An introduction to Elliptic Curve Cryptography: Motivation of ECC and Security Aspects of ECC

Ulrich Jetzek
University of Applied Sciences Kiel
Germany

12th International Symposium on
Ambient Intelligence and Embedded Systems

September 19th – 21st, 2013

Beuth University of Applied Sciences, Berlin, Germany

Overview

1. ECC Motivation: Exponentiation and Logarithm
2. Elliptic Curves
3. Elliptic Curve Discrete Logarithm Problem (ECDLP)
4. Security of Ciphers
5. Attacks on ECC attacks
   a) Analytical attacks
   b) Side channel attacks
6. Conclusions

Motivation for Elliptic Curve Cryptography

- **Problem:** Public key cryptosystems usually require algebraic operations in integer rings and fields with parameters of more than **1000 bits**.
  - **High computational effort** on CPUs with 32-bit or 64-bit arithmetic
  - **Large parameter sizes** critical for storage on small and embedded devices

- **Motivation:** Smaller key sizes providing **equivalent** security level are desirable

- **Solution:**
  - **Elliptic Curve Cryptography**:
  - group of points in a 2-dimensional plane
  - instead of integers (1-dimensional) as in RSA, DLP, ElGamal

Exponentiation and Logarithm

- Exponentiation over real numbers: $\alpha^x = \beta$
- Inverse function: „conventional“ Logarithm $x = \log_\alpha \beta$

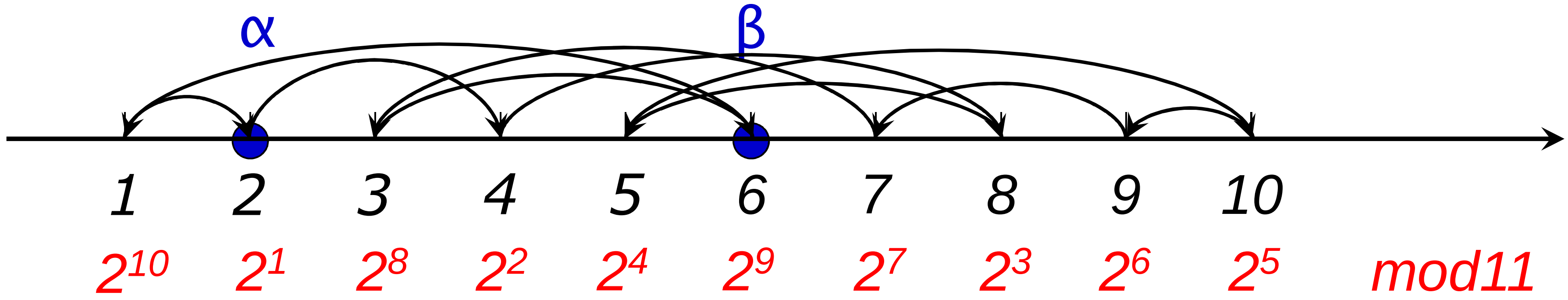
- Contrast: ONE-WAY-Function:
- Exponentiation over finite group, modulo p: $\alpha^x \equiv \beta \bmod p$
- Discrete Logarithm Problem (DLP): $x = \log_\alpha \beta \bmod p$

- For large p it is computationally infeasible to calculate x.

Plausibility Example for the DLP:

