European Cooperation
in the field of Scientific
and Technical Research
- COST -

Brussels, 22 November 2013

COST 066/13

MEMORANDUM OF UNDERSTANDING

Subject : Memorandum of Understanding for the implementation of a European Concerted Research Action designated as COST Action IC1306: Cryptography for Secure Digital Interaction

Delegations will find attached the Memorandum of Understanding for COST Action IC1306 as approved by the COST Committee of Senior Officials (CSO) at its 188th meeting on 14 November 2013.

MEMORANDUM OF UNDERSTANDING
For the implementation of a European Concerted Research Action designated as

COST Action IC1306
CRYPTOGRAPHY FOR SECURE DIGITAL INTERACTION

The Parties to this Memorandum of Understanding, declaring their common intention to participate in the concerted Action referred to above and described in the technical Annex to the Memorandum, have reached the following understanding:

1. The Action will be carried out in accordance with the provisions of document COST 4114/13 “COST Action Management” and document COST 4112/13 “Rules for Participation in and Implementation of COST Activities” , or in any new document amending or replacing them, the contents of which the Parties are fully aware of.

2. The main objective of this Action is to increase cooperation between European experts in cryptography with the main goal of designing, analyzing and implementing secure protocols that allow citizens and entities to interact securely with each other.

3. The economic dimension of the activities carried out under the Action has been estimated, on the basis of information available during the planning of the Action, at EUR 64 million in 2013 prices.

4. The Memorandum of Understanding will take effect on being accepted by at least five Parties.

5. The Memorandum of Understanding will remain in force for a period of 4 years, calculated from the date of the first meeting of the Management Committee, unless the duration of the Action is modified according to the provisions of section *2. Changes to a COST Action* in the document COST 4114/13.

A. ABSTRACT AND KEYWORDS

As increasing amounts of sensitive data are exchanged and processed every day on the Internet, the need for security is paramount.

Cryptography is the fundamental tool for securing digital interactions, and allows much more than secure communication: recent breakthroughs in cryptography enable the protection - at least from a theoretical point of view - of any interactive data processing task. This includes electronic voting, outsourcing of storage and computation, e-payments, electronic auctions, etc.

However, as cryptography advances and becomes more complex, single research groups become specialized and lose contact with “the big picture”. Fragmentation in this field can be dangerous, as a chain is only as strong as its weakest link. To ensure that the ideas produced in Europe’s many excellent research groups will have a practical impact, coordination among national efforts and different skills is needed.

The aim of this COST Action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments. The Action will foster a network of European research centers thus promoting movement of ideas and people between partners.

Keywords: Cryptography, Security, Interactive Computation, Secure Data Processing.

B. BACKGROUND

B.1 General Background

Cryptography is a powerful tool that can be used to protect the secrecy, the integrity, and the authenticity of data. The rigorous and scientific study of cryptography - what is called "modern cryptography" - originated with the advent of public-key cryptography at the end of the 70s. However, applying these techniques in practice is a highly challenging task. Indeed, this is reflected by the fact that the way that citizens and entities digitally interact and process each other's data is far from being "secured". In many cases, the digitalization of sensitive services between citizens and public administrations, governments, banks, etc. is done without taking into proper account the consequences for the security of the systems and the privacy of the citizens. As a result, the number of Internet-related crime is on the rise.

Unfortunately, organizations fail to see the importance of implementing appropriate cryptographic security tools until the security of those systems is breached. This is a very near-sighted point of view, as the consequences of a security breach can be devastating. For instance, in practice it is impossible to erase sensitive information from the net, once it has been leaked. It is therefore necessary to protect the confidentiality of sensitive data a priori, and security needs to be considered already in the design phase of systems that are used to process sensitive information. As an example, as more and more countries are considering the possibility of introducing electronic tools for direct democracy (polls, local elections, etc.), it is clear that these systems need to ensure the secrecy of the individual votes and that the winning candidate must be the expression of a democratic vote and not of an electronic attack. These and many others (e.g. electronic banking and other monetary transactions, management and processing of medical information, etc.) are examples of real-world applications that deal with sensitive data and therefore need to be implemented in a secure way.

Coming up with appropriate cryptographic solutions to current problems is a highly non-trivial task and traditional cryptographic algorithms (e.g., encryption and digital signatures) do not always provide a solution. There are several reasons for this:

- **Change in trust models:** in recent decades the scope of cryptography has been widely extended. In its original form, the goal of cryptography is to enable users to communicate securely over a public channel, like the Internet: the parties involved in the communication are afraid of potential attackers that, having full access to the channel, can eavesdrop the communication between the parties or change its content. Nowadays, over the Internet, a lot of communication is between parties who do not know and trust each other, and that potentially have conflicting interests. Thus, we also need to protect users from the parties they communicate with. In other words, it is typically unclear who is "good" and who is "evil". A clear example of this is the rise of cloud storage and cloud computing. An increasing amount of users nowadays store their data on cloud storage services, such as Dropbox, Google, iCloud or SkyDrive. Clearly, the use of these services opens a number of security questions: users have to trust those services with keeping their data private. It is not hard to see why putting all this trust into potentially insecure services might not be a good idea. Even if one trusts the storage company not to sell one's private data, systems get hacked and sensitive information leaks - as newspapers too often report. Also, governments might coerce companies to release user data (the recent revelations about US service-provider leaks to the NSA, further emphasize that traditional cryptographic methods are insufficient for protecting user data when they are transferred and stored across legal jurisdictions). On top of that, users using cloud computing services, such as Amazon EC2 or Windows Azure, need to trust the cloud not only about the privacy of their data, but even about the correctness of the computed results.

