Bibliography Prof. dr. ir. Bart Preneel

WARD 2005

Journal articles

Symeonidis, I., Rotaru, D., Mustafa, M.A., Mennink, B., Preneel, B., Papadimitratos, P. (2022). HERMES: Scalable, Secure, and Privacy-Enhancing Vehicular Sharing-Access System. *IEEE INTERNET OF THINGS JOURNAL*, *9* (1), 129-151. doi: 10.1109/JIOT.2021.3094930

Chen, Y.L., Luykx, A., Mennink, B., Preneel, B. (2021). Systematic Security Analysis of Stream Encryption With Key Erasure. *IEEE TRANSACTIONS ON INFORMATION THEORY*, *67* (11), 7518-7534. doi: 10.1109/TIT.2021.3109302

Wouters, L., Gierlichs, B., Preneel, B. (2021). My other car is your car: compromising the Tesla Model X keyless entry system. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2021* (4), 149-172. doi: 10.46586/tches.v2021.i4.149-172

Andreeva, E., Bhati, A.S., Preneel, B., Vizar, D. (2021). 1, 2, 3, Fork: Counter Mode Variants based on a Generalized Forkcipher. *IACR TRANSACTIONS ON SYMMETRIC CRYPTOLOGY*, *2021* (3), 1-35. doi: 10.46586/tosc.v2021.i3.1-35 Open Access

Wouters, L., Arribas, V., Gierlichs, B., Preneel, B. (2020). Revisiting a Methodology for Efficient CNN Architectures in Profiling Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2020* (3), 147-168. doi: 10.13154/tches.v2020.i3.147-168 Open Access

Wouters, L., Van den Herrewegen, J., D. Garcia, F., Oswald, D., Gierlichs, B., Preneel, B. (2020). Dismantling DST80-based Immobiliser Systems. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2020* (2), 99-127. doi: 10.13154/tches.v2020.i2.99-127 Open Access

Troncoso, C., Payer, M., Hubaux, J-P., Salathé, M., Larus, J.R., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D., Barman, L., Chatel, S., Paterson, K.G., Capkun, S., Basin, D.A., Beutel, J., Jackson, D., Roeschlin, M., Leu, P., Preneel, B., Smart, N.P., Abidin, A., Gurses, S., Veale, M., Cremers, C., Backes, M., Tippenhauer, N.O., Binns, R., Cattuto, C., Barrat, A., Fiore, D., Barbosa, M., Oliveira, R., Pereira, J. (2020). Decentralized Privacy-Preserving Proximity Tracing. *IEEE Data Engineering Bulletin*, *43*, Art.No. 2, 36-66. (URL)

Gorodilova, A., Agievich, S., Carlet, C., Hou, X-D., Idrisova, V., Kolomeec, N., Kutsenko, A., Mariot, L., Oblaukhov, A., Picek, S., Preneel, B., Rosie, R., Tokareva, N. (2019). The Fifth International Students? Olympiad in cryptography?NSUCRYPTO: Problems and their solutions. *CRYPTOLOGIA*, *44* (3), 223-256. doi: 10.1080/01611194.2019.1670282

Wouters, L., Marin, E., Ashur, T., Gierlichs, B., Preneel, B. (2019). Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2019* (3), 66-85. doi: 10.13154/tches.v2019.i3.66-85 Open Access

Meester, R., Preneel, B., Wenmackers, S. (2019). Reply to Lucas & Henneberg: Are human faces unique? *FORENSIC SCIENCE INTERNATIONAL*, *297*, 217-220. doi: 10.1016/j.forsciint.2019.01.038 Open Access

Biesmans, W., Balasch, J., Rial, A., Preneel, B., Verbauwhede, I. (2018). Private Mobile Pay-TV From Priced Oblivious Transfer. *IEEE Transactions on Information Forensics and Security*, *13* (2), 280-291. Open Access

Helleseth, T., Preneel, B. (2018). Editorial: Special issue on recent trends in cryptography. *CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES*, *10* (1), 1-3. doi: 10.1007/s12095-017-0269-y

Noorman, J., Van Bulck, J., Mühlberg, T., Piessens, F., Maene, P., Preneel, B., Verbauwhede, I., Götzfried, J., Müller, T., Freiling, F. (2017). Sancus 2.0: A low-cost security architecture for IoT devices. *ACM Transactions on Privacy and Security*, *20* (3), Art.No. 7. Open Access

Chen, Y.L., Luykx, A., Mennink, B., Preneel, B. (2017). Efficient Length Doubling From Tweakable Block Ciphers. *IACR Transactions on Symmetric Cryptology*, *2017* (3), 253-270.

Naya-Plasencia, M., Preneel, B. (2017). Preface to Volume 2017, Issue 1. *IACR TRANSACTIONS ON SYMMETRIC CRYPTOLOGY*, *2017* (1), 1-3. doi: 10.13154/tosc.v2017.i1.1-3

Mennink, B., Preneel, B. (2016). Efficient Parallelizable Hashing Using Small Non-Compressing Primitives. *International Journal of Information Security*, *15* (3), 285-300. Open Access

Ottoy, G., Hamelinckx, T., Preneel, B., De Strycker, L., Goemaere, J.P. (2016). On the choice of the appropriate AES data encryption method for ZigBee nodes. *Security and Communication Networks*, *9* (2), 87-93. doi: 10.1002/sec.267

Andreeva, E., Mennink, B., Preneel, B. (2015). Open Problems in Hash Function Security. *Designs, Codes and Cryptography*, *77* (2), 611-631. Open Access

Agievich, S., Gorodilova, A., Kolomeec, N., Nikova, S., Preneel, B., Rijmen, V., Shushuev, G., Tokareva, N., Vitkup, V. (2015). PROBLEMS, SOLUTIONS AND EXPERIENCE OF THE FIRST INTERNATIONAL STUDENT'S OLYMPIAD IN CRYPTOGRAPHY. *PRIKLADNAYA DISKRETNAYA MATEMATIKA*, *29* (3), 41-62. doi: 10.17223/20710410/29/4

Toli, C-A., Preneel, B. (2015). A bimodal verification cryptosystem as a framework against spoofing attacks. *International Journal of Intelligent Computing Research of Infonomics Society*, *6* (2), 540-549. doi: 10.20533/ijicr.2042.4655.2015.0069

Scheir, M., Balasch, J., Rial, A., Preneel, B., Verbauwhede, I. (2015). Anonymous Split E-Cash - Toward Mobile Anonymous Payments. *ACM Transactions on Embedded Computing Systems*, *14* (4), Art.No. 85. Open Access

Ramos Araújo Beato, F., Meul, S., Preneel, B. (2015). Practical identity-based private sharing for online social networks. *Computer Communications*, *73*, 243-250.

Luykx, A., Mennink, B., Preneel, B., Winnen, L. (2015). Two-Permutation-Based Hashing with Binary Mixing. *Journal of Mathematical Cryptology*, *9* (3), 139-150. Open Access

Preneel, B. (2015). Mathematicians discuss the Snowden revelations: Cryptographic standards, mass surveillance, and the NSA. *Notices of the American Mathematical Society*, *62* (4), 400-403. doi: 10.1090/noti1237

Szepieniec, A., Preneel, B. (2015). New Techniques for Electronic Voting. *USENIX Journal of Election Technology and Systems*, *3* (2), 46-69.

Agievich, S., Gorodilova, A., Kolomeec, N., Nikova, S., Preneel, B., Rijmen, V., Shushuev, G., Tokareva, N., Vitkup, V. (2015). Problems, Solutions and experience of the first international student's olympiad in cryptiography. *Applied Discrete Mathematics*, *3* (29), 41-62.

Preneel, B. (2014). Attacking a problem from the middle: technical perspective. *Communications of the ACM*, *57* (10), 97-97.

Sekar, G., Mouha, N., Preneel, B. (2014). Meet-in-the-Middle Attacks on Reduced-Round GOST. *Matematicheskie Voprosy Kriptografii [Mathematical Aspects of Cryptography]*, *5* (2), 117-125.

Hermans, J., Peeters, R., Preneel, B. (2014). Proper RFID Privacy: Model and Protocols. *IEEE Transaction on Mobile Computing*, *13* (12), 2888-2902. Open Access

Mavrogiannopoulos, N., Pashalidis, A., Preneel, B. (2014). Towards a secure Kerberos key exchange with smart cards. *International Journal of Information Security*, *13* (3), 217-228. Open Access

Ideguchi, K., Tischhauser, E., Preneel, B. (2014). Internal differential collision attacks on the reduced-round Grøstl-0 hash function. *Designs, Codes and Cryptography*, *70* (3), 251-271.

Wouters, K., Wyseur, B., Preneel, B. (2014). Lexical Natural Language Steganography Systems with Human Interaction. *IEEE Spectrum Magazine*, *35* (8), 303-312. Open Access

Lopez, J., Nikova, S., Pashalidis, A., Pernul, G., Preneel, B. (2013). EUROPKI-2011 Preface. *COMPUTERS & MATHEMATICS WITH APPLICATIONS*, *65* (5), 747-747. doi: 10.1016/j.camwa.2013.02.001

Ottoy, G., Preneel, B., Stevens, N., Goemaere, J.P., De Strycker, L. (2013). Open-source hardware for embedded security. *EDN*, Art.No. 4406271.

Bohó, A., Van Wallendael, G., Dooms, A., De Cock, J., Braeckman, G., Preneel, B., Schelkens, P., Van de Walle, R. (2013). End-To-End Security for Video Distribution: The Combination of Encryption, Watermarking, and Video Adaptation. *IEEE Signal Processing Magazine*, *30* (2), 97-107. Open Access

Aerts, W., Biham, E., De Moitié, D., De Mulder, E., Dunkelman, O., Indesteege, S., Keller, N., Preneel, B., Vandenbosch, G., Verbauwhede, I. (2012). A Practical Attack on KeeLoq. *Journal of Cryptology*, *25* (1), 136-157. Open Access

Andreeva, E., Mennink, B., Preneel, B. (2012). The Parazoa Family: Generalizing the Sponge Hash Functions. *International Journal of Information Security*, *11* (3), 149-165. Open Access

Andreeva, E., Bogdanov, A., Mennink, B., Preneel, B., Rechberger, C. (2012). On Security Arguments of the Second Round SHA-3 Candidates. *International Journal of Information Security*, *11* (2), 103-120. Open Access

Peeters, R., Singelée, D., Preneel, B. (2012). Towards More Secure and Reliable Access Control. *IEEE Pervasive Computing*, *11* (3), 76-83. Open Access

Kim, J., Hong, S., Preneel, B., Biham, E., Dunkelman, O., Keller, N. (2012). Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis. *IEEE Transactions on Information Theory*, *58* (7), 4948-4966.

Pashalidis, A., Preneel, B. (2012). Evaluating Tag-Based Preference Obfuscation Systems. *IEEE Transactions on Knowledge and Data Engineering*, *24* (9), 1613-1623.

Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B., Yoshida, H. (2012). An AES Based 256-bit Hash Function for Lightweight Applications: Lesamnta-LW. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, (1), 89-99.

Preneel, B., Kim, J., Sauveron, D. (2012). Advanced theory and practice for cryptography and future security. *MATHEMATICAL AND COMPUTER MODELLING*, *55* (1-2), 1-2. doi: 10.1016/j.mcm.2011.09.020

Mouha, N., Sekar, G., Preneel, B. (2012). Challenging the Increased Resistance of Regular Hash Functions Against Birthday Attacks. *Journal of Mathematical Cryptology*, *6* (3), 229-248. doi: 10.1515/jmc-2011-0010 Open Access

Indesteege, S., Preneel, B. (2012). DES Collisions Revisited. *Lecture Notes in Computer Science*, *6805*, 13-24.

Preneel, B. (2012). Privacy: het einde van de rit? *Karakter. Tijdschrift van Wetenschap.*, *2012* (37), 18-19.

Mavrogiannopoulos, N., Kisserli, N., Preneel, B. (2011). A Taxonomy Of Self-Modifying Code For Obfuscation. *Computers & Security*, *30* (8), 679-691. doi: 10.1016/j.cose.2011.08.007

Sakiyama, K., Knezevic, M., Fan, J., Preneel, B., Verbauwhede, I. (2011). Tripartite Modular Multiplication. *Integration, the VLSI Journal*, *44* (4), 259-269. Open Access

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering Journal*, *16* (1), 3-32.

Gu, Y., Wyseur, B., Preneel, B. (2011). Software-Based Protection is Moving to the Mainstream. *IEEE Software, Special Issue on Software Protection*, *28* (2), 56-59.

Ding, N., Gu, D., Preneel, B. (2011). Precise Bounded-Concurrent Zero-Knowledge in Almost Constant Rounds. *JOURNAL OF INTERNET TECHNOLOGY*, *12* (4), 609-617. (URL)

Indesteege, S., Preneel, B. (2011). Practical Collisions for EnRUPT. *Journal of Cryptology*, *24* (1), 1-23.

Troncoso, C., Danezis, G., Kosta, E., Balasch, J., Preneel, B. (2011). PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance. *IEEE Transactions on Dependable and Secure Computing*, *8* (5), 742-755.

Rial Duran, A., Balasch, J., Preneel, B. (2011). A Privacy-Preserving Buyer-Seller Watermarking Protocol Based on Priced Oblivious Transfer. *IEEE Transactions on Information Forensics and Security*, *6* (1), 202-212. doi: 10.1109/TIFS.2010.2095844

Wolf, C., Preneel, B. (2011). Equivalent keys in Multivariate quadratic public key systems. *Journal of Mathematical Cryptology*, *4* (4), 375-415.

Peeters, R., Singelée, D., Preneel, B. (2011). Threshold-Based Location-Aware Access Control. *International Journal of Handheld Computing Research*, *2* (3), 22-37.

De Beule, J., Edel, Y., Kasper, E., Klein, A., Nikova, S., Preneel, B., Schillewaert, J., Storme, L. (2010). Galois geometries and applications. *DESIGNS CODES AND CRYPTOGRAPHY*, *56* (2-3), 85-86. doi: 10.1007/s10623-010-9410-z

Wan, Z., Ren, K., Zhu, B., Preneel, B., Gu, M. (2010). Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks. *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*, *59* (2), 519-532. doi: 10.1109/TVT.2009.2028892

Singelée, D., Latré, B., Braem, B., Peeters, M., De Soete, M., De Cleyn, P., Preneel, B., Moerman, I., Blondia, C. (2010). A Secure Low-Delay Protocol for Wireless Body Area Networks. *Ad-hoc & Sensor Wireless Networks*, *9* (1), 53-72.

Rial, A., Deng, M., Bianchi, T., Piva, A., Preneel, B. (2010). A Provably Secure Anonymous Buyer–Seller Watermarking Protocol. *IEEE Transactions on Information Forensics and Security*, *5* (4), 920-931. doi: 10.1109/TIFS.2010.2072830

Velichkov, V., Rijmen, V., Preneel, B. (2010). Algebraic Cryptanalysis of a Small-Scale Version of Stream Cipher LEX. *IET Information Security*, *4* (2), 49-61.

Andreeva, E., Mennink, B., Preneel, B. (2010). Security Properties of Domain Extenders for Cryptographic Hash Functions. *Journal of Information Processing Systems*, *6* (4), 453-480.

Rivest, R.L., Chaum, D., Preneel, B., Rubin, A.D., Saari, D.G., Vora, P.L. (2009). Guest Editorial Special Issue on Electronic Voting. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, *4* (4), 593-596. doi: 10.1109/TIFS.2009.2034721

Deng, M., De Cock, D., Preneel, B. (2009). Towards a Cross-Context Identity Management Framework in E-Health. *Online Information Review*, *33* (3), 422-442.

Wan, Z., Deng, R., Bao, F., Preneel, B., Gu, M. (2009). n PAKE+: A Tree-Based Group Password-Authenticated Key Exchange Protocol Using Different Passwords. *Journal of Computer Science and Technology*, *24* (1), 138-151.

Van Alsenoy, B., De Cock, D., Simoens, K., Dumortier, J., Preneel, B. (2009). Delegation and Digital Mandates: Legal Requirements and Security Objectives. *Computer Law and Security Review*, *25* (5), 415-431. doi: 10.1016/j.clsr.2009.07.007

Seys, S., Preneel, B. (2009). ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks. *International Journal of Wireless and Mobile Computing*, *3* (3), 145-155.

Schellekens, D., Wyseur, B., Preneel, B. (2008). Remote attestation on legacy operating systems with trusted platform modules. *SCIENCE OF COMPUTER PROGRAMMING*, *74* (1-2), 13-22. doi: 10.1016/j.scico.2008.09.005

Aerts, W., De Mulder, E., Preneel, B., Vandenbosch, G., Verbauwhede, I. (2008). Dependence of RFID Reader Antenna Design on Read Out Distance. *IEEE Transactions on Antennas and Propagation*, *56* (12), 3829-3837.

Chen, L., Dawson, E., Lai, X., Mambo, M., Miyaji, A., Mu, Y., Pointcheval, D., Preneel, B., Smart, N., Susilo, W., Wang, H., Wong, D.S. (2008). Cryptography in computer system security J.UCS special issue. *JOURNAL OF UNIVERSAL COMPUTER SCIENCE*, *14* (3), 314-317. (URL)

Schellekens, D., Wyseur, B., Preneel, B. (2008). Remote Attestation on Legacy Operating Systems With Trusted Platform Modules. *1st International Workshop on Run Time Enforcement for Mobile and Distributed Systems (REM 2007)*, 59-72.

Örs, S., Batina, L., Preneel, B., Vandewalle, J. (2008). Hardware Implementation of an Elliptic Curve Processor over GF(p) with Montgomery Modular Multiplier. *International Journal of Embedded Systems (IJES)*, *3* (4), 229-240.

De Cock, D., Simoens, K., Preneel, B. (2008). Insights on identity documents based on the Belgian case study. *Information Security Technical Report*, *13* (2), 54-60.

Lano, J., Mentens, N., Preneel, B., Verbauwhede, I. (2008). Power Analysis of Synchronous Stream Ciphers with Resynchronization Mechanism. *International Journal of Intelligent Information Technology Application*, *1* (2), 327-333. Open Access

Schellekens, D., Wyseur, B., Preneel, B. (2008). Remote attestation on legacy operating systems with trusted platform modules. *Science of Computer Programming*, *74* (1), 13-22. doi: 10.1016/j.scico.2008.09.005

Deng, M., Preneel, B. (2008). Attacks on two buyer-seller watermarking protocols and an improvement for revocable anonymity. *International Journal of Intelligent Information Technology Application*, *1* (2), 53-64.

Elci, A., Örs, S.B., Preneel, B. (2008). Preface. *Security of Information and Networks - Proceedings of the 1st International Conference on Security of Information and Networks, SIN 2007*.

De Mulder, E., Örs, S., Preneel, B., Verbauwhede, I. (2007). Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems. *Computers & Electrical Engineering*, *33* (5), 367-382.

Sakiyama, K., Batina, L., Preneel, B., Verbauwhede, I. (2007). Multi-core Curve-based Cryptoprocessor with Reconfigurable Modular Arithmetic Logic Units over GF(2^n). *IEEE Transactions on Computers*, *56* (9), 1269-1282.

Sakiyama, K., Batina, L., Preneel, B., Verbauwhede, I. (2007). High-performance Public-key Cryptoprocessor for Wireless Mobile Applications. *Mobile Networks and Applications*, *12* (4), 245-258.

Sakiyama, K., Batina, L., Preneel, B., Verbauwhede, I. (2007). HW/SW Co-design for Public-Key Cryptosystems on the 8051 Micro-controller. *Computers & Electrical Engineering*, *33* (5), 324-332. Open Access

Sakiyama, K., Mentens, N., Batina, L., Preneel, B., Verbauwhede, I. (2007). Reconfigurable Modular Arithmetic Logic Unit Supporting High-performance RSA and ECC over GF(p). *International Journal of Electronics*, *94* (5), 501-514.

Preneel, B. (2007). A Survey of Recent Developments in Cryptographic Algorithms for Smart Cards. *Computer Networks*, *51* (9), 2223-2233.

Nikov, V., Nikova, S., Preneel, B. (2007). On proactive verifiable secret sharing schemes. *Serdica Journal of Computing*, *1* (1), 337-365.

Nikov, V., Nikova, S., Preneel, B. (2007). On distributed oblivious transfer. *Serdica Journal of Computing*, *1* (1), 313-337.

Mentens, N., Batina, L., Preneel, B., Verbauwhede, I. (2006). Time-memory trade-off attack on FPGA platforms: UNIX password cracking. *Lecture Notes in Computer Science*, *3985*, 323-334. Open Access

Sakiyama, K., Mentens, N., Batina, L., Preneel, B., Verbauwhede, I. (2006). Reconfigurable Modular Arithmetic Logic Unit for High-performance Public-key Cryptosystems. *Lecture Notes in Computer Science*, *3985*, 347-357. Open Access

De Cannière, C., Biryukov, A., Preneel, B. (2006). An Introduction to Block Cipher Cryptanalysis. *Proceedings of the IEEE*, *94* (2), 346-356.

Wolf, C., Braeken, A., Preneel, B. (2006). On the security of stepwise triangular systems. *Designs, Codes and Cryptography*, *40* (3), 285-302.

Braeken, A., Borissov, Y., Nikova, S., Preneel, B. (2006). Classification of Cubic (n-4)-resilient Boolean Functions. *IEEE Transactions on Information Theory*, *52* (4), 1670-1676.

De Mulder, E., Buysschaert, P., Ors, S.B., Delmotte, P., Preneel, B., Vandenbosch, G., Verbauwhede, I. (2006). Measuring the vulnerability of cryptographic algorithms. *IEEE Potentials*, *25* (2), 13-17.

Preneel, B. (2006). Digital signatures and key management. *IEEE Transactions on Computers*, *55* (4), 7-8.

Singelée, D., Preneel, B. (2006). Review of the Bluetooth Security Architecture. *Information Security Bulletin*, *11* (2), 45-53.

Mentens, N., Batina, L., Preneel, B., Verbauwhede, I. (2005). A Systematic Evaluation of Compact Hardware Implementations for the Rijndael S-box. *Lecture Notes in Computer Science*, *3376*, 323-333. Open Access

Quisquater, M., Preneel, B., Vandewalle, J. (2005). Spectral characterization of cryptographic Boolean functions satisfying the (extended) propagation criterion of degree l and order k. *Information Processing Letters*, *93* (1), 25-28.

Borissov, Y., Braeken, A., Nikova, S., Preneel, B. (2005). On the Covering Radii of Binary RM Codes in the Set of Resilient Boolean Functions. *IEEE Transactions on Information Theory*, *51* (3), 1182-1189.

Biryukov, A., Lano, J., Preneel, B. (2005). Recent Attacks on Alleged SecurID and their Practical Implications. *Computers & Security*, *24* (5), 364-370.

De Cannière, C., Lano, J., Preneel, B. (2005). Cryptanalysis of the Two-dimensional Circulation Encryption Algorithm (TDCEA). *EURASIP Journal on Applied Signal Processing*, *2005* (12), 1923-1927.

Batina, L., Mentens, N., Preneel, B., Verbauwhede, I. (2005). Balanced point operations for side-channel protection of elliptic curve cryptography. *IEE Proceedings - Information Security*, *152* (1), 57-65.

Mentens, N., Ors, S.B., Preneel, B., Vandewalle, J. (2005). An FPGA implementation of a Montgomery multiplier over GF(2^m). *Computing and informatics*, *23* (5), 487-499.

Paul, S., Preneel, B. (2005). Solving Systems of Differential Equations of Addition and Cryptanalysis of the Helix Cipher. *Lecture Notes in Computer Science*, *3574*, 75-88. Open Access

Braeken, A., Wolf, C., Preneel, B. (2005). Normality of Vectorial Boolean Functions. *Lecture Notes in Computer Science*, *3796*, 186-200.

Wolf, C., Preneel, B. (2005). Superfluous Keys in Multivariate Quadratic Asymmetric Systems. *Lecture Notes in Computer Science*, *3386*, 275-287.

Nikov, V., Nikova, S., Preneel, B. (2005). On the Size of Monotone Span Programs. *Lecture Notes in Computer Science*, *3352*, 252-265.

Preneel, B. (2005). ECRYPT: the cryptographic research challenges for the next decade. *Lecture Notes in Computer Science*, *3352*, 1-15. Open Access

Singelée, D., Preneel, B. (2005). The Wireless Application Protocol (WAP). *International Journal of Network Security*, *1* (3), 161-165.

Cappaert, J., Preneel, B. (2004). On the Importance of Code Obfuscation. *Electronics Letters*, *40* (4), 91-93.

