Public Key Crypto Systems and Elliptic Curves

Gerhard Frey

Public Key Crypto Systems and Elliptic Curves

Gerhard Frey

Institute for
Experimental Mathematics
University of Duisburg-Essen
frey@exp-math.uni-essen.de

CIMPA
École de cryptographie
Université Mohammed I
Oujda
18 - 30 Mai 2006

Contents

References

Everything needed about Elliptic Curves can be found in
J. Silverman: *The Arithmetic of Elliptic Curves, GTM 106*, Springer 1986

Everything used in the lecture about Public Key Cryptography and Elliptic Curves including the theory of finite fields both from the theoretical and algorithmic point of view can be found in
H. Cohen & G. Frey (eds.): *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC 2005
cited in the following as **BOOK**.

In this book one finds an exhausting list of references (40 pp)

Lecture 1

1 DISCRETE LOGARITHMS BASED on ELLIPTIC CURVES

Almost all practically used (or usable) crypto systems rely on crypto primitives based on hard computational problems in easily "implemented" mathematical objects.
-In these lectures we shall concentrate us to the **Discrete Logarithm Problem (DLP)** in groups G whose order is divided by a large prime number ℓ.

1.1 Key Exchange

1.1.1 Abstract setting

Assume
$A \subset \mathbb{N}$ and $B \subset End_{set}(A)$.
For simplicity we shall assume that B is closed under composition.
Key Exchange Assume that there is an element $a_0 \in A$ such that the elements of B commute on $B\{a_0\}$:
For all $b_1, b_2 \in B$ we have

$$b_1(b_2(a_0)) = b_2(b_1(a_0)).$$

Use

$$(A, a_0), B$$

for a key exchange system in an obvious way:

The partners P_i (i=1,2) choose b_i and publish $b_i(a_0)$.
Then

$$b_1(b_2(a_0)) = b_2(b_1(a_0))$$

is the common secret.
The security depends (not only) on the complexity to find for randomly chosen $a_1, a_2 \in B\{a_0\}$ **all** elements $b \in B$ with $b(a_0) = a_1$ modulo the relation:

$$b \sim b' \text{ iff } b(a_2) = b'(a_2).$$

1.1.2 One Realization

Choose $A =: G$ a cyclic group of prime order ℓ embedded into $\mathbb{N}$ by a numeration and let a_0 be a generator.

$$B := Aut_{\mathbb{Z}}(G) \cong (\mathbb{Z}/\ell)^*$$

can be identified with $\{1, ..., \ell - 1\}$ by

$$b(a) := a^b.$$

The key exchange scheme is:
P_i chooses $b_i \in \mathbb{Z}$ and publishes $a_0^{b_i}$.
Then

$$(a_0^{b_1})^{b_2}$$

is the common secret key.

A (non-trivial) result is:
The security is determined by the complexity of the
Discrete Logarithm Problem (**DLP**)
For randomly chosen $a_1, a_2 \in G$ compute $n \in \mathbb{N}$ with

$$a_2 = a_1^n.$$

The residue class of such an n modulo ℓ is called $log_{a_1}(a_2)$.
Remark:
There are "derived" cryptographic schemes for which the hardness of
DHDP: For randomly given elements a_0, a_1, a_2, a_3 decide whether

$$log_{a_0}(a_1) \cdot log_{a_0}(a_2) = log_{a_0}(a_3).$$

1.2 DL-Systems

Definition 1.1 *A* **DL-system** *is a group G of prime order ℓ with*

- *the elements in G are presented in a compact way i.e. by $O(log(\ell))$ bits*
- *the group composition $\oplus$ is easy to be implemented and very fast,i.e. has complexity $O(log(\ell))$.*

- *the discrete logarithm problem (DL-problem) i.e.:*
  for randomly chosen elements $g_1, g_2 \in G$ compute a number $k \in \mathbb{Z}$ such that $[k]g_2 = g_1$
  is hard to be computed.

1.2.1 Security Hierarchy

In the ideal case the complexity of DLP in a group G were

$$exp(C \cdot \log(\ell) + O(1))$$

with positive (and not too small) C.
This is obtained in *generic groups*, and, as we hope, in certain groups related to elliptic curves and abelian varieties of dimension 2.
In this case we say that the complexity of the DL is **exponential**.

In many cases one gets a weaker result: The complexity is **subexponential**, and this forces to take the parameters larger to get security.

Explicitly this means:
There are numbers $0 < \alpha < 1$ and C such that the complexity for computing the DL is

$$O(exp(C \cdot log(\ell)^{\alpha} \cdot log(log(\ell))^{1-\alpha})).$$

In practice α is often $1/2$ or $1/3$.

The security of the DL- system is very poor if the complexity is **polynomial**, i.e.

$$O(exp(C \cdot log(log(\ell)))).$$

In this case security could be achieved only because of big constants, and so it is not scalable by enlarging ℓ.

Remark 1.2 *A typical example for an algorithm with subexponential complexity is factoring numbers by the* **(general) number field sieve**.
The number α *is* $1/2$ *(respectively* $1/3$ *with the GNFS).*
This forces to take as parameters for RSA-systems numbers n *with* $log_2(n) \geq 2048$.

1.3 Attacks

We describe two types of rather general methods to compute discrete logarithms. Of course we can use for *every* key exchange scheme brute force attacks (e.g. exhaustive search).
This has complexity $O(\ell)$.

1.3.1 Generic Attacks

Using the algebraic realization, i.e. using the structure "group" the amazing fact is that we can do much better than brute force attacks: The Baby-Step-Giant-Step method of Shanks as well as the ρ- and Λ-methods of Pollard work in every finite group. All of them have time-complexity $O(\ell^{1/2})$ and the methods of Pollard need very little storage space (for more details cf. BOOK, sect. 19.4, 19.5, 19.6.)
Hence they are exponential with constant $C = 1/2$.
The good news is that in "generic groups" we cannot do better.

1.3.2 Index-Calculus

In reality we shall have to use a concrete presentation of our group. In many examples there are elements in G which are easier to deal with, and this gives rise to the index-calculus attack.

The principle of index-calculus methods in abelian groups G is to find a "factor base" $\mathcal{F}$ consisting of relatively few elements and to compute G as $\mathbb{Z}-$module given by the free abelian group generated by the base elements modulo relations.
Then one has to prove that with high probability every element of G can be written (fast and explicitly) as a sum of elements in the factor base.

The important task in this method is to balance the number of elements in the factor base to make the linear algebra over $\mathbb{Z}$ manageable and to guarantee "smoothness" of arbitrary elements with respect to this base. Typically successes give rise to algorithms for the computation of the DL in G which have **subexponential** complexity and so, for large enough order of G, the DL-systems have rather poor exponential security.

1.4 Examples

1.4.1 The additive group $\mathbb{Z}/\ell$.

This example shows that in special groups we may find special algorithms which are much faster than our general ones.
Take $a, b \in \mathbb{Z}/\ell \setminus \{0\}$.
We want to determine n such that

$$a - n \cdot b = \mu \cdot \ell.$$

Since $gcd(b, \ell) = 1$ we compute by the Euclidean algorithm number in time and space **linearly** in $log(\ell)$ numbers x_1, x_2 with

$$1 + x_1 \cdot b = x_2 \cdot \ell.$$

Hence $a \cdot x_1$ modulo ℓ is equal to $log_b(a)$.

1.4.2 The Classical DL

Take $q = p^f$ with a prime p and let $\mathbb{F}_q$ be the field with q elements.
Its multiplicative group $\mathbb{F}_q^*$ is a cyclic group with $q-1$ elements.
Let ζ be a primitive root of unity of order $q-1$ in $\mathbb{F}^*$ and $\bar{x} \in \mathbb{F}^*$ arbitrary.

Definition 1.3 *The discrete logarithm of $\bar{x}$ with respect to the base point ζ is (any) integer k with*

$$\bar{x} = \zeta^k.$$

It is clear that we can take k as element in $\mathbb{Z}/(q-1) = \{0, \ldots, q-1\}$.
We want to compute k !

1.4.3 Basic Idea

Interpret the field $\mathbb{F}$ as residue field of the ring of integers of a number field and then compute the discrete logarithm as **solution of a congruence equation**.

From now on assume the simplest case: $q = p$ is a prime.
The multiplicative group $\mathbb{F}^*$ can be represented as $(\mathbb{N}, \cdot)/\sim$ where $n_1 \sim n_2$ if and only if $n_1 \equiv n_2 \bmod p$.
A system of representatives is given by $\{1, \ldots, p-1\}$.

Let x_0 be a representative of ζ and x a representative of $\bar{x}$. Then the discrete logarithm problem translates to the congruence problem

$$\textbf{find}\, k \in \mathbb{N} \;\; \textbf{such that}\, x \equiv x_0^k \,\textbf{modulo}\, p.$$

The advantage of this formulation is that one sees the relation of the problem with the multiplicative structure of $\mathbb{N}$ and hence the factorization of numbers by prime powers can be used.
Moreover it is possible to introduce a kind of "size" for elements $\bar{x}$ in $\mathbb{F}$: it is $\log_2 x$.

