CURRICULUM VITAE

Personal Details

Name	Kaisa Tellervo Nyberg (née Holma)
Born	13 May 1948
Spouse	Ernst René Anselm Nyberg
Children	Eeva Silja (1976)
	Anna Maria (1977)
	Katariina Fanny (1984)

Education

Student	Tapiolan Yhteiskoulu	1966
Master in Science	University of Helsinki (Mathematics)	1971
Doctor in Philosophy	University of Helsinki (Mathematics)	1982

Employment

Statistician	Social Insurance Institution	1971
Assistant	University of Helsinki, Dept. of mathematics	1971–1982
Assistant	University of Helsinki, Dept. of mathematics	1986
Lecturer	University of Helsinki, Dept. of mathematics	1987
Special Researcher	Finnish Defence Forces	1987–1991
Special Researcher	Finnish Defence Forces	1996–1998
Principal Scientist, Nokia Research Center		1998–2000
Research Fellow, Nokia Research Center		2000–2012
Professor, Helsinki University of Technology		2005–2009
Professor, Aalto University School of Science		2010–2016
Professor emerita, Aalto University School of Science		2016–

Side Employment

Teaching associate, Cornell University	1982–1983
Docent (mathematics), University of Helsinki	1986–
Visiting lecturer, Universität Karlsruhe	1992
Visiting professor, TU Wien	1993
Docent (cryptology), Helsinki University of Technology	1997–2004
Academy of Finland, Council member	2000–2003

Research Fellow, Nokia Research Center 2005–2012

Scholarships

University of Helsinki Travel stipend 1980
Finnish Culture Fond stipend 1980
Academy of Finland travel stipends 1985, 1987

Awards

Ernst Lindelöf Master's thesis award 1971
Marshal Mannerheim Military Science Fond 2007
IACR Fellow 2015
Magnus Ehrnrooth Foundation 2015
Finnish Cultural Foundation 2018

Memberships

Finnish Mathematical Society 1971–
- board member 2004–2009

International Association for Cryptologic Research (IACR) 1988–
Finnish Academy of Science and Letters 2006–
Scientific Advisory Board for Defence, Board member 2006 – 2015

Program chair

EUROCRYPT 1998
Selected Areas of Cryptography SAC 2002
Fast Software Encryption FSE 2008
RSA Conference Cryptographers' Track 2015

Conference Board Memberships

Selected Areas of Cryptography SAC 2002–2004
Fast Software Encryption FSE 2011–2016
Dagstuhl Seminar 2014–
CT–RSA 2014–2017

Editorial Board Memberships

International Journal of Information Security, Springer-Verlag 2001 – 2006

International Journal of Security and Networks, Inderscience	2006 – 2010
Journal of Cryptology	2010 –
Transactions on Symmetric Cryptology	2016–

Research Projects with External Funding

Block cipher research project, MATINE	1991–1995
Krypto, Finnish Defence Forces	2005
Crydami, Academy of Finland	2004–2007
Stream cipher research project, MATINE	2006–2008
Ad Hoc –networks, Finnish Defence Forces	2006–2007
InHoNets, TEKES	2006–2007
Packet level authentication, TEKES	2006–2008
CACE, EU FP7	2008–2010
Symkrypto, MATINE	2010
BooMCrypt, Academy of Finland	2008–2011
Ecrypt Network of Excellence	2008–2012
PRIGENDA, Academy of Finland	2014–2016

Supervised Theses

Master's theses

Miia Hermelin. Cryptographic Properties of the Bluetooth Combination Generator. Helsinki University of Technology 2000

Kaarle Ritvanen. Protection of Data Confidentiality and Integrity in Radio Communications Systems. Helsinki University of Technology 2004

Jukka Valkonen. Ad-Hoc Security Associations for Wireless Devices. Helsinki University of Technology 2006

Billy Bob Brumley. Efficient Elliptic Curve Algorithms for Compact Digital Signatures. Helsinki University of Technology 2006

Risto Hakala. Linear Cryptanalysis of Two Stream Ciphers, Helsinki University of Technology 2007