Electronic elections, auctions (and more in general, interactive computations) are other examples of scenarios in which a number of users interact to reach a common goal, and where different parties in the same system might not trust each other with the privacy or the integrity of their respective private information, as they might have conflicting interests.

- **Change in threat models:** traditionally, cryptographers considered a somewhat idealized communication model with strict limits on what the attacker can access. In practice, many cryptographic schemes have been broken because the idealized model turned out to be too conservative. Namely, the attacker might indeed have access to auxiliary data deriving from physical measurements, like the power consumption or the running time of the cryptographic algorithms. Such attacks are commonly known under the name of *side-channel attacks*.

- **Shifts of the computational feasibility/infeasibility barrier:** the security of virtually every cryptographic algorithm is based on the belief that some computational problem is hard. For instance, most of the Internet traffic is nowadays encrypted using algorithms based on the hardness of factoring large numbers. However, most of the computational assumptions that underlie the security of cryptographic algorithms do not hold in novel computing paradigms, such as quantum computing: the advent of a quantum computer would render a large fraction of the cryptographic algorithms used nowadays completely useless. On top of that, computational assumptions may break down because of algorithmic advances, as shown by some very recent results on the hardness of discrete logarithm problem.

- **Gap between theory and practice:** even if we focus only on basic cryptographic tasks, such as providing confidentiality and authenticity of transmitted messages, we are still far from having true solutions in practice. For instance, every day we use several cryptographic schemes for secure communication, such as TLS (used in https), EMV (payment by credit card), and Kerberos (used for authentication of network services by many operating systems). But as a matter of fact, we only have a partial understanding of the actual security offered by the aforementioned protocols. One main reason for this gap is that these protocols deploy a number of mechanisms that are considered standard in practice but escape theoretical frameworks. Whilst cryptographers have done a very good job in defining security for primitives (block ciphers, one-way functions etc.), and then producing provably secure schemes based on these primitives (encryption schemes, signature schemes etc.), there has been less progress in applying a scientific methodology for the complex protocols that are used in the real world.

B.2 Current State of Knowledge

There is an extensive body of scientific literature addressing many of the issues described above, and a good deal of it is produced in some of the many excellent European research centers. For what is relevant to this Action we noticed a number of trends in recent results.

1. ***Theoretical protocols are becoming practical.*** A clear example of this is secure multiparty computation (MPC): this technology allows a set of parties to jointly compute a function of their inputs while ensuring privacy of the inputs and correctness of the output. When it was introduced, MPC was considered a result of theoretical interest that had no impact on real-world systems; nevertheless in the last decade the performances of MPC protocols have improved enormously and the first real-world MPC solutions are currently being deployed.

2. ***Deployed protocols (often) lack security analysis.*** Some of the most used and spread cryptographic protocols, such as SSL or IPsec, lack any proper security analysis. This is often for one of two reasons. Firstly, the theoretical security models typically cannot be applied to the type of protocols deployed in the real world. Secondly, real world protocols are notoriously complicated to understand and analyze in a mathematical sense. Recent efforts in the area of the analysis of real-world protocols such as TLS have refined the security modeling to include protocol implementation elements such as

padding, key-confirmation messages, key-derivation functions and special public-key encryption schemes. Nevertheless, many aspects remain poorly understood.

3. ***Secure protocols are insecurely implemented.*** A growing number of researches are focused on breaking cryptographic protocols based on the way they are implemented. As described above, sometimes protocols are broken because real world implementations are far from being ideal, e.g., they allow for side-channel attacks. Furthermore, implementations often depart from protocols specifications, and this leads to dreadful consequences. A great example of this was shown recently by two independent research groups that found out that a significant fraction of RSA public keys are insecure due to poor implementations and randomness management. Other attacks have shown vulnerabilities in elliptic curves software due to poor implementation of modulo arithmetic.

4. ***Bad cryptographic primitives are used.*** Even if cryptographic primitives are usually considered one of the strongest links in the security chain, sometimes attacks can actually be mounted to the primitives itself. For example, the designers of the virus Flame exploited a weakness in the cryptographic hash function MD5, which allowed them to forge a digital signature that certified the virus as a Microsoft Windows update. This made Flame look like harmless software and enabled it to infect computer systems very effectively. Other notable examples include the attacks on the CBC-mode used in IPsec, or a very recent attack on SSL which exploits a vulnerability of RC4. It is a never-ending task for cryptographers to come up with cryptographic primitives that are more efficient and more secure in different contexts.

The work on cryptographic protocols is ground-breaking and unifying. To make a complicated information and communication system such as the Internet secure, one needs to bring together expertise in symmetric cryptography, public-key cryptography, provable security and applied security engineering. This field presents unique research challenges, and it provides a great ground for academic cryptographers to make an impact on the real world. Positive examples in this direction are known, and the Action will extend this fruitful approach to the different sub-areas of cryptography.

B.3 Reasons for the Action

Solutions for real life are often a combination of different cryptographic tools, and therefore the interaction between the sub-disciplines of the cryptographic community is fundamental. Given the complex interdisciplinary landscape, a coordinated effort is required in order to tackle the problems we now face. As cryptographic techniques get more and more advanced, one single researcher (or a local group of researchers) cannot master the whole spectrum of cryptographic techniques. While specialization is crucial to obtain new results and breakthroughs, we need to remember that a chain is only as strong as its weakest link, and therefore it is important for cryptographers to keep a global vision of the field and avoid fragmentation.

