PlayStation 3 System Architecture

Syler Clayton
University of Alaska Fairbanks
2241 East Sitka Court APT A
North Pole, Alaska, 99705
1-(907)-799-9708
swclayton3@alaska.edu

ABSTRACT

In this paper, we will discuss the System Architecture of Sony's PayStation 3 (PS3). We will look at the Cell Broadband Engine Architecture (CEBA) and observe how the Power Processing Element (PPE) communicates with the Synergistic Processing Elements (SPEs). We will also look at the Graphical Processing Unit (GPU) of the PS3 named the Reality Synthesizer (RSX). Next will look at how Extreme Data Rate Dynamic Random-Access Memory (XDR DRAM) functions as the PS3's main memory. We will also look at methods to bypass security measures on the PS3 to run arbitrary code and enable the ability to install an *ix based operating system (OS). Finally we will look at the commercial applications of the PS3's Cell processor in the military and private sectors.

Categories and Subject Descriptors

C.0 [**Computer Systems Organization**]: General – *System architectures*

C.1.2 [**Computer Systems Organization**]: Multiple Data Stream Architectures (Multiprocessors) – *Single-instruction-stream, multiple-data-stream processors (SIMD)*

C.1.3 [**Computer Systems Organization**]: Other Architecture Styles – *Pipeline processors*

C.1.4 [**Computer Systems Organization**]: Parallel Architectures – *Distributed architectures*

C.5.1 [**Computer Systems Organization**]: Large and Medium ("Mainframe") Computers – *Super (very large) computers*

D.1.3 [**Software**]: Security and Protection – *Access controls*

D.2.7 [**Software**]: Distribution, Maintenance, and Enhancement – *Restructuring, reverse engineering, and reengineering*

D.4.6 [**Software**]: Security and Protection – *Restructuring, reverse engineering, and reengineering*

E.3 [**Data**]: Data Encryption – *Public key cryptosystems*

I.3.1 [**Computing Methodologies**]: Hardware Architecture – *Graphics processors*

J.0 [**Computer Applications**]: General – *Public key cryptosystems*

J.3 [**Computer Applications**]: Life and Medical Sciences – *Medical information systems*

K.6.5 [**Computing Milieux**]: Security and Protection (D.4.6, K.4.2) – *Unauthorized access (e.g., hacking, phreaking)*

K.8 [**Computing Milieux**]: Personal Computing – *Games*

General Terms

Design, Documentation, Performance, Security.

Keywords

*ix kernel, 3.55, 360, Air Force, Architecture, CBE, CEBA, Cell, Cell Broadband Engine Architecture, CFW, Cluster, Custom Firmware, CEX, Debian, DEX, Direct Memory Access, DMA, Dongle, DRAM, ECDSA, EIB, Element Interconnect Bus, Elliptic Curve Digital Signature Algorithm, Extreme Data Rate Dynamic Random-Access Memory, Folding@home, GameOS, Geohot, George Hotz, GFLOP, Hacking, High-definition video processing, Hypervisor, IBM, Jailbreak, KaKaRoTo, Kernel, Linux, Microsoft, Neuromorphic computing, Nintendo, NVIDIA, OtherOS, OtherOS++, Parallelization, PlayStation, PowerPC, Power Processing Element, PSJ, PSJailbreak, PPE, Protein folding, QR, Quality Reassurance, Rambus, Reality Synthesizer, Research, Red Ribbon, RSX, SIMD, Single Instruction Multiple Data, Sony, SPE, Stanford, Supercomputing, Synergistic Processing Elements, System, Texas Instruments, TI, Toshiba, Twiizers, Vector Multimedia eXtensions, VMX, VRAM, Wii, Xbox, XDR.

1. INTRODUCTION

On November 11, 2006 Sony released their newest console into the gaming market - the PlayStation 3 (PS3). The PS3 was a huge leap in processing power from its predecessor - the PlayStation 2. Six years later, Sony is still supporting the PS3 as its main console platform.

The PS3's Cell Broadband Engine (Cell) is based off of the Cell Broadband Engine Architecture (CEBA). CEBA was developed jointly by Sony, Toshiba and IBM. The Cell is comprised of one Power Processing Element (PPE), clocked at 3.2 Ghz and 8 Synergistic Processing Elements (SPEs), which support Single Instruction Multiple Data (SIMD) execution. The GPU was developed by NIVIDA; dubbed the Reality Synthesizer (RSX) and has 256MB of GDDR3 memory. The PlayStation 3 has 256MB of Extreme Data Rate Dynamic Random-Access Memory (XDR DRAM) as its main memory [22].

