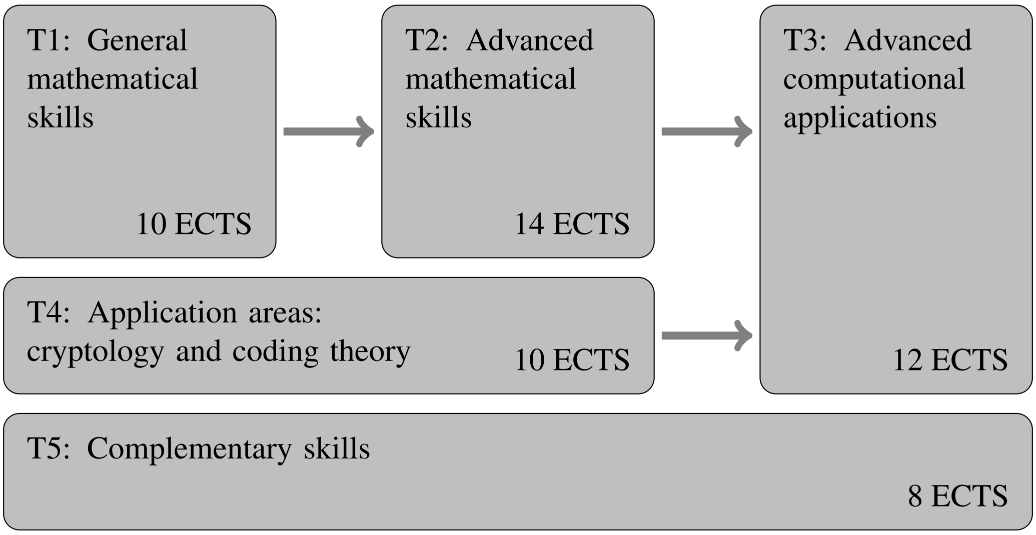
GTEM Training Program

1. Overview

The Training Program consist of five modules, which are given in Table 1. A broad description of each module is included below. In the next section the specific training instruments are specified.

Table 1: Training modules and dependencies



T1: General mathematical skills 10 ECTS

T2: Advanced mathematical skills 14 ECTS

T3: Advanced computational applications 12 ECTS

T4: Application areas: cryptology and coding theory 10 ECTS

T5: Complementary skills 8 ECTS

- Module **T1** gives the ESRs the necessary background in number theory and arithmetic geometry that is needed in all work packages. Specifically: computational algebraic number theory, function fields, lattice techniques, curves over finite fields.

- Module **T2** treats specific advanced topics in the areas of T1 which are distinct for the different work packages. Subjects here are Hurwitz spaces, p-adic cohomology, Arakelov theory, Differential Galois theory.

- Module **T3** treats specific advanced mathematical techniques that are needed for computational mastery of the objects at hand, and applications to various areas in data security and networking such as point counting techniques, constructing codes from algebraic curves and lattice cryptography.

- Module **T4** gives the ESRs the necessary knowledge of cryptology and coding theory and current hot topics of research in those areas.

- Module **T5** consists of complementary skills training: giving presentations for various kinds of audiences, research management, teaching skills, science promotion, writing grant proposals.

In Table 1 the dependency relation is also a temporal relation, so for instance, the training in T1 is offered early in the 48 month project period, while T5 runs for the entire period. This is in line with the schedule of Scientific Milestones, where the synthesis of newly developed theory and actual computational questions is projected in the second half of the network.

The modules are taught in a combination of local and network wide activities. The "training milestones" in network level activities are listed in Table 2. The details about the training modules are given in the next section.

Table 2: Training and Transfer of Knowledge schedule

Month	Event	Milestone	Responsible	Participating
9	Workshop	T4.1: Mathematics for digital content	2	1–12
9	Workshop	T2.1 : Arithmetic and differential Galois groups	10	2,5,10,8
12	Annual meeting	T1.1: Function fields T5.1: Research presentation	1	1–12
20	Workshop	T1.2: Curves and number fields	11	1–12
17	Workshop	T2.2: Constructive Galois theory	5	1–12
24	Midterm review	T1.3: Computer algebra T5.2: Mathematical graphics	3	1–12
32	Workshop	T2.3: Lattices and applications	6	1,3,4,6,9,11
32	Workshop	T2.4: Pairings in arithmetic geometry	4	2,4,7,9,10,12
33	Workshop	T3.1: Inverse Galois problems	8	2,3,5,8,10,12
36	Annual meeting	T3.2: Computational arithmetic geometry T5.3: Writing grant proposals	9	1–12
44	Workshop	T3.3: Computational Number Theory and Cryptography	7	1,2,4,7,9,10,11
48	Final conference	T5.4: Science promotion	2	1–12

2. Training list at local and network level.

The Training Program consists of the following Training Instruments which implement the training modules of Section 1.

