Light-weight Security Protocol in IoT with Less Computational Cost

Muhammad Imran Khan[1,*], Muhammad Naeem[1], Asim Zeb[1], Adnan Ahmed[2], Aamer Khan[1], Maneeha Rani[1], Muhammad Saeed Shah[3]

[1]Department of Computer Science, Abbottabad University of Science & Technology, Abbottabad, Pakistan.
[2]Department of Telecommunication Engineering, QUEST, Nawabshah, Pakistan.
[3]Department of Electronics, University of Peshawar, Peshawar, Pakistan.
[*]Corresponding author: m.imrankhan@aust.edu.pk

Abstract

Firewalls are the emerging technology to secure the internal network resources from outsider attacks. On the other hand, Authentication, integrity, and confidentiality are the main security challenges for firewalls. To achieve these security challenges, recently, two multicast signcryption schemes have been contributed to the literature. These two Signcryption suffer from two main flaws: computational cost and our head communication. Keeping in view these two flaws, we designed a new multi-receiver signcryption scheme that is lightweight. A lightweight and well-secured protocol is presented for smart-IOT-based homes that are proven to be secured against impersonation, replay, and exposed session key attacks. The Proposed technique is experimented with using the AVISPA tool to ensure that the various attacks do not crack it. The efficiency and security of the proposed scheme are based on a hyperelliptic curve cryptosystem. The hyperelliptic curve cryptography is the subtype of an elliptic curve cryptosystem, and the key size is low from the elliptic curve. Our scheme provides all the security requirements provided by the existing multi-receiver signcryption schemes with low computational and communication costs.

Keywords—Firewalls, Multi-Receiver Signcryption, Computational Cost, Communication Overhead, Hyper Elliptic Curve, IoT, smart-IoT home, Internet of Things

1 Introduction

Nowadays, cyber security is playing a vital role in the cyber age. Round the clock new day comes with a new challenge in cyber security [1]. The biggest challenge is how to perfectly secure the network resources so that availability of the information technology infrastructure should be possible; integrity, information availability, and confidentiality challenges come in different forms: theft, corruption, deletion, malware, malicious attacks, masquerading, eavesdropping, etc. [2]. Round the globe, researchers and developers try to handle these challenges and provide different solutions for better security. In computers, the network security domain firewall considers an essential component [3]. Firewalls reduce the risks and improve security over the networks. Firewalls reduce the risks of unwanted traffic and unauthorized access from the networks that have fatal consequences if succeeded. These firewalls are configured according to network security specialists. So that firewalls keep track of the audit trails of (log files) and insecure protocols also in the other hand, Data transmission over vulnerable networks places data confidentiality at risk, and data communication requires privacy and authentication at all times. Messages used to be encrypted before being sent by creating a digital signature, which was known as the signature-then-encryption mechanism. This method is used in two phases for privacy and verification, requiring more processing power. As a result, Zheng et al. were the first to introduce modern signcryption techniques to reduce computation. This is an encryption method that is incorporated into a single logical step by merging both digital signature and encryption. Afterward, plenty of other new signcryption methods emerged. The biggest downside of all these signature encryption mechanisms is that they do not provide multicast communication. Zheng [13] presented the idea of multi-receiver signcryption in 1998. The multi-receiver signcryption system allows the sender of a message to produce a signcryption code and

ISSN: 2523-0379 (Online), ISSN: 1605-8607 (Print)
DOI: https://doi.org/10.52584/QRJ.2001.04

