计算机科学
COMPUTER SCIENCE

基于申威众核处理器的Office口令恢复向量化研究

李辉, 韩林, 陶红伟, 董本松

引用本文

李辉, 韩林, 陶红伟, 董本松.基于申威众核处理器的Office口令恢复向量化研究[J]. 计算机科学, 2022, 49(11A): 210900176-5.

LI Hui, HAN Lin, TAO Hong-wei, DONG Ben-song. Study on Office Password Recovery Vectorization Technology Based on Sunway Many-core Processor [J]. Computer Science, 2022, 49(11A): 210900176-5.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210900176

基于申威众核处理器的 Office 口令恢复向量化研究

李 辉[1] 韩 林[2] 陶红伟[3] 董本松[4]
1 青岛农业大学经济学院 山东 青岛 266109
2 郑州大学河南省超级计算中心 郑州 450000
3 郑州轻工业大学计算机与通信工程学院 郑州 450002
4 郑州经贸学院计算机与人工智能学院 郑州 451191

摘 要 为了满足农业农村大数据应用中数据安全的需求,文章结合 Office 口令恢复中的计算热点问题,以申威众核处理器为硬件平台,提供了一种向量化密码解算方法。SHA-1 和 AES 函数的解析是方法的核心部分。首先,利用申威众核处理器的特点,对其进行自动向量化研究;其次,通过依赖性分析描述了明文块之间手动向量化过程,给出方法理论层面的可行性结论;最后,为验证方法的正确性和有效性,将 Office 各个版本的加密文档作为用例,开展多重数据测试,测试结果与传统的口令恢复工具和开源的 Hashcat 口令恢复工具进行对比。实验结果表明,方法能够有效地提高口令恢复的性能。

关键词:大数据;数据解密;SHA-1;AES;向量化
中图法分类号 TP391

Study on Office Password Recovery Vectorization Technology Based on Sunway Many-core Processor

LI Hui[1],HAN Lin[2],TAO Hong-wei[3] and DONG Ben-song[4]
1 School of Economics,Qingdao Agricultural University,Qingdao,Shandong 266109,China
2 Henan Supercomputing Centre,Zhengzhou University,Zhengzhou 450000,China
3 School of Computer and Communication Engineering,Zhengzhou University of Light Industry,Zhengzhou 450002,China
4 School of Computer and Artificial Intelligence,Zhengzhou University of Economics and Business,Zhengzhou 451191,China

Abstract In order to meet the needs of data security in agricultural and rural big data applications,the paper combines the hot computing issues in Office password recovery and uses Sunway many-core processors as the hardware platform to provide a vectorized password solution method. The analysis of SHA-1 and AES functions is the core part of the method. Firstly,using the characteristics of Sunway many-core processors to conduct automatic vectorization research. Secondly,through dependency analysis,the manual vectorization process between plaintext blocks is described,and the feasibility conclusion of the method theory is given. Finally,to verify the correctness and effectiveness of the method,the encrypted documents of each version of Office are used as use cases,and multiple data tests are carried out. The test results are compared with the traditional password recovery tool and the open-source Hashcat password recovery tool. Experimental results show that the method can effectively improve the performance of password recovery.

Keywords Big data,Data decryption,SHA-1,AES,Vectorization

1 引言

随着农业智能化的发展,农业农村数据安全问题日益突出,尤其在抗击计算机病毒侵害与网络恶意行为,保护核心数据安全方面的需求迫切。目前实现口令的各种加密算法的口令保护技术也在不断提高,使其恢复口令需要的时间和空间越来越大,用户对恢复口令的要求也越来越高。当前以 CPU 为基础的传统口令恢复工具已经不能满足用户的基本需求,在当前的复杂环境下,为了保护数据的安全性,研究更有效的口令恢复算法,迫切需要更强大的计算力作为支撑,以提高口令恢复性能,进而形成更强大的口令恢复计算能力。

目前,国内外许多学者都开展了针对 Office 口令恢复的研究。文献[1]使用 GPU 实现了 Office 2003 的口令恢复算法;文献[2]采用 GPU 作为硬件平台,实现了 Office 2007 和 Office 2010 的加密恢复算法;文献[3]在 GPU 上对 Office 2013 加密机制进行了分析;文献[4]利用 GPU 研究 Microsoft Office 密码恢复系统的关键技术;文献[5]利用 FPGA 实现了 Office 2010 的口令恢复;文献[6]介绍了多种提高口令恢复效率的方法,并指出使用 FPGA 异构部件可以获得较好的性能。但是,在当前恶劣的国际形势下,我们必须立足国产软、硬件,研发属于本国的先进数据安全技术,确保农业农村核心数据的安全,确保科技兴农战略的顺利实施。