Remark 1.4 *If $q = p^f$ choose g as monic irreducible polynomial over $\mathbb{F}_p$ of degree f. Then $\mathbb{F}^*$ is in a canonical way isomorphic to $(\mathbb{F}_p[X]/(g))^*$ and is represented by the polynomials of degree less than f over $\mathbb{F}_p$. We can interpret the polynomial ring $\mathbb{F}_p[X]/(g)$ as residue field of a polynomial ring $\mathbb{Z}[X]/(\tilde{g})$ where $\tilde{g}$ is a monic polynomial of degree f which is modulo p equal to g and then we can use the arithmetic of this ring to interpret and to solve the discrete logarithm problem by congruences.*

Remark 1.5 *None of the following arguments will use that $q = p$ is a prime. Hence we shall generalize the situation and try to solve–whenever it is possible– for natural numbers N and $x, x_0 \in \mathbb{N}$ the congruence equation*

$$x \equiv x_0^k \, modulo \, N \, with \, k \in \mathbb{N}.$$

1.5 Relevant Number Theory

It is well known that every natural number is the product of powers of prime numbers. Deep theorems in number theory predict some laws about properties of prime divisors, e.g. the powers which can occur or the size of the prime factors. Typically these results are asymptotic properties.
One observation is that relatively often only small factors occur. To make this precise we define the concept of smoothness.

Definition 1.6 *Let B be a positive number. A number n is $B-$smooth iff all prime divisors of n are $\leq B$.*

Theorem 1.7 *(Theorem of Canfield-Erdös-Pomerance)*
Let x, y be natural numbers which grow asymptotically such that (for some fixed $\epsilon \in]0,1[$) we have

$$(\log x)^{\epsilon} < \log u < (\log x)^{1-\epsilon}$$

with $u = \log x / \log y$ and x large enough. Let $\psi(x,y)$ be the number of numbers $n < x$ which are y-smooth.
Then

$$\psi(x,y) = xu^{-u(1-o(1))}$$

asymptotically for $x \to \infty$.

We need

Subexponential Functions:

Let α be a real number in $]0,1[$, $c \in \mathbb{R}$. Define

$$L_x(\alpha, c) := \exp(c \log x^{\alpha} \log\log x^{1-\alpha}).$$

Exercise

Show that for $\alpha > \alpha'$ we have

$$L_x(\alpha, c) L_x(\alpha', c') = L_x(\alpha, c)$$

and

$$L_x(\alpha, c) L_x(\alpha, c') = L_x(\alpha, c + c').$$

Use this and Theorem 1.7 to get
The heuristic probability to find a smooth number with smoothness bound $B = L_x(1/2, c)$ in a random walk in $[1, x]$ is

$$L_x(1/2, \frac{-1}{2c}).$$

If we want to find B such numbers we have (again heuristically) to make $\sim L_x(1/2, c)L_x(1/2, -1/2c) = L_x(1/2, \frac{2c-1}{2c})$ trials.

1.6 Strategy

The idea for the computation of the discrete logarithm modulo N is to divide the task.

1.6.1 First Step

We choose a smoothness bound B and assume that the base point x_0 is B-smooth with order $\varphi(N)$.
Take x as starting point of a controlled walk by taking powers of x modulo N which behaves like a random walk. The probability to meet a smooth element $y = x^d$ is as above.

Assume that we can compute $k \in N$ with $y \equiv x_0^k$ modulo N.
We can compute the (multiplicative) inverse d' of d modulo $\varphi(N)$ by using Euclid's algorithm and get

$$x \equiv y^{d'} \equiv x_0^{kd'} \text{ modulo } N.$$

So we have reduced the computation of the discrete logarithm to the

1.6.2 Second Step

Solve the congruence equation for *smooth numbers*!

Relations Assume that $\mathcal{F}$ consists of s prime numbers (e.g. all primes $\leq B$). Let $\mathcal{F}$ be the free lattice $\mathbb{Z}^s$ generated by exponents of $p_i \in \mathcal{F}$ as entries in the vectors $z = (\dots, z_i, \dots)$.
By $m(z)$ we denote the homomorphism from $\mathbb{Z}^s$ into the group of smooth numbers which maps $z = (\dots, z_i, \dots)$ to $\prod_{p_i \in \mathcal{F}} p_i^{z_i}$.

Remark 1.8 *If $z = (\dots, z_i, \dots)$ corresponds to a number $\leq N$ then it is a sparse vector.*

Define $\bar{m}$ from $\mathbb{Z}^s$ to $\mathbb{Z}/N^*$ by

$$\bar{m}(z) :\equiv m(z)$$

modulo N.
The kernel of $\bar{m}$ consist of vectors $(\dots, z_i, \dots)$ with

$$\prod_{p_i \in \mathcal{F}} p_i^{z_i} \equiv 1 \mod N.$$

Such vectors give **relations**: rational numbers with smooth numerator and denominator which are congruent to 1 modulo N. List resulting vectors

$$v_1 = (v_{j1}), \dots, v_t = (v_{jt})$$

in a matrix.

1.6.3 Linear Algebra

We assume that the base point x_0 is smooth and (to be explicit) has exponential vector $e = (1, 0, \ldots, 0)$.
The element x is assumed to be smooth with exponential vector
$v = (v_i), p_i \in \mathcal{F}$.
We look for $\lambda \in \mathbb{Z}$ such that $e - \lambda v$ is contained in Λ_R. Hence we should have

$$z_1 v_1 + z_2 v_2 + \cdots + z_t v_t - e + \lambda v = 0.$$

By this we get s linear equations

$$v_{1,1} z_1 + v_{1,2} z_2 + \cdots + v_{1,t} z_t + \lambda v_1 = 1$$

and for $2 \leq j \leq s$

$$v_{j,1} z_1 + v_{j,2} z_2 + \cdots + v_{j,t} z_t + \lambda v_j = 0$$

and any solution of this system in integers solves the DL-computation of v with base point e.

A priori this is an equation over $\mathbb{Z}$. But of course λ is only determined modulo the order of x in $(\mathbb{Z}/N)^*$. So we can compute modulo $\varphi(N)$ (or, if known, modulo the order of x).

Next it is more convenient to compute solutions of homogenous equations. This is easily achieved by changing our task: find λ, μ such that $-\lambda' v - \mu e \in \Lambda_R$.
If $\phi(N)$ is known (which we assumed) we get

$$\lambda = \lambda' \cdot \mu'$$

with μ' the inverse of μ modulo $\varphi(N)$.

We can describe the algorithm of the second step shortly in the following way:

- Choose and compute a factor base $\mathcal{F}$ with s elements.

To any relation take the attached exponential vector as $i-th$ row vector of the matrix $\mathcal{A}$ (relation matrix) till the rank of $\mathcal{A}$ is equal to s.
Add the exponential vectors of x_0 and x as additional rows to $\mathcal{A}$ to get the matric $\overline{\mathcal{A}}$.

Find a non-trivial solution of $\overline{\mathcal{A}} \cdot \underline{z} = \underline{0}$ modulo $\varphi(N)$.

1.6.4 Complexity

Again the size of $\mathcal{F}$ plays a crucial role for the complexity of the second step. For finding one relation it is good to have s large. But for finding enough relations s should be small.
Having enough relations one has to solve a system of linear equations of a large size. This would be hopeless in general. But the matrix $\mathcal{A}$ has a special shape (sparse) and so there are special methods to solve the system fast. Key words are sparse matrix techniques such as Wiedemann's or Lanczos' algorithms. The running time of this step of size $O(s^2)$.

1.6.5 RESULT

Take $N = p$ a prime.
With $B = L_{p^{-1}}\big(1/2, \sqrt{1/2}\big)$ the relation collection stage takes expected time $L_p\big(1/2; \sqrt{2}\big)$.
Solving the system of linear equations takes the same expected running time $L_p(1/2, \sqrt{2})$ because the matrix is sparse.

We get:
The expected running time for the computation of the DL in $\mathbb{F}^*$ is

$$L_p\big(1/2, \sqrt{1/2}\big).$$

1.6.6 HOPE

We hope that DL's in groups generated with the help of *carefully chosen* Elliptic Curves (or curves of genus 2) will have the same complexity as in generic groups.

Lecture 2

ELLIPTIC CURVES

2 Elliptic Curves over $\mathbb{C}$

For this section see BOOK, section 5.1.5.

2.1 Lattices and Curves

Let Λ be a lattice in $\mathbb{C}$, i.e.

$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $Im(w_2/w_1) > 0$.

The group

$$T_\Lambda = \mathbb{C}/\Lambda$$

carries in a natural way an analytic structure and is compact: it is a commutative compact Lie group, in fact it is a ***one-dimensional torus.***

It follows that there is an underlying structure of an

algebraic projective curve E_Λ

and that the meromorphic function on T_Λ form the field $F(E_\Lambda)$ of rational functions on E_Λ.

