International Journal of Information Processing, 9(4), 100-112, 2015
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Threshold Multi Secret Sharing Using Elliptic Curve and Pairing

V P Binu[a], A Sreekumar[a]

[a]Department of Computer Applications, Cochin University of Science and Technology, Cochin-682022 India, Contact: binuvp@gmail.com

Secret Sharing techniques are now the building blocks of several security protocols. A (t,n) threshold secret sharing scheme is one in which t or more participant can join together to retrieve the secret.Traditional single secret sharing schemes are modified and generalized to share multiple secrets.Use of elliptic curve and pairing in secret sharing is gaining more importance.In this paper we propose a threshold multi secret sharing scheme where more than one secret is shared.When the threshold number of participants collate, the multi secret can be retrieved. The scheme make use of elliptic curve and bilinear pairing.Verification of shares by the participants, shares consistency checking, detection and identification of cheaters are the extended capabilities achieved.The shared secrets are retrieved in single stage here, unlike the multi stage secret sharing scheme.The participants can be added very easily.The scheme is efficient and the number of public parameters are also less compared with the existing threshold multi secret sharing scheme based on the elliptic curve.The dealer can easily modify the secret or add additional secret by changing the public parameters of the scheme.This is the first proposal of a threshold multi secret sharing scheme with extended capabilities using self pairing.

Keywords : Cheater Identification, Elliptic Curve, Multi-Secret Sharing, Pairing, Secret Sharing.

1. INTRODUCTION

Secret sharing is an important technique used for secret management. Securing secret key is very important for the proper execution of security protocols[1-65]. The key idea comes from the problem of secure key storage by Shamir [46] and Blakley [5], however secret sharing schemes have found numerous other applications in cryptography, secret key agreement,visual cryptography, threshold encryption, distributed computing *etc*., [13].

Both Shamir's and Blakley's proposals are (t,n) threshold secret sharing schemes. The secret is shared among n users and t or more users can recover the secret by pooling their shares.Different proposals of threshold schemes are made using linear algebra, number theory, matroids, block codes *etc*., [1]. But Shamir's scheme was the most prominent because it offers perfect security and is flexible. The scheme is based on Lagrange Interpolation. There are also efficient $O(nlog^2n)$ algorithms which can be used for the easy implementation of Shamir's scheme.

Extended capabilities are added to threshold schemes in the later stages. A generalized secret sharing scheme is one where any authorized subset of participants is able to recover the shared secret by pooling their shares. These authorized subset is called the access structure of the scheme. The most efficient and easy to implement scheme was Ito, Saito, Nishizeki's construction [25]. The major issue with generalized secret secret sharing scheme is the share size or the number of shares each participant has to store corresponds to each authorized access structure. Some of the proposals for the generalized secret sharing can be found in [3] [7] [53] [26] [34].

Cheater identification and detection, share verification are the major security requirement in secret sharing scheme.Each participant must be able to check the validity of the shares submitted by other participants during the reconstruction phase and also the shares distributed by the Dealer in the share distribution phase. Verifiable and Publicly Verifiable Secret Sharing(PVSS) schemes are proposed in this regard where not only the participant but any one can publicly verify the validity and consistency of the shares distributed by the Dealer. Dynamic, proactive secret sharing *etc*., made the

Table 1
Comparison of Various Schemes Using Elliptic Curve and Pairing

scheme	Liu [33]	Chen [60]	Wang [59]	Eslami [15]	Proposed
single(ss)/multi secret(ms)	ms	ss	ms	ms	ms
secrets	t	1	t	m +n	$m \geq n$
public parameters	5 + 3m	8 +n-t	8+2*n	8+n+m-t	7+n+m
single stage	Yes	Yes	Yes	Yes	Yes
verifiability	No	Yes	Yes	Yes	Yes
cheater detection	No	Yes	No	Yes	Yes
cheater identification	No	Yes	No	Yes	Yes

problem. This is avoided in our scheme. The verification code does not reveal any information about the secret and is more secure compared with the existing scheme.

