Exploring Password Authenticated Key Exchange Algorithms

Final Year Project Screencast

Sam Leonard

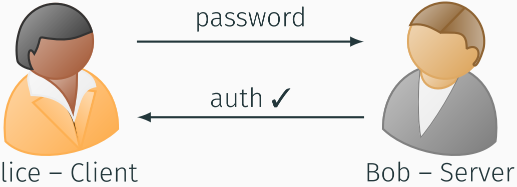
Supervisor: Bernardo Magri

Table of contents

1. Introduction
2. Context
3. Demo

Intro

Motivation



Traditional Authentication

Motivation

PAKEs are a radically different solution to this problem.

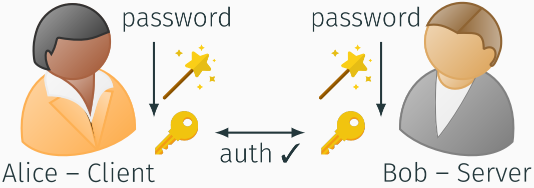
- the password never leaves a user’s device
- an eavesdropper cannot learn enough information to attack the protocol
- both the server and client are authenticated with each other

Project Summary

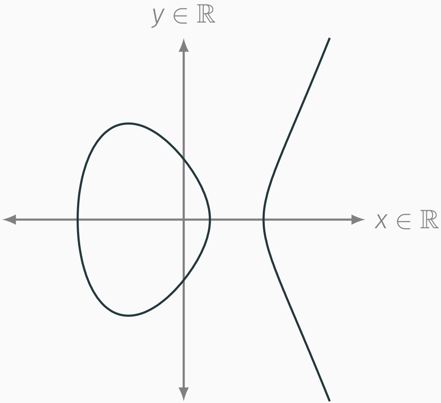
- implemented AuCPace in Rust
- contributed the implementation back to open-source
- created an example application of AuCPace running on real hardware

Context

What are PAKEs?

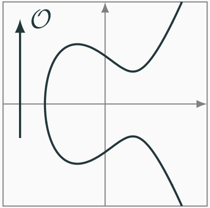


Elliptic Curves

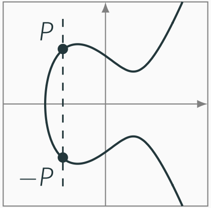


$y^2 = x^3 - 2x - 1$ over $\mathbb{R}$

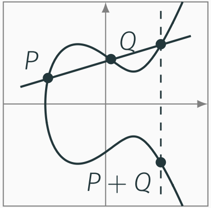
Point addition



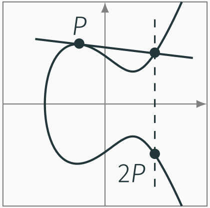
Neutral element $\mathcal{O}$



Inverse element $-P$



Addition $P+Q$
“Chord rule”



Doubling $P+P$
“Tangent rule”

Finite Fields

clock maths

Elliptic Curves Over Finite Fields

dotty curves

AuCPace

Augmented Composable what now?

Demo

Conclusion

I did a thing!

Thank you for watching!