsetmacro\zzc{\d}
                \pgfmathsetmacro\xxd{\d+1}
                \pgfmathsetmacro\yyd{0}
                \pgfmathsetmacro\zzd{\d}
                \pgfmathsetmacro\xxe{0}
                \pgfmathsetmacro\yye{\d}
                \pgfmathsetmacro\zze{\d}
                \pgfmathsetmacro\xxf{0}
                \pgfmathsetmacro\yyf{\d+1}
                \pgfmathsetmacro\zzf{\d}
                \pgfmathsetmacro\firstx{\xxa*\xdirx+\yya*\ydirx+\zza*\zdirx}
                \pgfmathsetmacro\secondx{\xxb*\xdirx+\yyb*\ydirx+\zzb*\zdirx}
                \pgfmathsetmacro\thirdx{\xxc*\xdirx+\yyc*\ydirx+\zzc*\zdirx}
                \pgfmathsetmacro\fourthx{\xxd*\xdirx+\yyd*\ydirx+\zzd*\zdirx}
                \pgfmathsetmacro\fifthx{\xxe*\xdirx+\yye*\ydirx+\zze*\zdirx}
                \pgfmathsetmacro\sixthx{\xxf*\xdirx+\yyf*\ydirx+\zzf*\zdirx}
                \pgfmathsetmacro\firsty{\xxa*\xdiry+\yya*\ydiry+\zza*\zdiry}
                \pgfmathsetmacro\secondy{\xxb*\xdiry+\yyb*\ydiry+\zzb*\zdiry}
                \pgfmathsetmacro\thirdy{\xxc*\xdiry+\yyc*\ydiry+\zzc*\zdiry}
                \pgfmathsetmacro\fourthy{\xxd*\xdiry+\yyd*\ydiry+\zzd*\zdiry}
                \pgfmathsetmacro\fifthy{\xxe*\xdiry+\yye*\ydiry+\zze*\zdiry}
                \pgfmathsetmacro\sixthy{\xxf*\xdiry+\yyf*\ydiry+\zzf*\zdiry}
                \draw [->] (\firstx,\firsty) -- (\secondx,\secondy);
                \draw [->] (\thirdx,\thirdy) -- (\fourthx,\fourthy);
                \draw [->] (\fifthx,\fifthy) -- (\sixthx,\sixthy);
                \node [above right] at (\fourthx,\fourthy) {$x_1$};
                \node [left] at (\sixthx,\sixthy) {$x_2$\phantom{.}};
                \node [above right] at (\secondx,\secondy) {$x_3$};
        }
    \end{tikzpicture}
    \caption{$3$-tensor structure of the third formal derivative of a band space map.  Solid regions correspond to
nonzero coefficients.  Transparent regions correspond to zero coefficients.}\label{fig:bsd}
\end{figure}



\section{A Variant of MinRank Exploiting the Column Band Space Structure}\label{sec:modminrank}

A minrank-like attack may be used to locate the column band space maps defined in the previous section. In this case,
the attack proceeds by selecting $s^2$-dimensional vectors $\mathbf{w}_1$ and $\mathbf{w}_2$, setting

\begin{align}\label{CubicPubRankEq}
\bsp
\sum_{i=1}^{2s^2}t_i\nabla\mathcal{E}_i(\mathbf{w}_1) = 0,\\
\sum_{i=1}^{2s^2}t_i\nabla\mathcal{E}_i(\mathbf{w}_2) = 0,\\
\esp
\end{align}
and then solving for the $t_i$. The attack succeeds when $\sum_{i=1}^{2s^2}t_i\mathcal{E}_i \in
\mathcal{B}_{\beta,\gamma}$, and $\mathbf{x}_1$  and $\mathbf{x}_2$ are within the corresponding band kernel. If
```

```
these conditions are met, then the 2-tensors
\[
\sum_{i=1}^{2s^2}t_i\mathbf{H}(\mathcal{E}_i)(\mathbf{w}_1)\mbox{  and  }\sum_{i=1}^{2s^2}t_i\mathbf{H}(\mathcal{E}_i)(\mathbf{w}_2),
\]
 will have rank at most $2s$ (see Figure 2), and this will be easily detectable. Here $\mathbf{H}(\mathcal{E}_i)$ is the Hessian matrix
\[
\mathbf{H}(\mathcal{E}_i):=\left[\begin{matrix}
\frac{\partial^2\mathcal{E}_i}{\partial x_1^2} & \frac{\partial^2\mathcal{E}_i}{\partial x_1\partial x_2} & \cdots & \frac{\partial^2\mathcal{E}_i}{\partial x_1\partial x_{n}}\\
\frac{\partial^2\mathcal{E}_i}{\partial x_1\partial x_2} & \frac{\partial^2\mathcal{E}_i}{\partial x_2^2} & \cdots & \frac{\partial^2\mathcal{E}_i}{\partial x_1\partial x_{n}}\\
\vdots & \vdots & \ddots & \vdots\\
\frac{\partial^2\mathcal{E}_i}{\partial x_{n}\partial x_1} & \frac{\partial^2\mathcal{E}_i}{\partial x_{n}\partial x_2} & \cdots & \frac{\partial^2\mathcal{E}_i}{\partial x_{n}^2}\\
\end{matrix}\right].
\]



\begin{Thm}\label{BandKernelProb}
The probability that 2 randomly chosen vectors, $\mathbf{w}_1$ and $\mathbf{w}_2$, are both in the band kernel of some band space $\mathcal{B}_{\beta,\gamma}$ is approximately $\frac{1}{q-1}$.
%The probability that 3 randomly chosen vectors, $\mathbf{w}_1$, $\mathbf{w}_2$, and $\mathbf{w}_3$, are all in the band kernel of some band space $\mathcal{B}_{\beta,\gamma}$ is
%approximately $\frac{1}{(q-1)q^s}$.
\end{Thm}
\begin{proof}
The condition that the $\mathbf{w}_1$ and $\mathbf{w}_2$ are contained within a band kernel is that there be a nontrivial linear combination of the columns of the following matrix which is equal to zero (i.e. that the matrix has nonzero column corank):
\begin{equation*}
\left[ \begin{matrix}
b_1(\mathbf{w}_1) & b_2(\mathbf{w}_1) & \ldots & b_s(\mathbf{w}_1) & \vline &c_1(\mathbf{w}_1) & c_2(\mathbf{w}_1) & \ldots & c_s(\mathbf{w}_1) \\
b_{s+1}(\mathbf{w}_1)&b_{s+2}(\mathbf{w}_1)&\ldots&b_{2s}(\mathbf{w}_1)& \vline &c_{s+1}(\mathbf{w}_1)&c_{s+2}(\mathbf{w}_1)&\ldots&c_{2s}(\mathbf{w}_1)\\
\vdots& \vdots & \ddots & \vdots & \vline & \vdots& \vdots & \ddots & \vdots\\
b_{s^2-s+1}(\mathbf{w}_1) & b_{s^2-s+2}(\mathbf{w}_1) & \ldots &b_{s^2}(\mathbf{w}_1) & \vline &c_{s^2-s+1}(\mathbf{w}_1) &c_{s^2-s+2}(\mathbf{w}_1) & \ldots &c_{s^2}(\mathbf{w}_1)\\
\hline
b_1(\mathbf{w}_2) & b_2(\mathbf{w}_2) & \ldots & b_s(\mathbf{w}_2) & \vline &c_1(\mathbf{w}_2) & c_2(\mathbf{w}_2) & \ldots & c_s(\mathbf{w}_2) \\
b_{s+1}(\mathbf{w}_2)&b_{s+2}(\mathbf{w}_2)&\ldots&b_{2s}(\mathbf{w}_2)& \vline &c_{s+1}(\mathbf{w}_2)&c_{s+2}(\mathbf{w}_2)&\ldots&c_{2s}(\mathbf{w}_2)\\
\vdots& \vdots & \ddots & \vdots & \vline & \vdots& \vdots & \ddots & \vdots\\
b_{s^2-s+1}(\mathbf{w}_2) & b_{s^2-s+2}(\mathbf{w}_2) & \ldots &b_{s^2}(\mathbf{w}_2) & \vline &c_{s^2-s+1}(\mathbf{w}_2) &c_{s^2-s+2}(\mathbf{w}_2) & \ldots &c_{s^2}(\mathbf{w}_2)\\
%\hline
%\vdots&\vdots& & \vdots & \vline & \vdots&\vdots& & \vdots\\
\end{matrix}\right].
\end{equation*}
The matrix is a uniformly random $2s \times 2s$ matrix, which has nonzero column corank with probability approximately  $\frac{1}{q-1}$.
```

```
\qed
\end{proof}

\begin{Thm}\label{BandSpaceSolutionProb}
If $\mathbf{w}_1$ and $\mathbf{w}_2$ are chosen in such a way that
they are both in the band kernel of a column band space $\mathcal{B}_{\beta,\gamma}$, and they are linearly
independent from one another and statistically
independent from the private quadratic forms, $p_{(i-1)s+ j}$ in the matrix $A$,
then  $\mathbf{w}_1$ and $\mathbf{w}_2$ are both in the kernel of the first formal derivative of some column band
space map, $\mathcal{E} = \sum_{\mathcal{E}_{\beta,\gamma,i}\in\mathcal{B}_{\beta,\gamma}}\tau_i
\mathcal{E}_{\beta,\gamma,i}$  with probability approximately $\frac{1}{(q-1)q^s}$.
\end{Thm}

\begin{proof}
An $\mathcal{E}$ meeting the above condition exists iff there is a nontrivial solution to the following system of
equations
\begin{align} \label{BandRankEq}
\bsp
\sum_{\mathcal{E}_{\beta,\gamma,i}\in\mathcal{B}_{\beta,\gamma}}\tau_i \nabla\mathcal{E}_{\beta,\gamma,i}
(\mathbf{w}_1)&=0,\\
\sum_{\mathcal{E}_{\beta,\gamma,i}\in\mathcal{B}_{\beta,\gamma}}\tau_i \nabla\mathcal{E}_{\beta,\gamma,i}
(\mathbf{w}_2)&=0.\\
\esp
\end{align}

We may express our band space maps in a basis (e.g. the $u'_i$ basis used in Definition~\ref{bandkerneldef}) where the
first $s$ basis vectors are chosen to be outside the band kernel, and the  remaining $s^2-s$ basis vectors are chosen from
within the band kernel. Combining this with Definition 1, we see that the band space maps can be  written as

\[
\mathcal{E}_{\beta,\gamma,i} = \sum_{j=1}^s{p_{(i-1)s+ j}u'_j}.
\]

