iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.48232

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

"Password Authentication Key Exchange Protocol using Fish Tank Image based True Random Number Generator"

Sonam Tamrkar[1], Mr. Rajneesh Pachouri[2], Mr. Anurag Jain[3]
[1, 2, 3]*Department of Computer Science and Engineering, RGPV, Bhopal*

Abstract*: *We employ a straightforward configuration of a fish tank as the changeable environment, recording its photos over time, in order to limit the computational complexity. To create the initial seed, the image data is then submitted to a reduction method and hash function. In order to get true random numbers, we suggest a method for economically removing the true seed from the image data and applying it to a pseudo-random generator, in this case, a Linear Congruential Generator (LCG). The need for information security is increasing across a range of industries, and security concerns are receiving more and more attention as a result of the Internet's explosive growth in recent years. Any future value cannot be accurately anticipated based on the current set of values and random numbers are those that are a part of a sequence in which values are uniformly distributed over a defined set. A safe session key can be provided to a pair of users interacting over an unstable channel using password-based encrypted key exchange protocols, even if the top secret key or password they share is chosen at random from a tiny set of values. We offer two straightforward Bellovin and Merritt-based encrypted key exchange systems..
Index Terms:* *True random number generator, Linear Congruential Generator Image data

I. INTRODUCTION

A. Computer Cryptography

The study of secure information transit is known as cryptography. Information security, information integrity, authentication, and non-repudiation are some of the fundamental aims of cryptography. Alternately, it can be described as the skill of concealing data by converting it to cypher text, an unintelligible format. The communication can only be deciphered (decrypted) into plain text by someone who has the secret key.

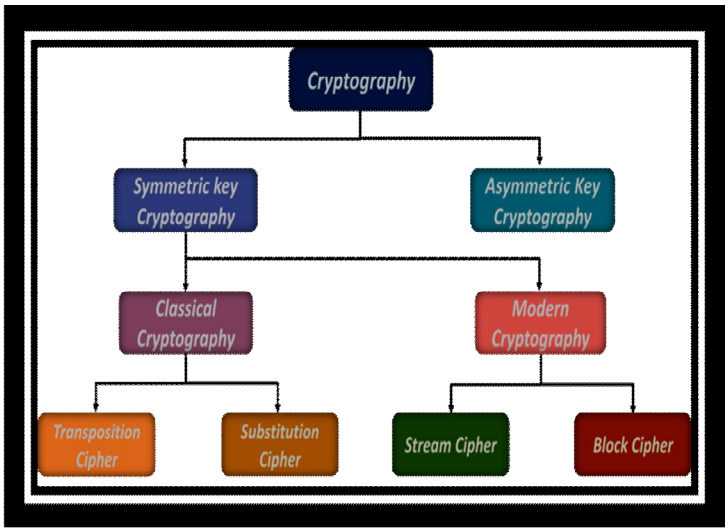


Fig. 1 Classification of Cryptography

©IJRASET: All Rights are Reserved

B. Computer Cryptography's Objectives.

Here are some of the cryptography objectives explained.

1) Confidentiality Information is kept private and confidential so that only those with permission can access it. The terms "secret" and "confidentiality" are interchangeable
2) Data integrity is a service that deals with the unintentional modification of data. One needs to be able to spot data tampering by unauthorised parties in order to ensure data integrity. Data manipulation includes operations such as insertion, deletion, and substitution.
3) Authentication Identification-related services include authentication. Both entities and the information itself fall under this function. Two parties should identify one another before engaging in conversation. Information transmitted over a channel must be verified in terms of its source, date of origin, data content, time of transmission, and so on.
4) Non-repudiation A service called "non-repudiation" forbids an organisation from retracting earlier agreements or actions. A method of resolving the situation is required when conflicts emerge because an entity denies that specific activities were conducted. For instance, one entity might, for instance, give another entity permission to buy property, only to later reject doing so. The disagreement must be settled through a process involving a reliable third party.