$\mathbb{Z}_{11}^{*}=\{1,2,3,4,5,6,7,8,9,10\}$

Exponentiation 2^x *mod 11: „jumping“ around within* $\mathbb{Z}_{11}^{*}$

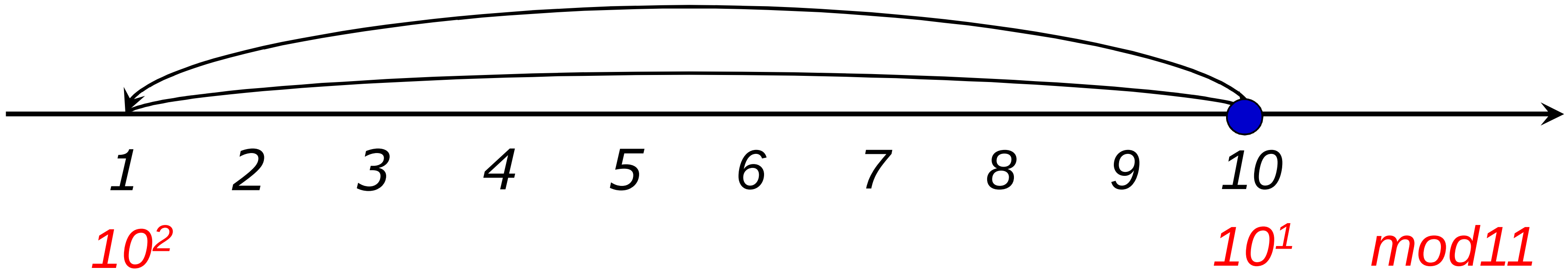


DLP: given „starting point“ α and „end point“ β, the problem is to find out how many „jumps“ are necessary from α to β

Plausibility Example for the DLP:

$\mathbb{Z}_{11}^{*}=\{1,2,3,4,5,6,7,8,9,10\}$

Exponentiation 2^x *mod 11: „jumping" around within* $\mathbb{Z}_{11}^{*}$



Starting point must be a primitive or generator point.

DLP not secure if starting point has low order!

Definition : Elliptic Curve

The elliptic curve over the field of real numbers $\mathbb{R}$ is the set of all pairs $(x,y) \in \mathbb{R}$ which fulfill the equation :

