The effectiveness of a hybrid Diffie-Hellman-RSA-AES model

Abdellahi Ahmed
Department of Mathematics and Computer Science
FST / Cheikh Anta Diop University (UCAD)
Dakar, Senegal
abdellahiahmedcheikh@gmail.com

Mohamedade Farouk Nanne
Department of Mathematics and Computer Science
FST / University of Nouakchott Al Aasriya (UNA)
Nouakchott, Mauritanie
Mohamedade@gmail.com

Bamba Gueye
Department of Mathematics and Computer Science
FST / Cheikh Anta Diop University(UCAD)
Dakar, Senegal
bamba.gueye@ucad.edu.sn

Abstract— **With the emerging of quantum PCs that have incredibly strong attributes, the Diffie-Hellman (DH) is an encryption algorithm set of rules used to guarantee communication between two users through a communication channel that isn't always secure, although this algorithm has sometimes been effective at some point, but it is more vulnerable, at the DH level there is no mechanism to guarantee key exchange security, that is why they can be intercepted by a man in the middle. Several studies have been conducted in this context in which our Diffie-Hellman_RSA_AES (DRA) model is a mixture model that joins DH, RSA, and AES encryption algorithm. This model means to further develop security whileexchanging DH keys. The outcomes acquired show the viability of the techniques executed by the proposed model. In this article, we perform a comparative study between DH and DRA to analyze the reliability stage of every version a stimulation that shows the advantage of our DRA model compared to DH in this case we have proposed DRA as an alternative model to replace DH.**

Keywords- **Security and Privacy, Cryptography, Public KeyTechniques**

I. INTRODUCTION

Security remains a major problem, especially with the evolution of technology and the rapid development of computer characteristics nowadays. The Diffie-Hellman DH algorithm is used to ensure the security of key exchange between two interlocutors [1] and it is used in many areas, such as HMQV [2], IPV6 [3], DNS [4], SSH [5], SSL [6]. But, the security issues connected with this exchange require a resolution.

The utilization of the DH algorithm as a method of communication between two users over an insecure channel poses a significant security risk because there is no instrument at the DH level to control user authentication. Several studies have been conducted in this direction to ensure the exchange of secrecy between the interlocutors. The results procured in our research, we proposed a model called DRA. This model was defined to replace the DH algorithm and to reduce the risk that data sent by both users could be intercepted by a man in the middle. Our objective for this research topic is to show the effectiveness of our DRA [7] model as an elective model of DH by contrasting it and DH.

Our article is divided into eight parts. The DH Key Exchange is presented in the section 2. Section 3 is presented in the Proposition for Resolutions of Diffie Hellman Flaws. Afterwards, section 4 depicts our DRA model. Section 5 is presented in the comparative Study between DRA and Existing Solutions. DRA Evaluation is presented in section 6. Section 7 is presented in conclusion. Finally, section eight is presented inreference.

II. The DH Key Exchange

The DH algorithm is an encryption algorithm created by Ronald Rivest, Adi Shamir and Leonard Adelman in 1976 [8] [9]. It establishes a shared secret key that can be used for secret communication between two users by exchanging data over a public network. This method does use Public Key to secretly exchange Private Key. Secret keys are created only if required, it is not necessary to keep the keys secret for a long time [10].

Table 1 depicts the key exchange steps of this algorithm are displayed as follows:

TABLE 1 The Steps of the DH algorithm [11]

1	The two numbers X and Y "p a prime number" and "g a integer «with g< p;
2	a is the secret number of X.
3	b is the secret number of Y
4	The public number of X is $X_a = g^a \bmod p$.
5	The public number of Y is $Y_b = g^b \bmod p$.
6	X and Y exchange their public numbers
7	$k_a = (X_b)^a$
8	$k_b=(X_a)^b$

Through the key exchange processes, both interlocutors X andY know the secret Ks.

