Institution: Royal Holloway, University of London

Unit of Assessment: Mathematical Sciences

Title of case study: Design of a block cipher used in TETRA secure radio

1. Summary of the impact (indicative maximum 100 words)

Terrestrial Trunked Radio (TETRA) is a very well known, international specification for secure mobile radio and 'walkie-talkie' communication, that is extensively used and relied upon by emergency and public safety services such as police, ambulance and fire services, as well as governmental and private bodies. The European Telecommunications Standards Institute (ETSI) began standardising TETRA in the 1990s and it is now widely used throughout the world. Foundations of its success include resilience and reliability, but security is a major feature, being underpinned by expert cryptographic design. In particular the authentication and key generation mechanisms in TETRA rely on a block cipher (HURDLE) which was designed by a team of cryptographers at Royal Holloway.

The work carried out at Royal Holloway underpins the integrity and security of TETRA safety-critical networks throughout the world to the present day. A secure design for emergency service communications minimises both the amount of disruption criminals can cause to service operations, and the amount of operational information such criminals can glean from eavesdropping, contributing to the safety and security of society as a whole as well as the economic benefits to manufacturers of TETRA-based equipment.

2. Underpinning research (indicative maximum 500 words)

A block cipher is an algorithm to efficiently realise a family of permutations of binary strings of a fixed length, these permutations being indexed by a (secret) key. The block cipher should be designed so that the permutations it realises behave as if they were randomly chosen to an observer not in possession of the key.

The underpinning research. HURDLE is a block cipher that was designed by a team of cryptographers at Royal Holloway: Matthew Dodd (PhD student; now an independent security consultant), Sean Murphy (lecturer; now Professor), Kenny Paterson (post-doctoral researcher; now Professor) and Fred Piper (Professor; now retired) [1]. This work was undertaken as part of a wider project to design and evaluate the security mechanisms of the TETRA standard. The project to standardise TETRA security was commissioned by ETSI-SAGE, the Security Algorithms Group of Experts at the European Telecommunications Standards Institute. The team at Royal Holloway designed the block cipher in 1996, and the specification was issued by ETSI-SAGE in January 1997 [1].

Quality. The design of a secure and efficient block cipher is a delicate process, which requires a combination of experience (in cipher design and cryptanalysis), technical precision and creativity. Any cipher to be used in a critical and large-scale project such as TETRA is expected to be world-leading in terms of its design and performance, and indeed cannot be allowed to fail in operational use.

The specification for HURDLE has been subject to a rigorous process of peer review by top experts in the area: the design was reviewed in detail by SAGE participants and contractors, including security experts from the mobile and wireless industries. These experts were drawn from the major companies of the time that were active in international standardisation, and included Alcatel, British Telecommunications, Deutsche Telecom, France Telecomm, KPN Research, Philips Electronics Eindhoven and Vodafone. This review process replaces, and is more rigorous than is usual for, the standard academic review process. The full specification for HURDLE and derivative TETRA Algorithms is available under an NDA to approved parties, but is otherwise confidential and so cannot be reviewed in the standard way. Attesting to the academic quality of

the specification, The President of the IACR (the main international organisation concerned with cryptographic research), a consultant for industry, and a member of ISO standards committees for security technologies) writes [2]:

> I would like to make two points: first, that good cipher specification is regarded as a significant research contribution in my field; second, that the review process for a key industrial cipher can be more demanding than the refereeing process for a top cryptography conference […] A typical submission to a cryptography conference will be reviewed by 2 or 3 academics (members of the programme committee, or their nominees). It is very unlikely that a typical reviewer will spend more than half a day examining each paper. For the […] TETRA ciphers above, the design will be reviewed by several teams (certainly more than 3), each team looking at the cipher for (as an absolute minimum) 2 days. The review procedure is therefore typically much longer than for a submission for an academic conference. Moreover, high-profile academics and highly-regarded industrial consultants are often the same people. This leads me to believe that the industrial review process is often more rigorous than for a top academic conference. I should mention a second, unofficial, 'reviewing' process of an industrial cipher takes place when the deployed cryptographic system is attacked by third parties. If the system remains resistant to real-world attacks, this gives further evidence of the quality of the cipher.
>
> All of this context points to the two ciphers that Royal Holloway are putting forward as being clearly of 2 star or higher research quality, as defined above.

In his letter of support, President of the IACR gives more detailed evidence of the high esteem the community gives to research of this type.

The President of the IACR makes the point above that resistance to real-world attacks is a measure of quality.
There is no evidence that HURDLE has been broken, despite being widely deployed in security-critical applications for many years. The former Chair of ETSI SAGE (Security Algorithms Group of Experts) and Chair of ETSI Project TETRA WG 6 (the TETRA security group) when the TETRA standard was created. He writes [1]:

> The security of TETRA was state-of-the-art, and I believe it is has stood up very well to developments over the past 15 years. I am not aware of any successful attacks on the security of TETRA.

