

Performance of Host Identity Protocol on Lightweight Hardware

Andrey Khurri, Ekaterina Vorobyeva, Andrei Gurtov

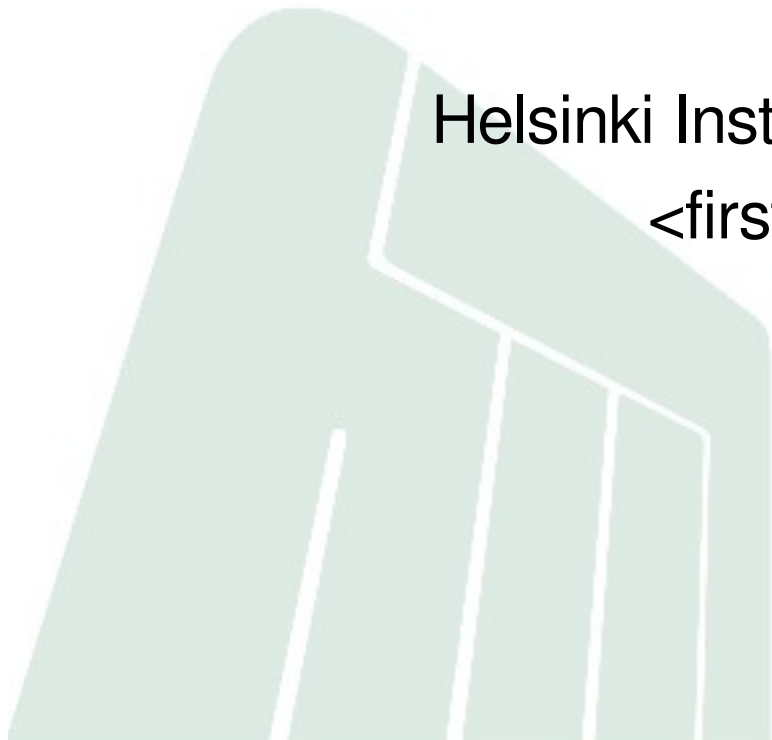
Helsinki Institute for Information Technology

