КОПРЕДСТАВЛЕНИЯ ГРУПП В КРИПТОГРАФИИ

М.А. Пудовкина

Московский инженерно-физический институт (государственный университет),
Каширское шоссе 31, г. Москва, Россия
maricap@rambler.ru

Теория групп активно используется в криптографии при синтезе и анализе криптосистем. При этом применятся, например, такие ее разделы, как теория групп подстановок, копредставления групп и др. На русском языке имеется ряд обзорных работ, посвященных этому направлению. Так в обзорной работе М.М. Глухова и А.Ю. Зубова [1] (библиография — 128 работ) рассмотрены образующие элементы групп S_n, A_n, представление элементов групп S_n, A_n через образующие, длины групп в заданной системе образующих. Также указана связь этих вопросов с криптографией. В обзоре М.М. Глухова и Б.А. Погорелова [2] по группам и криптографии рассматривались следующие вопросы: построение систем образующих симметрических и знакопеременных групп подстановок; параметры, связанные с заданием конечных групп системами образующих элементов; использование регулярных групп для построения множеств подстановок с заданными свойствами; распределение вероятностей на конечных группах; групп ы и полугруппы изометрий; групповая классификация функций; решение уравнений в группах (библиография — 44 работы). Однако, на русском языке имеется только одна обзорная работа общего характера А.Е. Жукова [3], посвященная вопросам синтеза криптосистем с использованием копредставлений групп (библиография — 4 работы).

Среди зарубежных авторов следует отметить обзоры [4, 5], посвященные группам кос и их применению в криптографии (библиография — 137 и 59 работ, соответственно) и работу [6].

В данной работе обзорного характера рассмотрена связь копредставлений групп с криптографией. Безопасность многих криптосистем основана на таких проблемах, как проблема равенства слов, проблема сопряжения и поиска сопрягающего элемента, проблема принадлежности подгруппе и факторизации, проблема извлечения корня и др. Так в работе [7] предложен новый криптографический протокол, основанный на проблеме равенства слов. В протоколе используются группы с малым сокращением (см., например, [8]). В работе [9] описана шифрсистема с открытым ключом, основанная на проблеме равенства слов в свободном частично коммутативном моноиде, и ее аналог для свободной частично коммутативной группы. Там же предложен протокол аутентификации с нулевым разглашением, также основанный на равенства слов в свободном частично коммутативном моноиде. В работах [10, 11] рассмотрены атаки на эти криптосистемы. Целый ряд работ [12–30] и др. посвящен синтезу криптосистем на базе различных свойств групп кос и затем их анализу.

Кроме групп кос используются, например, группа Томпсона [31], Кокстера [32], представление групп Григорчука [33].

Литература

1. *Глухов М. М., Зубов А. Ю.* О длинах симметрических и знакопеременных групп подстановок в различных системах образующих (обзор) // Математические вопросы кибернетики, 1999.

2. *Глухов М.М., Погорелов Б.А.* О некоторых применениях групп в криптографии // Математика и безопасность информационных технологий. М.: МЦНМО, 2005. С. 19–31.

3. *Жуков А.Е.* Криптография с открытым ключом и нечисловые алгебраические системы // http:// www.iu8.bmstu.ru

4. *Birman J.S., Brendle T. E.* Braids: A survey // arXiv:math.GT/0409205, 2005.

5. *Dehornoy P.* Braid-based cryptography. Group Theory, Statistics, and Cryptography // Contemporary Mathematics, 2004, v.360, p.5-33.

6. *Myasnikov A., Shpilrain V., Ushakov A.* Group-based cryptography // www.cs.stevens.eduãmiasnik.

7. *Shpilrain V., Zapata G.* Using decision problems in public key cryptography // ArXiv.org/math.GR/ 0703656, 2007.

8. *Линдон Р., Шупп П.* Линдон Р., Шупп П. Комбинаторная теория групп. М: Мир, 1980.

9. *Abisha P.J., Thomas D.G., Subramanian K.G.* Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups // INDOCRYPT'2003, LNCS, 2003, v.2904, p.218-227.

10. *Levy-dit-Vehel F.,Perret L.* Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups // INDOCRYPT'2003, LNCS. 2003, v.2904, p.218-227.

11. *Gonzalez-Vasco M.I., Steinwandt R.*Pitfalls in public key systems based on free partially commutative monoids an groups // http://eprint.iacr.org/2004/012.

