11th Workshop on Cryptographic Hardware and Embedded Systems

Lausanne
OLYMPIC CAPITAL

CHES 2009

September 6 -9

Switzerland

Guide Book

© LT/Régis Colombo - www.diapo.ch

Gold sponsors

Cryptography Research
DPA Countermeasure
Licensing Program

NAGRAVISION
KUDELSKI GROUP

Sponsors

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Oberthur Technologies

Riscure

SASEBO

RCIS Research Center for Information Security

TELECOM ParisTech

Design and edition: Marcelo E. Kaihara © EPFL IC IIF LACAL http://lacal.epfl.ch

Index

Switzerland

Introduction

Switzerland

TERRITORY AND POPULATION

With an area of 41'285 km^2, Switzerland is a relatively small country. The Jura mountains, the Swiss Plateau and the Alps are the three basic topographical areas. Switzerland has a population of 7,4 millions of inhabitants and an average density of 183 people per km^2. The population is, however, unequally distributed on the territory: only 10% of its population lives in the alpine area.

HISTORY AND CONSTITUTION

Switzerland is a federation of relatively autonomous cantons, some of which have a history of confederacy that goes back more than 700 years. Switzerland's 1848 Constitution made it into a federal state, giving it a central authority that counterbalanced the power of the individual cantons. Some issues, such as foreign policy, are now solely in the hands of the central government.
For historical reasons, Switzerland's official name is still the ≪Helvetic Confederation≫ (in Latin: *Confoederatio Helvetica*) from which the country's international abbreviation, CH, is derived.
The word Helvetic refers to the Helvetians, one of the many Celtic tribes living at the time of the Roman conquest in what has now become Switzerland.
The country is divided into 26 cantons. There are German-speaking and French-speaking cantons, one Italian-speaking canton and cantons in which both German and French are spoken. One canton (Graubunden) has three official languages: German, Italian and Rumantsch . Their population and size vary greatly. The canton of Geneva is virtually made up of only one city. Some other cantons, like Uri, consist almost entirely of mountains and valleys.
Each canton has its own constitution, its government, its parliament, its courts and its laws, though they must, of course, be compatible with those of the Confederation. The cantons enjoy a great deal of administrative autonomy and freedom of decision-making. They have independent control over their education system and social services, level of taxation and even have a separate police force.

LAKE GENEVA REGION

They came, saw, and stayed. Courbet, Kokoschka, Charlie Chaplin, David Bowie and Jorge Luis Borges are among the many who settled at Lake Geneva, attracted, no doubt, by the Alpine panorama and almost-Mediterranean vegetation. Gently sloping vineyards border the shores of the lake, with the capital city of Lausanne across from the highest Alpine peaks. Lively towns and small wine-growing villages appear scattered at random.
The region seems like half a dream and half reality. Though the people in the farm villages who work the wheat fields on the plain above the lake, the inhabitants of the medieval towns and the original inhabitants of the castles have always had both feet firmly on the ground.

For further information: http://www.myswitzerland.com/en.cfm/home

Lausanne at a glance

A STAY IN LAUSANNE

What most impresses a visitor from the world outside upon arriving in Lausanne is undoubtedly the unexpected possibility of finding all the facilities, services, institutions, schools and entertainments of a major metropolis in such a small city of only 127'000 inhabitants. Moreover, it is situated between a lake and the mountains, between forests and vineyards and all this only 65km away from Geneva-Cointrin International Airport and about 4 hours away from Paris or Milan by TGV. It is also close to many top excursion destinations such as Montreux and Chillon Castle, Zermatt and the Matterhorn, the Jungfrau and Lucerne, the historical hamlet of Gruyeres, the Diablerets Glacier, the Vaud Alps and the famous French resort of Chamonix.

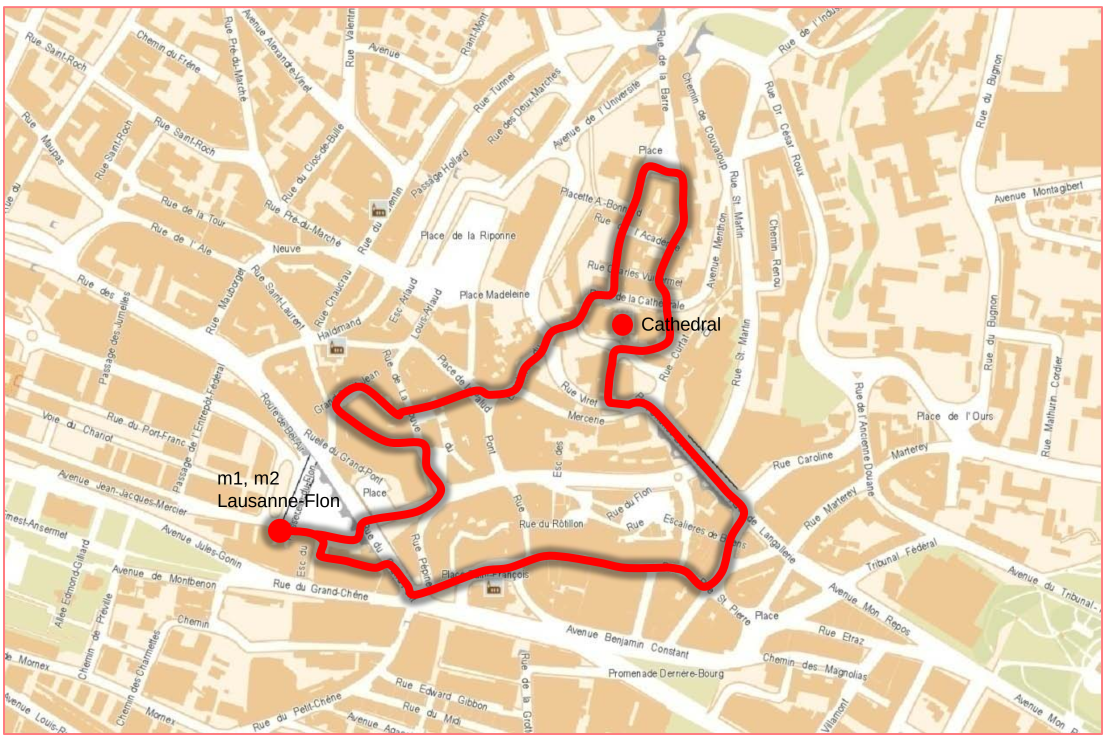
Lausanne offers all the advantages of a big city - 5000 hotel beds in all categories, the services of a top-rank tertiary capital (banks, insurance companies, international companies), a vast choice of shops and stores that make it a true shopping paradise. The city is permeated with big restaurants and small friendly cafes, a university, a polytechnic, advanced vocational colleges, a unique choice of private schools, an opera, theatres, about twenty museums, clubs, and many establishments for the young. Furthermore, there are many programs of culture, sports and recreational events for those who are not in the "go have a rest" mood.

