Dicle University Journal of Engineering (DUJE)
web: http://dergipark.gov.tr/dumf

Research Article

Password-Based SIMSec Protocol

Sedat AKLEYLEK[1,*], Engin KARACAN [2]

[1] Ondokuz Mayıs University, Department of Computer Engineering Engineering, Engineering Faculty, Samsun, Turkey

sedat.akleylek@bil.omu.edu.tr https://orcid.org/0000-0002-2306-6008

[2] Ondokuz Mayıs University, Computational Sciences Program, Graduate School of Sciences, Samsun, Turkey enginkaracan@gmail.com

https://orcid.org/0000-0002-2306-6008

ARTICLE INFO

Article history:

Received 17 June 2020
Received in revised form 25 August 2020
Accepted 30 August 2020
Available online 30 September 2020

Keywords:

Authentication, Key, Exchange, SIMSec

Doi: 10.24012/dumf.753942

ABSTRACT

The purpose of the SIMSec protocol is to provide the infrastructure to enable secured access between the SIM (Subscriber Identity Module) card which doesn't have an ephemeral key installed during production and the service provider. This infrastructure has a form based on agreements among the mobile network manufacturer, the user, the service provider and the card manufacturer. In order to secure transactions, authentication methods are used based on the fact that both parties can verify that they are the parties they claim to be. In this study, the key exchange and authentication models in the literature have been surveyed and the password-based authentication model is chosen. For the SIMSec protocol, the password-based authentication algorithm is integrated into the SIMSec protocol. Thanks to the proposed new structure, phase differences in the SIMSec protocol are shown. As a result, a new key exchange protocol is proposed for SIM cards.

* Corresponding author
Sedat, Akleylek
✉ sedat.akleylek@bil.omu.edu.tr

Please cite this article in press as S. Akleylek, E. Karacan, "Password-Based SIMSec Protocol", DUJE, vol. 11, no.3, pp. 1021-1030, September 2020.

Introduction

When the development process of communication technology is examined, it is seen that mobile phones cover a great place. It has been observed that mobile phone usage areas have increased in proportion to time so far. At the beginning mobile phones were served to users for voice calls and short message services. With the advances in communication technology, it has helped secure transactions such as mobile banking, mobile signature and mobile payment through the developing system. Thanks to these developments, cash out transactions, online shopping, credit card usage, online payments, e-commerce and the like can be secured safely via SIM on today's devices [1,2,3]. The secure provision of these services depends on the security of communications between the service providers and the SIM. SIM technology has been developing every year. SIM memory sizes update itself with advancing technology. These SIMs are installed by card manufacturers with ephemeral key protocols to ensure secured access between service providers and the SIM. In this study, transaction and memory costs are taken into consideration with a similar mentality in SIMSec protocol.

Key exchange can be defined as a protocol for two mutual parties to negotiate a secret key. The authentication method can be defined again as a protocol that are established by verifying that the two parties are the parties they are claiming each other to be. Key exchange and authentication methods for the secured access of the parties take an important place in the literature.

Related Works:

Today, SIM Cards (64kb 128kb 356kb 512kb) with different capacities are produced by card manufacturers. Secret keys are loaded on these cards during production in order to provide end-to-end secure communication over the produced cards. With the developing technology, communication security can be attacked. The attacker can cause problems by attacking this communication channel, such as changing data, listening and breaking data [1,2]. End-to-end communication has been made safer with the suggestion presented in this paper. A new key exchange protocol is proposed to the SIM cards with the presented method, where the card has been produced and the secret key has not been loaded.

Various different models have been investigated to provide for secure communication of SIM technology. In some of these models, secret keys were assigned during production process [3-8]. However in [3], while secret keys weren't assigned during production process, it was proposed that keys that they developed assign exchange protocol stack to SIM technology for providing secure communication.

This study will be categorized into four sections. In the first section, the literature review and the content of the study are described. Section 2 based on the latest years usage of smartphones and smart devices that work with SIM, the infrastructures and the mathematical structures of the key exchange and authentication models in the literature are examined for the security of SIM technology. It is mentioned the differences between analyzed models. In Section 3 to ensure SIM security password-based SIMSEC protocol is proposed and the infrastructure of the method is shown mathematically. In the last section, the results obtained in the study and the studies that are aimed to be done in the future are given and a hybrid model is presented using the password-based key exchange model and SIMSec protocol together. It is stated that reliable models will be studied on providing the infrastructure enabling secured access between SIM cards that are not loaded with an ephemeral key during the production and service provider.

Key Exchange and Authentication Models

This section summarizes the working principles and mathematical backgrounds of password-based password-protected models from key exchange and authentication models in a study [9,10]. The notations and parameters used in all models discussed throughout the study are given in Table 1.

Table 1. Notations

Parameters	Definitions
π	Password of client
p	Large prime number of at least 1024 bits
q	g / p-1 prime number
G	Z_p subgroup
g	Generator of group G
r_A, r_B	Figures randomly selected in the session
Z_p	Set of integers with elements 0 to p-1
t_A, t_B	$t_A = g^{r_A}$ $t_B = g^{r_B}$
x_A, x_B	Client and server's private long passwords
Z_{AB}	Shared information (secret)
K_{AB}	Derived session key
H_i (.)	Unicast sum functions. H_1 H_2 H_3…

Diffie-Hellman encrypted key exchange (EKE)

Encrypted key exchange In the Diffie-Hellman-EKE model is that a shared key is encrypted with a public key by using the password and is sent from client to server so that the client and server can communicate securely [11]. Only the party who knows the password can complete the protocol. The flow of this protocol is given in Figure 1 [11,12].

