Journal of Electrical and Electronic Engineering
2019; 7(4): 95-100
http://www.sciencepublishinggroup.com/j/jeee
doi: 10.11648/j.jeee.20190704.12
ISSN: 2329-1613 (Print); ISSN: 2329-1605 (Online)

China Net: Military and Special Supercomputer Centers

Andrey Molyakov

Institute of Information Technologies and Cybersecurity, Russian State University for the Humanities, Moscow, Russia

Email address:
andrei_molyakov@mail.ru

To cite this article:
Andrey Molyakov. China Net: Military and Special Supercomputer Centers. *Journal of Electrical and Electronic Engineering*. Special Issue: *Science Innovation*. Vol. 7, No. 4, 2019, pp. 95-100. doi: 10.11648/j.jeee.20190704.12

Received: August 18, 2019; **Accepted**: September 23, 2019; **Published**: October 9, 2019

Abstract: Author describes military and special supercomputer centers and networks by example CT-2. Work on highly productive and promising SC with a globally addressable memory and multi-thread architecture is carried out within the framework of the CT-2 project. The eponymous supercomputer belongs to the class of strategic supercomputers. The code name used is CT-2 (full name Qin Tao -2) - this is the idiom in the Chinese name “The main project in the interests of special studies of military intelligence of the Ministry of Defense of China”. Due to using of massive multi-thread streaming architecture increased tolerance to delays in performing operations with memory and the network, effectively support working with program models in the form of static graphs of data flows. Because of this, it will successfully cope with the processing in real time of multiple data streams and work effectively through a single address space with a huge memory capacity of several tens of petabytes, even in the mode of intensive irregular work with it, it will have exceptional fault tolerance and availability. The amount of available memory for the user program is 32PB, the physical memory is 64PB, which is done for hot standby. According to information received in 2011, the initially massive multi-thread microprocessor CT-2 with asynchronous threads for information systems has also become hybrid, it has enhanced numerical processing power - SIMD operations on short vectors have been introduced, as well as elements of modern graphic processors in the form of synchronous threads.

Keywords: Massive Mult-ithread, CT-2, Information Security, Supercomputer, Security Descriptor

1. Introduction

A powerful state system of information warfare has been created in China, which allows for the massive use of forces and means in a short time. In addition, as part of the reform of the country's armed forces by the Ministry of Defense of the People's Republic of China, NUDT is creating a Cyber War Research Center. It will be located in Zhengzhou City (the administrative center of Henan Province). It will include several departments whose main task is the formation of a theoretical base, as well as the development of the basic principles and methods of conducting information warfare for their further implementation. This center will be equipped with all the latest types of equipment [1]. A special group will operate here to use and improve methods for covert information interception using hardware-software bookmarks (Blue Team - “Blue Team Pearl of the East”). Its capabilities will make it possible to effectively carry out radio interception, suppress air defense and missile defense systems, and overcome the computer defense of the enemy. The implementation of this project is carried out under the direct supervision of the People's Liberation Army (PLA) General Staff. Intelligence activities in China are carried out by two key intelligence organizations: the Ministry of State Security and the Main Intelligence Directorate of the People's Liberation Army of China. The first department is engaged in political and economic intelligence, as well as the formation of separatist sentiments in "zones of vital interests of China outside the country". The second department concentrates on collecting data on the military potential of foreign countries and scientific and technical intelligence.

One of the main achievements of Deng Xiao Ping is the creation in the structures of the Ministry of State Security of the People's Republic of China powerful system-analytical divisions, where specialists (analysts, developers) are concentrated, who analyze the entire array of information extracted by secret services in vocal and unwritten ways, make long-term forecasts of the development of geostrategic and regional situation, develop and submit to the country's leadership variant plans for conducting complex operations (involving political, diplomatic, military-technical iCal,

financial, economic and special funds) to achieve the objectives of the political leadership [2].