Traditionally, most European research groups in cryptography bring together people from similar areas of expertise, which leads to increased specialization. This is definitely a strong point of European cryptographic research, as it allows for deep understanding of particular problems, but it also implies that interaction between researchers who work in different areas of cryptography is often limited. In addition, there has been an unfortunate lack of dialogue between the "theory" and "practice" communities. It is clear that if theory is to turn into practice, a seamless connection is required. There are some success stories in such interaction (e.g., recent work on "practical secure multiparty computation") but unfortunately this is not happening in many other sub-areas.

Similarly, the lack of interaction between the research community and industry is worrying: whilst academia researchers are working on cryptographic schemes that can withstand attacks by quantum computers, it still happens that schemes deployed by industry get broken because implementations suffer from very basic mistakes that could easily be avoided.

True interaction would ensure that both industry and academia would be working on problems in the middle space between these two extremes.

B.4 Complementarity with other Research Programmes

The importance of research in the field of cryptographic protocols and primitives and the excellence of European research is reflected in the number of European and national grants. Virtually all existing programmes are however focused on specific problems and often bring together scientists with similar expertise. Some relevant recent EU-projects are: PSPC on Provable Security for Physical Cryptography (ERC-SG-PE6 ERC Starting Grant 7th FWP), PRACTICE on advancing cryptographic technologies for security and privacy in cloud-computing (Large-scale integrating project, CP-IP, ICT-10-1.5 - Trustworthy ICT, FP7). The FET Project PUFFIN studies secure storage of cryptographic keys in processors and GPUs. There are also several EU projects that use cryptographic techniques for privacy friendly biometrics and identity management (e.g. ABC4Trust, Fidelity).

This COST Action is unique in its unifying goal of bringing together different and complementary skills. It will interact with these other research programmes, mainly by acting as a link between them, and will thus foster cross fertilization of ideas as well as communication between different communities. None of the above projects has the same overarching and integrating scope with as goal to solve practical problems in the next decade by addressing fundamental problems in the next few years. Those projects that have an important cryptographic component are rather focused on adapting and applying existing primitives in a narrow area.

C. OBJECTIVES AND BENEFITS

C.1 Aim

The main objective of this Action is to bring together European experts in the different sub-areas of cryptography, with special focus on closing the growing gap between theoretical and practical research, and with the main goal of designing, analyzing and implementing cryptographic algorithms that allow citizens and entities to interact securely with each other.

C.2 Objectives

The mission of this Action is:

- Gain new understanding of cryptographic models and techniques, in order to face current and future security challenges.

- Consolidating and strengthening the scientific excellence of European cryptographic research through cooperation between national efforts.

Specific scientific objectives include (but are not limited to):

- Designing more efficient cryptographic protocols for digital interaction, including: secure multiparty computation, fully-homomorphic encryption, electronic voting systems, secure outsourcing of computation and storage, verifiable computation, etc.

- Developing efficient cryptographic tools with advanced functionalities to be used in novel contexts, including: advanced encryption schemes (identity-based, functional encryption, searchable encryption etc.) and other advanced primitives such as homomorphic authenticators, anonymous credentials etc.

- Developing cryptographic models where theoretically secure schemes are also secure in practice and where practically secure schemes can be formally analyzed.

- Analyzing deployed cryptographic protocols, discovering vulnerabilities and designing appropriate countermeasures.

- Designing and developing formal verification tools that permit establishing the correctness and security of cryptographic implementations to a high degree of assurance, integrating the capability to reason about cryptographic security proofs, implementation correctness and physical security.

- Investigating optimizations and countermeasures (e.g., against side channel attacks) for cryptographic implementations, addressing possible vulnerabilities arising from incorrect implementation and the potential for automatic deployment via domain-specific development tools.

- Developing more efficient cryptographic primitives, with particular focus on low-power computing devices (e.g. RFID, Internet of Things, implantable devices).

- Assessing the plausibility of proposed computational assumptions, including novel lattice assumptions.

- Moving towards standardizing the most ubiquitous lattice-based schemes, such as digital signatures.

- Constructing more efficient "advanced" lattice-based cryptographic primitives.

Cooperation objectives include:

- Cooperating with regulations and standard bodies in the compilation of recommendation and good practices in cryptography.

- Training young scientists and PhD students with a proper understanding of the state of the art of cryptographic techniques.

- Consolidating the exchange between the scientific community and companies and other entities involved in the development of cryptographic solutions.

C.3 How Networking within the Action will yield the Objectives?

Networking within the Action will help the:

- *Creation of research projects within the Action topics:* the Action will promote and encourage the partners to form consortia and apply for national and transnational research projects, to fund the research to be carried within the Action.

- *Increase mobility among partners*: the Action will promote and facilitate the exchange of researchers between the participant institutions. This will take the form of Action supported events such as STSMs, Training Schools (TS) and Workshops (WS). At the same time, the Action will increase mobility across Europe by creating opportunities for recruiting among different parties, in particular helping matchmaking between graduating students and available postdoc/early stage research positions at other institutions.

- *Raise awareness and visibility for the Action topics:* by doing so the Action will promote interaction between the scientific community and other stakeholders, such as industries and regulation bodies. The Action will encourage its partners to seek collaborations between academia and industry in the form of research projects and other means of cooperation.

