%PDF-1.4 %ÐÔÅØ 1 0 obj << /S /GoTo /D (chapter.1) >> endobj 4 0 obj (Passive Cryptanalysis of the UnConditionally Secure Authentication Protocol for RFID Systems) endobj 5 0 obj << /S /GoTo /D (chapter.1) >> endobj 7 0 obj (Mohammad Reza Sohizadeh Abyaneh) endobj 8 0 obj << /S /GoTo /D (section.1.1) >> endobj 11 0 obj (Introduction) endobj 12 0 obj << /S /GoTo /D (section.1.2) >> endobj 15 0 obj (Description of the UCS-RFID Protocol) endobj 16 0 obj << /S /GoTo /D (subsection.1.2.1) >> endobj 19 0 obj (Mutual Authentication Phase) endobj 20 0 obj << /S /GoTo /D (subsection.1.2.2) >> endobj 23 0 obj (Key Updating Phase) endobj 24 0 obj << /S /GoTo /D (section.1.3) >> endobj 27 0 obj (Observation) endobj 28 0 obj << /S /GoTo /D (section.1.4) >> endobj 31 0 obj (Our Attack Scenario) endobj 32 0 obj << /S /GoTo /D (subsection.1.4.1) >> endobj 35 0 obj (Phase I: Finding m) endobj 36 0 obj << /S /GoTo /D (subsection.1.4.2) >> endobj 39 0 obj (Phase II: Finding the constant nonce) endobj 40 0 obj << /S /GoTo /D (subsection.1.4.3) >> endobj 43 0 obj (Phase III: Key Recovery) endobj 44 0 obj << /S /GoTo /D (section.1.5) >> endobj 47 0 obj (On the Traceability of the UCS-RFID) endobj 48 0 obj << /S /GoTo /D (subsection.1.5.1) >> endobj 51 0 obj (Adversarial Model) endobj 52 0 obj << /S /GoTo /D (subsection.1.5.2) >> endobj 55 0 obj (Attacking Untraceability) endobj 56 0 obj << /S /GoTo /D (section.1.6) >> endobj 59 0 obj (Conclusions) endobj 60 0 obj << /S /GoTo /D [61 0 R /Fit] >> endobj 107 0 obj << /Length 2373 /Filter /FlateDecode >> stream endstream endobj 370 0 obj << /Type /FontDescriptor /FontName /MEXDUI+CMR10 /Flags 4 /FontBBox [-40 -250 1009 750] /Ascent 694 /CapHeight 683 /Descent -194 /ItalicAngle 0 /StemV 69 /XHeight 431 /CharSet (/A/B/C/D/E/F/G/H/I/K/L/M/N/O/P/R/S/T/U/W/a/acute/asterisk/b/bracketleft/bracketright/c/colon/comma/d/e/eight/endash/equal/f/ff/ffi/fi/five/fl/four/g/h/hyphen/i/j/k/l/m/n/nine/o/one/p/parenleft/parenright/period/plus/q/quotedblleft/quotedblright/quoteright/r/s/semicolon/seven/six/t/three/two/u/v/w/x/y/z/zero) /FontFile 369 0 R >> endobj 371 0 obj << /Length1 1395 /Length2 6101 /Length3 0 /Length 7050 /Filter /FlateDecode >> stream

endstream endobj 372 0 obj << /Type /FontDescriptor /FontName /RHUHOI+CMR5 /Flags 4 /FontBBox [-10 -250 1304 750] /Ascent 694 /CapHeight 680 /Descent -194 /ItalicAngle 0 /StemV 89 /XHeight 431 /CharSet (/one/two) /FontFile 371 0 R >> endobj 373 0 obj << /Length1 1425 /Length2 6163 /Length3 0 /Length 7130 /Filter /FlateDecode >> stream