Note that $\mathbf{w}_1$ and $\mathbf{w}_2$ are band kernel vectors, and so for both vectors we have that $u'_j=0$
for $j = 1, \ldots, s$. Therefore, in such a basis, the only formal derivatives of $\mathcal{E}$ that can be nonzero are
$\frac{\partial \mathcal{E}}{\partial u'_j} = p_{(i-1)s+ j}$ for $j = 1, \ldots, s$. Thus in order for there to be a
nontrivial solution to Equation \eqref{BandRankEq}, it is necessary and sufficient that $\sum_{i=1}^s\tau_ip_{(i-1)s+
j}(\mathbf{w}_k)=0$ for $j = 1, \ldots, s$ and $k = 1,2$.
This condition will be satisfied if and only if the following $2s\times s$ matrix has nonzero column corank:
$$
\left[\begin{matrix}
p_1(\mathbf{w}_1) & p_{s+1} (\mathbf{w}_1) & \cdots & p_{s^2-s+1}(\mathbf{w}_1)\\
p_2(\mathbf{w}_1) & p_{s+2} (\mathbf{w}_1) & \cdots & p_{s^2-s+2}(\mathbf{w}_1)\\
\vdots & \vdots & \ddots & \vdots\\
p_s(\mathbf{w}_1) & p_{2s}(\mathbf{w}_1) & \cdots & p_{s^2}(\mathbf{w}_1).\\
\hline
p_1(\mathbf{w}_2) & p_{s+1}(\mathbf{w}_2) & \cdots & p_{s^2-s+1}(\mathbf{w}_2)\\
p_2(\mathbf{w}_2) & p_{s+2} (\mathbf{w}_2)& \cdots & p_{s^2-s+2}(\mathbf{w}_2)\\
\vdots & \vdots & \ddots & \vdots\\
p_s(\mathbf{w}_2) & p_{2s}(\mathbf{w}_2) & \cdots & p_{s^2}(\mathbf{w}_2)\\
\end{matrix}\right].
$$
This matrix is a random matrix over $k=\mathbb{F}_q$, which has nonzero column corank with
probability approximately $\frac{1}{(q-1)q^s}$, for practical parameters.
```

\qed
\end{proof}

Combining the results of Theorems \ref{BandKernelProb} and \ref{BandSpaceSolutionProb}, we find that for a random choice of the vectors $\mathbf{w}_1$ and $\mathbf{w}_2$, there is a column band space map among the solutions of Equation \eqref{CubicPubRankEq} with probability approximately $\frac{1}{(q-1)^2q^s}$. It may be somewhat undesirable to choose $\mathbf{w}_1$ and $\mathbf{w}_1$ completely randomly, however. The na\"ive algorithm for constructing the coefficients of Equation \eqref{CubicPubRankEq} for a random choice of $\mathbf{w}_1$ and $\mathbf{w}_2$ requires on the order of $s^8$ field operations. This can be reduced to $s^6$ operations if we make sure that each new choice of $\mathbf{w}_1$ and $\mathbf{w}_2$ differs from the previous choice at only a single coordinate. Then, rather than recomputing Equation \eqref{CubicPubRankEq} from scratch, we can use the previous values of the coefficients and we will only need to include corrections for the monomials that contain the variable that was changed from the previous iteration. Over a large number of iterations, the distribution of $\mathbf{w}_1$ and $\mathbf{w}_2$ should still be sufficiently close to random that the probability of success for the attack will not be meaningfully altered.

One final factor which may increase the cost of attacks is the expected dimension of the solution space of Equation \eqref{CubicPubRankEq}. If this space has a high dimension, then the attack will be slowed down since the attacker much search through a large number of spurious solutions to find a real solution (i.e. one where $\sum_{i=1}^{2s^2}t_i\mathbf{H}(\mathcal{E}_i)(\mathbf{w}_l)$ has rank at most $2s$ for $l = 1, 2$). Fortunately, Equation \eqref{CubicPubRankEq} is a system of $2s^2$ equations in $2s^2$ variables and it generally has a $0$-dimensional space of solutions. The lone exception occurs for characteristic 3. In this case, there are two linear dependencies among the equations, given by $\mathbf{w}_1\left[\nabla\mathcal{E}_i(\mathbf{w}_1)\right]^\top = 0$ and $\mathbf{w}_2\left[\nabla\mathcal{E}_i(\mathbf{w}_2)\right]^\top = 0$. In this situation we would therefore expect a 2-dimensional solution space. We can, however, recover two additional linear constraints on the $t_i$'s by also requiring:
\[
\sum_{i=1}^{2s^2}t_i \mathcal{E}_i(\mathbf{w}_l) = 0,\mbox{ for }l=1,2.\]
When these additional linear constraints are added to those given by Equation \eqref{CubicPubRankEq}, the expected dimension of the solution space drops back to 0. We can therefore assess the cost of the above attack at approximately $s^6q^{s+2}$, regardless of the characteristic.

\section {Application to the Quadratic ABC Scheme}

A similar technique was used to attack the original quadratic version of the ABC cryptosytem in \cite{DBLP:conf/pqcrypto/MoodyPS14}. While this technique was expressed in terms of the discrete differential, it can also be expressed using the formal derivative. In that case, the attack proceeds by selecting two random vectors $\mathbf{w}_1$ and $\mathbf{w}_2$, and solving an equation identical to Equation \eqref{CubicPubRankEq} for $t_i$, where the $\mathcal{E}_i$ are quadratic rather than cubic. The attack succeeds when $\sum_{i=1}^{2s^2}t_i\mathbf{H}(\mathcal{E}_i)$ has low rank.

When this attack is applied to parameters chosen over a field with characteristic 2, it is less efficient for the same reason as the basic attack given in the previous section is less efficient for the characteristic 3 parameters: the $2s^2$ linear equations given by Equation \eqref{CubicPubRankEq} have three linear dependencies given by
$\mathbf{w}_1\left[\nabla\mathcal{E}_i(\mathbf{w}_1)\right]^\top = 0,$
$\mathbf{w}_2\left[\nabla\mathcal{E}_i(\mathbf{w}_2)\right]^\top = 0,$ and
$\mathbf{w}_1\left[\nabla\mathcal{E}_i(\mathbf{w}_2)\right]^\top+
\mathbf{w}_2\left[\nabla\mathcal{E}_i(\mathbf{w}_1)\right]^\top = 0,$ and the attacker must generally search through a 3-dimensional solution space of spurious solutions in order to find a 1-dimensional space of useful solutions. As a result, the complexity of the attack for characteristic 2 is $s^{2\omega}q^{s+4},$ instead of $s^{2\omega}q^{s+2},$ as it is for all other characteristics. ($\omega \approx 2.373$ is the linear algebra constant.)

However, just as with cubic ABC parameters of characteristic 3, we can add two additional linear constraints and reduce the expected dimension of the solution space to 1:

\[
\sum_{i=1}^{2s^2}t_i \mathcal{E}_i(\mathbf{w}_l) = 0, \mbox{ for } l=1,2.
\]
Thus, we can also reduce the attack complexity for quadratic ABC parameters with characteristic 2 to
$s^{2\omega}q^{s+2}.$

%Equation \eqref{CubicPubRankEq} is a system of $2s^2$ equations in $2s^2$ variables; one might expect it to
generally have a $0$-dimensional space of solutions. In some cases,
%however, there are linear dependencies among the equations, due to the fact that the $D^2\mathcal{E}_i$ are
symmetric tensors. In even characteristic, we get 4 linear dependencies
%$D^2\mathcal{E}_i(\mathbf{x}_1,\mathbf{x}_2)(\mathbf{x}_1) = 0$,
$D^2\mathcal{E}_i(\mathbf{x}_1,\mathbf{x}_2)(\mathbf{x}_2)=0$, $D^2\mathcal{E}_i(\mathbf{x}_3
%\mathbf{x}_4)(\mathbf{x}_3)=0$, and $D^2\mathcal{E}_i(\mathbf{x}_3,\mathbf{x}_4)(\mathbf{x}_4)=0$, and an
additional linear dependency when we reduce the number of
%independent vectors to $3$ by setting $\mathbf{x}_1=\mathbf{x}_4$:
$D^2\mathcal{E}_i(\mathbf{x}_1,\mathbf{x}_2)(\mathbf{x}_3) + D^2\mathcal{E}_i(\mathbf{x}_3,\mathbf{x}_4
%(\mathbf{x}_2)=0$, resulting in a $5$-dimensional space of solutions. In characteristic 3, reducing the number of
independent vectors to $2$ results in $2$ linear dependencies among the
%equations: e.g. setting $\mathbf{x}_1 = \mathbf{x}_2$ and $\mathbf{x}_3=\mathbf{x}_4$, we have
$D^2\mathcal{E}_i(\mathbf{x}_1,\mathbf{x}_2)(\mathbf{x}_1)=0$ and
%$D^2\mathcal{E}_i(\mathbf{x}_3,\mathbf{x}_4)(\mathbf{x}_3)=0$. In higher characteristic, there are no linear
dependencies imposed on the equations by setting  $\mathbf{x}_1 =
%\mathbf{x}_2$ and $\mathbf{x}_3=\mathbf{x}_4$.

%For characteristic 2, finding the expected $1$-dimensional space of band space solutions in a $5$-dimensional space
costs $q^4+q^3+q^2+q+1$ rank operations, which in turn cost %$(s^2)^{\omega}$ field operations, where
$\omega\approx 2.373$ is the linear algebra constant. Likewise, for characteristic 3, finding the expected $1$-
dimensional space of band space %solutions in a $2$-dimensional space costs $q+1$ rank operations. Thus the total
cost of finding a column band space map using our variant of MinRank is approximately %$q^{2s+6}s^{2\omega}$ for
charactersitic 2, $q^{s+3}s^{2\omega}$ for characteristic 3, and $q^{s+2}s^{2\omega}$ for higher characteristic.

\section{Completing the Key Recovery}

%The detection of a low rank induced bilinear form $D^2\mathcal{E}(x)$ already constitutes a distinguisher from a
random system of equations.  Extending this calculation to a full key recovery requires further use of the differential
invariant structure of the public key.

Once the MinRank instance is solved, key extraction proceeds in a similar manner to \cite[Section 6]
{conf/sac/MoodyPS16} in the cubic case and \cite[Section 6]{DBLP:conf/pqcrypto/MoodyPS14}.  Here we discuss the
cubic version.

First, note that $U$ is not a critical element of the scheme.  If $A$ is a random matrix of quadratic forms and $B$ and
$C$ are random matrices of linear forms, then so are $A\circ U$, $B\circ U$ and $C\circ U$ for any full rank map $U$.
Thus, since $T\circ\phi(AB||AC)\circ U = T\circ\phi((A\circ U)(B\circ U)||(A\circ U)(C\circ U))$, we may absorb the
action of $U$ into $A$, $B$, and $C$, and consider the public key to be of the form
\[
P(\mathbf{x})=T\circ\phi(AB||AC)(\mathbf{x}).
\]

%Next, consider a trilinear form $D^2\mathcal{E}$ in the band space generated by $\mathcal{B}_{\beta, \gamma}$.
Since the coefficients of $D^2\mathcal{E}$ are products of coefficients of $A$ and coefficients of an element of
$Im(B||C)$, both of which are uniform i.i.d., there is a change of basis $M$ in which $D^2\mathcal{E}$ has the form in
Figure \ref{fig:bsd} and the nonzero coefficients are uniform i.i.d.

```
Let $\mathcal{E}\in\mathcal{B}_{\beta,\gamma}$, and consider $\mathbf{H}(\mathcal{E})$.  For $\mathbf{w}_1$ and $\mathbf{w}_2$ in the band kernel corresponding to $\mathcal{B}_{\beta,\gamma}$, there is a basis in which both $\mathbf{H}(\mathcal{E})(\mathbf{w}_1)$ and $\mathbf{H}(\mathcal{E})(\mathbf{w}_2)$ have the form illustrated in Figure \ref{fig:inducedForm}.  Thus, for $s \geq 3$, with high probability the kernels of both maps are contained in the corresponding band kernel $\mathcal{B}_{\beta,\gamma}$, and span$\left\{\mbox{ker}(\mathbf{H}(\mathcal{E})(\mathbf{w}_1),\mbox{ker}(\mathbf{H}(\mathcal{E})(\mathbf{w}_2)\right\} = \mathcal{B}_{\beta, \gamma}$.

%Consider $D^2\mathcal{E}(\mathbf{x}_1)$ and $D^2\mathcal{E}(\mathbf{x}_2)$ for $\mathbf{x}_1,\mathbf{x}_2$ in the band kernel corresponding to $\mathcal{B}_{\beta, \gamma}$.    Being maps from the same band space, there is a basis in which both $D^2\mathcal{E}(\mathbf{x}_1)$ and $D^2\mathcal{E}(\mathbf{x}_2)$ have the form in Figure \ref{fig:inducedForm}.  Thus, with high probability for $s \geq 2$, the kernels of both maps are contained in the corresponding band kernel, $\mathcal{B}_{\beta, \gamma}$, and $\mbox{span}(\mbox{ker}(D^2\mathcal{E}(\mathbf{x}_1)\cup \mbox{ker}(D^2\mathcal{E}(\mathbf{x}_2)) = \mathcal{B}_{\beta, \gamma}$.

\begin{figure}[!ht]
    \centering
    \begin{tikzpicture}
        \fill [fill=mediumgray] (0,0) -- (0,4) -- (4,4) -- (4,3) -- (1,3) -- (1,0) -- (0,0);
        \foreach \d in {0,1,2,3,4}{%
            \draw (\d,0) -- (\d,4);
            \draw (0,\d) -- (4,\d);
        }
    \end{tikzpicture}
    \caption{Structure of $\mathbf{H}(\mathcal{E})(\mathbf{w})$ when $\mathcal{E}\in\mathcal{B}_{\beta,\gamma}$ and $\mathbf{w}$ is in the band kernel corresponding to the band space $\mathcal{B}_{\beta,\gamma}$. The shaded region corresponds to nonzero coefficients.}\label{fig:inducedForm}
\end{figure}

%\begin{Rem}
%Here we have utilized a property which explicitly distinguishes differential invariant structure from rank structure.
%\end{Rem}

Given the basis for an $s^2-s$ dimensional band kernel $\mathcal{BK}$, we may choose a basis $\{v_1,\ldots, v_s\}$ for the subspace of the dual space vanishing on $\mathcal{BK}$.  We can also find a basis $\mathcal{E}_{v_1},\ldots,\mathcal{E}_{v_s}$ for the band space itself by solving the linear system
\begin{align*}
\bsp
\sum_{\mathcal{E}_i}\tau_i \mathcal{E}_i(\mathbf{w}_{1})&=0,\\
\sum_{\mathcal{E}_i}\tau_i \mathcal{E}_i(\mathbf{w}_{2})&=0,\\
\vdots &= \vdots\\
\sum_{\mathcal{E}_i}\tau_i \mathcal{E}_i(\mathbf{w}_{t})&=0,\\
\esp
\end{align*}
where $t\approx 2s^2$ and $\mathbf{w}_i$ is in the band kernel.

