

# NOVEL AUTHENTICATION FOR COMPUTER SECURITY

Long Hoang Nguyen

## PART 1: PREVIOUS RESEARCH TRACK RECORD

I have been studying for my D.Phil. (Ph.D.) with Prof. Bill Roscoe at the Oxford University Computing Laboratory since 2005. I have published one paper in the leading journal *Information & Computation* [7], and another two [8,9] appearing in the proceedings of international workshops on computer security in 2006 and 2008. At University College in Oxford, I won the Paul Memorial Scholarship: rewarding research excellence in 2007, and my D.Phil. is expected to be awarded in May 2009.

The explosion in digital technology, particularly in mass-produced handheld devices in pervasive environments, exposes ordinary users to new kinds of risk in computer security, such as *identity theft*. Similar risks also arise from a great variety of new network links connecting these devices, such as proximity or short-range channels between credit cards and their terminals as well as humans who interact with these devices and with each other through social communication. The network is therefore not as homogeneous as it used to be, and requires a richer model to capture a wider range of features, for example, low-power devices and low-bandwidth network links. Even though the new constraints and limitations in computation make conventional technology, most notably “Public Key Infrastructures” (PKI), unsuitable for many modern applications, they will potentially bring in new tools, interesting ideas, and different assumptions.

My papers introduce new cryptographic techniques, termed *digest functions*, and new families of authentication protocols to establish secure communication from *human actions* and *interactions* (i.e. human trust), thus eliminating the need for passwords, PKI, or any other pre-existing security infrastructures. It is believed that these can herald a new age of computer security that is more suitable for mobile and pervasive computing devices. The exciting and new research topic has been studied by many researchers around the world, such as Stajano and Anderson [16], Gehrman, Mitchell et al. [4], McCune, Perrig et al. [6], and Nyberg and Asokan [1,15]. It would also be reasonably accurate to say that the earlier sequence of papers of Creese, Roscoe et al. [2,3] defined the problem, while my recent ones [7,9] solved it.

Although all groups attempt to optimise the human element, the Oxford line of attacking the problem is more theoretical than that taken by others [4,5,6,15,16]. In particular, other researchers tend to work on specific practical implementations of human interactions, whereas Roscoe and I generalise them in order to quantify human interactions in terms of *bits*. This establishes a formal framework to prove the optimality of human effort relative to the level of security obtained. Subsequently, I was the first to categorise many known protocols in the area according to their aims (group, pair, and one-way) and structures (direct versus indirect information binding) [10], leading to some interesting results. For example, I discovered that some well-studied schemes neither optimise human effort nor offer as much security as was previously believed. I then proposed improved versions for all of these [8,10,11]. We, at Oxford, believe that we are the first to study the problem of optimising both human interaction and computational cost in a scientific way [7,9].

Since the work was published, it has received much attention from researchers in the field. I have been invited to develop some of my protocols into international standards [11], which will be presented at the ISO/IEC meeting in Cyprus in October 2008, since they are demonstrably superior to the current standards in this area. The work benefits the UK society and economy through many applications in supporting secure payments (e.g. CHIP&PIN, telephone and online banking), the military, telephony, and healthcare (e.g. telemedicine). This can be demonstrated by (1) patent protection for the families of protocols [12,13,14] sought through ISIS, Oxford University’s technology transfer company; and (2) the applications have been implemented and tested over a wide range of media, such as WIFI, the Internet, Telephone, Bluetooth, Email, and Text messages of mobile phones, which have attracted significant interest from major banks, telephone and defence companies, for example, HSBC, Barclays, BT, and QinetiQ.

As part of my research, I have been invited to give talks at institutions across the globe, including Cambridge University, Katholieke Universiteit Leuven, ETH Zurich, Stanford University, Carnegie Mellon University, and Xerox PARC, to name just a few. More details are given in my CV.

