PUBLIKATIONSLISTE PROF. DR.-ING. JAN PELZL

Stand: Dezember 2014

Einzelbänder

Paar, C., Pelzl, J.: Understanding Cryptography - A Textbook for Students and Practicioners. 1st Edition 2010. Springer Verlag 2009.

Pelzl, J.: Practical Aspects of Curve-Based Cryptography and Cryptanalysis. 1. Auflage. Europäischer Universitätsverlag 2006.

Journal Paper

Weimerskirch, A., Wollinger, T., Pelzl, J. u. a.: Data in Transit. In: Thinking Highways Vol.4, No.3 (2009), p.56--59.

Guajardo, J., Güneysu, T., Kumar, S. u. a.: Efficient Hardware Implementation of Finite Fields. In: Acta Applicandae Mathematicae September Vol. 93, No. 1-3 (2006). p 75–118.

Guajardo, J., Kumar, S., Paar, C. u. a.: Efficient Software-Implementation of Finite Fields with. In: Acta Applicandae Mathematicae August Vol. 93, No. 1-3 (2006). pp. 3-32.

Pelzl, J., Simka, M., Kleinjung, T. u. a.: Area-Time Efficient Hardware Architecture for Factoring Integers with the Elliptic Curve Method. In: IEE Proceedings - Information Security October 152(1) (2005). p.67--78.

Wollinger, T., Pelzl, J., Paar, C.: Cantor versus Harley: Optimization and Analysis of Explicit Formulae for Hyperelliptic Curve Cryptosystems. In: IEEE Transactions on Computers July 54(7) (2015). p. 861-872.

Wollinger, T., Pelzl, J., Wittelsberger, V. u. a.: Elliptic & Hyperelliptic Curves on Embedded µP. In: ACM Transactions in Embedded Computing Systems (TECS) August 3(3), (2004). p. 509-533.

Book Chapter

Pelzl, J.: Aus dem smarten Leben gegriffen. In: Sicherheit im Wandel von Technologien und Märkten. Hrsg. v. Bub, U., Wolfenstetter , K. Springer Verlag.

Pelzl, J.: e-security 4.0, Sicherheitsmanagement für das Internet der Dinge, in Beherrschbarkeit von Big Data. In: Cloud Computing und Cyber Security. Hrsg. v. Bub, U., Wolfenstetter, K.. Springer Verlag.

Pelzl, J., Wolf, M., Wollinger, T.: Smart Embedded Platform Automotive. In Secure Smart Embedded Devices, Platforms and Applications. ed. Markantonakis, K.. Springer Verlag.

Pelzl, J.: Sicherheit für die Verwaltung eingebetteter Systeme. In: IT-Sicherheit zwischen Regulierung und Innovation. Hrsg. v. Bub, U., Wolfenstetter, K.. Berlin: Vieweg + Teubner, GWV Fachverlag GmbH 2011.

Pelzl, J.: IT-Sicherheit im Automobil: Existierende Lösungen und neue Ansätze. In: Sicherheit und Vertrauen in der mobilen Informations- und Kommunikationstechnologie. Hrsg. v. Bub, U., Wolfenstetter, K.. Berlin: Vieweg+Teubner, GWV Fachverlag GmbH 2009.

PUBLIKATIONSLISTE PROF. DR.-ING. JAN PELZL

Stand: Dezember 2014

Pelzl, J., Wollinger, T.: *Security Aspects of Mobile Communication Systems*. In: Embedded Security in Cars - Securing Current and Future Automotive IT Applications, ed. Lemke, K., Paar,C., Wolf, M.. Springer-Verlag 2005. p.167--185.

Pelzl, J., Wollinger, T., Paar, C.: Special Hyperelliptic Curve Cryptosystems of Genus Two: Efficient Arithmetic and Fast implementation. In: Embedded Cryptographic Hardware: Design and Security, ed. Nedjah, N.. New York: Nova Science Publishers 2004.

