Scientific Research Publishing

Open Journal of Applied Sciences, 2016, 6, 893-902
http://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Research and Implementation of Time Synchronous Dynamic Password Based on SM3 Hash Algorithm

Dognery Sinaly Silue[1,2], Wanggen Wan[1,2*], Muhammad Rizwan[1,2]

[1]School of Communications and Information Engineering, Shanghai University, Shanghai, China
[2]Institute of Smart City, Shanghai, China
Email: sdognerysinaly@yahoo.fr, *wanwg@staff.shu.edu.cn

How to cite this paper: Silue, D.S., Wan, W.G. and Rizwan, M. (2016) Research and Implementation of Time Synchronous Dynamic Password Based on SM3 Hash Algorithm. *Open Journal of Applied Sciences*, **6**, 893-902.
http://dx.doi.org/10.4236/ojapps.2016.613077

Received: November 13, 2016
Accepted: December 25, 2016
Published: December 28, 2016

Abstract

With the rapid development of information technology, demand of network & information security has increased. People enjoy many benefits by virtue of information technology. At the same time network security has become the important challenge, but network information security has become a top priority. In the field of authentication, dynamic password technology has gained users' trust and favor because of its safety and ease of operation. Dynamic password, SHA (Secure Hash Algorithm) is widely used globally and acts as information security mechanism against potential threat. The cryptographic algorithm is an open research area, and development of these state-owned technology products helps secure encryption product and provides safeguard against threats. Dynamic password authentication technology is based on time synchronization, using the state-owned password algorithm. SM3 hash algorithm can meet the security needs of a variety of cryptographic applications for commercial cryptographic applications and verification of digital signatures, generation and verification of message authentication code. Dynamic password basically generates an unpredictable random numbers based on a combination of specialized algorithms. Each password can only be used once, and help provide high safety. Therefore, the dynamic password technology for network information security issues is of great significance. In our proposed algorithm, dynamic password is generated by SM3 Hash Algorithm using current time and the identity ID and it varies with time and changes randomly. Coupled with the SM3 hash algorithm security, dynamic password security properties can be further improved, thus it effectively improves network authentication security.

Keywords

Dynamic Password Authentication, SM3 Hash Algorithm, Network Authentication

Security, One Time Password

1. Introduction

Internet and mobile communications have developed rapidly; it increases the demand for securing user authentications in terms of managing money and personal information [1]. However, there is always a risk of monitoring the personal & private data. Therefore, it is necessary to authenticate users securely. If a user sends the same password for every session, an attacker can masquerade as the user and the attacker can get user's password via the Internet. One-time password authentication methods use one-way functions extensively [2]. Moreover, a synchronous data communication procedure is possible for one-time password authentication methods and realizes mutual authentication using a one-time password method. So, the user requires one-time password authentication methods that change the verifier every time. When a user logs in to the system, the user sends masking data to the server and the server certifies the user using those masking data and the stored verifier. Then the user and the server use a one-time password authentication method and apply a one-way function. The security of dynamic password system is mainly dependent on the encryption algorithm. Nowadays, most of the dynamic password technology in the domestic market adopts foreign algorithms, such as RSA, SHA-1, MD4, MD5 and so on [3]. With the growth of such algorithms, probability of cracking these algorithms also increases by time. In 2005 professor Xiaoyun Wang of Shandong University, proposed the cracking strategy of two classic hash algorithm systems (MD5 and SHA-1), so that the collision to crack the hash algorithm has become possible [4]. It has improved construction of signature schemes with forward security in the random oracle model [5]. This shows that in the field of identity authentication, the use of open source algorithms creates more risk of security. For the use of encryption products, No. 273 order of the State Council of China has published the regulation of the administration of commercial cipher, which shows that country attaches great importance to the information security of the localization. In this paper, the design and implementation of a dynamic password technology based on national commercial encryption standard, are proposed to solve the problem as follows: adopting the national commercial encryption SM3 hash algorithm as an encryption algorithm, to achieve the dynamic password authentication and encryption algorithm of domestic design; proposing the time truncated password algorithm based on the time to improve the safety performance of the algorithm [6].

2. Related Technology

2.1. The Definition of Hash Function

Hash function maps arbitrary length input message for fixed length output value, and the fixed length output value is called the input message's hash value. The definition of the hash function can be expressed as: $h:\{0,1\}^* \to \{0,1\}n,\{0,1\}^*$ is a set of bits that

represent arbitrary length; $\{0,1\}n$ is a set of bit strings that represent the length of *n*. In order to ensure the safety of the hash function, hash length *n* should be at least 256 bit. Usually there is the key in operation; the hash function is divided into two parts: hash function with key and hash function without key [7]. It is shows as follows.