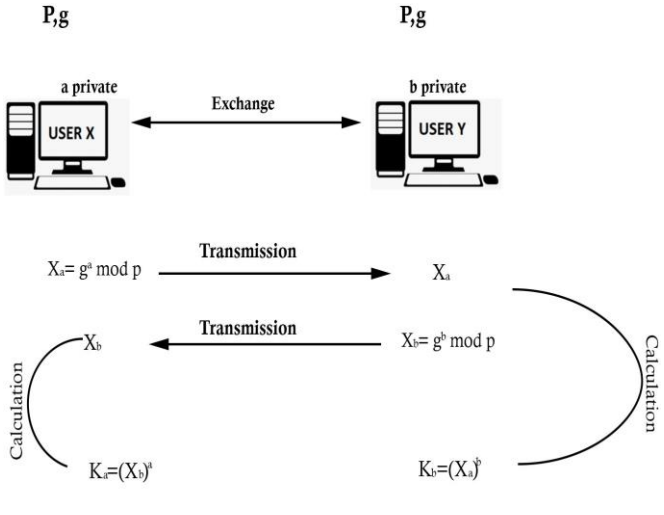

Fig. 1. Diffie-Hellman

Figure 1 depicts the key exchange processes and the manner inwhich both X and Y recognize the secret Ks.

The DH vulnerability is illustrated in the following figure:

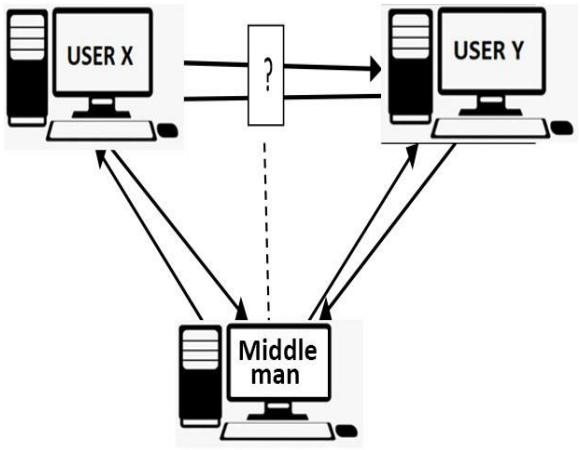

Fig. 2. Vulnerability of DH

Figure 2 shows that there is a third party communicating between the sender and the receiver. It illustrates the level of risk of an attack by a man in the middle and the interpretation of the information exchanged by users [12].

III. Proposition for Resolutions of DH Flaws

Studies have been achieved to be able to solve the problems identified at the DH level. These have led to protocols being put in place. It is in this sense that we have the STS [13] , A New- Two-Pass Key Agreement Protocol [14], HMQV [15], the SWANE model [14], and the S-SEJAD model [11].

The STS Protocol is a protocol that combines the DH algorithm with a digital signature [13] and is considered to be an alternative solution to the DH algorithm. Because of the mutual authentication performed for both users, this combination exposes both users to certain risks. These dangers include the interception of confidential data, identity theft, and delivery due to integrity.

This protocol consists of defining a session key, which is a combination of two interlocutors X and Y's private keys [16]. Each of the two interlocutors generates secret information, and a key agreement is produced. a test is performed on the key and the result is null, there is a problem. If necessary, the product secret will constitute the session key.

The HMQV (Hashed MVQ) protocol is a hashed variant of MQV. MQV is defined as an alternative to DH [17]. Thus, MQV enables dealing with problems encountered at the DH level, more precisely in relation to the "Man in the Middle" attack. Therefore,it is an alternative to DH.

The SWANE model is a hybrid model that combines the two RSA and DH encryption algorithms. Through the use of these two Mechanisms [18] [19], this model will inherit strengths and weaknesses.

The vulnerability of shared secrecy and RSA's strength lies in the difficulty of decrypting protected information. Key decryption with RSA is, indeed, difficult.

The S-SEJAD model is a hybrid model that combines the AES128 (Advanced Encryption Standard) and the DH algorithms to secure key exchange [11]. The S-SEJAD model can be used as a protection measure against middle-man attacks by encrypting the information exchanged between the two users.

IV. Presentation of DRA Model

Before the data exchange, the STS Protocol requires mutual authentication. This makes it possible to identify communicating third parties before the data transfer. Therefore, this protocol does not encrypt the data exchanged between two interlocutors.