2 国产高性能平台基础

申威众核处理器是我国自主研发的高性能处理器,是我国在国产自主可控方向上取得的一项重要突破,其主从核均

基金项目:河南省重大科技专项(201400210600)
This work was supported by the Henan Province Major Science and Technology(201400210600).
通信作者:李辉(leephil@163.com)

支持256位的向量化技术，具备运行并行Office口令恢复程序的可能性，是研制开发高性能Office口令恢复系统的基础，力争在吞吐量、效率、开销和速度方面取得较大改善。

为了更加有效地提高Office口令恢复的效率。本文提出了一种基于申威众核平台的Office口令恢复向量化的研究方案。重点研究了如何利用SIMD向量化技术提高Office口令恢复的性能。主要研究内容为：

(1)针对农业农村大数据应用中的数据安全问题，开展了国产自主可控平台的研究。为了提高Office口令恢复的性能，对Office口令恢复中的SHA-1和AES函数进行了充分的并行性分析；

(2)结合申威众核处理器的特点，首先对Office口令恢复程序进行了自动向量化研究，然后通过明文块之间的关系给出了手动向量化过程；

(3)为了验证向量化方法的正确性和有效性，本文采取多重数据测试。实验结果表明，经过向量化后，Office口令恢复的性能得到了改善，该方法具有一定的实用性。

2.1 申威众核处理器

图1给出了申威众核处理器的结构。该系统包括4个核组单元，共计260个核心，其中每个核组都包含一个运算控制核心(Management Processing Element，MPE)和一个运算核心阵列(Computer Processing Elements，CPEs)[7]，运算核心阵列由64个运算核心组成，并且运算核心之间是独立的，每个运算核心都有一个独立且容量为64 kB的局部存储(Local Direct Memory，LDM)，LDM与主存之间支持以直接内存访问(Direct Memory Access，DMA)方式传输数据。运算控制核心作为通用处理器核心，负责对运算单元进行分配和协调；64个运算核心作为加速计算核心，用来提高代码中计算密集部分的速度[8]。在硬件结构合理布局的基础上，对大数据环境下的农业农村数据安全问题进行研究，不仅能有效地执行各种哈希算法，而且还能有效地解决在并行处理系统设计中遇到的存储、互连和任务调度等问题[9]。