Marc Santamaria. The Internet Password Authentication Protocol SCRAM and Its Security, Aalto University School of Science and Technology and Technical University of Catalonia, 2010

Gian Pietro Farina. Distinguishing Distributions Using One Bit Linear Trails in PRESENT Cipher, University of Milan, 2012

Md. Mohsin Ali Khan. Statistical Model of the Statistical Saturation Attack. Aalto University, 2015

Licentiate's theses

Maarit Hietalahti. Requirements for a Security Architecture for Clustered Ad-Hoc Networks, Helsinki University of Technology 2007

Dmitrij Lagutin. Redesigning Internet – The Packet Level Authentication Architecture, Helsinki University of Technology 2008

Mikko Kiviharju. Cryptographic Key Management Architectures for Environments with Independent Subdomains, Helsinki University of Technology, 2008

Billy Bob Brumley. Studies on Elliptic Curve Cryptography Engineering, Helsinki University of Technology, 2009

Jan-Erik Ekberg. Efficient Baseband Security, Aalto University School of Electrical Engineering, 2011

PhD theses

Sven Laur. Cryptographic Protocol Design, Helsinki University of Technology, 2008

Miia Hermelin. Multidimensional Linear Cryptanalysis, Aalto University School of Science and Technology, 2010

Billy Bob Brumley. Covert Timing Channels, Caching, and Cryptography, Aalto University School of Science, 2011

Risto Matti Hakala. Results on Linear Models in Cryptography, Aalto University School of Science, 2013

Hadi Soleimany. Studies in Lightweight Cryptography, Aalto University School of Science, 2015

Mikko Kiviharju. Enforcing Role-Based Access Control with Attribute-Based Cryptography for Environments with Multi-Level Security Requirements, Aalto University School of Science, 2016

PhD and Habilitation Thesis Committees

Arto Karila, Helsinki University of Technology 1991

Audun Josang, Norwegian University of Science and Technology, Trondheim, 1998

Helger Lipmaa, University of Tartu 1999

Knut Johannessen, Norwegian University of Science and Technology, Trondheim 1999

Tonnes Brekne, Norwegian University of Science and Technology, Trondheim 2001

Enes Pasalic, Universitet Lund, Sweden, February 2003

Hahnsang Kim, L'Institut National des Télécommunications and l'Université d'Evry-Val d'Essonne, 2006

Alexander Maximov, Lund University, Sweden, 2006

Panu Hamalainen, Tampere Technical University, Finland, 2006

Mårten Trolin, Royal Technical University, Sweden, 2006

Håkan Englund, Lund University, Sweden, 2007

Sylvain Pasini, Ecole Polytechnique Federale de Lausanne, Switzerland, 2008

Henri Gilbert, Ecole Normale Superieure (Habilitation thesis), 2008

René Mayrhofer, Vienna University (Habilitation thesis), 2009

Andrea Röck, Ecole Polytechnique and INRIA, France, 2009

Benoît Gérard, L'Université Pierre et Marie Curie and INRIA, France, 2010

Céline Blondeau, L'Université Pierre et Marie Curie and INRIA, France, 2011

Rune Ødegård, Norwegian University of Science and Technology, Trondheim, 2012

Kimmo Halunen, University of Oulu, Finland, 2012

Asli Bay, Ecole Polytechnique Federale de Lausanne, Switzerland, 2014

Scientific Evaluation Committees

Finland
2000 Turku University Computer Science Institute, TUCS

2000–2003 Academy of Finland, Council of Natural Science and Technology

1999–2003 Research program on Mathematical Modeling (MaDaMe), Academy of Finland
2002–2005 Proactive Computing Research Program (PROACT), Academy of Finland

2006 –2016 Scientific Advisory Board for Defence (MATINE)

Foreign
2003–2007 Norges forskningsråd, Information Technology Research Programme