endstream endobj 374 0 obj << /Type /FontDescriptor /FontName /CESWVJ+CMR6 /Flags 4 /FontBBox [-20 -250 1193 750] /Ascent 694 /CapHeight 683 /Descent -194 /ItalicAngle 0 /StemV 83 /XHeight 431 /CharSet (/parenleft/parenright/zero) /FontFile 373 0 R >> endobj 375 0 obj << /Length1 1510 /Length2 6864 /Length3 0 /Length 7874 /Filter /FlateDecode >> stream

endstream endobj 376 0 obj << /Type /FontDescriptor /FontName /IZJPKI+CMR7 /Flags 4 /FontBBox [-27 -250 1122 750] /Ascent 694 /CapHeight 683 /Descent -194 /ItalicAngle 0 /StemV 79 /XHeight 431 /CharSet (/equal/one/parenleft/parenright/plus/three/two/zero) /FontFile 375 0 R >> endobj 377 0 obj << /Length1 2483 /Length2 20336 /Length3 0 /Length 21765 /Filter /FlateDecode >> stream endstream endobj 378 0 obj << /Type /FontDescriptor /FontName /KZLRKW+CMR9 /Flags 4 /FontBBox [-39 -250 1036 750] /Ascent 694 /CapHeight 683 /Descent -194 /ItalicAngle 0 /StemV 74 /XHeight 431 /CharSet (/A/B/C/D/E/F/G/H/I/J/K/L/M/N/O/P/R/S/T/U/V/W/Y/a/b/c/colon/comma/d/e/eight/equal/f/ff/ffi/fi/five/four/g/h/hyphen/i/j/k/l/m/n/nine/o/one/p/parenleft/parenright/period/plus/q/quoteright/r/s/seven/six/slash/t/three/two/u/v/w/x/y/z/zero) /FontFile 377 0 R >> endobj 379 0 obj << /Length1 1675 /Length2 7852 /Length3 0 /Length 8918 /Filter /FlateDecode >> stream

endstream endobj 382 0 obj << /Type /FontDescriptor /FontName /CLYDDF+CMSY10 /Flags 4 /FontBBox [-29 -960 1116 775] /Ascent 750 /CapHeight 683 /Descent -194 /ItalicAngle -14 /StemV 40 /XHeight 431 /CharSet (/A/O/R/T/backslash/bar/braceleft/braceright/circleplus/element/equivalence/greaterequal/lessequal/minus/multiply/radical/reflexsubset/universal) /FontFile 381 0 R >> endobj 383 0 obj << /Length1 1389 /Length2 6020 /Length3 0 /Length 6971 /Filter /FlateDecode >> stream

endobj 385 0 obj << /Length1 1466 /Length2 6653 /Length3 0 /Length 7652 /Filter /FlateDecode >> stream [illegible] endstream endobj 386 0 obj << /Type /FontDescriptor /FontName /FPFYPY+CMSY7 /Flags 4 /FontBBox [-15 -951 1251 782] /Ascent 750 /CapHeight 683 /Descent -194 /ItalicAngle -14 /StemV 49 /XHeight 431 /CharSet (/A/P/asteriskmath/minus/radical) /FontFile 385 0 R >> endobj 387 0 obj << /Length1 1402 /Length2 6018 /Length3 0 /Length 6966 /Filter /FlateDecode >> stream [illegible] endstream endobj 388 0 obj << /Type /FontDescriptor /FontName /HJLAUA+CMSY9 /Flags 4 /FontBBox [-29 -958 1146 777] /Ascent 750 /CapHeight 683 /Descent -194 /ItalicAngle -14 /StemV 43 /XHeight 431 /CharSet (/arrowdblright) /FontFile 