Moreover it follows at once that the (topological, analytical, algebraic) genus of E_Λ is 1.

By standard theorems (Weierstraß, Mittag-Leffler) one can construct generating functions (over $\mathbb{C}$) of $F(E_\Lambda)$.
Note that this are meromorphic functions on $\mathbb{C}$ which are periodic with respect to Λ.
One explicit example is the Weierstraß $\wp$-function

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{w^2}\right),$$

another one its derivative and there is a differential equation

$$\frac{\wp'^2}{2} = \wp^3 - 15G_4\wp - 35G_6$$

with Eisenstein series $G_4(\Lambda)$ and $G_6(\Lambda)$ with

$$G_n(\Lambda) := \sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-n}.$$

It is not difficult to see that

$$F(E_\Lambda) = \mathbb{C}(\wp, \wp').$$

Hence the map

$$\mathbb{C}/\Lambda \to \mathbb{C}^2 \cup \infty$$

$$z \mapsto (\wp(z), 1/2\wp'(z))$$

is a holomorphic bijection form the torus T_Λ to the projective *regular* plane curve

$$E_\Lambda : Y^2Z = X^3 - 15G_4XZ^2 - 35G_6Z^3.$$

There is one point $(0, 1, 0)$ "at infinity" which corresponds to $\bar{0} \in \mathbb{C}/\Lambda$, the poles of $\wp$ and $\wp'$.

It follows that the set $E_\Lambda(\mathbb{C})$ of $\mathbb{C}$-rational points on E_Λ is a Lie group and by general principles, the addition $\oplus$ is given by **algebraic** functions, i.e. by polynomials, and that the zero point is the unique point with $z = 0$.
Hence the Weierstraß functions satisfy *addition formulas.*

Conversely:
Given a projective curve

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3$$

without singularities there is a lattice Λ with $E = E_\Lambda$.

Definition 2.1 *Curves E given by equations*

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3$$

with $A, B \in \mathbb{C}$ without singularities *are called elliptic curves over $\mathbb{C}$.*

Two plane projective curves E, E' are isomorphic if there is projective invertible transformation of the projective plane mapping E to E'.

Theorem 2.2 *Two elliptic curves E and E' with lattices Λ and Λ' are isomorphic iff there is an element $\alpha \in \mathbb{C}$ with $\alpha \cdot \Lambda = \Lambda'$.*
Hence by identifying isomorphic elliptic curves we can assume that $\Lambda_E = \mathbb{Z} + \tau_E \cdot \mathbb{Z}$ with $Im(\tau_E) > 0$. τ_E is determined by E up to transformations $\tau_E \mapsto \frac{a\tau_E + b}{c\tau_E + d}$ with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.
Denote by $\mathbb{H}$ the set of complex numbers with positive imaginary part. The holomorphic function

$$j : \mathbb{H} \to \mathbb{C}$$

$$\tau_E \mapsto j(\tau_E) = 1728 \frac{A^3}{4A^3 + 27B^2}$$

is surjective and determines the isomorphy class of E uniquely.

Definition 2.3 $j_E = 1728\frac{4 \cdot A^3}{4A^3+27B^2}$ *is the absolute invariant (or: j-invariant) of E.*

Remark 2.4 *For given* $j \neq 0, 12^3$ *the elliptic curve*

$$E_j : Y^2Z = X^3 + \frac{27j}{12^3 - j}XZ^2 + \frac{27j}{12^3 - j}\mathbb{Z}^3$$

has invariant j.
To $j = 0$ *corresponds the curve* $Y^2Z = X^3 + Z^3$, *and to* $j = 12^3$ *corresponds the curve* $Y^2Z = X^3 + XZ^2$.

2.2 Isogenies and Endomorphisms

Definition 2.5 *Two elliptic curves E, E' are isogenous if there is a non-constant rational map η from E to E' mapping the point of infinity of E to the one of E'.*

Remark 2.6 *Let*

$$\eta : E \to E'$$

be an isogeny.
Then η is a group homomorphism from $E(\mathbb{C})$ to $E(\mathbb{C})$ with finite kernel.
The order of the kernel is called the degree of η.

We determine the *isogeny classes* again by using the theory of complex tori applied to elliptic curves and get:

Proposition 2.7 *Let E and E' be two elliptic curves defined over $\mathbb{C}$ with lattices Λ (respectively Λ').*

Then E is isogenous to E' iff there exists an $\alpha \in \mathbb{C}^*$ with $\alpha\Lambda \subset \Lambda'$. If so denote by η_α the isogeny from E to E'. Then the kernel of η_α is canonically isomorphic to $\alpha^{-1}\Lambda'/\Lambda$.

Corollary 2.8 *Assume that E is an elliptic curve over $\mathbb{C}$ with $j_E = j(\tau)$. Then*

$$\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_\tau \subset \Lambda_\tau\}.$$

In particular, $\mathrm{End}_{\mathbb{C}}(E)$ is a commutative integral domain.
There is a natural injection of $\mathrm{End}_{\mathbb{C}}(E)$ into $Gl_2(\mathbb{Q})$, and since $\mathrm{End}_{\mathbb{C}}(E)$ is commutative its image is of dimension ≤ 2 over $\mathbb{Q}$.

2.3 Torsion Points

The simplest isogenies are
$-id_E$ and $n \cdot id_E := [n]$,
the scalar multiplication by natural numbers n.
They generate a subring of $\mathrm{End}_{\mathbb{C}}(E)$ which is identified with $\mathbb{Z}$.
The kernel of $[n]$ is the group of n-torsion points $E[n]$.
It is isomorphic to

$$1/n\Lambda_E/\Lambda_E \cong \mathbb{Z}/n \times \mathbb{Z}/n.$$

As kernel of a morphism it is the set of zeroes of polynomials in X, Y, and it is easily shown that these polynomials have coefficients in $\mathbb{Z}$.
If n is odd an n-torsion point $\neq P_\infty$ is characterized by the fact that its X-coordinate is the zero of a polynomial $\Psi_n(X) \in \mathbb{Z}[X]$ of degree $(n^2-1)/2$.
By induction (or more elegant geometric arguments) one proves that $\Psi_n(X)$ is a separable polynomial modulo all primes p with $gcd(n,p) = 1$.

2.4 Elliptic Curves and Number Theory

We continue to assume that E is an elliptic curve over $\mathbb{C}$.

Definition 2.9 *The elliptic curve E has complex multiplication (CM) if and only if* $\mathrm{End}_{\mathbb{C}}(E)$ *is larger than* $\mathbb{Z}$.

Let E have CM and lattice

$$\Lambda_E = \mathbb{Z} + \tau\mathbb{Z}.$$

It is an easy exercise to show that τ is a *nonrational integer in an imaginary quadratic field* K_τ and $\mathrm{End}_{\mathbb{C}}(E)$ is the *order corresponding to* $\mathbb{Z} + \tau\mathbb{Z}$ in K_τ. The converse is true as well.

Proposition 2.10 *Let K be an imaginary quadratic field, let $\mathcal{O}$ be an order of K, and let A be an ideal of $\mathcal{O}$. Then $A \subset \mathbb{C}$ is a lattice, the elliptic curve $E_A := \mathbb{C}/A$ is an elliptic curve with complex multiplication and $\mathrm{End}_{\mathbb{C}}(E_A) = \mathcal{O}$. For two ideals A, A' of $\mathcal{O}$ we get: E_A is isomorphic to $E_{A'}$ over $\mathbb{C}$ (i.e. the absolute j-invariants are equal) iff A and A' are in the same ideal class.*

So elliptic curves with complex multiplication have *algebraic* periods τ.
But even more important:
the absolute invariant $j(\tau)$ is a very special algebraic integer, i.e. it is the zero of a monic polynomial over $\mathbb{Z}$, and is obtained as j-invariant of an ideal in an imaginary quadratic field.

The exact statement is the key result of class field theory of imaginary quadratic fields.

Theorem 2.11 *Assume that E is defined over $\mathbb{C}$ and has complex multiplication. Let τ be its period. Then $\mathbb{Q}(\tau)$ is an imaginary quadratic field, $\mathrm{End}_{\mathbb{Q}(\tau)}(E) = \mathrm{End}_{\mathbb{C}}(E)$ is an order $\mathcal{O}_E$ in $\mathbb{Q}(\tau)$ and the absolute invariant $j(\tau)$ is an algebraic integer that lies in the ring class field $H_{\mathcal{O}_E}$ over $\mathbb{Q}(\tau)$. The invariant $j(\tau)$ is the j-function evaluated at an ideal of $\mathcal{O}_E$.*

3 Elliptic Curves over General Fields

In the last section we began with analytic theory to define elliptic curves.
But since analytic tori of dimension 1 are compact Riemann surfaces we could use general principles to get an algebraic theory.
We use this to define elliptic curves over arbitrary (perfect) fields K with characteristic $p \geq 0$.