2003–2008 ECRYPT European Network of Excellence, Strategic Board

2008–2012 ECRYPT II European Network of Excellence, Strategic Board

2007–2014 Belgian Science Policy Office

2010 Swiss National Science Foundation

2011 Evaluation of INRIA Theme "Algorithmics, Certification, and Cryptography"

2012–2015 NSERC (Canada) Computer Science Evaluation Panel

2013–2017 Research Council of Norway

2015–2016 CFREF Canada First Research Excellence Fund, Panel member

2015–2018 ERC European Research Council, External expert

2017 Canada 150 Research Chairs Program

2017-2018 Austrian Science Fund

Assessments

Professor (tenure), University of Bergen, Norway 2004

Professor (tenure), Newfoundland Memorial University Canada, Canada 2005

Professor, University College of London, UK 2006

Professor, VTT, Finland 2007

Associate professor, KTH, Stockholm, Sweden 2009

Senior Lecturer, University of Haifa, Israel, 2014

Professor, University of Luxembourg, 2014

Research Chair, McGill University, Canada, 2014

Invited Talks

Reed-Muller Workshop 2011, Cryptographic Nonlinearity

FSE 2012, "Provable" Security Against Differential and Linear Cryptanalysis

Indocrypt 2013, Linear Cryptanalysis and Its Extensions

Lightweight Crypto Day 2015, Improving Accuracy of Statistical Cryptanalysis

BalkanCryptSec 2015, Key Variance in Statistical Cryptanalysis

Publications

Peer-reviewed journal articles

1. Twisted sums of nuclear Fréchet spaces, T. Ketonen, K. Nyberg. *Ann. Acad. Sci. Fenn. Ser A I Math.* Vol. 7, 1982, 323-335.

2. Tameness of pairs of nuclear power series spaces and related topics, K. Nyberg. *Transactions of the American Mathematical Society*, vol. 283, number 2, June 1984, 645-660.

3. Splitting a twisted sum of Fréchet sequence spaces, K. Nyberg. *Doğa, Turkish J. Math*, Vol. 10, Num. 1, 1986, 202-208.

4. Splitting twisted sums of nuclear Köthe spaces, K. Nyberg. *Ann. Acad. Sci. Fenn. Ser A I Math.* Vol. 11, 1986, 233-237

5. A tame splitting theorem for Köthe spaces, K. Nyberg. *Arch. Math*. 52, 1989, 471-481.

6. Weaknesses in some recent key agreement protocols, K. Nyberg, R.A. Rueppel. *Electronics Letters* 30:1, 1994

7. Provable security against a differential attack, K. Nyberg, L.R. Knudsen. *Journal of Cryptology* 8:1, 1995

8. Message recovery for signature schemes based on the discrete logarithm problem, K. Nyberg and R.A. Rueppel. *Designs, Codes and Cryptography* 7:1-2, 1996

9. Correlation theorems in cryptanalysis, K. Nyberg. *Discrete Applied Mathematics* 111, 2001, 177-188

10. Manual authentication for wireless devices. C. Gehrmann, C. J. Mitchell and K. Nyberg. RSA Cryptobytes, Spring 2004.

11. Risto Hakala and Kaisa Nyberg. A multidimensional linear distinguishing attack on the Shannon cipher. International Journal of Applied Cryptography, 1(3):161–168, 2009.

12. Zahra Ahmadian, Javad Mohajeri, Mahmoud Salmasizadeh, Risto Hakala, and Kaisa Nyberg. A practical distinguisher for the Shannon cipher. Journal of Systems and Software, 83(4):543–547, 2010.

13. Miia Hermelin and Kaisa Nyberg. Multidimensional linear distinguishing attacks and Boolean functions. Cryptography and Communications, 4(1):47–64, 2012.

14. Andrea Röck and Kaisa Nyberg. Generalization of Matsui's Algorithm 1 to linear hull for key-alternating block ciphers. Designs, Codes and Cryptography 66, 175-193, 2013

15. Hadi Soleimany and Kaisa Nyberg. Zero-correlation linear cryptanalysis of reduced-round LBlock. Designs, Codes and Cryptography 73, 683-698 (2014)

16. Céline Blondeau and Kaisa Nyberg. Céline Perfect nonlinear functions and cryptography. Finite Fields and Their Applications 32, 120-147 (2015)

