



Future Commercial Opportunities for Cryptography

Dr Robert Rowlingson, Chief Technology Officer, OrbisIP

David Lacey

June 2009

Abstract

This report describes future commercial opportunities for cryptography. In the 'potentially very attractive' box are secure financial transactions, data loss prevention, digital rights management, gaming, cloud computing, social networking and machine to machine encryption. There appears to be a good fit and a shared understanding of the commercial opportunities for cryptography amongst the academics and industry people we spoke to. The drivers for research are typically also important industry problems. But despite this there is a disconnect between the research and its commercialisation. There is a clear breakdown of the technology transfer life-cycle which is described in detail and needs to be addressed. This report should help funders and investors as part of their decision making and thereby improve wealth creation from cryptography research.



Table of Contents

Abstract	1
Executive Summary	4
Introduction	6
Aim of this Report	7
Sample Questions Considered by the Workshops.....	7
Academic Research Workshop Output	9
Taxonomy	9
Theory	9
Attacks.....	10
Proofs	10
Algorithms and Protocols	10
Implementations.....	11
Applications of Cryptography Research.....	12
Machine to Machine Cryptography	12
Multi-party computation	12
Hardware issues	13
Lattice-based cryptography.....	13
E-voting and Privacy	14
Key Management.....	15
Business Requirements for Cryptographic Technologies	16
Integrity protection	16
Agreed Data File format	17
Securing the Cloud.....	18
Development issues.....	18
Implementation issues	18



Operational issues.....	19
Maintenance issues.....	20
Usability issues	20
Weaknesses in Cryptography Technology Transfer	21
Conclusions	23
Acknowledgements	25
References	26
Appendix 1 Relevant Research Topics	28
From SECrypt 2007 conference.....	28
Area 1: Access Control and Intrusion Detection	28
Area 2: Network Security and Protocols	28
Area 3: Cryptographic Techniques and Key Management	29
Area 4: Information Assurance	29
Area 5: Security in Information Systems.....	29
Topics From the Financial Cryptography and Data Security Conference	30
Appendix 2 An Overview of Cryptanalysis.....	32
Types of cryptanalytic attack.....	32
Prior knowledge: scenarios for cryptanalysis.....	32
Classifying success in cryptanalysis.....	33
Complexity	34



Executive Summary

The aims of this report are:

- To understand the market and future requirements for cryptographic technology;
- To identify the options for customers and suppliers thinking of investing in crypto R&D;
- To be aware of emerging research and technology directions in cryptography;

In order to provide:

- Better understanding of future business opportunities;
- Better understanding of research directions with commercial potential;
- Better connectivity between researchers and innovators/entrepreneurs;

Some areas with highest commercial potential were identified as:

- Secure Financial Transactions;
- Data Loss Prevention;
- Digital Rights Management;
- Gaming;
- Cloud computing;
- Social networking;
- Machine to machine encryption.

In each of these market areas the future requirements are addressed by a number of possible research directions, teams, and developments which are ongoing. Some cryptographic approaches targeting these areas include lattice-based methods and secure multi-party computation, amongst a very large research community which has not been exhaustively scoped.

There appears to be a good fit and a shared understanding of the commercial opportunities for cryptography amongst academics and industry users and investors. The drivers for research are typically also important industry problems. But despite this there is a disconnect between the research and its commercialisation. There is a clear breakdown of the technology transfer life-cycle which needs to be addressed if suitable options for investors and customers are to emerge and better connectivity between researchers and innovators and entrepreneurs is to be achieved.



There are problems in IP protection, IT developer understanding, investor appreciation of the subtleties of the cryptographic research process, product marketing and communication, product usability and customer understanding. These are combining to make it difficult for novel cryptography technologies to come to market. These are in addition to the general issues of a long life-cycle in some cryptographic technologies.

It is clear that there is a huge market need for future commercial applications of cryptography. There is also some excellent research. There are opportunities for significant wealth creation and improved information security if the barriers identified in this report can be overcome.



Introduction

Advances in cryptography clearly have the potential to address key challenges in the cyber security domain, from identity management to secure communications, from privacy protection to secure e-commerce. Cryptography research is a UK strength and it is important that this strength is converted into effective commercialisation and business growth.

This project, sponsored by the Cyber Security KTN and carried out by OrbisIP and David Lacey, has organised meetings and interviews to identify the commercial challenges and opportunities for cryptography, in alignment with the KTN mission.

Part of the context of this work is recent developments and announcements in quantum cryptography (see for example [1]). These have raised awareness of quantum cryptography as a future commercial application of cryptography. In the cryptography research community, quantum cryptography is generally regarded as being over-hyped. The physics community has a long track record of attracting funding!

However, quantum cryptography is not the only direction for cryptography research which may have commercial potential. Other avenues may provide better commercial opportunities and this work is aimed at identifying them.

A considerable amount of cryptographic research concerns the security properties of algorithms. Essential though this is, as a necessary filter for sound solutions, it does not easily lead to new business opportunities for cryptography. A key premise of this report is that expert knowledge is required to extract the cryptographic developments that have commercial potential from the masses of published literature. The aim is to use these experts' knowledge of the current research base to identify those research topics and directions that may have commercial potential. The identified innovations may have the potential to open new markets and provide new commercial opportunities.