transmit it to a group of recipients with the same copy of the signcryption. Multicasting means that several recipients will deliver the same message with decreased computation and communication costs. These features make multicasts the best networking technique, where a community of people is coupled with the same mission. Secure and stable multicasting offers applications for protected data sharing from one source to many receiving sites (military monitoring and control, distance education, video conferencing on the Internet in real-time). In the context of the arithmetic operations, multi-receiver signcryption is altogether allocated the bilinear pairing, Revest-Shamir-Adleman (RSA), and elliptic curve cryptography. Method of cryptosystem proposed by the (RSA) Revest-Shamir-Adleman on the basis elliptic curve. The method of RSA deals with the problem of factorization of a big prime number. The scheme of RSA was enduring. The key size for the data encryption used by the technique RSA is 1024 bits for generating the signature. So when we think about recourse hungry devices (IoT) internet of things, the mechanism of encrypting the data and decrypting as well needs energy and resources. The approaches of RSA and bilinear paring are going to be replaced by the strategy of the Elliptic curve because the method of an elliptic curve is 14 times better than the bilinear pairing method. The smart size of the key size used by the elliptic curve strategy is 160 bits used for encryption of data and decryption with a digital signature. But still, this key size is not suited for encryption and decryption of data for small devices like body sensors, IOT resource-hungry devices, for example, PDA, PC Tablet and sensors, etc. recently, the hyperelliptic curve attracted research related to the signcryption [15], which suitable for resource-limited IoT environments. By addressing this issue of IoT devices, the method of RSA and Elliptic curve cryptosystem are more costly than the hyperelliptic curve approach; the key size used by the HEC (Hyper Elliptic Curve) is 80 bits. Which makes it a good choice for small devices like IoT sensors. Furthermore, the National Institute of Standard and Technology accepts that the security level of an elliptic curve cryptosystem with160 bits key size is the same as that of an RSA cryptosystem with a key size of 1024 bits, and more interesting is Hyper Elliptic Curve, which uses 80 bits key size with equal security level [16].

2 Related Work

The secure strategy for the multi-receiver encrypted message was proposed first of all by Zheng et al. [17]. Zheng's multi-receiver scheme is based on two major keys, one for encryption of message and another for decryption on the receiver side. Elkamchouchi et al. [18] give an idea of secure transmission of multi-message through a single logical step which was a dynamic scheme for signcryption. The basic logic behind this scheme was the generation of secret keys simultaneously for the algorithms of key hash and block cipher. The functions suggested for generating the multi keys, the necessary exponential function of multiple standards, was implemented in the work of Zheng's technique of signcryption [17] to generate the secure keys for multi-text. Communication time and computational time overhead of the technique were effective as compared to the scheme of Zheng. The current proposed practice shows that the security cost can be reduced by 27.7% and 41.7% for two and four signcryption throughout Zheng's method of signcryption. The scheme of Elkamchouchi et al. [19] for multi-message dynamic signcryption (PK-MM-DS) is based on one logical step for signcryption of multiple messages that can be seen securely. The suggested scheme has a great effect on saving communication and computational cost as it compares with Zheng (1998), which makes it prominent. This strategy represents the important quantifier for lower limit security measures, which shows the practice of lower limit security measures in existential quantifiers as the comparison test shows the great reduction in communicational and computational costs up to 75% and 41%. Analysis of different message signcryption schemes shows that the economic cost increase proportionally to achieve high-level security with minimum cost requirement. The main idea behind the Elkamchouchi et al. [20] strategy is the generate both keys for signcryption of message and hash key algorithms at the same time. The proposed scheme saves more as compared with the Elkamchouchi multi-message scheme. The strategy showed minimum-security measures recommendation, which is used in current practice. The current suggested strategy deals with minimum security quantifiers. The strategy proposed in this paper reduces the great cost of two recipient communication overhead for the single 50%, double 62.75%, and triple 69.12%. And more overhead will be reduced to increase the number of messages and recipients. As the current suggested scheme compared with the Zheng scheme of multi-receiver shows the result in a great saving of computational overhead of 50% for two and 75% for four encrypted messages. So it can save more computational overhead with an increase in the number of messages. Hagras et al. [21] propose a technique of a Threshold multi-message signcryption scheme of shared verification. The comparison of their proposed scheme with the existing techniques shows a good reduction of computational cost for two recipients and two and three receivers. Elkamchouchi [22] gives an idea of provable strategy with its multi-party variations. He suggests that variation in multi receivers is good for firewalls, but his scheme does not certify the ciphertext and is so not implementable on firewalls. Ahmed et al. [23] proposed a scheme of public message verification signcryption and claimed that his scheme is better than existing multi-receiver schemes in terms of reducing the overhead of communication and computation costs. Elkamchouchi et al. [24] also proposed a signcryption strategy for broadcast communication as the Multiple Broadcast Signcryption strategy (MBSS), the variable length of messages can securely send to multi recipients. In this proposed scheme, not all take benefit of it; only some particular users can focus on signed and encrypted messages to the group. This strategy is based on DLP, DHP, and irreversible one-way hash function security requirements. The proposed MBBS strategy uses public ciphertext authenticity and ciphertext source without showing the message content before receiving in the system and not taking any help from the recipient, which allows and confirms its validity. In large networks, the Unsigncryption process is more efficient. With sending of encrypted text, also need require public verifiability, which shows that the message is decrypted and verified by the receiver so that no one can challenge the authenticity of the message, which is ensured through the decrypted signature. Sanjeev et al [25] also suggest a strategy for multicast communication, but in his work, confidentiality is not efficient. Yiliang Han [26] proposed two strategies of multi-recipient: (SM-MR-SCS) Single Message-Multiple receivers Signcrypted Strategy and second (MM-MR-SCS) Multiple Messages- multiple receiver Signcryption Strategy. Both techniques are not efficient in terms of communication cost. A Firewall is a security framework that screens the system traffic dependent on a few principles. A few schemes are reasonable for firewalls, yet each has its disadvantages and constraints. As of late, Iqbal et al. [27] presented another effective signcryption conspire dependent on the elliptic bend for firewalls. They guarantee that their plan is secure and nobody can copy the first message. Malik and Ali [28] demonstrate that the scheme proposed in [27] isn't verified and has numerous security imperfections. They also provided an improved scheme based on the elliptic curve. Nizamuddin et al. [29] designed a Multi Receiver Signcryption Scheme depending on the elliptic curve for firewalls. It gives scrambled traffic verification by Firewalls and guarantees effective and secure multicast correspondence. It empowers the firewall to confirm an encrypted message without acquiring any unidentified parameter from the members. Isakkirajan and Ramakrishnan [30], repeat the same scheme as presented by Nizamuddin et al. [29] for firewalls security.

