Secure and private connectivity in smart environments

Acronym: SURPRISE

SSF Cyber Security Program

Project ID: RIT17-0005

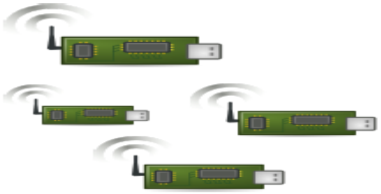
PI: Papadimitratos (KTH)

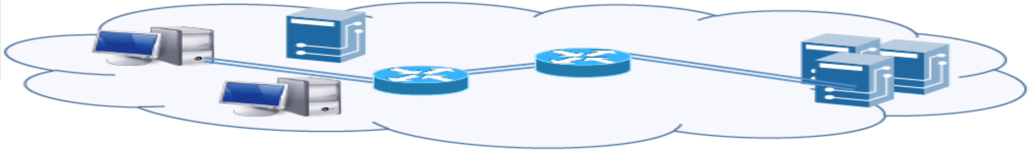
Co-PIs: Fischer-Hübner (KAU), Johansson (LTH), Larsson (LiU), Skoglund (KTH)

https://nss.proj.kth.se/surprise/

Overview & Goals

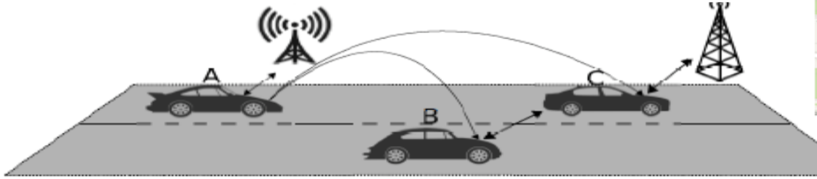
Identity and credential management

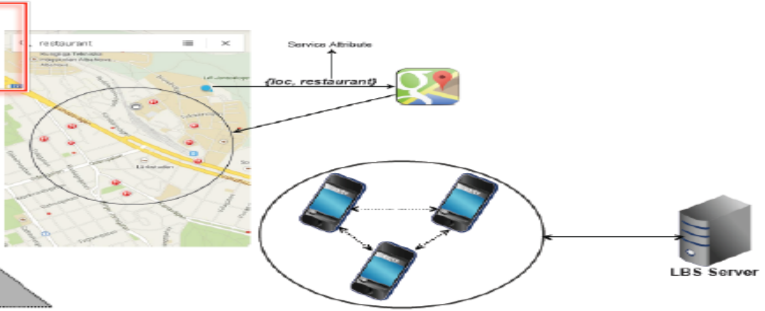




Secure and private data collection, storage, processing, and dissemination

Secure and private wireless communications and networking





- Three key security and privacy (S&P) enablers
  - Trust management, including identity and credential management for S&P
  - Lean, resilient S&P preserving communication and networking
  - Data validation and S&P preserving processing

