VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kansliets noteringar Kod	Dnr
2014-15355-112991-49	2014-4833

2014
Project Research Grant

Area of science
Natural and Engineering Sciences

Announced grants
Research grants NT April 9, 2014

Total amount for which applied (kSEK)

2015	2016	2017	2018	2019
1107	1121	1173	1197	1288

APPLICANT

Name(Last name, First name)
Sabelfeld, Andrei

Date of birth
741110-8876

Gender
Male

Email address
andrei@chalmers.se

Academic title
Professor

Position
Professor

Phone
0317721018

Doctoral degree awarded (yyyy-mm-dd)
2001-06-08

WORKING ADDRESS

University/corresponding, Department, Section/Unit, Address, etc.
Chalmers tekniska högskola
Institutionen för data-och informationsteknik
Programvaruteknik
Rännvägen 6B
41296 Göteborg, Sweden

ADMINISTRATING ORGANISATION

Administrating Organisation
Chalmers tekniska högskola

DESCRIPTIVE DATA

Project title, Swedish (max 200 char)
Robust decentraliserad plats-sekretess

Project title, English (max 200 char)
DecentLP: Robust decentralized location privacy

Abstract (max 1500 char)

Location based services (LBS) are becoming increasingly popular, ranging from device tracking to vehicle collision detection and to a wide variety of social LBS. As devices become increasingly interconnected, and the majority shares location information with different parties, often unbeknownst the user, it becomes increasingly important that location information can be used without violating user privacy.

While state-of-the-art privacy-preserving techniques make use of pragmatic approaches to obfuscating location data, they largely fall short to provide rigorous privacy guarantees.

DecentLP will build a solid foundation for location privacy. DecentLP will provide unhampered functionality while providing rigorous and robust privacy by means of secure multi-party computation (SMC), where participants can jointly compute a function based on private inputs. While most existing location privacy approaches focus on mitigating information disclosure, DecentLP will remove unintended information disclosure entirely. DecentLP will break away from centralized trust and will enable user privacy while not relying on trust to governments, service providers, or infrastructure owners.

There is an unsettling gap between the two communities dealing with location privacy and SMC. DecentLP will bridge this gap to achieve robust location-privacy by novel, rigorous, and efficient SMC techniques.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-15355-112991-49

Name of Applicant
Sabelfeld, Andrei

Date of birth
741110-8876

Abstract language
English

Keywords

Review panel
NT-2

Project also includes other research area

Classification codes (SCB) in order of priority
10201, 10205,

Aspects

Continuation grant
Application concerns: New grant
Registration Number:

Application is also submitted to

similar to: **identical to:**

ANIMAL STUDIES

Animal studies
No animal experiments

OTHER CO-WORKER

Name(Last name, First name) Mitrokotsa, Aikaterini	**University/corresponding, Department, Section/Unit, Addressetc.** Chalmers tekniska högskola Institutionen för data-och informationsteknik
Date of birth 781008-3662	**Gender** Female
Academic title PhD	**Doctoral degree awarded (yyyy-mm-dd)** 2007-11-12

Name(Last name, First name) ,	**University/corresponding, Department, Section/Unit, Addressetc.**
Date of birth	**Gender**
Academic title	**Doctoral degree awarded (yyyy-mm-dd)**

Name(Last name, First name) ,	**University/corresponding, Department, Section/Unit, Addressetc.**
Date of birth	**Gender**
Academic title	**Doctoral degree awarded (yyyy-mm-dd)**

Name(Last name, First name) ,	**University/corresponding, Department, Section/Unit, Addressetc.**
Date of birth	**Gender**
Academic title	**Doctoral degree awarded (yyyy-mm-dd)**

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-15355-112991-49

Name of Applicant
Sabelfeld, Andrei

Date of birth
741110-8876

ENCLOSED APPENDICES

A, B, B, C, C, N, S

APPLIED FUNDING: THIS APPLICATION

Funding period (planned start and end date)
2015-01-01 -- 2019-12-31

Staff/ salaries (kSEK)

Main applicant	**% of full time in the project**	**2015**	**2016**	**2017**	**2018**	**2019**
Andrei Sabelfeld	20	329	340	351	363	376
Other staff						
Aikaterini Mitrokotsa	5	53	55	57	59	61
PhD student	80	616	636	657	680	703
	Total, salaries (kSEK):	998	1031	1065	1102	1140

Other project related costs (kSEK)	**2015**	**2016**	**2017**	**2018**	**2019**
Travel	20	20	20	20	20
Licentiate and PhD thesis printing			15		50
Computer	20				
Premises	55	56	58	60	62
Direct IT costs	14	14	15	15	16
Total, other costs (kSEK):	109	90	108	95	148

Total amount for which applied (kSEK)

2015	2016	2017	2018	2019
1107	1121	1173	1197	1288

ALL FUNDING

Other VR-projects (granted and applied) by the applicant and co-workers, if applic. (kSEK)

Funded 2014	**Funded 2015**	**Applied 2015**
		5000

Project title	**Applicant**
AppFlow: Putting Information Flow Security to Work	David Sands

Funded 2014	**Funded 2015**	**Applied 2015**
		1000

Project title	**Applicant**
PRECIS: Privacy and Security in Wearable Computing Devices	Katerina Mitrokotsa

Funds received by the applicant from other funding sources, incl ALF-grant (kSEK)

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-15355-112991-49

Name of Applicant
Sabelfeld, Andrei

Date of birth
741110-8876

Funding source	Total	Proj.period	Applied 2015
ERC	15000	2013-2017	

Project title
ProSecuToR: Language-based Security To Rescue

Applicant

POPULAR SCIENCE DESCRIPTION

Popularscience heading and description (max 4500 char)

Platsbaserade tjänster (Location based services, LBS) blir allt mer vanliga. Utbredningen av mobila sammankopplade enheter öppnar enorma möjligheter för tjänster som utnyttjar data om aktörer. Logistikföretag spårar last extensivt genom land, luft och till sjöss. Tillsynsmyndigheter tillämpar spårningsteknik på enheter som bärs av personer såväl som inbäddade i fordon. Konsumenter åtnjuter ett brett utbud av platsbaserade tjänster, från att spåra en borttappad telefon till att söka efter närliggande restauranger eller tweets i närområdet. Däremot ser vi en stadig och bestämd önskan från allmänheten att skydda sin privata data. Detta har blivit uppenbart med fall så som Snowden och WikiLeaks, samt genom anonymiseringsvertyg såsom Tor.

Det är en konstant utmaning för företag att skydda sin mjukvara och sin data. När båda parterna som utnyttjar en tjänst vill bibehålla konfidentialitet uppstår en intressekonflikt, där ena parten måste ge upp sin hemliga data för att tjänsten skall bli funktionell, vilket ger ett mindre värde för en av utövarna. Detta kan innebära att en redovsningsbyrå gör sina program tillgängliga för nedladdning och drabbas av piratkopiering, eller att en konsument måste uppge sin position för att använda en navigeringstjänst.

En stor utmaning är att bibehålla data privat i en LBS utan att minska funktionaliteten genom att göra datan otillgänglig. Medan många sekretess-bevarande tekniker inom LBS använder pragmatiska tekniker och kan uppnå hög nivå av mörkläggning på ett effektivt sätt, är detta inte ett åtråvärt mål från ett kryptografiskt perspektiv. Det går att göra data beräkningsmässigt ouppnåelig för obehöriga, och med hjälp av säkra flerparts beräkningar (Secure Multiparty Computation, SMC).

I sin helhet har projektet som mål att skapa en solid grund för plats-sekretess, där säkerhet garanteras för varje deltagare utan tillförlit till en central myndighet. Vi ämnar se till att varken myndigheter, tjänsteleverantörer, eller infrastruktursägare har möjlighet att inskränka på personers privatliv, om detta är ett nyckelkoncept för en applikation. Där många existerande läsningar strävar att göra onödiga informationsläckor små, vill vi se till att de är obefintliga. Projektet kommer att luta på solida grunder inom kryptografisk verifiering, där löften, och inte endast förhoppningar baserat på tillit (trust), kan ges till användare. Detta är något som hittills är ytterst sällsynt för LBS och närliggande områden.

Vi ämnar brygga de två områdena SMC och sekretess-bevarande LBS. Utövare inom SMC är vana att ge robusta lösningar på abstrakta problem, vilket måste kombineras med expertis inom specifika ämnesområden, för att visa hur resultat från båda riktningarna kan sammanflätas i framgångsrika projekt som ger lösningar med praktiska tillämpningar.

Vi kommer påvisa svagheter i existerande protokoll inom LBS, som uppenbarar sig när man applicerar dem i verkligheten. Detta på grund av att det är vanligt att man modellerar begränsade angripare, som inte korrekt återspeglar verkliga scenarion. För att underlätta analys av LBS protokoll, kommer projektet leverera ramverk för verifiering av sekretess-bevarande LBS. Ramverket kommer att möjliggöra att inte endast specifika protokoll, utan alla protokoll i samma kontext, kan verifieras och mätas med samma mått. Projektet kommer att skapa tillämpningar av SMC inom LBS för att leverera konkreta, nydanande lösningar som kan garantera robust sekretess och säkerhet utan en central auktoritet. Existerande lösningar tillämpar oftast statiska scenarion, där varken angripare eller offer rör på sig, och där man bara garanterar säkerhet utan upprepning av ett protokoll. Vi uppmärksammar att korsningen vissa metoder för SMC och sekretess-bevarande LBS är ett ytterst outforskat område, där projektet har goda möjligheter att leverera inflytelserika resultat.

För att möjliggöra projektets framgång måste nya komponenter tas fram, som kan kombineras med mer generiska SMC-tekniker så att lösningen som helhet är effektiva nog för att användas i verkliga scenarion. Detta är något som blir allt vanligare för sekretess-bevarande metoder. Alla SMC-komponenter som används i projektet kommer att verifieras för att säkerställa lösningars robusthet. Detta skall utföras på ett sätt så att bevismaterial kan återanvändas i framtida projekt.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-15355-112991-49

Name of applicant
Sabelfeld, Andrei

Date of birth
741110-8876

Title of research programme
DecentLP: Robust decentralized location privacy

Appendix A

Research programme

1. Motivation

Location based services (LBS) are becoming increasingly popular. The ubiquity of mobile interconnected devices opens up tremendous opportunities for services that utilize location information. A single online resource features 1504 companies within LBS at the time of writing [LLC14]. Logistics companies make extensive usage of tracking the location of cargo throughout the land, sea, and air. Enforcement authorities exercise location tracking technology for devices carried by people and embedded in vehicles. Individual users enjoy a wide range of location-based services from tracking a lost phone to querying for nearby restaurants or nearby tweets.

There has been a steady increase of the awareness of the public when it comes to protecting their privacy. This has become very obvious with cases such as Snowden [WSG13] and the Tor project [DMS04]. In practice, it is by far more common that the end consumer has to send privacy-sensitive information about their location to a location based service, than that the service works hard to provide the user with privacy. A major challenge is to address the privacy of LBS without hampering the functionality of the services, as voiced by recent surveys [Kru09, Ter11].

Motivated by this challenge, our project, *DecentLP*: Robust *Decent*ralized *L*ocation *P*rivacy, aims to provide unhampered functionality without compromising privacy through means of *secure multi-party computation (SMC)*, where participants can jointly compute a function based on private inputs. SMC was historically initiated by largely theoretical investigations, but during later years has gained much towards being practically applicable [HEKM11, GSW13].

While state-of-the-art privacy-preserving techniques make use of pragmatic approaches to obfuscating location data, they largely fall short to provide rigorous privacy guarantees. In contrast, it is possible to make data computationally unobtainable using SMC techniques. Currently, there is an *unsettling gap* between the two communities dealing with SMC and location privacy. Bridging this gap is an important motivation for *DecentLP*. We take up the challenge to achieve robust location-privacy, and will do so by *novel, rigorous, and efficient SMC techniques*, showing how the fields can be fruitfully cross-pollinated to achieve robust and practical location privacy.

2. Significance

As devices become increasingly interconnected, and the majority shares location information with different parties, often unbeknownst the user, it becomes increasingly important that location information can be used without violating the users' privacy. The internet as a whole often employs trust in a central authority to ensure privacy. A prime example is SSL certificates, governed by central authorities. However, due to the severe breaches of certificate authorities in recent years [Lea11], this approach has asserted its weaknesses firmly in the minds of the security community. It is highly desirable to break away from centralized trust and develop systems with *decentralized* security.