After presenting DH's difficulty at the security level and most of its vulnerability caused by key exchange, it is important to find an effective solution to secure this exchange. The DRA model is a hybrid model that combines the three RSA, AES and DH algorithms to secure the exchange of the latter's keys [20], the DRA model uses the two RSA and AES algorithms as a measure of protection against the attacks expected by a man in the middle.

These operating steps are displayed as follows:

TABLE 2 The Steps of the DRA model

1	P, g are two numbers of User X and User Y, p is a prime number and g is strictly negative of p.
2	The secret number of X. is a and the secret number of Y is b.
3	The public number of User X is $X_a = g^a \bmod p$ and the public number of User Y is $Y_b = g^b \bmod p$.
4	The two users send their public key to each other, share the numbers p and g and everyone keeps the RSApri.
5	Each user encrypt its public key using the other's Public key.
6	The two users exchange the "CleAES" key.
7	The two users exchange the values encrypted by the pulic key of Y (RSApub(Y)) and the public key of X (RSApub(X)) before encryption with the unique key CleAES.
8	Both users decrypt the value sent using the CleAES key.
9	Each user decrypts again the values this received with RSApri key.
10	X calculates $k_a = (Y_b)^a$, Y calculates $k_b = (X_a)^b$
11	According to the algebra laws, $k_a = k_b = k_s$. X andY both know the secret value "k_s".

The DRA exchange allows protecting the values (Xa and Yb) by encrypting them with AES and RSA before sendingthem.

The DRA model is represented in the following figure:

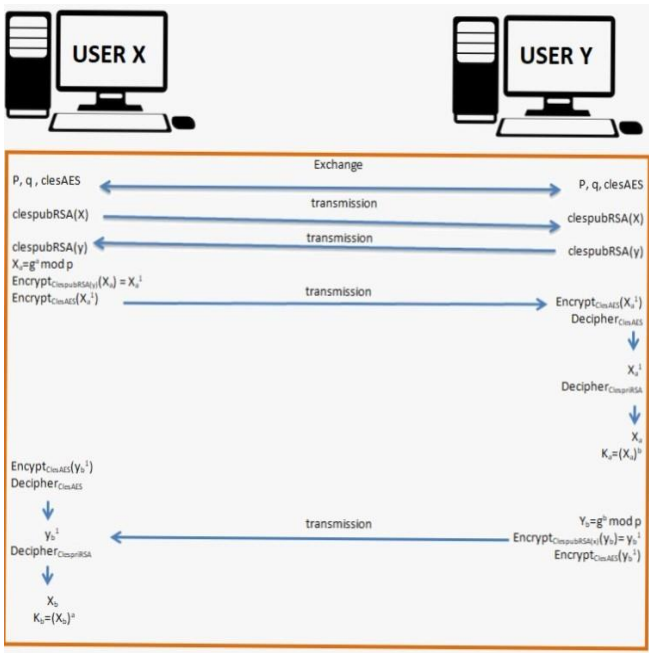

Fig3. Model DRA [20].

This figure represents the DRA model, which provides a very powerful reduction in security vulnerability by utilizing both the RSA and AES algorithms. X_a and Y_b are transmitted confidentially in this model.

The New-two Pass Agreement's protocol provides an agreement and secret information allowing the identification of communicating third parties and does not encrypt the informationbefore it is sent.

V. Comparative Study Between DRA and Existing Solutions

The comparison of our DRA model and the five existing solutions is based on several criteria, the attacks of middle men, the encryption of the secret exchanged and the robustness that ensures very effective reliability.

- The HMVQ protocol uses certificates for a fairly strong identification of communicating third parties before the exchange of data and also does not encrypt the data exchanged between two interlocutors.
- The SWANE model encrypts the data exchanged by the RSA algorithm, so even if it is intercepted, it will not be well interpreted, so in this case, the SWANE model exceeds the previous three protocols in terms of security.
- Because the S-SEJAD model encrypts data exchanged using the AES algorithm, it exceeds all three protocols in terms of security while also outperforming the SWANE model in terms of speed.
- With the appearance of quantum computers which carry extremely powerful capabilities, it has become necessary to find solutions that improve the security of data exchanged. The DRA model encrypts the exchanged information using both the RSA and AES algorithms, and because it uses these algorithms, we can say that our solution is more secure than all previous solutions.