Aim of this Report

The aim of this report is to identify and review possible technology areas, research activities and research papers from around the world, that demonstrate an innovative approach or direction in cryptography which may lead to new commercial opportunities. This short study cannot possibly cover the full scope of a large research space as cryptography, typified by the topics detailed in Appendix 1. The output of this work is therefore not intended to be an exhaustive list of such research, nor should it be seen as an endorsement of any particular work. Any omissions are the fault of the authors and are in no respects a reflection of any opinion on any work not mentioned. The idea is to provide better awareness of research with commercial potential and to guide potential funders and investors in evaluating new cryptographic developments. In summary the aims are:

- To understand the market and future requirements;
- To identify the options for customers and suppliers thinking of investing in crypto R&D;
- To be aware of emerging research and technology directions in cryptography;

In order to provide:

- Better understanding of future business opportunities;
- Better understanding of research directions with commercial potential;
- Better connectivity between researchers and innovators/entrepreneurs;

The aim is to identify and review possible technology areas, research activities and research papers that demonstrate an innovative approach or direction in cryptography which may lead to commercial potential. This is followed by a commercial view on how these technologies could be exploited, which parts of the market offer the highest potential and where further development is required to meet commercial needs.

This report should help funding bodies such as EPSRC and TSB, and commercial investors, to understand the upcoming business opportunities being facilitated by current research, and thereby it will influence UK investment strategy. It will also accelerate innovation by ensuring both technology push and commercial pull viewpoints are integrated into one report.

Sample Questions Considered by the Workshops



In order to structure discussions and provoke debate we addressed the following questions:

- What commercial opportunities exist in the various categories?
- What research is making progress in commercially relevant areas?
- What research is emerging to tackle future (currently unrecognised) problems?
- Where is research producing radical approaches to difficult problems that might open new markets?
- What research trends can be identified?
- What market trends can be identified?
- Where are the largest market opportunities?
- What technology gaps exist to meeting market requirements?

The size and scope of this report precluded an exhaustive study of these questions but examples and some discussion points are described below. We also considered more general issues around the commercialisation of cryptographic research. This led to very useful input on the barriers to cryptography commercialisation and technology transfer.



Academic Research Workshop Output

The next 10-20 years will see the research community looking to provide practical (and secure) solutions to problems which were previously only theoretically possible. Examples are computing on private data, multi-party computation. Indeed some systems have already been deployed. This could have major impact in areas such as cloud computing and outsourcing of functionality by companies.

Indeed in the context of business applications it is generally recognised that cryptography cannot be viewed in isolation e.g. IPSec was vulnerable in certain contexts of operation which were not foreseen, as the designers assumed a particular context. Similarly, SSH was vulnerable to simple attacks as the analysis had missed certain features. From our academic workshop it became clear that there is an important ecosystem of dependency in the evolution of cryptographic research towards commercial applications. This can be represented in a simple taxonomy.

Taxonomy

We may characterise cryptography research into the following 6 categories to help understand their commercial implications:

- Theory
- Attacks
- Proofs
- Algorithms and Protocols
- Implementations
- Applications

Theory

Theoretical work is important in the overall ecosystem of cryptography research. Without the underlying theory it would not be possible to prove the properties of various algorithms nor understand how to compose new algorithms and protocols. Although there are no obvious immediate commercial applications theoretical work underpins a lot of cryptographic research and provides the academic rigour for later, more application-oriented, results



Attacks

See Appendix 2 for an overview of cryptanalysis – this term is used to refer to any attempt to circumvent the security of any type of cryptographic algorithms and protocols in general, and not just encryption. However, cryptanalysis usually excludes methods of attack that do not primarily target weaknesses in the actual cryptography, such as bribery and physical coercion.

Embedded systems are vulnerable to side-channel analysis e.g. power analysis, timing analysis, fault analysis and radiation monitoring. Context and application are the keys to attacks. There is a lot of research in isolation but real-world environments are increasingly challenging, e.g. SSL messages were found to leak information because the padding has the wrong format. Cryptography cannot be viewed in isolation any more, e.g. IPSec was vulnerable in certain contexts of operation which were not foreseen, as the designers assumed a particular context.

High value crypto keys are especially vulnerable to power analysis. The MiFare travel smartcard used low-end, in-house crypto design which was inadequate and, therefore, hacked. The latest attack techniques are based on exploiting error responses that leak information about the key as well as, and sometimes combined with, the techniques of penetration testing honed on non-cryptographic software.

It is difficult for non-experts to know in practical terms which attacks seriously need to be addressed, witness the scare some years ago when a break was announced of the SHA-1 hash algorithm [2]. In particular industry need to know which attacks are commercially relevant in that they imply a need for novel counter-measure technology adoption or development. In the case of SHA-1 there was no need for immediate concern although the community has now moved on to a competition for its replacement as a standard.

Proofs

These are the bedrock of the academic community's understanding of the security of its research. Most papers proposing novel algorithmic or protocol approaches to cryptographic problems will contain mathematical assessments of security properties and complexity issues. These allow the evolution of improved algorithms by researchers.