In practice, the privacy of users are often neglected if there are no standard solutions to problem at hand. An illustrative attack on a dating service has been recently detailed by Include Security [Vey14]. From the public API of a LBS it was possible to find the exact position of an arbitrary user as the distance between principals were disclosed as a part of the service, and positions were easy to spoof. In a similar vein, the smartphone app *Girls around me* allowed users to find other users (profiled as female) who recently had checked in on Foursquare (a popular LBS) [Col12]. This was deemed as a serious privacy violation, and the app had since been banned from using the Foursquare API and removed from the app store.

An early example of robust privacy-preserving techniques in practice is during a sugar beets auction in Denmark, which clearly indicates that participants prefer privacy when they have the option to choose it [BCD+09]. When it comes to location privacy, users are sometimes willing to give away their location information [AEG+07, BKS10]. However, location privacy can be highly sensitive, as shown in the above scenarios. There is a trade-off between utility and privacy, where often using the service is judged more important than keeping private information hidden. We argue that this fact does not in any way lessen the importance of privacy, it simply shows that users are keen to use the service. Further, since it has hitherto not been possible to easily deploy privacy-preserving LBS, we conjecture that such approaches will be increasingly popular as they apply to more applications.

3. Goals

Motivated by the above, we propose to create a solid foundation for location privacy. We emphasize two different key points to improve location privacy: *decentralization* and *robustness*. Privacy must be guaranteed for each participant without a central authority, and any guarantees must be based on formal soundness proofs. The aim is that neither governments nor service providers or infrastructure owners may be able to compromise user privacy, when privacy is paramount for the application or the user. While most existing approaches focus on mitigating information disclosure, the aim of this work is to remove unintended information disclosure entirely.

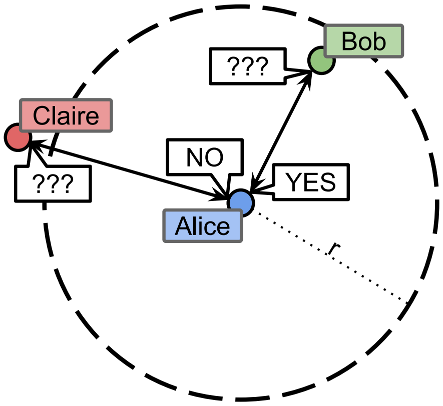


Figure 1: Information disclosure in a proximity protocol

Privacy-preserving location based services For a single information location disclosure, i.e. a single run of a protocol within a LBS, no more information than the result of the service must be disclosed. E.g. when the closest coffee shops is requested, *no* other information is disclosed regarding positions nor distances. Only the requesting party learns anything at all, and the coffee-shops and service provider remains oblivious about the requesting party's position. A popular example of a LBS is a *proximity* service which can be used in a wide range of applications, from collision detection between vehicles to checking if two friends are close to each other. Figure 1 illustrates the information disclosure for a proximity protocol, where Alice queries Bob and Claire to find out whether they are nearby or not. The intended information release is only the proximity result. Claire and Bob will allow Alice to learn whether they are nearby, but no principal wants to disclose their exact position, velocity, nor the relative distance between either pair of principals. Alice learns that she is near Bob but not near Clair, but Bob and Claire must learn nothing except that they have been queried by Alice.

For consecutive information disclosure, the total information disclosure will always be larger than an individual release. However, the release policy must be strictly adhered: if a single query discloses *distance*, it must be impossible to compute the *position* from any set of queries.

Decentralized location privacy As mentioned earlier, it is vital that users are relieved of having to trust an authority. Their privacy must be guaranteed by the design of the system, and not be based on the good will of any single party or group of participants. There is great potential to construct such schemes via SMC techniques, the key challenge lies in building solutions that are both practical and secure. *DecentLP* will explore the full range of trade-offs with respect to privacy, performance, and ease of deployment to enable users with rich yet secure services.

While there are obvious benefits in studies regarding secure computations in the generic case, such approaches are more complex and results are hard to guarantee. *DecentLP* will identify vital parts where SMC forms a bottleneck, and at such points evolve new techniques by both improving on existing schemes or devising novel protocols. Such points can be found as isolated problems within location privacy, as well as specific problems within secure multiparty computations.

Robust privacy guarantees As discussed below, the state of the art has a wide spread in the amount of rigor put into the security considerations. *DecentLP* will develop a robust foundation for privacy-preserving techniques for LBS by providing *game-based proofs* [Sho04] for groups of protocols. Game-based proofs are precise mathematical descriptions of the interaction between an adversary and a system. Such proofs yield exact definitions as to what guarantees are granted if the proofs hold for a protocol instance. A benefit of game-based proofs is that they are particularly suitable for machine-verification [Hal05, BGHB11]. Such verification yields high confidence in the evaluated constructs, and is the state of the art in protocol verification. Another benefit is that the proofs are reusable and composable, meaning that the effort of producing the proofs can be amortized in subsequent work.

4. Survey of the field

Privacy-Preserving Location-Based Services

There are a multitude of approaches overviewed in recent surveys [Kru09, Ter11] on location privacy. There are two main types of location privacy, where either the LBS can be prevented from learning the identity of the users while giving away location data, or the service can be allowed to know the identity and be prevented from learning usable location data. When protecting the identity of the user, the locations and movements of users can be disclosed, but the aim is that the identity of any specific user must remain unknown, such an example can for example be a heat-map showing where traffic is dense during any time of the day. An example of a scenario where users' location can be secret while their identity does not have to be, is when a principal queries a service for the closest sushi restaurant.

DecentLP focuses on computational approaches which protects location information, where the service is *unable* to intrude on location privacy, rather than being *unwilling*, as may be an affect of societal approaches and reliance on trust. In all cases, we assume that some information about the identity can be known, but that the location must remain secret.

Many simple approaches to location privacy are based on obfuscating a principal's position. Such techniques will often decrease the usability of the service due to the introduction of inaccurate results. A major challenge to be addressed by *DecentLP* is to provide precise results without unnecessary information disclosure, which can be accomplished using cryptographic techniques.

One round-trip solutions For the proximity problem, the literature includes approaches with varying levels of performance, communication overhead, privacy, precision, and trust assumptions [ZGH07, vTSY10, NTL$^+$11, PWS$^+$14]. Table 1 summarizes the different properties of these protocols. A *precise* protocol can (granted enough computational power) give proximity verdicts without false positives and false negatives. A *decentralized* protocol does not rely on a third party. A *privacy-preserving* proximity protocol has no output (no leakage) except the proximity result. Current state of the art does not provide a solution across all these categories.

Table 1: Comparison of proximity protocols

Protocol	Precise	Decentralized	Privacy-preserving
Narayanan 2 [NTL$^+$11]			
Narayanan 1,3 [NTL$^+$11]		X	
Pierre[ZGH07]		X	
Louis[ZGH07]	X		X
Lester[ZGH07]	X	X	
VicinityLocator[vTSY10]	X		X
LocX[PWS$^+$14]	X		X

The *closest POI* (point of interest) problem, also commonly referred to as the *k nearest neighbor* problem is a common example of a LBS, where users for example want to find the three coffee-shops closest to their current location. None of the approaches from the literature [KSMS13, PLW13], is both practical, privacy-preserving, precise, and free of a trusted third party.

Multi-run security When a location-based service is queried multiple times, it may not enough to introduce uncertainty about the positions of the principals, as multiple queries will create overlapping possible areas, and thus reduce the possible position of the victim. When the attacker has knowledge of the maximal velocity of the victim, there are several approaches proposed [CZBP06, YLL^{+}12]. Hashem et al. improve on this by also allowing partitions to overlap and thus increasing the precision of the service slightly [HKZ13]. All current solutions have in common that they add a larger uncertainty region, meaning that they decrease the precision of the service with subsequent requests, in order to improve privacy.

Secure Multiparty Computation

Rivest et al. introduced the idea of remote host computation, where they imagined that homomorphic encryption would enable such systems [RAD78]. Remote computations on private data was later formalized as secure multiparty computation [Yao82], and solved through secret sharing in 1979 by Shamir [Sha79], and garbled circuits in 1982 by Yao [Yao82], but not until 2009 through fully homomorphic encryption by Craig Gentry [Gen09]. Two distinct areas that currently dominate the SMC scene are *homomorphic encryption* and *garbled circuits*. Homomorphic encryption can compute arithmetic integer operations in constant time with respect to the size of the operands. Garbled circuits is often faster for more complex functions where variable size is small and fixed. There is active and accelerating research in both fields, and which solution to choose is typically application-dependent [LEB13, KSS13]. SMC techniques can be augmented with *verifiable computing* [GGP10, SMBW12] to allow Alice to verify Bobs computations without being privy to them, meaning that Bob cannot lie to Alice without being discovered.

Homomorphic encryption Homomorphic encryption exists only within public-key cryptography, and allows computing a function in the plaintext while only holding knowledge about ciphertexts. Usually, a homomorphic scheme can either compute additions or multiplications in the plaintexts. A fully homomorphic scheme is able to compute both additions and multiplications. Several schemes have been presented which in some sense perform better than Gentry's original [BGV11, HEKM11, GSW13], but none which is comparable in performance and space requirement to the schemes that are only additively or multiplicatively homomorphic [Sen13]. However, while fully homomorphic encryption allows evaluation of an arbitrary function, a scheme that is only additively or multiplicatively homomorphic does not.

Garbled circuits Garbled circuits was introduced by Yao [Yao82] to allow two principals to compute a function based on inputs from both sides, and only disclosing the result. The approach works with symmetric cryptographic primitives, and is therefore in many cases more efficient than homomorphic encryption. However, it is not always faster for simple arithmetic operations, where additively and multiplicatively homomorphic schemes often perform better. Since Yao's original protocol, many improvements have been proposed. Garbled circuits can now incorporate more than two parties, and are significantly more efficient. Many promising results have been presented [KS08, HEKM11, KhS12].

5. Project description

We identify areas within location-privacy where principals currently are not afforded enough privacy guarantees, including verification of such protocols, single-run guarantees as well as multi-run guarantees. Further, because the current practices are often not efficient enough, we will pursue development of novel, efficient SMC techniques and verification of all SMC constructs used.

Privacy-Preserving Location-Based Services

Threats to privacy-preserving LBS Much of the current work lacks formal attacker models or focuses only on limited attackers, such as the *honest-but-curious* attacker model [Gol04]. While there are some advances in the field, more realistic attacker models are needed. *DecentLP* will scrutinize existing work for threats from realistic attackers. We expect rich findings due to the informal nature of many approaches to LBS. We have already discovered some concrete attacks, as reported in Section 6, where we can alter the format of a message and gain more than the intended amount of location information. We expect to unveil further vulnerabilities and attacks by evaluating existing protocols using rigorous proof techniques. Wherever we expose vulnerabilities, significant effort will be made to provide means to rectify errors where possible.

Verifying Privacy-Preserving Location Protocols There is a need to define more rigorous frameworks to verify that a protocol respects the privacy requirements of every principal. Much work in the area lacks formal proofs. *DecentLP* will accomplish verification of a protocol security via semi-automatic verification of cryptographic games. We will develop a *general framework* for location protocol verification, that can be applied not only to specific protocols, but to an entire family of protocols. Such verification frameworks will help clarify exactly what a given protocol protects against, and help position different work towards each other in terms of privacy guarantees as they will be able to be evaluated using identical metrics.

It is vital that there is no ambiguity as to what kind of errors can be introduced if a real world attacker is more powerful than the one that has been evaluated by the designers of a protocol. The outcome of this project will allow precise reasoning about what kind of adversary (if any) a protocol protects against, be it an honest-but-curious attacker or a malicious adversary, or any shade in-between the two. To have precise delimitations and assurances is critical for any result to be useful; this is especially important when talking about secrecy of highly sensitive data.