The Ministry of State Security of China has a stable operational position in all key sectors of legal and illegal business in the countries of the Asia-Pacific region (APR) and controls the main information and financial flows. Chinese intelligence has penetrated the state and law enforcement agencies of the Asia-Pacific countries and has the ability to pursue its interests. For example, in Indonesia, 3.5 million Chinese people own 73% of the country's private capital, while in Singapore this index is even higher.

Chinese military and special services pay more attention to controlling the media in the Asia-Pacific region, an impressive number of newspapers, television and radio channels were acquired by agents and officers of Chinese intelligence, including through the mafia structures of the Triad, which actually became a division of the MGB. Thanks to the powerful Chinese lobby organized by Chinese intelligence, the PRC is solving a number of important economic problems in foreign countries: it is promoting the promotion of cheap Chinese goods and extracting advanced technologies and scientific developments for Chinese industry.

In Nanjing (Jiang-Su Province), there is a secret military computing center CADT (China Academy of Defense Technologies - 7 Bureau of the Ministry of National Security). reports to the main department of electronic warfare; prepares electronic warfare officers for the command profile of the middle and entry level and engineering profile of the middle and top level in the interests of the Armed Forces of China The academy also carries out research work on "the creation of engineering systems that reduce the degree of destruction and protect against weapons," "theory and design of weapons", "bridges and tunnels", "artillery, self-propelled weapons and ammunition." Moreover, the Chinese community of the so-called "red hackers - Mao brothers" operates here. In fact, we are talking about the formation of units of "military hackers", which first appeared in 2000 and currently number up to 1 million people. This center has access to five national supercomputer centers, China-GRID computing nodes, and transnational telecommunication networks.

2. Strategic Supercomputer CT-2 (“Thunderclap”): Methods and Technologies

Work is underway to create a strategic intelligence processing center and, obviously, a strategic command center of the Armed Forces of China. It should be a center such as the Utah Center being built by the Americans. Presumably, it should be located in a desert mountain area in the western part of the central region of China.

This center should use class supercomputers, which, like the Cray XMT-3 for the Utah Center, should have a massive multi-thread architecture and ensure efficient operation with large globally addressable memory. According to the terminology used, it was clear that this is an analogue of the American DARPA HPCS program. In mid-December, the first updated information was obtained about this area of work [3]. Their active phase in the form of OCD, as it turned out, was launched in mid-2009, and in the fall of 2011 it became known about the first results obtained in the form of prototypes of multi-thread microprocessors.

1. Work on highly productive and promising SC with a globally addressable memory and multi-thread architecture is carried out within the framework of the CT-2 project. The eponymous supercomputer belongs to the class of strategic supercomputers, it must have exaflops performance, heterogeneous architecture, i.e. use different types of microprocessors, but the main microprocessor CT-2 is massive multi-thread.

2. The code name used is CT-2 (full name Qin Tao -2) - this is the idiom in the Chinese name “The main project in the interests of special studies of military intelligence of the Ministry of Defense of China”. The initial application area of the CT-2, which is primarily considered as a supercomputer for information systems, is the creation of global operational-command centers for the collection, processing and storage of critical intelligence information (in this regard, it is similar to the UTAH-117 American project). The ciphers of the projects for creating such systems are “Thunderclap”, “Typhoon” and “Red Dragon Strike”. Work on CT-2 is carried out at the National University of Defense Technology of China (NUDT, Ministry of Defense of China, military intelligence, directly in the closed 15th zone of NUDT). According to 2009, the CT-2 project has the highest state priority, is directly under the control of the Chairman of the State Council of China Hu Jin Tao.

3. The main microprocessor CT-2 is a multi-core massive multi-thread microprocessor, based on the architecture of the J7 microprocessor of the Russian Angara project, but with elements of the most powerful J10 microprocessor project. Due to the use of massive multi-thread streaming architecture, it should have increased tolerance to delays in performing operations with memory and the network. Because of this, it will successfully cope with the real-time processing of multiple data streams and work effectively through a single address space with a huge memory capacity of several tens of petabytes even in the mode of intensive irregular work with it, it will have exceptional fault tolerance and availability (see Table 1).