387 0 R >> endobj 389 0 obj << /Length1 1743 /Length2 11564 /Length3 0 /Length 12665 /Filter /FlateDecode >> stream [illegible] endstream endobj 390 0 obj << /Type /FontDescriptor /FontName /GIFKID+CMTI10 /Flags 4 /FontBBox [-35 -250 1124 750] /Ascent 694 /CapHeight 683 /Descent -194 /ItalicAngle -14 /StemV 68 /XHeight 431 /CharSet (/A/P/a/b/c/d/e/f/g/h/hyphen/i/k/l/m/n/o/p/r/s/t/u/v/y) /FontFile 389 0 R >> endobj 391 0 obj << /Length1 1596 /Length2 8694 /Length3 0 /Length 9733 /Filter /FlateDecode >> stream [illegible]

endobj 396 0 obj << /Type /FontDescriptor /FontName /AICAWW+MSBM10 /Flags 4 /FontBBox [-55 -420 2343 920] /Ascent 464 /CapHeight 689 /Descent 0 /ItalicAngle 0 /StemV 40 /XHeight 463 /CharSet (/Z) /FontFile 395 0 R >> endobj 129 0 obj
<< /Type /Font /Subtype /Type1 /BaseFont /JEOZVC+CMBX10 /FontDescriptor 348 0 R /FirstChar 46 /LastChar 123 /Widths 338 0 R >> endobj 110 0 obj << /Type /Font /Subtype /Type1 /BaseFont /GJPDLT+CMBX12 /FontDescriptor 350 0 R /FirstChar 45 /LastChar 121 /Widths 346 0 R >> endobj 114 0 obj << /Type /Font /Subtype /Type1 /BaseFont /RQUDOX+CMBX9 /FontDescriptor 352 0 R /FirstChar 12 /LastChar 121 /Widths 342 0 R >> endobj 187 0 obj << /Type /Font /Subtype /Type1 /BaseFont /RQAUSW+CMEX10 /FontDescriptor 354 0 R /FirstChar 0 /LastChar 81 /Widths 327 0 R >> endobj 130 0 obj << /Type /Font /Subtype /Type1 /BaseFont /VNVJDH+CMMI10 /FontDescriptor 356 0 R /FirstChar 10 /LastChar 120 /Widths 337 0 R >> endobj 133 0 obj
<< /Type /Font /Subtype /Type1 /BaseFont /MNXJHA+CMMI5 /FontDescriptor 358 0 R /FirstChar 78 /LastChar 116 /Widths 334 0 R >> endobj 158 0 obj << /Type /Font /Subtype /Type1 /BaseFont /REFQFB+CMMI6 /FontDescriptor 360 0 R /FirstChar 97 /LastChar 117 /Widths 330 0 R >> endobj 131 0 obj << /Type /Font /Subtype /Type1 /BaseFont /YQFBDJ+CMMI7 /FontDescriptor 362 0 R /FirstChar 58 /LastChar 120 /Widths 336 0 R >> endobj 156 0 obj << /Type /Font /Subtype /Type1 /BaseFont /MBBQMZ+CMMI9 /FontDescriptor 364 0 R /FirstChar 59 /LastChar 112 /Widths 332 0 R >> endobj 212 0 obj << /Type /Font /Subtype /Type1 /BaseFont /ZXZAVR+CMMIB10 /FontDescriptor 366 0 R /FirstChar 109 /LastChar 109 /Widths 325 0 R >> endobj 213 0 obj
