HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

1 Cryptographical Strength

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

Chat: Cryptographical Strength Needed Today?

	Recommended Algorithms	Key Size	True Strength
Symmetric Encryption		bits	bits
Data Integrity (Hash Function)		bits	bits
Key Exchange between Peers		bits	bits
Digital Signature		bits	bits
Public Key Encryption		bits	bits
User Password		chars	bits

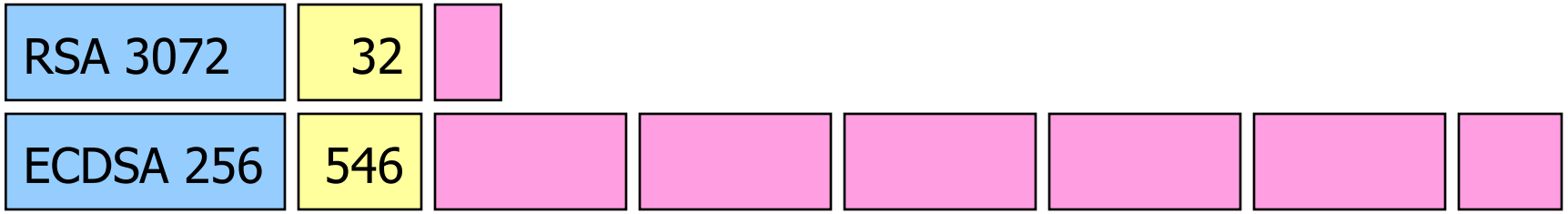
Cryptographical Strength Needed Today?

	Recommended Algorithms	Key Size	True Strength
Symmetric Encryption	AES (CBC or Counter-Mode)	128 bits	128 bits
Data Integrity / Hash Function	SHA-256 (SHA-2 or SHA-3)	256 bits	128 bits
Key Exchange between Peers	Diffie Hellman with Prime Modulus (MODP)	3072 bits	128 bits
Digital Signature	RSA / DSA	3072 bits	128 bits
Public Key Encryption	RSA / El Gamal	3072 bits	128 bits
User Password	Abbreviated Passphrase	14* chars	≈80 bits

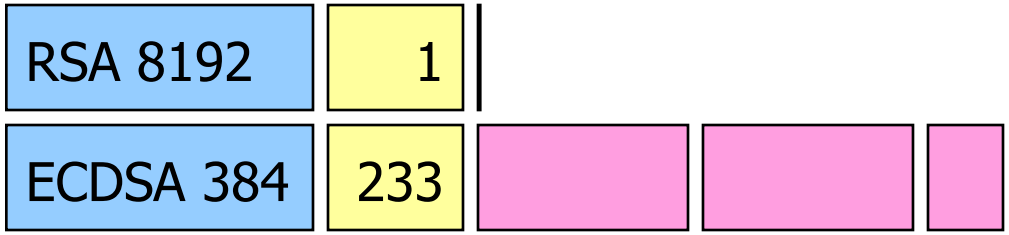
*22 base64 characters would be required for 128 bit strength but impossible to memorize!

Equivalent Cryptographic Strength

128 bit strength: number of private key signatures per second*



192 bit strength: number of private key signatures per second*



*measured on an Intel Core2Duo T9400 platform (one core, 32 bit Linux OS)

1.1 NSA Suite B Cryptography

NSA Suite B Cryptography 2005

- The secure sharing of information motivates the need for widespread cryptographic interoperability that meet appropriate security standards to protect classified information at the TOP SECRET level.
- NSA has initiated three efforts to address these needs:
  - The Cryptographic Interoperability Strategy.
  - Expanding the use of GOTS products that meet a revised set of security standards to protect information up to the TOP SECRET level.
  - Layered use of COTS products that meet a more robust set of security standards to protect information up to the TOP SECRET level.
- Several IETF protocol standards have been identified as having potential widespread use. IETF RFCs have been established to allow the use of Suite B Cryptography with these protocols.

NSA Suite B with 128 Bit Security (SECRET)