Practical Location Privacy Verification procedures are of little use when privacy-preserving techniques are not applicable in real-world applications. There is a much after-sought need to apply existing concepts to real-life applications, and to show how they can be used. *DecentLP* will develop novel practical solutions that can guarantee robust privacy in an decentralized manner. Significantly improving the state of the art (cf. Table 1), we will construct protocols with no centralized trust, where rigorous formal proofs will be provided, precisely showing what is guaranteed under which circumstances. We will present novel solutions to both the proximity and the k nearest neighbor problems, by utilizing modern SMC, and without applying imprecise obfuscation techniques.

As an illustration of a concrete track, recall the proximity problem, where Alice wants to know if Bob is nearby, i.e., within some radius r. Our protocols for proximity will use homomorphic encryption to compute the squared distance, and then for every value i from 0 to r^2 (ignoring values that do not have an integer square root) test whether the squared distance is equal to i using blinded multiplication techniques. We will prove that the principals may only learn whether they are in each others' proximity and no further information about their locations or the distance between the principals. We will show that third-party observers learn no useful information related to the location of the principals. We will develop an asymptotic analysis together with practical experiments of several instances of the protocol using different encryption schemes. Based on preliminary studies (elaborated in Section 6), we are confident that we will be able to demonstrate that our approach scales well to practical applications.

Dynamic Location Privacy Most current approaches yield protection within a single round of the protocol, as described in the previous section. This approach works for static scenarios where principles do not move. Dynamic location privacy addresses scenarios with principals that might move. The problem has been studied in two directions, where either the attacker or the victim is moving, studying different countermeasures.

When the moving party is the attacker, and the victim is stationary, using any partition of the space where each section is large enough to satisfy the victims privacy requirements is a good strategy [NTL$^+$11], though it incurs a large imprecision for the service. The victim can then never reveal more information than what partition it is located within. Cuellar et al. show why this is largely insufficient when the victim is moving [COR12]. A fundamental, largely open, problem is how to react to an attacker if both the victim and a suspected attacker has firm privacy requirements. That is, the attacker may be a user of a system to the same degree as the victim.

DecentLP will provide privacy for LBS services when both the attacker and the victim can move. We will leverage the synergies with homomorphic encryption, where the victim may use information about the attacker's movements without being privy. We envision high potential for homomorphic encryption to facilitate multi-run privacy preserving LBS techniques, and expect high-impact results in this direction.

Secure Multiparty Computation

Efficient specific SMC Using modern techniques there is an abundance of opportunities to combine the generality of garbled circuits with the efficiency of special-purpose functions based on homomorphic encryption. By constructing efficient homomorphic protocols that solve parts of an LBS-problem, fully-fledged application can be constructed where only minor parts are hampered by inefficient, general solutions.

In the scope of location privacy, it is often the case that geometric calculations take place which promotes algebraically efficient operations. The result is often followed by comparisons, or operations that piece algebraic results together, which promotes solution that are also efficient for non-algebraic operations. Such approaches are becoming more and more common; Sadeghi et al. present an approach to perform privacy-preserving face-recognition, where they apply methods that also are usable within location privacy. The approach first computing eigenvectors using additively homomorphic encryption, followed by computing the minimum value amongst the eigenvectors using garbled circuits [SSW10].

DecentLP will isolate and present each SMC construction used for specific problems separately, to be reusable by the community as a whole. In this context, comprehensive benchmarks with as much external validity as possible is of high value, to position each contribution clearly and help other researchers choose what to reuse, improve, or re-innovate.

Verification of SMC components Privacy-preserving techniques do not always properly verify every part of the solution. This is a grave mistake that can in practice render much subsequent research susceptible to serious intrusions, and is a direct effect of proofs not being reusable and easily composable. An example is the common usage of multiplication by a random number as a blinding technique. It is often assumed that the product of a generator of a group and a uniformly random number is another uniformly random number within the same group. However, this is not the case if the group also has subgroups. For instance, this approach does trivially not work with the Paillier [Pai99] cryptosystem (where the plaintext space has two subgroups), which is one of the most widely used additively homomorphic systems.

When designing protocols for specific applications, the designer wants a repository of concise constructions allowing each operation to be performed in a way that is *at least* as secure as required by the application. Machine verification of protocols can be made a much less time-consuming task if each building block is previously verified. Composable proofs to be reused in future endeavors is a valuable commodity for the cryptographic community. To this end, *DecentLP* will drive a rich research agenda on provable security. Not only will we develop proofs for our protocols as such, but we will device a modular and general proof framework for succinct constructions common in privacy-preserving applications. We envision that such efforts will have long-lasting impacts within several fields, not only location privacy.

Practical demonstration and Case studies

To evaluate our results, both towards investigating how easily they can be deployed, but also how efficiently they perform in a full-scale application, we will implement applications in their entirety. A key point is to show that SMC techniques can be used in two orthogonal directions. In part, to demonstrate the effectiveness with which we can execute privacy-preserving applications and show that these methods can become practical, which is important for outreach to industry and society. But also, it is important to show researchers and practitioners within other fields *how* to use them. Not only to exemplify implementation efforts, but also to show how to *declassify* precise location data in a robust manner [MSZ04], taking into account cryptographic primitives [AHS08]. It is vital that the implementation naturally connects to application security and gives rigorous control over *what* information is released, *who* releases information, *where* in the system information is released, and *when* information can be released [SS09].

We will develop practical applications based on our LBS protocols, leveraging the HTML5 geolocation API to provide positioning service for end users. Using such technologies, the implementation will be available both to web browsers and as embedded web applications in mobile devices [LGW13], being applicable in a wide range of scenarios. Our track record in application and web security [MAS10, HS12], gives us confidence in the success of this track.

6. Preliminary Results

Preliminary results uncover vulnerabilities in the published protocols and make initial progress on a robust framework for decentralized location privacy. Current state of the art, as described previously, does not employ full privacy-preserving protection for the user, either by design or by employing weak attacker models. Current approaches often employ impractically weak attacker models. When analyzing the literature on the subject, we have found several published approaches (e.g. ,[ZGH07, EFG^{+}09, SSW10]) where format attacks may cause a victim to disclose unwanted information. Some information derived from a principal's (call them Alice) information is assumed to be sent to a responding principal (call them Bob) of, but in the context where Bob receives them, he has no way of verifying Alice's information. We explain one of the discovered vulnerabilities of this type in a bit more detail. Zhong et al. [ZGH07] present three protocols (called *Louis*, *Lester* and *Pierre*) that use homomorphic encryption to create proximity protocols. Alice sends an aggregate of her coordinates (x, y) (the encryption of $2x$, $2y$, and $x^2 + y^2$, respectively) to Bob. We observe that a real-world attacker (in the role of Alice) may be dishonest and send data such that it does not correspond to a point in the plane. Alice can in reality create a proximity check around any point in the plane, of any size. The three protocols, however, assume that Bob knows the size of the area being queried. This implies that Alice can check, for example, whether Bob is in his office, while Bob thinks she will only learn whether he is in town.

We have obtained preliminary results towards an SMC protocol to make use of complex inputs through which we will provide remedies for protocols such as those mentioned above. We have initiated work on a framework for rapidly verifying proximity protocols, expressed in pWhile [BGZB09], and will be able to machine-verify an entire family protocols using this framework without significant added work per protocol. Towards a privacy-preserving, decentralized, and precise proximity protocol, we have preliminary results for a one round-trip solution which outshines the accomplishments of the work listed in Table 1, achieving all of privacy-preservation, decentralization, precision, and practicality. At its core, the protocol relies on a novel SMC technique, allows us to obtain a general technique of homomorphically computing $\leq$: when proximity is defined by being within radius r, it uses homomorphic encryption to compute the squared distance, and then for every value i from 0 to r^2 (ignoring values that do not have an integer square root) test whether the squared distance is equal to i using blinded multiplication techniques.

Our preliminary results on formalizing the protocol in pWhile give us full confidence that will be able to verify the security of the protocol using game-based proofs. We will prove that the principals may only learn whether they are in each others' proximity and no further information about their locations or the distance between the principals. We will show that third-party observers learn no useful information related to the location of the principals. Our preliminary studies of asymptotic complexity and experiments with early prototypes indicate that our approach has high potential to scale well in practice.

We have a strong track record and solid preliminary results on secure application support for cryptographic primitives. We have already built semantic framework for cryptographic primitives in code [AHS08] and conducted case studies on secure implementation of sophisticated cryptographic protocols [AS05].

7. Collaboration

Being a world-class authority in a range of areas from foundational security to web security, we are confident that our research group fits well with the topic of the project.

Further, we have strong ties to distinguished researchers both in location privacy, secure multiparty computation, and machine-verified cryptographic proofs.

On the heels of WebSand, a successful EU project on web application security, we have initiated collaboration with *Jorge Cuellar*, senior security advisor at Siemens, who is behind prominent research [COR12, RCL12] and standardization work [STM$^+$07, STC$^+$13] in location privacy. Work with Jorge will address the exploration of trade-offs between trust and performance, boosting the performance of protocols with lightweight trust assumptions (semi-trusted third parties). We expect publications in top venues, as well as patents and new standards to emerge from this collaboration.

We have collaborators in place with versatile cryptographic background that ranges from applied cryptography to machine-verified cryptographic proofs. The co-applicant of this proposal, *Katerina Mitrokotsa*, a freshly recruited Assistant Professor at Chalmers, has diverse background in applied cryptography including work on location privacy [MOV13] and distance-bounding protocols [BMV12, BMV13].

Cedric Fournet, our collaborator at Microsoft Research, has recent track record on computationally security by compilation, showing how programs written in high-level languages can be compiled to low-level languages with cryptographic primitives to guarantee computational security [FP11, FSC$^+$13]. Some of Cedric's recent work involves secure multi-party computation [FPR11].

Trough an earlier EU project Mobius, we have started collaboration with *Gilles Barthe* [BRRS10] at IMDEA Software, who also recently started collaboration with Cedric [BFG$^+$14]. Gilles is known for seminal results in the area of machine-verified cryptographic proofs. We will use cryptographic games [BGHB11] in the formalization of our protocols, which makes them directly suitable for machine-verified proofs. Gilles has already expressed strong enthusiasm to machine-check our security proofs for location privacy.

Together with Jorge, Katerina, Cedric, and Gilles, we plan to organize a *Dagstuhl Seminar on Robust Location Privacy.* The seminar will facilitate systematization of the area and, if this project is granted, it will be an excellent medium to disseminate the project's results.

Other VR grant applications Andrei Sabelfeld is a co-applicant on a framework grant proposal *AppFlow: Putting Information-flow Security to Work*, together with David Sands and Alejandro Russo. The proposal is on language-based techniques for securing information flow in applications written in object-oriented and functional languages with the focus on JavaScript, Java, and Haskell. The framework grant proposal is orthogonal to the topic of *DecentLP*.

Similarly, Katerina Mitrokotsa's VR application on *PRECIS: Privacy and Security in Wearable Computing Devices* is complimentary to *DecentLP*. The project focuses on the development of a unifying framework for accurate and privacy-preserving authentication in wearable computing, and so there is no overlap with *DecentLP*.

References

[AEG+07] Shane Ahern, Dean Eckles, Nathaniel Good, Simon King, Mor Naaman, and Rahul Nair. Over-exposed?: privacy patterns and considerations in online and mobile photo sharing. In Mary Beth Rosson and David J. Gilmore, editors, *CHI*, pages 357–366. ACM, 2007.

[AHS08] A. Askarov, D. Hedin, and A. Sabelfeld. Cryptographically-masked flows. *Theoretical Computer Science*, 402:82–101, August 2008.

[AS05] A. Askarov and A. Sabelfeld. Security-typed languages for implementation of cryptographic protocols: A case study. In *Proc. European Symp. on Research in Computer Security*, volume 3679 of *LNCS*, pages 197–221, September 2005.

[BCD+09] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas P. Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael I. Schwartzbach, and Tomas Toft. Secure multiparty computation goes live. In Roger Dingledine and Philippe Golle, editors, *Financial Cryptography*, volume 5628 of *Lecture Notes in Computer Science*, pages 325–343. Springer, 2009.

[BFG+14] Gilles Barthe, Cédric Fournet, Benjamin Grégoire, Pierre-Yves Strub, Nikhil Swamy, and Santiago Zanella Béguelin. Probabilistic relational verification for cryptographic implementations. In Suresh Jagannathan and Peter Sewell, editors, *POPL*, pages 193–206. ACM, 2014.