Batina, L., Buysschaert, P., De Mulder, E., Mentens, N., Ors, S.B., Preneel, B., Vandenbosch, G., Verbauwhede, I. (2004). Side channel attacks and fault attacks on cryptographic algorithms. *Revue HF Tijdschrift*, *2004* (3), 36-45. Open Access

Preneel, B. (2004). Cryptology and Communications Security. *Revue HF Tijdschrift*, *2004* (3), 2-3.

Preneel, B. (2004). Virussen, wormen, SPAM... is de geest uit de fles? *Het Ingenieursblad*, *73* (3), 24-30.

De Cannière, C., Preneel, B. (2004). A Short Introduction to Cryptology. *Revue HF Tijdschrift*, *2004* (3), 4-14.

Seys, S., Preneel, B. (2004). Network Security: Fixed Networks. *Revue HF Tijdschrift*, *2004* (3), 15-24.

Braeken, A., Nikov, V., Nikova, S., Preneel, B. (2004). On Boolean Functions with Generalized Cryptographic Properties. *Lecture Notes in Computer Science*, *3348*, 119-134. Open Access

Singelée, D., Seys, S., Preneel, B. (2004). Wireless Network Security. *Revue HF Tijdschrift*, *2004* (3), 25-35.

Diaz, C., Claessens, J., Preneel, B. (2003). APES: Anonymity and Privacy in Electronic Services. *Datenschutz und Datensicherheit*, *27* (3), 143-145.

Kang, J.S., Preneel, B., Ryu, H., Chung, K.I., Park, C.H. (2003). Pseudorandomness of Basic Structures in the Block Cipher KASUMI. *ETRI Journal*, *25* (2), 89-100.

Quisquater, M., Preneel, B., Vandewalle, J. (2003). A new inequality in discrete Fourier theory. *IEEE Transactions on Information Theory*, *49* (8), 2038-2040.

Claessens, J., Diaz, C., Goemans, C., Preneel, B., Vandewalle, J., Dumortier, J. (2003). Revocable anonymous access to the Internet. *Journal of Internet Research*, *13* (4), 242-258.

Batina, L., Ors, S.B., Preneel, B., Vandewalle, J. (2003). Hardware Architectures for Public Key Cryptography. *Integration, the VLSI Journal*, *34* (1), 1-64. doi: 10.1016/S0167-9260(02)00053-6

Iliadis, J., Gritzalis, S., Spinellis, D., De Cock, D., Preneel, B., Gritzalis, D. (2003). Towards a Framework for Evaluating Certificate Status Information Mechanisms. *Computer Communications*, *26* (16), 1839-1850. doi: 10.1016/S0140-3664(03)00079-3

Singelée, D., Preneel, B. (2003). The Wireless Application Protocol (WAP). *COSIC internal report*.

Claessens, J., Preneel, B., Vandewalle, J. (2003). (How) can mobile agents do secure electronic transactions on untrusted hosts? - A survey of the security issues and the current solutions. *ACM Transactions on Internet Technology*, *3* (1), 28-48.

Preneel, B. (2003). Het beveiligen van telecommunicatienetwerken met cryptografie. *Revue E Tijdschrift*, *191* (1), 41-50.

Knudsen, L., Preneel, B. (2002). Construction of secure and fast hash functions using nonbinary error-correcting codes. *IEEE TRANSACTIONS ON INFORMATION THEORY*, *48* (9), 2524-2539. doi: 10.1109/TIT.2002.801402

Claessens, J., Preneel, B., Vandewalle, J. (2002). A tangled world wide web of security issues. *First Monday*, *7* (3). doi: 10.5210/fm.v7i3.935

Claessens, J., Dem, V., De Cock, D., Preneel, B., Vandewalle, J. (2002). On the Security of Today's Online Electronic Banking Systems. *Computers & Security*, *21* (3), 253-265.

Knudsen, L., Preneel, B. (2002). Enhancing the security of hash functions using non-binary error correcting codes. *IEEE Transactions on Information Theory*, *48* (9), 2524-2539.

Borst, J., Preneel, B., Rijmen, V. (2001). Cryptography on smart cards. *Computer Networks*, *36* (4), 423-435.

Borst, J., Preneel, B., Vandewalle, J. (2000). Variation of Cramer-Shoup public key scheme. *ELECTRONICS LETTERS*, *36* (1), 32-32. doi: 10.1049/el:20000062

Borst, J., Preneel, B., Vandewalle, J. (2000). Comment: Variation of Cramer-Shoup public-key scheme. *Electronics Letters*, *36* (1), 32-32. Open Access

Claessens, J., Preneel, B., Vandewalle, J. (2000). Het World Wide Web beveiligen. *Het Ingenieursblad*, *69* (1), 14-21.

Csapodi, M., Vandewalle, J., Preneel, B. (1999). CNN algorithms for video authentication and copyright protection. *JOURNAL OF VLSI SIGNAL PROCESSING SYSTEMS FOR SIGNAL IMAGE AND VIDEO TECHNOLOGY*, *23* (2-3), 449-463. doi: 10.1023/A:1008113606327

Preneel, B. (1999). State-of-the-art ciphers for commercial applications. *Computers & Security*, *18* (1), 74-76.

Horn, G., Preneel, B. (1999). Authentication and payment in future mobile systems. *Journal of Computer Security*, *8* (2), 183-207.

Csapodi, M., Vandewalle, J., Preneel, B. (1999). CNN algorithms for video authentication and copyright protection. *Journal of Vlsi Signal Processing*, *23* (2), 449-463.

Preneel, B. (1999). The state of cryptographic hash functions. *Lecture Notes in Computer Science*, *1561*, 158-182.

Preneel, B., Rijmen, V., Bosselaers, A. (1998). Principles and performance of cryptographic algorithms. *DR DOBBS JOURNAL*, *23* (12), 126-131. (URL)

Knudsen, L.R., Preneel, B. (1998). MacDES: MAC algorithm based on DES. *Electronics Letters*, *34* (9), 871-873.

Knudsen, L.R., Lai, X.J., Preneel, B. (1998). Attacks on fast double block length hash functions. *Journal of Cryptology*, *11* (1), 59-72.

Preneel, B., Rijmen, V. (1998). Cryptographic primitives for information authentication - state of the art. *Lecture Notes in Computer Science*, *1528*, 49-104. Open Access

Preneel, B., Rijmen, V. (1998). Preface. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1528*.

Preneel, B. (1998). An Introduction to Cryptology. *Lecture Notes in Computer Science*, *1521*, 204-221. Open Access

Preneel, B., Rijmen, V., Bosselaers, A. (1998). Design principles and performance of conventional cryptographic algorithms. *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, *23* (12), 126-131.

Bosselaers, A., Dobbertin, H., Preneel, B. (1997). The new cryptographic hash function RIPEMD-160. *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, *22* (1), 24-28.

Preneel, B. (1997). MACs and Hash functions: State of the art. *Information Security Technical Report*, *2* (2), 33-43.

Rijmen, V., Preneel, B., De Win, E. (1997). On Weaknesses of Non-surjective Round Functions. *Designs, Codes and Cryptography*, *12* (3), 253-266.

Preneel, B., Walrand, J. (1996). Convergence of a quasistatic frequency allocation algorithm. *Journal of High Speed Networks*, *5* (1), 3-22.

Preneel, B., vanOorschot, P.C. (1996). A key recovery attack on the ANSI X9.19 retail MAC. *Electronics Letters*, *32* (17), 1568-1569.

Preneel, B. (1995). Introduction. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1008*, 1-5.

Preneel, B. (1994). Cryptographic hash functions. *European Transactions on Telecommunications*, *5* (4), 431-448.

Preneel, B., Govaerts, R., Vandewalle, J. (1991). Boolean Functions Satisfying Higher Order Propagation Criteria. *Lecture Notes in Computer Science*, *547*, 141-152. Open Access

Preneel, B., Chaum, D., Fumy, W., Jansen, C., Landrock, P., Roelofsen, G. (1991). Race Integrity Primitives Evaluation (RIPE): A Status Report. *Lecture Notes in Computer Science*, *547*, 547-551.

Bosselaers, A., Govaerts, R., Preneel, B., Vandewalle, J. (1990). Cryptanalysis of a fast cryptographic checksum algorithm. *Computers & Security*, *9* (3), 257-262.

Preneel, B., Vanleekwijck, W., Vanlinden, L., Govaerts, R., Vandewalle, J. (1990). Propagation Characteristics of Boolean Functions. *Lecture Notes in Computer Science*, *473*, 161-173. Open Access

PRENEEL, B., BOSSELAERS, A., GOVAERTS, R., VANDEWALLE, J. (1990). A CHOSEN TEXT ATTACK ON THE MODIFIED CRYPTOGRAPHIC CHECKSUM ALGORITHM OF COHEN AND HUANG. *LECTURE NOTES IN COMPUTER SCIENCE*, *435*, 154-163. (URL)

Accepted Journal articles

Biczok, G., Pérez-Solà, C., Preneel, B., Schroers, J., Shirazi, F., Symeonidis, I. (2018). Collateral information collection by Facebook applications: a comprehensive study. *Computers & Security*.

Dunkelman, O., Preneel, B. (2014). Generalizing the Herding Attack to Concatenated Hashing Schemes. *Journal of Computer Science and Technology*. Open Access

Books

Berendschot, A., Boly, J-P., Bosselaers, A., Brandt, J., Chaum, D., Damgård, I., de Rooij, P., Dichtl, M., Fumy, W., Jansen, C., Landrock, P., Preneel, B., Roelofsen, G., van der Ham, M., Vandewalle, J., Bosselaers, A., Preneel, B. (Eds.) (1995). *Integrity Primitives for Secure Information systems. Final Report of RACE Integrity Primitives Evaluation (RIPE-RACE 1040)*. (Lecture Notes in Computer Science, 1007). Springer-Verlag.

Edited books

Adhikari, A., Küsters, R., Preneel, B. (Eds.) (2021). *Progress in Cryptology* (Lecture Notes in Computer Science, 13143). Springer. ISBN 978-3-030-92517-8.

Preneel, B., Vercauteren, F. (Eds.) (2018). *Applied Cryptography and Network Security*. (Lecture Notes in Computer Science, 10892). Springer. ISBN: 978-3-319-93386-3.

Preneel, B., Ikonomou, D. (Eds.) (2014). *Privacy Technologies and Policy - Second Annual Privacy Forum, APF 2014*. (Lecture Notes in Computer Science, 8450). Springer-Verlag. ISBN: 978-3-319-06748-3.

Geffert, V., Preneel, B., Rovan, B., Stuller, J., Min Tjoa, A. (Eds.) (2014). *SOFSEM 2014: Theory and Practice of Computer Science*. (Lecture Notes in Computer Science, 8327). Springer-Verlag. ISBN: 978-3-319-04297-8.

Preneel, B., Ikonomou, D. (Eds.) (2014). *Privacy Technologies and Policy - First Annual Privacy Forum, APF 2012*. (Lecture Notes in Computer Science, 8319). Springer-Verlag. ISBN: 978-3-642-54068-4.

Preneel, B., Takagi, T. (Eds.) (2011). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*. (6917 LNCS). Springer. ISBN: 9783642239502. doi: 10.1007/978-3-642-23951-9

Preneel, B., Takagi, T. (Eds.) (2011). *Cryptographic Hardware and Embedded Systems - CHES 2011*. (Lecture Notes in Computer Science, 6917). Springer-Verlag.

Martinelli, F., Preneel, B. (Eds.) (2010). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*. (6391 LNCS). Springer. ISBN: 3642164404. doi: 10.1007/978-3-642-16441-5

Gritzalis, D., Preneel, B., Theoharidou, M. (Eds.) (2010). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*. (6345 LNCS). Springer. ISBN: 3642154964. (URL)

Gritzalis, D., Preneel, B., Theoharidou:, M. (Eds.) (2010). *2010th European Symposium on Research in Computer Security (ESORICS 2010)*. (Lecture Notes in Computer Science, 6345). Springer-Verlag.

Preneel, B., Dodunekov, S., Rijmen, V., Nikova, S. (Eds.) (2009). *Enhancing cryptographic primitives with techniques from error correcting codes*. (NATO Science for Peace and Security Series D - Information and Communication Security, 23). IOS Press.

Preneel, B. (Eds.) (2009). *Progress in Cryptology - AFRICACRYPT 2009*. (Lecture Notes in Computer Science, 5580). Springer-Verlag.

Martinelli, F., Preneel, B. (Eds.) (2009). *Public Key Infrastructure - 6th European PKI Workshop: Research and Applications, EuroPKI 2009*. (Lecture Notes in Computer Science, 6391). Springer-Verlag.

Geffert, V., Karhumäki, J., Bertoni, A., Preneel, B., Návrat, P., Bieliková, M. (Eds.) (2008). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics: Preface*. (4910 LNCS). Springer. ISBN: 354077565X. (URL)

Elci, A., Preneel, B., Örs, S. (Eds.) (2008). *Security of Information and Networks*. Trafford Publishing.

Elci, A., Preneel, B., Örs, S. (Eds.) (2008). *International Conference on Security of Information and Networks*. Trafford Publishing.

Geffert, V., Karhumaki, M.B., Preneel, B. (Eds.) (2008). *SOFSEM 2008: 2008th Conference on Current Trends in Theory and Practice of Informatics*. (Lecture Notes in Computer Science, 4910). Springer-Verlag.

Katsikas, S.K., Lopez, J., Backes, M., Gritzalis, S., Preneel, B. (Eds.) (2006). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*. (4176 LNCS). Springer. ISBN: 3540383417. doi: 10.1007/11836810

Nikova, S., Preneel, B., Storme, L. (Eds.) (2006). *Coding Theory and Cryptography*. Flemish Academy for Science and Art.

Backes, M., Gritzalis, S., Preneel, B. (Eds.) (2006). *Information Security - 9th International Conference, ISC 2006*. (Lecture Notes in Computer Science, 4176). Springer-Verlag.

Preneel, B., Tavares, S. (Eds.) (2006). *Selected Areas in Cryptography, 12th Annual International Workshop, SAC 2005*. (Lecture Notes in Computer Science, 3897). Springer-Verlag.

Bugliesi, M., Preneel, B., Sassone, V. (Eds.) (2006). *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006*. (Lecture Notes in Computer Science, 4052). Springer-Verlag.

Chadwick, D., Preneel, B. (Eds.) (2005). *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security (CMS 2004)*. (IFIP International Federation for Information Processing, 175). Springer.

Preneel, B. (Eds.) (2002). *Topics in Cryptology - CT-RSA 2002, The Cryptographers' Track at the RSA Conference*. (Lecture Notes in Computer Science, 2271). Springer-Verlag.

Preneel, B. (Eds.) (2000). *Advances in Cryptology - EUROCRYPT 2000*. (Lecture Notes in Computer Science, 1807). Springer-Verlag.

Preneel, B. (Eds.) (1999). *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security (CMS 1999)*. (IFIP Conference Proceedings, 152). Kluwer.

Preneel, B., Rijmen, V. (Eds.) (1998). *State of the Art and Evolution of Computer Security and Industrial Cryptography, 1997*. (Lecture Notes in Computer Science, 1528). Springer-Verlag.

Preneel, B. (Eds.) (1995). *Fast Software Encryption, FSE 1994*. (Lecture Notes in Computer Science, 1008). Springer-Verlag.

Govaerts, R., Preneel, B., Vandewalle, J. (Eds.) (1993). *State of the Art and Evolution of Computer Security and Industrial Cryptography, 1993*. (Lecture Notes in Computer Science, 741). Springer-Verlag.

Book Chapters

Preneel, B., Vercauteren, F. (2018). Preface. In: *Applied Cryptography and Network Security*, (I-XIV). (10892 LNCS). Springer. ISBN: 978-3-319-93386-3.

Grossklags, J., Preneel, B. (2017). Preface. (V-VI). (9603 LNCS). ISBN: 9783662549698.

Peeters, R., Singelée, D., Preneel, B. (2013). Threshold-based location-aware access control. In: W-C. Hu, S.H. Mousavinezhad (Eds.), *Mobile and Handheld Computing Solutions for Organizations and End-Users*, (20-36). IGI Global. ISBN: 1466627859. doi: 10.4018/978-1-4666-2785-7.ch002

De Cock, D., Van Alsenoy, B., Preneel, B., Dumortier, J. (2011). The Belgian eID Approach. In: W. Fumy, M. Paeschke (Eds.), *Handbook of eID Security. Concepts, Practical Experiences, Technologies*, Chapt. 9, (117-139). Erlangen: Publicis Publishing. ISBN: 978-3895783791. [RES]

Preneel, B. (2011). Cryptographic Techniques. In: W. Fumy, M. Paeschke (Eds.), *Handbook of eID Security. Concepts, Practical Experiences, Technologies*, (208-221). Publicis Publishing.

Lee, Y., Batina, L., Singelée, D., Preneel, B., Verbauwhede, I. (2010). Anti-counterfeiting, Untraceability and Other Security Challenges for RFID systems: Public-Key Based Protocols and Hardware. In: D. Naccache, A-R. Sadeghi (Eds.), *Towards Hardware-Intrinsic Security, Security and Cryptology*, (243-264). (Towards Hardware-Intrinsic Security). Springer. ISBN: 3642265782.

Preneel, B. (2009). Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface. (5580 LNCS). ISBN: 3642023835.

Deng, M., De Cock, D., Preneel, B. (2009). An interoperable cross-context architecture to manage distributed personal e-Health information. In: M. Cunha, R. Simoes, A. Tavares (Eds.), *Handbook of Research on Developments in e-Health and Telemedicine: Technological and Social Perspectives, ISBN: 978-1-61520-670-4*, (576-602). Hershey, PA, USA: IGI Global, Inc..

Deng, M., Preneel, B. (2009). On secure buyer-seller watermarking protocols with revocable anonymity. In: A. Lazinica (Eds.), *E-Commerce, ISBN 978-953-7619-98-5*, (183-202). IN-TECH, Vienna, Austria..

Batina, L., Seys, S., Preneel, B., Verbauwhede, I. (2008). Public-key Primitives. In: J. Lopez, J. Zhou (Eds.), *Wireless Sensor Network Security, IOS PRESS, 2008*, (77-109). (Wireless Sensor Network Security). IOS Press.

Singelée, D., Seys, S., Preneel, B. (2008). Security in Wireless PAN Mesh Networks. In: Hu, Zhang, Zheng (Eds.), *Security in Wireless Mesh Networks*, Chapt. 11, (349-381). AUERBACH. ISBN: 9780849382505.

Preneel, B. (2008). Modern Cryptology. In: S.M. Furnell, S. Katsikas, J. Lopez, A. Patel (Eds.), *SECURING INFORMATION AND COMMUNICATIONS SYSTEMS: PRINCIPLES, TECHNOLOGIES, AND APPLICATIONS*, (105-137). (Artech House Information Security and Privacy Series). ARTECH HOUSE. ISBN: 978-1-59693-228-9. (URL)

De Cannière, C., Preneel, B. (2008). Trivium. In: O. Billet, M. Robshaw (Eds.), *New Stream Cipher Designs - The eSTREAM Finalists, Lecture Notes in Computer Science, 4986*, (244-266). Springer-Verlag.

Batina, L., Guajardo, J., Preneel, B., Tuyls, P., Verbauwhede, I. (2008). Public-Key Cryptography for RFID Tags and Applications. In: P. Kitsos, Y. Zhang (Eds.), *RFID Security: Techniques,Protocols and System-On-Chip Design*, (317-348). Springer-Verlag.

Preneel, B. (2008). Mobile and wireless communications security. In: E. Haroutunian, E. Kranakis, E. Shahbazian (Eds.), *NATO ASI on Aspects of Network and Information Security*, (119-133). IOS Press.

Preneel, B. (2007). An Introduction to Modern Cryptology. In: J. Bergstra, K. de Leeuw (Eds.), *The History of Information Security. A Comprehensive Handbook*, (565-592). Elsevier.

Diaz, C., Preneel, B. (2007). Accountable Anonymous Communication. In: W. Jonker, M. Petkovic (Eds.), *Security, Privacy and Trust in Modern Data Management*, (239-256). Springer.

Preneel, B., Tavares, S. (2006). Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics: Preface. (3897 LNCS). ISBN: 3540331085.

Örs, S.B., Gürkaynak, F.K., Oswald, E., Preneel, B. (2005). Power-analysis attack on an ASIC AES implementation. In: *Embedded Cryptographic Hardware: Design and Security*, (51-66). ISBN: 1594541450.

Preneel, B. (2005). Hash Functions. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (256-267). Springer.

Preneel, B. (2005). MAC Algorithms. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (361-368). Springer.

Preneel, B. (2005). Mash Hash Functions. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (370-370). Springer.

Preneel, B. (2005). MDC-2 and MDC-4. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (379-380). Springer.

Preneel, B. (2005). NIESSIE Project. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (408-413). Springer.

Preneel, B. (2005). CBC-MAC and variants. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (63-65). Springer.

Preneel, B. (2005). Collision Resistance. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (81-82). Springer.

Preneel, B. (2005). Davies-Meyer Hash Function. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (136-136). Springer.

Preneel, B. (2005). Correcting-block Attack. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (102-103). Springer.

Preneel, B. (2005). Modes of operation of a block cipher. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (386-391). Springer.

Preneel, B. (2005). MAA - Message Authentication Algorithm. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (361-361). Springer.

Preneel, B. (2005). PMAC. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (460-461). Springer.

Preneel, B. (2005). Preimage Resistance. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (465-466). Springer.

Preneel, B. (2005). Second preimage resistance. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (543-544). Springer.

Preneel, B. (2005). Universal one-way hash functions. In: H. Van Tilborg (Eds.), *Encyclopedia of Cryptography and Security*, (643-643). Springer.

Maier, R., Sdralia, V., Claessens, J., Preneel, B. (2004). Security Issues in a MobileIPv6 Network. In: C. Mitchell (Eds.), *Security for Mobility, IEE Telecommunications, 51*, (269-284). The Institution of Electrical Engineers.

Preneel, B. (2004). Trends in cryptology research. In: S. Paulus, N. Pohlmann, H. Reimer (Eds.), *Securing Electronic Business Processes*, (51-58). Springer-Verlag.

Van Tilborg, H., Preneel, B., Macq, B. (2004). Cryptology. In: P. de With, R. Lagendijk, L. Tolhuizen (Eds.), *Information Theory in the Benelux: An Overview of WIC symposia 1980-2003*, (61-88). Werkgemeenschap voor Informatie- en Communicatietheorie (WIC), Enschede (NL).

Seys, S., Preneel, B. (2002). Cryptologie. In: *Kluwer Handboek Security*, (89-138). Kluwer.

Claessens, J., Preneel, B., Vandewalle, J. (2001). Secure Communication for Secure Agent-Based Electronic Commerce Applications. In: J. Liu, Y. Ye (Eds.), *E-Commerce Agents: Marketplace Solutions, Security Issues, and Supply and Demand, Lecture Notes in Artificial Intelligence, 2033*, (180-190). Springer-Verlag.

Preneel, B. (2000). The state of hash functions. In: P. Gil, C. Goya (Eds.), *Criptologia y Seguridad de la Informacion*, (3-37). Rama Publishing Company.

Vandewalle, J., Preneel, B., Govaerts, R., Daemen, J. (1995). Informatiebeveiliging. In: M-J. Bellen, C. De Ranter, A. Dupré, B. Pattyn, B. Raymaekers, C. Steel, H. Van Gorp (Eds.), *Wegen van Hoop. Universitaire Perspectieven*, (308-321). Universitaire Pers Leuven.

Preneel, B. (1995). Onderschepping van computercommunicatie - encryptie. In: *Handboek Informatiebeveiliging*, (101-146). Kluwer.