7. CONCLUSIONS

In this paper we have proposed a novel threshold multi-secret sharing scheme based on elliptic curve and bilinear pairing. Most of the scheme proposed in the literature use bilinear pairing for verification of shares or identification of cheating. We have used the method of point sharing and verification using self pairing. A non degenerate Tate pairing or modified Weil pairing can be used to share multiple secrets. The number of public parameters are greatly reduced and the security does not depend on the hard computational problem. The verification mechanism can prevent users from cheating. Also the consistency of the shares can be verified by the participants which avoids the need of a trusted dealer.

The proposed scheme is the first multi secret sharing scheme with the extended capabilities of share verification and cheater identification based on self pairing. The use of elliptic curve and self pairing can be further explored to develop secret sharing schemes with more generalized access structure.

REFERENCES

1. C Asmuth and J Bloom. A Modular Approach to Key Safeguarding, *In IEEE Transactions on Information Theory*, 29(2):208–210, 1983.
2. M Ben-Or, S Goldwasser, and A Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation, In *Proceedings of the Twentieth Annual ACM Symposium on Theory of computing*, pages 1–10 ACM, 1988.
3. J Benaloh and J Leichter. Generalized Secret Sharing and Monotone Functions, In *Advances in CryptologyCRYPTO88*, pages 27–35 Springer, 1990.
4. J Bethencourt, A Sahai, and B Waters. Ciphertext-Policy Attribute-Based Encryption In *IEEE Symposium on Security and Privacy*, pages 321–334 IEEE, 2007
5. G R Blakley *et al.*, Safeguarding Cryptographic Keys, In *Proceedings of the National Computer Conference*, 48:313–317, 1979.
6. D Boneh. The Decision Diffie-Hellman Problem, In *Algorithmic Number Theory, Springer*, pages 48–63, 1998.
7. E F Brickell. Some Ideal Secret Sharing Schemes, *Journal of Combinatorial Mathematics and Combinatorial Computing*, 9(2):105–113, 1989.
8. C W Chan and C C Chang. A Scheme for Threshold Multi-Secret Sharing, *Applied Mathematics and Computation*, 166(1):1–14, 2005 .
9. D Chaum, C Crépeau and I Damgard. Multiparty Unconditionally Secure Protocols, In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 11–19, 1988.
10. H Y Chien, J Jinn-Ke and Y -M Tseng. A Practical (t,n) Multi-Secret Sharing Scheme, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 83(12):2762–2765, 2000.
11. R Cramer, I Damgård and U Maurer. General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme, In *Advances in CryptologyEUROCRYPT, Springer*, pages 316–334, 2000.
12. M H Dehkordi and S Mashhadi. An Efficient Threshold Verifiable Multi-Secret Sharing, *Computer Standards & Interfaces*, 30(3):187–190, 2008.