[BGHB11] Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and Santiago Zanella Béguelin. Computer-aided security proofs for the working cryptographer. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 71–90. Springer, 2011.

[BGV11] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. Fully homomorphic encryption without bootstrapping. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:111, 2011.

[BGZB09] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. Formal certification of code-based cryptographic proofs. In *Proceedings of the 36th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, POPL '09, pages 90–101, New York, NY, USA, 2009. ACM.

[BKS10] A. J. Bernheim Brush, John Krumm, and James Scott. Exploring end user preferences for location obfuscation, location-based services, and the value of location. In Jakob E. Bardram, Marc Langheinrich, Khai N. Truong, and Paddy Nixon, editors, *UbiComp*, ACM International Conference Proceeding Series, pages 95–104. ACM, 2010.

[BMV12] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. On the pseudorandom function assumption in (secure) distance-bounding protocols - prf-ness alone does not stop the frauds! In Alejandro Hevia and Gregory Neven, editors, *LATINCRYPT*, volume 7533 of *Lecture Notes in Computer Science*, pages 100–120. Springer, 2012.

[BMV13] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Secure and lightweight distance-bounding. In Gildas Avoine and Orhun Kara, editors, *LightSec*, volume 8162 of *Lecture Notes in Computer Science*, pages 97–113. Springer, 2013.

[BRRS10] Gilles Barthe, Tamara Rezk, Alejandro Russo, and Andrei Sabelfeld. Security of multithreaded programs by compilation. *ACM Trans. Inf. Syst. Secur.*, 13(3), 2010.

[Col12] Devin Coldewey. ”girls around me” creeper app just might get people to pay attention to privacy settings. TechCrunch, March 2012.

[COR12] Jorge Cuéllar, Martín Ochoa, and Ruben Rios. Indistinguishable regions in geographic privacy. In *SAC*, pages 1463–1469. ACM, 2012.

[CZBP06] Reynold Cheng, Yu Zhang, Elisa Bertino, and Sunil Prabhakar. Preserving user location privacy in mobile data management infrastructures. In *Privacy Enhancing Technologies*, volume 4258 of *Lecture Notes in Computer Science*, pages 393–412. Springer, 2006.

[DMS04] Roger Dingledine, Nick Mathewson, and Paul F. Syverson. Tor: The second-generation onion router. In *USENIX Security Symposium*, pages 303–320. USENIX, 2004.

[EFG+09] Zekeriya Erkin, Martin Franz, Jorge Guajardo, Stefan Katzenbeisser, Inald Lagendijk, and Tomas Toft. Privacy-preserving face recognition. In Ian Goldberg and Mikhail J. Atallah, editors, *Privacy Enhancing Technologies*, volume 5672 of *Lecture Notes in Computer Science*, pages 235–253. Springer, 2009.

[FP11] Cédric Fournet and Jérémy Planul. Compiling information-flow security to minimal trusted computing bases. In Gilles Barthe, editor, *ESOP*, volume 6602 of *Lecture Notes in Computer Science*, pages 216–235. Springer, 2011.

[FPR11] Cédric Fournet, Jérémy Planul, and Tamara Rezk. Information-flow types for homomorphic encryptions. In Yan Chen, George Danezis, and Vitaly Shmatikov, editors, *ACM Conference on Computer and Communications Security*, pages 351–360. ACM, 2011.

[FSC+13] Cédric Fournet, Nikhil Swamy, Juan Chen, Pierre-Évariste Dagand, Pierre-Yves Strub, and Benjamin Livshits. Fully abstract compilation to javascript. In Roberto Giacobazzi and Radhia Cousot, editors, *POPL*, pages 371–384. ACM, 2013.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, pages 169–178. ACM, 2009.

[GGP10] Rosario Gennaro, Craig Gentry, and Bryan Parno. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In Tal Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 465–482. Springer, 2010.

[Gol04] Oded Goldreich. *The Foundations of Cryptography - Volume 2, Basic Applications.* Cambridge University Press, 2004.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *CRYPTO (1)*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2013.

[Hal05] Shai Halevi. A plausible approach to computer-aided cryptographic proofs. *IACR Cryptology ePrint Archive*, 2005:181, 2005.

[HEKM11] Yan Huang, David Evans, Jonathan Katz, and Lior Malka. Faster secure two-party computation using garbled circuits. In *USENIX Security Symposium*. USENIX Association, 2011.

[HKZ13] Tanzima Hashem, Lars Kulik, and Rui Zhang. Countering overlapping rectangle privacy attack for moving knn queries. *Inf. Syst.*, 38(3):430–453, 2013.

[HS12] Daniel Hedin and Andrei Sabelfeld. Information-flow security for a core of javascript. In Stephen Chong, editor, *CSF*, pages 3–18. IEEE, 2012.

[KhS12] Benjamin Kreuter and Chih hao Shen. Billion-gate secure computation with malicious adversaries. In *In USENIX Security*, 2012.

[Kru09] John Krumm. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6):391–399, 2009.

[KS08] Vladimir Kolesnikov and Thomas Schneider. Improved garbled circuit: Free xor gates and applications. In *ICALP (2)*, volume 5126 of *Lecture Notes in Computer Science*, pages 486–498. Springer, 2008.

[KSMS13] Ali Khoshgozaran, Houtan Shirani-Mehr, and Cyrus Shahabi. Blind evaluation of location based queries using space transformation to preserve location privacy. *GeoInformatica*, 17(4):599–634, 2013.

[KSS13] Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. A systematic approach to practically efficient general two-party secure function evaluation protocols and their modular design. *Journal of Computer Security*, 21(2):283–315, 2013.

[Lea11] Neal Leavitt. Internet security under attack: The undermining of digital certificates. *IEEE Computer*, 44(12):17–20, 2011.

[LEB13] Reginald L. Lagendijk, Zekeriya Erkin, and Mauro Barni. Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation. *IEEE Signal Process. Mag.*, 30(1):82–105, 2013.

[LGW13] Olivier Le Goaer and Sacha Waltham. Yet another dsl for cross-platforms mobile development. In *Proceedings of the First Workshop on the Globalization of Domain Specific Languages*, GlobalDSL '13, pages 28–33, New York, NY, USA, 2013. ACM.

[LLC14] AngelList LLC. Location based services startups, March 2014.

[MAS10] Jonas Magazinius, Aslan Askarov, and Andrei Sabelfeld. A lattice-based approach to mashup security. In Dengguo Feng, David A. Basin, and Peng Liu, editors, *ASIACCS*, pages 15–23. ACM, 2010.

[MOV13] Aikaterini Mitrokotsa, Cristina Onete, and Serge Vaudenay. Location leakage in distance bounding: Why location privacy does not work. *IACR Cryptology ePrint Archive*, 2013:776, 2013.

[MSZ04] Andrew C. Myers, Andrei Sabelfeld, and Steve Zdancewic. Enforcing robust declassification. In *CSFW*, pages 172–186. IEEE Computer Society, 2004.

[NTL$^+$11] Arvind Narayanan, Narendran Thiagarajan, Mugdha Lakhani, Michael Hamburg, and Dan Boneh. Location privacy via private proximity testing. In *NDSS*, 2011.

[Pai99] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology EUROCRYPT 99*, volume 1592, pages 223–238. Springer, 1999.

[PLW13] Tao Peng, Qin Liu, and Guojun Wang. Privacy preserving for location-based services using location transformation. In *CSS*, volume 8300 of *Lecture Notes in Computer Science*, pages 14–28. Springer, 2013.

[PWS$^+$14] Krishna P. N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel, and Ben Y. Zhao. Preserving location privacy in geosocial applications. *IEEE Trans. Mob. Comput.*, 13(1):159–173, 2014.

[RAD78] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. On data banks and privacy homomorphisms. *Foundations of secure computation*, 32(4):169–178, 1978.

[RCL12] Ruben Rios, Jorge Cuéllar, and Javier Lopez. Robust probabilistic fake packet injection for receiver-location privacy in wsn. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *ESORICS*, volume 7459 of *Lecture Notes in Computer Science*, pages 163–180. Springer, 2012.

[Sen13] Jaydip Sen. Homomorphic encryption: Theory &amp; applications. *CoRR*, abs/1305.5886, 2013.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.

[Sho04] Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive*, 2004:332, 2004.

[SMBW12] Srinath T. V. Setty, Richard McPherson, Andrew J. Blumberg, and Michael Walfish. Making argument systems for outsourced computation practical (sometimes). In *NDSS*. The Internet Society, 2012.

[SS09] A. Sabelfeld and D. Sands. Declassification: Dimensions and principles. *J. Computer Security*, 17(5):517–548, January 2009.

[SSW10] Ahmad-Reza Sadeghi, Thomas Schneider, and Immo Wehrenberg. Efficient privacy-preserving face recognition. In *Information, Security and Cryptology ICISC 2009*, volume 5984 of *Lecture Notes in Computer Science*, pages 229–244. Springer Berlin Heidelberg, 2010.

[STC$^+$13] H. Schulzrinne, H. Tschofenig, J. Cuellar, J. Polk, J. Morris, and M. Thomson. Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information. RFC 6772 (Proposed Standard), January 2013.

[STM$^+$07] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk, and J. Rosenberg. Common Policy: A Document Format for Expressing Privacy Preferences. RFC 4745 (Proposed Standard), February 2007.

[Ter11] Manolis Terrovitis. Privacy preservation in the dissemination of location data. *SIGKDD Explorations*, 13(1):6–18, 2011.

[Vey14] Max Veytsman. How i was able to track the location of any tinder user, February 2014. Web resource: http://blog.includesecurity.com/.

[vTSY10] Laurynas Šikšnys, Jeppe Rishede Thomsen, Simonas Saltenis, and Man Lung Yiu. Private and flexible proximity detection in mobile social networks. In *Mobile Data Management*, pages 75–84. IEEE Computer Society, 2010.

[WSG13] Matthias Wachs, Martin Schanzenbach, and Christian Grothoff. On the feasibility of a censorship resistant decentralized name system. In *6th International Symposium on Foundations & Practice of Security (FPS 2013)*, 2013.

[Yao82] Andrew Chi-Chih Yao. Protocols for secure computations. In *FOCS*, volume 82, pages 160–164, 1982.

[YLL$^+$12] Lin Yao, Chi Lin, Guangya Liu, Fangyu Deng, and Guowei Wu. Location anonymity based on fake queries in continuous location-based services. In *ARES*, pages 375–382. IEEE Computer Society, 2012.

[ZGH07] Ge Zhong, Ian Goldberg, and Urs Hengartner. Louis, lester and pierre: three protocols for location privacy. In *Proceedings of the 7th international conference on Privacy enhancing technologies*, PET'07, pages 62–76, Berlin, Heidelberg, 2007. Springer-Verlag.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-15355-112991-49

Name of applicant
Sabelfeld, Andrei

Date of birth
741110-8876

Title of research programme
DecentLP: Robust decentralized location privacy

Appendix B

Curriculum vitae

Andrei Sabelfeld: CV

Employments and education

Professor, Chalmers University of Technology and Gothenburg University, Gothenburg, Sweden, 2013–now; **Professor** (*biträdande professor*), 2011-12; **Associate Professor** (*docent*), 2006–10; **Senior Lecturer** (*unversitetslektor*), 2004–06.

Research Associate, Cornell University, Ithaca, NY, USA, 2002–03.

PhD student, Chalmers & GU, 1996–2001.

Software Engineer, Institute of Informatics Systems, Russian Academy of Sciences, Novosibirsk, Russia, 1995–96.

Bachelor student, Novosibirsk State University, Novosibirsk, Russia, 1991–95.

Capsule CV

Andrei Sabelfeld has developed the link between two areas of computer science: programming languages and computer security. He has pursued the certification of security according to principles of programming languages. He serves on the editorial board for JCS and IPL. He is a lecturer at the FOSAD'14, Marktoberdorf ('11 and '09), GLOBAN'08, FOSAD'04, and WSSA'03 international PhD summer schools; a steering committee member and program committee chair (2007/8) for CSF (top event in foundational computer security); a steering committee member for FCS and NordSec; program committee co-chair for ESORICS'06, the flagship computer security conference in Europe; program committee member of 57 international conferences, including IEEE Security & Privacy'14 and ACM CCS'14 (the two most prestigious conferences in computer security) as well as ACM POPL'13 (the most prestigious conference in programming languages); a keynote speaker at ASIACCS'10, ASIAN'07, TGC'06 and FCS'03, an editor of JCS and JFP special issues; and the initiator and co-chair of several Dagstuhl Seminars. Sabelfeld's article on Language-Based Information-Flow Security is one of the top most cited articles in all of Computer Science from 2003 (source: citeseer). He is among 536 recipients (out of 4741 candidates across all subjects) to receive the 1,5M€ ERC award in 2012. He is the recipient of the Chalmers Research Supervisor of the Year award in 2010. He is among the 20 recipients (out of 188 candidates across all subjects) of the 8,5MSEK Future Research Leader Award by SSF in 2008.