17. Soleimany, Hadi; Blondeau, Céline; Yu, Xiaoli; Wu, Wenling; Nyberg, Kaisa; Zhang, Huiling; Zhang, Lei; Wang, Yanfeng. Reflection Cryptanalysis of PRINCE-like Ciphers. Journal of Cryptology, 2015. Vol. 3, nr. 28, 718-744

18. Céline Blondeau and Kaisa Nyberg. Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to

data complexity. Designs, Codes and Cryptography (2017) 82:1-2, 319-349. doi: 10.1007/s10623-016-0268-6

19. Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-Linear Cryptanalysis Revisited. Journal of Cryptology 30(3): 859-888, 2017, http://link.springer.com/article/10.1007/s00145-016-9237-5

20. Céline Blondeau and Kaisa Nyberg. Improved Parameter Estimates for Correlation and Capacity Deviates in Linear Cryptanalysis. Transactions of Symmetric Cryptology vol. 2016, issue 2 (online) http://dx.doi.org/10.13154/tosc.v2016.i2.162-191

Peer-reviewed conference papers

1. Constructions of bent functions and difference sets, K. Nyberg. Eurocrypt'90, LNCS 473, Springer-Verlag, 1991.

2. Perfect nonlinear S-boxes, K. Nyberg. Eurocrypt'91, LNCS 547, Springer-Verlag, 1991.

3. On the construction of highly non-linear permutations, K. Nyberg. Eurocrypt'92, LNCS 658, Springer-Verlag, 1993.

4. Differentially uniform mappings for cryptography, K. Nyberg. Eurocrypt'93, LNCS 765, Springer-Verlag, 1994.

5. A new signature scheme based on the DSA giving message recovery, K. Nyberg, R.A. Rueppel. 1st ACM CCCS, Fairfax 1993

6. New bent mappings suitable for fast implementation, K. Nyberg. FSE'93, LNCS 809, Springer-Verlag, 1994.

7. Message recovery for signature schemes based on the discrete logarithm problem, K. Nyberg. Eurocrypt'94, LNCS 950, Springer-Verlag, 1995.

8. Linear approximation of block ciphers, K. Nyberg. Eurocrypt'94, LNCS 950, Springer-Verlag, 1995.

9. S-boxes and round functions with controllable linearity and differential uniformity, K. Nyberg. FSE'94, LNCS 1008, Springer-Verlag, 1995.

10. Commutativity in cryptography, K. Nyberg. 1st International Trier Conference in Functional Analysis, Walter Gruyter & Co, 1996.

11. Fast accumulated hashing, K. Nyberg. FSE'96, LNCS 1039, Springer-Verlag, 1996.

12. The Newton channel, R. Anderson, S. Vaudenay, B. Preneel, K. Nyberg. Cambridge Workshop on Information Hiding, LNCS 1174, Springer-Verlag, 1996

13. Generalized Feistel networks, K. Nyberg. Asiacrypt'96, LNCS 1163, Springer-Verlag, 1996.

14. Correlation properties of the Bluetooth combiner generator, M. Hermelin, K. Nyberg. In J.S. Song (Ed.), Proceedings of ICISC'99, LNCS 1787, Springer-Verlag, 2000.

15. Enhancements to Bluetooth Baseband Security, C. Gehrmann and K. Nyberg. Nordsec 2001, Copenhagen, November 2001.

16. Defining authorisation domains using virtual devices, S. Sovio, N. Asokan, K. Nyberg. IEEE 2003 Symposium on Applications and the Internet Workshops (SAINT Workshops 2003), January 27-31, 2003, Orlando, Florida, IEEE Computer Society Press, 2003, 331-336.

17. Man-in-the-Middle in Tunnelled Authentication Protocols, N. Asokan, V. Niemi, K. Nyberg. International Workshop on Security Protocols, 2-4 April 2003, Cambridge, England.

18. On Server-Aided Computation for RSA Protocols with Private Key Splitting, A-M. Ernvall, K. Nyberg. Proceedings of Nordsec 2003, Gjøvik 2003.