Definition 3.1 *An elliptic curve E defined over K is a cubic plane projective curve without singularities and with a rational point P_∞.*

Equivalently: *E is given by an equation*

$$Y^2Z + a_1XYZ + a_3YZ^2 =$$
$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$
$$\text{with } a_i \in K,$$

a Weierstraß equation, and there is no point on E for which all partial derivatives vanish..
If $p \neq 2, 3$ then one can choose the equation such that $a_1 = a_2 = a_3 = 0$.

Equivalently: *E is a projective non singular absolutely irreducible curve of genus* 1 *with K-rational point.*

Equivalently: *E is a projective curve which is isomorphic to its Jacobian variety, i.e. E is an abelian variety of dimension* 1.

Behind these equivalences is the fundamental theorem of Riemann-Roch.

3.0.1 Addition Law

A consequence of the equivalences above is that, in a natural and completely algebraic way, the set of rational points on elliptic curves E over any extension field L of K is an abelian group.
We have the following *geometric definition*:

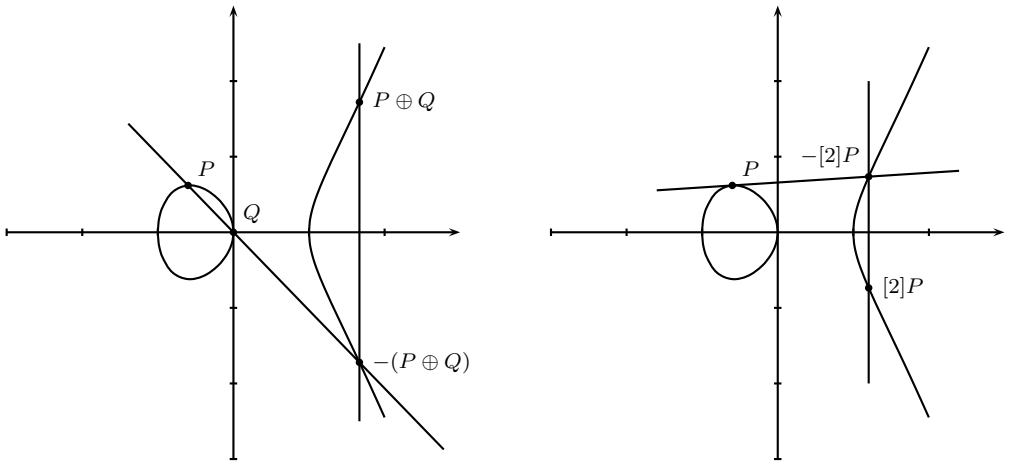
Three different points P, Q, R add up to the zero element

$$P \oplus Q \oplus R = 0$$

iff these points ar collinear.
If $P = Q$ this has to be interpreted as:
R lies on the tangent line of E in P.

If the equation for E is in Weierstraß form (with $a_1 = a_3 = 0$) we see at once that the neutral element is $P_\infty = (0, 1, 0)$ and that $-P$ is the point on E symmetric to P with respect to the X-axis.

Figure 1: Group law on elliptic curve $y^2 = f(x)$ over $\mathbb{R}$



It is easy to translate this in *algebraic formulas*:
In general we have (in affine coordinates (X, Y)

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3) \text{ with}$$
$$x_3 = -(x_1 + x_2) + (\frac{(y_1 - y_2)}{(x_1 - x_2)})^2$$

and y_3 such that $(x_3, y_3) \in E(K)$ not collinear with $(x_1, y_1), (x_2, y_2)$.

These formulas are rather easy to implement and do calculations with computers. But because of their importance for cryptography there were and are tremendous efforts to make them even faster. For details see corresponding chapters in BOOK.

3.0.2 Isogenies and Endomorphisms

Isomorphisms and Twists

For simplicity assume that the characteristic of K is prime to 6 and let E be given by a short (affine) Weierstraß equation

$$E : y^2 = x^3 + a_4x + a_6.$$

- If $a_4 = 0$ then for every $a_6' \in K^*$ the curve E is isomorphic to $E' : y^2 = x^3 + a_6'$ over $K\big((a_6/a_6')^{1/6}\big)$.
- If $a_6 = 0$ then for every $a_4' \in K^*$ the curve E is isomorphic to $E' : y^2 = x^3 + a_4'x$ over $K\big((a_4/a_4')^{1/4}\big)$.
- If $a_4a_6 \neq 0$ then for every $v \in K^*$ the curve E is isomorphic to $\widetilde{E}_v : y^2 = x^3 + a_4'x + a_6'$ with $a_4' = v^2a_4$ and $a_6' = v^3a_6$ over the field $K(\sqrt{v})$.

It is easily seen that the isomorphism class of E is, over algebraically closed fields, uniquely determined by

$$j_E = j = 12^3 \cdot 4 \frac{a_4^3}{4a_4^3 + 27a_6^2}.$$

If K is not algebraically closed j_E determines E only up to **twists**.
If $j \neq 0, 12^3$ these twists are quadratic:
The twisted curves are given by

$E^{(d)} : d \cdot y^2 = x^3 + a_4 x + a_6$ with $d \in K^*$.

Isogenies

Definition 3.2 *Two curves E/K and E'/K are isogenous over K if there exists a projective map of the plane $\mathbb{P}^2/K$ which, restricted to E, induces*

$$\psi : E \to E'$$

mapping the neutral element of E to the neutral element of E'.

Theorem 3.3 *The map ψ induces a group homomorphism from $E(K)$ to $E'(K)$.*

One important property is that for every isogeny ψ, there exists a unique isogeny $\hat{\psi} : E' \to E$, the dual isogeny of ψ, such that

$$\hat{\psi} \circ \psi = [m]_E \quad \text{and} \quad \psi \circ \hat{\psi} = [m]_{E'}.$$

The **degree of the isogeny** ψ is equal to this m.
If m is prime to $\mathrm{char}(K)$ the degree of ψ is equal to the order of $ker(\psi) = \{P \in E(\overline{K}); \psi(P) = 0\}$.
An isogeny ψ is separable, iff

$$degree(\psi) = \mid ker(\psi) \mid .$$

Endomorphisms

As usual isogenies between E and itself are called **endomorphisms.** The set of all endomorphisms of E defined over K will be denoted by $\mathrm{End}_K(E)$.
It has no zero divisors and contains $\mathbb{Z}$ in a natural way.

Definition 3.4 *If* $\mathrm{End}(E)$ *is strictly bigger than* $\mathbb{Z}$ *we say that* E *has complex multiplication (CM).*

We have seen in the previous chapter that over $\mathbb{C}$ (respectively, over fields of characteristic 0,) the ring $\mathrm{End}(E)$ is commutative, and in the case of $\mathbb{C}$, is equal to an order in an imaginary quadratic field.
This is "almost true" in characteristic $p > 0$, too.

Theorem 3.5 ***(Deuring)***
Assume that the endomorphism $[p]$ *is not totally inseparable, i.e. that* $E[p] \neq \{0\}$.
Then $\mathrm{End}_K(E)$ *is commutative and either equal to* $\mathbb{Z} \cdot id_E$ *or equal to an order in an imaginary quadratic field.*

The vague statement "almost true" is specified in the following way:
There is a polynomial $S_p(T) \in \mathbb{F}_p[T]$ such that

$$E[p] = 0 \text{ iff } S_p(j_E) = 0.$$

In this case j_E lies in $\mathbb{F}_{p^2}$.
Elliptic curves with this property are called **supersingular elliptic curves**.
If E is not supersingular we call it **ordinary**.

Since supersingular curves play only a minor role in cryptography we shall assume from now on *that E is ordinary* mostly without mentioning it .
Hence the field of endomorphisms of E,

$$End_K(E)^0 := End_K(E) \bigotimes \mathbb{Q}$$

is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$ with $d > 0$ square free.

3.0.3 Torsion Points and Tate Module

As before we denote by [n] the scalar multiplication corresponding to the endomorphism $[n] \cdot id_E$. The multiplication by n is an endomorphism of the curve E for every $n \in \mathbb{Z}$ of degree n^2.
If n is prime to p it is separable and hence as *abelian groups*

$$E[n] := ker([n]) \cong \mathbb{Z}/n \times \mathbb{Z}/n.$$

But $E[n]$ carries more structure: It is the set of common zeroes of a system of polynomials with coefficients in $\mathbb{Z}[a_4, a_6, X, Y]$.
In modern language:
$E[n]$ is a group scheme defined over K.
For $n = p^k$ one gets that the separability degree of $[p^k]$ is equal to p^k iff E is ordinary.

Take a prime $\ell \neq p$.
Multiplikation by $[l^k]$ maps $E[l^{n+k}]$ surjectively to $E[\ell^n]$ for all natural numbers k, n hence the groups $\{E[l^n]\}$ form a **projective system.**

Definition 3.6

$$T_\ell(E) := proj - lim_{n\to\infty} E[l^n]$$

is the ℓ-adic Tate module of E.

