Understanding group signature methods in making digital signatures to maintain the validity of messages

IOP Conf. Series: Journal of Physics: Conf. Series **1230** (2019) 012072 doi:10.1088/1742-6596/1230/1/012072

Understanding group signature methods in making digital signatures to maintain the validity of messages

Saut Dohot Siregar[1], Jepri Banjarnahor[1], N P Dharshinni[1], Saut Parsaoran Tamba[1], Robin[2]

[1]Faculty of Technology and Computer Science, Universitas Prima Indonesia, Indonesia
[2]Informatics Management Study Program, STMIK Mikroskil

E-mail: sautdohotsiregar@gmail.com*

Abstract. In this millennial era, a large amount of digital data traffic going through communication media on digital technology every day. Most of the data are documents and other essential information. The existing rapid development of technology nowadays, information can be easily faked. To make sure the validity of a digital document, a digital signature is required to verify the originality of the document. The purpose of this research is to design software which implemented the group signature algorithm to apply and verify digital signatures. The Signature Group algorithm used in this research is the Tseng-Jan scheme. The Tseng-Jan scheme consists of 5 stages: setup, join, sign, verify, and open. After applying the algorithm using 2 digits key and 3 digits key on the samples, 80% of the verification experiment on 2 digits key was succeeded 70% of the verification experiment on 3 digits key was succeeded.

1. Introduction

Digital signatures are now an important part in a digital document [1]. The document can in the form of rich text files, images, or multimedia files such as audio and video. Digital signatures are technically suitable and supportive for a system [2, 3]. The application of digital signatures includes: digital certificates for e-commerce security, for signing legal contracts and for securing software updates [4, 5]. For example, group signature was presented by Khader in 2007 [6, 7]. The digital signature is a mechanism to replace signatures manually on paper documents [6].

The need for these signatures is increasingly strengthened due to the growing development of internet technology, which enables to distribute documents easily and freely. One development of digital signatures is group signatures. The concept of Group signatures was first introduced by David Chaum and Eugene van Heyst in 1991 [9]. Each member of the group can sign a message as a representative of the group anonymously and unlink. We can see the group signature application in joint account ownership, electronic cash and others.

Digital signature is essential to validate the originality of an identity. To make sure validity of a document, a digital signature is required to avoid faked identity. There are many digital signature methods to secure and verify the validity of a document. One of them is group signature [9, 10]. The digital signature scheme group is a method that allows each member of a group to sign a message where the verifying can confirm that the signature is correctly from the group but it is not known who is signatory of the group. This scheme assumes that the existence of a group manager has the purpose

of calculating and giving a secret key to each member of the group that will be used to sign the message as a representative of the group. In this Group signatures scheme, the verification and open process is a very important process because if something goes wrong from this process, it will cause a user's distrust of the system. Where this verification process is useful for determine the validity of existing signatures. While the open process is used find out who the owner of the signature has been made.

Some security requirements must be met by a group digital signatures scheme are (1) Unforgeability. Only group members can issue valid signatures on behalf of all group members. Or in other words, only group members can issue signatures that can be verified using the group's public key; (2) Conditional Signer Anonymity. In a group, each member can easily check whether a pair messages and signatures have been signed by several group members. And each group member cannot know the group members who have not signed. Only group managers can correctly determine group members who have signed; (3) Undeniable Signer Identity. Group managers can always determine the identity of the group member who issued the signature. Furthermore, the group manager can also prove to other entities (e.g. judges, judges, etc.) that group members have signed a document. However, this does not harm the members of the group on messages that have been signed. And also it will not harm group members who will be signed by members of the group concerned, (4) Unlinkability. Computationally, each member cannot find out whether other members are doing twice or more signatures. Only group managers can prove that there are two or more signatures made by group members. Group managers can find out for their member groups; (5) Security Agains Framing Attacks. Framing attacks are attacks on digital signature groups where a group member can sign a document on behalf of another group member. In connection with this case, a safe digital signature group scheme should be able to overcome framing attacks; that is, there is no group member, including group managers who can sign a message on behalf of other group members. This can be guaranteed by performing an open procedure; and (6) Coalition Resistance. There are no groups of members, including group managers who can conspire and generate digital signatures that are valid but cannot be tracked. In particular, this security aspect aims to prevent attacks where a coalition between group members gathers, and collects information, and generates digital signatures that pass the verify procedure but cannot determine who the signatory is by the open procedure [11, 12]. For more details, in the figure 1 below there are several variations of group signatures.

