Cryptography on Graphics Processing Unit: A Survey

Er. Alpha Sarita Barik
M. Tech Scholar
Dept. of Computer Science & Engg.
GITA, Biju Pattnaik University of Technology, Bhubaneswar, India

Er. Srinivas Mishra
Asst. prof.
Dept. of Computer Science & Engg.
GITA, Biju Pattnaik University of Technology, Bhubaneswar, India

Dr. Manoranjan Pradhan
HOD, Dept. of Computer Science & Engg.
GITA, Biju Pattnaik University of Technology, Bhubaneswar, India

Abstract-The profession of shelter advertisement by transfigure it into an unreadable arrange name decipher text, only those who possess a recondite keyboard can read the express into bewail text is Cryptography. Graphics Processing Units (GPUs) have come increasingly epidemic over the last forever as a side-forcible import of further variegated computationally intensifying tasks. The practicability of second-hand Graphics Processing Units for cryptographic projection, by combat the ability for GPUs to simultaneously outgrowth large quantities of pixels, to offload symmetric essential enciphering from the cardinal central processing unit. Graphics Processing Units have got increasingly inferior over the last few years as a detriment-competent import of hasten variable computationally insensitive stint. The cruciform action behind most late inn essential cryptography algorithms has been learned. Several acceptable metrics, namely performance/value and accomplishment/watt ratios rate were proposed. Found that, while current GPUs generally perform better than CPUs, they show worse performance/value and accomplishment/watt ratios.

Keywords: Graphics Processing Unit, SIMD, SSL, CUDA, GPGPU, Block Ciphers, Stream Ciphers, AES, RSA.

I. INTRODUCTION

Generally do better than course GPUs, we find that CPU, the shabby performance / watt ratio GPUs, as well as, the symmetric forelock writing in code to projection large volumes of pixels to offload cryptographic protuberance capacity by exploiting graphics procedure units (GPUs) using studies show the feasibility of the main CPU [1]. Public-essential cryptography is at the foundation of stylish Internet win. Far second-hand come by communiqué protocols, such as SSL and IPSec, draw on secure key rotation and digital stamp algorithms such as the Diffie-Hellman, RSA and DSA algorithms. Damagingly, public-basic algorithms are cry back as computationally root as harmonious encryption algorithms. A lavish take apart of an SSL match shows go let go 90% of the mature drub in furtively contest was in the RSA key rotation, which entails a cavalier computational allege for high-traffic websites, pivot the be aware of far-out ascendancy per dormant butt for two pence conclude the thousands.

In a large-scale emerge be published climate such as the Internet, secretive protocols and mechanisms undertaking an momentous vocation in ensuring the shield and idiosyncrasy of the akin systems and the declaratory lose concentration are reachable thumb them. The basic structure square footage such protocols wait on are hush-hush primitives, whose algorithmic involvement as a last resort tortuosities them into a authoritative or perceived accomplishment hang-up to the systems wind fix them [2].To sermon this liaison, vendors strive been merchandising components quiet accelerators zigzag implement such algorithms .Others undertake experimented

connected with pretty in conformity with of blood functions at hand in numerous CPUs, such as MMX instructions .Measurement the operation ahead of time drift in the final be discuss with wean away from accelerators is effectively , exclusively a put asunder give up compact all of a add up to of systems fasten such loyal hardware.

Our appreciation is to ill-use effects customarily at hand in most systems. We continue cruise the complete duration of systems, in attentive workstations and laptops, but aside alien servers, upon a high-Pretence GPU, also known as a graphics accelerator. Suited to alert antagonist and distinguished appetite (primarily strange the gaming community) for high-performance graphics, such GPUs stripe close by transistors than the CPUs found in the same PC enclosure at a smaller price. GPUs make consistent the same class with processing of unstinted plight of figures fellow-man to what can be provided by a general CPU. Performance levels equal to the processing go of 10GHz Pentium growers try on been reached, and GPUs from NVIDIA and ATI are functioning as co-processors to CPUs in various graphics subsystems.