Conference Paper

Paar, C., Pelzl, J., Rupp, A. u. a.: Securing Green Cars - IT Security in Next-Generation Electric Vehicle Systems. In: D.A.CH. Security Konferenz, 2009, Bochum, Germany.

Geiselmann, W., Januszewski, F., Köpfer, H. u. a.: A Simpler Sieving Device:Combining ECM and TWIRL. In: 9th International Conference on Information Security and Cryptology – ICISC 2006, November 30 - December 1, 2006, Busan, Korea, Proceedings. LNCS, Springer-Verlag.

Kumar, S., Paar, C., Pelzl, J. u. a.: Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker. In: Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, October 10 - October 13, 2006, Yokohama, Japan. Proceedings. LNCS, Springer-Verlag.

Kumar, S., Paar, C., Pelzl, J. u. a.: A Configuration Concept for a Massively Parallel FPGA Architecture. In: International Conference on Computer Design - CDES'06, June 26-29, 2006, Las Vegas, USA.

Bogdanov, A., Mertens, M., Paar, C. u. a.: SMITH - A Parallel Hardware Architecture for fast Gaussian Elimination over GF(2). In: IEEE Symposium on Field-Programmable Custom Computing Machines - FCCM 2006, April 24-26, 2006, Napa, CA, USA.

Kumar, S., Paar, C., Pelzl, J. u. a.: Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker. In: IEEE Symposium on Field-Programmable Custom Computing Machines - FCCM 2006, April 24-26, 2006, Poster summary, Napa, CA, USA.

Kumar, S., Paar, C., Pelzl, J. u. a.: How to Break DES for USD 8,980. In: International Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems - SHARCS'06, April 3-4, 2006, Cologne, Germany.

Güneysu, T. E., Paar,C., Pelzl, J.: On the Security of Elliptic Curve Cryptosystems against Attacks with Special-Purpose Hardware. In: International Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems - SHARCS'06, April 3-4, 2006, Cologne, Germany.

Bogdanov, A., Mertens, M., Paar, C. u. a.: A Parallel Hardware Architecture for fast Gaussian Elimination over GF(2). In: International Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems - SHARCS'06, April 3-4, 2006, Cologne, Germany.

Franke, J., Kleinjung,T., Paar, C. u. a.: SHARK --- A Realizable Special Hardware Sieving Device for Factoring 1024-bit Integers. In: ed. Rao, J., Sunar, B., 7th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2005, August 29 - September 1, 2005, vol. 3659 of LNCS, Springer-Verlag, p. 119--130, Edinburgh, UK.

PUBLIKATIONSLISTE PROF. DR.-ING. JAN PELZL

Stand: Dezember 2014

Amanor, D.N., Paar, C., Pelzl, J. u. a.: Efficient Hardware Architectures for Modular Multiplication on FPGAs. In: IEEE Circuits and Systems Society, International Conference on Field Programmable Logic and Applications (FPL) 2005, August 24- 26, 2005, p. 539--542, Tampere, Finland.

Kaiser, U., Paar, C., Pelzl, J. u. a.: Auswahlkriterien für kryptographische Algorithmen bei Low-Cost-RFID Systemen. In: D.A.CH. Security Konferenz, March 17-18, 2005.

Simka, M., Pelzl, J., Kleinjung, T. u .a.: Hardware Factorization Based on Elliptic Curve Method. In: IEEE Symposium on Field-Programmable Custom Computing Machines - FCCM 2005, April 18-20, 2005, p.107-116, Napa, CA, USA.

Kleinjung, T., Franke, J., Paar, C. u. a.: An Efficient Hardware Architecture for Factoring Integers with the Elliptic Curve Method. In: International Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems --- SHARCS 2005, February 24-25, 2005, Paris, France.

Franke, J., Kleinjung, T., Paar, C. u. a.: SHARK --- A Realizable Special Hardware Sieving Device for Factoring 1024-bit Integers. In: International Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems --- SHARCS 2005, February 24-25, 2005, Paris, France.