Awards

- *ERC StG (Consolidator)* by EU, among 536 recipients (out of 4741 candidates across all subjects) to receive the 1,5M€ award, 2012.
- *Chalmers Research Supervisor of the Year* award, 2010.
- *Future Research Leader* award by SSF, among the 20 recipients (out of 188 candidates across all subjects) to receive the 8,5MSEK (900K€) award, 2008.

Academic activities

Editorship Editorial board member for *Journal of Computer Security (JCS)*, 2012–now, and *Information Processing Letters (IPL)*, 2012–13; editor for the following special issues: special issue of JCS on *Web Application Security*, to appear; special issue of JCS on 2008 IEEE Comp. Security Foundations Symp., 2010; special issue of JCS on 2007 IEEE Comp. Security Foundations Symp., 2008; special issue on *Language-Based Security* of the *Journal of Functional Programming*, 2005.

Steering committees *IEEE Computer Security Foundations Symposium*, 2006–now; *Nordic Workshop on Secure IT Systems*, 2008–now; *Workshop on Foundations of Computer Security*, 2005–13 (chair: 2005–08).

Program committees Member of 57 program committees of international conferences and workshops. This includes regularly serving on the program committees of IEEE Security & Privacy and ACM CCS (the two most prestigious conferencea in computer security) as well as ACM POPL (most prestigious in programming languages), chairing IEEE CSF'07 and '08, the top event in foundational computer security; and co-chairing ESORICS'06, the flagship computer security conference in Europe. The full list is as follows: *ACM CCS'14, NordSec'14, IEEE CSF'14, PSI'14, IEEE S&P'14, ACM SAC'14, NWPT'13, NordSec'13, ESORICS'13, AppSecEU'13, ESEC/ACM FSE'13 New Ideas*

Track, FCS'13, POST'13, ACM POPL'13, NWPT'12, NordSec'12, MMM-ACNS'12, POST'12, NWPT'11, NordSec'11, SEC'11, ESOP'11, NWPT'10, MMM-ACNS'10, AppSec Research'10, ACM PLAS'10, IEEE S&P'10, ACM ASIACCS'10, ACM CCS'09, IEEE CSF'09, ACM CCS'08, IEEE CSF'08 (chair), ESOP'08, NordSec'07 (co-chair), MMM-ACNS'07, IEEE CSF'07 (chair), ACM PLAS'07, ESOP'07, APLAS'06, ESORICS'06 (co-chair), IEEE CSFW'06, IEEE S&P'06, ACM POPL'06, MMM-ACNS'05, SAS'05, FCS'05 (chair), IEEE CSFW'05, ESOP'05, VODCA'04, SecCo'04, SAS'04, FCS'04 (chair), FAST'03, FCS'03, IEEE CSFW'03, IEEE CSFW'02.

Keynote invited talks and colloquia *Dept. Colloquium at University of Pennsylvania*, Philadelphia, 2012; *Dept. Colloquium at Harvard University*, Boston, 2011; *OWASP Gothenburg Kick-off*, Gothenburg, Sweden, 2011; *Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS)*, St.Petersburg, Russia, 2010; *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Beijing, China, 2010; *Dagstuhl WebAppSec*, Dagstuhl, Germany, 2009; *OWASP Sweden Kick-off*, Stockholm, Sweden, 2008; *Asian Computing Science Conference (ASIAN)*, Doha, Qatar, 2007; *Symposium on Trustworthy Global Computing (TGC)*, Lucca, Italy, 2006; *Workshop on Foundations of Computer Security (FCS)*, Ottawa, Canada, 2003.

Summer PhD school academic director *4th International School on Foundations of Security Analysis and Design (FOSAD)*, Bertinoro, Italy, September 2004.

Summer PhD school lecturer FOSAD 2014: *International School on Foundations of Security Analysis and Design*, Bertinoro, Italy, September 2014; Aalborg 2011: *Advanced Topics in Computer Security*, Aalborg University, Denmark, 2011; Marktoberdorf 2011: *Analysis and Verification of Safety and Security*, Marktoberdorf, Germany, August 2011; SSSEV 2011: Microsoft Research Summer School on *Software Engineering and Verification*, Moscow, Russia, July 2011; Marktoberdorf 2009: *Logics and Languages for Reliability and Security*, Marktoberdorf, Germany, August 2009; GLOBAN 2008: *Global Computing Approach to Analysis of Systems International Summer School*, Warsaw, Poland, September 2008; FOSAD 2004: *International School on Foundations of Security Analysis and Design*, Bertinoro, Italy, September 2004; WSSA 2003: *International School on Semantics and Applications*, Montevideo, Uruguay, July 2003.

Tutorial Tutorial on Language-Based Information Security at the *Dagstuhl Seminar on Language-Based Security*, Dagstuhl, Germany, October 5–10, 2003.

Workshop program chair *Dagstuhl Seminar on Web Application Security*, 2012; *Dagstuhl Seminar on Mobility, Ubiquity, and Security*, 2007; *Chalmers Security and Static Analysis Workshop*, 2005; *Verona Workshop on Programming Language Interference & Dependence*, 2004; *Dagstuhl Seminar on Language-Based Security*, 2003; *Cornell IAI Security Workshop*, 2003; *Chalmers Security Workshop*, 1999.

Panels Panel on Privacy Challenges at *ICT Fair*, Gothenburg, 2011; Panel on Availability vs. Security at *ICT Fair*, Gothenburg, 2010; Panel on Rigorous Security Analysis of Software at *CSF'09*.

PhD/Postdoc supervision (Main supervisor)

A. Birgisson (start: 2009, PhD degree: 2013), now software engineer at Google; J. Magazinius (start: 2008, PhD degree: 2013), now postdoc at Saarland University; A. Askarov (start: 2005, PhD degree: 2009), now Associate Professor at Aarhus University; A. Russo (start: 2005, PhD degree: 2008), now Associate Professor at Chalmers; W. Rafnsson (start: 2009, Licentiate: 2012, PhD degree expected: 2014); L. Bello (start: 2011, PhD degree expected: December 2015); D. Hausknecht (start: 2013, PhD degree expected: 2018); postdoc supervisor for D. Hedin (start: 2010, expected to finish: 2014) will start as lecturer at Mälardalen University; postdoc supervisor for A. Russo (2008–09), now Associate Professor at Chalmers.

Refereeing

PhD thesis referee J. Wilander, Linköping U., 2013; A. Lundblad, KTH, 2013; A. Larsson, Chalmers, 2012; M. Centenaro, U. Venice, 2011; B. Köpf, ETH, Zurich 2007; G. Le Guernic, IRISA/CNRS/ENS Cachan, 2007; T. Tolstrup, Technical U. of Denmark, 2007; J. Wilander (licentiate thesis), Linköping U., 2005.

Referee for promotion applications Associate professor (*docent*) promotion application, Royal Institute of Technology, Stockholm, Sweden, 2012.

Referee for funding agencies and industry Belgium's Research Foundation - Flanders (FWO) Postdoc Fellow Program, 2014; UK Royal Society (University Research Fellowship applications), 2011; US Air Force Office of Scientific Research (AFOSR), 2011; Microsoft Research PhD Scholarship Programme, 2008; Netherlands Organization for Scientific Research (NWO), 2008; Icelandic Research Fund, 2006.

Curriculum vitae (max. 2 pages)

Personal Information

Mitrokotsa, Aikaterini, ORCID: 0000-0002-7073-0258
Date of birth: 08/10/1978
Web site: `http://www.cse.chalmers.se/~aikmitr/`

Higher Education Qualifications

2002-2007: **PhD in Computer Science**, University of Piraeus, Greece, On the Subject: **"Intrusion Detection in Computer Networks Using Machine Learning Algorithms"**, Supervisor: Prof. Christos Douligeris, with highest distinction, **PhD Award date:** 12/11/2007.

1997-2001: **B.Sc. Degree in Computer Science**, University of Piraeus, GPA: 8.4/10.

Employment

08.2013-Today: Assistant Professor, Department of Compute Science & Engineering, **Chalmers University of Technology**, Sweden. (80% research, 20% teaching)

09.2012-08.2013: Professor Univ. of Applied Sciences Western Switzerland (HES-SO), Geneva.

07.2010-12.2012: Research Associate-**Marie Curie Fellow**, **EPFL**, Switzerland.

10.2008-04.2010: Research Associate-**NWO Rubicon Fellow**, **TU Delft**, The Netherlands.

09.2007-09.2008: Visitor Assistant Professor, **Vrije Universiteit**, The Netherlands.

02.2002-09.2007: Research assistant, University of Piraeus, Greece.

06.2002-07.2007: Visiting Faculty, Technological Education Institute (TEI) of Chalkida, Greece.

01.2004-03.2004: Research assistant, Hellenic Authority for the Information and Communication Security and Privacy (ADAE), Greece.

01.2002-05.2002: Consultant of Information Security for the Company Encode S.A., Greece.

Qualification required for appointment as docent: Applied in Jan. 2014 expected result April 2014

Educational courses followed:
- Supervision of Research (Chalmers) (3 ECTS)
- Educational Portfolio (Chalmers) (6 ECTS) Ongoing expected May 2014.
- Informatics & Education (Univ. of Piraeus) (5 ECTS).

Fellowships and Awards

2013-2014: **STINT Initiation Grant**, Project: *"Cross-layer Authentication Protocols for Wireless Networks"* (∼150.000 SEK - 2 partners).

2013-2017: **Chalmers ICT Areas of Advance** funding of research for 4 years (including funding for 1 PhD student) (∼900.000 €). Very competitive (1 selected from ∼70).

2012-2016 **STREP (FP7)**, Project: *"BEAT: Biometrics Evaluation & Testing"* (∼3.5 millions €-10 partners). Project number: 284989.

2010-2012: **Marie Curie IEF (FP7):** Project: *"PPIDR: Privacy-Preserving Intrusion Detection and Response in Wireless Communications"* (∼166.000 €). Project number: 252323.

2009-2010: **ICT Talent Grant** awarded by the TU Delft. Project:*"Intrusion Detection & Response in Wireless Communication"*. (∼35.000 €).

2008-2009: **NWO Rubicon Grant**. Project: *"Intrusion Detection in Ubiquitous Computing Technologies"* (55.000 €).

2002-2005: Scholarship by the **Foundation of Bodossaki** for PhD studies.

2001: Led the graduation oath for the **highest GPA among all students** of the Department.

1998-2000: Award by the **University of Piraeus** for best performance for undergraduate studies.

1997-1999: Best Student Award & Scholarship by the **National Scholarship Foundation**, GR.

Conference Organisation

– **Publication Chair:** *AfricaCrypt* 2012

– **Program Chair:** *ECML/PKDD Workshop on Privacy & Security Issues in Data Mining & Secure Machine Learning* 2010, *International Workshop on RFID Technology* 2009-2010.

Selected service in Program Committees

IEEE INFOCOM 2015-2014, IEEE Conference on Communications & Network Security (**IEEE CNS 2013-2014**), International Conference on Applied Cryptography & Network Security (**ACNS 2014**)
International Conference on Availability, Reliability & Security (**ARES 2013-2014**), Workshop on RFID Security & Privacy (**RFIDsec 2013**), **Indocrypt 2013**, **Africacrypt 2012**.

Supervised Post-doctoral Researchers

– Dr. Aysajan Abidin, 2014-Today, Topic: *“Privacy-preserving biometric authentication”*, Chalmers.

Supervised PhD students

– Asli Bay, EPFL 2011-2012, Topic: *“Attacks in Authentication Protocols”*.
– Sergio Pastrana, Carlos III University of Madrid 2009-2010, Topic: *“Intrusion Detection in MANET.*
– Michael Beye, TU Delft 2009-2010, Topic: *“RFID Security & Privacy”*.

Supervised Master students

– Erica Löfström, MSc. Thesis:*“Diversification in a white-box environment”*, Chalmers 2014.
– Christoffer Karlsson, MSc. Thesis:*“Distance-bounding protocols”*, Chalmers, 2014.
– Daniel Olausson, MSc. Thesis:*“Privacy-preserving biometrics”*, Chalmers, 2014.
– André Malm, MSc. Thesis: *“Obfuscation in a white-box environment”*, Chalmers 2014.
– Iosif Spulber, MSc. Project:*“Solving the Hidden Number problem”*, EPFL, 2012.
– Tamas Nagy, MSc. Thesis:*“Intrusion Detection in RFID systems”*, Vrije Universiteit, 2008.
– Despo Galataki, MSc. Project:*“Intrusion Detection within a building”*, Vrije Universiteit, 2008.
– Atul Mehta, MSc.Project:*“Intrusion Detection for Integrated WSN & RFID”*,Vrije Universiteit, 2008.
– Manolis Tsagkaris, MSc. Thesis:*“Intrusion detection in MANETs”*, Univ. of Piraeus, 2007.

Institutional Responsibilities

– **Director** of the *Master of Advanced Studies* Program: *Information Security Management Systems*, University of Applied Science Western Switzerland (HES-SO) (2012-2013).
– **PhD Thesis examiner-reviewer:** ■ J. Magazinius, Chalmers, Topic: *“Dynamic Enforcement of decentralized security policies”* 2013, ■ L. Mirowski, Univ. of Tasmania Topic: *“A whole of system approach of security analysis in RFID systems using an integrated layered & partitioned reference model”* 2011.
– *MSc. Thesis examiner* for Z. Chen, EPFL, Topic: *“The LPN Problem & algebraic methods”* 2013.

Commissions of Trust

– **Editorial Board:** ■ IEEE Communications Letters (2013-today).
■ Computers & Security, Elsevier (2013-today).
■ KSII Transactions on Internet & Information Systems (2013-today).
■ Information Security Journal (Taylor & Francis) (2012-today).

– **Guest editor:** ■ Special Issue in IEEE Transactions on Dependable & Secure Computing.
■ Special Issue in Journal of Personal & Ubiquitous Computing, Springer.
■ Special Isuue in Journal of Networks & Computer Applications.

– **Reviewer:** ■ National Science Foundation (NSF) CAREER Proposals.
■ Discovery Grants Natural Sciences & Engineering Research, Canada.

– **Groups of experts:** ■ ENISA Permanent Stakeholders Group (PSG) (2012-2015).
■ ENISA's expert group PROCENT-EG (2009-2010).
■ Network & Information Security (NIS) platform for the Working Group (WG 3) Secure ICT Research & Innovation.

Selected Teaching Experience

– Operating Systems, Chalmers, Winter semester, 2013.
– Security Protocols & Applications, EPFL, Spring semester 2011, 2012.
– Cryptography & Security, TU Delft, 2010.
– Computers & Network Security, Vrije Universiteit, Spring semester, 2008.
– Advanced Topics in Network Security, Vrije Universiteit, Winter semester 2007.

Memberships of Scientific Societies

■ **ERCIM** Working Group in Security & Trust Management, ■ **Sys-Sec** (NoE FP7) Associate Member, ■ **IEEE** member, ■ **ACM** member, ■ **IACR** member, ■ Member of **European Association for Biometrics**, ■ Award co-chair for Networking Networking **N2Women** (ACM SIGMOBILE).

Major Collaborations

■ **University of Tokyo**, Prof. Kanta Matsuura (Research visits) Topic: *“Authentication protocols”*.
■ **City University of Hong Kong**, Prof. Gerhard Hancke, Collaboration in STINT project.
■ **EPFL**, Prof. Serge Vaudenay, Topic: *“Provable Security”*.
■ **ETHZ**, Prof. Bernhard Pattner, Topic: *“Intrusion Response”*.
■ **Carlos III Univ. of Madrid**, Prof. Pedro Peris Lopez, Topic: *“RFID Security & Privacy”*.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-15355-112991-49

Name of applicant
Sabelfeld, Andrei

Date of birth
741110-8876

Title of research programme
DecentLP: Robust decentralized location privacy

Appendix C

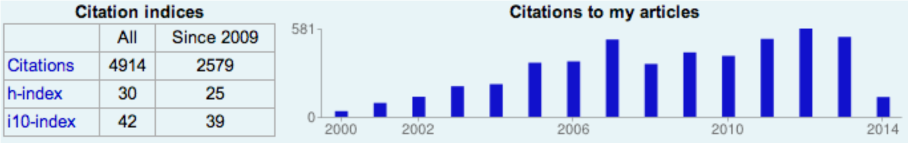
List of publications

Andrei Sabelfeld: Selected Publications

Note: Computer science is a very conference-oriented field. As a result we place less importance on journal papers than many other fields, and substantially more importance on conferences. Our conference and workshop papers are typically referreed by at least three reviewers, and are usually 15–20 pages long. However, the review process is not as thorough as for journal papers, and it is still expected that one might expand a conference or workshop paper into a journal paper at a later date (though this step is often neglected by computer scientists in favor of moving on to new conference publications). I have included both journal and conference/workshop papers here, under separate headings.

Acceptance rates for several of the conferences below are extremely competitive: for example, CCS'13 accepted 105 out of 403 submissions (20%), ESORICS'12 accepted 50 out of 248 submissions (20%) and IEEE Security and Privacy'07 accepted 29 out of 248 submissions (9%). Conferences such as IEEE CSF, which has accepted many of my publications, as well as IEEE Security and Privacy, ACM CCS, and ESORICS are all *Tier A* conferences according to the classification by the Australian Research Council, the most established ranking in computer science. According to this classification, ACM TISSEC and IEEE TDSC, featuring my publications, are *the* top two journals in computer security. More information about the ranking of various computer science journals and conferences is available at http://www.arc.gov.au/era/era_2012/era_2012.htm.

The number of citations, and statistics to the right, is from the *Google Scholar* database: http://scholar.google.com/citations?user=dQge5-AAAAAJ. Following VR's instructions, five publications that are most relevant for the proposal are marked by "*", and publications older than 8 years are displayed in gray. All publications are available electronically via http://www.cse.chalmers.se/~andrei/publications.html.



Citation indices

	All	Since 2009
Citations	4914	2579
h-index	30	25
i10-index	42	39

Articles in Refereed Journals

1. W. Rafnsson, K. Nakata, and A. Sabelfeld. Securing Class Initialization in Java-like Languages. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 10:1(1-13), January 2013. Citations: **1**
2. J. Magazinius, A. Russo, and A. Sabelfeld. On-the-fly Inlining of Dynamic Security Monitors. *Computers & Security*, 31:7(827-843), Elsevier, October 2012. Citations: **24**
3. G. Barthe, T. Rezk, A. Russo, and A. Sabelfeld. Security of Multithreaded Programs by Compilation. *ACM Transactions on Information and System Security (TISSEC)*, 13(3), July 2010. Citations: **9**
4. A. Russo and A. Sabelfeld. Securing Interaction between Threads and the Scheduler in the Presence of Synchronization. *Journal of Logic and Algebraic Programming*, Elsevier, 78(7), August 2009. Citations: **5**
5. A. Sabelfeld and D. Sands. Declassification: Dimensions and principles. *Journal of Computer Security*, 17(5), IOS Press, January 2009. Citations: **105** *
6. A. Askarov, D. Hedin, and A. Sabelfeld. Cryptographically-masked flows. *Theoretical Computer Science*, Elsevier, 402(2–3), August 2008. Citations: **12** *
7. A. C. Myers, A. Sabelfeld, and S. Zdancewic. Enforcing robust declassification and qualified robustness. *Journal of Computer Security*. 14(2), IOS Press, May 2006. Citations: **83** *
8. A. Sabelfeld and A. C. Myers. Language-Based Information-Flow Security. *IEEE Journal on Selected Areas in Communication*, 21(1), January 2003. Citations: **1424**
9. H. Mantel and A. Sabelfeld. A Unifying Approach to the Security of Distributed and Multi-Threaded Programs. *Journal of Computer Security*, 11(4), IOS Press, September 2003. Citations: **61**
10. A. Sabelfeld and D. Sands. A PER Model of Secure Information Flow in Sequential Programs. *Higher-Order and Symbolic Computation*, 14(1), March 2001. Citations: **149**

Articles in Refereed Conference Proceedings

11. D. Hedin, A. Birgisson, L.Bello, and A. Sabelfeld. JSFlow: Tracking Information Flow in JavaScript and its APIs. In *Proc. ACM Symposium on Applied Computing (SAC)*, March 2014. Citations: **4**
12. J. Magazinius, D. Hedin, and A. Sabelfeld. Architectures for Inlining Security Monitors in Web Application. In *Proc. International Symposium on Engineering Secure Software and Systems (ESSoS)*, Feb. 2014.
13. J. Magazinius, B. K. Rios, and A. Sabelfeld. Polyglots: Crossing Origins by Crossing Formats. In *Proc. ACM Conference on Computer and Communications Security (CCS)*, Nov. 2013. Citations: **1**
14. W. Rafnsson and A. Sabelfeld. Secure Multi-Execution: Fine-grained, Declassification-aware, and Transparent. In *Proc. IEEE Computer Security Foundations Symposium*, June 2013. Citations: **4**
15. P. Hallgren, D. Mauritzson, and A. Sabelfeld. GlassTube: A Lightweight Approach to Web Application Integrity In *Proc. ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS)*, June 2013.
16. A. Birgisson, D. Hedin, and A. Sabelfeld. Boosting the Permissiveness of Dynamic Information-Flow Tracking by Testing. In *Proc. European Symposium on Research in Computer Security (ESORICS)*, LNCS, Sept. 2012. Citations: **10**
17. D. Hedin and A. Sabelfeld. Information-Flow Security for a Core of JavaScript. In *Proc. IEEE Computer Security Foundations Symposium*, June 2012. Citations: **50**
18. W. Rafnsson, D. Hedin, and A. Sabelfeld. Securing Interactive Programs In *Proc. IEEE Computer Security Foundations Symposium*, June 2012. Citations: **4**
19. J. Magazinius, A. Askarov, and A. Sabelfeld. Decentralized Delimited Release. In *Proc. Asian Symposium on Programming Languages and Systems (APLAS)*, LNCS, Dec. 2011. Citations: **2**
20. A. Birgisson and A. Sabelfeld. Multi-run security. In *Proc. European Symposium on Research in Computer Security (ESORICS)*, LNCS, Sept. 2011. Citations: **1**
21. A. Birgisson, A. Russo, and A. Sabelfeld. Capabilities for information flow. In *Proc. ACM Workshop on Programming Languages and Analysis for Security (PLAS)*, June 2011. Citations: **9**
22. W. Rafnsson and A. Sabelfeld. Limiting Information Leakage in Event-based Communication. In *Proc. ACM Workshop on Programming Languages and Analysis for Security (PLAS)*, June 2011. Citations: **10**
23. A. Birgisson, A. Russo, and A. Sabelfeld. Unifying Facets of Information Integrity. In *Proc. International Conference on Information Systems Security (ICISS)*, LNCS, December 2010. Citations: **11**
24. J. Magazinius, A. Russo, and A. Sabelfeld. On-the-fly Inlining of Dynamic Security Monitors. In *Proc. IFIP International Information Security Conference (SEC)*, IFIP AICT 330, September 2010. Citations: **14**
25. A. Russo and A. Sabelfeld. Dynamic vs. Static Flow-Sensitive Security Analysis. In *Proc. IEEE Computer Security Foundations Symposium*, July 2010. Citations: **73**
26. K. Nakata and A. Sabelfeld. Securing Class Initialization. In *Proc. IFIP International Conference on Trust Management*, IFIP AIC 321, June 2010. Citations: **3**
27. A. Russo, A. Sabelfeld, and A. Chudnov. Tracking Information Flow in Dynamic Tree Structures. In *Proc. European Symposium on Research in Computer Security (ESORICS)*, LNCS 5789, September 2009. Citations: **47**
28. A. Russo and A. Sabelfeld. Securing Timeout Instructions in Web Applications. In *Proc. IEEE Computer Security Foundations Symposium*, July 2009. Citations: **35**
29. A. Askarov and A. Sabelfeld. Tight Enforcement of Information-Release Policies for Dynamic Languages. In *Proc.IEEE Computer Security Foundations Symposium*, July 2009. Citations: **75**
30. A. Sabelfeld and A. Russo. From dynamic to static and back: Riding the roller coaster of information-flow control research. In *Proc. Perspectives of System Informatics*, LNCS 5947, June 2009. Citations: **68**
31. A. Askarov and A. Sabelfeld. Catch Me If You Can: Permissive Yet Secure Error Handling. In *Proc. ACM Workshop on Programming Languages and Analysis for Security (PLAS)*, June 2009. Citations: **11**
32. A. Askarov, S. Hunt, A. Sabelfeld, and D. Sands. Termination-Insensitive Noninterference Leaks More Than Just a Bit. In *Proc. European Symposium on Research in Computer Security*, LNCS 5283, October 2008. Citations: **90**
33. G. Barthe, T. Rezk, A. Russo, and A. Sabelfeld. Security of Multithreaded Programs by Compilation, In *Proc. European Symposium on Research in Computer Security (ESORICS)*, LNCS 4734, September 2007. Citations: **23**
34. A. Askarov and A. Sabelfeld. Localized Delimited Release: Combining the What and Where Dimensions of Information Release. In *Proc. ACM Programming Languages and Analysis for Security*, June 2007. Citations: **47**
35. A. Askarov and A. Sabelfeld. Gradual Release: Unifying Declassification, Encryption and Key Release Policies. In *Proc. IEEE Symposium on Security and Privacy*, May 2007. Citations: **77**
36. A. Russo, J. Hughes, D. Naumann, and A. Sabelfeld. Closing Internal Timing Channels by Transformation. In *Proc. Annual Asian Computing Science Conference*, LNCS 4435, December 2006. Citations: **39**

37. A. Askarov, D. Hedin, and A. Sabelfeld. Cryptographically-masked flows. In *Proc. Symp. on Static Analysis*, LNCS 4134, August 2006. Citations: **32***
38. A. Russo and A. Sabelfeld. Securing interaction between threads and the scheduler. In *Proc. IEEE Computer Security Foundations Workshop*, July 2006. Citations: **52**
39. A. Russo and A. Sabelfeld. Security for multithreaded programs under cooperative scheduling. In *Proc. Perspectives of System Informatics*, LNCS 4378, June 2006. Citations: **31**
40. A. Askarov and A. Sabelfeld. Security-typed languages for implementation of cryptographic protocols: A case study. In *Proc. European Symp. on Research in Computer Security*, LNCS 3679, September 2005. Citations: **76***
41. A. Sabelfeld and D. Sands. Dimensions and principles of declassification. In *Proc. IEEE Computer Security Foundations Workshop*, June 2005. Citations: **221**
42. R. Focardi, S. Rossi, and A. Sabelfeld. Bridging language-based and process calculi security. In *Proc. Foundations of Software Science and Computation Structure*, LNCS 3441, April 2005. Citations: **31**
43. A. C. Myers, A. Sabelfeld, and S. Zdancewic. Enforcing robust declassification. In *Proc. IEEE Computer Security Foundations Workshop*, June 2004. Citations: **109**
44. A. Sabelfeld and A. C. Myers. A Model for Delimited Information Release. In *Proc. International Symp. on Software Security (ISSS)*, LNCS 3233, October 2004. Citations: **160**
45. A. Sabelfeld. Confidentiality for Multithreaded Programs via Bisimulation. In *Proc. Perspectives of System Informatics*, LNCS 2890, July 2003. Citations: **26**
46. A. Sabelfeld and H. Mantel. Static Confidentiality Enforcement for Distributed Programs. In *Proc. Static Analysis Symposium*, LNCS 2477, September 2002. Citations: **76**
47. A. Sabelfeld. The Impact of Synchronisation on Secure Information Flow in Concurrent Programs. In *Proc. Perspectives of System Informatics*, LNCS 2244, July 2001. Citations: **69**
48. H. Mantel and A. Sabelfeld. A Generic Approach to the Security of Multi-threaded Programs. In *Proc. IEEE Computer Security Foundations Workshop*, June 2001. Citations: **50**
49. A. Sabelfeld and D. Sands. Probabilistic Noninterference for Multi-threaded Programs. In *Proc. IEEE Computer Security Foundations Workshop*, July 2000. Citations: **275**
50. A. Sabelfeld and D. Sands. A Per Model of Secure Information Flow in Sequential Programs. In *Proc. European Symposium on Programming*, LNCS 1576, March 1999. Citations: **106**

Invited articles

51. D. Hedin and A. Sabelfeld A Perspective on Information-Flow Control. In *Proc. 2011 Marktoberdorf Summer School*, IOS Press. Citations: **5**
52. J. Magazinius, A. Askarov, and A. Sabelfeld. A lattice-based approach to mashup security. In *Proc. ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, April 2010. Citations: **42** *
53. A. Russo, A. Sabelfeld, and K. Li Implicit flows in malicious and nonmalicious code. In *Proc. 2009 Marktoberdorf Summer School*, IOS Press. Citations: **1**
54. A. Sabelfeld. Dimensions of Declassification in Theory and Practice. In *Proc. Asian Symp. on Programming Languages and Systems*, LNCS 4846, Springer-Verlag, December 2007.
55. A. Sabelfeld. Policies and Mechanisms for Safe Information Release. In *Proc. Programming Language Interference and Dependence (PLID)*, Verona, Italy, 25 August 2004.

Special Issues of Journals

56. L. Desmet, M. Johns, B. Livshits, and A. Sabelfeld (editors). Special issue on Web Application Security, *Journal of Computer Security*, IOS Press, To appear.
57. A. Sabelfeld (editor). Special issue on selected papers from the 2008 IEEE Computer Security Foundations Symposium, *Journal of Computer Security*, IOS Press, September 2010.
58. A. Sabelfeld (editor). Special issue on selected papers from the 2007 IEEE Computer Security Foundations Symposium, *Journal of Computer Security*, IOS Press, November 2008.
59. M. Abadi, G. Morrisett, and A. Sabelfeld (editors). Special Issue on Language-Based Security, *Journal of Functional Programming*, March 2005, Cambridge University Press.

Conference and Workshop Proceedings

60. D. Gollmann, J. Meier, and A. Sabelfeld (editors). *Proc. ESORICS 2006 11th European Symposium on Research in Computer Security*, Hamburg, Germany, September 18-20, 2006. LNCS 4189, Springer-Verlag.

61. U. Erlingsson and A. Sabelfeld (editors). *Proc. 12th Nordic Workshop on Secure IT Systems*, Reykjavik, Iceland, October 2007. Reykjavik University.

62. A. Sabelfeld (editor). *Proc. Foundations of Computer Security*, Chicago, IL, June 2005. DePaul University.

63. A. Sabelfeld (editor). *Proc. Foundations of Computer Security*, volume 31 of *TUCS General Publications*, Turku, Finland, June 2004. Turku Centre for Computer Science.

Theses

64. A. Sabelfeld. *Semantic Models for the Security of Sequential and Concurrent Programs*. Ph.D. thesis, Chalmers University of Technology and Gothenburg University, May 2001. Citations: **6**

65. A. Sabelfeld. *Semantic-based Program Security and Aspects of Program Analysis*. Licentiate thesis, Chalmers University of Technology and Gothenburg University, March 2000.

66. A. Sabelfeld. *Equivalent Transformations of Finite-recursive Schemes*. B.S. thesis. Novosibirsk State University, May 1995.

Software

67. D. Hedin, A. Birgisson, L. Bello, A. and Sabelfeld *JSFlow: security-enhanced JavaScript interpreter for fine-grained tracking of information flow*. Software distribution. October 2013. Available via `http://chalmerslbs.bitbucket.org/jsflow/`

Publication List[*][†]

Aikaterini Mitrokotsa

I have written more than 40 scientific publications in international journals, books, and conference proceedings and my work has been cited more than 700 times while my *h-index* is 12 and my *i10-index* is 14 (according to *Google Scholar*). I have participated in the organization of workshops, served as reviewer for 20 journals and multiple conferences, and have served as guest editor for three special issues focusing on secure communications and the RFID technology (Journal of Networks and Computer Applications (Elsevier), IEEE Transactions on Dependable and Secure Computing, Personal and Ubiquitous Computing (Springer)). Currently, among others I serve as associate editor for the *IEEE Communications Letters* and the *Computers & Security* journal (Elsevier). I have also been invited to give lectures on subjects related to my expertise by a number of institutions (International Telecommunication Union (ITU), European Patent Office (EPO)).

Peer-reviewed original articles in International Journals

[J1*] A.Mitrokotsa, C. Onete, S. Vaudenay, "Location Leakage in Distance-Bounding: Why Location Privacy does not Work", ***Computers & Security*****, Elsevier, To Appear 2014.**

[J2*] A. Mitrokotsa, P. Peris-Lopez, C. Dimitrakakis, S. Vaudenay. "On selecting the nonce length in distance-bounding protocols", ***Computer Journal (Oxford)*** **56(10): 1216-1227, (2013) doi: 10.1093/comjnl/bxt033.**

[J3] A. Mitrokotsa, C. Dimitrakakis, "Intrusion Detection in MANET using Classification Algorithms: The Effects of Cost and Model Selection", *Ad hoc Networks*, Elsevier, doi: 10.1016/j.adhoc.2012.05.006, 11(1): 226–237, Jan. 2013.

[J4] S. Pastrana, A. Mitrokotsa, A. Orfila, P. Peris-Lopez. "Evaluation of Classification Algorithms for Intrusion Detection in MANETs". Knowledge-Based Systems, Elsevier, doi: 10.1016/j.knosys.2012.06.016, Vol. 36, Dec. 2012, pages 217–225.

[J5] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, J.C.A. van der Lubbe, "A Comprehensive RFID solution to enhance inpatient medication safety", *International Journal of Medical Informatics*, 80(1): 13–24, Jan. 2011.

[J6] A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, J.C. Hernandez-Castro. "Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels". *IEEE Communications Letters*, Feb. 2010, 14(2):121–123, Feb. 2010.

[J7] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Protection of an Intrusion Detection Engine with Watermarking in Ad Hoc Networks". *International Journal of Network Security*, 10(2): 93–106, March 2010.

[J8] A. Mitrokotsa, M.R. Rieback, and A.S. Tanenbaum. "Classifying RFID Attacks and Defenses". *Special Issue on Advances in RFID Technology, Information Systems Frontiers, Springer*, LLC 2009, 12(5):491–505, 2010.

[J9] A. Mitrokotsa, N. Komninos, C. Douligeris, (2007), "Intrusion Detection and Response in Ad hoc Networks", *International Journal on Computer Research, Special Issue on Advances in Ad Hoc Network Security*, Nova Science Publishing Inc., Vol. 15, Issue 1, pages 23–55, 2007.

[*] This publication list correct ponds to the last eight years. The full publication list can be found in `http://www.cse.chalmers.se/~aikmitr/Publications.html`

[†] Selected relevant publications are denoted by * and bold letters.

Peer-reviewed Conference Contributions

[C1] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Practical & Provably Secure Distance-Bounding", In *Proceedings of the 16th Information Security Conference*, Dallas, Texas, USA, Nov. 2013.

[C2] C. Dimitrakakis, A. Mitrokotsa, and S. Vaudenay, "Expected loss bounds for authentication in constrained channels", In *Proceedings of INFOCOM 2012*, Orlando Florida 2012, March 2012.

[C3] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Secure & Lightweight Distance-Bounding", In Proceedings of the 2nd International Workshop on Lightweight Cryptography for Security & Privacy (LightSec 2013), May 2013, Gebze, Turkey.

[C4] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "On the Need for Secure Distance-Bounding", Extended abstract, In Proceedings of the Early Symmetric Crypto (ESC 2013), Jan. 2013, Mondorf-les Bains, Luxembourg.

[C5] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Towards Secure Distance Bounding", In Proceedings of the 20th International Workshop on Fast Software Encryption (FSE 2013), March 2013, Singapour.

[C6] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols - PRF-ness alone Does Not Stop the Frauds!", In *Proceedings of LATINCRYPT 2012, 2nd International Conference on Cryptology and Information Security in Latin America*, Santiago, Chile, Oct. 2012, pp. 100-120, LNCS 7533 Springer 2012.

[C7] A. Bay, I. Boureanu, A. Mitrokotsa, I. Spulber, S. Vaudenay, "The Bussard-Bagga and Other Distance Bounding Protocols under Man-in-the-Middle Attacks", In *Proceedings of Inscrypt'2012, 8th China International Conference on Information Security and Cryptology*, Nov. 2012, Beijing, China.

[C8] C. Dimitrakakis, A. Mitrokotsa, "Near-Optimal Node Blacklisting in Adversarial Networks", 2012 Conference on Decision and Game Theory for Security (GameSec 2012), Poster Session, Budapest, Hungary, Nov. 2012.

[C9] A. Mitrokotsa, C. Onete and S. Vaudenay, "Mafia Fraud Attack against the RC distance-Bounding Protocol", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, Nov. 2012, Nice, France, pages 74-79, IEEE Press.

[C10] M. Safkhani, N. Bagheri, A. Mitrokotsa, P. Peris-Lopez, "On the Traceability of Tags in SUAP RFID Authentication Protocols", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, Nov. 2012, Nice, France, pages 80-84, IEEE Press.

[C11] M. Safkhani, N. Bagheri, P. Peris-Lopez, A. Mitrokotsa, J.C. Hernandez-Castro, "Weaknesses in another Gen2-Based RFID Authentication Protocol", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, Nov. 2012, Nice, France, pages 292-296, IEEE Press.

[C12] J.-P. Aumasson, A. Mitrokotsa, P. Peris-Lopez, "A Note on a Privacy-Preserving Distance Bounding Protocol", In *Proceedings of the 13th International Conference on Information and Communication Security (ICICS 2011)*, Nov., Beijng China. Springer Vol. 7043, pp. 78-92.

[C13] P. Darcy, B. Stantic, A. Mitrokotsa, A. Sattar, "Detecting Intrusions within RFID Systems through Non-Monotonic Reasoning Cleaning", In *Proceedings of the 6th International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, Dec. 2010, Brisbane, Australia.

[C14] C. Dimitrakakis and A. Mitrokotsa. "Statistical Decision Making for Authentication and Intrusion Detection", In *Proceedings of the 8th IEEE International Conference on Machine Learning and Applications (ICMLA 2009)*, Miami, FL, USA, Dec. 2009, pp. 409-414, IEEE Computer Society.

[C15] A. Mitrokotsa, M.R. Rieback, and A.S. Tanenbaum. "Classification of RFID Attacks". In *Proceedings of the 2nd International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT 2008), in conjunction 10th International Conference on Enterprise Information Systems*, pages 73–86, Barcelona, Spain, June 2008. INSTICC Press, Portugal.

[C16] A. Mitrokotsa, M. Tsagkaris, and C. Douligeris. "Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms". In *Proceedings of the Seventh Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2008) - Advances in Ad Hoc Networking*, Computer Science, pages 133–144, Palma de Mallorca, Spain, June 2008. Springer.

[C17] A. Mitrokotsa, C. Dimitrakakis, and C. Douligeris. "Intrusion Detection Using Cost-Sensitive Classification". In *Proceedings of the 3rd European Conference on Computer Network Defense (EC2ND 2007)*, LNEE, pages 35–46, Heraklion, Crete, Greece, Oct. 2007. Springer-Verlag.

[C18] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET". In *Proceedings of IEEE International Conference on Pervasive Services 2007 (ICPS 2007)*, pages 118–127, Instabul, Turkey, July 2007.

[C19] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Towards an Effective Intrusion Response Engine Combined with Intrusion Detection in Ad Hoc Networks". In *Proceedings of the 6th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2007)*, pages 137–144, Corfu, Greece, June 2007.

[C20] A. Mitrokotsa, R. Mavropodi, and C. Douligeris. "Detecting Packet Dropping Attacks Using Emergent Self-Organizing Maps in Mobile Ad Hoc Networks". In *Proceedings of International Conference on Intelligent Systems and Computing: Theory and Applications*, pages 111–118, Ayia Napa, Cyprus, July 2006.

[C21] A. Mitrokotsa and C. Douligeris. "Intrusion Detection Using Emergent Self-Organizing Maps". In G. Antoniou et al., editor, *SETN 2006*, volume 3955 of *Lecture Notes in Artificial Intelligence*, pages 559–562, Heraklion, Greece, May 2006, Springer-Verlag.

Edited Books

[EB1] A. Mitrokotsa, S. Vaudenay, *Progress in Cryptology - Africacrypt 2012, Proceedings of the 5th International Conference on Cryptology in Africa*, Ifrane, Morocco, July 10-12, 2012, Lecture Notes in Computer Science, Vol. 7374.

[EB2] C. Dimitrakakis, A. Gkoulalas-Divanis, A. Mitrokotsa, V.S. Verykios, Y. Saygin, *Proceedings of the 1st International ECML/PKDD Workshop on Privacy and Security Issues in Data Mining and Machine Learning (PSDML 2010)*, Vol. 6549, Lecture Notes in Artificial Intelligence, Subseries of LNCS Springer.

[EB3] Q.Z. Sheng, A. Mitrokotsa, S. Zeadally, Z. Maamar, *Proceedings of the 4th International Workshop on RFID Technology - Concepts, Applications, Challenges IWRT 2010*, in conjunction with ICEIS 2010, Funchal, Madeira - Portugal, 8 - 12 June 2010, SciTePress Portugal, ISBN:978-989-8425-11-9.

[EB4] Q.Z. Sheng, A. Mitrokotsa, S. Zeadally, Z. Maamar, *Proceedings of the 3rd International Workshop on RFID Technology - Concepts, Applications, Challenges IWRT 2009*, in conjunction with ICEIS 2009, Milan, Italy, May 2009, INSTICC Press Portugal, ISBN: 978-989-8111-94-4.

Peer Reviewed Chapters in Books

[CB1] A. Mitrokotsa, M. Beye, P. Peris-Lopez, Chapter: "Threats to Networked RFID Systems". In Book: Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks. Eds. D. Ranasinghe, M. Sheng, S. Zeadally. Springer-Verlag., 2011, ISBN: 978-3-642-03461-9.

[CB2] A. Mitrokotsa and C. Douligeris. Chapter: "Integrated RFID and Sensor Networks: Architectures and Applications", In Book: *RFID and Sensor Networks: Architectures, Protocols, Security and Integrations.* Wireless Networks and Mobile Communication Series, pages 511–535. Auerbach Publications, CRC Press, Taylor and Francis Group, LLC 2010, ISBN: 978-1-4200-4288-7.

[CB3] A. Mitrokotsa and T. Karygiannis. Chapter: "Intrusion Detection Techniques in Sensor Networks", In Book: *Wireless Sensor Network Security*, pages 251–272. Cryptology and Information Security Series. IOS Press, 2008.

[CB4] A. Mitrokotsa and C. Douligeris. Chapter: "Denial of Service Attacks" In Book: *Network Security: Current Status and Future Directions*, pages 117–134. John Wiley and Sons. John Wiley and Sons, June 2007.

[CB5] A. Mitrokotsa and C. Douligeris. Chapter: "DoS Attacks and E-Government", In Book: *Secure eGovernment Web Services*, pages 124–142. Idea Group Publishing, Hershey PA, USA, 2007.

reprinted in:

Information Security and Ethics: Concepts, Methodologies, Tools, and Applications, Information Science Reference, 2008, IGI Global.

Thesis

[T1] A. Mitrokotsa. *Intrusion Detection in Computer Networks Using Machine Learning Algorithms.* PhD thesis, Department of Informatics, University of Piraeus, Greece, 2007.

Technical Reports

[R1] C. Dimitrakakis and A. Mitrokotsa, "Statistical Decision Making for Authentication and Intrusion Detection", *IAS Technical Report IAS-UVA-09-03*, April 2009.

[R2] C. Dimitrakakis, B. Nelson, A. Mitrokotsa and B. I.P. Rubinstein, "Robust, Secure and Private Bayesian Inference", *CoRR abs/1306.1066*, 2013.

[R3] I. Boureanu, A. Mitrokotsa and S. Vaudenay, "Practical & Provably Secure Distance-Bounding", *IACR Cryptology ePrint Archive 2013: 465 (2013).*

Popular science articles - Other publications

[O1] A. Årnes, J. Aguado, E. Boschi, R. Benito Cortiñas, F. Gaudino, G. Hobgen, T. Karagiannis, A. Mitrokotsa, I. Naumann, P. Papadimitratos, M. Papadopouli, G. Roussos, and K. Tsakona, "Mobile Identity Management", *ENISA Position Paper*, 13 April 2010.

[O2] I. Askoxylakis, P. Belimpasakis, M. Broda, L. Buttyan, S. Gorniak, S. Hoemstra de Grot, S. Ioannidis, P. Kijewski, A. Merle, A. Mitrokotsa, A. Munro, O. Popov, C.W. Probst M. Rohr, L. Romano, C. Siaterlis, C. Vishik, S. Zanero, "Priorities of Research on Current & Emerging Network Technologies", *ENISA Position Paper*, 20 April 2010.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-15355-112991-49

Name of applicant
Sabelfeld, Andrei

Date of birth
741110-8876

Title of research programme

Appendix N

Budget and research resources

Budget justification

Andrei Sabelfeld (PI) is also the principal investigator for the ERC project ProSecuToR. We are seeking to support 20% of his full working time.

Katerina Mitrokotsa, the co-applicant on this proposal, is the principal investigator for EU and STINT projects. We request to grant 5% of her full working time.

We are seeking to support 80% of the full working time for a PhD student to accelerate the achievement of the project's goals. The student will be supervised by Andrei and co-supervised by Katerina.

In addition to the personnel costs, the budget contains articles for conference and project meetings travel, for printing licentiate and PhD theses, premises, and for computer support.

The current funding resources are summarized as follows.

Person (role)	Status	Funding source	Period	Total KSEK
A. Sabelfeld (PI)	Granted	ERC	2013–17	15,000
A. Sabelfeld (co-applicant)	Applied	VR framework	2015–18	20,000
K. Mitrokotsa (PI)	Granted	EU	2013-16	894
K. Mitrokotsa (PI)	Granted	STINT	2014-15	149
K. Mitrokotsa (PI)	Applied	VR (junior researcher)	2015-19	5,000

VETENSKAPSRÅDET THE SWEDISH RESEARCH COUNCIL	Kod 2014-15355-112991-49	Dnr 2014 -
	Name of applicant Sabelfeld, Andrei	
	Date of birth 741110-8876	**Reg date** 2014-04-09 11:03:26

Project title

DecentLP: Robust decentralized location privacy

NT

NT-2

Research grants NT April 9, 2014
Project Research Grant
*Övrigt generellt
Chalmers tekniska högskola

Appendix S

Signatures

2015	2016	2017	2018	2019	
1107	1121	1173	1197	1288	2015-01-01 -- 2019-12-31

Applicant **Date**

Head of department at host University **Clarifi cation of signature** **Telephone**

A signature on the application is required not only from the applicant but also from the authorised representative of the administrating organisation/institution or equivalent (normally the head of the department or establishment where the research is to be conducted). The signature confirms that the department can accommodate the proposed research, position or equipment; that the costing in the application is approved for the department's part, that any proposed experimentation on human or animal subjects has been reported, and that the applicant has reported any secondary occupations and commercial ties (s)he may have, and nothing inconsistent with good research practice has thereby emerged. The applicant must have discussed these conditions with the representative of the administrating organisation/institution or equivalent before the latter approves and signs the application.

NOTE the exceptions!
Please note that a different procedure applies for the following types of grants:

- Infrastructure- Operation Grants
- Infrastructure- Grants for Expensive Equipment
- Infrastructure- Grants for Large Databases
- Framework Grant SIMSAM
- International Recruitment

For these types of grants the vice-chancellor, instead of the head of department, must sign Appendix S. Thereby (s)he confirms the commitments of the administrative organization. The details are specified in the Call for Proposals, published at www.vr.se.

Vetenskapsrådets noteringar
Kod

2014-15355-112991-49