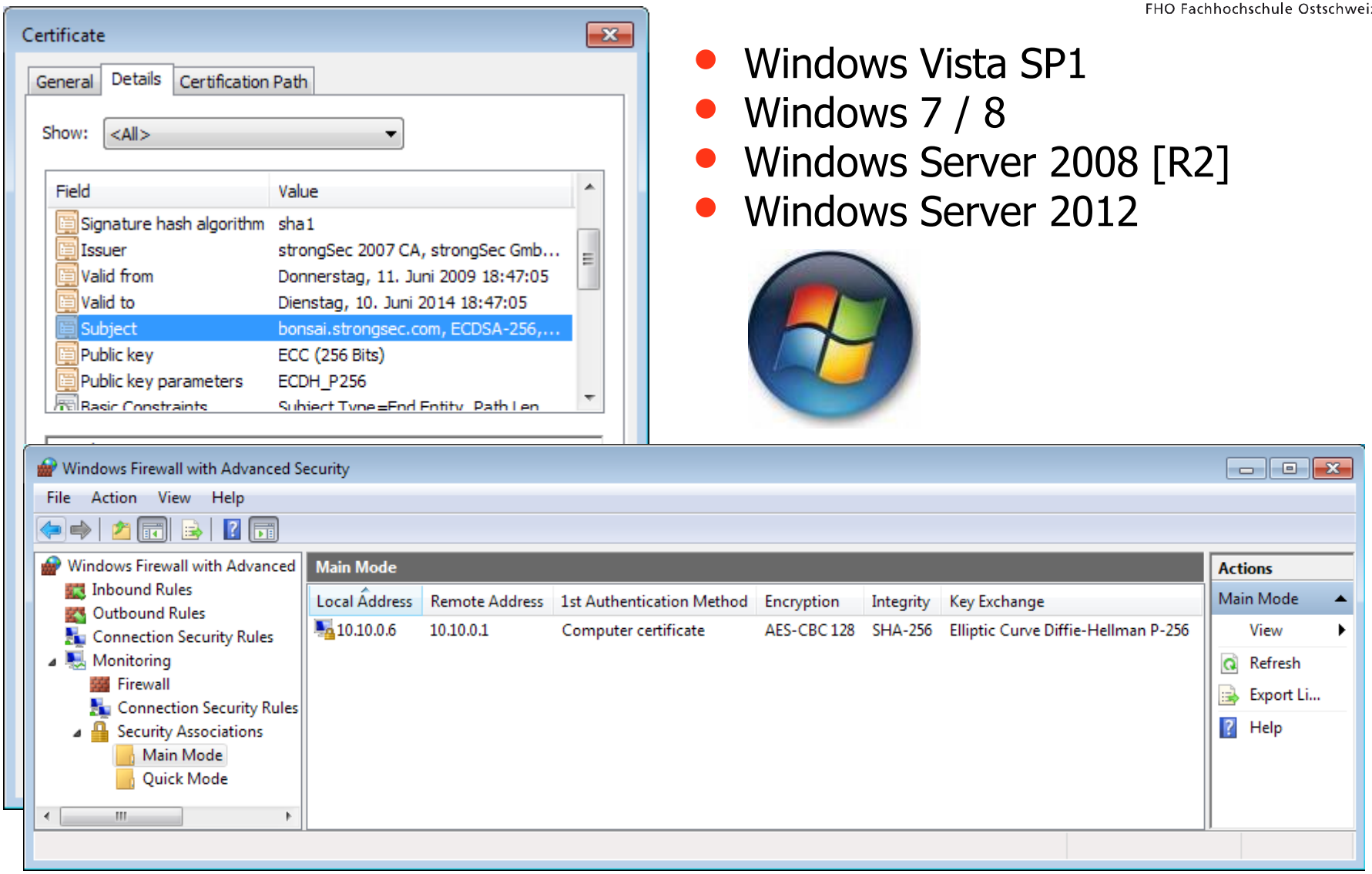
	Recommended Algorithms	Key Size	True Strength
Symmetric Encryption	AES	128 bits	128 bits
Data Integrity/ Hash Function	SHA-256	256 bits	128 bits
Authenticated Encryption	AES-GCM (Galois-Counter-Mode)	128 bits	128 bits
Key Exchange between Peers	Elliptic Curve Diffie Hellman (ECP)	256 bits	128 bits
Digital Signature	Elliptic Curve DSA	256 bits	128 bits

NSA Suite B with 192 Bit Security (TOP SECRET)

	Recommended Algorithms	Key Size	True Strength
Symmetric Encryption	AES	256* bits	256 bits
Data Integrity / Hash Function	SHA-384	384 bits	192 bits
Authenticated Encryption	AES-GCM (Galois-Counter-Mode)	256* bits	256 bits
Key Exchange between Peers	Elliptic Curve Diffie Hellman (ECP)	384 bits	192 bits
Digital Signature	ECDSA	384 bits	192 bits

* AES with 192 bit key is optional. Therefore AES with a 256 bit key is mandated.