## Specific expertise available at the Host Organisation

The security group at the Oxford University Computing Laboratory, headed by Prof. Bill Roscoe, is one of the leading centres in the world on Computer Security, and particularly in authentication. Prof. Bill Roscoe, in collaboration with current and former members of the department such as Sadie Creese and Michael Goldsmith, is an authority of an earlier thread of work in pervasive computing that was funded by ONR, QinetiQ, and DTI [2,3]. His research interest has mainly been connected to Communicating Sequential Processes (CSP) and its verification tool FDR, which have found many successful applications, such as formal verification of security protocols and hardware design (e.g. the floating point unit of the Transputer).

The security group includes five permanent faculties (Bill Roscoe, Gavin Lowe, Ivan Flechais, Andrew Simpson, and Andrew Martin), plus one Royal Society Research Fellow (Andrew Ker) and a long-term visiting academic from Kestrel Institute (Dusko Pavlovic). Of the first, Prof. Gavin Lowe is one of the principle developers of CSP-based approaches to the analysis of computer security, and the first to show the feasibility of model-checking analysis of security protocol via his attack on the Needham Schroeder Public Key Protocol. Dr. Ivan Flechais and Dr. Andrew Martin work on the issue of trust and human factors in computer security. Of the latter, Dr. Dusko Pavlovic has made many advances in semantics of computation, and is now working on formal verification of the new families of authentication protocols based on human interactions. Dr. Andrew Ker's interest is in information hiding: steganography and steganalysis, and in particular he has recently proved fundamental results on steganographic capacity.

Other members of the department whose expertise would be valuable help include Prof. Marta Kwiatkowska and her expertise in development of probabilistic model checkers (e.g. PRISM has been used for analysing many security protocols, such as PIN cracking scheme), Prof. Tom Melham and his work on Higher Order Logic theorem proving (e.g. HOL Theorem Prover supports formal reasoning for security), and Prof. David Gavaghan and his interdisciplinary research in applying computational techniques to biomedical problems.

## References (continued on page 8)

1. *Simple Pairing White Paper*. Lisbon release of the Bluetooth core specification (2006).
2. S.J. Creese, M.H. Goldsmith, A.W. Roscoe, I. Zakiuddin. *The attacker in ubiquitous computing environments: Formalising the threat model*. Formal Aspects in Security and Trust workshop (2003).
3. S.J. Creese, M. Goldsmith, R. Harrison, A.W. Roscoe, P. Whittaker, I. Zakiuddin. *Exploiting empirical engagement in authentication protocol design*. Security Pervasive Computing, LNCS **3450** (2005).
4. C. Gehrman, C. Mitchell, K. Nyberg. *Manual Authentication for Wireless Devices*. RSA Cryptobytes **7** (2004), 29-37.
5. M.T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, E. Uzun. *Loud and Clear: Human-Verifiable Authentication Based on Audio*. IEEE Conference on Distributed Computing Systems (2006).
6. J.M. McCune, A. Perrig, M.K. Reiter. *Seeing is Believing: Using Camera Phones for Human-Verifiable Authentication*. IEEE Symposium on Security and Privacy (2005).
7. L.H. Nguyen, A.W. Roscoe. *Authenticating ad-hoc networks by comparison of short digests*. Information and Computation **206** (2008), 250-271.
8. L.H. Nguyen, A.W. Roscoe. *Separating two roles of hashing in one-way message authentication*. FCS-ARSPA-WITS (2008), 195-210.
9. L.H. Nguyen, A.W. Roscoe. *Efficient group authentication protocol based on human interaction*. FCS-ARSPA (2006), 9-32.
10. L.H. Nguyen, A.W. Roscoe. *Authentication protocols based on low-bandwidth unspoofable channels: a comparative survey*, submitted to Journal of Computer Security.
11. L.H. Nguyen. *Revision of the international standard ISO/IEC 9798-6*, submitted to ISO/IEC committee.
12. A.W. Roscoe, L.H. Nguyen. *Security in computing networks*, International Patent Application, published by the World Intellectual Property Organization (WIPO), publication number: WO/2007/052045, (2007).
13. A.W. Roscoe, B. Chen, L.H. Nguyen. *Improvements in communications security*, International Patent Application No. PCT/GB07/004963, WIPO, publication number: WO/2008/078101 (2008).
14. A.W. Roscoe, L.H. Nguyen. *Improvements related to the authentication of messages*, UK Priority patent application number 0811210.4, filed on 18 June 2008.
15. J. Suomalainen, J. Valkonen, N. Asokan. *Security Associations in Personal Networks: A Comparative Analysis*. LNCS **4572** (2007).
16. F. Stajano, R. Anderson. *The resurrecting duckling: Security issues for ad-hoc wireless networks*. LNCS **1976** (1999), 172-194.