<firstname.lastname@hiit.fi>

MobiArch'07

Kyoto, Japan

August 27, 2007

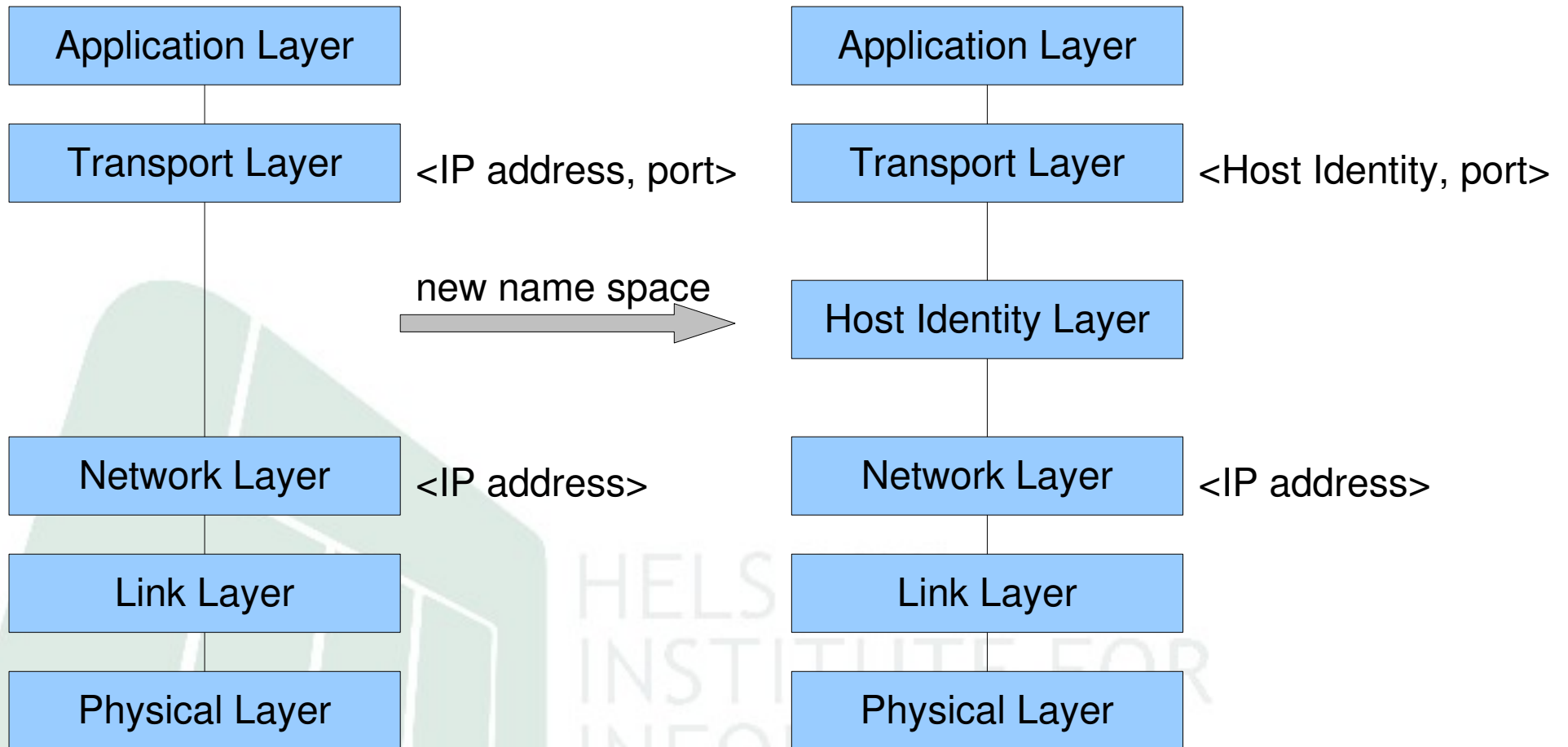


HEL SINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

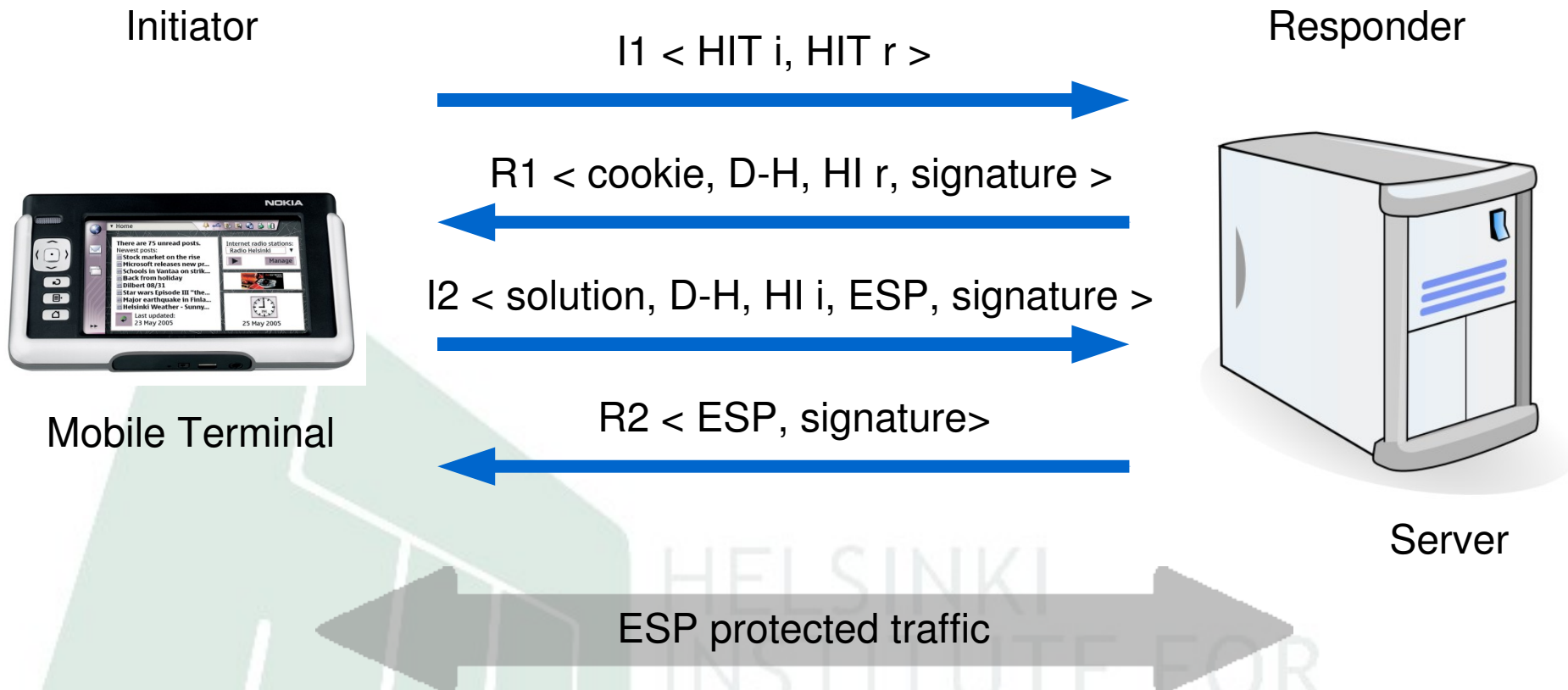
Outline

- Host Identity Protocol (HIP)
- Nokia 770 specifications
- Network setup
- Basic HIP and network characteristics measured
- Measurement results & analysis
- Conclusions

HIP Protocol Stack



HIP Base Exchange



HIP Mobility

Mobile Client

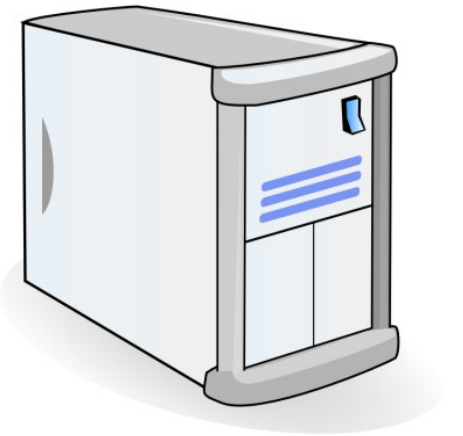


Address 1



Address 2

Server



HIP association

UPDATE < LOCATOR, ESP_INFO, SEQ >

UPDATE < ESP_INFO, SEQ, ACK, ECHO_REQUEST >

UPDATE < ACK, ECHO_RESPONSE >

ESP protected traffic

HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

Nokia 770: technical specifications

- *Processor*

- a 220-MHz, ARM9-based Texas Instruments (TI) OMAP 1710

- *Memory*

- 64 MB DDR RAM
- internal Flash, RS-MMC (Reduced Size – MultiMediaCard) slot

- *Connectivity*

- WLAN – IEEE 802.11b/g
- Bluetooth 1.2

- *Power*

- a 1500-mAh BP-5L Li-Polymer battery

- *Operating System*

- Internet Tablet OS 2006 edition (embedded Debian)
 - GNOME-based graphical user interface
 - Linux 2.6.16 kernel