12. *Anshel I., Anshel M., Goldfeld D.* An algebraic method for public-key cryptography // Math. Res. Lett. 1999. V. 6. P. 287–291.

13. *Hughes J., Tannenbaum A.* Length-based attacks for certain group based encryption rewriting systems// Institute for Mathematics and Its Applications, April, 2000, Minneapolis, MN, Preprint, N1696, http://www.ima. umn.edu/preprints/apr2000/1696.pdf

14. *Anshel I., Anshel M., Fisher B., Goldfeld D.* New Key Agreement Protocols in Braid Group Cryptography// Topics in Cryptology — CT-RSA 2001, LNCS, 2001. V. 2020. P. 13–27.

15. *Lee S.J., Lee E.* Potential Weaknesses of the Commutator Key Agreement Protocol based on Braid Groups // EUROCRYPT'2002, LNCS, 2002. V. 2332. P. 14–28.

16. *Hughes J.* A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem. Information Security and Privacy // 7th Australasian Conference, ACISP'2002, LNCS, 2002. V. 2384. P. 176–189.

17. *Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J., Park C.* New public-key cryptosystem using braid groups // CRYPTO'2000, LNCS, 2000. V. 1880. P. 166–183.

18. *Cha J.C., Ko K.H., Lee S. J., Han J.W., Cheon J.H.* An Efficient Implementation of Braid Groups// ASIACRYPT'2001, LNCS, 2001. V. 2248. P. 144–156.

19. *Lee E., Lee S.J., Hahn S.G.* Pseudorandomness from Braid Groups // CRYPTO'2001, LNCS, 2001. V. 2139. P. 486–502.

20. *Gennaro R., Micciancio D.* Cryptanalysis of a Pseudorandom Generator Based on Braid Groups // EUROCRYPT 2002, LNCS, 2002. V. 2332. P. 1–13.

21. *Hofheinz D., Steinwandt R.* A Practical Attack on Some Braid Group Based Cryptographic Primitives // PKC'2003, LNCS, 2003. V. 2567. P. 187–198.

22. *Cheon J.H., Jun B.* Diffie — Hellman Conjugacy Problem on Braids // preprint, 2003.

23. *Cheon J.H., Ju B.* A Polynomial time algorithm for the Diffie — Hellman Conjugacy problem // CRYPTO'2003, LNCS, 2003. V. 2729. P. 212–225.

24. *Lee E., Park J. H.* Cryptanalysis of the Public-Key Encryption Based on Braid Groups // EUROCRYPT'2003, LNCS, 2003. V. 2656. P. 477–490.

25. *Lal S., Chaturvedi A.* Authentication schemes using braid groups // http://arXiv.org/cs.CR/0507066.

26. *Tsaban.B.* On an authentication scheme based on the Root Problem in the braid group // http://eprint. iacr.org/ 2005/264.

27. *Groch A., Hofheinz D., Steinwandt R.* A Practical Attack on the Root Problem in Braid Groups // http://eprint.iacr.org/2005/459.

28. *Myasnikov A., Shpilrain V., Ushakov A.* A Practical Attack on a Braid Group Based Cryptographic Protocol// CRYPTO'2005, LNCS. 2005. V. 3621. P. 86–96.

29. *Myasnikov A., Shpilrain V., Ushakov A.* Random Subgroups of Braid Groups: An Approach to Cryptanalysis of a Braid Group Based Cryptographic Protocol // PKC'2006, LNCS, 2006. V. 3958. P. 302–314.

30. *Myasnikov A.D., Ushakov A.* Based Attack and Braid Groups: Cryptanalysis of Anshel — Anshel — Goldfeld Key Exchange Protocol // PKC'2007, LNCS, 2007. V. 4450. P. 76–88.

31. *Shpilrain V., Ushakov A.* Thompson's group and public key cryptography // LNCS, 2005. V. 3531. P. 151–164.

32. *Безверхний В.Н., Добрынина И.В.* Решение проблемы обобщенной сопряженности слов в группах Кокстера большого типа // Дискрет. матем. 2005. Т. 17, № 3. С. 123–124.

33. *Gonzales V.M.I., Hofheinz D., Martinez C., Steinwandt R.* On the security of two public key cryptosystems using non-Abelian groups // 3-th Pythagorean Conference, Faliraki, 2003, Des., Codes and Cryptogr. 2004. V. 32, N 1–3. P. 207–216.