2.1.1. Hash Function with Key

Hash function with hash key keeps the key participation in the process of operation. This kind of hash functions is required to satisfy all the security requirements and the hash value depends on the key input message, and key can calculate the corresponding hash value. It not only provides a complete test as well as provides the function for identity authentication, named as message authentication code (MAC). The nature of message and authentication code ensures the generation of right message with hash function [8].

2.1.2. Hash Function without Key

As compared to hash function with key, no key is used by hash function for the input messages, so this type of hash function does not have the function of identity authentication. It provides only integrity checking, such as tampering detection code (MDC). According to the properties of the MDC, it can be divided into weak one-way hash function (OWHF) and strong one-way hash function (CRHF) [9].

2.2. SM3 Hash Algorithm Decryption

The SM3 hash function compresses any message no more than 2^{64}-1 bits into a 256-bit hash value. The algorithm first pads any given message into *n* 512-bit message blocks. The hash function consists of the following two parts: the message expansion and the state update transformation.

Message Expansion: The message expansion of SM3 splits the 512-bit message blocks M into 16 words $w_i\left(0 \le i \le 15\right)$, and expands them into 68 expanded message words $w_i\left(0 \le i \le 67\right)$ and 64 expanded message words $w'_i\left(0 \le i \le 63\right)$ as follows:

$$w_i = P_i\left(w_{i-16} \oplus w_{i-9} \oplus \left(w_{i-3} \lll 15\right)\right) \oplus \left(w_{i-13} \lll 7\right) \oplus w_{i-6}, 16 \le i \le 67,$$

$$w'_i = w_i \oplus w_{i-4}, 0 \le i \le 63, \text{ where } P_1\left(X\right) = X \oplus \left(X \lll 15\right) \oplus \left(X \lll 23\right)$$

State Update Transformation: The state update transformation starts from an initial value $(A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0) = IV$ of eight 32-bit words and updates them in 64 steps. In step $i+1\left(0 \le i \le 63\right)$ the 32-bit words w_i and w'_i are used to update the state variables $A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i$ as follows:

$$SS1_i = \left(\left(A_i \lll 12\right) + E_i + \left(T_i \lll i\right)\right) \lll 7,$$

$$SS2_i = SS1_i \oplus \left(A_i \lll 12\right),$$

$$TT1_i = FF_i\left(A_i, B_i, C_i\right) + D_i + SS2_i + w'_i,$$

$$TT2_i = GG_i\left(E_i, F_i, G_i\right) + H_i + SS1_i + w_i,$$

$$A_{i+1} = TT1_i, B_{i+1} = A_i, C_{i+1} = \left(B_i \lll 9\right), D_{i+1} = C_i,$$

$$E_{i+1} = P_0\left(TT2_i\right), F_{i+1} = E_i, G_{i+1} = \left(F_i \lll 9\right), H_{i+1} = G_i.$$

where $P_0\left(X\right) = X \oplus \left(X \lll 9\right) \oplus \left(X \lll 17\right)$.

The bitwise Boolean functions $FF_i(X_i, Y_i, Z_i)$ and $GG_i(X_i, Y_i, Z_i)$ are defined as follows.

$$FF_i(X_i, Y_i, Z_i) = \begin{cases} X_i \oplus Y_i \oplus Z_i, & 0 \le i \le 15, \\ (X_i \wedge Y_i) \vee (X_i \wedge Z_i) \vee (Y_i \wedge Z_i) & 0 \le i \le 63, \end{cases}$$

$$GG_i(X_i, Y_i, Z_i) = \begin{cases} X_i \oplus Y_i \oplus Z_i, & 0 \le i \le 15, \\ (X_i \wedge Y_i) \vee (\neg X_i \wedge Z_i) & 0 \le i \le 63, \end{cases}$$

If M is the last block, then $A64\_A(A_{64} \oplus A_0, B_{64} \oplus B_0, C_{64} \oplus C_0, D_{64} \oplus D_0, E_{64} \oplus E_0, F_{64} \oplus F_0, G_{64} \oplus G_0, H_{64} \oplus_0)$ is the hash value. Otherwise it is part of the input of the next message block.