$T_\ell(E)$ is a module over the ring of ℓ-adic numbers $\mathbb{Z}_\ell$ and is isomorphic to $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$.

The Tate modules replace the lattice Λ known from the analytic theory.
In modern language: $T_\ell(E)$ is the first cohomology group of E in the étale topology.

3.0.4 ℓ-adic Representations

Here is a hint how to use the Tate modules.
Let η be an endomorphism of E.
Obviously η maps $E[l^n]$ to itself and is compatible with multiplication by l^k and so it induces a $\mathbb{Z}_\ell$ morphism

$$\tilde{\eta}_\ell : T_\ell(E) \to T_\ell(E)$$

which is injective if $\eta \neq 0$.
By elementary linear algebra one concludes that for n large enough
$\mid ker(\eta) \cap E[\ell^n] \mid$ is equal to the highest ℓ-power dividing $(det(\tilde{\eta})_\ell)$.

The morphisms $\tilde{\eta}_\ell$ depend on ℓ.
An important (and not so deep) fact is

Theorem 3.7 ***(Weil)***

- *For all primes $\ell \neq p$ the polynomials $\chi_{\eta\ell}(T)$ lie in $\mathbb{Z}[T]$ and are* ***independent*** *of ℓ.*
- *For all numbers n prime to p the characteristic polynomial of η restricted to $E[n]$ is equal to $\chi_{\eta\ell}(T)$ modulo n.*
- *Identify η with an element π in $End(E)^0$.*
  Assume that $\eta \notin \mathbb{Z}$.
  Then $\chi_{\eta\ell}(T)$ is equal to the minimal polynomial $\chi_\pi(T)$ of π.

4 Elliptic Curves over Finite Fields

We assume that the ground field K is equal to $\mathbb{F}_q$ with $q = p^k$.

4.1 The Frobenius Morphism

Let ϕ_q be the Frobenius automorphism of $\mathbb{F}_q$ defined by

$$\phi_q(x) = x^q \text{ for all } x \in \overline{\mathbb{F}_q}.$$

Let E be an elliptic curve defined over $\mathbb{F}_q$.
We assume that E is ordinary.
The **Frobenius morphism** on the projective plane is obtained by applying ϕ_q to coordinates sending points (X, Y, Z) to (X^q, Y^q, Z^q).

Let E be an elliptic curve defined over $\mathbb{F}_q$.
Then it is obvious that ϕ_q maps $E(\overline{\mathbb{F}_q})$ to $E(\overline{\mathbb{F}_q})$.
We note that this map is bijective.
but is **no isomorphism**!
It is a purely inseparable endomorphism of degree q. It follows that $\phi_q \notin \mathbb{Z}$.
Hence E has CM and its field of endomorphisms is an imaginary quadratic field $\mathbb{Q}(\sqrt{-d_E})$ and ϕ_q corresponds to an integer π_q in this field with norm q.

4.1.1 Rational Points

A trivial but crucial remark is: The elements fixed by ϕ_q in $E(\overline{\mathbb{F}}_q)$ are $E(\mathbb{F}_q)$. Hence $E(\mathbb{F}_q)$ is the kernel of $id_E - \phi_q$. Since $id_E - \phi_q$ is separabel, it follows

Theorem 4.1

$$\mid E(\mathbb{F}_q) \mid = degree(id_E - \phi_q).$$

Corollary 4.2 *Let $f(T)$ be the characteristic polynomial of $\phi_q - id_E$, interpreted as numbers in the field of endomorphisms of E.*
Then

$$\mid E(\mathbb{F}_q) \mid = f(0).$$

4.2 The Characteristic Polynomial of ϕ_q

We associate to ϕ_q the characteristic polynomial of π_q

$$\chi\pi_q(T) = T^2 - Trace(\pi_q) + q.$$

Let λ_1, λ_2 be the eigenvalues of ϕ_q (for instance interpreted by actions on Tate modules).
We can take $\lambda_1 = \pi_q$.
It follows that $\lambda_2 = q/\pi_q$ and $Trace(\lambda_1) = \lambda_1 + q/\lambda_1 = 2 \cdot Re(\pi_q)$.
Since π_q is not a rational number we must have

$$\mid (Trace(\pi_q) \mid < 2\sqrt{q}.$$

We use the Corollary 4.1.1 and the fact that $f(0) = \chi_{\pi_q}(1)$ and get

Theorem 4.3 *We have*

$$\mid E(\mathbb{F}_q) \mid = \chi_{\pi_q}(1) = q+1-Trace(\pi_q).$$

Hence

$$\mid E(\mathbb{F}_q) - q - 1 \mid \leq 2\sqrt{q}.$$

The inequality in the theorem is for elliptic curves over finite fields the analogue of the **Riemann hypothesis**. It is often called the Hasse-Weil bound.

4.2.1 Tate-Honda Theory

We saw that the Frobenius endomorphism of an elliptic curve over $\mathbb{F}_q$ can be identified with an integer π in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with the additional property that $\mid \pi \mid = \sqrt{q}$.
The theory of Tate-Honda (valid in a much more general frame) states that the converse is true, too.
Moreover, two elliptic curves over $\mathbb{F}_q$ are isogenous iff their field of endomorphisms are equal, and this is the case iff the characteristic polynomials of the Frobenius endomorphisms are equal.
Hence we get the

Theorem 4.4 ***(Tate)***
E and E' are isogenous over $\mathbb{F}_q$ iff

$$\mid E(\mathbb{F}_q) \mid = \mid E'(\mathbb{F}_q) \mid .$$

Lecture 3

DISCRETE LOGARITHM BASED on ELLIPTIC CURVES

5 Pure Math and Technique

In the second lecture I was totally in the realm of pure Mathematic
(according to Gauß: even the PUREST of Sciences: Number Theory). Is this L'art pour l'art?
At least, it seemed to be so for a long time.

An extreme opinion was expressed by Hardy.

In particular he states:

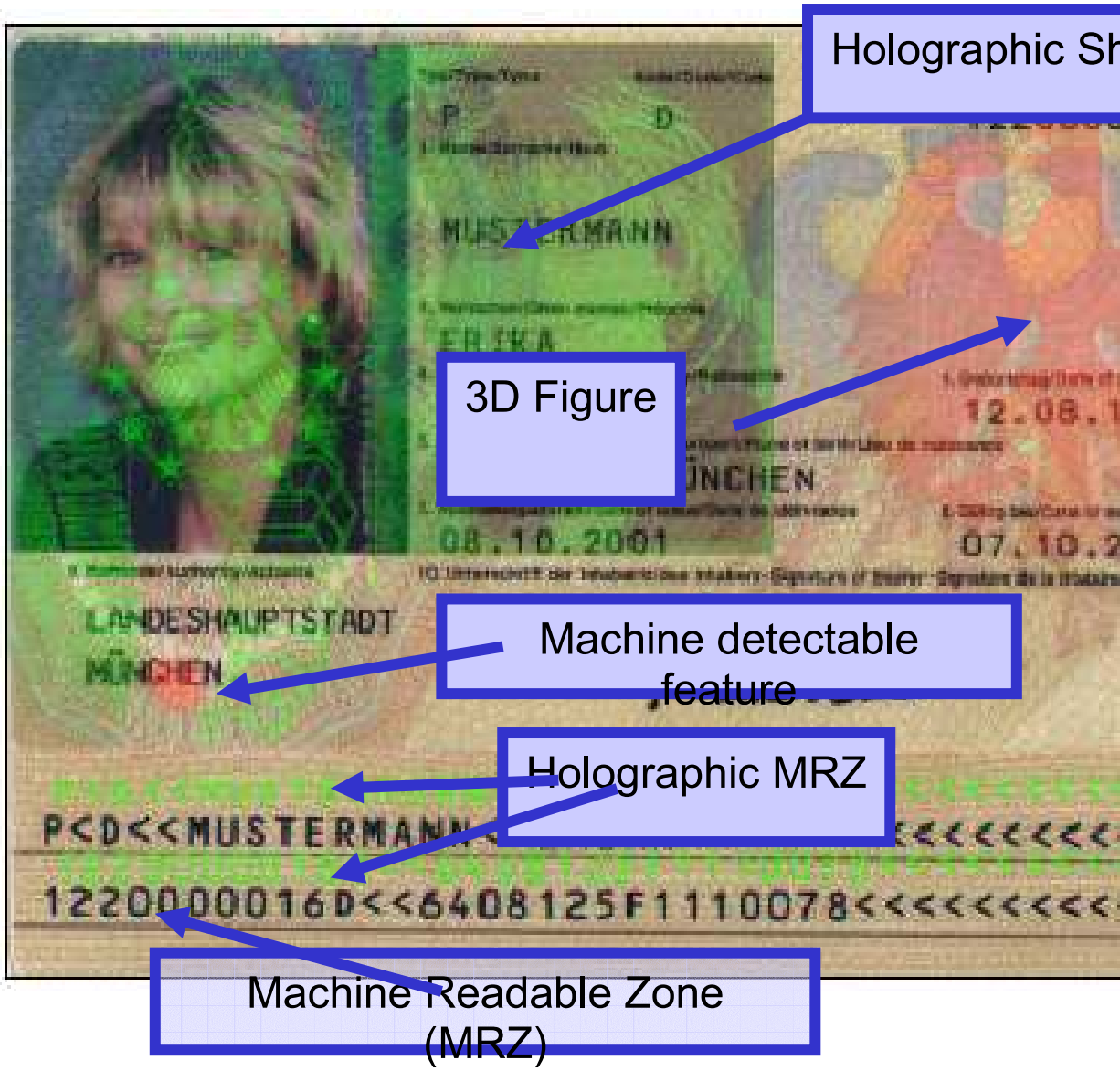
“... applied math is dull”.