II. RELATED WORK

There have been numerous PAKE (password authentication key exchange) protocol proposals in recent years. PAKE protocol has been applied in a variety of applications for resolving security issues in earlier works. Following are some of these:

The optimistic fair exchange protocol makes very little use of a trusted third party; the third party is only required when one player tries to cheat or simply crashes; for the vast majority of transactions, the third party is not required at all. The optimistic method significantly reduces the burden on the third party when compared to a protocol that uses an online third party, which in turn lowers the cost and security associated with replicating the service in order to maintain availability. A fair protocol enables fair digital signature exchange between two parties over the Internet, ensuring that either both parties receive the other's signature or neither party does. Digital signatures like RSA, DSS, Schnorr, Fiat-Shamir, GQ, and Ong-Schnorr are frequently exchanged between two parties. Some too optimistic fair exchange protocols may potentially keep one player hanging for a very long time, unsure of whether the exchange will be successful and powerless to stop it. When it comes to time-sensitive information like stock quotes, this might not only be a major inconvenience but also result in a genuine loss. In actuality, fair exchange encompasses many but connected issues: e-payment methods in electronic commerce, non-repudiation protocols, certified e-mail systems, contract signature protocols, and so on. All of these protocols have their own advantages and disadvantages.

The verified escrows-based protocol enables two parties to exchange digital signatures so that either both players receive the other's signature, or neither player receives it. This protocol [2] guarantees a prompt conclusion to equitable exchange. A reliable third party is required only in situations where one participant crashes or makes an attempt to cheat. In this case, the reliable third party serves as an "escrow service." The fundamental concept is that Alice, the initiator, encrypts her signature using the trusted third party's public key. Bob, the respondent, can then have the trusted third party decrypt it. This escrow mechanism is verified by the use of a conventional "cut-and-choose" interactive proof. In that the player who receives this escrow is able to confirm that it is, in fact, an escrow of a signature on the requested form with the proper condition attached. A resolve protocol for the initiator, a resolve protocol for the receiver, and an abort protocol for the initiator are used in this protocol. The protocol can be used to encrypt data in order to protect its integrity while being transferred over the internet.

Fair trade must be ensured for e-commerce apps. The construction of an effective fair-exchange protocol by sharing the computation of RSA signatures is detailed in this protocol [15]. The computation can be decreased by creating a protocol that does not require zero-knowledge proofs in the exchange protocol by employing the features of the multi-signature model. Use of zero knowledge proofs is only required during protocol setup. In this approach, fairness is ensured by splitting an RSA private key into two parts. The TTP only holds one of the components while the signer holds both.

In a non-repudiation service, computer networks must be used to create, exchange, and validate indisputable evidence. Each participant engaged in the transaction should receive the products they were expecting after it is over. Others may challenge a dishonest party's denial of involvement in a particular transaction by presenting electronic proof to a judge. This non-repudiation protocol [8] has transparent off-line TTP and is a general-fair protocol. This protocol uses the Internet to transmit a digital message and an unrefutable receipt between two untrustworthy parties. This protocol is said to be fair when both parties receive the products they expected at the end of its execution, or when neither party does.

In a protocol for contract signing, two parties who distrust each other fairly exchange commitments to a contract so that either each party can get the other's commitment or neither party can. Using an unnoticed, trustworthy third party during contract signing is a practical and effective strategy. In the sense that the trusted party need not be involved in the protocol unless a conflict arises, this contract signing process [13] upholds fairness while being optimistic. The protocol is a generic one because it may be implemented using most safe encryption techniques and any secure digital signature scheme.