## PART 2: DESCRIPTION OF THE PROPOSED RESEARCH AND ITS CONTEXT

### A. Background

One of the most important problems in computer security is authentication: users want proof that the agent they are communicating with, or who has generated a piece of data for them, is the one he or she claims to be. Just about every computer security application, such as digital signatures, digital rights management (DRM), message authentication codes (MAC), and key agreement protocols, depends on authentication. This has been recognised in the development and the popularity of the Bluetooth protocol, although this has been recognised as having significant security flaws [21], due to severe off-line password guessing or dictionary attacks. Bellare et al. [17] subsequently introduced various formal frameworks to fix the problems.

The two ideas most frequently used in authentication techniques are Public Key Infrastructures (PKI) and *cryptographic hashing*. It is known that PKIs are expensive algorithmically and too complex to be managed by non-experts. Furthermore, they authenticate names as opposed to specific contextual information required in many modern applications, such as “the laptop I can *see* in front of me” or “the till *sitting in front* of Jim”.

A (cryptographic) hash function inputs an arbitrary length bit string and produces a fixed length bit string as output. Its main purpose is to provide data integrity, and therefore it should have the properties of being inversion and collision-resistant. For this reason, hash output length should be large, i.e. 160 to 256 bits, which is expensive when it comes to processing large quantities of data for applications, such as DRM. There is a variant of hash functions, termed *universal* hash functions invented by Wegman and Carter in their influential paper [19], which forms the basic building block for constructing MAC.

My proposed research aims to design and use digest functions to support secure communication, and thereby reduce the need for PKI and hashing. This offers an alternative to traditional authentication techniques. Digests are similar to (universal) hashes, but some extra restrictions are imposed. They have much shorter outputs – individually less secure in terms of collision and inversion resistances – than has typically been the case. However, they are required to deliver a sufficient security against *one-shot attacks* (i.e. the enemy makes a single attempt without doing any searching), and to be more efficient to run than (universal) hashes.

$digest(k, M)$  is the  $b$ -bit digest of an arbitrary length message  $M$  relative to key  $k$ .

As key  $k$  varies uniformly over its domain:

1.  $digest(k, M)$  is uniformly distributed for any fixed  $M$ ;
2. For any pair of distinct messages  $(M, M')$ , and any  $\theta$ :  $\Pr_k[ digest(k, M) = digest(k \oplus \theta, M') ] \leq 2^{-b}$

The challenges are (1) to overcome a tension between efficiency and security in designing digest functions; and (2) to use digests such that the enemy cannot discover or constructively modify the key that the checker of a digest will use (i.e. protecting digests against *combinatorial manipulation*). In the mechanisms, devices exchange data over some medium, e.g. WIFI, and then display a digest of the protocol’s run that owners of these devices compare *manually* (e.g. verbally or visually) to ensure they have the same piece of data they try to agree on (i.e. the latter represents human interactions involved).

There has been some recent work constructing short output functions with similar security properties and purposes to digest functions, due to Pasini and Vaudenay [28], and Gehrman et al. [4]. Their approach relies on applying a standard cryptographic hash to the input message, something which is less efficient than required, especially for large size messages in important applications, e.g. DRM. Equally, the theory and behaviour of universal hash functions (such as the *Wegman-Carter* effect [19]), which are strongly related to digest functions, have been investigated extensively to date. For example, Stinson [29] and Bierbrauer et al. [18,22,23] established a remarkable connection between universal hash functions, coding theory, and combinatorics. More recently, Roscoe and I extended the results to demonstrate that a well-studied Toeplitz matrix-based construction of digests and universal hash functions resembles integer multiplication [27].