Baktir, S., Pelzl, J., Wollinger, T. u. a.: Optimal Tower Fields for Hyperelliptic Curve Cryptosystems. In: 38th Asilomar Conference on Signals, Systems and Computers, November 7-10, 2004, Pacific Grove, USA.

Pelzl, J.: Arithmetic on Elliptic Curves over GF(2^n). In: ECC Summer-School 2004, (Invited Paper), September 14-16, 2004, Ruhr University Bochum, Germany.

Pelzl, J.: Hardware Implementation of ECC. In: ECC Summer-School 2004, (Invited Paper), September 14- 16, 2004, Ruhr University Bochum, Germany.

Barteska, E., Pelzl, J., Paar, C. u. a.: Case Study: Compiler Comparison for an Embedded Cryptographical Application. In: The 2004 International Conference on Embedded Systems and Applications - ESA, June 21-24, 2004, Las Vegas, USA.

Pelzl, J., Wollinger, T., Paar, C.: High Performance Arithmetic for Special Hyperelliptic Curve Cryptosystems of Genus Two. In: International Conference on Information Technology: Coding and Computing - ITCC 2004, IEEE Computer Society, April 2004, Las Vegas, USA.

Paar, C., Pelzl, J., Schramm, K. u. a.: Eingebettete Sicherheit: State-of-the-art und zukünftige Entwicklungen, DACH Security, March 30-31, 2004, Basel, Swiss.

Pelzl, J., Wollinger, T., Guajardo, J. u. a.: Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves. In: eds. Walter, C.D., Koc, C.K., Paar, C.. International Workshop on Cryptographic Hardware and Embedded Systems --- CHES 2003, Springer-Verlag Vol. 2779 of LNCS, September 7-10, 2003, p. 349-365, Köln, Deutschland.

Pelzl, J., Wollinger, T., Paar, C.: Low Cost Security: Explicit Formulae for Genus-4 Hyperelliptic Curves. In: eds. Matsui, M., Zuccherato, R.J.. Selected Areas in Cryptography SAC, Lecture Notes in Computer Science, Vol. 3006, 2003, Springer Verlag Berlin Heidelberg, Deutschland.

PUBLIKATIONSLISTE PROF. DR.-ING. JAN PELZL

Stand: Dezember 2014

Technical Reports

Batina, L., Mentens, N., Pelzl, J. u. a.: Hardware Crackers. In: ECRYPT - European Network of Excellence in Cryptology. ed. Oswald, E..31. July, 2005.

Babbage, S., Catalano, D., Granboulan, L. u. a.: Yearly Report on Algorithms and Keysizes (2004), ECRYPT - European Network of Excellence in Cryptology. ed. Gehrmann, C., Näslund, M.. 17. March, 2005.

Paar, C., Pelzl, J., Wollinger, T.: Hyperelliptic Cryptosystems in Practice. In: 1. Krypto-Tag, Gesellschaft für Informatik - GI, Dezember, 2004, Mannheim, Deutschland.

Thesis

Pelzl, J.: Practical Aspects of Curve-Based Cryptography and Cryptanalysis. In: Dissertation, Department of Electrical Engineering and Information Sciences, Juni, 2006, Ruhr-Universität Bochum, Bochum, Deutschland.

Pelzl, J.: Hyperelliptic Cryptosystems on Embedded Microprocessor. In: Master's thesis, Department of Electrical Engineering and Information Sciences, September 2002, Ruhr-Universität Bochum, Bochum, Deutschland.

Further Contributions and Activities

Wolf, M., Pelzl, J.: Airborne Stuxnet? IT Security Threats for Modern Computerized Aircrafts. In: Avionics Europe Conference, March 21st-22nd 2012, Munich, Germany.

Pelzl, J.: Absicherung von Geschäftsmodellen im mobilen Handel. In: 3. thinksmart – secure communication for mobile networks, November 6th-7th, 2013, Berlin, Germany.

Küster, M., Pelzl, J.: Manipulationsschutz vernetzter Sicherheitssysteme durch IT-Sicherheit, Workshop. In: Innosecure Velbert, September 25th - 26th, 2013, Velbert/ Heiligenhaus, Germany.