%Given the basis for an $s^2-s$ dimensional band kernel $\mathcal{BK}$, we may choose a basis $\{v_1,\ldots, v_s\}$ for the subspace of the dual space vanishing on $\mathcal{BK}$.  We can also find a basis $\mathcal{E}_{v_1},\ldots,\mathcal{E}_{v_s}$ for the band space itself by solving the linear system
%\begin{align*}
%\bsp
%\sum_{\mathcal{E}_i}\tau_i D^2\mathcal{E}_i(\mathbf{x}_{11},\mathbf{x}_{12},\mathbf{x}_{13})&=0,\\
%\sum_{\mathcal{E}_i}\tau_i D^2\mathcal{E}_i(\mathbf{x}_{21},\mathbf{x}_{22},\mathbf{x}_{23})&=0,\\
%\vdots &= \vdots\\
%\sum_{\mathcal{E}_i}\tau_i D^2\mathcal{E}_i(\mathbf{x}_{t1},\mathbf{x}_{t2},\mathbf{x}_{t3})&=0,\\
%\esp
%\end{align*}
%where $t\approx 2s^2$ and $\mathbf{x}_{ij}$ is in the band kernel.

Since the basis $\mathcal{E}_{v_1},\ldots,\mathcal{E}_{v_s}$ is in a single band space, there exists an element
$\left[\begin{matrix}b_1' & \cdots  & b_s'\end{matrix}\right]^{\top}$ in ColumnSpace$(B||C)$, and two matrices
$\Omega_1$ and $\Omega_2$ such that
\[
\Omega_1A\left(\Omega_2\left[\begin{matrix}b_1' \\ \vdots \\
b_s'\end{matrix}\right]\right)=:A'\left(\left[\begin{matrix}v_1 \\ \vdots \\
v_s\end{matrix}\right]\right)=\left[\begin{matrix}\mathcal{E}_{v_1} \\ \vdots
\\\mathcal{E}_{v_s}\end{matrix}\right].
\]
Solving the above system of equations over $\mathbb{F}_q[x_1,\ldots,x_{s^2}]$ uniquely determines $A'$ in the
quotient $\mathbb{F}_q[x_1,\ldots,x_{s^2}]/\left<v_1,\ldots,v_s\right>$.  To recover all of $A'$, note that the above
system is part of an equivalent key
\[
\mathcal{F}=T'\circ A'(B'||C')
\]
where $\left[\begin{matrix}v_1 & \cdots  & v_s\end{matrix}\right]^{\top}$ is the first column of $B'$.

Applying $T'^{-1}$ to both sides and inserting the information we know we may construct the system
\beq \label{SolveForBCT}
A'(B'||C')=T'^{-1}\mathcal{F}.
\eeq
Solving this system of equations modulo $\left<v_1,\ldots,v_s\right>$ for $B'$, $C'$ and $T'^{-1}$ we can recover a
space of solutions, which we will restrict by arbitrarily fixing the value of $T'^{-1}$. Note that the elements of
$T'^{-1}$ are constant polynomials, and therefore $T'^{-1} (\mbox{mod} \left<v_1,\ldots,v_s\right>)$ is the same as
$T'^{-1}$. Thus, for any choice of $T'^{-1}$ in this space, the second column of $T'^{-1}\mathcal{F}$ is a basis for a
band space.  Moreover, the elements $v'_{s+1},\ldots,v'_{2s}$ of the second column of $B' (\mbox{mod}
\left<v_1,\ldots,v_s\right>)$ are the image,  modulo $\left<v_1,\ldots,v_s\right>$, of linear forms vanishing on the
corresponding band kernel.  Therefore, we obtain the equality
\[
\left(\bigcap_{i=1}^{s}\mbox{ker}(v_i)\right) \bigcap \left(\bigcap_{i=s+1}^{2s}\mbox{ker}
(v'_i)\right)=\mathcal{BK}_2 \cap \mathcal{BK}_1,
\]
the intersection of the band kernels of our two band spaces.

We can reconstruct the full band kernel of this second band space using the same method we used to obtain our first
band kernel.  We take a map $\mathcal{E}_2$ from the second column of $T'^{-1}\mathcal{F}$, and two vectors
$\mathbf{w}_a$ and $\mathbf{w}_b$ from $\mathcal{BK}_2 \cap \mathcal{BK}_1$, and we compute
$\mathcal{BK}_2 =$ span$\left\{\mbox{ker}(\mathbf{H}(\mathcal{E}_2)(\mathbf{w}_a)\cup \mbox{ker}
(\mathbf{H}(\mathcal{E}_2)(\mathbf{w}_b)\right\}$. We can now solve for the second column of $B'$,
$\left[\begin{matrix}v_{s+1} & \cdots  & v_{2s}\end{matrix}\right]^{\top}$, uniquely over
$\mathbb{F}_q[x_1,\ldots,x_{s^2}]$ (NOT modulo $\left<v_1,\ldots,v_s\right>$) by solving the following system of
linear equations:

\begin{align*}
v_i \equiv v'_i \mbox{mod} \left<v_1,\ldots,v_s\right>,\\
v_i(\mathbf{w}_1)=0,\\
v_i(\mathbf{w}_2)=0,\\
\vdots = \vdots\\
```

v_i(\mathbf{w}_{s^2-s})=0,\\
\end{align*}
where $ i=s+1, \ldots, 2s$, and $\left\{\mathbf{w}_1, \ldots, \mathbf{w}_{s^2-s}\right\}$ is a basis for $\mathcal{BK}_2$. We can now solve for $A'$ (again, uniquely over $\mathbb{F}_q[x_1,\ldots,x_{s^2}]$) by solving:

\[
A'\left(\left[\begin{matrix}v_1 \\ \vdots \\  v_s\end{matrix}\right]\right) \equiv \left[\begin{matrix}\mathcal{E}_{v_1} \\ \vdots \\ \mathcal{E}_{v_s}\end{matrix}\right]
\mbox{mod} \left<v_1,\ldots,v_s\right>,
\]
\[
A'\left(\left[\begin{matrix}v_{s+1} \\ \vdots \\  v_{2s}\end{matrix}\right]\right) \equiv
\left[\begin{matrix}\mathcal{E}_{v_{s+1}} \\ \vdots \\ \mathcal{E}_{v_{2s}}\end{matrix}\right]
\mbox{mod} \left<v_{s+1},\ldots,v_{2s}\right>,
\]
where $\left[\begin{matrix}\mathcal{E}_{v_{s+1}} & \cdots  & \mathcal{E}_{v_{2s}}\end{matrix}\right]^{\top}$ is the second column of $T'^{-1}\mathcal{F}$. This allows us to solve Equation \eqref{SolveForBCT} for the rest of $B'$ and $C'$, completing the attack.

The primary cost of the attack involves finding the band space map.  The rest of the key recovery is additive in complexity and dominated by the band space map recovery; thus the total complexity of the attack is of the same order as the band space map recovery.  Hence, the cost of private key extraction is approximately $q^{s+2}s^{6}$ for all characteristics.  %We note that with these parameters we can break full sized instances of this scheme with parameters chosen for the $80$-bit and $100$-bit security levels via the criteria presented in \cite{DBLP:conf/pqcrypto/DingPW14}.

The original parameters of Cubic ABC were designed for a security level of $80$-bits and $100$-bits.  Since NIST has been recommending a security level of $112$-bits since 2015, see \cite{SP800-131A}, these figures may be a bit out of date.  In fact, our attack seems more effective for larger parameter sets than small.

We note that our attack breaks CubicABC($q=2^8,s=7$), designed for $80$-bit security, in approximately $2^{88}$ operations.  More convincingly, our attack breaks CubicABC($q=2^8,s=8$), designed for $100$-bit security, in approximately $2^{98}$ operations, indicating that for parameters as small as these, we have already crossed the threshold of algebraic attack efficiency.  Furthermore, the attack is fully parallelizable and requires very little memory.  Hence, this technique is asymptotically far more efficient than algebraic attacks, the basis for the original security estimation in \cite{DBLP:conf/pqcrypto/DingPW14}.

In the case of the quadratic ABC scheme, the original $86$-bit secure parameters ABC$(q=2^8,s=8)$.  The attack complexity with the new methodology presented here is $2^{87}$, just above the claimed level.  We note, however, that the authors of \cite{DBLP:conf/pqcrypto/TaoDTD13} supplied additional parameters using odd characteristic in their presentation at PQCRYPTO 2013, see \cite{abcpres}, with a claimed security level of $108$-bits.  This scheme, ABC$(q=127,s=8)$ offers resistance only to the level of $2^{77}$ to our slight improvement in technique over that of \cite{DBLP:conf/pqcrypto/MoodyPS14}.  Thus, our attack definitively breaks these parameters.

\section{Comparison with Minors Methods}

The MinRank problem has been a central computational challenge related to the security of various multivariate schemes since the beginning of the century, and as discussed in the previous section, is the primary bottleneck of our attack.  There are two main disparate techniques for solving MinRank.

The first technique, which we employ here, can be called ``linear algebra search."  The linear algebra search technique randomly selects vectors $\mathbf{x}_1,\ldots,\mathbf{x}_\ell\in k^n$ in an attempt to solve a system of equations of the form:
\[

\left(\sum_{i=1}^mt_i\mathbf{M}_i \right) \mathbf{x}_j=\mathbf{0}\mbox{ for }j\in\{1,\ldots,\ell\}.
\]
The technique is essentially free in terms of memory, but is exponential in $q$, the size of $k$. The linear algebra search can benefit from certain exponential speedups depending on the structure of the equations. In particular, the linear algebra search is exponentially faster in the case of ``interlaced kernels" as specified in \cite{DBLP:journals/dcc/BettaleFP13} or in the case of differential invariants, as in the case of the original ABC scheme, see \cite{DBLP:conf/pqcrypto/MoodyPS14}.

The second technique is known as minors modeling. Given an instance of minrank, $\mathbf{M}_1,\ldots,\mathbf{M}_m$ with target rank $r$, construct the matrix
\[
\sum_{i=1}^my_i\mathbf{M}_i,
\]
with entries in $k[y_1,\ldots,y_m]$. Since there is an assignment of values of the $y_i$ in $k$ such that the resulting matrix has rank $r$, via the Finite Field Nullstellensatz, the system of $r+1\times r+1$ minors of this matrix, along with the field equations $y_i^q-y_i$, form a positive dimensional ideal. Fixing a variable to a nonzero value by adding another equation, say $y_1-1$ still statistically results in a nonempty variety containing solutions to the MinRank problem.

The complexity of the minors modeling technique is dependent upon the degree of regularity of minors system, though this can easily be seen for large systems to be r+1, since for sufficiently large schemes the application of a Gr\"obner basis algorithm is equivalent to linearization. Thus the complexity is $\mathcal{O}\left({m+r+1 \choose r+1}^\omega\right)$, where $\omega$ is the linear algebra constant. A serious drawback of this technique is memory usage, which also nontrivially complicates the practical time complexity. The space complexity of the minors approach can be roughly estimated as $\mathcal{O}\left({m+r\choose r+1}^2\right)$.

To make a direct comparison of these techniques for the MinRank portion of the attack, we use the parameters $q=2^8$ and $s=8$ discussed in the previous section. Recall that the linear algebra search technique requires memory on the order of $s^4q=2^{20}$ and that the time complexity is about $2^{87}$. For the minors modeling method, the space complexity can be computed from the above estimates using $m=2s^2=128$ and $r=2s=16$ to be about $2^{144}$, roughly the square root of the number of subatomic particles in the universe, and the time complexity is $2^{172}$. We thus conclude that for such small values of $q$ that the linear algebra search, due to the interlaced nature of the kernels, is far more efficient. Furthermore, for ABC schemes, it is questionable whether the memory constraints for the minors approach can ever be realistic.

\section{Experiments}

Using SAGE \cite{sagemath}, we performed some experiments as a sanity check to confirm the efficiency of our ideas on small scale variants of the Cubic ABC scheme. The computer used has a 64 bit quad-core Intel i7 processor, with clock cycle 2.8 GHz. Rather than considering the full attack, we were most interested in confirming our complexity estimates on the most costly step in the attack, the MinRank instance. Given as input the finite field size $q$, and the scheme parameter $s$, we computed the average number of vectors $v$ required to be sampled in order for the rank of the $2$-tensor $\mathbf{H}(\mathcal{E})(v)$ to fall to $2s$. As explained in Section 4, when the rank falls to this level, we have identified the subspace differential invariant structure of the scheme which can then be exploited to attack the scheme.

As this paper is only concerned with binary fields, we ran experiments with $q=2, 4$ and $8$. We found that for $s=3$ and $q=2,4$, or $8$, with high probability only a single vector was needed before the rank fell to $2s$. For $s=4$ and $s=5$, the computations were only feasible in SAGE for $q=2$ and $q=4$. The average values obtained are presented in the table below. Note that for $q=4$ and $s=5$ the average value is based on a small number of samples as the computation time was quite lengthy.

