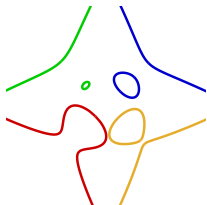
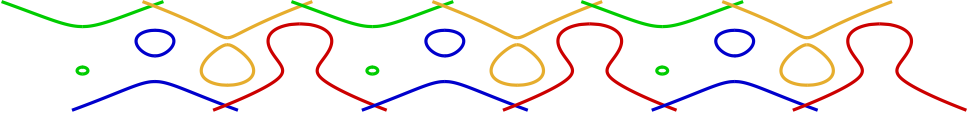


# Projekt Digitale Signaturen

Georg Grasegger



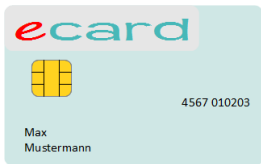


Unterschrift

“Im rechtwinkligen Dreieck ist die Summe der Kathetenquadrate  
ungleich dem Hypotenusenquadrat.”

*Πυθαγόρας*


# Anwendung



## Bürgerkarte



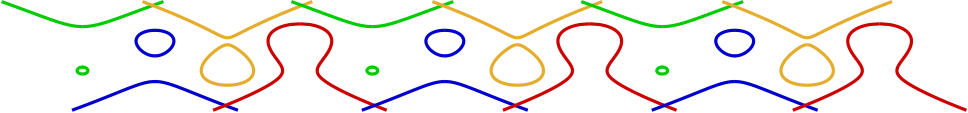
## Email

Signaturwert	n77uQwPyEt00ytfQwCp/Li4mJFEU7G8-eusgoWe;OTFqj7zetAyztbC\1GB82-r2bbj 8G73EMKso6 40;So>j51PvV-sa1fj GKaJ8ervb`Be D=KpL301yct` ;dMj 2 N`>6p0o8Gos818Wv:0pyR:nAMS-grfawW221147H014`_Tel<vWZ3Ip_<01E												
	<table border="1"><tr><td>Untersigner</td><td>serialNumber=0123456789</td></tr><tr><td>Datum/Zeit-UTC</td><td>2015-03-09T14:00:00Z</td></tr><tr><td>Aussteller-Zertifikat</td><td>Vertrauensdienst-Zertifikat</td></tr><tr><td>Serien-Nr.</td><td>9978</td></tr><tr><td>Medium</td><td>Elektronisch</td></tr><tr><td>PubKeyInfo</td><td>Para-1.2</td></tr></table>	Untersigner	serialNumber=0123456789	Datum/Zeit-UTC	2015-03-09T14:00:00Z	Aussteller-Zertifikat	Vertrauensdienst-Zertifikat	Serien-Nr.	9978	Medium	Elektronisch	PubKeyInfo	Para-1.2
Untersigner	serialNumber=0123456789												
Datum/Zeit-UTC	2015-03-09T14:00:00Z												
Aussteller-Zertifikat	Vertrauensdienst-Zertifikat												
Serien-Nr.	9978												
Medium	Elektronisch												
PubKeyInfo	Para-1.2												
PrüfInformation	Informationen zur Prüfung elektronischer Signaturen finden Sie unter:												

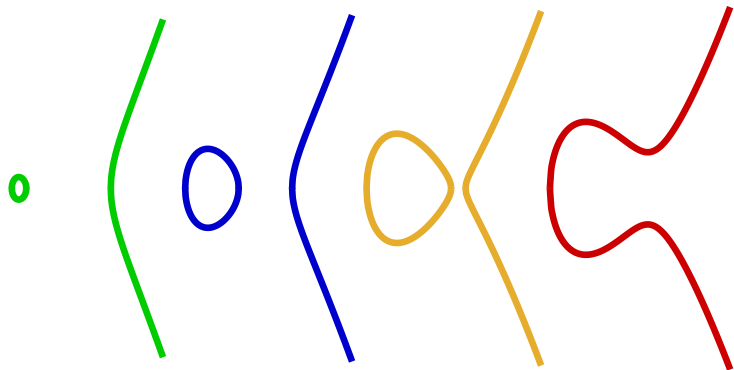
## Dokumente

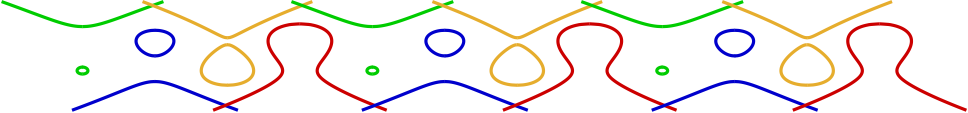


## Mobilgerät



## Elliptische Kurven





## Aufgabe(n)

- Verfahren kennen lernen
- Schwachstellen herausfinden
- Software erstellen/verwenden
- Rechenoperationen für elliptische Kurven entwickeln