Network Setup

Ubuntu 6.06 Dapper Drake
Linux Kernel 2.6.16






Intel Pentium 4 CPU 3.00 GHz
1 GB RAM

Switch



IEEE 802.11g

-  Tablet-to-PC
-  Tablet-to-Tablet
-  Laptop-to-PC

Intel Pentium 4 3.00 GHz
IBM R51 Laptop 2.6.16
1 GB RAM

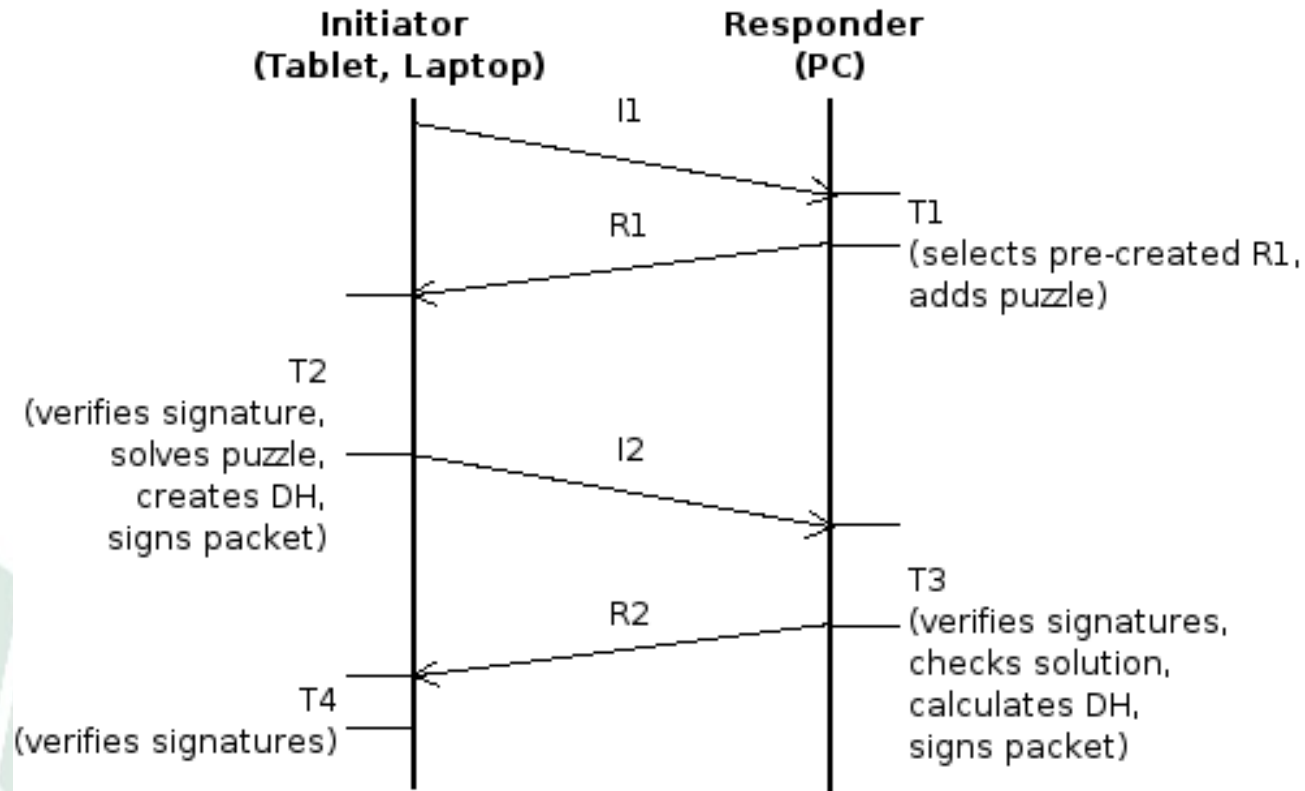


HELSINKI
INSTITUTE OF
INFORMATION
TECHNOLOGY

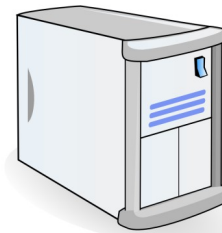
Basic Characteristics

- Duration of HIP Base Exchange
- Duration of Mobility Update
- Round Trip Time
- TCP Throughput
- Power consumption