Conference Proceedings

de Figueiredo, S., Madhusudan, A., Reniers, V., Petkova-Nikova, S., Preneel, B. (2021). Exploring the storj network: a security analysis. In: *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, (257-264). Presented at the 36th Annual ACM Symposium on Applied Computing (SAC '21), Virtual, 22 Mar 2021-25 Mar 2021. ISBN: 978-1-4503-8104-8. doi: 10.1145/3412841.3441908

Brunner, C., Madhusudan, A., Engel, D., Preneel, B. (2021). Off-chain state channels in the energy domain. In: *2021 IEEE POWER & ENERGY SOCIETY INNOVATIVE SMART GRID TECHNOLOGIES CONFERENCE (ISGT)*. Presented at the IEEE-Power-and-Energy-Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, 16 Feb 2021-18 Feb 2021. doi: 10.1109/ISGT49243.2021.9372246

Ranea, A., Preneel, B. (2021). On Self-Equivalence Encodings in White-Box Implementations. In: O. Dunkelman, J. Jacobson, C. O'Flynn (Eds.), *Lecture Notes in Computer Science, vol 12804.*, (639-669). Presented at the Selected Areas in Cryptography, Online. Cham. ISBN: 978-3-030-81652-0. doi: 10.1007/978-3-030-81652-0_25

Yoshizawa, T., Preneel, B. (2020). Verification Schemes of Multi-SIM Devices in Mobile Communication Systems. In: *Symposium proceedings published by ACM press*, (Paper No. 91–97). Presented at the ACM International Symposium on Mobility Management and Wireless Access (MobiWac'20), Online, 16 Nov 2020-17 Nov 2020. ISBN: 978-1-4503-8119-2. doi: 10.1145/3416012.3424620

Szepieniec, A., Preneel, B. (2020). Block-Anti-Circulant Unbalanced Oil and Vinegar. In: *Selected Areas in Cryptography – SAC 2019. SAC 2019. Lecture Notes in Computer Science*: *vol. 11959*, (574-588). Presented at the Selected Areas in Cryptography – SAC 2019, Waterloo, Ontario. ISBN: 978-3-030-38470-8. doi: 10.1007/978-3-030-38471-5_23

Reniers, V., Gao, Y., Zhang, R., Viviani, P., Madhusudan, A., Lagaisse, B., Nikova, S., Van Landuyt, D., Lombardi, R., Preneel, B., Joosen, W. (2020). Authenticated and Auditable Data Sharing via Smart Contract. In: *PROCEEDINGS OF THE 35TH ANNUAL ACM SYMPOSIUM ON APPLIED COMPUTING (SAC'20)*, (324-331). Presented at the 35th Annual ACM Symposium on Applied Computing (SAC), Czech Tech Univ, ELECTR NETWORK, 30 Mar 2020-03 Apr 2020. doi: 10.1145/3341105.3373957 Open Access

Yoshizawa, T., Preneel, B. (2019). Survey of Security Aspect of V2X Standards and Related Issues. In: *Proceedings of 2019 IEEE Conference on Standards for Communications and Networking*, (161-165). Presented at the 2019 IEEE Conference on Standards for Communications and Networking, Granada, Spain, 28 Oct 2019-30 Oct 2019. ISBN: 9781728108650.

Li, C., Preneel, B. (2019). Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree. In: *Selected Areas in Cryptography – SAC 2019. SAC 2019. Lecture Notes in Computer Science, vol 11959*, (171-193). Presented at the Selected Areas in Cryptography – SAC 2019, Waterloo, ON, Canada. ISBN: 978-3-030-38470-8. doi: 10.1007/978-3-030-38471-5_8

Zhang, R., Preneel, B. (2019). Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security. In: *2019 IEEE Symposium on Security and Privacy (SP)*: *vol. 1*, (1190-1207). Presented at the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, USA, 20 May 2019-22 May 2019. ISBN: 978-1-5386-6660-9. doi: 10.1109/SP.2019.00086

Beullens, W., Szepieniec, A., Preneel, B. (2019). Public Key Compression for Constrained Linear Signature Scheme. In: *Selected Areas In Cryptography - SAC 2018*: *vol. 2018*, (300-321). Presented at the SAC 2018, Calgary, Canada. ISBN: 978-3-030-10969-1. doi: 10.1007/978-3-030-10970-7_14 Open Access

Madhusudan, A., Symeonidis, I., Mustafa, M.A., Zhang, R., Preneel, B. (2019). SC 2 Share: Smart contract for secure car sharing. In: *ICISSP 2019 - Proceedings of the 5th International Conference on Information Systems Security and Privacy*, (163-171). ISBN: 9789897583599.

Marin, E., Rua, E.A., Singelee, D., Preneel, B. (2019). On the Difficulty of Using Patient's Physiological Signals in Cryptographic Protocols. In: *PROCEEDINGS OF THE 24TH ACM SYMPOSIUM ON ACCESS CONTROL MODELS AND TECHNOLOGIES (SACMAT '19)*, (113-122). Presented at the 24th ACM Symposium on Access Control Models and Technologies (SACMAT), Ryerson Univ, Toronto, CANADA, 03 Jun 2019-06 Jun 2019. doi: 10.1145/3322431.3325099

Toli, C-A., Preneel, B. (2018). Privacy-Preserving Biometric Authentication Model for e-Finance Applications. In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP, 2018*, (353-360). Presented at the ICISSP 2018, Funchal, Madeira Portugal, 22 Jan 2018-24 Jan 2018. ISBN: 978-989-758-282-0. doi: 10.5220/0006611303530360

Symeonidis, I., SHIRAZI HOSSEINI DOKHT, F., Biczok, G., Pérez Solà, C., Preneel, B. (2018). Collateral damage of Facebook third-party applications: a comprehensive study. In: *ICT SYSTEMS SECURITY AND PRIVACY PROTECTION, SEC 2016*, (194-208). Presented at the 31st IFIP TC 11 International Conference International Conference on ICT Systems Security and Privacy Protection (SEC), Ghent, BELGIUM, 30 May 2018-01 Jun 2018. ISBN: 978-3-319-33629-9. doi: 10.1007/978-3-319-33630-5_14 Open Access

Marín Fàbregas, E., Singelée, D., Yang, B., Volskiy, V., Vandenbosch, G., Nuttin, B., Preneel, B. (2018). Securing wireless neurostimulators. In: *ACM Conference on Data and Application Security and Privacy (CODASPY)*. Presented at the ACM CODASPY, Tempe, AZ, 19 Mar 2018-21 Mar 2018. doi: 10.1145/3176258.3176310

Cleemput, S., Mustafa, M., Marin, E., Preneel, B. (2018). De-pseudonymization of Smart Metering Data: Analysis and Countermeasures. In: *Workshop on Industrial Internet of Things Security 2018*, (73-78). Presented at the Workshop on Industrial Internet of Things Security 2018, Bilbao, Spain, 04 Jun 2018-07 Jun 2018.

Luykx, A., Preneel, B. (2018). Optimal forgeries against polynomial-based MACs and GCM. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 10820 LNCS*, (445-467). ISBN: 9783319783802. doi: 10.1007/978-3-319-78381-9_17

Ruan, R., De Keulenaer, R., Maene, P., De Sutter, B., Preneel, B., Verbauwhede, I. (2017). SCM: Secure Code Memory Architecture. In: *Proceedings of the 12th ACM Symposium on Information, Computer, and Communications Security*, (12), (771-776). Presented at the ASIACCS 2017, Abu Dhabi, 01 Jan 2017-01 Jan 2017. ISBN: 978-1-4503-4944-4. doi: 10.1145/3052973.3053044 Open Access

Zhang, R., Preneel, B. (2017). Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin. In: *Lecture Notes in Computer Science*, (277-292). Presented at the RSA Conference on Cryptographer's Track (CT-RSA), San Francisco, CA, 14 Feb 2017-17 Feb 2017. doi: 10.1007/978-3-319-52153-4_16

Symeonidis, I., Aly, A., Mustafa, M., Mennink, B., Dhooghe, S., Preneel, B. (2017). SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision. In: *Lecture Notes in Computer Science*: *vol. 10493*, (475-493). Presented at the ESORICS 2017, 11 Sep 2017-15 Sep 2017.

Beullens, W., Preneel, B. (2017). Field lifting for smaller UOV public keys. In: *Lecture Notes in Computer Science*, (227-246). Presented at the INDOCRYPT 2017 (International Conference on Cryptology in India), Chennai, INDIA, 10 Dec 2017-13 Dec 2017. ISBN: 9783319716664. doi: 10.1007/978-3-319-71667-1_12

Etemad, M., Beato, F., Kupcu, A., Preneel, B. (2017). Are You Really My Friend? Efficient and Secure Friend-matching in Mobile Social Networks. In: *2017 2ND IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EUROS&PW)*, (122-131). Presented at the 2nd IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Pierre & Marie Curie Univ, Paris, FRANCE, 26 Apr 2017-30 Apr 2017. doi: 10.1109/EuroSPW.2017.61

Kim, H., Hong, S., Preneel, B., Verbauwhede, I. (2017). STBC: Side Channel Attack Tolerant Balanced Circuit with Reduced Propagation Delay. In: *IEEE Computer Society Annual Symposium on VLSI (ISVLSI 2017)*, (74-79). Presented at the ISVLSI 2017, Bochum, GERMANY, 03 Jul 2017-05 Jul 2017. doi: 10.1109/ISVLSI.2017.22

Abidin, A., Marín Fàbregas, E., Singelée, D., Preneel, B. (2017). Towards quantum distance bounding protocols. In: *RADIO FREQUENCY IDENTIFICATION AND IOT SECURITY*: *vol. 10155*, (151-162). Presented at the 12th International Workshop on Radio Frequency Identification and IoT Security (RFIDSec), Hong Kong, PEOPLES R CHINA, 30 Nov 2016-02 Dec 2016. ISBN: 978-3-319-62023-7. doi: 10.1007/978-3-319-62024-4_11 Open Access

Szepieniec, A., Beullens, W., Preneel, B. (2017). MQ Signatures for PKI. In: *Lecture Notes in Computer Science*, (0-0). Presented at the PQCRYPTO, 26 Jun 2017-28 Jun 2017.

Szepieniec, A., Preneel, B. (2017). Short Solutions to Nonlinear Systems of Equations. In: *Lecture Notes in Computer Science*: *vol. 10737*, (0-0). Presented at the NUTMIC, 11 Sep 2017-13 Sep 2017.

Toli, C-A., Aly, A., Preneel, B. (2016). A Privacy-Preserving Model for Biometric Fusion. In: S. Foresti, P. Persiano (Eds.), *Cryptology and Network Security - 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016, Proceedings*: *vol. 10052*, (743-748). Presented at the CANS, Milan, Italy, 14 Nov 2016-16 Nov 2016. ISBN: 978-3-319-48964-3. doi: 10.1007/978-3-319-48965-0_54

Marín Fàbregas, E., Singelée, D., Yang, B., Verbauwhede, I., Preneel, B. (2016). On the Feasibility of Cryptography for a Wireless Insulin Pump System. In: *ACM Conference on Data and Application Security and Privacy (CODASPY)*, (113-120). Presented at the ACM CODASPY, 09 Mar 2016-11 Mar 2016.

Kim, H., Hong, S., Preneel, B., Verbauwhede, I. (2016). Binary decision diagram to design balanced secure logic styles. In: *2016 IEEE 22nd International On-Line Testing Symposium (IOLTS 2016)*, (239-244). Presented at the IOLTS 2016, 04 Jul 2016-06 Jul 2016.

De Clercq, R., De Keulenaer, R., Coppens, B., Yang, B., De Bosschere, K., De Sutter, B., Maene, P., Preneel, B., Verbauwhede, I. (2016). SOFIA: Software and Control Flow Integrity Architecture. In: *Design, Automation and Test in Europe (DATE 2016)*, (1-6). Presented at the DATE 2016, 14 Mar 2016-18 Mar 2016.

Mühlberg, J.T., Cleemput, S., Mustafa, A.M., Van Bulck, J., Preneel, B., Piessens, F. (2016). Implementation of a high assurance smart meter using protected module architectures. In: *10th WISTP International Conference on Information Security Theory and Practice (WISTP'16)*: *vol. 9895*, (53-69). Presented at the Information Security Theory and Practice - 10th IFIP WG 11.2 International Conference (WISTP 2016), Heraklion, Greece. ISBN: 978-3-319-45930-1. doi: 10.1007/978-3-319-45931-8_4 Open Access

Razavi, K., Gras, B., Bosman, E., Preneel, B., Giuffrida, C., Bos, H. (2016). Flip Feng Shui: Hammering a Needle in the Software Stack. In: *25th USENIX Security Symposium 2016*, (Paper No. 2016). Presented at the USENIX Security Symposium 2016, 10 Aug 2016-12 Aug 2016.

Luykx, A., Preneel, B., Szepieniec, A., Yasuda, K. (2016). On the Influence of Message Length in PMAC's Security Bounds. In: *Lecture Notes in Computer Science*: *vol. 9665*, (596-621). Presented at the EUROCRYPT 2016, Vienna, AT, 08 May 2016-12 May 2016. Open Access

Cleemput, S., Mustafa, M., Preneel, B. (2016). High Assurance Smart Metering. In: *IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, (294-297). Presented at the HASE 2016, Orlando, FL, USA, 07 Jan 2016-09 Jan 2016.

Szepieniec, A., Ding, J., Preneel, B. (2016). Extension Field Cancellation: a New Central Trapdoor for Multivariate Quadratic Systems. In: *Lecture Notes in Computer Science*: *vol. 9606*, (182-196). Presented at the PQCRYPTO, 24 Feb 2016-26 Feb 2016. Open Access

Symeonidis, I., Mustafa, M., Preneel, B. (2016). Keyless Car Sharing System: A Security and Privacy Analysis. In: *IEEE International Smart Cities Conference (ISC2 2016).*, (153-159). Presented at the ISC2 2016, 12 Sep 2016-15 Sep 2016.

Abidin, A., Argones Rua, E., Preneel, B. (2016). An efficient entity authentication protocol with enhanced security and privacy properties. In: *Lecture Notes in Computer Science*: *vol. 10052*, (335-349). Presented at the CANS 2016, Milan, ITALY, 14 Nov 2016-16 Nov 2016. ISBN: 978-3-319-48964-3. doi: 10.1007/978-3-319-48965-0_20 Open Access

Marín Fàbregas, E., Mustafa, M., Singelée, D., Preneel, B. (2016). A Privacy-preserving Remote Healthcare System Offering End-to-End Security. In: *Lecture Notes in Computer Science*: *vol. 9724*, (237-250). Presented at the ADHOC-NOW 2016, 04 Jul 2016-06 Jul 2016.

Luykx, A., Preneel, B., Tischhauser, E., Yasuda, K. (2016). A MAC Mode for Lightweight Block Ciphers. In: *Lecture Notes in Computer Science*. Presented at the FSE 2016, Bochum, GERMANY, 20 Mar 2016-23 Mar 2016. doi: 10.1007/978-3-662-52993-5_3 Open Access

Preneel, B. (2016). The future of cryptography. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 9665*, (XVI-XVII). ISBN: 9783662498897.

Symeonidis, I., Tsormpatzoudi, P., Preneel, B. (2016). Collateral damage of Online Social Network Applications. In: *Proceedings of the International Conference on Information Systems Security and Privacy*, (536-541). Presented at the International Conference on Information Systems Security and Privacy (ICISSP), Rome, ITALY, 19 Feb 2016-21 Feb 2016. ISBN: 9789897581670.

Toli, C-A., Preneel, B. (2015). Provoking Security: Spoofing attacks against crypto-biometrics. In: *2015 World Congress on Internet Security WorldCIS*, (67-72). Presented at the World Congress on Internet Security (WorldCIS-2015), Dublin, Ireland, 19 Oct 2015-21 Oct 2015. ISBN: 978-1-908320-50-6. doi: 10.1109/WorldCIS.2015.7359416

Mennink, B., Preneel, B. (2015). On the Impact of Known-Key Attacks on Hash Functions. In: *Lecture Notes in Computer Science*, (59-84). Presented at the ASIACRYPT 2015, 27 Nov 2015-03 Dec 2015. Open Access

Preneel, B. (2015). Software Security: Squaring the Circle? In: *2015 IEEE/ACM 1ST INTERNATIONAL WORKSHOP ON SOFTWARE PROTECTION (SPRO)*, (1-1). Presented at the IEEE/ACM 1st International Workshop on Software Protection (SPRO), Florence, ITALY, 19 May 2015. doi: 10.1109/SPRO.2015.8

Preneel, B. (2015). Cryptography and Information Security in the Post-Snowden Era. In: *2015 IEEE/ACM 1ST INTERNATIONAL WORKSHOP ON TECHNICAL AND LEGAL ASPECTS OF DATA PRIVACY AND SECURITY TELERISE 2015*, (1-1). Presented at the International Workshop on TEchnical and LEgal aspects of data pRIvacy and SEcurity, Florence, ITALY, 18 May 2015-18 May 2015. doi: 10.1109/TELERISE.2015.8

Schroé, W., Mennink, B., Andreeva, E., Preneel, B. (2015). Forgery and Subkey Recovery on CAESAR candidate iFeed. In: *Lecture Notes in Computer Science*, (197-204). Presented at the SAC 2015 (Selected Areas in Cryptography), Mount Allison University in Sackville, New Brunswick, Canada, 12 Aug 2015-14 Aug 2015. ISBN: 9783319313009. doi: 10.1007/978-3-319-31301-6_11 Open Access

Mennink, B., Preneel, B. (2015). On the XOR of Multiple Random Permutations. In: *Lecture Notes in Computer Science*, (619-634). Presented at the 13th International Conference on Applied Cryptography and Network Security (ACNS 2015), Columbia University, New York, 02 Jun 2015-05 Jun 2015. ISBN: 9783319281650. doi: 10.1007/978-3-319-28166-7_30 Open Access

Ors, B., Preneel, B. (2015). Cryptography and information security in the balkans: First international conference, BalkanCryptSec 2014 Istanbul, Turkey, October 16-17, 2014 revised selected papers. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 9024*. ISBN: 9783319213552. doi: 10.1007/978-3-319-21356-9

Mouha, N., Mennink, B., Van Herrewege, A., Watanabe, D., Preneel, B., Verbauwhede, I. (2014). Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In: *Lecture Notes in Computer Science*: *vol. 8781*, (306-323). Presented at the SAC 2014, 14 Aug 2014-15 Aug 2014. ISBN: 978-3-319-13050-7. Open Access

Mennink, B., Preneel, B. (2014). Breaking and Fixing Cryptophia's Short Combiner. In: *Lecture Notes in Computer Science*: *vol. 8813*, (50-63). Presented at the CANS 2014, Heraklion, Greece, 22 Oct 2014-24 Oct 2014. Open Access

Weng, L., Preneel, B. (2014). On encryption and authentication of the DC DCT coefficient. In: *IEEE Software, Special Issue on Software Protection*: *vol. 51* (8), (375-379).

Herrmann, M., Zhang, R., Ning, K-C., Diaz, C., Preneel, B. (2014). Censorship-Resistant and Privacy-Preserving Distributed Web Search. In: *14th IEEE International Conference on Peer-to-Peer Computing (P2P 2014)*. Presented at the P2P 2014, 08 Sep 2014-12 Sep 2014.

Toli, C-A., Preneel, B. (2014). A Survey on Multimodal Biometrics and the Protection of their Templates. In: *Privacy and Identity Management for the Future Internet in the Age of Globalisation - 9th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, Patras, Greece, September 7-12, 2014, Revised Selected Papers*: *vol. 457*, (169-184). Presented at the 9th IFIP International Summer School, Privacy and Identity Management for the Future Internet in the Age of Globalisation, 09 Jul 2014-12 Jul 2014. ISBN: 978-3-319-18620-7. doi: 10.1007/978-3-319-18621-4_12

Preneel, B. (2014). Lightweight and Secure Cryptographic Implementations for the Internet of Things. In: D. Naccache, D. Sauveron (Eds.), *INFORMATION SECURITY THEORY AND PRACTICE: SECURING THE INTERNET OF THINGS*: *vol. 8501*, (XIII-XIV). Presented at the 8th IFIP WG 11.2 International Workshop on Information Security Theory and Practice (WISTP), Heraklion, GREECE, 30 Jun 2014-02 Jul 2014. ISBN: 978-3-662-43825-1. (URL)

Wu, H., Preneel, B. (2014). AEGIS: A Fast Authenticated Encryption Algorithm. In: T. Lange, K. Lauter, P. Lisonek (Eds.), *SELECTED AREAS IN CRYPTOGRAPHY - SAC 2013*: *vol. 8282*, (185-201). Presented at the 20th International Conference on Selected Areas in Cryptography, Simon Fraser Univ, Burnaby, CANADA, 14 Aug 2013-16 Aug 2013. ISBN: 978-3-662-43413-0. doi: 10.1007/978-3-662-43414-7_10

Ramos Araújo Beato, F., Conti, M., Preneel, B., Vettore, D. (2014). VirtualFriendship: Hiding interactions on Online Social Networks. In: *IEEE Conference on Communications and Network Security*, (328-336). Presented at the CNS 2014, 29 Oct 2014-31 Oct 2014.

Preneel, B., Ikonomou, D. (2014). Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012 Limassol, Cyprus, October 10-11, 2012 Revised Selected Papers 13. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 8319*. ISBN: 9783642540684. doi: 10.1007/978-3-642-54069-1

Herrmann, M., Rial, A., Diaz, C., Preneel, B. (2014). Practical Privacy-Preserving Location-Sharing Based Services with Aggregate Statistics. In: *Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2014)*, (87-98). Presented at the WiSec 2014, 23 Jul 2014-25 Jul 2014.

Preneel, B. (2013). The SHA-3 competition: Lessons learned. In: *SIN 2013 - Proceedings of the 6th International Conference on Security of Information and Networks*, (16-19). ISBN: 9781450324984. doi: 10.1145/2523514.2523592

Van Wallendael, G., De Cock, J., Van Leuven, S., Lampert, P., Preneel, B., Van de Walle, R. (2013). Format Compliant Encryption Techniques for HEVC. In: *IEEE International Conference on Image Processing*, (4583-4587). Presented at the IEEE International Conference on Image Processing, Melbourne, VIC, AU, 15 Sep 2013-18 Sep 2013. doi: 10.1109/ICIP.2013.6738944

Ottoy, G., Lapon, J., Naessens, V., Preneel, B., De Strycker, L. (2013). Dedicated Hardware for Attribute-Based Credential Verification. In: B. De Decker, J. Dittmann, K. Christian, V. Claus (Eds.), *Communications and Multimedia Security*: *vol. 8099*, (50-65). Presented at the 14th IFIP TC 6/TC 11 International Conference, CMS 2013, Magdeburg, Germany, 25 Sep 2013-26 Sep 2013. doi: 10.1007/978-3-642-40779-6_4

Noorman, J., Agten, P., Daniels, W., Strackx, R., Van Herrewege, A., Huygens, C., Preneel, B., Verbauwhede, I., Piessens, F. (2013). Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base. In: *22nd USENIX Security symposium*, (479-494). Presented at the USENIX Security Symposium, Washington D.C., 14 Aug 2013-16 Aug 2013. Open Access

Sekar, G., Mouha, N., Preneel, B. (2013). Meet-in-the-Middle Attacks on Reduced-Round GOST. Presented at the Workshop on Current Trends in Cryptology (CTCrypt 2013), Ekaterinburg, Russia, 23 Jun 2013-24 Jun 2013. Open Access

De Meyer, L., Bilgin, B., Preneel, B. (2013). Extended Analysis of DES S-boxes. In: *Proceedings of the 34th Symposium on Information Theory in the Benelux*, (21-30). Presented at the 34th Symposium on Information Theory in the Benelux, Leuven, Belgium, 30 May 2013-31 May 2013. ISBN: 9781627487375.

Ottoy, G., Preneel, B., Goemaere, J.P., De Strycker, L. (2013). Flexible Design of a Modular Simultaneous Exponentiation Core for Embedded Platforms. In: *Lecture Notes in Computer Science*: *vol. 7806*, (115-121). Presented at the ARC 2013, 25 Mar 2013-27 Mar 2013.

Lepoint, T., Rivain, M., De Mulder, Y., Roelse, P., Preneel, B. (2013). Two Attacks on a White-Box AES Implementation. In: *Lecture Notes in Computer Science*: *vol. 8282*, (265-285). Presented at the SAC 2013, Simon Fraser Univ, Burnaby, CANADA, 14 Aug 2013-16 Aug 2013. Open Access

Beato, F., Conti, M., Preneel, B. (2013). Friend in the Middle (FiM): Tackling De-Anonymization in Social Networks. In: *2013 IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS (PERCOM WORKSHOPS)*, (279-284). Presented at the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), San Diego, CA, 18 Mar 2013-22 Mar 2013. ISBN: 978-1-4673-5075-4. (URL)

Herrmann, M., Troncoso, C., Diaz, C., Preneel, B. (2013). Optimal Sporadic Location Privacy Preserving Systems in Presence of Bandwidth Constraints. In: *Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society (WPES 2013)*, (167-178). Presented at the WPES 2013, 04 Nov 2013-04 Nov 2013.