Pelzl, J.: Program Chair and Technical Organization, IT-Sec - Industrial Security & Automation, September 23rd – 24th, 2013, Essen, Germany.

Pelzl, J.: Challenges in Embedded Key Management, Omnicard, January 15th-17th, 2013, Berlin, Germany.

Pelzl, J.: Program Chair and Technical Organization, 2nd Think Smart International Conference on Secure Communication for Energy Networks, November 21th – 22th, 2012, Düsseldorf, Germany.

Pelzl, J., Program Committee, IT-Sec, IT Security Industrial & Automation 2012, November 13th - 14th, Dresden, Germany.

Carluccio, D., Pelzl, J.: IT-Sicherheit als Treiber moderner Sicherheitstechnologie. In: Workshop, Innosecure Velbert, May 23th - 24th, 2012, Velbert/ Heiligenhaus, Germany.

Pelzl, J.: Anforderungen und Lösungen für Sicheres Smart Metering, ConLife 2012, June 28th, 2012, Cologne, Germany.

PUBLIKATIONSLISTE PROF. DR.-ING. JAN PELZL

Stand: Dezember 2014

Pelzl, J.: Organization and Moderation, Introduction to Industrial Cryptography and IT Security. In: Embedded World Conference, February 28th, 2012, Nuremberg, Germany.

Pelzl, J.: Organization and Moderation, Workshop on Cryptography and Embedded Security, Embedded World Conference 2011, March 1st, 2011, Nuremberg, Germany.

Pelzl, J.: Program Chair, escar 2010, Embedded Security in Cars, November 2010, Bremen, Germany.

Pelzl, J.: Program Comitte, CryptArchi, June 27th -30th, 2010, CNRS conference center, Paris, France.

J.Pelzl: Program Comitte, S&D4RCES: International Workshop on Security and Dependability for Resource Constrained Embedded Systems (Secure and dependable RCES by design) in conjunction with SAFECOMP 2010 conference, September 14th, 2010, Vienna, Austria.

Pelzl, J.: Organization and Moderation, Workshop on Cryptography and Embedded Security In: Embedded World Conference 2010, March 2nd, 2010, Nuremberg, Germany.

Pelzl, J., Wollinger, T.: Workshop on Mobile and Embedded IT-Security. In: Wireless Technologies Kongress 2010, September 22th - 23th, Bochum, Germany.

Pelzl, J., Wollinger, T.: Tutorial IT-Security in Mobile Applications. In: Wireless Congress 2010 - Systems & Applications, November 10th - 11th, Munich, Germany.

Pelzl, J.: Wie behalte ich die Kontrolle über meine ausgelieferten Produkte? In: IHK Forum Mittelstand, December 6th, 2010, Bochum, Germany.

Pelzl, J., Wollinger, T.: Sicheres Aktivieren von Features und Funktionen für Embedded Systeme. In: DESIGN&ELEKTRONIK Entwicklerforum Embedded-System-Entwicklung, October 7th - 8th, 2009, Ludwigsburg, Germany.

Pelzl, J., Wollinger, T.: Eingebettete Sicherheit in der Medizintechnik – Ein Überblick. In: DESIGN&ELEKTRONIK Entwicklerforum Embedded goes medical, September 9th, Leipzig, Germany.

Osterhues, A., Pelzl, J., Wollinger, T.: Workshop on Embedded Security, 6th Wireless Congress. In: Systems & Applications, October 21st - 22nd, 2009, Munich, Germany.

Bußmeyer, D., Driessen, B., Osterhues, A. u.a.: A Generic Architecture and Extension of eCryptfs: Secret Sharing Scheme, Smartcard Integration and a new Linux Security Module. In: Linux Kongress 2009, Germany.

Pelzl, J., Wollinger, T.: Sicherheitsaspekte bei Embedded IT. In: IM - die Fachzeitschrift für Information Management & Consulting, April 2009.