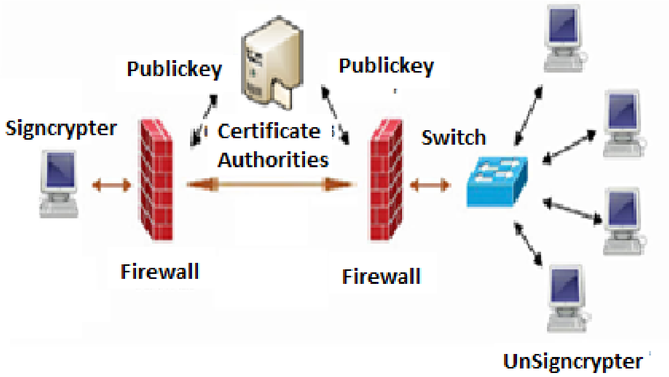

Fig. 1: The flow of the proposed scheme

3 Proposed Scheme

Our work will start by defining the environment of the multicast data exchange mechanism and investigating the model of the multicast technique. Our basic work will go through the same way as in Nizam at el [29] and include lightweight nature. So below in figure 1, we illustrate the model of the multicast mechanism for the firewall. In our multicast mechanism, before the communication, every device over the network has to generate the public key and private key for itself. After that, every device over the network will hand over its public key to the certificate authority. The certificate authority issues the certificate based on a public key. Now before the message sending to the receiver sender first verifies the public key of the receiving group from the certificate authority. Then by using its public key, private key, and secret key, it will generate the multi-signcrypted message for the multi receivers. After that, the signcrypted message sends to the receiving device over the open network. So, the firewall verifies the multi-signcrypted message. After a verification message sends to every receiver, so, each device needs only to decrypt the message.

3.1 Constructions & Key Generation

The above model includes the sub-parts such as key generation, signcryption, and Unsigncryption, respectively. In this stage, the signcrypter arbitrarily chooses a private key $U_s \in \{1, 2, 3, \ldots\ldots, p-1\}$ and produces public key $V_s = U_s.D$ and every participant in the group arbitrarily chooses a private key $U_j \in \{1, 2, 3, \ldots\ldots., p-1\}$ and produces public key

$$V_j = U_j.D \tag{1}$$

3.2 Multi-Receiver Signcryption

This algorithm takes the public key of every participant V_j, the private key of signcrypter U_s and a message M and produces a cipher text

$$\psi = (C, C_j, S, \Omega) \tag{2}$$

1) The signcrypter arbitrarily chooses a number $\delta \in \{1, 2, 3, \ldots\ldots., p-1\}$ Compute $C = E_\delta(M)$
2) Arbitrarily chooses a number $\gamma \in 1, 2, 3, \ldots\ldots., p-1$
3) Encrypt the session key δ for every participant in the group
4) Calculate $K = \gamma.V_j$
5) Compute $C_j = \in_K (\sigma, N_j)$
6) Compute $\Omega = \gamma.D$
7) Calculate $R = H(C, C_j, \Omega)$
8) Compute $S = \gamma/(U_s + R)\ mod\, p$
9) Compute $\psi = (C, C_j, S, R)$

3.3 Firewalls Verification

This algorithm runs by a firewall. It takes the signcrypted text $\psi = (C, C_j, S, R)$ and the public key of sender for verifying the signcrypted text. The verification process is followed:

- The firewall first computes $\Omega = S.(V_s + R.D)$
- Compute $\beta = H(C, C_j, \Omega)$
- Accept the signcryptext if $R = \beta$.

