1 Discrete Logarithms

Problem:

$$A \qquad\qquad \overrightarrow{open} \qquad\qquad B$$

$$\uparrow$$
$$C$$

$$(A, m, B) \qquad\qquad \mapsto \qquad\qquad (B, m, A)$$

The transfer of the message has to be “secure”. I.e. we want

- Authenticity and privateness by using cryptography.

We want

- exchange keys
- sign
- authenticate
- (encrypt and decrypt)

with simple protocols
clear and easy to follow implementation rules
based on secure crypto primitives
with a well understood mathematical background.
We want to realize these aims by
applying

to data security.

More precisely:
In this series of lectures we want to explain one family of public key systems which can be used (in simple protocols) for key exchange, signature and encryption by using as crypto primitives discrete logarithms.
Recall: the basic idea of
public key cryptography
is the idea of
One Way Functions and the role of MATHEMATICS is

- to construct candidates for one way functions
- to bring them in such a shape that computation is fast
- to analyze possible attacks

1.1 Key exchange

Assume that $A \subset \mathbb{N}$ is finite
and that $B \subset End_{set}(A)$. Assume that the elements of B commute:
For all a and $b_1, b_2 \in B$ we have

$$b_1(b_2(a)) = b_2(b_1(a)).$$

Then we can use

$$A, B$$

for a key exchange system in the
following way: We fix a (publicly known)
base point $P_0 \in A$.
The members of the
crypto community
Q_i choose $s_i \in B$

and publish
$p_i := s_i(P_0)$.
Then
$s_i(p_j) = s_j(p_i)$
is the shared secret of
Q_i and Q_j. The **security** depends (not only) on the complexity to find from the knowledge of randomly chosen $a \in A$ and given a_1, a_2 in $B \circ \{a\}$ **all** elements $b \in B$ with $b(a) = a_1$ modulo

$$Fix_B(a_2) = \{b \in B; b(a_2) = a_2\}.$$

The **efficiency** depends on the “size” of elements in A, B and on the complexity of evaluating $b \in B$.

1.2 Signature Scheme of El Gamal-Type

Again we assume that $B \subset End_{set}(A)$.
In addition we assume that there are three more structures:

1. $$h : \mathbb{N} \to B,$$
   a hash function

2. $$\mu : A \times A \to C$$
   a map into a set C in which equality of elements can be checked fast

3. $$\nu : B \times B \to D \subset Hom_{set}(A, C)$$

with

$$\nu(b_1, b_2)(a) = \mu(b_1(a), b_2(a)).$$

Signature:
$a \in A$ is given (or introduced as part as the public key).

P chooses b and publishes $b(a)$.
Let m be a message.
P chooses a random element $k \in B$.
P computes

$$\phi := \nu(h(m) \circ b, h(k(a)) \circ k)$$

in D.
P publishes

$$(\phi, m, k(a)).$$

Verification:
V computes

$$\mu(h(m)(b(a)), h(k(a))(k(a)))$$

and compares it with $\phi(a)$.

1.3 The most popular realization

$A \subset \mathbb{N}$ a cyclic group
of prime order p
(with composition written multiplicatively.
with a numeration:

Let $(G, \times)$ be a finite group.

Definition 1.1 *A* **numeration** (A, f) *of* G *is a bijective map*

$$f : G \to A$$

where A *is a finite subset of* $\mathbb{N}$.
A **presentation** *of an abstract finite group* G *is an embedding of* G *into a group with numeration.*

Define

$$\oplus : A \times A \to A$$

by

$$a_1 \oplus a_2 := f(f^{-1}(a_1) \times f^{-1}(a_2)).$$

Note:
We require that $\oplus$ is rapidly computable *without* the knowledge of f^{-1} and the security and the efficiency of the DL-System based on $\oplus$ will depend crucially on f.

From now on we assume that we have a numeration f of G and identify G with its presentation given by f.

Choose g_0, a generator of G.
$B = Aut_{\mathbb{Z}}(G) \cong (\mathbb{Z}/p)^*$
identified with $\{1, ..., p-1\}$
by $b(g) := g^b$.

