INNOVARE JOURNAL OF ENGINEERING & TECHNOLOGY

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Vol 6, Issue 1, 2018

ISSN - 2347-1573

Review Article

A KEY EXCHANGE PROTOCOL USING CONJUGACY PROBLEM IN THE DIVISION SEMIRINGS

VIJAYARAGAVAN R*

Department of Mathematics, Thiruvalluvar University, Vellore, Tamil Nadu, India. Email: rvijayaraagavantvu@gmail.com

Received: 12 January 2018, Revised and Accepted: 14 April 2018

ABSTRACT

In this article, we present a new key exchange protocol which works in the division semiring. We prove that the protocol meets the security of key establishment based on the conjugacy search problem and security attribute also discussed.

Keywords: Key exchange protocol, Conjugacy decision problem, Non-commutative division semirings, Conjugacy.

INTRODUCTION

Since Diffie and Hellman first presented a public-key cryptosystem (PKC) in using a trapdoor one-way function, and many PKCs have been proposed and broken. Most of successful PKCs require large prime numbers. The difficulty of factorization of integers with large prime factors forms the ground of RSA and its variants such as Rabin- Williams, LUC's scheme, or elliptic curve versions of RSA like KMOV. Furthermore, the difficulty of the discrete logarithm problem forms the ground of Diffie–Hellman type schemes such as ElGamal, elliptic curve cryptosystem, DSS, and McCurley. There have been several efforts to develop alternative PKCs that are not based on number theory. The first attempt was to use NP-hard problems in combinatorics like Merkle–Hellman Knapsack and its modifications. Though many cryptographers have been pessimistic about combinatorial cryptography after the breakdown of the Knapsack-type PKCs by Shamir *et a*l., and after the appearance of Brassard theorem, there may still be some hopes as Koblitz has noted in. The other systems that are worth to mention are the quantum cryptography proposed by Bennet and Brassard, and the lattice cryptography proposed by Goldreich and Halevi. Another approach is to use hard problems in combinatorial group theory such as the word problem or using the Lyndon words. Recently, Anshel-Anshel-Goldfeld proposed a key agreement system and a PKC using groups where the word problem is easy but the conjugacy problem is intractable. Moreover, they noted that the usage of braid groups is particularly promising. Our proposed systems are based on the braid groups but are independent from their algebraic key establishment protocol on monoids in. Most of cryptosystems derived from combinatorial group theory are mainly theoretical or have certain limitations in wide and general practice. This is perhaps due to the lack of efficient description of group elements and operations or due to the difficulty of implementing cryptosystems themselves.

A protocol which allows for a key exchange between two parties using a secret key to use in their succeeding private communication is known to be a key exchange protocol. Diffie and Hellman introduced the first key exchange protocol in 1976 [3]. Many key exchange protocols were developed using discrete logarithm problem. The development in quantum computing made easy to solve the discrete logarithm problem. Hence, the mathematicians search for new key exchange relying on hard problem. The new key exchange protocols work over non-commutative cryptography. A public-key cryptosystem was built using finite non-abelian groups. The system works under the conjugate action defined on the discrete logarithm problem in the inner automorphism groups. This public key cryptosystem was proposed [12]. Diffie and Hellman key agreement using Braid group was proposed by Koetal, in 2001 [8]. Cryptography based on braid group uses conjugacy search problem (CSP). Anshel *et al.*'s key exchange also uses CSP for the secured protocol. Grigoriev and Shpilrain proposed on authentication scheme using CSP in non-commutative semigroup in 2010 [6].

In this paper, we introduce a key exchange scheme over non-commutative division semirings. The base for our construction is CSP in non-commutative division semirings. Conjugacy decision problem (CDP) is easy to compute and CSP is computationally hard. In this article, we propose a first key exchange scheme over non-commutative division semirings. This demonstrates the usefulness of division semirings in cryptography as implementation over a computer system.

PRELIMINARIES

Definition 1

A semiring *R* is a non-empty set, on which operations of addition and multiplication have been defined as follows:

i. *(R,+)* is a commutative monoid with identity element
ii. *(R,+•)* is a monoid with identity element
iii. Multiplication distributes over addition from either side
iv. $0•r=r•0$ for all in R.

Definition 2

An element r of a semiring *R* is a "unit" if and only if there exists an element r^1 of *R* satisfying $r•r^1=r^1•r=1$. The element r^1 is called the inverse of *r* in ***R***. If such an inverse r^1 exists for a unit *r*, it must be unique. We will normally denote the inverse of *r* by r^{-1}. It is straightforward to see that, if *r* and r^1 units of R, then $r•r^{-1}=r^{-1}•r$ and in particular $(r^{-1})^{-1}=r$. We will denote the set of all units of *R*, by *U(R).* This set is non-empty, since it contains "1," and is not all of R, since it does not contain "0". We have just noted that *U(R)* is a submonoid of *(R,•)*, which is in fact a group. If *U(R)=R/{0}*, then R is a division semiring.

Further cryptographic assumptions on non-commutative division semirings

We consider some mathematically hard problem in division semirings. We say that *x* and *y* are conjugate if there is an element *α* such that $y=\alpha x\alpha^{-1}$.

CDP

Instance
$(x,y)\in S\times S$ such that $y=axa^{-1}$ for some $\alpha\in s$.

Objective
The objective is to determine whether x and y are conjugate or not.

CSP

Instance

(x,y)$\in S\times S$ such that $y=axa^{-1}$ for some $\alpha\in s$.

Objective

The objective is to find $b\in S$ such that $y=bxb^{-1}$.

KEY AGREEMENT PROTOCOL BASED ON CSP

The CSP

The CSP is to find $X\in T$ satisfying $\phi\rightarrow X\phi X^{-1}$ for some $X\in T$ CSP asks to locate at least one exacting element $X\in T$ 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 $X\in T$;

$\phi\in$ T be A's long-term private key.

$X_A = \phi x\phi^{-1}$ is A's long-term public key.

$X\in T$ 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 $KEY_A = \tau K_A^{-1}Y_AK_A\tau^{-1}$.

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:.