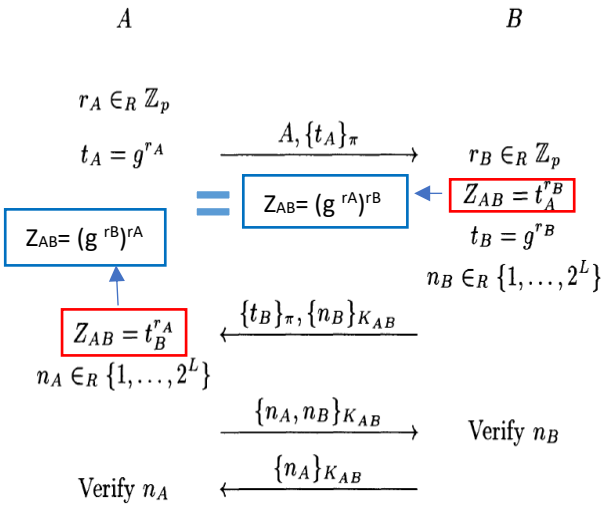

Fig. 1. Diffie-Hellman-EKE

This protocol was developed against "partition" attacks. According to this idea, the attacker who guesses the password can check whether the values t_A and t_B are valid. This set of protocols is based on the difficulty of finding the parameters selected by the attacker [12].

Password–based protocol (PAK)

The biggest problem in the password-based protocol (PAK) model is to estimate the π value of the client [12,13]. If the attacker knows the value π and has an idea of how the algorithm will work, the attacker can find all t_A, t_B values. An attacker could damage the communication information between the parties. Therefore, Bellare has customized the key generation function to make it difficult to find the session key. However, the symmetric encryption algorithm used in the protocol must provide randomness characteristics. Boyko obtained the "P" value by using relatively prime values [14] between r and q in the protocol set called PAK. With the help of these values, the switch in group G was produced. The proposed key exchange protocol is given in Figure 2 [15].

Since the PAK protocol uses the summary function and the "r" value in calculating P, the cost is higher than Diffie-Hellman. Another difference between the two protocols is the customization of the key generation function. So, the authentication mechanism was added.

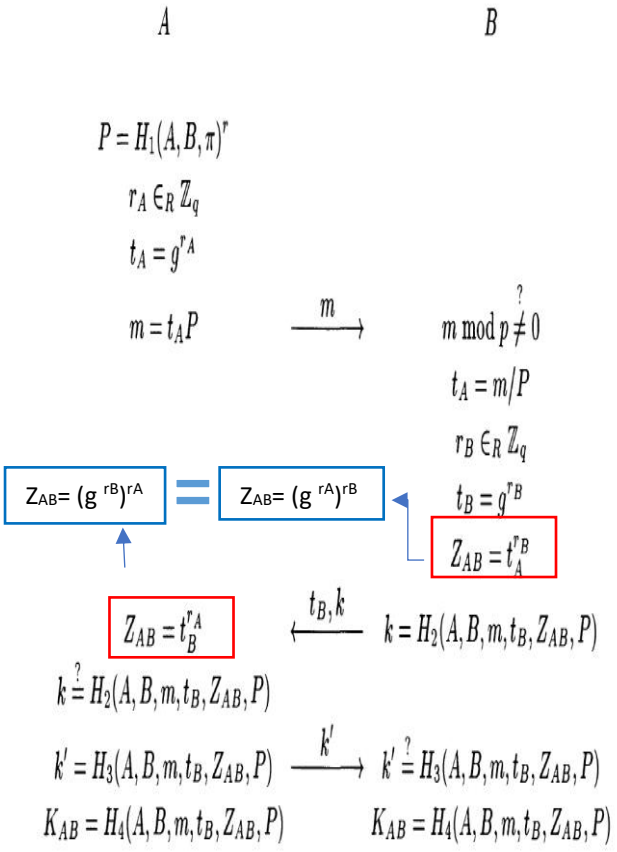

Fig. 2. Password–based Protocol (PAK)

Password protected key exchange (PPK)

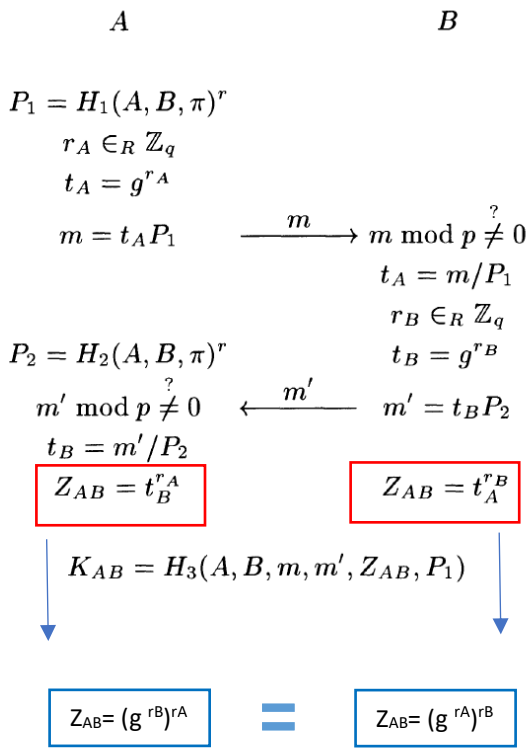

Fig. 3. Password protected key exchange protocol (PPK)

In the password protected key exchange (PPK) model, it is harder for an attacker to obtain the "π" value. The client calculates P_1 and P_2 using the values "π" and "r"[14]. This brings an extra calculation cost for the client. The PPK model is shown in Figure 3 [14, 16].