Table 1. *General information about the RAM of different supercomputers with global addressing.*

The characteristic	CT-2	Angara	Cray Black Widow
OS memory	64 Pb	8 Pb	4 Pb
Memory of one unit	512 Gb	256 Gb	512 Gb
Quantity (amount) of units	63648	32768	8192

The characteristic	CT-2	Angara	Cray Black Widow
Quantity (amount) of accessible segments of a problem (task)	128M	1M	1024-67 M
The maximal size of a segment	512 Gb	256 Gb	4 Gb
The maximal size of a supersegment	256 Tb	256 Tb	-
Quantity (amount) of records in TLB	2048+128	2048	65536
Address space, achievable from TLB without misses	32 Pb	8 Pb	1 Pb
microprocessor	CT-2	J7	BlackWidow

4. According to information that has become known, the initially massive multi-thread microprocessor CT-2 with asynchronous threads for information systems has also become hybrid, it has enhanced numerical processing power - SIMD operations on short vectors have been introduced, as well as elements of modern graphic processors in the form of synchronous threads. A prototype of such a microprocessor modified in architecture at the Taiwanese TSMC factory using 45 nm technology was manufactured, the number of cores (such as the J7 microprocessor) on one chip was 12, each core should have 256 hardware threads (there were 64 in J7). The introduction of hybridity in the CT-2 microprocessor allows us to understand the plans of Chinese experts on the use of CT-2 for a wider class of tasks. We can assume that by changing the assembly of computing nodes (increasing the share of CT-2 microprocessors and removing network data receiving-output units), it is possible to create a supercomputer for scientific and technical calculations with real performance on scientific and technical tasks at the exaflops level.

2.1. Stages of Creating Special Supercomputers

The following are known about the main stages of creating transetaflops systems and further exaflops systems, including the use of the results of the CT-2 project.

a) 10PF (2012, modification of Tianhe-1A). According to the decree of the PRC government, the first stage of the strategic development plan for HPC-China (2012) was set to develop a supercomputer system with a capacity of 10 PFLOPS (Tianhe-1A modification) containing about 10 thousand new TC3700 blade servers, in which 40 thousand were installed. Tesla GPU, 60 thousand 8-core Godson-3B, as well as server boards with 20 thousand multi-thread microprocessors FT-1000/1500. 30PF (2014, Tianhe-2, code - Dragon Flight). Between 2011 and 2014, NUDT was commissioned to develop a new Tianhe-2 supercomputer system with 30 PFLOPS performance, presumably based on Godson-3C or Godson-4A, FT-1500 multi-thread microprocessors and the new version of the Arch communication network. This development is contrasted with the American supercomputer IBM BlueGene/Q (Sequoia) on 17-core (4 threads in the core) Power microprocessors and a 5-dimensional torus type network. The goal is to surpass the American supercomputer by 1.5 times.

b) 100PF (2016, code - Taiwan hawk). Until 2016, the Chinese government has set the task of four leading departments (National Air and Space Intelligence Center (NASIC), NUDT, ICT and National Applied Research Laboratories (NARL)) to develop and commission a computer complex with a capacity of 100 PFLOPS.

c) Exaflops (2017-2018) - A heterogeneous supercomputer that includes three types of massive multi-thread microprocessors, classic superscalar microprocessors, graphic microprocessors and network microprocessors. The base microprocessor is CT-2, its modifications are possible. Construct 4D with liquid cooling system.

