

Position paper  
on future research on the  
**foundations of cryptography**

Joachim von zur Gathen  
Universität Paderborn  
gathen@uni-paderborn.de  
<http://www-math.upb.de/~aggathen/>

October 7, 2002

In the context of the STORK project, I want to outline my views on some directions for research on the fundamentals of cryptography.

Most of public-key cryptography today bases its security on the presumed computational difficulty of two problems: integer factorization and discrete logarithms in finite groups. Should anyone ever find efficient algorithms for (one of) these problems, then public-key cryptography would plunge into a crisis. (There even is a concrete proposal for such algorithms, namely via quantum computing.) In our day-to-day work we may presumably ignore such hypothetical dangers, but it is a challenge

to broaden the base of problems providing secure and efficient cryptosystems.

Steps taken in this direction involve, e.g., high-dimensional polynomial equations, and arithmetic in mixed radices.

The basic foundations of cryptography include one-way and trapdoor functions, and various types of pseudorandom generators. They have been intensively studied, with considerable success, but it still remains

to investigate the basic cryptographic tools and their relations.

A similar task exists at the higher level of protocols ranging from secure data transmission to signatures, identification, and authentication. Here we strive

to understand the relation between various protocols and requirements, in particular security interrelations.

The last two problems include the search for lower bounds on the resources used in an attack. Given our civilization's lack of tools to deal with such questions in general models of computation, as witnessed by the unsatisfactory state of the  $P$  vs.  $NP$  question, we should aim

to build meaningful structured models and prove lower bounds (relative or absolute) for cryptographic tasks.

The theory of cryptography was at first concerned with algorithmic attacks on cryptosystems, say integer factorization algorithms against RSA. Today a major concern in real-world applications are “hardware attacks” from power analysis to various side channel attacks, and more. This is well-studied in specific contexts, and protective steps like appropriate paddings have been proposed. But we still have

to build a meaningful general theory of hardware attacks, and then devise efficient counter-measures.

The tasks outlined above are all of a technical nature. However, probably the most important foundational issue is not directly related to research, namely

to create educational programs whose graduates form the strong basis of skilled cryptographers required to push the field ahead, in industry, government, and academia.

Cryptography is a vibrant and energetic field with plenty of opportunities ahead.