The parties involved in any business transaction do not always trust one another. In such cases, a contract signature is necessary. Two parties can sign a digital contract using this protocol via the Internet in a minute. A fair contract signing protocol enables the exchange of digital signatures on a contract between two untrusted parties. In this case, in order to provide fairness, the initiator's private key is divided into two parts, with one part going to the TTPhold and the remaining secret. The private key's two components are held by the initiator. This digital contract signing procedure is based on the RSA signature and is confident since it only involves the trusted third party when one side is deceiving the other or the communication channel is broken Furthermore, neither of the two parties can demonstrate the reliability of intermediate outcomes to other parties if the protocol is unsuccessfully carried out. The protocol is hence abuse-free. The abuse-freeness is ensured via the trapdoor commitment mechanism, a cryptographic primitive. The absence of abuse is a crucial security criterion for contract-signing methods, particularly in circumstances where making only a portion of a commitment to a contract might be advantageous to a dishonest party or an outsider.

III.PASSWORD AUTHENTICATION KEY EXCHANGE PROTOCOL

Using a two-way handshake, the Password Authentication Protocol (PAP) offers a straightforward means for the peer to establish its identity. An ID and password combination is repeatedly sent from the peer to the authenticator after the link has been created until authentication is acknowledged or the connection is cut off. Only at the time of link formation is this done.

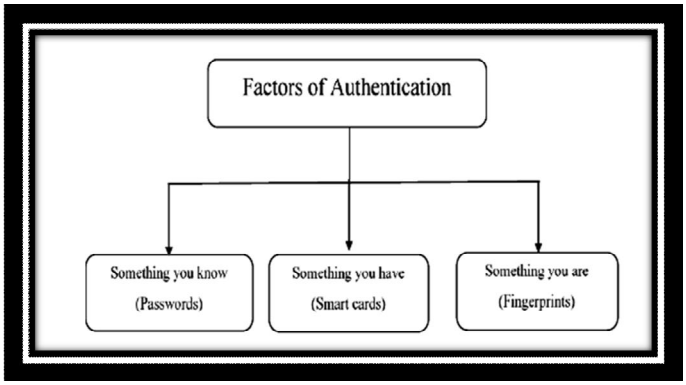


Fig. 2 Factors of Authentication

A. Password Authentication Protocol (PAP)

The Point-to-Point Mechanism (PPP) uses the password-based authentication protocol known as the Password Authentication Protocol to verify users. The RFC 1334 specification for PAP PPP with PAP is supported by the majority of network access servers and almost all network operating systems. PAP is also used by PPPoE to verify the identity of DSL customers.

PAP is exposed to any attacker who can view the PPP session since the Point-to-Point Protocol (PPP) transfers data unencrypted and "in the clear." The user's identity, password, and any other data connected to the PPP session are all visible to an attacker. Using CHAP or EAP will give the PPP link some more security. There are always sacrifices to be made when selecting an authentication mechanism, and there is no clear winner in terms of security.

PPP is regarded as a weak authentication mechanism when PAP is utilised. Weak systems are less computationally intensive and more straightforward than more sophisticated ones like Transport Layer Security (TLS), but they are significantly more open to intrusion. While weak techniques are utilised in situations where it is anticipated that the transport layer will be physically secure, such as a home DSL link. A system like Transport Layer Security (TLS) or Internet Protocol Security (IPsec) is employed in its place when the transport layer is not physically secure.

B. One Time Random Key

The OTRK concept is alarmingly simple to understand. Whenever a digital signature is required, the private key is generated, certified, used to compute the digital signature and immediately deleted. All that remains is the digital signature and the public key certificate from the Certification Authority (CA) that is used to verify the digital signature. There is no possible compromise on the private key, no need for user smart cards/USB tokens, no need for CRLs, no need for LDAP directories, no need for OCSP. It is compliant to international digital signature laws. The OTRK technology should be evaluated as a new and cost effective solution for on-line digital signature providing full mobility for mass usage of the public in different industries. It should be evaluated for this perspective, not from a CA perspective.

C. The concept of OTRK

The main concept behind OTRK is that the private key is a "One-Time Private Key" that works in connection with a short time certificate and is used for digital signature only to secure on-line transactions. As it is, OTRK cannot be used effectively for data encryption and user authentication. There are essentially four steps that are carried out for each OTRK digital signature:

1) Generate the asymmetric key.
2) Send the public key for certification with the CA. At this step, OTRK relies on some form of authentication (strong 2-factor authentication is recommended) with the CA
3) Receive the certificate and sign the transaction
4) Delete the private key.