Research Environment

Consortium

KARLSTADS UNIVERSITET

KTH VETENSKAP OCH KONST

NSS

LTH FACULTY OF ENGINEERING

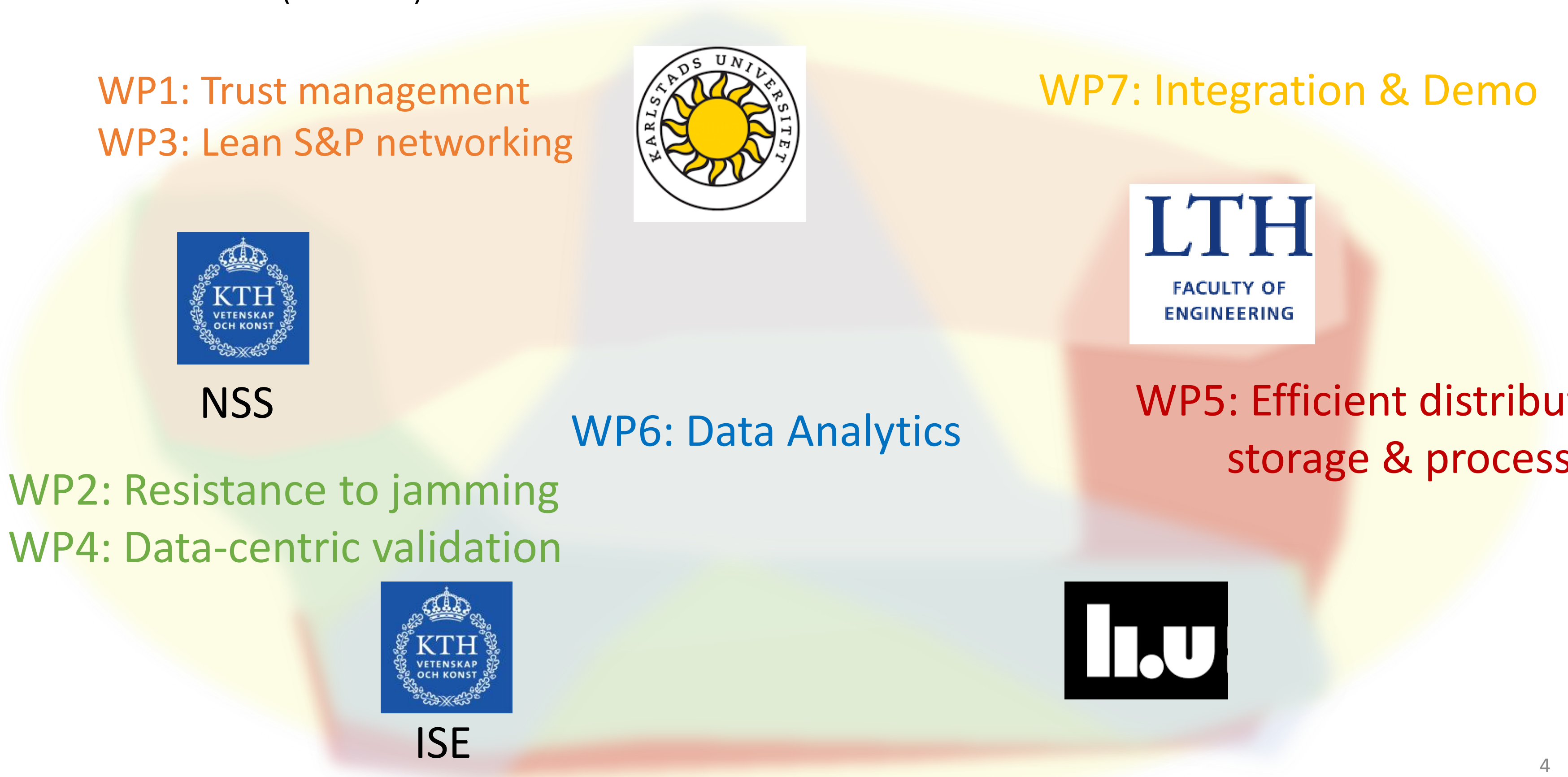
KTH VETENSKAP OCH KONST

ISE

li.u

Research Environment

Consortium (cont'd)



WP1: Trust management

WP3: Lean S&P networking

WP7: Integration & Demo

NSS

WP6: Data Analytics

WP5: Efficient distributed storage & processing

WP2: Resistance to jamming

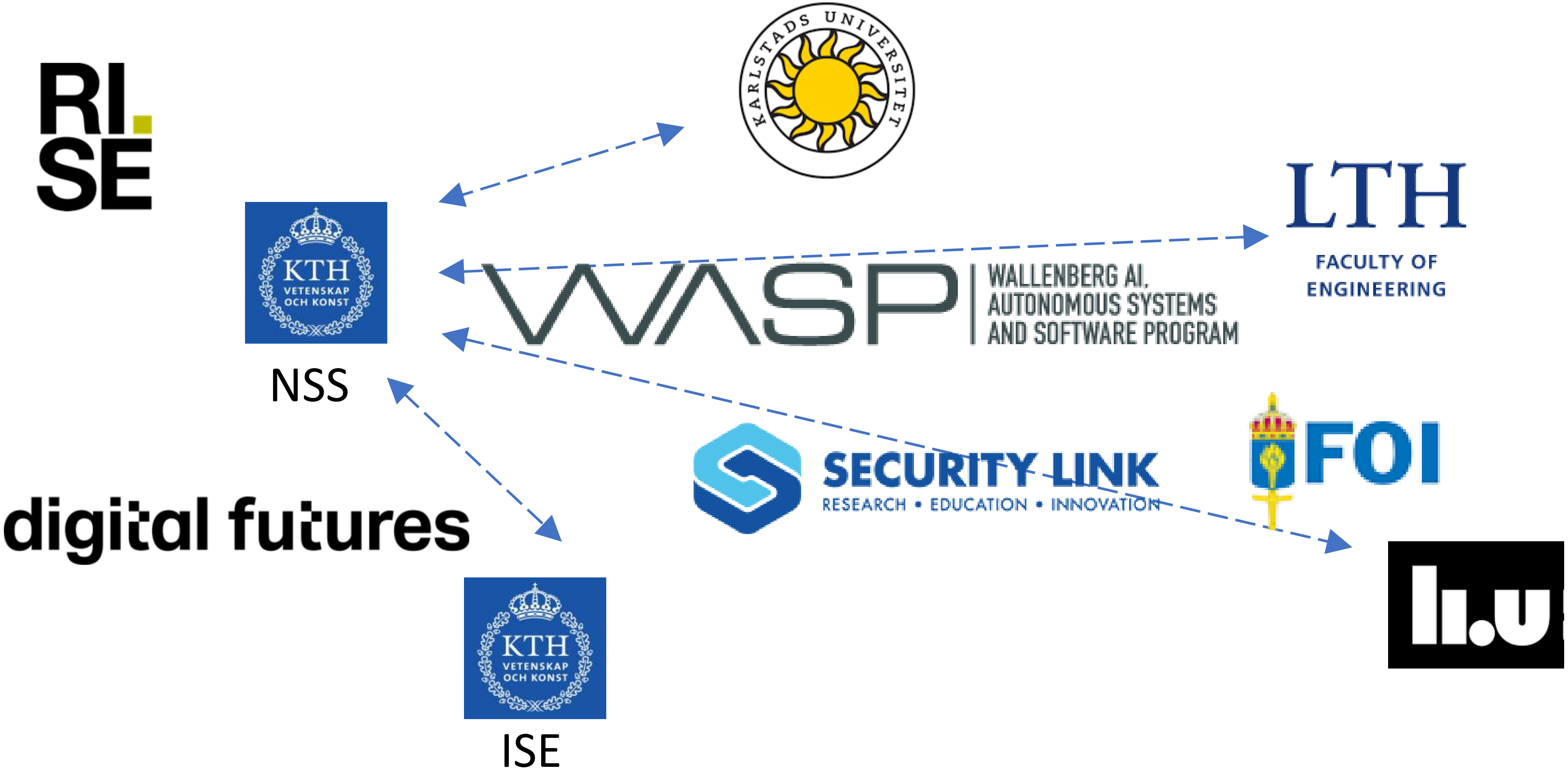
WP4: Data-centric validation

ISE

Research Environment

Academic collaborations

Beyond the proposal:
RISE, Digital Futures,
SecurityLink & FOI



Research Environment

Academic collaborations (cont'd)

Beyond the proposal: ESA, KI; several bilateral collaborations; top conference organization

