Veröffentlichungen

Christopher Wolf

Journale *(Peer-Reviewed)*

1. C. Wolf, B. Preneel, “Equivalent keys in Multivariate Quadratic public key systems”, Journal of Mathematical Cryptology, 4(4), pp. 375-415, 2011.
2. C. Wolf, A. Braeken, B. Preneel, “On the Security of Stepwise Triangular Systems”, Designs, Codes and Cryptography 40(3), pp. 285-302, 2006.
3. P. Fitzpatrick and C. Wolf, “Direct division in factor rings”, In Electronic Letters, Vol. 38, No. 21, p. 1253-1254, October 10, 2002.

Herausgeber *(international)*

1. S. Lucks, A.-R. Sadeghi, C. Wolf (Eds.), “WEWoRC 2007 - Western Europen Workshop on Research in Cryptology”, In the Lecture Notes in Computer Science LNCS 4945, Springer, 2008.
2. C.Wolf, St. Lucks, P.-W. Yau (Eds.), “WEWoRC 2005 - Western Europen Workshop on Research in Cryptology”, In the Lecture Notes in Informatics LNI P-74, Gesellschaft für Informatik, 2005.

Internationale Konferenzen & Workshops (*Peer-Reviewed*)

1. F.Quedenfeld, C.Wolf: “Advanced Algebraic Attack on Trivium”, Sixth International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) 2015, 17 pages, *accepted*.
2. S.Uellenbeck, T.Hupperich, C.Wolf, T.Holz: “Tactile One-Time Pad: Leakage-Resilient Authentication for Smartphones.” Financial Cryptography and Data Security (FC) 2015, LNCS 8975, Springer Verlag, pp. 237-253.
3. S.Uellenbeck, M.Dürmuth, C.Wolf, T.Holz: “Quantifying the security of graphical passwords: the case of android unlock patterns.” ACM Conference on Computer and Communications Security (CCS) 2013, pp. 161-172.
4. E. Struse, J.Seifert, S.Uellenbeck, E.Rukzio, C.Wolf: “Permission Watcher: Creating User Awareness of Application Permissions in Mobile Systems.” In International Joint Conference on Ambient Intelligence (AmI), Lecture Notes in Computer Science LNCS 7683, Springer Verlag, pp. 65-80, 2012.