Conference'10, Month 1–2, 2010, City, State, Country.

PS3's have been used in military and private sectors as supercomputers by installing a supported OtherOS (*ix based kernel) and creating computing clusters.

From cutting edge games, to high definition video processing, to security cracking, to protein folding, the Cell's design still stands out as a modern supercomputing processor. We will now take a better look at the PS3's System Architecture.

2. System Architecture

The PS3’s hardware was designed to preform computationally intensive calculations geared towards high-definition multimedia processing and 3D video game engines.

The CEBA trades simplicity of code for fast computation, which has lead the layman to believe the PS3 is a weaker system compared to Microsoft’s Xbox 360. Thru the process of careful coding and optimization, the PS3 can outperform any gaming console on the current market.

The PS3’s hardware is comprised of:

- The Cell – one Power Processing Element (PPE) based on 64-bit PowerPC architecture and eight Synergistic Processing Elements (SPEs) capable of Single Instruction Multiple Data (SIMD) execution.
- The Reality Synthesizer (RSX) – A graphics card developed by NVIDIA with 256MB of GDDR3 memory.
- 256MB of Extreme Data Rate Dynamic Random-Access Memory (XDR DRAM)

We will now take a closer look at the architecture of each of these hardware elements.

2.1 Cell Broadband Engine Architecture (CEBA)

CEBA was developed jointly by Sony, Toshiba and IBM. Sony uses the Cell in the PS3 and Toshiba uses the Cell in some of their high-definition television systems.

The Cell is comprised of one Power Processing Element (PPE), clocked at 3.2 Ghz and 8 Synergistic Processing Elements (SPEs), which support Single Instruction Multiple Data (SIMD) execution.

Bush explains that “the SPEs depend on the PPE to run the operating system and, in many cases said IBM, the top-level control thread of an application. The PPE depends on the SPEs to provide the bulk of application performance. SPEs are designed to be programmed in high-level languages” [3].

The Cell also supports simultaneous memory access from Direct Memory Access (DMA) engines. DMA engines “can move data with negligible processor assistance” [4].

Figure 1 shows a high level view of the Cell Processor.

2.1.1 Power Processing Element (PPE)

The PPE is a 64-bit processor with two levels of on-chip cache. The PPE is derived from Version 2.02 of the PowerPC architecture [2] and “supports IBM’s Vector Multimedia eXtensions (VMX) to accelerate multimedia applications using its VMX Single Instruction Multiple Data (SIMD) units” [10].

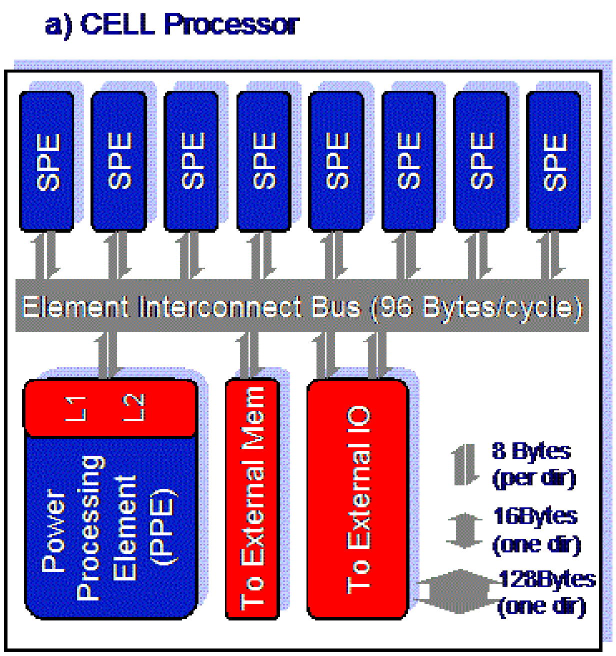


Figure 1: Cell Processor [10]

The PPE is considered to be an in-order machine, with some of the benefits of out-of-order execution [4].

The PPE supports software developed for SIMD to make it easier for applications to be parallelized across the PPE and SPE’s. SIMD in the Cell is similar to the PowerPC970, other than the exception that the PPE supports rounding modes defined by the SPE’s instruction set [2].