Algorithms and Protocols

Protocols are becoming more complex and yet the tools for dealing with the analysis of such protocols are not keeping pace. Most academic work is still on relatively simple examples such as



Needham-Schroeder etc. Protocols are becoming more complex. Cryptography researchers avoid this. There is an interesting synergy with the formal methods community, who set out to analyse complex protocols. There used to be a separation between algorithm and protocol analysis. The trend now is to look at the whole problem space, though this is not yet a mature approach.

Implementations

In 10-20 years almost all deployed crypto algorithms will need replacing (indeed this is happening now) - DES->AES, RSA->ECC, MD5/SHA->SHA-3? There is a need to find better ways of doing such upgrades since this is highly disruptive. In particular, if a significant attack on a cryptographic standard were made public then replacements would need to be in place rapidly.

Another important implementation issue is the risk of loss of access to old or archival data because of the unavailability of cryptographic keys (an example of so-called 'bit-rot'). National archives will be highly vulnerable to such loss of crypto keys. We need future-proof encryption to ensure long-lived archives.



Applications of Cryptography Research

Machine to Machine Cryptography

Machine-to-machine crypto requirements are not widely appreciated. Some cars can have around 80 processors and in sensor networks there is a great opportunity for mobile, ad hoc network security as we move to more pervasive networks and ubiquitous computing models. Cryptography on motes, sensors and RFID are emerging requirements, especially with the visions of smart grids to support critical national infrastructure. An example of work here is on applying PKI to small devices such as motes¹ [3].

Multi-party computation

Secure multi-party computation is a problem that was initially suggested by Andrew C. Yao in a 1982 paper. In that publication, the millionaire problem was introduced: Alice and Bob are two millionaires who want to find out which is richer without revealing the precise amount of their wealth. Yao proposed a solution allowing Alice and Bob to satisfy their curiosity while respecting the constraints.

This problem and result gave way to a generalization called multi-party computation (MPC) protocols. In an MPC, a given number of participants p_1, p_2, \dots, p_N each have a private data, respectively d_1, d_2, \dots, d_N . The participants want to compute the value of a public function F on N variables at the point (d_1, d_2, \dots, d_N) . An MPC protocol is dubbed secure if no participant can learn more from the description of the public function and the result of the global calculation than what he/she can learn from his/her own entry — under particular conditions depending on the model used.

Cachin [4] discusses an interesting example protocol for the following problem: 'A' wants to buy some goods from 'B' if the price is less than his maximum buying price a . 'B' would like to sell, but

¹ A small device, typically consisting of a wireless transmitter/receiver along with a sensor, that can be deployed in large numbers in an ad hoc network.



only for more than her minimum selling price b . Neither of them wants to reveal their secret bounds. The solution uses an oblivious third party T who learns no information about a or b , not even whether $a > b$. The protocol needs only a single round of interaction, is efficient and ensures fairness. Applications include bargaining between two parties and secure and efficient auctions in the absence of a fully trusted auction service.

In certain scenarios confidentiality of information is crucial, but at the same time significant value can often be obtained by combining confidential information from various sources. This fundamental conflict between the benefits of confidentiality and the benefits of information sharing may be overcome using MPC, where computations are performed on secret values and results are only revealed according to specific protocols. Examples also include applications in on-line gambling however some on-line gambling applications might lack a business model if the need for a third party is eliminated.

Further interesting work in this area has developed a domain-specific programming language for Secure Multi-party Computation [5]. This work bridges the gap between high-level security requirements and low-level cryptographic operations constituting an MPC platform, thus improving the efficiency and security of MPC application development. The language is implemented in a prototype compiler that generates Java code exploiting a distributed cryptographic runtime.

Hardware issues

There is very little theory on APIs, attacks, etc. for hardware security modules. However, the idea that for all high security modules you can have custom hardware with special crypto accelerators will not be economically viable. Indeed similar changes are already affecting suppliers of coding solutions. In considering hardware versus software for implementation of software - each offers a different set of problems. The unit cost of chips is influenced by costs of verification, which grows exponentially with the increase in gates. People are moving to programmable and reconfigurable solutions. How to do this whilst still maintaining security against side-channel analysis?

Lattice-based cryptography



There are several reasons for interest in lattice-based cryptography² [6,7]. One is its potential in the area of cloud computing and secondly that the computations involved are very simple which can be advantageous in certain practical scenarios when encryption is performed by a low-cost device (also see above). Another reason is that currently there are not too many alternatives to traditional number-theoretic based cryptography such as RSA. Such alternatives will be needed in case an efficient algorithm for factoring integers is ever found. In fact, efficient quantum algorithms for factoring integers and computing discrete logarithms already exist. Although large-scale quantum computers are not expected to exist for some time, this fact should already be regarded as a warning. There are currently no known quantum algorithms for lattice problems.

IBM have recently reported the solution of a long-standing problem using lattice methods, called "privacy homomorphism," or "fully homomorphic encryption," it makes possible the deep and unlimited analysis of encrypted information without sacrificing confidentiality [8]. IBM's solution, uses a mathematical object called an "ideal lattice," and allows people to fully interact with encrypted data in ways previously thought impossible. Computer vendors storing the confidential, electronic data of others will be able to fully analyze data on their clients' behalf without expensive interaction with the client, and without seeing any of the private data. With this technique, the analysis of encrypted information can yield the same detailed results as if the original data was fully visible to all.