Lausanne, as the Olympic capital city, has the IOC Headquarters and its institutions, about 15 international sports federations and especially the famous Olympic Museum: a unique attraction in the world. Indeed, there are many sports events such as Athletissima - one of the biggest meetings in the world, the Lausanne Marathon that ranks among the greatest, and very regular world championships, and cycling stages. .

Further tourist information:
http://www.lausanne-tourisme.ch
http://www.lake-geneva-region.ch/

DISCOVER THE OLD TOWN

Even if you have little time for sightseeing, do not forget to visit the Cité, the old medieval town of Lausanne. Below is a proposition for a 1.9km walk mainly through the pedestrian streets of the old town. A detailed map can be found at:
http://maps.google.ch/maps/ms?hl=en&gl=ch&ie=UTF8&msa=0&msid=111562524912530863738.000465f88304580629a00&ll=46.521733,6.634326&spn=0.005426,0.016512&z=17



© Ville de Lausanne, © Etat de Vaud, © swisstopo, © Cartosphere

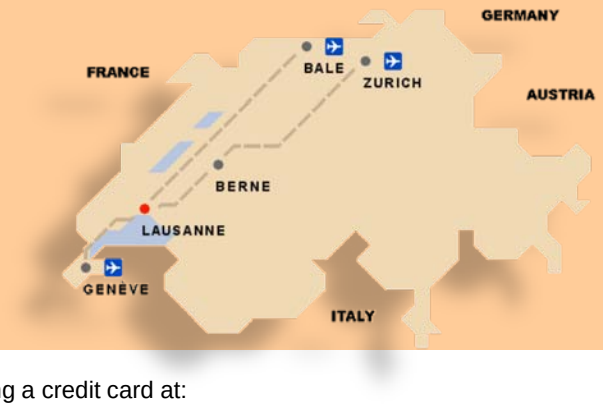
Access to Lausanne

ACCESS BY TRAIN

Lausanne railroad station is a hub of The Swiss National Railway system and offers very convenient and efficient links to : Bern, The Federal Capital, in 1h00 / Brussels, in 6h30 / Paris by TGV, in 3h40 / Milan by Cisalpino, in 2h30 / Frankfurt by ICE, in 5h45.

From Geneva to Lausanne (~ 45')
From Geneva Airport train station, take the ≪InterCity (IC)≫ or ≪InterRegio (IR)≫ train for Lausanne station.There are 4 trains per hour.

From Zurich to Lausanne (~ 2h30)
From Zurich Airport train station, take the ≪InterCity (IC)≫ or ≪InterCityPendular (ICN)≫ train for Lausanne station. There are 2 trains per hour.



The train tickets within Switzerland can be purchased on-line using a credit card at:
http://www.sbb.ch/en/
You need to bring a printed pdf of the tickets (valid only with an accompanying form of identity, e.g. a passport). You have the option to include the ticket for city transportation.
You can alternatively buy a ticket in one of the vending machines once you arrive to Lausanne.
Types of ticket:

a) For a maximum of three stops, the ticket costs 1.90 CHF (valid for 30min.)
b) For 1 zone (zone 11) is valid for 1h and costs CHF 2.60.
c) For 2 zones (zone 11 + 12) is valid for 1h and the ticket costs CHF 3.00.

The map of the zones can be found at:
http://www.mobilis-vaud.ch/images/plan/Zoom_lausanne-08-V.pdf

Once you arrive to the hotel in Lausanne, you will get the Lausanne Transport Card at the reception desk. This card will give you access to free rides in public transportation in the greater Lausanne area. This card is personal and non-transferable. (Not applicable to hotel L'Union)

For more information about the train, metro and bus schedules, please visit: http://www.sbb.ch/en/

ACCESS BY CAR

From Geneva to Lausanne (~ 30')
Take the A1 motorway for Lausanne. Drive close by Nyon, then Morges.

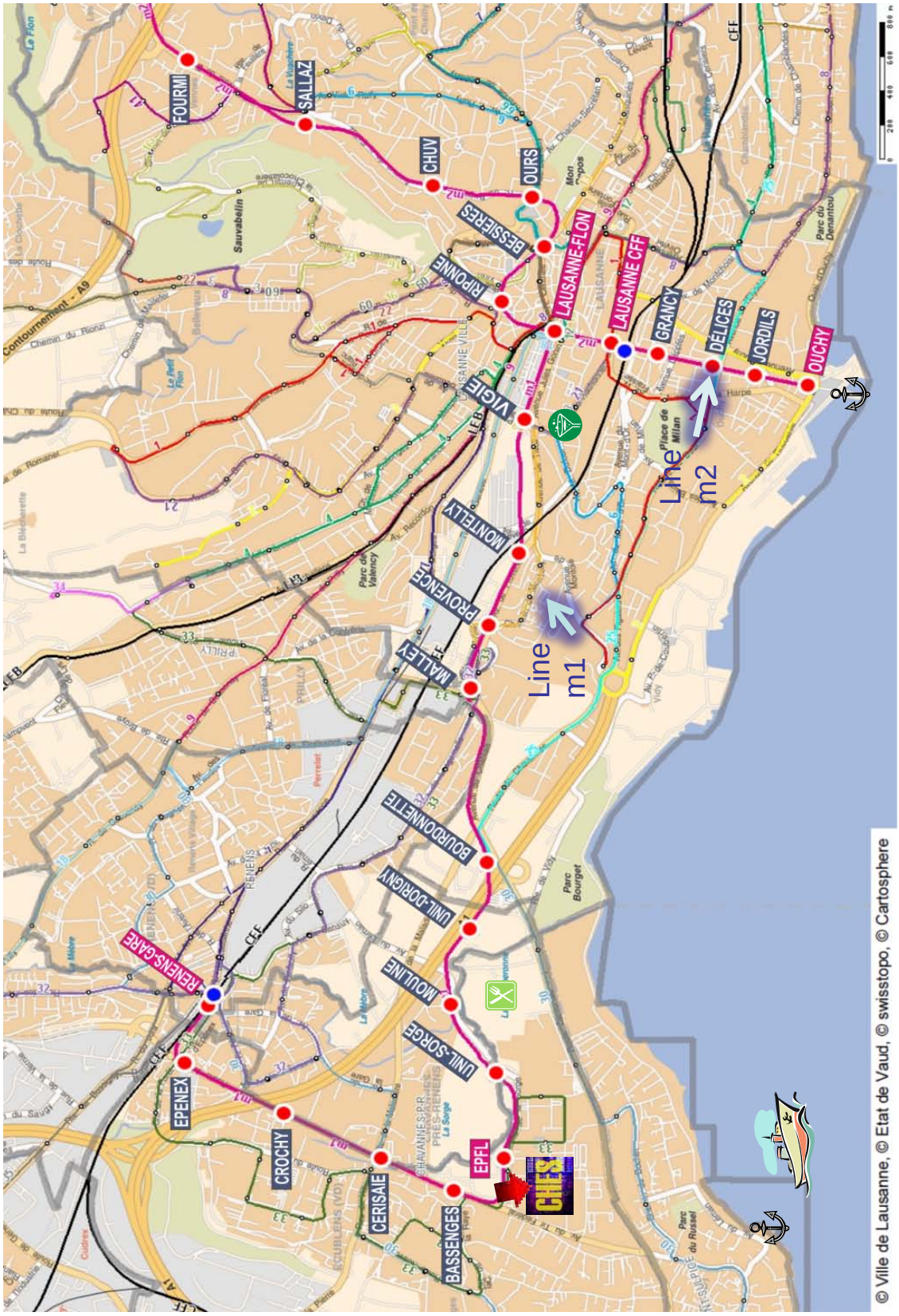
From Zurich to Lausanne (~ 2h15')
Catch up with the A1 motorway for Bern, then Lausanne. Drive close by Dietikon, Olten, Bern, Yverdon-les-Bains.