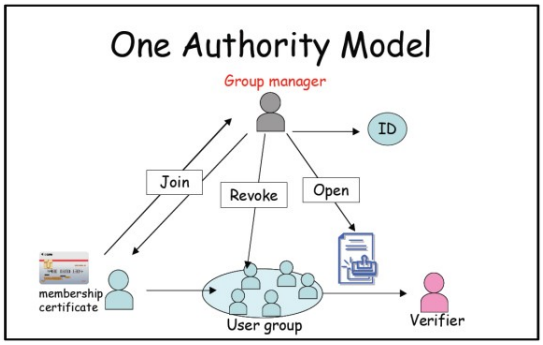

Figure 1. One Authority Model [13]

2. Methodology

In the group digital signatures scheme, members of a group can do a digital signature on a document on behalf of all group members. The signature can be verified using the group's public key. When a document has been signed, only a group leader can determine who the member has signed the document [5]. Furthermore, these group signatures must be designed so that no group member can falsify the signature of other group members. So, in the group digital signatures, there is one group public key and more than one secret key for group members. This concept is often applied in

companies; where group signatures are used to validate price lists, press releases, or digital contracts; the customer only knows the company's single public key to verify the signature. By using this digital signatures group, companies can hide their internal structure while determining which employees sign the document.

To facilitate understanding of Group signatures, several examples will be given for implementing group signatures. A company has many computers, where each computer is connected to the network. Each division of the company has its own printer and is connected to the network and only staff from each division allowed to use their own printers. Before using the printer, the printer must first ensure that the staff is working in the division. At the same time, the company wants confidentiality. The name of the user is not displayed. However, if at the end of the day someone is found using a printer often, the director can find out who is abusing the printer, and the director will bill the person. Another example is Group signatures that are suitable for use by staff from a fairly large company. And the staff represents the company to sign a document. In this example, the verifier only knows that the representative of the company has signed the document. The verifier does not need to know who signed the document Verifier only knows the public key of the company.

The scheme used is the Tseng-Jan Group Signatures Scheme which consists of 5 stages: (1) the setup stage, namely the stage of public and private key generation of groups and public parameters to be used; (2) join stage which is the stage of public and private key generation for members who will join the group; (3) the signing stage is the signaling stage of a message by using the private key of the member that will produce a signature; (4) the verify stage is the stage to determine the validity of the signature that has been produced; and (5) the open stage is the stage to find out who the owner of the signature is by using the public and private keys of the existing members [14]. One of the most popular public key algorithms in cryptography is the RSA algorithm, the RSA algorithm was created by 3 researchers from Massachusetts Institute of Technology in 1976, namely Ron Rivest, Adi Shamir, and Leonard Adleman. The security of the RSA algorithm lies in the difficulty of factoring large numbers into prime numbers. Factoring is done to obtain the private key. As long as the factoring of these numbers has not been found, during that time the security of the RSA is still maintained. The RSA algorithm is based on the Euler theorem which states that: [15, 16]

$$a^{\Phi(n)} \equiv 1 \ (mod\ n) \tag{1}$$

At RSA, the key generator algorithm is stated as follows select two arbitrary primer p and q; calculate n = p. q (preferably $p \neq q$); calculate $\Phi(n) = (p - 1)*(q - 1)$; select Public key e which is relatively prime to $\Phi(n)$.

Generate the priority key (d) with the following equation:

$$d = (1 + k\ \Phi(n))/e \tag{2}$$

While for the encryption and decryption, the following formula is used respectively: [16, 17]

$$E_e(m) = m^e \bmod n \tag{3}$$

$$d_d(c) = c^d \bmod n, \tag{4}$$

where: at process setup (1) P is a prime number and a minimum of 2 digits and a maximum of 4 digits; (2) q is the biggest factor of (p-1); (3) g is generator of p; and (4) x is a number greater than 0 and smaller than (q-1). At process join the parameters used to calculate are in the form of numbers with the requirement that x[i] and k[i] are numbers greater than 0 and smaller than (q-1). At process sign the parameters used are t1, t2, t3 and t4 which are all in the form of numbers greater than 0 and smaller than (q-1) [18].

3. Result

The result obtained using Tseng-Jan Group Signatures Scheme process is deviced into 5 phase.

- The first phase is the setup phase where public key and private key from group and public parameter used had been determined.
  First, determine the value of *p* which must be a prime number, 47 for example. Second, determine to value of *q* which is the biggest factor of (*p*-1) 23 for example. Third, determine the value of *g*

which is a *p* generator, 13 for example. Last step is calculating the public group key *y* where *y=g^x* mod *p*, 4 for example.

