ECRYPT: the Cryptographic Research Challenges for the Next Decade

B. Preneel

Katholieke Univ. Leuven, Dept. Electrical Engineering-ESAT,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
bart.preneel@esat.kuleuven.ac.be

Abstract. In the past thirty years, cryptology has evolved from a secret art to a modern science. Weaker algorithms and algorithms with short keys are disappearing, political controls of cryptography have been reduced, and secure cryptography is becoming more and more a commodity. Moreover, implementations are being becoming more secure as well. This progress may lead to the belief that the cryptography problem is "solved." However, this article discusses some of the challenging problems ahead in the area of cryptographic algorithms and protocols. We also explain how the ECRYPT Network of Excellence (www.ecrypt.eu.org) tries to address some of the challenges by bringing together 250 European researchers in the area of cryptology and the related area of watermarking.

1 Introduction

While cryptology is getting increasingly important in the information society, it is also becoming less and less visible. Cryptology has been integrated into smart cards for financial transactions, web browsers, operating systems, mobile phones and electronic identity cards. This success can be explained by several factors: first, there is a clear need for cryptographic solutions, second adequate algorithms and protocols have been developed, and third the decreasing cost of computation makes it inexpensive to implement symmetric and even asymmetric cryptology. For outsiders, who have limited understanding of the complexity of the field, the widespread deployment of cryptology may give the impression that there a no important problems left in cryptography. We have cryptographic algorithms and protocols available that can be called as a "black box" by security engineers to solve some standard problems and the security and performance of these implementations is improving.

Consequently, one may believe that research efforts in security should be focused exclusively on building trust infrastructures and integrating security into applications. This (incorrect) impression is strengthened by the (correct) observation that security systems fail usually due to other reasons than cryptographic flaws (such as incorrect specifications or implementations, bad management, viruses, social engineering attacks. . .) [2].

A second (but incorrect) conclusion that one may draw from these observations is that research discipline cryptology has ran out of practical problem, and hence researchers now work on purely theoretical problems such as general multi-party computation, exotic protocols and on the question whether or not one-way functions exist. Any cryptographic protocol (encryption, authentication, key establishment, e-payment, e-voting, ...) can be described as a multi-party computation, and generic but highly inefficient solutions to this problem are known since the late 1980s [5, 12, 25]. An interesting challenge is to make these protocols more efficient, either in the general case or for concrete problems (such as group signatures or e-voting) for example by introducing stronger cryptographic assumptions. The most fundamental assumption is the existence of one-way functions: while our intuition seems to suggest that it is very easy to design a function that is "easy" to compute but "hard" to invert, so far the best theoretical result can prove that there exist functions that are twice as hard to invert as to compute [27]; it is clear that such functions would be completely useless to practical cryptology. This is quite remarkable, since one-way functions are a cornerstone of cryptology.

Section 2 presents an overview of the challenges that remain in both practical and theoretical cryptography. Since the area of cryptology is rather broad, the emphasis will be on symmetric cryptology by summarizing the status after recent attacks on block ciphers, stream ciphers and hash functions. We briefly address some research issues in asymmetric cryptology, but due to lack of space we do not provide details on areas such as protocols, secure implementation, watermarking, and perceptual hashing. Next we attempt to explain the problems problems that arise in the standardization of cryptographic algorithms and protocols. Section 3 explains how the ECRYPT project intends to address some of these research challenges. Some concluding remarks are presented in Sect. 4.

2 Research Challenges in Cryptology

2.1 State of the Art

Most of the applications are covered by the block ciphers triple-DES [19] and AES [20]; DES, which was widely used until the late 1990s, is being replaced quickly (NIST has announced in July 2004 that it will withdraw support for the DES algorithm since its strength is no longer sufficient to adequately protect Federal government information). In addition 3rd generation mobile networks (3GPP) use KASUMI [1] and Bluetooth uses SAFER+ [8]. While military environments still use proprietary stream ciphers, RC4 [24] is widely deployed in the commercial world (e.g., SSL/TLS, WEP); GSM uses the stream ciphers A5/1 and A5/2 [7, 42] and Bluetooth uses E0 [8]. The most popular hash functions are MD5 [37], which was broken in August 2004 [43], SHA-1 [23] and in some applications RIPEMD-160 [17] and MDC-2 (see [35]). For MAC algorithms, HMAC and several variants of CBC-MAC are widely used. In the area of public-key cryptology, RSA [38] is clearly the most popular algorithm, both for public key encryption and for digital signatures. For digital signatures, DSA, ECDSA (Elliptic Curve DSA) and variants of these are also successful. For public key encryption, ElGamal and some elliptic curve variants can also be found in applications. For key establishment several variants of authenticated Diffie-Hellman are widely deployed. For entity authentication, there is a limited use of zero-knowledge protocols, o.a. in the pay-TV world and in Novell networks. It is not feasible within the scope of this article to discuss in detail all the cryptographic algorithms and protocols included in standards such as SSL/TLS, IPsec/IKE, SSH, S/MIME, PGP, GSM, 3GPP, WEP, WPA, RSN, Bluetooth, EMV, Global Platform, ... It is clear that this could be a useful exercise to assess the impact of developments in cryptology.

