International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

An Efficient Keyless Signature and Improved Version of Merkle Signature Scheme - CMSS

Remya Chandran, A.Sasi Kumar

Abstract: ***Keyless Signature Infrastructure (KSI) is an adjustment and a globally broadcast arrangement basement for the arising and analysis of KSI signatures. Unlike customary schemes of digital signature, e.g. the method of Public Key Infrastructure (PKI) acquires the concept of cryptographic asymmetric key encryption and KSI employs the hash-alone cryptography, acceptance analysis to wait alone on the hash-function protection and the accessibility of a frequently accessible device is called as a block chain. Google is one of the internet service which is said to be the multi-server atmosphere offered in the current environment, then the subsistence of Single Sign on (SSO) elucidation have proposed many capable technologies. The applications that are similar afford clients with the capability of single sign on by utilizing one username and password system which alleviates the requirement of diverse identities and password methods. Even though the method may be capable, the methods of SSO need to be extra robust and must afford utmost authentication for their clients. The medium of authentication is unidirectional among the client and service provider in SSO and the usage of improper authentication key made the investigators to tell their view about the vulnerabilities in such methods and the attacks may be impersonation attacks. In this work, keyless signature scheme is projected which solves all the above described criteria. An interesting alternative for perfectly installed signature method is the Merkle signature scheme (MSS) which is comprised of RSA, ECDSA and DSA. The security measure of MSS is totally depending on the subsistence of secure hash functions in cryptography. The method of MSS works efficiently to become quantum computer resistant. The work recommends CMSS, a deviation of MSS, with decreased the length of the private key, creation time of signature and the generation time of key pair. It has shown that CMSS is more aggressive for conveying a enormous and effectual implementation.***

Index Terms: Authentication, Keyless signatures, Private Key, Merkle Signature

I. INTRODUCTION

The option provided to standard PKI signatures are keyless signature schemes. The term called as keyless and it does no longer seem that the cryptographic keys are not employed throughout the evolution of signature method. Keys are nevertheless known to be vital for verification; however the signatures can be consistently recognized without considering the endured nature.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
Remya Chandran*, PhD Research Scholar, Department of Information Technology, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, India.
A.Sasi Kumar, Professor, Department of Information Technology, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, India.

Single Sign-On (SSO) protocols acquiesce to authorize an amalgamated environment, where the area users can login once and access the casework offered by altered systems. This access addresses the problem of accepting assorted user-names and passwords. The requirement for an associated ambiance looks stronger due to the circulation of assimilated web services: a website can have accumulated capacity and casework from added sites, which may crave a specific protection or authentication (e.g., a folio embedding a video from YouTube, an agenda from Google and a slideshow from Flickr). The concept of identity providers are required by associated authentication mechanisms, that is, sites affording client identities allotment and user authentication. In recent times, amusing networks are actuality proposed as accessible identity providers. In fact, users are ardent to annals to these sites, and to amend consistently their profile; in this way amusing networks already accumulate lots of claimed advice about users, such as habits, tastes, acquaintance networks, etc.—all abstracts that is priceless for third parties. Moreover, the acquaintance arrangement of a user can be apparent as an absolute “web of trust” for that user’s identity. Security has continued apparently as an accomplishing problem that is particular technology. In any case, in the advanced Internet society, the social change may impacts security pertinent client conduct, it is the obligation of the risk investigator to give guidelines based on the perspectives of the security. Single sign up (SSO) could be a category of rules or methods that facilitate clients to obtain their internet identity to an oversized range of websites that they're performing. For ventures it has been converted into a vital objective to be a piece of a SSO method with different locales so as to fulfill client requests. In this manner, colleges are likewise starting to actualize SSO for the reasons of research assistance and understudy fulfillment. In any case, the security is considered as a mission-basic drawback for associations. Carelessness can prompt genuine ramifications for clients, and expedite legitimate implications that harm an association. Subsequently the endeavors need exact hazard appraisals in the language of the venture. If the venture event needs to satisfy its potential, a structure has to be created that can convey solid explanations on the dimension of the undertaking model while as yet being the foundation of innovation. The last method is modeled but it is based on the lower and also level of platform-dependency.

The methodology that os said to be model-driven is needed and the models based on various dimensions can be adjusted and thought about. With respect to this, there exist the issues for the external service providers. Each client in an association should be set up for the application of service provider and this must have a mimic data set.