```
\begin{table}
\centering
\begin{tabular}{|c| c c c| c c c|}
\hline
& $s=4$ & & $(q-1)^2q^s$ & $s=5$ & & $(q-1)^2 q^s$ \\
\hline
$q=2$ & 24 & & 16  & 35 & & 32  \\ \hline
$q=4$ & 1962 & & 2304 & 7021 & & 9216 \\
\hline
\end{tabular}
\caption{Average number of vectors needed for the rank to fall to $2s$ versus the predicted values.}
\label{table:1}
\end{table}

In comparison, our previous experiments \cite{conf/sac/MoodyPS16} were only able to obtain data for $q=2$ and $s=4,5$.  The average number of vectors needed in the $s=4$ case was 244, while for $s=5$, the average number in our experiments was 994 (with the predicted values being 256 and 1024).



%Using SAGE \cite{sage}, we performed some minrank computations on small scale variants of the Cubic ABC scheme. The computations were done on a computer with a 64 bit quad-core Intel i7 processor, with clock cycle 2.8 GHz.  We were interested in verifying our complexity estimates on the most costly step in the attack, the MinRank instance, rather than the full attack on the ABC scheme.  Given as input the finite field size $q$, and the scheme parameter $s$, we computed the average number of vectors $v$ required to be sampled in order for the rank of the $2$-tensor $D^2\mathcal{E}(v)$ to fall to $2s$.  As explained in Section \ref{sec:modminrank}, when the rank falls to this level, we have identified the subspace differential invariant structure of the scheme and can exploit this structure to attack the scheme.  Our results for odd $q$ are given in Table 1.
%
%\begin{table}
%\centering
%\begin{tabular}{|c| c c| c c| c c|}
% \hline
% & $s=3$ & $(q-1)^2q^s$ & $s=4$ & $(q-1)^2q^s$ & $s=5$ & $(q-1)^2q^s$\\
% \hline
% $q=3$ & 14.75 & 108 & 333 & 324 & 952 & 972\\ \hline
% $q=5$ & 378 & 2000 & 9986 &  10000 & &\\ \hline
% $q=7$ & 1688 & 12348 & 72951 & 86436 & & \\ \hline
% $q=9$ & 606 &  46656 & & & & \\ \hline
% $q=11$ & 13574 &  133100 &  & & &\\
% \hline
%\end{tabular}
%\caption{Average number of vectors needed for the rank to fall to $2s$ (for odd $q$)}
%\label{table:1}
%\end{table}
%For higher values of $q$ and $s$ the computations took too long to produce sufficiently many data points and obtain meaningful results with SAGE.  When $q$ is odd, our analysis predicted the number of vectors needed would be on the order of $(q-1)^2q^s$.  Table 1 shows the comparison between our experiments and the expected value.  We see that for $s=3$, the rank fell quicker than expected, while for $s>3$ the results are quite near the predicted value.  This is because when $s=3$ our complexity estimates given in Section \ref{sec:modminrank} are simply not accurate enough, which happens for small values of $q$ and/or $s$.
%
%For even $q$, we also ran some experiments.  We found that for $s=3$ and $q=2,4$, or $8$, with high probability only a single vector was needed before the rank fell to $2s$.  For $s=4$ and $s=5$, the computations were only feasible in SAGE for $q=2$.  The average number of vectors needed in the $s=4$ case was 244, with the expected value being
```

$(q-1)^2q^{2s}=256$.  With $s=5$, the average number in our experiments was 994 (although the number of trials was small), with the expected value 1024.  For higher values of $q$ and $s$ the computations took too long to obtain meaningful results.

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

\section{Conclusion}

The ABC schemes offer an interesting new technique for the construction of multivariate public key schemes.  Previously, we have used the multiplicative structure of an extension field to generate an efficiently invertible map.  Schemes built on such a construct are known as ``big field'' schemes.  The ABC framework is essentially a ``large structure'' or perhaps ``large algebra'' scheme, depending on multiplication from a matrix algebra over the base field.  Since the only simple algebras are either matrix algebras or field extensions, we seem to have exhausted the possibilities.  Interestingly, MinRank techniques seem optimal in this setting, at least asymptotically in the dimension of the extension.

Also interesting to note is the fact that the authors present in \cite{DBLP:conf/pqcrypto/DingPW14} a heuristic security argument for the provable security of the scheme and reinforce the notion of provable security in this venue at the presentation of the scheme at \cite{DBLP:conf/pqcrypto/2014}.  Unfortunately, this analysis does not contribute a sound conclusion, as demonstrated by the methodology of \cite{conf/sac/MoodyPS16}. With our improved attack, we rule out the possibility that the cubic variant of ABC offers any security advantage over the original quadratic scheme.  Likewise, our improved attack on quadratic ABC eliminates any security benefit associated with characteristic-2 parameters in the quadratic case.

%The ABC scheme offers a promising new idea for the development of multivariate encryption schemes.  Although the original presentation of the scheme contained errors--- most significantly in the estimated probability of decryption failure--- the scheme is easily generalized to nonsquare matrices and these anomalies are inconsequential in this context.  In particular, the HOLEs attack is nonexistent when $A$, $B$, and $C$ are replaced with rectangular matrices.
%
%The attack outlined in this article exploits the subspace differential invariant structure inherent to the ABC methodology.  The attack method works both for the original scheme and when applied to the updated scheme.  With the original parameters, the attack is asymptotically the most efficient structural attack, with bit complexity scaling linearly with $s$, the square root of the number of variables.  In the improved scheme, the attack scales in bit complexity in proportion to the parameter $r$ which is less than the square root of the number of variables.  This analysis is tighter than any relevant rank analysis in the literature, with the most appropriate technique in \cite{DBLP:conf/acisp/YangC05} scaling in bit complexity linearly with $2s$.  In comparison, even the bit complexity of algebraic attacks scale superlinearly in $s$, though the break-even point for the two attacks is slightly beyond the 120-bit security threshold.  Taking both time and memory into consideration, however, the differential invariant attack may be the more practical.
%
%A remarkable fact about the attack outlined in this article is that it exploits characteristics which uniquely distinguish the public polynomials in the ABC scheme or its improvement from random formulae, namely, the existence of the $s$ subspace differential invariants.  The existence of the differential invariants relative to the band spaces is \emph{equivalent} to the property of being isomorphic to a product of matrices of linear forms as in the central map of the ABC scheme; indeed, the attack produces such an isomorphism.  In this sense, it is hard to imagine any key recovery attack on such a scheme designed for $80$-bit security which is significantly more efficient in terms of time than the algebraic attack, directly solving the system via Gr\"{o}bner Bases, or an XL variant such as the Mutant XL algorithms, see \cite{mxl,mxl2,DBLP:conf/icisc/MohamedCDBB09}.
%
%On the other hand, it is worthwhile mentioning Gr\"{o}bner basis techniques for solving MinRank problems using minors modeling as in \cite{DBLP:conf/issac/FaugereDS10}, and perhaps most notably exemplified in \cite{DBLP:journals/dcc/BettaleFP13}.  Assuming no additional structure in the MinRank instances arising from the cryptanalysis of the ABC scheme generic, the degree of regularity of the resulting MinRank polynomial systems is $2s+1$ for small values of $s$, and so the complexity of this approach is immense.  The actual MinRank instances

arising from the ABC scheme, however, hold some of the structure of the central map and so there is some hope for improvement in this area, though this remains an open problem.
%
%While it is clear that the decryption failure issue of the ABC scheme can be fixed by inflating the field size and/or by making the core matrices rectangular, the scalability of the scheme is an issue.  The public key size of the original scheme scales with the \emph{sixth} power of $s$.  If we take into consideration security requirements beyond $80$ bits, the ABC scheme becomes problematic; increasing $s$ by one more than doubles the key size.  While the evidence seems to suggest that the enhanced ABC scheme, despite having such a distinct differential structure, may ironically be secure, the task of turning the scheme into a more finely tuneable technology is still an open question.

```
% ==============================================================================
\bibliographystyle{splncs}
\bibliography{References}
\end{document}
```

```
@inproceedings{conf/pqcrypto/BaenaCEPBV15,
  author    = {John Baena and Daniel Cabarcas and Daniel Escudero and Jailberth Porras-Barrera and Javier Verbel},
  title     = {Efficient ZHFE Key Generation},
  booktitle = {Post-Quantum Cryptography - 7th International Conference, PQCrypto 2016, Fukuoka, Japan, February
24-26, 2016. Proceedings},
  year      = {2016},
}

@inproceedings{DBLP:conf/eurocrypt/DuboisFS07,
  author    = {Vivien Dubois and
               Pierre-Alain Fouque and
               Jacques Stern},
  title     = {Cryptanalysis of {SFLASH} with {S}lightly {M}odified {P}arameters},
  booktitle = {EUROCRYPT},
  year      = {2007},
  pages     = {264-275},
  ee        = {http://dx.doi.org/10.1007/978-3-540-72540-4_15},
  crossref  = {DBLP:conf/eurocrypt/2007},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@proceedings{DBLP:conf/eurocrypt/2007,
  editor    = {Moni Naor},
  title     = {Advances in Cryptology - EUROCRYPT 2007, 26th Annual International
               Conference on the Theory and Applications of Cryptographic
               Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings},
  booktitle = {EUROCRYPT},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {4515},
  year      = {2007},
  isbn      = {978-3-540-72539-8},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@manual{sagemath,
  Key          = {SageMath},
  Author       = {The Sage Developers},
  Title        = {{S}ageMath, the {S}age {M}athematics {S}oftware {S}ystem ({V}ersion x.y.z)},
  note         = {{\tt http://www.sagemath.org}},
  Year         = {YYYY},
}

@inproceedings{DBLP:conf/crypto/DuboisFSS07,
  author    = {Vivien Dubois and
               Pierre-Alain Fouque and
               Adi Shamir and
               Jacques Stern},
  title     = {Practical {C}ryptanalysis of {SFLASH}},
  booktitle = {CRYPTO},
  year      = {2007},
  pages     = {1-12},
  ee        = {http://dx.doi.org/10.1007/978-3-540-74143-5_1},
  crossref  = {DBLP:conf/crypto/2007},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@proceedings{DBLP:conf/crypto/2007,
  editor    = {Alfred Menezes},
  title     = {Advances in Cryptology - CRYPTO 2007, 27th Annual International
               Cryptology Conference, Santa Barbara, CA, USA, August 19-23,
               2007, Proceedings},
  booktitle = {CRYPTO},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {4622},
  year      = {2007},
  isbn      = {978-3-540-74142-8},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{DBLP:conf/pqcrypto/SzepieniecDP16,
  author    = {Alan Szepieniec and
               Jintai Ding and
               Bart Preneel},
  title     = {Extension Field Cancellation: {A} New Central Trapdoor for Multivariate
               Quadratic Systems},
  booktitle = {Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016,
               Fukuoka, Japan, February 24-26, 2016, Proceedings},
  pages     = {182--196},
  year      = {2016},
  crossref  = {DBLP:conf/pqcrypto/2016},
  url       = {http://dx.doi.org/10.1007/978-3-319-29360-8_12},
  doi       = {10.1007/978-3-319-29360-8_12},
  timestamp = {Wed, 10 Feb 2016 14:52:29 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pqcrypto/SzepieniecDP16},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@article{Feynman:1981tf,
      author         = "Feynman, Richard P.",
      title          = "{Simulating physics with computers}",
      journal        = "Int. J. Theor. Phys.",
      volume         = "21",
      year           = "1982",
      pages          = "467-488",
      doi            = "10.1007/BF02650179"
}

@misc{CFP,
    author = {Cryptographic Technology Group},
    title = {Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization
Process},
    howpublished = {NIST CSRC},
    year = {2016},
    note = {http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf}
}
```

```
@misc{SP800-131A,
   author = {Elaine Barker and Allen Roginsky},
   title = {Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths},
   howpublished = {NIST Special Publication},
   year = {2015},
   note = {http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf}
}



@misc{Ding,
   author = {Jintai Ding and Bo-Yin Yang and Chen-Mou Cheng and  Owen Chen and Vivien Dubois},
   title = {Breaking the {S}ymmetry: a {W}ay to {R}esist the {N}ew {D}ifferential {A}ttack},
   howpublished = {Cryptology ePrint Archive, Report 2007/366},
   year = {2007},
   note = {http://eprint.iacr.org/}
}



