

Building Blocks for Cryptography

Ronald Cramer

Robbert de Haan

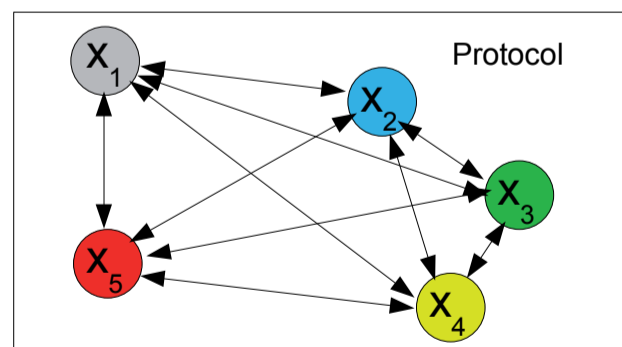
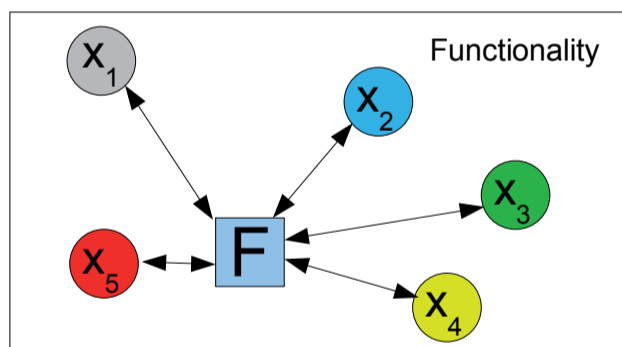
Herman te Riele

Centrum voor Wiskunde en Informatica (CWI)

Most current-day cryptography relies on unproven number-theoretic assumptions. However, it is often possible to perform cryptographic tasks without such assumptions. For instance, having a shared key, a noisy channel or a majority of honest parties is already sufficient for many tasks in cryptography. Interesting examples of these are encryption, electronic voting and the dating problem, where two people want to find out whether they both want to date each other, but not be embarrassed if one doesn't. We need to investigate when we can do without number-theoretic assumptions and how we can in these situations best implement our cryptographic primitives. Furthermore, we need to continuously challenge the number-theoretic assumptions that are used in practice to assess their practical difficulty.

Secure Computation

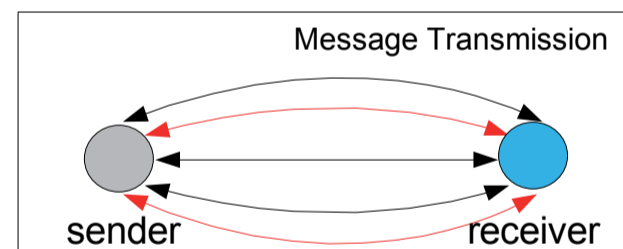
Secure computation protocols consist of a number of parties that want to jointly compute a certain function F on their input values, while only revealing the output to each other. Well-known examples of such protocols are electronic voting and anonymous auctions. The functionality of these protocols is as if all the parties send their input to someone they trust and only receive the output of the function from this person afterwards.



Such secure protocols exist, *without* relying on any number-theoretic assumptions, when the majority of the parties behaves honestly. Part of our research focuses on investigating and improving the fundamental techniques underlying the protocols for secure computation. In this area, we have developed a number of techniques that allow for much more efficient protocols in many natural settings.

Perfectly Secure Message Transmission

Perfectly secure message transmission protocols allow to privately and reliably transmit a message using multiple channels. They do this *without* an initially shared encryption key or reliance on any number-theoretic assumptions. These protocols simultaneously deal with many problems that arise in typical communication networks, such as failing channels and eavesdropping. We developed an optimally efficient protocol for the worst-case scenario where just over half of the channels is clean and untapped and where only two unidirectional transmissions are used.



Regulator Computation

Cryptographic schemes have recently been based on the structure of quadratic number fields. We focus on the underlying problem of one class of these, the schemes based on real quadratic number fields. For these fields it seems to be very difficult to determine the regulator up to any decent precision. Just as for RSA it is important to continuously analyze the difficulty of the factoring problem, it is crucial here to continuously investigate the difficulty of regulator approximation. We developed a new algorithm that rigorously computes the regulator of a real quadratic number field and which is the fastest of its kind known to date.

Part of this research has been funded by the Dutch BSIK/BRICKS project PDC1.