



FNR Awards 2011
Scientific Publications &
Promotion of Scientific Culture

 Fonds National de la
Recherche Luxembourg

FNR Award for Outstanding Scientific Publications 2011

Alex Biryukov & Dmitry Khovratovich
Related-Key Cryptanalysis of the Full AES-192 and AES-256
ASIACRYPT 2009, LNCS 5912, pp. 1-18, 2009

Related-key Cryptanalysis of Advanced Encryption Standard

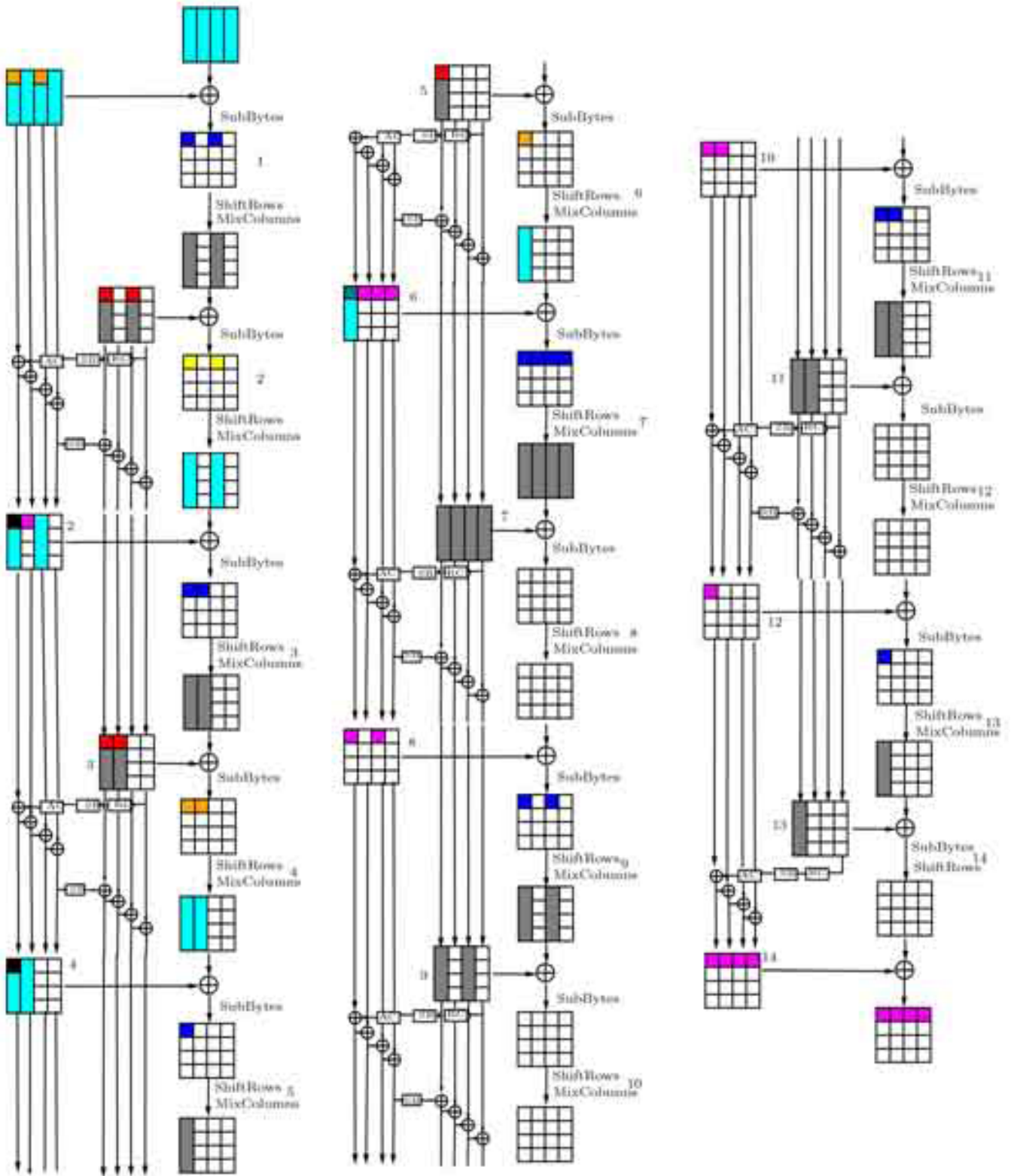
The Advanced Encryption Standard (AES) is one of the most popular and important ciphers in the world. We all seamlessly use it when we do internet shopping, e-banking or use our wireless networks. This standard was designed in 1998 by two Belgian researchers and became a winner of a three year-long competition in which 15 international teams participated. In 2001 it became a US NIST and world-wide standard for encryption suitable for protecting classified information of SECRET and TOP SECRET levels.