Privacy Enhancing Technologies Symposium
On the Internet, 2021

South Africa
Sweden
University Forum

acm

esa
European Space Agency

Cyber Security for Europe

Young Academy of Europe

IEEE
Advancing Technology for Humanity

KAROLINSKA INSTITUTET ANNO 1810
Karolinska Institutet

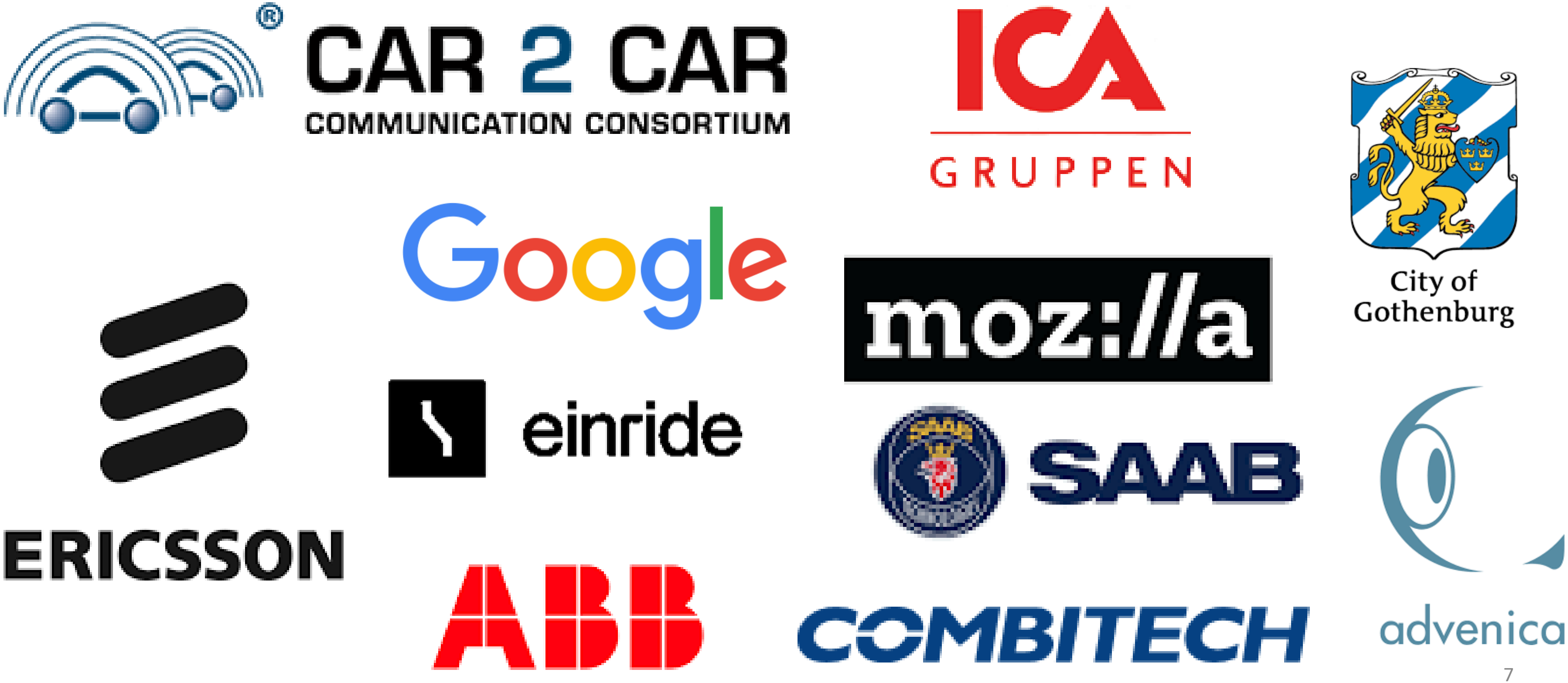
Swedish Defence University

European Commission
HORIZON 2020

Research Environment

Industrial collaborations

Beyond the proposal: ICA, mozilla, einride, Google, City of Gothenburg



Scientific Results

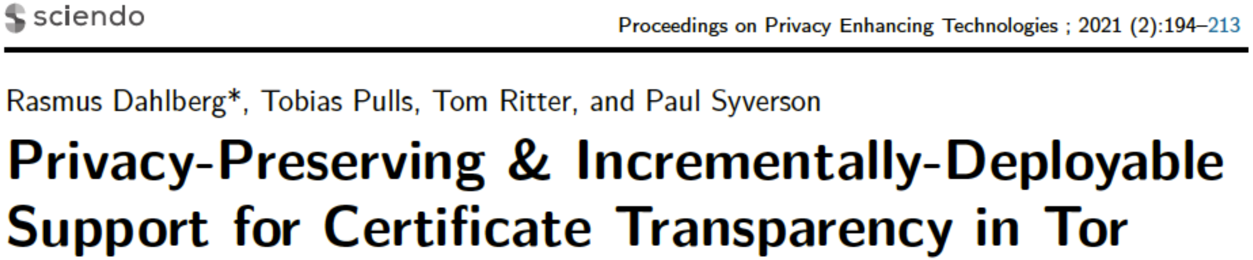
WP1: Selected paper

Tor | Blog

About Suppor

Privacy-Preserving and Incrementally-Deployable Support for Certificate Transparency in Tor

by Rasmus Dahlberg, Tobias Pulls, Tom Ritter, and Paul Syverson | November 30, 2021