$C = G$ and $\mu =$ multiplication in G

$\nu =$ addition of endomorphisms
$h =$ a hash function
from $\mathbb{N}$ to $\{1, ..., p-1\}$. We translate the

Signature scheme to this situation:
P chooses randomly and secretly, his **private key** $x \in \{1, ..., p-1\}$ and publishes his **public key** $Y := g_0^x$.

To sign a message m, P chooses a second random number k and computes

$$s := h(m)x + h(g_0^k)k \bmod p.$$

The signed message consists of

$$(m, g_0^k, s)$$

To check the authenticity of (P, m) one computes

$$S = g_0^s, T = Y^{h(m)}, H = g_0^{h(g_0^k)}.$$

and checks whether

$$S = T \circ H.$$

The security considerations
for the crypto primitive
boil down to the complexity of the computation of the
Discrete Logarithm:
For randomly chosen $g_1, g_2 \in G$ compute $n \in \mathbb{N}$ with

$$g_2 = g_1^n.$$

Challenge:
Construct
groups with numerations
of large prime order
such that the computation of the discrete discrete logarithm has the required complexity.

Time *or* space needed (probabilistically) for the computation of the logarithm:
polynomial in p.

Time *and* space needed to write down the elements and the group law of G and execute a group composition:
polynomial in $\log(p)$.

1.4 Generic Systems

We use the algebraic structure "group".
This allows "generic" attacks..

Shanks' Baby-Step-Giant-Step Method
(deterministic)
Take $P, Q \in G$.
Find k with $Q = k \cdot P$.
Principle:
Looking up an element in an ordered set is inexpensive.
Baby step: For $i = 0, ..., S \leq \sqrt{p}$
compute

$$(i \cdot P, i).$$

Giant step:
Compute

$$Q - i \cdot S \cdot P$$

.
Compare the two lists. If

$$i_0 \cdot P = Q - i_1 \cdot S \cdot P$$

then

$$k = i_0 + i_1 \cdot S.$$

Complexity:$O(\sqrt{p})$

Disadvantage:

- needs $O(\sqrt{p})$ space

Pollard's ρ-Algorithm(probabilistic)[1] Principle: Random walk in G closes with high probability after

$$\approx 1.03\sqrt{p}$$

steps.
Controlled random walk (simplest version) :

[1] Pollard's method is used for the "world record" w.r.t. Certicom challenge: Compute DL in an 109-bit elliptic curve.

The result x_i of the $i-$th step should depend only on x_{i-1}.
So partite G "randomly" into three sets T_j of size $\approx p/3$ and take

$$x_i = P + x_{i-1} \,\mathrm{if}\, x_{i-1} \in T_1,$$

$$x_i = Q + x_{i-1} \,\mathrm{if}\, x_{i-1} \in T_2,$$

$$x_i = 2x_{i-1} \,\mathrm{if}\, x_{i-1} \in T_3.$$

There are efficient methods to detect collisions.

Security hierarchy
We measure the complexity of a DL-system by the function

$$L_p(\alpha, c) := exp(C(logp)^{\alpha}(loglogp)^{1-\alpha})$$

with $0 \leq \alpha \leq 1$ and $c > 0$.

Best case: $\alpha = 1$:**Exponential complexity**.

Worst case: $\alpha = 0$: **Polynomial complexity**

The case between...: $0 < \alpha < 1$: The complexity is **subexponential**.

1.5 Very special examples

Example 1:
$G := \mathbb{Z}/p$.
Numeration:

$$f : G \to \{1, \cdots, p\}$$

given by

$$f(r + p\mathbb{Z}) := [r]_p$$

where $[r]_p$ is the smallest positive representative of the class of r modulo p.
The function $\oplus$ is given by

$$r_1 \oplus r_2 = [r_1 + r_2]_p$$

which is easy to compute from the knowledge of r_i.
Security?
Given: b with $b = [na]_p$.
Solve