Password–based protocol-R (PAK-R)

The R-password-based protocol (PAK-R) refers to the PAK model [16,17]. The main difference with PAK is that the calculation costs of the client is transferred to the server. In the PAK-R model, many operations are performed on the server. In this way, the cost balance between the client and the server is achieved. For an attacker it is difficult to estimate the client or the server. Therefore, it becomes efficient to use even in devices with low computational power. Another difference is; The "t_A" value calculated on the server-side is customized. The PAK-R model is shown in Figure 4 [16, 17].

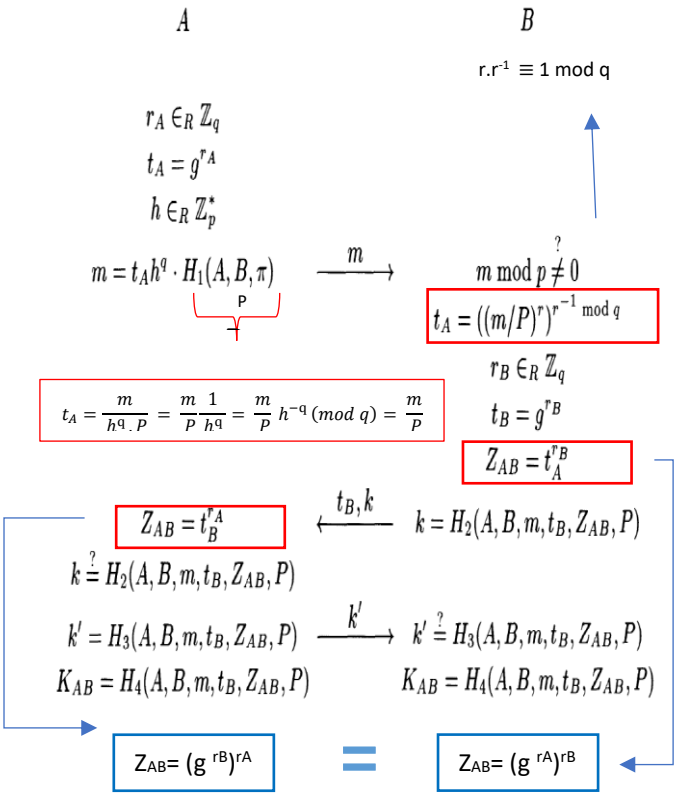

Fig. 4. Password–based protocol-R protocol (PAK-R)

Password–based protocol-Y (PAK-Y)

The PAK-Y model, called the Y-password-based key exchange protocol, refers to the PAK model as the PAK-R model [18]. The problem in this model as well is that the attacker finds the π value that the client has. As with the PAK model, an attacker can find all t_A, t_B values if he has any idea about the π parameter and the algorithm. In order to avoid this situation, it is made difficult to find π value in PAK-Y model. The "v" function is defined to provide this difficulty. "V" is defined by the client with the value "v". The hash value of the defined expression is also computed. In this way, it is made difficult to reach "π" value for the attacker. Schnorr signature was added in the authentication section and the protocol set was terminated. The PAK-Y model is shown in Figure 5 [18,19].

In this protocol, the t_A value for computing the information shared by the server; As with other models, no additional calculation has been made on the server side. The value is obtained by processing in the "m" message from the client.

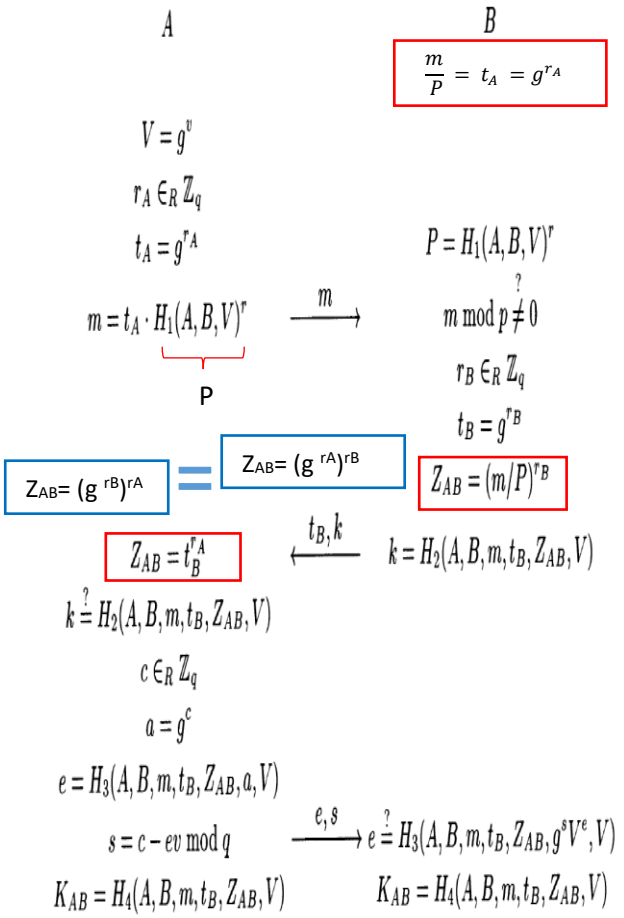

Fig. 5. Password–based protocol-Y protocol (PAK-Y)

