CSP

Instance
(x,y)∈S×S such that *y=axa*$^{-1}$ for some *α∈s.*

Objective
The objective is to find *b∈S* such that y=*bxb*$^{-1}$.

KEY AGREEMENT PROTOCOL BASED ON CSP

The CSP

The CSP is to find *X∈T* satisfying $\phi \rightarrow X\phi X^{-1}$ for some *X∈T* CSP asks to locate at least one exacting element *X∈T* It is measured infeasible to solve CSP and is to be hard. The random conjugate of ϕ fto be equal to *X* is insignificant. Hence, the probability is negligible.

Let T be the division semiring of inner automorphism.

Let *X∈T*;
$\phi \in$ T be A's long-term private key.
$X_A = \phi x \phi^{-1}$ is A's long-term public key.
X∈T be B's long-term private key.
X_B = XxX^{-1} B's long- term public key.

Key exchange

S1. A chooses $\tau \in T$ and computes
$Y_A = \tau x \tau^{-1}$.
If Y_A = I (identity), the protocol terminates, otherwise A sends Y_A to B.
S2. After receiving Y_A, B chooses $\in$T and computes $K_B = \chi \ X_A \chi^{-1}$ and $Y_B = K_B \omega \ Y_A \omega^{-1} \ K_B^{-1}$
S3. If Y_B or K_B = I, then the protocol terminates, else B sends Y_B to A.
S4. After receiving Y_B, A computes.
$K_A = \phi X_B \phi^{-1}$.
The shared key for A is $KEY_A = \tau K_A^{-1} Y_A K_A \tau^{-1}$.
S5. B computes the shared key $KEY_B = \omega Y_A \omega^{-1}$.
S6. If KEY_A or KEY_B is I, then termination of protocol run occurs.
S7. A and B share the secret key after a regular protocol running.
$K = KEY_A = KEY_B$.

SECURITY CONSIDERATION

As by our assumption that the CSP is hard, our protocol meets the following desirable attributes.

Security of known-key

It is clearly known that A and B share their unique session key K if they follow the Key exchange protocol as proposed above.

Forward secrecy

For each entity, the random elements τ and ω act on the session key K during the computation. For an intruder who knows the private keys of A or B, i.e., ϕ or *X* could extract K_A or K_B from Y_A and Y_B to know the previous or next session keys. He has to compute XX_AX^{-1} which is impossible as the CSP is well secured, and hence, our key exchange protocol has the forward secrecy.

Key-compromise impersonation

If an adversary E wants to impersonate A by knowing *A*'s long-term private key ϕ, it is not possible for him to impersonate B to A without knowing B's long-term private key *X*. To impersonate successfully, E should know the ephemeral key τ of *A* for this he should extract *τ* from *A*'s ephemeral public value $Y_A = \tau x \tau^{-1}$ which is not possible as the CSP is hard.

Unknown key-share

An adversary E should try to make A believing that the session key is shared with B, where B believes that the session key shared with E. For this, he sets his public key to be certified using the public keys of A and B, i.e., X_A, X_B, and *x*. However, after simple calculation, we come to know that the unknown key-share attack fails.

Key control

The key control can be possible only by the key agreeing parties and no third party can have a key control. Hence, the key control attack may happen only by the key exchanging party of the protocol B. For this, B should solve the following $K = \omega Y_A \omega^{-1}$. Again, it is impossible because of the hardness of CSP.

CONCLUSIONS

In this article, we proposed a new key exchange protocol using division semiring generated by inner automorphism. For the security consideration of the protocol, we rely on the CSP in a division semiring generated by inner automorphism. Our protocol makes use of the fact that the CSP is hard in the described structure. We prove that our key exchange protocol is secure against many well-known attacks.

REFERENCES

1. Clay R. Nearrings: Genesis and Applications. New York: Oxford Science Publication; 1992.
2. Climent JJ, Navarro PR, Tortosa L. Key exchange protocols over noncommutative rings. The case of. Int J Comput Math 2012;89:1753-63.
3. Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory 1976;22:644-54.
4. Frohlich A. The near-ring generated by the inner automorphisms of a finite simple group. J Lond Math Soc 1958;1:95-107.
5. Gu L, Zheng S. Conjugacy systems based on nonabelian factorization problems and their applications in cryptography. J Appl Math 2014;2014:630607.
6. Grigoriev D, Shpilrain V. Authentication from matrix conjugation. arXiv preprint arXiv: 1010.5034; 2012.
7. Kamal AA, Youssef AM. Cryptanalysis of a key exchange protocol based on the endomorphisms ring End(Zp*Zp2). Appl Algebra Eng Commun Comput 2012;23:143-9.
8. Koetal KH, Lee SJ, Cheon JH, Han JW, Kang JS, Park C. New public-key cryptosystem using braid groups. In: Annual International Cryptology Conference. Berlin Heidelberg: Springer; 2000. p. 166-83.
9. Moldovyan DN, Moldovyan NA. A new hard problem over non-commutative finite groups for cryptographic protocols. In: International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Berlin Heidelberg: Springer; 2010. p. 183-94.
10. Paeng SH, Ha KC, Kim JH, Chee S, Park C. New public key cryptosystem using finite non Abelian groups. In: Annual International Cryptology Conference. Berlin Heidelberg: Springer; 2012. p. 470-85.
11. Pilz G. Near-rings North Holland. Amsterdam: American Elsevier; 1983.
12. Paeng SH. On the security of cryptosystem using automorphism groups. Inf Proces Lett 2003;88:293-8.
13. Lal S, Awasthi AK. Proxy blind signature scheme. J Inf Sci Eng Cryptol ePrint Archive Report 2003;72:???.

Author Queries???
AQ1:Kindly review the sentence.
AQ2:Kindly review the sentence.
AQ3:Kindly cite References 1, 2, 4, 5, 7, 9-11, 13 in the text part and also cite in chronological order
AQ4:Kindly provide page number