The service providers time can be saved if the client information is controlled the association itself. Moreover, one focal source would enable the information to be progressively precise and up to date. It is said that the SAML 2.0 - Security Assertion Markup Language convention do not give confirmation that has to be carried out employing only a single SSL association. Because of challenges relating to the idea of SSL, for example, the trouble to continue an officially settled association after it has been ended, it is normal to accept that SAML 2.0 convention is completed utilizing distinctive SSL associations. Accordingly, the recentness of authentication statement is beyond the realm of imagination to expect to accomplish except if the convention is kept running with SSL association's every run, which is fundamentally adjacent to the entire idea of SSO. The second statement is that, the customer certifications are not offered by the SAML 2.0 about the realness of the SP's. The issues are compared and distinguished in the state of OpenID. In this theory it is necessary to think about how boundless these vulnerabilities are and with the verdict that they are genuinely normal and represent a believable hazard when the framework based on OpenID turn into an important target. The discoveries from these genuinely specialized examinations are fed once again into suggestions for authorities in an association, just as for the network procedure around OpenID. The outcome is a decent counsel, rather than the energy of numerous OpenID defenders or the inside and out dismissal of numerous depreciators. Digital signatures are the methods that have converted into a key innovation for providing secure IT networks. A digital signature affords authenticity, data non repudiation as well as integrity. They are broadly utilized in distinguishing proof and a verification convention, for instance for programming downloads. Subsequently, safe and security oriented digital signatures are vital for security frameworks of IT concern.

The digital signature schemes like RSA, ECDSA and DSA are commonly used. The security assumption of those plans depends on the trouble of figuring vast composite whole numbers and discrete logarithms. Notwithstanding, it is obscure whether the problems of computation stay unmanageable later on. For instance, Peter Shor demonstrated that quantum PCs can factor whole numbers and discrete logarithms can be figured in the pertinent gatherings in the given amount of polynomial time. Before this there has been huge advancement in unraveling the whole number factorization as well as discrete logarithm issue utilizing established PCs. It is in this way important to think of new signature plans which don't depend on the calculation difficulties and processing discrete logarithms that are more secure and adjacent to quantum PC assaults and this scheme is called as post-quantum signature plans. An intriguing signature applicant is the Merkle signature scheme (MSS). The security feature is totally dependent on the presence of cryptographic hash capacities. By utilizing only one public key, MSS can just check a limited number of signatures. Additionally, MSS has proficiency issues (creation of key pair, secret keys and also the signatures). This was not utilized much by and by. In this projected work, CMSS, a variation of MSS is proposed which has the reduced size of the private key, creation of key pair and signature. It is demonstrated that CMSS is aggressive by displaying an exceedingly effective CMSS Java usage. This execution allows simple coordination into functions that utilizes the architecture of Java Cryptography. The analyses that appear: When signing the 2^{40} reports, the creation of key pair time of CMSS is reasonable, and creating the signature and validation method is aggressive or it is more secure and produces good results than Merkle hash tree, Merkle calendar and MSS. The work indicates that the utilization of Abstract Syntax Notation One (ASN.1) by CMSS keys ensures licenses effectual creation of X.509 declarations, interoperability and PKCS individual data trade documents.

II. PROBLEM DEFINITION

The conventions made on the Single sign-on (SSO) enable single user to utilize the equivalent signing eligibility for a few associations. Endeavors face expanding aggressive strain to position themselves as to SSO, but the consequences of shifting to SSO convention are not completely comprehended.