Pelzl, J., Wollinger, T.: Automotive Security: Absicherung des Gesamtsystems Kraftfahrzeug durch eingebettete Hard- und Software. In: IM - Die Fachzeitschrift für Information Management & Consulting, March (2007).

PUBLIKATIONSLISTE PROF. DR.-ING. JAN PELZL

Stand: Dezember 2014

Pelzl, J., Wollinger, T., Guajardo, J.: Hyperelliptic Curve Cryptosystems, Closing the Performance Gap to Elliptic Curves. In: Euler Institute of Discrete Mathematics - EIDMA Symposium, PhD Conference, November 21-22, 2002, Carlton De Brug, Mierlo.

Invited Talks

Pelzl, J.: Automotive Embedded Security - Challenges and Chances. In: SIAT - Symposium on International Automotive Technology January 9th-11th, 2013, Pune, India.

Pelzl, J.: Schutz vor möglichen Eingriffen und Risiken – Vertrauenswürdige Software. In: 12. EUROFORUM Jahrestagung Software im Automobil, May 14th - 15th, 2012, Stuttgart, Germany.

Pelzl, J.: TeleTrusT-Informationstag - Das Automobil als IT-Sicherheitsfall, Moderation, May 11th, 2012, Berlin. Germany.

Pelzl, J.: Eingebettete Sicherheit in der Medizintechnik, Anforderungen an IT-Sicherheit und Datenschutz bei Medizinprodukten. In: Nürnberger Medizinproduktekonferenz, March 22nd, 2012, TüV Rheinland Nuremberg, Germany.

Pelzl, J.: Moderation und Program Organization, Cryptography and embedded Security – The Workshop. In: Embedded World Conference, February 2nd, 2012, Nuremberg, Germany.

Pelzl, J.: Security Requirements for Connected Life. In: ConLife 2011, June 29th - 30th, 2011, Cologne, Germany.

Pelzl, J., Wolf, M.: Mehr Funktionssicherheit durch IT-Sicherheit. In: 3. EUROFORUM Jahrestagung "ISO 26262", September 26th – 27th, 2011, Stuttgart, Germany.

Pelzl, J.: Warum die konventionelle IT-Sicherheit für PCs im Automobil nicht funktioniert. In: MAHREG 11, Innovationsforum 'SICHERER: Trends, Entwicklungen und Projekte für mobile und stationäre Systeme, October 1st, Barleben, Germany.

Pelzl, J.: Sicherheit für die Verwaltung eingebetteter Systeme. In: EICT Konferenz IT-Sicherheit Vertrauen, Datenschutz, Sicherheit und Innovation, February 10th, 2011, Berlin, Germany.

Pelzl, J.: IT-Sicherheit im Automobil: Existierende Lösungen und neue Ansätze. In: EICT Konferenz IT-Sicherheit, Sicherheit und Vertrauen in der mobilen Informations- und Kommunikationstechnologie, 2009, Berlin, Germany.

Pelzl, J.: Cryptanalysis with a cost-optimized FPGA cluster. In: Securing Cyberspace: Application and Foundations of Cryptography and Computer Security, Workshop IV: Special purpose hardware for cryptography: Attacks and Applications, December 4 - 8, 2006, Institute for Pure and Applied Mathematics (IPAM), University of California, Los Angeles (UCLA).

Pelzl, J.: Exact Cost Estimates of ECC Attacks with Special-Purpose Hardware. In: The 10th Workshop on Elliptic Curve Cryptography - ECC 2006, September 18-20, 2006, The Fields Institute, Toronto, Canada.

PUBLIKATIONSLISTE PROF. DR.-ING. JAN PELZL

Stand: Dezember 2014

Pelzl, J.: Hardware Implementation of ECC. In: ECC Summer-School 2004, September 16th, 2004, Ruhr University Bochum, Germany.

Pelzl, J.: Arithmetic on Elliptic Curves over GF(2^n). In: ECC Summer-School 2004, September 14th, 2004, Ruhr University Bochum, Germany.