2.2. Technologies for Controlling Internet Traffic and New Protocols

Chinese scientist Yoon Wang from Chengdu University of Research has proposed a unique three-step algorithm for determining the location of Internet users. Developed jointly with scientists from the United States, the new algorithm allows you to find out the user's physical location with an accuracy of 690 meters. Until now, if the user did not give direct consent to determine their location, third-party websites could calculate this data with an accuracy of about 200 kilometers. The new three-stage technology significantly increases the accuracy of the “pick-up”, without requiring user consent, which can significantly change the market for targeted advertising on the Internet [4-8].

The algorithm proposed by Wang and colleagues involves three stages: at the first stage, a quite familiar action is taken with sending a test packet and controlling the delay. It is assumed that the time taken to process the packet and response allows us to judge, and rather roughly, the distance from the site to the user. For a more accurate location estimate, Wang decided to use the fact that organizations in China, including businesses and educational institutions, have fixed IP addresses that are tied to a specific physical location. For example, if the IP address belongs to a university, you can quickly determine the coordinates of that university using a map service. For his research, Wang collected about 76 thousand pairs linking IP addresses and physical addresses. Now the new system polls all points with a known location within the initial 200km radius, and then, by comparing the response time, the search circle narrows even more when the program finds 10 out of 12 nearest marks with the same response time [9, 10].

After polling the nearest points with a known location. the algorithm repeats the survey until it becomes clear which of these points is located closest to the desired user. In China, with a large number of IP-addresses attached to the place (two-billionth population and, accordingly, many users on the network) and clearly-connected MAC-addresses of gateways through which the Internet is accessed to China (PRC special services use a limited set of federal providers, gateway equipment whose switches have constant MAC addresses),

the accuracy of pickup is incredibly high [11].

Who might need a highly accurate user location algorithm? First of all, it is those who publish ads on the Internet, and this advertisement is aimed solely at a local audience. Just imagine - you open a well-known website in a browser, and it displays a store advertisement near your home. Nevertheless, over-precise advertising positioning is not the worst thing yet. Much more dangerous is the potential breach of privacy from both individuals and small groups or government agencies.

With the widespread dissemination of such tools, a fashion for camouflage proxy servers and other auxiliary tools may appear. It is possible that all the benefits of the new technology will be more than offset by negative effects. Canadian human rights activists from Citizen Lab, together with computer security experts, found evidence that a global system for monitoring and archiving Skype traffic was deployed in China. Voice traffic is not analyzed, but all text messages are checked against a list of suspicious words. As it was found out, the Chinese authorities have at least eight servers that are monitoring Skype.

To date, more than a million text messages have already accumulated on them, each of which contains a particular word from the list of "suspicious" words. In the past two months alone, more than 166,000 new messages from 44,000 users have arrived on the server.

The IPv6 specification implies the presence of three groups of root DNS servers and two groups of subordinate servers, each of which is designed for three million users. In experiments conducted in two districts of Shanghai, IPv6 networks supported Latin and Chinese domain names, digitally presented IP addresses, DHCP servers (Dynamic Host Configuration Protocol), IPv4/IPv6-compatible routers with a bandwidth of 1000Mbps/s and IPv4/IPv6 compatible switches. It is important that by supporting the IPv6 specification, China has actually become the only country in the world to accept ten-digit IP and MAC addresses. Moreover, today only China and the United States have independent root DNS servers and independent domain names [12, 13].

In addition, with the launch of the national DNS system, 44 subdomains in the China (CN) domain are added: 7 industry domains, 34 regional domains for the autonomous regions, provinces, municipalities and special administrative zones of China, and 3 domains (AC. CN, GOV. CN, MIL. CN) for resources of academic, state and military departments. It's expected that for most users the transition to DNSSEC will go smoothly, but users of incorrectly configured firewalls, as well as those who use the services of untrusted providers, may lose access to many sites and web services. DNSSEC adds digital signatures to regular DNS queries - this greatly reduces the risk of becoming a victim of man-in-the-middle attacks associated with spoofing information in DNS server caches. Currently, the new protocol is being carefully implemented in the root DNS servers of the WAN.