Secure password exponential key exchange (SPEKE)

In another model, the security encrypted exponential key exchange model (SPEKE), and the security dimension of the transactions are increased by using "P" instead of g in Diffie-Hellman EKE [19]. P is defined as π^2. In the PAK protocol, the calculation cost and processing power of P' (π^2) is lower than the calculation cost of the function H_1 (A, B, π) ^{r} .Given the client's computing power, calculating $P = \pi^2$ is inappreciable enough for the client to ignore.

The calculation costs in Diffie-Hellman depends on the size of r_A and r_B exponents. Parameter selections are made according to security levels. The difference of SPEKE and PAK is that it is easier calculating P with SPEKE since the summary value H and the temporary key (r_A and r_B) values are not processed. Models in other studies examined that the temporary key values "r_A, r_B" were randomly selected from the set of integers in the mode p and q bases. As for this model, for each session, any value between 1 and 2^L is chosen instead of randomly chosen temporary key values of r_A, r_B . SPEKE protocol is given in Figure 6 and there is no security proof for this protocol [19,20].

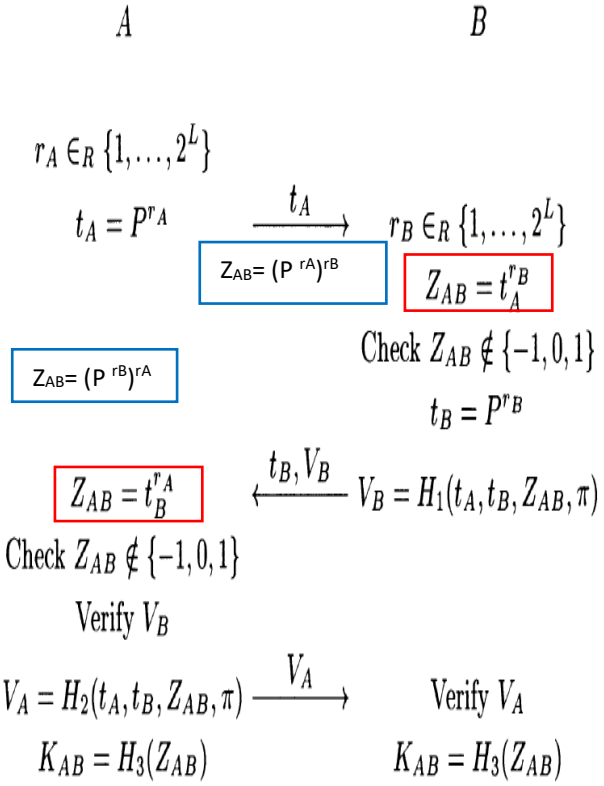

Fig. 6. Secure password exponential key exchange protocol (SPEKE)

B-Secure password exponential key exchange (B-SPEKE)

Security password exponential key exchange-B (B-SPEKE) is an improvement of the SPEKE model [21]. This model uses two password messages. The first one is the Z_{AB} value, the other one is $\overline{Z_{AB}}$ value. The Z_{AB} value is sent to the other party by taking the summary function against the risk of attack by the attacker. It is aimed to make the model more secure by using $\overline{Z_{AB}}$ value. Verification is performed with two (Z_{AB}, $\overline{Z_{AB}}$) different shared information values.

The protocol set is terminated with session keys generated after passing these validators. Unlike PAK models, in the B-SPEKE protocol given in

Figure 7, randomly selected transient key values for each session are selected from any value between 1 and 2^L values as in SPEKE [21,22].

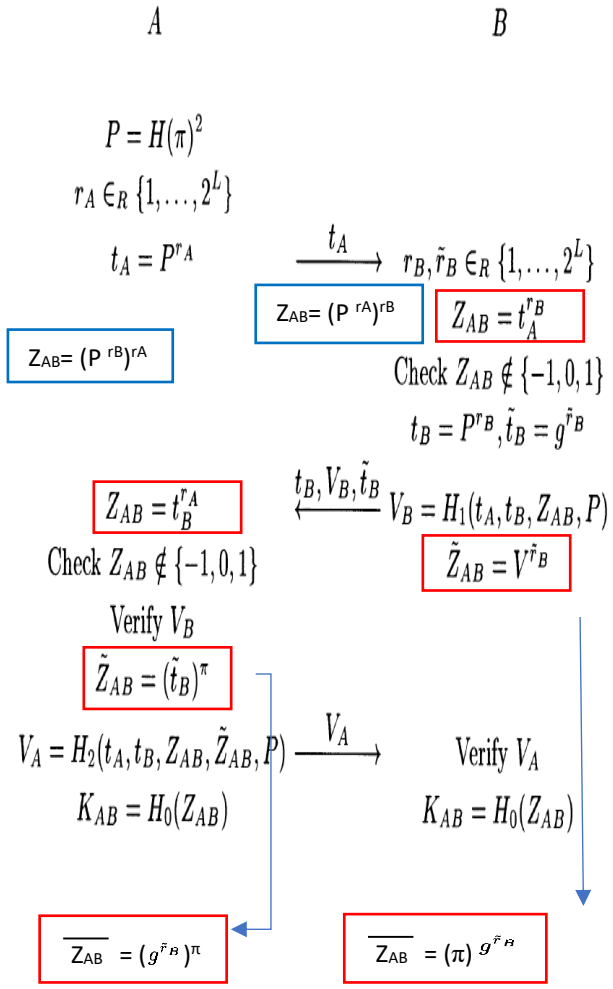

Fig. 7. B-Secure password exponential key exchange (B- SPEKE) protocol

Secure remote password (SRP)