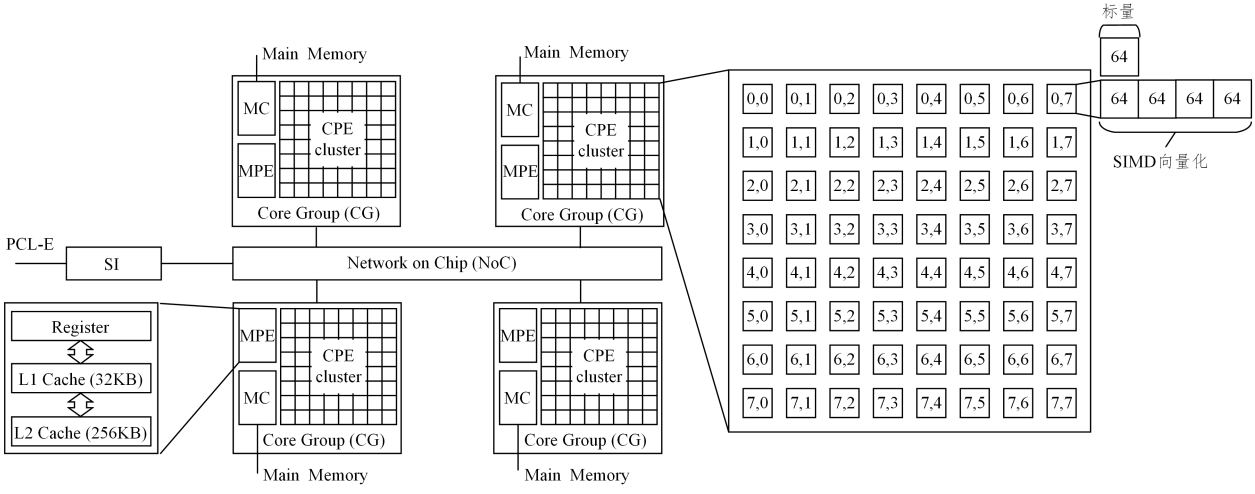

图1 申威众核处理器

Fig. 1 Sunway many-core processor

2.2 Office口令恢复分析

根据Amdahl加速定律和Gustafson定律可知，一个程序的加速比潜力由其可以并行的部分所占的比例所决定。Office口令恢复程序主要包括Office文档解析、预处理、口令扩展、Hash迭代、AES、对比验证6个模块，其中Office口令恢复的主要计算量集中在Hash迭代和AES加解密的运算上，Hash的高次迭代是口令恢复的关键，它主要通过SHA-1高速迭代运算5/10万次，每一次迭代又包括80次子循环，最后生成160位的消息摘要。AES是以Hash高次迭代的结果和部分验证串作为输入来执行口令恢复操作，主要完成AES加解密的工作。

在Office口令恢复程序中对SHA-1函数进行相关性分析和向量化处理[10]。SHA-1操作的循环次数为明文的分组数。哈希算法的执行流程如图2所示，首先对明文进行预处理，使其长度为512位的整数倍，然后按照512位的长度进行分组，将512位划分成16个子明文组，每个子明文组32位。申请5个链接变量a,b,c,d,e，初始值分别为H_0,H_1,H_2,H_3,H_4。将16个子分组扩展为80份，80个子分组进行4轮运算，得到新的a,b,c,d,e值。将新的链接变量与原始链接变量进行求和。链接变量作为下一个明文分组的初始化链接变量。最后一个分组的5个链接变量拼接成SHA-1。因为将子明文分成了16个组，每一步操作都是独立的，互不影响，所以非常适合SIMD向量化操作。

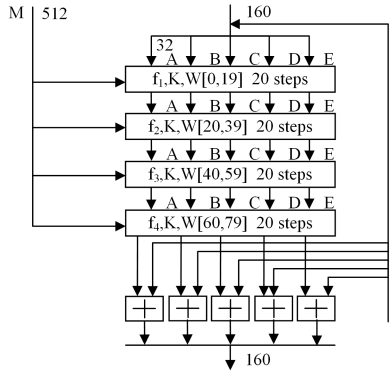

图2 SHA-1函数执行流程

Fig. 2 SHA-1 function execution process

在Office口令恢复程序中，对AES函数进行相关性分析和向量化处理[11]。AES函数虽然采用128位的分组方式，但是从算法实现的角度来看，每一轮的转换操作都是以字节或字为单位，可以将串行执行的步骤并行执行，如图3所示。字节替换是以执行相同操作的字节为单位向替换单元输入数据。同样，将列混淆以字为单位分别输入到4个列混淆单元

中，轮密钥加以字节为单位将数据与相应的轮密钥进行异或运算。可以同时执行多个转换操作，一条指令可以控制多个单元同时执行，因此，非常适合 SIMD 向量化操作。

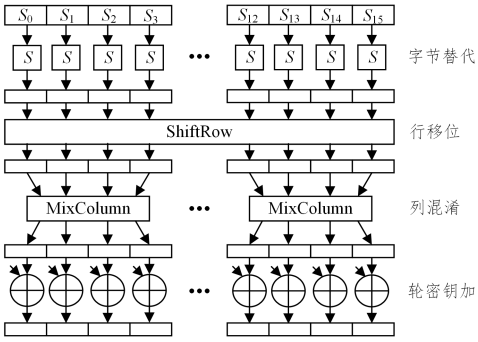

图 3　AES 算法执行流程

Fig. 3　AES algorithm execution process

3　向量化实现方法

本文提出的方法是以申威众核处理器为研究平台，采用 SIMD 向量化技术，对 Office 口令恢复程序进行自动向量化研究，利用 Office 口令恢复程序的热点函数，结合申威众核平台的并行优势，对 Office 口令恢复程序进行依赖性分析，进行手动向量化研究并实现。