Acar, G., Juarez, M., Nikiforakis, N., Diaz, C., Gürses, S., Piessens, F., Preneel, B. (2013). FPDetective: Dusting the web for fingerprinters. In: *20th ACM Conference on Computer and Communications Security*, (1129-1140). Presented at the CCS 2013, 04 Nov 2013-08 Nov 2013. Open Access

Strackx, R., Noorman, J., Verbauwhede, I., Preneel, B., Piessens, F. (2013). Protected software module architectures. In: H. Reimer, N. Pohlman, W. Schneider (Eds.), *ISSE 2013 Securing Electronic Business Processes*, (241-251). Presented at the Information Security Solutions Europe. Open Access

Tapiador, J.E., Li, R., Preneel, B., Duan, G. (2012). Message from ACS-2012 workshop chairs. In: *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*. ISBN: 9780769547459. doi: 10.1109/TrustCom.2012.306

Uhsadel, L., Ullrich, M., Verbauwhede, I., Preneel, B. (2012). Interface design for mapping a variety of RSA exponentiation algorithms on a HW/SW co-design platform. In: *23rd IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2012)*, (109-116). Presented at the ASAP 2012, 09 Jul 2012-11 Jul 2012. ISBN: 978-0-7695-4768-8.

Mennink, B., Preneel, B. (2012). Hash Functions Based on Three Permutations: A Generic Security Analysis. In: *Lecture Notes in Computer Science*: *vol. 7417*, (330-347). Presented at the CRYPTO 2012, 19 Aug 2012-23 Aug 2012. Open Access

Preneel, B. (2012). It's Not My Fault On - Fault Attacks on Symmetric Cryptography. In: G. Bertoni, B. Gierlichs (Eds.), *2012 WORKSHOP ON FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY (FDTC)*, (57-60). Presented at the 9th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Leuven, BELGIUM, 09 Sep 2012. doi: 10.1109/FDTC.2012.20

Sun, Y., Tischhauser, E., Wang, M., Preneel, B. (2012). A Model for Structure Attacks, with Applications to PRESENT and Serpent. In: *Lecture Notes in Computer Science*: *vol. 7549*, (49-68). Presented at the FSE 2012, 19 Mar 2012-21 Mar 2012.

Van der Leest, V., Preneel, B., Van der Sluis, E. (2012). Soft Decision Error Correction for Compact Memory-Based PUFs Using a Single Enrollment. In: *Lecture Notes in Computer Science*: *vol. 7428*, (268-282). Presented at the CHES 2012, 09 Sep 2012-12 Sep 2012.

Velichkov, V., Mouha, N., De Cannière, C., Preneel, B. (2012). UNAF: A Special Set of Additive Differences with Application to the Differential Analysis of ARX. In: *Lecture Notes in Computer Science*: *vol. 7549*, (287-305). Presented at the FSE 2012, 19 Mar 2012-21 Mar 2012. Open Access

De Mulder, Y., Roelse, P., Preneel, B. (2012). Cryptanalysis of the Xiao - Lai White-Box AES Implementation. In: *Lecture Notes in Computer Science*: *vol. 7707*, (34-49). Presented at the SAC 2012, 16 Aug 2012-17 Aug 2012. Open Access

Weng, L., Darazi, R., Preneel, B., Macq, B., Dooms, A. (2012). Robust image content authentication using perceptual hashing and watermarking. In: *Lecture Notes in Computer Science*: *vol. 7674*, (315-326). Presented at the Pacific-rim Conference on Multimedia, 04 Dec 2012-06 Dec 2012. Open Access

Mavrogiannopoulos, N., Vercauteren, F., Velichkov, V., Preneel, B. (2012). A cross-protocol attack on the TLS protocol. In: *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS 2012)*, (62-71). Presented at the CCS 2012, 16 Oct 2012-18 Oct 2012.

Weng, L., Braeckman, G., Dooms, A., Preneel, B. (2012). Robust image content authentication with tamper location. In: *Proc. of IEEE International Conference on Multimedia and Expo 2012*, (380-385). Presented at the ICME 2012, 09 Jul 2012-13 Jul 2012.

Andreeva, E., Mennink, B., Preneel, B., Skrobot, M. (2012). Security Analysis and Comparison of the SHA-3 Finalists BLAKE, Grøstl, JH, Keccak, and Skein. In: *Lecture Notes in Computer Science*: *vol. 7374*, (287-305). Presented at the AFRICACRYPT 2012, 10 Jul 2012-12 Jul 2012. Open Access

Chen, J., Wang, M., Preneel, B. (2012). Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT. In: *Lecture Notes in Computer Science*: *vol. 7374*, (117-137). Presented at the AFRICACRYPT 2012, 10 Jul 2012-12 Jul 2012.

Mavrogiannopoulos, N., Trmac, M., Preneel, B. (2012). A Linux kernel cryptographic framework: Decoupling cryptographic keys from applications. In: *Proceedings of the 2012 ACM Symposium on Applied Computing*, (1435-1442). Presented at the ACM Symposium on Applied Computing, 26 Mar 2012-30 Mar 2012.

Uhsadel, L., Ullrich, M., Preneel, B., Verbauwhede, I. (2012). HW/SW co-design of RSA on 8051. In: *European Workshop on Microelectronics Education*, (41-44). Presented at the EWME, 09 May 2012-11 May 2012.

Mouha, N., Sekar, G., Preneel, B. (2011). Challenging the Increased Resistance of Regular Hash Functions Against Birthday Attacks. In: C. Rechberger (Eds.), (1-18). Presented at the ECRYPT II Hash Workshop, Tallinn, Estonia, 19 May 2011-20 May 2011. Open Access

Andreeva, E., Mennink, B., Preneel, B. (2011). Security reductions of the second round SHA-3 candidates. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 6531 LNCS*, (39-53). ISBN: 9783642181771. doi: 10.1007/978-3-642-18178-8-5

Ideguchi, K., Tischhauser, E., Preneel, B. (2011). Improved collision attacks on the reduced-round Grøstl hash function. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 6531 LNCS*, (1-16). ISBN: 9783642181771. doi: 10.1007/978-3-642-18178-8-1

Hermans, J., Pashalidis, A., Vercauteren, F., Preneel, B. (2011). A New RFID Privacy Model. In: *Lecture Notes in Computer Science*: *vol. 6879*, (568-587). Presented at the ESORICS 2011, 12 Sep 2011-14 Sep 2011. Open Access

Ottoy, G., Martens, J., Saeys, N., Preneel, B., De Strycker, L., Goemaere, J-P., Hamelinckx, T. (2011). A Modular Test Platform for Evaluation of Security Protocols in NFC Applications. In: B. De Decker (Eds.), *Lecture Notes in Computer Science*: *vol. 7025*, (171-177). Presented at the CMS 2011, Ghent, 19 Oct 2011-21 Oct 2011. doi: 10.1007/978-3-642-24712-5_15

De Mulder, Y., Wouters, K., Preneel, B. (2011). A Privacy-preserving ID-based Group Key Agreement Scheme applied in VPAN. In: *Lecture Notes in Computer Science*: *vol. 6543*, (214-222). Presented at the SOFSEM 2011, 22 Jan 2011-28 Jan 2011. ISBN: 978-3-642-18380-5. Open Access

De Cannière, C., Mouha, N., Velichkov, V., Preneel, B. (2011). The Additive Differential Probability of ARX. In: *Lecture Notes in Computer Science*: *vol. 6733*, (342-358). Presented at the FSE 2011, 13 Feb 2011-16 Feb 2011. Open Access

Wang, M., Sun, Y., Mouha, N., Preneel, B. (2011). Algebraic Techniques in Differential Cryptanalysis Revisited. In: *Lecture Notes in Computer Science*, (120-141). Presented at the ACISP 2011, 11 Jul 2011-13 Jul 2011. Open Access

Weng, L., Preneel, B. (2011). A secure perceptual hash algorithm for image content authentication. In: *Lecture Notes in Computer Science*: *vol. 7025*, (108-121). Presented at the CMS 2011, 19 Oct 2011-21 Oct 2011. Open Access

Nguyen, D., Weng, L., Preneel, B. (2011). Radon Transform-Based Secure Image Hashing. In: *Lecture Notes in Computer Science*: *vol. 7025*, (186-193). Presented at the CMS 2011, 19 Oct 2011-21 Oct 2011. Open Access

Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B., Yoshida, H. (2011). A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW. In: K.H. Rhee, D.H. Nyang (Eds.), *INFORMATION SECURITY AND CRYPTOLOGY - ICISC 2010*: *vol. 6829*, (151-+). Presented at the 13th Annual International Conference on Information Security and Cryptology (ICISC 2010), Cung-Ang Univ, Seoul, SOUTH KOREA, 01 Dec 2010-03 Dec 2010. ISBN: 978-3-642-24209-0. (URL)

Weng, L., Preneel, B. (2011). Image distortion estimation by hash comparison. In: *Lecture Notes in Computer Science*, (62-72). Presented at the MMM 2011, 05 Jan 2011-07 Jan 2011. ISBN: 978-3-642-17831-3. Open Access

Preneel, B. (2011). The NIST SHA-3 Competition: A Perspective on the Final Year. In: *Lecture Notes in Computer Science*: *vol. 6737*, (383-386). Presented at the AFRICACRYPT 2011, 05 Jul 2011-07 Jul 2011. ISBN: 978-3-642-21969-6. Open Access

Preneel, B., Yoshida, H., Watanabe, D. (2011). Finding Collisions for Reduced Luffa-256 v2. In: *Lecture Notes in Computer Science*: *vol. 6812*, (423-427). Presented at the ACISP 2011, Melbourne, Australia, 11 Jul 2011-13 Jul 2011. doi: 10.1007/978-3-642-22497-3_29

Mouha, N., Wang, Q., Gu, D., Preneel, B. (2011). Differential and Linear Cryptanalysis using Mixed-Integer Linear Programming. In: *Lecture Notes in Computer Science*: *vol. 7537*, (57-76). Presented at the China International Conference on Information Security and Cryptology (Inscrypt) 2011, 30 Nov 2011-03 Dec 2011. Open Access

Sekar, G., Preneel, B. (2011). Practical Attacks on a Cryptosystem Proposed in Patent WO/2009/066313. In: *Lecture Notes in Computer Science*: *vol. 7115*, (1-12). Presented at the WISA 2011, 22 Aug 2011-24 Aug 2011.

Sekar, G., Mouha, N., Velichkov, V., Preneel, B. (2011). Meet-in-the-Middle Attacks on Reduced-Round XTEA. In: *Lecture Notes in Computer Science*: *vol. 6558*, (250-267). Presented at the CT-RSA 2011, 14 Feb 2011-18 Feb 2011. Open Access

Strackx, R., Piessens, F., Preneel, B. (2010). Efficient isolation of trusted subsystems in embedded systems. In: S. Jajodia, J. Zhou (Eds.), *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering: Security and Privacy in Communication Networks*: *vol. 50*, (344-361). Presented at the International ICST Conference, SecureComm 2010, Singapore, 07 Sep 2010-09 Sep 2010. ISBN: 978-3-642-16160-5. doi: 10.1007/978-3-642-16161-2_20 Open Access

Balasch, J., Verbauwhede, I. (2010). An Embedded Platform for Privacy-Friendly Road Charging Applications. In: *Design, Automation and Test in Europe (DATE 2010)*, (867-872). Presented at the DATE 2010, 08 Mar 2010-12 Mar 2010.

Lee, Y.K., Batina, L., Singelee, D., Preneel, B., Verbauwhede, I. (2010). Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware. In: A.R. Sadeghi, D. Naccache (Eds.), *TOWARDS HARDWARE-INTRINSIC SECURITY: FOUNDATIONS AND PRACTICE*, (237-257). Presented at the Dagstuhl Seminar on Foundations for Forgery-Resilient Cryptographic Hardware, Schloss Dagstuhl Leibniz Ctr Informat, Wadern, GERMANY, 05 Jul 2009-08 Jul 2009. ISBN: 978-3-642-14451-6. doi: 10.1007/978-3-642-14452-3_11

Gierlichs, B., Batina, L., Preneel, B., Verbauwhede, I. (2010). Revisiting Higher-Order DPA Attacks: Multivariate Mutual Information Analysis. In: *Lecture Notes in Computer Science*: *vol. 5985*, (221-234). Presented at the CT-RSA 2010, 01 Mar 2010-05 Mar 2010. Open Access

Hermans, J., Schneider, M., Buchmann, J., Preneel, B., Vercauteren, F. (2010). Parallel Shortest Lattice Vector Enumeration on Graphics Cards. In: *Lecture Notes in Computer Science*: *vol. 6055*, (52-68). Presented at the AFRICACRYPT 2010, 03 May 2010-06 May 2010. Open Access

Hermans, J., Vercauteren, F., Preneel, B. (2010). Speed records for NTRU. In: *Lecture Notes in Computer Science*: *vol. 5985*, (73-88). Presented at the CT-RSA 2010, 01 Mar 2010-05 Mar 2010. Open Access

Andreeva, E., Mennink, B., Preneel, B. (2010). Security Reductions of the Second Round SHA-3 Candidates. In: *Lecture Notes in Computer Science*: *vol. 6531*, (39-53). Presented at the ISC 2010, Florida Atlantic Univ, Math Sci Dept, Ctr Cryptol & Informat Seur, Boca Raton, FL, 25 Oct 2010-28 Oct 2010. ISBN: 978-3-642-18177-1. doi: 10.1007/978-3-642-18178-8_5 Open Access

Andreeva, E., Mennink, B., Preneel, B. (2010). On the Indifferentiability of the Grøstl Hash Function. In: *Lecture Notes in Computer Science*: *vol. 6280*, (88-105). Presented at the SCN 2010, 13 Sep 2010-15 Sep 2010. Open Access

Simoens, K., Peeters, R., Preneel, B. (2010). Increased Resilience in Threshold Cryptography: Sharing a Secret with Devices That Cannot Store Shares. In: *Lecture Notes in Computer Science*: *vol. 6487*, (116-135). Presented at the Pairing 2010, Yamanaka Hot Spring, Japan, 13 Dec 2010-15 Dec 2010. ISBN: 978-3-642-17454-4. Open Access

De Mulder, Y., Wyseur, B., Preneel, B. (2010). Cryptanalysis of a Perturbated White-box AES Implementation. In: *Lecture Notes in Computer Science*: *vol. 6498*, (292-310). Presented at the INDOCRYPT 2010, 12 Dec 2010-15 Dec 2010. Open Access

Preneel, B. (2010). Cryptographic Hash Functions: Theory and Practice. In: *Lecture Notes in Computer Science*: *vol. 6476*, (1-3). Presented at the ICICS 2010, Barcelona, Spain, 15 Dec 2010-17 Dec 2010. Open Access

Ideguchi, K., Tischhauser, E., Preneel, B. (2010). Improved Collision Attacks on the Reduced-Round Grøstl Hash Function. In: *Lecture Notes in Computer Science*: *vol. 6531*, (1-16). Presented at the ISC 2010, 25 Oct 2010-28 Oct 2010.

Mouha, N., Velichkov, V., De Cannière, C., Preneel, B. (2010). The Differential Analysis of S-functions. In: *Lecture Notes in Computer Science*, (36-56). Presented at the SAC 2010, 12 Aug 2010-13 Aug 2010. ISBN: 978-3-642-19573-0. Open Access

Preneel, B. (2010). Cryptographic Hash Functions: Theory and Practice. In: *Lecture Notes in Computer Science*: *vol. 6498*, (115-117). Presented at the INDOCRYPT 2010, 12 Dec 2010-15 Dec 2010. Open Access

Rial Duran, A., Preneel, B. (2010). Optimistic Fair Priced Oblivious Transfer. In: *Lecture Notes in Computer Science*: *vol. 6055*, (131-147). Presented at the AFRICACRYPT 2010, 03 May 2010-06 May 2010. Open Access

Preneel, B. (2010). Cryptography for Network Security: Failures, Successes and Challenges. In: *Lecture Notes in Computer Science*: *vol. 6258*, (36-54). Presented at the MMM-ACNS 2010, 08 Sep 2010-10 Sep 2010. Open Access

Preneel, B. (2010). The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition. In: *Lecture Notes in Computer Science*: *vol. 5985*, (1-14). Presented at the CT-RSA 2010, 01 Mar 2010-05 Mar 2010. Open Access

Weng, L., Preneel, B. (2010). From image hashing to video hashing. In: *Lecture Notes in Computer Science*: *vol. 5916*, (662-668). Presented at the MMM 2010, 06 Jan 2010-08 Jan 2010. Open Access

(2010). Communications and multimedia security. In: B. De Decker, I. Schaumüller (Eds.), *vol. 6109*. Presented at the CMS2010, Linz, Autria. Berlin, Germany: Springer. ISBN: 3-642-13240-5. doi: 10.1007/978-3-642-13241-4 Open Access

Ottoy, G., Hamelinckx, T., Preneel, B., De Strycker, L., Goemaere, J.P. (2010). AES Data Encryption in a ZigBee Network: Software or Hardware? In: A.U. Schmidt, G. Russello, A. Lioy, N.R. Prasad, S. Lian (Eds.), (Paper No. 5), (163-173). Presented at the Second International ICST Conference, MobiSec 2010, Catania/Sicily, 27 May 2010-28 May 2010. Springer.

Fan, J., Guo, X., De Mulder, E., Schaumont, P., Preneel, B., Verbauwhede, I. (2010). State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures. In: *3rd IEEE International Workshop on Hardware-Oriented Security and Trust - HOST 2010*, (76-87). Presented at the 3rd HOST 2010, 13 Jun 2010-14 Jun 2010.

Simoens, K., Chang, C-M., Preneel, B. (2010). Reversing Protected Minutiae Vicinities. In: A. Ross, K-A. Toh, S. Sarkar (Eds.), *IEEE Fourth International Conference on Biometrics: Theory, Applications and Systems (BTAS 10)*, (1-8). Presented at the BTAS 2010, Washington DC, 27 Sep 2010-29 Sep 2010. Piscataway, NJ.

Weng, L., Preneel, B. (2010). A novel video hash algorithm. In: *Proceedings of the International Conference on Multimedia*, (739-742). Presented at the International Multimedia Conference, 25 Oct 2010-29 Oct 2010.

Cappaert, J., Preneel, B. (2010). A General Model for Hiding Control Flow. In: *Proceedings of the 10th ACM workshop on Digital Rights Management (DRM 2010)*, (35-42). Presented at the ACM Workshop on Digital Rights Management, 04 Oct 2010-04 Oct 2010.

Balasch, J., Rial Duran, A., Gonzalez Troncoso, C., Geuens, C., Preneel, B., Verbauwhede, I. (2010). PrETP: Privacy-Preserving Electronic Toll Pricing. In: *19th USENIX Security Symposium 2010*, (63-78). Presented at the USENIX Security Symposium 2010, 11 Aug 2010-13 Aug 2010.

Mouha, N., Velichkov, V., De Cannière, C., Preneel, B. (2010). Toolkit for the Differential Cryptanalysis of ARX-based Cryptographic Constructions. In: *Workshop on Tools for Cryptanalysis 2010*, (125-126). Presented at the Workshop on Tools for Cryptanalysis 2010, 22 Jun 2010-23 Jun 2010.

Peeters, R., Singelée, D., Preneel, B. (2010). Threshold-Based Distance Bounding. In: *International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use 2010*, (24-30). Presented at the International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use 2010, 17 May 2010-17 May 2010.

Simoens, K., Tuyls, P., Preneel, B. (2009). Privacy Weaknesses in Biometric Sketches. In: *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, (188-203). Presented at the SP 2009, Oakland, CA, USA, 17 May 2009-20 May 2009. doi: 10.1109/SP.2009.24

Aerts, W., De Mulder, E., Preneel, B., Vandenbosch, G., Verbauwhede, I. (2009). 'Designing Maximal Resolution Loop Sensors for Cryptographic Analysis. In: *3rd European Conference on Antennas and Propagation (EuCAP 2009)*, (1-5). Presented at the EuCAP 2009, Berlin, Germany, 01 Mar 2009-01 Mar 2009.

Sterckx, M., Gierlichs, B., Preneel, B., Verbauwhede, I. (2009). Efficient Implementation of Anonymous Credentials on Java Card Smart Cards. In: *1st IEEE International Workshop on Information Forensics and Security (WIFS 2009)*, (106-110). Presented at the WIFS 2009, 06 Dec 2009-09 Dec 2009.

De Mulder, E., Gierlichs, B., Preneel, B., Verbauwhede, I. (2009). Practical DPA Attacks on MDPL. In: *1st IEEE International Workshop on Information Forensics and Security (WIFS 2009)*, (191-195). Presented at the WIFS 2009, London, 06 Dec 2009-09 Dec 2009.

De Mulder, E., Aerts, W., Preneel, B., Verbauwhede, I., Vandenbosch, G. (2009). Case Study : A Class E Power Amplifier for ISO-14443A. In: *PROCEEDINGS OF THE 2009 IEEE SYMPOSIUM ON DESIGN AND DIAGNOSTICS OF ELECTRONIC CIRCUITS AND SYSTEMS*, (20-+). Presented at the IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems, Liberec, CZECH REPUBLIC, 15 Apr 2009-17 Apr 2009. ISBN: 978-1-4244-3339-1. doi: 10.1109/DDECS.2009.5012091

Gierlichs, B., De Mulder, E., Preneel, B., Verbauwhede, I. (2009). Empirical Comparison of Side Channel Analysis Distinguishers on DES in Hardware. In: *European Conference on Circuit Theory and Design (ECCTD 2009)*, (391-394). Presented at the ECCTD 2009, 23 Aug 2009-27 Aug 2009.

Peeters, R., Kohlweiss, M., Preneel, B., Sulmon, N. (2009). Threshold things that think: usable authorization for resharing. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*, (Paper No. 18), (111-124). Presented at the Symposium on Usable Privacy and Security, Mountain View, California, 23 Apr 2009-24 Apr 2009. New York, USA. ISBN: 978-1-60558-736-3. Open Access

Saxena, A., Wyseur, B., Preneel, B. (2009). Towards Security Notions for White-Box Cryptography. In: *Lecture Notes in Computer Science*: *vol. 5735*. Presented at the ISC 2009, 07 Sep 2009-09 Sep 2009. Open Access

Van Damme, G., Wouters, K., Karahan, H., Preneel, B. (2009). Offline NFC Payments with Electronic Vouchers. In: *Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds (MobiHeld 2009)*, (25-30). Presented at the MobiHeld 2009, 17 Aug 2009-17 Aug 2009.

Indesteege, S., Preneel, B. (2009). Coding Theory and Hash Function Design. In: S. Dodunekov, S. Nikova, B. Preneel, V. Rijmen (Eds.), (63-68). IOS Press.

Mouha, N., Sekar, G., Aumasson, J-P., Peyrin, T., Thomsen, S., Turan, M., Preneel, B. (2009). Cryptanalysis of the ESSENCE Family of Hash Functions. In: *Lecture Notes in Computer Science*: *vol. 6151*, (15-34). Presented at the Inscrypt 2009, 12 Dec 2009-15 Dec 2009. Open Access

Weng, L., Preneel, B. (2009). Shape-based features for image hashing. In: *Proc. of IEEE International Conference on Multimedia and Expo 2009*. Presented at the ICME 2009, 28 Jun 2009-03 Jul 2009.

Mouha, N., De Cannière, C., Indesteege, S., Preneel, B. (2009). Finding Collisions for a 45-Step Simplified HAS-V. In: *Lecture Notes in Computer Science*: *vol. 5932*, (206-225). Presented at the WISA 2009, 25 Aug 2009-27 Aug 2009. Open Access

Indesteege, S., Mendel, F., Schläffer, M., Preneel, B. (2009). Practical Collisions for SHAMATA-256. In: *Lecture Notes in Computer Science*: *vol. 5867*, (1-15). Presented at the SAC 2009, 13 Aug 2009-14 Aug 2009. Open Access

Aumasson, J-P., Dunkelman, O., Indesteege, S., Preneel, B. (2009). Cryptanalysis of Dynamic SHA(2). In: *Lecture Notes in Computer Science*: *vol. 5867*, (415-432). Presented at the SAC 2009, 13 Aug 2009-14 Aug 2009. Open Access

Indesteege, S., Preneel, B. (2009). Practical Collisions for EnRUPT. In: *Lecture Notes in Computer Science*: *vol. 5665*, (246-259). Presented at the FSE 2009, 22 Feb 2009-25 Feb 2009. Open Access

Rial Duran, A., Kohlweiss, M., Preneel, B. (2009). Universally Composable Adaptive Priced Oblivious Transfer. In: *Lecture Notes in Computer Science*: *vol. 5671*, (231-247). Presented at the Pairing 2009, 12 Aug 2009-14 Aug 2009. Open Access

Deng, M., Bianchi, T., Piva, A., Preneel, B. (2009). An Efficient Buyer-Seller Watermarking Protocol Based on Composite Signal Representation. In: *MM&SEC'09: PROCEEDINGS OF THE 2009 ACM SIGMM MULTIMEDIA AND SECURITY WORKSHOP*, (9-18). Presented at the 11th ACM Multimedia and Security Workshop, Princeton, NJ, 07 Sep 2009-08 Sep 2009. ISBN: 978-1-60558-492-8. (URL)

Nakahara, J., Sekar, G., de Freitas, D., Chiann, C., de Souza, R., Preneel, B. (2009). A New Approach to chi^2 Cryptanalysis of Block Ciphers. In: *Lecture Notes in Computer Science*: *vol. 5735*, (1-16). Presented at the ISC 2009, 07 Sep 2009-09 Sep 2009. Open Access

Sekar, G., Preneel, B. (2009). Improved Distinguishing Attacks on HC-256. In: *Lecture Notes in Computer Science*: *vol. 5824*, (38-52). Presented at the IWSEC 2009, 28 Oct 2009-30 Oct 2009. Open Access

Preneel, B. (2009). The State of Hash Functions and the NIST SHA-3 Competition. In: M. Yung, P. Liu, D.D. Lin (Eds.), *INFORMATION SECURITY AND CRYPTOLOGY*: *vol. 5487*, (1-11). Presented at the 4th International Conference on Information Security and Cryptology (Inscript 2008), Beijing, PEOPLES R CHINA, 14 Dec 2008-17 Dec 2008. ISBN: 978-3-642-01439-0. (URL)

Wan, Z., Ren, K., Zhu, B., Preneel, B., Gu, M. (2009). Anonymous user communication for privacy protection in wireless metropolitan mesh networks. In: *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS 2009)*, (368-371). Presented at the ASIACCS 2009, 10 Mar 2009-12 Mar 2009.

