西 南 交 通 大 学 学 报

第 54 卷第 6 期
2019 年 12 月

JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY

Vol. 54 No. 6
Dec. 2019

ISSN: 0258-2724 DOI：10.35741/issn.0258-2724.54.6.2

Research article

Computer and Information Science

A SURVEY: CRYPTOGRAPHIC HASH FUNCTIONS FOR DIGITAL STAMPING

调查：用于数字戳记的密码散列函数

Israa Ezzat Salem, Adil M. Salman, Maad M. Mijwil
Baghdad College of Economic Sciences University
Al-Ramadan (Housing), M/625, g/21, d/32, Baghdad, Iraq, israa.ezzat@baghdadcollege.edu.iq, adelmsk63@baghdadcollege.edu.iq, mr.maad.alnaimiy@baghdadcollege.edu.iq

Abstract

The current study aims to examine a general overview of the application of hash functions in cryptography and study the relationships between cryptographic hash functions and uses of the digital signature. Functions of the cryptographic hash are an important tool applied in several sections of data security, and application of hash function is common and used for various purposes such as File Integrity Verification, Key Derivation, Time stamping, Password Hashing, Rootkit Detection and Digital Signature. Digital Signature is a code that is linked electronically with the document including the sender's identity. Therefore, the digital signature is of high value in verifying digital messages or documents. Cryptographic hash functions do not present without mathematics. The success of computer science is attributed to mathematics; in other words, it is because of mathematical science, that computer science was understood and could be explained to all. The study aims to teach the reader hash functions and its applications such as digital signature and to show in details some hash functions and their designing.

Keywords: Hash Function, Cryptography, Digital Stamping

摘要 当前的研究旨在检查哈希函数在密码学中的应用概述，并研究密码哈希函数与数字签名使用之间的关系。密码散列的功能是在数据安全性的多个部分中应用的重要工具，并且散列功能的应用是常见的，并用于各种目的，例如文件完整性验证，密钥派生，时间戳，密码散列，根套件检测和数字签名。数字签名是一种与文件电子链接的代码，包括发件人的身份。因此，数字签名在验证数字消息或文档中具有很高的价值。没有数学就不会出现密码哈希函数。计算机科学的成功归功于数学。换句话说，正是由于数学科学，计算机科学才被理解并可以向所有人解释。该研究旨在教给读者哈希函数及其应用（例如数字签名），并详细显示一些哈希函数及其设计。

关键词: 哈希函数，密码学，数字印记

I. INTRODUCTION

The digital stamp in scrapbooking, stamping and crafting is printed on the paper in TIFF, JPG and PNG formats. Digital stamps have many advantages compared to rubber stamps because it

can be resized, flipped, easily stored and rotated [1].

Also, the digital stamps can be printed on several types of papers using several colours if it is sealed such as watercolours, Copic markers, and coloured pencil. Many companies all over the world produce digital stamps [2].

The digital stamp in philately and mail is the same stamp of the postage except that it stays inside the computer. But the digital stamp can be printed and downloaded. Some artistamp issuing remained as pictures in the digital world [3]. The digital stamp can be replaced and duplicated for easily authorization and exchanging of data [4].

The function of the cryptographic hash is a mathematical function. Hash functions are usually inputted in certain length and output at a fixed length. The function of cryptographic hash is combined with message-passing with security properties [5].

Hash functions are used to input information into the computing systems, such as authenticating information and checking message integrity. Function cryptographic hash adds security aspect to the hash functions, making it difficult to detect the message information [6].

Cryptographic hash functions have three properties:

1. Two input hashes to resemble output hash that are called collision-free;
2. Impossible to know input value depends on output value that are called hidden;
3. Impossible to choose input value that a pre-defined output its puzzle-friendly [7].

II. Literature Review and Related Work

Hash functions are often used in all data security applications. It is a mathematical function. Hash values or message digest are values returned by a hash function [8].

A. Types of Hash Functions

1) Fixed Length Output:

- Hashing the data hash is process that includes converting length (arbitrary) to the fixed length;
- The hash value is smaller from input data; compression functions are called on hash functions;
- Digest means the hash is a small data, as it compares with large data;
- Values of hash functions ranged between (160-512) bits.

2) The Efficiency of Operation:

- Fast operation means the hash function with the input represents h(x). Wherever h indicates the hash function, and x indicates the input;
- The symmetric encryption is slower than the hash functions [9], [10], [50].

B. Hash Function Properties

1) Pre-Image Resistance

It is difficult to reverse a hash function. When the hash function produces hash value, that means it is very difficult to determine the concluding input value (x). That protects against an attacker.

a) Second Pre-Image Resistance

It is hard to find the input value with the same hash. This prevents the attacker who has a hash value and its input, and they try to change to another value;

b) Collision Resistance

It is impossible to get two inputs to have the same hash. Finding tow inputs (x) and (y) by has function [11], [12].