3.1　自动向量化

申威众核处理器的主从核均支持 256 位的 SIMD 向量化技术[12]。SIMD 的主要特点是，向量中的每一个元素都不相关，而且一个向量的运算结果也不会影响其他向量元素。一条 SIMD 指令相当于一个小的循环，它可以减少程序中的指令数量，降低对指令访问带宽的需求，并减少循环引起的控制相关[13]。但是，串行程序向量化也存在一定的局限性。对于申威众核处理器而言，向量化访存操作必须是连续的地址，并且要求 32 字节对界。另外，由于 SIMD 扩展定点类型的指令集是不完备的，一些操作运算不支持向量化。从程序上讲，循环体向量化是最常见的，收益也相对较好，但是循环体中存在复杂的关键字、操作、数据访问和内存操作等问题，这些问题都会影响对程序的相关性分析和向量化处理，因此不利于用户对程序进行向量化。

根据 SIMD 扩展部件的特点，利用申威自动向量化系统，对应用程序进行基础的依赖分析和并行分析，挖掘 Office 口令恢复程序中蕴含的数据并行部分，生成面向从核心的可执行向量程序。在 Office 口令恢复程序中自动对数据层进行数据级并行的挖掘，当可执行代码生成时，将标量指令替换为 SIMD 指令，进而提高 Office 口令恢复的性能。自动向量化系统是基于神威编译器开发的，使用时必须指定一个带有 SIMD 自动向量化版本号“5.421-sw-gy”的编译器。首先使用最基本的方法优化程序，测试 Office 口令恢复的基础优化效果，方法是在编译选项上添加-O0，-O1，-O2，-O3。然后，在-O3 的基础上进行自动向量化研究，在编译选项上添加-LNO:simd=1，打开神威编译器的自动向量化功能，以便更直观地反映 Office 口令恢复程序中适合向量化的部分，还需要将-LNO:simd_report=2 添加到编译语句中，以便输出关于向量化成功和失败的信息。最后，通过 SWACC 编译器提供的选项-HCFlags 和-SCFlags 将参数分别传递给主核和从核的编译器，进行自动向量化。Office 口令恢复程序通过自动向量化后，可以在一定程度上提高 Office 口令恢复的性能，即只对简单的、无依赖的程序有效果，如果程序能够自动向量化，输出的信息为：LOOP WAS VECTORIZED。同时还提示具有依赖性的函数，输出的信息为：Loop has dependencies. Loop was not vectorized。如果想让 Office 口令恢复程序有更好的性能改进，则需要在自动向量化的基础上增加手动向量化，并且需要对程序的依赖性进行充分分析，因为依赖关系分析是进行程序交换和向量化挖掘的基础。

3.2　手动向量化

申威众核处理器支持 256 位的 SIMD 向量化技术，使用 SIMD 向量化技术[14]，相当于将 Office 口令恢复并行处理，如果对 Office 口令恢复程序进行向量化处理，则 Office 口令恢复的速度理论上可以提高 4 倍，恢复时间则缩短 4 倍。一条 SIMD 指令相当于一个小的循环，既减少了指令数量，又降低了指令访问带宽的需求。目前申威众核处理器的自动向量化系统尚不完善，程序的代码需要手动替换为一个能够识别的 SIMD 指令，不依赖于并行编程模型，使其减少循环迭代次数，从而提高 Office 口令恢复的性能。

在 Office 口令恢复程序中，对 SHA-1 算法进行 SIMD 向量化处理[15]。基于申威众核平台的特点，SHA-1 函数主要负责哈希计算，消息摘要是由哈希计算生成的最终哈希值。在 SHA-1 函数中，每个消息块都有 512 位字节，并用 16 个 32 位字表示。使用具有不同函数的几轮算法来处理一个消息块，并对每个块都进行重复计算。利用 SIMD 向量化操作，可以实现 SHA-1 函数的并行执行，同时对多个数据元素执行 SIMD 向量化操作，从而达到加速哈希计算的效果；为了同时处理不同的数据，需要充分分析 SHA-1 函数内部的并行度，以确定该操作是否适合 SIMD 向量化，并使用 SIMD 指令一次执行相同的操作，从而提高 Office 口令恢复的性能。在充分分析 SHA-1 函数内部并行度的基础上，结合申威众核处理器的特点，对 SHA-1 函数进行 SIMD 向量化，SHA-1 函数内部适合 SIMD 向量化的部分如表 1 所列。

表 1　SHA-1 函数内部适合 SIMD 向量化以及循环数

Table 1　SHA-1 function is suitable for SIMD quantization and number of cycles

操作	循环数
$W_{t-8}\oplus W_{t-14}\oplus W_{t-16}$	4
$ROTL_1(W_{t-3}\oplus W_{t-8}\oplus W_{t-14}\oplus W_{t-16})$	3
W_t+K_t	4
$E+W_t+K_t$	3
$f_t(B,C,D)$	2
$ROTL_{30}(B)$	2