@inproceedings{DBLP:conf/icalp/DingDYCC08,
  author    = {Jintai Ding and
               Vivien Dubois and
               Bo-Yin Yang and
               Chia-Hsin Owen Chen and
               Chen-Mou Cheng},
  title     = {Could {SFLASH} be {R}epaired?},
  booktitle = {ICALP (2)},
  year      = {2008},
  pages     = {691-701},
  ee        = {http://dx.doi.org/10.1007/978-3-540-70583-3_56},
  crossref  = {DBLP:conf/icalp/2008-2},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@proceedings{DBLP:conf/icalp/2008-2,
  editor    = {Luca Aceto and
               Ivan Damg{\aa}rd and
               Leslie Ann Goldberg and
               Magn{\'u}s M. Halld{\'o}rsson and
               Anna Ing{\'o}lfsd{\'o}ttir and
               Igor Walukiewicz},
  title     = {Automata, Languages and Programming, 35th International
               Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008,
               Proceedings, Part II - Track B: Logic, Semantics, and Theory
               of Programming {\&} Track C: Security and Cryptography
               Foundations},
  booktitle = {ICALP (2)},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {5126},
  year      = {2008},
  isbn      = {978-3-540-70582-6},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@article{DBLP:journals/dcc/BettaleFP13,
  author    = {Luk Bettale and
               Jean{-}Charles Faug{\`{e}}re and
               Ludovic Perret},
  title     = {Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic},
  journal   = {Des. Codes Cryptography},
  volume    = {69},
  number    = {1},
  pages     = {1--52},
  year      = {2013},
  url       = {http://dx.doi.org/10.1007/s10623-012-9617-2},
  doi       = {10.1007/s10623-012-9617-2},
  timestamp = {Mon, 24 Jun 2013 15:07:47 +0200},
  biburl    = {http://dblp.uni-trier.de/rec/bib/journals/dcc/BettaleFP13},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@article{Dinglic,
    author = "J. Ding and C. Wolf and B.-Y. Yang",
    title = "l-invertible cycles for multivariate quadratic public key cryptography",
    journal = "PKC 2007 of LNCS",
    volume = 4450,
    year = 2007,
    pages = "266-281",
}

@inproceedings{DBLP:conf/eurocrypt/MatsumotoI88,
  author    = {Tsutomu Matsumoto and
               Hideki Imai},
  title     = {Public {Q}uadratic {P}olynominal-{T}uples for {E}fficient {S}ignature-{V}erification
               and {M}essage-{E}ncryption},
  booktitle = {EUROCRYPT},
  year      = {1988},
  pages     = {419-453},
  ee        = {http://link.springer.de/link/service/series/0558/bibs/0330/03300419.htm},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}


@inproceedings{DBLP:conf/crypto/Patarin95,
  author    = {Jacques Patarin},
  title     = {Cryptoanalysis of the {M}atsumoto and {I}mai {P}ublic {K}ey {S}cheme
               of {E}urocrypt'88},
  booktitle = {CRYPTO},
  year      = {1995},
  pages     = {248-261},
  ee        = {http://dx.doi.org/10.1007/3-540-44750-4_20},
  crossref  = {DBLP:conf/crypto/1995},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}
```

```
@proceedings{DBLP:conf/crypto/1995,
  editor    = {Don Coppersmith},
  title     = {Advances in Cryptology - CRYPTO '95, 15th Annual International
               Cryptology Conference, Santa Barbara, California, USA, August
               27-31, 1995, Proceedings},
  booktitle = {CRYPTO},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {963},
  year      = {1995},
  isbn      = {3-540-60221-6},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{DBLP:conf/asiacrypt/PatarinGC98,
  author    = {Jacques Patarin and
               Louis Goubin and
               Nicolas Courtois},
  title     = {${C}^*_{-+}$ and {HM}: {V}ariations {A}round
               {T}wo {S}chemes of {T}. {M}atsumoto and {H}. {I}mai},
  booktitle = {ASIACRYPT},
  year      = {1998},
  pages     = {35-49},
  ee        = {http://link.springer.de/link/service/series/0558/bibs/1514/15140035.htm},
  crossref  = {DBLP:conf/asiacrypt/1998},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@proceedings{DBLP:conf/asiacrypt/1998,
  editor    = {Kazuo Ohta and
               Dingyi Pei},
  title     = {Advances in Cryptology - ASIACRYPT '98, International Conference
               on the Theory and Applications of Cryptology and Information
               Security, Beijing, China, October 18-22, 1998, Proceedings},
  booktitle = {ASIACRYPT},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {1514},
  year      = {1998},
  isbn      = {3-540-65109-8},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}



@inproceedings{DBLP:conf/eurocrypt/Patarin96,
  author    = {Jacques Patarin},
  title     = {Hidden {F}ields {E}quations ({HFE}) and {I}somorphisms of {P}olynomials
               ({IP}): {T}wo {N}ew {F}amilies of {A}symmetric {A}lgorithms},
  booktitle = {EUROCRYPT},
  year      = {1996},
  pages     = {33-48},
  ee        = {http://link.springer.de/link/service/series/0558/bibs/1070/10700033.htm},
  bibsource = {DBLP, http://dblp.uni-trier.de}
```

```
}


@article{Mollin,
  author = "R. A. Mollin and C. Small",
  title = "On {P}ermutation {P}olynomials over {F}inite {F}ields",
  journal = "Internat. J. Math. and Math. Sci.",
  pages = "535-543",
  volume = 10,
  year = 1987,
  }

@misc{Wolf,
    author = {C. Wolf and B. Preneel},
    title = {Taxonomy of {P}ublic {K}ey {S}chemes {B}ased on the {P}roblem of {M}ultivariate {Q}uadratic
{E}quations},
    howpublished = {Cryptology ePrint Archive, Report 2005/077},
    year = {2005},
    note = {http://eprint.iacr.org/},
}

@INPROCEEDINGS{MurphyRobshaw:easaes,
    author = {S. Murphy and M. J. B. Robshaw and Royal Holloway},
    title = {Essential algebraic structure within the AES},
    booktitle = {},
    year = {2002},
    pages = {1--16},
    publisher = {Springer-Verlag}
}

@book{LidlNied,
 author = {Lidl, Rudolf and Niederreiter, Harald},
 title = {Introduction to {F}inite {F}ields and their {A}pplications},
 year = {1986},
 isbn = {0-521-30706-6},
 publisher = {Cambridge University Press},
 address = {New York, NY, USA},
 }



@inproceedings{DBLP:conf/ctrsa/CloughBDYC09,
  author    = {Crystal Clough and
               John Baena and
               Jintai Ding and
               Bo-Yin Yang and
               Ming-Shing Chen},
  title     = {Square, a {N}ew {M}ultivariate {E}ncryption {S}cheme},
  booktitle = {CT-RSA},
  year      = {2009},
  pages     = {252-264},
  ee        = {http://dx.doi.org/10.1007/978-3-642-00862-7_17},
  crossref  = {DBLP:conf/ctrsa/2009},
  bibsource = {DBLP, http://dblp.uni-trier.de}
```

```
}

@proceedings{DBLP:conf/ctrsa/2009,
  editor    = {Marc Fischlin},
  title     = {Topics in Cryptology - CT-RSA 2009, The Cryptographers'
               Track at the RSA Conference 2009, San Francisco, CA, USA,
               April 20-24, 2009. Proceedings},
  booktitle = {CT-RSA},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {5473},
  year      = {2009},
  isbn      = {978-3-642-00861-0},
  ee        = {http:/dx.doi.org/10.1007/978-3-642-00862-7},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}



@book{DummitFoote,
    author = {David S. Dummit and Richard M. Foote},
    title = {Abstract Algebra, 3rd ed.},
    publisher = {John Wiley and Sons, Inc.},
    isbn = {978-0471433347},
    year = {2004}
}



@book{DaemenRijnmen,
    author = {J. Daemen and V. Rijmen},
    title = {The Design of Rijndael: AES - The Advanced Encryption Standard},
    publisher = {Springer-Verlag},
    isbn = {30540-42580-2},
    year = {2002}
}

@article{Buss1999572,
title = "The Computational Complexity of Some Problems of Linear Algebra ",
journal = "Journal of Computer and System Sciences ",
volume = "58",
number = "3",
pages = "572 - 596",
year = "1999",
note = "",
issn = "0022-0000",
doi = "http://dx.doi.org/10.1006/jcss.1998.1608",
url = "http://www.sciencedirect.com/science/article/pii/S0022000098916087",
author = "Jonathan F Buss and Gudmund S Frandsen and Jeffrey O Shallit"
}

@article{KipnisShamir:relin,
  author = "A. Kipnis and A. Shamir",
  title = "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization",
  journal = "Advances in Cryptology - CRYPTO 1999, Springer",
  pages = "788",
  volume = 1666,
  year = 1999,
  }

@inproceedings{JiangDing,
  author    = {Xin Jiang and
               Jintai Ding and
               Lei Hu},
  title     = {Kipnis-Shamir Attack on HFE Revisited},
  booktitle = {Inscrypt},
  year      = {2007},
  pages     = {399-411},
  ee        = {http://dx.doi.org/10.1007/978-3-540-79499-8_31},
  crossref  = {DBLP:conf/cisc/2008},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@INPROCEEDINGS{CidMurphyRobshaw:ssvaes,
    author = {C. Cid and S. Murphy and M. J. B. Robshaw},
    title = {Small Scale Variants of the AES},
    booktitle = {In: Fast Software Encryption, 12th International Workshop, FSE 2005},
    year = {2005},
    pages = {145--162},
    publisher = {Springer}
}

@article{KBFS,
  author = "Oleg Kiselyov and William E. Byrd and Daniel P. Friedman and Chung-chieh Shan",
  title = "Pure, declarative, and constructive arithmetic relations (declarative pearl)",
  journal = "In Proceedings of the 9th international symposium on functional and logic programming, Lecture notes in
computer science",
  pages = "64-80",
  volume = 4989,
  year = 2008,
  }

  @article{Dubois1,
  author = "V. Dubois and P.-A. Fouque and J. Stern",
  title = "Cryptanalysis of {SFLASH} with Slightly Modified Parameters",
  journal = "Eurocrypt ï¿½07, Springer",
  volume = 4515,
  year = 2007,
  pages = "264-275",
  }

@article{Dubois2,
  author = "V. Dubois and P.-A. Fouque and A. Shamir and J. Stern",
  title = "Practical cryptanalysis of {SFLASH}",
  journal = "Advances in Cryptology - CRYPTO 2007, Springer",
  volume = 4622,
  year = 2007,
  pages = "1-12",
  }
```

```
@inproceedings{2004-3306,
 author={Jintai Ding},
 title={A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation.},
 booktitle={Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key
Cryptography, Singapore, March 1-4, 2004},
 pages={305-318},
 url={http://www.iacr.org/cryptodb/archive/2004/PKC/3306/3306.pdf},
 year=2004
}



@article{Dingpmiplus,
   author = "J. Ding and J. E. Gower",
   title = "Innoculating Multivariate Schemes Against Differential Attacks",
   journal = "PKC 2006 of LNCS",
   volume = 3958,
   year = 2006,
   pages = "290-301",
}

@article{Matsu,
 author = "T. Matsumoto and H. Imai",
 title = "Public quadratic polynomial-tuples for efficient signature verification and message-encryption",
 journal = "Eurocrypt '88, Springer",
 volume = 330,
 year = 1988,
 pages = "419-545",
  }

@inproceedings{DBLP:conf/ctrsa/PatarinCG01,
 author    = {Jacques Patarin and
              Nicolas Courtois and
              Louis Goubin},
 title     = {QUARTZ, 128-Bit Long Digital Signatures},
 booktitle = {CT-RSA},
 year      = {2001},
 pages     = {282-297},
 ee        = {http://dx.doi.org/10.1007/3-540-45353-9_21},
 crossref  = {DBLP:conf/ctrsa/2001},
 bibsource = {DBLP, http://dblp.uni-trier.de}
}
@proceedings{DBLP:conf/ctrsa/2001,
 editor    = {David Naccache},
 title     = {Topics in Cryptology - CT-RSA 2001, The Cryptographer's
              Track at RSA Conference 2001, San Francisco, CA, USA, April
              8-12, 2001, Proceedings},
 booktitle = {CT-RSA},
 publisher = {Springer},
 series    = {Lecture Notes in Computer Science},
 volume    = {2020},
 year      = {2001},
 isbn      = {3-540-41898-9},
 bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{DBLP:conf/indocrypt/PetzoldtBB10,
 author    = {Albrecht Petzoldt and
              Stanislav Bulygin and
              Johannes Buchmann},
 title     = {CyclicRainbow - A Multivariate Signature Scheme with a Partially
              Cyclic Public Key},
 booktitle = {INDOCRYPT},
 year      = {2010},
 pages     = {33-48},
 ee        = {http://dx.doi.org/10.1007/978-3-642-17401-8_4},
 crossref  = {DBLP:conf/indocrypt/2010},
 bibsource = {DBLP, http://dblp.uni-trier.de}
}
@proceedings{DBLP:conf/indocrypt/2010,
 editor    = {Guang Gong and
              Kishan Chand Gupta},
 title     = {Progress in Cryptology - INDOCRYPT 2010 - 11th International
              Conference on Cryptology in India, Hyderabad, India, December
              12-15, 2010. Proceedings},
 booktitle = {INDOCRYPT},
 publisher = {Springer},
 series    = {Lecture Notes in Computer Science},
 volume    = {6498},
 year      = {2010},
 isbn      = {978-3-642-17400-1},
 ee        = {http://dx.doi.org/10.1007/978-3-642-17401-8},
 bibsource = {DBLP, http://dblp.uni-trier.de}
}