Then follow: **Lausanne – Sud**

And take the exit : **St-Sulpice Ecublens**

UNIL-EPFL

Access to CHES 2009



http://maps.google.ch/maps/ms?hl=en&gl=ch&ie=UTF8&msa=0&msid=111562524912530863738.000465f88304580629a00&ll=46.521681,6.634262&spn=0.008933,0.017445&z=16

Access to CHES 2009

PUBLIC TRANSPORTATION

In front of the Lausanne main train station, you will find the subway station «Lausanne Gare» of the m2 line. Take this line bound for «Croisettes» and get off at «Lausanne-Flon», the next station. From «Lausanne-Flon», take the subway m1 for «Renens Gare» and get off at the « EPFL» station.
Departure from Lausanne-Flon: every 7 - 10 minutes
Duration from Lausanne-Flon: 12 - 13 minutes
The conference main area is in the SG building about 100 meter south west of the EPFL stop. Follow the CHES 2009 road signs.

Taxi drive from Lausanne main train station or Lausanne-Flon station to the conference (EPFL) will cost around CHF25.00 one way, depending on traffic.
The phone number for taxi reservation is 0800 810 810 (toll free).

An abstract of the subway timetable is printed for your convenience on the right. You can find the complete online timetable on a dynamic basis using this Internet service:

http://fahrplan.sbb.ch/bin/query.exe/en?from=Lausanne-Flon%20(TL)&To=Ecublens%20VD,%20EPFL

You can use the same site to find timetable from your hotel, entering the proper addresses.

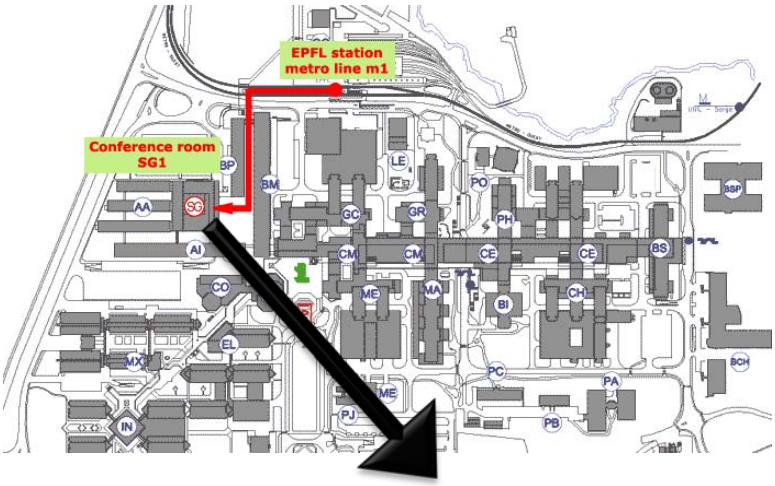
Departure time			Arrival time
Ouchy	Lausanne CFF	Lausanne-Flon	Esplanade EPFL
	Line m2	Line m1	
7h00	7h08	7h10	7h23
7h07	7h15	7h18	7h30
7h20	7h24	7h26	7h38
7h26	7h30	7h33	7h45
7h33	7h40	7h41	7h53
7h39	7h47	7h48	8h00
7h46	7h54	7h56	8h08
7h52	8h00	8h03	8h15
8h05	8h09	8h11	8h23
8h12	8h16	8h18	8h30
8h18	8h22	8h26	8h38
	8h26	8h30	8h43
8h30	8h38	8h40	8h53
8h47	8h47	8h50	9h03

SHUTTLE BUSES FOR IBIS CRISSIER AND NOVOTEL BUSSIGNY

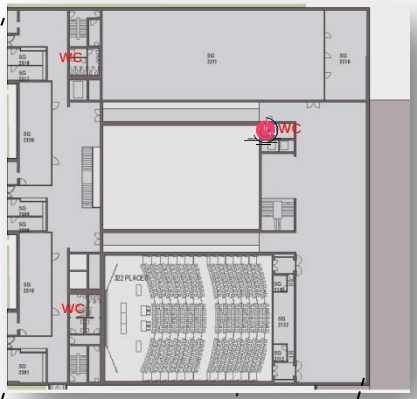
Time table for people who are staying at Ibis Crissier and Novotel Bussigny hotels, and requested shuttle buses, is provided below.

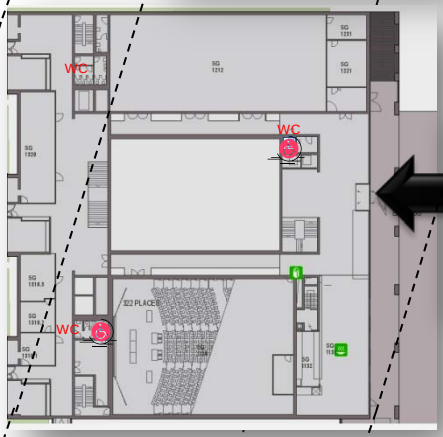
Dates	Departure	Departure Time	Intermediate Stop	Arrival Time	Departure Time	Arrival	Arrival Time
Sept 06 (SUN)	Hôtel Ibis	17h40	Hôtel Novotel	17h45	17h50	Esplanade EPFL	18h10
	Esplanade EPFL	20h30	Hôtel Novotel	20h45	20h50	Hôtel Ibis	20h55
Seot 07 (MON)	Hôtel Ibis	07h45	Hôtel Novotel	07h50	07h55	Esplanade EPFL	08h15
	Lausanne Ouchy	22h30	Hôtel Novotel	22h50	22h55	Hôtel Ibis	23h00
Sept 08 (TUE)	Hôtel Ibis	08h00	Hôtel Novotel	08h05	08h10	Esplanade EPFL	08h30
	Grand Café du Casino	22h30	Hôtel Novotel	22h50	22h55	Hôtel Ibis	23h00
Sept 09 (WED)	Hôtel Ibis	08h00	Hôtel Novotel	08h05	08h10	Esplanade EPFL	08h30

Conference area



Level 2
- Registration
- Main entrance to the conference room
- Internet area
- Welcome Coffee





