Universiteit
Leiden
The Netherlands

Algorithmic techniques in algebraic cryptanalysis and their applications

Makarim, R.H.

Citation
Makarim, R. H. (2026, May 27). *Algorithmic techniques in algebraic cryptanalysis and their applications*. Retrieved from https://hdl.handle.net/1887/4304336

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/4304336

Note: To cite this publication please use the final published version (if applicable).

Algorithmic Techniques in Algebraic Cryptanalysis and their Applications

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr. S. de Rijcke,
volgens besluit van het college voor promoties
te verdedigen op woensdag 27 mei 2026
klokke 14:30 uur

door

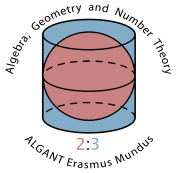
Rusydi Hasan Makarim
geboren te Cilacap, Indonesië
in 1989

Promotor:
Prof.dr. R. Cramer (CWI Amsterdam & Universiteit Leiden)

Co-promotor:
Dr.ir. M. Stevens (CWI Amsterdam)

Promotiecommissie:
Prof.dr.ir. G.L.A. Derks
Prof.dr. P. Stevenhagen
Prof.dr. C. Cid (Simula UiB, Norway & OIST, Japan)
Prof.dr. A. May (Ruhr-University Bochum, Germany)
Dr. S. Samardjiska (Radboud Universiteit, Nijmegen)

The research was carried out in the Cryptology Group at Centrum Wiskunde & Informatica (CWI) Amsterdam. The PhD position was largely funded by the ALGANT-DOC Erasmus-Mundus program and partially funded by the ERC Advanced Grant 740972 (ALGSTRONGCRYPTO).



Algorithmic Techniques in Algebraic Cryptanalysis and their Applications

Rusydi H. Makarim

Contents

I Introduction and Overview of the Results 3

1 Cryptography and Cryptanalysis 4
1.1 Cryptography 4
1.2 Cryptanalysis 7
1.3 Contributions 10

II Technical Preliminaries 23

2 Multivariate Quadratic (MQ) Problems in Cryptology 24
2.1 The Intractability of the MQ Problem 25
2.2 Multivariate Public-Key Cryptography 29
2.3 Algebraic Cryptanalysis of Symmetric-Key Cryptography 30
2.4 Algebraic Cryptanalysis of Post-Quantum Cryptography 36
2.5 Solving Systems of Polynomials in Algebraic Cryptanalysis . . . 37

3 Theory of Gröbner Bases 48
3.1 Notations and Preliminaries 48
3.2 Monomial Orderings 51
3.3 Polynomial Reduction 53
3.4 Gröbner Bases 56
3.5 Applications 58

4 Gröbner Bases Algorithms 64
4.1 Buchberger Algorithm 65
4.2 Faugère's F_4 Algorithm 71
4.3 Extended Linearization (XL) Algorithm 78

III Contributions and Main Results 82

5 M4GB: An Efficient Gröbner Bases Algorithm 83
5.1 Revisiting the Reduction Step of the F_4 Algorithm 85
5.2 M4GB Reduction 87
5.3 M4GB Algorithm 89
5.4 Comparison with the F_4 Algorithm 94
5.5 Correctness 95
5.6 Efficient Implementation 96
5.7 Benchmark and Performance Comparison 97

6 Solving MQ Challenges 103
6.1 Overview of the MQ Challenge 104
6.2 Related Work 105
6.3 Overview of Hybrid Approach 107
6.4 Solving Type V and VI of the MQ Challenge 111
6.5 Cost Estimation for Other Parameters 115

7 Solving Binary Puzzles using Gröbner Bases Algorithms 118
7.1 Overview of Binary Puzzles 119
7.2 Constraint Satisfaction Problem 119
7.3 Related Work 120
7.4 Notations and Preliminaries 120
7.5 Polynomial Equations over $\mathbb{F}_2$ 122
7.6 Polynomial Equations over $\mathbb{Q}$ (or $\mathbb{Z}$) 125
7.7 Solving Binary Puzzles using Gröbner Bases 126
7.8 Scope and Limitations 128

8 Ideals of Vectorial Boolean Functions 131
8.1 Notations and Preliminaries 132
8.2 Multivariate Ideals and Linear Property 135
8.3 Multivariate Ideals and Differential Property 138
8.4 Multivariate Ideals and Autocorrelation 141

A Solutions to Type V and VI MQ Challenge 147

B CPU Time and Memory usage of M4GB 148

References 150

Notations 173

Index 175

List of Algorithms 177

List of Figures 178

List of Tables 180

English Summary 182

Nederlandse Samenvatting 184

Acknowledgments 186

Curriculum Vitae 187