3.4 Decryption

After firewall verification, every participant can decrypt the cipher text, by taking input their own private key U_j and some signcrypted text pairs (C, C_j).

- Compute $K = \Omega.U_j$
- Decrypt the session key $(\delta, N_j) = D_K(C_j)$
- Then decrypt the cipher text $(M, N_j) = D_K(C)$

3.5 Correctness

The firewalls can easily verify the received signcrypted text validity if the following computations satisfy the equalities:

$$\Omega = S.(V_s + R.D) \tag{3}$$

$$\begin{aligned}
&= S.(V_s + R.D) = \gamma/(U_s + R).(V_s + R.D)\\
&whereS = \gamma/(U_s + R)\\
&= \gamma/(U_s + R).(U_s.D + R.D),\ where\ V_s = U_s.D\\
&= (\gamma.D)/(U_s + R).(U_s + R) = \gamma.D = \Omega
\end{aligned}$$

Also the unsigncrypter can easily recover the secret by using the below computations:

$$K = \Omega.U_j \tag{4}$$

$$\begin{aligned}
&= S.(V_s + R.D).U_j,\ where\Omega = S.(V_s + R.D)\\
&= \gamma/(U_s + R).(V_s + R.D).U_j,\ where\ S = \gamma/(U_s + R)\\
&= \gamma/(U_s + R).(U_s.D + R.D).U_j,\ where\ V_s = U_s.D\\
&= (\gamma.D)/(U_s + R).U_j = \gamma.V_j = K
\end{aligned}$$

3.6 Hyper Elliptic Curve

In this section, some of the basics are related to hyper elliptic curves, and notations used in the proposed algorithm are presented.

Suppose there is a prime number σ and the $\sigma \geq 2^{80}$. Let there is a finite field F_σ having order σ and supposes a hyper elliptic $HC(F_\sigma)$ over the finite field F_σ, which is explained In the following equation:

$$HC : \gamma^2 + h(\Omega)\gamma = f(\Omega)\ mod\ \delta \tag{5}$$

Let $h(\Omega) \in F[\Omega]$ is the polynomial having dgree $h(\Omega) \leq g$. Also $f(\Omega) \in F[\Omega]$ is said to be a monic polynomial having degree $f(\Omega) \leq 2g + 1$.

3.7 Divisor

The divisor is the formal sum of finite points on the hyperelliptic curve and the num for D form of the divisor is:

$$D = (a(\Omega), b(\Omega)) = (\sum_{i=0}^{g} a_i \Omega^i, \sum_{i=0}^{g-1} b_i \Omega^i \tag{6}$$

Another group is called Jacobian $J_c(F_\delta)$, which make by utilizing the divisor on hyperelliptic. The Jacobian group $J_c(F_\delta)$ is as followed:

$$|(\sqrt{\delta - 1})^{2g}| <= 0(J_c(F_\delta)) <= |(\sqrt{\delta + 1})^{2g}| \tag{7}$$

3.8 Hyper Elliptic Curve Discrete Logarithm Problem (HECDLP)

Suppose there is divisor D of the hyperelliptic curve having order δ in $J_c(F_\delta)$. Thus, computing a random number $x \in F_\delta$ from $\beta = x.D$.

4 Problem and Contributions

We studied the other existing multi-receiver signcrypted techniques and found the conclusion that these techniques consume more bandwidth because of the heavy key size, which leads to more cast on communication and computation. So, it requires more latency delay. We inspected the latest paper on the multi-receiver signcryption technique based on the

Symbol	Description
D	Divisor
p	Prime number 80 bits
U_s	Private key of signcrypter
$V_s = U_s.D$	Public key of signcrypter
U_j	Private key of each unsigncrypter
$V_j = U_j.D$	Public key of each unsigncrypter
H	Hash function
S	Digital signature
K	Secret key to encrypt receivers' session keys
δ	Session key for each receiver
C_j	Receiver's encrypted session key
C	Encrypted text
M	Plain text
E	Encryption
D	Decryption

