Publications by Mats Näslund (Updated March 22, 2019)

Externally Reviewed Scientific Publications (Journals and Books)

[1] M. Näslund, *On Steiner Triple Systems and Perfect Codes*, Ars Combinatoria 53 (1999), 129-132.
[2] M. I. Gonzàlez Vasco and M. Näslund, *A Survey of Bit-security and Hard-core Functions*, In "Computational Number Theory and Cryptography", pp. 227-256, Birkhäuser, 2000.
[3] M. Näslund and A. Russell, *Achieving Optimal Fairness from Biased Coinflips*, In "Computational Number Theory and Cryptography", pp. 303-320, Birkhäuser, 2000.
[4] M. Näslund and A. Russell, *Extraction of Optimally Unbiased Bits from a Biased Source*, IEEE Trans. on Information Theory, vol IT-48 (2000), no 3, 1093-1103.
[5] M. Goldmann, M. Näslund, and A. Russell, *Complexity Bounds on General Hard-core Predicates*, Journal of Cryptology 14 (2001), 177-195.
[6] J. Håstad and M. Näslund, *The Security of all RSA and Discrete Log bits*, Journal of the ACM 51 (2004), no 2, 187-230.
[7] R. Blom, E. Carrara, F. Lindholm, K. Norrman and M. Näslund, *Key Management and Protection for IP Multimedia,* In "Multimedia Security Handbook", CRC Press, 2004.
[8] J. Håstad and M. Näslund, *Efficient construction of provably secure pseudo-randomness primitives,* Journal of Cryptology, Journal of Cryptology 21 (2008), no 1, 1-26.
[9] N. Gonzalez, C. Miers, F. Redigolo, M. Simplicio Jr, T. Carvalho, M. Näslund and M. Pourzandi, *A quantitative analysis of current security concerns and solutions for cloud computing*, Journal of Cloud Computing: Advances, Systems and Applications, vol 1, no 11. (Earlier version in IEEE CloudCom 2011, p 231-238.)
[10] L. H. Iwaya, M. A. L. Gomes, M. Simplício, T. Carvalho, C. Dominicini, R. Sakuragui, M. Rebelo, M. Gutierrez, M. Näslund and P. Håkansson, *Mobile health in emerging countries: A survey of research initiatives in Brazil*, International Journal of Medical Informatics, Volume 82, Issue 5, 283-298, 2013.
[11] M. Simplicio Jr, L. Iwaya, B. Barros, T. Carvalho and M. Näslund, *SecourHealth: a delay-tolerant security framework for mobile health data collection*, IEEE Journal of Biomedical and Health Informatics, vol 19 (2), 761-772, 2015.
[12] E. Dubrova, M. Näslund, G. Carlsson, J. Fornehed and B. Smeets, *Two countermeasures against hardware Trojans exploiting non-zero aliasing probability of BIST*, Journal of Signal Processing Systems, 371-381, June 2017.
[13] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P. Kumar Nakarmi, M. Näslund, P. O'Hanlon, J. Papay, J. Suomalainen, M. Surridge, J.-P. Wary and A. Zahariev, *A Security Architecture for 5G Networks*, IEEE Access, vol 6, 22466-22479, 2018.
[14] E. Dubrova, M. Näslund, G. Selander and F. Lindqvist, *Message authentication based on cryptographically secure CRC without polynomial irreducibility test*, Cryptography and Communications 10 (2), 383-399, Mar 2018.

Conference and Workshop Presentations

[1] M. Näslund, *Universal Hash Functions and Hard Core Bits*, Proceedings, Advances in Cryptology - EUROCRYPT '95, Saint Malo, France. LNCS 921, pp. 356-366, Springer Verlag, 1995.
[2] M. Näslund, *All Bits in ax+b mod p are Hard*, Proceedings, Advances in Cryptology - CRYPTO '96, Santa Barbara, Ca. LNCS 1109, pp. 114-128, Springer Verlag, 1996.
[3] M. Goldmann and M. Näslund, *The Complexity of Computing Hard Core Predicates*, Proceedings, Advances in Cryptology - CRYPTo '97, Santa Barbara, Ca. LNCS 1294, pp.1-15, Springer Verlag, 1997.
[4] M. Näslund and A. Russell, *Extraction of Optimally Unbiased Bits from a Biased Source (extended abstract)*, Proceedings, ITW '98, Killarney, Ireland. pp. 90-91, IEEE, 1998.
[5] J. Håstad and M. Näslund, *The Security of Individual RSA bits*, Proceedings of IEEE FOCS '98, Palo Alto, Ca. pp. 510-519, IEEE, 1998.
[6] M. Näslund and A. Russell, *Hard Core Functions: Survey and New Results*, Proceedings, Nordsec '99, Stockholm, Sweden. pp. 305-322, 1999.
[7] J. Håstad and M. Näslund, *BMGL: Synchronous Key-stream Generator with Provable Security*, Proceedings, 1st Open NESSIE Workshop, Leuven, Belgium. Nov. 2000.