- The second phase is the join phase where the public and private key for the group member will be merge into group.
  First, input a public group key, 4 for example. Second, calculate the public key y[1] which result is 32 (y[1] = g^x[1] mod p) and input private key value k[1], 4 for example (0 < k[1] < q). Third, calculate r[1] which result is 9 (r[1] = g^(-k[i])*y^k[i] mod p) and s[1] which result is 9 (s[1] = k[1] – r[1]*x mod q). Fourth, check if g^s[1] * y^r[1] = g^k[1] mod p, if they are equal then next to the sign phase, if they are not equal then repeat this phase beginning from determining the value of k[1] until g^s[1] * y^r[1] is equal to g^k[1] mod p.
- The third phase is the sign phase where the signature processing on digital message using private key from group member will generate a digital signature.
  First, input a digital message to be generate digital signature, ”Unpri” for example using hash code B6531561D0FCF451CCAB56CC0DBE072D1D2975B9. Second, determine value of t1, t2, t3 and t4 where (0 < t < q). Second, calculate value of A which result in 7 (A = r[1]^t1 mod p), calculate the value of B which result in 4 (B = t1*s[1] - t2*Hash(A||C||D||E) mod q), calculate the value of C which result in 9 (C = (r[1]*t1 - t3) Mod q), calculate the value of D which result in 3 (D = g^t2 mod p), calculate the value of E which result in 2 (E = y^t3 mod p). The third step is calculate the value of Alpha which result in 16 (Alpha = g^B*y^C*E *D^Hash(A||C||D||E) mod p). The last step is checking if Aplha*A is equal to Alpha^x[i] mod p (Aplha*A = Alpha^x[i] mod p) then the calculation result of digital signature is 25|19|7|4|9|3|2.
- The fourth phase is verification phase where the validity of the digital signature obtained will be validated.
  First, enter or input the message containing the digital signature followed by the B6531561D0FCF451CCAB56CC0DBE072D1D2975B9 hash code and the 25|19|7|4|9|3|2 digital signature. Determine the value of A = 7, B = 4, C = 9, D = 3, E = 2, V = 25, and W = 19. Calculate the value of alpha which result in 16 (alpha = g^B*y^C*E*D^Hash(A||C||D||E) mod p). Check if Aplha^Hash(MD||V) ≡ ((Alpha*A)^V)*(V^W) mod p. In this process, the result obtained is 17 ≡ 42 * 6 mod 47, so that 17 ≡ 17 resulted in True which means the digital signature is “Valid”.

- The last phase is the open phase to verify the right user’s digital signature using the public and private key and other group members.

  MD = Hash(Message) = B6531561D0FCF451CCAB56CC0DBE072D1D2975B9, resulted in 25|19|7|4|9|3|2 digital signature.

  Alpha = g^B*y^C*E*D^Hash(A||C||D||E) mod p

  = 21 ^ 10 * 4 ^ 8 * 12 * 18 ^ Hash(2||8||18||12) mod 23

  = 18

  18 = 18 → True

  A pair of the (k[1] = 6; r[1] = 2; s[1] = 2) key is the owner of the digital signature.

After doing some testing sample with 2 digit key and 3 digit key using type *.txt, *.doc and *.ico. Then the following results are obtained:

Table 1. Calculation results of 2 digit key file type *.txt

No	p	Q	G	X	Xi	ki	t1	t2	t3	t4	Digital Signature	Validation
1	47	23	13	4	9	16	15	18	9	14	25|19|7|4|9|3|2	Yes
2	59	29	31	15	4	3	27	13	16	8	22|18|33|4|21|30|36	Yes
3	23	11	5	6	3	2	5	2	3	5	8|0|12|4|6|2|6	Yes
4	47	23	31	1	9	8	1	10	6	2	25|12|8|0|2|36|2	Yes
5	23	11	10	5	9	6	1	3	5	9	16|1|18|9|2|11|11	Yes
6	47	23	39	7	20	20	1	7	21	7	17|20|14|18|16|35|31	Yes
7	83	41	22	14	16	30	2	11	2	32	40|18|77|14|14|20|75	Yes
8	59	29	44	18	4	3	20	22	14	11	41|27|26|0|14|41|7	Yes
9	79	13	66	8	11	11	4	7	1	1	72|8|5|11|3|77|26	No
10	89	11	51	7	9	8	6	2	1	8	8|5|8|4|9|20|24	No

