

# Table of Contents

|          |                                                    |           |
|----------|----------------------------------------------------|-----------|
| <b>1</b> | <b>Overview</b>                                    | <b>1</b>  |
| 1.1      | Background.....                                    | 1         |
| 1.2      | Public-Key Cryptography and RSA.....               | 2         |
| 1.3      | Research Goals.....                                | 3         |
| 1.4      | Prime Generation .....                             | 3         |
| 1.5      | The Competing Servers Array .....                  | 5         |
| 1.6      | Special-Purpose Factoring .....                    | 6         |
| 1.7      | RSA Enciphering .....                              | 7         |
| 1.8      | The Synchronized Servers Pipeline .....            | 7         |
| 1.9      | Generating Deterministically Certified Primes..... | 8         |
| 1.10     | Conclusions.....                                   | 8         |
| <b>2</b> | <b>The RSA Public-Key Cryptosystem</b>             | <b>11</b> |
| 2.1      | Public-Key Cryptography .....                      | 11        |
| 2.2      | Overview of the RSA Cryptosystem.....              | 11        |
| 2.3      | How the RSA Cryptosystem Works .....               | 12        |
| 2.4      | Authenticity.....                                  | 15        |
| <b>3</b> | <b>Notation for Distributed Algorithms</b>         | <b>17</b> |
| 3.1      | Introduction.....                                  | 17        |
| 3.2      | Process Creation and Termination.....              | 17        |
| 3.3      | Process Communication.....                         | 18        |
| 3.4      | Polling .....                                      | 19        |
| <b>4</b> | <b>The Competing Servers Array</b>                 | <b>21</b> |
| 4.1      | Introduction.....                                  | 21        |
| 4.2      | Searches Suitable for Competing Servers.....       | 21        |
| 4.3      | Overview of the Competing Servers Array .....      | 22        |
| 4.4      | Implementing Competing Servers .....               | 24        |
| 4.5      | Search Completion and Process Termination .....    | 32        |
| 4.6      | Timing Out.....                                    | 32        |
| 4.7      | Determinism versus Non-Determinism .....           | 33        |
| 4.8      | Performance .....                                  | 34        |

|          |                                                               |           |
|----------|---------------------------------------------------------------|-----------|
| <b>5</b> | <b>A Distributed Algorithm to Find Safe RSA Keys</b>          | <b>37</b> |
| 5.1      | Introduction.....                                             | 37        |
| 5.2      | Considerations for RSA Keys.....                              | 37        |
| 5.3      | Characteristics of Strong Primes.....                         | 38        |
| 5.4      | Constructing Strong Primes.....                               | 40        |
| 5.5      | Certifying Primes.....                                        | 43        |
| 5.6      | Generating Primes.....                                        | 44        |
| 5.7      | Parallel Algorithm.....                                       | 46        |
| 5.8      | Parallel Candidate Generation.....                            | 47        |
| 5.9      | Parallel Prime Certification.....                             | 48        |
| 5.10     | Combining Generation and Certification.....                   | 50        |
| 5.11     | Generating Strong Primes.....                                 | 52        |
| 5.12     | Implementation Concerns.....                                  | 56        |
| 5.13     | Performance Analysis.....                                     | 57        |
| <b>6</b> | <b>Distributed Factoring with Competing Servers</b>           | <b>61</b> |
| 6.1      | Introduction.....                                             | 61        |
| 6.2      | Special-Purpose Factoring Algorithms.....                     | 61        |
| 6.3      | Pollard's $p - 1$ Method.....                                 | 63        |
| 6.4      | Parallel Factoring.....                                       | 66        |
| 6.5      | Implementation Concerns.....                                  | 69        |
| 6.6      | Performance.....                                              | 69        |
| <b>7</b> | <b>The Synchronized Servers Pipeline</b>                      | <b>71</b> |
| 7.1      | Introduction.....                                             | 71        |
| 7.2      | The Synchronized Servers Pipeline.....                        | 72        |
| 7.3      | Implementing Synchronized Servers.....                        | 73        |
| 7.4      | Distribution and Collection.....                              | 76        |
| 7.5      | I/O Traces.....                                               | 77        |
| 7.6      | Repeated Use of the Pipeline.....                             | 80        |
| 7.7      | Performance.....                                              | 81        |
| <b>8</b> | <b>Message Block Chaining for Distributed RSA Enciphering</b> | <b>83</b> |
| 8.1      | Introduction.....                                             | 83        |
| 8.2      | Modes of Operation.....                                       | 84        |
| 8.3      | Strategy for Parallelization.....                             | 85        |
| 8.4      | Message Block Chaining.....                                   | 85        |
| 8.5      | Sequential Algorithms.....                                    | 87        |
| 8.6      | Parallel Enciphering and Deciphering.....                     | 88        |
| 8.7      | Implementation Concerns.....                                  | 91        |
| 8.8      | Performance.....                                              | 91        |
| <b>9</b> | <b>Generating Deterministically Certified Primes</b>          | <b>95</b> |
| 9.1      | Introduction.....                                             | 95        |
| 9.2      | The Primality Test.....                                       | 95        |
| 9.3      | Generating Suitable Prime Candidates.....                     | 96        |

|                                                         |                                             |            |
|---------------------------------------------------------|---------------------------------------------|------------|
| 9.4                                                     | Sequential Algorithm .....                  | 97         |
| 9.5                                                     | Parallel Algorithm.....                     | 99         |
| 9.6                                                     | Parallel Candidate Generation .....         | 100        |
| 9.7                                                     | Parallel Certification .....                | 103        |
| 9.8                                                     | Combining Generation and Certification..... | 105        |
| 9.9                                                     | Performance .....                           | 107        |
| 9.10                                                    | Generating Strong Primes .....              | 109        |
| <b>Appendix 1: A Proof of Lucas' Theorem</b>            |                                             | <b>111</b> |
| <b>Appendix 2: Multiple-Length Arithmetic</b>           |                                             | <b>115</b> |
| <b>Appendix 3: Strong Prime Generation</b>              |                                             | <b>125</b> |
| <b>Appendix 4: Pollard <math>p - 1</math> Factoring</b> |                                             | <b>137</b> |
| <b>Appendix 5: RSA Enciphering</b>                      |                                             | <b>145</b> |
| <b>Appendix 6: RSA Deciphering</b>                      |                                             | <b>151</b> |
| <b>Appendix 7: Deterministic Prime Certification</b>    |                                             | <b>157</b> |
| <b>Bibliography</b>                                     |                                             | <b>167</b> |
| <b>Index</b>                                            |                                             | <b>175</b> |
| <b>List of Figures</b>                                  |                                             | <b>177</b> |
| <b>List of Tables</b>                                   |                                             | <b>179</b> |
| <b>List of Algorithms</b>                               |                                             | <b>181</b> |