IV. PROPOSED PROTOCOL

Compared to symmetric key cryptography, the former is more secure, while the latter has the drawback of requiring more time to encrypt or decrypt a message if the packet size is very large. To solve this issue, we sent huge files over unsecure networks using symmetric key cryptography. Symmetric cryptography has difficulty with how to share the shared session key on an unsecured network, so we came up with an effective protocol that uses an image-based key generation process. Below is a discussion of the key generation process. The user must first register on the server, after which the server verifies all the requirements and sends the OTP via various channels, such as email or a cell phone number. The user enters OTP and waits for the session key. The server validates OTP and generates another secret key to further strengthen protocol security. This time, we used a fish tank with about 50 live fish to generate the key. The movement of the fish added uncertainty and made it harder to estimate the key.

A. Proposed Client Server Architecture

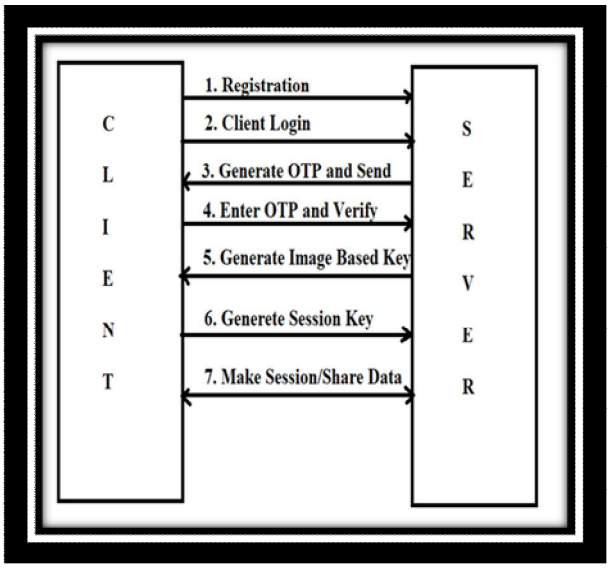


Fig. 3 Proposed Client Server Architecture

B. Key Generation

Known as an entropy source, a TRNG is a function or apparatus that uses randomness to produce non-deterministic data (such as a series of numbers) to seed security algorithms. We generated real random numbers using a fish tank setup with more than 50 live fish as our variable environment source. As we click on the photographs over time, we obtain illogical and erratic image data. After applying a reduction algorithm and hashing to the image data, a true and unpredictable value is produced. To produce truly random numbers, this seed is placed through a pseudo-random method that resembles a linear congruential algorithm. In order to cut down on processing time and complexity, we used the 640x480 GIF image format. The following six image samples are displayed along with their actual seed values.

C. Samples

This is the sample picture that is taken as an input and performs a specific operation on this image.

Here, we generated TRNGs using fish tank capture photos. With the aid of straightforward Java functions, the image's pixel value may be retrieved and transformed to a string value. We examine each and every pixel's RGB value as we convert a picture to binary format. After that, we compare those pixel values. The text file contains the relevant values (0s and 1s), which can be written in any format or from left to right. A slight modification in the image causes a significant variation in the generated random numbers.

Below are the steps for creating a key using an image:

1) Scan pixel values of image from top to bottom and left to right.
2) Concatenating the value to generate random number consisting of 0's & 1's.
3) We can apply any rule for deriving random numbers like XOR, mapping, discarding etc, we have used mapping in this place.
4) Random value can be generated by concatenating columns only or rows only or rows and columns.
5) Similarly unique values can be generated for two parties from the same image for authentication.