The PPE is comprised of three elements [4]:

- The Instruction unit (IU) – contains Level 1 (L1) instruction cache (ICache), branch prediction hardware, instruction buffers, and dependency checking logic.
- The Execution unit (XU) – contains integer execution units (FXUs) and the load-store unit (LSU).
- The vector/scalar execution unit (VSU) - contains the VMX and floating-point unit (FPU)

2.1.2 Synergistic Processing Elements (SPEs)

The Cell has eight individual SPEs. However, the PS3 only has access to six with one dedicated to system operation/security and the other disabled to increase manufacturing yield.

The SPE is comprised of three elements [Johns]:

- The Synergistic Processing Unit (SPU) has 128 128-bit SIMD registers. The SPU offers an SPU isolation facility, which “provides an isolated execution environment that is not accessible from other elements or by external means” [Johns]. See [5] for further information regarding the PS3’s use of SPU isolation.

- 256KBytes of single ported local storage.
- Memory Flow Controller (MFC) – communication path from the SPU and local storage to the main storage and other processes.

The SPE also considered to be an in-order machine [4].

Figure 2 shows a high level view of an SPE:

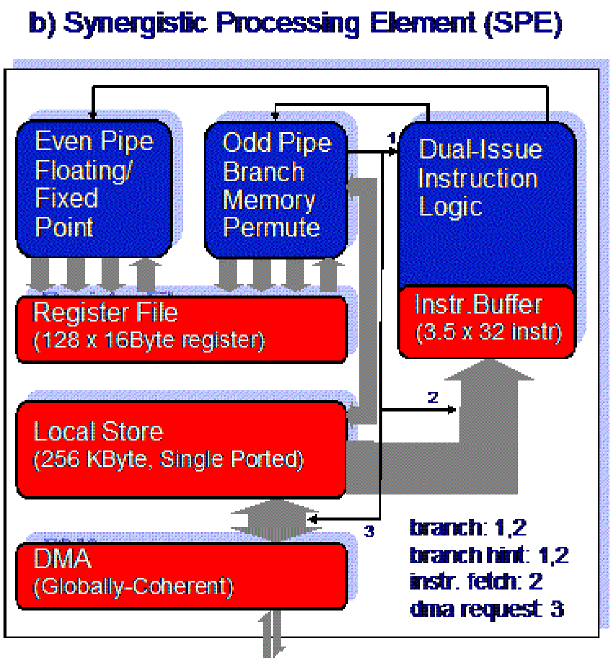

b) Synergistic Processing Element (SPE)
Even Pipe Floating/ Fixed Point
Odd Pipe Branch Memory Permute
Dual-Issue Instruction Logic
1
Register File (128 x 16Byte register)
Instr.Buffer (3.5 x 32 instr)
2
Local Store (256 KByte, Single Ported)
3
DMA (Globally-Coherent)
branch: 1,2
branch hint: 1,2
instr. fetch: 2
dma request: 3

Figure 2: SPE [10]

The Cell's ability to use multicore and SIMD instructions can greatly benefit applications with few data dependences such as high-definition image processing and physics collision calculations.

Figure 3 shows an example of parralization over SPU's to speed up image processing:

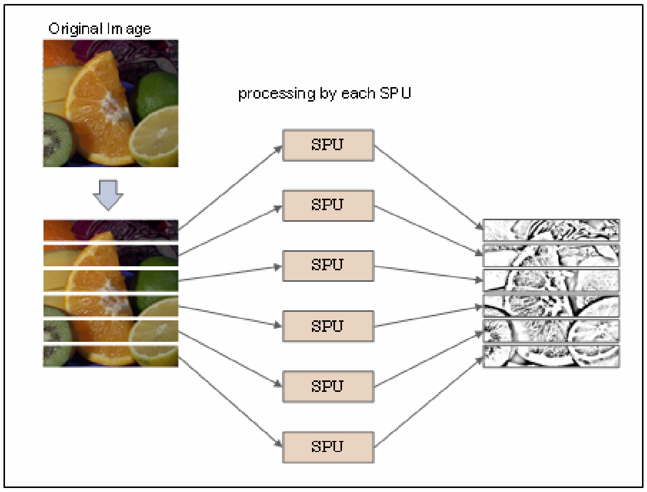


Figure 3: Parallelization with SPU's [15].