<< /Type /Font /Subtype /Type1 /BaseFont /FWBRQC+CMMIB7 /FontDescriptor 368 0 R /FirstChar 116 /LastChar 116 /Widths 324 0 R >> endobj 111 0 obj << /Type /Font /Subtype /Type1 /BaseFont /MEXDUI+CMR10 /FontDescriptor 370 0 R /FirstChar 11 /LastChar 123 /Widths 345 0 R >> endobj 197 0 obj << /Type /Font /Subtype /Type1 /BaseFont /RHUHOI+CMR5 /FontDescriptor 372 0 R /FirstChar 49 /LastChar 50 /Widths 326 0 R >> endobj 157 0 obj << /Type /Font /Subtype /Type1 /BaseFont /CESWVJ+CMR6 /FontDescriptor 374 0 R /FirstChar 40 /LastChar 48 /Widths 331 0 R >> endobj 128 0 obj << /Type /Font /Subtype /Type1 /BaseFont /IZJPKI+CMR7 /FontDescriptor 376 0 R /FirstChar 40 /LastChar 61 /Widths 339 0 R >> endobj 112 0 obj << /Type /Font /Subtype /Type1 /BaseFont /KZLRKW+CMR9 /FontDescriptor 378 0 R /FirstChar 11 /LastChar 122 /Widths 344 0 R >> endobj 306 0 obj << /Type /Font /Subtype /Type1 /BaseFont /KHAEDF+CMSS10 /FontDescriptor 380 0 R /FirstChar 40 /LastChar 121 /Widths 323 0 R >> endobj 134 0 obj
<< /Type /Font /Subtype /Type1 /BaseFont /CLYDDF+CMSY10 /FontDescriptor 382 0 R /FirstChar 0 /LastChar 112 /Widths 333 0 R >> endobj 307 0 obj << /Type /Font /Subtype /Type1 /BaseFont /PFSTSG+CMSY5 /FontDescriptor 384 0 R /FirstChar 80 /LastChar 80 /Widths 322 0 R >> endobj 161 0 obj << /Type /Font /Subtype /Type1 /BaseFont /FPFYPY+CMSY7 /FontDescriptor 386 0 R /FirstChar 0 /LastChar 112 /Widths 328 0 R >> endobj 159 0 obj << /Type /Font /Subtype /Type1 /BaseFont /HJLAUA+CMSY9 /FontDescriptor 388 0 R /FirstChar 41 /LastChar 41 /Widths 329 0 R >> endobj 116 0 obj << /Type /Font /Subtype /Type1 /BaseFont /GIFKID+CMTI10 /FontDescriptor 390 0 R /FirstChar 45 /LastChar 121 /Widths 340 0 R >> endobj 115 0 obj << /Type /Font /Subtype /Type1 /BaseFont /WYQTDD+CMTI9 /FontDescriptor 392 0 R /FirstChar 67 /LastChar 121 /Widths 341 0 R >> endobj 113 0 obj << /Type /Font /Subtype /Type1 /BaseFont /LZUAQK+CMTT9 /FontDescriptor 394 0 R /FirstChar 46 /LastChar 125 /Widths 343 0 R >> endobj 132 0 obj
<< /Type /Font /Subtype /Type1 /BaseFont /AICAWW+MSBM10 /FontDescriptor 396 0 R /FirstChar 90 /LastChar 90 /Widths 335 0 R >> endobj 117 0 obj << /Type /Pages /Count 6 /Parent 397 0 R /Kids [61 0 R 125 0 R 153 0 R 180 0 R 194 0 R 206 0 R] >> endobj 239 0 obj
<< /Type /Pages /Count 6 /Parent 397 0 R /Kids [232 0 R 249 0 R 287 0 R 303 0 R 310 0 R 315 0 R] >> endobj 397 0 obj << /Type /Pages /Count 12 /Kids [117 0 R 239 0 R] >> endobj 398 0 obj << /Type /Outlines /First 3 0 R /Last 6 0 R /Count 1 >> endobj 58 0 obj << /Title 59 0 R /A 56 0 R /Parent 6 0 R /Prev 46 0 R >> endobj 54 0 obj << /Title 55 0 R /A 52 0 R /Parent 46 0 R /Prev 50 0 R >> endobj 50 0 obj << /Title 51 0 R /A 48 0 R /Parent 46 0 R /Next 54 0 R >> endobj 46 0 obj << /Title 47 0 R /A 44 0 R /Parent 6 0 R /Prev 30 0 R /Next 58 0 R /First 50 0 R /Last 54 0 R /Count -2 >> endobj 42 0 obj << /Title 43 0 R /A 40 0 R /Parent 30 0 R /Prev 38 0 R >> endobj 38 0 obj << /Title 39 0 R /A 36 0 R /Parent 30 0 R /Prev 34 0 R /Next 42 0 R >> endobj 34 0 obj << /Title 35 0 R /A 32 0 R /Parent 30 0 R /Next 38 0 R >> endobj 30 0 obj << /Title 31 0 R /A 28 0 R /Parent 6 0 R /Prev 26 0 R /Next 46 0 R /First 34 0 R /Last 42 0 R /Count -3 >> endobj 26 0 obj << /Title 27 0 R /A 24 0 R /Parent 6 0 R /Prev 14 0 R /Next 30 0 R >> endobj 22 0 obj << /Title 23 0 R /A 20 0 R /Parent 14 0 R /Prev 18 0 R >> endobj 18 0 obj << /Title 19 0 R /A 16 0 R /Parent 14 0 R /Next 22 0 R >> endobj 14 0 obj << /Title 15 0 R /A 12 0 R /Parent 6 0 R /Prev 10 0 R /Next 26 0 R /First 18 0 R /Last 22 0 R /Count -2 >> endobj 10 0 obj << /Title 11 0 R /A 8 0 R /Parent 6 0 R /Next 14 0 R >> endobj 6 0 obj << /Title 7 0 R /A 5 0 R /Parent 3 0 R /First 10 0 R /Last 58 0 R /Count -6 >> endobj 3 0 obj << /Title 4 0 R /A 1 0 R /Parent 398 0 R /First 6 0 R /Last 6 0 R /Count -1 >> endobj 399 0 obj << /Names [(Doc-Start) 109 0 R (Item.1) 209 0 R (Item.10) 257 0 R (Item.11) 258 0 R (Item.12) 259 0 R (Item.13) 290 0 R] /Limits [(Doc-Start) (Item.13)] >> endobj 400 0 obj << /Names [(Item.14) 291 0 R (Item.15) 292 0 R (Item.2) 210 0 R (Item.3) 211 0 R (Item.4) 238 0 R (Item.5) 252 0 R] /Limits [(Item.14) (Item.5)] >> endobj 401 0 obj << /Names [(Item.6) 253 0 R (Item.7) 254 0 R (Item.8) 255 0 R (Item.9) 256 0 R (chapter.1) 2 0 R (cite.Alomair) 146 0 R] /Limits [(Item.6) (cite.Alomair)] >> endobj 402 0 obj << /Names [(cite.Avoine) 308 0 R (cite.Benjamin) 120 0 R (cite.Bringer1) 136 0 R (cite.Bringer2) 137 0 R (cite.Bringer3) 138 0 R (cite.Carluccio) 118 0 R] /Limits [(cite.Avoine) (cite.Carluccio)] >> endobj 403 0 obj << /Names [(cite.Caspian) 121 0 R (cite.Duc) 139 0 R (cite.Feller) 200 0 R (cite.Gilbert) 141 0 R (cite.Henrici1) 319 0 R (cite.Henrici2) 320 0 R] /Limits [(cite.Caspian) (cite.Henrici2)] >> endobj 404 0 obj << /Names [(cite.Hoepman) 119 0 R (cite.Hopper) 135 0 R (cite.Kulseng) 321 0 R (cite.Lopez1) 143 0 R (cite.Lopez2) 144 0 R (cite.Lopez3) 145 0 R] /Limits [(cite.Hoepman) (cite.Lopez3)] >> endobj 405 0 obj << /Names [(cite.Madhavan) 142 0 R (cite.Mitsubishi) 122 0 R (cite.Munilla) 140 0 R (cite.Ohkubo) 318 0 R (cite.Walmart) 123 0 R (equation.1.2.1) 162 0 R] /Limits [(cite.Madhavan) (equation.1.2.1)] >> endobj 406 0 obj << /Names [(equation.1.2.2) 163 0 R (equation.1.2.3) 164 0 R (equation.1.2.4) 165 0 R (equation.1.2.5) 166 0 R (equation.1.2.6) 167 0 R (equation.1.2.7) 183 0 R] /Limits [(equation.1.2.2) (equation.1.2.7)] >> endobj 407 0 obj