@article{Patarin1,
 author = "J. Patarin",
 title = "Cryptanalysis of the {M}atsumoto and {I}mai public key scheme of {E}urocrypt ï¿½88",
 journal = "Crypto 1995, Springer",
 volume = 963,
 year = 1995,
 pages = "248-261",
 }

@article{Patarin2,
 author = "J. Patarin and L. Goubin and N. Courtois",
 title = "C $^*_{-+}$ and {HM}: {V}ariations around two schemes of {T}.{M}atsumoto and {H}.{I}mai",
 journal = "Asiacrypt 1998, Springer",
 pages = "35-49",
 volume = 1514,
 year = 1998,
 }

@article{Patarin3,
 author = "J. Patarin",
 title = "{H}idden {Field} {E}quations ({HFE}) and {I}somorphisms of {P}olynomials: two new {F}amilies of
{A}symmetric {A}lgorithms",
 journal = "Eurocrypt '96, Springer",
 pages = "33-48",
 volume = 1070,
 year = 1996,
 }

@article{Mollin,
 author = "R. A. Mollin and C. Small",
 title = "On permutation polynomials over finite fields",
 journal = "Internat. J. Math. and Math. Sci.",
 pages = "535-543",
 volume = 10,
 year = 1987,
 }

@article{FouqueStern,
 author = "P.-A. Fouque and L. Granboulan and J. Stern",
 title = "Differential Cryptanalysis for Multivariate Schemes",
 journal = "Eurocrypt '05, Springer",
 pages = "341-353",
 volume = 3494,
 year = 2005,
 }

@article{DBLP:journals/jmc/WolfP11,
 author    = {Christopher Wolf and
              Bart Preneel},
 title     = {Equivalent keys in Multivariate Quadratic public key
              systems},
 journal   = {J. Mathematical Cryptology},
 volume    = {4},
 number    = {4},
 pages     = {375--415},
 year      = {2011},
 url       = {http://dx.doi.org/10.1515/jmc.2011.004},
 doi       = {10.1515/jmc.2011.004},
 timestamp = {Tue, 08 Jan 2013 19:28:27 +0100},
 biburl    = {http://dblp.uni-trier.de/rec/bib/journals/jmc/WolfP11},
 bibsource = {dblp computer science bibliography, http://dblp.org}
}

@misc{Wolf,
    author = {C. Wolf and B. Preneel},
    title = {Taxonomy of public key schemes based on the problem of multivariate quadratic equations},
    howpublished = {Cryptology ePrint Archive, Report 2005/077},
    year = {2005},
    note = {http://eprint.iacr.org/},
}



@misc{Smith2,
    author = {D. C. Smith-Tone},
    title = {A Reduction of Variants of the Projected {SFLASH}},
    howpublished = {preprint},
    year = {2008},
 }

 @article{Wu,
 author = {Chuan-Kun Wu and Ed Dawson},
 title = "Existence of Generalized Inverse of Linear Transformations over Finite Fields",
 journal = "Finite Fields and Their Applications",
 pages = "307-315",
 volume = 4,
 year = 1998,
 }

 @article{Dubois1,
 author = "V. Dubois and P. A. Fouque and J. Stern",
 title = "Cryptanalysis of {SFLASH} with Slightly Modified Parameters",
 journal = "Eurocrypt '07, Springer",
 volume = 4515,
 year = 2007,
 pages = "264-275",
 }

 @article{Dubois2,
 author = "V. Dubois and P.-A. Fouque and A. Shamir and J. Stern",
 title = "Practical cryptanalysis of {SFLASH}",
 journal = "Advances in Cryptology - CRYPTO 2007, Springer",
 volume = 4622,
 year = 2007,
 pages = "1-12",
 }

 @misc{Biercuk,
    author = {M. Biercuk},
    title = {Quantum Control and Complexity using Ion Crystals in a Penning Trap},
    howpublished = {From Quantum Information and Complexity to Post Quantum Information Security},
    year = {2010},
 }

 @misc{S-TYPFLASH,
    author = {M.-S. Chen and B.-Y. Yang and D. Smith-Tone},
    title = {PFLASH - Secure Asymmetric Signatures on Smart Cards},
    howpublished = {Lightweight Cryptography Workshop 2015},
    year = {2015},
        note = {http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session3-smith-tone-paper.pdf},
 }



 @article{Ding2,
    author = "J. Ding and V. Dubois and B.-Y. Yang and O. C.-H. Chen and C.-M. Cheng",
    title = "Could SFLASH be Repaired?",
    journal = "Automata, Languages and Programming",
    volume = 4450,
    year = 2009,
    pages = "691-701",
}

@article{Dingpmi,
    author = "J. Ding",
    title = "A new variant of the Matsumoto-Imai cryptosystem through perturbation",
    journal = "PKC 2004, LNCS",
    volume = 2947,
    year = 2004,
    pages = "305-318",
}

@article{Dingpmi+,
    author = "J. Ding and J. Gower",
    title = "Inoculating multivariate schemes against differential attacks",
    journal = "PKC 2006, LNCS",
    volume = 3958,
    year = 2006,
    pages = "290-301",
}

@article{Dinghfev,
    author = "J. Ding and D. Schmidt",
    title = "Cryptanalysis of HFEv and internal perturbation of HFE",
    journal = "PKC 2005, LNCS",
    volume = 3386,
    year = 2005,
    pages = "288-301",
}

@article{Dingrainbow,
    author = "J. Ding and D. Schmidt",
    title = "Rainbow, a new multivariable polynomial signature scheme",
    journal = "ACNS 2005, LNCS",
    volume = 3531,
    year = 2005,
    pages = "164-175",
}

@article{Dingholes,
    author = "J. Ding and L. Hu and X. Nie and J. Li and J. Wagner",
    title = "High order linearization equation (hole) attack on multivariate public key cryptosystems",
    journal = "PKC 2007, LNCS",
    volume = 4450,
    year = 2007,
    pages = "230-247",
}

@article{DingYang,
    author = "J. Ding and B.-Y. Yang",
    title = "Multivariate Public Key Cryptography",
    book = "Post-Quantum Cryptography",
    publisher = "Springer-Heidelberg",
    year = 2009,
    pages = "193-241",
}

@article{xl,
    author = "N. Courtois and A. Klimov and J. Patarin and A.Shamir",
    title = "Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations",
    journal = "EUROCRYPT 2000, LNCS",
    volume = 1807,
    year = 2000,
    pages = "392-407",
}

@article{xsl,
    author = "N. Courtois and J. Pieprzyk",
    title = "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations",
    journal = "ASIACRYPT 2002, LNCS",
    volume = 2501,
    year = 2002,
    pages = "267-287",
}

@article{mxl,
    author = "J. Ding and J. Buchmann and M.S.E. Mohamed and W.S.A.E. Mohamed and R.P. Weinmann",
    title = "Mutant XL",
    journal = "SCC 2008, LMIB",
    year = 2008,
    pages = "16-22",
}

@article{mxl2,
    author = "M. S. E. Mohamed and W. S. A. E. Mohamed and J. Ding and J. Buchmann",
    title = "MXL2 : Solving Polynomial Equations over GF(2) Using an Improved Mutant Strategy",
    journal = "PQCRYPTO 2008, LNCS",
    volume = 5299,
    year = 2008,
    pages = "205-215",
}

@inproceedings{DBLP:conf/icisc/MohamedCDBB09,
  author    = {Mohamed Saied Emam Mohamed and
               Daniel Cabarcas and
               Jintai Ding and
               Johannes Buchmann and
               Stanislav Bulygin},
  title     = {MXL$_{\mbox{3}}$: An Efficient Algorithm for Computing Gr{\"o}bner
               Bases of Zero-Dimensional Ideals},
  booktitle = {ICISC},
  year      = {2009},
  pages     = {87-100},
  ee        = {http://dx.doi.org/10.1007/978-3-642-14423-3_7},
  crossref  = {DBLP:conf/icisc/2009},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}
@proceedings{DBLP:conf/icisc/2009,
  editor    = {Donghoon Lee and
```

```
            Seokhie Hong},
  title     = {Information, Security and Cryptology - ICISC 2009, 12th
            International Conference, Seoul, Korea, December 2-4, 2009,
            Revised Selected Papers},
  booktitle = {ICISC},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {5984},
  year      = {2010},
  isbn      = {978-3-642-14422-6},
  ee        = {http://dx.doi.org/10.1007/978-3-642-14423-3},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@article{mxl3,
   author = "J. Buchmann and J. Ding and M. S. E. Mohamed and W. S. A. E. Mohamed and D. Cabarcas",
   title = "MutantXL: An Effcient Algorithm for Solving Multivariate Polynomial Equations",
   journal = "Presentation: Special Session on the Algebraic Aspects of Cryptology, JMM 2010",
   volume = "1056-14-477",
   year = 2010,
   note = {http://www.ams.org/amsmtgs/2124_abstracts/1056-14-477.pdf},
}

@misc{Gotaishieprint,
   author = {M. Gotaishi and S. Tsujii},
   title = {Hidden Pair of Bijection Signature Scheme},
   howpublished = {Cryptology ePrint Archive, Report 2011/353},
   year = {2011},
   note = {http://eprint.iacr.org/},
}

@article{Gotaishipqcrump,
   author = "M. Gotaishi",
   title = "Hidden Pair of Bijection Signature ({P}art {II})",
   journal = "Presentation: Rump Session PQCRYPTO 2011",
   year = 2011,
   note = {http://troll.iis.sinica.edu.tw/pqc11/recent.shtml},
}

@article{abcpres,
   author = "A. Diene and C. Tao and J. Ding",
   title = "Simple Matrix Scheme for Encryption (ABC)",
   journal = "Presentation: PQCRYPTO 2013",
   year = 2013,
   note = {http://pqcrypto2013.xlim.fr/slides/05-06-2013/Diene.pdf},
}

@article{ABCnewer,
   author = "C. Tao and A. Diene and S. Tang and J. Ding",
   title = "Improvement of Simple Matrix Scheme for Encryption",
   journal = "Personally Communicated",
   year = 2013,
   note = "Corresponding Author: Ding, J.",
}
```