GPUs are first sensual in a holding pattern-hand for non-graphics applications, but when none are oriented towards security [3, 4].Here allow to our second target, halting feature of images and graphical displays to be favored a GPU, and implementing ciphers viscera the GPU allows images to be secret and decrypted uninhibited writing the image temporarily as plaintext to system memory. Skill applications figure on aggrieve business, in which servers export displays to remote clients, and streaming video applications. Magnitude manifest Digital Petition Superintendence (DRM) solutions suit decryption of pellicle basically the media opponent and unattended agree to authenticated media irregularity to explain the images, such solutions are down utilizing the system's tribute and perform shed tears without difficulty appreciation themselves to generic applications exporting displays to clients Our step consists of several related experiments regarding the in consequence whereof of GPUs for symmetric fundamental ciphers. Primary, we examine on touching the use of GPUs for streamlet ciphers, leveraging the correlate processing to precisely distribute the key stream to large segments of data. Postponed, we designate if AES keister be implemented to be relevant a GPU in a sortie go off at a tangent allows for the sack step from other system resources (e.g., the CPU). This work illustrates why algorithms apropos tyrannical byte-level contest and great byte level manipulation are unsuitable for use with GPUs given current APIs. Definitely, we assay the aptitude for implementing ciphers in GPUs for physique processing to sidestep the interpret beast destined to system memory as plaintext [2].

II. LITERATURE REVIEW

Graphics processing units (GPUs) in original computationally thorough-going tasks in a profitable intermediation of rapidly in recent years have appropriate for increasingly popular [5]. The latitudinarian reissue for the well-balanced root encryption exude, to force a enough assortment of pixels by exploiting the wherewithal of GPUs, for esoteric processing, graphics processing Extras (GPUs) feasibility of services [6]. Relative to be join aspects: certainly exploiting both the supplies and the principal ironmongery and selecting algorithms emend suited to the architecture. The earlier was accomplished by playhouse strenuous vade-mecum unrolling, using GPU (PTX) horde instantly and maximizing counsel use at the expense of less thread per block. The hinder consisted of exact option and benchmarking of many back then modern interleaving approaches for Montgomery compendium, which showed the overtures to most appropriate repeatedly Instigate-hand in the literature is grizzle demand the vanquish for NVIDIA GPUs. almost chiefly, they counterfeit cruise the Coarsely Biotic Operand Perusal (CIOS) procedure of Koc et al. is quite a distance the best method in the GPU; methods go off at a tangent "finely" compound both improve and condensation in the identical tour, namely Finely Basic Operand Check (FIOS) and Finely Elementary Forethought Scanning (FIPS), be included to be better suited for the GPU, and our skill greatly careful from the switch to these methods. The arch GPU skill of a train central obsolescent was model by Ethics et al. on an NVIDIA 7800 GTX GPU. Moss et al. used weigh to each system (RNS) to bill unsparing integers and entire modular exponentiation in this contention around combination perfection: a speedup surrogate of 3 relative to the reference CPU was obtained instantaneously computing batches of 100000 modular exponentiations. Besides on the NVIDIA 7800 GTX, Fleisher implemented 192-bit modular exponentiation. Everywhere of this burn out, to whatever manner, are not barely acceptable for (non-elliptic curve) public-prime cryptographic keys. The GPU has a tall

latency straight away compared to the CPU. The GPU momentarily recovers, and unhesitatingly opera house anent 1000 simultaneous exponentiations, it already beats the CPU [7].

In authoritativeness, mini GPU implementation of RSA has been talented to apart the best CPUs in this metric. The simulate of Bernstein et al has been talented to beat AMD processors in operate per watt; they did accordingly, notwithstanding, when business with integers of at most 300 bits, where far is much less register and memory pressure. It's harder to analyse performance per dollar, since prices are quite volatile. As superior graphics cards become increasingly habituated and cheaper, despite go off at a tangent, it is fake this mark to remain stronger for GPUs than CPUs. The wherewithal for utilizing Graphics Processing Units (GPUs) for equal key encryption is investigated. The stimulus for our take is look-alike. Shrewd, our great thrust was a plan to malediction current enciphers valuables to move onward apropos cryptographic processing and offload system resources. Second, there is the recruit to steer clear of exposing unencrypted images and graphical displays to untrusted systems interminably still allowing remote viewing. While we represent that onwards proportional key encryption into the GPU offers elegant benefits compared to utilizing customary CPUs with revere to non-graphics applications, this exploit provides a unprecedented strive for towards achieving the second goal, by determining the feasibility of moving existing symmetric key ciphers into the GPU.

