Doing research (in cryptography) – tools of the trade

Krystian Matusiewicz and Scott Contini

Centre for Advanced Computing Algorithms and Cryptography,
Department of Computing, Macquarie University

NTU Seminar, 12 October 2007

Outline

Outline

Introduction: why this talk?

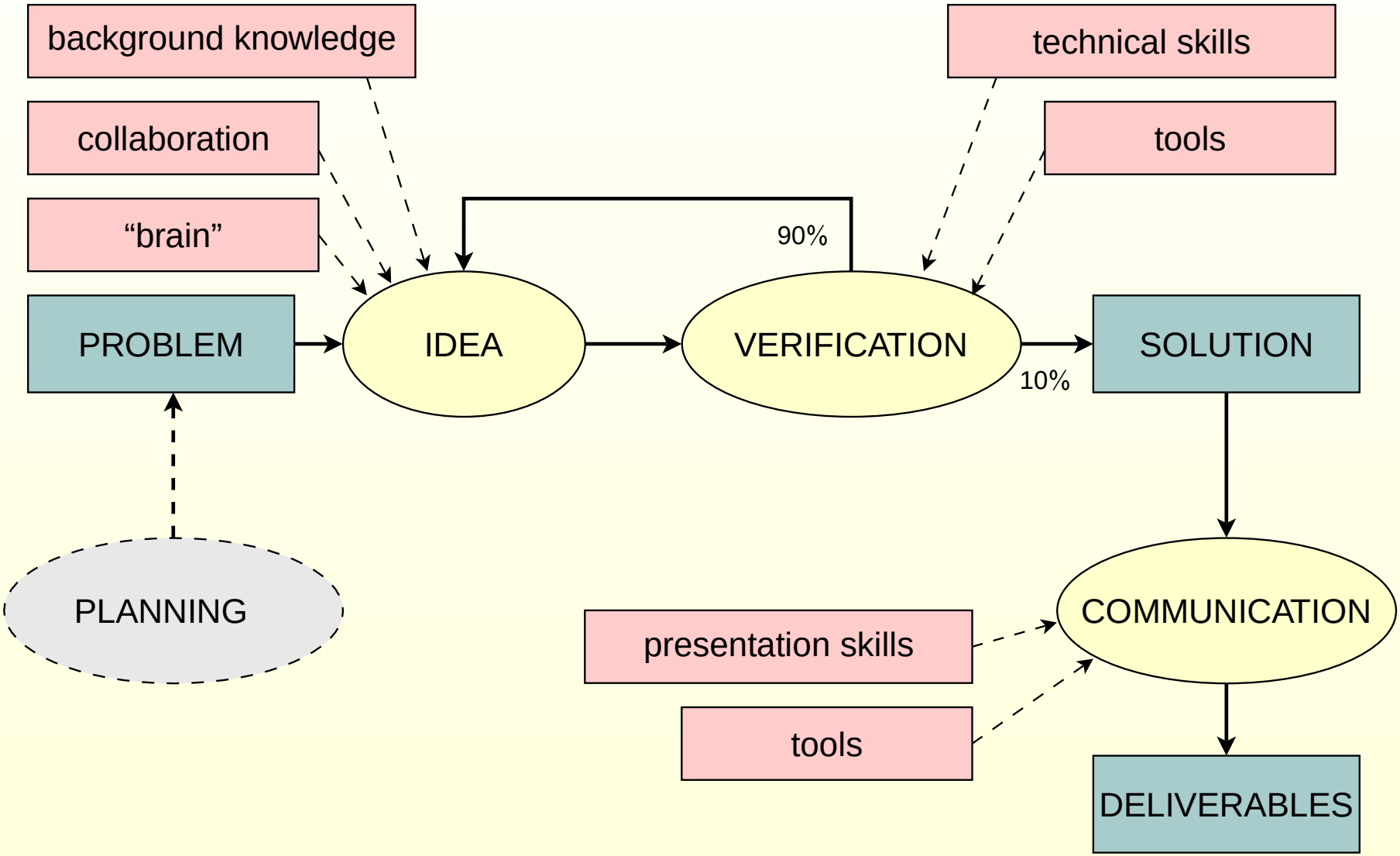
- Share our research experience
- Hopefully some will find some of our advice useful
- We are very brief but:

Mądrej głowie dość dwie słowie.