Using the solution could help strengthen the business model of "cloud computing," where a computer vendor is entrusted to host the confidential data of others in a ubiquitous Internet presence. It might better enable a cloud computing vendor to perform computations on clients' data at their request, such as analyzing sales patterns, without exposing the original data.

E-voting and Privacy

E-Voting and privacy are growing requirements and there are relatively few technologies, e.g. TOR (onion routing)

Secure electronic voting is the subject of a 4 year EPSRC funded project that has recently started. Cryptography can be used to preserve anonymity/secretcy of the ballot, to provide receipts of casting a vote, and also voter verifiability - assurances to the voter that their vote was actually included in

² A lattice is a set of points in n-dimensional space with a periodic structure (in 3-d think crystal) – the mathematical properties of which lend themselves to cryptanalysis and crypto design problems.



the final tally. Given the situation in Iran recently this is something that is important to voters if they have cause to doubt it. The wikipedia entry for Pret a Voter (the principal subject of the research) is at http://en.wikipedia.org/wiki/Pr%C3%AAt_%C3%A0_Voter.

Key Management

Key management is a major area but has so far attracted very little research. There is considerable research on public key cryptography but a lot less on key exchange issues.



Business Requirements for Cryptographic Technologies

Business requirements for cryptography are becoming increasingly broader and more pervasive. Reviewing the list of technologies in Appendix 1 from the SEcrypt conference the following are noted as having strong commercial potential:

- Securing financial transactions
- Counter espionage
- Data leakage prevention (DLP)
- Enabling secure collaborative working across corporate boundaries
- Ensuring data and software integrity
- Upholding digital rights management (DRM)
- Ensuring privacy and anonymity of user transactions
- Gaming
- e-Voting
- Enabling “externalization” of clients and applications on public networks
- Supporting virtualization of storage & processing
- Securing Cloud computing
- Searchable encryption
- Social networking
- Machine-to-machine communications (M2M)

Some of the above technologies may be particularly important to society, such as secure e-voting, but not as commercially attractive as others due to their respective market size. In the ‘potentially very attractive’ box are financial transactions, DLP, DRM, gaming, cloud computing, social networking and M2M encryption. The rest of this section discusses some important business issues related to the above technologies.

Integrity protection

Safeguarding data integrity is a growing business requirement and a potentially large driver for cryptographic solutions in the future. Attacks on data integrity can represent the most serious and



sophisticated forms of threat, causing irreparable damage to data assets. Yet visibility of this risk amongst user organisations remains very low, reflecting a lack of maturity by both attackers and target organisations in appreciation of the problem space.

A few damaging incidents could transform this perception. There are indications that many “early adopter” organisations, i.e. those in high threat environments such as on-line gaming or defence and aerospace sectors, are beginning to address this problem space. Others will follow over time. One or two specialist products have emerged in this area, but the business case is not yet sufficiently compelling to generate a sizable demand for technology purchases. But this is likely to change over the next decade.

Data integrity protection is needed for both data and software. Current solutions to software protection are inadequate, as they are limited in application. Code-signing, for example, is only useful at the time that software is being installed.

Ensuring audit data remains unchanged is an early potential candidate for cryptographic integrity protection. This idea first emerged during the 1990s but was neither mandated nor easy to implement. Demand for such a solution needs to be driven by regulatory compliance, and also supported by vendors of leading financial accounting software.

Schneier and Kelsey [9] point out that in many real-world applications, sensitive information must be kept in log files on an un-trusted machine. In the event that an attacker captures this machine, we would like to guarantee that he will gain little or no information from the log files and to limit his ability to corrupt the log files. They describe a computationally cheap method for making all log entries generated prior to the logging machine's compromise impossible for the attacker to read, and also impossible to undetectably modify or destroy.

Agreed Data File format

There is a strong, immediate need for an agreed, single, standard data file format to support message and file exchanges between organisations deploying different encryption products – a sort of encrypted analogue of pdf. The absence of such a solution is holding back efficient collaborative working across virtual supply chains. Standards exist (such as XML) but there is no clear accepted de facto standard, for example in the way that acceptance of SSL/TLS transformed e-Commerce.



Securing the Cloud

Ensuring security of data and software within an uncertain cloud of external network infrastructure is perhaps the most pressing contemporary challenge. Clouds of shared services can operate at all levels of the infrastructure, ranging from raw processing power to sophisticated business applications, and they can be positioned inside or outside corporate perimeters, presenting a broad range of risks and demanding a hierarchy of physical and technical solutions. The assets to be protected are also broad ranging from data to software algorithms and relationships. Business risk assessments for cloud computing are still at a very early stage, as corporate security functions have yet to study the full implications.

Development issues

The industry is inefficient. Some companies have good crypto skills but no business applications, other companies have good business applications but no crypto expertise. Secure programming is not the same science as secure crypto programming. There is a general lack of appreciation by IT people of the difficulty of cryptography.