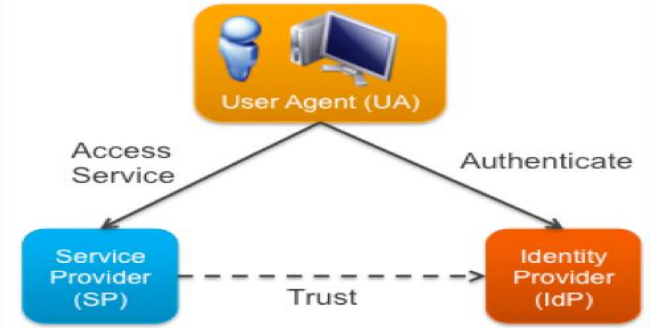

Figure 1. SSO Framework

The OpenID is examined which is moderately a novel SSO convention that is needed utmost on the web. The venture application is applied and demonstrating procedures to OpenID so as to acquire very much established choice guides for undertakings: It is also shown that how distributed displaying methodologies can be utilized to examine the options held in OpenID by exhibiting the features which can determine the security measures correlated with regular OpenID framework. The framework is depicted in figure 1. The convention of SSO is a conceivable answer for secret phrase weariness. The current scenario's cutting edge is Intranet wide SSO and was advanced as an exploration objective in the nineties. The method that propelled this examination was SSO for computerized networks. Distinctive designs have been projected, and for computerized networks intermediary dependent arrangements were made for the most part utilized. These early triumphs have enlivened investigation into comparative SSO arrangements that work for the whole web. It is demonstrated that the fundamental driver of SSO masquerade assaults are identified with the plan of the correspondence medium among the service as well as identity provider which needs two way confirmation. The correspondence amongst the customer is continually shown by the SAML 2.0 who is commonly called as a program offered and assisted by the client, and the SP present in it offers a one-sided SSL association.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Then the correspondence between the IdP and the customer begins as a one-sided association of SSL which ends up two sided once the customer is validated through the trading of legitimate declarations from the IdP and fitting qualifications from the customers. These two presumptions are, dangerous because of two fundamental motives: 1) the need/equivocalness of validation schemes which is a coherent necessity in any plan of confirmation and 2) the one-way scheme of verification amongst the customer and the SP. With respect to the concerned reason, the SAML 2.0 expresses that the customer and SP commonly confirm and concur on the URI estimation, but fails to assure the statement is later or not. The element is especially imperative and paved the way that the validation is not assured by SAML 2.0 convention and this needs to be done utilizing a solitary SSL association. Because of challenges relating to the idea of SSL, for example, the trouble to continue an effectively settled association after it has been ended, it is normal to accept that SAML 2.0 convention is done utilizing distinctive SSL associations. In this way, the recentness of verification affirmation is beyond the realm of imagination to expect to accomplish except if the convention is kept running with all the iterations of the SSL association and fundamentally in opposition to the entire idea of SSO. The second reason is, the genuineness of the SP's is not provided by SAML 2.0 after he/she has been allowed admittance by the IdP. Comparable issues have additionally been recognized in the terms of the OpenID. Clients require their security to be ensured, implying that they should possibly need to uncover data about themselves on the off chance that they wish to do as such. It ought to be simple for clients to perceive whether it is sheltered to enter their certifications. Clients ought not to need to express a similar data over and again; particularly the site endeavoring to correlate with does not require it. Clients likewise necessitate that the manner through which they contract with their digital identity is simple, clear and straightforward. The requirement of Clients approach is to switch their identity from network to network. At long last, clients need their identity to be ensured legitimately with the goal that nobody can mimic them. Ventures need an approach to convey their service to any number of clients. This should be done safely without incidentally imparting classified data to unapproved clients. Furthermore, ventures should most likely get certain client certifications affirmed by a trusted third party. This is termed to be irrefutable and incorporate cases, for instance, having a place with the association they state they do, and being of the age they state they are. These additionally incorporate and ensure that the communication is with a genuine human individual. On the off chance that endeavors enable their representatives to utilize OpenIDs because the OpenID is said to be secure. When any one of the representatives utilizes an innovation, for example, OpenID carelessly, the association itself can be considered capable. The absence of the SSL conventions used in the terms of SSO and the SSO terminology of one way plan for a vindictive SP makes it feasible to mimic a customer and origin it to get to specific assets without its assent. In this manner, it is basic for any verification plan to be appropriate for SSO to fulfill these necessities notwithstanding the basic confirmation prerequisites.

III. EXISTING SYSTEM

The network standard of OpenID is a Web-wide SSO. The method is developed since 2005, and is at present administered by a council which includes the network and industry individuals. OpenID has got help from numerous ventures during that time and various expansive associations, for example, Google, VeriSign, Microsoft, AOL and Yahoo are currently OpenID suppliers. In that capacity it is presently possible for undertakings to depend totally on OpenID to verify clients. The OpenID convention is mind boggling and just indicated literarily in a network standard archive. It became difficult to execute and inclined to uncertainty and the results obtained shows that the prevailing usage are quite resistant and enriched with security blemishes, as the exploration has appeared. During this work, a strategy is portrayed for demonstrating verification conventions by applying strategies, for example, structure graphs and UML arrangement charts. At OpenID, these models are important and exhibited in a few different means: the method helps to distinguish by clearing the dangers and conceivable expansions, and thus helps the enterprise to moderate issues of security. The representation of OpenID is just like a client driven as opposed to a site driven way to deal with identity management. The confirmation is enabled by OpenID and it is to be performed through an identity provider by affording an administration situated interface required for certification or authentication. The exceptional feature about OpenID that is contrasted with other types of SSO conventions is that the earlier interrelation is not required by identity provider with the network or the confirmation provided by the web administration. The identity providers of their own clients can be picked by them (OpenID suppliers for this method) and also provide them with novel URL who communicate with their identity. Here URL is delivered to a network (depending party) who underpins confirmation with the topology of OpenID. The structure represents that the depending parties are those enterprises who use the confirmation system of different associations by decreasing the time needed for clients to get enrolled for their administrations. Hash functions are more secure and the existence of signature methods are combined together and founded on hash functions. Lamport invented this method in 1979. The Lamport signature is wasteful due to signature measure and the public key size. Merkle proposed by utilizing hash trees so as to effectively distribute an expansive public key in 1980. The Lamport signature and its progressively productive adjustment by Merkle are said to be secure adjacent to realized quantum assaults, despite everything they have a crucial shortcoming identified with mystery keys—the mystery of keys is a fundamental supposition for the security of signatures as well as for the security of confirmation. In the event that the key is undermined, all signatures end up questionable. Thus, the denial issue still remains.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