本节对 Office 口令恢复程序中的 AES 加解密进行了 SIMD 向量化处理[16]，基于申威众核平台的特点，它可以每次处理一个固定的 16 字节明文块，明文块之间不存在任何的数据相关性，并且可以连续访问，因此适合向量化。若按顺序依次执行 16 字节的明文块，则计算量很大，导致计算效率低下。为了提高 Office 口令恢复的计算效率，采用有效的向量化指令进行替换，针对 AES 算法中大量密集数据的计算问题，可以采用手工 SIMD 指令进行替换。对于 AES 算法的 SIMD 向量化运算，具体步骤如下：首先执行对界装入——simd_load()，把标准类型的数据扩展为向量化类型的变量；其次，将任务分配到 64 个 CPE 从核心上，原来 1 个 CPE 只能计算 1 个明文块，经过 SIMD 指令替换后，一个 CPE 可以同时计算 4 个明文块；然后，计算结果通过对界存储——simd_store()，

按照标准要求，把扩展类型数据重新映射回标准类型中去，其中每个 CPE 计算结果通过向量加法 simd_vaddw()拼接在一起，最后，输出 128 位的消息摘要，具体代码如算法 1 所示。

算法 1 SIMD 向量化并行

```
输入：16 字节的明文块
输出：128 位的消息摘要
1. Begin
2.   #include“simd.h”
3.   ……
4.   intv8va,vb,vc
5.   simd_load(va,block)
6.   simd_load(vb,block)
7.     va←Hash calculate
8.     vb←Hash calculate
9.       for(i=0;i<=block_count;i+=4)
10.      {
11.          vc=simd_vaddw(va,vb)
12.      }
13.  simd_print_intv8(vc)
14.  simd_store(vc,encrypted_verifier_value)
End
```

4 实验结果与性能分析

4.1 实验环境与测试程序

本文设计的实验平台为申威小型超级计算机系统，它由 1 台管理节点计算机和 1 台双星服务器组成。其中双星服务器包含 1 颗 AST2400 作为 BMC(Baseboard Management Controller)处理器，以及 1 颗 SW26010 申威众核处理器作为 1 个计算节点。实验环境的详细信息如表 2 所列。

表 2 实验环境

Table 2 Lab environment

名称	描述
服务器	申威小型超级计算机
操作系统	Deepin Linux Server 15.5
CPU	Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz 4 核
编程语言	C 语言
编译器	gcc
CPU 内存	8GB
SW	SW26010 @1.45GHz 260 核
编程语言	C 语言
编译器	sw5cc
SW 内存	32GB
测试程序	SW-Office 口令恢复程序

4.2 实验结果与对比分析

为了验证本文提出的方法的正确性和有效性，以单核组为基础，采用向量化技术对口令恢复程序中的 SHA-1 和 AES 热点函数进行向量化处理，与未利用向量化技术前的口令恢复程序相比，对主从核的性能进行了测试。选择 Office DOC 2003，Office DOCX 2007，Office DOCX 2010，Office DOCX 2013 作为测试的加密文档。每项测试实验进行 20 次，取平均值，保留整数。图 4 给出了性能测试的结果。为了保持图形的可观性，图 4 中的 Office DOC 2003 的性能缩小了 1000 倍。如图 4 所示，在申威众核处理器的基础上，对本文提出的向量化方法进行了验证和比较，验证的方法是在不改变硬件条件的前提下进行使用向量化方法和未使用向量化方法之间的比较。使用向量化技术后，基于申威众核处理器的口令恢复性能得到了显著改善。实验结果表明，采用向量化技术处理后，Office DOC 2003 的口令恢复性能提高了 6.24 倍，Office DOCX 2007 的口令恢复性能提高了 5.85 倍，Office DOCX 2010 的口令恢复性能提高了 6.05 倍，Office DOCX 2013 的口令恢复性能提高了 9.09 倍，从而证明了所提方法的有效性和正确性。