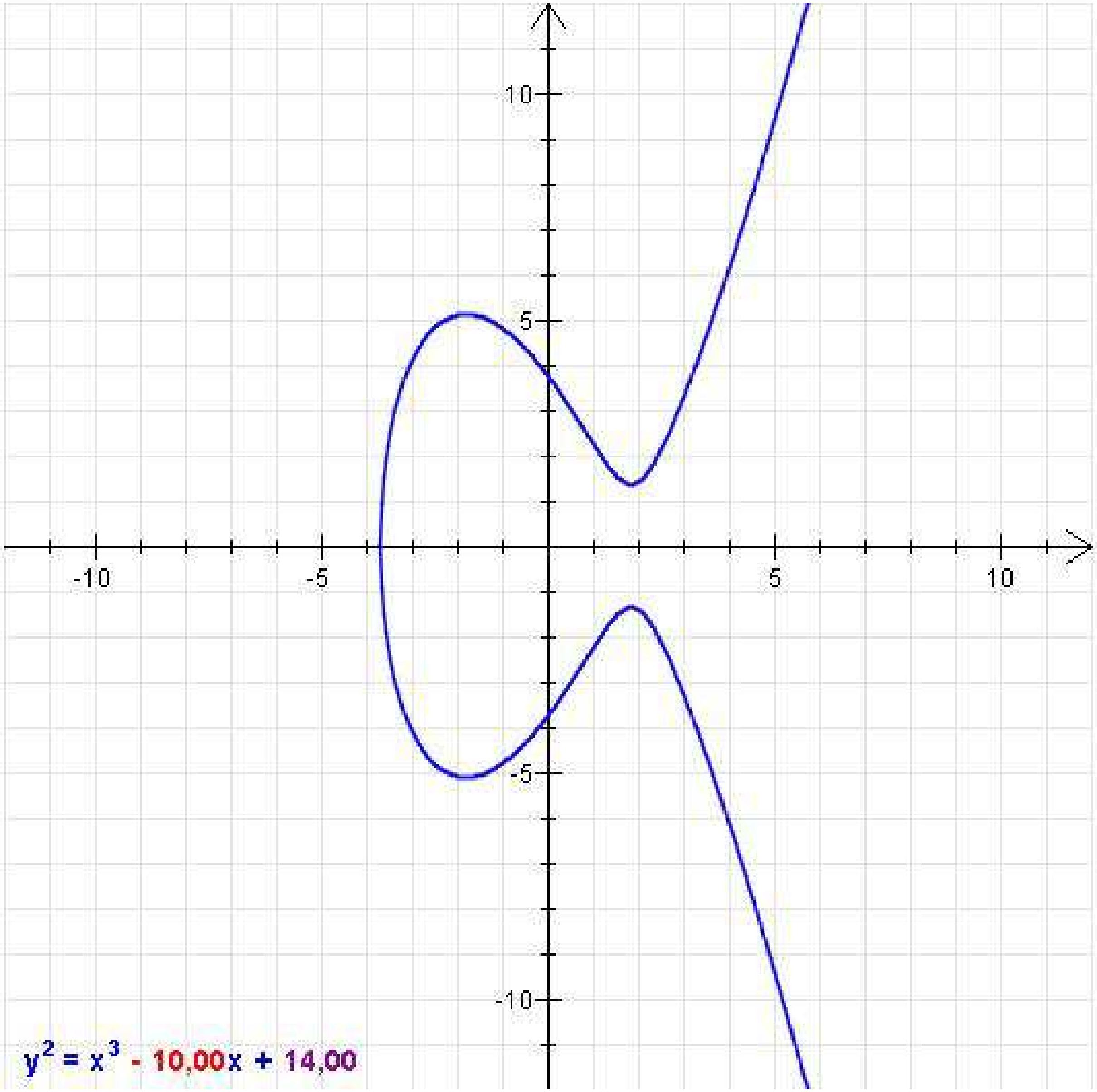
$$E : y^2 = x^3 + a \cdot x + b$$

together with an imaginary point of infinity $\mathcal{O}$, where $a,b \in \mathbb{R}$

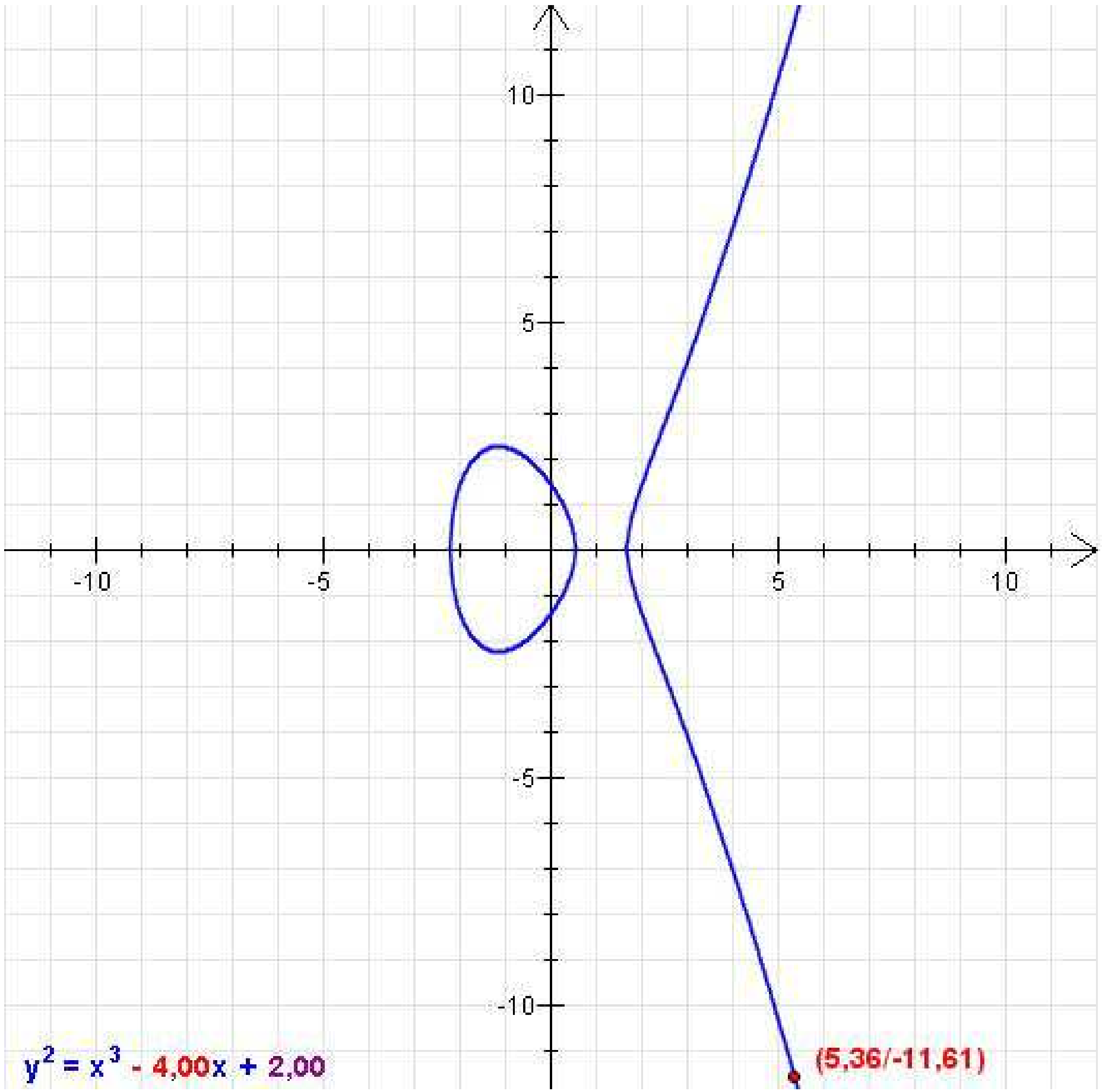
and the condition $4 \cdot a^3 + 27 \cdot b^2 \neq 0$