Main Entrance To the Building

Level 1
- Main entrance
- Information desk

Level 0
- Coffee-breaks
- Exhibition
- Poster Session

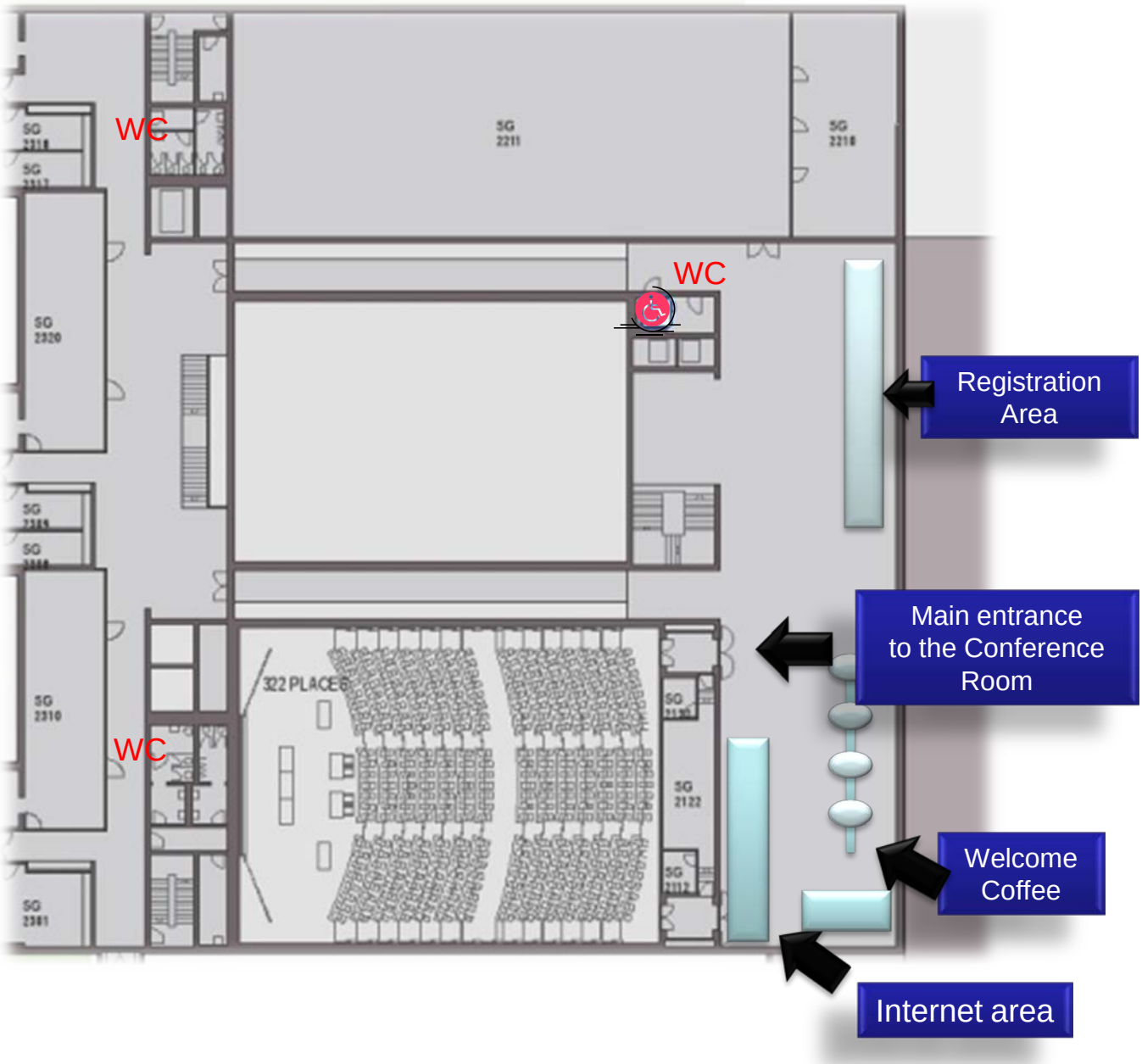
For campus maps:
http://documents.epfl.ch/groups/e/ep/epfl-unit/www/plan/PLAN_EPFL-PRINT.pdf
http://documents.epfl.ch/groups/e/ep/epfl-unit/www/plan/PLAN_EPFL-WEB.pdf

Conference area

Level 2

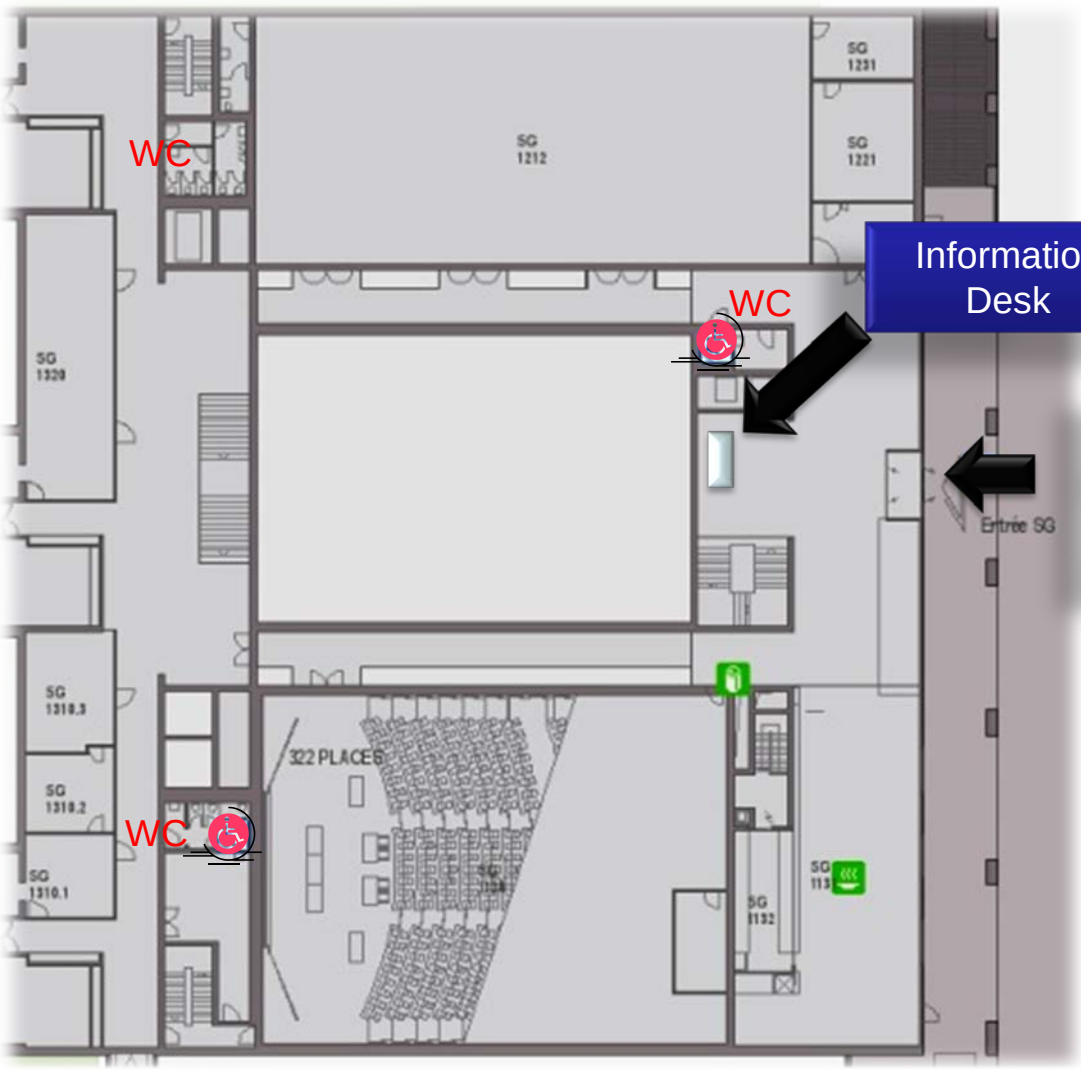
- Registration
- Main entrance to the conference room
- Internet area
- Welcome Coffee

- Electric outlets are installed below the tables. Please see page 17 for the details about the type of plug.