13. Y Desmedt and Y Frankel. Shared Generation of Authenticators and Signatures, In *Advances in CryptologyCRYPTO91*, pages 457–469 Springer, 1992.
14. R Dutta, R Barua and P Sarkar. Pairing-based Cryptographic Protocols: A Survey, *IACR Cryptology ePrint Archive*, 2004:64, 2004.
15. Z Eslami and S K Rad. A New Verifiable Multi-Secret Sharing Scheme based on Bilinear Maps, *Wireless Personal Communications*, 63(2):459–467, 2012.
16. M Fatemi, R Ghasemi, T Eghlidos and M R Aref. Efficient Multistage Secret Sharing Scheme using Bilinear Map, *Information Security, IET*, 8(4):224–229, 2014.
17. P Feldman. A Practical Scheme for Non-Interactive Verifiable Secret Sharing, In 28^{th} *IEEE Annual Symposium on Foundations of Computer Science, 1987*, pages 427–438, 1987.
18. M Franklin and M Yung. Communication Complexity of Secure Computation, In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, pages 699–710, 1992.
19. E Fujisaki and T Okamoto. A Practical and Provably Secure Scheme for Publicly Verifiable Secret Sharing and its Applications, In *Advances in CryptologyEUROCRYPT'98*, pages 32–46 Springer, 1998.
20. V Goyal, O Pandey, A Sahai and B Waters. Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data, In *Proceedings of the* 13^{th} *ACM Conference on Computer and Communications Security*, pages 89–98 ACM, 2006.
21. L Harn. Efficient Sharing (Broadcasting) of Multiple Secrets, *IEE Proceedings-Computers and Digital Techniques*, 142(3):237–240, 1995.
22. L Harn and C Lin. Detection and Identification of Cheaters in (t, n) Secret Sharing Scheme, *Designs, Codes and Cryptography*, 52(1):15–24, 2009.
23. J He and E Dawson. Multisecret-Sharing Scheme based on One-Way Function, *Electronics Letters*, 31(2):93–95, 1995.
24. J Herranz, A Ruiz and G Sáez. New Results and Applications for Multi-Secret Sharing Schemes, *Designs, Codes and Cryptography*, pages 1–24, 2013.
25. M Ito, A Saito and T Nishizeki. Secret Sharing Scheme Realizing General Access Structure, *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.
26. W -A Jackson and K M Martin. Cumulative Arrays and Geometric Secret Sharing Schemes, In *Advances in CryptologyAUSCRYPT'92*, pages 48–55 Springer, 1993.
27. A Joux. The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems, In *Algorithmic Number Theory*, pages 20–32 Springer, 2002.
28. E Karnin, J Greene and M Hellman. On Secret Sharing Systems, *IEEE Transactions on Information Theory*, 29(1):35–41, 1983.
29. N Koblitz. Elliptic Curve Cryptosystems, *Mathematics of Computation*, 48(177):203–209, 1987.
30. N Koblitz, A Menezes and S Vanstone. The State of Elliptic Curve Cryptography, In *Towards a Quarter-Century of Public Key Cryptography*, pages 103–123 Springer, 2000.
31. S Kothari. Generalized Linear Threshold Scheme, In *Advances in Cryptology*, pages 231–241 Springer, 1985.
32. H -S Lee. A Self-Pairing Map and its Applications to Cryptography, *Applied Mathematics and Computation*, 151(3):671–678, 2004.
33. D Liu, D Huang, P Luo and Y Dai. New Schemes for Sharing Points on an Elliptic Curve, *Computers & Mathematics with Applications*, 56(6):1556–1561, 2008.
34. S Long, J Pieprzyk, H Wang and D S Wong. Generalised Cumulative Arrays in Secret Sharing, *Designs, Codes and Cryptography*, 40(2):191–209, 2006.
35. J L Massey. Minimal Codewords and Secret Sharing, In *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279, Citeseer, 1993.
36. A J Menezes, T Okamoto and S A Vanstone. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.
37. A J Menezes and S A Vanstone. Elliptic Curve Cryptosystems and their Implementation, *Journal of Cryptology*, 6(4):209–224, 1993.
38. M Mignotte. How to Share a Secret, In *Cryptography*, pages 371–375 Springer, 1983.
39. V S Miller. Use of Elliptic Curves in Cryptography, In *Proceedings of Conference on Advances in CryptologyCRYPTO85*, pages 417–426 Springer, 1986.
40. M Naor and A Shamir. Visual Cryptography, In *Advances in CryptologyEUROCRYPT'94*, pages 1–12 Springer, 1995.
41. M Naor and A Wool. Access Control and Signatures *via* Quorum Secret Sharing, *IEEE Transactions on Parallel and Distributed Systems*, 9(9):909–922, 1998.
42. L J Pang and Y M Wang. A new (t,n) Multi-Secret Sharing Scheme based on Shamirs Secret Sharing, *Applied Mathematics and Computation*, 167(2):840–848, 2005.