Preneel, B. (2009). The Future of Cryptographic Algorithms. In: *Lecture Notes in Computer Science*: *vol. 5824*, (1-2). Presented at the IWSEC 2009, 28 Oct 2009-30 Oct 2009.

De Mulder, E., Aerts, W., Preneel, B., Vandenbosch, G., Verbauwhede, I. (2009). A class E Power Amplifier for ISO-14443A. In: *12th IEEE Workshop on Design and Diagnostics of Electronic Circuits & Systems (DDECS 2009)*, (20-23). Presented at the DDECS 2009, 15 Apr 2009-17 Apr 2009.

Indesteege, S., Preneel, B. (2009). Practical Preimages for Maraca. In: *Proceedings of the 30th Symposium on Information Theory in the Benelux*, (119-126). Presented at the 30th Symposium on Information Theory in the Benelux, 28 May 2009-29 May 2009.

Peeters, R., Kohlweiss, M., Preneel, B. (2009). Threshold Things That Think: Authorisation for Resharing. In: *Proceedings of iNetSec 2009 – Open Research Problems in Network Security*, (111-124). Presented at the iNetSec 2009, 23 Apr 2009-24 Apr 2009.

Troncoso, C., De Cock, D., Preneel, B. (2008). Improving secure long-term archival of digitally signed documents. In: *Proceedings of the ACM Conference on Computer and Communications Security*, (27-36). ISBN: 9781605582993. doi: 10.1145/1456469.1456476

Singelée, D., Braem, B., Latre, B., Peeters, M., De Cleyn, P., Blondia, C., De Soete, M., Moerman, I., Preneel, B. (2008). A Secure Cross-layer Protocol for Multihop Wireless Body Area Networks. In: *Lecture Notes in Computer Science*: *vol. 5198*, (94-107). Presented at the ADHOC-NOW 2008, 10 Sep 2008-12 Sep 2008. Open Access

Gonzalez Troncoso, C., Gierlichs, B., Preneel, B., Verbauwhede, I. (2008). Perfect Matching Disclosure Attacks. In: *Lecture Notes in Computer Science*: *vol. 5134*, (2-23). Presented at the PETS 2008, 23 Jul 2008-25 Jul 2008. Open Access

Knezevic, M., Velichkov, V., Preneel, B., Verbauwhede, I. (2008). On the Practical Performance of Rateless Codes. In: *International Conference on Wireless Information Networks and Systems*, (173-176). Presented at the WINSYS 2008, 26 Jul 2008-29 Jul 2008.

Deng, M., Scandariato, R., De Cock, D., Preneel, B., Joosen, W. (2008). Identity in federated electronic healthcare. In: *IFIP Wireless Days - 6th IFIP Network Control conference (Netcon 2008)*, (1-5). Presented at the IFIP Wireless Days - 6th IFIP Network Control conference (Netcon 2008), 24 Nov 2008-27 Nov 2008.

Andreeva, E., Preneel, B. (2008). A Three-Property-Secure Hash Function. In: *Lecture Notes in Computer Science*: *vol. 5381*, (228-244). Presented at the SAC 2008, 14 Aug 2008-15 Aug 2008.

Handschuh, H., Preneel, B. (2008). Key-Recovery Attacks on Universal Hash Function based MAC Algorithms. In: *Lecture Notes in Computer Science*: *vol. 5157*, (144-161). Presented at the CRYPTO 2008, 17 Aug 2008-21 Aug 2008. Open Access

Wouters, K.M., Simoens, K., Lathouwers, D., Preneel, B. (2008). Secure and Privacy-Friendly Logging for eGovernment Services. In: *3rd International Conference on Availability, Reliability and Security (ARES 2008)*, (1091-1096). Presented at the ARES 2008, Technical University of Catalonia, Barcelona, Spain, 04 Mar 2008-07 Mar 2008.

Gierlichs, B., Batina, L., Tuyls, P., Preneel, B. (2008). Mutual Information Analysis - A Generic Side-Channel Distinguisher. In: *Lecture Notes in Computer Science*: *vol. 5154*, (426-442). Presented at the CHES 2008, 10 Aug 2008-13 Aug 2008. Open Access

Indesteege, S., Preneel, B. (2008). Collisions for RC4-Hash. In: *Lecture Notes in Computer Science*: *vol. 5222*, (355-366). Presented at the ISC 2008, 15 Sep 2008-18 Sep 2008. Open Access

Schellekens, D., Tuyls, P., Preneel, B. (2008). Embedded Trusted Computing with Authenticated Non-Volatile Memory. In: *Lecture Notes in Computer Science*: *vol. 4968*, (60-74). Presented at the TRUST 2008, 11 Mar 2008-12 Mar 2008. Open Access

Deng, M., Weng, L., Preneel, B. (2008). Anonymous buyer-seller watermarking protocol with additive homomorphism. In: P. Assuncao, S. Faria (Eds.), *SIGMAP 2008: PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING AND MULTIMEDIA APPLICATIONS*, (300-307). Presented at the International Conference on Signal Processing and Multimedia Applications, Oporto, PORTUGAL, 26 Jul 2008. ISBN: 978-989-8111-60-9. (URL)

Preneel, B. (2008). Cryptographic algorithms - Successes, failures and challenges. In: J. Filipe, D.A. Marca, B. Shishkov, M. VanSinderen (Eds.), *ICE-B 2008: PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON E-BUSINESS*, (IS21-IS27). Presented at the International Conference on e-Business (ICE-B 2008), Oporto, PORTUGAL, 26 Jul 2008-29 Jul 2008. ISBN: 978-989-8111-58-6. (URL)

Deng, M., Preneel, B. (2008). Attacks On Two Buyer-Seller Watermarking Protocols and an Improvement For Revocable Anonymity. In: *International Symposium on Electronic Commerce and Security (ISECS 2008)*, (923-929). Presented at the ISECS 2008, 03 Aug 2008-05 Aug 2008.

Wan, Z., Ren, K., Lou, W., Preneel, B. (2008). Anonymous ID-based Group Key Agreement for Wireless Networks. In: *IEEE Wireless Communications and Networking Conference (WCNC 2008)*, (2615-2620). Presented at the WCNC 2008, 31 Mar 2008-03 Apr 2008.

Preneel, B. (2008). Cryptographic algorithms - Successes, failures and challenges. In: M.S. Obaidat, R. Caldeirinha (Eds.), *WINSYS 2008: PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON WIRELESS INFORMATION NETWORKS AND SYSTEMS*, (IS21-IS27). Presented at the International Conference on Wireless Information Networks and Systems, Oporto, PORTUGAL, 26 Jul 2008-29 Jul 2008. ISBN: 978-989-8111-62-3. (URL)

De Cannière, C., Küçük, Ö., Preneel, B. (2008). Analysis of Grain's Initialization Algorithm. In: *Lecture Notes in Computer Science*: *vol. 5023*, (276-289). Presented at the AFRICACRYPT 2008, 11 Jun 2008-14 Jun 2008. Open Access

Indesteege, S., Keller, N., Biham, E., Dunkelman, O., Preneel, B. (2008). A Practical Attack on KeeLoq. In: *Lecture Notes in Computer Science*: *vol. 4965*, (1-18). Presented at the EUROCRYPT 2008, 14 Apr 2008-17 Apr 2008. Open Access

Cappaert, J., Preneel, B., Anckaert, B., Madou, M., De Bosschere, K. (2008). Towards Tamper Resistant Code Encryption: Practice and Experience. In: *Lecture Notes in Computer Science*: *vol. 4991*, (86-100). Presented at the ISPEC 2008, 21 Apr 2008-23 Apr 2008. Open Access

Preneel, B. (2008). Cryptographic algorithms - Successes, failures and challenges. In: P. Assuncao, S. Faria (Eds.), *SIGMAP 2008: PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING AND MULTIMEDIA APPLICATIONS*, (IS21-IS27). Presented at the International Conference on Signal Processing and Multimedia Applications, Oporto, PORTUGAL, 26 Jul 2008. ISBN: 978-989-8111-60-9. (URL)

Preneel, B. (2008). Cryptographic algorithms - Successes, failures and challenges. In: E. FernandezMedina, M. Malek, J. Hernando (Eds.), *SECRYPT 2008: PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SECURITY AND CRYPTOGRAPHY*, (IS21-IS27). Presented at the International Conference on Security and Cryptography, Oporto, PORTUGAL, 26 Jul 2008-29 Jul 2008. ISBN: 978-989-8111-59-3. (URL)

Indesteege, S., Mendel, F., Preneel, B., Rechberger, C. (2008). Collisions and other Non-Random Properties for Step-Reduced SHA-256. In: *Lecture Notes in Computer Science*: *vol. 5381*, (276-293). Presented at the SAC 2008, 14 Aug 2008-15 Aug 2008. Open Access

Deng, M., Preneel, B. (2008). On secure and anonymous buyer-seller watermarking protocol. In: *3rd International Conference on Internet and Web Applications and Services (ICIW 2008)*, (524-529). Presented at the ICIW 2008, 08 Jun 2008-13 Jun 2008.

Wan, Z., Ren, K., Preneel, B. (2008). A Secure Privacy-Preserving Roaming Protocol Based on Hierarchical Identity-Based Encryption for Mobile Networks. In: *Proceedings of the 1st ACM conference on Wireless network security (WiSec 2008)*, (62-67). Presented at the WiSec 2008, 31 Mar 2008-02 Apr 2008.

Diaz, C., Gonzalez Troncoso, C., Preneel, B. (2008). A Framework for the Analysis of Mix-Based Steganographic File Systems. In: *Lecture Notes in Computer Science*: *vol. 5283*, (428-445). Presented at the ESORICS 2008, 06 Oct 2008-08 Oct 2008. Open Access

Zhang, Y., Gu, D., Preneel, B. (2008). Reliable Key Establishment Scheme Exploiting Unidirectional Links in Wireless Sensor Networks. In: C.Z. Xu, M. Guo (Eds.), *EUC 2008: PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON EMBEDDED AND UBIQUITOUS COMPUTING, VOL 1, MAIN CONFERENCE*, (272-+). Presented at the 5th International Conference on Embedded and Ubiquitous Computing, Shanghai, PEOPLES R CHINA, 17 Dec 2008-20 Dec 2008. ISBN: 978-0-7695-3492-3. doi: 10.1109/EUC.2008.10

Preneel, B. (2008). Research Challenges in Cryptology (invited keynote). In: *International Conference on Security of Information and Networks*, (268-272). Presented at the Security of Information and Networks 2007, 08 May 2007-10 May 2007.

Peeters, R., Simoens, K., De Cock, D., Preneel, B. (2008). Cross-Context Delegation through Identity Federation. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, (79-92). Presented at the BIOSIG 2008, 11 Sep 2008-12 Sep 2008.

Gierlichs, B., Gonzalez Troncoso, C., Diaz, C., Preneel, B., Verbauwhede, I. (2008). Revisiting A Combinatorial Approach Toward Measuring Anonymity. In: *Proceedings of the 7th ACM workshop on Privacy in the electronic society (WPES 2008)*, (111-116). Presented at the WPES 2008, 27 Oct 2008-27 Oct 2008.

De Mulder, Y., Danezis, G., Batina, L., Preneel, B. (2008). Identification via Location-Profiling in GSM Networks. In: *Proceedings of the 7th ACM workshop on Privacy in the electronic society (WPES 2008)*, (23-32). Presented at the WPES 2008, 27 Oct 2008-27 Oct 2008.

Mentens, N., Genoe, J., Preneel, B., Verbauwhede, I. (2008). A low-cost implementation of Trivium. Presented at the ECRYPT workshop SASC, 01 Jan 2008-01 Jan 2008.

Sassaman, L., Preneel, B. (2008). The Byzantine Postman Problem. In: *Proceedings of the 29th Symposium on Information Theory in the Benelux*, (129-135). Presented at the 29th Symposium on Information Theory in the Benelux, 29 May 2008-30 May 2008.

Batina, L., Mentens, N., Sakiyama, K., Preneel, B., Verbauwhede, I. (2007). Public-Key Cryptography on the Top of a Needle. In: *IEEE International Symposium on Circuits and Systems (ISCAS 2007)*, (1831-1834). Presented at the ISCAS 2007, 27 May 2007-30 May 2007.

Mentens, N., Sakiyama, K., Batina, L., Preneel, B., Verbauwhede, I. (2007). A side-channel attack resistant programmable PKC coprocessor for embedded applications. In: *International Conference on Systems, Architectures, MOdeling and Simulation (IC-SAMOS 2007)*, (194-200). Presented at the IC-SAMOS 2007, 16 Jul 2007-19 Jul 2007.

Sakiyama, K., De Mulder, E., Preneel, B., Verbauwhede, I. (2007). Side-channel Resistant System-level Design Flow for Public-key Cryptography. In: *Proceedings of the 17th ACM Great Lakes symposium on VLSI (GLSVLSI 2007)*, (144-147). Presented at the GLSVLSI 2007, 11 Mar 2007-13 Mar 2007.

Mentens, N., Sakiyama, K., Preneel, B., Verbauwhede, I. (2007). Efficient Pipelining for Modular Multiplication Architectures in Prime Fields. In: *Proceedings of the 17th ACM Great Lakes symposium on VLSI (GLSVLSI 2007)*, (534-539). Presented at the GLSVLSI 2007, 11 Mar 2007-13 Mar 2007.

Andreeva, E., Neven, G., Preneel, B., Shrimpton, T. (2007). Seven-Property-Preserving Iterated Hashing: ROX. In: *Lecture Notes in Computer Science*: *vol. 4833*, (130-146). Presented at the ASIACRYPT 2007, 02 Dec 2007-06 Dec 2007.

Handschuh, H., Preneel, B. (2007). Blind differential cryptanalysis for enhanced power attacks. In: E. Biham, A.M. Youssef (Eds.), *SELECTED AREAS IN CRYPTOGRAPHY*: *vol. 4356*, (163-+). Presented at the 13th Annual International Workshop on Selected Areas in Cryptography, Montreal, CANADA, 17 Aug 2006-18 Aug 2006. ISBN: 978-3-540-74461-0. (URL)

Wyseur, B., Michiels, W., Gorissen, P., Preneel, B. (2007). Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings. In: *Lecture Notes in Computer Science*: *vol. 4876*, (264-277). Presented at the SAC 2007, 16 Aug 2007-17 Aug 2007. Open Access

Wouters, K., Wyseur, B., Preneel, B. (2007). Security Model for a Shared Multimedia Archive. In: *3rd International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS 2007)*, (249-255). Presented at the AXMEDIS 2007, 28 Nov 2007-30 Nov 2007.

Wyseur, B., Wouters, K., Preneel, B. (2007). Lexical natural language steganography systems with human interaction. In: D. Remenyi (Eds.), *ECIW 2007: PROCEEDINGS OF THE 6TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY*, (313-320). Presented at the 6th European Conference on Information Warfare and Security, Defence Coll Management & Technol, Shrivenham, ENGLAND, 02 Jul 2007-03 Jul 2007. ISBN: 978-1-905305-48-3. (URL)

Dunkelman, O., Sekar, G., Preneel, B. (2007). Improved Meet-in-the-Middle Attacks on Reduced-Round DES. In: *Lecture Notes in Computer Science*: *vol. 4859*, (86-100). Presented at the INDOCRYPT 2007, 09 Dec 2007-13 Dec 2007. Open Access

Wan, Z., Deng, R., Bao, F., Preneel, B. (2007). nPAKE+: A Hierarchical Group Password-Authenticated Key Exchange Protocol Using Different Passwords. In: *Lecture Notes in Computer Science*: *vol. 4861*, (31-43). Presented at the ICICS 2007, 12 Dec 2007-15 Dec 2007. Open Access

Kohlweiss, M., Faust, S., Fritsch, L., Gedrojc, B., Preneel, B. (2007). Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker. In: *Lecture Notes in Computer Science*: *vol. 4776*, (77-94). Presented at the PET 2007, 20 Jun 2007-22 Jun 2007. Open Access

Gonzalez Troncoso, C., Diaz, C., Dunkelman, O., Preneel, B. (2007). Traffic Analysis Attacks on a Continuously-Observable Steganographic File. In: *Lecture Notes in Computer Science*: *vol. 4567*, (220-236). Presented at the IH 2007, 11 Jun 2007-13 Jun 2007. Open Access

Sekar, G., Paul, S., Preneel, B. (2007). Related-Key Attacks on the Py-Family of Ciphers and an Approach to Repair the Weaknesses. In: *Lecture Notes in Computer Science*: *vol. 4859*, (58-72). Presented at the INDOCRYPT 2007, 09 Dec 2007-13 Dec 2007. Open Access

Singelee, D., Preneel, B. (2007). Key establishment using secure distance bounding protocols. In: *2007 FOURTH ANNUAL INTERNATIONAL CONFERENCE ON MOBILE AND UBIQUITOUS SYSTEMS: NETWORKING & SERVICES*, (516-521). Presented at the 4th Annual International Conference on Mobile and Ubiquitous Systems (MOBIQUITOUS 2007), Philadelphia, PA, 06 Aug 2007-10 Aug 2007. ISBN: 978-1-4244-1024-8. (URL)

De Cock, D., Preneel, B. (2007). Electronic Voting in Belgium: Past and Future. In: *Lecture Notes in Computer Science*: *vol. 4896*, (76-87). Presented at the VOTE-ID 2007, 04 Oct 2007-05 Oct 2007.

Danezis, G., Diaz, C., Faust, S., Käsper, E., Gonzalez Troncoso, C., Preneel, B. (2007). Efficient Negative Databases from Cryptographic Hash Functions. In: *Lecture Notes in Computer Science*: *vol. 4779*, (423-436). Presented at the ISC 2007, 09 Oct 2007-12 Oct 2007. Open Access

Weng, L., Preneel, B. (2007). Attacking some perceptual image hash algorithms. In: *Proc. of IEEE International Conference on Multimedia and Expo 2007*, (879-882). Presented at the ICME 2007, 02 Jul 2007-05 Jul 2007.

Sekar, G., Paul, S., Preneel, B. (2007). New Weaknesses in the Keystream Generation Algorithms of the Stream Ciphers TPy and Py. In: *Lecture Notes in Computer Science*: *vol. 4779*, (249-262). Presented at the ISC 2007, 09 Oct 2007-12 Oct 2007. Open Access

Yoshida, H., Watanabe, D., Okeya, K., Kitahara, J., Wu, H., Küçük, Ö., Preneel, B. (2007). MAME: A compression function with reduced hardware requirements. In: *Lecture Notes in Computer Science*: *vol. 4727*, (148-165). Presented at the CHES 2007, 10 Sep 2007-13 Sep 2007.

Mendel, F., Lano, J., Preneel, B. (2007). Cryptanalysis of Reduced Variants of the FORK-256 Hash Function. In: *Lecture Notes in Computer Science*: *vol. 4377*, (85-100). Presented at the CT-RSA 2007, 05 Feb 2007-09 Feb 2007. Open Access

Singelée, D., Preneel, B. (2007). Distance Bounding in Noisy Environments. In: *Lecture Notes in Computer Science*: *vol. 4572*, (101-115). Presented at the ESAS 2007, 02 Jul 2007-03 Jul 2007. Open Access

Kim, J., Hong, S., Preneel, B. (2007). Related-key rectangle attacks on reduced AES-192 and AES-256. In: A. Biryukov (Eds.), *FAST SOFTWARE ENCRYPTION*: *vol. 4593*, (225-+). Presented at the 14th International Workshop on Fast Software Encryption, Luxembourg, LUXEMBOURG, 26 Mar 2007-28 Mar 2007. ISBN: 978-3-540-74617-1. (URL)

Wu, H., Preneel, B. (2007). Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy. In: *Lecture Notes in Computer Science*: *vol. 4515*, (276-290). Presented at the EUROCRYPT 2007, 20 May 2007-24 May 2007. Open Access

Wu, H., Preneel, B. (2007). Differential-Linear Attacks against the Stream Cipher Phelix. In: *Lecture Notes in Computer Science*: *vol. 4593*, (87-100). Presented at the FSE 2007, 26 Mar 2007-28 Mar 2007. Open Access

Indesteege, S., Preneel, B. (2007). Preimages for Reduced-Round Tiger. In: *Lecture Notes in Computer Science*: *vol. 4945*, (90-99). Presented at the WEWoRC 2007, 04 Jul 2007-06 Jul 2007. Open Access

Sekar, G., Paul, S., Preneel, B. (2007). New Attacks on the Stream Cipher TPy6 and Design of New Ciphers the TPy6-A and the TPy6-B. In: *Lecture Notes in Computer Science*: *vol. 4945*, (127-141). Presented at the WEWoRC 2007, 04 Jul 2007-06 Jul 2007. Open Access

Anckaert, B., Madou, M., De Sutter, B., De Bus, B., De Bosschere, K., Preneel, B. (2007). Program obfuscation: a quantitative approach. In: *Proceedings of the 2007 ACM workshop on Quality of protection (QoP 2007)*, (15-20). Presented at the QoP 2007, 29 Oct 2007-29 Oct 2007.

Gonzalez Troncoso, C., Danezis, G., Kosta, E., Preneel, B. (2007). PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance. In: *Proceedings of the 6th ACM workshop on Privacy in the electronic society (WPES 2007)*, (99-107). Presented at the WPES 2007, 29 Oct 2007-29 Oct 2007.

Weng, L., Preneel, B. (2007). On secure image hashing by higher-order statistics. In: *IEEE International Conference on Signal Processing and Communications (ICSPC 2007)*, (1063-1066). Presented at the ICSPC 2007, 24 Nov 2007-27 Nov 2007.

Preneel, B. (2007). An Introduction to Cryptology. Presented at the IPICS 2007 - Intensive Programme on Information and Communications Security, Cardiff UK, 01 Jul 2007-13 Jul 2007.

Braeken, A., Nikov, V., Nikova, S., Preneel, B. (2007). On Boolean Functions with Generalized Cryptographic Properties. In: *NATO ASI on "Boolean Functions in Cryptology and Information Security"*, (73-96). Presented at the NATO ASI on "Boolean Functions in Cryptology and Information Security", 09 Aug 2007-09 Jun 2008.

Borissov, Y., Braeken, A., Nikova, S., Preneel, B. (2007). Classification of the Cosets of RM(1,7). In: *NATO ASI on "Boolean Functions in Cryptology and Information Security"*, (58-73). Presented at the NATO ASI on "Boolean Functions in Cryptology and Information Security", 09 Aug 2007-09 Jun 2008.

Singelée, D., Preneel, B. (2007). Key Establishment Using Secure Distance Bounding Protocols. In: *4th Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2007)*, (1-6). Presented at the MobiQuitous 2007, 10 Aug 2007-10 Aug 2007.

Scholten, H., Van Dijk, H., De Cock, D., Preneel, B., D'Hooge, M., Kung, A. (2006). Secure service discovery in home networks. In: *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*: *vol. 2006*, (115-116). ISBN: 0780394593. doi: 10.1109/ICCE.2006.1598337

Sakiyama, K., Preneel, B., Verbauwhede, I. (2006). A Fast Dual-Field Modular Arithmetic Logic Unit and Its Hardware Implementation. In: *IEEE International Symposium on Circuits and Systems (ISCAS 2006)*, (787-790). Presented at the ISCAS 2006, 21 May 2006-24 May 2006.