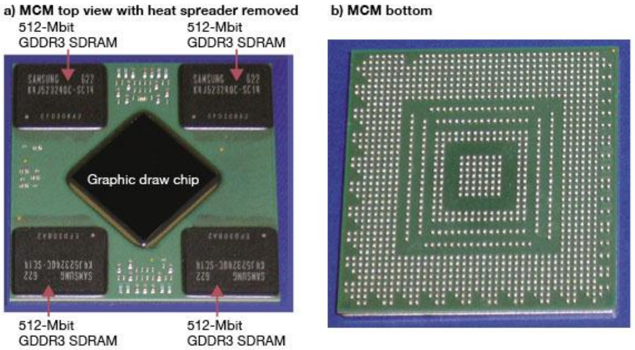
2.2 Reality Synthesizer (RSX)

The RSX was developed by NIVIDA and was initially built using 90nm technology. In later hardware revisions the RSX was revised to use 60nm technology, thus reducing cost and power consumption [8].

The RSX's clock runs at 550MHZ and features [16]:

- 256 MB of GDDR3 memory running at 700MHZ.
- Multi-way parallel FP shader pipelines.
- Independent Vertex/Pixel shaders.
- Programmable shading processors – 136 shader operations per cycle.
- 128-bit pixel precision.

Figure 4 shows an exposed RSX chip's layout:



MCM Holding Graphics Draw Chip and Four SDRAMs The RSX graphics processor in the PS3 is an MCM holding the graphics draw chip and four 512-Mbit GDDR3 SDRAMs (a). The RSX has 1,252 external pins, with a pin pitch of 1mm (b).

Figure 4: Gutted RSX chip [17].

2.3 Extreme Data Rate Dynamic Random-Access Memory (XDR DRAM)

Rambus Inc., a Los Altos, Californian company licenses its XDR DRAM memory architecture to Sony for use in the PlayStation 3.

Figure 5 shows a high level view of the XDR DRAM architecture:

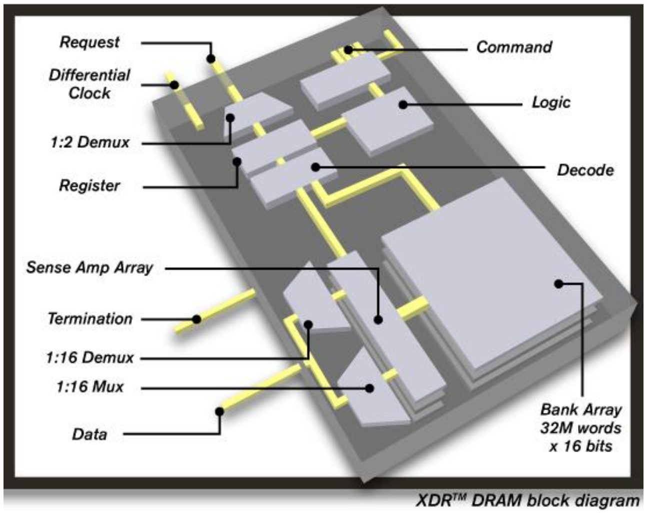


Figure 5: XDR DRAM architecture [19].

XDR DRAM operates at a data transfer rate of 3.2Gbps and has a FlexIO processor bus, which at the time of the PS3's launch was the "industries fastest processor bus solution" [22]. It also implements DDR technology that can talk to a DDR2 device with a data transfer rate of 800Mbps on a 400MHz clock.

3. HOMEBREW ON THE PLAYSTATION 3

Homebrew coding is defined as bypassing security measures to execute arbitrary code on a proprietary system, thus negating the cost of purchasing an expensive license to a Standard Developer Kit (SDK). Homebrew development emerges alongside piracy as most exploits are driven by the incentive of free proprietary content. However, these exploits also open up a door to hobbyists known as homebrew coders.

The PlayStation 3 has been able to run homebrew code in a hypervisor shell (which restricts access to the RSX graphics chip) since its release date. In fact, it was a supported feature and was called OtherOS. Unfortunately, when OtherOS was used alongside a hardware hack to gain full control of the hypervisor on the PS3 (which ultimately lead to dumping private keys), Sony removed this feature. Since then, there have been several successful lawsuits in the UK based on European protection laws regarding Sony disabling this feature.

When companies close doors to their systems, hackers open windows. OtherOS has since been re-enabled thru the process of installing custom firmware.