TABLE 1: Basic Notations

elliptic curve for firewall applications proposed in [29,30]. However, it's an attractive technique in case of saving communication and computational cost. But still, these techniques have greater communication and computation cost. So we propose a new lightweight multi-receiver signcryption for firewalls based on the hyperelliptic curve. The purpose of our work is to point out and provide appropriate solutions for the security lack of a firewall in a multicast environment for the signcrypted message. To accomplish our goal, we are going to improve the is based on a hyperelliptic curve, a method of signcryption for multi-receiver, which makes it possible for the firewalls to authenticate the data on the network and no need to reveal the content of the encrypted message. Our proposed technique contains the security requirements of "integrity, unforgeability, confidentiality, non-repudiation, and public verifiability, respectively. Firewalls check the authenticity of the message that is in encrypted form through the property of encrypted message authentication. It's a good practice in terms of securing the multicast data and saving bandwidth consumption, and also reducing the communication cost. It could be a better choice for the multicast environment in terms of security reasons.

5 Security Analysis

In This phase, the security requirements which fulfill the proposed scheme are presented. It includes a requirement, for example, confidentiality, integrity, unforgeability, non-repudiation, and public verifiability, respectively.

5.1 Confidentiality

It should be infeasible for an intruder to get any data from the signcrypted text without knowing the secret key. In our case, in case an intruder needs to see the encrypted contents $C =_{\delta} (, N_j)$, the intruder needs to get the session key and a secret key K. To obtain the session key, the intruder can get first the secret key from the equation (8). Hence, by getting the secret key from equation (8), the intruder can compute from equation (9). Thus, it is infeasible for the intruder, because finding from the equation (9) is equal to calculating a hyperelliptic curve discrete logarithm hard problem (HEDHP). Keeping in view the above discussion, we can say that our scheme meets the confidentiality of the signcrypted text.

$$K = \gamma.V_j \tag{8}$$

$$\Omega = \gamma.D \tag{9}$$

5.2 Integrity

The meant or verified user can only change the content of the message. In our scheme, the firewalls can check whether the got signcrypted content is the original, besides being sent by the real sender. In our designed method, the signcrypter computes $R = H(C, C_j, \Omega)$ utilizing a one-way hash function, which is collision-resistant, and then delivers it to each recipient in the group. On the off chance that an intruder changes the original encrypted text C as C' then R is changed to $R' = H(C', C_j, \Omega)$. It is incapable of being done for an attacker to change C such that $R = R'$, due to the irreversibility of a one-way collision-resistant hash function. Hence, we can conclude that our scheme provides the integrity of communicating ciphertext.

5.3 Unforgeability

It ought to be computationally incapable of being done for an attacker to pretend an honest sender in creating a real signcrypted text that can be accepted by the unsigncrypter. In our method, the signcrypter computes the digital signature $S = \gamma/(U_s + R)$ of a plaintext using the random number γ and its own private key U_s. In case, if the intruder wants to make a forged digital signature, then the intruder must be getting the random number γ from equation (8) and the signcrypter private key U_s from equation (10) respectively. According to the definition of hyperelliptic curve discrete logarithm problem, it is computationally infeasible for an attacker to compute U_s. So, from the above discussion, we can conclude that our new system ensures the property of unforgeability.

$$V_s = U_s.D \tag{10}$$

5.4 Non-repudiation

The non-repudiation restricts the signcrypter from denying the delivered signcrypted text. In our designed scheme, the signcrypter cannot deny from their delivered signature $S = \gamma/(U_s + R)$. In this signature, the signcrypter used its private key, which is associated with the public key of the signcrypter. Hence the signcrypter cannot be denied from their communicated signcrypted text.

5.5 Public variability

It means that when the conflict occurs between a signcrypter and an un-signcrypter, the trusted third party can resolve it. In our case, if the sender denies the communicated signcrypted text, then the third party resolves the conflict by using theorem one.

