

# *Curriculum Vitae*

1. **Name:** Jan Villemson (Willemsen)
2. **Date and place of birth:** 30.07.1974, Tartu, Estonia
3. **Nationality:** Estonian
4. **Marital status:** married to Kairi Willemsen
5. **Contacts:**
  - (a) Email: jan@ut.ee, jan@cyber.ee
  - (b) Address: Cybernetica, Lai 6, 51005 Tartu, Estonia
  - (c) Phone: (+372 7) 302 667 (office), (+372 5) 150 919 (mobile)
6. **Education:**
  - (a) BSc in mathematics (*cum laude*), 1996, Tartu University, Estonia
  - (b) MSc in informatics (*cum laude*), 1998, Tartu University, Estonia
  - (c) PhD in informatics, 2002, Tartu University, Estonia
7. **Working experience:**
  - (a) 1998 – 2002: Cybernetica, research engineer
  - (b) 2002 – . . . : Cybernetica, senior research engineer
  - (c) 2000 – 2004: Tartu University, lecturer
  - (d) 2004 – . . . : Tartu University, assistant professor
8. **Languages skills:**
  - (a) Estonian: mother tongue
  - (b) English: excellent
  - (c) Russian: excellent
  - (d) German: modest
  - (e) Finnish: modest

# Background information

## Research background

There were two important things in my research career that began at the same time: my PhD studies and employment in Cybernetica. Since Cybernetica is the leading data security company in Baltic region, it determined my field of studies to be related to cryptology. More specifically, the question of retaining the proof value of digital signatures over a long time was (and it still is) a hot topic back in 1998 and I became a member of a working group dealing with it. We concentrated on time-stamping as the most promising approach to solve the problem.

It turned out that secure and efficient time-stamping systems can be built using cryptographic hash functions. The way a hash function is used in the process of time-stamping is described by a certain directed graph whose properties determine the quality of the whole process. This turned the study of retaining the proof value of digital signatures into a research in graph theory. Hence, although theoretically dealing with data security, my field of study almost entirely belongs to combinatorics. The most important publication in this field is the paper number 1.2.1 in the publication list which presented first practical graphs to be used as the basis of time-stamping. There have been several improvements made since then by several authors. My recent results on time-stamping are written down in my PhD thesis “Size-efficient interval time stamps”, defended in June 2002 at Tartu University, Estonia. One of the main results of the thesis is the proof optimality of a new graph family in the context of interval time-stamping (i.e. a flavor of time-stamping where we are not interested in specifying exact moments of events, but rather some time intervals). My time-stamping and related papers are 1.1.1, 1.2.3, 1.2.4, 1.2.5 and 1.2.10 from publication list.

My other larger area of interest has been applying combinatorial methods for mobile robot path planning. The papers related to this topic are 1.1.2, 1.2.7, 1.2.8 and 1.2.12. These papers include both theoretical analysis of robot path space covering and practical test results with real robots.

I have also dealt with personal security environments (1.2.2), security of document formats (1.2.6 and 1.6.2) and tutorial environments for cryptographic protocols (1.2.11).

## Organizational activities

1. I am a member of International Association for Cryptographic Research (IACR).
2. I am a member of British Computer Society Special Interest Group on Artificial Intelligence (BCS-SGAI).
3. I am a member of of the Board of Estonian Mathematical Society.
4. I am a member of Estonian Information Technology Society.
5. For several time periods (including the year 2002) I have been a member of the council of the Department of Mathematics and Informatics of Tartu University.
6. Since 1992, I have been participating in preparation of Estonian high school students for International Mathematical Olympiads (IMO). Since 1995 I have also acted as a team leader of Estonian IMO and Baltic Way team competition teams.

## Teaching experience

1. Throughout the years 1996 – 2002 I have prepared and given several regular lecture courses in Tartu University, the most important ones being
  - (a) Discrete Mathematics 1996
  - (b) Introduction to Cryptography 1999 – 2004
  - (c) Game Theory 2002, 2004
2. For supporting the course Introduction to Cryptography, I lead a working group that produced Tutorial Environment for Cryptographic Protocols. The tool helps visualizing modular arithmetic based cryptographic protocols and can be used as an aid for lectures, homework or as a specialized computer algebra system. The environment is described in the paper 1.2.11 in the publication list.
3. During 1996–2004 I have given several exercise classes to the courses of Discrete Mathematics, Graphs and Mathematical Logics.