We produced the key using the genuine random generation approach via a fish tank-based image, since we knew that a long

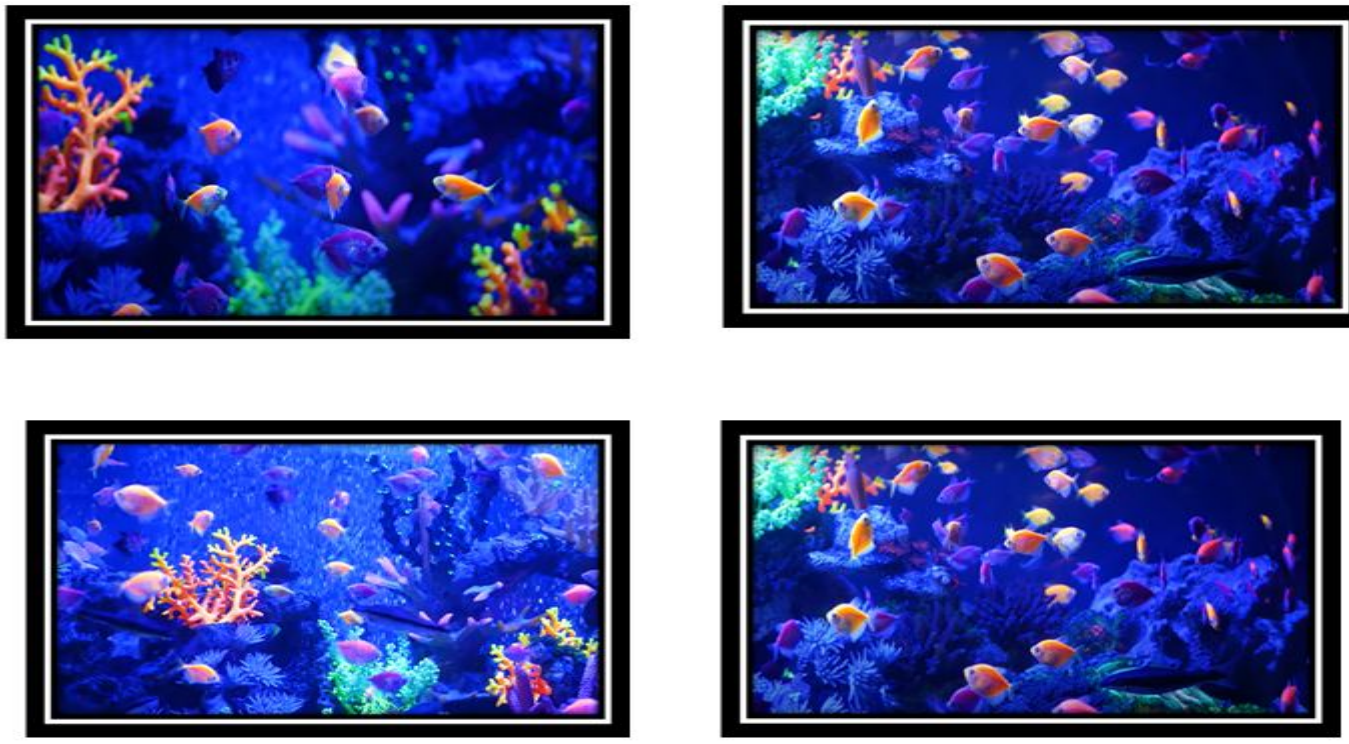


Fig. 4 Sample Picture

Key would be more secure than a short one. We can easily produce bit values of 256, 512, 1024, or higher. We create a real random number key from an image, which is always extremely robust and safe. This method uses a server or trustworthy third party to choose an image and randomly generate a key.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

V. RESULT ANALYSIS

The Graph is shown in the comparison graph of DH-BPAKE Vs Proposed Protocol and this is clearly shown in this graph that our proposed protocol gives better performance as compare to DH-BPAKE.