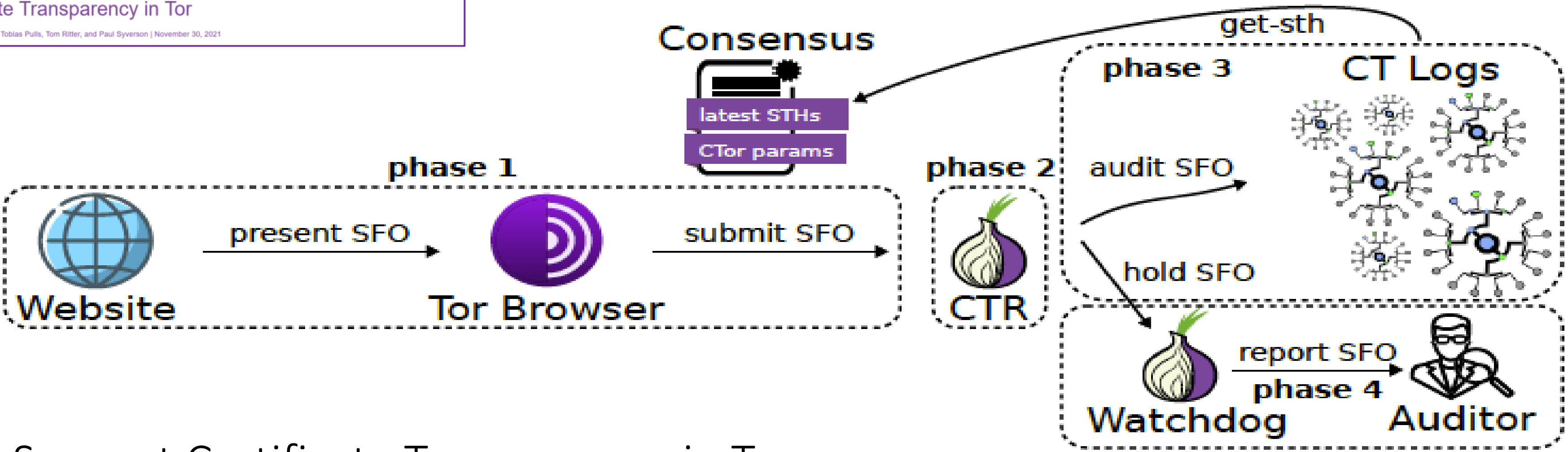


sciendo

Proceedings on Privacy Enhancing Technologies ; 2021 (2):194–213

Rasmus Dahlberg*, Tobias Pulls, Tom Ritter, and Paul Syverson

Privacy-Preserving & Incrementally-Deployable Support for Certificate Transparency in Tor



- Support Certificate Transparency in Tor
- Privacy-Preserving
- Incrementally-deployable

Scientific Results

WP2: Selected paper

IEEE INTERNET OF THINGS JOURNAL, VOL. 8, NO. 10, MAY 15, 2021

Cooperative Location Privacy in Vehicular Networks: Why Simple Mix Zones Are Not Enough

Mohammad Khodaei, *Member, IEEE*, and Panos Papadimitratos, *Fellow, IEEE*

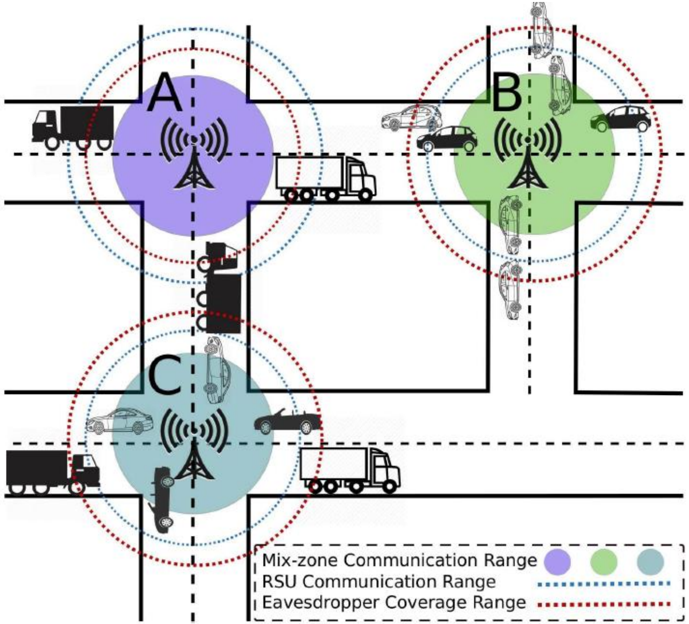


Fig. 2. Mix-zone construction with decoy traffic.

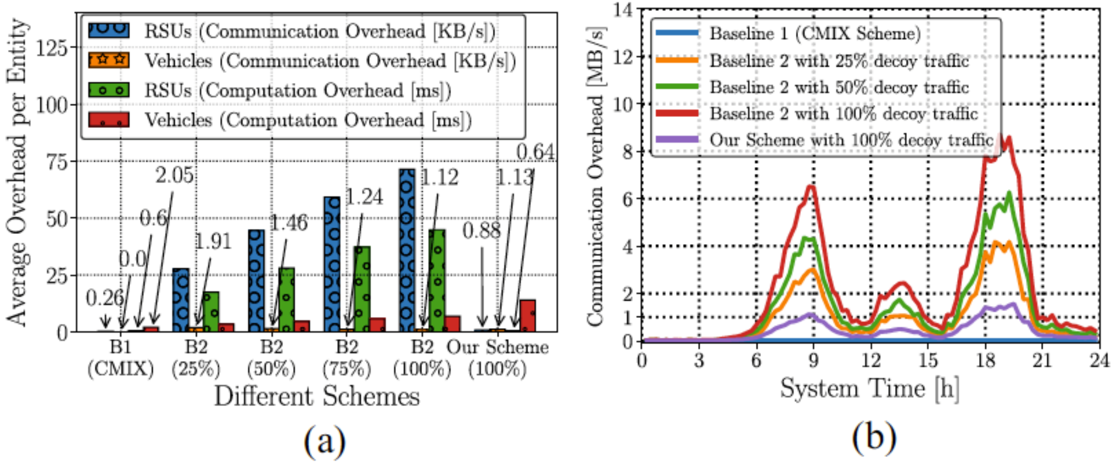
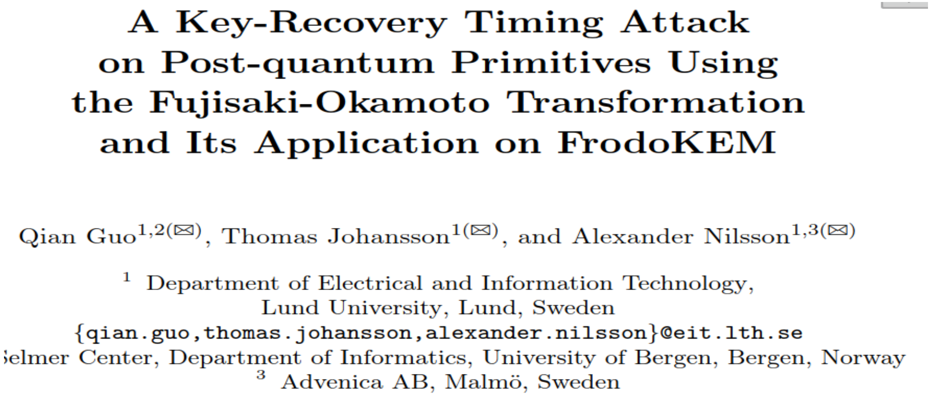


Fig. 8. Comparison among CMIX (B1) [37], chaff-based CMIX (B2) [42], and our scheme: 1K chaff pseudonyms in a CF with $\rho = 10^{-25}$; beacon frequency: $\gamma_{mz} = 0.5$, $\gamma_v = 0.2$. (a) Computation and communication overheads. (b) Communication overhead, averaged every 300 s.