$$b = na + kp$$

with $k \in \mathbb{Z}$.
The *Euclidean algorithm* solves this in $O(\log(p))$ operations in $\mathbb{Z}/p$:
$\alpha = 0$!
We do not get a secure Discrete Logarithm System. **Example 2:** $G = \mathbb{Z}/p$.
Choose a prime q such that p divides $q - 1$.
Choose $\zeta \neq 1$ in $\mathbb{Z}/q$ with $\zeta^p = 1$ (i.e. ζ is a primitive p-th root of unity).
Numeration:For $1 \leq i \leq p$ define
$z_i := [\zeta^i]_q$ and for $\bar{i} = i + p\mathbb{Z} \in G$

$$f(\bar{i}) := [z_i]_q.$$

Addition:
$a_i = f(x_i + p\mathbb{Z}) \in \{1, \cdots, q-1\}$

$$a_1 \oplus a_2 = [[\zeta^{x_1 + x_2}]_q.$$

Security?
For fixed a and random $b \in A$ find n in $\mathbb{N}$ with

$$b = [a^n]_q.$$

This means:
For one fixed p-th root of unity and one random p-th root of unity in the multiplicative group of $\mathbb{Z}/q$ one has to determine the exponent needed to transform the fixed root of unity into the random element.
The best known method to compute this discrete logarithm is **subexponential** in q.
It usually is compared with factorization (this is no accident). Hence its security is to be compared with RSA. **Example 3:**
A most important example:
Elliptic Curves
An elliptic curve E over a field K is a regular plane projective cubic with at

least one rational point.
For simplicity we shall assume that $\mathrm{char}(K)$ is prime to 6. Then we find an equation

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

with $A, B \in K$ and $4A^2 + 27B^2 \neq 0$.
A very special property of elliptic curves is that their points form an abelian group.

Elliptic curve with addition

This addition is easily transformed into formulas:
Given

$$P_1 = (x_1, y_1) \;, P_2 = (x_2, y_2)$$

then

$$P_3 \; = (x_3, y_3) \;\; := \;\; P_1 \; \oplus \; P_2$$

with (in general):

$$x_3 \;\; = \;\; -(x_1 + x_2) + \;\; ((y_1 - y_2)/(x_1 - x_2))^2$$

To use elliptic curves E for DL-systems we have to solve the following diophantine problem:
Find $\mathbb{F}_q$ and an elliptic curve E such that the group of $\mathbb{F}_q-$ points has (almost) prime order of size $\approx 10^{60}$.

If we succeed we have to analyze attacks **using** the structures introduced during construction.
The state of the art :
For "generic" elliptic curves over "generic" finite fields the complexity of the computation of the Discrete Logarithm in the group of rational points is exponential.

But special elliptic curves are weak.

1.6 Numeration by Algebraic Groups

We generalize and systematize the examples by using numerations by **algebraic groups** over finite fields $\mathbb{F}_q$ where q is a power of a prime l_0.

We shall give a sketch of the mathematical background.
Later on we shall explain (down to earth) what can be done in practice.

1.6.1 Algebraic Groups

An algebraic group $\mathcal{G}$ over a field K is an algebraic reduced, non-singular, noetherian scheme with an addition law, i.e. there is a morphism (in the category of schemes)

$$m\,:\,\mathcal{G}\times\mathcal{G}\rightarrow\mathcal{G},$$

an inverse, i.e. a morphism

$$i\,:\,\mathcal{G}\rightarrow\mathcal{G},$$

and a neutral element, i.e. a morphism

$$e:\mathrm{Spec}(K)\rightarrow\mathcal{G},$$

satisfying the usual group laws:

$$m\circ(id_{\mathcal{G}}\times m)=m\circ(m\times id_{\mathcal{G}})\ \text{(associativity)},$$

$$m\circ(e\times id_{\mathcal{G}})=pr_2$$

where pr_2 is the projection of $\mathrm{Spec}(K)\times\mathcal{G}$ to $\mathcal{G}$, and

$$m\circ(i\times id_{\mathcal{G}})\circ\delta=j_e$$

where δ is the diagonal map from $\mathcal{G}$ to $\mathcal{G}\times\mathcal{G}$ and j_e is the map which sends $\mathcal{G}$ to $e(\mathrm{Spec}(K))$.