VI. DRA Evaluation

The comparison between the DH algorithm and the DRA model shows the latter's superiority in terms of security, the DRA model can be used as a measure of protection against attacks, and shows the impossibility of the interpretation of the information shared between users.

-

TABLE 3 DRA VS DH

Model / Criteria	DH	DRA
Encryption of Exchanged data	The data are not Encrypted.	The data are Encrypted.
Man-in-the-middle attacks	Possible because the Shared data are Unencrypted.	Impossible because the data are encrypted with the two algorithms RSA And AES.
The interpretation of exchanged data	Possible because the Data are Unencrypted.	Impossible because the data are encrypted with RSA after encrypting them Again, with AES.
Time of execution	Lower	Higher

The advantage of our DRA model over DH is that the encryption is done before sending the data into the transmission channel, the data is encrypted by the RSA algorithm before encrypting it with the AES algorithm, which confirms the impossibility of interpreting the data exchanged even if it is intercepted by a man-in-the-middle and promotes security against man-in-the- middle attacks.

A. Experimental Setup

The evaluation of the execution time of our DRA model compared to DH is done via a simulation program written in MATLAB.

The execution of the simulation was done on a computer with the characteristics shown in the following table:

- CPU: Intel(R) Core (TM) i3-2350M CPU @ 2.30GHz (4 CPUs), ~2.3GHZ.
- RAM: 4GB.
- OS: Windows 8.1 Professional.

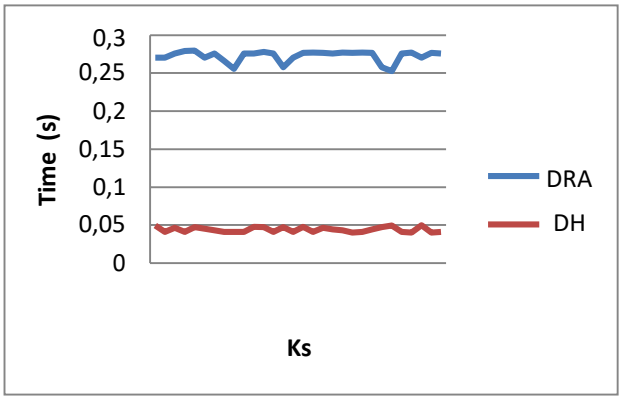

Fig. 4. Average Time between DRA and DH

The shared secret is represented by the X axis, and the execution time per second is represented by the Y axis Time(s).

B. Results

Figure 4 illustrates the average time of DRA and Diffie-Hellman (average of 32 experiments for each Ks value) (DH). We observe that the difference between the average DRA time and the average DH time remains very large for all Ks values, due mainly to the encryption performed by two algorithms, which increases the time required to ensure better security.

We note that the DRA model has a longer average time than DH. This is quite normal due to the additional time required by the use of RSA and AES at the level of our DRA model.

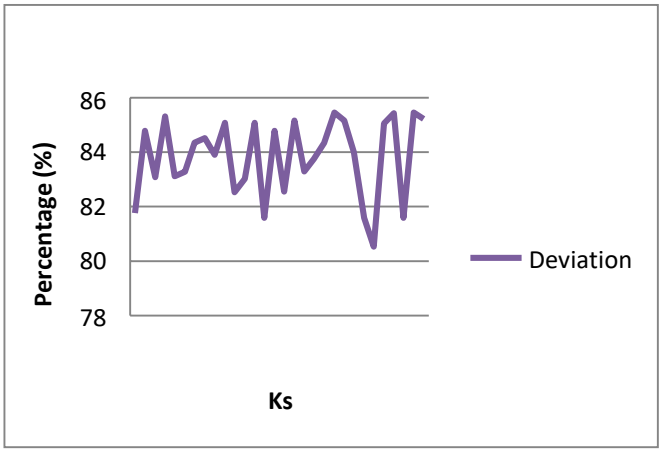

Fig. 5. Deviation between DRA and DH

Based on the results indicated in Figure 5, we observe that the deviation between our DRA model and the DH algorithm as a Percentage does not exceed 93% on average.