2.3. Dynamic Password Generation Algorithm Based on SM3

Dynamic password, also known as a one-time password, which is a one-time e form of a password that changes by time, for user new password is created every time [10] [11]. In a certain time interval, a password can only be used once; repeated use of the same password will be rejected. The main idea of dynamic password is to add some uncertain factors in the process, such as the use of time, frequency of use or random numbers, and these changing factors acts as a dynamic factor of password. The basic goal is to improve the safety of password. Dynamic password technology has many advantages: randomness, dynamic, one-time. The current paper proposed SH3 based algorithm for dynamic password authentication generation based on time [12]. The dynamic password authentication scheme is time saver and used for dynamic token holding, keep synchronization based on time may be considered as dynamic token of the uncertain factors, the mutual authentication using same responsible for the algorithm to generate a consistent user login password. Only legitimate users can hold the token, the token time refreshed after 60 seconds, and creates new token after 60 seconds.

In addition, the time certification system and dynamic password authentication technology is based on, challenge/response mechanism of dynamic password authentication technology and the password sequence of dynamic password authentication technology. This certification system can therefore be explained as follows:

The basic idea of the technology authentication word dynamic password is, to create variable counter value as an uncertain factor and it has no relation with the principle of system time [13]. Therefore, the problem of time synchronization and certification has less communication between the two sides. Challenge and response of dynamic password identity authentication technology are based on the basic idea that the system certification randomly generates a number of challenges to the user. The users generate dynamic password according to the random number and their authentication information.

Proposed method has no strict synchronization requirements, so it can fundamentally avoid the problem of loss of step. But it needs to verify the operational steps, only one-way communication; several typical one-time password authentication mechanism [14] based on the time mechanism is relatively simple, and the client computation is small and has no special hardware requirements, and the anti-attack ability is strong.

The generation of dynamic password [15] is determined by three things; the sequence number "SN", the key and time "T". Sequence number "SN" and key are fixed but time "T" is changed in minutes, so the three factors constitute the text "M" as a variable, that is, the encrypted text is dynamic, so that it can prevent the attack [16]. At this point one-way hash function of the encryption algorithm, first encrypt the plaintext block. Our proposed SM3 algorithm is based on encryption algorithm for the state password, the plaintext string processing length is 256 bits (32 bytes, which accounted for 6 of T bytes of SN 6 bytes of key, 20 bytes). The design obviates the calculation steps of grouping plaintext, realize simple and feasible encryption algorithm.

The serial number "SN", key and time "T" are connected to get the plain text string "M". Time accurate to minutes, the format is "yyyymmddhhmm". For example, t is assumed that the current time is 14:41 in February 27, 2012, that is, T = 201202271441, SN = 555888, key = 11223333445566778899005558881122334455 66.

That is, M = 555888 778899001122334455 667788990020120022 144144556677889-9001122. The overall goal of the above process is to get the initial password, so that it is difficult to guess.

It needs to convert 64-bit hexadecimal number to 6-bitdecimal number to produce the output hash value using SH3 Algorithm [17].

The truncated dynamic password algorithm based on time and the implementation flow in **Figure 1**:

1) User ID, key, and time T after SM3 algorithm generates the hexadecimal array M [64];

2) Take T minute position t, $m = t \bmod 10$, remove the M [t], M [t + 10], M [t + 20], M [t + 30], M [t + 40], M [t +50] composition OTP [5] (hex);

3) The OTP [6] is converted to decimal, and combined into a decimal OTP';

4) result 1 = OTP' mod $10 \wedge 6$, is the final dynamic password generated by the dynamic password token based on SM3 algorithm.

For example, if the current time is 14:53, t = 53 mod 10 = 3 and this time recorded

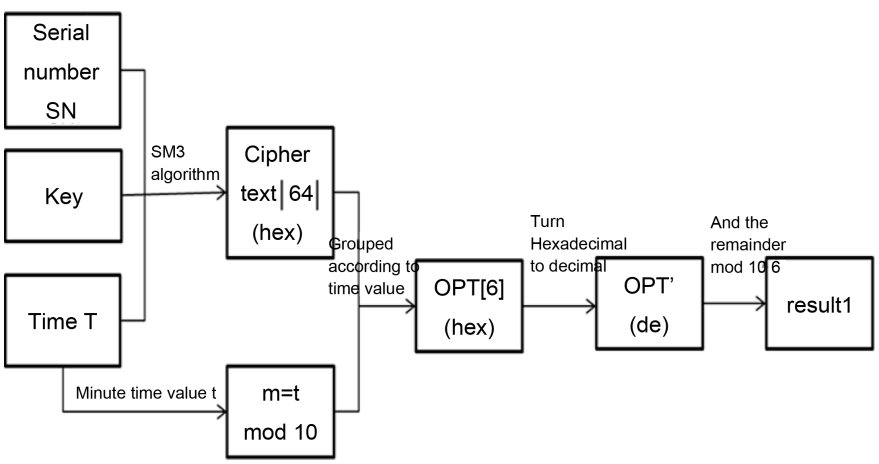

Figure 1. Dynamic password algorithm flowchart.