Microsoft Windows with Suite B Support



- Windows Vista SP1
- Windows 7 / 8
- Windows Server 2008 [R2]
- Windows Server 2012

strongSwan VPN Solution with Suite B Support


```
# ipsec.secrets for gateway moon
: ECDSA moonKey.der
```

```
# ipsec.conf for gateway moon
conn rw
     keyexchange=ikev2
     ike=aes256-sha384-ecp384,aes128-sha256-ecp256!
     esp=aes256gcm16,aes128gcm16!
     leftsubnet=10.1.0.0/24
     leftcert=moonCert.der
     leftid=@moon.strongswan.org
     right=%any
     rightsourceip=10.3.0.0/24
     auto=add
```

```
rw[1]: ESTABLISHED 9 seconds ago, 192.168.0.1[moon.strongswan.org]...
                                  192.168.0.100[carol@strongswan.org]
rw[1]: IKE SPIs: 7c1dcd22a8266a3b_i 12bc51bc21994cdc_r*,
rw[1]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256
rw{1}:  INSTALLED, TUNNEL, ESP SPIs: c05d34cd_i c9f09b38_o
rw{1}:  AES_GCM_16_128, 84 bytes_i (6s ago), 84 bytes_o (6s ago),
rw{1}:   10.1.0.0/24 === 10.3.0.1/32
```

1.2 What the Heck are Elliptic Curves!

What are Elliptic Curves?

General form:

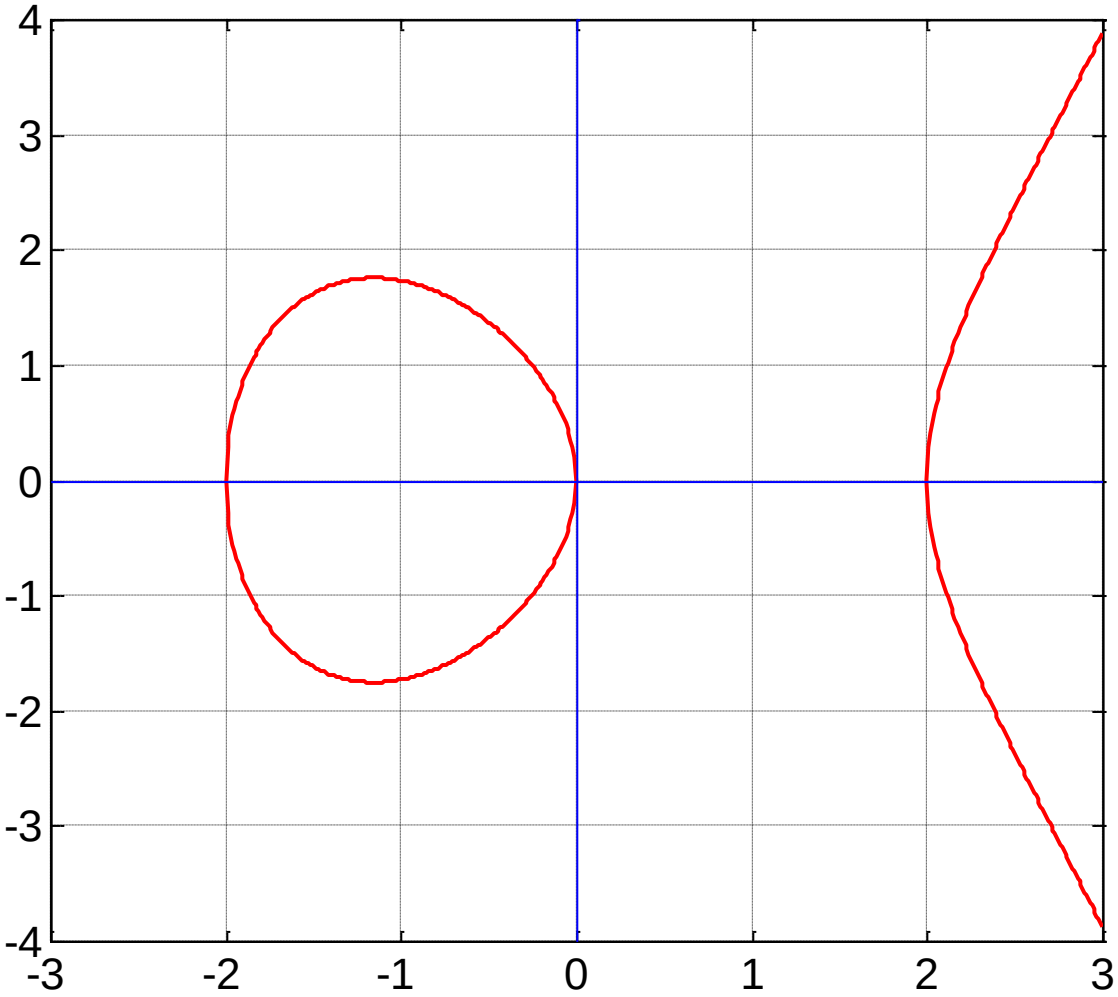
$$y^2 = x^3 + ax + b$$

Condition for distinct single roots:

$$4a^3 + 27b^2 \neq 0$$

Example:

$$y^2 = x^3 - 4x$$
$$= x(x-2)(x+2)$$



What is an Algebraic Group <G,∗> ?