A. Merkle Hash Tree

Data Signature is a component to ensure the trustworthiness of information, for example to forestall unapproved change of information. The purported hashing and distributing component is utilized for that reason. The message can be hashed by utilizing open standard uni directional hash functions of cryptography. The hash is distributed in generally seen ways (in papers and so forth.)

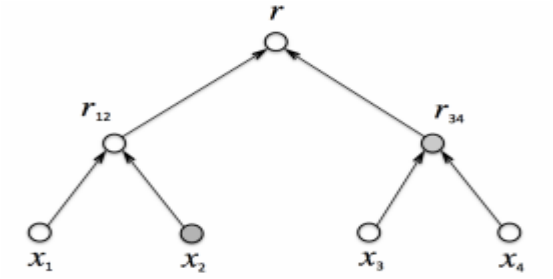

Figure 2. Merkle Hash Tree

In this Merkle Hash Tree the numerous hashes are distributed together (Fig. 2). The tree leaves (x_1, . . . , x_4) are hashed and combined to register the r (root) of the distributed hash oriented tree. An information record's signature is a proof that the information record removes a portion that produces a global hash tree in particular time. The verification is the hash chain of a global tree which needs the important information to restructure the hash tree's foundation. In figure 2, the time stamp afforded for x_1 contains x_2 (for restructuring r_{12}) and r_{34} (for recomputing r from r_{12}). Time stamps are minimized, on the grounds that in the event of N leaves and the size is O(log N).

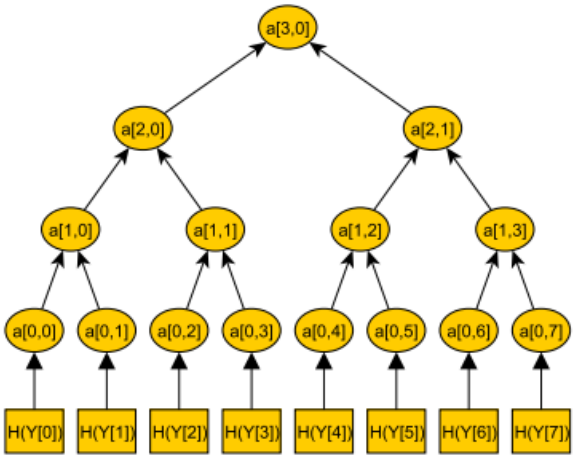

Figure 3. Eight Leafs in Merkle Tree

Thus, couple of open keys ought to be utilized and the open keys ought to be fairly short. However, a public key is employed in One-Time Signature Schemes for each signature whereas the public key is very enormous, contrasted and other types of signature methods. The One-Time Signature Scheme can be made more practical by having a productive key organization that diminishes the size and the measure of public keys. The Merkle Signature Scheme (MSS) was presented by Merkle. To sign the multiple information only one public key is required.