Down to earth:
For all extension fields L of K the set $\mathcal{G}(L)$ (see below) is a group in which the sum and the inverse of elements are computed by

evaluating morphisms which are defined over K and in which the neutral element is the point

$$0 := e(\mathrm{Spec}(K)) \in \mathcal{G}(K).$$

Because of the Noether property of $\mathcal{G}$ it follows that it has only finitely many connected components, and it is a fact that the set of these components forms a finite group Z with $\mathcal{G}_0$ as neutral element. We see easily that the unique connected component of $\mathcal{G}$ which contains 0 is a subgroup scheme of $\mathcal{G}$ denoted by $\mathcal{G}_0$.

There are several reasons (both security and complexity are bad) for the fact that Z is of little interest for our cryptographic purposes, and so we shall assume from now on that $\mathcal{G}$ is connected.
Now choose an affine open subvariety U of $\mathcal{G}$ with coordinate functions $X_1, \cdots, X_n$. The morphism m induces a morphism

$$m_U : U \times U \to \mathcal{G}$$

and its image contains a non-empty open subset $V \subset U$. Take W as the inverse image of V in $U \times U$. Then m induces a map from W to V which can be written as:

$$m_W : W \to V$$

sending pairs of L-rational points $(x_1, \cdots, x_n) \times (y_1, \cdots, y_n)$ in W to

$$(R_1(x_1, \cdots, x_n; y_1, \cdots, y_n),$$

$$\cdots, R_n(x_1, \cdots x_n; y_1, \cdots, y_n))$$

with $R_i \in K(X_1, \cdots, X_n, Y_1, \cdots, Y_n)$. This is a birational description of the addition law which is enough for all cryptographic applications. (The set of points where this map is not defined is of small dimension and hence with high probability one will not run into it by chance.)
Application:
Take K and L as finite fields and use use a numeration of L to get a numeration of the $L-$rational points of the affine parts of $\mathcal{G}$

For the performance of the crypto system the choice of (W, m_W) is crucial; we require small n and low degree of R_i. If we can take $U = \mathcal{G}$ then $\mathcal{G}$ is an

affine group scheme.
The other important kind of group schemes are projective, i.e. they can be embedded into a projective space $\mathbb{P}^n/K$ and are closed in it.
They are called **abelian varieties**

If we restrict ourselves to connected commutative group schemes (there are good reasons for this) a structure theorem tells us that for use in cryptography we can restrict ourselves to affine schemes or abelian varieties.

1.7 Manageable Abelian Varieties

The first task to solve is to describe (birationally) abelian varieties and the addition laws in a time and space saving way.
This seems to be hopeless as long as we work with **general** abelian varieties A: The number of coordinate functions and the degree of the addition formulas both grow exponentially with the dimension of the abelian variety (cf. results of Mumford and Lange-Ruppert and so we have to use **special** abelian varieties. The first specialisation is to take A as Jacobian variety J_C of a curve C.
The big advantage is that both the coordinates and the addition can use objects defined by C since

$$(C \times \ldots \times C)/S_g \quad (g = \text{genus}(C),$$

$$S_g \,\text{the symmetric group in}\, g \,\text{letters})$$

is birationally isomorphic to J_C and the points of J_C correspond to divisor classes of degree 0 of the function field of C. We can assume that we have an $\mathbb{F}_q-$rational point P_∞ on C. The theorem of Riemann-Roch implies that we find "standard " representatives in divisor classes of the form $D - g\,P_\infty$ with D a positive $\mathbb{F}_q-$rational divisor of degree g (i.e. a formal sum of g points of C).
The addition in J_C is induced by the addition of divisors and the task is to find in the class of the sum of two divisors standard representatives either by formulas or by an algorithm involving the coordinates of the points occurring in the added divisors. So we need an effective (and very fast) version of the

Riemann-Roch theorem.

Example 1 corresponds to the additive group G_a
Example 2 to the multiplicative group G_m,
and Example 3 is a curve of genus 1 with rational point which is isomorphic to its Jacobian variety.