```
@inproceedings{DBLP:conf/pqcrypto/DingPW14,
  author    = {Jintai Ding and
               Albrecht Petzoldt and
               Lih{-}chung Wang},
  title     = {The Cubic Simple Matrix Encryption Scheme},
  booktitle = {Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014,
               Waterloo, ON, Canada, October 1-3, 2014. Proceedings},
  pages     = {76--87},
  year      = {2014},
  crossref  = {DBLP:conf/pqcrypto/2014},
  url       = {http://dx.doi.org/10.1007/978-3-319-11659-4_5},
  doi       = {10.1007/978-3-319-11659-4_5},
  timestamp = {Thu, 25 Sep 2014 13:25:45 +0200},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pqcrypto/DingPW14},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@inproceedings{DBLP:conf/asiacrypt/PetzoldtCYTD15,
  author    = {Albrecht Petzoldt and
               Ming{-}Shing Chen and
               Bo{-}Yin Yang and
               Chengdong Tao and
               Jintai Ding},
  title     = {Design Principles for HFEv- Based Multivariate Signature Schemes},
  booktitle = {Advances in Cryptology - {ASIACRYPT} 2015 - 21st International Conference
               on the Theory and Application of Cryptology and Information Security,
               Auckland, New Zealand, November 29 - December 3, 2015, Proceedings,
               Part {I}},
  pages     = {311--334},
  year      = {2015},
  crossref  = {DBLP:conf/asiacrypt/2015-1},
  url       = {http://dx.doi.org/10.1007/978-3-662-48797-6_14},
  doi       = {10.1007/978-3-662-48797-6_14},
  timestamp = {Fri, 27 Nov 2015 10:50:18 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/asiacrypt/PetzoldtCYTD15},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}
@proceedings{DBLP:conf/asiacrypt/2015-1,
  editor    = {Tetsu Iwata and
               Jung Hee Cheon},
  title     = {Advances in Cryptology - {ASIACRYPT} 2015 - 21st International Conference
               on the Theory and Application of Cryptology and Information Security,
               Auckland, New Zealand, November 29 - December 3, 2015, Proceedings,
               Part {I}},
  series    = {Lecture Notes in Computer Science},
  volume    = {9452},
  publisher = {Springer},
  year      = {2015},
  url       = {http://dx.doi.org/10.1007/978-3-662-48797-6},
  doi       = {10.1007/978-3-662-48797-6},
  isbn      = {978-3-662-48796-9},
  timestamp = {Fri, 27 Nov 2015 10:47:32 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/asiacrypt/2015-1},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@inproceedings{DBLP:conf/pqcrypto/DanielsS14,
  author    = {Taylor Daniels and
               Daniel Smith{-}Tone},
  title     = {Differential Properties of the {HFE} Cryptosystem},
  booktitle = {Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014,
               Waterloo, ON, Canada, October 1-3, 2014. Proceedings},
  pages     = {59--75},
  year      = {2014},
  crossref  = {DBLP:conf/pqcrypto/2014},
  url       = {http://dx.doi.org/10.1007/978-3-319-11659-4_4},
  doi       = {10.1007/978-3-319-11659-4_4},
  timestamp = {Thu, 25 Sep 2014 13:25:45 +0200},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pqcrypto/DanielsS14},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@inproceedings{DBLP:conf/pkc/FaugereGPST15,
  author    = {Jean{-}Charles Faug{\`{e}}re and
               Danilo Gligoroski and
               Ludovic Perret and
               Simona Samardjiska and
               Enrico Thomae},
  title     = {A Polynomial-Time Key-Recovery Attack on {MQQ} Cryptosystems},
  booktitle = {Public-Key Cryptography - {PKC} 2015 - 18th {IACR} International Conference
               on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD,
               USA, March 30 - April 1, 2015, Proceedings},
  pages     = {150--174},
  year      = {2015},
  crossref  = {DBLP:conf/pkc/2015},
  url       = {http://dx.doi.org/10.1007/978-3-662-46447-2_7},
  doi       = {10.1007/978-3-662-46447-2_7},
  timestamp = {Tue, 17 Mar 2015 14:37:50 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pkc/FaugereGPST15},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}
@proceedings{DBLP:conf/pkc/2015,
  editor    = {Jonathan Katz},
  title     = {Public-Key Cryptography - {PKC} 2015 - 18th {IACR} International Conference
               on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD,
               USA, March 30 - April 1, 2015, Proceedings},
  series    = {Lecture Notes in Computer Science},
  volume    = {9020},
  publisher = {Springer},
  year      = {2015},
  url       = {http://dx.doi.org/10.1007/978-3-662-46447-2},
  doi       = {10.1007/978-3-662-46447-2},
  isbn      = {978-3-662-46446-5},
  timestamp = {Tue, 17 Mar 2015 14:34:20 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pkc/2015},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}
```

```
@inproceedings{DBLP:conf/pqcrypto/MoodyPS14,
  author    = {Dustin Moody and
               Ray A. Perlner and
               Daniel Smith{-}Tone},
  title     = {An Asymptotically Optimal Structural Attack on the {ABC} Multivariate
               Encryption Scheme},
  booktitle = {Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014,
               Waterloo, ON, Canada, October 1-3, 2014. Proceedings},
  pages     = {180--196},
  year      = {2014},
  crossref  = {DBLP:conf/pqcrypto/2014},
  url       = {http://dx.doi.org/10.1007/978-3-319-11659-4_11},
  doi       = {10.1007/978-3-319-11659-4_11},
  timestamp = {Thu, 25 Sep 2014 13:25:45 +0200},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pqcrypto/MoodyPS14},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@inproceedings{DBLP:conf/pqcrypto/PerlnerS16,
  author    = {Ray A. Perlner and
               Daniel Smith{-}Tone},
  title     = {Security Analysis and Key Modification for {ZHFE}},
  booktitle = {Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016,
               Fukuoka, Japan, February 24-26, 2016, Proceedings},
  pages     = {197--212},
  year      = {2016},
  crossref  = {DBLP:conf/pqcrypto/2016},
  url       = {http://dx.doi.org/10.1007/978-3-319-29360-8_13},
  doi       = {10.1007/978-3-319-29360-8_13},
  timestamp = {Wed, 10 Feb 2016 14:52:29 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pqcrypto/PerlnerS16},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@proceedings{DBLP:conf/pqcrypto/2016,
  editor    = {Tsuyoshi Takagi},
  title     = {Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016,
               Fukuoka, Japan, February 24-26, 2016, Proceedings},
  series    = {Lecture Notes in Computer Science},
  volume    = {9606},
  publisher = {Springer},
  year      = {2016},
  url       = {http://dx.doi.org/10.1007/978-3-319-29360-8},
  doi       = {10.1007/978-3-319-29360-8},
  isbn      = {978-3-319-29359-2},
  timestamp = {Wed, 10 Feb 2016 14:02:15 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pqcrypto/2016},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@inproceedings{DBLP:conf/pqcrypto/PorrasBD14,
  author    = {Jaiberth Porras and
               John Baena and
```

```
             Jintai Ding},
  title     = {ZHFE, a New Multivariate Public Key Encryption Scheme},
  booktitle = {Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014,
             Waterloo, ON, Canada, October 1-3, 2014. Proceedings},
  pages     = {229--245},
  year      = {2014},
  crossref  = {DBLP:conf/pqcrypto/2014},
  url       = {http://dx.doi.org/10.1007/978-3-319-11659-4_14},
  doi       = {10.1007/978-3-319-11659-4_14},
  timestamp = {Thu, 25 Sep 2014 13:25:45 +0200},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pqcrypto/PorrasBD14},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@proceedings{DBLP:conf/pqcrypto/2014,
  editor    = {Michele Mosca},
  title     = {Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014,
             Waterloo, ON, Canada, October 1-3, 2014. Proceedings},
  series    = {Lecture Notes in Computer Science},
  volume    = {8772},
  publisher = {Springer},
  year      = {2014},
  url       = {http://dx.doi.org/10.1007/978-3-319-11659-4},
  doi       = {10.1007/978-3-319-11659-4},
  isbn      = {978-3-319-11658-7},
  timestamp = {Thu, 25 Sep 2014 13:19:37 +0200},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/pqcrypto/2014},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}


@inproceedings{DBLP:conf/pqcrypto/PerlnerS13,
  author    = {Ray A. Perlner and
             Daniel Smith-Tone},
  title     = {A Classification of Differential Invariants for Multivariate
             Post-quantum Cryptosystems},
  booktitle = {PQCrypto},
  year      = {2013},
  pages     = {165-173},
  ee        = {http://dx.doi.org/10.1007/978-3-642-38616-9_11},
  crossref  = {DBLP:conf/pqcrypto/2013},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{bardet2004complexity,
  title={On the complexity of Gr{\"o}bner basis computation of semi-regular overdetermined algebraic equations},
  author={Bardet, Magali and Faugere, Jean-Charles and Salvy, Bruno},
  booktitle = {Proceedings of the International Conference on Polynomial System Solving},
  year = {2004}
}

@inproceedings{DBLP:conf/pqcrypto/TaoDTD13,
  author    = {Chengdong Tao and
             Adama Diene and
```

```
              Shaohua Tang and
              Jintai Ding},
  title     = {Simple Matrix Scheme for Encryption},
  booktitle = {PQCrypto},
  year      = {2013},
  pages     = {231-242},
  ee        = {http://dx.doi.org/10.1007/978-3-642-38616-9_16},
  crossref  = {DBLP:conf/pqcrypto/2013},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{DBLP:conf/pqcrypto/TsujiiGTF10,
  author    = {Shigeo Tsujii and
              Masahito Gotaishi and
              Kohtaro Tadaki and
              Ryou Fujita},
  title     = {Proposal of a Signature Scheme Based on STS Trapdoor},
  booktitle = {PQCrypto},
  year      = {2010},
  pages     = {201-217},
  ee        = {http://dx.doi.org/10.1007/978-3-642-12929-2_15},
  crossref  = {DBLP:conf/pqcrypto/2010},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@article{lic,
    author = "J. Ding and C. Wolf and B.-Y. Yang",
    title = "l-invertible cycles for multivariate quadratic public key cryptography",
    journal = "PKC 2007 of LNCS",
    volume = 4450,
    year = 2007,
    pages = "266-281",
}

@article{licbreak,
    author = "P. A. Fouque and G. Macario-Rat and L. Perret and J. Stern",
    title = "Total break of the    $\ell$IC- signature scheme",
    journal = "PKC 2008, LNCS",
    volume = "4939",
    year = 2008,
    pages = "1-17",
}

@article{Faugere,
    author = "J. C. Faugere",
    title = "A new efficient algorithm for computing Grobner bases (F4)",
    journal = "Journal of Pure and Applied Algebra",
    volume = "139",
    year = 1999,
    pages = "61-88",
}

@article{faugere2,
    author = "J. C. Faugere",
    title = "A new efficient algorithm for computing Grobner bases without reduction to zero (F5)",
    journal = "ISSAC 2002, ACM Press",
    year = 2002,
    pages = "75-83",
}

@article{fouque,
    author = "P.-A. Fouque and L. Granboulan and J. Stern",
    title = "Differential Cryptanalysis for Multivariate Schemes ",
    journal = "EUROCRYPT 2005, LNCS",
    volume = 3494,
    year = 2005,
    pages = "341-353",
}

@article{faugere3,
    author = "J. C. Faugere",
    title = "Algebraic cryptanalysis of Hidden Field Equations (HFE) using Grobner bases",
    journal = "CRYPTO 2003, LNCS",
    volume = "2729",
    year = 2003,
    pages = "44-60",
}

@article{moh,
    author = "T. Moh",
    title = "A public key system with signature and master key function",
    journal = "Communications in Algebra",
    volume = "27(5)",
    year = 1999,
    pages = "2207-2222",
}

@article{Shor,
  author = "P. W. Shor",
  title = "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer",
  journal = "SIAM J. Sci. Stat. Comp.",
  volume = "26, 1484",
  year = 1997,
  }

@article{Grover:1996rk,
     author         = "Grover, Lov K.",
     title          = "{A Fast quantum mechanical algorithm for database
                       search}",
     year           = "1996",
     note           = "Proceedings STOC 1996, 212-219",
     eprint         = "quant-ph/9605043",
     archivePrefix  = "arXiv",
     primaryClass   = "quant-ph",
     SLACcitation   = "%%CITATION = QUANT-PH/9605043;%%",
}
```

```
@inproceedings{DBLP:conf/pqcrypto/ThomaeW11,
  author    = {Enrico Thomae and
               Christopher Wolf},
  title     = {Roots of Square: Cryptanalysis of Double-Layer Square and
               Square+},
  booktitle = {PQCrypto},
  year      = {2011},
  pages     = {83-97},
  ee        = {http://dx.doi.org/10.1007/978-3-642-25405-5_6},
  crossref  = {DBLP:conf/pqcrypto/2011},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@article{Berlekamp,
    author = {Berlekamp, E. R.},
    title = {Factoring Polynomials Over Large Finite Fields},
    journal = {Mathematics of Computation},
    volume = {24},
    number = {111},
    pages = {pp. 713-735},
    year = {1970},
    publisher = {American Mathematical Society}
}

@inproceedings{DBLP:conf/pqcrypto/Smith-Tone11,
  author    = {Daniel Smith-Tone},
  title     = {On the Differential Security of Multivariate Public Key
               Cryptosystems},
  booktitle = {PQCrypto},
  year      = {2011},
  pages     = {130-142},
  ee        = {http://dx.doi.org/10.1007/978-3-642-25405-5_9},
  crossref  = {DBLP:conf/pqcrypto/2011},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@proceedings{DBLP:conf/pqcrypto/2011,
  editor    = {Bo-Yin Yang},
  title     = {Post-Quantum Cryptography - 4th International Workshop,
               PQCrypto 2011, Taipei, Taiwan, November 29 - December 2,
               2011. Proceedings},
  booktitle = {PQCrypto},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {7071},
  year      = {2011},
  isbn      = {978-3-642-25404-8},
  ee        = {http://dx.doi.org/10.1007/978-3-642-25405-5},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{DBLP:conf/pqcrypto/Smith-Tone10,
  author    = {Daniel Smith-Tone},
  title     = {Properties of the Discrete Differential with Cryptographic
```