For a wise head, two words are enough.

– traditional Polish saying.

Doing research: the big picture



Outline

Getting ideas...

The most . . .

- . . . important
- . . . subjective
- . . . difficult to capture

part of the research process.

Important factors

- Background knowledge
- Collaboration
- Asking yourself questions
- “brain management”

Background knowledge

- Logic, foundations of mathematics
- Discrete mathematics
- Algebra, number theory
- Algorithms, data structures, computational complexity
- Cryptography
- Previous research, solved problems

Collaboration

- Using broader background knowledge of all participants
- “resonance” and “positive feedback”: “$1 + 1 > 2 * 1$”

Asking yourself questions

- Why does it work that way?
- Why it cannot be done better?
- What is the meaning/importance of something?
- Is some paper/theory/statement correct?
- What are the assumptions and are they appropriate?

“Brain management”

- brain is for us what muscles for an athlete are
- know your brain, train it
- know when to work and when to rest
- “Mens sana in corpore sano” – “sound mind in a sound body”, healthy lifestyle will help in a long run

But brain also works differently from muscles:

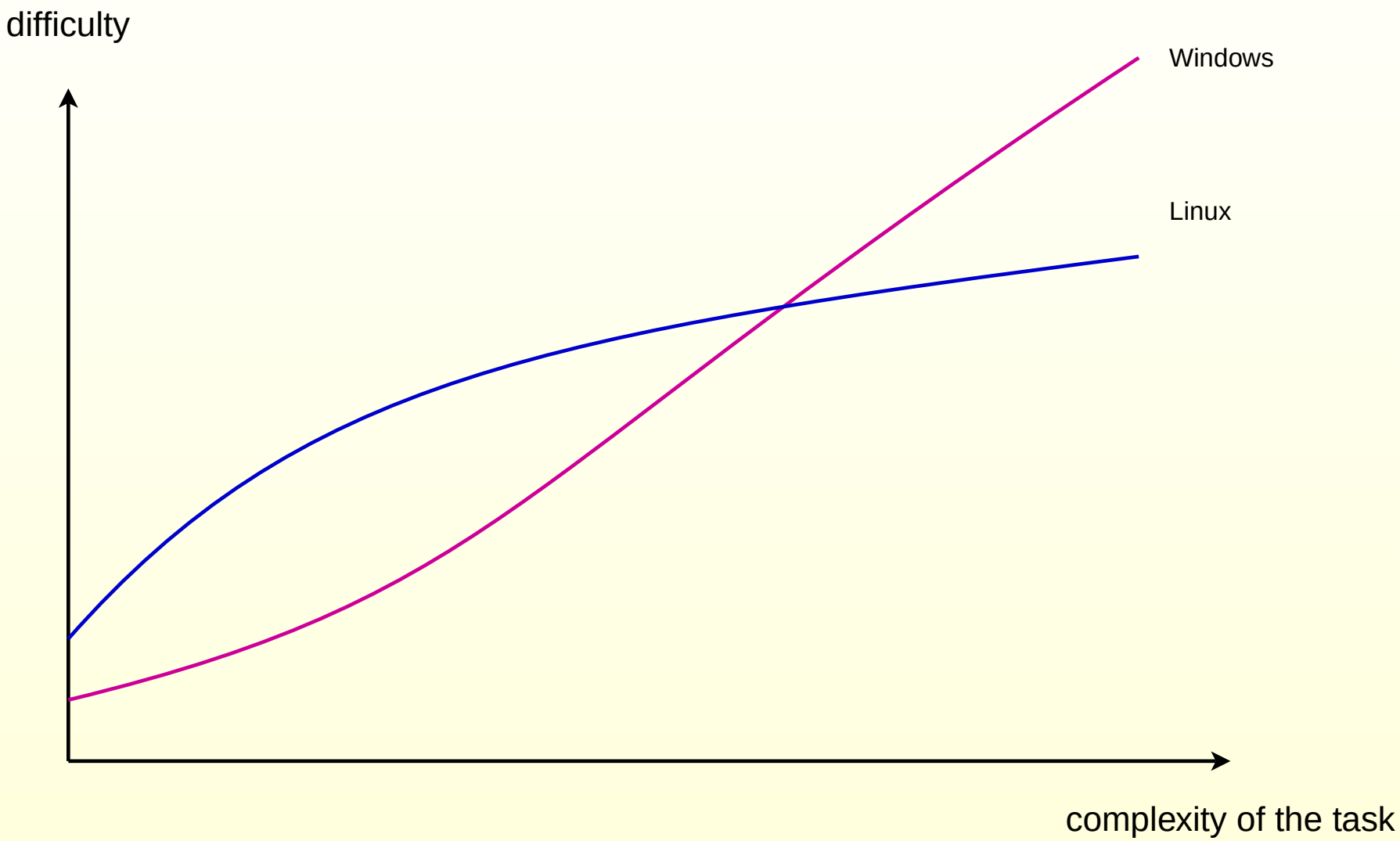
- subconscious processes – brain works even when we are asleep
- use this power to your advantage