6 Efficiency

For efficiency, we compare our scheme with those of [29,30] in terms of two types of cost called computational and communications cost. The computational cost recommends the extent of computational efforts contributed by the sender and receiver. Everything considered the computational expense is surveyed by checking the measurable of overwhelming errands included. Routinely these activities join secret key encryption and deciphering, hashing, division, addition, multiplication, and exponentiations. Due to less cost, we neglect the secret key encryption and deciphering, hashing, division, and addition. We observe from Our study that the most expensive operations in our designed Scheme and those of [29,30] are EPM and HEM. Further, In table 1, we provide the comparisons between the design scheme and those of [29,30] with the help of EPM and HEM. The schemes [29,30] need 2 EPM on the signcryption side, 2 EPM at the Firewall verification phase, and 3 EPM on the Unsigncryption step; in contrast, our scheme needs 2HEM at the signcryption step, 2HEM at the firewall verification phase, and 1 HEM at Unsigncryption side, respectively. For more clarifications, in table 2, we compare our scheme with those of [29,30]with the help of milliseconds. It is seen that the single elliptic curve point multiplication (EPM) devours 4.24 ms and 2.2 ms for hyperelliptic curve divisors multiplication (HEM) on a PC running JDK 1.6 having two cores of Intel CPU with a preparing velocity of 2.00 GHz and an essential memory limit of 4 GB RAM, working with Microsoft Windows Vista [31]. If we in table 2, our scheme surfing 4.2 milliseconds at signcryption, 4.6 milliseconds at firewall verification, and 2.2 at the Unsigncryption step, respectively. On the other hand, the schemes [29,30] consumes 8.48 milliseconds at signcryption, 8.48 millisecond at firewall verification, and 12.72 at the Unsigncryption step. We also used the reduction formula [32] to show that our scheme reduced how much computational time in milliseconds in table 2. Thus, it is clear from table 2 that our scheme has a low computational cost and is reduced by about 62.93 % from [29,30]. We preferably enhance and generalize the close equation used for the group functions of the genus for HEC designed for the area of properties. Compared to previously published best results, we improved the 62% complexity. Other than this, defined new ECC and HEC metrics for complexity, allowing efficiency comparison functional relevance. Related work shows that ECC performance for the specific perimeters keeps a more fantastic range of complexity values. HECC performs better results with less complexity over the same security perimeters as ECC. HEC cryptosystem is implemented on a processor(ARM7). HEC is quite adorable for the constrained environment, and a case study should be relevant [8].

Schemes	Signcryption	Firewall verification	Unsigncry
schemes [29,30]	2 EPM	2 EPM	3EPM
Proposed	2HEM	2HEM	1 HEM

TABLE 2: Major operations, comparisons

Schemes	Schemes [29, 30]	Proposed
Signcryption	8.44	4.2
Firewall verification	8.48	4.6
Unsigncryption	12.72	2.2
Total	29.68	11
Reduction in %	29.68 -11/29.68*100 = 62.93 %	

TABLE 3: Milliseconds comparisons

Communication cost relies upon the selection of parameters and measurement of data and is determined as the extent of plain text versus signcrypted message in bits of existing schemes and proposed schemes. It is seen from [33] the elliptic curve parameter size of $|n| = |h| = 160$ and the secret key for multi-recipient $|C_i| = 128$ bits. In the case of the hyperelliptic curve, we assume that, $|p| = |h| = 80$ and the secret key for multi-recipient $|C_j| = 64$ bits, as suggested hyperelliptic curve method it shows it will use half computation and communicational cost. Note we assume the cipher text $|C| = 1024$ bits size is the same in both elliptic curve and hyperelliptic curves. The communication cost consumes by schemes [29,30], during communication are $|C| + |C_i| + |n| + |h|$ and our designed scheme is $|C| + |C_j| + |p| + |h|$. According to the above parameter sizes, the schemes [29,30], communication cost is $|1024| + |128| + |160| + |160| = 1472$ and our scheme is $|1024| + |64| + |80| + |80| = 1248$. We use the same reduction formula as we used in the above computational cost, to show the reduction of communication cost of proposed and existing schemes [29,30]. The reduction is 1472-1248/1472*100=15.21%, so it is also clear that our scheme has low communication costs than the existing schemes.

7 Conclusion

A lightweight multi-receiver signcryption scheme for firewalls is introduced in this article. Our scheme's security and efficiency are realized on the bases of the hyperelliptic curve. The article improved the two main issues of current schemes, such as computational cost and communication cost. A few limitations associated with the existing protocol presented such as, lost smart devices, leaked Session keys, replay, and impersonation [4]. It is often cumbersome to deal with these shortcomings and to address those, a lightweight and well-secured protocol is presented for smart-IOT-based homes. It is proven to be secured against impersonation, replay, and exposed session key attacks. Moreover, the proposed method is tested by the use of the AVISPA tool to overcome such attacks. To verify the effectiveness of our system; a comparison report is demonstrated that ensures its competence with existing solutions in terms of security, computational and communication costs. The proposed technique is compared with well-known algorithms like HEM and ECPM. The results show that the elliptic curve method is around 62% more efficient than current HEM, ECP, and M-Exp schemes. Moreover, the computational cost is also reduced in milliseconds in the proposed method by using a security controller [30]. Therefore, the proposed method improves the general equation of HEC by reducing the cost of computation and communication with the same security measures as suggested by the elliptic curve cryptosystem. The technical benefit of this strategy is very beneficial for resource-hungry internet of things (IoT) and microdevices because of the low competition and communication power needed. In the future, it is planned to enhance it further and implement it in the actual environment to report its effectiveness in various applications like smart homes, hospitals, and industries.