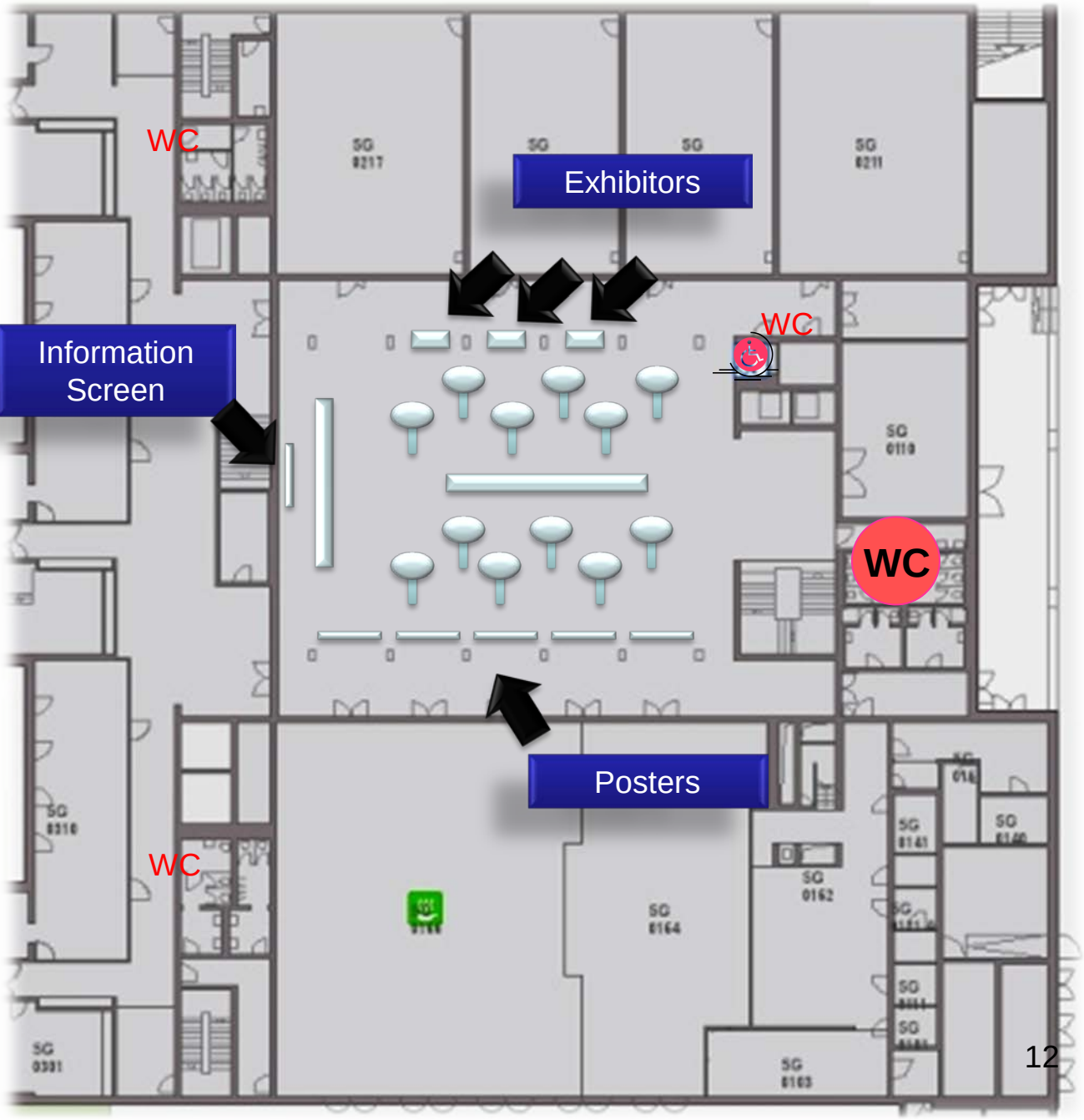
Conference area

Level 1
- Main entrance
- Information desk



Conference area

Level 0
- Coffee-breaks
- Exhibition
- Poster Session



Registration

There are 300 attendees registered to the CHES 2009 workshop, so we ask you to show up early for the registration. We strongly advise attendees coming to Lausanne on Sunday to **register on that day. The registration desk will be open from** 18h00 to 20h30 at the EPFL, SG building, 2nd floor (Level 2). You will receive a delegate pack with the items described below. The Reception will take place in the same building on level 0.

For those who opted for a vegetarian menu, you will also receive special cards to identify yourself at the restaurants. Please place it on the table during the meals
(Kosher or Halal food will not be available during the conference).

Those who have not yet paid their registration fee can pay this by credit card or in cash (Swiss Francs only) at the registration desk upon arrival to finish their registration and obtain access to the conference.

For those coming by car, parking tickets will be available at the registration desk for 15CHF (for the duration of the workshop)