2.2 Challenges

In this section we discuss the research challenges from a generic perspective. Even if we have currently a large toolbox of cryptographic algorithms and protocols, this may not be adequate for the next years due to several reasons. A first issue is the changing environment and threat models in which cryptology will be deployed: we are evolving towards ambient intelligence, pervasive networking or ubiquitous computing, which have completely new characteristics. A second element is the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based; this erosion is created in part by developments in computation (progress in electronics and in the future in optical and maybe even quantum computing) and in part by progress in cryptanalytic algorithms. A final element is the requirements of new applications and cryptographic implementations, including the lack of physical security in devices.

In order to structure these new requirements, the areas in which further research is needed can be organized according to three parameters: cost (hardware, memory, power), performance (throughput, latency) and security level. Ideally one would like to achieve a high security level and a high performance at a low cost, but this is not feasible. In practice one has to focus on at least one criterion; depending on the choice, one obtains different solutions. Within this choice, there may still exist trade-offs between the remaining two parameters.

Low cost and/or low power: this can be achieved by giving up high performance or high security; this approach is essential to allow for integration of cryptography in even the tiniest devices (e.g., ambient intelligence). Design goals could be the implementation of a stream cipher that offers a reasonable security level (say 80 bits) with uses less than 1000 gates.

High performance: this is required for highly efficient solutions for applications such as bus encryption, hard disk encryption, encryption in Terabit networks. If cryptography presents too large an overhead/cost, it will not be deployed, or it will be switched off. In this context, it is important to note that while Moore's 'law' predicts that in 2018, the computational power for the same cost will have increased with a factor of about 100, Gilder's 'law' predicts that the speed of LANs and storage devices will increase with a factor of 10 000. This shows that parallelism will become increasingly important in cryptographic operations, but also demonstrates the need for high performance designs.

High security: some application areas require cryptographic algorithms and protocols that can offer a higher confidence and assurance level than the state of the art. E.g., for e-voting, we need secure and robust protocols that survive even if a subset of the players are faulty or corrupt and that provide long-term security; for e-health and national security we need cryptographic algorithms which provide guaranteed protection for 50 years or more. As an example, information on our DNA has implications on the DNA of our children and grandchildren, hence this is information that may need to be protected for a very long time.

These requirements guide the approaches taken by the research teams in the ECRYPT project (cf. Sect. 3).

2.3 Symmetric Cryptology

In this section we comment on the challenges in the area of block ciphers, stream ciphers and cryptographic hash functions; we omit MAC algorithms for two reasons: they are mostly derived from other block ciphers and hash functions, and highly efficient constructions based on universal hash functions are known (even if they are not yet widely used).

Block ciphers. The area of block ciphers has always been very particular in cryptology due to the availability of widely supported standards. The impact of the publication of the Data Encryption Standard (DES) in 1977 by the US NIST [33] (at that time called NBS) on both practice and research is hard to overestimate. DES was obtained after an open competition, in which IBM provided the winning entry; the final design was performed by IBM in cooperation with NSA. After some initial controversy, DES became widely used, first in the financial sector and later on in a broad range of applications.

In the 1990s it became clear that the key length of DES (56 bits) was no longer adequate (see for example Wiener [44]); moreover, the block length of 64 bits will also be too short in the next decade, which means that triple-DES (which is also rather slow) is not an adequate replacement. Therefore NIST launched a call for a successor in 1997. After an open competition with 22 entries, NIST selected the Belgian Rijndael algorithm (designed by J. Daemen and V. Rijmen) as the winner in October 2000. The AES standard FIPS 197 (Federal Information Processing Standard) was published in December 2001 [20]; it is a 128-bit block cipher with a key of 128, 192 and 256 bits. AES is mandatory for sensitive but unclassified data. In 2003, the US government announced that AES can also be used for classified information up to the secret level, while AES with key lengths of 192 and 256 bits can be used for top secret information. In software, AES is more than twice as fast as DES, and thus significantly faster than triple-DES.

In 2004, AES has been included in more than thousand products, and as of August 2004, 171 AES product certifications have been performed by NIST. AES is being adopted very quickly as a standard in other environments (IETF, ISO, IEEE, 3GPP, ...), with the exception of the financial sector, which is finalizing its slow migration from DES to triple-DES.