References

[1] Deal, Richard. “Cisco router firewall security”y. Cisco Press, 2004.

[2] Peng, Cong, Jianhua Chen, Mohammad S. Obaidat, Pandi Vijayakumar, and Debiao He. ”Efficient and provably secure multireceiver signcryption scheme for multicast communication in edge computing.” IEEE Internet of Things Journal 7, no. 7 (2019): 6056-6068.

[3] Fu, Maomao, Xiaozhuo Gu, Wenhao Dai, Jingqiang Lin, and Han Wang. ”Secure Multi-receiver Communications: Models, Proofs, and Implementation.” In International Conference on Algorithms and Architectures for Parallel Processing, pp. 689-709. Springer, Cham, 2019.

[4] Zheng, Yuliang. ”Digital signcryption or how to achieve cost (signature encryption) cost (signature)+ cost (encryption).” In Annual international cryptology conference, pp. 165-179. Springer, Berlin, Heidelberg, 1997.

[5] Elkamchouchi, Hassan M., Mohamed H. El-Atiky, and Eman Abouelkheir. ”A Public Verifiability Signcryption Scheme without Pairings.” International Journal of Computer Applications 157, no. 9 (2017).

[6] Huang, Yueying, and Junjie Yang. ”A novel identity-based signcryption scheme in the standard model.” Information 8, no. 2 (2017): 58.

[7] Ullah, Subhan, Lucio Marcenaro, and Bernhard Rinner. ”Secure smart cameras by aggregate-signcryption with decryption fairness for multi-receiver IoT applications.” Sensors 19, no. 2 (2019): 327.

[8] Pelzl, Jan, Thomas Wollinger, Jorge Guajardo, and Christof Paar. ”Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves.” In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 351-365. Springer, Berlin, Heidelberg, 2003.

[9] Gao, Ronghai, Jiwen Zeng, and Lunzhi Deng. ”An efficient certificateless multi-receiver threshold decryption scheme.” RAIRO-Theoretical Informatics and Applications 53.1-2 (2019): 67-84.

[10] Wang, Lipeng, Zhi Guan, Zhong Chen, and Mingsheng Hu. ”Multi-receiver signcryption scheme with multiple key generation centers through public channel in edge computing.” China Communications 19, no. 4 (2022): 177-198.

[11] Wang, Lipeng, Zhi Guan, Zhong Chen, and Mingsheng Hu. ”Multi-receiver signcryption scheme with multiple key generation centers through public channel in edge computing.” China Communications 19, no. 4 (2022): 177-198.

[12] Li, Fagen, Yanan Han, and Chunhua Jin. ”Cost-effective and anonymous access control for wireless body area networks.” IEEE Systems Journal 12, no. 1 (2016): 747-758.

[13] Zheng, Yuliang. ”Signcryption and its applications in efficient public key solutions.” In International Workshop on Information Security, pp. 291-312. Springer, Berlin, Heidelberg, 2017.

[14] Zhou, Caixue, Zhiqiang Zhao, Wan Zhou, and Yuan Mei. ”Certificateless key-insulated generalized signcryption scheme without bilinear pairings.” Security and Communication Networks 2017 (2017).

[15] Pang, Liaojun, Mengmeng Wei, and Huixian Li. ”Efficient and anonymous certificateless multi-message and multireceiver signcryption scheme based on ECC.” IEEE Access 7 (2019): 24511-24526.

[16] Ch, Shehzad Ashraf, and Noorul Amin. ”Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem.” In 8th International Conference on High-capacity Optical Networks and Emerging Technologies, pp. 244-247. IEEE, 2011.

[17] Wang, Lipeng, Zhi Guan, Zhong Chen, and Mingsheng Hu. ”Multi-receiver signcryption scheme with multiple key generation centers through public channel in edge computing.” China Communications 19, no. 4 (2022): 177-198.

