Indian Journal of Science and Technology, *Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/96037, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Review on Security in Cache Memories

R. Vijay Sai* **and S. Saravanan**

School of Computing, SASTRA University, Thanjavur – 613401, Tamil Nadu, India;
vijaysai@it.sastra.edu, saran@core.sastra.edu

Abstract

Objectives: Security in cache memory is a major issue in memory related applications such as smart cards and bio-metric implementations. The objective of this review is to analyze various attacks targeting cache memory and suggest remedial measures to thwart such attacks and assure cache memory security. **Methods/Statistical Analysis:** Information stored in cache memory can be recovered whenever required. This data is in danger of being hacked by the intruder. Statistical analysis show that attacks such as side channel attacks, timing attacks and power based attacks are adopted to challenge information security in caches. **Findings:** Discussed solutions involve in the design of secured cryptographic based algorithms, secure aware cache mapping and low power cache design by employing techniques such as code convertors, nested XOR operations, extended Hamming codes and multi-bit clustered ECC. **Application/Improvements:** Improving and authenticating cache memory security will result in numerous applications involving smart cards and bio-metric applications where secrecy of data is of extreme importance.

Keywords: Cache Memory, Power Based Attacks, Side Channel Attack, Timing Attacks

1. Introduction

Cache is a small and limited memory present between central processing unit and main memory unit. Cache is located closer physically and logically to main memory. Different levels of caches are Level1, Level2 and Level3 levels designed and included according to the requirement. Cache lines and blocks have address fields which are divided into dynamic (tag) and static (index). Tag holds higher address bits and index holds lower address bits. Higher order bits are changeable and lower order address bits are fixed. Cache contents are cleared initially before being utilized. Cache memory is partitioned into segments. When particular information wants to be searched, the central processing unit searches into cache memory, if it is present in it or not, if it is present, it is called as cache hit, else cache miss. Delay encountered in such cases is termed as hit latency and miss latency. Different cache mapping techniques are studied. Data cache and Instruction cache are types of caches. Some of the advantages of cache memory are high speed, less latency, faster information retrieval and swift data access. Power consumption and area are also important factors while designing cache memories.

2. Security Issues in Cache Memories

Cache storage attacks[1] deal with covert channel, which is a fundamental concept of crypt analytic side channel attacks. A new storage channel probing cache debug facility is applied in embedded systems. Storage channels involve interlock, threshold and ordering schemes. The

*Author for correspondence

author uses the state of variables, on or off, representing digits and characters. Covert channel and side channel intersect together. Micro architecture involves software features in crypto system implementation for transfer of data. A new covert channel provides data cache populating per line for privilege bits. It is observed that covert channels do not rely on heuristic timings.

Cubic based set associative cache encoded mapping[2] involves in handling internal and external interrupts of bunch of words to be loaded into cache memory. Factors inclusive as cache size hit and write policy, cache map techniques and cache depth level influence processor performance. Set associate mapping remaps with cubic set associative technique. Hash functions can be a viable solution. Temporal and Spatial locality of reference are studied. The target is to explore time convolution of novel associative mapping. Associative memory refers to physical memory. Tag, block and word are attributes. Cubic cache map involves in remapping actual reference with standard scheme in linear pattern. Graceful Code (GC) is a probable study in this context. State of the art memory testing algorithm is the need of the hour. Unique one to one mapping is an extension of cubic one to one recursive mapping. These solutions throw opening to enhance cache architecture and to guard against attacks.

Cache resembling architecture using Instruction Cache and Data Cache[3] are targeted by side channel attacks to extract encrypted keys by software activities and hence efficient defense is missing. The author makes preload information with software random permutation. Hardware complexity and performance overhead is a tradeoff. Use of branch target buffer and update policy prevents information leakage. Side channel attacks power, heat and electromagnetic radiation. Shared architecture components contain Instruction Cache. Software attacks listed as access driven and time driven attacks cannot be ruled out. Based on software permutation scheme, AES and RSA are used. In modular exponentiation, square matrix multiply algorithm is employed. Conditional branch such as Branch Target Buffer (BTB) should be thwarted. Instruction cache attacks depend on secret keys. Merging of software and hardware bring protection schemes against data cache attacks. Exception handler directs all critical data into cache.