C.4 Potential impact of the Action

As more and more interactions between citizens, entities and governments are now carried online, and the Internet of Things is gradually becoming a reality, the solutions and the proposals that will arise within the Action have the potential to make a great impact on the future of the security of digital interactions across Europe and beyond.

The Action will have an impact in pushing the state of the art of cryptographic research, from its theoretical foundations to its practical applications. New approaches are expected to arise by combining the different, and in some cases complementary, skills of the partners.

The Action will impact the future of cryptographic research and its applications by contributing to training the next generation of cryptography experts that will lead European research centers and will work in companies that develop or use ICT security solutions.

C.5 Target groups/end users

The outcomes of this Action will be exploited by:

- The scientific community as the Action will help the development of the scientific and technological advances in the field of cryptography.

- Citizens, governments and other entities that will benefit from the solutions to security problems proposed by the scientific community.

- Regulations and standard bodies that will have access to the documents produced by the Action.

- European companies that can get access to fully trained recruits, thus facilitating knowledge transfer between academia and industry.

D. SCIENTIFIC PROGRAMME

D.1 Scientific Focus

A non-exhaustive list of scientific tasks (STs) to be addressed by this Action includes:

ST1. Secure Multiparty Computation (MPC): MPC allows a set of distrusting parties to jointly compute a function of their inputs in such a way that the inputs are kept secret and the correctness of the output is ensured. MPC has been considered only of theoretical interest until the release of the first garbled circuits implementation in 2004. Since then, MPC protocols have gained several orders of magnitude in efficiency. Yet, current solutions are still far from reaching their potential in real world systems. The Action will coordinate the different efforts towards realizing practically efficient generic protocols (i.e., protocols that can be used to compute any function securely) as well specific solutions tailored for concrete tasks. The latter ones have indeed the potential of great efficiency improvements. At the same time the Action will coordinate the work on the theory of secure computation, engaging some of the most important open problems, including: mathematical and algorithmic aspects of secret sharing (and their impact on MPC); feasibility of MPC protocols where even the size of the parties' inputs is protected; protocol with security against different type of attackers (covert, rational etc.). The field of MPC was recently shaken by the introduction of fully homomorphic encryption (FHE): this is an extremely powerful tool in terms of asymptotic efficiency but still too cumbersome to be used in practice. The Action will coordinate the efforts in advancing FHE schemes.

A special task is the design of electronic voting schemes: while the cryptographic components of those systems are well understood, there are no rigorous definitions of security and proofs of security for the systems as a whole. Providing such definitions and proofs is challenging, since the protocols have complicated trust models and involve heterogeneous parties, physical objects, and even human operators who are supposed to behave in a certain way. The goal is therefore to apply rigorous cryptographic analysis in the domain of electronic voting and to improve (or even to come up with new) protocols as needed.

ST2. Secure Outsourcing of Storage and Computation: Cloud computing is here to stay, and we need appropriate cryptographic tools to prevent future (in)security disasters. The Action will coordinate efforts with respect to the various research directions in this area, mostly focused around privacy and correctness. The main problem in this area is that, if we want to enable the cloud to manipulate the outsourced user data (e.g., to search over encrypted emails) and thus to relieve clients of expensive computational efforts, then traditional cryptographic tools are no longer sufficient. In terms of privacy, we need solutions to protect the privacy of the users' data from the cloud, including solutions where users may wish to hide from the provider even the access pattern to the data. In terms of correctness, mechanisms to ensure that tasks delegated to the cloud are performed correctly will also be investigated. Important cryptographic tools for this setting are verifiable computation protocols and homomorphic authenticators. The former allows a user to check the correctness of the result provided by the cloud using less time than by redoing the computation from scratch. The latter ones are special kind of signatures (or MACs in the symmetric setting) that allow for computations over authenticated data. While recent breakthroughs in the area of fully homomorphic encryption have received a lot of attention, less attention has been paid to realizing homomorphic authenticators: even the security modeling of these primitives is non-trivial, as the required functionality seems to contradict the traditional unforgeability requirement of digital signatures. All current realizations of these advanced primitives are only at an early stage of investigation and practically efficient solutions are still far from being ready for practical uses. The Action will coordinate efforts to advance the research of these cryptographic tools both from a theoretical and a practical point of view.

ST3. Real-life Protocols for Secure Channels: Providing confidentiality and authenticity of transmitted messages is a central application for cryptography, and each of us uses one or several secure channel protocols every day, e.g., TLS (used in https), IPsec (used for virtual private networks), EMV (payment by credit card), Kerberos (used widely for authentication of network services). Unfortunately, the cryptographic community still has only a partial understanding of the security of the aforementioned protocols, mainly because they deploy a number of mechanisms that are considered standard in practice but escape theoretical frameworks. However, interesting progress has been made in this direction: In recent efforts in the area of TLS, the study of practical mechanisms such as padding, key confirmation messages, key derivation functions and special public key encryption schemes was initiated. Nevertheless, many aspects remain poorly understood: What amount of security is added by key confirmation messages? Which assumptions are needed for key derivation functions? Which assumptions are needed for key transport via public-key encryption? The final goal is to design improved protocols for secure channels that take into account the practical constraints and, at the same time, offer a better efficiency and stronger security modeling.