for T [3], plaintext encrypted, the output value M = debe9ff9 2275b8a1 38604889 c18e5a4d 6fdb70e5 387e5765 293dcba3 9c0c5732,to M [3] = f9, M [13] = 8e, M [23] = 65, order groups into OTP = f98e65, converted to decimal OTP' = 16354917 and eventually generated dynamic password P = 16354917 mod $10 \wedge 6$ = 354917. This method ensures the second dynamic of the password, which makes it impossible for the illegal users to obtain the key by guessing, and further improve the security of the dynamic password algorithm.

3. Implementation of Security Analysis

3.1. Challenge/Response and Time Synchronization Authentication Methods

Dynamic password authentication method is based on challenge/response and time synchronization mode and acts as dynamic authentication method, it has dynamic factor: challenge/response, generate random number by triggering event (such as login) produced Challenge code; it is a way to change the time synchronization time. When challenge/response user for login authentication system generates a random number-the challenge code is sent to the user. The code received by the user in an encryption algorithm which is mixed with the users own password and a random number is sent subsequently to the server, authentication system can authenticate users with the appropriate method for checking.

A time synchronization authentication method is the elapsed time of a factor of change, after hashing we make comparison between the current values of time together with the seed key. Time synchronization is actually a way of parallel computing authentication methods; regular time factor is utilized instead of the random challenge code, thereby reducing the authenticator with the inter-working certified party, simple, easy to use and so on. However, the boundaries of time synchronization authentication method for time synchronization and time accuracy are higher; In order to meet the requirements of time synchronization, time synchronization mode password over time is constant, the delay suffered or replay attacks, and since the time factor is a regular change, increasing the probability of attacks; achieving time synchronization server the challenge is more complex than the response server, usually combined with adaptive calibration mechanism (such as a server implementation of some design time window automatically adjust the design); the reliability of authentication is not as challenge-response type authentication method, the jumping point critical time will have a blind spot. In summary, the dynamic password authentication system improves the authentication mechanism and provides more security against threats; provide more emphasis on safety and reliability and use the challenge-response based authentication methodology [18].

3.2. Encryption/Decryption Mode and Parallel Computation Mode

Challenge/Response authentication can be implemented in two modes; encryption/decryption mode and parallel computation mode. Encryption/decryption mode authenti-

cation can be divided into public key system which is based on symmetric key system. On the other hand, randomized user authentication uses its private or shared symmetric key of the authentication server (AS) emitted RN encrypted challenge code, Then the encrypted authentication result respond back to the server, using the corresponding public key or shared symmetric key to decrypt the response code, as a result if same RN is generated then the user authentication is successful. In the encryption/decryption of authentication mode, the speed is relatively slow due to the complete encryption/decryption process. Especially for asymmetric keys; the most important thing is, even if the user is using a 128-bit symmetric key, although the number of bits encrypted output will vary depending on different algorithms, but at the end the length of the packet is a symmetric key, that is 32 hexadecimal digits, For accurate user input it is a challenging and complicated thing. The encryption/decryption mode of authentication is not mainly in the hardware token applications [19]. Parallel computing requires token authentication operation mode, the authenticator and the authenticator use the same factors separately according to a certain algorithm (hash encryption) operation, and then compares each other. Although it is based on parallel computing methodology of hash algorithm for its easy to use system resources and needs to oppose to 1/decryption less computing speed into the mainstream embedded system design approach, but it is not based on the full implementation of the digital signature manner, in law, it does not have auditable significance. The system is based on DSA [20] [21] (Digital Signature Algorithm) as authentication, is a total non-factor-based authentication method are inherently non-repudiation, and the system has been incorporated undeniable factor time-stamp, which implement a strong auditable login authentication system. Meanwhile, the implementation of the system to take half the software effectively solves the speed problem that DSA brought [22].