The problem of designing good hash functions has a long history in computer science, ranging from hash tables in data storage to (customised) cryptographic and universal hashes in computer security. However, this seems to be the first attempt to study efficient and secure short output functions in a comprehensive and scientific way. This would benefit the theory of hashing, and might shed new light on the use of hash functions in existing and new applications in secure payment, healthcare, telephony, and the military, as will be demonstrated in my research proposal. Moreover, authentication has a tradition of drawing on different areas of cryptography for its tools. It is exciting that digest functions can now play an important role.

## B. Programme and methodology

### Aims and Objectives:

I intend to pursue some potentially ground-breaking concepts in computer security, based on the use of short-output digest functions as an alternative to standard cryptographic hashes.

My thesis centred on the design of new families of authentication protocols, in which I attempted to optimise both human interactions and computational cost through the use of digest functions. In contrast to this, in my proposed research I plan to investigate the theory of digests, and then propose constructions that meet criteria set out previously. I aim to exploit the speed advantage of digests in many other potential applications.

In addition to editing an international standard on some of my protocols, the general aims are to:

- develop efficient and secure algorithms for computing digest functions, and then verify the security and efficiency of the constructions relative to standard cryptographic hashing (**milestones 1 & 2**).
- unify the theory of many classes of universal hash functions, and from this derive fundamental insights into the nature and design of both universal hashes and digest functions (**milestone 3**).
- develop protocols that can authenticate an extremely large amount of data efficiently, such as in DRM, using digest functions to replace standard cryptographic hash functions (**milestone 4**).
- extend successful applications of the new families of protocols in supporting secure payments into other potential areas, such as healthcare informatics (telemedicine) and telephony (**milestone 5**).
- investigate and formalise different forms of relaxation in human actions and interactions, involved in the new families of authentication protocols developed in my D.Phil. thesis (**milestones 6 & 7**).

The specific details of the programme of research are outlined below.

### **Constructing efficient and secure digest functions.**

Besides being useful in the new families of protocols, the study of digest functions has cryptographic applications on the design of (universal) hashing algorithms, which has surged since the recent breakthrough in techniques of breaking cryptographic hashes [31], e.g. SHA-1 and MD5. As digest output is short, my aim is to construct digest algorithms that are significantly faster than cryptographic hashes, but have a demonstrable security. The new and fresh ideas appear challenging due to a tension between efficiency and security in designing digest functions; yet there are two lines of attack that merit further investigation.

My papers present some schemes for computing digests, and their customised versions, based on the use of a *pseudo-random number generator* (PRNG) and Toeplitz matrix multiplication, traced back to the successful work of Krawczyk on universal hashes [24]. These are faster to compute than cryptographic hashes, e.g. MD5 and SHA, as has been demonstrated by comparative performance figures. However, I need to investigate further ones, and to provide convincing proof that digest functions' requirements are in fact met. I aim to optimise the use of PRNG in the definitions together with statistical analysis of such functions, i.e. the *strict avalanche condition* and *chi-squared test* for uniformity (**milestone 1**). It is exciting that one could hope to perform the statistical and combinatorial tests exhaustively, or at least on the major components of these algorithms individually, thanks to short digest output. If this approach works, the methods of computing digests could generate much research in the area of PRNG, and in particular almost  $k$ -wise independent random variables.

Although many PRNGs can be implemented efficiently, the process of generating good pseudo-random numbers is not completely understood. Subject to this, I propose to investigate digest constructions which are not based, or significantly less reliant, on a PRNG, and which have a coherent mathematical structure; thus eliminating the need for statistical tests on the digest algorithms. There has been an enormous amount of research building efficient universal hash functions as opposed to cryptographic hashes. Of particular interest are constructions based on *error-correcting codes* [18], *cyclic redundancy codes* [24], and *polynomials hashing* over finite fields [22]. However, these put a limit on input-message length. It is likely that this work will transfer easily to digest algorithms because of their many close relationships, and the challenge would be to overcome, or significantly extend, the limit on input-message length (**milestone 2**).