Only one public key is required to sign a diverse amount of messages in Merkle Signature Scheme. The quantity of conceivable information must be an intensity of two, with the goal by indicating that N = 2n which is said to be a conceivable number of messages. The first step is executed to produce the public key which helps in creating X_i → public keys, Y_i → private keys which is called as 2n one-time signatures. A hash esteem = H (Y_i) with $1 \leq i \leq 2n$, is registered for each private key Y_i. Having this hash function, a Merkle Tree i.e. hash tree is fabricated. The node of the tree is $a_{i,j}$, where i signifies the node dimension. The node's dimension is characterized from the node to leaf separation. Consequently, the tree has leaves having the levels i = 0 and i = n that is obtained by the root. All the nodes are numbered which is from left to one side has one dimension and $a_{i,0}$ is the furthest level i's left hub. In the Merkle Tree the hash esteems hello there are the leafs of a binary tree, so $h_i = a_{0,i}$. Each inward hub of the tree is the hash estimation of the connection of its two youngsters. So $a_{1,0} = H(a_{0,0}||a_{0,1})$ and $a_{2,0} = H(a_{1,0}||a_{1,1})$. A case of a Merkle tree is delineated in figure 4. Along these lines, a tree with 2n leafs and 2n+1 − 1 hubs is fabricated. The foundation of the tree $a_{n,0}$ is the public key of the Merkle Signature Scheme.The message M can be signed with the Merkle Signature Scheme and it is marked with a one-time signature method by sig′ signature first. It can be performed by utilizing one of people in public and private key sets (X_i, Y_i,). The leaf node of the hash tree can be compared to a one-time public key Y_i and it is denoted as $a_{0,i} = Hash(Y_i)$. It is said that the way in the hash tree from $a_{0,i}$ to the root A. A root comprises of n + 1 hubs, A_0,...A_n, with $A_0 = a_{0,i}$ being the leaf and $A = a_{n,0}$ = pub being the foundation of the tree. A can be figured and each offspring of the nodes A_1,...,A_n are needed. Then it is realized that A_i is an offspring A_{i+1}. The following hub $A_{i+1}$of the way A can be ascertained by knowing the two offspring of A_{i+1}. A_i → sibling hub is needed. The $auth_i$ is the hub and said to be $A_{i+1} = H(A_i ||auth_i)$. Then there are n hubs called as $auth_0$,..., $auth_{n-1}$ are required for the way A registration. Then currently compute and spare these hubs. These hubs, the one-time signature sig′ of M is the mark sig = (sig′ $||auth_2||auth_3||...||auth_{n-1}$) of the Merkle Signature Scheme and the confirmation way is figured in 4. The public key, mark sig = (sig′ $||auth_0||auth_1||...||auth_{n-1}$) and the message M is known to the beneficiary. The first thing to verify the one-time signature "sig′" of the message M by the receiver. Here, the M's substantial signature is sig′ and the one time signature hashing can be performed for A_0 = Hash(Y_i). For j = 1,..,n − 1, the hubs of A_j of the way A_n are registered with $A_j = H(a_{j-1}||b_{j-1})$ If A_n equivalents the public key of the Merkle signature conspire, the signature is substantial.

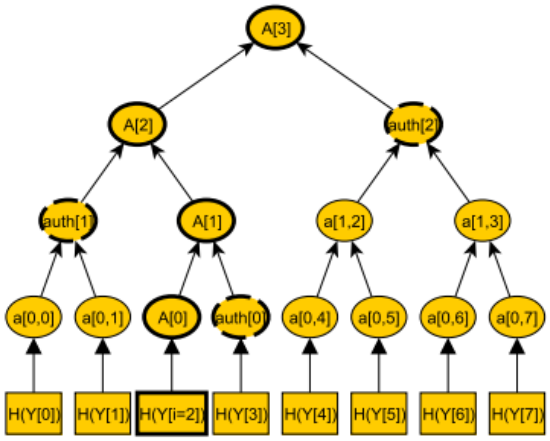

Figure 4. Merkle Tree and authentication path for i=2 with Path A

The extremely post quantum fascinating signature competitor is said to be the Merkle signature scheme (MSS). The security measures depend on the presence of hash oriented functions of cryptography. Since this may be opposed to other categories of signature methods, because the MSS can only check a limited signatures i.e. by utilizing one public key. Likewise, MSS contains productivity issues (creation of the key pair, secret keys with large size and signatures) and hence the method is not practically utilized.

IV. PROPOSED SYSTEM

A. CMSS

In this area, CMSS is portrayed. CMSS is the enhancement of the Merkle signature scheme (MSS). In any h ∈ N, it needs N number of keys for the signing of MSS for N = 2^h of a one-time signature method. Lamentably, for N > 225, the MSS ends up illogical in light of the fact that they have large private keys and creation of key pair takes long time. The signing of CMSS with N = 2^{2h} reports for any number of h ∈ N can be performed. For this reason, two trees for MSS confirmation, a sub tree and a primary tree each containing leaves of 2^h are utilized. The CMSS key is public and the support of the fundamental tree. Information signing is executed by utilizing MSS along with the integration of subtree. However, the public key is not the foot of the subtree. The root validation and the fundamental tree utilization can be done and it is performed by a MSS signature. The creation of 2^h signatures has been made and then another subtree is built and employed to generate the following signatures of 2^h. The private keys can be made smaller by having the OTSS signature keys that is created by utilizing a pseudo random number generator (PRNG). Only the PRNG seed is put away in the private key of CMSS.