```
             Applications},
  booktitle = {PQCrypto},
  year      = {2010},
  pages     = {1-12},
  ee        = {http://dx.doi.org/10.1007/978-3-642-12929-2_1},
  crossref  = {DBLP:conf/pqcrypto/2010},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@proceedings{DBLP:conf/pqcrypto/2010,
  editor    = {Nicolas Sendrier},
  title     = {Post-Quantum Cryptography, Third International Workshop,
             PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings},
  booktitle = {PQCrypto},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {6061},
  year      = {2010},
  isbn      = {978-3-642-12928-5},
  ee        = {http://dx.doi.org/10.1007/978-3-642-12929-2},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{ESTSPQCRYPTO10,
  author    = {Shigeo Tsujii and
             Masahito Gotaishi and
             Kohtaro Tadaki and
             Ryou Fujita},
  title     = {Proposal of a Signature Scheme Based on STS Trapdoor},
  booktitle = {PQCrypto},
  year      = {2010},
  pages     = {201-217},
  ee        = {http://dx.doi.org/10.1007/978-3-642-12929-2_15},
  crossref  = {DBLP:conf/pqcrypto/2010},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{conf/sac/MoodyPS16,
author={Dustin Moody and Ray A. Perlner and Daniel Smith{-}Tone},
title={Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme},
booktitle={Selected Areas in Cryptography -- SAC 2016: 23rd International Conference, Revised Selected Papers},
year={2017},
publisher={LNCS, Springer}
}

  @article{IM,
  author = "T. Matsumoto and H. Imai",
  title = "Public quadratic polynomial-tuples for efficient signature verification and message-encryption",
  journal = "Eurocrypt '88, Springer",
  volume = 330,
  year = 1988,
  pages = "419-545",
  }
```

```
 @article{Pat,
 author = "J. Patarin",
 title = "Cryptanalysis of the {M}atsumoto and {I}mai public key scheme of {E}urocrypt '88",
 journal = "Crypto 1995, Springer",
 volume = 963,
 year = 1995,
 pages = "248-261",
 }

 @article{Pat2,
 author = "J. Patarin and L. Goubin and N. Courtois",
 title = "C $^*_{-+}$ and {HM}: {V}ariations around two schemes of {T}.{M}atsumoto and {H}.{I}mai",
 journal = "Asiacrypt 1998, Springer",
 pages = "35-49",
 volume = 1514,
 year = 1998,
 }

 @article{sflash,
 author = "J. Patarin and N. Courtois and L. Goubin ",
 title = "FLASH, a Fast Multivariate Signature Algorithm",
 journal = "CT-RSA 2001, LNCS",
 pages = "297-307",
 volume = 2020,
 year = 2001,
 }



@article{Smith-Tone,
 author = "D. C. Smith-Tone",
 title = "Properties of the Discrete Differential with Cryptographic Applications",
 journal = "PQCRYPTO 2010, LNCS",
 pages = "1-12",
 volume = 6061,
 year = 2010,
 }

@misc{Smith-ToneGeometricFoundations,
  author = {D. Smith-Tone},
  title = {Discrete Geometric Foundations for Multivariate Public Key Cryptography},
  howpublished = {In Submission},
}

@misc{Smith-Tone2,
  author = {D. C. Smith-Tone},
  title = {Extensible Distillation},
  howpublished = {Preprint to appear: http://eprint.iacr.org/},
}

 @article{Crystal,
 author = "J. Baena and C. Clough and J. Ding",
 title = "Square-vinegar signature scheme",
 journal = "PQCRYPTO 2008, LNCS",
  pages = "17-30",
  volume = 5299,
  year = 2008,
  }

  @article{crystal2,
  author = "C. Clough and J. Baena and J. Ding and B.-Y. Yang and M.-S. Chen",
  title = "Square, a new multivariate encryption scheme",
  journal = "CT-RSA 2009, LNCS",
  pages = "252-264",
  volume = 5473,
  year = 2009,
  }

  @article{newcrystal,
  author = "Anonymous",
  title = "Secure Variants of Square",
  journal = "Private Communication",
  year = 2010,
  }

@article{newQuartz,
  author = "Anonymous",
  title = "New Parameters for QUARTZ",
  journal = "Private Communication",
  year = 2013,
  }

@inproceedings{DBLP:conf/asiacrypt/DuboisG10,
  author    = {Vivien Dubois and
               Nicolas Gama},
  title     = {The Degree of Regularity of {HFE} Systems},
  booktitle = {Advances in Cryptology - {ASIACRYPT} 2010 - 16th International Conference
               on the Theory and Application of Cryptology and Information Security,
               Singapore, December 5-9, 2010. Proceedings},
  pages     = {557--576},
  year      = {2010},
  crossref  = {DBLP:conf/asiacrypt/2010},
  url       = {http://dx.doi.org/10.1007/978-3-642-17373-8_32},
  doi       = {10.1007/978-3-642-17373-8_32},
  timestamp = {Wed, 08 Dec 2010 10:32:54 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/asiacrypt/DuboisG10},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}
@proceedings{DBLP:conf/asiacrypt/2010,
  editor    = {Masayuki Abe},
  title     = {Advances in Cryptology - {ASIACRYPT} 2010 - 16th International Conference
               on the Theory and Application of Cryptology and Information Security,
               Singapore, December 5-9, 2010. Proceedings},
  series    = {Lecture Notes in Computer Science},
  volume    = {6477},
  publisher = {Springer},
  year      = {2010},
  url       = {http://dx.doi.org/10.1007/978-3-642-17373-8},
  doi       = {10.1007/978-3-642-17373-8},
  isbn      = {978-3-642-17372-1},
  timestamp = {Wed, 08 Dec 2010 10:25:48 +0100},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/asiacrypt/2010},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@inproceedings{DBLP:conf/crypto/DingH11,
  author    = {Jintai Ding and
               Timothy J. Hodges},
  title     = {Inverting {HFE} Systems Is Quasi-Polynomial for All Fields},
  booktitle = {Advances in Cryptology - {CRYPTO} 2011 - 31st Annual Cryptology Conference,
               Santa Barbara, CA, USA, August 14-18, 2011. Proceedings},
  pages     = {724--742},
  year      = {2011},
  crossref  = {DBLP:conf/crypto/2011},
  url       = {http://dx.doi.org/10.1007/978-3-642-22792-9_41},
  doi       = {10.1007/978-3-642-22792-9_41},
  timestamp = {Mon, 15 Aug 2011 21:29:40 +0200},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/crypto/DingH11},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}
@proceedings{DBLP:conf/crypto/2011,
  editor    = {Phillip Rogaway},
  title     = {Advances in Cryptology - {CRYPTO} 2011 - 31st Annual Cryptology Conference,
               Santa Barbara, CA, USA, August 14-18, 2011. Proceedings},
  series    = {Lecture Notes in Computer Science},
  volume    = {6841},
  publisher = {Springer},
  year      = {2011},
  url       = {http://dx.doi.org/10.1007/978-3-642-22792-9},
  doi       = {10.1007/978-3-642-22792-9},
  isbn      = {978-3-642-22791-2},
  timestamp = {Mon, 15 Aug 2011 21:26:36 +0200},
  biburl    = {http://dblp.uni-trier.de/rec/bib/conf/crypto/2011},
  bibsource = {dblp computer science bibliography, http://dblp.org}
}

@article{DBLP:journals/iacr/DingK11,
  author    = {Jintai Ding and
               Thorsten Kleinjung},
  title     = {Degree of regularity for {HFE} minus ({HFE-})},
  journal   = {J. Math-for-Ind.},
  volume    = {4B},
  pages     = {97-104},
  year      = {2012},
  url       = {http://j-mi.org/articles/view/272}
}

@inproceedings{DBLP:conf/pqcrypto/DingY13,
  author    = {Jintai Ding and
               Bo-Yin Yang},
  title     = {Degree of Regularity for HFEv and HFEv-},
  booktitle = {PQCrypto},
  year      = {2013},
  pages     = {52-66},
  ee        = {http://dx.doi.org/10.1007/978-3-642-38616-9_4},
  crossref  = {DBLP:conf/pqcrypto/2013},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}
@proceedings{DBLP:conf/pqcrypto/2013,
  editor    = {Philippe Gaborit},
  title     = {Post-Quantum Cryptography - 5th International Workshop,
               PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings},
  booktitle = {PQCrypto},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {7932},
  year      = {2013},
  isbn      = {978-3-642-38615-2},
  ee        = {http://dx.doi.org/10.1007/978-3-642-38616-9},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@inproceedings{DBLP:conf/asiacrypt/GoubinC00,
  author    = {Louis Goubin and
               Nicolas Courtois},
  title     = {Cryptanalysis of the TTM Cryptosystem},
  booktitle = {ASIACRYPT},
  year      = {2000},
  pages     = {44-57},
  ee        = {http://dx.doi.org/10.1007/3-540-44448-3_4},
  crossref  = {DBLP:conf/asiacrypt/2000},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}
@proceedings{DBLP:conf/asiacrypt/2000,
  editor    = {Tatsuaki Okamoto},
  title     = {Advances in Cryptology - ASIACRYPT 2000, 6th International
               Conference on the Theory and Application of Cryptology and
               Information Security, Kyoto, Japan, December 3-7, 2000,
               Proceedings},
  booktitle = {ASIACRYPT},
  publisher = {Springer},
  series    = {Lecture Notes in Computer Science},
  volume    = {1976},
  year      = {2000},
  isbn      = {3-540-41404-5},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}

@article{billet,
author = "O. Billet and G. Macario-Rat",
title = "Cryptanalysis of the Square Cryptosystems",
journal = "ASIACRYPT 2009, LNCS",
pages = "451-486",
volume = 5912,
year = 2009,
}
```

```
 @article{NESSIE,
 author = "NESSIE",
 title = "New European Schemes for Signatures, Integrity, and Encryption",
 journal = "Information Society Technologies programme of the European commission",
 volume = "IST-1999-12324",
 note = {http://www.cryptonessie.org/},
 }

 @article{cryptuov,
 author = "A. Braeken and C. Wolf and B. Preneel ",
 title = "A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes",
 journal = "CT-RSA 2005, LNCS",
 pages = "29-43",
 volume = 3376,
 year = 2005,
 }

 @article{ov,
 author = "J. Patarin",
 title = "The Oil and Vinegar Algorithm for Signatures",
 journal = "Presented at the Dagsthul Workshop on Cryptography",
 year = 1997,
 }

 @article{breakov,
 author = "A. Shamir and A. Kipnis",
 title = "Cryptanalysis of the Oil \& Vinegar Signature Scheme",
 journal = "CRYPTO 1998. LNCS",
 volume = 1462,
 year = 1998,
 pages = "257-266",
 }

 @article{uov,
 author = "A. Kipnis and J. Patarin and L. Goubin",
 title = "Unbalanced Oil and Vinegar Signature Schemes",
 journal = "EUROCRYPT 1999. LNCS",
 volume = 1592,
 year = 1999,
 pages = "206-222",
 }

 @article{boyin,
 author = "A. I.-T. Chen and M.-S. Chen and T.-R. Chen and C.-M. Cheng and J. Ding and E. L.-H. Kuo and F. Y.-S. Lee and B.-Y. Yang",
 title = "SSE implementation of multivariate PKCs on modern x86 CPUs",
 journal = "CHES 2009, LNCS, Springer, IACR",
 volume = 5747,
 year = 2009,
 pages = "33-48",
 }

@article{boyin2,
author = "A. I.-T. Chen and C.-H. O. Chen and M.-S. Chen and C.-M. Cheng and B.-Y. Yang",
title = "Practical-Sized Instances of Multivariate PKCs: Rainbow, TTS, and $\ell$IC-derivatives",
journal = "Post-Quantum Crypto, LNCS",
volume = 5299,
year = 2008,
pages = "95-106",
}

@article{boyin3,
author = "B.-Y. Yang and C.-M. Cheng and B.-R. Chen and J.-M. Chen",
title = "Implementing Minimized Multivariate Public-Key Cryptosystems on Low-Resource Embedded Systems",
journal = "3rd Security of Pervasive Computing Conference, LNCS",
volume = 3934,
year = 2006,
pages = "73-88",
}

@article{boyin4,
author = "B.-Y. Yang and J.-M. Chen and Y.-H. Chen",
title = "TTS: High-Speed Signatures on a Low-Cost Smart Card",
journal = "Proc. 2004 Workshop on Cryptographic Hardware and Embedded Systems, LNCS",
volume = 3156,
year = 2004,
pages = "371-385",
}

@article{boyin5,
author = "J.-M. Chen and B.-Y. Yang",
title = "A More Secure and Efficacious TTS Signature Scheme",
journal = "Proc. 6th Intï¿½l Conference on Info. Sec. \& Cryptology, LNCS",
volume = 2971,
year = 2003,
pages = "320-338",
}

@article{boyin6,
author = "J.-M. Chen and B.-Y. Yang and B.-Y. Peng",
title = "Tame Transformation Signatures and Topsy-Turvy Hashes",
journal = "IWAP",
year = 2002,
pages = "93-100",
}
```