Bachelorthesis-Aufgabe

Efficient and Secure Outsourcing of Modular Exponentiation

ID	IHNR1-2-17
Studierende	Pascal Serge Mainini
Betreuer	Prof. Dr. Rolf Haenni
Experten	Dr. Federico Flueckiger
Aufgabe	Modular exponentiations are the key operations in many modern cryptographic schemes and protocols. Since this involves a large amount of computations with very large numbers, powerful machines are needed to perform the computations in a reasonable amount of time. This project considers the problem of delegating the computation of modular exponentiations from a computationally weaker client to one or multiple computationally stronger servers. Since some of the input parameters of the exponentiations -- usually the exponents and the results -- are often secret values in a cryptographic application, this delegation is a non-trivial task. Any solution should prohibit, that the involved servers learn anything about the secret values. The main task of the project is to implement a server infrastructure, which offers private delegation of modular exponentiations to potential weak clients such as web browsers or smartcards. The implemented algorithms should correspond to the state-of-the-art methods in the scientific literature. The system should be flexible (number of servers, private/public base, private/public exponent, private/public result), efficient, and easy to use. The goal of the project is to provide a solution for cryptographic applications, in which the cost of computing a large amount of modular exponentiations is problematical.