ulm university universität
uulm

Bogdan Dina

Seminar/Proseminar im WS 2018/19
Thema: Das Diskrete-Logarithmus Problem und Kryptographie mit elliptischen Kurven.

Bei diesem (Pro)Seminar geht es darum den Zusammenhang zwischen dem DLP und der Sicherheit einiger wichtiger Kryptosysteme zu verstehen. Im Grunde genommen beruht die Sicherheit des RSA-Verfahrens und Kryptographie mit elliptische Kurven auf zwei Probleme:

- Faktorisieren ganzer Zahlen und
- Das Diskrete Logarithmus-Problem.

Wir werden uns in diesem (Pro)Seminar mit dem zweiten Punkt näher beschäftigen. Dabei geht es darum dass wir das DLP verstehen und einige Angriffsarten gegen das DLP entwickeln. Anschließend werden wir u.a. verstehen welche *Gruppen* weniger geeignet für kryptographische Verfahren sind. Kryptographie mit elliptischen Kurven ist das andere Thema, welches wir näher betrachten werden. Wir werden u.a. kennenlernen wie man das Additionsgesetz auf elliptische Kurven definiert ...

1 Das Diskrete-Logarithmus Problem (*DLP*).

1.1 Grundlagen und der Babystep-Giantstep Algorithmus.
Teilnehmer(Ba.): 2.

1.2 Chinesischer Restsatz und der Pohlig-Hellman Algorithmus.
Teilnehmer (Ba.): 2

1.3 Pollard's ρ-Algorithmus und das DLP.
Teilnehmer (Ba.): 2

2 Kryptographie mit elliptischen Kurven

2.1 Grundlagen elliptische Kurven.
Teilnehmer (Ba/Ma.): 2

2.2 Elliptische Kurven über endliche Körpern.
Teilnehmer (Ma.): 2

2.3 Kryptographie mit elliptische Kurven.
Teilnehmer (Ba.): 2

2.4 Das elliptische Kurven Diskrete Logarithmus-Problem (ECDLP).
Teilnehmer (Ba.): 2

2.5 Divisoren, Paarungen und das ECDLP (anspruchsvoll).

Bitte wenden!

Teilnehmer (Ma.): 2

Literatur

[1] J. Silverman J. Hoffstein, J.Pipher. *An Introduction to Mathematical Cryptography*. Springer.

[2] L.C.Washington. *Elliptic Curves Number Theory and Cryptography*, volume Second Edition. Chapman & Hall/CRC.

[3] J.H. Silverman M.Hindry. *Diophantine Geometry An Introduction*. Springer.