DELEGATE PACK

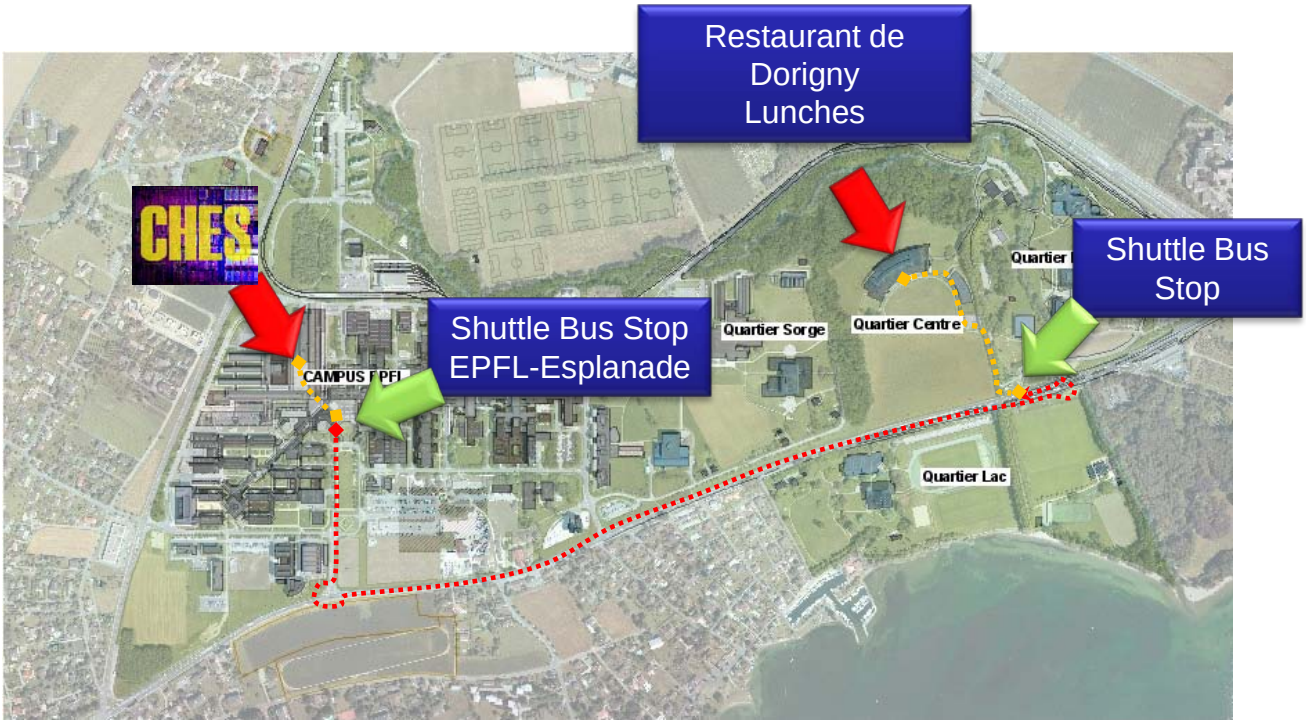
- Bag
- T-shirt
- Mug
- Proceedings
- Pen
- Paper Notebook
- Lausanne City Maps
- Attendee List
- Promotional Materials

INTERNET

Internet Access - Wi-Fi
Wi-Fi Internet access is available for free for all attendees. An **open Wi-Fi access is available in most of the building of the campus.**

Connect to **SSID : public-epfl**
Go to the page: https://enclair.epfl.ch/enclair.php
Select Login **EnClair**
Guest account: **x-ches**
Password: **adeger60**
Use DHCP network setup
There is NO security to activate (WEP key, WPA, etc.)

Lunches



Lunches will take place at the Restaurant de Dorigny.
Shuttle buses will be provided for rapid transportation.
The shuttle buses will be waiting on the place marked on the map. The bus stop at the EPFL is called EPFL – Esplanade.

In order to respect a tight schedule, it is highly advisable to follow the instruction of the assistants who will guide you to the shuttle bus stops.

Access to the restaurant will be controlled by inspection of the badges.
Please wear your CHES 2009 badge at all times.

For those who opted for a vegetarian menu. Special cards will be provided inside the badges.
Please place the cards on the table to identify yourself.

If you get lost on campus, ask for “Banane – Unil” (this is how it is called by the students).
It is 15-20 min. walking distance from the conference room.

Special Event Sponsors & Exhibitors

SPECIAL EVENT SPONSOR & EXHIBITOR

Cryptography Research Inc.

Cryptography Research, Inc. specializes in solving complex data security problems. In addition to security evaluation and applied engineering work, CRI is actively involved in long-term research and technology licensing in areas including tamper resistance, content protection, network security, and financial services. Security systems designed by Cryptography Research engineers protect more than $100 billion of commerce annually for telecommunications, financial, digital television, and Internet industries. Founded in the early 1990's by internationally renowned cryptographer Paul Kocher, Cryptography Research's client list includes dozens of leading firms in Silicon Valley and worldwide.

SPECIAL EVENT SPONSOR

Nagravision Kudelski Group

Nagravision, a Kudelski Group company, is the leading supplier of open conditional access systems, DRM and integrated on-demand solutions for content providers and digital TV operators over broadcast, broadband and mobile platforms. Its technologies are currently being used by more than 120 leading Pay-TV operators worldwide securing content delivered to over 101 million active smart cards and devices.Please visit www.nagravision.com for more information.

EXHIBITOR

Riscure

Riscure is an independent security test laboratory specialized in testing the resistance of smart card products and embedded devices against software, side channel and hardware attacks. Riscure also develops and maintains security test tools for manufacturers, security labs and other organizations interested in performing in-house security testing. Our customers are international industry leaders.

GALA DINNER ON LAKE GENEVA

The CHES Workshop gala dinner will be on a cruise with a wonderful alpine scenery and a view to the famous Lavaux vineyards (designated part of the UNESCO World Heritage in 2007). The boat will set sail from St-Sulpice near the EPFL and will end its journey at Ouchy in Lausanne, near the hotels.

Program:
Shuttle bus departs from the EPFL-Esplanade at 18h00.
Check-in at Saint-Sulpice: 18h30
Return to Ouchy: 22h30

RUMP SESSION IN THE CASINO MONTBENON

The rump session will take place in the Casino Montbenon. Built in 1908, it is located just five minutes away from the city center on foot. Surrounded by magnificent gardens with an unparalleled view of the mountains and the lake, it was renovated in 1981 and transformed into a Centrex for cultural and social events.

Program:
Shuttle bus departs from the EPFL-Esplanade at 18h00.
Aperitif + Music: 18h30
Semi-Standing Dinner: 19h15
Best Paper Awards: 20h15
Rump Session: 20h30
Presentation of the Program Committee: 22h00
Aperitif+ Music: 22h15
End of the event: 22h45

Access to the boat and to the casino Montbenon will be controlled by inspection of the badges. Please wear your CHES 2009 badge at all times.
Dress code for all the events: Business casual / Casual
Internet connection will not be available during these two events.

Language
French, German, Italian and Rumantsch are the four official languages.
Lausanne is located in the French-speaking part of Switzerland. In the urban area of Geneva Lake Region many inhabitants understand or speak at least some English.

Currency
The currency in Switzerland is the Swiss Franc (CHF). 1 CHF ~= 0.66 EUR, 0.94 USD, 88.83 JPY

Time zone
GMT+1. In September, it is still daylight saving period, so it is actually GMT+2.
http://www.timeanddate.com/worldclock/results.html?query=lausanne

Population
125,000 / Greater Lausanne: 250,000

Altitude
372 m/1,124 feet at lakeside.
495 m/1,628 feet at city center.

Climate
Average temperature in September: 21 C/70 F

Power and electrical plugs

Electricity is 220-240V, 50 Hz.
There is a special electrical plug in Switzerland
(different from France or Germany).
Please bring an adapter as we will not have any available for you.
(Electric outlets are installed below the tables in the conference room SG1)

Phone
General information:
•Switzerland country code : 41
•Lausanne area code : 21
•To call inside Switzerland, use 0 as prefix to area code: for example 021 693 82 10
•To call foreign countries 00 + country code + area code + number. For example 00 33 4 79 44 44 96 (example for France)

Emergency numbers during the conference are the following.
During the registration desk opening : 021 693 82 10
Anytime when the above number is not available : 078 783 8308

Opening hours of the shops:
Monday – Friday: 9h00 – 19h00
Saturday: 9h00 – 18h00
Sunday closed

Smoking area:
Smoking will not be permitted from September 1st 2009, indoor in the canton Vaud.