In the ten years since its design AES has been intensively studied by the cryptographic community, with more than hundred papers written on the subject, however no dent was found in the security of AES. An attack on the full version of AES has been one of the greatest challenges in cryptography and cryptanalysis.

In this paper we present the first attack on AES that recovers its secret key much faster than an exhaustive search. We show that under certain conditions on a pair of keys (related keys) both are vulnerable to a specific version of a so-called boomerang attack. The weakness that we were able to identify invalidates security claims made by the designers of AES regarding the secret key mixing part (called key-schedule) of the cipher. While still being impractical in terms of resources and effort required by attacker, our analysis puts a serious question on the long-term security of this worldwide standard.

The following picture (with colors representing the differences in the algorithm execution) illustrates the predictable propagation of the key relation that we have chosen.

Techniques that we developed in our study of AES have been quickly put to use by other research teams for the analysis of old and the design of new, more secure cryptographic primitives.



FNR Award for Outstanding Scientific Publications 2011

Adrien Oth

Oth, A., Böse, M., Wenzel, F., Köhler, N., and Erdik, M. (2010). Evaluation and optimization of seismic networks and algorithms for earthquake early warning – the case of Istanbul (Turkey). *Journal of Geophysical Research* 115, B10311, doi: 10.1029/2010JB007447.

Earthquakes pose a serious threat to many highly populated areas in the world. Indeed, megacities such as Tokyo, Istanbul or Los Angeles are located close to major fault systems, and many of these enormous agglomerations are expected to be hit by a significant earthquake of magnitude 7 or larger within the decades to come. Recent earthquake occurrences around the world (e.g., Haiti, Japan, New Zealand) clearly demonstrate the disastrous consequences that many of these megacities have to face if such an event occurs in their immediate vicinity.

For these regions, the rigorous implementation of seismic risk mitigation measures is therefore a top priority. Among such measures, the implementation of an earthquake early warning (EEW) system represents an important component. EEW systems are real-time information systems destined to detect as soon as possible whether a potentially hazardous earthquake has occurred and to provide fast warnings of the impending strong ground shaking. This is made possible by the fact that seismic waves travel much slower (on the order of several km/s) than electromagnetic waves that are used in modern communication systems to transmit information. Thus, if the occurrence of an earthquake is detected by the EEW system, the information can be processed and transmitted before the damaging seismic waves arrive at a given location, for instance a large metropolitan area.

The available warning times range from as little as a few seconds to as much as a minute or longer, depending on the distance between the site of interest and the causative fault. Even though such warning times may appear to be very short, EEW systems hold the potential to significantly reduce the death toll and mitigate economic losses during an earthquake. Their warnings may provide people with sufficient time to take protective measures and allow for the launching of automated procedures to mitigate the secondary effects caused by strong ground shaking.