I plan to work on the two milestones in the first 15 months of the Fellowship. The primary outcomes expected to be efficient and secure digest algorithms, which would be reported in one or more publications in, for example, *Cryptographic Hash Workshop* (CHW) or *ECRYPT Hash Workshop* (EHW). However, the algorithms will be continuously refined and tested throughout the course of this project, perhaps with the help of Master and final year students, whose theses on this research topic will be supervised by me.

### **Unifying the theory of many classes of universal hash functions (UHF).**

This work is important since it could reveal fundamental insights into the nature of many classes of UHFs, e.g. *AU*, *AXU*, and *ASU*, as well as *digest* functions. Similar to a digest, the following is the definition of an  $\epsilon$ -almost universal hash function (or *AU*): for any pair of distinct messages  $(M, M')$ , as key  $k$  varies uniformly over its domain:  $\Pr_k[ H(k, M) = H(k, M') ] \leq \epsilon$ . Of particular interest is the problem of unifying many known lower bounds on the key length of these classes of UHF (**milestone 3**).

In the last two decades, several bounds for each class of UHF have been introduced by many researchers [20,23,26,29], but unfortunately they work in different ranges of the security parameter  $\epsilon$ . Until recently, it has appeared difficult to combine these into a single one due of some behaviour, which is hard to be captured within a single formula, most notably the *Wegman-Carter* effect [19]. However, by including further parameters into the proof of a new *AU*-bound, derived by Roscoe and myself, I have successfully extended the *pair-wise* version of the bound into the corresponding *k-wise* version [26]. Consequently, one should hope to be able to apply this new approach to obtain similar effects with respect to other properties.

Another interesting observation is that these classes of UHF are strongly related to one another, i.e. *ASU* is a stronger version of *AXU*, which in turns is a generalisation of *AU*. I therefore propose to explore the possibility of unifying the various bounds of different classes of UHF as follows. Some striking results of Stinson [29] and Bierbrauer et al. [18] demonstrate theoretical equivalences between UHF, *error-correcting codes*, and *combinatorial* designs. Subsequently, known bounds on classical combinatorial designs, e.g. *orthogonal arrays* and *difference matrices*, have been used successfully to derive equivalent bounds on UHF. Hence, I hypothesise that finding other ways to transfer between other combinatorial designs, e.g. *Latin squares*, and combinations of different classes of UHF, could give rise to better bounds. In addition to this, related work by Krawczyk [24] and Kurosawa et al. [25] makes a connection between *k-wise* independent random variables and UHF, which might offer another line of attacking this problem.

This is, however, an ambitious and independent aspect of my project, and is not without risk, but even if it were unsuccessful it would still be interesting to combine only a few of the bounds. I wish to spend the second year of the Fellowship working on milestone 3. Research outcome would be published at a leading conference in cryptology, such as *Eurocrypt*, *Asiacrypt*, and *Crypto*. I believe that this work is useful in not only cryptography but also numerous other branches of computer science, such as data storage or any applications that make use of hash tables.

### **Authentication without (cryptographic) hashing.**

When communicating an extremely large message  $M$  whose origin needs to be authenticated (for example, to prove authorship of a DVD or photographs), it is conventional to accompany this message with its cryptographically signed hash (i.e. a MAC or a signature):  $M//H(k, M)$  or  $M//Sign(hash(M))$ . Typically, the computation of this *long* hash dominates the calculation. I intend to develop methods, which can solve this problem more efficiently through the use of *short* output digests (**milestone 4**).

The challenge of this approach is that, since digest functions are less secure than cryptographic hashes, one needs to separate one-shot attacks, which can be defeated by good digests, from combinatorial manipulation. This idea is known as the principle of “separation of security concerns”, originally developed in my D.Phil. work. It is perhaps surprising to realise that this principle actually underlies the design of many well-studied protocols in the literature, most notably the various improved versions of Bluetooth [1,17]. More recently, a new concept, termed *Flexi-MAC* [8] and based on this idea, has been introduced by Roscoe and myself which offers advantages in security, efficiency, and flexibility over the usual format of data authentication.

