

周报 向嘉豪(2026-01-12)

摘要: 本周完成硕士学位论文第一章绪论与第二章基础知识的撰写工作。论文围绕 SPN 结构密码的软硬件优化实现展开研究, 第一章绪论部分完成了选题背景及研究意义的阐述、国内外研究现状的综述以及三个主要研究方向的介绍; 第二章完成了 SPN 结构密码基本原理、密码算法的软件实现技术和硬件实现技术三个方面的基础知识论述, 为后续章节的具体优化实现方法奠定了理论基础。

下周计划: 继续完成第三章面向资源受限环境的 CRAFT 密码 FPGA 高效实现的撰写工作

1 第一章绪论撰写

完成了论文第一章绪论部分的撰写工作。该章节包括选题背景及研究意义、国内外研究现状和研究内容三个主要部分。选题背景部分阐述了 SPN 结构密码在现代分组密码设计中的主流地位及其在物联网安全领域的应用需求。国内外研究现状部分从轻量级密码硬件实现、比特切片密码软件实现和 GPU 并行密码实现三个方向对相关研究进行了系统综述, 涵盖了 PRESENT、LED、Midori、GIFT、CRAFT 等轻量级密码的设计与实现进展, 以及针对 32 位处理器和 GPU 平台的优化技术发展。

研究内容部分明确了论文的三个主要研究方向: 面向资源受限环境的 CRAFT 密码 FPGA 高效实现、面向 32 位处理器的 SPN 密码比特切片低延迟实现、以及面向 GPU 的 AES 算法线程自适应并行优化实现。每个研究方向均阐述了主要贡献, 包括串行与展开两种 FPGA 架构设计、置换分解算法和改进的门复杂度模型编码方法、以及自适应线程分配和函数级并行化方法等技术创新点。

2 第二章基础知识撰写

完成了第二章 SPN 结构密码的软硬件优化实现基础知识的撰写工作。该章节系统介绍了 SPN 密码基本原理、软件实现技术和硬件实现技术三个方面的理论基础。在 SPN 密码基本原理部分, 从数学角度形式化定义了 S 盒变换和线性变换, 详细分析了 AES-128 的 SubBytes、ShiftRows、MixColumns 和 AddRoundKey 四个基本操作的设计原理与实现方式, 阐述了 SPN 结构通过替代层和线性层的协同作用实现 Shannon 混淆和扩散原理的安全机制。

软件实现技术部分介绍了查找表实现、比特切片实现和 SIMD 向量化实现三种主要技术路线, 分析了各自的优势与局限性。比特切片技术的核心思想是将密码操作映射到位级布尔运算, 利用处理器的位并行性同时处理多个数据分组, 具有高吞吐率和恒定时间执行的优势。硬件实现技术部分介绍了 ASIC 和 FPGA 两类平台, 详细阐述了迭代架构、串行架构和展开架构三种实现架构的特点与适用场景, 分析了 S 盒的查找表方法和逻辑门电路方法, 以及线性层比特置换和矩阵乘法的硬件实现优化策略。