5. E.Thomae, C.Wolf, “Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited.” In Public Key Cryptography PKC 2012, Lecture Notes in Computer Science LNCS 7293 Springer Verlag, pp. 156-171, 2012.
6. E.Thomae, C.Wolf, “Cryptanalysis of Enhanced TTS, STS and All Its Variants, or: Why Cross-Terms Are Important.” AFRICACRYPT 2012, Lecture Notes in Computer Science LNCS 7374, Springer Verlag, pp. 188-202, 2012.
7. M.Becher, F.C.Freiling, J.Hoffmann, T.Holz, S.Uellenbeck, C.Wolf, “Mobile Security Catching Up? - Revealing the nuts and bolts of the security of mobile devices”, In IEEE Computer Society 2011 Security and Privacy Symposium, pp. 96-111, 2011
8. A.Petzoldt, E.Thomae, S.Bulygin, C.Wolf, “Small Public Keys and Fast Verification for ***M***ultivariate ***Q***uadratic Public Key Systems.” In Proceedings of Cryptographic Hardware and Embedded Systems – CHES 2011, Lecture Notes in Computer Science LNCS 6917, Springer Verlag, pp. 475-490, 2011.
9. E.Thomae, C.Wolf, “Theoretical Analysis and Run Time Complexity of MutantXL”, in CMMSE 2011 – International Conference Computational and Mathematical Methods in Science and Engineering*, pp. 1123-1135, 2011.*
10. E.Thomae, C.Wolf, “Roots of Square: Cryptanalysis of Double-Layer Square and Square+.” Post Quantum Cryptography – PQCrypto 2011, Lecture Notes in Computer Science LNCS 7071, Springer Verlag, pp. 83-97, 2011.
11. A.Bogdanov, Th.Eisenbarth, A.Rupp, C.Wolf, “Time-Area Optimized Public-Key Engines-Cryptosystems as Replacement for Elliptic Curves?”, In Proceedings of Cryptographic Hardware and Embedded Systems – CHES 2008, Lecture Notes in Computer Science LNCS 5154, Springer-Verlag, pp. 45-61, 2008
12. J.Ding, C.Wolf, B.-Y. Yang, "*l*-invertible cycles for multivariate quadratic public key cryptography", In Proceedings of Public Key Cryptography 2007, Lecture Notes in Computer Science LNCS 4450, Springer-Verlag, pp. 266-281, 2007.
13. C. Wolf, “Introduction to Multivariate Quadratic Public Key Systems and their Applications”, In Proceedings of YACC 2006 – Yet Another Conference on Cryptography, Porquerolles, France, pp. 44-55.
14. C.Wolf, B.Preneel, “Equivalent keys in multivariate quadratic public key systems",In Proceedings of PQCrypto 2006: International Workshop on Post-Quantum Cryptography, Leuven, Belgium, pp. 195-214.
15. J.Ding, J. E.Gower, D.Schmidt, C.Wolf, and Z.Yin, "Complexity Estimates for the F_4 Attack on the Perturbed Matsumoto-Imai Cryptosystem," In Proceedings of 10th IMA Internation Conference on Cryptography and Coding, Lecture Notes in Computer Science LNCS 3796, Springer-Verlag, pp. 262-277, 2005.
16. A.Braeken, B.Preneel, C.Wolf, "Normality of Vectorial Boolean Functions," In Proceedings of 10th IMA Internation Conference on Cryptography and Coding, Lecture Notes in Computer Science LNCS 3796, Springer-Verlag, pp. 186-200, 2005.

17. C.Wolf, and B.Preneel, “Equivalent Keys in HFE, C*, and variations," International Conference on Cryptology in Malaysia 2005, Lecture Notes in Computer Science LNCS 3715, S. Vaudenay (ed.), Springer-Verlag, pp. 33-49, 2005.
18. K.Kursawe, and C.Wolf, "Trusted Computing or The Gatekeeper," In Proceedings of Landscapes of ICT and Social Accountability, P. Duquenoy, K. Kimppa, and C. Zielinski (eds.), pp. 339-354, 2005.
19. A.Braeken, C.Wolf, and B. Preneel, "A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes", In Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science LNCS 3376, A. Menezes (ed.), Springer-Verlag, pp. 29-43, 2005.
20. C.Wolf, and B.Preneel, "Superfluous Keys in Multivariate Quadratic Asymmetric Systems", In Public Key Cryptography, 8th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2005, Lecture Notes in Computer Science 3386, S. Vaudenay (ed.), Springer-Verlag, pp. 275-287, 2005.
21. A.Braeken, C. Wolf, and B. Preneel, "Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC", In Security in Communication Networks, 4th International Conference, SCN 2004, Lecture Notes in Computer Science 3352, C. Blundo, and S. Cimato (eds.), Springer-Verlag, pp. 294-307, 2005.
22. A.Braeken, C. Wolf, and B. Preneel, “A Randomised Algorithm for Checking the Normality of Cryptographic Boolean Functions", In 3rd International Conference on Theoretical Computer Science 2004, J. Levy, E. W. Mayr, and J. C. Mitchell (eds.), Kluwer, pp. 51-66, 2004.
23. C.Wolf, “Efficient Public Key Generation for HFE and Variations", In Cryptographic Algorithms and their Uses - 2004, E. Dawson, and W. Klemm (eds.), QUT Publications, pp. 78-93, 2004.
24. C.Wolf, “Deriving Public Polynomials Efficiently for HFE-like Systems", In 2nd Yet Another Conference on Cryptography (YACC), 1 Seiten, 2004.
25. C.Wolf, “Implementing Quartz in Java”, 3rd New European Schemes for Signatures, Integrity, and Encryption Workshop, Munich, Germany, November 6 - 7, 2002, 12 pages.