The work demonstrates the use of digest functions as an alternative to standard cryptographic hashing in a variety of applications. Since the credibility of these new methods will depend crucially on the development

of digest functions which have demonstrable security and are fast to run (see milestones 1 and 2), I aim to work further on this problem after some progress on building digests has been made, i.e. from the last quarter of the first year. I hope that this work (patent pending [14]) will find applications in, for example, the field of *digital rights management*, through the help of ISIS.

### **Applications in healthcare informatics.**

I am seeking to engage with a variety of potential users for the new families of authentication protocols developed in my D.Phil. thesis not only in secure payments but also in healthcare, telephony, and the military by developing new and existing contacts with the industry. The crucial point is that these protocols build security on new concepts of trust, which are derived from human actions and interactions. These are both relevant and understandable by non-experts in contrast to a PKI. Since this research could have a huge impact on society, research centres around the world are, often independently and confidentially, seeking different applications of the new families of protocols. A typical example is the Simple Pairing Whitepaper [1] (Bluetooth) whose contributors are from Microsoft, Nokia, and Intel. Equally, I am currently pursuing the international standardisation and patent process of some of my protocols [11,12,13,14].

Many challenges in creating secure communication are born out of medical applications, particularly in *telemedicine*, where sensitive data, such as heart rate pattern or mental health data (e.g. Psychosis or Bipolar), are collected or uploaded via local WIFI, cellphones, and the Internet, from wearable sensors on patients. I believe that the solutions found (patent pending [13]) for credit card security in similar circumstances, for example, CHIP&PIN technology, online and telephone banking, are all readily adaptable. Another advantage of the protocols and digest functions is that they offer extremely efficient authentication of large quantities of medical data compared to cryptographic hashes. With this new approach, telemedicine could become more secure and useable; healthcare conditions could be monitored from many parts of the world, thus enabling a virtual healthcare system (**milestone 5**).

I am aware of the legal and ethical issues that might be involved in exploiting the potential of this work in healthcare. Through the help of ISIS, I would endeavour to approach medical companies, such as “T+ Medical” whose remote disease management systems were developed by Oxford University. Another possibility is to develop military applications via my established contact with QinetiQ, a defence company who funded my D.Phil. studies. Meanwhile, many banks and telephone companies, such as HSBC, Barclays, and BT, have shown their interest in the applications of my work in supporting secure payments and local WIFI connection.

I propose to work on milestone 5 in the second year, after having made progress on digest functions (see milestones 1 and 2) and authentication without hashing (see milestone 4). I plan to take a two-month visit at the security groups in Stanford and Xerox PACR, and I hope to take advantage of the expertise available at these institutions. For example, D. Boneh, J. Mitchell (Stanford), and D. Smetters (Xerox PARC) have made many contributions in peer to peer network, web security, and pervasive computation. The research outcome would be filed for either international patents (WIPO) or standardisations (ISO/IEC).

### **Relaxation in human work.**

Arising from the wide range of applications of the new families of authentication protocols, the problem of how humans can play their parts efficiently and reliably in the protocols will potentially become important. As there is a tension between ease of use and ensuring compliance with the protocols, this problem has received considerable interest from worldwide research groups, notably Asokan of Nokia [15], Perrig at CMU [6], and Tsudik at UCI [5]. In my research, I propose two different approaches to those of both these groups, aiming to reduce (1) the likelihood of human error, and (2) human work, as laid out below.

The authors of [5,6,15] introduced and tested a number of ways of comparing digests, for example, human and telephone conversation, typing a string of digits, voice recognition, and scanning barcode. However, their approaches do not give users any room for *human tolerance* or noisy human channels. Since humans are error-prone, I intend to take human tolerance into account (**milestone 6**). In this context, I first plan to survey popular types of human tolerance, such as incorrect or missing characters in comparing digests, which can be formalised in terms of the *maximum Hamming* distance. This could then be used to quantify the level of security obtained relative to different degrees of the types of human tolerance. This suggests a scope for the use of *error-correcting code* in displaying digests.