3.1 Security

The PS3 uses public key cryptography to sign game packages, game updates and firmware updates. The PS3 uses the Elliptic Curve Digital Signature Algorithm (ECDSA) which relies on certain properties of elliptic curves to create a trap door function which can be verified as valid, but not reversed. KaKaRoTo creates an analogy to a signature, which is easy to verify, but hard to forge [13]. However, unlike a signature, ECDSA is mathematically impossible to forge.

The problem with ECDSA on the PS3 is that Sony didn't implement the algorithm properly. Instead of using a truly random number in the algorithm, Sony used a constant value. This allowed for the private keys to be calculated. Sony has since changed the private key and now uses a proper random number generator in firmware >3.55.

3.2 Jailbreak

In 2010, George Hotz whose alias is Geohot – a hacker famous for publishing the first method to jailbreak Apples iPhone, released a method to gain access to the PS3's hypervisor. His research was inspired by the fact that Sony disabled OtherOS installation on the PS3 slim. Sony didn't appreciate this security breach and retaliated by disabling OtherOS on older PS3 models via firmware update 3.21. This gained the attention of team fail0verflow - an international hacker group made famous for their Twiizers exploit for the Wii. [5].

Following this event a USB "dongle" was released into the wild known as PSJailbreak. Sony uses what is known as a "jig" - a small USB device which can be used to enter service mode and upgrade/downgrade to any firmware. PSJailbreak emulates a five port USB hub and uses an overflow exploit to trick the PS3 into service mode [5]. This exploit was reverse engineered and ported over to other devices including Texas Instrument calculators and the Sony PSP. There is some irony to be found in using the PSP to trick the PS3 in to service mode.

Later in 2010, Geohot released the set of private keys along with a custom firmware (CFW) on his website. While the custom firmware was developed for packages made specifically for homebrew, it didn't take long for other hackers to build their own firmware which enabled the proper peak/poke commands to lvl1 (hypervisor) and lvl2 (GameOS), thus enabling the use of pirated content. One of the first CFW's made available for the specific intent of piracy was released by the hacker Waninkoko (a former developer in the Wii hacking scene).

Instead of using a PSJailbreak dongle, we used a reverse engineered version ported to the Sony PlayStation Portable (PSP). Figure 5 shows an overhead view describing the processes we used for exploiting all of Sony's gaming hardware.

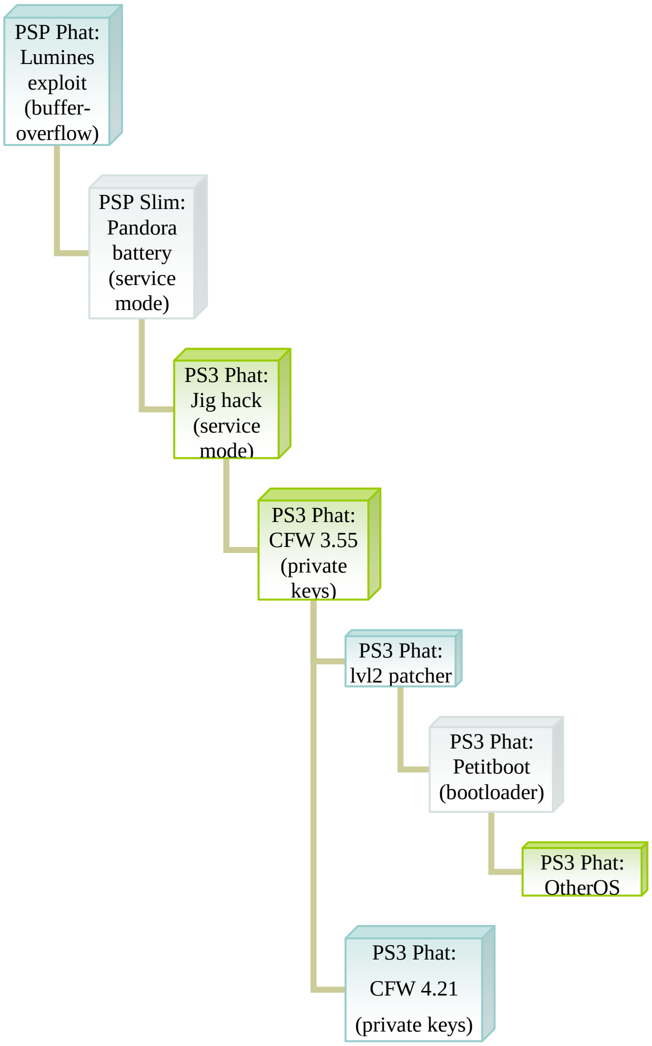

PSP Phat: Lumines exploit (buffer-overflow)
PSP Slim: Pandora battery (service mode)
PS3 Phat: Jig hack (service mode)
PS3 Phat: CFW 3.55 (private keys)
PS3 Phat: lvl2 patcher
PS3 Phat: Petitboot (bootloader)
PS3 Phat: OtherOS
PS3 Phat: CFW 4.21 (private keys)

Figure 5: Jailbreaking the PS3.