Designing cache memory with cache controller[4] involves in set associative mapping based on cache controller. Spatial location of reference is used. Based on the technique, cache miss ratio is studied. Work is made on four-way set associative mapping related to parallel accelerator processors. They are accessed through shared L1 cache in semi-conductor memories. In embedded applications, it is used for power optimization and high performance. They find application in FPGA based processors. Address range is given to microprocessors by cache controller which replaces address range in cache tag memory.

Security of a secure cache design is maneuvered when side channel attacks are common. New-cache technique involves dynamic memory for cache re-mapping[5] based on eviction randomization. Slight modification of replacement algorithm can yield better results. Address memory exploitation can make secret keys to be known. Various attacks need to be watched. Attacks based on prime and probe techniques may fill entire cache area with malicious data. In this context, spy process involving counting of cache hits will prove efficient. Evict and Time attack measures encryption time. This attack is Bernstein's attack. Moving Target Design (MTD) and Large Direct Map (LDM) can be considered. Attacks are redesigned for new cache. Replacement algorithm can be improved. New cache fails to counter evict and time attack. New cache need to be improved. Here, move protected bit (P bit) from tag array to index field. Randomization is done.

Time driven cache attacks on mobile devices[6] involve in mobile devices which utilize cache memory for user security and privacy. T-table based AES implementation on android mobiles is performed. Investigation of time driven attacks target applications related to Bernstein's attack. This type has study phase and attack phase. Correlation phase involves exhaustive key search phase. Algorithm to counter time driven cache attacks reduce key space. Energy leakage is studied involving wide collisions.

Cache-coloring based technique[7] for saving leakage energy in multi-tasking systems involves in dealing with energy efficiency which is a prominent factor. Leakage of energy in caches is consistently monitored. Energy save algorithm is designed and implemented. The model is compared with Decay Cache Technique (DCT). Presence of on chip cache increases energy consumption, which is an important criterion. Dynamic profiling with dynamic cache reconfiguration for optimal memory sub system for energy efficiency is observed.

Improving memory encryptions performance in multi-processor systems[8] considers central processing unit which is the most trusted chip, vulnerable to physical

attacks. Security schemes such as confidentiality and integrity outside the chip is important. Unipolar leads to mathematical counter mode encryption methods applying xor padding. One Time Password is suggested for improving data security in caches. A suitable algorithm for counter cache coherence protocol increases rate of hit placed on counter cache, co-operating with transit cache by the application of coherence protocol. Such methods such as stated before increases overall performance of cache memory architectures.

Theoretical application of cache memory on a side channel based on crypt analysis[9] is a potential solution where side channel leaking information is observed. Encryption based on plain text openly throws wide chances for hacking data. Method of computing power based on techniques such as simple and differential power analysis can be utilized to veil secret data in memory devices. The other side channel attacks are timing attacks, electromagnetic radiation attacks, glitch and fault analysis based attacks. There is a threat on main memory attack through cache memory. Cache hit, cache misses and cache size are important parameters. When power is switched off, cache needs to be switched off for avoiding data theft. An algorithm based on Fiestal network structure is studied. To avoid attack on algorithm implementation, cache is contained within processor. Timing skews and dummy operation is appended to the technique to confuse the intruder. DES algorithm is altered and cache behavior analysis is observed.

Software approach to safeguard against attacks[10] is based on timing phenomenon. By certain attacks based on side channel confrontation, there is a chance of recovering secret keys. Changes in algorithm provide security to some extent only. Dynamic Binary Translation Technique (DBTT) is followed. This technique creates sand box based cryptographic implementation. Redundancy instruction is inserted into binary codes of cipher mode. The leakage information is skewed which is of no use to attackers. This provides strong protection against cache based timing attacks. Dummy codes skews execution time for security. Using binary codes, architecture is altered. Sandbox technique uses interpreter and translator as components. Read Time Stamped Counter (RTSC) is used with Pseudo Random Number (PRN) generation. Redundancy provides extra time.