Scientific Results

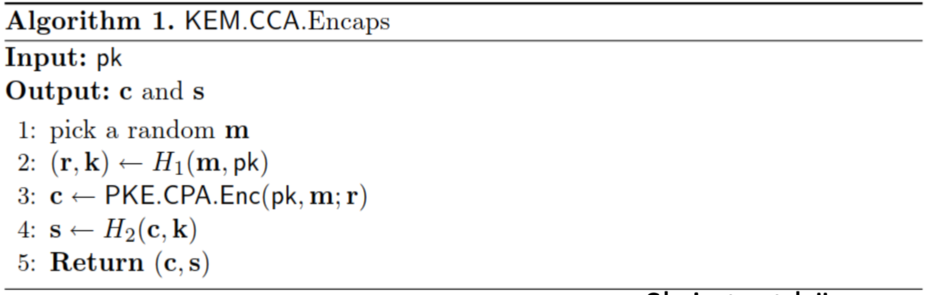
WP3: Selected paper



A Key-Recovery Timing Attack on Post-quantum Primitives Using the Fujisaki-Okamoto Transformation and Its Application on FrodoKEM

Qian Guo[1,2](✉), Thomas Johansson[1](✉), and Alexander Nilsson[1,3](✉)

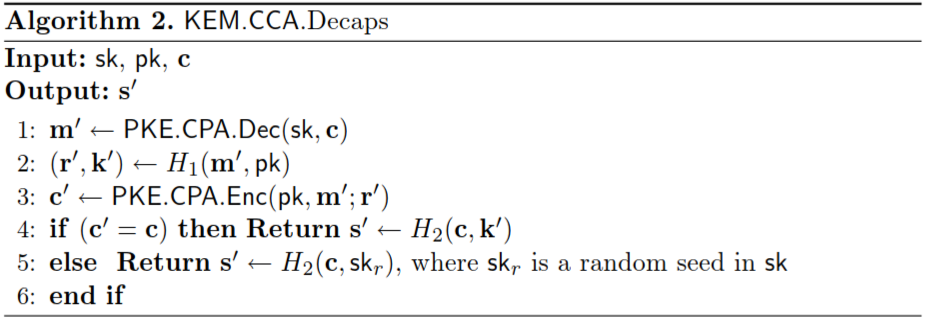
[1] Department of Electrical and Information Technology,
Lund University, Lund, Sweden
{qian.guo,thomas.johansson,alexander.nilsson}@eit.lth.se
Selmer Center, Department of Informatics, University of Bergen, Bergen, Norway
[3] Advenica AB, Malmö, Sweden



Algorithm 1. KEM.CCA.Encaps

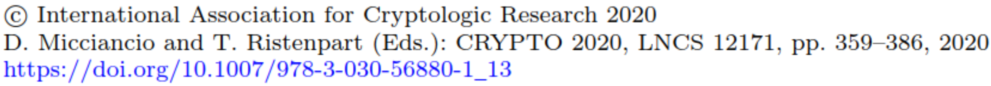
```
Input: $\mathsf{pk}$
Output: $\mathbf{c}$ and $\mathbf{s}$
pick a random $\mathbf{m}$
$(\mathbf{r}, \mathbf{k}) \leftarrow H_1(\mathbf{m}, \mathsf{pk})$
$\mathbf{c} \leftarrow \mathsf{PKE.CPA.Enc}(\mathsf{pk}, \mathbf{m}; \mathbf{r})$
$\mathbf{s} \leftarrow H_2(\mathbf{c}, \mathbf{k})$
Return $(\mathbf{c}, \mathbf{s})$
```

Skriv text här



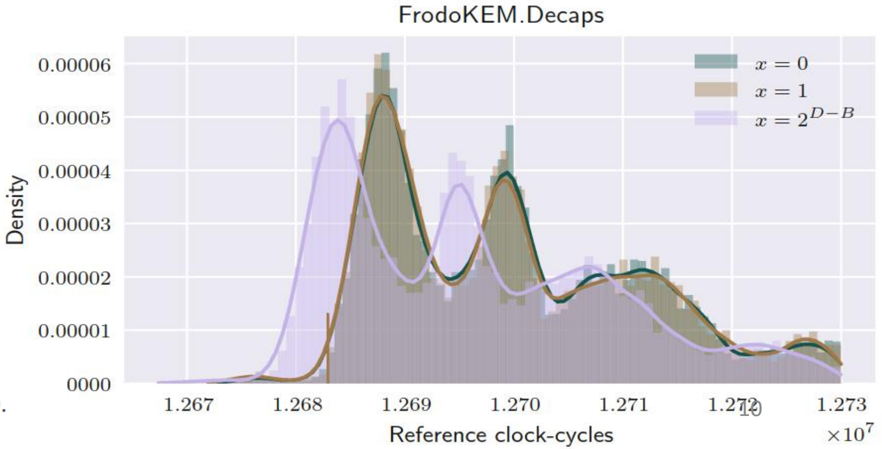
Algorithm 2. KEM.CCA.Decaps

```
Input: $\mathsf{sk}$, $\mathsf{pk}$, $\mathbf{c}$
Output: $\mathbf{s}'$
$\mathbf{m}' \leftarrow \mathsf{PKE.CPA.Dec}(\mathsf{sk}, \mathbf{c})$
$(\mathbf{r}', \mathbf{k}') \leftarrow H_1(\mathbf{m}', \mathsf{pk})$
$\mathbf{c}' \leftarrow \mathsf{PKE.CPA.Enc}(\mathsf{pk}, \mathbf{m}'; \mathbf{r}')$
if $(\mathbf{c}' = \mathbf{c})$ then Return $\mathbf{s}' \leftarrow H_2(\mathbf{c}, \mathbf{k}')$
else  Return $\mathbf{s}' \leftarrow H_2(\mathbf{c}, \mathsf{sk}_r)$, where $\mathsf{sk}_r$ is a random seed in $\mathsf{sk}$
end if
```