(curve must be non-singular) holds.

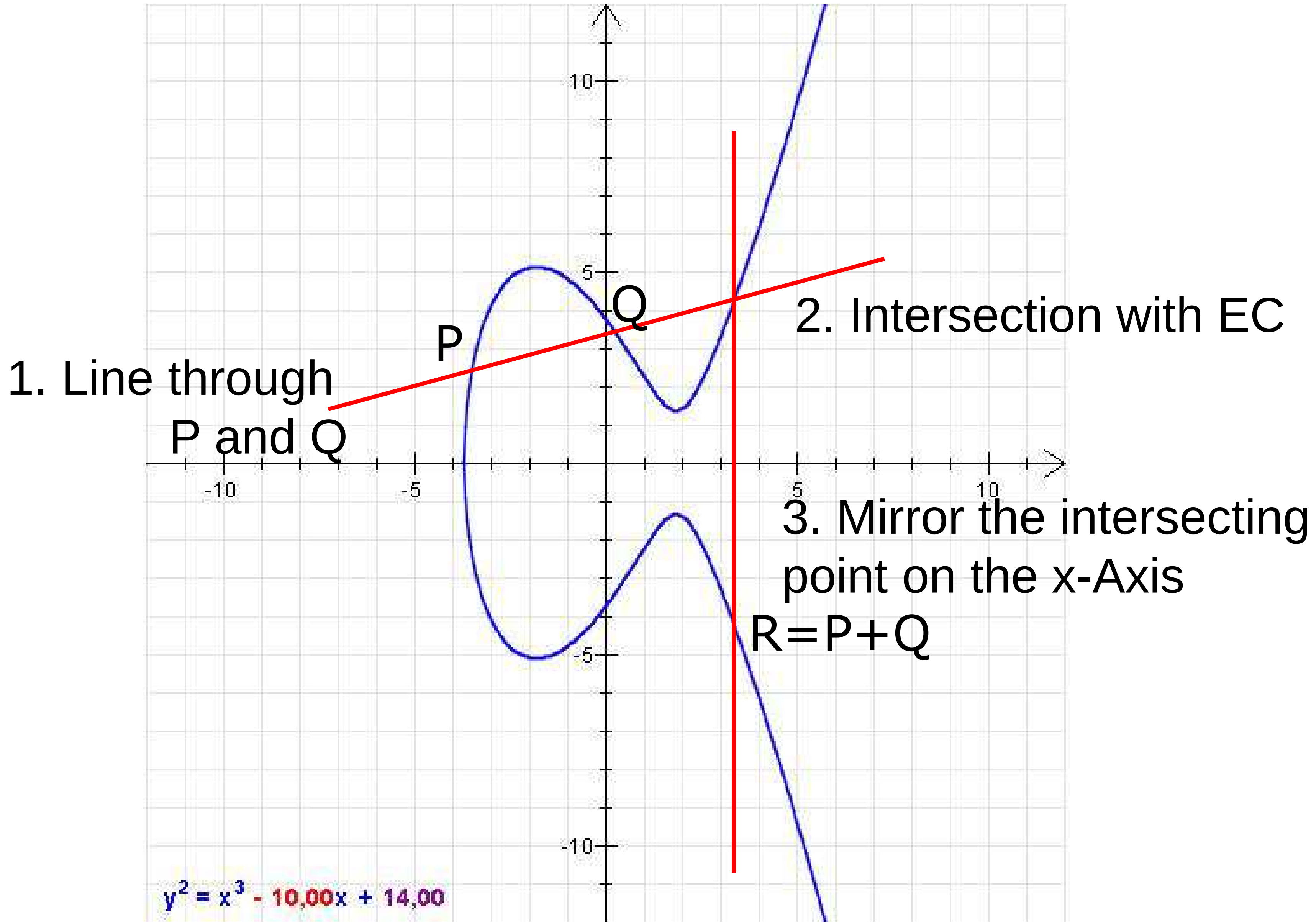
Point Addition on Elliptic Curves



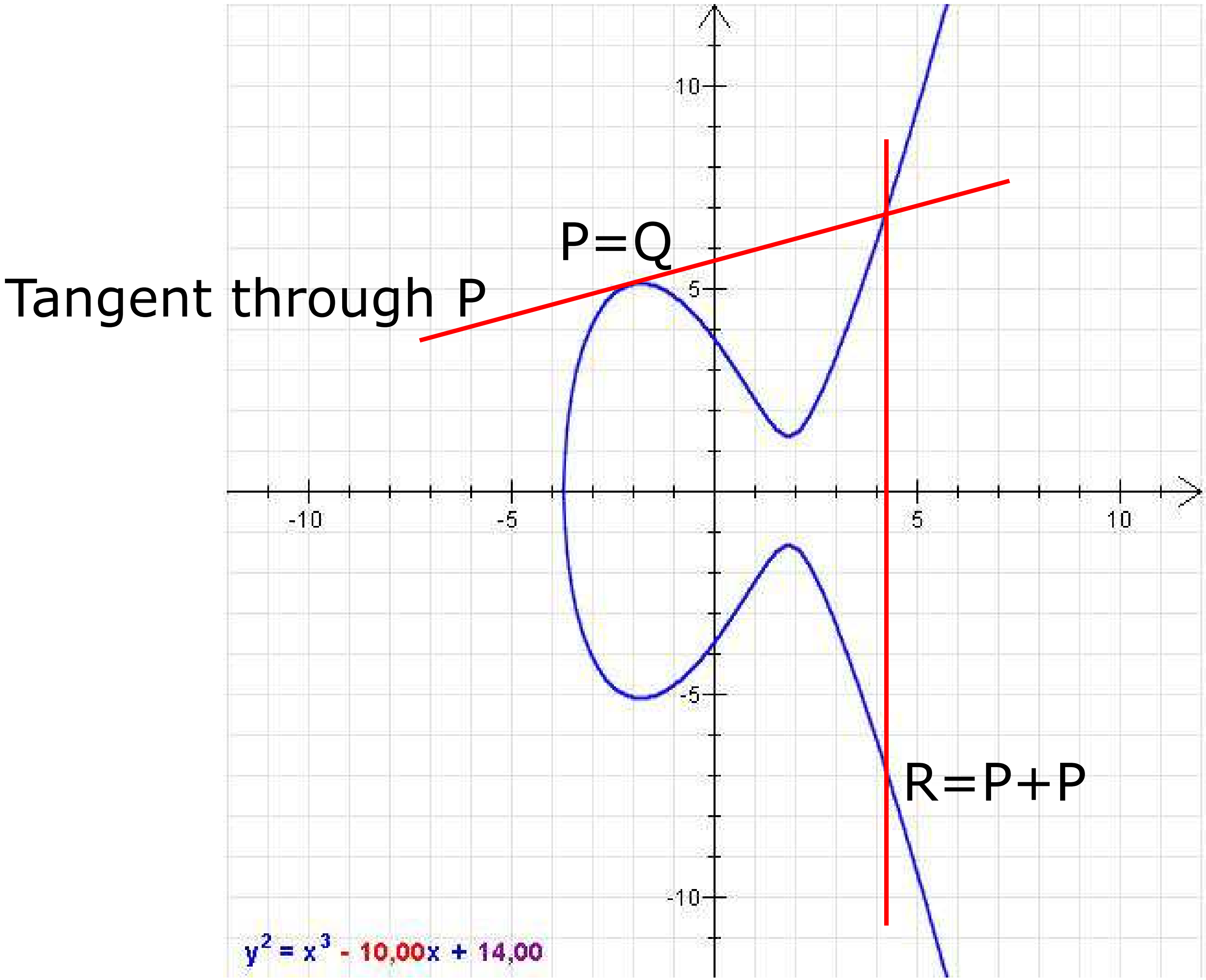
Elliptic Curves – Example 2



Point Addition on Elliptic Curves



Point Doubling on Elliptic Curves



Introduction to Elliptic Curves

- For a DLP we need a cyclic group. For a group we need:
  - a set of elements
  - a group operation which fulfills the group laws.

Property	Prime fields / groups	Elliptic curves
Group Elements	Integers	Points on the curve (x,y)
Group operation in case of DLP	Multiplication	Addition

Introduction to Elliptic Curves

- For a DLP we need a cyclic group. For a group we need:
  - a set of elements
  - a group operation which fulfills the group laws.

Property	Prime fields / groups	Elliptic curves
Group Elements	Integers	
Group operation in case of DLP	Multiplication	

Introduction to Elliptic Curves

- In cryptography *finite fields* are needed (instead of fields with an infinite number of elements), hence we define:

Definition : Elliptic Curve over prime fields

The elliptic curve over the field $\mathbb{Z}_p$, p > 3 is

the set of all pairs $(x,y) \in \mathbb{Z}_p$ which fulfill the equation :