Decreasing area overhead to protecting large caches against errors[11] deals transient failures caused by soft errors. The end work is to reduce power by power scaling techniques. Current microprocessors involve on chip memory structures in caches. Register files are monitored and TLB is loaded and queue storage is carried out. For the purpose, re-order buffer technique is applied. The design of microprocessors involves large components. Here, a novel concept on cache architectures provides low area over-head for error protection for large level2 and level3 caches. The architecture revolves around different schemes. First scheme, worked out on error correction and protection protocol involves dirty cache lines. Cache lines are cleaned for protection and parity check is used. The second scheme consists of periodically cleaning dirty caches and writing the contents to main memory without increasing traffic. General cache line behavior is monitored. Dirty cache lines are reduced by almost fifty percent.

New cache designs for attacks[12] are provided which are easy to perform on many platforms. No special instruments are needed to carry out this process. Additionally, no excess computation power is required. A simple time measure may recover secret key. Two basic mitigation techniques are observed in this work. First work concentrates on partition based, where elimination of cache memory interference is worked out. Second scheme provides randomization of cache interference. New security aware cache design involves Partition Locked (PL) cache and Randomized Permutation (RP) which are about defending side channel attacks. Main work is on reducing cache interference and reduced mitigation, which is the root cause of such attacks. The schemes mentioned here provide hardware solution through theoretic method by mathematical provisions.

Cryptographic side-channels acquired from cache memory having low power[13] involves in focusing of microprocessors centered on area and power consumption, neglecting physical security. Analysis of power parameters such as simple power analysis and differential power analysis are made. Side channel attacks target physical security, making it vulnerable. Research is made on micro architecture side channel attacks. Low power cache memory design is made. Branch prediction based on BTB attacks is a special form for cache memory. Power analysis attack on RSA algorithm is noted. Defensive techniques in algorithm and architectural levels based on square and multiply method give vital solutions. Usage of non-state low power cache memory preserving level1 data cache controls flow within square and multiply algorithm.

Advanced encryption standard power attack[14] shows induced cache miss and countermeasure. Traditional attacks aim at cracking data by flushing elements of S-box from cache. Cache miss is induced in encryption phase and power traces used. Complete cache invalidation before encryption is not needed. The basic idea involves forcing a cache miss when processor executes AES. In this context, cache size, block size and study of associative technique is required. They are fitted in block ciphers later. No randomization is needed. Countermeasures on insertion of a set of s-boxes in encryption function are carried out before real computation starts.

Intelligent Web Proxy Cache Replacement Algorithm[15] based on Adaptive Weight Ranking Policy via Dynamic Aging provides additional intelligence in cache security. Selective Placement of Caches[16] for Hash-Based Off-Path Caching in ICN provide a better technique in cache placement. Reliability of cache memories[17–19] using identical tag bits, reduction of power and cell stability based on dynamic isolated read static random success memory and data scrambling based secured data authentication storied in memories respectively are discussed elaborately which gives potential solutions. Design of exclusive cache architecture[20] which saves power is a solution to cache parameter challenges. Performance analysis[21] of cache consistency maintenance in mobile environment using agent technique is a viable approach to providing cache security.

3. Proposed Works

Some of the critical parameters to be considered while designing cache memories are size, access time, area occupied, power consumption, latency and speed. Cache memory becomes insecure when targeted. It is difficult to generate random vectors. There is a threat of secret data recovery when power is switched off. AES algorithm chosen is vulnerable to D cache attack. Data is sensitive to cool temperature. Emission of electromagnetic radiations will increase probability of hacking. Replica of circuit design can recover secure data and make them insecure. Providing circuit complexity to thwart attacks results more cost in design.