Herausgeber *(national)*

1. M.Kleffmann , A.Meurer, E.Thomae, C.Wolf (Hrsg.), “14. Kryptotag - Workshop über Kryptographie", Ruhr-Universität Bochum, 14 Seiten, März 2011.
2. W.Lindner, and C.Wolf (Hrsg.), “2. Kryptotag - Workshop über Kryptographie", Technical Report 2005-CW-1, COSIC, K.U.Leuven, Belgium and Ulmer Informatik Berichte 2005-02, University of Ulm, Germany, 12 Seiten, 2005.
3. S.Lucks, and C.Wolf (Hrsg.), “1. Kryptotag - Workshop über Kryptographie", Technical Report 2004-CW-1, COSIC, K.U.Leuven, Belgium and TR 2004-10, Reihe Informatik, University of Mannheim, Germany, 17 Seiten, 2004.

Populärwissenschaftliche Beiträge

1. C.Wolf: "Kurze Signaturen in Public Key Kryptographie: Multivariate Quadratische Polynome", In MultiSysteme & Internet Security Cookbook (MISC), 9 Seiten, 2006.
2. C.Wolf and E. Zenner, “Zur Sicherheit von SHA-1, Tragweite und Konsequenzen – ein aktueller Überblick”, in Datenschutz und Datensicherheit 29 (5), pp. 275-278, 2005.

Nationale Konferenzen & Workshops *(Peer-Reviewed)*

1. Christopher Wolf: “Welt-weites Wählen am Beispiel der IACR.” In GI Jahrestagung 2013, Lecture Notes in Informatics – LNI 220, pp. 819-833.
2. C.Wolf, J.Schwenk, Z.Wang, “Sicherheitsanalyse von Kreditkarten am Beispiel von EMV.” In GI Jahrestagung 2009, Lecture Notes in Informatics – LNI 154, pp. 1732-1743, 2009.
3. C.Wolf: “Äquivalente Schlüssel in Multivariate Quadratic Public Key Systemen — Aktueller Stand”, In Proceedings of Kryptowochenende 2006 - Workshop über Kryptographie, F. Armknecht, D. Stegemann (ed.), Technical Report of the University of Mannheim, Department of Computer Science, TR-2006-013,pp. 6-9, 2006.
4. C.Wolf, “Über Hash-Funktionen”, In 4. Kryptotag, Technical Report University of Bochum, Ulrich Greveler (Hg.), Technical Report No. NDS-1/06, p. 4, May 11, 2006.
5. D.De Cock, C.Wolf, and B.Preneel, "The Belgian Electronic Identity Card (Overview)," In Sicherheit 2006: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Lecture Notes in Informatics (LNI) LNI P-77, J. Dittmann (ed.), Bonner Köllen Verlag, pp. 298-301, 2006.
6. C.Wolf and B.Preneel, “Applications of Multivariate Quadratic Public Key Systems", In Sicherheit - Schutz und Zuverlässigkeit, Lecture Notes in Informatics LNI P-62, Gesellschaft für Informatik, pp. 413-424, 2005.
7. C. Wolf, P. Fitzpatrick, S.N. Foley, and E. Popovici, “HFE in Java: Implementing Hidden Field Equations for Public Key Cryptography”, Irish Signals and Systems Conference ISSC, June 24 - 26, 2002, Cork, Ireland, 6 Seiten.

Promotionsschrift

1. C.Wolf, “Multivariate Quadratic Polynomials in Public Key Cryptography,” PhD thesis, Katholieke Universiteit Leuven, B. Preneel (promotor), 156+xxiv Seiten, 2005.

Weitere Internationale Veröffentlichungen

1. C.Wolf, and B.Preneel, “Asymmetric Cryptography: Hidden Field Equations", In European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS), Jyvaskyla University Press, 20 Seiten, 2004.
2. C.Wolf, “Overview of Hidden Field Equations", In Polynomial-based Cryptography 2004, 3 Seiten, 2004.