The Security remote password (SRP) model is based on the importance of the "u" value [23]. The purpose of selecting "u" is to ensure that the client knows π. The first message is defined in the protocol when the client knows the "V" value. It is made difficult by the attacker to estimate the value of "u", by randomly assigning "u" value by the server in each session. In this way, communication becomes secure. The Communication doesn't start immediately after you verify the session key. The second authentication is done by taking the hash value and the protocol terminates when it is verified that the other party is the person claimed. Temporary key values are selected in"mod q" integers and t_A values are sent directly by the client to the server through the transitions. Shared information and session key functions have been customized by adding additional parameters to prevent the attacker from making the communication unsafe. The SRP protocol is given in Figure 8 [23].

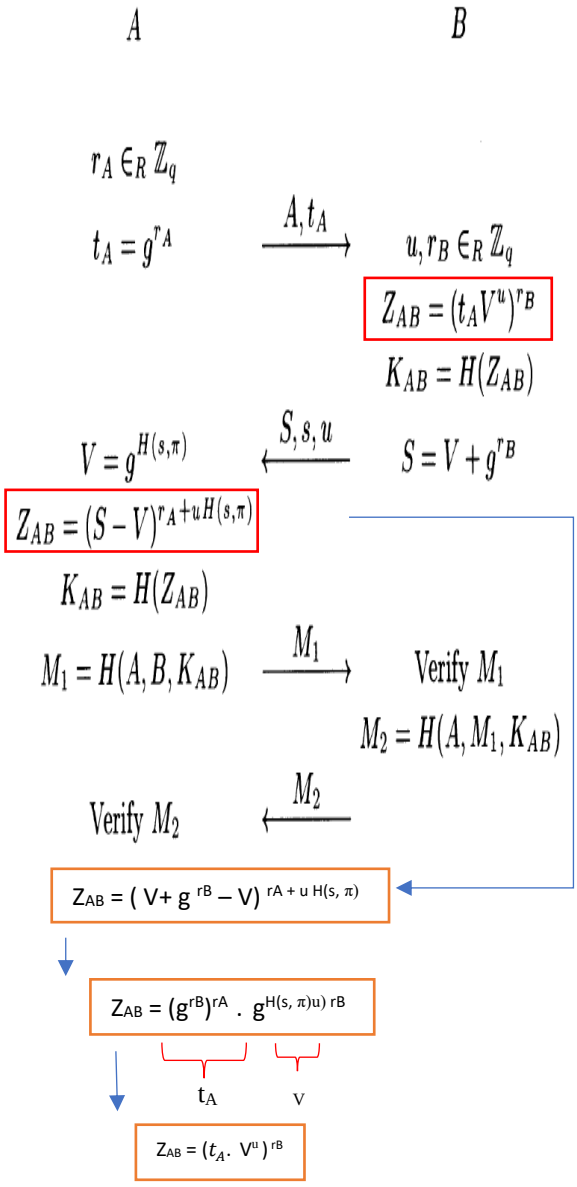

Fig. 8. Secure remote password protocol

Authentication via memorable password (AMP)

Calculating of shared (secret) information values differ in authentication via memorable password model [24]. The Z_{AB} value is calculated by using "e" which is the summary of t_A and T values. Here, as in SRP, after the session key is

validated, the communication does not start immediately and the second authentication is performed by taking the summary value. The protocol terminates when it is confirmed that the other party is claimed person. The generated AMP protocol is given in Figure 9. There is no security proof for SRP and AMP protocols [24].

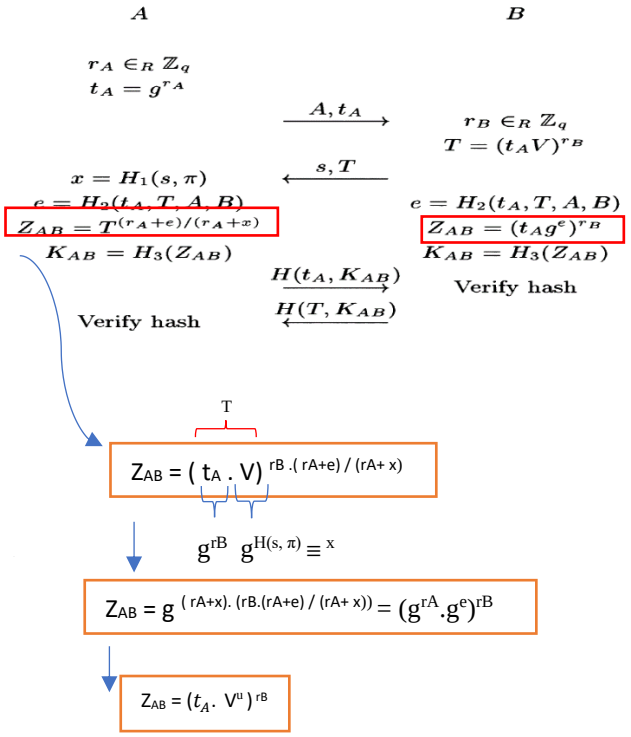

Fig. 9. Authentication via memorable password protocol.