III. Hashing Algorithm Design

The mathematical function hashing works on two fixed-sizes to create a hash code. Usually, the block size consists of (128-512) bits. Hashing algorithm includes many hash function rounds such as block cipher. All rounds take input that has a fixed size, a combination of message blocks, and the output of the last round. The operation included repeating many rounds and it needs to hash all messages [13].

A. Hash Functions

1) Message Digest

Such as MD5 is used as a hash function for a long time. It included MD2, MD4, MD5 and MD6. File servers usually provide MD5. The analytical attack was confirmed as successful in an hour. The collision attack produces in MD5.

2) Secure Hash Function

It included four types of SHA are SHA-3, SHA-2, SHA-1, SHA-0. In spite of it belonging to the same family, it has several forms depending on the structure. (SHA-0) the original version is consisting of (160) bit; in 1993, in 1995, SHA-1 was made for correcting of SHA-0 weaknesses and it is the most common.

3) RIPEMD

It is a set of hash functions that has worked. RIPEMD-160 and RIPEMD-128 are examples of RIPENED. It has two versions: 256 and 320-bit.

4) Whirlpool

It consists of a 512-bit hash function. There are several types, including WHIRLPOOL, WHIRLPOOL-T, WHIRLPOOL-0, which are three widely used versions [14], [15].

B. Hash Function Applications

1) Password Storage

It protects the password. It prevents storing of password in the clear. The Password file included table contains (Id, h (P).

2) Checking Data Integrity

It is common in the hash functions. Check sums on data files were generated from it. Checks the application correctness of the data and assures the users.

3) Digital Signatures

They are keys used for message authentication. The handwritten signatures are used commonly with the messages. A digital signature is a procedure link the person identified with the digital data [16], [17].

C. The General Explanation of the Process

1. Each one using this scheme has two keys (public and private);
2. The two keys could be used for signing/verifying. Encryption/decryption are different wherever the public key is for verification and the private key is for signature;
3. The one provided the data to the hash function;
4. Hash value and signature key are feeding the signature algorithm those results in the digital signature;
5. The verifier feeds the verification key and digital signature in the verification algorithm that it provided some output value;
6. The user uses the same specific data hash function to make the hash value;
7. After compression between the hash value and output of the verification algorithm, the verifier knows the digital signature is incorrect;
8. Digital signature is generated by private key of user [18], [19].

D. Digital Signature Importance

The public key is considered an important tool for dealing with data security. The digital signature gives message authentication and data integrity.

1) Data Integrity

If the attacker succeeds in getting the information, the digital signature doesn't work. Output and changed data do not match.

2) Message Authentication

The user knows the digital signature by using the public key.

3) Non-Repudiation

The user only knows the signature key, and he is only able to use it to create a unique signature [20], [21].

E. Encryption with a Digital Stamp

Document encryption makes a document illegible to anybody except for the owner of the key that allows decryption. Encryption of the digital stamp grants confidentiality of the information [22].

Encryption of a message or document in such a way that only a particular user can read it, the sender must have at their disposal a certificate of said user, as encryption needs to use the public key. To decrypt a document, the user must have his smartcard, as encryption needs to use the private key [23].

Encryption and a digital stamp can be mixed: a document can be signed and subsequently encrypted, to grant both authorship and privacy [24], [25].

IV. Applications of Cryptographic Hash Functions

1. *Message Digest*: the function that doesn't produce output values from the input or are sometimes called irreversibility;
2. *Password Verification:* is included in password verification;
3. *Data Structures:* many programming languages have been used in Data Structures. The main aim is to generate unique key-value pair, and it can be different keys, such as Hash Set, C++, and Java Hash Map;
4. *Compiler Operation:* the difference between the keywords of a programming language and other identifiers wherever the compiler saves all keywords in implemented groups;
5. *Rabin-Karp Algorithm:* the difference between the keywords of a programming

language and other identifiers wherever the compiler saves all keywords in implemented groups;

6. *Name and path of the file together:* When observing files, we will find that the two components are the file path and file name. The map is used for storing the name and path of the file and is implemented by a hash table [26], [27];

7. *Digital stamp:* it is the same postage stamp in the mail, except it is saved in the computer. It can be downloaded and printed onto packages.

A. Digital Documents (Text, Audio, Video)

Due to the wide using of video and images, the hashing technique becomes more important [28]. The digital fingerprinting is a technique that is used to prevent any hacker user from getting multimedia data [29], [30]. Also, it uses wireless networking and mobile computing techniques; multimedia data is often distributed through unreliable wireless channels where packet losses or errors may occur [31], [32]. Hash functions are used widely in the digital world. It is used for identifying similar files (e.g. spam/virus detection). Also, it uses the image classification for processing high-dimensional data [33], [34]. Hashing is used for high search speed and low storage cost, compact binary codes, and integrates image representation learning [35].

B. Simple Scheme Based on the Third Party

Authentication of the public key is important to prevent using the public key by a fake user. Without authentication, the hacker could take, read, and use all encrypted messages between the receiver and sender. The certificate is provided and digitally signed such as the CA signature. When the CA is destroyed by war or terror or by system faults, the assumption cannot be preserved. We should find a practical and simple scheme for authentication of the public key without a third party. The message authentication code was used by the scheme to taking a short value for authenticating public keys [36], [37], [38].