D. Micciancio and T. Ristenpart (Eds.): CRYPTO 2020, LNCS 12171, pp. 359–386, 2020.
https://doi.org/10.1007/978-3-030-56880-1_13

- NIST PQ project candidate
- We show how to recover the secret key by feeding the Decaps with special c and then study timing information



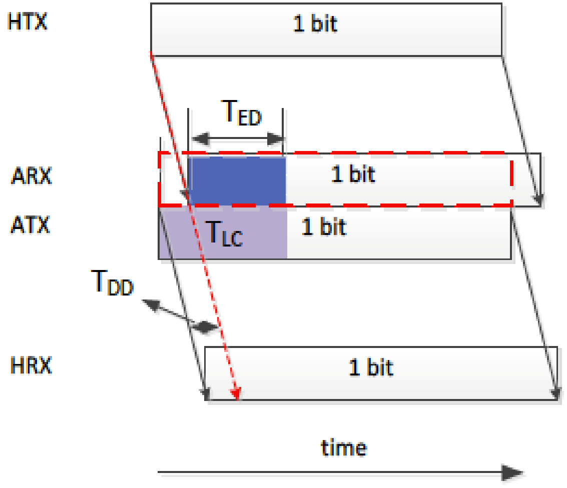
Scientific Results

WP4: Selected paper

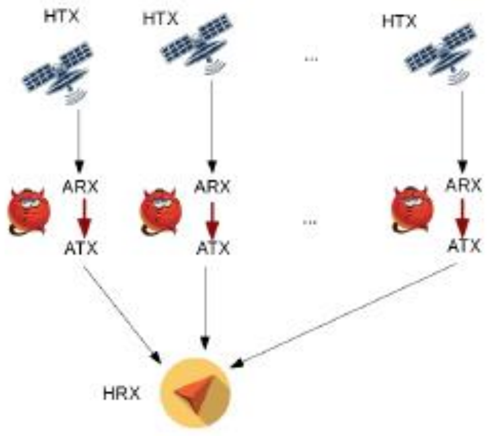
IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS, NOVEMBER 2021

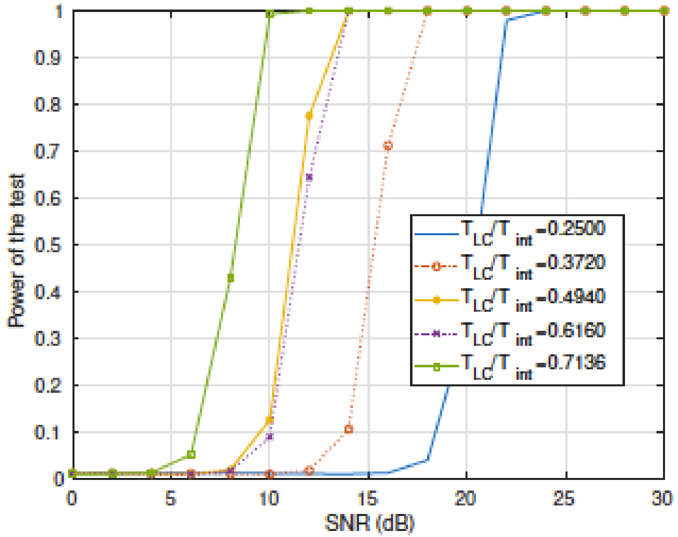
Protecting GNSS Open Service-Navigation Message Authentication against Distance-Decreasing Attacks

Kewei Zhang, Erik G. Larsson *Fellow, IEEE* and Panos Papadimitratos *Fellow, IEEE*



(a) Illustration of DD attack.





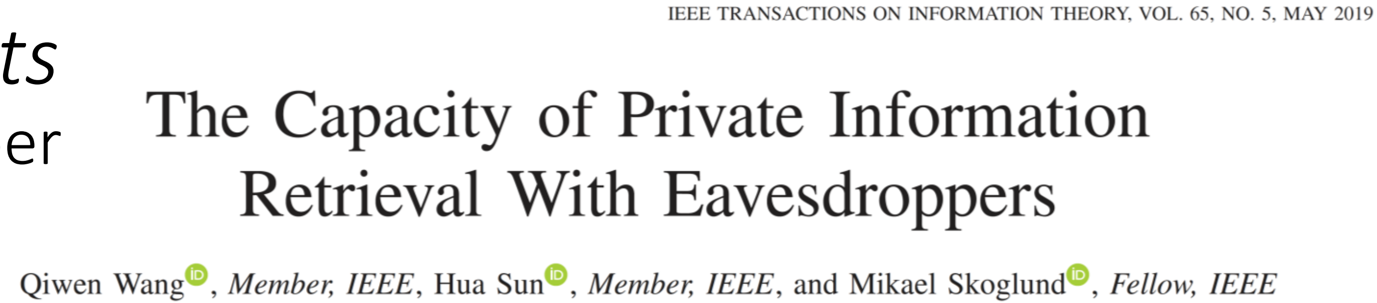
(a) Detection probability with the Shapiro-Wilk test.

(b) Adversary illustration for DD attack on GNSS.

Fig. 1: Distance-decreasing attacks on GNSS signals.