A group is an algebraic system consisting of a set G and an operation ∗ such that for all elements a, b and c in G the following conditions must be fulfilled:

- Closure: $a * b$ must remain in G
- Associativity: $a * (b * c) = (a * b) * c$
- Neutral Element: $a * e = e * a = a$
- Inverse Element: $a * a' = a' * a = e$
- Commutativity: $a * b = b * a$ (Abelian Group)

Examples:

- Addition: $\langle R, + \rangle$ $e = 0$, $a' = -a$
- Multiplication: $\langle R-\{0\}, \cdot \rangle$ $e = 1$, $a' = a^{-1}$

Points P(x,y) on an Elliptic Curve form a Group

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

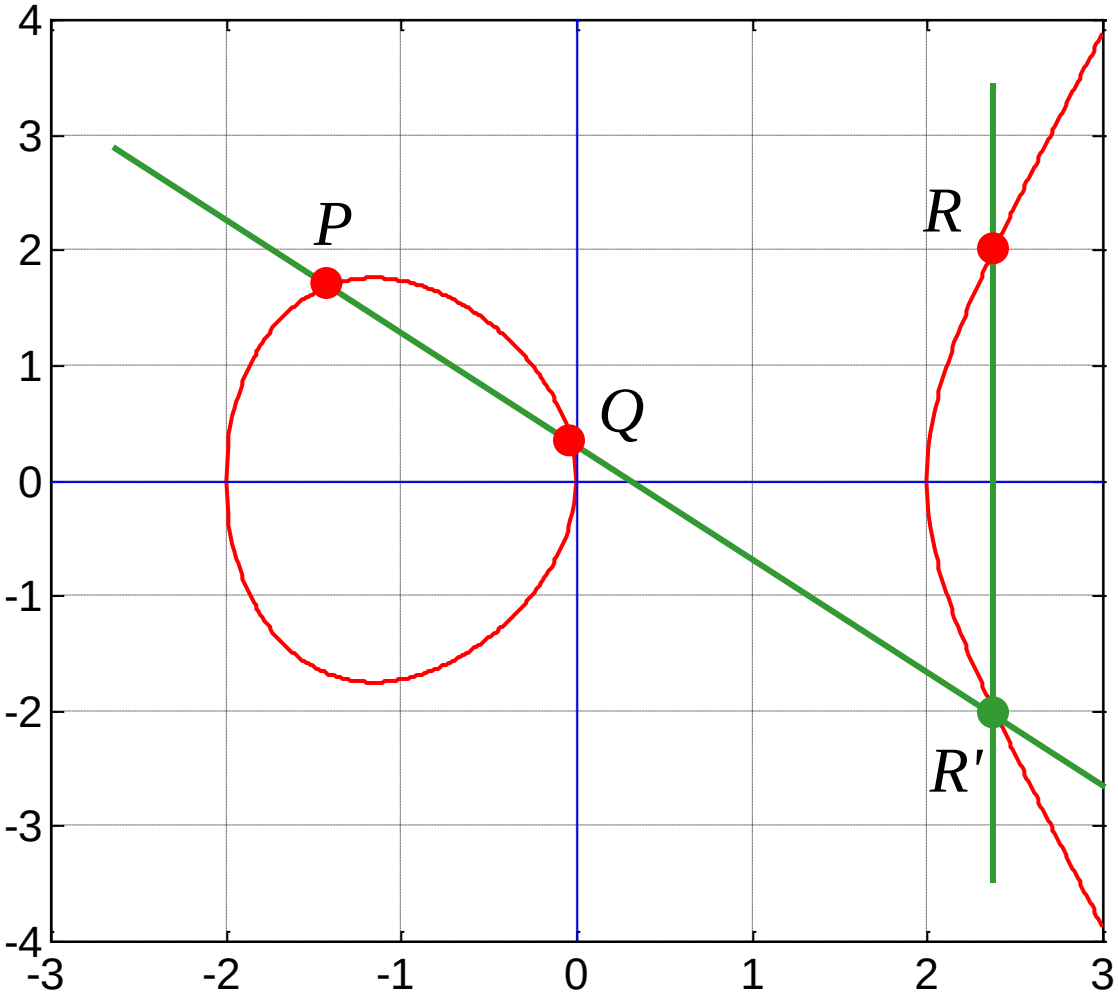
Group set:

All points P(x,y) lying on an elliptic curve

Group operation:

Point addition

$$R = P + Q$$



Neutral and Inverse Elements

Inverse element:

P'(x,-y) = P(x,y)

is mirrored on x-axis

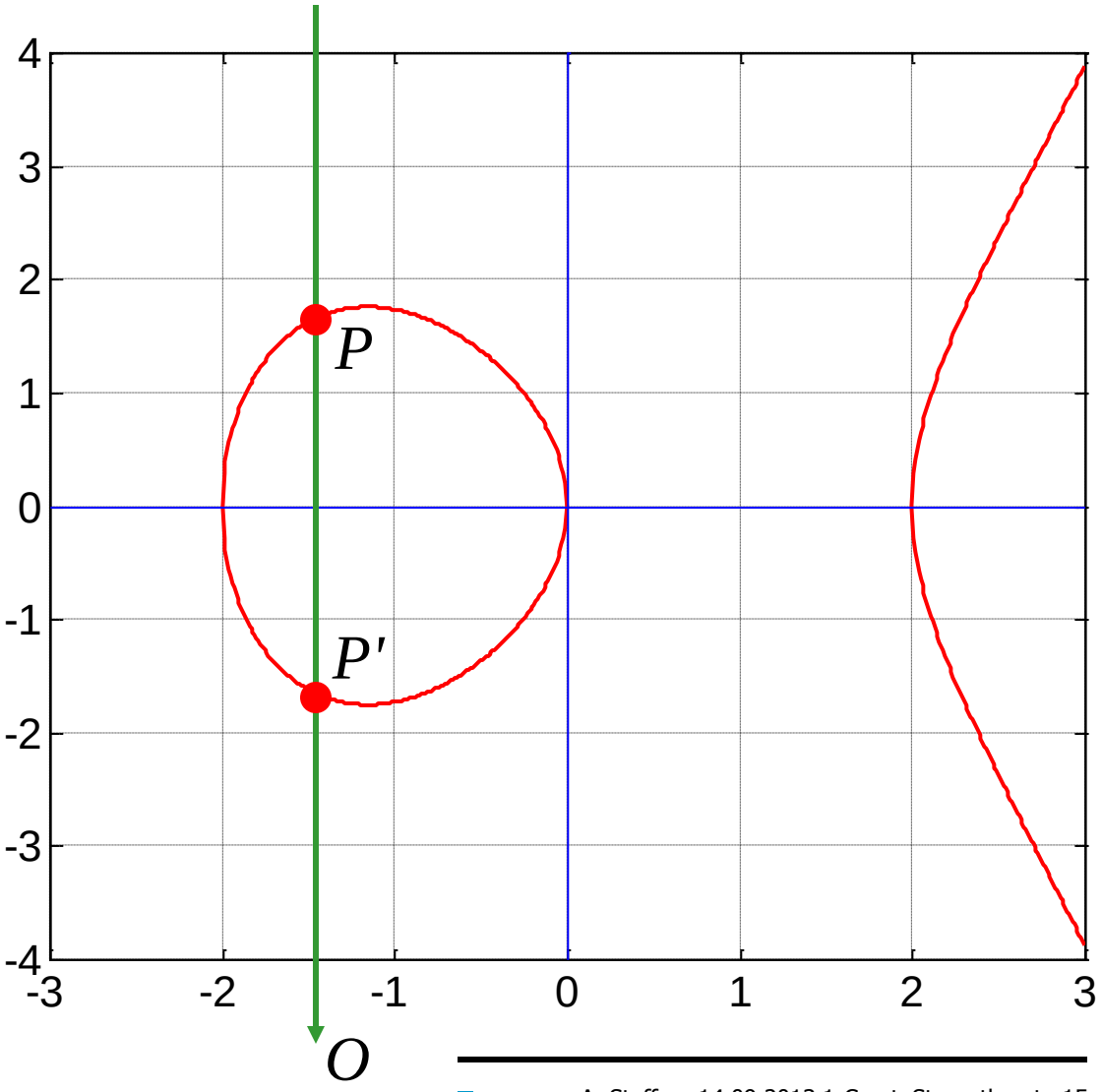
Point addition with inverse element:

P + P' = O

results in a neutral element O(x,∞) at infinity

Neutral element:

P + O = P

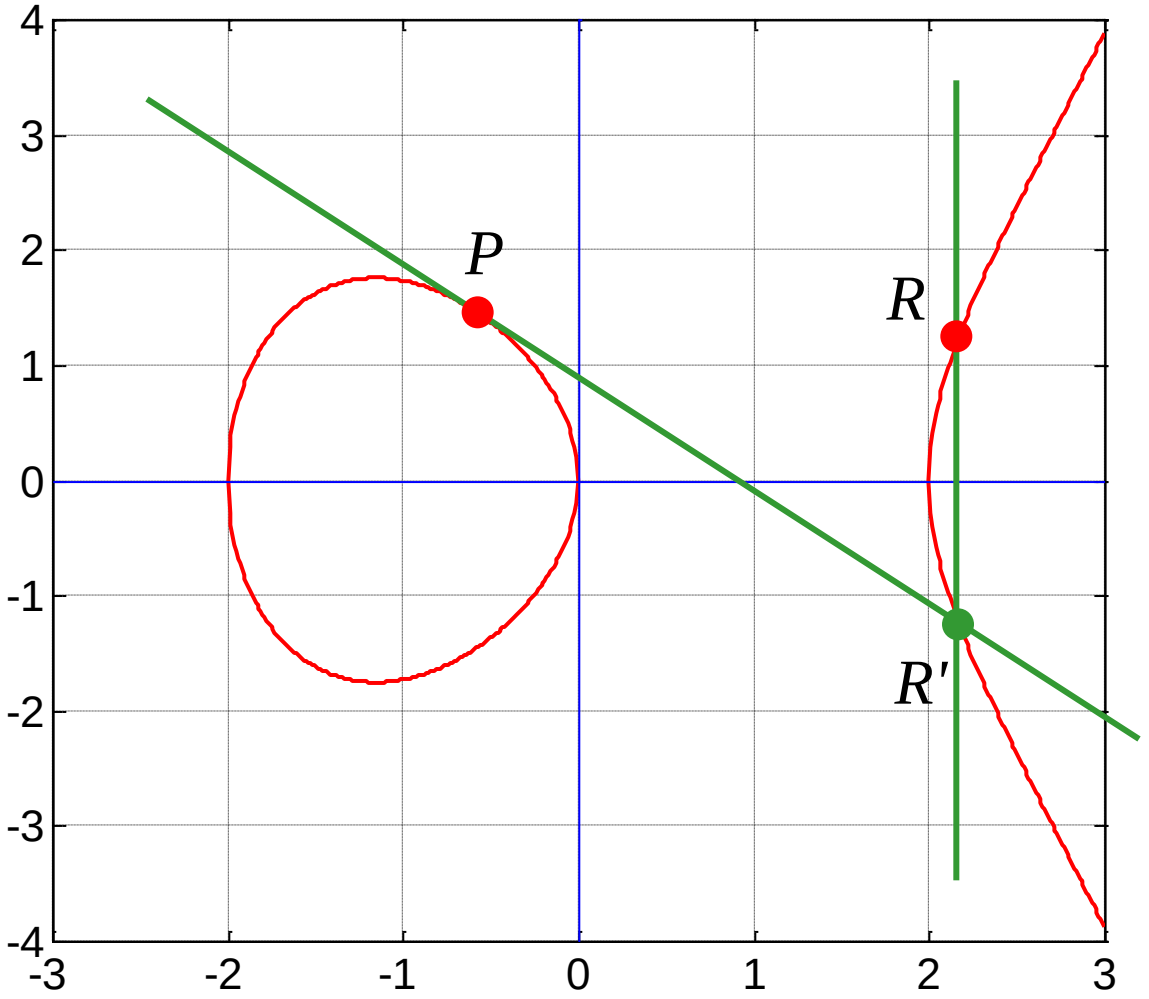


Point Doubling – Adding a point to itself

Point Doubling:

Form the tangent in Point P(x,y)