C. Make Use of Merkle Tree in Digital Stamping

A Merkle tree is a tree. Hash trees or the Merkle tree allows verification and efficiency of data. Hash trees consist of hash chains and hash lists. The leaf node is shown a part of a hash tree which requires a digital number of hashes [39].

Hash trees could verifiy all types of stored data. It can receive the data blocks on the peer-to-peer network. Also, the hash trees are used in the Btrfs, ZFS and IPFS, Apache Wave protocol, Dat protocol, Tahoe-LAFS backup system, and Zeronet [40], [41].

V. Advantage and a Disadvantage of Digital Stamping

A. Advantages of Digital Signatures

A digital stamp can be printed for scrapbooking, cardstocks, and card making. The digital stamps take many different formats, such as TIFF, JPG, and PNG. It can be rotated, flipped, easily stored, and resized. Also, it could take any colour when it is sealed by heating. Its digital stamp application is easily applicable.

A digital stamp could be printed and downloaded as packages or envelopes by authorized persons. Furthermore, it could be encoded as remarking or approving on a digital copy of the file. The digital paper stamp can be initialed, signed, or remarked in a unique manner [42], [43].

B. The Disadvantage of Digital Stamping

The digital stamps limitations are only fit for projects on printed images. This means its uses digital stamp images on the surfaces which cannot be run through a printer. So, it is difficult to use digital stamps on pre-formed boxes, fabric, and cardstock, very thick or thin paper, pre-formed boxes and large pieces of paper.

Many of the digital stamps features are used with traditional stamps, in addition to the ever-expanding stamping family [44], [45], [46], [47], [48], [49].

VI. Conclusion

Using the hash functions in cryptography is very important, especially with the digital stamp. The cryptographic hash functions have significant benefits in information security wherever; it provides top security to messages and documents, the cryptographic hash function is used in File Integrity Verification, Key Derivation, Password Hashing, Digital Time-Stamping. The digital stamp is a digital code which is attached to the messages to give high authority and for confirming the sender's identity. Developing A digital stamp are developing of data security. All digital security depends on verifying the identity of senders and receivers. Developing digital stamp will make more people use computer application safety and without problems.

REFERENCES

[1] LI, A. (2006) Fast Photo Time-Stamp Recognition Based on SGNN. In: *Proceedings of the International Symposium on Neural Networks: Advances in Neural Networks, Chengdu, May-June 2006.* Berlin, Heidelberg: Springer, pp. 316-321.

[2] LADANI, M.J. and GAZANCHAEI, A.K. (2014) Using Asynchronous Hot Standby Spare in Time-Stamped, Fault-Tolerant, Real-Time System. In: JIA, L., LIU, Z., QIN, Y., ZHAO, M., and DIAO, L. (eds.) *Proceedings of the International Conference on Electrical and Information Technologies for Rail Transportation - Volume II. Lecture Notes in Electrical Engineering*, Vol. 288. Berlin, Heidelberg: Springer, pp. 309-312.

[3] WEIK, M.H. (2000) Time Stamp. In: *Computer Science and Communications Dictionary.* Boston, Massachusetts: Springer.

[4] HABER, S. and MASSIAS, H. (2005) Time-stamping. In: VAN TILBORG, H.C.A. (ed.) *Encyclopedia of Cryptography and Security*. Boston, Massachusetts: Springer.

[5] BAO, F.M., LI, A.G., and QIN, Z. (2004) Photo Time-Stamp Recognition Based on Particle Swarm Optimization. In: *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence, Beijing, September 2004.* Los Alamitos: IEEE Computer Society, pp. 529-532.

[6] YIN, P., HUA, X.S., and ZHANG, H.J. (2002) Automatic Time Stamp Extraction System for Home Videos. In: *Proceedings of the 2002 IEEE International Symposium on Circuits and Systems, Scottsdale, Arizona, May 2002.* New York: Institute of Electrical and Electronics Engineers, pp. 73-76.

[7] RJAŠKO, M. (2012) Black-Box Property of Cryptographic Hash Functions. In: GARCIA-ALFARO, J. and LAFOURCADE, P. (eds.) *Foundations and Practice of Security. Lecture Notes in Computer Science*, Vol. 6888. Berlin, Heidelberg: Springer, pp. 181-193.

[8] AMERICAN NATIONAL STANDARDS INSTITUTE (2000) *ANSI X9.71. Keyed-Hash Message Authentication Code.* Washington, District of Columbia: American National Standards Institute.

[9] ANDREEVA, E., NEVEN, G., PRENEEL, B., and SHRIMPTON, T. (2007) Seven-Property-Preserving Iterated Hashing: ROX. In: KUROSAWA, K. (ed.) *Advances in Cryptology, Proceedings Asiacrypt'07. Lecture Notes in Computer Science*, Vol. 4833. Berlin: Springer, pp. 130-146.