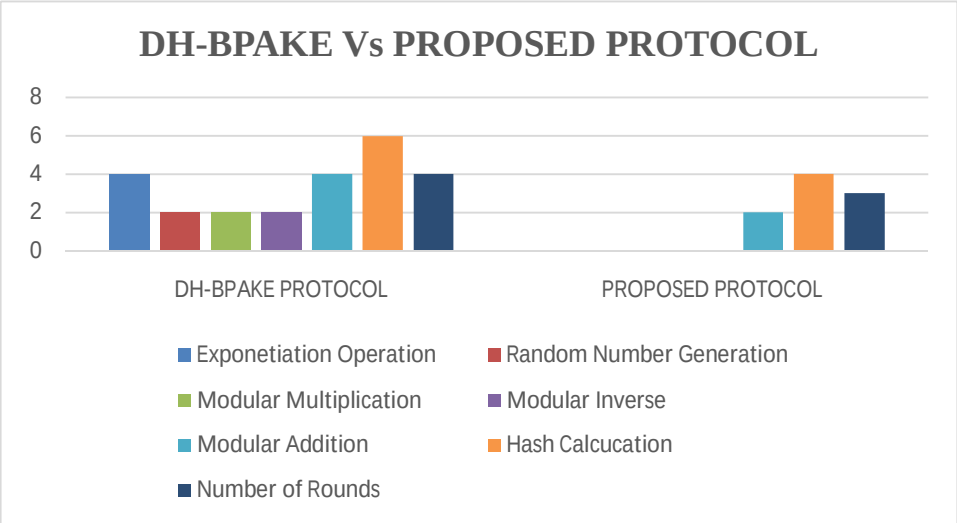


Fig. 5 DH-BPAKE Vs Proposed Protocol

As we know that our proposed protocol is better performance as compare to some pre- exists protocol, we compare our proposed protocol with DH-BPAKE
Protocol with parameter Exponentiation operation, Random Number Generation, Modular multiplication, Modular inverse, Modular addition, Hash Calculation, Number of rounds we shown that our proposed protocol gives better performance as compare to DH-BPAKE. That is shown in the table 1

Protocols	Participants	Exponentiation operation	Random Number Generation	Modular multiplication	Modular inverse	Modular addition	Hash Calculation	Number of rounds
DH-BPAKE Protocol	Client	2	1	1	1	2	3	4
	Server	2	1	1	1	2	3	
Our proposed protocol	Client	0	0	0	0	2	2	3
	Server	0	2	0	0	0	2	

Table 1 Parameter Comparisons

VI. CONCLUSION AND FUTURE WORK

Since the seed value utilised in the random numeral generator comes from an unreliable source, the results are truly random. As a result, it entirely eliminates the risk of determinism, which is present in pseudo-random numeral generators. Up to 16 bits, or 65536, the generator produces really random numbers with a high level of randomness. Image to seed conversion and pseudo random generation are the two primary divisions of the random number generation process.