19. IKE in Ad-Hoc IP Networking, K. Nyberg. European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), LNCS 3313, Springer-Verlag, 2005

20. New Key Replay Attacks on Bluetooth, K. Ritvanen, K. Nyberg. Nordsec 2004, Helsinki, 2004.

21. Improved Linear Distinguishers for SNOW 2.0. Kaisa Nyberg, Johan Wallén. FSE 2006, Graz, March 2006, LNCS 4047, Springer-Verlag, 144-162.

22. Efficient Mutual Data Authentication Using Manually Authenticated Strings. Sven Laur, Kaisa Nyberg, CANS 2006, LNCS 4301, Springer-Verlag,90-107.

23. Ad-Hoc Associations for Groups. Jukka Valkonen, N.Asokan, Kaisa Nyberg. 3rd European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2006), 20-21 September, 2006, Hamburg, Germany, LNCS 4357, Springer-Verlag, 150-164.

24. Wireless Group Security Using MAC Layer Multicast. Kaisa Nyberg, Jukka Valkonen. Proceedings of WoWMoM 2007. June 2007, Helsinki, Finland (to appear)

25. Multidimensional Walsh Transform and a Characterization of Bent Functions. Kaisa Nyberg, Miia Hermelin. ITW 2007, July 2007, Bergen, Norway.

26. A key-recovery attack on SOBER-128. Kaisa Nyberg and Risto Hakala. In Eli Biham, Helena Handschuh, Stefan Lucks, and Vincent Rijmen, editors, Symmetric Cryptography, number 07021 in Dagstuhl Seminar Proceedings. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany, 2007.

27. Differential properties of elliptic curves and blind signatures. Billy Bob Brumley and Kaisa Nyberg. In Information Security, 10th International Conference – ISC'07, Lecture Notes in Computer Science, Valparaiso, Chile, Springer-Verlag 2007.

28. Miia Hermelin and Kaisa Nyberg. Multidimensional linear distinguishing attacks and Boolean functions. In Fourth International Workshop on Boolean Functions: Cryptography and Applications, 2008.

29. Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional linear cryptanalysis of reduced round Serpent. In Jennifer Seberry Yi Mu, Willy Susilo, editor, Proceedings of the 13th Australasian Conference on Information Security and Privacy ACISP 2008, volume 5107 of LNCS. Springer, 2008.

30. Risto Hakala and Kaisa Nyberg. Linear distinguishing attack on Shannon. In Jennifer Seberry, Yi Mu, Willy Susilo, editors, Proceedings of the 13th Australasian Conference on Information Security and Privacy (ACISP 2008), volume 5107 of LNCS. Springer, 2008.

31. Aleksi Saarela, Jan-Erik Ekberg and Kaisa Nyberg. Anonymous Beacons for Privacy and Key Agreement. WiMob 2008, SecPri Workshop, Avignon, October 2008.

32. Billy Bob Brumley and Kaisa Nyberg. On modular decomposition of integers. In Progress in Cryptology—AFRICACRYPT 2009, volume 5580 of Lecture Notes in Computer Science, pages 386–402. Springer-Verlag, 2009.

33. Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional Extension of Matsui's Algorithm 2. In Fast Software Encryption 2009, volume 5665 of Lecture Notes in Computer Science, pages 209–227. Springer, 2009.

34. Billy Bob Brumley, Risto M. Hakala, Kaisa Nyberg, and Sampo Sovio. Consecutive s-box lookups: A timing attack on SNOW 3G. In Information and Communications Security, 12th International Conference—ICICS '10, volume 6476, pages 171–185. Springer-Verlag, 2010.

35. Risto M. Hakala and Kaisa Nyberg. On the nonlinearity of discrete logarithm in . In Claude Carlet and Alexander Pott, editors, Sequences and Their Applications – SETA 2010, volume 6338 of Lecture Notes in Computer Science, pages 333–345. Springer, 2010.

36. Kaisa Nyberg. ISO MANA certificates in practice. In 2nd International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, PERVASIVE 2010, 2010.

37. Miia Hermelin and Kaisa Nyberg. Dependent linear approximations - the algorithm of Biryukov and others revisited. In CT-RSA'10, volume 5985 of Lecture Notes in Computer Science, pages 318–333. Springer, 2010.