Batina, L., Mentens, N., Preneel, B., Verbauwhede, I. (2006). Flexible Hardware Architectures for Curve-based Cryptography. In: *IEEE International Symposium on Circuits and Systems (ISCAS 2006)*, (4839-4842). Presented at the ISCAS 2006, 21 May 2006-24 May 2006.

Batina, L., Mentens, N., Sakiyama, K., Preneel, B., Verbauwhede, I. (2006). Low-cost Elliptic Curve Cryptography for wireless sensor networks. In: *Lecture Notes in Computer Science*: *vol. 4357*, (6-17). Presented at the ESAS 2006, 20 Sep 2006-21 Sep 2006. Open Access

Sakiyama, K., Batina, L., Preneel, B., Verbauwhede, I. (2006). Superscalar Coprocessor for High-speed Curve-based Cryptography. In: *Lecture Notes in Computer Science*: *vol. 4249*, (415-429). Presented at the 8th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006), Yokohama, JAPAN.

Sakiyama, K., De Mulder, E., Preneel, B., Verbauwhede, I. (2006). A Parallel Processing Hardware Architecture for Elliptic Curve Cryptosystems. In: *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2006)*. Presented at the ICASSP 2006, 15 May 2006-19 May 2006.

Mentens, N., Sakiyama, K., Batina, L., Verbauwhede, I., Preneel, B. (2006). FPGA-ORIENTED SECURE DATA PATH DESIGN: IMPLEMENTATION OF A PUBLIC KEY COPROCESSOR. In: A. Koch, P. Leong, A. Koch (Eds.), *2006 INTERNATIONAL CONFERENCE ON FIELD PROGRAMMABLE LOGIC AND APPLICATIONS, PROCEEDINGS*, (133-138). Presented at the 16th International Conference on Field Programmable Logic and Applications, Madrid, SPAIN, 28 Aug 2006-30 Aug 2006. ISBN: 978-1-4244-0312-7. (URL)

Schellekens, D., Preneel, B., Verbauwhede, I. (2006). FPGA vendor agnostic True Random Number Generator. In: *16th International Conference on Field Programmable Logic and Applications (FPL 2006)*, (139-144). Presented at the FPL 2006, 28 Aug 2006-30 Aug 2006.

Seys, S., Preneel, B. (2006). ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks. In: *20th IEEE International Conference on Advanced Information Networking and Applications (AINA 2006)*, (133-137). Presented at the AINA 2006, 18 Apr 2006-20 Apr 2006.

Weng, L., Wouters, K., Preneel, B. (2006). Extending the Selective MPEG Encryption Algorithm PVEA. In: *Internation Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2006)*, (117-120). Presented at the IIH-MSP 2006, 18 Dec 2006-20 Dec 2006.

Wu, H., Preneel, B. (2006). Cryptanalysis of the Stream Cipher ABC v2. In: *Lecture Notes in Computer Science*: *vol. 4356*, (56-66). Presented at the Annual International Workshop on Selected Areas in Cryptography, Montreal: CANADA. Open Access

Kim, J., Biryukov, A., Preneel, B., Hong, S. (2006). On the security of HMAC and NMAC based on HAVAL, MD4, MD5, SHA-0 and SHA-1 - (Extended abstract). In: R. DePrisco, M. Yung (Eds.), *SECURITY AND CRYPTOGRAPHY FOR NETWORKS, PROCEEDINGS*: *vol. 4116*, (242-256). Presented at the 5th International Conference on Security and Cryptography for Networks, Maiori, ITALY, 06 Sep 2006-08 Sep 2006. ISBN: 3-540-38080-9. (URL)

Singelée, D., Preneel, B. (2006). Improved Pairing Protocol for Bluetooth. In: *Lecture Notes in Computer Science*: *vol. 4104*, (252-265). Presented at the ADHOC-NOW 2006, Ottawa.

Wu, H., Preneel, B. (2006). Resynchronization Attacks on WG and LEX. In: *Lecture Notes in Computer Science*: *vol. 4047*, (422-432). Presented at the 13th International Workshop on Fast Software Encryption, Graz, AUSTRIA.

Paul, S., Preneel, B., Sekar, G. (2006). Distinguishing Attacks on the Stream Cipher Py. In: *Lecture Notes in Computer Science*: *vol. 4047*, (405-421). Presented at the 13th International Workshop on Fast Software Encryption, Graz, AUSTRIA.

Mendel, F., Preneel, B., Rijmen, V., Yoshida, H., Watanabe, D. (2006). Update on Tiger. In: *Lecture Notes in Computer Science*: *vol. 4329*, (63-79). Presented at the INDOCRYPT 2006, 11 Dec 2006-13 Dec 2006. Open Access

Braeken, A., Lano, J., Preneel, B. (2006). Evaluating the Resistance of Stream Ciphers with Linear Feedback Against Fast Algebraic Attacks. In: *Lecture Notes in Computer Science*: *vol. 4058*, (40-51). Presented at the 11th Australasian Conference on Information Security and Privacy, Melbourne, AUSTRALIA.

Paul, S., Preneel, B. (2006). On the (In)security of Stream Ciphers Based on Arrays and Modular Addition. In: *Lecture Notes in Computer Science*: *vol. 4284*, (69-83). Presented at the ASIACRYPT 2006, 03 Dec 2006-07 Dec 2006. Open Access

Wu, H., Preneel, B. (2006). Cryptanalysis of the Stream Cipher DECIM. In: *Lecture Notes in Computer Science*: *vol. 4047*, (30-40). Presented at the FSE 2006.

Nikov, V., Nikova, S., Preneel, B. (2006). A Weakness in Some Oblivious Transfer and Zero-Knowledge Protocols. In: *Lecture Notes in Computer Science*: *vol. 4284*, (348-363). Presented at the ASIACRYPT 2006, 03 Dec 2006-07 Dec 2006.

De Cock, D., Wolf, C., Preneel, B. (2006). The Belgian Electronic Identity Card (Overview). In: *Sicherheit 2005: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 3rd Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI)*, (298-301). Presented at the Sicherheit 2006, 20 Feb 2006-22 Feb 2006.

Mendel, F., Preneel, B., Rijmen, V., Yoshida, H., Watanabe, D. (2006). Update on tiger⋆. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 4329 LNCS*, (63-79). ISBN: 9783540497677.

Singelée, D., Preneel, B. (2006). Location Privacy in Wireless Personal Area Networks. In: *Proceedings of the 5th ACM workshop on Wireless Security (WiSe 2006)*, (11-18). Presented at the WiSe 2006, 29 Sep 2006-29 Sep 2006.

Aerts, W., De Mulder, E., Preneel, B., Vandenbosch, G., Verbauwhede, I. (2006). Matching shielded loops for cryptographic analysis. In: *1st European Conference on Antennas and Propagation (EuCAP 2006)*, (1-6). Presented at the EuCAP 2006, Nice, 06 Nov 2006-10 Nov 2006.

Sakiyama, K., Batina, L., Preneel, B., Verbauwhede, I. (2006). HW/SW Co-design for Accelerating Public-Key Cryptosystems over GF(p) on the 8051 μ-controller. In: *World Automation Congress (WAC 2006)*, (1-6). Presented at the WAC 2006, 24 Jul 2006-27 Jul 2006.

Kim, J., Biryukov, A., Preneel, B., Hong, S. (2006). On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1. In: *Lecture Notes in Computer Science*: *vol. 4116*, (242-256). Presented at the 5th International Conferencs on Security and Cryptography for Networks, Maiori, ITALY.

Mentens, N., Sakiyama, K., Batina, L., Verbauwhede, I., Preneel, B. (2006). FPGA-oriented Secure Data Path Design: Implementation of a Public Key Coprocessor. In: *16th International Conference on Field Programmable Logic and Applications (FPL 2006)*, (133-138). Presented at the FPL 2006, 28 Aug 2006-30 Aug 2006.

De Mulder, E., Örs, S., Preneel, B., Verbauwhede, I. (2006). Differential Electromagnetic Attack on an FPGA. In: *World Automation Congress (WAC 2006)*, (1-7). Presented at the WAC 2006, 24 Jul 2006-27 Jul 2006.

Sakiyama, K., Batina, L., Mentens, N., Preneel, B., Verbauwhede, I. (2006). Small footprint ALU for public-key processors for pervasive security. Presented at the Workshop on RFID security, 01 Jan 2006-01 Jan 2006.

Batina, L., Kumar, S., Lano, J., Lemke-Rust, K., Mentens, N., Paar, C., Preneel, B., Sakiyama, K., Verbauwhede, I. (2006). Testing framework for eSTREAM profile II candidates. Presented at the ECRYPT workshop SASC - the state of the art of stream ciphers.

Madou, M., Anckaert, B., De Bus, B., De Bosschere, K., Cappaert, J., Preneel, B. (2006). On the Effectiveness of Source Code Transformations for Binary Obfuscation. In: *Proceedings of 2006 International Conference on Software Engineering Research and Practice (SERP 2006)*, (527-533). Presented at the SERP 2006, 26 Jun 2006-29 Jun 2006.

De Mulder, E., Buysschaert, P., Ors, S.B., Delmotte, P., Preneel, B., Vandenbosch, G., Verbauwhede, I. (2005). Electromagnetic analysis attack on an FPGA implementation of an elliptic curve cryptosystem. In: *EUROCON 2005 - The International Conference on "Computer as a Tool"*, (1879-1882). Presented at the EUROCON 2005, 21 Nov 2005-24 Nov 2005.

Batina, L., Mentens, N., Preneel, B., Verbauwhede, I. (2005). Side channel aware design: Algorithms and Architectures for Curve-based Cryptography over GF(2^n). In: *16th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2005)*, (350-355). Presented at the ASAP 2005, 23 Jul 2005-25 Jul 2005.

Batina, L., Hwang, D., Hodjat, A., Preneel, B., Verbauwhede, I. (2005). Hardware/Software Co-design for Hyperelliptic Curve Cryptography (HECC) on the 8051 microprocessor. In: *Lecture Notes in Computer Science*: *vol. 3659*, (106-118). Presented at the CHES 2005. Open Access

Seys, S., Preneel, B. (2005). Efficient Cooperative Signatures: A Novel Authentication Scheme for Sensor Networks. In: *Lecture Notes in Computer Science*: *vol. 3450*, (86-100). Presented at the SPC 2005. Open Access

Seys, S., Preneel, B. (2005). Power Consumption Evaluation of Efficient Digital Signature Schemes for Low Power Devices. In: *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB 2005)*, (79-86). Presented at the WIMOB 2005, 22 Aug 2005-24 Aug 2005.

De Cock, D., Wouters, K.M., Schellekens, D., Singelée, D., Preneel, B. (2005). Threat Modelling for Security Tokens in Web Applications. In: Chadwick, B. Preneel (Eds.), *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, (183-193). Presented at the CMS, Windermere (UK), 01 Jan 2004-01 Jan 2004.

Braeken, A., Wolf, C., Preneel, B. (2005). Normality of vectorial functions. In: N.P. Smart (Eds.), *CRYPTOGRAPHY AND CODING, PROCEEDINGS*: *vol. 3796*, (186-200). Presented at the 10th IMA International Conference on Cryptography and Coding, Royal Agr Coll, Cirencester, ENGLAND, 19 Dec 2005-21 Dec 2005. ISBN: 3-540-30276-X. (URL)

Braeken, A., Preneel, B. (2005). On the Algebraic Immunity of Symmetric Boolean Functions. In: *Lecture Notes in Computer Science*: *vol. 3797*, (35-48). Presented at the INDOCRYPT 2005.

Braeken, A., Preneel, B. (2005). Probabilistic Algebraic Attacks. In: *Lecture Notes in Computer Science*: *vol. 3796*, (290-303). Presented at the Cryptography and Coding, 10th IMA International Conference.

Paul, S., Preneel, B. (2005). Near Optimal Algorithms for Solving Differential Equations of Addition with Batch Queries. In: *Lecture Notes in Computer Science*: *vol. 3797*, (90-103). Presented at the INDOCRYPT 2005. Open Access

Wolf, C., Braeken, A., Preneel, B. (2005). Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC. In: *Lecture Notes in Computer Science*: *vol. 3352*, (294-307). Presented at the SCN 2004.

Wolf, C., Preneel, B. (2005). Large superfluous keys in multivariate quadratic asymmetric systems. In: S. Vaudenay (Eds.), *PUBLIC KEY CRYPTOGRAPHY - PKC 2005*: *vol. 3386*, (275-287). Presented at the 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, SWITZERLAND, 23 Jan 2005-26 Jan 2005. ISBN: 3-540-24454-9. (URL)

Nikov, V., Nikova, S., Preneel, B. (2005). On the size of monotone span programs. In: *SECURITY IN COMMUNICATION NETWORKS*: *vol. 3352*, (249-262). Presented at the 4th International Conference on Security in Communication Networks, Amalfi, ITALY, 08 Sep 2004-10 Sep 2004. ISBN: 3-540-24301-1. (URL)

Hong, S., Kim, J., Lee, S., Preneel, B. (2005). Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192. In: *Lecture Notes in Computer Science*: *vol. 3557*, (368-383). Presented at the FSE 2005.

Braeken, A., Borissov, Y., Nikova, S., Preneel, B. (2005). Classification of Boolean Functions of 6 variables or Less with respect to some Cryptographic Properties. In: *Lecture Notes in Computer Science*: *vol. 3580*, (324-334). Presented at the ICALP 2005.

Paul, S., Preneel, B. (2005). Solving systems of differential equations of addition. In: C. Boyd, J.M. GonzalezNieto (Eds.), *INFORMATION SECURITY AND PRIVACY, PROCEEDINGS*: *vol. 3574*, (75-88). Presented at the 10th Australasian Conference on Information Security and Privacy, Brisbane, AUSTRALIA, 04 Jul 2005-06 Jul 2005. ISBN: 3-540-26547-3. (URL)

Yoshida, H., Biryukov, A., De Cannière, C., Lano, J., Preneel, B. (2005). Non-randomness of the Full 4 and 5-pass HAVAL. In: *Lecture Notes in Computer Science*: *vol. 3352*, (324-336). Presented at the SCN 2004.

Wolf, C., Preneel, B. (2005). Equivalent Keys in HFE, C*, and variations. In: *Lecture Notes in Computer Science*: *vol. 3715*, (33-49). Presented at the Mycrypt 2005.

Braeken, A., Wolf, C., Preneel, B. (2005). A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes. In: *Lecture Notes in Computer Science*: *vol. 3376*, (29-43). Presented at the CT-RSA 2005.

Nikov, V., Nikova, S., Preneel, B. (2005). Upper Bound for the Size of Monotone Span Programs. In: *IEEE Transactions on Information Theory*: *vol. 51* (6), (284-284). Presented at the IEEE International Symposium on Information Theory, Yokohama, Japan, 29 Jun 2003-04 Jul 2003. ISBN: 0-7803-7728-1.

Kim, J., Biryukov, A., Preneel, B., Lee, S. (2005). On the Security of Encryption Modes of MD4, MD5 and HAVAL. In: *Lecture Notes in Computer Science*: *vol. 3783*, (147-158). Presented at the ICICS 2005. Open Access

Wolf, C., Preneel, B. (2005). Applications of Multivariate Quadratic Public Key Systems. In: *Sicherheit 2005: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 2nd Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI)*, (413-424). Presented at the Sicherheit 2005, 05 Apr 2005-08 Apr 2005.

Singelée, D., Preneel, B. (2005). Location Verification using Secure Distance Bounding Protocols. In: *2005 International Workshop on Wireless and Sensor Networks Security (WSNS 2005)*, (834-840). Presented at the WSNS 2005, 07 Nov 2005-07 Nov 2005.

Mentens, N., Batina, L., Preneel, B., Verbauwhede, I. (2005). Cracking Unix passwords using FPGA platforms. In: *ECRYPT workshop SHARCS - Special Purpose Hardware for Attacking Cryptographic Systems*, (83-91). Presented at the ECRYPT workshop SHARCS, 01 Jan 2005-01 Jan 2005.

Braeken, A., Lano, J., Mentens, N., Preneel, B., Verbauwhede, I. (2005). SFINKS: A synchronous stream cipher for restricted hardware environments. In: *SKEW - Symmetric key encryption workshop*. Presented at the SKEW - Symmetric Key Encryption Workshop, 01 Jan 2005-01 Jan 2005.

Wyseur, B., Preneel, B. (2005). Condensed White-Box Implementations. In: *Proceedings of the 26th Symposium on Information Theory in the Benelux*, (296-301). Presented at the 26th Symposium on Information Theory in the Benelux, 19 May 2005-20 May 2005.

Seys, S., Preneel, B. (2005). The Wandering Nodes: Key Management for Low-power Mobile Ad Hoc Networks. In: *25th IEEE International Conference on Distributed Computing Systems - Workshops (ICDCS 2005 Workshops)*, (916-922). Presented at the ICDCS Workshops 2005, 06 Jun 2005-10 Jun 2005.

Kim, J., Biryukov, A., Preneel, B., Lee, S. (2005). On the security of encryption modes of MD4, MD5 and HAVAL (Extended abstract). In: S. Qing, W. Mao, J. Lopez, G. Wang (Eds.), *INFORMATION AND COMMUNICATIONS SECURITY, PROCEEDINGS*: *vol. 3783*, (147-158). Presented at the 7th International Conference on Information and Communications Security, Beijing, PEOPLES R CHINA, 10 Dec 2005-13 Dec 2005. ISBN: 3-540-30934-9. (URL)

Wolf, C., Preneel, B. (2004). Asymmetric cryptography: Hidden field equations. In: *ECCOMAS 2004 - European Congress on Computational Methods in Applied Sciences and Engineering*.

Diaz, C., Preneel, B. (2004). Anonymous communication. In: *WHOLES - A Multiple View of Individual Privacy in a Networked World. Internet publication*, (1-7). Presented at the WHOLES, Sweden, 30 Jan 2004-31 Jan 2004.

Mentens, N., Örs, S., Preneel, B., Vandewalle, J. (2004). An FPGA Implementation of a Montgomery multiplier over GF(2^m). In: *7th IEEE Workshop on Design and Diagnostics of Electronic Circuits & Systems (DDECS 2004)*, (121-128). Presented at the DDECS 2004, 18 Apr 2004-21 Apr 2004.

Batina, L., Mentens, N., Örs, S., Preneel, B. (2004). Serial Multiplier Architectures over GF(2^n) for Elliptic Curve Cryptosystems. In: *12th IEEE Mediterranean Electrotechnical Conference (MELECON 2004)*, (779-782). Presented at the MELECON 2004, 12 May 2004-15 May 2004.

De Cock, D., Wouters, K.M., Preneel, B. (2004). Introduction to the Belgian EID Card: BELPIC. In: *Lecture Notes in Computer Science*: *vol. 3093*, (1-13). Presented at the EuroPKI 2004.

Diaz, C., Preneel, B. (2004). Taxonomy of mixes and dummy traffic. In: Y. Deswarte, F. Cuppens, S. Jajodia, L. Wang (Eds.), *INFORMATION SECURITY MANAGEMENT, EDUCATION AND PRIVACY*: *vol. 148*, (217-232). Presented at the 19th International Information Security Conference held at the 18th World Computer Congress, Toulouse, FRANCE, 22 Aug 2004-27 Aug 2004. ISBN: 1-4020-8144-8. doi: 10.1007/1-4020-8145-6_18

Braeken, A., Nikov, V., Nikova, S., Preneel, B. (2004). On Boolean functions with generalized cryptographic properties. In: A. Canteaut, K. Viswanathan (Eds.), *PROGRESS IN CRYPTOLOGY - INDOCRYPT 2004, PROCEEDINGS*: *vol. 3348*, (120-135). Presented at the 5th International Conference on Cryptology in India, Chennai, INDIA, 20 Dec 2004-22 Dec 2004. ISBN: 3-540-24130-2. (URL)

Braeken, A., Wolf, C., Preneel, B. (2004). A Randomised Algorithm for Checking the Normality of Cryptographic Boolean Functions. In: *3rd International Conference on Theoretical Computer Science 2004*, (51-66). Presented at the TCS 2004, 22 Aug 2004-27 Aug 2004.

Hong, D.J., Preneel, B., Lee, S. (2004). Higher Order Universal One-Way Hash Functions. In: *Lecture Notes in Computer Science*: *vol. 3329*, (201-213). Presented at the ASIACRYPT 2004.

Shirai, T., Preneel, B. (2004). On Feistel ciphers using optimal diffusion mappings across multiple rounds. In: *Lecture Notes in Computer Science*: *vol. 3329*, (1-15). Presented at the ASIACRYPT 2004.

Nikov, V., Nikova, S., Preneel, B. (2004). Robust Metering Schemes for General Access Structures. In: *Lecture Notes in Computer Science*: *vol. 3269*, (53-66). Presented at the ICICS 2004.

Diaz, C., Preneel, B. (2004). Reasoning about the Anonymity Provided by Pool Mixes that Generate Dummy Traffic. In: *Lecture Notes in Computer Science*: *vol. 3200*, (309-325). Presented at the IH 2004. Open Access

Armknecht, F., Lano, J., Preneel, B. (2004). Extending the Resynchronization Attack. In: *Lecture Notes in Computer Science*: *vol. 3357*, (19-38). Presented at the SAC 2004. Open Access

Standaert, F.X., Ors, S.B., Preneel, B. (2004). Power Analysis Attack on an FPGA Implementation of Rijndael: Is Pipelining a DPA Countermeasure? In: *Lecture Notes in Computer Science*: *vol. 3156*, (30-44). Presented at the CHES 2004.

Nakahara, J., Preneel, B., Vandewalle, J. (2004). The Biryukov-Demirci Attack on Reduced-Round Versions of IDEA and MESH Ciphers. In: *Lecture Notes in Computer Science*: *vol. 3108*, (98-109). Presented at the ACISP 2004.

Örs, S., Gurkaynak, F., Oswald, E., Preneel, B. (2004). Power-Analysis Attack on an ASIC AES implementation. In: *International Conference on Information Technology: Coding and Computing (ITCC 2004)*, (546-552). Presented at the ITCC 2004, 05 Apr 2004-07 Apr 2004.

Standaert, F.X., Ors, S.B., Quisquater, J.J., Preneel, B. (2004). Power Analysis Attacks against FPGA Implementations of the DES. In: *Lecture Notes in Computer Science*: *vol. 3203*, (84-94). Presented at the FPL 2004. Open Access

Nakahara, J., Rijmen, V., Preneel, B., Vandewalle, J. (2004). The MESH Block Ciphers. In: *Lecture Notes in Computer Science*: *vol. 2908*, (458-473). Presented at the WISA 2003.

Biryukov, A., Lano, J., Preneel, B. (2004). Cryptanalysis of the Alleged SecurID Hash Function. In: *Lecture Notes in Computer Science*: *vol. 3006*, (130-144). Presented at the SAC 2003. Open Access

Paul, S., Preneel, B. (2004). A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher. In: *Lecture Notes in Computer Science*: *vol. 3017*, (245-259). Presented at the FSE 2004. Open Access

Mentens, N., Örs, S., Preneel, B. (2004). An FPGA Implementation of an Elliptic Curve Processor over GF(2^m). In: *Proceedings of the 14th ACM Great Lakes symposium on VLSI (GLSVLSI 2004)*, (454-457). Presented at the GLSVLSI 2004, 26 Apr 2004-28 Apr 2004.

Watanabe, D., Furuya, S., Yoshida, H., Takaragi, K., Preneel, B. (2004). A new keystream generator MUGI. In: *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, (1), (37-45).

Batina, L., Lano, J., Mentens, N., Preneel, B., Verbauwhede, I., Örs, S.B. (2004). Energy, performance, area versus security trade-offs for stream ciphers. In: *ECRYPT workshop SASC - the state-of-the art of stream ciphers*, (302-310). Presented at the ECRYPT workshop SASC, 01 Jan 2004-01 Jan 2004.

Mentens, N., Batina, L., Preneel, B., Verbauwhede, I. (2004). An FPGA Implementation of Rijndael: Trade-offs for side-channel security. In: *IFAC Workshop - PDS 2004, Programmable Devices and Systems*, (493-498). Presented at the PDS 2004, 17 Nov 2004-18 Nov 2004.

Lano, J., Mentens, N., Preneel, B., Verbauwhede, I. (2004). Power analysis of synchronous stream ciphers with resynchronization mechanism. In: *ECRYPT workshop SASC - The state-of-the-art of stream ciphers*. Presented at the ECRYPT workshop SASC, 01 Jan 2004-01 Jan 2004. Open Access

Batina, L., Mentens, N., Preneel, B. (2004). A New Systolic Architecture for Multiplication in GF(2^n). In: *IFAC Workshop - PDS 2004, Programmable Devices and Systems*, (461-466). Presented at the PDS 2004, 17 Nov 2004-18 Nov 2004.