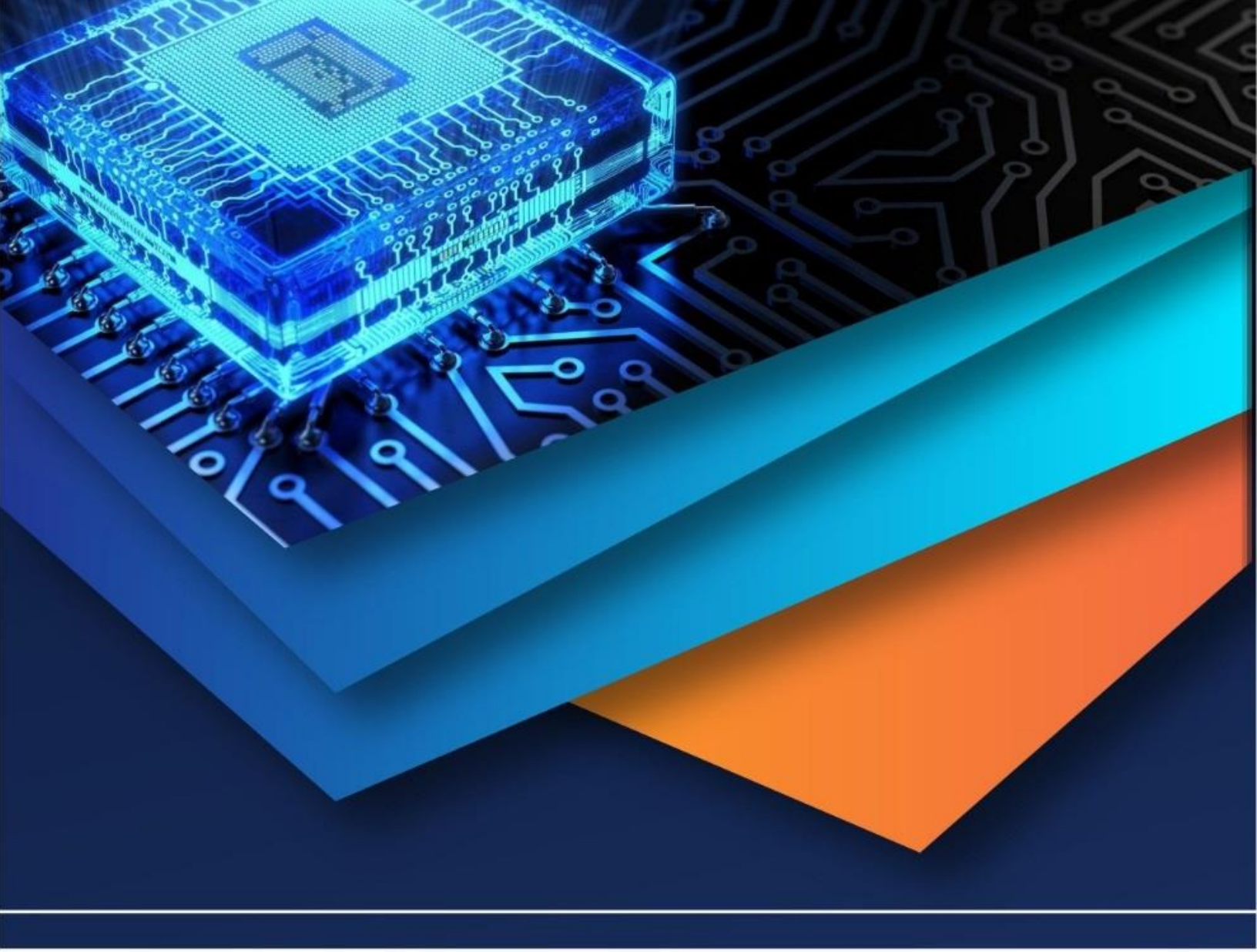
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

In comparison to other hardware random numeral generators that generate randomness using radioactive decay, atmospheric noise, electrical noise, etc., it is also significantly simpler to put into operation. Truly random numbers can be produced at a reasonable cost by employing the TRNG with data from fish tank images.

With the quick development of computer technology, the implication of network security keeps growing, and it is currently the most crucial element in the computing industry. Computer crimes weren't even a concept fifty years ago. As computer technology develops rapidly and the phenomenon of computer crimes threatens computer security, new technologies also present new issues. Computer security is becoming essential due to the rising number of computer crimes that are being done today. Effective computer security is further important than ever, and there is a strong need to raise awareness.