While there was a broad consensus on the choice by NIST, there were also some critical comments on the algebraic structure present in the AES. This structure allows for an elegant description and efficient implementations both in hardware and software (8-bit and 32-bit machines), but may also induce weaknesses. For example, it was shown by Courtois and Pieprzyk [11] that the algebraic structure in the AES S-box leads to simple quadratic equations. The authors of [11] claim that it may be possible to solve these equations faster than an exhaustive key search. See also more recent work on algorithms [3, 13] to solve quadratic equations. Murphy and Robshaw have shown that the simple overall structure leads to an embedding in larger block cipher BES [31], which has certain weaknesses; however, these weaknesses do not seem to apply to AES. Finally, several authors have shown that the algebraic structure leads to equivalent descriptions of the AES.

In conclusion, more than two years after the announcement of these properties, none of these attacks seems to pose a realistic threat to the security of AES. It is clear that in view of the importance of the AES, more research is needed to increase our understanding of this algorithm. On the other hand, in the past 15 years the cryptographic community has built up some extensive design expertise for block ciphers; even if it would turn out that a less elegant (and less mathematical) design is more desirable, it would not be too difficult to modify the design accordingly.

Stream ciphers. In contrast to block ciphers, the area of stream cipher has been characterized by many proprietary algorithms and a lack of standards. The first generation of stream ciphers (1920s–1950s) used mechanical and electromechanical designs based on rotors. Subsequently, electronic designs were developed using Linear Feedback Shift Registers (LFSRs); an extensive mathematical theory has been created to analyze these stream ciphers. In the last 15 years a new generation of software-oriented stream ciphers has been proposed, which uses word lengths between 8 and 32 bits and runs efficiently on modern processors.

Designing a secure stream cipher should in principle be easier than designing a block cipher, since a stream cipher has an internal state that cannot be influenced by the opponent (there is no equivalent of a chosen plaintext attack). However, stream cipher designers aim for a significantly better performance than a block cipher in OFB (Output FeedBack) or CTR (CounTeR) mode, which is a natural benchmark. As a consequence, output bits are produced after a few operations, which implies that mixing may be less thorough as desirable. In addition, new attack models are being introduced which exploit the fact that the output stream needs to be restarted or re-synchronized at regular intervals using an Initialization Vector (IV). A chosen IV attack gives an opponent some control over the initialization of the internal state.

The rich algebraic algebraic structure of LFSRs has resulted in a large number of attack strategies: linear attacks, algebraic attacks, correlation attacks, divide and conquer attacks, ... As a consequence, some researchers are convinced that LFSRs should be eliminated altogether from the design of a stream cipher. As an alternative, one could consider the T-functions proposed by Klimov and Shamir [29]; these functions provide an efficient implementation of a single-cycle non-linear iteration on 2^n bits.

Software-oriented stream ciphers have been analyzed using an ad-hoc approach, that use a broad variety of techniques. The NESSIE project [32], which organized an open competition to develop standard proposals for cryptographic algorithms, concluded that none of the submitted stream ciphers satisfied the security criteria. In most cases, the attacks found were so-called distinguishing attacks with a very high data complexity, which may not represent a realistic threat on applications. However, the NESSIE project asked for a very high security margin, and the submitters initially believed that they could provide this. The motivation was to obtain a sufficient security margin for long-term security. More research is needed to evaluate to which extent we need to reduce the security requirements to obtain the expected performance benefit from stream ciphers.

In order for stream ciphers to be useful in practice, they may also need efficient resynchronization procedures, and an optional mode for authenticated encryption. There is clearly a need for standardized stream ciphers that offer either a very low cost (in terms of gate count or power) or that are highly efficient in software. ECRYPT intends to this

Hash functions. The area of hash functions has been characterized by a large number of broken schemes in their 25-year history (see [34, 35] for an overview). In practice however, only a limited number of schemes are widely used: MD5 and SHA-1, and to a limited extent RIPEMD-160 and MDC-2.

MD4 was proposed by Rivest in 1990 and broken by Dobbertin in 1996 [16]. MD5 was proposed one year later as a strengthened version of MD4. However, it was discredited by attacks by den Boer and Bosselaers in 1992 [15] and Dobbertin in 1996 [18]; the last attack led RSA Security to withdraw its support for new applications. These attacks showed serious weaknesses of the compression function of MD5, but they did not provide collisions for the complete function. In the mean time, brute force collision attacks on MD5 – which require 2^{64} operations only – are also within reach. In spite of these development, MD5 remained widely used in a broad range of applications until today. In August 2004, four researchers (X. Wang, D. Feng, X. Lai, and H. Yu) announced that they had found collisions for MD5 [43]; their attack requires only 15 minutes on a normal laptop.

The Secure Hash Algorithm, was proposed by NIST [21] in 1993; SHA has a 160-bit hash result. After one year, NIST discovered a certificational weakness in SHA; apparently collisions could be found in less than 2^{80} operations. Consequently a new release of the standard was published. The new algorithm is called SHA-1 [22], which prompted some researchers to rename the original SHA as SHA-0 (this has created some confusion).