[8] R. Blom, M. Näslund and G. Selander, *Object Security and Personal Information Management*, Proceedings, INET 2001, Stockholm, Sweden.
[9] J. Håstad and M. Näslund, *Improved Analysis of the BMGL Key-stream Generator*, Proceedings, 2nd Open NESSIE Workshop, Egham, UK. Sep. 2001.
[10] M. I. Gonzàlez Vasco, M. Näslund and I. E. Shparlinski, *Trace Interpolation Problem for Polynomials over Finite Fields*, Proceedings of the 14th Applied Algebra, Algebraic Algorithms, and Error-correcting Codes (AAECC) Conference, Melbourne, Australia, Nov. 2001.
[11] J. Håstad and M. Näslund, *Practical Construction and Analysis of Pseudo-randomness Primitives*, Proceedings, Advances in Cryptology - Asiacrypt '01, Gold Coast, Austraila, LNCS vol 2248, pp. 442-459, Springer Verlag, 2001.
[12] M. I. Gonzàlez Vasco, M. Näslund and I. E. Shparlinski, *The Hidden Number Problem in Extension Fields and Its Applications*, "Latin American Theoretical Informatics" (LATIN02), Cancun, Mexico, LNCS vol 2286, pp. 105-117, Springer Verlag, 2002.
[13] W-C. W. Li, M. Näslund and I. E. Shparlinski, *Hidden Number Problem with the Trace and Bit Security of XTR and LUC*, Proceedings, Advances in Cryptology - CRYPTO '02, Santa Barbara, CA, LNCS vol 2442, pp. 433-448, Springer Verlag, 2002.
[14] M. Näslund, *Security for Real Time Multimedia in Heterogeneous Environments*, Proceedings, RSA Europe 2002, Paris, France, Oct. 2002.
[15] M. Näslund and I. E. Shparlinski and W. Whyte, *On the bit-security of NTRU*, Proceedings of PKC 03, LNCS vol 2567, pp. 62-70, Springer-Verlag, 2003.
[16] M. I. Gonzàlez Vasco, M. Näslund and I. E. Shparlinski, *New results on the bit-security of Diffie-Hellman*, Proceedings of PKC 04, LNCS vol 2947, pp. 159-172, Springer-Verlag, 2004.
[17] P. Chandrasiri, O. Gurleyen, C. Gehrmann, A. Jonsson, and M. Näslund, *Personal Security Domains*, In proceedings of 2nd International Workshop on Wireless Security, 6-7 April, 2004, London, UK.
[18] J. Håstad and M. Näslund, *The stream cipher Polar Bear*, SKEW Workshop, May 2005.
[19] Y. R. Venturini, R. R. Sakuragui, R. Matushima, T. Carvalho, W. V. Ruggiero, M. Näslund and M. Pourzandi, *Security Enforcement Layer for Security Domain*, proceedings of 4th International Information and Telecommunication Technologies Symposium, 2005.
[20] R. Matushima, Y. R. Venturini, R. Sakuragui, T. Carvalho, W. V. Ruggiero, M. Näslund and M. Pourzandi, *Multiple personal security domains*, Proceedings of IWCMC 2006, pp. 361-366.
[21] Y. Venturini, V. Coroama, T. Carvalho, M. Näslund and M. Pourzandi, *Security for Context-Aware ad-hoc Networking Applications*, In Advanced of ad-hoc networking, IFIP vol 265, pp. 145-156, Springer-Verlag, 2008.
[22] M. Simplıcio Jr, P. S. L. M. Barreto, T. Carvalho, C. Margi and M. Näslund, *The CURUPIRA-2 block cipher for constrained platforms: specification and benchmarking,* proceedings of PiLBA '08.
[23] R. Blom, P. de Bruin, J. Eman, M. Folke, H. Hannu, M. Näslund, M. Stålnacke and P. Synnergren, *Public Safety Communication using Commercial Cellular Technology*, Proceedings of NGMAST 2008, pp. 291-296.
[24] C. Margi, B. T. de Oliveira, G. Sousa, M. Simplicio Jr, P. Barreto, T. Carvalho, M. Näslund and R. Gold, *Security Mechanisms Impact and Feasibility on Wireless Sensor Networks Applications,* demonstration at IEEE INFOCOM 2009.
[25] M. Simplício Jr, V. Coroama, T. Carvalho, M. Näslund and M. Pourzandi, *PHD – A Generic and Flexible Architecture for IPTV in Authorized Domains*, proceedings, Proceedings of AINA 2009, pp. 487-494.
[26] C. Margi, B. T. de Oliviera, G. de Sousa, M. Simplicio, P. Barreto, T. Carvalho, M. Näslund and R. Gold, *Impact of Operating Systems on Wireless Sensor Networks (Security) Applications and Testbeds*, Proceedings of ICCCN 2010, pp. 1-6, 2010.
[27] C. Dominicini, M. Simplício, R. Sakuragui, T. Carvalho, M. Näslund and M. Pourzandi, *Threat Modeling ad Identity Management System for Mobile Internet*, Proceedings of I2TS 2010.
[28] N. Gonzalez, C. Miers, F. Redígolo, M. Simplício, L. Simões, T. Carvalho, M. Näslund and M. Pourzandi, *A taxonomy for cloud computing services*, Proceedings of CLOSER 2011, pp. 56-65, 2011.
[29] S. Baucke, D. Catrein, C. Curescu, J. Halén, J. Kempf, Y. Lemieux, B. Melander, J. Mångs, M. Näslund, A. Shohel, J. Ylitalo and S. Thorelli, *Cloud Computing and Telecommunications: Business Opportunities, Technologies and Experimental Setup,* World Telecommunication Congress (WTC) 2012, pp. 1-6, 2012.