REFERENCES

[1] Pieprzyk, J., Hardjono, T., & Seberry, J. (2003). Fundamentals of computer security. Berlin: Springer
[2] G. Wang, “An abuse-free fair contract signing protocol based on the RSA signature,” IEEE Transactions on Information Forensics andSecurity, vol. 5, no. 1, pp. 158–168, Mar 2010.
[3] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” IEEE J. Sel. Areas Commun., vol. 18, no. 4,pp. 591–606, Apr. 2000.
[4] M. Abadi, N. Glew, B. Horne, and B. Pinkas, “Certified e-mail with a light on-line trusted third party: Design and implementation,” inProc. 2002 Int.World Wide Web Conf. (WWW’02), 2002, pp. 387–395, ACM Press.
[5] Z. Zhao, Z. Dong, and Y. Wang, “Security analysis of a password-based authentication protocol proposed to IEEE 1363,” Theoretical Computer Science, vol. 352, no. 1, pp. 280–287, 2006.
[6] G. Ateniese, “Efficient verifiable encryption (and fair exchange) of digital signature,” in Proc. ACMConf. Computer andCommunications Security (CCS’99), 1999, pp. 138–146, ACM Press.
[7] G. Ateniese and C. Nita-Rotaru, “Stateless-receipient certified e-mail system based on verifiable encryption,” in Proc. CT-RSA’02,2002, vol. 2271, LNCS, pp. 182–199, Springer-Verlag.
[8] F. Bao, R. H. Deng, and W. Mao, “Efficient and practical fair exchange protocols with off-line TTP,” in Proc. IEEE Symp. Securityand Privacy, 1998, pp. 77–85.
[9] S. Gürgens, C. Rudolph, and H. Vogt, “On the security of fair nonrepudiation protocols,” in Proc. ISC’03, 2003, vol. 2851, LNCS, pp.193–207, Springer-Verlag.
[10] G. Wang, “Generic non-repudiation protocols supporting transparent off-line TTP,” J. Comput. Security, vol. 14, no. 5, pp. 441–467,Nov. 2006.
[11] S. Micali, “Simple and fast optimistic protocols for fair electronic exchange,” in Proc. PODC’03, 2003, pp. 12–19, ACM Press.
[12] M. Toorani, “Cryptanalysis of a new protocol of wide use for email with perfect forward secrecy,” Security and Communication Networks, 2014.
[13] J. Yang and T. Cao, “Provably Secure Three-party Password Authenticated Key Exchange Protocol in the Standard Model,” Journal of Systems and Software, vol. 85, no. 2, pp. 340–350, 2012.
[14] C. Boyd and E. Foo, “Off-line fair payment protocols using convertible signatures,” in Proc. ASIACRYPT’98, 1998, vol. 1514, LNCS,pp. 271–285, Springer-Verlag.
[15] S. Kremer, O. Markowitch, and J. Zhou, “An intensive survey of fair non-repudiation protocols,” Comput. Commun., vol. 25, no. 17,pp. 1606–1621, Nov. 2002, Elsevier.
[16] S. Kremer, O. Markowitch, and J. Zhou, “An intensive survey of fair non-repudiation protocols,” Comput. Commun., vol. 25, no. 17,pp. 1606–1621, Nov. 2002, Elsevier.
[17] F. Bao, G. Wang, J. Zhou, and H. Zhu, “Analysis and improvement of Micali’s fair contract signing protocol,” in Proc. ACISP’04,2004, vol. 3108, LNCS, pp. 176–187, Springer-Verlag.
[18] M. Bellare and R. Sandhu, The Security of Practical Two-Party RSA Signature Schemes 2001 [Online]. Available: http://wwwcse.ucsd.edu/users/mihir/papers/
[19] J. M. Park, E. Chong, H. J. Siegel, and I. Ray, “Constructing fair exchange protocols for e-commerce via distributed computation ofRSA signatures,” in Proc. PODC’03, 2003, pp. 172–181, ACM Press.
[20] M. Bellare and P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols,” in Proc. 1st ACM Conf.Computer and Communications Security (CCS’93), 1993, pp. 62–73, ACM press.
[21] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM,vol. 21, no. 2, pp. 120–126, Feb. 1978.
[22] O. Markowitch and S. Kremer. An optimistic non-repudiation protocol with transparent trusted third party. In: Information SecurityConference (ISC’01), LNCS 2200, pp. 363-378. Springer-Verlag, 2001.
[23] Y. Dodis and L. Reyzin, “Breaking and repairing optimistic fair exchange from PODC 2003,” in Proc. ACM Workshop on DigitalRights Management (DRM’03), 2003, pp. 47–54, ACM Press.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)