se Modelle und versuchen zu beweisen, dass die Schutzmaßnahmen diese definierten Anforderungen erfüllen."

Weil das sehr abstrakt wirkt, ein paar Beispiele: Es kann möglich sein, quasi über Umwege an das „Geheimnis" (so nenen es die Experten) zu gelangen, das im Chip verborgen ist. Ein derartiger „Seitenkanal" kann zum Beispiel sein, dass man den Stromverbrauch eines Chips genau analysiert. Auch die Zeit, die bestimmte Rechenoperationen benötigen, können wesentliche Hinweise auf ein „Geheimnis" liefern. Bloem untersucht nun, ob die Algorithmen im Chip gegen solche Angriffe gefeit sind. Er beweist mit Methoden der Mathematik und der Logik, dass ein Verfahren im Chip sicher gegenüber von Angriffen ist.

Professor Roderick Bloem

Das Thema „beweisbare Sicherheit" ist jedoch nicht nur darauf beschränkt, sondern umfasst viele Aspekte von der Hardware bis zur Netzwerkkommunikation.

Österreichweit wurde deshalb ein Spezialforschungsbereich unter der Bezeichnung „SPyCoDE" genehmigt. Mit dabei sind TU Wien, die Unis Wien und Klagenfurt und das ISTA in Klosterneuburg.

Denn es sind nicht nur theoretische Arbeiten, die Wissenschaftler arbeiten eng mit der Industrie (etwa NXP) zusammen. Die Methoden und Tools, die hier entwickelt werden, sollen später dazu dienen, den Entwurf von sicherheitsrelevanten Chips zu verbessern. „Wir entwickeln systematische Methoden, damit man ganze Klassen von Sicherheitslücken bewerten kann", sagt Bloem. Das hat auch für die Zertifizierung, die bei diesen Chips vorgeschrieben ist, große Bedeutung.

Das gesamte Feld der Sicherheit von Hardware und Software wird immer bedeutender, und Mangard und Bloem wünschen sich viel mehr Studierende. Auch wenn bereits etwa jeder Vierte, der an der TU Graz studiert, im Bereich der Informatik unterwegs ist, ist die Nachfrage von der Wirtschaft enorm.

Digitale Sicherheit

Das IAIK (Institut Angewandte Informationsverarbeitung und Kommunikationstechnologie) an der Technischen Universität Graz ist das größte Institut zum Thema digitale Sicherheit in Österreich. Rund 60 Wissenschaftler haben etwa 1000 Publikationen veröffentlicht. **Weltweit** einer breiteren Öffentlichkeit bekannt wurde das Institut bei der Aufdeckung von Sicherheitsmängeln in Chips.

SPAZIERGANG IM SCIENCE GARDEN

Ingrid Krumphals ist Hochschulprofessorin an der PH Steiermark PH/HILBE

1 Was machen qualitätsvolle Erlebnisse aus den Bereichen Mathematik, Informatik, Naturwissenschaften und Technik (MINT) aus?

INGRID KRUMPHALS: Ein qualitätsvolles MINT-Erlebnis ist stets auf die Zielgruppe abgestimmt. Anbieter von solchen Erlebnissen müssen sich an der Lebenswelt der Teilnehmer orientieren. Es sollen positive Emotionen geschaffen und praktische Aufgaben umgesetzt werden.

2 Wie wirkt sich das auf die Projekte aus?

Die Qualitätskriterien geben den Anbietern einen wichtigen Orientierungsrahmen. So finden sich im Science Garden Erlebnisse, bei denen Probleme aus dem Alltag gelöst werden, offenen Fragen nachgegangen wird und im Labor experimentiert werden kann.

3 Was bedeutet das für die Teilnehmer?

Der Science Garden steht für MINT-Erlebnisse, die von Expertinnen der Pädagogischen Hochschule Steiermark und der Privaten Pädagogischen Hochschule Augustinum erarbeitet wurden. Damit sind den Teilnehmern lehrreiche und unvergessliche Erlebnisse garantiert.

Mehr „Science Garden" gibt es auf der Homepage der Initiative, die Hunderte Angebote steirischer Hochschulen zusammenfasst. **www.sciencegarden.at**