4. For the courses of Introduction to Cryptography and Graphs I have written corresponding teaching materials. The study book of Graphs course was published in 2003 (see publication nr 2.3 in the publication list).
5. Since 1998 I have been responsible for the theoretical computer science seminars in Tartu University. The seminars have covered the topics of cryptography, error-correcting codes, algebraic graph theory and game theory.
6. Since 2000 I have been active in Tartu Information and Communication Technology Applications Center (TICTAC). The center has organized a series of technology seminars on Information Technology and its Economic Aspects, Applications of Mobile Communications (I–III), Information Security Technologies and Robotics Technologies.
7. Since 1993 I have been involved with preparation of high school students for International Mathematical Olympiad (IMO) and Baltic Way team competitions and acted as the team leader on many occasions. Based on the problem sets and other preparational material I have produced series of teaching materials, most notably in geometry and algebra. The booklet *Võrratud (Inequalities)* was published in 2003 (publication number 2.2 in the publication list). In years 1994 and 2002 problem booklets of mathematical team contest Baltic Way were edited by me and published (publication nr 2.1 in the publication list). I have also created numerous problems for all levels of mathematical contests, including problem 1 on IMO 1999 and problem 3 on IMO 2004. My problems have been published in yearly collections of Estonian mathematical olympiads' problems.
8. I have supervised three successful MSc theses (by Kuldar Aas, Jelena Zaitseva (see publication nr 1.2.11 in the publication list) and Vladimir Šor). Currently I am supervising 3 PhD students (Mart Anton (1st year), Kristo Heero (3rd year, see publications 1.2.8 and 1.2.12 in the publication list) and Asko Tiidumaa (3rd year)) and 5 MSc students (Jaanus Jaeger, Indrek Saar, Hardi Teder, Kaspar Ilves, Jaak Pruulmann).
9. Under my supervision, Jaak Pruulmann created the first free ispell-based speller for Estonian language.
10. I have given several public lectures and written popular articles concerning topics of general interest connected to mathematics and computer

science, see e.g. the paper 3.2 and the section 6 in the publication list.

## Prizes obtained

1. 3rd rank diploma on All-Soviet mathematical olympiad, 1990.
2. Sharing the 1st place on Estonian mathematical olympiad, 1991.
3. 2nd place on Estonian mathematical olympiad, 1992.
4. Estonian Academy of Sciences, distinguished theses prize for MSc thesis, 1998.
5. 3rd Estonian Winter School on Computer Science (EWSCS), Palmse, Estonia, best student presentation, 1998.
6. 5th Estonian Winter School on Computer Science (EWSCS), Palmse, Estonia, best student presentation, 2000.
7. Best refereed technical paper in 22nd SGAI International Conference on Knowledge Based Systems and Applied Artificial Intelligence, 2002.

## Research plans

My current research plans include several directions. The first direction is motivated by the observation that most of the results in cryptography hold under very strong assumptions – keys and passwords are stored safely, trusted parties do not attempt to harm the system, etc. When one tries to apply such results in practice, it is necessary to estimate, to which extent such assumptions hold. This extent can be measured by the probability of breaking them. For example about 1% of employees of British banks are accused of inside attacks against their employer. Besides the attack probabilities, one also has to take into account the potential benefits obtained as a consequence of a successful attack, and the penalty that follows an unsuccessful one.

We see that a detailed risk analysis is needed in order to estimate the likelihoods and consequences of the attacks. The applications of risk analysis in data security however constitute rather a young area of research with lots of open questions and novel techniques. One potentially useful technique that fascinates me is using evolutionary game theory. The parties of several global security issues (virus attacks, spam e-mail) can be viewed as antagonistic populations with contradicting interests. But as none of the populations can

survive without the others, the system will approach a certain stable state or even an equilibrium. Being able to predict or even influence the behavior of the system may have enormous economic effect.

The second research topic I would like to deal with is (mobile) gaming and gaming security. Although many game applications involve great security risks (especially if monetary prizes are involved), gaming and security communities have cooperated surprisingly little. It is not uncommon for internet game protocols to use proprietary (weak) cryptographic solutions and this situation requires a wide range of studies to be conducted.

Another security related research area that is of interest for me are tools for teaching cryptographic protocols and algorithms. My experience shows that many students have difficulties dealing with all kinds of abstract communication protocols. Evenmore, cryptography is rich of quite complicated algorithms relying on many deep mathematical areas (number theory, lattice theory, abstract algebra etc). This makes the motivation behind visual teaching tools for cryptography even stronger. I have supervised one successful project in this field and had positive feedback both from students and pedagogical community. I feel that this direction has good prospects for future.