2.3. Architectural Features

The organization of a computing node based on new microprocessors uses the ideas of the American ParalleX project proposed by T. Sterling. Using of 3D and 4D constructs with direct liquid cooling is supposed.

The CT-2 supercomputer being created with several levels of hierarchy, high parallelism and globally addressable memory requires powerful software with dynamic parallelization of programs, optimization tools that take into account the heterogeneity of access to globally addressed memory. It is clear that issues of parallelization and optimization of work with memory should be hidden as much as possible from the end user. According to reports, an average level of system software is being developed (GASNet (active messages), ARMCI (message aggregation), Charm ++ (object-oriented computing models with message transfer control) approaches are analyzed and modified, transactional memory (process localization over memory and saving locks).

It became known about new implementations of the microprocessor CT-2. Now we know about three implementations of hybrid massive multi-thread vector microprocessors of the Chinese project CT-2: 12-core, 45nm technology; 48 nuclear, technology 45nm (larger crystal); 96-core, 32nm technology. These microprocessors were manufactured at the TSMC factory, which is located in Taiwan, but currently belongs to mainland China by 75-80%.

The results obtained on the development of basic microprocessors of the CT-2 project allow China to reach a new level in the field of on-board systems for unmanned aerospace means, as well as other autonomous systems such as combat robots and communications. Among Chinese experts, there is even an opinion that the appearance of these microprocessors makes it unnecessary to use FPGAs with their although obvious modern advantage in implementing stream-based computing schemes with data management, but also with obvious shortcomings in programming complexity and cost, energy consumption. It is also known that the developed CT-2 base hybrid microprocessors allow software to emulate the PowerPC, X86 command systems and the Monarch microprocessor (this microprocessor includes a decisive field of heterogeneous elements and universal RISC-type processor cores), which ensures portability of previously created complexes.

In other words, as expected, this type of hybrid microprocessor turned out to be not only the basic building block of the petaflops supercomputer, but also the "battlefield" microprocessor used in various weapons systems, up to the fighter's equipment.

3. Result

Consideration of exaflops projects allows us to draw the following results:

Firstly, in the considered foreign countries (USA, China, Japan and Western Europe) projects for the development of

exaflops supercomputers have the status of programs of the largest government departments or federal. The clear leader is the USA. China and Japan have been catching up with the USA in the field of supercomputers in the highest performance range for the second decade. This was clearly evident in the previous DARPA HPCS program, and it should be noted that these countries coped with their national counterparts of this American program. Each of these countries has its own specifics of ongoing projects, strategies and tactics for their implementation. Western Europe began independent work in this area recently, this is a clear manifestation of the desire for independence from the Americans. All these countries are characterized by increased attention to the innovative direction of work, because if successful, this allows you to "cut the corner" and get closer to the leader faster. This is also understood in the United States, which is why innovation projects are also receiving increased attention [14].

Secondly, in the USA, the main responsibility for exaflops topics was assumed by DoE, both in evolutionary (DoE NNSA) and in innovative directions (DoE OS/R). The UHPC program announced earlier by DARPA continues, but it is believed that it is not performing very well, and therefore it transferred responsibility to DoE as the most powerful US scientific and technical infrastructure. DARPA UHPC projects are duplicated in DoE and received additional support, but besides them, many more projects have been launched.

In the evolutionary direction, the level of 30 petaflops was reached. The level of 100 petaflops should be reached in supercomputers on "heavy" cores (ORNL, Cray and NVIDIA) and "light" cores (ANL, IBM). Both directions suggest peak exaflops in 2018-2020. According to the innovation line, three centers for co-development of special exaflops supercomputers have been created for the following areas: materials science (LANL - head), promising reactors (ANL - head) and combustion processes (SNL - head). This direction can be described as optimization of the use of CMOS technologies. Many small basic research projects are underway, and one of the main areas is new models for organizing parallel programs for exaflops supercomputers, new run-time systems and operating systems, and new parallel programming tools. DoE's large innovative development program for an innovative exaflops supercomputer is expected after 2013. To support the main industrial vendors, the FastForward pre-proprietary program has been launched to develop processors and memory modules, as well as data storage systems. According to the authors, the project of Cray/NVIDIA Echelon firms is of most interest [15].

Thirdly, China traditionally masterly perceives, copies and develops other people's projects, while applying the latest technology, which also often has a foreign origin, often from Japan, Singapore and Taiwan. Evolutionary and innovative directions are underway. The main developer is the Ministry of Defense of China in the form of NUDT, the University of Defense Technology of China. According to the evolutionary line, the authors estimate that China lags behind the United States for no more than 2-3 years. At present, the Tianhe-2 supercomputer (Dragon Flight project) with a capacity of 30 Pflops has been assembled. This development has not yet been advertised, the American and its own element base are used, both microprocessors and network VLSIs.

Fourthly, Japan is more independent and creative in its projects, and is highly closed. There are evolutionary and innovative directions. In the evolutionary direction, the Tsubame supercomputer and a K-computer (10 petaflops) were developed, and if Tsubame uses the American element base, then the K-computer uses its own. It is planned to create Tsubame-3 with a productivity of 30 petaflops. So far only the project of the military super-computer "Arrow of Time", which is being developed by the Self-Defense Forces of Japan, is known through the innovation line, but due to a change in the composition of microprocessors in computing nodes it can be reoriented to solving scientific and technical problems. On the line of work on the element base of the post-Murov era, significant results have been achieved in the field of superconducting electronics.

4. Conclusion

China Net has its branches in every province, in every city and county. In addition, the state widely encourages the development of commercial services on the Web, especially related to distance learning, education and medicine. Priorities in the field of network services are given, of course, to the banking sector. However, e-commerce, entertainment, and other areas are also encouraged. The authoritarianism of the PRC in matters of control over the media is quite understandable to many Chinese, even those who belong to the current political leadership are by no means loyal. Many foreign researchers note that complete freedom of speech in very special, specific Chinese conditions is not only impossible due to national security considerations, but also fraught with very serious consequences for international security. The Chinese authorities were faced with a dilemma: to "let go" of the Internet, ignoring possible threats to state interests, or to "squeeze in a vice", missing the many benefits of using the Network for economic purposes. As a result of a short and unshuffled debate, the Chinese decided, as in many other cases, to approach the problem comprehensively.

China's approach to defending public interests on the Web can be figuratively described as "diversity control." Fears regarding the "human factor" on the Internet are resolved precisely by this human factor.

Realizing that it will be impossible to track the "offenses" of several millions (or maybe tens of millions) of users, the authorities redistributed the control and accounting functions between telecom operators and administrative authorities. At the centralized level, only a blocking of broad access to pornographic content sites and to some news sites such as Reuters or The New York Times was undertaken. Special filters that Internet service providers are required to set at their own expense also block access to foreign political

content using keywords such as Taiwan, dissident, Tibet, etc.

Basically, the monitoring of user work is carried out locally and begins already from the moment of user registration. In order to become an Internet user, an individual must be checked at the local police station and provide the provider with a certificate of the established form. According to some unofficial data, the staff of the Ministry of Public Security often work in senior positions in large provider firms.

For individuals, there is a whole range of various punishments: from monetary fines to deprivation of the right to use the Internet for a certain period. The requirements for corporate users are an order of magnitude higher than for individuals. Checking the reliability of a company that wants to "join" the Internet, sometimes takes several months. For reputable commercial companies or government organizations that have a full-time security service or the first department, the practice of removing locks in the interests of business. However, any "pranks" of the employees of these companies are carefully recorded on special equipment, and violators of the regime are severely punished. Firms keep a journal where they argue visits to each dubious site.

References

[1] N. Sun, D. Kahaner, D. Chen. High-performance Computing in China: Research and Applications. International Journal of High Performance Computing Applications, 24 (4), 21. 09. 2010, pp. 363-409.

[2] X. Guo, D. Lecarpentier, P. Oster, M. Parsons, L. Smith. Investigation Report on Existing HPC Initiatives. European Exascale Software Initiative, CSA-2010-261513, 29. 09. 2010, 44 pp.

[3] P. Kogge et al. ExaScale Computing Study: Technology Challenges in Achiving Exascale Systems. DARPA IPTO, US Air Force Research Laboratory, September 28, 2008, 278 pp.

[4] Molyakov, A. S. New Multilevel Architecture of Secured Supercomputers/A. S. Molyakov//Current Trends in Computer Sciences & Applications 1 (3) – 2019. – PP. 57-59. – ISSN: 2643-6744 – https://lupinepublishers.com/computer-science-journal/special-issue/CTCSA.MS.ID.000112.pdf. – DOI: 10.32474/CTCSA.2019.01.000112.

[5] Molyakov, A. S. Technological Methods Analysis in the Field of Exaflops Supercomputers Development Approaching/A. S. Molyakov, L. K. Eisymont//Global Journal of Computer Science and Technology: Information & Technology. – 2017. – № 1 (17). – PP. 37-44.

[6] Molyakov, A. S. A Prototype Computer with Non-von Neumann Architecture Based on Strategic Domestic J7 Microprocessor/A. S. Molyakov//Automatic Control and Computer Sciences. – 2016. – № 50 (8). – PP. 682-686.

[7] Rao A. et al. Effect of Grammar on Security of Long Passwords. CODASPY'13, February 18-20, 2013, 8 pp.

[8] Archana A., Kohila N. Probabilistic Context-Free Grammar (PCFG) Wiser Password Cracking Techniques. International Journal of Research in Computer Applications and Robotics, February 2016, vol. 4, Issue 2, p. 1-6.

[9] Goldstein Seth Copen, Schmit Herman, Budiu Mihai, Cadambi Srihari, Moe Matt, Taylor R. Reed. PipeRench: a reconfigurable architecture and compiler. Computer, April 2000, pp. 70-77.

[10] Vahey M., et al. "MONARCH: A First Generation Polymorphic Computing Processor", Raytheon, 2007, 2 pp.

[11] Xu Guo, Meeta Srivastav, Sian Huang, Denesh Ganta, Michael B. Henry, Leyla Nazhandali, Patrick Schaumont. Silicon Implementation of SHA-3 Finalists: BLAKE, Grostl, JH, Keccak and Skein. 2011, 16 pp.

[12] Meeta Srivastav, Xu Guo, Sian Huang, Denesh Ganta, Michael B. Henry, Leyla Nazhandali, Patrick Schaumont. Design and Benchmarking of an ASIC with Five SHA-3 Finalist Candidates. Center for Embedded Systems for Critical Applications (CESCA), USA, April 20, 2012, 27 pp.

[13] Xu Guo, Meeta Srivastav, Sian Huang, Denesh Ganta, Michael B. Henry, Leyla Nazhandali, Patrick Schaumont. ASIC Implementations of Five SHA-3 Finalists. 2012, 6 pp.

[14] Patrice Guillet, Enrico Pargaetzi, Martin Zoller. Silicon Implementation of Second-Round SHA-3 Candidates. February 2010, Swiss Federal Institute of Technology Zurich, Integrated System Laboratory, 2010, 46 pp.

[15] Frank K. Gurkaynak, Kris Gaj, Beat Muheim, Ekawat Homsirikamol, Christoph Keller, Marcin Rogawski, Hubert Kaeslin, Jens-Peter Kaps. Lessons Learned from Designing a 65nm ASIC for Third Round SHA-3 Candidates. ETH Zurich - George Mason University, 22-23 March 2012, 65 slides.