Proposed solutions involve in the design of secured cryptographic based algorithms, secure aware cache mapping and low power cache design. Modifying the concept of encryption algorithm using light weight encryption to suit cache memory implementation can be a better idea. Increase in bit length may make data hacking challenging. Sub-key generation can be derived from main key to improve security. Intelligence in data scrambling techniques can be carefully thought out and implemented. Employment of code convertors improves encryption and decryption. Nested XOR operations and error detection mechanism such as implementation of Hamming code to detect single bit errors can also come under reckoning. Observation of I cache and D cache timing attacks over cache memory can be carried out. Implementation of Sliding Window Exponential algorithm may improve cache security. Application of semantic array partitioning, employing hash functions to skewed associative caches and repetition of multiple identical rounds involving substitution, transposition, mixing rows and columns and shifting them are also some of the solutions. Partitioning schemes on cache can be studied. Time can be estimated. Adaptive security quality controller, contention based attack, reuse based attack and dynamic remapping table are also viable solutions. Observations of prime and probe attack, evict and time attack is made. Supply voltage scaling to reduce system energy consumption for core processors and deep nanometer designs can be observed. Some more possibilities are extended hamming codes and multi-bit clustered ECC.

Based on various crucial factors involving cache memory design such as technology, size, access time, area occupied, power consumption, latency and speed, Table 1 has been formulated, which shows concepts, threats, benefits and shortcomings of cache technologies.

4. Conclusion

Cache memory security is a major issue in memory related applications such as smart cards and bio-metric implementations, where secrecy of data is of extreme importance. Hackers use various techniques based on mostly side channel attacks to hack the content of integrated circuits. Information of leakage power is enough for the hacker to crack secret data, which becomes vulnerable when they are exposed to electromagnetic interferences

Table 1. Performance comparison of caching techniques

Concept	Threat	Benefits	Shortcomings
Introduces new storage channel based on cache debug facility[1]	Vulnerable to crypt-analytic side channel attacks	New covert channel technique did not rely on heuristic timings	Difficulty in cache debug facility in embedded microprocessors
Set associative mapping remapped with cubic set associative technique. Spatial and temporal concepts applied[2]	Cache depth level is targeted.	Cache remap is in linear order fashion. Graceful code technique is advantageous to implement	Crucial factors are cache size and hit-write policies.
Preloading information based on Secure Partition Locked cache and Random Permutation cache[3]	Cache like architectures can retrieve secret keys by software activities	Integrated software and hardware protection scheme against D cache attacks	Tradeoff between hardware complexity and performance overhead
Spatial locality of reference used to track cache miss. Four-way set associative mapping is used. Accessed through shared L1 cache[4]	Security threats in shared memory model	Low power and high performance in embedded applications, used in FPGA processors	Challenges in circuit complexity and power consumption
Moving Target Design and Logical Direct Mapping techniques used[5]	Address memory exploited and danger of secret key bits to be known	Improved replacement and new cache algorithm	Defects in access driven attacks and fails in evict and time attacks
Investigating time driven attacks based on AES on android mobiles[6]	Users privacy and security is an issue	Time driven cache attacks reduce key space	Leakage by devices and wide collisions
Dynamic profiling with dynamic cache reconfiguration[7]	Energy save algorithm is under threat	Reduce leakage energy in caches	On chip cache is increased and energy consumption is more
Counter cache coherence protocol used to raise hit rate on counter caches[8]	Security threats on confidentiality and integrity outside chip	Overall performance improved by MESI protocol	Vulnerable to physical attacks
Algorithm based on Fiestal network structure and non deterministic access ordering cache placement technique used[9]	Attack on algorithm implementation on cache within processor	Timing skews and dummy operations confuse attackers	Cache Behavior Analysis on hardware targets algorithm
Dynamic binary translation technique used[10]	Keys can be retrieved by side channel attacks by changing algorithm	Strong protection against cache based timing attacks	Redundancy consumes extra time
Cache protection by ECC scheme and reducing dirty cache lines[11]	Transient failures and soft errors. Supply voltage reduced	Low area overhead for error protection	Microprocessor based applications require large components
Mitigation approaches based on partition and randomization techniques[12]	Simple time measures can recover key	Cache interference reduced by mitigation approaches	Attacks easy to perform on most platforms
Simple power and differential power analysis used[13]	Neglects physical security	Deploys defense against algorithm in architectural levels	Security flaws in physical implementation
Forcing cache miss when processor executes AES based on cache size, block size[14]	S-box accessed in encryption function before real computation starts	No randomization needed	Attacks flush elements of s-box from cache.

and hence the crux of this review is to find out various data attacks and suggest counter measures against such attacks to provide data security. Future works may revolve on more secure techniques to improve security of data, especially on cache memories.

