AMMO
Angewandte Mathematische Modellierung & Optimierung

FH Bielefeld
University of
Applied Sciences

Treffpunkt AMMO

Car-to-Car-Kommunikation als Beispiel für angewandte Kryptographie

In naher Zukunft werden Autos miteinander kommunizieren, um in Gefahrensituationen, wie etwa einem Stauende in einer unübersichtlichen Kurve, einen automatischen Bremsvorgang auslösen zu können.

Die dazu ausgetauschten Daten werden digital signiert, damit sie vor Manipulationen durch Angreifer geschützt sind. Dabei kommen kryptographische Verfahren auf Basis Elliptischer Kurven zum Einsatz, die aufgrund ihrer geringen Schlüssellänge und kurzen Signaturen für diesen Zweck prädestiniert sind.

Die ESCRYPT GmbH arbeitet seit ihrer Gründung im Jahre 2004 an innovativen Sicherheitslösungen für eingebettete Systeme, insbesondere für Fahrzeuge.

Der Vortrag beim "Treffpunkt AMMO" gibt anhand der praktischen Anwendung "Car-to-Car-Kommunikation" einen Überblick über Kryptographie auf Elliptischen Kurven und stellt das Signaturverfahren ECDSA im Detail vor. Dabei werden auch Implementierungsaspekte (Seitenkanalresistenz, Optimierung für ressourcen-beschränkte Steuergeräte) beachtet.

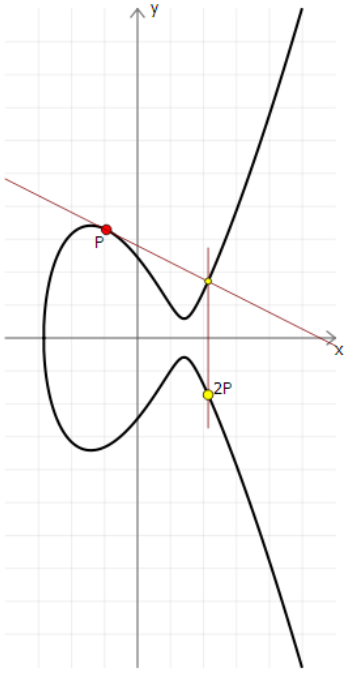

Abb.: *Punktverdopplung als eine der Basis-operationen für Elliptische Kurven*

Do, 06.06.2019
14:00 Uhr

Interaktion 1, Raum: D014
33619 Bielefeld

Referent: **Dipl.-Inf. André Osterhues** (ESCRYPT GmbH, Bochum)

Moderation: **Prof. Dr. Jörg Horst** (FSP AMMO, FH Bielefeld)

Alle Interessierten sind herzlich eingeladen!

Fachhochschule Bielefeld – University of Applied Sciences
Fachbereich Ingenieurwissenschaften und Mathematik – FSP AMMO
http://www.fh-bielefeld.de/ammo – +49 521 106-7410 – ammo@fh-bielefeld.de