Since research in human interactions has mainly focused on pair-wise situations [5,6,15], the possibility of *human work distribution*, as far as I am aware, has never been investigated in pair-wise or group scenarios. For example, a number of participants, perhaps in different locations, distribute the work of comparing different portions of a digest, and then report the results to one another at the end. On one hand, the length of digest can be extended to make the protocols more secure. On the other hand, I need to minimise the amount of overhead communication required between nodes (**milestone 7**). This, perhaps surprisingly, resembles the well studied “*Gossiping and Broadcasting problem*” in combinatorics [30], i.e. the number of pair-wise conversations grows linearly with the number of people involved. There is probably a trade-off between the size of sub-groups and cross-group communication; I intend to simulate experiments with respect to real time delays in communication and a variable group size.

Building on many applications of the families of authentication protocols (see milestones 4 and 5), the third year of my project is to be devoted to milestones 6 and 7. I would look to benefit from the expertise and knowledge of many researchers, who are working on human interfaces for security in this department as well as the Cybersecurity Laboratory at CMU. Of the latter, I plan to take a 2-month visit at CMU, where Perrig is an authority on many aspects of human factors. The outcome would be presented at international workshops, such as *Security and Privacy in Pervasive Computing* (SPPC), *Security Pervasive Computing* (SPC), and *Symposium on Security and Privacy* (S&P).

#### **Editing a revision to an international standard, ISO/IEC 9798-6 [11].**

I have been invited to serve as editor of the revision to an international standard on entity authentication, using manual data transfers. Typically, editing an ISO standard takes two or three years. As well as incorporating my improved protocols, I will have the duty to consider algorithms proposed elsewhere. This would involve collaboration with experts, many of whom I have met while giving seminars at leading research groups across the globe. If successful, this could help me promote my work to the industry of smart cards, telephony, and particularly in healthcare informatics (see milestone 5).

#### **C. Relevance to beneficiaries**

My work is theoretical, but it has applications in many areas. It spans from pure mathematics and probability theory to computer science where I expect to be able to influence the technology we all use every day. For example, users of handheld devices would benefit from this research, both in finance, telephony, the military, and healthcare, through less heavy burden on human interaction and more efficient authentication protocols.

The invention of digest functions not only offers a new cryptographic tool to researchers designing security protocols generally, but also can make authentication more feasible and accessible in new applications, thanks to its efficient speed of computation in relation to standard cryptographic hashes.

#### **D. Justification for the Fellowship**

This Fellowship will enable me to pursue a personal research programme, which is expected to make a unique and valuable contribution to a rapidly developing field over the next three years. Although I have initiated the majority of this work, the project might be considered high risk as it departs from mainstream approaches to authentication; the Fellowship offers a secure position from which to carry out this ambitious programme without external distractions.

Although I have benefited from my supervisor’s invaluable advice, my proposed research (i.e. working on digests and universal hash functions: the theory of cryptology, and their applications) is significantly different from his research, which is mainly connected to formal verification techniques through CSP and its verification tool FDR. Furthermore, he is going to be on sabbatical, and therefore I will be ideally placed to undertake this original research independently. It is an excellent opportunity for me to guide the growing team of his research students who are already working in this area during his absence. This valuable experience will help me consider the option of founding a new research group in cryptography to work alongside the already well-known security group at Oxford in the future. This ambition is reflected in the theme of my proposed research as well as my decision to leave Bristol University, where I did my undergraduate thesis in a large cryptography group, in order to do a D.Phil. at Oxford University.

I propose to remain at Oxford for two principle reasons: the presence of the foremost experts in authentication, Bill Roscoe, Gavin Lowe, along with Dusko Pavlovic, represents the most productive and knowledgeable potential collaborators for the work proposed. (More details are given in “The Expertise at

the Host Institution”). Moreover, Oxford University has an excellent infrastructure of identifying, protecting, and marketing technologies through ISIS and its extensive link to the industry, such as “T+ Medical” and QinetiQ mentioned above. This will help me apply my research outcome to real world problems.