But in the same book we find:

”Pure mathematics is on the whole distinctly more useful than applied. For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics.”

So let us come to **technique**

MRTDs

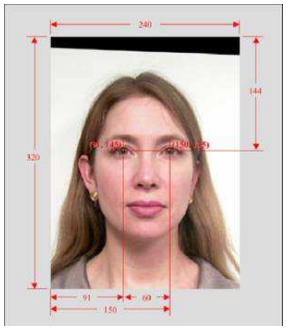


a classical machine readable passport

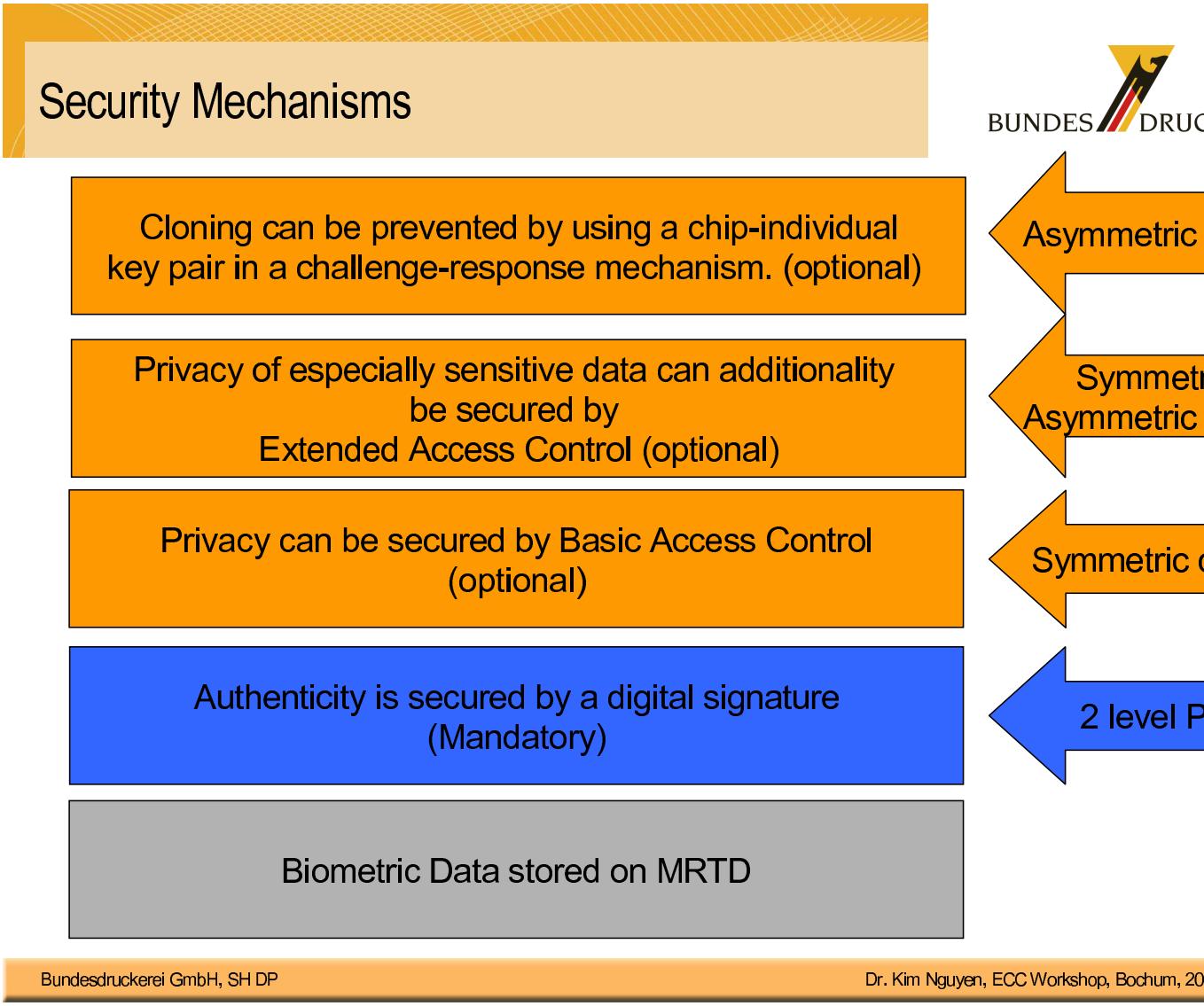
Advanced MRTDs

BUNDESDRUCKEREI

- **Machine-assisted identity confirmation (i.e. biometrics)**
  - Displayed identity features (portrait, signature, fingerprint)
  - Encoded identity features (face, signature, fingerprints, hand voice, eyes)



add: electronic signature



necessary: a whole bunch of security tools

6 Generation of Instances

We want to use the group of rational points

$$E(\mathbb{F}_q)$$

of elliptic curves E over finite fields $\mathbb{F}_q$ for DL-systems.
Hence a first task is to find $(\mathbb{F}_q, E)$ such that

$\mid E(\mathbb{F}_q) \mid = h \cdot \ell$ with $\ell \sim 10^{80}$ prime, h small .

6.1 Strategy

We know by the Hasse-Weil bound that $q \sim 10^{80}$.
So we choose q randomly of this size and then E randomly.
By counting points we decide whether we have found a good pair.
For this strategy we have to estimate the chance for success *and* to be able to count points on elliptic curves rapidly.
It is useful to divide the strategy in two subcases.

1. We fix q and look for random curves over $\mathbb{F}_q$ (maybe we have a favorite field), or
2. we fix E (e.g. over $\mathbb{Q}$ and vary q (maybe we have a favorite elliptic curve).

6.2 Density Theorems

For both strategies we have theoretical results which tell us that we shall succeed with high probability after relatively few trials (but it may happen that we shall need about 100 trials).
Look at the first strategy and assume for simplicity that $p = q$ (which is the most important case anyway.)
By Deuring , Hasse-Weil and Honda we know that for every integer t in the interval

$$I_q = [-2\sqrt{q}, 2\sqrt{q}]$$

of length $4\sqrt{q}$ there is an isogeny class of elliptic curves E with

$$\mid E(\mathbb{F}_q) \mid = q + 1 - t.$$

Now the prime number theorem tells us that (asymptotically) there are

$$\sim \frac{4\sqrt{q}}{loqq}$$

prime numbers amongst these possible orders, and (together with a known probability distribution of numbers in isogeny classes) this gives the desired probabilistic success rate.

The success rate for the second strategy is given by theorems/conjectures of Lang-Trotter type which predict the distribution of traces of Frobenius elements for elliptic curves over number fields.

6.3 The CM Method

We describe a method to find "good" elliptic curves for many prime fields $\mathbb{F}_p$ by using CM theory.
Historically this was the first method to produce elliptic curves with known order, it was used by Morain et al. for factoring numbers, and it was implemented by A. Spallek 1992 in a Diploma thesis (Essen) suitable for cryptography. It is very fast and is till today, in prticular if one wants to find series of elliptic curves.
The strategy is of the second type.
But we choose the ring of endomorphism and hence a whole isogeny class instead of choosing an equation for the elliptic curve.

Take d as square free natural number and O as ring of integers in $\mathbb{Q}(\sqrt{-d})$.
d should be not too large ($\sim 10^6$) such that the class number is not too big ($\sim 10^3$).
In a pre computation we compute a set of representatives $\{A_i\}$ of the ideal class group of O.
We have to make another pre computation.
We compute an approximation (over $\mathbb{C}$) of the polynomial

$$H_d(X) = \prod_{A_i} (X - j(A_i)).$$

We know from CM theory that this polynomial has integer coefficients, and if our approximation is good enough we can determine $H_d(X)$ exactly. (This is the most delicate part of the algorithm.)

We are looking for primes p with $p \sim 10^{80}$ which split in O into two principal prime ideals.
Let π be a generator of one of these prime ideals.
Then π is a Weil number and we know that it is the Frobenius endomorphism of an elliptic curve E over $\mathbb{F}_p$ (use class field theory for this) with

$$d_p = \mid E(\mathbb{F}_q) \mid = p + 1 - (\pi + \bar{\pi}.$$

We test easily whether d_p is (almost) a prime.
If not, we look at another p.