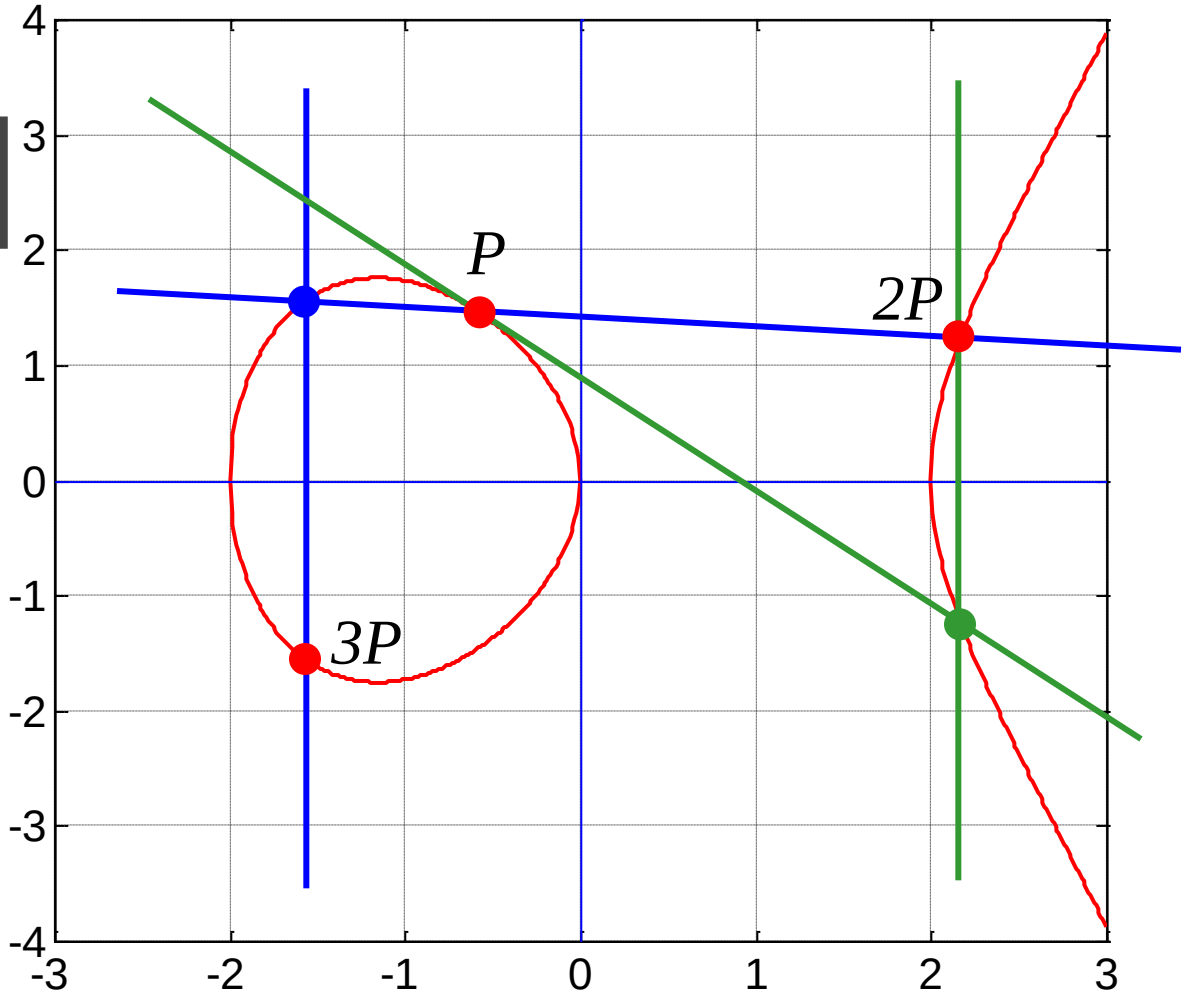
$$R = P + P = 2P$$



Point Iteration – Adding a point k-1 times to itself

Point Iteration:

$$kP = P + P + \ldots + P$$



How can Geometry be useful for Cryptography?

Elliptic curves can be defined in a finite or Galois field GF_p:

$$y^2 = x^3 + ax + b \mod p$$

where the field size p is a prime number and

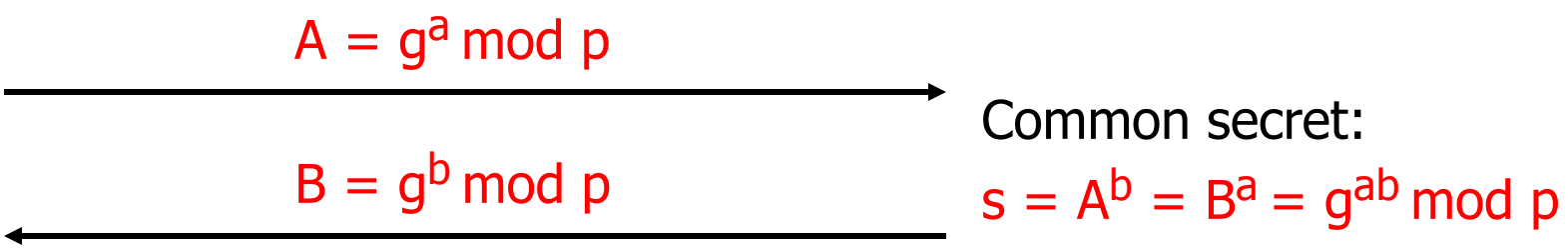
{0,1, ..., p-1} is an abelian group under addition mod p

and

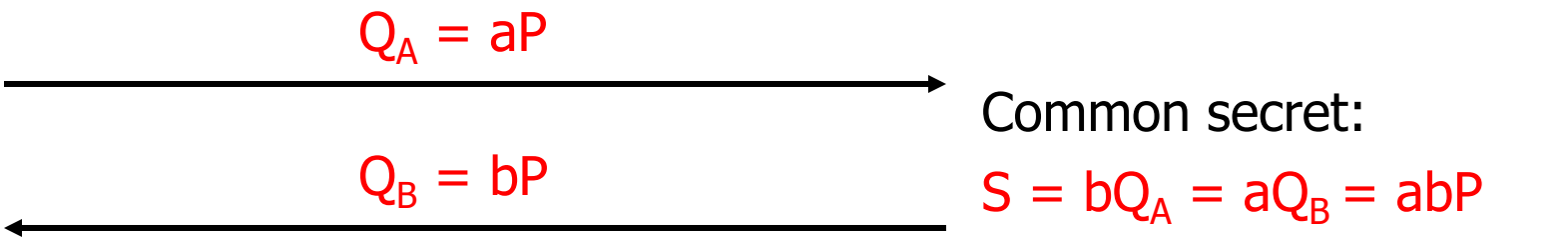
{1, ..., p-1} is an abelian group under multiplication mod p.