<< /Names [(equation.1.3.13) 184 0 R (equation.1.3.14) 185 0 R (equation.1.3.15) 186 0 R (equation.1.3.21) 198 0 R (equation.1.3.22) 199 0 R (equation.1.4.23) 235 0 R] /Limits [(equation.1.3.13) (equation.1.4.23)] >> endobj 408 0 obj << /Names [(equation.1.4.24) 236 0 R (equation.1.4.25) 237 0 R (equation.1.4.26) 293 0 R (equation.1.4.30) 294 0 R (equation.1.4.32) 295 0 R (equation.1.4.34) 296 0 R] /Limits [(equation.1.4.24) (equation.1.4.34)] >> endobj 409 0 obj << /Names [(equation.1.4.35) 297 0 R (figure.1.1) 160 0 R (figure.1.2) 201 0 R (figure.1.3) 240 0 R (page.1) 108 0 R (page.10) 305 0 R] /Limits [(equation.1.4.35) (page.10)] >> endobj 410 0 obj << /Names [(page.11) 312 0 R (page.12) 317 0 R (page.2) 127 0 R (page.3) 155 0 R (page.4) 182 0 R (page.5) 196 0 R] /Limits [(page.11) (page.5)] >> endobj 411 0 obj << /Names [(page.6) 208 0 R (page.7) 234 0 R (page.8) 251 0 R (page.9) 289 0 R (section*.1) 313 0 R (section.1.1) 9 0 R] /Limits [(page.6) (section.1.1)] >> endobj 412 0 obj << /Names [(section.1.2) 13 0 R (section.1.3) 25 0 R (section.1.4) 29 0 R (section.1.5) 45 0 R (section.1.6) 57 0 R (subsection.1.2.1) 17 0 R] /Limits [(section.1.2) (subsection.1.2.1)] >> endobj 413 0 obj << /Names [(subsection.1.2.2) 21 0 R (subsection.1.4.1) 33 0 R (subsection.1.4.2) 37 0 R (subsection.1.4.3) 41 0 R (subsection.1.5.1) 49 0 R (subsection.1.5.2) 53 0 R] /Limits [(subsection.1.2.2) (subsection.1.5.2)] >> endobj 414 0 obj << /Kids [399 0 R 400 0 R 401 0 R 402 0 R 403 0 R 404 0 R] /Limits [(Doc-Start) (cite.Lopez3)] >> endobj 415 0 obj << /Kids [405 0 R 406 0 R 407 0 R 408 0 R 409 0 R 410 0 R] /Limits [(cite.Madhavan) (page.5)] >> endobj 416 0 obj << /Kids [411 0 R 412 0 R 413 0 R] /Limits [(page.6) (subsection.1.5.2)] >> endobj 417 0 obj << /Kids [414 0 R 415 0 R 416 0 R] /Limits [(Doc-Start) (subsection.1.5.2)] >> endobj 418 0 obj << /Dests 417 0 R >> endobj 419 0 obj << /Type /Catalog /Pages 397 0 R /Outlines 398 0 R /Names 418 0 R /PageMode/UseOutlines /OpenAction 60 0 R >> endobj 420 0 obj << /Author()/Title()/Subject()/Creator(LaTeX with hyperref package)/Producer(pdfTeX-1.40.10)/Keywords() /CreationDate (D:20101103133644+01'00') /ModDate (D:20101103133644+01'00') /Trapped /False /PTEX.Fullbanner (This is MiKTeX-pdfTeX 2.8.3563 (1.40.10)) >> endobj
xref 0 421

```
0000396544 00000 n 0000396582 00000 n 0000396709 00000 n trailer << /Size 421 /Root 419 0 R /Info 420 0 R /ID [ ] >> startxref 396984 %%EOF
```