Implementation issues

Many current devices on the market do not support encryption and are not built to withstand sophisticated attacks (IO Active have demonstrated this in the US). Even some widely deployed systems assumed to be secure are not.

The 'MiFare' travel card used low-end, in-house crypto design which was inadequate and, therefore, has already been the subject of three attacks. The latest will be published in a security conference in October but has led to claims that the London Oyster card, which uses the Mifare technology, is fundamentally flawed. The research leader has stated that he can "reverse the Mifare algorithmic code, allowing him to put credit back on his Oyster card".

<http://news.bbc.co.uk/1/hi/technology/7516869.stm>.

Perhaps more worrying is the serious risk to security as swipe cards to sensitive areas could be cloned. After learning of the breach in April, the Dutch Government posted armed guards outside all its buildings and it now plans to spend millions of euros upgrading its systems. It also postponed the



introduction of a €1 billion transport payment system similar to the Oyster card until security issues were addressed.

All smart card companies are concerned to get the security of their smart card chips sufficient to achieve the necessary certification processes not only through Common Criteria but also the extra processes applied by both Mastercard and Visa. In all these cases there is a need to address DPA (Differential Power Analysis) [10].

The company 'Cryptography research' announced the basis of these attacks back in 1998. The basic idea of the attacks is that the power consumption of a device is statistically correlated to the operations it performs. By monitoring the power usage (or electromagnetic radiation, etc.) during cryptographic operations, it is possible to obtain information correlated to the keys. The collected data is then analysed to actually determine the keys.

At the time they claimed to have implemented the attacks against a large number of smartcards, and did not believe that any cryptographic smartcards on the market were immune to these analysis techniques. Further information on Differential Power Analysis is on their web page at <http://www.cryptography.com/dpa>.

Now the leading silicon provider, Infineon, with about 30% of the smart card market has signed up to license the DPA resistance IP from Cryptographic research.

The terms of the deal have been kept private but Smart Card News [11] estimates the likely size of the deal. Infineon currently produces about 800 million microcontrollers for smart card applications. Their original agreement with Visa saw Cryptography research getting 25 cents (USD) per chip but with the market depressed this could not be sustained at those levels so the licensing could be in the range 1 – 5 cents per chip depending on the silicon manufacturer's margins.

The low margin business might yield, over the next 10 years, 1 cent for 500 million chips and for the higher margins perhaps 5 cents for say up to 100 million chips per year which over the 10 year remaining life of the patents would produce up to \$100 million [11].

Operational issues

Key management is a major area for business but appears to have attracted very little research and



very little innovation at the business level.

There is also a huge gap in practice between the potential strength of many cryptographic solutions and the actual strength of the products used in practice. Many implementations operate by transforming a simple password into a crypto key, substantially reducing the strength of the protection.

Maintenance issues

Current hardware implementations of cryptographic algorithms (e.g. in ATMs) are expensive and slow to change, requiring the manufacture of new printed circuit boards and the deployment of teams of engineers. On the other hand, software implementations can be more vulnerable to remote attacks by hackers or unauthorised changes introduced by inside staff. Given the need to periodically upgrade cryptographic algorithms, there is a clear need for more efficient maintenance mechanisms.

National Archives will be highly vulnerable to “bit rot” of crypto keys. We need future-proof archives. Timescales to implement and ease of replacement are big business issues.

Usability issues

Usability of cryptography is a long recognised issue first highlighted by a turn-of-the-century paper by Alma Whitten of Carnegie Mellon University called “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0” which analysed the difficulties as well as the security risks associated with inexpert use of complex cryptographic software. Although the ease of use of security software has improved, it falls far short of the requirements of the broader marketplace and continues to present the possibility of large scale breaches of data through a lack of knowledge and skills by users.

The safe and correct use of cryptographic software requires much better ergonomic design and usability testing. Products would benefit, for example, from the design of better, more concrete metaphors to help users appreciate the implications of particular actions.



Weaknesses in Cryptography Technology Transfer

Although the business requirements for cryptographic technologies are both numerous and pressing, there are currently a number of barriers to the uptake of new products.

These barriers are far from insurmountable, however, and could be overcome with better education, communication and marketing effort.

The first barrier is a widespread negative perception of crypto products by business customers, as a result of the confusion created by the emergence of a large number of relatively new products with uncertain provenance and unclear business benefits. Vendors need to market products based on clear business benefits and evidence of security claims, supported by case studies of successful implementations, rather than technology features. The problem space is highlighted by typical business disinterest (both buyers and investors) in new crypto products and companies.

A second barrier is the lack of customer knowledge about the strengths and suitability of individual products for particular applications. For example, one experienced business customer we interviewed described the need for a table showing the relative strengths of different technologies used for particular purposes against varying levels of threat.

The third barrier is that the technology itself solves only part of a business problem and business customers today are more comfortable with complete, integrated solutions rather than bolt-on, single-point products. Vendors need to offer better implementation support for technologies that might appear to be complex to deploy or use.

A further barrier is that most business customers view cryptography as a minimum requirement rather than a means of gaining competitive edge. Some key market sectors, e.g. financial services, adopt a "herd mentality" aiming for general agreement on a product before committing to a purchase. This can discourage the adoption of new, innovative products but on the positive side should allow a greater investment and testing of the security of proposed solutions.