3.3. Experimental Results

Input information: "AA", it's ASCII code is "616263", after filling the message shows in Table 1.

As show in the table, arbitrarily length information will be filled into affixed length information.

When after extending, W0, W1 … W67 are as follow Table 2.

The filled message after extending is show in Table 2. The table reflects that the message is messy. Same as above, W0', W1' … W63' are as follow Table 3.

After 64 rounds of iterative form 256 bit hash values are as follows.

Table 1. The message after filling.

61626380	00000000	00000000	00000000
61626380	00000000	00000000	00000000
00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000018

Table 2. After extending: W_0, W_1 … W_{67}.

61626380	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000018	9092e200	00000000
0000c060	719c70ed	00000000	8001801f	939f7da9	00000000
2c6fa1f9	adaaef14	00000000	0001801e	9a965f89	49710048
23ce86a1	b2d12f1b	e1dae338	f8061807	055d68be	86cfd481
1f447d83	d9023dbf	185898e0	e0061807	050df55c	cde0104c
a5b9c955	a7df0184	6e46cd08	e3babdf8	70caa422	0353af50
a92dbca1	5f33cfd2	e16f6e89	f70fe941	ca5462dc	85a90152
76af6296	c922bdb2	68378cf5	97585344	09008723	86faee74
2ab908b0	4a64bc50	864e6e08	f07e6590	325c8f78	accb8011
e11db9dd	b99c0545				

Table 3. After extending: W0', W1' … W63'.

61626380	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000018
9090e200	8001801f	93937baf	719c70ed	2c6fa1f9	2dab6f0b
939f7da9	0001801e	b6f9fe70	e4dbef5c	23ce86a1	b2d0af05
7b4cbcb1	b177184f	2693ee1f	341efb9a	fe9e9ebb	e4dbef5c
23ce86a1	b2d0af05	7b4cbcb1	b177184f	2693ee1f	341efb9a
fe9e9ebb	210425b8	1d05f05e	66c9cc86	1a4988df	14e22df3
a5b9c955	a7df0184	6e46cd08	e3babdf8	70caa422	0353af50
47d91983	93937baf	6b4b3854	2e5aadb4	d5736d77	a48caed4
6379de7d	da9ace80	97c00c1f	3e2d54f3	a263ee29	12f15216
49e260d5	6753d7d5	864e6e08	18e587c8		

66c7f0f4 62eeedd9 d1f2d46b dc10e4e2 4167c487 5cf2f7a2 297da02b 8f4b8e0

According to local time, 2016, 4, 24, 14:54:25, get the initial value of dynamic password OTP = 62e229, convert it into decimal OTP' = 6480937, finally get the truncated dynamic password P = 048093.

4. Conclusion

In network management, security management is a critical task during communication and transmission. To achieve high end security technology, hardware and software devices are developed recently by using firewalls. Still authentication technology is an important aspect of information security that needs to be addressed. Authentication is the first line of defence against possible attacks from hacker's. With the rapid developments in authentication security, it has somehow increased security demands and is one of the hot research areas. Dynamic password relatively has many advantages over static password and provides one more layer of security, and provides more security to

users with incorporation in the software, which results in improved security and reduces the chances of data loss and hacking [23] [24]. This paper basically proposed SH3 Algorithm. The basic functionality of SH3 Algorithm is to generate dynamic password by SM3 Hash Algorithm using current time and the identity ID and it varies with time and changes randomly. Coupled with the SM3 hash algorithm security, dynamic password security properties can be further improved, thus it effectively improves network authentication security. Experimental results show the reliability and improved performance of SH3 Hash Algorithm.

Acknowledgements

The research was partially supported by the National Nature Science Foundation of China (No. 61373084) and the innovation Program of Shanghai Municipal Education Commission (No. 14YZ011).

References

[1] Sandirigama, M., Shimizu, A. and Noda, M.T. (2000) Simple and Secure Password Authentication Protocol (SAS). *IEICE Technical Report Office Information Systems*, **83**, 1363-1365.

[2] Stallings, W. (2006) Cryptography and Network Security: Principles and Practice. *IEEE Transactions on Dielectrics & Electrical Insulation*, **13**, 98-104.

[3] De Canniere, C. and Rechberger, C. (2002) Finding SHA-1 Characteristics: General Results and Application. IACR Cryplogye Print Archive, p. 391.

[4] Wang, X.Y. and Yu, H.B. (2012) How to Break MD5 and Other Hash Function. *Lecture Notes in Computer Science*, **3494**, 19-35.