[10] BELLARE, M., CANETTI, R., and KRAWCZYK, H. (1996) Keying Hash Functions for Message Authentication. In: KOBLITZ, N. (ed.) *Advances in Cryptology – Crypto '96. Lecture Notes in Computer Science*, Vol. 1109. Berlin, Heidelberg: Springer, pp. 1-15.

[11] CANETTI, R. (1997) Towards realizing random oracles: Hash functions that hide all partial information. In: KALISKI, B.S. (ed.) *Advances in Cryptology - CRYPTO '97. Lecture Notes in Computer Science*, Vol. 1294. Berlin, Heidelberg: Springer, pp. 455-469.

[12] YONEYAMA, K. and HANAOKA, G. (2014) Compact Public Key Encryption with Minimum Ideal Property of Hash Functions. In: CHOW, S.S.M., LIU, J.K., HUI, L.C.K., and YIU, S.M. (eds.) *Provable Security. Lecture Notes in Computer Science*, Vol. 8782. Cham: Springer, pp. 178-193

[13] FARACH, M. and MUTHUKRISHNAN, S. (1996) Perfect hashing for strings: Formalization and algorithms. In: HIRSCHBERG, D. and MYERS, G. (eds.) *Combinatorial Pattern Matching. Lecture Notes in Computer Science*, Vol. 1075. Berlin, Heidelberg: Springer, pp. 130-140.

[14] CHANG, D., LEE, S., NANDI, M., and YUNG, M. (2006) Indifferentiable Security Analysis of Popular Hash Functions with Prefix-Free Padding. In: LAI, X. and CHEN, K. (eds.) *Advances in Cryptology – ASIACRYPT 2006. Lecture Notes in Computer Science*, Vol. 4284. Berlin, Heidelberg: Springer, pp. 283-298.

[15] BHATTACHARYYA, R., MANDAL, A., and NANDI, M. (2009) Indifferentiability Characterization of Hash Functions and Optimal Bounds of Popular Domain Extensions. In: ROY, B. and

SENDRIER, N. (eds.) *Progress in Cryptology - INDOCRYPT 2009. Lecture Notes in Computer Science*, Vol. 5922. Berlin, Heidelberg: Springer, pp. 199-218.

[16] BALUJA, S. and COVELL, M. (2008) Learning to hash: forgiving hash functions and applications. *Data Mining and Knowledge Discovery*, 17 (3), pp. 402-430.

[17] ALON, N. and GUTNER, S. (2007) Balanced Families of Perfect Hash Functions and Their Applications. In: ARGE, L., CACHIN, C., JURDZIŃSKI, T., and TARLECKI, A. (eds.) *Automata, Languages and Programming. ICALP 2007. Lecture Notes in Computer Science*, Vol. 4596. Berlin, Heidelberg: Springer, pp. 435-446.

[18] KIRSCH, A., MITZENMACHER, M., and VARGHESE, G. (2010) Hash-Based Techniques for High-Speed Packet Processing. In: CORMODE, G. and THOTTAN, M. (eds.) *Algorithms for Next Generation Networks. Computer Communications and Networks.* London: Springer, pp. 181-218.

[19] IWAMOTO, M., PEYRIN, T., and SASAKI, Y. (2013) Limited-Birthday Distinguishers for Hash Functions. In: SAKO, K. and SARKAR, P. (eds.) *Advances in Cryptology - ASIACRYPT 2013. Lecture Notes in Computer Science*, Vol. 8270. Berlin, Heidelberg: Springer, pp. 504-523.

[20] ZHANG, L., SHAN, L., and WANG, J. (2012) Summary of Digital Signature. In: ZENG, D. (ed.) *Advances in Control and Communication. Lecture Notes in Electrical Engineering*, Vol. 137. Berlin, Heidelberg: Springer, pp. 115-120.

[21] ZHENG, Y. (1997) Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption). In: KALISKI, B.S. (ed.) *Advances in Cryptology - CRYPTO '97. CRYPTO 1997. Lecture Notes in Computer Science*, Vol. 1294. Berlin, Heidelberg: Springer, pp. 165-179.

[22] SUN, X. (2010) An Improved Symmetric Key Encryption Algorithm for Digital Signature. In: LUO, Q. (ed.) *Advances in Wireless Networks and Information Systems. Lecture Notes in Electrical Engineering*, Vol. 72. Berlin, Heidelberg: Springer.

[23] KATZ, J. and LINDELL, Y. (2008) *Introduction to Modern Cryptography*. Boca Raton, London, New York, Washington, District of Columbia: Chapman & Hall/CRC.

[24] SCHNEIER, B. (2004) Cryptanalysis of MD5 and SHA: Time for a New Standard. *Computer World*. Available from https://www.schneier.com/essays/archives/2004/08/cryptanalysis_of_md5.

[25] SCHNEIER, B. (1996) *Applied Cryptography*. Hoboken, New Jersey: John Wiley & Sons, Computer Security Division - Computer Security Resource Center.