Information for conference presenters

The conference room is setup with a laptop computer (Pentium(R) Dual-Core T4200 @ 2GHz, 4096 Mb RAM), connected to Internet, and a projector.
The following software are installed on the laptop:

- Microsoft Windows Vista (32-bit) with SP1, U.S. English
- Open Office 3
- Microsoft Office 2007
- Firefox 3.5.2
- Internet Explorer 8
- Windows Media Player v.11.0.6001.7007
- Adobe Acrobat 9 PRO Version 9.1.3
- Java Runtime Environment Version 6.0 Update 15
- 7ZIP

- A laser pointer will be available during the presentations.

Instruction to upload the presentation files to a server will be provided by the PC chairs.
For those who are not able to upload their files are requested to bring the presentation file on a USB key and transfer on the conference computer **THE DAY BEFORE the beginning of the session. Internet connection will not be available during the rump session at the Casino Montbenon.**

Each of the session talks will consist of 20 min. of presentation followed by 5 min. of questions.
In order to respect a tight schedule, color coded cards will mark the minutes left of the talk.
The following code will be used: Green for 5min. left; yellow for 3 min. left; orange (+ bell) for 1 min. left and red (+bell) for the end of the talk.

Information for poster presenters

Posters can be set up on Tuesday from 8h15 in the posters area on the dedicated wood panels with pins or tape.
The maximum size of the poster is A0 portrait (118.9 cm height 84.1cm width).

Steering Committee meeting

The meeting will take place at the B. Vittoz room (the presidential room) at 19h30 on Sunday 6th of September.
See details on the map on the right.

GPS COORDINATES OF IMPORTANT PLACES

•Conference venue:
Conference Room, SG Building, EPFL: 46.520953,6.564575

•Lunches:
Restaurant de Dorigny: 46.522555,6.57999

•Rump session:
Casino Montbenon: 46.520498,6.625072

•Gala Dinner:
Saint Sulpice (departure point): 46.508644,6.561252
Ouchy (arrival point) 46.50536,6.627749

•Other touristic places:
Lausanne Flon: 46.520326,6.629865
Lausanne CFF: 46.516773,6.629087
Cathedral: 46.522576,6.635691

SUPERMARKETS

Most of the shops are open until 18h00 on Saturday, 19h00 on working days and are closed on Sundays. Below are the addresses for supermarkets with extended opening times.

•Coop pronto: Lausanne-Ouchy
Avenue d'Ouchy 68
1006 Lausanne/Ouchy
Open: 6h00 – 22h00

•Coop pronto: Lausanne CFF (Main Station)
(Inside the station)
Rue du Simplon
1018 Lausanne
Open: 6h00 – 24h00

•Coop pronto Chauderon
place Chauderon 3
1003 Lausanne
Open: 6h00 – 22h00

•Migros Ouchy
Avenue de Rhodanie 2
1007 Lausanne/Ouchy
Open: Ma-Su 8h00 – 21h45
Lu 9h00 – 21h45

RESTAURANTS

Restaurant le Pur (Méditerranéen)
Address : Rue du Port-Franc 17
1003 Lausanne, Switzerland
Tel : +41 21 311 99 33
Opening : Mo-We 08.00 - 24.00
Th 08.00 - 01.00,
Fri-Sa 09.00 - 02.00
Su 09.00 - 24.00
WiFi
http://www.pur-flon.ch

For an extensive list of restaurants:
http://www.swisspassport.ch/?cat=2&lp_lang_pref=en&paged=1

BAR, CAFES AND CLUBS

Taco's bar
rue de Genève 17
1003 Lausanne, Switzerland
Su-Th 17h30-01h00
Fr-Sa17h30-02h00
Phone: 021 320 15 25
FAX: 021 320 15 26
http://www.tacos-bar.ch

Café Luna
Address : Place de l'Europe 7
Tel : +41 21 329 08 46
Opening : Mo-We 07.00 - 24.00
Th 07.00 - 01.00,
Fr 07.00 - 02.00, Sa 09.00 - 02.00
WiFi
http://cafe-luna.ch

For an extensive list of bars, cafes and clubs:
http://www.swisspassport.ch/?cat=3&lp_lang_pref=en&paged=1

MUSEUMS

"Art Brut" Collection
Av. des Bergières 11
tel: +41 21 315 25 70
Tu-Su & public holiday 11h -18h
http://www.artbrut.ch/

Olympic Museum
Quai d'Ouchy 1
tel: +41 21 621 65 11
7 days 9h-18h, closed on Mondays from October to April, 25th December & 1st January
http://www.olympic.org/uk/passion/museum/

Further information about museums:
http://www.swisspassport.ch/?page_id=40&lp_lang_pref=en

GENEVA

If you want to spend some time in Geneva, you may consider visiting the St-Peter's Cathedral (Cathédrale Saint-Pierre). A beautiful panoramic view of the city awaits you.

Place de la Taconnerie 6
1204 Genève, Switzerland
022 310 09 76
Mo-Sa 9h30 - 18h30 (access to the tower 18h00)
Su 12h00 - 18h30 (access to the tower 17h00)
Access to the tower : 4CHF (there are no elevators)

For further information about the city:
http://www.geneve.ch/welcome_en.html

Further information about St-Peter Cathedral:
http://www.saintpierre-geneve.ch/index2.html

MONTREUX – CHILLON CASTLE

The castle of Chillon, a 13th-century castle on the shore of Lake Geneva, is one of the best preserved medieval castles in Europe and one of the most visited in Switzerland.
You can get there from Lausanne CFF by train. Get off at Montreux CFF (19-32 min). You may then enjoy a pedestrian walk along the shores of lake Geneva until the castle (~32 min.).