Dewitte, E., De Moor, B., Preneel, B. (2004). Information theoretic measures applied to power and electromagnetic traces measured from an FPGA performing an Elliptic Curve Point Multiplication. In: *Proceedings of the 25th Symposium on Information Theory in the Benelux*, (105-111). Presented at the 25th Symposium on Information Theory in the Benelux, 02 Jun 2004-04 Jun 2004.

Diaz, C., Preneel, B. (2004). Taxonomy of Mixes and Dummy Traffic. In: *Working Conference on Privacy and Anonymity in Networked and Distributed Systems*, (215-230). Presented at the I-NetSec, 23 Aug 2004-26 Aug 2004.

Watanabe, D., Furuya, S., Yoshida, H., Takaragi, K., Preneel, B. (2004). A new keystream generator MUGI. In: *IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS COMMUNICATIONS AND COMPUTER SCIENCES*: *vol. E87A* (1), (37-45). Presented at the Symposium of Cryptography and information Security, HAMAMATSU, JAPAN, 26 Jan 2003-29 Jan 2003. (URL)

Hong, D., Kang, J.S., Preneel, B., Ryu, H. (2003). A concrete security analysis for 3GPP-MAC. In: *Lecture Notes in Computer Science*: *vol. 2887*, (154-169). Presented at the FSE 2003.

Nakahara, J., Preneel, B., Vandewalle, J. (2003). A Note on Weak Keys of PES, IDEA, and Some Extended Variants. In: *Lecture Notes in Computer Science*: *vol. 2851*, (267-279). Presented at the ISC 2003.

Nikov, V., Nikova, S., Preneel, B. (2003). Multi-party Computation from Any Linear Secret Sharing Scheme Unconditionally Secure against Adaptive Adversary: The Zero-Error Case. In: *Lecture Notes in Computer Science*: *vol. 2846*, (1-15). Presented at the ACNS 2003. Open Access

Babbage, S., De Cannière, C., Lano, J., Preneel, B., Vandewalle, J. (2003). Cryptanalysis of SOBER-t32. In: *Lecture Notes in Computer Science*: *vol. 2887*, (111-128). Presented at the FSE 2003. Open Access

Borissov, Y., Braeken, A., Nikova, S., Preneel, B. (2003). On the Covering Radius of Second Order Binary Reed-Muller Code in the Set of Resilient Boolean Functions. In: *Lecture Notes in Computer Science*: *vol. 2898*, (82-92). Presented at the Cryptography and Coding, 9th IMA International Conference. Open Access

Nikov, V., Nikova, S., Preneel, B. (2003). On Multiplicative Linear Secret Sharing Schemes. In: *Lecture Notes in Computer Science*: *vol. 2904*, (135-147). Presented at the INDOCRYPT 2003.

Paul, S., Preneel, B. (2003). Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator. In: *Lecture Notes in Computer Science*: *vol. 2904*, (52-67). Presented at the INDOCRYPT 2003. Open Access

Van Rompay, B., Biryukov, A., Preneel, B., Vandewalle, J. (2003). Cryptanalysis of 3-Pass HAVAL. In: *Lecture Notes in Computer Science*: *vol. 2894*, (228-245). Presented at the ASIACRYPT 2003.

Preneel, B. (2003). The cryptography challenge: the past and the future. In: *Lecture Notes in Computer Science*: *vol. 2629*, (167-182). Presented at the FASec 2002.

Örs, S., Batina, L., Preneel, B., Vandewalle, J. (2003). Hardware Implementation of an Elliptic Curve Processor over GF(p). In: *14th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2003)*, (433-443). Presented at the ASAP 2003, 24 Jun 2003-26 Jun 2003.

Ors, S.B., Oswald, E., Preneel, B. (2003). Power-Analysis Attacks on an FPGA - First Experimental Results. In: *Lecture Notes in Computer Science*: *vol. 2779*, (35-50). Presented at the CHES 2003. Open Access

Borissov, Y., Nikova, S., Preneel, B., Vandewalle, J. (2003). On a Resynchronization Weakness in a Class of Combiners with Memory. In: *Lecture Notes in Computer Science*: *vol. 2576*, (164-173). Presented at the SCN 2002. Open Access

Biryukov, A., De Cannière, C., Braeken, A., Preneel, B. (2003). A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. In: *Lecture Notes in Computer Science*: *vol. 2656*, (33-50). Presented at the EUROCRYPT 2003. Open Access

Örs, S.B., Batina, L., Preneel, B., Vandewalle, J. (2003). Hardware implementation of a Montgomery modular multiplier in a systolic array. In: *Proceedings - International Parallel and Distributed Processing Symposium, IPDPS 2003*. ISBN: 0769519261. doi: 10.1109/IPDPS.2003.1213341

Wouters, K., Preneel, B., Gonzalez-Tablas, A., Ribagorda, A. (2003). Towards an XML Format for TimeStamps. In: *Proceedings of the 2002 ACM workshop on XML security (XMLSEC 2002)*. Presented at the XMLSEC 2002, 22 Nov 2002-22 Nov 2002.

Preneel, B. (2003). Trends in cryptology research. In: *Highlights of the Information Security Solutions Europe 2003 Conference (ISSE 2003)*, (51-58). Presented at the Information Security Solutions Europe (ISSE 2003), 07 Oct 2003-09 Oct 2003.

Seys, S., Preneel, B. (2003). Authenticated and efficient key management for wireless ad hoc networks. In: *Proceedings of the 24th Symposium on Information Theory in the Benelux*, (195-202). Presented at the 24th Symposium on Information Theory in the Benelux, 22 May 2003-23 May 2003.

Nikova, S., Nikov, V., Preneel, B., Vandewalle, J. (2003). Applying General Access Structure to Metering Schemes. In: *Proceedings of the International Workshop on Coding and Cryptography (WCC 2003)*, (337-347). Presented at the Workshop on Coding and Cryptography (WCC 2003), 24 Mar 2003-28 Mar 2003.

Diaz, C., Seys, S., Claessens, J., Preneel, B. (2002). Towards measuring anonymity. In: *Lecture Notes in Computer Science*: *vol. 2482*, (54-68). Presented at the PET 2002. Open Access

Nikov, V., Nikova, S., Preneel, B., Vandewalle, J. (2002). On Unconditionally Secure Distributed Oblivious Transfer. In: *Lecture Notes in Computer Science*: *vol. 2551*, (395-408). Presented at the INDOCRYPT 2002. Open Access

Rijmen, V., Van Rompay, B., Preneel, B., Vandewalle, J. (2002). Producing Collisions for PANAMA. In: *Lecture Notes in Computer Science*: *vol. 2355*, (37-51). Presented at the FSE 2001. Open Access

Biryukov, A., Nakahara, J., Preneel, B., Vandewalle, J. (2002). New Weak-Key Classes of IDEA. In: *Lecture Notes in Computer Science*: *vol. 2513*, (315-326). Presented at the ICICS 2002. Open Access

Barreto, P.S L M., Rijmen, V., Nakahara, J., Preneel, B., Vandewalle, J., Kim, H. (2002). Improved SQUARE Attacks against Reduced-Round HIEROCRYPT. In: *Lecture Notes in Computer Science*: *vol. 2355*, (165-173). Presented at the FSE 2001. Open Access

Nikov, V., Nikova, S., Preneel, B., Vandewalle, J. (2002). On Distributed Key Distribution Centers and Unconditionally Secure Proactive Verifiable Secret Sharing Schemes Based on General Access Structure. In: *Lecture Notes in Computer Science*: *vol. 2551*, (422-436). Presented at the INDOCRYPT 2002. Open Access

Preneel, B. (2002). NESSIE: A European Approach to Evaluate Cryptographic Algorithms. In: *Lecture Notes in Computer Science*: *vol. 2355*, (267-276). Presented at the FSE 2001. Open Access

Watanabe, D., Furuya, S., Yoshida, H., Takaragi, K., Preneel, B. (2002). A new keystream generator MUGI. In: *Lecture Notes in Computer Science*: *vol. 2365*, (179-194). Presented at the FSE 2002.

Quisquater, M., Preneel, B., Vandewalle, J. (2002). On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem. In: *Lecture Notes in Computer Science*: *vol. 2274*, (199-210). Presented at the PKC 2002, 12 Feb 2002-14 Feb 2002.

Preneel, B. (2002). New European Schemes for Signature, Integrity and Encryption (NESSIE): A Status Report. In: *Lecture Notes in Computer Science*: *vol. 2274*, (297-309). Presented at the PKC 2002, 12 Feb 2002-14 Feb 2002. Open Access

Claessens, J., Preneel, B., Vandewalle, J. (2002). Combining World Wide Web and Wireless Security. In: *Informatica*: *vol. 26* (2), (123-132).

Nikova, S., Nikov, V., Preneel, B., Vandewalle, J. (2002). Operations on Access Structures. In: *Proceedings of the EWM International Workshop on Groups and Graphs 2002*, (79-83). Presented at the EWM International Workshop on Groups and Graphs 2002, 01 Sep 2002-06 Sep 2002.

Preneel, B. (2002). The NESSIE project: towards new cryptographic algorithms. In: *Information Security Applications, 3rd International Workshop, WISA 2002*, (16-33). Presented at the WISA 2002, 01 Jan 2002-01 Jan 2002.

Nakahara, J., Barreto, P., Preneel, B., Vandewalle, J. (2002). Square Attacks on Reduced-Round PES and IDEA Block Ciphers. In: *Proceedings of the 23rd Symposium on Information Theory in the Benelux*, (187-195). Presented at the 23rd Symposium on Information Theory in the Benelux, 29 May 2002-31 May 2002.

Nikova, S., Nikov, V., Preneel, B., Vandewalle, J. (2002). Applying General Access Structure to Proactive Secret Sharing Schemes. In: *Proceedings of the 23rd Symposium on Information Theory in the Benelux*, (197-206). Presented at the 23rd Symposium on Information Theory in the Benelux, 29 May 2002-31 May 2002.

Diaz, C., Claessens, J., Seys, S., Preneel, B. (2002). Information Theory and Anonymity. In: *Proceedings of the 23rd Symposium on Information Theory in the Benelux*, (179-186). Presented at the 23rd Symposium on Information Theory in the Benelux, 29 May 2002-31 May 2002.

Janssens, S., Thomas, J., Borremans, W., Gijsels, P., Verbauwhede, I., Vercauteren, F., Preneel, B., Vandewalle, J. (2001). Hardware/Software Co-design of an elliptic curve public-key cryptosystem. In: *IEEE Workshop on Signal Processing Systems: Design and Implementation (SIPS 2001)*, (209-216). Presented at the SIPS 2001, 26 Sep 2001-28 Sep 2001.

Herlea, T., Claessens, J., Neven, G., Piessens, F., Preneel, B., De Decker, B. (2001). On securely scheduling a meeting. In: M. Dupuy, P. Paradinas (Eds.), *Trusted information - the new decade challenge*, (183-198). Presented at the 16th International Conference on Information Security, Paris, France, 11 Jun 2001-13 Jun 2001.

Vercauteren, F., Preneel, B., Vandewalle, J. (2001). A Memory Efficient Version of Satoh's Algorithm. In: *Lecture Notes in Computer Science*: *vol. 2045*, (1-13). Presented at the EUROCRYPT 2001.

Claessens, J., Preneel, B., Vandewalle, J. (2001). Combining World Wide Web and Wireless Security. In: *Advances in Network and Distributed Systems Security, 1st Annual Working Conference on Network Security*, (153-172). Presented at the Network Security 2001, 26 Nov 2001-27 Nov 2001.

Herlea, T., Claessens, J., De Cock, D., Preneel, B., Vandewalle, J. (2001). Secure meeting scheduling with agenTa. In: *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security (CMS 2001)*, (327-338). Presented at the IFIP TC6/TC11 International Conference on Communications and Multimedia Security (CMS 2001), 21 May 2001-22 May 2001.

Nakahara, J., Preneel, B., Vandewalle, J. (2001). Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Family. In: *Lecture Notes in Computer Science*: *vol. 1978*, (244-261). Presented at the FSE 2000, 10 Apr 2000-12 Apr 2000. Open Access

Den Boer, B., Van Rompay, B., Preneel, B., Vandewalle, J. (2001). New (Two-Track-)MAC based on the two trails of RIPEMD: Efficient, especially on short messages and for frequent Key-Changes. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 2259*, (314-324). ISBN: 9783540430667.

den Boer, B., Van Rompay, B., Preneel, B., Vandewalle, J. (2001). New (Two-Track-)MAC Based on the Two Trails of RIPEMD. In: *Lecture Notes in Computer Science*: *vol. 2259*, (314-324). Presented at the SAC 2001, 16 Aug 2001-17 Aug 2001. Open Access

Preneel, B. (2000). Advances in cryptology – EUROCRYPT 2000: International conference on the theory and application of cryptographic techniques bruges, Belgium, may 14-18, 2000 proceedings. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 1807*. ISBN: 9783540675174.

Iliadis, J., Spinellis, D., Gritzalis, D., Preneel, B., Katsikas, S. (2000). Evaluating certificate status information mechanisms. In: *Proceedings of the 7th ACM Conference on Computer and Communications Security (CCS 2000)*, (1-8). Presented at the CCS 2000, 01 Nov 2000-04 Nov 2000.

Borst, J., Preneel, B., Vandewalle, J. (2000). Power Analysis: Methods and Countermeasures. In: *Proceedings of the 21st Symposium on Information Theory in the Benelux*, (115-120). Presented at the 21st Symposium on Information Theory in the Benelux, 25 May 2000-26 May 2000.

D'Halluin, C., Bijnens, G., Preneel, B., Rijmen, V. (1999). Equivalent Keys of HPC. In: *Lecture Notes in Computer Science*: *vol. 1716*, (29-42). Presented at the ASIACRYPT 1999. Open Access

D'Halluin, C., Bijnens, G., Rijmen, V., Preneel, B. (1999). Attack on Six Rounds of Crypton. In: *Lecture Notes in Computer Science*: *vol. 1636*, (46-59). Presented at the FSE 1999. Open Access

Handschuh, H., Preneel, B. (1999). On the Security of Double and 2-Key Triple Modes of Operation. In: *Lecture Notes in Computer Science*: *vol. 1636*, (215-230). Presented at the FSE 1999. Open Access

Preneel, B., van Oorschot, P.C. (1999). On the security of iterated Message Authentication Codes. In: *IEEE Transactions on Information Theory*: *vol. 45* (1), (188-199).

Borst, J., Preneel, B., Vandewalle, J. (1999). Linear Cryptanalysis of RC5 and RC6. In: *Lecture Notes in Computer Science*: *vol. 1636*, (16-30). Presented at the FSE 1999. Open Access

Nevelsteen, W., Preneel, B. (1999). Software Performance of Universal Hash Functions. In: *Lecture Notes in Computer Science*: *vol. 1592*, (24-41). Presented at the EUROCRYPT 1999. Open Access

D'halluin, C., Bijnens, G., Preneel, B., Rijmen, V. (1999). Equivalent keys of HPC. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 1716*, (1-14). ISBN: 3540666664.

Claessens, J., Preneel, B., Vandewalle, J. (1999). Solutions for Anonymous Communication on the Internet. In: *33rd IEEE International Carnahan Conference on Security Technology (CCST 1999)*, (298-303). Presented at the CCST 1999, 05 Oct 1999-07 Oct 1999.

Knudsen, L., Preneel, B. (1999). Error correcting codes and collision-resistant hashing. In: *IEEE Information Theory and Communications Workshop 1999*, (55-57). Presented at the IEEE Information Theory and Communications Workshop 1999, 20 Jun 1999-25 Jun 1999.

Claessens, J., Preneel, B., Vandewalle, J. (1999). Enabling a lightweight software agent framework for secure agent-based electronic commerce applications. In: *Proceedings of the Workshop on Agents in Electronic Commerce (WAEC 1999) at the 1st Asia-Pacific Conference on Intelligent Agent Technology (IAT 1999)*, (151-158). Presented at the Workshop on Agents in Electronic Commerce (WAEC 1999) at the 1st Asia-Pacific Conference on Intelligent Agent Technology (IAT 1999), 14 Dec 1999-17 Dec 1999.

Nakahara, J., Vandewalle, J., Preneel, B. (1999). Diffusion analysis of Feistel networks. In: *Proceedings of the 20th Symposium on Information Theory in the Benelux*, (101-108). Presented at the 20th Symposium on Information Theory in the Benelux, 27 May 1999-28 May 1999.

Knudsen, L.R., Meier, W., Preneel, B., Rijmen, V., Verdoolaege, S. (1998). Analysis Methods for (Alleged) RC4. In: *Lecture Notes in Computer Science*: *vol. 1514*, (327-341). Presented at the ASIACRYPT 1998. Open Access

Horn, G., Preneel, B. (1998). Authentication and payment in future mobile systems. In: *Lecture Notes in Computer Science*: *vol. 1485*, (277-293). Presented at the 5th European Symposium on Research in Computer Security, Louvain La Neuve. Belgium. Open Access

Preneel, B., Rijmen, V., Bosselaers, A. (1998). Recent developments in the design of conventional cryptographic algorithms. In: *Lecture Notes in Computer Science*: *vol. 1528*, (105-130). Presented at the State of the Art and Evolution of Computer Security and Industrial Cryptography, 1997. Open Access

Vandewalle, J., Preneel, B., Csapodi, M. (1998). Data security issues, cryptographic protection methods, and the use of cellular neural networks and cellular automata. In: V. Tavsanoglu (Eds.), *CNNA 98 - 1998 FIFTH IEEE INTERNATIONAL WORKSHOP ON CELLULAR NEURAL NETWORKS AND THEIR APPLICATIONS - PROCEEDINGS*, (39-44). Presented at the 5th IEEE International Workshop on Cellular Neural Networks and Their Applications, SO BANK UNIV LONDON, LONDON, ENGLAND, 14 Apr 1998-17 Apr 1998. ISBN: 0-7803-4867-2. doi: 10.1109/CNNA.1998.685326

De Win, E., Preneel, B. (1998). Elliptic curve public-key cryptosystems - an introduction. In: *Lecture Notes in Computer Science*: *vol. 1528*, (131-141). Presented at the State of the Art and Evolution of Computer Security and Industrial Cryptography, 1997. Open Access

Claessens, J., Vandenwauver, M., Preneel, B., Vandewalle, J. (1998). Setting up a Secure Web Server and Clients on an Intranet. In: *7th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 1998)*, (295-300). Presented at the WETICE 1998, 17 Jun 1998-19 Jun 1998.

De Win, E., Mister, S., Preneel, B., Wiener, M. (1998). On the Performance of Signature Schemes Based on Elliptic Curves. In: *Lecture Notes in Computer Science*: *vol. 1423*, (252-266). Presented at the ANTS 1998, 21 Jun 1998-25 Jun 1998. Open Access

Martin, K., Preneel, B., Mitchell, C., Hitz, H-J., Horn, G., Howard, P., Poliakova, A. (1998). Secure Billing for Mobile Information Services in UMTS. In: *Lecture Notes in Computer Science*: *vol. 1430*, (535-548). Presented at the IS&N 1998, 25 May 1998-28 May 1998. Open Access

Horn, G., Howard, P., Martin, K., Mitchell, C., Preneel, B., Rantos, K. (1998). Trialling secure billing with trusted third party support for UMTS applications. In: *Proceedings of the 3rd ACTS Mobile Telecommunications Summit 1998*, (574-579). Presented at the 3rd ACTS Mobile Telecommunications Summit 1998, 08 Jun 1998-11 Jun 1998.

Van Rompay, B., Preneel, B., Vandewalle, J. (1998). On the security of dedicated hash functions. In: *Proceedings of the 19th Symposium on Information Theory in the Benelux*, (103-110). Presented at the 19th Symposium on Information Theory in the Benelux, 28 May 1998-29 May 1998.

Borst, J., Preneel, B., Vandewalle, J. (1998). On the time-memory tradeoff between exhaustive key search and table precomputation. In: *Proceedings of the 19th Symposium on Information Theory in the Benelux*, (111-118). Presented at the 19th Symposium on Information Theory in the Benelux, 28 May 1998-29 May 1998.

Vandewalle, J., Preneel, B., Csapodi, M. (1998). Data security issues, cryptographic protection methods, and the use of cellular automata. In: *5th IEEE International Workshop on Cellular Neural Networks and their Applications (CNNA 1998)*, (39-44). Presented at the CNNA 1998, England, UK, 17 Apr 1998-17 Apr 1998.

Rijmen, V., Preneel, B. (1997). A Family of Trapdoor Ciphers. In: *Lecture Notes in Computer Science*: *vol. 1267*, (139-148). Presented at the FSE 1997. Open Access

Preneel, B., Rijmen, V., van Oorschot, P. (1997). A security analysis of the Message Authenticator Algorithm (MAA). In: *European Transactions on Telecommunications and Related Technologies*: *vol. 8* (5), (455-470).

Preneel, B. (1997). Cryptanalysis of Message Authentication Codes. In: *Lecture Notes in Computer Science*: *vol. 1396*, (55-65). Presented at the ISW 1997, 17 Sep 1997-19 Sep 1997. Open Access

Preneel, B. (1997). Hash Functions and MAC Algorithms Based on Block Ciphers. In: *Lecture Notes in Computer Science*: *vol. 1355*, (270-282). Presented at the Cryptography and Coding, 6th IMA International Conference, 17 Dec 1997-19 Dec 1997. Open Access

Knudsen, L., Preneel, B. (1997). Fast and Secure Hashing Based on Codes. In: *Lecture Notes in Computer Science*: *vol. 1294*, (485-498). Presented at the CRYPTO 1997, 17 Aug 1997-21 Aug 1997. Open Access

Burge, P., Shawe-Taylor, J., Moreau, Y., Preneel, B., Stoermann, C., Cooke, C. (1997). Fraud detection and management in mobile telecommunications. In: *Conference on Security and Detection (ECOS 1997)*, (91-96). Presented at the ECOS 1997, London, UK, 28 Apr 1997-30 Apr 1997.

Preneel, B., Csapodi, M., Vandewalle, J. (1997). Cryptographic algorithms: basic concepts and applications to multimedia security. In: *Proceedings of the Design Automation Day on Cellular Computing Architectures for Multimedia and Intelligent Sensors, European Conference on Circuit Theory and Design (ECCTD 1997)*, (60-87). Presented at the Design Automation Day on Cellular Computing Architectures for Multimedia and Intelligent Sensors, European Conference on Circuit Theory and Design (ECCTD 1997), 31 Aug 1997-31 Aug 1997.

Preneel, B., vanOorschot, P.C. (1996). On the Security of Two MAC Algorithms. In: *Lecture Notes in Computer Science*: *vol. 1070*, (19-32). Presented at the EUROCRYPT 1996, 12 May 1996-16 May 1996. Open Access

Dobbertin, H., Bosselaers, A., Preneel, B. (1996). RIPEMD-160: A Strengthened Version of RIPEMD. In: *Lecture Notes in Computer Science*: *vol. 1039*, (71-82). Presented at the FSE 1996, 21 Feb 1996-23 Feb 1996. Open Access

Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., De Win, E. (1996). The Cipher SHARK. In: *Lecture Notes in Computer Science*: *vol. 1039*, (99-111). Presented at the FSE 1996, 21 Feb 1996-23 Feb 1996. Open Access

Anderson, R., Vaudenay, S., Preneel, B., Nyberg, K. (1996). The Newton Channel. In: *Lecture Notes in Computer Science*: *vol. 1174*, (151-156). Presented at the IH 1996, 30 May 1996-01 Jun 1996. Open Access

Knudsen, L., Preneel, B. (1996). Hash Functions Based on Block Ciphers and Quaternary Codes. In: *Lecture Notes in Computer Science*: *vol. 1163*, (77-90). Presented at the ASIACRYPT 1996, 03 Nov 1996-07 Nov 1996. Open Access

Moreau, Y., Preneel, B., Burge, P., Shawe-Taylor, J., Stoermann, C., Cooke, C. (1996). Novel techniques for fraud dectection in mobile telecommunications. In: *Proc. of the ACTS Mobile Summit*. Presented at the ACTS Mobile Summit, Grenada, Spain, 01 Nov 1996-01 Nov 1996.

Preneel, B., vanOorschot, P.C. (1995). MDx-MAC and Building Fast MACs from Hash Functions. In: *Lecture Notes in Computer Science*: *vol. 963*, (1-14). Presented at the CRYPTO 1995, 27 Aug 1995-31 Aug 1995. Open Access

Preneel, B. (1995). Fast software encryption: Second international workshop leuven, Belgium, december 14-16, 1994 proceedings. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 1008*. ISBN: 3540605908.