[26] BROMBERG, L. (2017) Cryptographic Hash Functions and Some Applications to Information Security. In: NATHANSON, M. (ed.) *Combinatorial and Additive Number Theory II. CANT 2015, CANT 2016. Springer Proceedings in Mathematics & Statistics*, Vol. 220. Cham: Springer, pp. 85-97.

[27] PETIT, C. and QUISQUATER, J.J. (2016) Cryptographic Hash Functions and Expander Graphs: The End of the Story? In: RYAN, P., NACCACHE, D., and QUISQUATER, J.J. (eds.) *The New Codebreakers. Lecture Notes in Computer Science*, Vol. 9100. Berlin, Heidelberg: Springer, pp. 304-311.

[28] WANG, G., HU, Q., CHENG, J., and HOU, Z. (2018) Semi-supervised Generative Adversarial Hashing for Image Retrieval. In: FERRARI, V., HEBERT, M., SMINCHISESCU, C., and WEISS, Y. (eds.) *Computer Vision – ECCV 2018. Lecture Notes in Computer Science*, Vol. 11219. Cham: Springer, pp. 491-507.

[29] LIU, C., LING, H., ZOU, F., WANG, Y., FENG, H., and YAN, L. (2015) Local and global structure preserving hashing for fast digital fingerprint tracing. *Multimedia Tools and Applications*, 74 (18), pp. 8003-8023.

[30] WU, F., HAN, Y., LIU, X., SHAO, J., ZHUANG, Y., and ZHANG, Z. (2012) The heterogeneous feature selection with structural sparsity for multimedia annotation and hashing: a survey. *International Journal of Multimedia Information Retrieval*, 1 (1), pp. 3-15.

[31] SHIN, J. and RULAND, C. (2015) Perceptual Image Hashing Technique for Image Authentication in WMSNs. In: ŽIVIĆ, N. (ed.) *Robust Image Authentication in the Presence of Noise.* Cham: Springer, pp. 75-103.

[32] LU, C.S. and HSU, C.Y. (2005) Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication. *Multimedia Systems,* 11 (2), pp. 159-173.

[33] BREITINGER, F. and BAIER, H. (2013) Similarity Preserving Hashing: Eligible Properties and a New Algorithm MRSH-v2. In: ROGERS, M. and SEIGFRIED-SPELLAR, K.C. (eds.) *Digital Forensics and Cyber Crime. ICDF2C. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,* Vol. 114. Berlin, Heidelberg: Springer, pp. 167-182.

[34] LIU, Y., BAI, X., YAN, C., and ZHOU, J. (2017) Bilinear Discriminant Analysis Hashing: A Supervised Hashing Approach for High-Dimensional Data. In: LAI, S.H., LEPETIT, V., NISHINO, K., and SATO, Y. (eds.) *Computer Vision – ACCV 2016. Lecture Notes in Computer Science,* Vol. 10115. Cham: Springer, pp. 297-310.

[35] LI, Q., FU, H., KONG, X., and TIAN, Q. (2018) Deep hashing with top similarity preserving for image retrieval. *Multimedia Tools and Applications,* 77 (18), pp. 24121-24141.

[36] KOO, J.H., KIM, B.H., and LEE, D.H. (2005) Authenticated Public Key Distribution Scheme without Trusted Third Party. In: ENOKIDO, T., YAN, L., XIAO, B., KIM, D., DAI, Y., and YANG, L.T. (eds.) *Embedded and Ubiquitous Computing – EUC 2005 Workshops. Lecture Notes in Computer Science,* Vol. 3823. Berlin, Heidelberg: Springer, pp. 926-935.

[37] KWON, T. (2004) Practical authenticated key agreement using passwords. In: ZHANG, K. and ZHENG, Y. (eds.) *Information Security. ISC 2004. Lecture Notes in Computer Science,* Vol. 3225. Berlin, Heidelberg: Springer, pp. 1-12.

[38] BULDAS, A., LAUD, P., LIPMAA, H., and VILLEMSON, J. (1998) Time-Stamping with Binary Linking Schemes. In: KRAWCZYK, H. (ed.) *Advances in Cryptology — CRYPTO '98. CRYPTO 1998. Lecture Notes in Computer Science,* Vol. 1462. Berlin, Heidelberg: Springer, pp. 486-501.

[39] MERKLE, R.C. (1988) A Digital Signature Based on a Conventional Encryption Function. In: POMERANCE, C. (ed.) *Advances in Cryptology — CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science,* Vol. 293. Berlin, Heidelberg: Springer, pp. 369-378.

[40] MAHJABIN, S. (2018) Implementation of DoS and DDoS Attacks on Cloud Servers. *Periodicals of Engineering and Natural Sciences,* 6 (2), pp. 148-158.

[41] MCGREW, D., CURCIO, M., and FLUHRER, S. (2018) *Hash-based signatures.* [Online] Crypto Forum Research Group. Available from: https://tools.ietf.org/id/draft-mcgrew-hash-sigs-11.html [Accessed 29/08/19].

[42] GUERON, S. and MOUHA, N. (2017) *SPHINCS-Simpira: Fast stateless hash-based signatures with post-quantum security.* [Online] IACR Cryptology ePrint Archive. Available from: https://eprint.iacr.org/2017/645 [Accessed 30/08/19].