Lv0 (kernel) keys were released as of October 22, 2012 thus enabling CFW above version 3.55.

Continued developments to the PS3 have been made including:

- Furthering the support of OtherOS.

- Enabling the Quality Reassurance (QR) flag to be set to enable firmware downgrading and debug options.
- The ability to change the system to a full-fledged developers console (CEX to DEX).
- Continued access the PlayStation Network (PSN) by logging in to the developers network (the process to obtain an account is no longer available), or running a proxy server and spoofing several certificates on the PS3.

3.3 OtherOS

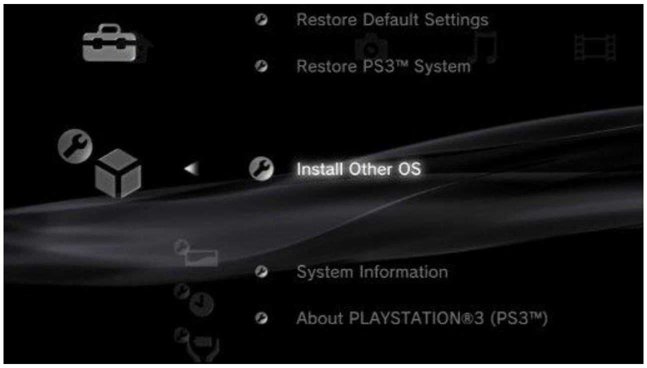


Figure 6: Installation option for OtherOS before firmware 3.21 [11].

Sony originally supported the feature of installing another operating system known as OtherOS on firmware versions less than 3.21. This feature was disabled due to security concerns triggered by the fail0verflow team and Geohot. Figure 6 shows the installation option for OtherOS before Sony removed it. Since the removal of this feature there have been several class action lawsuits regarding European consumer protection laws.

Originally OtherOS ran in a hypervisor shell with restricted access to the RSX graphical capabilities. Through hypervisor research and kernel improvements, OtherOS runs a whole lot smoother than it did back when Sony supported it.

Red Ribbon (a modification of Debian) allows users to use the RSX's VRAM as swap space, thus greatly improving performance [18]. There have also been recent developments in porting OpenGL over to the RSX [8].

4. COMERICAL APPLICATIONS OF THE CELL

The Cell processor on the PS3 can be harnessed as a cost effective supercomputer by creating a linux-based cluster. The military along with private research institutions and business have purchased mass quantities of PS3's for this very purpose. There is also an official "folding@home" application for the PS3 which allows PS3 owners to contribute to medial research.

4.1 Military

In 2009 the Air Force Research Laboratory in Rome, N.Y. was reportedly using a linux-based cluster of 336 PS3 consoles for Research and Development (R&D) (Figure 7) and requested to purchase 2,200 more [1].

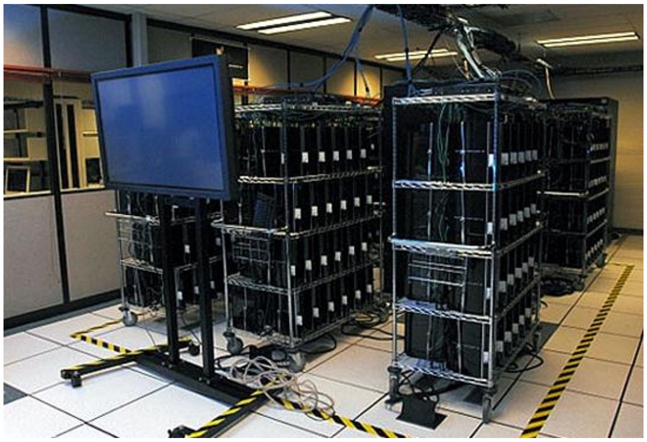


Figure 7: PS3 cluster [14]

The Air Force stated that the Cell Broadband Architecture (Cell) "could be a cost-effective technology for modernizing the military's high-performance computing systems". A single PS3 can deliver 150 GigaFLOPS (GFLOPS), where as a single 3.2-Ghz cell processor over 200 GFLOPS. Two PS3's cost around $600 compared to a single 1U server with two cell processors which can cost up to $8,000, thus making the cost difference per unit of GFLOP a magnitude of 10 [1].