After work by Chabaud and Joux in 1998 [10], Biham and Chen in 2004 [6], Joux, Carribault, Jalby and Lemuet presented a collision for SHA in August 2004 [28]; their attack requires 2^{51} compression function computations. Wang et al. [43] claim an improved attack that requires only 2^{40} compression function computations; however, this attack has not yet been implemented.

Biham and Chen have also investigated the extension of their attacks to SHA-1 [6]. The current status is that they can find collisions for 43 (out of 80) rounds of SHA-1; they also show that finding collisions for up to 53 (out of 80) rounds of SHA-1 is faster than a brute force collision attack, which requires 2^{80} steps of the compression function.

The implications of the new cryptanalytic techniques discovered in 2004 on SHA-1 and on RIPEMD-160 are still under study. At this time it is too early to make a reliable assessment, but there does not seem to be an immediate threat to either hash function; however, brute force attacks on these hash functions – requiring 2^{80} compression function evaluations – may become within reach within 10-15 years.

In 2004, Hawkes and Rose [26] have presented some critical observations on the security of SHA-256 (with a 256-bit result). While it is probably too early to draw firm conclusions, it seems now plausible that finding collisions for SHA-256 could take less than 2^{128} evaluations of the compression function, but it may still be out of reach for the next 20 years or more.

For the time being, there is still a lack of understanding of the security of hash function designs. Most practical constructions build on the original ideas of MD4 (32-bit arithmetic and logical operations); we have learned in the last decade that these designs are probably less secure than anticipated. The next generation standards SHA-256 through SHA-512 [23] offers better security levels based on similar principles. However, they are also significantly slower than SHA-1 (about 2-6 times) and it may be that some of the new attack techniques can be extended to these designs.

2.4 Asymmetric Cryptology

The research challenges in asymmetric cryptology are certainly not smaller. The first results in security reductions focused on asymmetric cryptology; in this line of research, one attempts to prove that the security of a cryptographic primitive or protocol can be reduced to an assumption on the difficulty of a mathematical problem (such as extracting modular roots, factoring the product of two large primes or solving the discrete logarithm problem in a specific group). Research concentrates on finding efficient and meaningful reductions, on reducing assumptions used in the proof (such as the ‘random oracle model’ [4, 9]), on establishing relations between assumptions, and on finding primitives with better and/or more complex security properties. It should also be pointed out that the security of most asymmetric primitives depends on a small set of problems from algebraic number theory; any breakthrough in solving some of these problems could have dramatic consequences. This shows that there is a need for new asymmetric algorithms that depend on new problems.

Cryptology also needs to take into account the ever increasing speed of electronic computers; typically this can be addressed by an adequate upgrade path for key lengths at the cost of a decreased performance and increased key sizes. However, we should also consider the emergence of new computer models such as optical computers and even quantum computers. Shamir, Tromer, and others have shown that optical computers could bring significant progress in factoring large integers [30, 39]. Shor has proved in 1994 [40] that if a large quantum computer could be built, factoring and discrete logarithms in $\mathbb{Z}_p$ would be easy; his results have also been extended to elliptic curve groups. After slow initial progress, in 1992 a 7-bit quantum computer has been demonstrated [41], which managed to factor 15 (note that the technology used in this approach is not scalable). Experts are divided on the question whether sufficiently powerful quantum computers can be built in the next 15-20 years. Nevertheless, this provides an additional motivation to develop asymmetric algorithms that are resistant to quantum computers.

Research on new asymmetric algorithms is progressing slowly; many proposals have a very short lifetime. Candidate systems that are still being studied include algorithms based on the following techniques: large error-correcting codes (e.g., McEliece and variants), multivariate polynomial equations (HFE and variants), lattices (NTRU), number field systems and braid groups. So far it seems very hard to match both the performance and the security of the most popular algorithms.

2.5 Standards

It is well understood that standards are essential for interoperability and economy of scale. Establishing high quality standards is very difficult, particular in areas which are evolving quickly such as information technology. For cryptographic standards, another dimension needs to be added: the standard does not only need to be competitive, it also needs to offer an adequate security level. Several cryptographic standards had to be revised after publication and even deployment because serious security problems were identified. If an adequate security evaluation has been performed, the standard brings some security guarantees as an additional benefit. On the other hand, security standards imply the risks of a single target of attack and of a lack of diversity. There are several standardization bodies in the area of cryptographic algorithms and protocols; the main players include ISO/IEC JTC1/SC27, ISO/TC68, IETF (with limited coordination between the many working groups), NIST, ANSI, IEEE, ETSI, 3GPP, Bluetooth SIG, RSA Labs (PKCS). To quote A.S. Tanenbaum: “The nice thing about standards is there’s so many to choose from.”