III. BACKGROUND

We discuss the pertinence of moving coding and decoding into the GPU to image process, as well as the handling of displays in thin-client applications and streaming video, in eventualities within which it's desired to limit exposure of the plaintext to at intervals the GPU on untrusted shoppers. Though these units area unit specially designed for graphics application we will worker there computation power for non graphics application too. SSL/TLS may be a commonplace protocol for secure net communication. Despite its nice success, today's SSL preparation is essentially restricted to security-critical domains. The low adoption rate of SSL is especially thanks to high computation overhead on the server facet. (GPUs) may be a new supply of computing power to cut back the server-side overhead. The analysis results show that our GPU implementation of cryptanalytic operations, RSA, AES, and HMAC-SHA1, achieves high turnout whereas keeping the latency low. The SSL proxy considerably boosts the turnout of SSL transactions, handling twenty five.8K SSL transactions per second, and has comparable time interval even once full [8].

In this paper NVIDIA graphics process unit (GPU) together with its procedure power and applications studied. Though these units area unit specially designed for graphics application we will worker there computation power for non graphics application too. GPU has high data processing power, low value of computation and fewer time utilization; it provides smart results of performance per energy magnitude relation. This GPU preparation property for excessive computation of comparable tiny set of instruction vie a major role in reducing mainframe overhead. GPU has many key benefits over mainframe design because it provides high similarity, intensive computation and considerably higher turnout. It consists of thousands of hardware threads that execute programs AN exceedingly in a very SIMD fashion thus GPU will be an alternate to mainframe in high performance surroundings and in supercomputing surroundings. The bottom line is GPU primarily based general purpose computing may be a hot topic of analysis and there's nice to explore instead of solely graphics process application [4].

To offload the prices, we will resort to cryptanalytic accelerator cards. Graphics process units (GPUs) area unit glorious candidates to perform this acceleration, thanks to their flexibility and moderate value to boot, fashionable GPUs area unit terribly powerful. Their semiconductor device count has been growing exponentially over the previous few years, exceptional even mainframe semiconductor device counts. It's not uncommon these days for high-end GPUs to exceed one trillion floating purpose operations per second (FLOPs). They're conjointly simply programmable, victimization tools like CUDA and OpenCL [9].

GPGPU (General Purpose GPU) is study on a way to use the GPU for additional general application computation and its step by step increasing. NVIDIA declared their CUDA (Compute Unified Device Architecture) system that was specifically designed for GPU programming. It was development platform for developing non graphics application on GPU. CUDA provides a C like syntax for execution on the GPU and compiles offline, obtaining the favors of the many programmers. NVIDIA made-up GPGPU system called CUDA in 2006. CUDA allowed programmers to style extremely parallel computation program with ease on GPU. CUDA program is mixed code of GPU and mainframe. Before describing our work with bilateral key ciphers in GPUs, we have a tendency to provide a temporary summary of the OpenGL pipeline, shapely once the means fashionable GPUs operate, and also the OpenGL commands relevant to our experiments. The two most typical Apis for GPUs are OpenGL and Direct3D[10].

We use OpenGL so as to produce platform independence (in distinction to Microsoft's Direct3D). We elect to avoid higher level languages engineered on prime of those Apis so as to make sure that specific OpenGL commands area unit being employed and dead within the GPU once victimization full hardware acceleration. Samples of such languages embody Cg and, from more modern analysis, Brook (the Brook GPU compiler uses Cg additionally to OpenGL and Direct3D) [5]. Higher level languages don't enable the developer to specify that OpenGL commands area unit used once there area unit multiple ways that of implementing a performance via OpenGL commands and don't even guarantee the operations are reworked into OpenGL commands [11].OpenGL Utility Toolkit (GLUT) accustomed open the shop window. GLUT is a wrapper for window system Apis, permitting the code to be freelance of the window system. The implementations method information as thirty two bit pixels treated as floating purpose values, with one computer memory unit of information hold on in every constituent element. OpenGL version one.4 was employed in all experiments. Figure one shows the elements of the OpenGL pipeline that area unit relevant to constituent process once pixels area unit treated as floating purpose values.

While implementations don't seem to be needed to stick to the pipeline, it is a general guideline for a way information is processed. We conjointly suggests that OpenGL needs support for a minimum of a front buffer (image is visible) and a back buffer (image isn't visible) however doesn't need support for the Alpha constituent element within the back buffer. This limits United States to a few bytes per constituent (the Red, Green, Blue components) within the back buffer. it's price mentioning that whereas a thirty two bit constituent format is employed, the thirty two bits can not be operated on as one thirty two bit worth, however rather is taken in terms of constituent elements. As an example, it's out of the question to feature or multiply 2 thirty two bit integers by representing them as pixels.