It is observed that parameter values differed in these models. Selected parameter values are selected from different sets. In this way, newly produced functions are introduced. Table 2 provides information about the transmission and usage of the shared information that constitutes these models and the password of the client.

Table 2. Client and server cost and the number of phases

Models	Client		Server		
	Number of Hash functions	Number of exponentiations	Number of Hash functions	Number of exponentiations	Number of messages (transmission)
EKE	0	2	0	2	4
PAK	4	2	3	2	3
PPK	3	2	1	2	2
PAK-R	4	3	3	3	3
PAK-Y	4	4	4	2	3
SPEKE	2	2	2	2	3
B- SPEKE	3	3	2	4	3
SRP	1	3	1	2	4
AMP	4	2	3	2	4
This paper	**4**	**2**	**3**	**2**	**3**

Table 3.Differences and usage of parameters

Models / Notations	π	t_A	t_A t_B	Z_{AB} $\overline{Z_{AB}}$
EKE	π	π	------	$Z_{AB} = (g^{rB})^{rA}$
PAK	$P = H_1(A, B, \pi)^r$	$P = H_1(A, B, \pi)^r$	$P_2 = H_2(A, B, \pi)^r$	$Z_{AB} = (g^{rB})^{rA}$
PPK	$P_2 = H_2(A, B, \pi)^r$ $P_1 = H_1(A, B, \pi)^r$	$P_1 = H_1(A, B, \pi)^r$	------	$Z_{AB} = (g^{rB})^{rA}$
PAK-R	$m = t_A . h^q . H_1(A, B, \pi)$	$h^q . H_1(A, B, \pi)$	------	$Z_{AB} = (g^{rB})^{rA}$
PAK-Y	$m = t_A . H_1(A, B, V)^r$	$H_1(A, B, V)^r$	------	$Z_{AB} = (g^{rB})^{rA}$
SPEKE	$P = \pi^2$	------	------	$Z_{AB} = (P^{rB})^{rA}$
B-SPEKE	$P = H(\pi)^2$	------	------	$\overline{Z_{AB}} = (g^{\pi})^{rB}$ $Z_{AB} = (P^{rA})^{rB}$
SRP	$V = g^{H(s,\pi)}$	------	$S = V + g^{rB}$	$Z_{AB} = (t_A . V^u)^{rB}$
AMP	$V = g^{H(s,\pi)}$	------	------	$Z_{AB} = (t_A . g^e)^{rB}$
This PAPER	**V**	**t_{SS}**	------	**$Z_{SS->SK}$**
	$P = H_1(ID_{SIM}, V)$	$P = H_1(ID_{SIM}, V)$		$Z_{SS->SK} = t_{SK}^a$

The transmission of these parameters varies in the models. Some models have transmission confidentiality, while others have been ignored.

Transmission confidentiality has been strengthened by these operations during transmission. Another advantage is the difficulty of computing the password-accepted parameters for models by the attacker.

With some models the parameters that make up these protocols are transmitted to the opposite side without any parameters being processed. And with other models, they are processed with other parameters.

The hash functions and exponential expressions used in these models are of great importance. The calculation costs of the client and server parts of these models are calculated according to the number of uses and the upper dimensions of the different summary functions. The scarcity of these transactions decreases the cost account. These cost accounts are observed to differ between the client and server, and these differences were found to be distinctive by the attacker. It is understood that a balanced distribution of the cost account by the client and server is a better solution for protocol sets. The phases of these values and the number of passing is presented in Table 3.

Authorized Key Exchange for SIMSEC Protocol

In this section, a protocol is proposed to enable secure communication between the service provider and the SIM which did not have a secret key installed during production. Password-based authentication algorithm offers an integrated approach to the SIMSec protocol. Secure communication between the service provider and the SIM must be extremely safe. SIM mobile service provider, IMSI (international mobile subscriber identity) international identification number, ICCID (integrated circuit card ID) card number, LAI (local area identity) area code, K_i (authentication key) authentication key, SMSC (short message service center) the short message service number and the SPN (service providers number) store data about the service provide [25]. Figure 10 illustrates how these operations are performed.

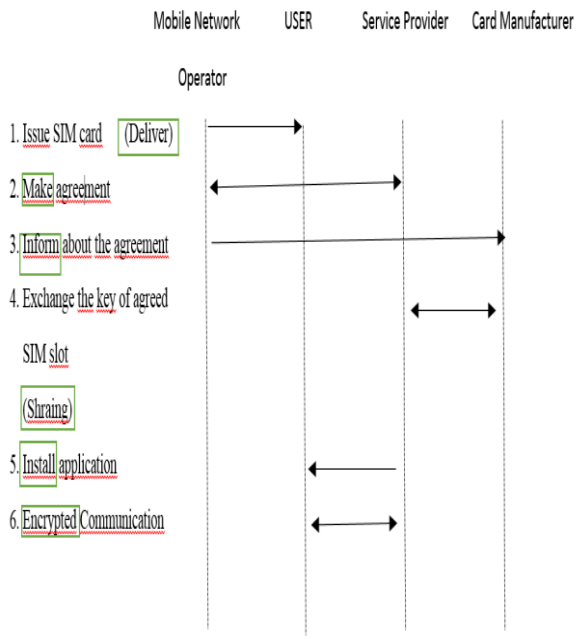

Fig. 10. Secure communication between service provider and SIM

The transactions among mobile network operator, user, service provider and card manufacturer are expressed as follows.