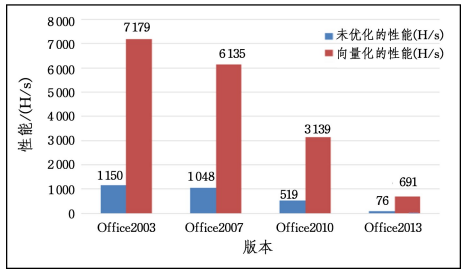

图 4 正确性测试

Fig. 4 Correctness test

Office 不同版本的口令恢复性能表现出了不同的性能提升效果，主要原因是不同版本的 Office 文档加密所采用的加密算法不同。例如，Office DOC 2003 版本使用的是 MD5 的加密算法，Office DOCX 2007 版本和 Office DOCX 2010 版本使用的是 AES-128 的加密算法，Office DOCX 2013 版本使用的是 AES-256 的加密算法，由此可见加密算法不同，计算的时间复杂度也会有所不同，最终导致口令恢复性能提升的效果也存在差异性。

为了更好地评估申威众核平台的口令恢复性能，本文基于申威众核平台(SW26010 处理器)、科学计算 GPU 服务器(NVIDIA Tesla P100-PCIE-12GB)、高性能 KNL 并行计算工作站(Intel Xeon Phi CPU 7210 @ 1.30GHz)、通用研发计算机(Intel Core i5-7500 CPU @ 3.40GHz)等平台对 Office 口令恢复的性能进行了测试对比，分别对 Office DOC 2003，Office DOCX 2007，Office DOCX 2010，Office DOCX 2013 进行 20 次测试，取平均值，保留整数。图 5 显示了基于各个平台的性能测试结果。为了保持图形的可观性，图 5 中的 Office DOC 2003 的性能缩小了 1000 倍。

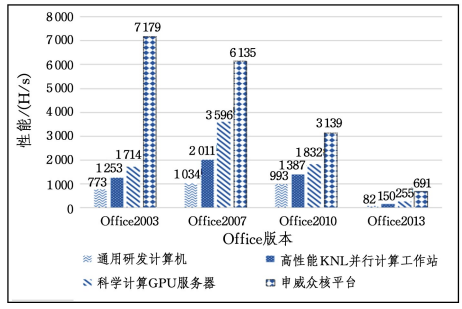

图 5 不同平台的性能测试

Fig. 5 Performance test of different platforms

如图 5 所示，实验结果证明，基于申威众核平台的口令恢复性能明显优于其他平台。比如，在 Office DOC 2003 版本上，申威众核平台的口令恢复性能是科学计算 GPU 服务器的 4.19 倍，是高性能 KNL 并行计算工作站的 5.73 倍，是通用研发计算机的 9.23 倍。在 Office DOCX 2007 版本上，申威众核平台的口令恢复性能是科学计算 GPU 服务器的 1.71 倍，是高性能 KNL 并行计算工作站的 3.05 倍，是通用研发计算机的 5.93 倍。在 Office DOCX 2010 版本上，申威众核平台的口令恢复性能是科学计算 GPU 服务器的 1.71 倍，是

高性能 KNL 并行计算工作站的 2.26 倍，是通用研发计算机的 3.16 倍。Office DOCX 2013 版本上，申威众核平台的口令恢复性能是科学计算 GPU 服务器的 2.71 倍，是高性能 KNL 并行计算工作站的 4.61 倍，是通用研发计算机的 8.43 倍。利用 4 个不同 Office 版本的加密文件分别对 4 个平台进行了口令恢复测试的实验结果表明，基于不同平台的相同口令恢复工具测试，申威众核平台的口令恢复性能表现较好，除了对口令恢复程序优化的方法起到了一定的作用，申威众核处理器也为口令计算提供了强有力的硬件支持。

为了进一步验证基于申威众核平台的口令恢复性能，将与市场上较为流行的 Office 口令恢复软件进行性能对比评测，图 6 给出了 AOPR 单机版、EDPR、AccentSoft、Hashcat 和 SW-Office 口令恢复程序的性能，选择的测试加密文档为 Office DOCX 2007。

