Dipl.-Ing. Dr.techn. Maria Elisabeth Oswald
Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie
E-Mail: elisabeth.oswald@iaik.tugraz.at
Tel.: 0316 873 5527

Kryptografische Algorithmen
Cryptographic Algorithms

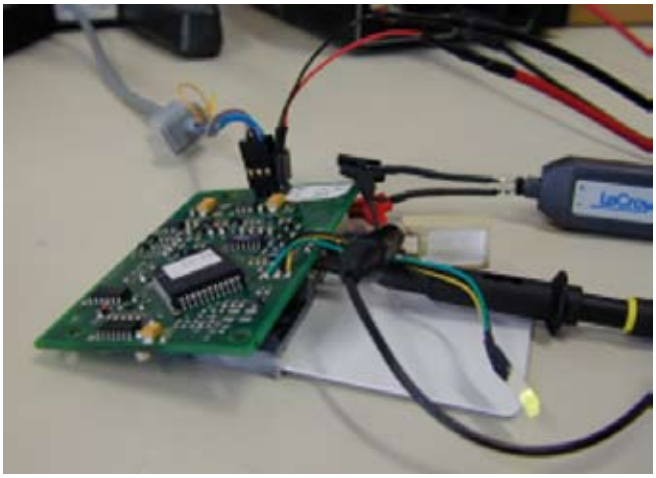
In meinem beruflichen Alltag dreht sich alles um zwei Personen namens Alice und Bob. Alice und Bob möchten „sicher" über ein offenes Netzwerk kommunizieren. Das Adjektiv „sicher" kann hier mehrere Bedeutungen haben. „Sicher" kann zum Beispiel „vertraulich" bedeuten. Meistens hat „sicher" aber mehrere Bedeutungen wie zum Beispiel „integer" oder „authentisch". Kryptografie ist die Wissenschaft, die sich mit der Absicherung von Information beschäftigt. Ein kryptografischer Algorithmus ist eine öffentlich bekannte mathematische Funktion, die mit Hilfe eines Schlüssels Daten verschlüsselt. Ohne diesen Schlüssel ist eine Entschlüsselung nicht möglich.

Ich hätte mir vor meinem Studium der technischen Mathematik, das ich 1999 an der TU Graz abschloss, nie träumen lassen, dass ich eine Leidenschaft für Kryptografie entwickeln würde. Am Ende meines Studiums habe ich aber die Lehrveranstaltungen am meisten genossen, die sich mit dem Thema Kryptografie beschäftigten. Meine Diplomarbeit beschäftigte sich mit einem durchaus praktischen Problem in der Kryptografie: Alice und Bob benutzen zum Absichern ihrer Kommunikation nämlich so komplizierte mathematische Verfahren, dass sie diese nicht selbst berechnen können. Stattdessen benützen sie einen Computer der den Algorithmus berechnet. Die Sicherheit der Implementierung des kryptografischen Algorithmus war das Thema mit dem ich mich im Rahmen meiner Diplomarbeit auseinandergesetzt habe, und mit dem ich mich auch jetzt noch beschäftige.

Die praktische Sicherheit von kryptografischen Algorithmen ist auch ein Forschungsgebiet, das wir am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) vorrangig bearbeiten. Im Sog meiner Diplomarbeit, und später dann meiner Dissertation, für die ich auch einige Monate in Belgien geforscht habe, sind noch viele weitere Arbeiten entstanden. Einige der Studentinnen und Studenten, die mir in diesem Themengebiet nachgefolgt sind, sind am IAIK geblieben, und arbeiten mit mir gemeinsam im Seitenkanallabor (SCA-Lab, http://www.iaik.tugraz.at/research/sca-lab/index.php). Wir sind Teil der VLSI Gruppe und stark verknüpft mit der Krypto Gruppe. Wir entwickeln sichere Implementierungen von kryptografischen Algorithmen für Hardware und für Software. Der Aspekt, der uns dabei besonders interessiert, ist die Sicherheit gegen Seitenkanalattacken. Eine Seitenkanalattacke lässt sich leicht erklären und (leider) oft leicht durchführen. Einfache Smartcards sind ein gutes Opfer. Während so eine Smartcard einen kryptografischen Algorithmus berechnet, misst der Angreifer einfach ihren Stromverbrauch, ihr elektro-magnetisches Feld oder die Zeit die sie zur Berechnung des Algorithmus braucht. Aus diesen Informationen, den so genannten Seitenkanälen, kann der Angreifer dann mittels statistischer Methoden den geheimen Schlüssel berechnen.

Im Bereich der Seitenkanalattacken ist unser SCA-Lab mittlerweile international anerkannt. Wir leiten im Moment das größte von der EU geförderte Forschungsprojekt auf dem Gebiet (SCARD—Side Channel Analysis Resistant Design Flow), und sind Gruppenleiter in ECRYPT, dem Network of Excellence in Cryptology (einem weiteren von der EU geförderten Projekt). Weiters forschen wir im Rahmen von nationalen Forschungsprojekten die vom FWF gefördert werden (ISDPA – Investigation of Simple and Differential Power Analysis, ISCA – Investigation of Side-Channel Analysis). Die Ergebnisse unserer Arbeit werden regelmäßig bei den wichtigsten Konferenzen im Bereich der Angewandten Kryptografie publiziert.

Die Erkenntnisse aus unserer Forschung gebe ich auch in der Lehre an Studierende weiter. Ich leite die Lehrveranstaltung „Einführung in die Informationssicherheit", die eine Pflichtlehrveranstaltung für Studierende der Studienrichtungen „Softwareentwicklung-Wirtschaft" und „Informatik" ist. Weiters leite ich die Lehrveranstaltung „IT-Sicherheit", die im Magisterstudium belegbar ist. Ich wirke bei der Lehrveranstaltung „Angewandte Kryptografie 2" mit und betreue zahlreiche Projekte (im Bakkalaureatsstudium und im Magisterstudium) und Diplomarbeiten. Ich bin derzeit Universitätsassistentin am IAIK an der TU Graz.



Messaufbau für Seitenkanalattacke

Cryptographic Algorithms

In my job I am mainly concerned with the problem that Alice and Bob want to communicate securely over an open network. Cryptography is the science of protecting information. A cryptographic algorithm is a mathematical function that uses a key to encipher information. Without knowledge of the key, deciphering is not possible. Cryptographic algorithms are difficult mathematical functions -- we use computers to compute them. Unfortunately, information leaks from a computer while it executes something in form of power consumption, electromagnetic emanation and execution time. Exploiting this leaked information, the so-called side-channel information, is the field I have specialized in. After my initial work in this field, many students have followed and we now work together in the Side-Channel Analysis Lab. We are well known internationally and lead the SCARD (Side-Channel Analysis Resistant Design Flow, EU funded) project. We are also group leaders within ECRYPT (the European Network of Excellence in Cryptology, EU funded). In addition to my research, I am involved in several teaching activities. I am currently an assistant professor at Graz University of Technology.