[43] PAAR, C. and PELZL, J. (2010) *Understanding Cryptography: A Textbook for Students and Practitioners.* Berlin, Heidelberg: Springer.

[44] ALHARBI, E. and ABDULLAH, M. (2019) Asthma Attack Prediction based on Weather Factors. *Periodicals of Engineering and Natural Sciences,* 7 (1), pp. 408-419.

[45] MACCORMICK, J. (2012) *Nine Algorithms That Changed the Future: The Ingenious Ideas That Drive Today's Computers.* Princeton, New Jersey: Princeton University Press.

[46] PRIYANKA, Y., SINDHU, S., and VANI, T. (2012) Digital Signature. *International Journal of Engineering and Management Sciences,* 3 (2), pp. 115-118.

[47] BOYD, C. and MAO, W. (2003) *Information Security: 6th International Conference.* New York: Springer.

[48] SOMNATH, S. (2019) Lightweight novel trust based framework for IoT enabled wireless network

communications. *Periodicals of Engineering and Natural Sciences*, 7 (3), pp. 1126-1137.
[49] MOHAMMED, G.N., AL-FATLAWI, A.A.H., and KAMIL, A.T. (2019) Combined DWT-DISB based image watermarking optimized for decision making problems. *Periodicals of Engineering and Natural Sciences*, 7 (3), pp. 1009-1020.
[50] HUSSEIN, K.A., MEHDI, S.A., and HUSSEIN, S.A. (2019) Image Encryption Based on Parallel Algorithm via Zigzag Manner with a New Chaotic System. *Journal of Southwest Jiaotong University*, 54(4).

参考文:

[1] LI，A。（2006）基于神经网络的快速照片时间戳识别。于：《神经网络国际研讨会论文集：神经网络的进展》，成都，2006 年 5 月至 6 月。柏林，海德堡：施普林格，第 316-321 页。
[2] M.J. LADANI 和 A.K. GAZANCHAEI（2014）在带时间戳的，容错的实时系统中使用异步热备件。载于：贾 L.，刘 Z.，秦 Y.，赵 M.和刁 L.（编）《国际铁路运输电子信息技术会议论文集-第二卷》。电气工程讲义，第 1 卷。 288.柏林，海德堡：施普林格，第 309-312 页。
[3] WEIK，M.H.（2000）时间戳。在：计算机科学与通信词典。马萨诸塞州波士顿：施普林格。
[4] HABER，S. 和 MASSIAS，H.（2005）时间戳记。在：VAN TILBORG，H.C.A.（编。）密码学和安全性百科全书。马萨诸塞州波士顿：施普林格。
[5] BAO，F.M.，LI，A.G。和 QIN，Z.（2004）基于粒子群优化的照片时间戳识别。于：2004 年 9 月在北京召开的电气工程师学会 / WIC / ACM 网络智能国际会议论文集。洛斯阿拉米托斯：电气工程师学会计算机协会，第 529-532 页。
[6] 尹平华，华胜兴和张恒杰（2002）家庭视频自动时间戳提取系统。于：2002 年 5 月在亚利桑那州斯科茨代尔举行的 2002 电气工程师学会国际电路与系统研讨会论文集。纽约：电气与电子工程师协会，第 73-76 页。
[7] RJAŠKO，M.（2012）密码哈希函数的黑盒特性。在：GARCIA-ALFARO，J。和 LAFOURCADE，P。（编辑）《安全的基础和实践》中。计算机科学讲义，第一卷。 6888。柏林，海德堡：施普林格，第 181-193 页。
[8] 美国国家标准学会（2000）ANSI X9.71。键控哈希消息认证代码。哥伦比亚特区华盛顿：美国国家标准协会。
[9] ANDREEVA，E.，NEVEN，G.，PRENEEL，B. 和 SHRIMPTON，T.（2007）保留七属性的迭代哈希：罗克斯。于：KUROSAWA，K.（编。）密码学进展，亚洲解密会议论文集 07。计算机科学讲义，第一卷。 4833。柏林：施普林格，第 130-146 页。
[10] BELLARE，M.，CANETTI，R. 和 KRAWCZYK，H.（1996）消息身份验证的键哈希函数。于：KOBLITZ，N.（编。）密码学进展–密码'96。计算机科学讲义，第一卷。 1109.柏林，海德堡：施普林格，第 1-15 页。
[11] CANETTI，R.（1997），实现随机预言：隐藏所有部分信息的哈希函数。在：B.S. KALISKI（编。）密码学的进展-CRYPTO '97。计算机科学讲义，第一卷。 1294.柏林，海德堡：施普林格，第 455-469 页。
[12] YONEYAMA，K. 和 HANAOKA，G.（2014）具有最小哈希函数理想属性的紧凑型公钥加密。于：周小龙，刘建强，许国良和姚小龙（可编辑）。可证明的安全性。计算机科学讲义，第一卷。 8782.湛：施普林格，第 178-193 页
[13] FARACH，M. 和 MUTHUKRISHNAN，S.（1996）字符串的完美哈希：形式化和算法。在：HIRSCHBERG，D。和 MYERS，G。（编辑）组合模式匹配中。计算机科学讲义，第一卷。 1075.柏林，海德堡：施普林格，第 130-140 页。
[14] CHANG, D.，LEE, S.，NANDI, M. 和 YUNG，M.（2006）具有无前缀填充的流