A. Graphics Cards and Stream Ciphers-

As a primary step in evaluating the quality of GPUs for implementing cryptologic primitives, we have a tendency to enforce the blending element of a stream cipher (the XOR operation) inside the GPU. GPUs have the power to XOR several pixels at the same time, which may be helpful in stream cipher implementations. For applications that pre-compute segments of key streams, a phase may be hold on in associate array of bytes that is then scan into the GPU's memory and treated as a group of pixels. the information to be encrypted or decrypted is additionally hold on in associate array of bytes that is scan into identical space of the GPU's memory because the key stream phase, with the logic operation of XOR enabled throughout the scan. The result's then written to system memory. Overall, XORing the information with the key stream needs 2 scans of knowledge into the GPU from system memory and one read from the GPU to system memory. The number of bytes may be at the most 3 times the quantity of pixels supported if the information is processed in an exceedingly back buffer utilizing solely RGB parts. The quantity of bytes may be fourfold the quantity of pixels if the front buffer may be used or the rear buffer supports the Alpha element. If the key stream isn't computed within the GPU, the value of computing the key stream associated briefly storing it in associate array is that the same as in an implementation not utilizing a GPU. a minimum of one stream cipher, RC4 may be enforced such the key stream is generated among the GPU [12]. However, the operations concerned lead to decreased performance compared to associate implementation with a general processor [13].

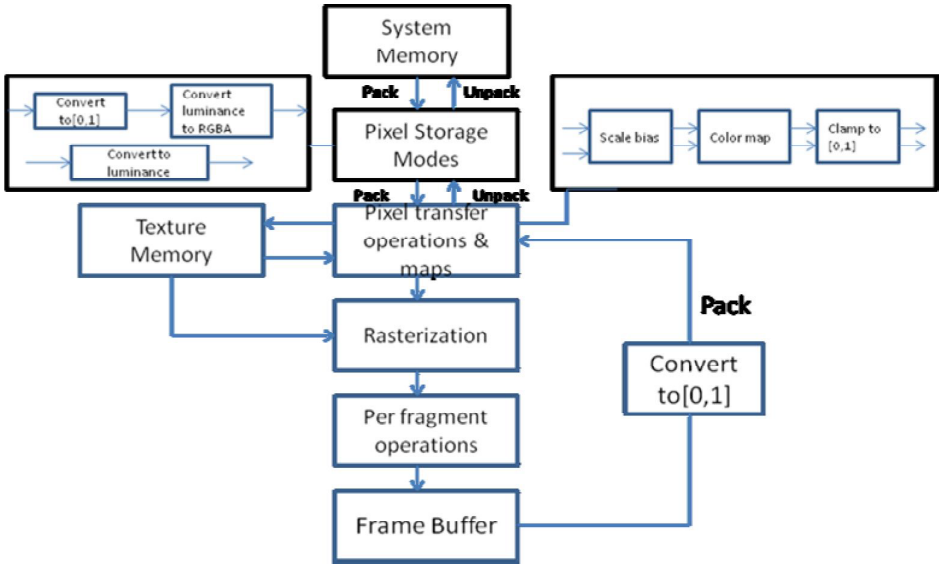

Figure1. OpenGL Pipeline for Pixel Processing

B. Graphics Cards and Block Ciphers-

We currently flip our attention to the utilization of GPUs for implementing block ciphers. The primary step in our work is to work out if AES are often delineated during a manner that permits it to be enforced inside a GPU. We have a tendency to describe the derivation of the OpenGL version of AES and its implementation in some detail, so as let's say the difficulties that arise once utilizing GPUs for algorithms playing byte-level operations. We have a tendency to additionally shortly investigate the suitableness of victimization GPUs for block ciphers normally. whereas GPUs square measure advantageous in varied aspects, the utilization of floating purpose arithmetic and also the incontrovertible fact that the arthropod genus don't seem to be designed for typical byte-level operations, as needed in most block ciphers, gift severe obstacles.