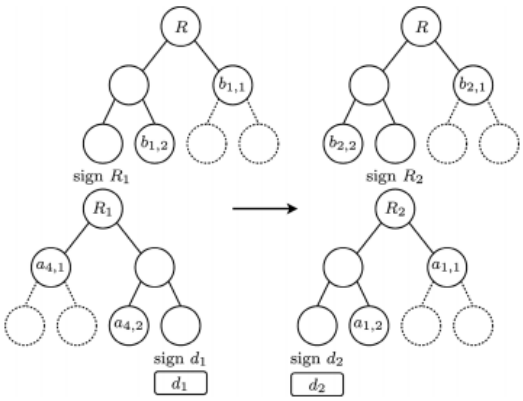

Figure 5. h=2 in CMSS

CMSS key pair creation quicker than MSS, since it has dynamic key generation. At some random time, the two trees with just 2^h leafs, must be initiated. The effectual utilization of CMSS helps to join to provide the records of N = 240. Likewise, generation of private keys in CMSS are smaller than the private key creation of MSS, since it is just a PRNG seed is put away in the private key of CMSS, as opposed to a succession of N amount of signature of OTSS and it enters on account of MSS. Along these lines, CMSS can be employed in any functional area. The Figure 6 shows the scheme of CMSS for the given h = 2.

B. Key Generation Method

The generation of key pair in CMSS is executed in two sections. The first step is done by creating the first authentication and sub tree way. Here the first authentication and sub trees are figured. The foundations of the fundamental tree are the public key of the CMSS. The private key of the CMSS consists of two records i and j and it also contains three seeds for the PRNG, validations are done in three ways (constructed during the creation of signature), three subroutines computation and the base of the current subtree. The routines are depicted in algorithm 1.

C. Generating the Signature

The creation of CMSS signature is completed in four numbers of sections. To start with, the MSS signature of'd' is processed by sub tree utilization. The foundation of the sub tree is processed by the fundamental tree in the MSS signature. Here, the following subtree is constructed. At long last, the CMSS private key is refreshed.

D. Validating the Signature

The validation of CMSS signature takes place in two stages. To begin with, the two verification ways are approved; at that point the one time signature legitimacy of is confirmed. It is shown in algorithm 3. To outline, CMSS offers a decent exchange off concern about the generation of signature and confirmation times contrasted with DSA as well as RSA while safeguarding both the private key size and sensible signature.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Algorithm 1 Generation of Key pair

System Parameters: hash function $H: \{0,1\}^* \rightarrow \{0,1\}^s$, PRNG $f: \{0,1\}^s \rightarrow \{0,1\}^s \times \{0,1\}^s$, Winternitz parameter w

Input: parameter $h \in N$, two seeds $seed_{main}$ and $seed_{sub}$ chosen uniformly at random in $\{0,1\}^s$

Output: a CMSS key pair (priv, R)

1: set $N = 2^h$ and $seed_0 = seed_{sub}$

2: initialize empty stack $stack_{sub}$ and empty sequence of nodes A_1

3: for i = 1,....N do

4: compute $((X_i, Y_i), seed_i) \leftarrow (seed_{i-1})$

5: compute $(stack_{sub}, A_1) \leftarrow (H(Y_i), stack_{sub}, A_1)$

6: let R_1 be the single node in $stack_{sub}$; R_1 is the root of the first subtree

7: set $seed_{next} = seed_N$ and $seed_0 = seed_{main}$

8: initialize empty stack $stack_{main}$ and empty sequence of nodes B_1

9: for j = 1,....N do

10: compute $((X_j, Y_j), seed_j) \leftarrow (seed_{j-1})$

11: compute $(stack_{main}, B_1) \leftarrow (H(Y_j), stack_{main}, B_1)$

12: let R be the single node in stackmain; R is the root of the main tree

13: initialize empty stacks $stack_{main}$, $stack_{sub}$, and $stack_{next}$ and empty sequence of nodes C_1

14: set priv = $(1, 1, seed_{\{main,sub,next\}}, A_1, B_1, C_1, R_1, stack_{(main,sub,next)})$

15: return (priv, R).