Problems with security standards are not only created by the technical difficulty of developing cryptographic algorithms and protocols as discussed above. Often, there is no time or expertise for an in-depth security analysis. Mechanisms are sometimes selected based on vested interests or ‘negotiated’, rather than chosen based on merit. In the past there has also be significant political pressure to include on crippled algorithms or protocols. It may also be that commercial considerations result in the introduction in the standard of a weak solution, while at the same time one sells a proprietary high-security solution at a premium price.

Even if a standard is adequate when it is published, progress in research may make it obsolete or insecure. Many standardization bodies do not have efficient maintenance procedures to respond efficiently to such developments. Once a standard has been widely deployed, upgrading it brings significant costs, hence the typical pattern is that upgrades of algorithms and protocols take a very long time; moreover backward compatibility with older insecure solutions may open avenues for attacks. Examples of algorithms that have been widely deployed beyond their useful lifetime include DES and MD5.

3 The ECRYPT Project

ECRYPT is a Network of Excellence funded under the 6th Framework Programme in the thematic area Information Society Technologies (IST); ECRYPT is one of the projects that contribute to the development of a global dependability and security framework. ECRYPT has started on February 1, 2004 and is funded for four years. The total estimated cost of the project is about 8.4 MEURO, of which 5.6 MEURO is funded by the European Commission.

ECRYPT has 32 partners from 14 countries; 7 are large companies, and 2 are small ones; the remaining 23 are universities or research institutions. The ECRYPT partners are: Katholieke Universiteit Leuven (B), Coördinator, École Normale Supérieure, Paris (F), Ruhr-Universität Bochum (D), Royal Holloway, University of London (UK), BRICS, University of Aarhus (DK), University of Salerno (I), Institut National de Recherche en Informatique et en Automatique (F), University of Bristol (UK), Gemplus SA (F), France Telecom R&D (F), IBM Research GmbH (CH), Technical University Eindhoven (NL), Université Catholique de Louvain (B), Universität Duisburg-Essen (D), Technical University of Denmark (DK), University of Bergen (N), Lund University (S), Institute for Applied Information Processing and Communications (A), Institute of Mathematics of the Polish Academy of Sciences (P), Cryptolog International SAS (F), Vodafone Group Services Ltd (UK), Ericsson AB (S), Axalto SA (F), MasterCard Europe sprl (B), Edizone GmbH (D), Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (D), Otto-von-Guericke University Magdeburg (D), Centre National de la Recherche Scientifique (F), University of Vigo (S), National Inter-University Consortium for Telecommunications (I), University of Geneva (CH), Aristotle University of Thessaloniki (GR).

3.1 Objectives

The main objective of ECRYPT is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. In order to reach this goal, the ECRYPT partners propose to integrate their research capabilities within five virtual labs focused on the following five core research areas: symmetric key algorithms, public key algorithms, protocols, implementation, and watermarking (cf. Sect. 3.3).

The integration activities include joint workshops, exchange of researchers and students, development of common tools and benchmarks and a website (http://www.ecrypt.eu.org) and forum which will be a focal point for the network and the wider cryptographic community. Each virtual lab organizes one formal *open* workshop per year; in the first project year, there have been open workshops on multi-party protocols, stream ciphers, provable security, and special purpose hardware (for cryptanalysis). In addition there are a number of 'ad hoc' internal research meetings. The ECRYPT website will contain a number of web resources on stream ciphers, AES hardware implementations, side-channel attacks,... A joint infrastructure is being developed which includes tools for the evaluation of cryptographic algorithms, a benchmarking environment for cryptographic hardware and software, infrastructure for side channel analysis measurements and tools, and tools for benchmarking watermarking schemes. It is important to note that ECRYPT has set aside a substantial budget to sponsor research visits and of non-ECRYPT researchers.

Spreading activities include a training program, a substantial contribution towards standardization bodies and an active publication policy. Each year several summer schools will be organized of at least one week, jointly between two virtual labs. The topic for the first schools are elliptic curve cryptology, cryptanalysis (both symmetric and asymmetric), unconditionally secure protocols and multimedia security. ECRYPT intends to improve the interaction between the research community, standardization bodies and the users of cryptology (government, industry, end users). The goal is to make sure that the new developments are integrated into applications and benefit the end-users. ECRYPT will also publish an annual list of recommended algorithms, protocols and parameter sizes for symmetric and asymmetric algorithms (including digital signature suites, encryption algorithms, ...).