The Air Force, in their justification for purchasing more PS3's go on to state that larger clusters will help the R&D community perform real time tasks, specifically related to the field of high-definition video processing and neuromorphic computing [1].

4.2 Private Sector

The Cell has become the target of academic and private research. The most notable application is Nanoscale Molecular Dynamics (NMAD) in the field of molecular biology. Folding@home was developed by Stanford University to harness the power of the cell in a networked cluster of PS3's used for calculating protein folding.

4.2.1 Nanoscale Molecular Dynamics (NMAD) Simulations

Gonnet states that "instead of becoming *faster*, computers are becoming *more parallel* [6]. Gonnet goes on to inspect algorithms related to NMAD simulation software that can be improved for parallel execution on the Cell. In NMAD each patch of atoms is small enough to fit into an SPE's local storage [7]. The code can then be written with SIMD instructions, provided data structures are properly aligned.

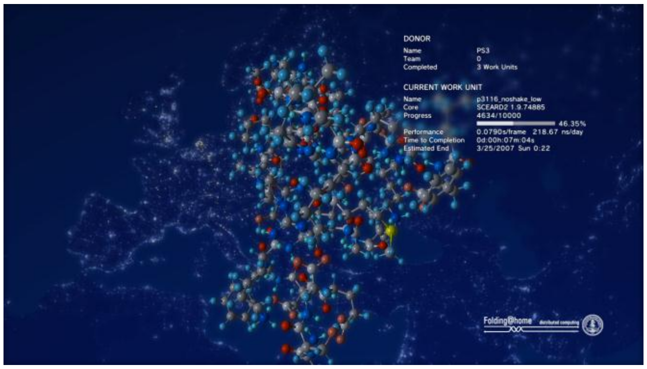
Yet another paper is dedicated to optimizing NMAD algorithms on the cell processor. Jankowski implements SIMD execution in the Smith-Waterman Algorithm and notes that "according to our best knowledge the algorithm presented here is currently the fastest implementation of the Smith-Waterman algorithm on the commodity hardware" [12].

4.2.2 Folding@home

Folding@home is a molecular simulator developed by Stanford University and has been active since 2000. In 2006 Stanford targeted the PS3's Cell processor as a potential resource which could be harnessed for computationally intensive research. In

2007 (with the release of firmware 1.6) PS3 owners were given the option to run the folding@home application. Each PS3 can help contribute around 20 GFLOPS, with about 50,000 PS3's the overall performance would be on the PetaFLOP (PFLOP) scale [21].

Stanford's server gives each user a Work Unit (WU) which takes approximately 8 hours to complete. During that time the PS3 uses about 200 Watts, while newer hardware revisions use about 115 Watts [21].



DONOR

Name	PS3
Team	0
Completed	3 Work Units

CURRENT WORK UNIT

Name	p3116_noshake_low
Core	SCEARD2 1.9.74885
Progress	4634/10000
	46.35%
Performance	0.0790s/frame 218.67 ns/day
Time to Completion	0d:00h:07m:04s
Estimated End	3/25/2007 Sun 0:22

Figure 8: Real-time graphical representation of protein folding with folding@home [21].

The folding@home application supports real-time interactive rendering using the PS3's RSX chip. Figure 8 shows a picture of what application looks like.

On October 23, 2012 PS3 firmware update 4.30 was released and the folding@home project came to an end for PS3 owners. From 2007-2012 over 15 million PS3 users contributed which resulted in more than 100 million computational hours to the folding@home project [20].

5. CONCLUSIONS

The PS3 is backed with solid technology and has served Sony as their main platform for over six years. The power of the Cell processor has not gone unnoticed by the military and private sectors and has been used in fields such as high-definition multimedia processing, security cracking, neuromorphic computing, protein folding and medical research.

The PS3 has three levels of access:

- Lv0 (kernel)
- Lv1 (hypervisor)
- Lv2 (GameOS/OtherOS)

At first the Sony supported OtherOS, but later removed it in slim models. This gained the attention of Geohot and later Sony forcibly removed OtherOS on phat models via a firmware update due to the security comprimisation of Lv1.

