

Zero-Knowledge Proofs

Showing you *can* do something, without showing how

Alex Dehnert

6.UAT

Fall 2011