3 论文撰写进展展示

专业硕士论文	SPN 结构密钥的软硬件优化实现研究	专业硕士论文	SPN 结构密钥的软硬件优化实现研究	专业硕士论文	SPN 结构密钥的软硬件优化实现研究
第一章 绪论					
1.1 选题背景及研究意义					
这是对论文的介绍部分。					
1.2 国内国外研究现状					
SPN 结构密钥的高效率研究涵盖硬件实现、软件实现和并行计算三个主要方向。国内外学者在上述方向均取得了一系列的研究成果。					
1.2.1 软件级密钥实现研究现状					
近年来, 经典密码学研究领域广泛, 如 PRESENT ¹ 、LEDP ² 、Milen ³ 、GCL ⁴ 、GIFT ⁵ 、RAFT ⁶ 、Shao ⁷ 、DULC ⁸ 、VIBLOC ⁹ 、Bigip ¹⁰ 和 LELBC ¹¹ 等算法相继提出, 更多算法正在逐步提出。物理安全领域在文献 ¹² 中也有讨论, 相关密钥技术文献 ¹³ 中也有讨论, 但能直接应用到 SPN 中的较少。					
在硬件实现方面, 已有学者对不同算法提出了优化方案。Lara ¹⁴ 提出了 PRESENT 的 16 位位级并行架构, Pandya ¹⁵ 提出了并行化设计架构, Shabani ¹⁶ 提出了 AES 的 8 位并行架构, Li ¹⁷ 等对 PRINCE 提出了并行化设计架构, Bharati ¹⁸ 扩展了 PRESENT 的密钥长度, Yam ¹⁹ 等通过并行架构优化了 LILIPUT。					
在穷路攻击的防护方面, 王彦峰等 ²⁰ 提出, 后来在文献 ²¹ 中又有更多详细说明。为应对此类攻击, 韩 ²² 等提出了检测侧信道机制, Canno ²³ 等在后量子密钥领域提出了专属性检测方法。					
1.2.2 比特切片密钥实现研究现状					
比特切片技术由 Baum ²⁴ 引入, 作为在 64 位复杂度集算机上实现 DES 密钥的高效率方法, 对于密钥的全部密钥值已应用了所有的密钥计算方法 ²⁵ 。文献 ²⁶ 对发展了更多位数的比特切片密钥提出了新的方法。					
比特切片密钥实现研究的另一个方向是将比特切片技术应用于 SPN 的密钥实现。在文献 ²⁷ 中多模数 (SMID) 指令的高性能 CPU 上提出了密钥生成 ²⁸ , 在图形处理器 (GPU) 中 ²⁹ 已实现高效的 AES-CTR 和 AES-ICB 实现 ³⁰ 。					
针对 32 位处理器的优化工作主要集中在位级和寄存器层面。在位级层面, 位级线性 ³¹ 提出的优化方法对复杂的密钥分量为寄存器的重叠和对称性, 在非线性层面, 门级复杂度最小化技术减少了 S 盒实现的密钥操作数据 ³² , 但只满足线性解密器被用于 S 盒变换 ^{33,34} , 32 位处理器的架构优化需要量身定制的优化策略 ³⁵⁻⁴¹ 。					
1.3 研究内容					
本文针对 SPN 结构密钥的硬件级实现展开研究, 针对不同应用场景和平台特点, 提出了两种高效实现方案。研究内容包括以下三个方面:					
1.3.1 面向资源受限环境的 CRAFT 密码 FPGA 高效实现					
CRAFT 密码在设计时考虑过攻击强度, 但其高效实现有待提升, 特别是在资源受限环境下。本次工作对 FPGAs 平台上实现的 CRAFT 密码, 提出了串行 (Serial) 与展开 (Unrolled) 两种实现方案, 通过将密钥位数限制在 64 位至 4 位, 采用一个 S 盒, 复杂度降低至 16 位, 展开架构将密钥位数限制在 32 位至 8 位, 提高了效率。S 盒实现在解密结合 GEC 编码码字化实现, 进一步降低能耗。主要贡献如下:					
<ul style="list-style-type: none"> 提出了针对 CRAFT 的串行和展开两种架构, 分别优化串行与吞吐率, 串行架构和串行架构的复杂度均降低 10.10%。 利用 SAT 求解器优化 S 盒实现, 面积减少 28.9%。 在串行 FPGAs 平台上实现, 便于工程应用相应用需求选择合适平台。 					
1.3.2 面向 32 位处理器的 SPN 密钥比特切片低延迟实现					
将比特切片优化技术应用到 32 位处理器架构中带来重大挑战, 包括受限指令集架构缺少专门指令。较少的内存带宽限制了并行处理的内存存取约束, 从而影响存取速度。本文通过设计针对 32 位处理器上 SPN 密钥实现的新型优化策略, 解决了上述挑战, 主要贡献如下:					
<ul style="list-style-type: none"> 提出了一种优化位数在位级中操作数的分解算法, 通过进位优化策略将复杂操作转换为最小位数级, 显著降低延时和操作码大小。 引入了一种改进的比特切片分支度模型编码方法来优化 S 盒实现, 利用布尔可满足性求解器高效确定最优指令序列, 加速求解过程。 					
1.4 文论组织结构					
本文组织结构如下:					
第二章 章 SPN 构造密钥的软硬件优化实现研究基础					
2.1 SPN 结构密钥基本原理					
该章节主要介绍 SPN 构造密钥的背景、Galois-Espresso Standard (AES) ⁴² 中的 Feistel 架构, 通过左右分支的密钥和密文的输入输出, 介绍密钥分摊 (Substitution-permutation Network, SPN) 构造密钥为实现非线性变换的密钥设计范式, 与 Feistel 架构相比, SPN 构造具有更好的设计, 支持密钥并行处理, 并通过将密钥的线性关系应用到安全强度, 同时 SPN 构造和密钥分摊先利用标准 (Advanced Encryption Standard, AES) ⁴³ 、PRESENT 密钥 ⁴⁴ 、GIFT 密钥 ⁴⁵ 。					