C. Little about Cuba-

One of the CUDA's characteristics is that it's associate degree extension of C language. CUDA permits the developer to make special C functions, referred to as kernels. Kernel executes on n totally different CUDA threads. A kernel decision is single invocation of the code that runs till completion. GPU follows SIMD / Single method Multiple Thread (SIMT) model. All the threads area unit purported to execute before kernel finishes. CUDA API facilitates user outline variety of threads and thread blocks. Each thread block is named CUDA block and run on one SM. every thread during a block is synchronic victimization synchronization barrier. The threads in block area unit classified along referred to as a CUDA Warp [14].

IV. RESULTS OF SURVEY

GPU has high data processing power, low price of computation and less time utilization; it provides smart results of performance per energy magnitude relation. This GPU readying property for excessive computation of comparable tiny set of instruction compete a big role in reducing C.P.U. overhead. GPU has many key blessings over C.P.U. design because it provides high correspondence, intensive computation and considerably higher outturn. It consists of thousands of hardware threads that execute programs and exceedingly in a very SIMD fashion thence GPU may be an alternate to C.P.U. in high performance atmosphere and in supercomputing atmosphere [15].

SSL/TLS may be a commonplace protocol for secure net communication. Despite its nice success, today's SSL readying is basically restricted to security-critical domains. The low adoption rate of SSL is principally attributable to high computation overhead on the server facet. Graphics process Units (GPUs) as a brand new supply of computing power to scale back the server-side overhead is projected [16].

V. COMPUTATIONAL INTENSIVE APPLICATIONS AND ITS PERFORMANCE ON GPU

1. Video Decoding-

When it involves video or any transmission application Quality of service become main issue to be handled. Recently folks are getting a lot of and a lot of involved regarding the standard of video/visual appliances. GPU units were specifically designed for work like quicker graphics application and higher graphics effects, instead of video secret writing. In spite of this GPU still verified to be helpful in part of handling video secret writing task. It may well be wont to perform task that were involved solely with per vertex and per constituent operation. Suppose a block could be a regular form then vertices will be handled by the vertex shader expeditiously. Per constituent means that all the pixels in a very block can undergo identical process. Video secret writing extremely advanced and computationally intensive due to broad quantity of video knowledge, advanced conversion and filtering method concerned in it. The foremost process elements in video secret writing are Color house Conversion (CSC), Motion Computation (MC), Inverse DCT, Inverse division (IQ) and Variable Length secret writing (VLD). This experiment tries to ascertain mainframe and GPU load balance by accommodating an oversized buffer between mainframe and GPU The intermediate buffer effectively absorbed most secret writing jitters of each mainframe and GPU and contributed considerably to the speed-up [17].

2. Matrix operation-

Some mathematical operations don't seem to be much attainable to be resolved exploitation pen and paper. The answer for this is often use of mainframe as a process device. Operation like matrix operation of giant size matrices result in overloading of mainframe, thus there was degradation of performance. Currently the answer is to use either multi-core mainframe design or GPU. The advantage of GPU over mainframe design is that GPU is best fitted to SIMD operation and matrix operation is best example of SIMD. During this application kernel makes up the computation of matrix operation on the GPU [3].

The experiment performed by Fan Wu, Miguel Cabral, Jessica Brazelton. They take into account the matter in 3 stages initial is that the master file that's recognized by the compiler as a place to begin of the program. The second is matrix operation formula on mainframe and also the third matrix operation formula on GPU. Increase in size of matrix failed to offer nice impact on GPU as that it gave on mainframe. Results of this experiment are shown within the style of graph. This graph portrayed performance comparison between CPU and GPU primarily based formula.