38. Joo Yeon Cho and Kaisa Nyberg. Improved linear cryptanalysis of sms4 block cipher. In Symmetric Key Encryption Workshop 2011 (SKEW 2011) Lyngby, Denmark, 16 – 17 February 2011, 2011.

39. Andrea Röck and Kaisa Nyberg. Exploiting Linear Hull in Matsui's Algorithm 1. In The Seventh International Workshop on Coding and Cryptography, WCC 2011, April 11-15, 2011, Paris, France, 2011.

40. Céline Blondeau, Benoît Gérard, and Kaisa Nyberg. Multiple Differential Cryptanalysis Using LLR and X^2 Statistics. In 8th Conference on Security and Cryptography for Networks, SCN 2012 Proceedings, Lecture Notes in Computer Science 7485, 343-360, 2012

41. Kaisa Nyberg. "Provable" Security against Differential and Linear Cryptanalysis. Fast Software Encryption FSE 2012. Lecture Notes in Computer Science 7549, 1-8, 2012

42. Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang. Integral and Multidimensional Linear Distinguishers with Correlation Zero. Advances in Cryptology -- ASIACRYPT 2012. Lecture Notes in Computer Science 7658, 244-261, 2012

43. Hadi Soleimany and Kaisa Nyberg. Zero-Correlation Linear Cryptanalysis of Reduced-Round LBlock. Pre-proceedings of WCC 2013 (2013)

44. Céline Blondeau and Kaisa Nyberg. New Links between Differential and Linear Cryptanalysis. Eurocrypt 2013. Lecture Notes in Computer Science 7881, 388-404, 2013

45. Risto M. Hakala Risto, Atle Kivelä, and Kaisa Nyberg. Estimating Resistance against Multidimensional Linear Attacks: An Application on DEAN. Information Security and Cryptology, 8th International Conference, Inscrypt 2012, Proceedings. Lecture Notes in Computer Science 7763, 246-262, 2013

46. Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang, Yanfeng Wang. Reflection Cryptanalysis of PRINCE-like Ciphers. Fast Software Encryption, FSE 2013. Lecture Notes in Computer Science 8424, 71-91, 2014

47. Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-Linear Cryptanalysis Revisited. Fast Software Encryption, FSE 2014. Lecture Notes in Computer Science 8540, 411-430, 2015

48. Céline Blondeau and Kaisa Nyberg. Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. Eurocrypt 2014, Lecture Notes in Computer Science 8441, 165-183, 2014

Books and book articles

1. *Advances in Cryptology – EUROCRYPT '98*, K. Nyberg (Ed.). Lecture Notes in Computer Science 1403, Springer-Verlag 1998.

2. *Selected Areas in Cryptography*, K. Nyberg, H. Heys (Eds.). Lecture Notes in Computer Science 2595, Springer-Verlag 2002.

3. *UMTS Security*, V. Niemi, K. Nyberg. Wiley & Sons, Chichester 2003.

4. Securing network access in future mobile systems, G. Horn, V. Niemi, K. Nyberg, H. Tschofenig. In Chris J. Mitchell (Ed.) *Security for Mobility*. IEE 2004.

5. Security in Personal Area Networks, C. Gehrmann, K. Nyberg. In Chris J. Mitchell (Ed.) *Security for Mobility*. IEE 2004.

6. Kaisa Nyberg, editor. Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers, volume 5086 of Lecture Notes in Computer Science. Springer, 2008.

7. René Mayrhofer, Kaisa Nyberg, and Tim Kindberg. Secure Spontaneous Interaction, Special issue, International Journal of Security and Networks Volume 4 Nos. 1/2. Inderscience, 2009.

8. N. Asokan and Kaisa Nyberg. Security associations for wireless devices. In Stefanos Gritzalis, Tom Karygiannis, and Charalabos Skianis, editors, Security and Privacy in Mobile and Wireless Networking. Troubador Publishing Ltd, Leicester, UK, 2009.

9. Miia Hermelin and Kaisa Nyberg. Linear cryptanalysis using multiple linear approximations. In Pascal Junod and Anne Canteaut, editors, Advanced Linear Cryptanalysis of Block and Stream Ciphers. IOS Press, 2011.