In the secure communication between the service provider and the SIM, the SIM is first provided to the user by the MNO. For the service provider to use the SIM, an agreement is made between the service provider and MNO. This agreement is notified to the card maker. In addition to this, the SIM, which has an agreement between the card and the service provider makes a key exhange. (the encryption key is transmitted to the service provider). By downloading the application from step 5 in Figure 10, secure encrypted communication is provided between the service provider and the SIM Card. The proposed protocol is summarized step by step in Figure 11.

The service provider calculates the P value by generating a random variable called V, which is 10 characters long, as shown in the first step in Figure 11. In the protocol known only by the service provider, the value of "a" randomly generated by the service provider is used as the upper value of the exponentiation process. Length is 384-bit, adhering to the standard. After creating a value, g^a is calculated and t_{ss} value is obtained. The P value created with this value is processed and sent to the SIM card. The SIM card calculates the t_{ss} value after checking

whether the incoming value is empty. The value b is then set to 384-bit, the length of which is bound to the standard. The t_{sk} value is then calculated. By using the t_{ss} value sent from the other party, the shared information $Z_{SS->SK}$ value is obtained.

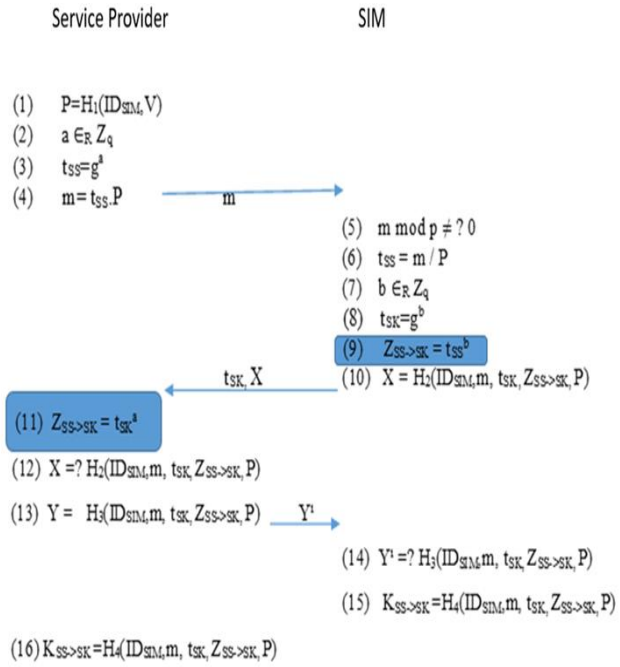

Fig.11. Password-based Key Exchange for SIMSEC Protocol

The SIM card calculates the X value defined in step 10 in Figure 13 and sends it to the service provider along with the t_{sk} value. The service provider obtains the shared information $Z_{SS->SK}$ value by means of the sent t_{sk} value. It then calculates the value X' in step 12 given in Figure 13, which is the same as the X value. If the two results are equal (only the service provider and the SIM card know the V value), the service provider verifies the identity of the SIM card. Otherwise, the protocol is terminated.

The service provider also calculates the Y value defined in step 13 of Figure 13 and sends it to the SIM card. The SIM card calculates the Y value in step 14 of Figure 13, which is the same as the Y value. The only difference found when calculating the Y' value is that the hash function $(g^b)^a$ is replaced with $(g^a)^b$ instead. Since these two values are the same, the results of the hash function will be the same. The SIM card and service providers agree on $C_{SR->SK}$ and the protocol is terminated.

The biggest problem in this approach; It is a problem of estimating the V value owned by the service provider. If the attacker knows the value of V and has an idea of how the algorithm works, he can find all t_{ss}, t_{sk} values. An attacker could damage the communication information between the parties. Therefore, V must be selected randomly.

The security analysis of the SIMSEC protocol is examined in three different attacker types;

- An attacker in the SMS channel who knows the public values g and p can execute an attack through the key exchange protocol.
- Although the MNO is known as a thrustworthy institution there is an employee risk. Individual employees could acces ID_{SIM} and perform an attack on the SMS channel. Therefore MNO employees can't be trusted on an individual basis.
- Another type of attacker is that; another service provider may have previously entered into an agreement with MNO and executed the key generation protocol with the SIM card. In this case, this service provider knows the ID_{SIM} data and therefore can attack the key exchange protocol by knowing the ID_{SIM} value and the public g and p values.

Diffie-Hellman algorithm is used on SIMSec basis. It is not possible to calculate the numbers $(g^b)^a$ (mode n) and $(g^a)^b$ (mode n) in this algorithm by those who do not know the numbers a or b. To generate the same key, the attacker must be able to obtain one of these two numbers. In the SIMSec key generation protocol, key confidentiality between the SIM card and the service provider is ensured in this way.