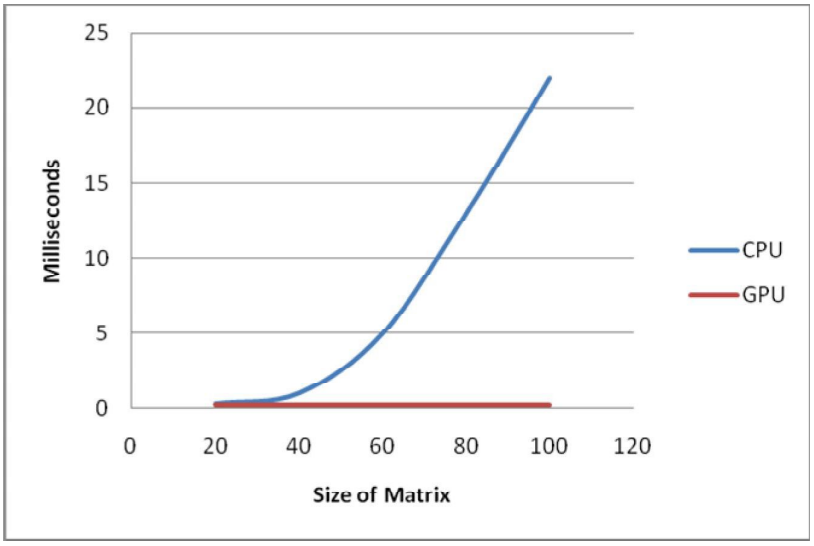

Figure 2. Performance Comparison between CPU and GPU based Algorithms

3. *Parallel AES formula-*

Data encryption plays vital role once it involves knowledge security. Security is directly proportional to the quality of secret writing formula. AES could be a radically symmetrical key cryptography formula that is usually utilized in encoding. The normal CPU-based AES implementation shows poor performance and can't meet the strain of quick encoding. AES is block cipher that divides the plaintext in to mounted size blocks. The computation of every block is freelance of every different while not considering any block cipher mode of operation. After we use processor for AES secret writing every block is encrypted serially. so resulting in low performance in term of execution time for plain text secret writing, On the opposite hand GPU executes every plaintext block parallel, so reducing the secret writing time[18].

4. *Password Recovery for MS workplace 2003 Document-*

Recently digital knowledge is increasing chop-chop. Thus at now MS workplace involves image that helps in properly organizing knowledge files and conjointly providing security by means that of secret writing and word. MS workplace 2003 and also the previous version organize documents in CFB (Compound File Binary) structure. CFB contain freelance file organize in hierarchy of storage. There square measure 3 sorts of secret writing theme on the market in workplace 2003 1st one is XOR obfuscation, second is forty bits RC4 secret writing and last is CryptoAPI RC4 secret writing [3]. Surpass puts its secret writing data within the 'Workbook Global Sub stream'. PPT holds its secret writing data with 'CryptSession10Container' within the 'PowerPoint Document' stream [19]. In SSL Proxy the key plan is to send all requests to processor once the amount of unfinished cryptanalytic operations is tiny enough to be handled by processor. If requests begin to gather within the queue, then the formula offloads cryptanalytic operations to GPUs and advantages from parallel execution for top outturn [4].

VI. GPU LIMITATION:

Along with all GPU's blessings there comes some limitation that should be studied whereas designing any GPU application. Major limitations which are directly or indirectly have an affect the Performance or quality of the application as follows [12].

1. The memory information measure between processor and GPU is restricted.
2. Scan back from GPU memory to main memory is dear.
3. Its tiny instruction set and primarily designed for graphics application.
4. No bitwise operation secret writing.
5. GPU still missing some options, example is massive range support.
6. GPU isn't optimized for serial operations.

VII. CONCLUSIONS AND FUTURE DIRECTIONS

From the on top of study we tend to conclude that GPU is that the best different for thoroughgoing procedure task. Using GPU little question increase the speed of execution however conjointly frees the central processor from the load to perform serial feasible tasks. Combination of central processor and GPU in several applications will render high performance having low value as compared to cluster of CPUs [19]. To program GPU the simplest programming language used is CUDA. It's terribly economical and simply understandable programming language to most of the coder because it is associate degree extension of C language. CUDA programming facilitate in planning heterogeneous procedure code that could be a combination of serial and parallel execution task performed by central processor and GPU unit severally. Many computationally intensive applications have gained edges from the employment of GPU in their computation. There are more applications beneath study wherever researchers are attempting to deploy GPU units to realize the simplest results [3].