10. Tuomas Aura, Kimmo Järvinen, and Kaisa Nyberg, editors. Information Security Technology for Applications, 15th Nordic Conference on Secure IT Systems, NordSec 2010, Aalto University, Finland, October 27-29, 2010, Revised Selected Papers. Lecture Notes in Computer Science 7127, 2012

11. Nyberg, Kaisa, editor. Topics in Cryptology - CT-RSA 2015. The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Lecture Notes in Computer Science 9048, 2015

PhD thesis

On Subspaces of Products of Nuclear Fréchet Spaces. *Ann. Acad. Sci. Fenn. Ser A I Math. Dissertationes* 31, Finnish Academy for Science and Letters, Helsinki 1980.

Patents

1. Digital signature method and key agreement method, RA Rueppel, K Nyberg, US Patent 5,600,725 (1997)

2. Subscriber authentication, K. Nyberg, FI 109864 B (2000), US Patent 8,503,676 (2013), FI 109864 (2000)

3. Method for ensuring data transmission security, communication system and communication device, K Nyberg, V Niemi, US Patent 7,995,760 (2011), FI 114062 (2001)

4. Method and system for access point roaming, T Heinonen, K Nyberg, US Patent 7,103,359 (2006)

5. Method for sharing the authorization to use specific resources, S Sovio, N Asokan, K Nyberg, V Niemi, US Patent 7,343,014 (2008)

6. Replay prevention mechanism for EAP/SIM authentication, P Eronen, H Haverinen, K Nyberg, US Patent 7,418,595 (2008)

7. Method for securing a communication, K Nyberg, US Patent 7,607,012 (2009)

8. Linked authentication protocols, K Nyberg, V Niemi, N Asokan, US Patent 7,707,412 (2010)

9. System, method and computer program product for authenticating a data agreement between network entities, N Asokan, K Nyberg, US Patent 7,783,041 (2010)

10. Authenticated group key agreement in groups such as ad-hoc scenarios, K Nyberg, N Asokan, US Patent 8,386,782 (2013)

Patent Applications

1. Replay prevention in wireless communications networks, K Nyberg, K Ritvanen, US Patent App. 10/944,042 (2006)

2. Handshake procedure, K Nyberg, US Patent App. 11/783,856 (2008)

3. Method, apparatus and computer program product for efficient elliptic curve cryptography, K Nyberg, US Patent App. 13/121,345 (2011)

Other publications

1. The Ramsey theorem and complemented basic sequences in Fréchet spaces. Reports of the Department of Mathematics, University of Helsinki, 1988.

2. Link layer security for the first hop. European Cooperation in the field of development of mobile personal communication, K. Nyberg. International workshop, May 15-17, 2002, Moscow, Russia, 104-112.

3. Trust model, communication and configuration security for Personal Area Networks, C. Gehrmann, T. Kuhn, K. Nyberg, P. Windirsch. IST Mobile & Wireless Telecommunications Summit 2002, 16-19 June 2002, Thessaloniki, Greece.

4. The personal CA - PKI for a Personal Area Network, C. Gehrmann, K. Nyberg, C. Mitchell. IST Mobile & Wireless Telecommunications Summit 2002,16-19 June 2002, Thessaloniki, Greece

5. Cryptographic Algorithms for UMTS, K. Nyberg, In P. Neittaanmäki, T. Rossi, S. Korotov, E. Oñate, J. Périaux, and D. Knörzer (eds.) European Congress on Computational Methods in Applied Sciences and Engineering, ECCOMAS 2004, Jyväskylä, 24-28 July 2004.

6. Establishing Security in Personal Area Networks. K. Nyberg, D. Sisalem. ECWT Workshop on *Secure Wireless Personal Networks*, European Microwave Week, Amsterdam, 13 October, 2004.

7. Cryptology – The Science of Information Security (in Finnish). Kaisa Nyberg. Tietojenkäsittelytiede, 26, July 2007, 32-53

8. Jukka Valkonen and Kaisa Nyberg. New cryptographic methods improve privacy (in Finnish). Tietosuoja, 4:24–27, 2008.