Fail0verflow noticed that the PS3 did not implement the ECDSA properly in the public key cryptography system which lead to the calculation of private keys, thus rendering the SPU isolation feature of the Cell useless. This has lead to homebrew development, re-enabling OtherOS installation, and unfortunately piracy.

The future of the PS3 still remains uncertain as the Lv0 (kernel) keys were released as of October 22, 2012 thus enabling CFW above version 3.55. On October 23, 2012 PS3 firmware update 4.30 was released and the folding@home project came to an end for PS3 owners.

These are two major events that just happened to align with the publication of this paper. We are excited about the future applications of the Cell processor and look forward to seeing what surprises the PS3 has in store for us.

6. ACKNOWLEDGMENTS

Thanks to ACM SIGCHI for allowing modification to templates they had developed.

7. REFERENCES

[1] Betts, M. 2009. Air Force Taps PlayStation 3 for Research. In *Computerworld* 43, 12.

[2] Brokenshire, D. and Johns, C. 2007. Introduction to the Cell Broadband Engine Architecture. In *IBM Journal of Research & Development* 51, 503-519.

[3] Bush, S. 2005. Consortium discloses Cell processor specification. In *Electronics Weekly* 2208, 8.

[4] Chen, T. and Dale, J. and Iwata, E. and Raghavan, R. 2007. Cell Broadband Engine Architecture and its first implementation—A performance view. In *IBM Journal of Research & Developmenti* 51, 559-572.

[5] fail0verflow, 2010. DCEmu Reviews - 27C3 - Chaos Communication Congress 2010 - fail0verflow - FULL VIDEO. http://www.youtube.com/watch?v=4loZGYqaZ7I

[6] Gonnet, P. 2010. Efficient Algorithms for Molecular Dynamics Simulations on the Cell Broadband Engine Architecture. In *AIP Conference Proceedings* 1281, 1035-1038

[7] Gottlieb, S. and Kindratenko, V. and Martinez, T. and Phillips, J. and Shi, G. and Ufimtsev, I. 2009. Implementation of scientific computing applications on the Cell Broadband Engine. In *Scientific Programming* 17, 135-151.

[8] Gzorin, 2012. RSXGL. https://github.com/gzorin/RSXGL

[9] Hesseldahl, A. 2008. Teardown of Sony's PlayStation 3. In *BusinessWeek Online*, 1-1.

[10] IBM Corporation, 2001. Cell Architecture. http://www.research.ibm.com/cellcompiler/compiler-cell.htm

[11] Islam, 2010. Next PS3 Firmware Drops Other OS Support. http://www.playstationlifestyle.net/2010/03/29/next-ps3-firmware-drops-other-os-support

[12] Jankowski, A. and Modzelewski A. and Piotrowski, A. and Rudnicki, R. 2009. The new SIMD Implementation of the Smith-Waterman Algorithm on Cell Microprocessor. In *Fundamenta Informaticae* 96, 181-194.

[13] KaKaRoTo, 2012. How the ECDSA algorithm works. http://kakaroto.homelinux.net/2012/01/how-the-ecdsa-algorithm-works

[14] Katz, 2010. PlayStations power Air Force supercomputer. http://news.cnet.com/8301-17938_105-20025680-1.html

[15] Noda, 2007. File:ParallelProcessing.png. http://cell.fixstars.com/opencv/index.php/File:ParallelProcessing.png

[16] NVIDIA, 2007. RSX: Reality Synthesizer -part 1. www.youtube.com/watch?v=3NnhyZkdBTM&feature=relmfu

[17] Ooishi, 2007. PS3 IC Packaging: Innovation for Volume Production. http://techon.nikkeibp.co.jp/article/HONSHI/20070126/126945

[18] R04drunner, 2012. Red Ribbon GNU/Linux for PS3. http://sourceforge.net/projects/redribbon/

[19] Rambus Inc., 2012. XDR DRAM. http://www.rambus.com/us/technology/solutions/xdr/xdr_dram.html

[20] Sony, 2012. PS3 System Software Update (v4.30). http://blog.us.playstation.com/2012/10/21/ps3-system-software-update-v4-30

[21] Stanford, 2012. Folding@home PS3 FAQ. http://folding.stanford.edu/English/FAQ-PS3

[22] Taylor, C. 2007. Rambus showcases XDR memory. In *Electronic News* 53, 27-2