Table 2. Calculation results of 2 digit key file type *.doc

No	p	Q	G	X	Xi	ki	t1	t2	t3	t4	Digital Signature	Validation
1	47	23	13	4	9	16	15	18	9	14	28|17|21|12|6|27|24	Yes
2	59	29	31	15	4	3	27	13	16	8	22|3|33|4|21|30|36	No
3	23	11	5	6	3	2	5	2	3	5	8|3|12|4|6|2|6	Yes
4	47	23	31	1	9	8	1	10	6	2	25|2|8|0|2|36|2	Yes
5	23	11	10	5	9	6	1	3	5	9	16|1|18|9|2|11|11	Yes
6	47	23	39	7	20	20	1	7	21	7	17|5|14|18|16|35|31	Yes
7	83	41	22	14	16	30	2	11	2	32	40|0|77|14|14|20|75	Yes
8	59	29	44	18	4	3	20	22	14	11	41|1|26|0|14|41|7	Yes
9	79	13	66	8	11	11	4	7	1	1	72|0|5|11|3|77|26	No
10	89	11	51	7	9	8	6	2	1	8	8|0|8|4|9|20|24	No

Table 3. Calculation results of 2 digit key file type *.ico

No	p	Q	G	X	xi	ki	t1	t2	t3	t4	Digital Signature	Validation
1	47	23	13	4	9	16	15	18	9	14	28|5|21|12|6|27|24	Yes
2	59	29	31	15	4	3	27	13	16	8	22|12|33|4|21|30|36	Yes
3	23	11	5	6	3	2	5	2	3	5	8|3|12|4|6|2|6	Yes
4	47	23	31	1	9	8	1	10	6	2	25|22|8|0|2|36|2	Yes
5	23	11	10	5	9	6	1	3	5	9	16|1|18|9|2|11|11	Yes
6	47	23	39	7	20	20	1	7	21	7	17|6|14|18|16|35|31	Yes
7	83	41	22	14	16	30	2	11	2	32	40|10|77|14|14|20|75	Yes
8	59	29	44	18	4	3	20	22	14	11	41|21|26|0|14|41|7	Yes
9	79	13	66	8	11	11	4	7	1	1	72|4|5|11|3|77|26	No
10	89	11	51	7	9	8	6	2	1	8	8|0|8|4|9|20|24	No

Table 4. Calculation results of 3 digit key file type *.txt

No	p	Q	G	X	xi	ki	t1	t2	t3	t4	Digital Signature	Validation
1	503	251	137	25	111	200	209	120	204	136	207|31|122|60|42|13|201	Yes
2	863	431	125	234	100	325	33	221	87	176	4|172|822|192|355|815|289	No
3	383	191	312	134	136	189	52	187	161	188	36|172|206|42|5|82|3	Yes
4	587	293	276	248	127	87	216	274	100	176	555|106|67|108|97|30|108	Yes
5	263	131	175	54	80	128	128	101	50	38	50|118|86|12|108|261|50	Yes
6	587	293	326	207	12	113	218	134	95	135	464|272|537|13|40|516|97	Yes
7	347	173	69	31	44	113	144	87	86	43	87|60|87|53|18|322|119	Yes
8	263	131	230	82	63	110	56	35	98	6	111|48|234|104|11|57|148	No
9	347	173	57	117	37	5	61	114	80	90	121|87|330|13|12|202|48	No
10	107	53	5	36	27	2	33	42	42	40	86|17|33|48|3|47|14	No

Table 5. Calculation results of 3 digit key file type *.doc

No	P	Q	G	X	xi	ki	t1	t2	t3	t4	Digital Signature	Validation
1	503	251	137	25	111	200	209	120	204	136	207|217|122|60|42|13|201	Yes
2	863	431	125	234	100	325	33	221	87	176	4|249|822|192|355|815|289	No
3	383	191	312	134	136	189	52	187	161	188	36|94|206|42|5|82|3	Yes
4	587	293	276	248	127	87	216	274	100	176	555|101|67|108|97|30|108	Yes
5	263	131	175	54	80	128	128	101	50	38	50|17|86|12|108|261|50	Yes
6	587	293	326	207	12	113	218	134	95	135	464|228|537|13|40|516|97	Yes
7	347	173	69	31	44	113	144	87	86	43	87|85|87|53|18|322|119	Yes
8	263	131	230	82	63	110	56	35	98	6	111|84|234|104|11|57|148	No
9	347	173	57	117	37	5	61	114	80	90	121|67|330|13|12|202|48	No
10	107	53	5	36	27	2	33	42	42	40	86|19|33|48|3|47|14	No

Table 6. Calculation results of 3 digit key file type *.ico

No	P	Q	G	X	xi	ki	t1	t2	t3	t4	Digital Signature	Validation
1	503	251	137	25	111	200	209	120	204	136	207|227|122|60|42|13|201	Yes
2	863	431	125	234	100	325	33	221	87	176	4|357|822|192|355|815|289	Yes
3	383	191	312	134	136	189	52	187	161	188	36|102|206|42|5|82|3	Yes
4	587	293	276	248	127	87	216	274	100	176	555|99|67|108|97|30|108	Yes
5	263	131	175	54	80	128	128	101	50	38	50|70|86|12|108|261|50	Yes
6	587	293	326	207	12	113	218	134	95	135	464|58|537|13|40|516|97	Yes
7	347	173	69	31	44	113	144	87	86	43	87|164|87|53|18|322|119	Yes
8	263	131	230	82	63	110	56	35	98	6	111|100|234|104|11|57|148	No
9	347	173	57	117	37	5	61	114	80	90	121|99|330|13|12|202|48	No
10	107	53	5	36	27	2	33	42	42	40	86|21|33|48|3|47|14	No

From the results obtained, the percentage of success of verifying and open for the 2 digit key is around 80% and for the 3 digit key around 70%.

4. Conclusion

These are conclusions obtained from the test result. (1) digital signatures can be stored in the form of files and (2) the process of making signatures can be re-learned (3) successfull percentage for 2 digits test is 80% and successfull percentage for 3 digits 70%.

5. References

[1] Shah F., and Patel H. 2016 *A Survey of Digital and Group Signature*, IJCSMC **5** (1) p 274-278
[2] He, D., Chen, J., and Zhang, R. 2012 *An efficient and provably secure certificateless signature scheme without bilinear pairings*. International Journal of Communication Systems **25** p 1432-1442.
[3] Liang Yan, Zhang Xiao, and Zheng Zhi-ming 2016 *An Electronic Cash System Based on Certificateless Group Signature* **10** p 237-300
[4] Mollin, R. A, 2007 *An introduction to cryptography* (Newyork: Taylor & Francis Group)
[5] Mohamad Ihwani 2016 *Model keamanan informasi berbasis digital signature dengan algoritma RSA* **1** p 15-20
[6] Dalia Khader 2007 *Attribute based group signatures* (Cryptology ePrint Archive, Report 2007/159) p 1-18
[7] Sattar J. Aboud and Sufian Yousef 2013 *Cryptanalysis of attribute typed signature scheme* **28** p 1172-1176
[8] David Cham 1991 *Group Signatures* **91** p 257-265
[9] Rochman, F. F., Raharjana, I. K., and Taufik, 2017 *Implementation of QR Code and Digital Signature to Determine the Validity of KRS and KHS Documents*, Scientific Journal of Informatics, **4** (1) p 8-19
[10] Rouillard, J. 2008 *Contextual QR codes*. In Computing in the Global Information Technology. ICCGI'08. The Third International Multi-Conference p 50-55
[11] Harn, L. and Y. Xu, *Design of generalized ElGamal type digital signature schemes based on discrete logarithm*, Electronics Letters, 1994.
[12] Agarwal, A. and Saraswat, R. 2013 *A Survey of Group Signature Technique, its Applications and Attacks*, International Journal of Engineering and Innovative Technology (IJEIT) **2** (10) p 28-35
[13] Stallings, William, 2011 *Cryptography and network security principles and practices*, (USA: Perason Education)
[14] Bellare, M., Micciancio, D., and *Warinschi*, B. 2003 *Foundations of group signatures*. In Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques, EUROCRYPT'03, p 614–629
[15] Yusuf, M. and Rohman, T. 2012 *Implementasi group blind digital signature dalam sistem e-voting pemilihan kepala daerah*. National seminar on informatics UPN Veteran Yogyakarta p A75-A81
[16] Camenisch, J. 1997 *Efficient and generalized group signatures*, in Advances in Cryptology, Euro Crypto
[17] Schneier, Bruce 1996 *Applied cryptography* (Canada: Wiley & Sons)
[18] e-book Cryptography Theroy and Practice by Douglas R. Stinson www.christianroepke.de/studium/krypto/Crypto-TaP/

Acknowledgement

This paper is funded by Universitas Prima Indonesia