[30] Y. Cheng, M. Näslund, G. Selander and E. Fogelström, *Privacy in Machine-to-Machine Communications, A state-of-the-art survey*, Proceedings of the 13th International Conference on Communication Systems (IEEE ICCS), Nov. 2012.
[31] N. Gonzalez, M. Torrez Rojas, M. da Silva, F. Redígolo, T. Carvalho, C. Miers, M. Näslund and A.S. Ahmed, *A framework for authentication and authorization credentials in cloud computing,* Proceedings of IEEE TrustCom-13, pp. 509-516, 2013.
[32] E. Dubrova, M. Näslund and G. Selander, *Secure and Efficient LBIST for Feedback Shift Register-Based Cryptographic Systems*, proceedings of European Test Symposium (ETS), pp. 1-6, 2014.
[33] J. Mattsson and M. Näslund, *Detection and Mitigation of HTTPS Man-in-the-Middles and Impersonators*, W3C WebCrypto workshop, 2014.
[34] E. Dubrova, M. Näslund and G. Selander, *Energy-Efficient Message Authentication for IEEE 802.15.4-Based Wireless Sensor Networks,* proceedings of IEEE NORCHIP, pp. 1-4, 2014.
[35] E. Dubrova, M. Näslund, G. Carlsson and B. Smeets, *Keyed Logic BIST for Trojan Detection*, proceedings of IEEE International Symposium on System-on-Chip (SOC'2014), pp. 1-4, 2014.
[36] E. Dubrova, M. Näslund and G. Selander, *CRC-based message authentication for 5G mobile technology*, proceedings of IEEE Trustcom, pp. 1186-1191, Aug 2015.
[37] M. Näslund, E. Dubrova, G. Selander and F. Lindqvist, *A random access procedure based on tunable puzzles*, proceedings of IEEE Communications and Network Security (CNS), pp. 535-540, 2015.
[38] E. Dubrova, K. Norrman and M. Näslund, *Protecting IMSI and user privacy in 5G networks*, proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, pp. 159-166, 2016.
[39] C. Baumann, M. Näslund, C. Gehrmann, O. Schwarz and H. Thorsen, *A high assurance virtualization platform for ARMv8*, proceedings of the European Conference on Networks and Communications (EuCNC), pp. 210-214, 2016.
[40] E. C. Jiménez, P. K. Nakarmi, M. Näslund and K. Norrman, *Subscription identifier privacy in 5G systems*, proceedings of IEEE MoWNet, pp. 1-8, 2017.
[41] M. A. Torrez Rojas, F. F. Redígolo, N. M. Gonzalez, F. V. Sbampato, T. C. M. de Brito Carvalho, K. W. Ullah, M. Näslund and A. S. Ahmed, *Managing the Lifecycle of Security SLA Requirements in Cloud Computing*, Developments and Advances in Intelligent Systems and Applications, pp. 119-140, Springer, 2018.
[42] E. Dubrova, M. Näslund, G. Selander and F. Lindqvist, *Lightweight Message Authentication for Constrained Devices*, proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp. 196-201, 2018.
[43] Y. Yu, E. Dubrova, M. Näslund and S. Tao, *On Designing PUF-Based TRNGs with Known Answer Tests*, proceedings of the 2018 IEEE Nordic Circuits and Systems Conference (NORCAS): NORCHIP and International Symposium of System-on-Chip (SoC), pp. 1-6, 2018.

Co-authored Internet Standards (IETF)

[1] *RFC 3711, The Secure Real Time Transport Protocol,* 2004.
[2] *RFC 3830, MIKEY: Multimedia Internet KEYing,* 2004.
[3] *RFC 4169, Digest AKA version 2,* 2005.
[4] *RFC 4567, Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP),* 2006.
[5] *RFC 4771, Integrity Transform Carrying Roll-Over Counter,* 2007.
[6] *RFC 6043*, *MIKEY-TICKET: Ticket Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY),* 2011.

Patents

Named (co)inventor of more than 100 patent families.