ST4. Attacks: The Action will coordinate the efforts in discovering vulnerabilities and attacks in existing cryptographic schemes with a particular focus on those that are widely used. For example, the seminal encryption scheme developed by Rivest, Shamir and Adleman (RSA) is a popular building block for complex real-life protocols such as TLS (used in https), but also for simpler protocols such as PGP (used for email encryption). Several variants of RSA exist and the differences between them are seemingly minor. However, only certain versions of TLS are secure under realistic notions of security. Some, in turn, are known to achieve weaker, but still reasonable security guarantees. Finally, some RSA schemes are known not to admit any security proof. Maybe surprisingly, the most widely deployed variants of RSA (PKCS #1 v1.5) are in the latter group. Even without a security proof, these schemes have so far resisted to all cryptanalysis attempts (or at least none have been made public so far), and therefore these schemes are not known to admit real-life executable attacks either. Among the goal of the Action is to narrow this gap for RSA as standardized in PKCS #1 v1.5 and related schemes, that is, to come up with both, new security proofs and optimized attacks. These attacks/proofs will then be translated into a more accurate analysis of real-life protocols for secure channels such as TLS.

ST5. Verification of Cryptography: Verification of cryptographic protocols is a widely studied field. Historically, this verification has been mostly done using symbolic abstractions that idealize away from cryptographic details, in order to facilitate automated analysis. The downside of this approach is that many possible attacks may be overlooked. For this reason, a new generation of verification tools has very recently emerged. The goal of these tools is to increase the trust in the security of cryptographic schemes and protocols by allowing computer-aided verification in the so-called computational model. To this end, they allow the formalization of computational security properties through short programs that specify how an adversary can interact with a system. These programs are essentially a direct translation of the "security games" used by cryptographers, creating a natural environment in which to formalize and verify cryptographic code-based proofs. The aim of these proof-assistant tools is to allow the analysis of a wide range of cryptographic constructions and, at the same time, be usable by the cryptographic community. However, further research is needed to both expand the range of proof techniques that can be addressed (to include, e.g., proofs that rely on the simulation paradigm or in the Universal Composability framework) and improve the usability of such tools so that they can be widely adopted (at the moment, writing proofs still requires significant skill in interactive theorem proving). The Action will bring together experts in provable security and formal verification and will coordinate research efforts towards this goal.

ST6. Domain-Specific Tools for High-assurance Crypto Implementations: The development of cryptographic components for real-world systems remains an active and highly challenging field of research. In addition to being correct with respect to a theoretically secure high-level specification, a cryptographic implementation must also be efficient and satisfy low-level security requirements such as those imposed by countermeasures against physical attacks (e.g. fault attacks, side-channel attacks, etc.). These extra requirements, which are often conflicting (e.g., an optimization can introduce a side-channel vulnerability) make the development of cryptographic components a resource-intensive, error-prone and costly process. The development of domain-specific development tools that can assist practitioners in their task by introducing automation is therefore an important challenge in cryptography. Partial solutions to this problem have been proposed in recent years, but significant progress is required to enable widespread use of this technology in the development of ICT systems. The Action will bring together theoreticians and practitioners to collaborate on research and development activities in this direction. Additionally, ST6 will also address significant challenges that arise when dealing with cryptography-specific implementation techniques in formal verification scenarios. Indeed, although the development of high-assurance hardware and software is not a new topic – current formal verification technology may even be argued to have reached the maturity required to handle general-purpose software – existing formal verification tools are not equipped to deal with implementations that intensively rely on, for example, bit-wise operations or Streaming SIMD Extensions. Furthermore, there is currently poor support of tools for establishing a formal link between the theoretical security guarantees that can be proved using the tools described in ST5 and the guarantees that can be obtained by formally verifying implementations.

ST7. Symmetric Cryptography: Symmetric cryptology is a very active research area which is stimulated by a pressing industrial demand for low-cost implementations (here low cost refers to reduced area, power consumption, energy, latency or a combination of these). These extremely restrictive implementation requirements substantially constraint design choices and leave little room for complexity based security arguments that are employed elsewhere in cryptographic designs. In order to guarantee a provable resistance to the known attacks and to achieve extremely good performance, a symmetric cipher must use very particular building blocks, whose structures may introduce unintended weaknesses. Finding new appropriate building blocks is still a challenging field of research. Despite many mathematical works in this area during the last ten years, the inverse function in a field of characteristic two is still the only known example (up to equivalence) of a permutation which guarantees the best known resistance to differential and to linear attacks when the number of variables is divisible by four. And the fact that an S-box with such a strong algebraic structure may cause some unexpected weaknesses in the cipher is still an open question, more than 10 years after the selection of AES as a new standard. Choosing an S-box which has been picked at random avoids this type of threat, but random S-boxes obviously have a high implementation complexity. Then, the choice of non-optimal S-boxes (or of S-boxes operating on a very few variables) requires the designer to increase the minimal number of iterations needed for achieving a suitable security margin. The consequence of such a design, used in many recent lightweight block ciphers, is a very high latency which is unacceptable in many applications. There is a need for a better understanding of the trade-offs between implementation efficiency and cost.

Defining simple and secure constructions for a block cipher is also an open problem in general, and the large variety of key schedules which have been recently proposed shows that this issue is far from being solved. It is usually believed that a secure key schedule should be nonlinear. Some designs rely on a very strong key schedule, which performs the same operations on the key as on the plaintext. Yet others, especially lightweight ciphers, have a very simple (or even nonexistent) key schedule, and the recent results on the indifferentiability of key-alternating ciphers without any key schedule tend to show that adding the same round key at each iteration may be a reasonable solution. Therefore, finding a flexible and efficient key schedule (where the key size is not limited by the block size) is an important issue in the design of block ciphers.

The search for efficient general constructions of symmetric encryption schemes is actually much more general. It includes for instance the construction of efficient tweakable block ciphers. Indeed, tweakable ciphers are needed in many applications and the classical constructions all require some operations on the tweak before the beginning of encryption, which increases the latency of the cipher. Finding efficient modes of operation which provide both privacy and authenticity is also a major issue which is currently the topic of a public call for proposals (CAESAR). One can expect that the evaluation process will give rise to interesting fundamental research questions on security/performance tradeoffs for authenticated encryption, which can in turn lead to better solutions for secure channels (ST3).

ST8. Lattice Based Cryptography: Lattice-based cryptography provides arguably the most promising approach for constructing primitives that are both efficient and, at the same time, secure against quantum computing. Recent advances in constructions of encryption schemes and digital signatures have put lattices on par, efficiency-wise, with traditional number-theoretic approaches. One of the goals is to move forward and produce "advanced" lattice-based primitives (e.g. Identity-Based Encryption, group signatures, etc.) that are also efficient enough to be used in practice. Currently, the central tool for realizing these primitives is the Gaussian sampling algorithm that works over arbitrary lattices. While this algorithm is incredibly versatile in allowing constructions of multitudes of primitives, it is unfortunately not very practical. Even the simplest applications result in keys and outputs that are prohibitively large when using Gaussian sampling.

A possible way around this problem is to consider stronger lattice assumptions that could lead to more efficient ways to perform Gaussian sampling. One has to be extremely careful that the essence of the underlying hardness is not lost when making stronger assumptions. Despite the potential dangers of making new assumptions, there have been several cases which resulted in more efficient schemes without an impact on our trust in the security of those systems (e.g. the

NTRU cryptosystem). A second possible approach for achieving advanced, practical lattice primitives is to combine techniques that have been recently successfully employed for constructing simpler, but much more efficient, lattice primitives such as encryption and digital signature schemes. Evaluating the viability of these two approaches will require close collaboration between experts in lattice constructions and lattice cryptanalysis.

ST9. Multilinear Maps: The introduction of bilinear maps in cryptography one decade ago allowed for many and surprising applications such as encryption schemes with extended functionalities (identity based encryption, attribute based encryption, anonymous credentials etc.). Recent work proposed a candidate for cryptographic multilinear maps, and this breakthrough is already leading to numerous new applications in cryptography. Multilinear encodings are a promising tool for the development of improved cryptosystems, potentially more secure and efficient but based on new computational assumptions. The introduction of new computational assumptions comes together with the need for tools to assess the hardness of these assumptions in a uniform way, using for instance generic models as the multilinear generic group model. Therefore, it is important to extend the known algebraic framework for Diffie-Hellman like problems (like the Linear Problem) to other computational problems (like the Decisional Bilinear Diffie-Hellman problem) in which the instance description is heterogeneous, that is, it includes elements from different groups, as usually occurs in the multilinear group setting. This kind of tool would give new families of problems that are generically hard while the instance description is reasonably compact (e.g., linear or even constant with respect to the order of the multilinear map), thus having an impact on the size of the parameters in the cryptosystem.

D.2 Scientific Work Plan Methods and Means

The Action will be divided in four working groups (WG):

WG1. Protocol Design: The STs that are more relevant for this WG are ST1, ST2. The WG will coordinate efforts for the design of practical MPC protocols. In particular the WG will promote the dialogue between protocol designers and practitioners to understand where the real bottlenecks in implementing MPC protocols are, as theoretical measures of communication and computational complexity are not always good predictors of the actual performances. The WG aims at developing a framework for benchmarking different protocols, as it is not clear today how to compare protocols that use different resources (network, CPU, etc.) in different ways, or how to compare protocols that rely on different computational assumptions. By combining the experience of privacy experts, cryptographers and systems researchers, the WG will coordinate the design of privacy-preserving data processing schemes that provide security guarantee to the users. In terms of techniques, this WG will include tools such as garbled circuits, homomorphic encryption, zero-knowledge protocols etc. This WG will also lead the study of relevant cryptographic tools with advanced functionalities that can be used in interactive and outsourced computation, such as functional encryption schemes, searchable encryption, order preserving encryption etc.

WG2. Protocol Analysis: This working group will be mostly concerned with ST3 and ST4. The WG focuses on understanding the security of real-life protocols such as TLS, IPSec, EMV etc. as their security is poorly understood. Towards this goal, the WG will develop appropriate security models for the building blocks used within the protocols. Illustrating the above on the TLS example, this WG will analyze the TLS-primitives such as RSA encryption and key derivation functions with respect to the new models. The WG will bring together practitioners and modeling experts towards tackling these questions. In particular, the WG will extract appropriate protocol and primitive descriptions from the standards, and develop new analysis tools and models inspired by approaches such as the Bellare-Rogaway model. The goal is to obtain security notions that capture the real world attacks in a concise fashion. The new tools and models will then be combined with classical techniques such as "game hopping" to obtain a rigorous security analysis. Finally, in case positive results turn out to be hard to obtain, the WG will bring in experts from the area of impossibility results and use techniques such as oracle separations and meta-reductions.

WG3. Implementation and Verification: The STs that are more relevant for this WG are ST5, ST6. The WG will bring together theoreticians and practitioners in the areas of cryptography, programming languages and formal verification, and coordinate research and development initiatives centered on the implementation and verification of cryptographic schemes and protocols. The overarching goal is to resolve the existing tension between the need to guarantee efficiency, correctness and security at the level of executable code; versus the absence of adequate techniques and tools to assist developers in obtaining such guarantees (e.g., there is little support to ensure the preservation of correctness and security properties established for implementations constructed using a high-level programming language). To this end, collaborative research effort will be promoted in three complementary directions: i) the investigation of existing and novel optimizations and countermeasures (e.g., against side channel attacks), their deployment in cryptographic implementations, and the study of potential vulnerabilities arising from incorrect implementation; ii) the automation and integration of these techniques into domain-specific development tools that can assist practitioners in the implementation of cryptographic schemes and protocols; and iii) the design and development of formal verification tools that permit establishing the correctness and security of cryptographic implementations to a high degree of assurance, integrating the capability of reasoning about cryptographic security proofs, implementation correctness and physical security. **WG4. Cryptographic Primitives:** The STs that are most relevant for this WG are ST7, ST8 and ST9. The WG aims at finding new primitives having a low implementation cost which achieve the functionalities required by the main cryptographic protocols. Identifying the needs arising from real-life protocols is an important issue and will clearly benefit from an interaction with WG1 and WG2. This WG will focus on building both symmetric-key and public-key primitives and in particular it will encourage closer interaction between researchers in the areas of public-key cryptography, secret-key cryptography, hardware constructions, and automated verification. Indeed, the current lack of communication between these communities is a clear obstacle to the design of new real-world primitives. Constructions of new modes of operation, leakage-resilient public-key primitives, as well as the understanding of new mathematical assumptions that can lead to practical and provably-secure primitives, will greatly benefit from this added cooperation.

E. ORGANISATION

E.1 Coordination and Organization

The Action will be coordinated by the Management Committee which will be formed and act according to COST Rules and Procedures. The Management Committee will nominate committees dedicated to coordinate different aspects of the Action (e.g., website, STSMs, TSs, editorial production of the annual reports, etc.).

The MC will invite an industrial advisory board (IAB) to help the evaluation of the Action progress. The IAB will be created with an effort to balance the different geographical areas and industrial sectors

The Action will organize workshops and training schools. Workshops and training schools will be open for the general audience in cryptography, with particular focus on PhD students and young researchers. As detailed in Part F, each TS will be followed after one year by a workshop on the same topic, so that in particular PhD students and other parties without the necessary background (researchers in other sub-disciplines, practitioners etc.) can receive the necessary training before being exposed to state-of-the-art research.

By the end of each year, a report with the main results and contribution achieved by the Action will be published. At the end of the Action a final conference will be held, to summarize and present the contribution and the results in a single venue.

Events will be co-located within the Action and with other major events in the cryptographic community to facilitate interaction between different Working Groups and to save on travel and organization costs.

A website will be set up and continuously maintained throughout the lifetime of the Action in order to publish results, innovations and applications generated by members of the Action's network, as well as to announce and promote Action events. The Website will be launched within 3 months from the beginning of the Action.

Close links will be maintained with national scientific and research institutions throughout Europe in order to gather information, organize workshops and conferences, specific training seminars to involve early-stage researchers, exchange documentation and publications, coordinate existing research activities, propose new joint projects and disseminate findings. The Action will facilitate and promote research visits, and international research collaborations. The Action will keep an open and flexible framework to allow for an easy integration of new partners in the Action.

E.2 Working Groups

The Action will consist of four Working Groups as detailed in Section D.2. The four working groups are:

- ***WG1. Protocol Design***
- ***WG2. Protocol Analysis***
- ***WG3. Implementation and Verification***
- ***WG4. Cryptographic Primitives***

Each Working Group will be composed of a broad base of European experts from the various fields of cryptography, such as theoreticians, practitioners, and implementers. Solutions for real applications often require a combination of different cryptographic tools, and therefore the interaction between the sub-disciplines of the cryptographic community is fundamental and essential.

The working groups have been designed in such a way that most participants are expected to join the activities of more than one Working Group, to facilitate the interaction between different skills and expertise. As an example, researchers in the area of practical MPC will have interest in attending the activities of both WG1 and WG3. Participants with an interest in the study of IPSec will be interested in the activities of both WG2 and WG4. Participants with an interest in fully-homomorphic encryption will be interested in joining the activities of WG1 and WG4, and so on. Towards the same goal, joint events between Working Groups will be held. Each Working Group will be internally coordinated by a Working Group leader.

E.3 Liaison and Interaction with other Research Programmes

The Action values positively liaison and interaction with other COST Actions and other European and international research programmes whose scientific focus intersects with the focus of the Actions. A primary goal of such interactions will be joint publications and system development. Such programmes include: "ICT COST Action 1204 Trustworthy Manufacturing and Utilization of Secure Devices" and "SysSec NoE (FP7): Network of Excellence in the field of Systems Security for Europe". The Action has an open and positive attitude towards interaction with other programmes in related areas and disciplines such as hardware, networks, databases and algorithms.

E.4 Gender Balance and Involvement of Early-stage Researchers

The lack of women in computer science in Europe is a well-known problem, and it has to be tackled by coordinated efforts at all levels of education. This Action will make concrete steps in addressing this issue by:

- ensuring gender balance at a managerial level and among the chairs of the Working Groups;
- encouraging female participation to training schools e.g., by reserving a quota of stipends for female participants;
- cooperating with existing events particularly targeted at female researchers in cryptography (such as the CrossFyre workshop).

This Action will encourage the participation of early-stage researchers in all managerial positions, aiming at 50% ESR among the managerial roles of the Action. To ensure a sustainable development of the field of cryptographic research in Europe, it is crucial that ESR take responsibility not only for the scientific development of the field, but also of the managerial and networking aspects.

F. TIMETABLE

The Action lasts four years. The Management Committee and the Working Groups will meet at least once a year for a minimum of 6 meetings during the Action. In addition, the Action will organize a minimum of 3 Training Schools, in Year 1, 2 and 3 and a minimum of 3 Workshops in Year 2, 3 and 4. As mentioned in Part E, the Workshop in Year n will follow the theme of the Training School in Year n-1. This will allow young researchers, PhD students and other interested parties to get the necessary training before being exposed to the state of the art research presented at the workshops. The topics of the TSs and WSs are chosen to cover all the areas of the Action in a meaningful way:

- TS1-WS1: The first school/workshop pair will interest WG2 and WG4 and will cover real world protocols analysis and vulnerabilities of cryptographic primitives.

- TS2-WS2: The second school/workshop pair will interest WG1 and WG4 and will cover the theory of provably secure protocol and cryptographic primitives.

- TS3-WS3: The last school/workshop pair will be focused around WG3 and be of interest to all other WGs.

The rationale behind this schedule is that the topic covered by TS1-WS1 is a pressing one, and that it is important to understand the limitations of current cryptographic protocols and their shortcomings, to ensure that the theory and protocol design developed in TS2-WS2 answers to real world problem, and in turn the implementation and verification issues logically come after the design of the protocol to be implemented.

Efforts will be made to co-locate events, both within the Action and with other relevant events for the cryptographic community (major conferences etc.), to reduce travel and organization costs and to allow for interaction across the different WGs. STSMs will take place at any time during the Action. At the end of the Action, a Final Conference will be held. The main activities in the Action are shown in the following table. Working Group meetings will be scheduled during the Action, both autonomously from within the Working Groups and with a coordinated effort across Working Groups.

	Year 1	Year 2	Year 3	Year 4
Months 1-3	MC-M			
Months 4-6		MC-M,WS1	MC-M,WS2	MC-M,WS3
Months 7-9	MC-M			
Months 10-12	TS1	TS2	TS3	MC-M,Final Conference

G. ECONOMIC DIMENSION

The following COST countries have actively participated in the preparation of the Action or otherwise indicated their interest: AT, BE, CH, DE, DK, EE, EL, ES, FR, IL, IT, NL, PL, PT, SE, UK. On the basis of national estimates, the economic dimension of the activities to be carried out under the Action has been estimated at 64 Million € for the total duration of the Action. This estimate is valid under the assumption that all the countries mentioned above but no other countries will participate in the Action. Any departure from this will change the total cost accordingly.

H. DISSEMINATION PLAN

H.1 Who?

The main target audience for the dissemination of the Action will include:

- the COST Action members;
- the international research community in the fields of Cryptography and ICT Security;
- PhD students and early-stage researchers in the above fields;
- international and regional industry in related fields (ICT, security);

- governmental institutions;

- EU and national bodies policy makers, in particular in the areas of security and privacy (e.g. ENISA);

- standardization bodies.

H.2 What?

To reach the above target audience, the Action will rely on several dissemination methods including:

- Action's website and mailing-lists;

- publication of scientific papers in peer-reviewed conferences and journals;

- progress reports and final reports;

- special reports (evaluation of current cryptographic schemes);

- Short-Term Scientific Missions (STSMs);

- thematic workshops;

- training schools for early-stage researchers (young scientists and PhD students).

H.3 How?

The dissemination activities of this Action will take place at essentially two levels: internal and external.

Internal dissemination will target Action members and will be mainly conducted through the Action's website and mailing-lists. The website will contain a private area to help sharing information among and within the MC and the WGs (e.g., by posting minutes of MC and WG meetings). Also, appropriate mailing-lists will be created in order to facilitate communication within the WGs and to spread information about the Action's activities and events.

External dissemination will be targeted to both members and non-members of this COST Action, and it will be achieved by the following means:

Action website. The Action will set up a public website within the first 3 months following the MC's kick-off meeting. Among other things, the website will contain:

- general information about this COST Action, such as the list of official members, its organization (composition of MC and WGs), and contact information;
- list of past and future Action events (WG meetings, workshops, training schools);
- annual progress reports and special reports (see below).

Publication and special reports. The scientific results of the Action will be disseminated through peer-reviewed journals and conference proceedings. Final and progress reports describing such results will be prepared as well and publicly posted on the Action website. In addition to these classical dissemination methods, we plan to produce special reports evaluating the state-of-the-art of current cryptographic schemes (new proposals, improvements, attacks and cryptanalysis). The latter reports will find the interest of industry and governmental institutions.

Workshops and training schools. The MC together with the WGs will organize thematic workshops and training schools to inform interested scientists and industrial practitioners about the results of the Action and about state-of-the-art scientific results on topics in the Action's interest as detailed in Part F.

Short-Term Scientific Missions. The Action will encourage STSMs, especially of PhD students, to facilitate the scientific transfer between the Action partners.