Scientific Results

WP5: Selected paper

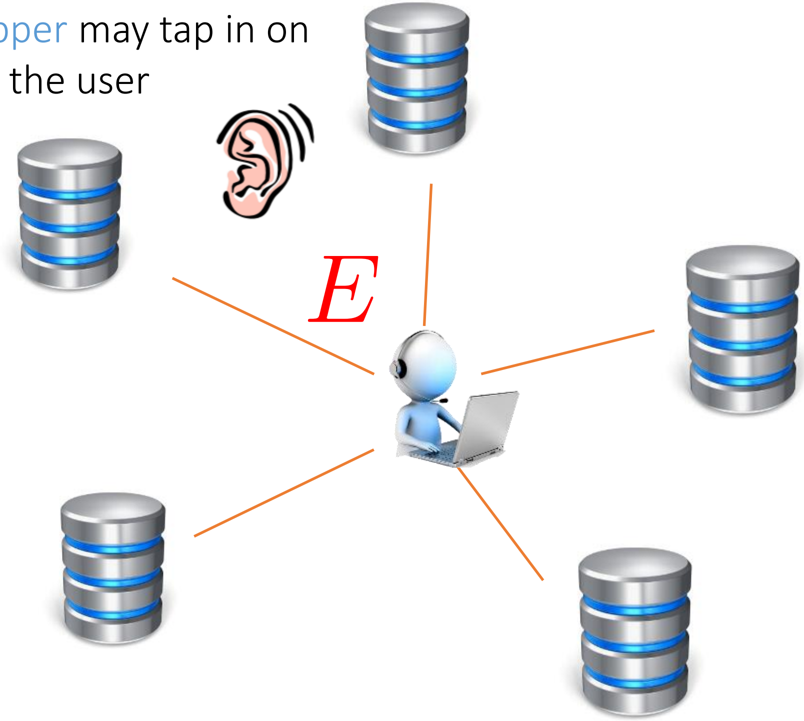


IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 65, NO. 5, MAY 2019

The Capacity of Private Information Retrieval With Eavesdroppers

Qiwen Wang, *Member, IEEE*, Hua Sun, *Member, IEEE*, and Mikael Skoglund, *Fellow, IEEE*

An eavesdropper may tap in on any *E* links to the user



A set of messages stored on multiple servers

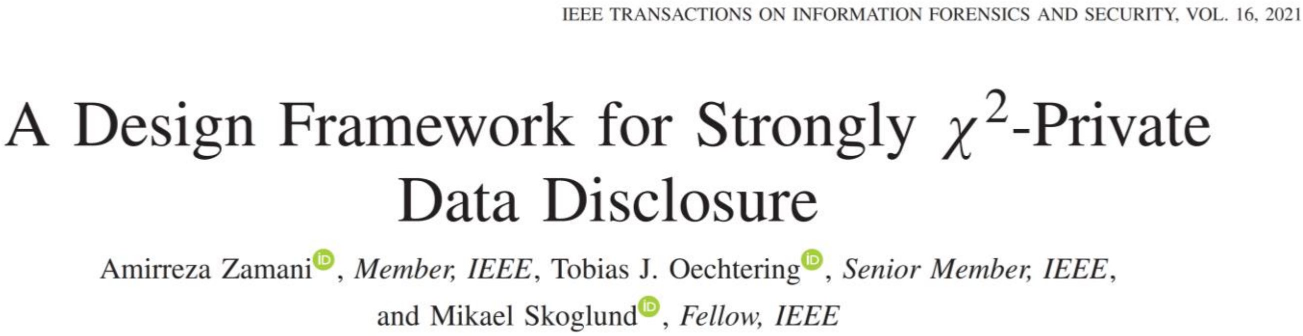
User should be able to download any message without revealing which data is of interest

Naïve approach: download everything

Capacity *C* = maximum number of requested message bits per downloaded bit

Scientific Results

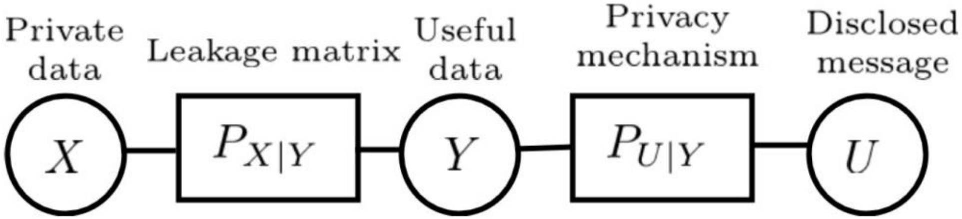
WP6: Selected paper



IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 16, 2021

A Design Framework for Strongly χ^2-Private Data Disclosure

Amirreza Zamani, *Member, IEEE*, Tobias J. Oechtering, *Senior Member, IEEE*, and Mikael Skoglund, *Fellow, IEEE*