5. Reference

1. Brumley BB. Cache storage attacks. Topics in Cryptology. CT-RSA; 2015. p. 22–34.
2. Vinothini S, Segar TC, Vijayaragavan R, Kumar MS. A cubic based set associative cache encoded mapping. IRJET. 2015; 2(2):360–4.
3. Kong J, Aciicmez O, Seifert JP, Zhou H. Architecting against software cache-based side-channel attacks. IEEE Transactions Computers. 2013; 62(7):1276–88.
4. Yogesh S, Watile AS, Khobragade K. Design of cache memory with cache controller using VHDL. International Journal of Innovative Research in Science, Engineering and Technology. 2013; 7(2):2914–9.
5. Liu L, Lee RB. Security testing of a secure cache design in hardware and architectural support for security and privacy. HASP'13; 2013.
6. Spreitzer R, Plos T. On the applicability of time-driven cache attacks on mobile devices. LNCS Springer, Heidelberg. 2013; 7873:656–62.
7. Mittal S. A cache-coloring based technique for saving leakage energy in multitasking systems. CoRR. 2013; 1309:5647.
8. Yuanyuan Z, Junzhong G. Using counter cache coherence to improve memory encryptions performance in multiprocessor systems. Secure and Trust Computing, Data Management and Applications. 2011; 186:79–87.
9. Page D. Theoretical use of cache memory as a cryptanalytic side-channel. IACR Cryptology ePrint Archive; 2002. p. 1–23.
10. Yuemei H, Haibing G, Kai C, Alei L. A new software approach to defend against cache-based timing attacks. Information Engineering and Computer Science Conference (ICIECS); 2009. p. 1–4.
11. Kim K, Soontae S. Reducing area overhead for error-protecting large L2/L3 caches. IEEE Transactions Computers. 2009; 58(3):300–10.
12. Wang W, Zhenghong Z, Ruby B, Lee L. New cache designs for thwarting software cache-based side channel attacks. ACM SIGARCH, Computer Architecture News. 2007; 35:494–505.
13. Grabher P, Großschädl J, Page D. Cryptographic side-channels from low-power cache memory in Cryptography and Coding. 11th IMA International Conference; U K. 2007. p. 170–84.
14. Bertoni G, Zaccaria V, Breveglieri L, Monchiero M, Palermo G. AES power attack based on induced cache miss and countermeasure. Information Technology: Coding and Computing, ITCC International Conference on IEEE; Italy. 2005. p. 586–91.
15. Olanrewaju RF, Al-Qudah DMM, Azman AW, Yaacob M. Intelligent web proxy cache replacement algorithm based on adaptive weight ranking policy via dynamic aging. Indian Journal of Science and Technology. 2016; 9(36):1–7.
16. Kalla AK, Sharma SK. Selective placement of caches for hash-based off-path caching in ICN. Indian Journal of Science and Technology. 2016; 9(37):1–9.
17. Bharathi SM, Sai RV, Saravanan S. Improving the reliability of cache memories using identical tag bits. Indian Journal of Science and Technology. 2016; 9(29):1–5.
18. Vandhana MS, Sai RV, Saravanan S. Cell stability and power reduction using dynamic isolated read static random access memory. Indian Journal of Science and Technology. 2016; 9(29):1–6.
19. Sai RV, Saravanan S, Anandkumar V. Implementation of a novel data scrambling based security measure in memories for VLSI circuits. Indian Journal of Science and Technology. 2015; 8(35):1–6.
20. Subha S. An exclusive cache architecture with power saving. Indian Journal of Science and Technology. 2015; 8(33):1–5.
21. Shanmugarathinam G, Vivekanandan K. Performance analysis of cache consistency maintenance in mobile environment using agent technique. Indian Journal of Science and Technology. 2013 Nov; 6(11):1–6.