Giving talks at universities worldwide during my D.Phil. has enabled me to establish personal contacts with many researchers active in diverse areas related to this proposal. As a result, I plan to take short visits of two months each at the security groups in Stanford and Xerox PARC, and CMU as mentioned above.

### **E. Dissemination and exploitation**

The results of my research would be published in leading scientific journals and conferences, as pointed out at the end of each branch of the research programme. This would expose the work to both the cryptography and security communities. During the Fellowship, I would expect to produce at least one paper on each of the following: the theory and constructions of digest functions; theoretical bounds of universal hash functions; applying digest functions to other applications of security, and authentication in particular; relaxation of human work in the new families of protocols.

My international standardisation [11] and patent applications [12,13,14] of the protocols, digest functions, and their many applications in supporting secure payments (e.g. CHIP&PIN, online and telephone banking), healthcare informatics (e.g. telemedicine), telephony, and the military (see milestones 4 and 5) would benefit the UK society and economy. These together with the protocols’ implementation across a wide range of mediums, such as WIFI, the Internet, Bluetooth, Email, Telephone, and Text messages, potentially will be fully exploited to solve real world problems, as can be demonstrated by interest shown from many banks, telephone and defence companies, for example, HSBC, Barclays, QinetiQ, and BT, to name just a few.

I wish to attend the Communication skills and Media training courses, organised by the Royal Society, which could give me the confidence and skills needed to communicate my work on a non-technical level to a wide range of audiences, whether it be pupils, researchers from other disciplines, or the media and the public.

I intend to continue giving talks at research groups worldwide as well as familiarising the industry with the significance and applications of my work, as I have been doing throughout my D.Phil. studies.

### **References** (continued from page 2)

17. M. Bellare, D. Pointcheval, P. Rogaway. *Authenticated Key Exchange Secure against Dictionary Attacks*. Eurocrypt, LNCS **1807** (2000), 139-155.
18. J. Bierbrauer, T. Johansson, G.A. Kabatianskii, B.J.M. Smeets. *On Families of Hash Functions via Geometric Codes and Concatenation*. Crypto, LNCS **773** (1993).
19. J.L. Carter, M.N. Wegman. *Universal Classes of Hash Functions*. Journal of Computer and System Sciences, **18** (1979), 143-154.
20. P. Gemmell, M. Naor. *Codes for Interactive Authentication*. Crypto, LNCS **773** (1993)
21. M. Jakobsson, S. Wetzel. *Security Weaknesses in Bluetooth*. CT-RSA, LNCS **2020** (2001), 176-191.
22. T. Johansson, G.A. Kabatianskii, B. Smeets. *On the relation between A-Codes and Codes correcting independent errors*. Eurocrypt, LNCS **765** (1993), 1-11.
23. G.A. Kabatianskii, B. Smeets, T. Johansson. *On the cardinality of systematic authentication codes via error-correcting codes*. IEEE trans. Inform. Theory, **42** (96), 566-578.
24. H. Krawczyk. *New Hash Functions For Message Authentication*. Eurocrypt, LNCS **921**(1995),301-310.
25. K. Kurosawa, T. Johansson, D.R. Stinson. *Almost k-wise independent sample spaces and their cryptologic applications*. Eurocrypt, LNCS **1233** (1997), 409-421.
26. L.H. Nguyen, A.W. Roscoe. *New combinatorial bounds for universal families of hash functions*, submitted to Eurocrypt 2009.
27. L.H. Nguyen, A.W. Roscoe. *Efficient digest functions based on Toeplitz matrix and integer multiplication*, in preparation (manuscript is available).
28. S. Pasini, S. Vaudenay. *An Optimal Non-interactive Message Authentication Protocol*. CT-RSA, LNCS **3860** (2006), 280-294.
29. D.R. Stinson. *On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes*. Congressus Numerantium, **114** (1996), 7-27.
30. R. Tijdeman. *On a Telephone Problem*. Nieuw Archief voor Wiskunde **19**, 188-192, 1971.
31. X. Wang, Y.L. Yin, H. Yu. *Finding Collisions in the Full SHA-1*. CRYPTO 2005.