[18] Elkamchouchi, Hassan M., Abdel-Aty M. Emarah, and Esam AA Hagras. ”A new efficient public key multi-message multi-recipient signcryption (PK-MM-MRS) scheme for provable secure communications.” In 2007 International Conference on Computer Engineering Systems, pp. 89-94. IEEE, 2007.

[19] Elkamchouchi, Hassan M., Abdel-Aty M. Emarah, and Esam AA Hagras. ”A new public key multi-message dynamic signcryption (PK-MM-DS) scheme for cryptographic transmission.” In 2007 National Radio Science Conference, pp. 1-10. IEEE, 2007.

[20] Porambage, Pawani, An Braeken, and Corinna Schmitt. ”Public Key Based Protocols–EC Crypto.” IoT Security: Advances in Authentication (2020): 85-99.

[21] Elkamchouchi, Hassan M., Abdel-Aty M. Emarah, and Esam AA Hagras. ”A new efficient public key multi-message multi-recipient signcryption (PK-MM-MRS) scheme for provable secure communications.” In 2007 International Conference on Computer Engineering Systems, pp. 89-94. IEEE, 2007.

[22] Pang, Liaojun, Man Kou, Mengmeng Wei, and Huixian Li. ”Efficient anonymous certificateless multi-receiver signcryption scheme without bilinear pairings.” IEEE Access 6 (2018): 78123-78135.

[23] Vanathy, B., and M. Ramakrishnan. ”Signcryption based hyper elliptical curve cryptography framework for key escrow in manet.” International Journal of Advanced Research in Engineering and Technology (IJARET) 11, no. 3 (2020): 91-107.

[24] Elkamchouchi, H., Mohammed Nasr, and Roayat Ismail. ”A New Efficient Multiple Broadcasters Signcryption Scheme (MBSS) for Secure Distributed Networks.” In 2009 Fifth International Conference on Networking and Services, pp. 204-209. IEEE, 2009.

[25] Deng, Lunzhi. ”Anonymous certificateless multi-receiver encryption scheme for smart community management systems.” Soft Computing 24, no. 1 (2020): 281-292.

[26] Han, Yiliang, and Xiaolin Gui. ”Multi-recipient signcryption for secure group communication.” In 2009 4th IEEE Conference on Industrial Electronics and Applications, pp. 161-165. IEEE, 2009.

[27] Iqbal, Waseem, Mehreen Afzal, and Farhan Ahmad. ”An efficient elliptic curve based signcryption scheme for firewalls.” In 2013 2nd National Conference on Information Assurance (NCIA), pp. 67-72. IEEE, 2013.

[28] Karthik, L., Gaurav Kumar, Tarun Keswani, Arindam Bhattacharyya, S. Sarath Chandar, and K. V. Bhaskara Rao. ”Protease inhibitors from marine actinobacteria as a potential source for antimalarial compound.” PloS one 9, no. 3 (2014): e90972.

[29] Nizamuddin, Arif Iqbal Umar, Noor Ul Amin, and Abdul Waheed. ”A novel multi receiver signcryption scheme based on elliptic curves for firewalls.” J. Appl. Environ. Biol. Sci 6, no. 2S (2016): 144-150.

[30] Porambage, Pawani, An Braeken, and Corinna Schmitt. ”Public Key Based Protocols–EC Crypto.” IoT Security: Advances in Authentication (2020): 85-99.

[31] Pagar, Yogita S., and G. V. Chowdhary. ”Strengthening elliptic curve cryptography—key generation via biometric fusion approach.” In Computing in Engineering and Technology, pp. 87-101. Springer, Singapore, 2020.

[32] Kumar, Adarsh, Alok Aggarwal, Neelu Jyoti Ahuja, and Ravi Singhal. ”Design and analysis of elliptic curve cryptography-based multi-round authentication protocols for resource-constrained devices.” In Intelligent Communication, Control and Devices, pp. 707-717. Springer, Singapore, 2020.

[33] Sadat, Anwar, Rashid Ahmad, Insaf Ullah, Hizbullah Khattak, and Sultan Ullah. ”Multi receiver signcryption based on hyperelliptic curve cryptosystem.” J Appl Environ Biol Sci 7, no. 12 (2017): 194-200.

[34] Rahman, Abid, Insaf Ullah, Muhammad Naeem, Rehan Anwar, Hizbullah Khattak, and Sultan Ullah. ”A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyperelliptic curve.” International Journal of Advanced Computer Science and Applications 9, no. 5 (2018).