Algorithm 2 Signature Generation

System Parameters: hash function $H: \{0,1\}^* \rightarrow \{0,1\}s$

Input: document d, CMSS private key priv = $(i, j, seed_{main}, seed_{sub}, seed_{next}, A_i, B_j, C_1, R_j, stack_{main}, stack_{sub}, stack_{next})$

Output: signature sig of d, updated private key priv, or STOP if no more signatures can be generated

1: if $j = 2h + 1$ then STOP

2: obtain an OTSS key pair: $((X_i, Y_i), seed_{sub}) \leftarrow (seed_{sub})$

3: compute the one-time signature of d: $\sigma_i \leftarrow (d, X_i)$

4: obtain second OTSS key pair: $((X_j, Y_j), seed_{temp}) \leftarrow (seed_{main})$

5: compute the one-time signature of R_j : $\tau_j \leftarrow (R_j, X_j)$

6: set sig = $(i, j, \sigma_i, \tau_j, A_i, B_j)$

7: compute the next authentication path for the subtree: $(A_{i+1}, stack_{sub}) \leftarrow (A_i, seed_{sub}, stack_{sub})$ and replace A_i in priv by A_{i+1}

8: partially construct the next subtree: $((X_i, Y_i), seed_{next}) \leftarrow (seed_{next})$ $(stack_{next}, C_1) \leftarrow (H(Y_i), stack_{next}, C_1)$

9: if $i < 2^h$ then set $i = i + 1$

10: else

11: let R_{j+1} be the single node in $stack_{next}$; R_{j+1} is the root of the (j+1)th subtree.

12: compute the next authentication path for the main tree: $(B_{j+1}, stack_{main}) \leftarrow (B_j, seed_{main}, stack_{main})$ and replace B_j in priv by B_{j+1}

13: replace R_j in priv by R_{j+1}, $seed_{main}$ by $seed_{temp}$, and A_i by C_1

14: set $i = 1$ and $j = j + 1$

15: return the CMSS signature sig of d and the updated private key priv

Algorithm 3 Signature Verification

System Parameters: hash function $H: \{0,1\}^* \rightarrow \{0,1\}^s$

Input: document d, CMSS signature sig = $(i, j, \sigma_i, \tau_j, A_i, B_j)$, CMSS public key R

Output: TRUE if the signature is valid, FALSE otherwise.

1: Take input d and σ_i to obtain an alleged verification key Φ_i

2: using Φ_i and A_i, compute the root R_j of the current subtree as in the case of MSS signature verification.

3: take input R_j and τ_j to obtain an alleged verification key Ψ_j

4: using Ψ_j and B_j, compute the root Q of the main tree as in the case of MSS.

5: if Q is not equal to the CMSS public key R then return FALSE

6: verify the one-time signature σ_i of d and verification key Φ_i

7: verify the one-time signature τ_j of R_j and verification key Ψ_j

8: if both verifications succeed return TRUE else return FALSE

V. RESULTS AND DISCUSSION

The CMSS implementation is compared with Merkle Hash tree, Hash calendar, MSS and CMSS. The execution time required for the creation of key pair, signature and validating the signature is compared. The results of generation of key are summarized in Table 1 and figure 6.

Table 1. Key Pair Generation Time

S.No	Methods	Key Pair Generation Time
1	Merkle Hash tree	18.2 seconds
2	Hash calendar	3.4 seconds
3	MSS	2.3 seconds
4	CMSS	1.2 seconds

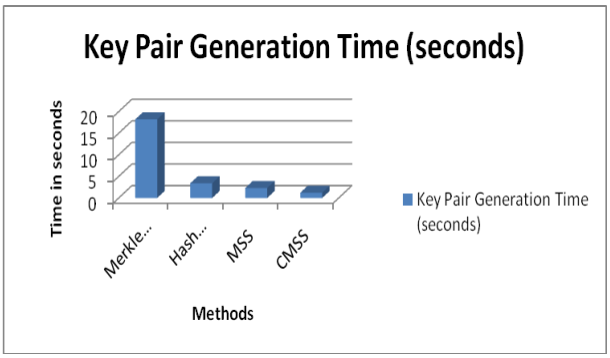

Figure 6. Key Pair Generation Time

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Similarly, the signature generation time is recorded in table 2 and figure 7.

Table No: 2 Signature Generation Time

S.No	Methods	Signature Generation Time
1	Merkle Hash tree	16.3 seconds
2	Hash calendar	2.3 seconds
3	MSS	2.0 seconds
4	CMSS	0.6 seconds

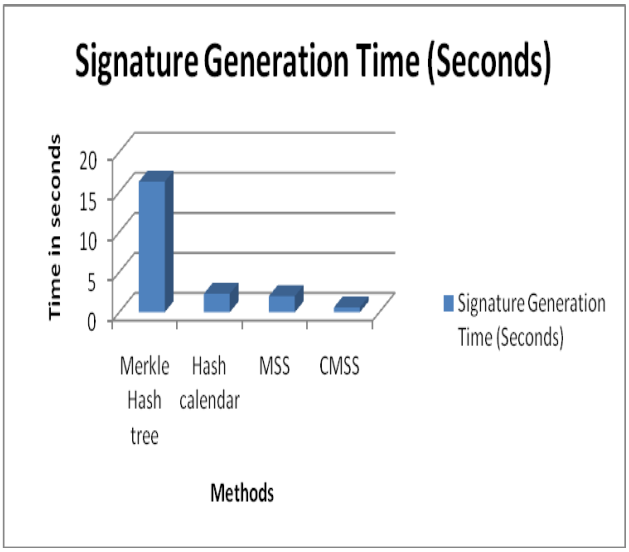

Figure 7. Signature Generation Time

In the same time, the signature verification time is illustrated in table 3 and figure 8.

Table 3. Signature Verification Time

S.No	Methods	Signature Verification Time
1	Merkle Hash tree	14.1 seconds
2	Hash calendar	12.3 seconds
3	MSS	1.0 seconds
4	CMSS	0.4 seconds

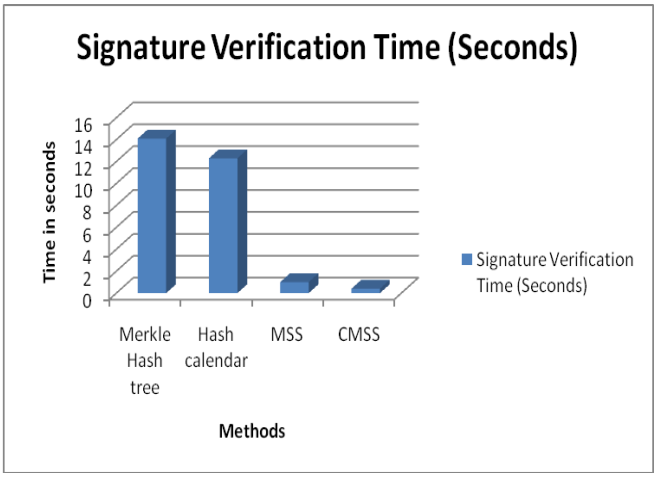

Figure 8. Signature Verification Time

The table affords that the implementation of CMSS offers aggressive signing and verifying times when compared to Merkle Hash Tree, Merkle calendar, MSS and CMSS. Since it is done by generating a pseudo random number the time is feasible and the attacks can be avoided.

VI. CONCLUSION

In this work, CMSS is presented, an enhanced version of Merkle signature method with altogether decreased size of the private key, generation of key pair and generating the signature. A proficient CMSS Flexi Provider usage is depicted. The execution gives focused or even better timings looked at than the usually utilized signature methods like Merkle Hash Tree, Merkle calendar, MSS and CMSS. This is as of now conceivable to utilize quantum PC safe signature methods with no productivity loss that is concerned with signature confirmation and creation times with the length of the key and sensible signature. It is conceivable to join to 2^{40} messages by utilizing CMSS and moderate generation of key pair can be protected.

VII. ACKNOLODGEMENT

This paper is funded by RUSA Phase II, St.Joseph's college Devagiri, Calicut.

REFERENCES

1. Qian et al, "A New Image Encryption Scheme Based on DES Algorithm and Chua's Circuit", In Proc. of IEEE International Workshop on Imaging Systems and Techniques, pp. 168-172, 2009.
2. Ling et al, "Image Encryption Algorithm Based on Chaotic Map and S-DES", Advanced Computer Control (ICACC), IEEE, Vol. 5, pp 41-44, 2010.
3. Kaufman, "Network Security: Private Communication in a Public World", Upper Saddle River, NJ, US, Prentice Hall Press, 2002.
4. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", In Proc. of International Workshop on FSE, Springer, Vol. 809, pp. 191-204, 1994.
5. Riad (2012), "A New Efficient Image Encryption Technique Based on Arnold and IDEA Algorithms", ICIIP, Vol. 46, pp. 140-145, 2012.
6. C.C. Lee, T.-H. Lin and R X. Chang , "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards," Expert Systems with Applications, Vol. 38, pp. 13863-13870, 2011.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)