Opening hours: 9h00 to 19h00
Admission until: 18h00
Adult : 12CHF

Further information about Chillon Castle:
http://www.chillon.ch/en/

Further information about the city of Montreux:
http://www.montreux.ch/

Program

Switzerland

SUNDAY, SEPTEMBER 6

Time	Event
18h00 – 20h30	Registration
18h30 – 20h30	Reception

MONDAY, SEPTEMBER 7

Time	Event		
	Session	Authors	Title
07h30 – 18h00	Registration		
08h00 – 08h30	Welcome Coffee		
08h30 – 08h45	Welcome		
08h45 – 10h25	Session 1: Software Implementations Chair: Guido Bertoni	Emilia Käsper, Peter Schwabe	Faster and Timing-Attack Resistant AES-GCM
		Mike Hamburg	Accelerating AES with Vector Permute Instructions
		Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Li, Bo-Yin Yang	SSE Implementation of Multivariate PKCs on Modern x86 CPUs
		Thomas Eisenbarth, Tim Güneysu, Stefan Heyse, Christof Paar	MicroEliece: McEliece for Embedded Devices
10h25 – 10h50	Coffee Break – Exhibition		
10h50 – 11h50	Invited Talk I Chair: Kris Gaj	Srini Devadas MIT, USA	Physical Unclonable Functions and Secure Processors
11h50 – 12h05	Transfer EPFL - Dorigny		
12h05 – 13h35	Lunch (Doringy)		
13h35 – 13h50	Transfer Dorigny - EPFL		
13h50 – 15h30	Session 2: Side Channel Analysis of Secret Key Cryptosystems Chair: Helena Handschuh	Pierre-Alain Fouque, Gaëtan Leurent, Denis Réal, Frédéric Valette	Practical Electromagnetic Template Attack on HMAC
		Emmanuel Prouff, Robert McEvoy	First-Order Side-Channel Attacks on the Permutation Tables Countermeasure
		Mathieu Renauld, François-Xavier Standaert, Nicolas Veyrat-Charvillon	Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA
		Lejla Batina, Benedikt Gierlichs, Kerstin Lemke-Rust	Differential Cluster Analysis
15h30 – 15h50	Coffee Break – Exhibition		
15h50 – 16h40	Session 3: Side Channel Analysis of Public Key Cryptosystems Chair: Marc Joye	Martin Hlaváč	Known-Plaintext-Only Attack on RSA-CRT with Montgomery Multiplication
		Thomas Finke, Max Gebhardt, Werner Schindler	A New Side-Channel Attack on RSA Prime Generation
16h40 – 16h45	Technical Break		
16h45 – 18h00	Special Session 1: DPA Contest Chair: Elisabeth Oswald		
18h00 – 18h30	Transfer EPFL – St. Sulpice		
18h30 – 22h30	Dinner Cruise		

Program

Switzerland

TUESDAY, SEPTEMBER 8

Time	Event		
	Session	Authors	Title
08h15 – 18h00	Registration		
08h15 – 08h45	Welcome Coffee		
08h45 – 10h25	Session 4: Side Channel and Fault Analysis, Countermeasures (I) Chair: Catherine Gebotys	Jean-Sébastien Coron, Ilya Kizhvatov	An Efficient Method for Random Delay Generation in Embedded Software
		Matthieu Rivain (Speaker: Christophe Giraud)	Differential Fault Analysis on DES Middle Rounds
		Minoru Saeki, Daisuke Suzuki, Koichi Shimizu, Akashi Satoh	A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques
		Francesco Regazzoni, Alessandro Cevrero, François-Xavier Standaert, Stephane Badel, Theo Kluter, Philip Brisk, Yusuf Leblebici, Paolo Ienne	A Design Flow and Evaluation Framework for DPA-resistant Instruction Set Extensions
10h25 – 10h55	Coffee Break - Poster Session - Exhibition		
10h55 – 11h55	Invited Talk II Chair: Christophe Clavier	Christof Paar Ruhr-Universität Bochum, Germany	Crypto Engineering: Some History and Some Case Studies
11h55 – 12h10	Transfer EPFL - Dorigny		
12h10 – 13h40	Lunch (Doringy)		
13h40 – 13h55	Transfer Dorigny - EPFL		
13h55 – 15h10	Session 5: Pairing-Based Cryptography Chair: Erkay Savas	Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto, Francisco Rodríguez-Henríquez	Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers
		Junfeng Fan, Frederik Vercauteren, Ingrid Verbauwhede	Faster F_p-arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves
		David Kammler, Diandian Zhang, Peter Schwabe, Hanno Scharwaechter, Markus Langenberg, Dominik Auras, Gerd Ascheid, Rudolf Mathar	Designing an ASIP for Cryptographic Pairings over Barreto-Naehrig Curves
15h10 – 15h40	Coffee Break - Poster Session - Exhibition		
15h40 – 16h55	Session 6: New Ciphers and Efficient Implementations Chair: Luca Breveglieri	Christophe De Cannière, Orr Dunkelman, Miroslav Knežević	KATAN & KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers
		Xu Guo, Junfeng Fan, Patrick Schaumont, Ingrid Verbauwhede	Runtime Programmable and Parallel ECC Coprocessor Architecture: Tradeoffs between Area, Speed and Security
		Nicolas Méloni, M. Anwar Hasan	Elliptic Curve Point Scalar Multiplication Combining Yao's Algorithm and Double Bases
16h55 – 17h00	Technical Break		
17h00 – 18h00	Special Session 2: Benchmarking of Cryptographic Hardware Chair: Patrick Schaumont		
18h00 – 18h30	Transfer EPFL – Casino Montbenon		
18h30 – 19h15	Aperitif + Music		
19h15 – 20h15	Semi-Standing Dinner		
20h15 – 20h30	Best Paper Awards		
20h30 – 22h00	Rump Session		
22h00 – 22h15	Presentation of the Program Committee		
22h15 – 22h45	Aperitif + Music		

WEDNESDAY, SEPTEMBER 9

Time	Event		
	Session	Authors	Title
08h15 – 16h00	Registration		
08h15 – 08h45	Welcome Coffee		
08h45 – 10h00	Session 7: TRNGs and Device Identification Chair: Jorge Guajardo	A. Theodore Markettos, Simon W. Moore	The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators
		Roel Maes, Pim Tuyls, Ingrid Verbauwhede	Low-Overhead Implementation of a Soft-Decision Helper Data Algorithm for SRAM PUFs
		Ghaith Hammouri, Aykutlu Dana, Berk Sunar	CDs Have Fingerprints Too
10h00 – 10h30	Coffee Break - Poster Session - Exhibition		
10h30 – 11h30	Invited Talk III Chair: Pankaj Rohatgi	Randy Torrance Chipworks Inc., Canada	The State-of-the-Art in IC Reverse Engineering
11h30 – 12h20	Hot Topic Session: Hardware Trojan and Trusted ICs Chair: Pankaj Rohatgi	Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, Wayne Burleson	Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering
		Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou, Swarup Bhunia	MERO: A Statistical Approach for Hardware Trojan Detection
12h20 – 12h35	Transfer EPFL - Dorigny		
12h35 – 14h05	Lunch (Doringy)		
14h05 – 14h20	Transfer Dorigny - EPFL		
14h20 – 15h10	Session 8: Theoretical Aspects Chair: Louis Goubin	Paulo Mateus, Serge Vaudenay	On Tamper-Resistance from a Theoretical Viewpoint
		Nicolas Veyrat-Charvillon, François-Xavier Standaert	Mutual Information Analysis: How, When and Why?
15h10 – 16h00	Session 9: Side Channel and Fault Analysis, Countermeasures (II) Chair: Louis Goubin	Jean-Sébastien Coron, Antoine Joux, Ilya Kizhvatov, David Naccache, Pascal Paillier	Fault Attacks on RSA Signatures with Partially Unknown Messages
		Matthieu Rivain, Emmanuel Prouff, Julien Doget	Higher-order Masking and Shuffling for Software Implementations of Block Ciphers
16h00 – 16h10	Good Bye		