Bad marketing of new crypto products turns off potential business customers. More emphasis on business applications is needed. Some products appear useful on the surface but have inadequate crypto. At the same time there are others that have great crypto but lack practical applications. Ideally there should be greater cooperation between companies with useful applications and those



with good crypto capability.

There is a general lack of appreciation by IT people of the difficulty of cryptography [12]. It is not solely a programming problem but principally a highly mathematical problem. Only cryptographers with the pre-requisite mathematical expertise and academic research background can satisfactorily review and assess new crypto research. Crypto, produced by non-crypto experts, is commonly broken easily. However cryptographers cannot easily endorse the security of cryptographic products, as their security will depend on the implementation as well as the strength of the algorithm. In addition the strength of any cryptography can only be 'proven' by publication and peer review as experts try to find weaknesses and breaks. An investor or customer can only have confidence in a crypto product if the underlying theory, protocol and architecture has gone through this peer review process [13] and this may not be the case for trade secrets and crypto developed by non-experts. The Jericho Forum, an international thought leadership circle led by senior security practitioners from leading companies, strongly promotes the development and use of open, secure protocols.

The product itself will also need to prove its credentials in terms of its resistance to 'standard' software vulnerabilities as well as crypto related vulnerabilities such as the risk that key related information can be extracted from an implementation.



Conclusions

There appears to be a good fit and a shared understanding of the commercial opportunities for cryptography amongst the academics and industry people we spoke to. The drivers for research are typically also important industry problems. But despite this there is a disconnect between the research and its commercialisation. There is a clear breakdown of the technology transfer life-cycle which needs to be addressed.

This project was originally looking to focus on specific technologies with commercial potential but in each of the areas seen as potentially interesting there are a number of possible research directions, teams, and developments which are ongoing.

Some areas with highest commercial potential were identified as:

- Secure Financial Transactions;
- Data Loss Prevention;
- Digital Rights Management;
- Gaming;
- Cloud computing;
- Social networking;
- M2M encryption.

It is not in the remit of this report to give an authoritative comparison of these developments but in a number of areas example technologies and research have been identified. What we have also done is effectively to have analysed the technology transfer life-cycle of cryptography and found a number of systemic issues which prevent good solutions coming to market. Some of these are well-known to the cryptography and security community, some of them less so. Certainly many of these issues need to be more visible to investors, research funders and customers who ultimately dictate what technology is transferred to the market.

From our academic workshop it became clear that there is an ecosystem of dependency in the evolution of cryptographic technologies through the taxonomy of research we presented. Proofs should be built on theory, implementations will follow protocols or algorithms, attacks will lead to



new implementations or revised algorithms or provoke the development of new theoretical approaches. The research moves forward iteratively by peer review.

In order to clarify the maturity and commercial readiness of a cryptographic technology it is worth asking the question ‘where does it fit within the context of this ecosystem?’ What theory underpins the development? What attacks have been tried? How might applications which use this protocol be protected? How might they be attacked in practice? And so on.

The answers to these questions should help investors, research funders and users understand the position of a technology within the life-cycle and thereby ensure appropriate action can be taken if they wish that technology to move further towards commercialisation.

There is some indication that patenting and commercialisation is not being carried out effectively for a number of reasons – common in this area – typically this is because the length of time before a technology is commercialisable may mean lengthy patent maintenance costs (witness the time between the announcement of differential power analysis attacks and the recent adoption of resistant technologies); academics’ drive to publish rather than protect IP; the difficulty for university technology transfer offices to understand the opportunities, the difficulty of all parties to understand or estimate the size of the market.

This may put a brake on commercialisation and on the eventual uptake of research since new start-ups may prefer to use patented cryptography to protect their commercial position even if there are ‘better’ publicly available systems. EPSRC for example could encourage protection of IP and monitor the IP produced in their recently approved 4 year project on secure e-voting. The recent success of ‘Cryptography research’ in licensing their DPA technology is an indicator of the potential returns (and concomitant security benefits) of seriously addressing the IP and licensing issues.

A “silo mentality” has developed between researchers and practitioners in different areas of crypto, and they are becoming more entrenched with the growth and increasing specialisation of the overall problem and solution spaces. There would be a lot more “interesting stuff” generated by breaking down these silos. Research funding models do not help: there is a tendency towards “themed research” rather than problem solving. UK research grants favour blue sky research. The US has more focus on demonstrators.

Business needs better guidance on how to determine which solutions are “good enough” for



safeguarding particular business applications against different levels of threat. Something on the lines of a table mapping threats against applications. For example, how easy is it to break different systems for file protection or communications security?

So there are problems in IP protection, IT developer understanding, investor appreciation of the subtleties of the cryptographic research process, product marketing and communication, product usability and customer understanding. These are combining to make it difficult for novel cryptography technologies to come to market. These are in addition to the inherent conservatism of traditional crypto users and the need for solutions to be 'proven' in some way. There is a huge market need for future commercial applications of cryptography. There is some excellent research. There are opportunities for significant wealth creation and improved information security if these barriers can be overcome.