SPN 构造的基本设计流程如图 2-1 所示。一个密文 (plain text) 由密钥 (substitution layer, 线性层 (Linear Layer) 和密钥加 (Round Key Add) 三部分组成。对密文进行密钥分摊 (Substitution), 然后进行线性层 (Linear) 处理, 与 Feistel 架构相比, SPN 构造具有更好的设计, 支持密钥并行处理, 并通过将密钥的线性关系应用到安全强度, 同时 SPN 构造和密钥分摊先利用标准 (Advanced Encryption Standard, AES) ⁴³ 、PRESENT 密钥 ⁴⁴ 、GIFT 密钥 ⁴⁵ 。					
图 2-1 SPN 密钥设计流程					
密文经过 S 盒实现后, 是 SPN 构造中非线性变换的核心组件。S 盒是一个从密文到密文的映射, 通常为非线性函数将输入到比特级为输出比特级, 使得攻击者难以从输入到输出之间的关系。在实现中, S 盒可以表示为查找表或通过逻辑门实现。					
定义 2.1 (S 盒比特函数)。给定有限域 F_q 上的向量空间 V_q , 对于每个输出比特 i , 比特 S 盒函数 $S_i: V_q \rightarrow F_q$ 定义为:					
$S_i(x) = \bigoplus_{j=0}^{q-1} c_{ij} x_j \quad (2-1)$					
其中, $x = (x_0, \dots, x_{n-1}) \in F_q^n$ 为输入向量, $T_i(x) \in F_q$ 为输出向量的第 i 个分量, $a_{ij} \in F_q$ 为变换系数。					
定义 2.2 (线性变换)。给定有限域 F_q 上的向量空间 V_q , 线性变换 $T: V_q \rightarrow V_q$ 定义为:					
$T(b) = \bigoplus_{j=0}^{q-1} a_{j0} b_j \quad (2-2)$					
其中, $b = (b_0, \dots, b_{n-1}) \in F_q^n$ 为输入向量, $T(b) \in F_q^n$ 为输出向量, 第 j 个分量, $a_{j0} \in F_q$ 为变换系数。					
定义 2.3 (线性变换矩阵)。线性变换的矩阵表示 $L \in F_q^{n \times n}$ 定义为:					
$L = (a_{ij})_{0 \leq i, j \leq n-1} = \begin{bmatrix} a_{00} & a_{01} & \cdots & a_{0n-1} \\ a_{10} & a_{11} & \cdots & a_{1n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1, 0} & a_{n-1, 1} & \cdots & a_{n-1, n-1} \end{bmatrix} \quad (2-4)$					
其中, $a_{ij} \in F_q$ 表示矩阵 L 的第 i 行第 j 列的系数。					
矩阵 L 中的系数 a_{ij} 决定了第 i 行第 j 列, 对输出比特 i 的贡献。当 $a_{ij} = 1$ 时, 输入比特 j 通过或运算或异或运算到输出比特 i 的计算中。通过精心设计矩阵 L 的结构, 可					
其中, $x = (x_0, \dots, x_{n-1}) \in F_q^n$ 为输入向量, $P_i(x) \in F_q$ 表示索引为 i 的子密钥的密文。					
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 290 291 292 293 294 295 296 297 298 299 299 300 301 302 303 304 305 306 307 308 309 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 390 391 392 393 394 395 396 397 398 399 399 400 401 402 403 404 405 406 407 408 409 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 490 491 492 493 494 495 496 497 498 499 499 500 501 502 503 504 505 506 507 508 509 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 580 581 582 583 584 585 586 587 588 589 589 590 591 592 593 594 595 596 597 598 599 590 591 592 593 594 595 596 597 598 599 599 600 601 602 603 604 605 606 607 608 609 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 680 681 682 683 684 685 686 687 688 689 689 690 691 692 693 694 695 696 697 698 699 690 691 692 693 694 695 696 697 698 699 699 700 701 702 703 704 705 706 707 708 709 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 780 781 782 783 784 785 786 787 788 789 789 790 791 792 793 794 795 796 797 798 799 790 791 792 793 794 795 796 797 798 799 799 800 801 802 803 804 805 806 807 808 809 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 880 881 882 883 884 885 886					

图 1 第一章与第二章论文页面展示 (第 1-6 页)