[5] Abdalla, M. and Reyzin, L. (2007) A New Forward-Secure Digital Signature Scheme. *IEEE International Workshop on Anti-Counterfeiting*, *Security*, *Identification*, Springer Berlin Heidelberg, 116-129.

[6] Zou, J., Wu, W.L., Wu, S., Su, B.Z. and Dong, L. (2011) Preimage Attacks on Step-Reduced SM3 Hash Function. *Lecture Notes in Computer Science*, **7259**, 375-390.

[7] Joan, D. and Vincent, R. (2012) The Design of Rijndael: AES—The Advanced Encryption Standard. Springer Science & Business Media.

[8] Diffie, W. and Hellman, M.E. (1976) New Directions in Cryptography. *IEEE Transactions on Information Theory*, **22**, 644-654. https://doi.org/10.1109/TIT.1976.1055638

[9] Peng, F., Qiu, S.S. and Long, M. (2005) A Secure Digital Signature Algorithm Based on Elliptic Curve and Chaotic Mappings. *Circuits Systems & Signal Processing*, **24**, 585-597. https://doi.org/10.1007/s00034-005-2409-4

[10] Sandirigama, M., Shimizu, A. and Noda, M.T. (2011) Simple and Secure Password Authentication Protocol. *IEICE Transactions on Communications*, **83**, 1363-1365.

[11] Haller, N. (1995) The S/KEY One-Time Password System. *Proceedings of the Internet Society Symposium on Network & Distributed Systems*, San Diego, February 1995, 151-157. https://doi.org/10.17487/rfc1760

[12] Halevi, S., Hall, W.E. and Jutla, C.S. (2008) The Hash Function Fugue. Submission to Nist.

[13] Young-Hwa, A. (2013) Security Improvements of Dynamic ID-based Remote User Authentication Scheme with Session Key Agreement. *IEEE Transactions on Consumer Electronics*, **8**, 1072-1076.

[14] Si, J., Jin, C. and Liu, G. (2013) Research and Improvement on the Remote Dynamics Password Authentication Scheme. *Computer Applications and Software*, **25**, 54-55.

[15] Detchast, P. and Thawatchai, C. (2011) Web Security Improving by Using Dynamic Password Authentication. 2011 *International Conference on NetWork and Electronics Engineering IPCSIT*, **11**, 32-36.

[16] Wang, B. and Liu, G. (2012) Study and Amend Dynamic Password Authentication Scheme. *Computer Engineering and Design*, **28**, 2806-2808.

[17] Guo, L., Wang, L. and Li, Q. (2015) Differential Power Analysis of Dynamic Password Token Based on SM3 Algorithm, and Countermeasures. 11*th International Conference on Computational Intelligence and Security*, Shenzhen, 19-20 December 2015, 354-357.

[18] Pointcheval, D. and Stern, J. (2000) Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*, **13**, 361-396. https://doi.org/10.1007/s001450010003

[19] Biryukov, A., Lamberger, M., Mendel, F. and Nikolić, I. (2011) Second-Order Differential Collisions for Reduced SHA-256. In: Lee, D.H. and Wang, X., Eds., *Advances in Cryptology—ASIACRYPT* 2011, Springer, Berlin, 270-287. https://doi.org/10.1007/978-3-642-25385-0_15

[20] Brosa, A.M. and Figueras, J. (2000) Digital Signature Proposal for Mixed-Signal Circuits. *Journal of Electronic Testing*, **17**, 1041-1050. https://doi.org/10.1109/test.2000.894317

[21] Goldwasser, S. and Waisbard, E. (2004) Transformation of Digital Signature Schemes into Designated Confirmer Signature Schemes. *Theory of Cryptography Conference*, Cambridge, 19-21 February 2004, 77-100. https://doi.org/10.1007/978-3-540-24638-1_5

[22] Johnson, D., Menezes, A. and Vanstone, S. (2010) The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, **1**, 36-63. https://doi.org/10.1007/s102070100002

[23] Song, C., Qu, Z., Blumm, N. and Barabási, A. (2010) Limits of Predictability in Human Mobility. *Science*, **327**, 1018-1021. https://doi.org/10.1126/science.1177170

[24] Haller, N., Metz, C., Nesser, P. and Straw, M. (1998) A One-Time Password System. *Network and Distributed System Security Symposium*, San Diego, 11-13 March 1998, 98-100. https://doi.org/10.17487/rfc2289