1. A list of training elements at **Network meetings** and workshops is given in Table 2. It is further specified in the list below.

2. Participation of ESRs in **international conferences** such as Eurocrypt, Algorithmic Number Theory Symposium (ANTS), Journées Arithmétiques provide training in cryptography and state of the art computational number theory. This training will be personally supervised and reported by a senior staff member of the network. Each ESR will go to one conference for training in advanced mathematical techniques (T2.7) and one on coding theory or cryptography (T4.2).

3. **Local courses** at the partner institutes, which an ESR can also follow in secondment at another partner, are given for several of the Teaching modules. See the previous Section for specifications.

4. **Local seminars**, which an ESR can also follow in secondment at another partner, offer training of a specialized nature and stimulating interaction with local researchers in number theory and arithmetic geometry.

5. **Personal instruction** by an experienced staff member will provide training in highly specialized application techniques such as generation of special codes, Arakelov class group algorithms, differential Galois group algorithms.

6. **Local complementary skills training**, which an ESR can also follow in secondment at another partner, envolves the ESR in local science promotion projects, grant proposal writing, language training, and it familiarizes the ESR with teaching and the general academic environment.

The breakdown of these training instruments in ECTS (European Credit Transfer System) contributions to the training modules is indicated in the following table. In total, ESRs spend 30% of their time on training, which is 54 ECTS over 36 months.

Training action	T1	T2	T3	T4	T5	Total
Network gatherings	6	2	3	2	2	15
International conferences		2		2		4
Local courses	4	6		6		16
Local seminars		4	4			8
Personal supervision			5			5
Local complementary training					6	6
Total	10	14	12	10	8	54

Training list for the training modules

Training module T1: general mathematical skills

	Description/plan	Instrument	ECTS
T1.1	Function fields. *Plan:* review basic results as Riemann Roch, Riemann hypothesis and stress the analogy with number fields	Workshop	2
T1.2	Curves and number fields. *Plan:* review algorithmic theory of number fields in analogy with curves	Workshop	2
T1.3	Computer algebra. *Plan:* review modern techniques needed all Work Packages	Workshop	2
T1.4	Computational number theory. *Plan:* review essential results such as linear algebra over the integers (lattice reduction) and quadratic forms	Local course	4

Training module T2: advanced mathematical skills

	Description/plan	Instrument	ECTS
T2.1	Arithmetic and differential Galois groups. *Plan:* review state of the art	Workshop	2
T2.2	Constructive Galois theory. *Plan:* review traditional techniques, and modern methods	Workshop	2
T2.3	Lattices and applications. *Plan:* review reduction theory and techniques from the geometry of numbers, and prepare for applications in coding theory	Workshop	2
T2.4	Pairings in arithmetic geometry. *Plan:* review cohomological pairings as needed in Work Package D	Workshop	2
T2.5	Specialized local courses catering to specific task needs	Local course	6
T2.6	Specialized local seminars	Local seminar	4
T2.7	Advanced techniques training at International conference (see point 2 of Section 2.2).	Conference	2

Training module T3: advanced computational techniques

	Description/plan	Instrument	ECTS
T3.1	Inverse Galois problems. *Plan:* review techniques applying Hurwitz spaces.	Workshop	2
T3.2	Computational arithmetic geometry. *Plan:* treat general and special purpose computational techniques for curves over finite fields, and over number fields	Workshop	2
T3.3	Computational number theory and cryptography. *Plan:* review state of the art, particularly of p-adic methods.	Workshop	2
T3.4	Advanced computational applications	Local seminar	4
T3.5	Personal instruction on explicit methods in specific task setting	Personal	6