3.2 Organization

The highest authority within ECRYPT is the General Assembly, in which each partner has one vote. The General Assembly decides on all strategic matters, including budget allocation. The project is run by the Ecrypt Management Committee (EMC) that meets on a quarterly basis. The EMC consists of the five virtual lab leaders, the chairman of the strategic committee and two additional members in charge of IPR issues and standardization. The EMC is chaired by the project manager, who is in charge of the day to day management; he is supported by the project administrator. The strategic committee consists of highly experienced people from industry and academia; it provides guidance and feedback on the long-term approach taken by the research network. The virtual labs are organized in smaller working groups. A typical working group consists of 5 to 15 people; one or two people are in charge for the directions of the working group. Working groups can be reorganized on a yearly basis depending on the research needs.

3.3 Research Goals of the Virtual Labs

The activities of the ECRYPT Network of Excellence are organized into five virtual laboratories established as follows:

1. Symmetric techniques virtual lab (STVL);
2. Asymmetric techniques virtual lab (AZTEC);
3. Protocols virtual lab (PROVILAB);
4. Secure and efficient implementations virtual lab (VAMPIRE); and
5. Watermarking and perceptual hashing virtual lab (WAVILA).

Each virtual lab intends to promote and facilitate cryptographic research on a pan-European level.

STVL. This virtual lab covers the design and analysis of symmetric cryptosystems. Three particular areas of research have been identified within the scope of the STVL, corresponding to three working groups. The first target for the efforts of the STVL is the development of secure and efficient stream ciphers; a task that will require considerable input from industry and academia alike. A second target for the STVL is a coordinated cryptanalytic assessment of the Advanced Encryption Standard (AES). A third virtual lab of STVL focuses on strategic research; in the next years, one of the items that will be to addressed is the development of lightweight cryptographic primitives as a fundamental building block for ambient intelligence.

AZTEC. The focus of AZTEC is the design and analysis of asymmetric cryptographic techniques. Four main areas of study have been identified. First, it is important to study, compare and propose mechanisms for provable security, to improve and better understand the security of asymmetric schemes. A second target for the AZTEC efforts is to develop alternatives to the RSA scheme, with particular attention to lightweight solutions. In the Internet era, many new applications are emerging for which asymmetric primitives with some specific properties are required; this forms the topic of the third working group. Finally, since it is clear that no unconditionally secure asymmetric cryptography can exist, the fourth area of AZTEC is the study of the hardness of the computational problems that are used as underlying assumptions in asymmetric cryptology.

PROVILAB. This virtual lab is concerned with cryptographic protocols, where two or more agents interact in order to reach some common goal; this can be to establish a secure network connection, to realize a payment transaction securely, or to carry out a secure auction or voting protocol over a network. A large body of theoretical research on protocols already exists, but our basic knowledge is still far from complete. Furthermore, analyzing the security of concrete protocols is notoriously difficult, and several solutions proposed and sometimes even used in practice have later turned out to be insecure. The first objective of PROVILAB is therefore to construct practically useful protocols for a wide range of applications with well understood and provable security. The second is to expand our basic knowledge, for instance in the area of unconditional security, i.e., protocols that remain secure, no matter the resources invested in breaking them. PROVILAB has three working groups, that focus on two-party protocols and secure point-to-point connections, practical multi-party protocols with provable security, and on unconditionally secure protocols.

VAMPIRE. The VAMPIRE lab has a dual role in ECRYPT. On the one hand, it studies new techniques that are related to efficient and secure implementation. On the other hand, VAMPIRE provides a bridge between the research and the user community. In concrete terms, the technical goals of the VAMPIRE lab for the duration of ECRYPT can be summarized as follows: development of novel efficient implementation techniques in hardware and software; development of a solid understanding of existing and new side channel attacks and efficient countermeasures; researching and understanding of cryptanalytical hardware and its impact on cryptographic parameters. There are also non-technical objectives. VAMPIRE intends to stimulate the interesting interplay of secure algorithms and secure implementations; it also hopes to foster cooperation between strong engineering groups and pure crypto groups. Also, it is a major goal to bridge the existing gap between the research community and engineers in industry who need to apply implementation techniques. Another important objective is to assist the researchers in the other (more theoretical) Virtual Labs in understanding the requirements and meeting the needs of applied cryptography. The four working groups of VAMPIRE focus on software implementation, hardware implementation, side-channel attacks, and strategic research.

WAVILA. The watermarking and perceptual hashing virtual lab (WAVILA) intends to broaden the scope of ECRYPT beyond the classical cryptographic techniques into the domain embedded signalling and fuzzy signatures. These two techniques have recently been proposed as important ingredients in digital rights management (DRM) systems, but they have never fully been analyzed with respect to security and usage (protocols), comparable to the standard of cryptography. It is the goal of WAVILA to build tools and techniques for assessing the security aspects of watermarking and perceptual hashing, to design advanced algorithms with a well-defined security level, to design protocols, both stand-alone as well as integrated in cryptographic protocols, and to develop methods and techniques for efficient and secure implementations. The overall and broader goal is to bring watermarking and perceptual hashing to such a level that they can be successfully be integrated into future DRM systems.