43. T P Pedersen. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing, In *Advances in CryptologyCRYPTO91*, pages 129–140 Springer, 1992.
44. M O Rabin. Randomized Byzantine Generals, In *24th Annual Symposium on Foundations of Computer Science, 1983*, pages 403–409, IEEE, 1983.
45. B Schoenmakers. A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting, In *Advances in Cryptology-CRYPTO99*, pages 148–164 Springer, 1999.
46. A Shamir. How to Share a Secret, *Communications of the ACM*, 22(11):612–613, 1979.
47. B Shankar, K Srinathan and C P Rangan. Alternative Protocols for Generalized Oblivious Transfer, In *Distributed Computing and Networking*, pages 304–309 Springer, 2008.
48. J Shao. Efficient Verifiable Multi-Secret Sharing Scheme based on Hash Function, *Information Sciences*, 278:104–109, 2014.
49. J Shao and Z Cao. A New Efficient (*t*,*n*) Verifiable Multi-Secret Sharing (VMSS) based on YCH Scheme, *Applied Mathematics and Computation*, 168(1):135–140, 2005.
50. R Shi, H Zhong and L Huang. A (t, n)-Threshold Verified Multi-Secret Sharing Scheme based on ECDLP, In *Proceedings of Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007 SNPD 2007*, 2:9–13, IEEE, 2007.
51. G J Simmons. An Introduction to Shared Secret and/or Shared Control Schemes and their Application, *Contemporary Cryptology: The Science of Information Integrity*, pages 441–497, 1992.
52. M Stadler. Publicly Verifiable Secret Sharing, In *Advances in CryptologyEUROCRYPT96*, pages 190–199 Springer, 1996.
53. D R Stinson and R Wei. Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures, In *Selected Areas in Cryptography*, pages 200–214 Springer, 2000.
54. C Tang, D Pei, Z Liu and Y He. Non-Interactive and Information-Theoretic Secure Publicly Verifiable Secret Sharing, *IACR Cryptology ePrint Archive*, 2004:201, 2004.
55. T Tassa. Generalized Oblivious Transfer by Secret Sharing, *Designs, Codes and Cryptography*, 58(1):11–21, 2011.
56. Y Tian, C Peng and J Ma. Publicly Verifiable Secret Sharing Schemes using Bilinear Pairings, *I J Network Security*, 14(3):142–148, 2012.
57. Y Tian, C Peng, R Zhang and Y Chen. A Practical Publicly Verifiable Secret Sharing Scheme based on Bilinear Pairing, In *2nd IEEE International Conference on Anti-counterfeiting, Security and Identification, ASID 2008*, pages 71–75, 2008.
58. M Tompa and H Woll. How to Share a Secret with Cheaters, *Journal of Cryptology*, 1(3):133–138, 1989.
59. S J Wang, Y R Tsai and C C Shen. Verifiable Threshold Scheme in Multi-Secret Sharing Distributions upon Extensions of ECC, *Wireless Personal Communications*, 56(1):173–182, 2011.
60. C Wei, L Xiang, B Yuebin and G Xiaopeng. A New Dynamic Threshold Secret Sharing Scheme from Bilinear Maps, In *IEEE International Conference on Parallel Processing Workshops*, pages 19–27, 2007.
61. T C Wu and T S Wu. Cheating Detection and Cheater Identification in Secret Sharing Schemes, In *IEEE Proceedings Computers and Digital Techniques*, 142:367–369, IET, 1995.
62. T Y Wu and Y M Tseng. A Pairing-Based Publicly Verifiable Secret Sharing Scheme, *Journal of Systems Science and Complexity*, 24(1):186–194, 2011.
63. C C Yang, T Y Chang and M S Hwang. A (t,n) Multi-Secret Sharing Scheme, *Applied Mathematics and Computation*, 151(2):483–490, 2004.
64. F ZHANG and J ZHANG. Efficient and Information-Theoretical Secure Verifiable Secret Sharing over Bilinear Groups, *Chinese Journal of Electronics*, 23(1), 2014.
65. J Zhao, J Zhang and R Zhao. A Practical Verifiable Multi-Secret Sharing Scheme, *Computer Standards and Interfaces*, 29(1):138–141, 2007.

Binu V P is currently a Research Scholar in the Department of Computer Applications, Cochin University of Science and Technology(CUSAT). He Holds a Bachelor Degree in Computer Science and Engineering and Masters Degree in Computer and Information Science His research area includes Cryptography and Secret Sharing.

A Sreekumar received his MTech Degree in Computer Science and Engineering from IIT Madras, in 1992 and Ph.D in Cryptography from Cochin University of Science and Technology, in 2010. He joined as a Lecturer in the Department of Computer Applications, CUSAT in 1994 and currently he is working as an Associate Professor. He had more than 20 years of teaching experience. His research interest includes Cryptography, Secret Sharing Schemes and Number Theory.