VII. Conclusion

The comparison between DRA and DH shows that the gap between the average time of DRA and DH is very large and the deviation does not exceed 93% on average.

Furthermore, this study also shows that the DRA model is more robust than the DH algorithm, because it has completely reduced the risk of a man-in-the-middle attacks and the interpretation of intercepted data, using the two RSA and AES encryption algorithms for encrypted data exchanged by two users.

According to the results achieved from this study, we are tempted to replace DH with the DRA model to obtain better safety. Indeed, with the enhanced safety of our DRA model, we ensure more robustness to these systems.

VIII. REFERENCES

[1] S. Goldwasser, "New directions in cryptography: twenty some years later (or cryptograpy and complexity theory: a match made in heaven)," Proceedings 38th Annual Symposium on Foundations of Computer Science, 1997, pp.

[2] Krawczyk H. (2005) HMQV: A High-Performance Secure Diffie-Hellman Protocol. In: Shoup V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, vol 3621. Springer, Berlin, Heidelberg.

[3] S. Deering, R. Hinden, Rfc 2460 Internet Protocol Version6 (IPv6) Specification, December 1999.

[4] M. A. Hussain, H. Jin, Z. A. Hussien, Z. A. Abduljabbar, S.
H. Abbdal and A. Ibrahim, "DNS Protection against Spoofing and Poisoning Attacks," 2016 3rd International Conference on Information Science and Control Engineering (ICISCE), 2016, pp.

[5] Stephen. C. Williams; Analysis of the SSH Key Exchange Protocol, BAE Systems Detica, Gloucester Business Park, Gloucester, GL3 4AB, United Kingdom.

[6] P. Bhattacharya, M. Debbabi and H. Otrok, "Improving the Diffie-Hellman secure key exchange," 2005 International Conference on Wireless Networks, Communications and Mobile Computing, 2005, pp.

[7] A. Ahmed, M. F. Nanne and B. Gueye, "A hybrid model to secure the exchange of DH keys," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp.

[8] S. Gupta and J. Sharma, "A hybrid encryption algorithm based on RSA and Diffie-Hellman," 2012 IEEE International Conference on Computational Intelligence and Computing Research, 2012, pp.

[9] 6 Maurer, U.M., Wolf, S. The Diffie–Hellman Protocol. Designs, Codes and Cryptography 19, 147–171 (2000).

[10] Nan Li, "Research on Diffie-Hellman key exchange protocol," 2010 2nd International Conference on ComputerEngineering and Technology, 2010,

[11] A. El Emine Sejad, K. W. Keita, K. Tall and I. Diop, " Proposal of a DH optimization model," Systems (CITS), 2020, pp.

[12] A. El Emine Sejad, K. W. Keita, K. Tall and I. Diop, "S- SEJAD versus DH," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021,pp.

[13] Blake-Wilson S., Menezes A. (1999) Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol. In: Public Key Cryptography. PKC 1999. Lecture Notes in Computer Science, vol 1560. Springer, Berlin, Heidelberg.

[14] K. Al Sultan, M. Saeb and U. A. El-Raouf Badawi, "A new two-pass key agreement protocol," 2003 46th Midwest Symposium on Circuits and Systems, 2003, pp.

[15] Krawczyk H. (2005) HMQV: A High-Performance Secure Diffie-Hellman Protocol. In: Shoup V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, vol 3621. Springer, Berlin, Heidelberg.

[16] K. Al Sultan, M. Saeb and U. A. El-Raouf Badawi, "A new two-pass key agreement protocol," 2003 46th Midwest Symposium on Circuits and Systems, 2003, pp.

[17] Krawczyk H. (2005) HMQV: A High-Performance Secure Diffie-Hellman Protocol. In: Shoup V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, vol 3621. Springer, Berlin, Heidelberg.

[18] K. W. Keïta, S. M. Farssi, C. Lishou and A. Corenthin, "The impact of model S-wane on IPv6," 2014 International Conference on Multimedia Computing and Systems (ICMCS), 2014, pp.

[19] K. W. Keita, B. Bodian, I. Diop, C. Lishou and S. M. Farssi, "The S-WANE model, a real alternative of DH system," 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), 2016, pp.