intelligence problem. In the protocol, ψ(r,t) is a distorted picture function and specific CAPTCHA scheme wherer € Ωn, Ω is the set of all 52 upper case and lower case characters and 10 digits, Ωn is the set of all strings of symbols in Ω of length n, and t is a random integer to generate a random distorted picture function of r such that people can recognize r from the picture but machines cannot. ψ(r,t1) and ψ(r,t2) are different to machines due to different values of t1 and t2,but to humans they are the same string.[10]

The description of the protocol is as follows:

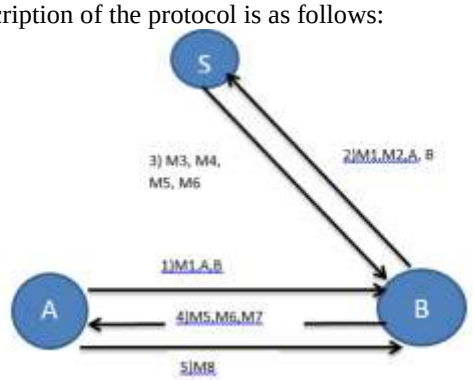

Figure 4: WH-3PAKE protocol

M1= Epwa(g^x)
M2= Epwb(g^y)
K_{AS}= g^{xs1}, K_{BS}= g^{ys2}, M3= E_{KBS}(ψ(r,t1)),
M4= E_{pwb} (g^{s2}), M5=E_{KAS} (ψ(r, t2)),
M6= E_{pwa} (g^{s1})
M7= H (1||r||B||A)
M8= H (1||r||A||B)

Value of session key is calculated as sk=H (2||r||A||B). The advantages of protocol is that it resists the continual detectable and undetectable online attacks on the clients as well as trusted serverbeing participators ,the complexities of client side computing and communication are reduced largely. So this protocol is well suited for mobile or light-weight clients. Also the perfect forward secrecy is ensured.

The authors concluded the paper by comparing the protocol with some existing schemes of three-party setting and stating that none of the schemes proposed take into account the human being's abilities different from machines which have an impact on the efficiency and security of the protocol.

4. Performance Comparison

Considering the efficiency and security of the protocols, the steps required for execution and the complexity of cryptographic operations are used to measure the performance of the proposed schemes. The higher the computation cost, the greater the time required by the two parties to establish secure communication, which is a drawback. Thus, developing a low cost 3-PAKE protocol needs to take into account the computation complexity, number of steps and security properties. Table 1,summarizes the various the protocols on the parameters such as modular exponentiations, no. of times hash function needs to be calculated, no. of XOR operations, communication steps, random numbers, encryptions and decryptions for public key and private key.

5. Conclusion

The various three party methods of key exchange allow the two clients to establish a symmetric key between them. This key can be used to encrypt and decrypt further communication between the clients.

Table 1: Performance comparison

Parameter → Protocol ↓	Modular exponentiations	Hash functions	Pseudorandom numbers	Public key en/decryption	Private key en/decryption	XOR operations	No.of steps
S-3PAKE	10	8	3	0	0	0	5
STPKE'	12	10	5	0	0	4	5
N-3PAKE	6	4	4	0	10	0	4
LHX-3-PAKE-1	8	8	3	0	0	0	4
WH-PAKE	8	6	7	0	16	0	5

Though the methods provide security and efficiency but also pose a disadvantage in case of multiple communication sessions between the same pair of clients. Every time the complex process of key generation is carried out while communication. Like during communication on SSL, abbreviated handshake with previous session resume can save resources.Since the secret key value calculated is not travelling through the network even once and remains secure with the clients (assuming personal secrecy), the efficiency of key exchange algorithm can be increased by reusing the value of the key for subsequent sessions and providing authentication during each session establishment. This would reduce the number of complex and costly calculations to be performed at the client and server side.Hence a mechanism needs to be developed which allows for the reuse of the secret key in a particular time interval yet ensuring authenticity of the clients.

References

[1] Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval, "Password-Based Authenticated Key Exchange in the Three-Party Setting", IEEE Proceedings on InformationSecurity, Volume 153, number 1, March 2006 , pp. 27-39.
[2] Whitefield Diffie, Martin E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, pp. 644-654,1976.

[3] Behrouz A. Forouzan, Cryptography and network security, Tata McGraw-Hill, 2007.
[4] Hyun-SeokKim ,Jin-Young Choi, "Enhanced password-based simple three-party key exchange protocol", Elsevier, Computers and Electrical Engineering, 35, pp.107–114,2009.
[5] Yuanhui Lin, MengboHou, Qiuliang Xu, "Strongly password based three party authenticated key exchange protocol", Ninth International conference on Computational Intelligence and security, IEEE, pp. 555-558,2013.
[6] Rongxing Lu, Zhenfu Cao, "Simple three-party key exchange protocol", Elsevier, computers & security 26, pp. 94-97,2007.
[7] Chao Lv , MaodeMab, Hui Li, JianfengMaa, Yaoyu Zhang, "An novel three-party authenticated key exchange protocol using one-time key", Elsevier, Journal of Network and Computer Applications (36), pp. 498–503,2013.
[8] Alfred Menezes, BerkantUstaoglu, "On reusing ephemeral keys in Diffie Hellman key agreement protocol",International Journal of Applied Cryptography,ACM,pp. 154-158, 2010.
[9] Tang, Wen, "A simple three party password based key exchange protocol", International Conference on Mechanical and Electrical Technology, IEEE, pp. 730-732, 2010.
[10] Wejia Wang, Lei Hu, "Three party password-based authenticated key establishment protocol resisting detectable online attack", Advances in information sciences and service sciences (AISS), pp. 680-687, 2013.
[11] Shuhua Wu, Kefei Chen, and Yuefei Zhu, "Enhancements of a Three-Party Password-Based Authenticated Key Exchange Protocol", The International Arab Journal of Information Technology, Vol. 10, No. 3, pp. 215-221,2013.

Author Profile

Ms. RekhaSaraswatreceived her MCA degree from Uttar Pradesh Technical University in 2004. She joined CDAC Noida in 2006 and then completed her MS degree from BITS,Pilani in 2010. She currently works as an Assistant Professor in CDAC, Noida. Her research interests include network security, information security and image processing.

Shivani Bhatia completed her B.Tech in Electronics & Communication from Maharishi Dayanand University, Rohtak in 2013. She is currently pursuing M. Tech in Information Technology from CDAC Noida. Her research interests include cryptography and network security.