However, the usefulness of EEW systems strongly depends on their ability to provide at the same time fast and reliable warnings, and several major difficulties are encountered when developing or implementing such a system:

- It is necessary to evaluate how the intended system will perform under operational conditions. Many regions threatened by the potential occurrence of a large earthquake in the future lack recordings of comparable past events due to the long recurrence times of such earthquakes. As a consequence, it is impossible to assess the performance of an EEW system in a systematic way (i.e., taking into account all possibly relevant scenarios) by using recorded data from past earthquakes alone.
- Most EEW systems are based on existing seismic networks that have not originally been deployed for this purpose. As a result, it may be necessary to rearrange the existing network or supplement it with several new sensors in order to guarantee an acceptable performance and optimally use the available resources.
- Each EEW methodology involves automated rules to decide if a warning shall be issued or not. These rules need a certain number of system parameters that have to be set appropriately. In order to solve these problems, the usage of simulated scenario earthquakes and the development of a rigorous evaluation and optimization scheme to assess and improve the performance of EEW systems is an indispensable necessity.

Efficient EEW aiming at both fast and accurate warnings thus requires an optimally designed seismic network and the best set of algorithm parameters. Optimum network design is not straightforward since it strongly depends on the seismotectonic setting of the region of interest, funding availability and other constraints. These requirements might also differ for different EEW algorithms.

While significant advances have been made in understanding the general feasibility and limitations of EEW algorithms and communication technology, little attention has been paid to optimization so far. We therefore developed a novel approach for evaluating and optimizing seismic networks for EEW, in particular in regions with a scarce number of instrumentally recorded earthquakes, and demonstrate the potential of this method with a case study of the situation of the megacity Istanbul. Located only about 15 km north of the North Anatolian fault beneath the Sea of Marmara and with a population exceeding 12 million inhabitants, its seismic risk is considerable.

As a first step of the methodology, we consider what scenario earthquakes need to be included in the analysis. Synthetic seismograms are then simulated for these scenarios with state-of-the-art modeling techniques throughout the entire region of interest. Using these seismograms, we evaluate the performance of the current EEW system for Istanbul, which is composed of 10 stations distributed along the northern shoreline of the Sea of Marmara. As benchmarks for the current system's performance, we consider a large variety of situations, such as the completely new design of an EEW system with different numbers of sensors, the supplementation of the current system with additional sensors, as well as the usage of ocean bottom seismometers.

The results of these analyses provide unprecedented insights into the performance and optimization potential of an EEW system. They clearly show that the sensor locations of the current Istanbul EEW system are rather well chosen, but that the system parameters need revision to reduce the risk of false alarms. Furthermore, contrary to first expectations, adding further seismic sensors to the network does not lead to any significant performance increase within the given seismotectonic setting considered, except if ocean bottom seismometers were to be deployed in the Sea of Marmara.

Full reference:

Oth, A., Böse, M., Wenzel, F., Köhler, N., and Erdik, M. (2010). Evaluation and optimization of seismic networks and algorithms for earthquake early warning – the case of Istanbul (Turkey). *Journal of Geophysical Research* 115, B10311, doi: 10.1029/2010JB007447.

Contact for further information: adrien.oth@ecgs.lu

Pascal Daman & Janine Goedert The Lycée de Garçons Project: Michael Frayn's 'Copenhagen' on Stage Lycée de Garçons Luxembourg

RESEARCH HIGHLIGHT ACCOMPANYING MEASURES AM1

COPENHAGEN COMES TO LUXEMBOURG

In April 2010, a group of students from the Limpertsberg-based *Lycée de Garçons Luxembourg* (LGL) performed a truly physical prelude to *Copenhagen*, a play on show in the *Théâtre National du Luxembourg*. The piece was the finale of a 4-month project combining art, languages and science, involving teachers and students from the LGL as well as theatre professionals, and financed chiefly through the FNR's AM1 grant for the promotion of scientific culture.

In the summer of 1922, two of the world's greatest physicists meet for the first time at a conference in Göttingen. Two years later, they join academic forces: Werner Heisenberg, then 22, travels to Copenhagen to commence work in Niels Bohr's Institute of Theoretical Physics. Over the following 15 years the two men will revolutionise atomic physics. Their close friendship comes to an abrupt end in 1941, after an enigmatic visit that the German Heisenberg pays Bohr, the Dane with Jewish ancestors, in Copenhagen.