$$E : y^2 = x^3 + a \cdot x + b \bmod p$$

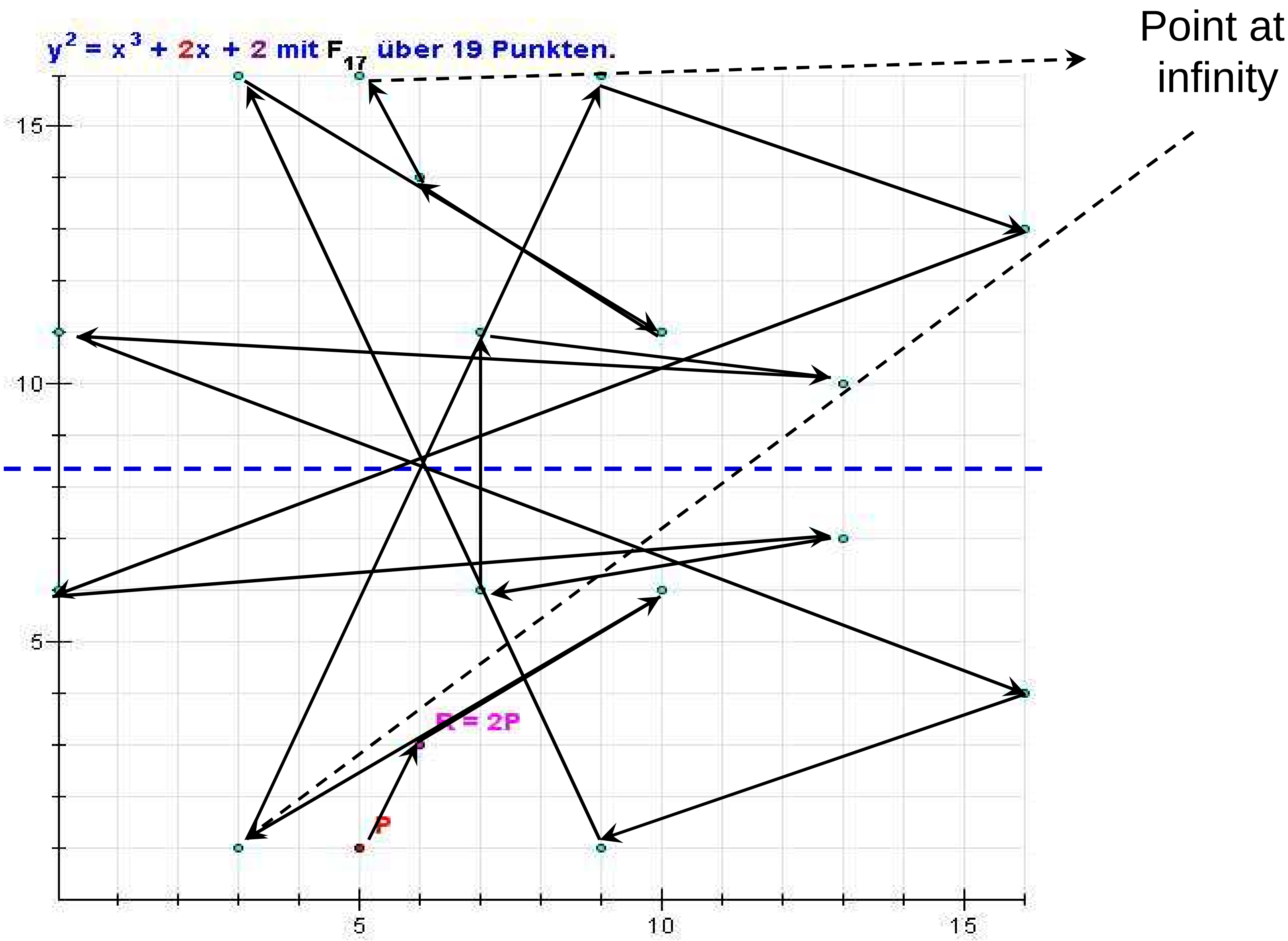
together with an imaginary point of infinity $\mathcal{O}$, where

$a,b \in \mathbb{Z}_p$

and the condition $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \mod p$

(curve must be non-singular) holds.

Elliptic Curve over finite group



Elliptic Curve Discrete Logarithm Problem

Given:

Elliptic Curve E,

primitive point P and

another point T.

The ECDLP is:

finding the integer d (1≤d≤|E|), such that:

$$\underbrace{P + P + \ldots + P}_{d\ times} = d \cdot P = T$$

Security levels and key lengths of crypto systems

- „Security level of n bit“: Best known attack requires 2^n steps.

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Analytical Attacks on ECC [Pelzl]

- Order of point P: ord(P)=n (e.g. 2^{160})
- Naïve Search: Sequentially test P, 2P, 3P, 4P, …
  - Brute force attack, infeasible for groups with more than 2^{80} elements. **Complexity in the order of n**.
- Shanks Baby-Step-Giant-Step Algorithm
  - **Complexity in time AND memory of about sqrt(n)** (e.g. $2^{160/2}=2^{80}$)
- Pollard's Rho method
  - Most efficient algorithm for solving the general ECDLP so far
  - Requires less memory space that Shanks
  - Parallel implementation possible
  - **Complexity in time of about sqrt(n) (e.g. $2^{160/2}=2^{80}$)**

- NOTE: All attacks have **exponential** complexity!