Acknowledgements

The authors would like to thank the many people who provided input, suggestions and advice to our work, during the workshops, by email and in conversations. In particular we would like to thank, Kenny Paterson, Geraint Price, Nigel Smart, Steve Schneider and Andrew Yeomans. We would also like to thank the Information Security Group at Royal Holloway College and the Security Innovation and Technology Consortium at Cranfield University for helping us to arrange workshops and meetings.



References

- [1] 'Unbreakable' encryption unveiled, BBC News, October 2008, <http://news.bbc.co.uk/1/hi/sci/tech/7661311.stm>
- [2] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full sha-1. In CRYPTO, volume 3621 of LNCS, pages 17–36. Springer, 2005. <http://people.csail.mit.edu/yiqun/SHA1AttackProceedingVersion.pdf>
- [3] Bo Zhu, Feng Bao, et al, Efficient and Robust Key Management for Large Mobile Ad-hoc Networks, Computer Networks, 48(4): 657-682. Elsevier, July 2005.
- [4] Christian Cachin. Efficient private bidding and auctions with an oblivious third party. In *Proc. 6th ACM Conference on Computer and Communications Security*, pages 120-127, 1999 <http://www.zurich.ibm.com/~cca/papers/bid.pdf>
- [5] Janus Dam Nielsen, Michael I. Schwartzbach, A domain-specific programming language for secure multiparty computation, Programming languages and analysis for security archive Proceedings of the 2007 workshop on Programming languages and analysis for security pp 21 -30,
- [6] Daniele Micciancio, Oded Regev, Lattice-based Cryptography Book chapter in Post-quantum Cryptography, D. J. Bernstein and J. Buchmann (eds.), Springer (2008) <http://www.cs.tau.ac.il/~odedr/papers/pqc.pdf>
- [7] Oded Regev, Lattice-based Cryptography <http://www.cs.tau.ac.il/~odedr/papers/crypto2006.pdf>
- [8] Cryptography breakthrough paves way to secure cloud services , Computer Weekly, June 2009, <http://www.computerweekly.com/Articles/2009/06/30/236695/cryptography-breakthrough-paves-way-to-secure-cloud.htm>
- [9] B. Schneier and J. Kelsey Cryptographic Support for Secure Logs on Untrusted Machines, The Seventh USENIX Security Symposium Proceedings, USENIX Press, January 1998, pp. 53-62.



<http://www.schneier.com/paper-secure-logs.pdf>

[10] The Risks Digest, Volume 19: Issue 80, Differential Power Analysis, June 1998, <http://catless.ncl.ac.uk/Risks/19.80.html#subj3>

[11] Cryptography Research Clinches \$100m deal with Infineon, Smart Card and Identity News, August 2008, <http://www.smartcard.co.uk/articles/InfineonDeal.php>

[12] Schneier, B. Why Cryptography Is Harder Than It Looks, 1997, <http://www.schneier.com/essay-037.html>

[13] Schneier, B. Secrecy, Security, and Obscurity, Cryptogram Newsletter, May 2002, <http://www.schneier.com/crypto-gram-0205.html>



Appendix 1 Relevant Research Topics

From SECrypt 2007 conference

Area 1: Access Control and Intrusion Detection

- Intrusion Detection and Vulnerability Assessment
- Authentication and Non-repudiation
- Identification and Authentication
- Insider Threats and Countermeasures
- Intrusion Detection & Prevention
- Identity and Trust Management
- Biometric Security
- Trust models and metrics
- Regulation and Trust Mechanisms
- Data Integrity
- Models for Authentication, Trust and Authorization
- Access Control in Computing Environments
- Multiuser Information

Area 2: Network Security and Protocols

- IPsec, VPNs and encryption modes
- Service and Systems Design and QoS Network Security
- Fairness Scheduling and QoS Guarantee
- Reliability and Dependability
- Web Performance and Reliability
- Denial of Service and other attacks
- Data and Systems Security
- Data Access & Synchronization
- GPRS and CDMA Security
- Mobile System Security
- Ubiquitous Computing Security
- Security in Localization systems
- Sensor and Mobile Ad Hoc Network Security
- Wireless Network Security (WiFi, WiMAX, WiMedia and others)



- Security of GSM/GPRS/UMTS systems
- Peer-to-Peer Security
- E-commerce protocols and micropayment schemes

Area 3: Cryptographic Techniques and Key Management

- Smart Card Security
- Public Key Crypto Applications
- Coding Theory and Practice
- Spread Spectrum Systems
- Speech/Image Coding
- Shannon Theory
- Stochastic Processes
- Quantum Information Processing
- Mobile Code & Agent Security
- Digital Rights Management

Area 4: Information Assurance

- Planning Security
- Risk Assessment
- Security Area Control
- Organizational Security Policies and Responsibility
- Security Through Collaboration
- Human Factors and Human Behaviour Recognition Techniques
- Ethical and Legal Implications
- Intrusive, Explicit Security vs. Invisible, Implicit Computing
- Information Hiding
- Information Systems Auditing
- Management of Computing Security

Area 5: Security in Information Systems

- Security for Grid Computing
- Secure Software Development Methodologies
- Security for Web Services
- Security for Databases and Data Warehouses
- E-Health
- Security Engineering
- Security Information Systems Architectures
- Security requirements



