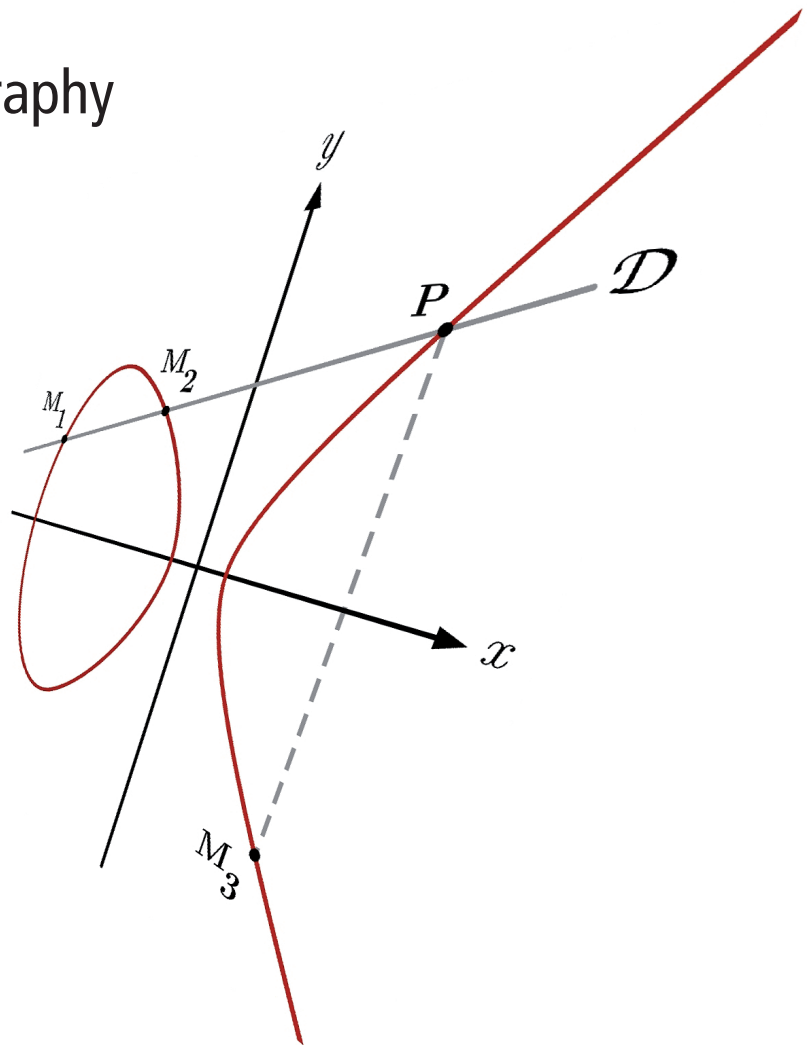


# OMTE CRYPTONET: SECURITY IN AD-HOC NETWORKS

## Securing OLSR version 2 using elliptic curve cryptography and digital signature

Despite its major importance in the advent of large scale industrial deployments, security is all too often left as “a poor cousin” or simply an “afterthought” in current efforts in mobile ad-hoc network research. The Cryptonet team is currently working towards securing the popular OLSRv2 protocol in order to make it robust against disruptive attacks. Our approach: using digital signatures based on elliptic curves.

The underlying problems extend far beyond mere application of cryptographic primitives, and so this work does not pretend to be the “be-all-end-all” solution to mobile ad-hoc network security. However, by presenting a first milestone, our goal is to spread awareness on major security issues arising in mobile ad-hoc networks, attract industrial partners with a practical stance on security and ultimately foster new academic-industrial partnerships.



### Keywords:

*Elliptic curve cryptography,  
digital signature, integrity,  
mobile ad-hoc network,  
OLSR.*



Contacts: Morain@lix.polytechnique.fr ■ Thomas@thomasclausen.org