Conclusion and Future Works

Models are examined for secure communication between SIM Card and service provider. The biggest limitation of SIMs is their low capacity and processing power. In this study, these limitations are ignored. A protocol has been proposed to enable secure communication between the service provider and the SIM which doesn't have a secret key installed during production. This set of protocols has been integrated into the SIMSec protocol and introduced a new approach. As a future study, a reliable post-quantum protocol will be studied.

This method verifies each other's identities, protected data integrity with a new approach,

and increased security against Man-in-the-middle attack and replay attacks. With this proposed perspective, attacks that can be carried out over the values that are open to everyone are made more secure thanks to the directed algorithm. Secure communications will continue as attacks that may occur through the key that any employee at a different service provider knows will not go through verification from the other party.

For post-quantum, the Shor algorithm [11] makes traditional public-key cryptography systems insecure, based on problems that are computationally hard for today's technology. This development has made the communication of computers after quantum insecure and necessitated the creation of reliable structures that can replace the systems. Based on this requirement, a new key exchange protocol will be proposed in order to provide the infrastructure enabling secure communication between SIM cards that have not been loaded with secret key during production and service provider.

References

[1] He, S., & Paar, I. C. (2007, July). SIM card security. In *Seminar Work, Ruhr-University of Bochum*

[2] Kapoor, V., Abraham, V. S., & Singh, R. (2008). Elliptic curve cryptography. *Ubiquity*, *2008*(May), 1-8.

[3] Ok, K., Coskun, V., Yarman, S. B., Cevikbas, C., & Ozdenizci, B. (2016). SIMSec: A key exchange protocol between SIM card and service provider. *Wireless Personal Communications*, *89*(4), 1371-1390.

[4] Rongyu, H., Guolei, Z., Chaowen, C., Hui, X., Xi, Q., & Zheng, Q. (2009). A PK-SIM card based end-to-end security framework for SMS. *Computer Standards & Interfaces*, *31*(4), 629-641.

[5] Li, Y., Chen, M., & Nie, J. (2011, September). Mobile commerce security model construction based on sms. In *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1-3). IEEE.

[6] Badra, M., & Urien, P. (2004, March). Toward SSL integration in SIM smartcards. In *2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No. 04TH8733)* (Vol. 2, pp. 889-893). IEEE.

[7] Markantonakis, K., & Mayes, K. (2005). A Secure Channel protocol for multi-application smart cards based on public key cryptography. In *Communications and Multimedia Security* (pp. 79-95). Springer, Boston, MA.

[8] Handschuh, H., & Paillier, P. (1998, September). Smart card crypto-coprocessors for public-key cryptography. In *International Conference on Smart Card Research and Advanced Applications* (pp. 372-379). Springer, Berlin, Heidelberg.

[9] Schnorr, C. P. (1989, August). Efficient identification and signatures for smart cards. In *Conference on the Theory and Application of Cryptology* (pp. 239-252). Springer, New York, NY.

[10] Boyd, C., Mathuria, A., & Stebila, D. (2003). *Protocols for authentication and key establishment* (Vol. 1). Heidelberg: Springer.

[11] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). Ieee.

[12] Bellovin, S. M., & Merritt, M. (1992). Encrypted key exchange: Password-based protocols secure against dictionary attacks..

[13] Bellare, M., Pointcheval, D., & Rogaway, P. (2000, May). Authenticated key exchange secure against dictionary attacks. In *International conference on the theory and applications of cryptographic techniques* (pp. 139-155). Springer, Berlin, Heidelberg.

[14] Boyko, V., MacKenzie, P., & Patel, S. (2000, May). Provably secure password-authenticated key exchange using Diffie-Hellman. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 156-171). Springer, Berlin, Heidelberg.

[15] MacKenzie, P. (2002). The PAK suite: Protocols for password-authenticated key exchange. In *IEEE P1363. 2*.

[16] Mackenzie, P. (2001, April). More efficient password-authenticated key exchange. In *Cryptographers' Track at the RSA Conference* (pp. 361-377). Springer, Berlin, Heidelberg.

[17] Lenstra, A. K., & Verheul, E. R. (2000, August). The XTR public key system. In *Annual International Cryptology Conference* (pp. 1-19). Springer, Berlin, Heidelberg.

[18] Jablon, D. P. (1996). Strong password-only authenticated key exchange. *ACM SIGCOMM Computer Communication Review*, *26*(5), 5-26.

[19] MacKenzie, P. (2001). On the Security of the SPEKE Password-Authenticated Key Exchange Protocol. *IACR Cryptol. ePrint Arch.*, *2001*, 57.

[20] IEEE P1363 Working Group. (2003). Standard specifications for password-based public-key cryptographic techniques. *IEEE P1363. 2/D11*.

[21] Perlman, R., & Kaufman, C. (2001, August). PDM: A new strong password-based protocol. In *Proceedings of the 10th USENIX Security Symposium* (pp. 313-321).

[22] Jablon, D. P. (1997, June). Extended password key exchange protocols immune to dictionary attack. In *Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises* (pp. 248-255). IEEE.

[23] Wu, T. D. (1998, March). The Secure Remote Password Protocol. In *NDSS* (Vol. 98, pp. 97-111).

[24] Kwon, T. (2000). Ultimate solution to authentication via memorable password. *Contribution to the IEEE P1363 Study Group*.

[25] Lee, W. C. (1995). *Mobile cellular telecommunications: analog and digital systems*. McGraw-Hill Professional.