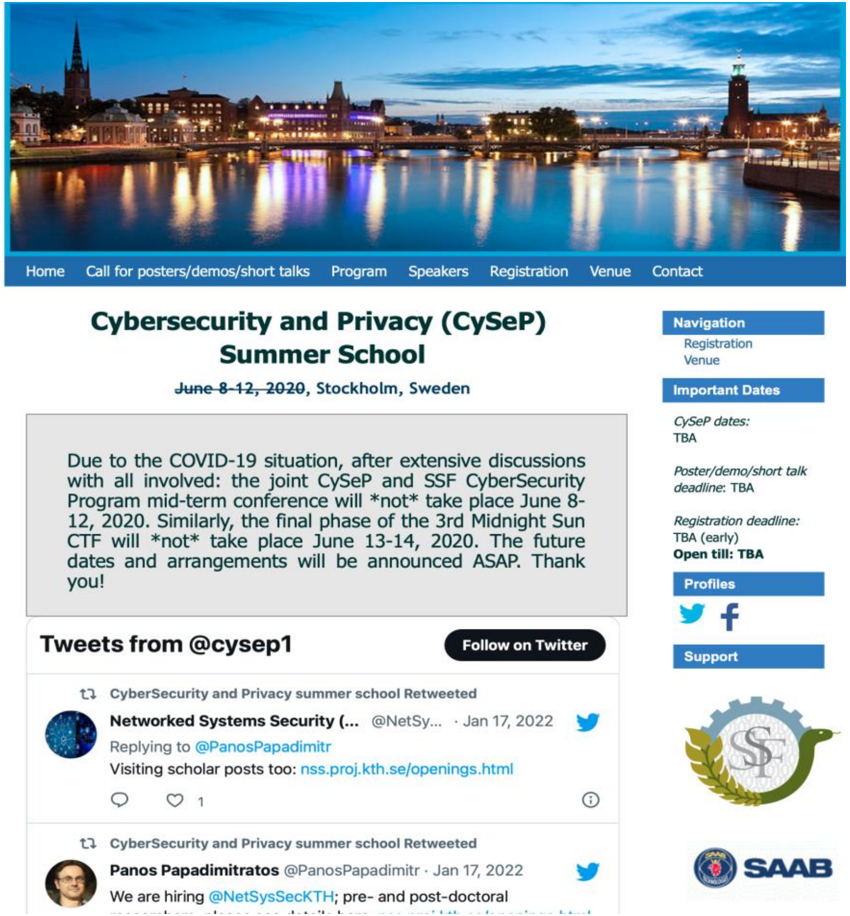


Efficient design framework for privacy mechanisms

Nonlinear non-convex problem approximated by linear program

New designs and geometrical insight

Events



Cybersecurity and Privacy (CySeP) Summer School

~~June 8-12, 2020~~, Stockholm, Sweden

Due to the COVID-19 situation, after extensive discussions with all involved: the joint CySeP and SSF CyberSecurity Program mid-term conference will *not* take place June 8-12, 2020. Similarly, the final phase of the 3rd Midnight Sun CTF will *not* take place June 13-14, 2020. The future dates and arrangements will be announced ASAP. Thank you!

CySeP dates:
TBA

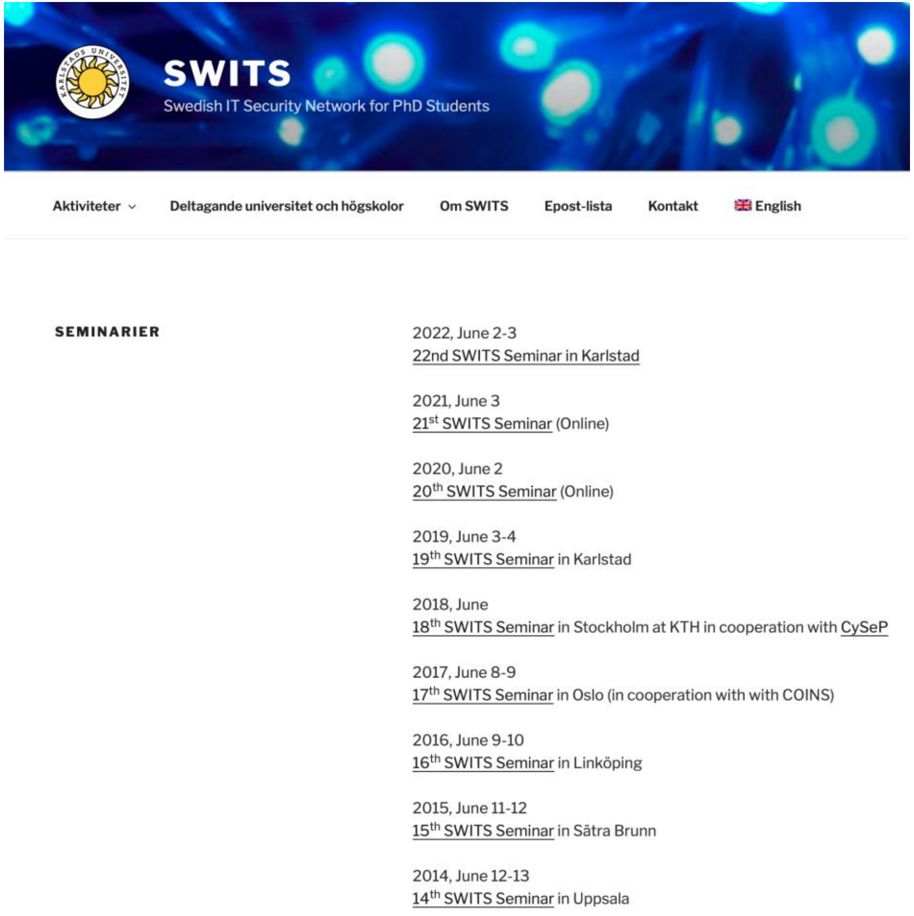
Poster/demo/short talk deadline: TBA

Registration deadline:
TBA (early)
Open till: TBA

Tweets from @cysep1

CyberSecurity and Privacy summer school Retweeted
Networked Systems Security (... @NetSy... · Jan 17, 2022
Replying to @PanosPapadimitr
Visiting scholar posts too: nss.proj.kth.se/openings.html
1

CyberSecurity and Privacy summer school Retweeted
Panos Papadimitratos @PanosPapadimitr · Jan 17, 2022
We are hiring @NetSysSecKTH; pre- and post-doctoral


KARLSTADS UNIVERSITET
SWITS
Swedish IT Security Network for PhD Students
Aktiviteter
Deltagande universitet och högskolor
Om SWITS
Epost-lista
Kontakt
English

SEMINARIER

2022, June 2-3
22nd SWITS Seminar in Karlstad

2021, June 3
21st SWITS Seminar (Online)

2020, June 2
20th SWITS Seminar (Online)

2019, June 3-4
19th SWITS Seminar in Karlstad

2018, June
18th SWITS Seminar in Stockholm at KTH in cooperation with CySeP

2017, June 8-9
17th SWITS Seminar in Oslo (in cooperation with with COINS)

2016, June 9-10
16th SWITS Seminar in Linköping

2015, June 11-12
15th SWITS Seminar in Såtra Brunn

2014, June 12-13
14th SWITS Seminar in Uppsala

Secure and private connectivity in smart environments

Acronym: SURPRISE

SSF Cyber Security Program

Project ID: RIT17-0005

PI: Papadimitratos (KTH)

Co-PIs: Fischer-Hübner (KAU), Johansson (LTH), Larsson (LiU), Skoglund (KTH)

https://nss.proj.kth.se/surprise/