行哈希函数的不可分安全性分析。载于：LAI，X. 和 CHEN，K.（编）密码学进展–亚太统计 2006。计算机科学讲义，第 1 卷。 4284。柏林，海德堡：施普林格，第 283-298 页。

[15] BHATTACHARYYA，R.，MANDAL，A。和 NANDI，M。（2009 年），哈希函数的不可区分性表征和流行域扩展的最优边界。于：ROY，B. 和 SENDRIER，N.（编辑）密码学进展- 2009 年印度文字。 5922。柏林，海德堡：施普林格，第 199-218 页。

[16] BALUJA，S. 和 COVELL，M.（2008）学习哈希：原谅哈希函数和应用程序。数据挖掘和知识发现， 17(3)，第 402-430 页。

[17] ALON，N. 和 GUTNER，S.（2007）完美哈希函数的平衡族及其应用。在：ARGE，L.，CACHIN，C.，JURDZIŃSKI，T. 和 TARLECKI，A.（编辑）自动机，语言和程序设计中。 ICALP2007。计算机科学讲义，第 1 卷。 4596。柏林，海德堡：施普林格，第 435-446 页。

[18] KIRSCH，A.，MITZENMACHER，M。和 VARGHESE，G。（2010 年）《基于哈希的高速数据包处理技术》。在：CORMODE，G。和 THOTTAN，M.（编辑）的下一代网络算法中。计算机通信和网络。伦敦：施普林格，第 181-218 页。

[19] IWAMOTO，M.，PEYRIN，T. 和 SASAKI，Y.（2013）哈希函数的有限生日鉴别器。在：SAKO，K. 和 SARKAR，P.（编辑）密码学的进展-亚洲科技 2013。 8270。柏林，海德堡：施普林格，第 504-523 页。

[20] 张琳，单琳，和王健（2012）数字签名摘要。在：ZENG，D.（编。）控制和通信进展。电气工程讲义，第 1 卷。 137. 柏林，海德堡：施普林格，第 115-120 页。

[21] ZHENG Y.（1997）数字签章或如何实现费用（签章和加密）≪费用（签章）+ 费用（加密）。在：B.S. KALISKI（编。）密码学的进展-CRYPTO '97。加密 1997。计算机科学讲义，第 1 卷。 1294.柏林，海德堡：施普林格，第 165-179 页。

[22] SUN，X.（2010）一种改进的用于数字签名的对称密钥加密算法。在：LUO，Q。（编辑）无线网络和信息系统的进展中。电气工程讲义，第 1 卷。 72.柏林，海德堡：施普林格。

[23] KATZ，J. 和 LINDELL，Y.（2008）现代密码学导论。博卡拉顿，伦敦，纽约，华盛顿，哥伦比亚特区：查普曼和霍尔/CRC。

[24] SCHNEIER，B.（2004）对 MD5 和 SHA 的密码分析：新标准的时间。计算机世界。可从 https://www.schneier.com/essays/archives/2004/08/cryptanalysis_of_md5 获得。

[25] SCHNEIER，B.（1996）应用密码学。新泽西州霍博肯：约翰· 威利父子，计算机安全部门-计算机安全资源中心。

[26] BROMBERG，L.（2017）密码哈希函数和信息安全的某些应用。在：NATHANSON，M.（编）组合和加法数论 II。 2015 年不能，2016 年不能。施普林格论文集，《数学与统计》，第 1 卷。 220. 湛：施普林格，第 85-97 页。

[27] PETIT，C。和 QUISQUATER，J.J.。（2016）密码哈希函数和扩展图：故事的结局？在：RYAN，P.，NACCACHE，D. 和 QUISQUATER，J.J.（编）。新密码破解者。计算机科学讲义，第一卷。 9100。柏林，海德堡：施普林格，第 304-311 页。

[28] WANG，G.，HU，Q.，CHENG，J.，和 HOU，Z.（2018）用于图像检索的半监督生成对抗式哈希。在：FERRARI，V.，HEBERT，M.，SMINCHISESCU，C. 和 WEISS，Y.（编辑）计算机视觉– ECCV 2018。 11219. 湛：施普林格，第 491-507 页。

[29] LIU，C.，LING，H.，ZOU，F.，WANG，Y.，FENG，H. 和 YAN，L.（2015）保留哈希的本地和全局结构，用于快速数字指纹跟踪。多媒体工具和应用，74（18），第 8003-8023 页。