Times Measured



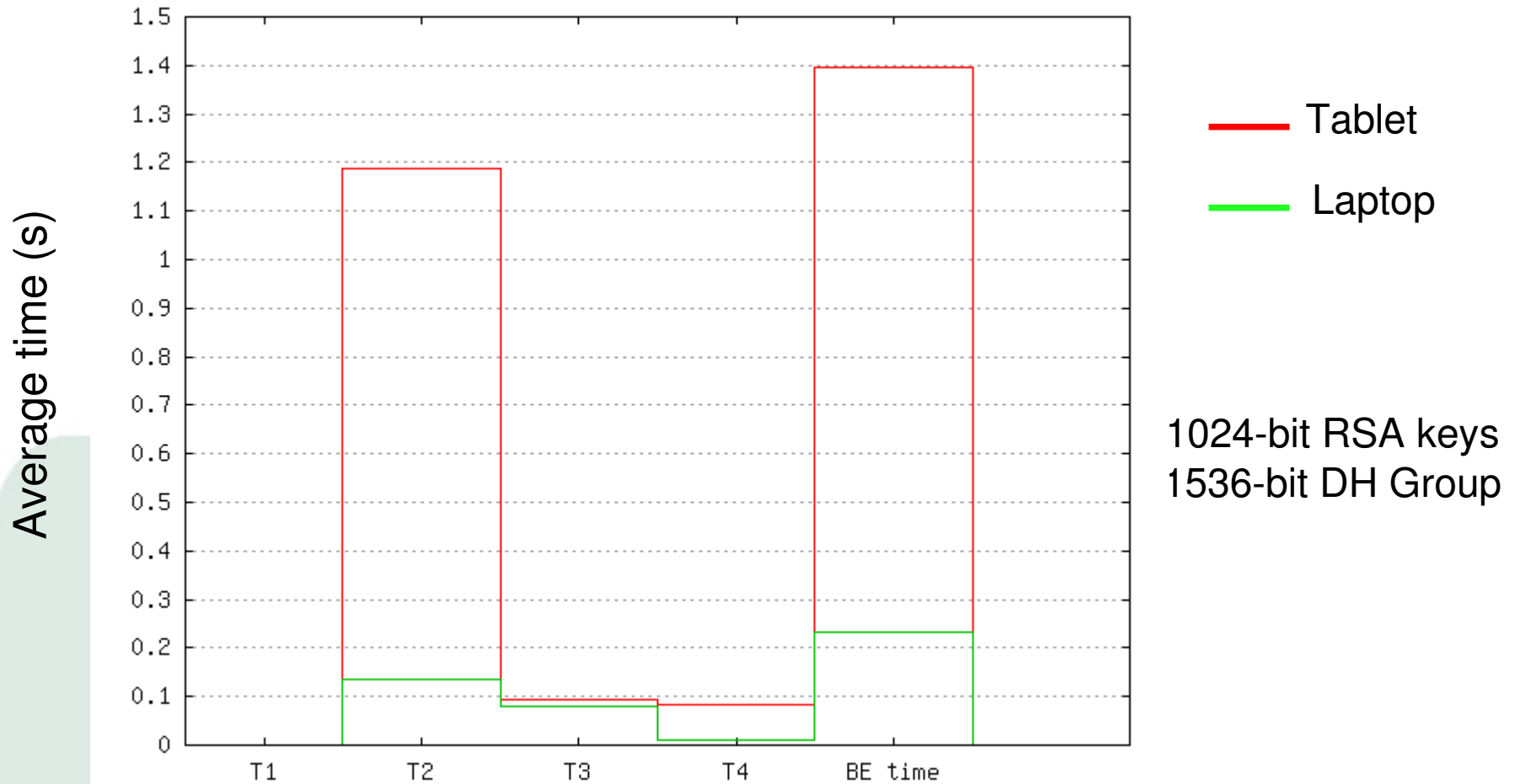
Mobile terminal



Server

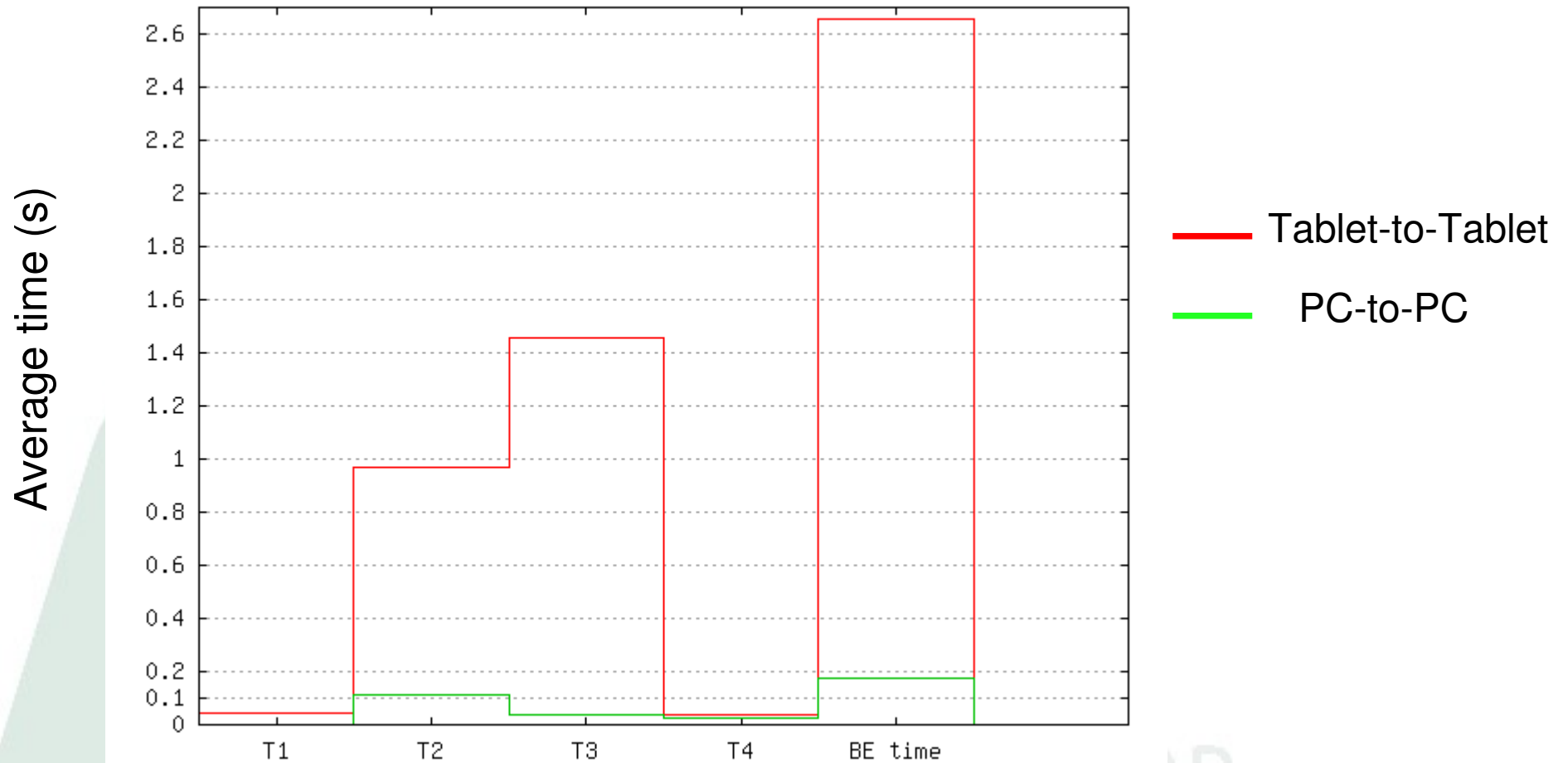
SINK
INSTITUTE
INFORMATION
TECHNOLOGY