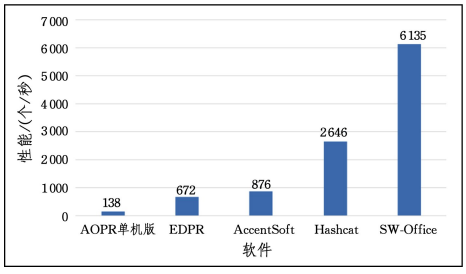

图 6　各软件的性能对比分析

Fig. 6　Performance comparison of each software

本文使用 Office DOCX 2007 加密文档作为研究对象，测试并统计各种常用口令恢复软件的性能。因为目前市场上大部分口令恢复工具并不支持申威众核平台，只能在有限的条件内，提供支持的硬件平台，对口令恢复软件进行测试并统计数据。实验结果表明，当使用不同口令恢复软件对同一类型加密文档进行口令恢复时，SW-Office 的性能是 AOPR 单机版的44.46 倍，是 EDPR 的 9.13 倍，是 AccentSoft 的 7.00 倍，是 Hashcat 的 2.32 倍。综上所述，基于申威众核平台的 Office 口令恢复性能表现较好，同时，在申威众核平台的基础上，对未优化的软件进行了相同类型加密文档的口令测试，测试的性能结果并没有使用向量化方法优化的效果好，从而进一步验证了方法的正确性和有效性。

结束语　本文针对 Office 口令恢复算法的向量化研究，结合申威众核平台的特点，利用 SIMD 向量化技术，对热点函数 SHA-1 和 AES 函数进行了向量化操作，实现了 Office 口令的高效恢复，提高了口令恢复的性能。实验结果表明，相对于串行的口令恢复算法，该方法进一步发挥了申威众核平台的并行能力，增加了 Office 口令恢复算法的并行比例，提高了 Office 口令恢复程序的吞吐量，缓解了农业农村在大数据智能化应用的实际需求。下一步是将 Office 口令恢复算法移植到神威太湖之光，进一步提高口令恢复的性能。

参 考 文 献

[1] ZHAN X, HONG J. Study on GPU-based password recovery for MS Office2003 document[C]// 2012 7th International Conference on Computer Science & Education(ICCSE). IEEE, 2012: 517-520.

[2] LU H. Research on Office Ciphertic Crack Technology Based on CUDA Architecture [D]. Zhengzhou: PLA Information Engineering University, 2014.

[3] HONG J, CHEN Z, HU J. Analysis of encryption mechanism in Office 2013[C]// 2015 IEEE 9th International Conference on Anti-counterfeiting, Security, and Identification(ASID). IEEE, 2015: 29-32.

[4] LI J J. Research and Implementation of Document Password Recovery System [D]. Chengdu: University of Electronic Science and Technology, 2013.

[5] LI L P, ZHOU Q L, LI B. Method for implementing Office documentation in multi-core FPGA [J]. Small Microcomputer System, 2019, 40(5): 929-934.

[6] LI B, ZHOU Q L, SI X M. A new type of mixed beomabileon set recovery system [J]. Journal of Computer, 2018, 41(12): 2804-2822.

[7] LIU W, ZHENG L, ZHENG K, et al. Method of NSGA-II Parallel and Optimization Based on Nuclear Processor [J]. Computer Application Research, 2020, 37(1): 96-101.

[8] GU W J, SUN C, WANG B. Research and Application of Parallel Optimization of High Performance Computing Based on OpenAcc [J]. Computer Technology and Development, 2018, 28(4): 65-70.

[9] DONGARRA J. Report on the Sunway TaihuLight System. University of Tennessee Department of Electrical Engineering and Computer Science Tech: Report UT-EECS16-742[R]. 2016.

[10] MERRILL N. Better Not to Know? The SHA1 Collision & the Limits of Polemic Computation[C]// Proceedings of the 2017 Workshop on Computing Within Limits. 2017: 37-42.

[11] LI L, FANG J, JIANG J, et al. Efficient AES implementation on Sunway TaihuLight supercomputer: A systematic approach[J]. Journal of Parallel and Distributed Computing, 2020, 138: 178-189.

[12] CHEN D X, LIU X. Design and optimization of the light parallel program of Shenwei Taihu [M/OL]. 2017. http://www.nsccwx.cn.

[13] DONG W Q. Research and Implementation of Scalable Molecular Simulation Algorithm Based on Taihu Lake [D]. Changsha: Hunan University, 2018.

[14] GAO W, LI Y Y, SUN H H, et al. An improved control flow SIMD to quantization method [J]. Journal of Software, 2017, 28(8): 2046-2063.

[15] ZENG Q M. Research on the key technology of high-throughput rations based on ARMV8 [D]. Guangzhou: South China University of Technology, 2019.

[16] LI L, FANG J, JIANG J, et al. SW-AES: Accelerating AES Algorithm on the Sunway TaihuLight[C]// 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications(ISPA/IUCC). IEEE, 2017: 1204-1211.

LI Hui, born in 1978, Ph. D, lecturer. His main research interests include risk management and actuarial.