[30] WU，F.，HAN，Y.，LIU，X.，SHAO，J.，ZHUANG，Y.，和 ZHANG，

Z.（2012）带有结构稀疏性的异构特征选择，用于多媒体注释和哈希：调查。国际多媒体信息检索杂志，1（1），第 3-15 页。
[31] SHIN，J. 和 RULAND，C.（2015）WMSN 中用于图像认证的感知图像哈希技术。在：北卡罗来纳州的 IVI（（编辑）在存在噪声的情况下进行稳健的图像认证。湛：施普林格，第 75-103 页。
[32] LU，C.S. 和 HSU，C.Y.（2005）几何失真弹性图像哈希方案及其在复制检测和认证中的应用。多媒体系统，11（2），第 159-173 页。
[33] BREITINGER，F. 和 BAIER，H.（2013）相似性保留哈希：合格属性和新算法 MRSH-v2。于：M. ROGERS 和 K.C. SEIGFRIED-SPELLAR。（合编）数字取证和网络犯罪。ICDF2C。计算机科学，社会信息学和电信工程学院，第 1 卷的讲义。114.柏林，海德堡：施普林格，第 167-182 页。
[34] LIU，Y.，BAI，X.，YAN，C。和 ZHOU，J。（2017）双线性判别分析哈希：一种用于高维数据的监督哈希方法。在：LAI，S.H.，LEPETIT，V.，NISHINO，K. 和 SATO，Y.（编辑）《计算机视觉– ACCV 2016》中。10115. 湛：施普林格，第 297-310 页。
[35] LI，Q.，FU，H.，KONG，X.，和 TIAN，Q.（2018）保留具有顶级相似性的深度哈希用于图像检索。多媒体工具和应用，77（18），第 24121-24141 页。
[36] KOO，J.H.，KIM，B.H. 和 LEE，D.H.（2005）经过认证的无受信任第三方的公钥分发方案。在：ENOKIDO，T.，YAN，L.，XIAO，B.，KIM，D.，DAI，Y.，和 YANG，L.T.（合编）嵌入式和泛在计算– EUC 2005 研讨会。计算机科学讲义，第一卷。3823。柏林，海德堡：施普林格，第 926-935 页。
[37] KWON，T.（2004）使用密码的实用认证密钥协议。于：张 K 和郑 Y（主编）信息安全。ISC2004。计算机科学讲义，第 1 卷。3225。柏林，海德堡：施普林格，第 1-12 页。
[38] BULDAS，A.，LAUD，P.，LIPMAA，H. 和 VILLEMSON，J.（1998）带有二进制链接方案的时间戳。在：KRAWCZYK，H.（编。）密码学进展—加密'98。加密 1998。计算机科学讲义，第 1 卷。1462 年。柏林，海德堡：施普林格，第 486-501 页。
[39] 默克（RC）（1988）基于常规加密功能的数字签名。在：POMERANCE，C。（编），密码学进展—加密’87。加密 1987 年。计算机科学讲义，第 1 卷。293. 柏林，海德堡：施普林格，第 369-378 页。
[40] MAHJABIN，S.（2018）在云服务器上实施拒绝服务和拒绝服务攻击。工程与自然科学期刊，6（2），第 148-158 页。
[41] MCGREW，D.，CURCIO，M. 和 FLUHRER，S.（2018）基于哈希的签名。[在线]加密论坛研究组。可从以下网站获得：https://tools.ietf.org/id/draft-mcgrew-hash-sigs-11.html [访问时间：19/08/29]。
[42] GUERON，S. 和 MOUHA，N.（2017）菲尼克斯-辛皮拉：具有后量子安全性的基于无状态哈希的快速签名。[在线] IACR 密码学电子打印存档。可从以下网站获得：https://eprint.iacr.org/2017/645 [1919 年 8 月 30 日访问]。
[43] PAAR，C。和 PELZL，J。（2010 年），《了解密码学：学生和从业者的教科书》。柏林，海德堡：施普林格。
[44] ALHARBI，E. 和 ABDULLAH，M.（2019）基于天气因素的哮喘发作预测。工程与自然科学期刊，7（1），第 408-419 页。
[45] MACCORMICK，J.（2012）改变未来的九种算法：推动当今计算机发展的精巧思想。新泽西州普林斯顿：普林斯顿大学出版社。
[46] PRIYANKA，Y.，SINDHU，S. 和 VANI，T.（2012）数字签名。国际工程与管理科学杂志，3（2），第 115-118 页。
[47] BOYD，C. 和 MAO，W.（2003）信息安全：第六届国际会议。纽约：施普林格。

[48] SOMNATH，S.（2019）用于物联网的无线网络通信的轻量新颖的基于信任的框架。工程与自然科学期刊，7（3），第 1126-1137 页。
[49] G.N. MOHAMMED，A.A.H。的 AL-FATLAWI 和 A.T.的 KAMIL （2019）针对决策问题优化的基于载重吨盘的组合图像水印。工程与自然科学期刊，7（3），第 1009-1020 页。
[50] HUSSEIN，K.A.，MEHDI，S.A. 和 HUSSEIN，S.A.（2019）基于并行算法的 Zigzag 方式与新混沌系统的图像加密。西南交通大学学报，54（4）。