Duration of HIP handshake stages



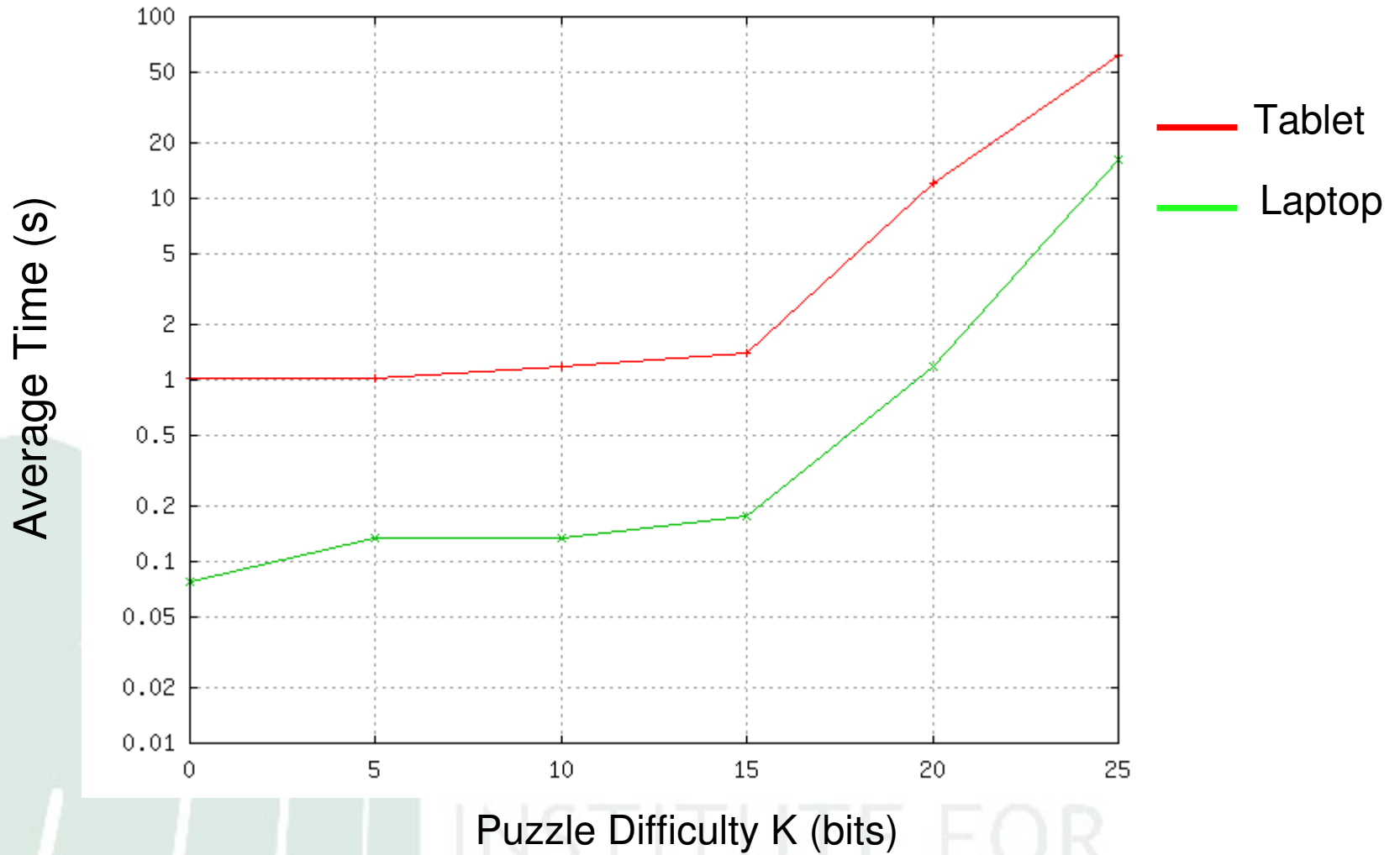
Base Exchange stages and total BE time

Duration of HIP handshake stages (2)