If yes, we compute by Berlekamp's algorithm a zero j_p of $H_d(X)$ modulo p. This needs $O(deg(H_d)logp)$ time.)
(By class field theory we know that all zeroes of H_d modulo p lie in F_p.) Now take

$$E_p : Y^2Z = X^3 + \frac{j_p}{12^3 - j_p}XZ^2 + \frac{j_p}{12^3 - j_p}Z^3,$$

choose a random point $P_0 \in E_p(\mathbb{F}_p)$ and test whether

$$d_p \cdot P_0 = 0.$$

If the answer is yes then E_p is the looked-for curve.
If the answer is no a twist of E_p does the job.

6.4 Schoof's Algorithm

The first algorithm which computed for random q and for random E the order of $E(\mathbb{F}_q)$ in polynomial time is due to René Schoof.
Remember: Let $L_E(T)$ be the characteristic polynomial of the Frobenius endomorphism of E.
It is a polynomial with integral coefficients which simultaneously for all natural numbers n is the characteristic polynomial of ϕ_q acting on torsion points of order n of E. Since the absolute value of its coefficients are bounded by q it is determined by this action for small n.

This is the starting point of Schoof's algorithm. To carry it through one has to describe the points of order n by the division polynomials,e.g. $\psi_n(X)$ which is of degree $O(n^2)$.
It is made effective by a well known fact: There is a linear recurrency between the n-division polynomials of elliptic curves.

Theorem 6.1 (Schoof)
For elliptic curves E the complexity to compute $L_E(T)$ is bounded by a polynomial function in $\log(q)$.

6.4.1 The Atkin-Elkies Variant

In this original version the algorithm is much to slow for practical use. The reason is the high degree of $\psi_n(X)$. things have become much better by observations and refinements due to **Atkin** and **Elkies**:
Instead of using the kernel of the multiplication by small n on elliptic curves E one can use the kernel of endomorphisms of small norm and determine $L_E(T)$ modulo ideals in the endomorphism ring O_E of E.
This is especially easy if the prime l splits in O_E.

For the actual computation one has to find convenient methods to describe isogenies of elliptic curves.
Here enter the *modular curves* $X_0(l)$. These curves parametrize pairs of elliptic curves with cyclic isogenies of degree l. Their rich theory is the key to many of the important results in arithmetic geometry (e.g. FLT).
We get the following refinement of Schoof' theorem.

Proposition 6.2 *Let ϵ be a positive real number.*
Let E be an elliptic curve over $\mathbb{F}$ and l a prime which is split in O_E.
Then $L_E(T)$ modulo l can be computed with probabilistic complexity $O((\log(l)^2 \cdot \log(q))^{1+\epsilon})$.

The estimates due to Hasse-Weil imply that $O(\log(q))$ different primes l are sufficient.
To use Proposition 6.2 we want to use split primes only and so we need bounds which ensure that we have found enough of them.
We observe that q is a non-trivial norm with respect to $O_E/\mathbb{Z}$ and so the size of the discriminant of R_E is bounded by $O(\mid q \mid)$.
This implies conjecturally (and in practice) that it is enough to use primes l up to a bound of size $O(\log(q))$.

Under the assumption of the Generalised Riemann Hypothesis (GRH) it can be proved that the bound $O((\log(q))^2)$ (with explicitly computable constants) is big enough.
So we get

Theorem 6.3 *Assume that GRH is true. Let ϵ be a positive real number. Let E be an elliptic curve defined over $\mathbb{F}$.*
The order of $E(\mathbb{F})$ can be computed with (probabilistic) complexity $O((\log(q))^\delta)$ with $\delta \leq 5 + \epsilon$ and conjecturally $\delta \leq 4 + \epsilon$.

6.5 $\mathfrak{p}$-adic Methods

This is maybe the theoretically most interesting family of algorithms to compute the characteristic polynomial of the Frobenius endomorphism over a field $\mathbb{F}_q$, and it is definitely the fastest one as long as p is small. But because of lack of time I have to be very sketchy and ask the interested audience to look for for mor information in the BOOK where these algorithms
are discussed in great detail.

The principle is the following.
We have the Frobenius operation over finite fields in two variants.
First we have the Frobenius automorphism from Galois theory.
It is very easy both theoretically and algorithmically to lift this automorphism to a Galois automorphism in the absolute Galois group of a $\mathfrak{p}$-adic field K with residue field $\mathbb{F}_q$.
Secondly, we have the Frobenius endomorphism ϕ_q as element of $End(E)$ for any elliptic curve E defined over $\mathbb{F}_q$. If we lift E to an elliptic curve defined over K we cannot expect that there is a lift of ϕ_q to the endomorphism ring of the lifted curve. In fact, we have to expect that the lifted curve has no CM. This excludes in general that we can use $\mathfrak{p}$-adic approximation to compute $L_E(T)$.

6.5.1 Satoh's Method

We now assume that E is ordinary.
Then by Deuring's theorem there is a very special lift with the same ring of endomorphism as E: this is the canonical lift.
Using Newton iteration applied to the modular curve $X_0(p)$ **Satoh** showed how to compute this canonical lift $\mathfrak{p}$-adically.
He gets the result:

Theorem 6.4 ***(Satoh)***
There exists a deterministic algorithm to compute the number of points on an elliptic curve E over a finite field $\mathbb{F}_q$ with $q = p^k$ and $j(E) \notin \mathbb{F}_{p^2}$, which requires $O(k^{2\mu+1})$ bit-operations and $O(k^3)$ space for fixed p. Here μ is the cost of the multiplication in $\mathbb{F}_q$.

6.5.2 The AGM-method

This method is, in its original variant, due to Mestre. It works for the most important case $p = 2$ (and for $p = 3$) and is the fastest algorithm for these ground fields. It is a variant of Satoh's method. Classically, the Arithmetic-Geometric-Mean (AGM) was introduced by Lagrange and Gauß to compute elliptic integrals or equivalently the period matrix of an elliptic curve over $\mathbb{C}$.

Mestre showed how a 2-adic version of the AGM can be used to count the number of points on an ordinary elliptic curve over a finite field of characteristic 2. The reason is that it is used to describe an isogeny of degree 2 and hence in the ordinary case the Frobenius. Later, Mestre reinterpreted this algorithm as a special case of Riemann's duplication formula for theta functions and generalized it to ordinary hyperelliptic curves.
The complexity of Algorithm is $O(k^{2\mu+1})$ bit-operations. The space complexity is $O(d^2)$.

6.5.3 Kedlaya' Method

This is maybe the most interesting and universal method.
The difficulty of lifing the Frobenius endomorphism is solved by using a formal lifting (i.e. using power series instead of polynomials) of E and than uses the (now easy) description of the Frobenius as power series operation. The characteristic polynomial of ϕ_q is obtained by the operation on the de Rham cohomology of the corresponding power series ring.
This idea goes back to Dwork.

To get finite dimensional cohomology groups one has to use overconvergent power series, the so-called "dagger lift". This and the development of the corresponding cohomology theory including a Lefschetz fixed point formula is due to Monsky-Washnitzer.
The method is very easily implemented in spite of its complicated mathematical background, and it is applicable for nearly all varieties over finite fields.

6.5.4 Optimalzation

In the end and mixing all methods together one gets an asymptotically optimal elliptic curve point counting algorithm that runs in time $O(k^{2\mu}logk)$ and requires $O(k^2)$ space, for p fixed and with μ the cost of multiplication in $\mathbb{F}_q$.

6.6 Conclusion

Using the results from above and taking into account the predictions on the structure of $E(\mathbb{F}_q)$ we can find very rapidly many cryptographically good **random** elliptic curves in a range which is sufficient for cryptography. So it is worthwhile to discuss security.

7 Security

The good news is: There is no algorithm known which computes **directly** inside of $E(\mathbb{F}_q)$ the discrete logarithm faster than the generic algorithms.
In particular, there is no Index-Calculus algorithm known which works with lifting points to number fields.
There is a mathematical reason for this: The theorem of Mordell-Weil and the existence of the Néron-Tate pairing.

BUT
there are in special situations transfers to other groups which are vulnerable.

7.1 Index-Calculus in Jacobian Varieties of Positive Dimension

By work of Adleman, Huang, Gaudry, Enge.... we have a classical result: Index Calculus yields a subexponential algorithm for the computation of the DL in class groups of curves of large genus. More important for us is a result of C. Diem, P. Gaudry, N. Thériault, E. Thom
:

Theorem
There exists a (probabilistic) algorithm which computes the DL in the divisor class group of curves of genus g , up to a log factor, in expected time of $\tilde{O}(q^{(2-2/g)})$.

This rules out $g = 4$ and $g = 3$ is in danger.

But things are worse.
By using a different approach for the choice of factor bases Diem could show that the **degree** d of a plane curve representation is another crucial, too.

Theorem (**Diem**)
Fix $d \geq 4$ such that d or $d-1$ is prime. Then the DLP in the degree 0 class groups of curves given by (reflexive) plane models of degree d can be solved in an expected time of $\tilde{O}(q^{2-\frac{2}{d-2}})$.

We can take $d = 4$ (**non-hyperelliptic curves of genus** 3) to get a bound for the complexity of DLP by $\tilde{O}(q)$.

For many hyperelliptic curves there is a correspondence to a non-hyperelliptic curve of genus 3 which can be computed efficiently.
Hence (many of the) curves of genus 3 are insecure.
Why are these results important for elliptic curves?

7.2 Weil Descent

Assume that the used base field is $\mathbb{F}_q$ with $q = p^d$.
By restricting scalars we find an abelian variety W_E defined over $\mathbb{F}_p$ given in an explicit way of dimension d with

$$W(\mathbb{F}_p) = E(\mathbb{F}_q).$$

Hence the DL in $\mathbb{F}_q$ is equivalent with the DL in $W_E(\mathbb{F}_p)$, and it may happen that we can apply index-calculus as above to W_E!
I suggested to study this situation in a talk at ECC 1998.
This turned out to be rather fruitful.
There is work of Galbraith, Hess and Smart, of Diem, Gaudry,....

For instance we know that the very nice field $\mathbb{F}_{2^{155}}$ is not the best choice as base field for secure Elliptic curves, since

$$155 = 5 \cdot (32 - 1).$$

But the real strength of the method is again in low dimension.
As one result we shall see that 4 is a bad degree,too.

Diem's and Gaudry's Results

Theorem 7.1 *Fix $n > 2$.*
Then the DLP in $E(\mathbb{F}_{q^n})$ can be solved in an expected time of $\tilde{O}(q^{2-2/n})$ (with q growing).
In particular, for $n = 4$ the complexity of the DLP is $\tilde{O}(q)$.

Use as factor base points "with X-coordinate in $\mathbb{F}_q$". More precisely one uses subvarieties defined by Semaev's summation polynomials. As smoothness test one has to solve systems of polynomial equations defining zero dimensional schemes. This is a very nice piece of computational arithmetic geometry.
So we should use elliptic curves either over prime fields or over fields $\mathbb{F}_{2^n}$ with n a prime but not Mersenne.

7.3 Bilinear Structures

Definition 7.2 *Assume that there are $\mathbb{Z}$-modules B and C and a bilinear map*

$$Q : A \times B \to C$$

with

i) *the group composition laws in A, B and C as well as the map Q are fast (e.g. in polynomial time).*

ii) *$Q(.,.)$ is non-degenerate in the first variable. Hence, for random $b \in B$ we have $Q(a_1, b) = Q(a_2, b)$ iff $a_1 = a_2$.*

We call (A, Q) a DL-system with bilinear structure.

7.3.1 Applications of Bilinear Structures

There are destructive aspects which may weaken DL-systems if they carry a bilinear structure.
Here is one.

> The DL-system $(A, \circ)$ is at most as secure as the discrete logarithm in $(C, \circ)$.

And there are constructive aspects, for instance

> Tripartite Key Exchange,
>
> Identity Based Protocols, and
>
> Short Signatures.

For more information the interested reader is advised to visit *Paulo Barretos Pairing Based Crypto Lounge.*

7.3.2 Tate Pairing

It is not easy to find bilinear structures. One main source are the duality theorems from number theory and geometry:
Key word is class field theory.
Here is a consequence. Let ℓ be a prime different from p.
Let $E[\ell]^{(q)} \subset E[\ell]$ be defined as ℓ-torsion points on which ϕ_q acts by scalar multiplication with q.
Let k be minimal such that $\ell \mid q^k - 1$.
Hence $\mathbb{F}_{q^k}$ is the smallest extension field of $\mathbb{F}_q$ containing an ℓ-th root of unity.
k is called the embedding degree (with respect to E and ℓ).

Theorem 7.3 *There is a non-degenerate pairing*

$$<,>_\ell : E(\mathbb{F}_q)/\ell \cdot E(\mathbb{F}_q) \times E[\ell]^{(q)} \longrightarrow \mathbb{F}^*_{q^k}/\mathbb{F}^{*\ell}_{q^k}$$

given by the the following rule:
Take $Q \in E[\ell]^{(q)}$ *and* f_Q *as function with only pole of order* ℓ *in* $\cdot P_\infty$ *and only zero in* Q *and of order* ℓ.
Take $P \in E(\mathbb{F}_q)$ *and represent the divisor class of* $P - P_\infty$ *by a divisor* D *coprime to* $Q - P_\infty$.
Then

$$< P + \ell \cdot E(\mathbb{F}_q), Q >= f_Q(D) \cdot \mathbb{F}^{*\ell}_{q^k}.$$

Remark 7.4 *This theorem is a consequence of the p-adic Tate pairing in the presentation found by Lichtenbaum. In the early 1990 H. G. Rück and myself suggested to use this pairing (which is in fact defined for divisor class groups of curves of arbitrary genus) to transfer the DL into multiplicative groups.*
Then Menezes, Okamoto and Vanstone used a related but more complicated pairing, the Weil pairing, and applied it to supersingular elliptic curves. One finds this as so-called MOV attack in the literature.

Consequence: one can transfer the DL-problem in $E(\mathbb{F}_q)[\ell]$ to the DL in in $\mathbb{F}^*_{q^k}$ provided that one can compute $f_Q(D)$ fast enough.

7.4 Computation of the Duality Pairing

The problem is that the degree of the zero- resp. pole divisor of f_Q are very large and so a direct approach to do this evaluation is not possible. The way out is given by the theory of Mumford Theta groups and was implemented by V. Miller for elliptic curves (applied to the Weil pairing). So this fast evaluation is called "Miller algorithmus" in the literature.
The principle is that the evaluation is a result of a scalar multiplication in a group, and hence adding and doubling can be applied.

CONSEQUENCE:
We can reduce the discrete logarithm in $E(\mathbb{F}_q))[\ell]$ to the discrete logarithm in $\mathbb{F}^*_{q^k}$ with the costs $O(log(\mid \mathbb{F}_{q^k} \mid)$.
In general k is very large ($\sim \ell$) and so the pairing cannot be computed.

Proposition 7.5 *If* $E[\ell](\mathbb{F}_q) \neq 0$ *then the trace of* ϕ_q *is congruent to* $q+1$ *modulo* ℓ *and the corresponding discrete logarithm in* $E(\mathbb{F}_q)$ *can be reduced to the discrete logarithm inin the field* $\mathbb{F}_{q^m}$ *where* m *is the smallest integer such that the trace of* ϕ_q^m *becomes congruent to* 2 *modulo* ℓ.

7.4.1 Dangerous Pairings

The pairing is dangerous for the security of the DL if the embedding degree k is so small that the DL in $\mathbb{F}^*_{q^k}$ has complexity $< \ell^{1/2}$.
This implies that k has to be at least ≥ 12.

Example 7.6 *Let E be a supersingular elliptic curve.*
Then $k \leq 6$, and it is ≤ 4 if $p \neq 3$, and ≤ 2 if p is prime to 6.
Hence supersingular elliptic curves provide only subexponential security.
As examples for such curves one can take $E : Y^2Z = X^3 - XZ^2$ and $p \equiv 3$ modulo 4, or $E : Y^2Z = X^3 + Z^3$ and $p \equiv 2$ modulo 3.

7.4.2 Pairing Friendly Curves

As we have mentioned there are positive aspects of bilinear structures.
So it is important to find E, q, ℓ with $k \geq 12$ and ≤ 30.
By work of Freeman, Cock, Pinch, Barreto, Nährig et al. we have now many of such curves but still the final story is not written.

8 Conclusion

We can use the most efficient machinery of Arithmetic Geometry to construct crypto systems and to analyze their security.

Concrete Examples (travelling on every new German passport)

brainpoolP224r1

p: D7C134AA264366862A18302575D1D787B
09F075797DA89F57EC8C0FF
A: 68A5E62CA9CE6C1C299803A6C1530B514
E182AD8B0042A59CAD29F43
B: 2580F63CCFE44138870713B1A92369E33E2
135D266DBB372386C400B
q: D7C134AA264366862A18302575D0F
B98D116BC4B6DDEBCA3A5A7939F

brainpoolP256r1

p:A9FB57DBA1EEA9BC3E660A909D838D726
E 3BF623D52620282013481D1F6E5377
A:7D5A0975FC2C3057EEF67530417AFFE7FB
80 55C126DC5C6CE94A4B44F330B5D9
B:26DC5C6CE94A4B44F330B5D9BBD77CB
F958416295CF7E1CE6BCCDC18FF8C07B6
q:A9FB57DBA1EEA9BC3E660A909D838D
718C397AA3B561A6F7901E0E82974856A7

So we have found an important application of Arithmetic Geometry to one of the fundamental needs of our civilization: *Data Security*.

BUT

We should not forget that nearly all of the results we use were found without the aim of direct application leading to these curves
and we should not forget the beauty of "pure" Mathematics and its inspiration!

THANK YOU!