Advertisement Hide
Soft Computing
IF:3.05 h-index:64 欢迎中国学者投稿!
点击了解更多
Springer
springer.com

International Conference on Information Security Practice and Experience
ISPEC 2017: Information Security Practice and Experience pp 156-167 | Cite as

A Secure Variant of the SRP Encryption Scheme with Shorter Private Key

Authors Authors and affiliations

Bo Lv, Zhiniang Peng, Shaohua Tang

Conference paper
First Online: 08 December 2017

2.1k
Downloads

Part of the Lecture Notes in Computer Science book series (LNCS, volume 10701)

Abstract

The study of multivariate encryption algorithm is an important topic of multivariate public key cryptography research. However, quite few secure and practical multivariate encryption algorithms have been found up to now. The SRP encryption scheme is a multivariate encryption scheme that combines Square, Rainbow and the Plus method technique, which is of high efficiency and resistant to existing known attacks against multivariate schemes. In this paper, an improved SRP scheme with shorter private key and higher decryption efficiency is proposed. We introduce rotation relations into parts of the private key, which enables us to reduce the private key size by about 61%. And the decryption speed is 2.1 times faster than that of the original SRP. In terms of theory and experiment, we analyze the security of the improved SRP for several attacks against SRP. The results show that our modifications do not weaken the security of the original schemes.

Keywords

Multivariate public key algorithm | SRP encryption | Quantum-safe public key cryptography | Shorter private key

This is a preview of subscription content, log in to check access.

Notes

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Nos. 61632013, U1135004 and 61170080), 973 Program (No. 2014CB360501), Guangdong Provincial Natural Science Foundation (No. 2014A030308006), and Guangdong Provincial Project of Science and Technology (no. 2016B090920081).

References

1. Billet, O., Gilbert, H.: Cryptanalysis of rainbow. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 336–347. Springer, Heidelberg (2006). https://doi.org/10.1007/11832072_23
CrossRef Google Scholar

2. Ding, J., Gower, J.E.: Inoculating multivariate schemes against differential attacks. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 290–301. Springer, Heidelberg (2006). https://doi.org/10.1007/11745853_19
CrossRef Google Scholar

3. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 164–175. Springer, Heidelberg (2005). https://doi.org/10.1007/11496137_12
CrossRef Google Scholar

4. Duong, D.H., Petzoldt, A., Takagi, T.: Reducing the key size of the SRP encryption scheme. In: Liu, J.K., Steinfeld, R. (eds.) ACISP 2016. LNCS, vol. 9723, pp. 427–434. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-40367-0_27
CrossRef Google Scholar

5. Eder, C., Faugére, J.C.: A survey on signature-based algorithms for computing Gröbner bases. J. Symb. Comput. **80**, 719–784 (2017)
CrossRef Google Scholar

6. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra **139**(1), 61–88 (1999)
MathSciNet CrossRef zbMATH Google Scholar

7. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: ACM ISSAC 2002, pp. 75–83 (2002)
Google Scholar

Log in to check access
Buy eBook
EUR 96.29
Buy paper (PDF)
EUR 24.95
- Instant download
- Readable on all devices
- Own it forever
- Local sales tax included if applicable

Buy Physical Book
Learn about institutional subscriptions
Cite paper

Advertisement
springer.com
Soft Computing
IF:3.05 h-index:64
欢迎中国学者投稿!
点击了解更多
Springer
Hide

8. Faugère, J.C., Din, M.S.E., Spaenlehauer, P.J.: On the complexity of the generalized MinRank problem. J. Symb. Comput. **55**, 30–58 (2013)
MathSciNet CrossRef zbMATH Google Scholar

9. Faugère, J.-C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 280–296. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_16
CrossRef Google Scholar

10. Fouque, P.-A., Granboulan, L., Stern, J.: Differential cryptanalysis for multivariate schemes. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 341–353. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_20
CrossRef Google Scholar

11. Gover, M.J.C., Barnett, S.: Inversion of certain extensions of Toeplitz matrices. J. Math. Anal. Appl. **100**(2), 339–353 (1984)
MathSciNet CrossRef zbMATH Google Scholar

12. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_15
Google Scholar

13. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Barstow, D., et al. (eds.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988). https://doi.org/10.1007/3-540-45961-8_39
Google Scholar

14. Ng, M.K., Rost, K., Wen, Y.W.: On inversion of Toeplitz matrices. Linear Algebra Appl. **348**(1), 145–151 (2002)
MathSciNet CrossRef zbMATH Google Scholar

15. Patarin, J.: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 248–261. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-44750-4_20
Google Scholar

16. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_4
Google Scholar

17. Patarin, J., Courtois, N., Goubin, L.: QUARTZ, 128-bit long digital signatures. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 282–297. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45353-9_21
CrossRef Google Scholar

18. Petzoldt, A., Chen, M.-S., Yang, B.-Y., Tao, C., Ding, J.: Design principles for HFEv- based multivariate signature schemes. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 311–334. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_14
CrossRef Google Scholar

19. Porras, J., Baena, J., Ding, J.: ZHFE, a new multivariate public key encryption scheme. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 229–245. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11659-4_14
Google Scholar

20. Shen, W., Tang, S.: RGB, a mixed multivariate signature scheme. Comput. J. **59**(4), 439–451 (2015)
CrossRef Google Scholar

21. Smith-Tone, D.: On the differential security of multivariate public key cryptosystems. In: Yang, B.-Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 130–142. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25405-5_9
CrossRef Google Scholar

22. Tao, C., Diene, A., Tang, S., Ding, J.: Simple matrix scheme for encryption. In: Gaborit, P. (ed.) PQCrypto 2013. LNCS, vol. 7932, pp. 231–242. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38616-9_16
CrossRef Google Scholar

23. Thomae, E., Wolf, C.: Roots of square: cryptanalysis of double-layer square and square+. In: Yang, B.-Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 83–97. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25405-5_6
CrossRef Google Scholar

24. Wolf, C., An, B., Preneel, B.: On the security of stepwise triangular systems. Des. Codes Crypt. **40**(3), 285–302 (2006)
MathSciNet CrossRef zbMATH Google Scholar

25. Yang, B.-Y., Chen, J.-M.: Building secure Tame-like multivariate public-key cryptosystems: the new TTS. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 518–531. Springer, Heidelberg (2005). https://doi.org/10.1007/11506157_43
CrossRef Google Scholar

26. Yasuda, T., Sakurai, K.: A multivariate encryption scheme with rainbow. In: Qing, S., Okamoto, E., Kim, K., Liu, D. (eds.) ICICS 2015. LNCS, vol. 9543, pp. 236–251. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29814-6_19
CrossRef Google Scholar

27. Zohar, S.: Toeplitz matrix inversion: the algoritm of W. F. Trench. J. ACM **16**(4), 592–601 (1969)
MathSciNet CrossRef zbMATH Google Scholar

Copyright information

© Springer International Publishing AG 2017

About this paper

Check for updates

Cite this paper as:
Lv B., Peng Z., Tang S. (2017) A Secure Variant of the SRP Encryption Scheme with Shorter Private Key. In: Liu J., Samarati P. (eds) Information Security Practice and Experience. ISPEC 2017. Lecture Notes in Computer Science, vol 10701. Springer, Cham. https://doi.org/10.1007/978-3-319-72359-4_9

First Online
08 December 2017

DOI
https://doi.org/10.1007/978-3-319-72359-4_9

Publisher Name
Springer, Cham

Print ISBN
978-3-319-72358-7

Online ISBN
978-3-319-72359-4

eBook Packages
Computer Science
Computer Science (R0)

Buy this book on publisher's site

Reprints and Permissions

Over 10 million scientific documents at your fingertips

Academic Edition

Home | Impressum | Legal information | Privacy statement | California privacy statement | How we use cookies | Manage cookies/Do not sell my data | Accessibility | Contact us

SPRINGER NATURE

© 2020 Springer Nature Switzerland AG. Part of Springer Nature.
Not logged in · Not affiliated · 193.110.203.90