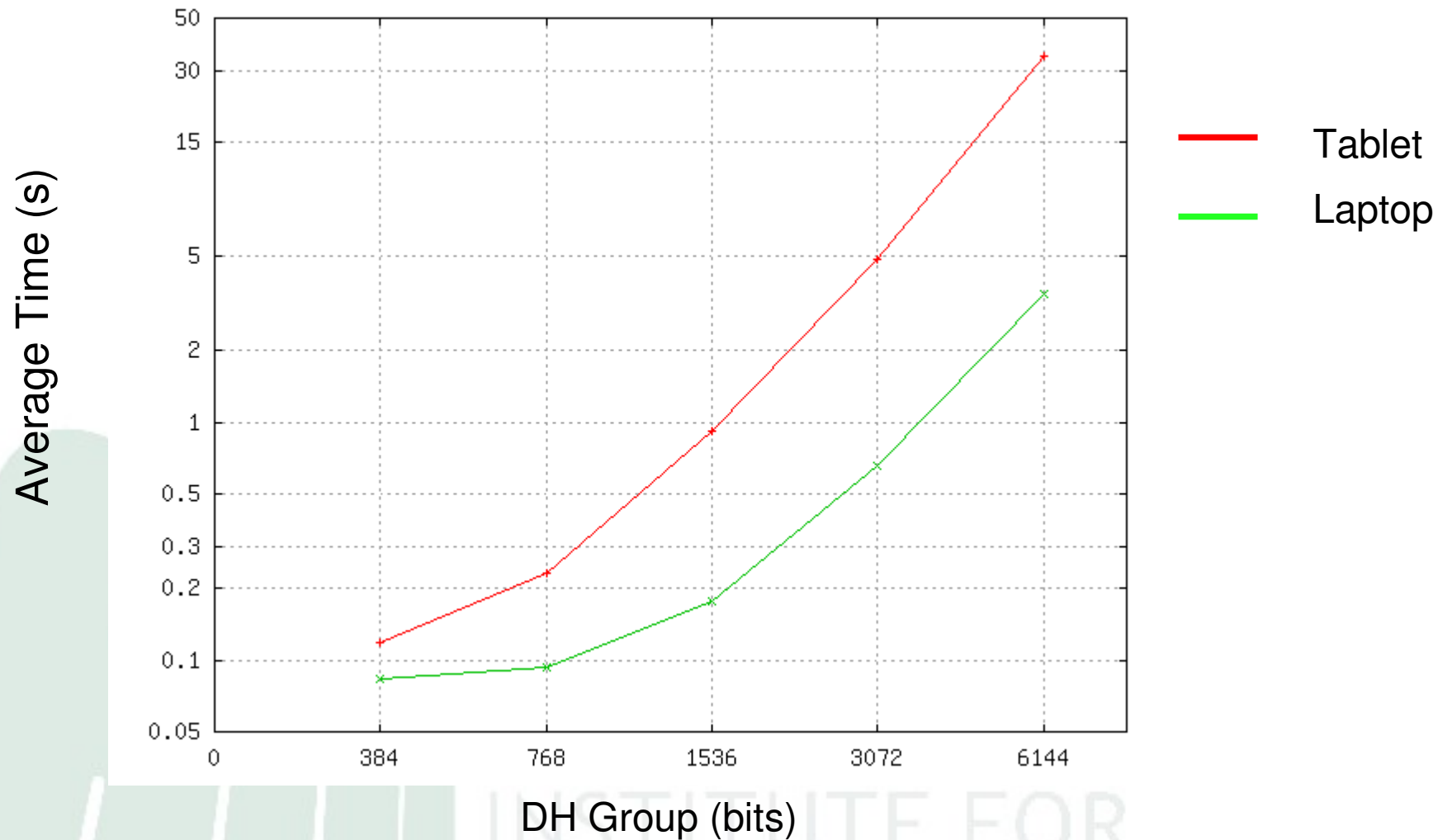
Base Exchange stages and total BE time

Puzzle Difficulty Impact



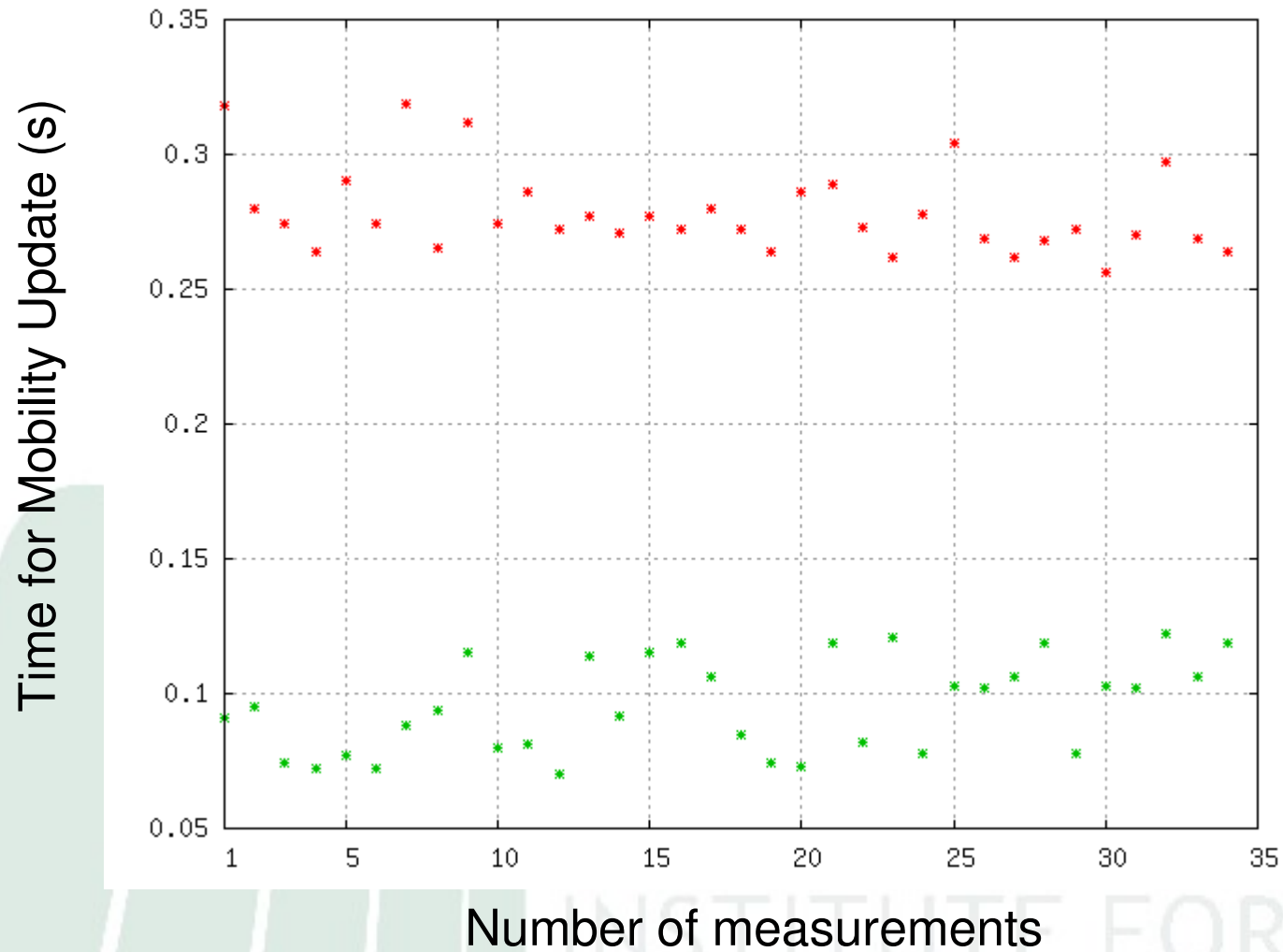
T2 processing time dependence on K

Influence of Diffie-Hellman Group ID



T2 processing time with different DH Groups

Duration of Mobility Update



Tablet



Laptop

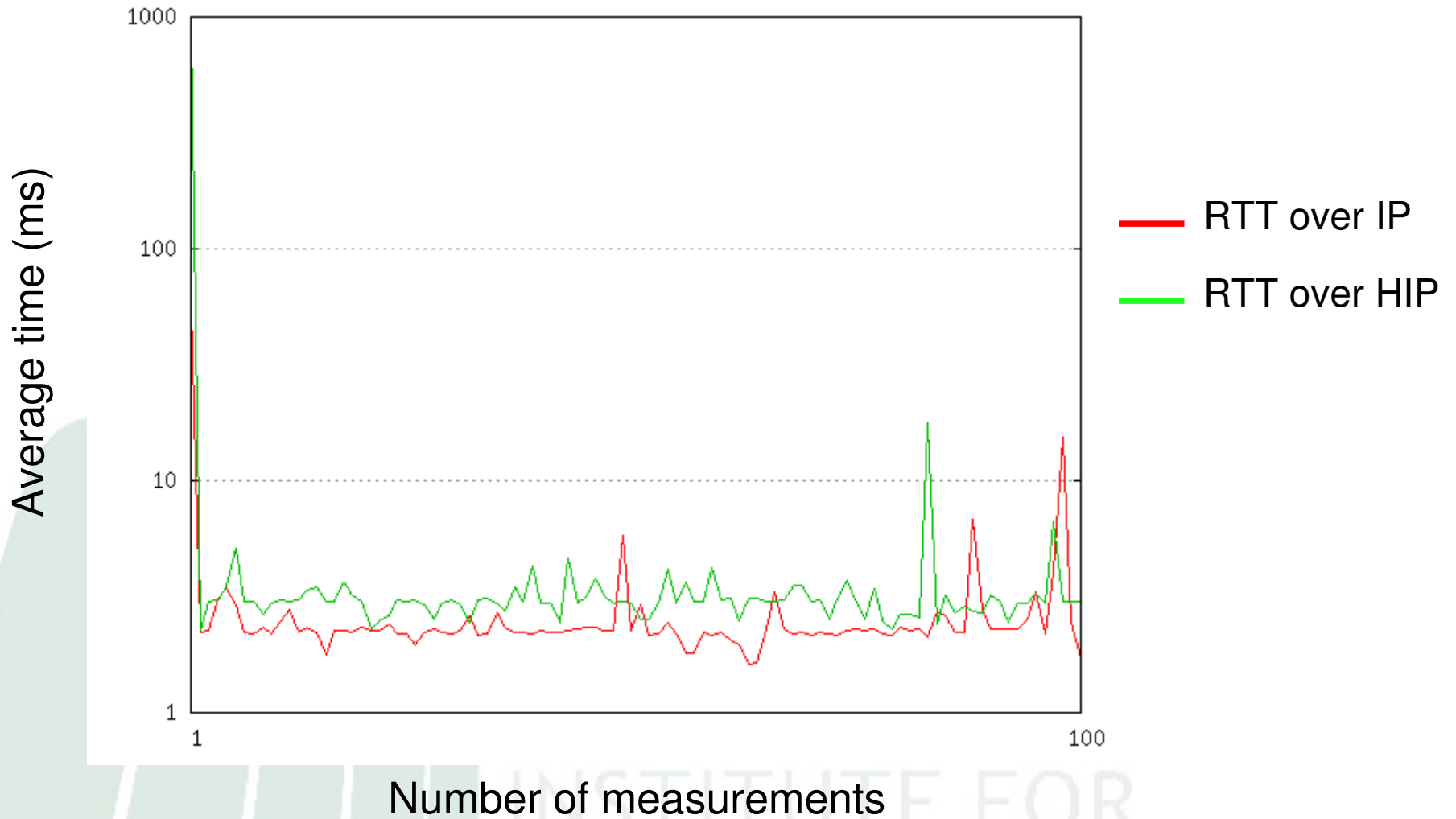
Average time: Tablet – 287 ms; Laptop – 100 ms

Round Trip Time

<i>RTT</i>	<i>Mean ± Standard deviation (ms)</i>		
	IPv6 (64 B)	IPv6 (116 B)	IPv6/HIP (116 B)
PC --> Tablet	2.223 ± 0.470	2.358 ± 0.425	2.936 ± 0.931
Tablet --> PC	1.901 ± 0.332	1.900 ± 1.235	2.748 ± 1.347
PC --> Laptop	1.026 ± 0.340	1.049 ± 0.312	1.177 ± 0.243
Laptop --> PC	1.065 ± 0.338	1.070 ± 0.427	1.207 ± 0.502

Average Round Trip Time of plain ICMP packets of different size and HIP packets

Round Trip Time (cont'd)