Cryptographic Application – Secret Key Exchange

- Diffie-Hellman: Basis g and prime p



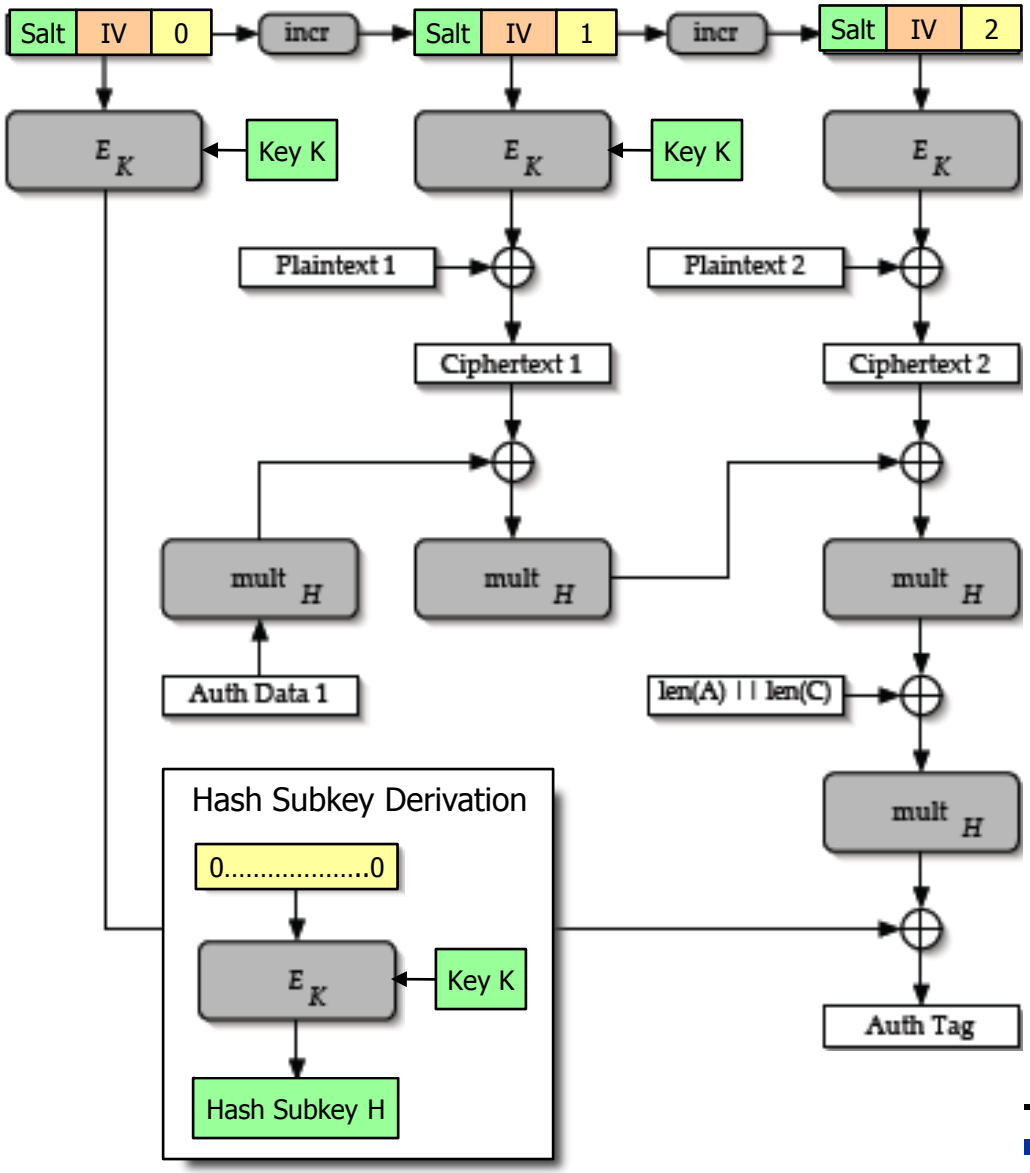
- Elliptic Curve Cryptosystem: ECC, basis point P and prime p



HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

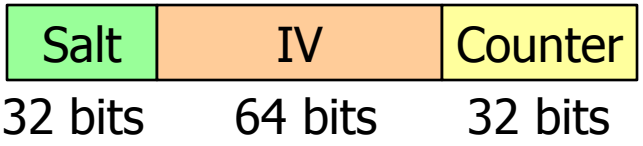
1.3 Authenticated Encryption with Associated Data (AEAD)

Authenticated Encryption with Associated Data



- AEAD is based on special block cipher modes:

- Block size: 128 bits
- Key size: 128/256 bits
- Tag size : 128/96/64 bits
- Nonce size: 128 bits



- Recommended AEAD Modes:
  AES-Galois/Counter Mode
  AES-GMAC (auth. only)

- Alternative AEAD Modes:
  AES-CCM
  CAMELLIA-GCM
  CAMELLIA-CCM