Training module T4: cryptography and coding theory

	Description/plan	Instrument	ECTS
T4.1	Mathematics for digital content	Workshop	2
T4.2	Cryptography or coding theory training at International conference (see point 2 of Section 2.2).	Conference	2
T4.3	Overview course on cryptography or coding theory to gain acquaintance with existing techinques in the prospective application areas of the project	Local course	6

Training module T5: complementary skills

	Description/plan	Instrument	ECTS
T5.1	Research presentation	Meeting	2/3
T5.2	Mathematical graphics	Meeting	2/3
T5.3	Grant proposal writing	Meeting	2/3
T5.4	Science promotion	Meeting	2/3
T5.5	Local complementary skills training	Local	6

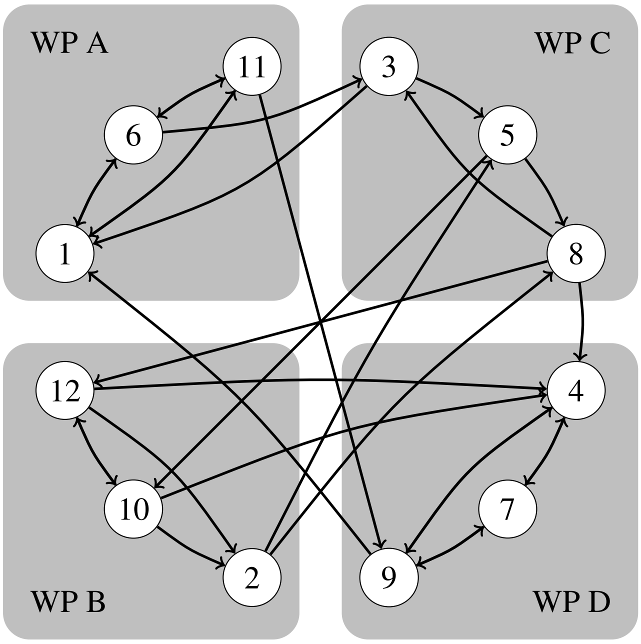
3. Multidisciplinary/intersectoral knowledge

All ESRs will spend an estimated total of 25% of their time in secondment at other nodes and at short term research internships at our industrial associates. The preliminary plan of secondments at partners is illustrated in Table 3, where the partners are grouped by their primary work package.

While the research objectives are phrased within pure mathematics, the focus is on topics with proven or expected industrial potential. The network will establish collaborations with companies to evaluate the industrial relevance of research output, identify industry needs, and organise short-term research internships of ESRs of the network. There is no specific program yet of the planned short term research internships in industry, since the relation between the network and the industry associates is still at an early stage. Contacts will be expanded in the course of the project. Present contacts include Axalto, France; Crypto AG, Switzerland; Cryptomathic, Denmark; Cryptovision, Germany; EDI-ZONE GmbH, Electronic Business Communications and Security, Germany; Elta, Israel; Gemplus, France; Telecom France; IBM Research, Switzerland; Philips Research, Netherlands; Siemens AG, Germany.

Table 3: Indicative schedule of secondments

From	To (Year)
1	6 (2), 11 (3)
2	5 (1), 8 (2)
3	1 (1), 5 (2)
4	9 (1), 7 (3)
5	8 (2), 10 (4)
6	11 (3), 1 (2), 3 (4)
7	9 (1), 4 (3)
8	12 (2), 3 (3), 4 (4)
9	4 (1), 7 (3), 1 (4)
10	4 (1), 12 (3), 2 (4)
11	1 (2), 6 (4), 9 (4)
12	2 (2), 4 (3), 10 (3)



4. Integration of young researchers

All ESRs will be informed of their contractual rights and obligations, and their possibilities to participate in and contribute to all network activities, as well as local institute activities.

For each ESR in the network a personalised career development plan will be developed to provide them with a balanced set of skills and advanced knowledge at the research front of mathematics. The plan will contain the following components:

- a concise description of planned research and educational objectives, including training for complementary skills, together with a time chart;
- an overview of the courses to be taken and examined, quantified by ECTS credit points;
- planning of at least two presentations per year by the student, at least one of which will be given at an international meeting;
- planning of secondments to other partners and a short-term research internship in industry.

The plan will be drawn up by the ESR and the local supervisor in consultation with the WP Coordinator at the start of employment, and submitted to the management team. It will be updated annually.

All ESRs will have ample opportunity to interact with other network members though network events, secondments, and other short visits to other nodes, for lectures, and short consultation.