4 Conclusion

In this article, we have provided some arguments to support our claim that the cryptographic problem is not solved at all. Both at the practical and at the theoretical level, there are some very interesting problems and challenges that need to be addressed. We are convinced that the coordinated approach towards these research problems that is being developed in the Network of Excellence ECRYPT will bring significant benefits. By strengthening the cooperation between researchers both in industry and academia and by stimulating interdisciplinary research in the broad area of cryptology and watermarking, substantial progress can be made towards solving the security problems we will face in the next decade.

Acknowledgements and Disclaimer

The author would like to thank all the ECRYPT members and in particular the ECRYPT Management Committee for their contributions towards creating the Network of Excellence. The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.

The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

1. 3GPP, http://www.3gpp.org.
2. R.J. Anderson, "Why cryptosystems fail," *Communications ACM*, Vol. 37, No. 11, November 1994, pp. 32–40.
3. G. Ars, J-C. Faugère, M. Sugita, M. Kawazoe, H. Imai, "Comparison between XL and Gröbner Basis Algorithms," *Advances in Cryptology, Asiacrypt 2004, LNCS*, P.J. Lee, Ed., Springer-Verlag, 2004, in print.
4. M. Bellare, P. Rogaway, "Random oracles are practical," *Proc. First Annual Conference on Computer and Communications Security,* ACM, 1993, pp. 62–73.
5. M. Ben-Or, S. Goldwasser, A. Wigderson, "Completeness theorems for noncryptographic fault-tolerant distributed computing," *Proc. of 20th Annual Symposium on the Theory of Computing,* 1988, pp. 1–10.
6. E. Biham, R. Chen, "Near-collisions of SHA-0," *Advances in Cryptology – Crypto'04, LNCS 3152,* M. Franklin, Ed., Springer-Verlag, 2004, pp. 290–305.
7. A. Biryukov, A. Shamir, D. Wagner, "Real time cryptanalysis of A5/1 on a PC," *Fast Software Encryption, LNCS 1978*, B. Schneier, Ed., Springer-Verlag, 2001, pp. 1–18.
8. Bluetooth Specification, https://www.bluetooth.org/spec/.
9. R. Canetti, O. Goldreich, S. Halevi, "The random oracle methodology, revisited," *Proc. of 30th Annual Symposium on the Theory of Computing,* 1998, pp. 209–218.
10. F. Chabaud, A. Joux, "Differential collisions: an explanation for SHA-1," *Advances in Cryptology, Proc. Crypto'98, LNCS 1462*, H. Krawczyk, Ed., Springer-Verlag, 1998, pp. 56–71.
11. N. Courtois, J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," *Advances in Cryptology, Proc. Asiacrypt'02, LNCS 2501*, Y. Zheng, Ed., Springer-Verlag, 2002, pp. 267–287.