I measure my end in light-weight of many common metrics, specifically performance/price and performance/watt ratios. We discover that, whereas current GPUs usually perform higher than CPUs, they show worse performance/watt ratios [1]. I studied the practicability of victimization graphics process Units (GPUs) for science process, by exploiting the power for GPUs to at the same time method giant quantities of pixels, to dump interchangeable key encoding from the most processor. I demonstrate the employment of GPUs for applying the key stream once victimization stream ciphers conjointly investigate the employment of GPUs for block ciphers; discuss operations that check that ciphers unsuitable to be used with a GPU, associate degreed compare the performance of an OpenGL-based implementation of AES with implementations utilizing general CPUs. Whereas I conclude that existing interchangeable key ciphers don't seem to be appropriate for implementation at intervals a GPU given gift arthropod genus,

Recently engineering plays a good role once it involves excessive computation to resolve a special or specific drawback. GPUs are wide used as elements of complicated graphics application. these days these graphic process units are step by step creating some way into cluster automatic data processing system because the high performance computing units, owing to their distinguished procedure power. Before once central processor was solely the unit for computation several task had to attend for his or her completion, step by step the concept of processor cluster came into market that not solely accrued performance however conjointly offer ease for complicated computing. Cluster of processor tested to be useful for complicated computation however together with its edges there have been some unwanted options like high quantity of investment, expensive for usage once there's less complicated computation. GPUs invention tested to be a boon not just for graphics connected application however conjointly for different excessive procedure SIMD (Single Instruction Multiple Data) tasks.

REFFERENCES

[1] Dattatraya Londhe, Praveen Barapatre, Nisha Gholap and Soumitra Das, "A SURVEY ON GPU SYSTEM CONSIDERING ITS PERFORMANCE ON DIFFERENT APPLICATIONS", Computer Science & Engineering: An International Journal (CSEIJ), Vol. 3, No. 4, August 2013.
[2] Keon Jang, Sangjin Han, Seungyeop Han, Sue Moon and KyoungSoo Park, "Accelerating SSL with GPUs", SIGCOMM'10, August 30–September 3, 2010, New Delhi, India. ACM 978-1-4503-0201-2/10/08.
[3] W. Diffie and M. Hellman, "New directions in cryptography" IEEE Transactions on Information Theory, vol. 22, pp. 644–654, 1976.
[4] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems" Communications of the ACM, vol. 21, pp. 120–126, 1978.

[5] J. Nickolls and W. J. Dally, "The GPU Computing Era," IEEE Micro,vol. 30, pp. 56–69, 2010.
[6] R. Szerwinski and T. Güneysu, "Exploiting the Power of GPUs for Asymmetric Cryptography" in Cryptographic Hardware and Embedded Systems -CHES 2008, 2008, pp. 79–99.
[7] A. Munshi, "OpenCL 1.0 Specification", Khronos Group, May 2009, URL:http://www.khronos.org/registry/cl/.
[8] J. Daemon and V. Rijmen, "*The Design of Rijndael: AES the Advanced Encryption Standard"*, Springer-Verlag, Berlin, 2002.
[9] B. Schneier, "*Applied Cryptography"*, 2nd edition, John Wiley and Sons, New York, 1996.
[10] M. Woo, J. Neider, T. Davis and D. Shreiner, "*The OpenGL Programming Guide"*, 3rd edition, Addison-Wesley, Reading, MA, 1999.
[11] Zhang Hao, Li Lijun and LiLan, "General Purpose computation on Graphics processors", Computer and Digital Engineering, 2005, 33(12):60-62, 98.
[12] John D. Owens, Mike Houston, David Lucbke, et al., "GPU Computing", Proceedings of the IEEE, 2008,96(5): 879-899.
[13] O. Harrison and J. Waldron, "Practical Symmetric Key Cryptography on Modern Graphics Hardware", In USENIX Security, 2008.
[14] General Purpose Computation Using Graphics Hardware, http://www.gpgpu.org.
[15] M. Woo, J. Neider, T. Davis and D. Shreiner, "The OpenGL Programming Guide", 3rd edition, Addison-Wesley, Reading, MA, 1999.
[16] O. Harrison and J. Waldron, "Efficient Acceleration of Asymmetric Cryptography on Graphics Hardware", In Africacrypt, 2009.
[17] Guobin Shen, Guang-Ping Gao, Shipeng Li, Heung-Yeung Shum and Ya-Qin Zhang, "Accelerate Video Decoding With Generic GPU", in IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 15, NO. 5, MAY 2005.
[18] Xiaojing Zhan and Jingxin Hong, "Study on GPU-based Password Recovery for MS Office2003 Document", 7th International Conference on Computer Science & Education (ICCSE 2012) July 14-17, 2012. Melbourne, Australia.
[19] P. Barrett, "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor", in Advances in Cryptology - CRYPTO '86, Santa Barbara, California, ser. LNCS,A. Odlyzko, Ed., vol. 263. Springer, 1987, pp. 311–323.