Even today, nobody knows for sure what the two men said to each other on that September night in Copenhagen – except that the main topic was nuclear weaponry. As Heisenberg wrote to the journalist Robert Jungk in 1956: "This talk probably started with my question as to whether or not it was right for physicists to devote themselves in wartime to the uranium problem – as there was the possibility that progress in this sphere could lead to grave consequences in the technique of war." Michael Frayn's play *Copenhagen* tries to elucidate possible courses of this conversation and attempts to answer why Heisenberg ever came to Copenhagen in order to discuss nuclear physics with someone in an occupied country – surely a risky endeavour.

But why choose this play for a school project? Four years ago, Pascal Daman, physics teacher at the LGL, found himself frustrated by the obvious disregard his science students showed for languages and the theatre. He decided to make them read a play. His choice, *Copenhagen*, was to pose a double challenge – complicated physics and advanced English wrapped up in two acts; to be read in their English class and scientifically explained in physics. Two years later, the initial *Copenhagen* project got revived into the *LanGues déLiées*, an internal school project (*Projet d'établissement*) dedicated chiefly to languages, but also their relationship with arts, sciences and communication. Why not actually stage a production of the play and get the students involved directly in as many aspects as possible?

The FNR grant, as well as support from the *Projet d'établissement* and BGL-BNP-Paribas, covered all the financial aspects. Anne Simon from the TNL provided both a location and theatrical support to the students (and incidentally directed the main play, *Copenhagen*). Students from three classes were involved, two of them with a scientific vocation (2^e B and C, Mathematics and natural sciences), one with a focus on arts (2^e E). "In January 2010, the students would read the play in their English class and work on the physical principles behind Heisenberg's and Bohr's science," Daman explains. This is where the play really comes into its own as a means of promoting scientific culture. Although *Copenhagen* itself is based on a specific event in the life of two scientists, rather than their science *per se*, a certain understanding of the physics leading to the creation of nuclear bombs seems essential - or at least desirable - for a thorough understanding of the play.

Obviously, such knowledge should not be restricted to the participating students, but instead be conveyed to the theatre audience. As such, the initial project idea was to build up a physics exhibition, to use the intervals for further explanations and to leave the stage entirely to the professionals. Reactions were then mixed amongst the students, when informed that plans had changed and they were to create a short prelude to the play, in which they themselves were to enact the necessary physical background knowledge.



In a series of humorous sketches the students presented Bohr's theory of the quantum atom, ionisation, Young's demonstration of light waves and Einstein's interpretation of light as a particle. They visualised the paradox of Schrödinger's cat and ultimately showed how Hahn, Strassmann, Meitner and Frisch's work on nuclear fission lead to the discovery of the nuclear chain reaction. It was this work that in due course led to the arms race between Germany and the Allies to develop the first atom bomb - the crux of the *Copenhagen* play set in the middle of World War II.

The sketches – a clever and funny way to make physics more palpable to the general public – were devised by one of several student groups in the course of a project week and enacted by nearly everyone. Other groups took care of condensing the original 3-hour long play into a shorter version, whereas still others were responsible for the content of the play's programme. Meanwhile, the arts students met with stage and costume designers and created various models for the stage set. Overall, the *Copenhagen* project has certainly provided the students with many new experiences and proved to be a great success with the audience as well: in the course of seven representations for school classes and two for the general public roughly 800 people came to see the play.

When asked what he sees as the project's biggest success, Daman will not pick out a single event: "All of it – the entire experience. The fact that it was so multi-faceted, that so many people were involved, that the students got an inside view of the world of theatre, that we could combine language and science..."

Copenhagen was certainly not the last project that the teachers and students of the LGL have laid their hands on. The current school project, *LGL en FRVScience*, aims to promote and elucidate scientific culture. For example, students reaching the age of 16 need to choose the academic direction they want to pursue. "Yet at that time," Daman explains, "they do not really know enough about science, and many get scared off. The students should be shown where science could lead them." For this reason, a programme initiated by the FNR, *Chercheurs à l'école*, giving students the opportunity to talk to scientists first hand, has been continued independently within FRVScience.