12. D. Chaum, C. Crépeau, I. Damgård, "Multi-party unconditionally secure protocols," *Proc. 20th ACM Symposium on Theory of Computing,* 1988, pp. 11–19.
13. C. Diem, "The XL-algorithm and a conjecture from commutative algebra," *Advances in Cryptology, Asiacrypt 2004, LNCS*, P.J. Lee, Ed., Springer-Verlag, 2004, in print.
14. J. Daemen, V. Rijmen, *"The Design of Rijndael. AES – The Advanced Encryption Standard,"* Springer-Verlag, 2001.
15. B. den Boer, A. Bosselaers, "Collisions for the compression function of MD5," *Advances in Cryptology, Proc. Eurocrypt'93, LNCS 765*, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 293–304.
16. H. Dobbertin, "Cryptanalysis of MD4," *Journal of Cryptology*, Vol. 11, No. 4, 1998, pp. 253–271. See also *Fast Software Encryption, LNCS 1039*, D. Gollmann, Ed., Springer-Verlag, 1996, pp. 53–69.
17. H. Dobbertin, A. Bosselaers, B. Preneel, "RIPEMD-160: a strengthened version of RIPEMD," *Fast Software Encryption, LNCS 1039*, D. Gollmann, Ed., Springer-Verlag, 1996, pp. 71–82.
    See also `http://www.esat.kuleuven.ac.be/∼bosselae/ripemd160`.
18. H. Dobbertin, "The status of MD5 after a recent attack," *CryptoBytes*, Vol. 2, No. 2, Summer 1996, pp. 1–6.
19. FIPS 46, *"Data Encryption Standard,"* Federal Information Processing Standard, National Bureau of Standards, U.S. Department of Commerce, January 1977 (revised as FIPS 46-1:1988; FIPS 46-2:1993).
20. FIPS 197, *"Advanced Encryption Standard (AES),"* Federal Information Processing Standard, National Institute of Standards and Technologies, U.S. Department of Commerce, December 6, 2001.
21. FIPS 180, *"Secure Hash Standard,"* Federal Information Processing Standard (FIPS), Publication 180, National Institute of Standards and Technology, US Department of Commerce, Washington D.C., May 11, 1993.
22. FIPS 180-1, *"Secure Hash Standard,"* Federal Information Processing Standard (FIPS), Publication 180-1, National Institute of Standards and Technology, US Department of Commerce, Washington D.C., April 17, 1995.
23. FIPS 180-2, *"Secure Hash Standard (SHS),"* Federal Information Processing Standard (FIPS), Publication 180-2, National Institute of Standards and Technology, US Department of Commerce, Washington D.C., August 2002 http://csrc.nist.gov/publications/fips/.
24. S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," *Selected Areas in Cryptography, SAC 2001, LNCS 2259*, S. Vaudenay, A. Youssef, Eds., Springer-Verlag, 2001, pp. 1–24.
25. S. Goldwasser, S. Micali, A. Wigderson, "How to play any mental game, or: a completeness theorem for protocols with honest majority," *Proc. 19th ACM Symposium on Theory of Computing,* 1987, pp. 221–229.
26. P. Hawkes, G. Rose, "On corrective patterns for the SHA-2 family," *Presented at the Rump Session of Crypto'04,* August 2004.
27. A.P.L. Hiltgen, "Constructions of feebly-one-way families of permutations," *Advances in Cryptology, Proc. Auscrypt '92, LNCS 718,* J. Seberry and Y. Zheng, Eds., Springer-Verlag, 1992, pp. 422-434,
28. A. Joux, P. Carribault, W. Jalby, C. Lemuet, "Collisions in SHA-0," *Presented at the Rump Session of Crypto'04,* August 2004.
29. A. Klimov, A. Shamir, "New cryptographic primitives based on multiword T-functions," *Fast Software Encryption, LNCS 3017*, B. Roy, W. Meier, Eds., Springer-Verlag, 2004, pp. 1–15.

30. A.K. Lenstra, E. Tromer, A. Shamir, W. Kortsmit, B. Dodson, J. Hughes, P.C. Leyland, "Factoring estimates for a 1024-bit RSA modulus," *Advances in Cryptology, Proc. Asiacrypt'03, LNCS 2894*, C.S. Lai, Ed., Springer-Verlag, 2003, pp. 55–74.
31. S. Murphy, M.J.B. Robshaw, "Essential algebraic structures within the AES," *Advances in Cryptology, Proc. Crypto'02, LNCS 2442*, M. Yung, Ed., Springer-Verlag, 2002, pp. 1–16.
32. NESSIE, http://www.cryptonessie.org.
33. NIST, AES Initiative, http://www.nist.gov/aes.
34. B. Preneel, "Analysis and design of cryptographic hash functions," *Doctoral Dissertation*, Katholieke Universiteit Leuven, 1993.
35. B. Preneel, "Cryptographic primitives for information authentication – state of the art," *State of the Art in Applied Cryptography, LNCS 1528*, B. Preneel, V. Rijmen, Eds., Springer-Verlag, 1998, pp. 50–105.
36. RIPE, *"Integrity Primitives for Secure Information Systems. Final Report of RACE Integrity Primitives Evaluation (RIPE-RACE 1040)," LNCS 1007*, A. Bosselaers, B. Preneel, Eds., Springer-Verlag, 1995.
37. R.L. Rivest, "The MD5 message-digest algorithm," *Request for Comments (RFC) 1321*, Internet Activities Board, Internet Privacy Task Force, April 1992.
38. R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications ACM*, Vol. 21, February 1978, pp. 120–126.
39. A. Shamir, E. Tromer, "Factoring large numbers with the TWIRL device," *Advances in Cryptology, Proc. Crypto'03, LNCS 2729*, D. Boneh, Ed., Springer-Verlag, 2003, pp. 1–26.
40. P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proc. 35nd Annual Symposium on Foundations of Computer Science*, S. Goldwasser, Ed., IEEE Computer Society Press, 1994, pp. 124–134.
41. L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, I.L. Chuang, '’Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, 414, 2001, pp. 883–887.
42. K. Vedder, "Security aspects of mobile communications," *State of the Art in Applied Cryptography, LNCS 741*, B. Preneel, R. Govaerts, J. Vandewalle, Eds., Springer-Verlag, 1993, pp. 193–210.
43. X. Wang, X. Lai, D. Feng, H. Yu, "Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD," *Presented at the Rump Session of Crypto'04,* August 2004.
44. M.J. Wiener, "Efficient DES key search," *Presented at the Rump Session of Crypto'93.* Reprinted in *"Practical Cryptography for Data Internetworks,"* W. Stallings, Ed., IEEE Computer Society, 1996, pp. 31–79.