- Security Metrics
- Personal Data Protection
- XML Security
- Workflow and Business Process Security

Topics From the Financial Cryptography and Data Security Conference

- Anonymity and Privacy
- Auctions and Audits
- Authentication and Identification
- Backup Authentication
- Biometrics
- Certification and Authorization
- Cloud Computing Security
- Commercial Cryptographic Applications
- Transactions and Contracts
- Data Outsourcing Security
- Digital Cash and Payment Systems
- Digital Incentive and Loyalty Systems
- Digital Rights Management
- Fraud Detection
- Game Theoretic Approaches to Security
- Identity Theft
- Spam
- Phishing and Social Engineering
- Infrastructure Design
- Legal and Regulatory Issues
- Management and Operations
- Microfinance and Micropayments
- Mobile Internet Device Security
- Monitoring
- Reputation Systems
- RFID-Based and Contactless Payment Systems
- Risk Assessment and Management
- Secure Banking and Financial Web Services
- Securing Emerging Computational Paradigms



- Security and Risk Perceptions and Judgments
- Security Economics
- Smartcards
- Secure Tokens and Hardware
- Trust Management
- Underground-Market Economics
- Usability
- Virtual Economies
- Voting Systems.

Appendix 2 An Overview of Cryptanalysis

From Wikipedia on 30th June 2009

Types of cryptanalytic attack

Cryptanalytic attacks vary in potency and how much of a threat they pose to real-world cryptosystems. A certification weakness is a theoretical attack that is unlikely to be applicable in any real-world situation; the majority of results found in modern cryptanalytic research are of this type. Essentially, the practical importance of an attack is dependent on the answers to the following three questions:

1. What knowledge and capabilities are needed as a prerequisite?
2. How much additional secret information is deduced?
3. How much effort is required? (What is the computational complexity?)

Prior knowledge: scenarios for cryptanalysis

Cryptanalysis can be performed under a number of assumptions about how much can be observed or found out about the system under attack. As a basic starting point it is normally assumed that, for the purposes of analysis, the general algorithm is known; this is Kerckhoffs' principle of "the enemy knows the system". This is a reasonable assumption in practice — throughout history, there are countless examples of secret algorithms falling into wider knowledge, variously through espionage, betrayal and reverse engineering. (On occasion, ciphers have been reconstructed through pure deduction; for example, the German Lorenz cipher and the Japanese Purple code, and a variety of classical schemes).

Other assumptions include:

- Ciphertext-only: the cryptanalyst has access only to a collection of ciphertexts or codetexts.
- Known-plaintext: the attacker has a set of ciphertexts to which he knows the corresponding plaintext.
- Chosen-plaintext (chosen-ciphertext): the attacker can obtain the ciphertexts (plaintexts) corresponding to an arbitrary set of plaintexts (ciphertexts) of his own choosing.
- Adaptive chosen-plaintext: like a chosen-plaintext attack, except the attacker can choose

subsequent plaintexts based on information learned from previous encryptions. Similarly Adaptive chosen ciphertext attack.

- Related-key attack: Like a chosen-plaintext attack, except the attacker can obtain ciphertexts encrypted under two different keys. The keys are unknown, but the relationship between them is known; for example, two keys that differ in the one bit.

These types of attack clearly differ in how plausible they would be to mount in practice. Although some are more likely than others, cryptographers will often take a conservative approach to security and assume the worst-case when designing algorithms, reasoning that if a scheme is secure even against unrealistic threats, then it should also resist real-world cryptanalysis as well.

The assumptions are often more realistic than they might seem upon first glance. For a known-plaintext attack, the cryptanalyst might well know or be able to guess at a likely part of the plaintext, such as an encrypted letter beginning with "Dear Sir", or a computer session starting with "LOGIN:". A chosen-plaintext attack is less likely, but it is sometimes plausible: for example, you could convince someone to forward a message you have given them, but in encrypted form. Related-key attacks are mostly theoretical, although they can be realistic in certain situations, for example, when constructing cryptographic hash functions using a block cipher.

Classifying success in cryptanalysis

The results of cryptanalysis can also vary in usefulness. For example, cryptographer Lars Knudsen (1998) classified various types of attack on block ciphers according to the amount and quality of secret information that was discovered:

- Total break — the attacker deduces the secret key.
- Global deduction — the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.
- Instance (local) deduction — the attacker discovers additional plaintexts (or ciphertexts) not previously known.
- Information deduction — the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.
- Distinguishing algorithm — the attacker can distinguish the cipher from a random permutation.

Similar considerations apply to attacks on other types of cryptographic algorithm.



Complexity

Attacks can also be characterised by the amount of resources they require. This can be in the form of:

- Time — the number of "primitive operations" which must be performed. This is quite loose; primitive operations could be basic computer instructions, such as addition, XOR, shift, and so forth, or entire encryption methods.
- Memory — the amount of storage required to perform the attack.
- Data — the quantity of plaintexts and ciphertexts required.

In academic cryptography, a weakness or a break in a scheme is usually defined quite conservatively. Bruce Schneier sums up this approach: "*Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity less than brute force*".