Another project, again with the financial support of the FNR's AM1 programme, will see a host of students visiting scientific workshops and exhibitions in the *Cité des Sciences* in Paris. Furthermore – not unlike *Copenhagen* did with the theatre snobbing scientists – FRVScience aims, once more, to breach the gap between languages and sciences. In a monumental three-year project language and economics students are compiling a *Scientific Guide to the Cities of Europe*. First international contacts in (amongst others) Edinburgh, Berlin and Leipzig have been established, and a special highlight awaits one of the students in the near future: an interview with Hans-Peter Dürr, a world-renowned physicist and – incidentally – an old friend of Heisenberg's.

FNR Award for the Outstanding Promotion of Scientific Culture 2011

David Degouis & Virginie Schmitt Semaine de la Science 2010 Ecole Privée Notre-Dame (Sainte-Sophie)

Présentation de la semaine de la science

L'Ecole Privée Notre-Dame (Sainte-Sophie) a organisé du 14 au 18 juin 2010 une « semaine de la science » durant laquelle tous ses élèves de la Petite Section de Maternelle à la dernière année du lycée ont participé à des activités à caractère scientifique (ateliers, « conférences » expérimentales, spectacles, exposition, exposés, voyage éducatif).

Les 170 enfants de l'école élémentaire française (du CP au CM2) n'ont pas eu de cours normaux durant la semaine du 14 au 18 juin 2010.

Pour les autres élèves de l'école (Maternelle française, primaire luxembourgeois, Ecole Secondaire et Secondaire Technique) ainsi que pour les élèves d'une école invitée (EFL), il s'agissait d'une participation moins intensive mais importante.

Tous les ateliers ont été animés soit par nos professeurs des écoles ou professeurs de sciences soit par des partenaires invités. Au programme étaient notamment prévus des ateliers expérimentaux, des conférences expérimentales, des ateliers de démonstration, des spectacles scientifiques, une exposition, un voyage éducatif...

Les thèmes abordés furent divers et variés :

- Électricité et magnétisme, champ magnétique terrestre
- Optique et lumière
- Ecologie, tri des déchets
- Eau et la mer
- Azote liquide
- Pression et vide
- Médecine et hygiène
- Biologie animale et végétale
- Astronomie et l'aéronautique
- Les 5 sens
- Chimie
- Mathématiques et informatique

Financement

L'organisation d'un tel événement a engendré des frais importants. Nous avons introduit avec succès une demande de subvention auprès du Fonds National de la Recherche qui a pris ainsi en charge une partie des frais.

Les Amis de Sainte-Sophie ont également apporté leur contribution.

Une contribution symbolique a été demandée aux parents des élèves des écoles primaires et maternelles.

Le solde restant dû était à la charge de l'Ecole.

Partenaires

Différents intervenants extérieurs ont accepté de nous suivre dans ce projet :

- Ligue Médico-Sociale (L)
- CIACANE via Félix Ferrauto (F)
- Observatoire de Meuse (F)
- SuperDrecksKëscht (L)
- ALUSEAU (L)
- Les électrons libres ASBL (L)
- Planètemômes (B)
- M. Michel Bultingaire (F) et Air Liquide (L)
- Mekruphy GMBH (D) pour le matériel scientifique
- Atelier Sorcier ASBL (B)
- Euro Space Center de Redu (B)

Description des ateliers

Ateliers expérimentaux durant lesquels les élèves ont manipulé eux-mêmes ou ont fabriqué des objets à caractère scientifique :

- Récolte et observation d'insectes (encadrée par un professeur de biologie)
- Expériences de chimie (encadrées par un professeur de chimie)
- Lumière et fabrication d'un kaléidoscope, d'une chambre noire, d'un jet lumineux (encadrés par des instituteurs)
- Approche ludique et expérimentale des cinq sens (encadrée par deux institutrices)
- Ateliers relatifs à la santé et l'hygiène (encadrés par la Ligue Médico-Sociale)
- Fabrication d'une fusée à eau (encadrée par un instituteur)
- Electricité (encadré par une institutrice)

Démonstrations expérimentales sur l'azote liquide et la pression et le vide (encadré par un invité extérieur, spécialiste du domaine)

Ateliers relatifs à la gestion de l'eau, des déchets (présence d'un bus avec ateliers et d'un camion avec ateliers)

Ateliers relatifs à l'astronomie animés par la CIACANE (regroupement d'astronomes amateurs français) et par l'Observatoire de Meuse avec entre autres l'observation du soleil en pleine journée.