Outline

Working out the solutions

- The most important part here is efficiency – spend as little time as possible to achieve the result.
- Pick the right tool for the right task

Our view on the holy war Windows vs. Linux



Verification: Useful skills

Programming:

- C, C++ – for computationally demanding tasks where speed really counts, wealth of specialised libraries
- magma, gp/pari, mathematica – high level systems for mathematical computations
- shell scripting (bash, sed, awk) – manipulating text files, managing computational experiments
- perl, python – high level languages particularly useful for manipulating text files (e.g. output data)

Theoretical work:

- Proving theorems!

Outline

Presenting results

There are two main modes of presenting a result to the scientific community

- Writing a paper
- Giving a talk

Writing papers: tools

The main tool for writing papers in mathematics, computer science and physics is LaTeX.

- TeX : Typesetting system developed by D. Knuth
- LaTeX : a set of macros for using TeX developed by L. Lamport

Available on almost any platform. Popular implementations:

- Windows: MikTeX
- Linux: tetex

LaTeX : how to learn

Starters:

- “Not so short introduction to LaTeX” – free online book
- documentation to amslatex package – free online resource

Main courses:

- Very good book: Kopka, Helmut; Daly, Patrick W. “Guide to LaTeX”, (4th edition)
- For more detailed solutions: Mittelbach, Frank; Goosens, Michel (2004). “The LaTeX Companion”, (2nd edition)

Desserts:

- Victor Eijkhout, “TEX by topic, a TEXnician’s reference”, free to download from: `http://www.eijkhout.net/tbt/`
- Donald Knuth “The TEX book”

What to use

GUI Editors:

- Windows: TexnicCenter
- Linux: Kile, Texmaker

Managing BibTeX bibliographies:

- jabRef (Java, all platforms)

What to use: pictures in LaTeX

Including pictures in LaTeX is sometimes a bit of a problem.

- for any raster image formats: problems with resolution, big file sizes
- eps : compatibility issues

My solution:

- use PStricks package
- use jPicEdt as a GUI editor for pictures
- gnuplot with PStricks output for graphs

Using PStricks for LaTeX pictures

Pros:

- fully scalable vector graphics
- small size of files with even complex pictures
- no problems with compatibility

Cons:

- cannot use pdflatex directly
- learning another program

Talks

Most important part of the talk: good slides.

- Slides are the backbone of the talk
- Not too much text
- Diagrams better than words
- Not too many details
- Good looking!

Preparing presentation slides: beamer

- Use LaTeX for beautiful formulae
  - Package beamer for simple preparation of slides
  - Many templates ready to use
  - Advanced customization features
- For presentations with a lot of raster graphics [pictures, screenshots] and no formulae it might be easier to use something different

Outline

Summary

- Main phases of research work:
  - getting new ideas
  - verifying them
  - communicating results
- Each phase needs its own tools and skills
- We presented some tips which tools proved useful in our experience
- Ultimately, research is a very personal experience!