Rijmen, V., Preneel, B. (1995). Cryptanalysis of McGuffin. In: *Lecture Notes in Computer Science*: *vol. 1008*, (353-358). Presented at the FSE 1994, 14 Dec 1994-16 Dec 1994. Open Access

Rijmen, V., Preneel, B. (1995). Improved Characteristics for Differential Cryptanalysis of Hash Functions Based on Block Ciphers. In: *Lecture Notes in Computer Science*: *vol. 1008*, (242-248). Presented at the FSE 1994, 14 Dec 1994-16 Dec 1994. Open Access

Preneel, B. (1995). Software performance of encryption algorithms and hash functions. In: *Selected Areas in Cryptography, 2nd Annual International Workshop, SAC 1995*, (89-98). Presented at the SAC 1995, 18 May 1995-19 May 1995.

Rijmen, V., Preneel, B. (1995). On Weaknesses of Non-surjective Round Functions. In: *Selected Areas in Cryptography, 2nd Annual International Workshop, SAC 1995*, (100-106). Presented at the SAC 1995, 18 May 1995-19 May 1995.

Preneel, B., Nuttin, M., Rijmen, V., Buelens, J. (1994). Cryptanalysis of the CFB mode of the DES with a reduced number of rounds. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 773 LNCS*, (212-223). ISBN: 9783540577669.

Preneel, B. (1994). Message authentication with cryptographic hash functions. In: *Proceedings of the 2nd URSI Forum 1994*, (44-46). Presented at the 2nd URSI Forum 1994, 09 Dec 1994-09 Dec 1994.

Vandewalle, J., Govaerts, R., Preneel, B. (1993). Technical approaches to thwart computer fraud. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*: *vol. 708 LNCS*, (20-30). ISBN: 9783540573418.

Preneel, B. (1993). Standardization of cryptographic techniques. In: *Lecture Notes in Computer Science*: *vol. 741*, (162-173). Presented at the State of the Art and Evolution of Computer Security and Industrial Cryptography, 1993, 01 Jun 1993-04 Jun 1993.

Preneel, B., Govaerts, R., Vandewalle, J. (1993). Hash Functions Based on Block Ciphers: A Synthetic Approach. In: *Lecture Notes in Computer Science*: *vol. 773*, (368-378). Presented at the CRYPTO 1993, 22 Aug 1993-26 Aug 1993. Open Access

Preneel, B. (1993). Design Principles for Dedicated Hash Functions. In: *Lecture Notes in Computer Science*: *vol. 809*, (71-82). Presented at the FSE 1993, 09 Dec 1993-11 Dec 1993. Open Access

Preneel, B., Govaerts, R., Vandewalle, J. (1993). Information authentication: hash functions and digital signatures. In: *Lecture Notes in Computer Science*: *vol. 741*, (87-131). Presented at the State of the Art and Evolution of Computer Security and Industrial Cryptography, 1993, 01 Jun 1993-04 Jun 1993.

Preneel, B., Govaerts, R., Vandewalle, J. (1993). Differential Cryptanalysis of Hash Functions Based on Block Ciphers. In: *Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS 1993)*, (183-188). Presented at the CCS 1993, 03 Nov 1993-05 Nov 1993.

Preneel, B., Govaerts, R., Vandewalle, J. (1993). Cryptographic hash functions. In: *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, (161-171). Presented at the 3rd Symposium on State and Progress of Research in Cryptography, 15 Feb 1993-16 Feb 1993.

Govaerts, R., Vandewalle, J., Preneel, B. (1993). Technical approaches to thwart computer fraud. In: *Lecture Notes in Computer Science*: *vol. 741*, (19-29). Presented at the State of the Art and Evolution of Computer Security and Industrial Cryptography, 1993, 01 Jun 1993-04 Jun 1993.

Preneel, B., Govaerts, R., Vandewalle, J. (1992). An Attack on Two Hash Functions by Zheng-Matsumoto-Imai. In: *Lecture Notes in Computer Science*: *vol. 718*, (535-538). Presented at the ASIACRYPT 1992, 13 Dec 1992-16 Dec 1992. Open Access

Govaerts, R., Preneel, B., Vandewalle, J. (1992). On the Power of Memory in the Design of Collision Resistant Hash Functions. In: *Lecture Notes in Computer Science*: *vol. 718*, (105-121). Presented at the ASIACRYPT 1992, 13 Dec 1992-16 Dec 1992. Open Access

Govaerts, R., Preneel, B., Vandewalle, J., Bosselaers, A. (1992). A software implementation of the McEliece public-key cryptosystem. In: *Proceedings of the 13th Symposium on Information Theory in the Benelux*, (119-126). Presented at the 13th Symposium on Information Theory in the Benelux, 01 Jun 1992-02 Jun 1992.

Preneel, B., Govaerts, R., Vandewalle, J. (1992). Hash functions for information authentication. In: *6th Annual European Conference on Computer Systems and Software Engineering (COMPEURO 1992)*, (475-480). Presented at the COMPEURO 1992, 04 May 1992-08 May 1992.

PRENEEL, B., CHAUM, D., FUMY, W., JANSEN, C.J A., LANDROCK, P., ROELOFSEN, G. (1991). RACE INTEGRITY PRIMITIVES EVALUATION (RIPE) - A STATUS-REPORT. In: D.W. Davies (Eds.), *ADVANCES IN CRYPTOLOGY - EUROCRYPT 91*: *vol. 547*, (547-551). Presented at the WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, BRIGHTON, ENGLAND, 08 Apr 1991-11 Apr 1991. ISBN: 3-540-54620-0. (URL)

Preneel, B., Bosselaers, A., Govaerts, R., Vandewalle, J. (1990). A chosen text attack on the modified cryptographic checksum algorithm of Cohen and Huang. In: *Lecture Notes in Computer Science*: *vol. 435*, (154-163). Presented at the CRYPTO 1989, 17 Aug 1989-21 Aug 1989. Open Access

Preneel, B., Van Leekwijck, W., Van Linden, L., Govaerts, R., Vandewalle, J. (1990). An extension of higher order propagation criteria for Boolean functions. In: *Proceedings of the 11th Symposium on Information Theory in the Benelux*, (52-59). Presented at the 11th Symposium on Information Theory in the Benelux, 25 Oct 1990-26 Oct 1990.

Preneel, B., Bosselaers, A., Govaerts, R., Vandewalle, J. (1989). Collision free hash functions based on blockcipher algorithms. In: *23rd IEEE International Carnahan Conference on Security Technology (CCST 1989)*, (203-210). Presented at the CCST 1989, 02 Oct 1989-05 Oct 1989.

Accepted Conference Proceedings

Robyns, P., Marín Fàbregas, E., Lamotte, W., Quax, P., Singelée, D., Preneel, B. (2017). Physical-Layer Fingerprinting of LoRa devices using Supervised and Zero-Shot Learning. In: *Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2017)*. Presented at the WiSec 2017, 18 Jul 2017-20 Jul 2017.

Zhang, R., Preneel, B. (2017). On the Necessity of a Prescribed Block Validity Consensus: Analyzing Bitcoin Unlimited Mining Protocol. In: *International Conference on emerging Networking EXperiments and Technologies - CoNEXT 2017*. Presented at the CoNEXT 2017, 12 Dec 2017-15 Dec 2017.

Ashur, T., Delvaux, J., Lee, S., Maene, P., Marín Fàbregas, E., Nikova, S., Reparaz, O., Rozic, V., Singelée, D., Yang, B., Preneel, B. (2017). A Privacy-Preserving Device Tracking System Using a Low-Power Wide-Area Network (LPWAN). In: *Lecture Notes in Computer Science*. Presented at the CANS 2017, 30 Nov 2017-02 Dec 2017. Open Access

Marín Fàbregas, E., Singelée, D., Garcia, F., Chothia, T., Willems, R., Preneel, B. (2016). On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them. In: *Annual Computer Security Applications Conference (ACSAC)*. Presented at the Annual Computer Security Applications Conference, 05 Dec 2016-09 Dec 2016.

Ramos Araújo Beato, F., Ion, I., Capkun, S., Langheinrich, M., Preneel, B. (2013). For Some Eyes Only: Protecting Online Information Sharing. In: *ACM Conference on Data and Application Security and Privacy*. Presented at the ACM CODASPY, 18 Feb 2013-20 Feb 2013.

Mavrogiannopoulos, N., Pashalidis, A., Preneel, B. (2012). Security implications in Kerberos by the introduction of smart cards. In: *Proceedings of the 7th ACM Symposium on Information, Computer, and Communications Security (ASIACCS 2012)*. Presented at the ASIACCS 2012, 02 May 2012-04 May 2012.

Simoens, K., Yang, B., Zhou, X., Ramos Araújo Beato, F., Busch, C., Newton, E., Preneel, B. (2012). Criteria Towards Metrics for Benchmarking Template Protection Algorithms. In: *2012 5th IAPR International Conference on Biometrics*. Presented at the ICB 2012, 29 Mar 2012-01 Apr 2012.

Darazi, R., Sales, M., Weng, L., Macq, B., Preneel, B. (2011). Disparity Guided Exhibition Watermarking for 3D Stereo. In: *Proc. of International Workshop on Security and Privacy Preserving in e-Societies*. Presented at the SECES 2011, 09 Jun 2011-10 Jun 2011.

Velichkov, V., Rijmen, V., Preneel, B. (2009). Algebraic Cryptanalysis of a Small-Scale Version of Stream Cipher LEX. In: *Proceedings of the 30th Symposium on Information Theory in the Benelux*. Presented at the 30th Symposium on Information Theory in the Benelux, 28 May 2009-29 May 2009.

PhD Theses

Makri, E., Preneel, B. (sup.), Vercauteren, F. (cosup.) (2021). *Secure and Efficient Computing on Private Data*. Open Access

Bonte, C., Preneel, B. (sup.), Vercauteren, F. (cosup.) (2021). *Optimising Privacy-Preserving Computations*. Open Access

Beullens, W., Preneel, B. (sup.), Vercauteren, F. (cosup.) (2021). *The Design and Cryptanalysis of Post-Quantum Digital Signature Algorithms*. Open Access

Bootland, C., Preneel, B. (sup.), Vercauteren, F. (cosup.) (2021). *Efficiency and Security Aspects of Lattice-based Cryptography*. Open Access

Li, C., Preneel, B. (sup.) (2020). *New Methods for Symmetric Cryptography*. Open Access

Porto Balsa, E., Diaz Martinez, M.C. (sup.), Preneel, B. (cosup.) (2019). *Chaff-Based Profile Obfuscation*. Open Access

Zhang, R., Preneel, B. (sup.) (2019). *Analyzing and Improving Proof-of-Work Consensus Protocols*.

Friedberger, S., Preneel, B. (sup.), Hermans, J. (cosup.) (2019). *Security of Cryptographic Implementations*. Open Access

Iliashenko, I., Preneel, B. (sup.), Vercauteren, F. (cosup.) (2019). *Optimisations of Fully Homomorphic Encryption*. Open Access

Szepieniec, A., Preneel, B. (sup.), Vercauteren, F. (cosup.) (2018). *Mathematical and Provable Security Aspects of Post-Quantum Cryptography*. Open Access

Toli, C., Preneel, B. (sup.) (2018). *Secure and Privacy-Preserving Biometric Systems*. Open Access

Cleemput, S., Preneel, B. (sup.) (2018). *Secure and Privacy-friendly Smart Electricity Metering*. Open Access

Symeonidis, I., Preneel, B. (sup.) (2018). *Analysis and Design of Privacy-Enhancing Information Sharing Systems*. Open Access

Marín Fàbregas, E., Preneel, B. (sup.), Singelée, D. (cosup.) (2018). *Security and Privacy of Implantable Medical Devices*. 210Open Access

Kim, H., Hong, S. (sup.), Preneel, B. (sup.), Verbauwhede, I. (cosup.) (2017). *Side-Channel Security by Design: Hardware Level Countermeasures*.

Acar, M.G C., Diaz, C. (sup.), Preneel, B. (sup.) (2017). *Online Tracking Technologies and Web Privacy*. 214Open Access

Herrmann, M., Diaz, C. (sup.), Preneel, B. (sup.) (2016). *Privacy in Location-Based Services*. 284Open Access

Wang, Q., Preneel, B. (sup.), Rijmen, V. (cosup.), Gu, D. (cosup.) (2016). *Design and Cryptanalysis of Symmetric Key Primitives*. 253

Luykx, A., Preneel, B. (sup.) (2016). *The Design and Analysis of Message Authentication and Authenticated Encryption Schemes*. Open Access

Pérez Solà, C., Preneel, B. (sup.), Diaz, C. (cosup.), Herrera Joancomartí, J. (cosup.) (2016). *Towards Understanding Privacy Risks in Online Social Networks*. 234

Ramos Araújo Beato, F., Preneel, B. (sup.) (2015). *Private Information Sharing in Online Communities*. 184

Bilgin, B., Rijmen, V. (sup.), Preneel, B. (cosup.), Petkova-Nikova, S. (cosup.), Hartel, P. (cosup.) (2015). *Threshold Implementations: As Countermeasure Against Higher-Order Differential Power Analysis*. Open Access

De Mulder, Y., Preneel, B. (sup.) (2014). *White-Box Cryptography: Analysis of White-Box AES Implementations (White-Box Cryptografie: Analyse van White-Box AES implementaties)*. Open Access

Ottoy, G., Preneel, B. (sup.), De Strycker, L. (sup.) (2013). *Study and Design of a Reusable Embedded Hardware Architecture for Secure Wireless Communication (Studie en ontwerp van een herbruikbare ingebedde hardware architectuur voor veilige draadloze communicatie)*. Open Access

Mavrogiannopoulos, N., Preneel, B. (sup.) (2013). *Secure Communications Protocols and the Protection of Cryptographic Keys (Beveiligde communicatieprotocollen en bescherming van cryptografische sleutels)*. 232Open Access

Mennink, B., Preneel, B. (sup.), Rijmen, V. (sup.) (2013). *Provable Security of Cryptographic Hash Functions (Bewijsbare veiligheid van cryptografische hashfuncties)*.

Rial Duran, A., Preneel, B. (sup.) (2013). *Privacy-Preserving E-Commerce Protocols (Privacy-beschermende E-Commerce protocollen)*. 318

Yoshida, H., Preneel, B. (sup.) (2013). *Design and Analysis of Cryptographic Hash Functions (Ontwerp en analyse van cryptografische hashfuncties)*. 276

Schellekens, D., Preneel, B. (sup.) (2013). *Design and Analysis of Trusted Computing Platforms (Ontwerp en analyse van vertrouwde computerplatformen)*. 213+22Open Access

Simoens, K., Preneel, B. (sup.) (2012). *Analysis of Fuzzy Encryption Schemes for the Protection of Biometric Data (Analyse van fuzzy encryptieschema's voor het afschermen van biometrische gegevens)*.

Schiffner, S., Preneel, B. (sup.) (2012). *Design and Modeling of Privacy-Friendly Reputation (Ontwerp en modellering van privacy vriendelijke reputatie-systemen)*.

Weng, L., Preneel, B. (sup.) (2012). *Perceptual Multimedia Hashing (Perceptuele multimedia hashing)*. 208

Hermans, J., Preneel, B. (sup.), Vercauteren, F. (sup.), Vercauteren, F. (cosup.) (2012). *Lightweight Public Key Cryptography (Lichtgewicht publieke-sleutel cryptografie)*.

Mouha, N., Preneel, B. (sup.) (2012). *Automated Techniques for Hash Function and Block Cipher Cryptanalysis (Automatische technieken voor hashfunctie- en blokcijfercryptanalyse)*. 284Open Access

Peeters, R., Preneel, B. (sup.) (2012). *Security Architecture for Things That Think (Beveiligingsarchitectuur voor intelligente objecten)*. 148+20

Wouters, K., Preneel, B. (sup.) (2012). *Hash-Chain based Protocols for Time-Stamping and Secure Logging: Formats, Analysis and Design (Hash-keten gebaseerde protocollen voor tijdszegels en beveiligde logbestanden: formaten, analyse en ontwerp)*.

Cappaert, J., Preneel, B. (sup.) (2012). *Code Obfuscation Techniques for Software Protection (Code obfuscatietechnieken voor softwarebeveiliging)*. 112+14

Küçük, Ö., Preneel, B. (sup.), Rijmen, V. (sup.) (2012). *Design and Analysis of Cryptographic Hash Functions (Ontwerp en analyse van cryptografische hashfuncties)*.

Bichsel, P., Preneel, B. (sup.), Camenish, J. (cosup.) (2012). *Cryptographic Protocols and System Aspects for Practical Data-minimizing Authentication (Cryptographische protocollen en systeemaspecten voor praktische data-minimaliserende authenticatie)*. 234Open Access

Velichkov, V., Preneel, B. (sup.), Rijmen, V. (sup.) (2012). *Recent Methods for Cryptanalysis of Symmetric-key Cryptographic Algorithms (Recente Methoden voor de Cryptanalyse van Symmetrische-sleutel Cryptografische Algoritmen)*. 256

Fan, J., Preneel, B. (sup.), Verbauwhede, I. (sup.) (2012). *Efficient Arithmetic for Embedded Cryptography and Cryptanalysis (Efficiënte aritmetica voor ingebedde cryptografie en cryptanalyse)*. 153

De Cock, D., Preneel, B. (sup.) (2011). *Contributions to the Analysis and Design of Large-Scale Identity Management Systems (Bijdragen aan de analyse en het ontwerp van grote identiteitsbeheerssystemen)*.

Gonzalez Troncoso, C., Preneel, B. (sup.), Diaz Martinez, M.C. (sup.) (2011). *Design and Analysis Methods for Privacy Technologies (Ontwerp- en analysemethodes van privacytechnologieën)*. 189+17

Sekar, G., Preneel, B. (sup.) (2011). *Cryptanalysis and Design of Symmetric Cryptographic Algorithms (Cryptanalyse en ontwerp van symmetrische cryptografische algoritmen)*. 256

Käsper, E., Preneel, B. (sup.) (2011). *Information Theoretic Methods in Cryptography (Informatietheoretische methoden in de cryptografie)*.

Gierlichs, B., Verbauwhede, I. (sup.), Preneel, B. (sup.) (2011). *Statistical and Information-Theoretic Methods for Power Analysis on Embedded Cryptography (Statistische en informatietheoretische methoden voor vermogensanalyse op ingebedde cryptografie)*.

Andreeva, E., Preneel, B. (sup.) (2010). *Domain Extenders for Cryptographic Hash Functions (Domeinuitbreidingen voor cryptografische hashfuncties)*. 194

Faust, S., Preneel, B. (sup.), Neven, G. (cosup.) (2010). *Provable Security at Implementation-Level (Bewijsbare veiligheid op implementatieniveau)*. 167

De Mulder, E., Preneel, B. (sup.), Verbauwhede, I. (sup.) (2010). *Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices (Elektromagnetische technieken en probes voor nevenkanaalsanalyse op cryptografische toestellen)*. 170+40

Deng, M., Preneel, B. (sup.) (2010). *Privacy Preserving Content Protection (Privacy behoud content protection)*. 244Open Access

Gürses, F.S., Berendt, B. (sup.), Preneel, B. (sup.) (2010). *Multilateral Privacy Requirements Analysis in Online Social Network Services (Analyse van multilaterale privacyvereisten voor Internetgebaseerde sociale netwerkdiensten)*.

Indesteege, S., Preneel, B. (sup.) (2010). *Analysis and Design of Cryptographic Hash Functions (Analyse en ontwerp van cryptografische hashfuncties)*. 306+xxOpen Access

Kohlweiss, M., Preneel, B. (sup.) (2010). *Cryptographic Protocols for Privacy Enhanced Identity Management (Cryptografische protocollen voor identiteitsbeheer met een verbeterde privacy)*. 257Open Access

Wyseur, B., Preneel, B. (sup.) (2009). *White-Box Cryptography (White-box cryptografie)*. Open Access

Singelée, D., Preneel, B. (sup.) (2008). *Study and Design of a Security Architecture for Wireless Personal Area Networks (Studie en ontwerp van een beveiligingsarchitectuur voor draadloze Personal Area Netwerken)*. Open Access

Wu, H., Preneel, B. (sup.) (2008). *Cryptanalysis and Design of Stream Ciphers (Cryptanalyse en ontwerp van stroomcijfers)*. Open Access

Sakiyama, K., Preneel, B. (sup.), Verbauwhede, I. (sup.) (2007). *Secure Design Methodology and Implementation for Embedded Public-Key Cryptosystems (Veilige ontwerpen en methoden voor ingebedde publieke sleutel crypto-grafische systemen)*. Open Access

Mentens, N., Preneel, B. (sup.), Verbauwhede, I. (sup.) (2007). *Secure and efficient coprocessor design for cryptographic applications on FPGAs*. Open Access

De Cannière, C., Preneel, B. (sup.) (2007). *Analysis and Design of Symmetric Encryption Algorithms (Analyse en ontwerp van symmetrische encryptie-algoritmen)*.

Kim, J., Preneel, B. (sup.), Lee, S. (cosup.) (2006). *Combined Differential, Linear and Related-Key Attacks on Block Ciphersand MAC AlgorithmsCombined Differential, Linear and Related-Key Attacks on Block Ciphersand MAC Algorithms (Gecombineerde differentiële, lineaire enverwante-sleutel aanvallen op blokcijfers en MAC algoritmes)*.

Paul, S., Preneel, B. (sup.) (2006). *Cryptanalysis of Stream Ciphers Based on Arrays and Modular Addition (Cryptanalyse van stroomcijfers gebaseerd op arrays en modulaire optelling)*.

Lano, J., Preneel, B. (sup.) (2006). *Cryptanalysis and Design of Synchronous Stream Ciphers (Cryptanalyse en ontwerp van synchrone stroomcijfers)*. Open Access

Vanden Berghe, C., Piessens, F. (sup.), Preneel, B. (cosup.) (2006). *Pragmatic Countermeasures for Implementation-Related Vulnerabilities in Web Applications (Pragmatische tegenmaatregelen voor implementatie-gerelateerde beveiligingszwakheden in webtoepassingen)*. 141Open Access

Seys, S., Preneel, B. (sup.) (2006). *Cryptographic Algorithms and Protocols for Security and Privacy in Wireless Ad Hoc Networks (Algoritmen en protocollen voor beveiliging en privacy in draadloze ad-hoc netwerken)*. Open Access

Braeken, A., Preneel, B. (sup.) (2006). *Cryptographic Properties of Boolean Functions and S-Boxes (Cryptografische eigenschappen van Booleaanse functies en S-Boxen)*. Open Access

Diaz, C., Preneel, B. (sup.), Vandewalle, J. (cosup.) (2005). *Anonymity and Privacy in Electronic Services (Anonimiteit en geheimhouding in elektronische diensten)*.

Batina, L., Preneel, B. (sup.), Verbauwhede, I. (cosup.) (2005). *Arithmetic and Architectures for Secure Hardware Implementations of Public-Key Cryptography (Bewerkingen en architecturen voor veilige hardware implementaties van publieke sleutel cryptografie)*.

Wolf, C., Preneel, B. (sup.) (2005). *Multivariate Quadratic Polynomials in Public Key Cryptography (Stelsels van multivariate kwadratische veeltermen in publieke sleutelcryptografie)*. Open Access

Örs, S., Preneel, B. (sup.), Verbauwhede, I. (cosup.) (2005). *Hardware Design of Elliptic Curve Cryptosystems and Side-Channel Attacks (Hardware ontwerp van elliptische kromme cryptosystemen en nevenkanaal aanvallen)*.

Nakahara Junior, J., Preneel, B. (sup.), Vandewalle, J. (sup.) (2003). *Cryptanalysis and design of block ciphers*. 234+xix

Borst, J., Preneel, B. (sup.), Vandewalle, J. (cosup.) (2001). *Block Ciphers: Design, Analysis and Side-Channel Analysis*. xv1+152Open Access

Internet publications

Zhang, R., Zhang, D., Wang, Q., Xie, J., Preneel, B. (2020). NC-Max: Breaking the Throughput Limit of Nakamoto Consensus. (URL) Open Access

Mühlberg, J.T., Van Bulck, J., Maene, P., Noorman, J., Preneel, B., Verbauwhede, I., Piessens, F. (2019). Architectural security for embedded control systems. (professional oriented)

Beullens, W., Szepieniec, A., Vercauteren, F., Preneel, B. LUOV: Signature scheme proposal for NIST PQC project. (URL)

Other

Preneel, B. (2012). The hash function crisis and its solution. *Hakin9*, *2012* (1), 30-33.