State of the Art ECCs Attacks until 2009

Curve	Field Size	Machine Days (based on Pentium 100)	Status
ECC2-79	79	352	Solved 12/1997
ECCp-79		146	Solved 12/1997
ECC2-97	89	180448	Solved 3/1998
ECCp-97		71982	Solved 9/1998
ECC2-109	109	$2,1 \cdot 10^7$	Solved 4/2004
ECCp-109		$9 \cdot 10^7$	Solved 11/2002
ECCp-112 [LACAL]	112	177 (PS3-Cluster-days)	Solved 7/2009

112-bit prime ECDLP Infos [Lacal]

$$\text{prime p}: p = 0x\text{DB7C 2ABF62E35E668076 BEAD208B}$$

$$\text{Elliptic Curve E}: y^2 = x^3 + ax + b$$

$$with:$$

$$a = 4451685225093714772084598273548424$$

$$\text{b} = 2061118396808653202902996166388514$$

$$\text{Point P with coordinates}:$$

$$(\text{x} = 188281465057972534892223778713752,$$

$$\text{y} = 3419875491033170827167861896082688)$$

$$\text{Order of point P} \quad ord(P) = 4451685225093714776491891542548933$$

Side Channel Attacks to ECC [Fan]

- Simple Power Analysis [Coron]
  - Value of scalar bits of d can be revealed if bad guy ‚Oscar' can distinguish between point doubling and addition from power trace.
- Differential Power Analysis [Kocher]:
  - Statistical techniques to find out the secret information (d) out of measurements.
  - Feed device with N input points P_i.
  - Measure and store time for point multiplications $d \cdot P_i$.
  - Choose intermediate value, depending on P_i and small part of d
  - Transform this value into hypothetical leakage value by using hypothetical leakage model.
  - Guess small part of secret scalar d.
  - Reveal the whole scalar d incrementally using same method.

Side Channel Attacks to ECC [Fan]

- Comparative Side Channel Attacks [Fouque]:
  - Resides between Simple Power Analysis and Differential Power Analysis
  - 2 portions of same of different leakage trace are compared
  - Example: Assume 2 point doublings, 2P and 2Q, even if bad guy ‚Oscar' does not know P and Q, he may tell if P=Q.
  - Comparing traces for d·P and d·2P, Oscar may recover all bits of d.
- Refined Power Analysis [Goubin]:
  - Exploits the existence of special points: (x,0) and (0,y).
  - Feeding a point *P* into a device that leads to one of the special points after *i* point additions leads to side channel leakage information, that can be exploited to find out scalar *d*.
- Zero-Value Point Attack:
  - Extension of Refined Power Analysis – considers points stored in auxiliary registers.

Conclusion

- ECC may be used for key exchange, digital signatures and for encryption
- ECC provides same level of security as RSA or the discrete logarithm with considerably shorter key lengths (160-256 bits).
- But …
- More and more side channel attacks and Fault Analysis Attacks are coming up recently, which exploit
  - Timing patterns, power consumption and/or
  - Specific properties of the curves, such as e.g. special points.

Thank you !

References

- [Pelzl]: Jan Pelzl: „Exact Cost Estimates for ECC Attacks with Special Purpose Hardware“, 10th Workshop on Elliptic Curve Cryptography, Toronto, 2006
- [Lacal]: École Polytechnique Fédérale de Lausanne, Laboratory for Cryptographic Algorithms: „Play Station 3 computing breaks 2^{160} barrier, 112-bit prime ECDLP solved“, 2009
- [Fan]: Junfeng Fan, Ingrid Verbauwhede: „An updated Survey on Secure ECC Impelementations“, Attacks, Countermeasures and Cost“, Quisquater Festschrift, LNCS 6805, pp. 265-282, 2012
- [Coron]: J.Coron: „Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems“, CHES 1999, LNCS, vol. 1717, pp.292-302, 1999
- [Kocher]: P.C.Kocher et al.: „Differential Power Analysis“ in M.Wiener: CRYPTO 1999. LNCS, vol. 1666, pp. 388-397, 1999.
- [Fouque]: P.-A. Fouque et al.: „The Doubling Attack“ – why Upwards is better than Downwards.“ in CHES 2003, LNCS, vol 5154, pp. 269-280, 2003
- [Goubin]: L.Goubin: „Refined Power Analysis on Elliptic Curve Cryptosystems“.In LNCS, vol 2567, pp. 199-2010, 2002