Exposition sur l'orientation et le champ magnétique terrestre (fournie par l'ASBL « Atelier Sorcier » de Belgique)

Spectacles ou conférences ludico-scientifiques pour tous à partir de 3 ans jusque 19 ans animés par « Planètemômes » et par « Les électrons libres ».

Excursion d'un jour à l'Euro Space Center de Redu (Belgique) pour 57 élèves qui ont participé toute la journée à l'entraînement d'un spationaute en s'essayant à des engins d'entraînement.

La semaine de la science en quelques chiffres

430 créneaux horaires consacrés aux Sciences durant 5 jours à Sainte-Sophie !

800 élèves concernés

20 intervenants extérieurs à l'école

1 conférence d'intérêt général

8 professeurs du lycée engagés dans des ateliers

7 professeurs des écoles engagés dans des ateliers

9 spectacles

2 enseignants engagés dans des ateliers

27 ateliers

1 informaticien

1 excursion scientifique

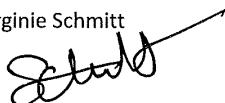
3 éducatrices

1 exposition

2 coordinateurs

Les coordinateurs :

Virginie Schmitt



David Degouis



FNR Award for the Outstanding Promotion of Scientific Culture 2011

Workshop “Experimental Cosmetics” & Science Café “Wissenschaft in der Werbung” Anne-Marie Ternes, Danièle Moes & Monika Dieterle Centre de Recherche Public de la Santé (CRP-Santé)

“Coming together is a beginning, staying together is progress, and working together is success.” Henry Ford

Having taken part in CRP-Santé’s workshops at the FNR Researchers’ Night 2008 and Science Festival 2009, three collaborators of CRP-Santé, namely Anne-Marie Ternes from the Laboratory of Retrovirology, as well as Monika Dieterle and Danièle Moes (both from the Laboratory of Plant Molecular Biology) agreed to organize their own workshop for Researchers’ Night 2010. Finally, due to the effort to satisfy the divergent ideas of a bioinformatician (A.M. Ternes) and of two plant molecular biologists (M. Dieterle and D. Moes), two proposals were submitted.

The proposals’ concept:

In the past the three researchers experienced that the public’s knowledge of plants is astonishingly restricted, as people are often unable to relate/assign vegetarian food to the respective plant organ (e.g. the apple to a fruit of a tree, the Brussel’s sprout to a cabbage’s flower bud, the rocket to a plant’s leaf or the carrot to a plant’s root). Thus, they decided to organize a workshop aimed at awakening public interest in plants that grow within spitting distance. Therefore, the focus of attention lied on the features and usage of local medicinal plants and linked this traditional view of plants to today’s research and, in this context, (furthermore) to an ongoing research project in our laboratory at CRP-Santé, which aims at isolating anti-cancer compounds from plants.

The second proposal concerning the organization of a science café was born in a discussion about the increasing number of advertisements claiming scientifically proven benefits for various products (e.g. dairy products, cosmetics, baby food...). The idea arose that it might be of general interest to choose few advertising spots and to examine the scientific evidence stated in order to increase people’s awareness to the (mis) use of scientific claims in advertisements.