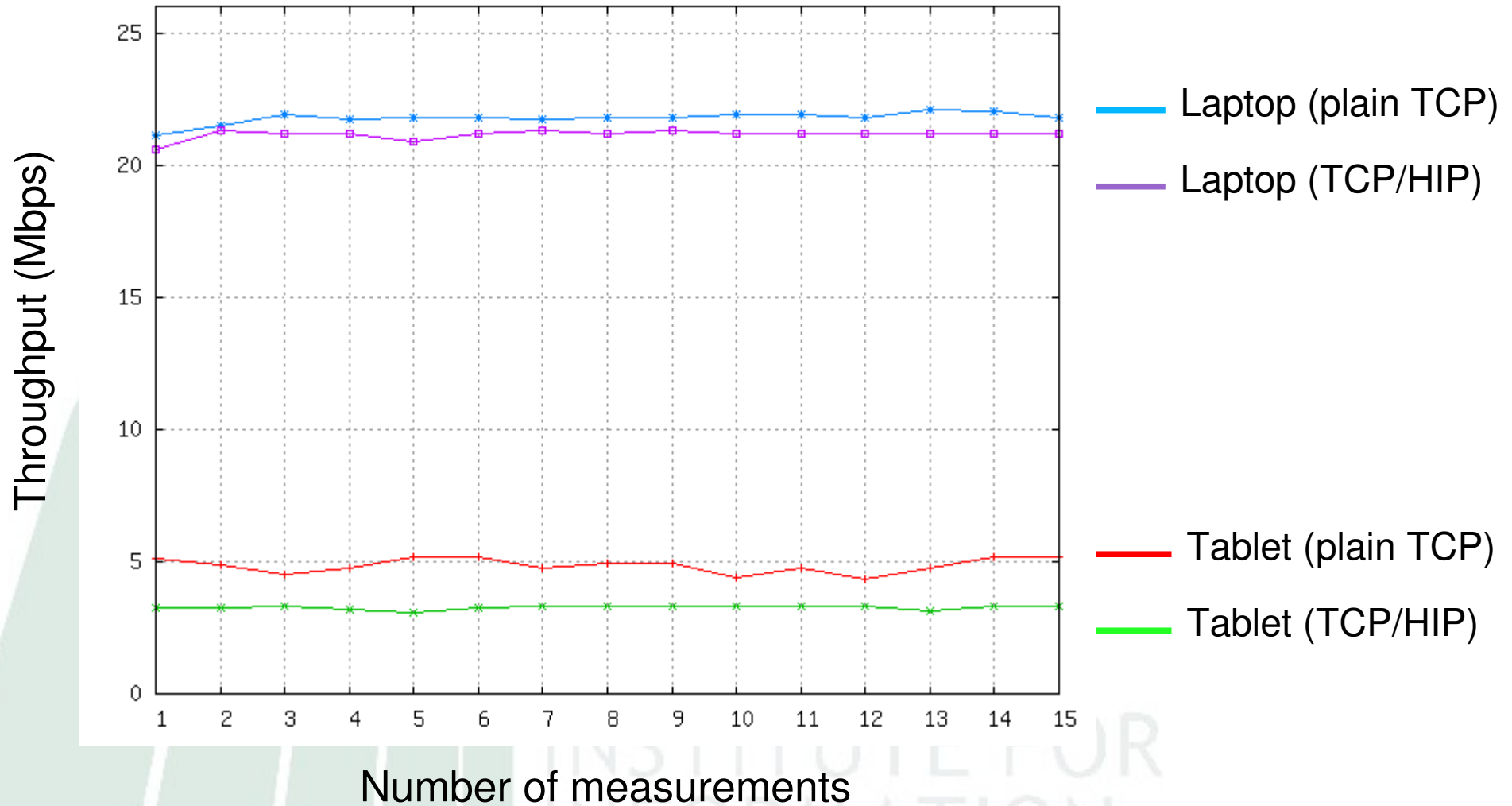
PC as the initiator of the HIP Base Exchange

TCP Throughput

<i>Throughput</i>	<i>Mean ± Standard deviation (Mbps)</i>			
	TCP	TCP/HIP	TCP + WPA	TCP/HIP + WPA
Tablet --> PC	4.86 ± 0.28	3.27 ± 0.08	4.84 ± 0.05	3.14 ± 0.03
Laptop --> PC	21.77 ± 0.23	21.16 ± 0.18		

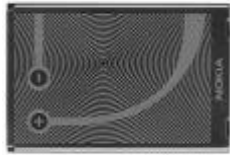
Average TCP throughput with Tablet and Laptop in different scenarios

TCP Throughput (cont'd)



Power consumption

1500 mAh



Applications/Mode	Current (A)
HIP Base Exchange	0.36
ESP traffic (<i>iperf</i> with HIP)	0.38
Plain TCP (<i>iperf</i> without HIP)	0.38
Video stream from a server	> 0.50
Local video	0.27
Audio stream from a server	0.40 – 0.50
Local audio	0.20
Browsing (active WLAN)	0.35 – 0.50
Passive WLAN	0.12
Activating screen	0.12 – 0.14
Standby mode	< 0.01



Current consumption by applications

HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

Power consumption (cont'd)

- Almost no difference in power consumption between the HIP-enabled and non-HIP applications
 - Tablet's CPU is kept busy always upon data transmission over WLAN
 - regardless of the protocol and the application being used
- If compared to the data throughput HIP does consume more energy than plain TCP/IP
 - IPsec data encryption requires a notably longer CPU utilization for a task to be completed
 - The more CPU time is needed the more total energy will be consumed for an operation by the mobile device

Conclusions

- Unmodified HIP might be used in a number of scenarios with a lightweight device communicating via a single proxy server
 - a HIP association establishment requires 1.4 sec
 - duration of mobility update is 287 ms
- HIP is too heavy for two mobile hosts and/or multiple parallel HIP associations
 - Two tablets need nearly two times more of CPU utilization (2.6 sec)
- With the 768-bit DH Group HIP association establishment with a server might be reduced up to 0.35 sec
- Surprisingly, tablet only achieves 4.86 Mbps in a IEEE 802.11g WLAN (Laptop achieves 21.77 Mbps over the same link)

Conclusions (2)

- WPA encryption has minor impact on the throughput. In contrast, ESP encryption involved with HIP reduces TCP throughput by 32%
- HIP slightly increases the RTT that does not noticeably affect the applications
- The use of HIP does not affect the speed of battery depletion
- Energy cost per byte is higher with HIP due to reduced throughput
- Applicability of the measurement results to a wide range of mobility and security protocols
 - most such protocols are based on similar public key and IPsec ESP operations like HIP

Thank You!

Questions?



HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY