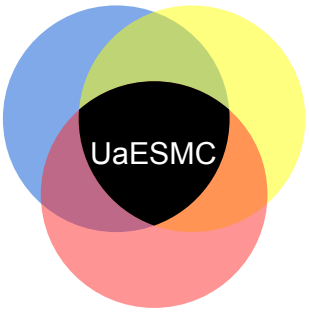

Project N°: **FP7-284731**

Project Acronym: **UaESMC**

Project Title: **Usable and Efficient Secure Multiparty Computation**

Instrument: **Specific Targeted Research Project**

Scheme: **Information & Communication Technologies**

Future and Emerging Technologies (FET-Open)

Deliverable D6.3
Intermediate plan for the use and dissemination of foreground knowledge

Due date of deliverable: 31st January 2013

Actual submission date: 31st January 2013

Revision date: 26th March 2013

Start date of the project: **1st February 2012** Duration: **36 months**

Organisation name of lead contractor for this deliverable: **CYB**

Specific Targeted Research Project supported by the 7th Framework Programme of the EC		
Dissemination level		
PU	Public	✓
PP	Restricted to other programme participants (including Commission Services)	
RE	Restricted to a group specified by the consortium (including Commission Services)	
CO	Confidential, only for members of the consortium (including Commission Services)	

Executive Summary:

Intermediate plan for the use and dissemination of foreground knowledge

This document summarizes deliverable D6.3 of project FP7-284731 (UaESMC), a Specific Targeted Research Project supported by the 7th Framework Programme of the EC within the FET-Open (Future and Emerging Technologies) scheme. Full information on this project, including the contents of this deliverable, is available online at `http://www.usable-security.eu`.

Based on the results of the first year of UaESMC, this deliverable describes the likely follow-up actions during and after the project for exploiting the knowledge acquired during the project. In particular, the deliverable states what kinds of actions are planned for the SMC methods developed in UaESMC to be included in Sharemind, how much extra effort that will take, and what are the possible sources of funding those efforts.

List of Authors

Dan Bogdanov (CYB)

Contents

Chapter 1

Introduction

This document gives an overview on how the results of this project will reach wider use in technological platforms and applications. We describe the kinds of artifacts that the project will produce and how these artifacts can be used to develop new research results, new technologies and real-world applications. This includes direct exploitation and also dissemination of secure multiparty computation (SMC) to enable the large-scale use of the results.

We will consider the following main kinds of artifacts:

1. reusable secure multiparty computation protocols,
2. algorithms adapted specially for secure multiparty computation,
3. application prototypes that use secure multiparty computation and
4. best practices for deploying and applying secure multiparty computaiton.

While our exploitation strategy focuses on how to exploit the created artifacts in the Sharemind secure multiparty computation system, some of the techniques are applicable also to other secure multiparty computation protocols. There are some restrictions, depending on the kind of artifact. For example, secure multiparty computation protocols are quite specific and a protocol that works efficiently for one paradigm (e.g., secret sharing) will not be as efficient with another (garbled circuits).

However, algorithms that are designed to be implemented using secure multiparty computation are relatively independent of the paradigm. For example, an oblivious sorting algorithm may be suitable for use with a wide range of secure computation protocols. Similarly, best practices for setting up and maintaing secure multiparty computation applications have both generic and protocol-specific provisions.

Finally, we will discuss exact steps on how to plan exploitation. This includes determining what has to be implemented first, how should the work be funded and how it should be marketed to end users. We stress the usefulness of pilot studies with actual end users and discuss integration issues with existing software platforms.

Chapter 2

Reusable secure computation protocols

2.1 Description

Reusable secure computation protocols make SMC systems more economic to use, because new applications can be put together from existing building blocks without needing to develop new protocols. Ideally, these protocols preserve security under composition so that the user can run them in any order without losing the guarantees of secure multiparty computation.

This last property also makes secure computation protocols *programmable*—one can build a domain-specific programming language that provides secure data types and operations. The runtime environment of that language can then execute secure multiparty computation protocols to guarantee the security of the data. There are three main development directions for secure multiparty computation protocols:

1. **Functionality**—develop new protocols to secure process different types of data.
2. **Efficiency**—make the protocols more efficient by reducing the secure computation overhead.
3. **Security**—make the protocols more secure by protecting against more complex attacks or different numbers of corrupt parties.

A protocol development effort can follow any number of these directions simultaneously. For example, one could design a really efficient protocol for securely processing fixed-point numbers in the presence of a malicious adversary.

However, it also makes sense to pursue individual directions, as the insights gained in this way can later be used to improve other protocols. For example, by developing a generic strategy for ensuring security against a malicious server, we can apply this to protocols that process any data type.

In UaESMC, we work in all these directions, with a special focus on usability and efficiency. We are focusing on protocols that will provide practical security gains in real-world applications on real-world data sizes. However, we are also looking at fundamental approaches for improving the security of protocols.

2.2 Ongoing work and results

Currently, UaESMC is not focusing on protocol development, as the Sharemind secure multiparty computation system developed by CYB has provided a sufficient set of efficient operations on both integer and floating point data. This has allowed UaESMC to focus on solving practical problems and developing high-level algorithms and applications.

However, UaESMC has identified two shortcomings in the current Sharemind design. First, sometimes it is really hard to find three hosts for a secure computation system. In these cases, two is the intuitive number and two hosts are easier to find. Second, some application scenarios require that confidentiality and correctness are protected against a malicious adversary.

Based on these observations, UaESMC has started looking at efficient two-party protocols for several security levels. More specifically, CYB is evaluating existing protocols and looking for an approach that could extend the efficient design of SHAREMIND to a two-party model with different security guarantees. This work is underway and we expect results by the end of the second year of UaESMC.

2.3 Possible exploitation strategies

The exploitation of reusable secure multiparty computation protocols makes the most sense if these protocols are packaged into a runtime that allows programmability using a special (possibly embedded) domain-specific language.

Such secure multiparty computation frameworks enable easier application development, as one does not need to re-develop the protocols and can just invoke them as needed. Examples of downloadable frameworks include SHAREMIND[1], VIFF[2], Fairplay[3] and SEPIA[4].

New frameworks emerge as new protocols are developed. Some frameworks like VIFF and SHAREMIND 3 have the capability to support several protocol suites. Therefore, publishing protocol descriptions is a dissemination strategy that may lead to exploitation, as framework providers implement the protocols to enhance the capabilities of their frameworks.

It is also possible to not publish protocol designs and keep them proprietary. This way, the secure multiparty computation framework implementation may be able to gain advantages compared to other frameworks which cannot implement the same approaches. However, keeping the protocols secret will complicate proving the security claims. If third parties cannot verify the security properties of the system, the general trust against the system may erode.

2.4 Dissemination and exploitation of protocols from UaESMC

We plan to publish the results of fundamental protocol research in academic papers to validate the approaches with the global cryptography/security community. We also plan to implement more promising protocols in the SHAREMIND system so we can easily measure their performance as primitive operations and also in applications.

The SHAREMIND system is not open source at this time. However, CYB is regularly posting freely downloadable versions of the SHAREMIND Software Development Kit for academic use and evaluation. We believe that this increases the acceptance of the new technology and helps students and hobbyists to play around with it.

[1] The Sharemind Software Development Kit - `http://sharemind.cyber.ee`
[2] Virtual Ideal Functionality Framework - `http://viff.dk`
[3] Fairplay and FairplayMP - `http://www.cs.huji.ac.il/project/Fairplay/`
[4] Security through Private Information Aggregation - `http://sepia.ee.ethz.ch`

Chapter 3

Algorithms adapted for secure multiparty computation

3.1 Description

Thousands of algorithms have been developed for efficiently solving a large variety of computational tasks. All of them have their performance profiles, making them either practical or impractical for running on computers. Sometimes, an algorithm with an excellent theoretical complexity (e.g., constant or linear complexity) is totally infeasible in practice because the constants in the complexity equation are infeasibly large.

Similarly, an algorithm that is efficient in solving a task on everyday computing hardware, may not be the best solution for a secure multiparty computation system. The actual performance of a data processing algorithm on a secure multiparty computation system depends on the protocols that are performing the primitive operations in the secure computation platform.

To illustrate this, consider the following example. In most secure multiparty computation systems based on secret sharing, operations on vectors are significantly more efficient than operations on single inputs. On standard hardware, one thousand integer multiplications may take 100–1000 times more time than a single multiplication. However, it has been observed on some secure multiparty computation platforms that the running time of a protocol performing one thousand parallel integer multiplications can be just a few times longer than the running time of a protocol performing just one multiplication. In these cases, we need to select algorithms that employ parallel operations as much as possible.

Based on these observations, we identify two significant algorithm development tasks to support the development of secure multiparty computation applications.

1. **Adapting** known efficient algorithms for use with secure multiparty computation platforms. The algorithms are modified to take maximum advantage from the speedups resulting from the use of parallel operations.

2. **Designing** new algorithms that are efficient in secure multiparty computation platforms. Instead of starting with a known algorithm, we start with the mathematical foundations of the task and construct a highly vectorized algorithmic solution.

Adapting existing algorithms is more efficient as we don't need to go through the whole process of algorithm design and validation. However, we can achieve grater performance gains by starting from scratch and designing the whole algorithm in a parallel manner.

3.2 Ongoing work and results

UaESMC has identified several areas where we are adapting and designing algorithms to solve real-life problems. Currently, the focus is on the following problems.

1. **Statistical analysis.** UaESMC has been developing algorithms and implementations for applying secure multiparty computation to compute descriptive statistics, perform statistical tests, outlier detection, sorting, linear regression and data management tasks like privately linking tables and deriving new tables from existing ones.

2. **Optimization.** UaESMC has been prototyping genetic algorithm based solutions for finding shortest paths and solving the secure subset covering problem.

The developed algorithms have been implemented as proof-of-concept solutions, mostly on the Sharemind platform. The goal has been to validate the approach and get an understanding of what is possible and what is infeasible.

We have established that secure multiparty computation can be successfully used for performing statistical studies. We have been able to deploy algorithms for various phases in such studies and we believe that there are no fundamental obstacles in developing more. Therefore, we consider secure statistical studies a breakthrough application with confirmed exploitation possibilities.

Optimization and search problems are important in UaESMC since they are also important to the interviewees. However, our results in designing efficient algorithms for secure optimization are mixed. We have had promising results in solving the subset covering problem. The solution was demonstrated as a part of an expert system design that gives optimal suggestions to its users based on a database of rules. However, a similar approach to finding shortest paths in a graph was less successful. Work in this area is still ongoing and we hope to have more conclusive results later.

UaESMC will continue to develop algorithms for all the listed areas and other focus areas of the project.

3.3 Possible exploitation strategies

If reusable secure protocols are just building blocks that do not guarantee the feasibility of practical applications, the existence of efficient algorithms for a particular task is a strong enabler for an application. If we can demonstrate that we can successfully securely compute a useful output from confidential inputs, we can package the resulting work into an application and easily provide value to the end user.

There are two exploitation strategies for algorithms that run using secure multiparty computation. The obvious approach is to package them into a specific application that solves a problem. The application ensures that the inputs to the algorithm are available and the outputs are published to the respective parties. The algorithm fulfils the part of the business logic that transforms inputs to outputs. In this case, the algorithms are part of the proprietary application design. The developer of the application uses either published algorithm designs or develops an efficient solution in-house. This approach makes application design more efficient in the short term, but can increase costs, if the same algorithm needs to be adapted for several applications.

Alternatively, we can modify the algorithm implementation to be reusable and build a more complex software platform that supports several applications. For example, we can build a database and application server based on secure multiparty computation that contains stored procedures that perform a certain algorithmic task on the data stored in the system. This approach is very similar to how modern ICT systems are built, with complex middleware that can solve more complex task than just arithmetics. The application is then reduced to data model descriptions and calls to the algorithms implemented in the middleware.

The upfront cost of developing such an application platform is high, but the reuse cost is negligible and the ease of use is also improved. Furthermore, such a platform can be the foundation for a cloud-based technology offering, whether in the Platform-as-a-Service or Software-as-a-Service form. By creating the necessary interfaces, we could make the technology available to a larger number of users.

In either case, algorithm designs can be published as academic papers or tutorials, but it is not critical for proving the security of the system as the latter is more dependent on the security and composability of the underlying secure multiparty computation platforms. The correctness of the algorithm can be validated

by testing. This allows the algorithm designs to be proprietary and a motivation for businesses to commit resources to designing better algorithms than the competition.

3.4 Dissemination and exploitation of algorithms from UaESMC

UaESMC is actively looking for pilot projects to validate its secure statistics technology. CYB has performed several presentations to stakeholders in both public and the private sector. CYB has identified promising leads for applications of secure multiparty computation in performing privacy-preserving statistics on several linked databases. In the coming year, CYB will pursue these leads in the hope of negotiating a pilot project that would let the statistical algorithms developed in UaESMC to be tested in practical applications.

CYB is also evaluating the possibility of developing a cloud-based offering of secure multiparty computation technology. Since the effort to achieve this is large and requires further research, CYB is participating as a partner in the EU FP7 integrated project proposal called PRACTICE with the intention to take the theoretical results from UaESMC into practice and deploy them on the public cloud to improve the availability of secure statistical technology for all European stakeholders.

The rest of the results from the algorithms research are currently of an academic value and UaESMC partners will continue work to decide whether to publish the algorithms as isolated results or as parts of an application case study.

Chapter 4

Applications using secure multiparty computation technology

4.1 Description

The true exploitation of secure multiparty computation technology becomes possible with real-world applications that solve a problem for a customer. Secure multiparty computation is a disruptive technology that allows applications to be created where none were possible before. We can show that data can be collected and processed without letting anyone except for the owner access the individual values.

However, the price for gaining this property in an applications is the deep integration of secure multiparty computation technology into the whole application. Secure multiparty computation is not another layer above or on the side of an application—to be really effective at guaranteeing security, SMC must be the layer underneath the whole application. The reason is simple—standard applications require that their input and output data is in a plaintext form that is clearly understandable to the underlying computer (and anyone observing its processes).

SMC replaces the basic primitive operations on data with ones that do not require plaintext access to inputs. However, it is not possible to directly translate standard computer software to run on SMC platforms for two reasons. First, as stated earlier, different algorithms are efficient on SMC systems, making a direct translation inefficient. Second, if an algorithm makes decisions on the input data, its execution will leak information about the input values. Some algorithms can be rewritten to remove branching on private data, making them straight line programs. However, this is again an algorithmic task.

Another aspect of SMC application deployment is the possible requirement of multiple parties to meet the security guarantees. The application developer has to find the stakeholders with the capability of hosting the servers of a secure multiparty computation system. In theory, this is made easier by cloud computing—one could just use a cloud server, if one does not have host capabilities. However, SMC protocols and algorithms must then be packaged into a platform that is easily exploitable on the cloud.

Finally, to provide the best possible privacy, data collection interfaces must also be changed to ensure that data is protected at the source. Similarly, query interfaces must know the protection technique to ensure that the results are reconstructed as late as possible.

All these factors affect the direct exploitation of SMC technology and require us to take further steps to make enough tools and algorithms available on SMC platforms. In the first phases of SMC exploitation, building SMC applications with little reusability is justified as we experiment with different approaches and decide what parts of the application could be made reusable. However, the economic exploitation of SMC requires the creation of an application platform that hides the cryptographic complexity from the developer.

4.2 Ongoing work and results

UaESMC has studied the problem statements of various stakeholders and is developing algorithms and mechanisms that will enable the creation of the respective applications. Currently, UaESMC is targeting the following applications.

1. Joint statistical studies among multiple organizations (medical institutions, companies).
2. Privacy-preserving statistical studies over several linked government databases.
3. Expert systems that solve optimization tasks on private inputs.

At this time, UaESMC has successfully developed several fundamental algorithms that demonstrate the feasibility of the statistics applications. However, no fully functional prototypes have yet been developed.

4.3 Possible exploitation strategies

The development of information systems that use SMC technology is no different from developing other ICT systems. We start with a customer need, perform a requirements analysis, design the application architecture, develop and deploy all the components.

The main challenge with SMC applications is finding the customer who is willing to commit the extra resources needed for SMC to enjoy the unparalleled security guarantees. This is a challenge for dissemination—we must explain the merits of SMC and give explanations what kind of applications benefit most. Such dissemination can be in the form of articles in papers and magazines, both trade and research journals.

The exploitation startegy that the UaESMC consortium will take, consists of three steps:

1. **Inform** the possible stakeholders of the new technology to identify interested parties.
2. **Present** the technology to interested stakeholders and find our their needs.
3. **Develop** prototypes (or full applications) to demonstrate the capabilities of SMC.

4.4 From research to applications in UaESMC

The UaESMC consortium is actively informing stakeholders of SMC technology. We have started giving talks in security workshops, privacy conferences and research events. We are also preparing articles to both research and trade journals. For example, we submitted a paper to the ISACA Journal, detailing the use of SMC technologies in cloud applications. ISACA is a major international community of information security specialists. CYB employs several ISACA members who helped prepare the paper to make it more suitable for information security specialists in the community.

CYB has conducted several private presentations to stakeholders who have shown interest in secure multiparty computation. Some of these stakeholders have shown interest in using the technology and CYB is developing these leads further.

The consortium has not yet negotiated the development of any full applications or demonstrators, but we are hopeful that CYB will continue their efforts in making this happen. CYB has experience in bringing technologies like digital signatures, timestamping, electronic voting and other technologies from theory to practice. The first applications are usually developed in a close partnership with the customer and product development starts after the first deployments have been successful. CYB has also shown readiness in committing developer resources to develop the missing applications components for the first customers as an investment for future deployments.

Chapter 5

Best practice for the development and use of SMC applications

5.1 Description

SMC is a complex technology that must be used deployed following certain rules. These rules are needed to ensure that secure multiparty computation is applied in the most effective way and its security assumptions hold.

The best practices for working with SMC applications will be developed based on the underlying security research, practical ICT security considerations and software engineering practices. These materials will be of use to various specialists.

1. Information security specialists will use them to evaluate the security guarantees of the system and how it integrates with the rest of the enterprise software.

2. ICT system developers will use the guidelines during the requirements analysis and development of the customer's application.

3. ICT system maintainers and system administrators will use the guidelines to ensure that the system is operated and disposed of without compromising confidentiality.

5.2 Ongoing work and results

UaESMC is not focusing on developing procedures and standardizing them as these activities are not in the scope of the project. However, developing application prototypes and models requires some insight into how they would be developed later.

Therefore, our work on application deployment models can be considered as a step in the direction of developing guidelines for deploying secure multiparty computation.

5.3 Possible exploitation strategies

There are two main dissemination and exploitation paths for best practices. The first is to create developer references, examples and tutorials for the SMC platform. These assist the user of the platform in applying it the correct way. Such work is up to the developer of the SMC application platform.

The second approach is to get involved in international standardization. SMC is a technology with several standardization opportunities (distributed storage, data collection, application models). Standardization will serve two purposes. First, it will encourage a multitude of secure computation technologies to be developed by different technology providers. This, in turn reduces the danger of being dependent on a single implementation.

The second benefit of standardization results from standardizing SMC as a technology that gives certain systems a certain property. For example, if SMC is shown as an enabling technique for privacy or confidentiality in an industrial sector, the stakeholders in that sector may become interested if they have problems processing private or confidential data in their work.

5.4 Dissemination of guidelines for exploiting UaESMC results

The guidelines for exploiting UaESMC results will be developed together with any applications (or prototypes).

CYB personnel are performing the role of Estonian experts in the subcommittee 27 of ISO/IEC JTC 1. This subcommittee works on information security techniques and has recently started considering secure multiparty computation as a possible privacy enhancing technology. For example, the ISO/IEC 29101 Privacy Architecture Framework lists SMC as a component for processing Personally Identifiable Information (PII) with good security.

CYB is informing the UaESMC consortium of further developments and if there is a need to take further action.

Chapter 6

Dissemination of Scientific Results

To reach the vision of UaESMC, scientific advances in several different areas are necessary. To make this vision a reality, it has to be communicated as widely as possible. We have identified the following three communities as the target audiences of our dissemination efforts.

Researchers This group encompasses the researchers and developers in the information security and cryptography community that may be interested in considering the techniques and methods proposed in the UaESMC project for their own developments in privacy-preserving functionalities and applications. It also includes the experts and academic peers of the project members in other areas of computer science, where the results of UaESMC may have an impact.

Potential users of SMC / stakeholders This group contains the practitioners — the designers and developers of IT-systems, as well as the managers in the organizations developing the systems that may benefit from the use of SMC techniques. It also includes stakeholders, meaning groups who potentially would be connected to different implementation aspects of SMC.

General public The entire society will benefit from the availability of SMC techniques through improved guarantees for their privacy. To make the society accept these techniques and the guarantees associated with them, its awareness of their possibilities and limitations has to be sufficiently high.

For the dissemination among researchers, conferences and journals are the typical venues, with the emphasis on the conferences due to the traditions of publishing in the field of computer science. While the biggest achievement of UaESMC may be the overall framework, it does not lend itself well to a publication in a conference or a journal paper. Suitable pieces of the results of UaESMC must be identified, each of which can be published in a venue aligned with its topic.

We can identify the following areas of computer science and related fields, in which UaESMC may produce new results.

Innovation communication UaESMC has chosen a novel approach of communicating with the potential user and stakeholder communities of its results. We foresee the repeatability of this approach for other kinds of technologies. Therefore there is an interest towards these communication methods in the whole innovation and technology communication community.

ICT development and adoption The involvement of potential users and stakeholders in the development process of SMC enables UaESMC to contribute to the field of ICT development and adoption. The novelty of involving users and stakeholders in the early stages of the development process allows UaESMC to discuss the user and stakeholder perspective of a technology that is still in its early stages of development.

Secure multiparty computation techniques UaESMC may produce more efficient protocols for certain primitive computational operations, satisfying certain privacy and correctness conditions. Through

UaESMC, these protocols will find use in the Sharemind SMC framework. Similar protocols may be useful for other SMC frameworks and thus interesting for the designers and developers of these frameworks.

Privacy-preserving algorithms for specific tasks UaESMC investigates certain concrete algorithmic problems to which many interesting tasks can be reduced to. The privacy-preserving protocols for these problems may be quite dissimilar to the combinations privacy-preserving protocols for primitive computational operations.

SMC frameworks The development of new protocols for either primitive operations or more complex tasks may affect the design of whole SMC frameworks, as these protocols have to be smoothly integrated and made available to the applications built on top of these frameworks.

Theory of SMC Certain aspects of the theoretical underpinnings of SMC (protocols providing privacy, but no correctness against active adversaries) have not been well-studied so far. At the same time, they may affect the design space of SMC applications that UaESMC is researching.

Applications of game theory in SMC Taking into perspective that adversarial and selfish behavior, as well as the underlying incentives of the different parties, are key elements in SMC settings, UaESMC will try to model some of its problem using motivation, notions and techniques from (algorithmic) game theory and mechanism design.

Construction of privacy-preserving applications The ultimate goal of UaESMC is to simplify the construction of applications using SMC, and we expect to have results directly addressing this goal.

In addition to regularly publishing at conferences and journals, we also plan to organize a dissemination workshop of UaESMC during its third year. This workshop will target academics and graduate students in order to share knowledge and project results to academic communities and verify the scientific outcomes. Besides the presentations by the project members, invited guest speakers will add their reflections on the reliability and applicability of the results.

For the dissemination among the potential users of SMC technologies, we have planned to use the following activities and channels of distributing information:

Whitepapers, flyers, etc. This sort of information brochures will be produced towards the end of the project, containing the precise description of technical details in an easily accessible language. These brochures will be distributed on innovation-related conferences and events, but also distributed through the targeted professional community networks.

Presentations at conferences, workshops, training schools If the opportunity presents itself, the participants of UaESMC will explain the benefits of SMC in general and UaESMC technologies in particular at the meetings of information systems developers, managers, procurers, etc.

Overview articles in trade magazines Such articles will appear in journals and magazines published by professional societies, and circulated among its members.

Standardization We are already active in ISO, standardizing privacy technologies. In the future, the technologies developed in UaESMC will be included in these activities.

Dissemination workshop This dissemination workshop will be organised in conjunction with some security or ICT related conference which brings together academics, business and government representatives (e.g. ICEGOV, International eDemocracy Conference). The aim is to disseminate UaESMC related scientific and practical knoweldge to the mixed audiences in order to verify the scientific results and promote the project results and SMC in general to potential interested groups.

For the dissemination among general public, we plan to publish articles in science communication online portals, popular science magazines or popular computing related magazines. During the second and third year of the project, we will also produce graphical material explaining SMC to wider audiences, to spark discussion and find innovative uses.

In the following, we will discuss in more detail the publication strategy of UaESMC, pointing out the potential publishable results of the project (Sec. 6.2), as well as the potential venues for them.

6.1 Venues for scientific results

The different kinds of scientific results of UaESMC will be attracted by the publication venues of different areas. Here we provide a selection of these venues. For venues with periodic calls for papers, we also indicate, to which time of the year the deadlines typically fall.

6.1.1 Innovation communication

The results of UaESMC were presented on the European Communication Conference organized by ECREA (European Communication Research and Education Association). In the future we will aim to present the results of UaESMC in smaller-scale and more focused seminars and conferences organized by ECREA and also on other communication related venues.

6.1.2 ICT development and adoption

We are aiming to present the results of UaESMC on communication conferences and other venues that take more interdisciplinary approach.

- ICA 2013 conference Challenging Communication Research. Takes place in June, submission accepted.
- 1st International conference on Internet Science. Takes places in April, paper submitted.

6.1.3 Security and cryptography

There are several major annual scientific conferences on the general topic of information security, each of which would be a suitable venue for a significant result from UaESMC. Among those are

- ACM Conference on Computer and Communication Security (CCS). Takes place in Autumn. Typically, the deadline for submitting papers (the "CfP deadline") is in April or May.
- IEEE Symposium on Security and Privacy. Takes place in May. CfP deadline typically in October – November.
- Network and Distributed System Security Symposium (NDSS). Takes place in February. CfP deadline typically in August.
- USENIX Security Symposium. Takes place in August. CfP deadline typically in February.
- European Symposium on Research in Computer Security (ESORICS). Takes place typically in September. CfP deadline typically in March.

The first four conferences of this list are of American origin, but may take place elsewhere from time to time.

For a major result of cryptographic nature, the flagship conferences of the International Association of Cryptographic Research (IACR) provide a suitable venue:

- Eurocrypt — in Spring, somewhere in Europe. CfP deadline typically in October.

- CRYPTO — in mid-August, in Santa Barbara, CA, USA. CfP deadline typically in February.
- Asiacrypt — in November-December, somewhere in Asia (or Australia). CfP deadline typically in May.

Beside the large conferences, there are also many smaller *general security* conferences, which are too numerous to be listed here. Both CYB and KTH are involved in the organization of the annual Nordic Conference in Secure IT Systems (Nordsec), which will take place for the 18th time in October, 2013.

In the following we list some specialized security conferences that fit well with the topics of UaESMC.

6.1.3.1 SMC techniques and privacy

- Symposium on Privacy Enhancing Technologies (PETS). Takes place in July–August. CfP deadline typically in February.
- Conference on Privacy, Security and Trust (PST). Takes place in July–August. CfP deadline typically in March.
- IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBsec). Takes place in July. CfP deadline typically in February.

6.1.3.2 Privacy-preserving specific algorithms

Application specific algorithms developed during UaESMC can be presented in conferences related to the specific case studies. There are several scientific conferences and journals on topics related to inter domain routing and QoS-aware networks:

- ACM SPAA: June/July, Deadline: January/March
- IEEE INFOCOM: Spring, Deadline: July
- The IEEE/ACM Transactions on Networking: bimonthly journal
- CSAC: December, Deadline: June
- IEEE/IFIP Network Operations and Management Symposium: January, Deadline: August

6.1.3.3 Secure systems

- Applied Cryptography and Network Security (ACNS). Takes place in June, typically in Asia, sometimes elsewhere. CfP deadline typically in February.
- Annual Computer Security Applications Conference (ACSAC). Takes place in December, typically in the Southern USA. CfP deadline typically in May–June.
- ACM Symposium on Applied Computing (ACM SAC) has several tracks where secure systems would be on topic. Takes place in March. CfP deadline typically in September.
- Trustworthy Global Computing (TGC). Takes place in late Summer or in Autumn.
- Symposium On Usable Privacy and Security (SOUPS). Takes place in July, in USA. CfP deadline typically in March.

6.1.4 Game-theoretic and Mechanism Design aspects

- ESA (European Symposium on Algorithms). September 02-04, 2013 (Sophia Antipolis, France). Submission: April 22, 2013.
- RANDOM-APPROX (Intl. Workshop on Approximation Algorithms for Combinatorial Optimization Problems, Intl. Workshop on Randomization and Computation). August 21-23, 2013 (UC Berkeley, USA). Submission: April 17, 2013.
- WINE (Web Interaction and Network Economics). December 2013 (Harvard University in Boston, MA). Submission: August 2013.
- SAGT (International Symposium on Algorithmic Game Theory). October 21-23, 2013 (Aachen, Germany). Submission: May 22, 2013.
- STACS (Symposium on Theoretical Aspects of Computer Science). March 5-8, 2014 (Lyon, France). Submission: September 2013.

6.2 Potentially publishable results

Below we list the potential publishable results and their sets of UaESMC, giving the following data on it. This list is definitely not exhaustive.

Description A couple of sentences about the result.

Dependencies Which other items in this list must be available for us to obtained the described result?

Area Into which area of computer science or related fields does this potentially publishable result belong to?

Time-frame When do we expect to have this result in a shape that allows the preparation of a conference or journal paper?

Suitable venues Which conferences / journals are the most suitable for this result?

Linear programming based on problem transformation

Description A linear programming (LP) problem is privately transformed to a different LP problem, such that the original one cannot be recognized from the transformed one. The transformed problem can be solved in public. The solution for the original problem can be easily recovered from the solution to the transformed problem and the transformation. The privacy-preservation of the transformation relies on novel hardness assumptions on computations with real numbers.

Area Privacy-preserving solution for a specific task.

Time-frame Spring 2013.

Suitable venues Large conferences, the program committee of which is capable of evaluating, and taking the risk of accepting new cryptographic assumptions. As the LP task is not related to cryptography, we feel that we have better chances at general security conferences.

Privacy-preserving statistics (algorithm design and implementation)

Description Secure multiparty computation is used to solve statistical analysis problems. UaESMC has developed a set of statistical techniques and algorithms that can compute various statistical analysis tasks. Both the algorithm design and applications are publishable resuls.

Area Privacy-preserving solution for a specific task.

Time-frame Summer-Autumn 2013.

Suitable venues Privacy and security conferences. Data mining conferences.

Privacy-preserving statistics (applications)

Description Secure multiparty computation is used to solve statistical analysis problems. UaESMC has developed a set of statistical techniques and algorithms that can compute various statistical analysis tasks. Both the algorithm design and applications are publishable resuls.

Area Privacy-preserving solution for a specific task.

Time-frame Autumn 2013.

Suitable venues Privacy and security conferences (possibly). Data mining conferences (probably).

Privacy-preserving, heuristic solving of NP optimization problems

Description Various heuristics for NP problems are implemented (mostly) on top of SMC platforms. These implementations are optimized, taking into account the performance profiles of privacy-preserving operations. We will learn, how the algorithmic techniques demanded by a particular heuristic are turned into a privacy-preserving protocol.

Dependency The proposed techniques may want to use privacy-preserving linear programming as a sub-protocol.

Area Secure multiparty computation technique.

Time-frame The first results have been obtained in 2012. More are expected in 2013–2014.

Suitable venues Security and privacy conferences. Even more suitable may be conferences on computer security applications. In papers, it is important to explain that the optimizations of the implementations according to the particularities of SMC frameworks are interesting and non-trivial.

Accountability towards the results of secure computation

Description An addition to SMC protocols that makes the participants in the computation committed to the result of that computation at or near the start of the protocol. The availability of such commitment allows more leeway in mechanism design.

Area Secure multiparty computation techniques, SMC frameworks.

Time-frame Late 2013.

Suitable venues Security conferences.

A privacy-preserving application

Description An SMC application prototype will be developed, deployed, and the users interviewed.

Dependency The necessary theoretical results, and the design of algorithms must be complete. Most likely, we need privacy-preserving statistics.

Area Construction of privacy-preserving applications.

Time-frame Spring-Summer 2014.

Suitable venues Conferences on computer security applications, conferences in the area of the prototype application (likely data mining). Venues on secure software engineering may also be suitable.

Privacy-preserving QoS routing

Description An inter-domain routing protocol that takes into account domain network metrics and enforces the participant privacy constraints.

Dependency The interplay with the game theoretic framework must be investigated to take into account competitive behaviors.

Area Application specific protocols.

Time-frame Late 2013.

Suitable venues Conferences on computer security applications, conferences on distributed algorithms, conferences on networking.

Privacy without correctness

Description Which protocols can still provide information-theoretic privacy, even if the number of actively corrupted parties is at least $n/3$ (where n is the total number of parties)? How can the allowed compositions be characterized?

Area Theory of SMC.

Time-frame In 2014.

Suitable venues Privacy and security conferences. The techniques we use will probably come from the areas of formal methods and programming languages, but the importance of the result may be difficult to characterize to these communities.

Implementation barriers for emerging technologies : stakeholder and user perspective

Description Interviews with potential stakeholders and users have given us insight on how those groups view the barriers that may hinder the implementation of the technology.

Area ICT adoption, user involvement.

Time-frame 2013

Suitable venues Technology innovation conferences.

User and stakeholder involvement in a technology development process

Description Discuss the benefits and dificulties of involving stakeholders and potential users in the development process of a novel, yet complicated emerging technology.

Area User involvement.

Time-frame 2013

Suitable venues Technology innovation conferences, communication conferences.

Communicating emerging technologies to non-experts

Description Discuss the methodological aspects of communicating a novel and emerging technology to the non-experts.

Area Technology communication, user involvement.

Time-frame 2013

Suitable venues Technology innovation conferences, communication conferences.