The prompt acceptance of both projects posed a sizeable challenge, because both animation concepts had to be worked out from scratch. As all three workshop organizers are employees of an institution with research mission, they consider the promotion of scientific culture in public in large part as spare-time work. But finally, both workshop and Science Café were achieved by the intensive multi-disciplinary collaboration between researchers, PhD students, technical staff and administrators from different departments and competence centers of CRP-Santé (e.g. Laboratory of Retrovirology, Laboratory of Plant Molecular Biology, Laboratory of Immunogenetics and Allergology, Center for Health Studies, Microarray Center), as well as by the creative input and expertise of professional outsiders (e.g. Mr Paul Lesch, a history teacher from Athénée de Luxembourg or M. Yves Stephany, a radio presenter at “Radio 100,7”). With the great financial and technical assistance of FNR, all collaborators formed a remarkable team and set up a well-attended workshop and a stimulating Science Café which, at Researchers’ Night 2010, that both met with the public’s approval, as reflected by the large number of visitors.

Detailed description of the activity:

Researchers' Night 2010

Workshop "Experimental Cosmetics - Use of local medicinal herbs"

24.09.2010 , 14.00-21.00 h, Place Guillaume II

"Das Äussere einer Pflanze ist nur die Hälfte ihrer Wirklichkeit."

Johann Wolfgang von Goethe

Our workshop aimed at acquainting the participants with domestic plants and, especially, with their alleviating and curative effects. By focusing on the habitat of our "local" medicinal plants, we emphasized the fact that a considerable number of beneficial herbs are growing within spitting distance. For more than twenty exemplary species, we provided information about their prominent features (see attached profile of chamomile, common St.-John's-wort and milfoil) and a side-mounted poster gave tips and tricks about herb collection and use (see poster WS14.1). Additionally field guides were shown to teach people how to identify plants.

In discussions with the animators of the workshop and with the help/aid of several posters a link was drawn between "old-fashioned" usage of medicinal herbs and the role of plant-derived pharmaceuticals in "modern" medicine. Two posters illustrated the development of plant derived pharmaceuticals. A first poster featured the history of Aspirin (poster WS14.2). A second one focused on Taxol, as one of several plant derived anti-cancer drugs (and 14.3). A poster about novel bioactive components from Chinese medicinal plants allowed people to see behind the curtain of one CRP-Santé's current research projects (poster 14.4).

To directly apply the acquired knowledge, people mixed their own take-away salve or ointment based on our home-made ethanol and oil extracts from chamomile and thyme, as well as from freshly pressed cucumber juice (see photos and lotion recipes). This practical part of our workshop found great approval, as both children and adults patiently queued at the three workstations equipped with laboratory tools and glass ware to finally prepare their own take-away lotion.

Moreover, together with the other workshops held by CRP-Santé we organized a quiz with very specific questions, which motivated people to have a closer look at the posters on display and the distributed flyers. Among the prizes were herbal teas and field guides for medicinal herbs.

Science Café: "Gene mit Sosse – Wissenschaft in der Werbung

24.09.2010 , 18:00 h , Art Café

"Advertising may be described as the science of arresting the human intelligence long enough to get money from it"

Stephen Butler Leacock, quoted in Michael Jackman, Crown's Book of Political Quotations, 1982

"Scientific" claims are often used in publicities to increase the legitimacy and creditability of products. The aim of the Science Café was to awaken healthy skeptics towards science in any forms of advertising. To stimulate a discussion with the public, we had composed a short movie sequence composed of popular TV spots and magazine advertisements (see DVD). Ways and means of the introduced advertisements covered the accentuation of "white coats" (e.g. Dr. Best), the extensive usage of pseudo-scientific word compositions (e. g. "Collagen-Biosphären", "Struktur-Ceramide") and the presentation of reliable to unserious or incomprehensible studies and trials. We challenged the scientific facts given in the ads and unraveled the source of the data (e.g. "resveratrol extends lifespan by 70 %", which was actually shown in budding yeast only). After this twenty-minute presentation radio presenter Yves Stephany chaired the lively discussion with the audience.



CORE

research = excellence + priority



ATTRACT

research = opportunity + challenge



PEARL

research = flexibility + synergies



INTER

research = mobility + collaboration



AFR

research = training + perspective



AM

research = support + promotion



PSC

research = communication + promotion

