From:	Daniel Smith
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 <dcs.xmr@gmail.com>
> **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

```
@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 �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",
  }


@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 �88",
  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 Int�l 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",
 }
```