The Chief Executive of the TETRA+ Association, a trade association to support TETRA which counts over 150 operators, manufacturers and other interested parties as members. He writes [3] of TETRA:

> As far as I am aware there have not been any reports of this security being breached ever and it continues to be deployed in existing and new implementations around the world. I am pleased to give credit for this remarkable achievement to Royal Holloway, University of London who designed the algorithms that provide this security.

Context. The design of HURDLE forms part of a strong tradition of the study of cryptology in the School that continues to the present day. Royal Holloway is designated as an Academic Centre of Excellence in Cyber Security Research (2012-) and hosts a Centre for Doctoral Training in Cyber Security (2013-); and our expertise in cryptography (as part of an interdisciplinary group spanning mathematics and computer science) contributes significantly to this. Highlights of work completed over the history of the group include the invention of key distribution schemes (Mitchell-Piper), the cryptanalysis of FEAL (the first use of differential cryptanalysis; Murphy), the algebraic framework for the cryptanalysis of AES (Cid-Murphy-Robshaw), pairing-based cryptography (Galbraith-McKee), ID-based cryptography (Paterson), key predistribution for Wireless Sensor Networks (Blackburn-Martin-Ng), codes for copyright protection (Blackburn-Ng) and group-based cryptography (Blackburn-Cid). Consultancy in the field of information security is regularly carried

out, including the design and cryptanalysis of ciphers and work with new digital mobile telephony standards. Blackburn, Cid, Martin, McKee, Murphy, Ng and Paterson are current academic staff who have published cryptography papers and/or undertaken cryptographic consultancy within the current REF period.

3. References to the research (indicative maximum of six references)

ETSI/SAGE Specification, 'Specification of the HURDLE-II Algorithm', European Telecommunications Standards Institute, 20 January 1997. Available under an appropriate NDA.

4. Details of the impact (indicative maximum 750 words)

What is the link between the research and the benefit? HURDLE is the cryptographic primitive that underpins authentication and key derivation in TETRA [1]. Authentication allows two mobile devices, or a base station and a mobile device, to confirm that each is a valid party in the network. Key derivation allows the generation of secret keys (such as session keys) used in communication protocols from longer-term secret key material. The TETRA standard [4] specifies authentication and key derivation operations in terms of TETRA Algorithms (denoted TA*n* in [4], where *n* is an integer). HURDLE is the cryptographic component in all the TETRA Algorithms in [4].

Who benefits? The TETRA mobile radio and 'walkie-talkie' communication standard is tailored for use by the public safety sector (such as police, fire and ambulance services), government agencies and the military. It was first developed as a European standard in the late 1990s, but is now marketed worldwide for a wide variety of safety-critical applications. There are now more than 1400 TETRA contracts, and TETRA is in use in over 130 countries, with over 200,000 users in the UK alone [3,5,6]. For example, the police forces from the following European countries use TETRA: Austria, Belgium, Denmark, Estonia, Finland, Germany, Greece, Iceland, Ireland, Italy, the Netherlands, Norway, Portugal, Poland, Romania, Slovenia, Sweden and the U.K. The standard is used by a range of other organisations with safety-critical needs. UK examples include London Underground, airport services at Aberdeen, Birmingham, Glasgow, Heathrow and Manchester and the UK Highways Agency. The TETRA Industry Group [5] lists a selection of recent TETRA implementations, showing that new users continue to switch to the standard. Since 2008, there have been applications to airport services, bus and tram services, disaster relief, fire services, gas extraction, the military, mining, oil extraction, roadside assistance, train communications, and communications in underground/metro networks. A wide range of European countries have been involved, plus Australia, Brazil, Canada, China, Haiti, India, Jordan, Kazakhstan, Kuwait, Malaysia, Mexico, Pakistan, Qatar, Russia and Singapore. Beyond the systems themselves, society as a whole benefits from the provision of secure and efficient infrastructure that keeps many millions of citizens protected from crime and terrorism, and safe in cases of emergency.

How do they benefit? Authentication in TETRA is used to prevent cloned devices from becoming part of the network, and to prevent illegitimate parties from masquerading as base stations. Key derivation algorithms are an essential part of other security functions provided by the network; for example, an insecure key derivation algorithm could result in decryption of TETRA communications, thereby compromising the confidentiality of sensitive data.

Security is a major feature of TETRA; indeed, the Pocket Guide [7] produced by the TETRA Association lists Communications Security as its first benefit, with authentication and encryption (both dependent on HURDLE) specifically highlighted:

> Communications security is a prerequisite for public safety agencies, and a critical requirement for the increasing number of commercial organisations that rely on TETRA.
>
> TETRA builds on the inherent security strengths of digital technology. A key feature of TETRA is the protection of the radio connection between devices and radio sites through the application of advanced Air Interface Encryption techniques.

TETRA's security measures deliver the strongest levels of protection; ensuring the privacy of conversations and the secure transmission of sensitive data.

A potential security loophole in networks – devices – is also addressed. Authentication at the connection between device and network controls traffic to ensure that transmissions are from approved users. If a terminal is misplaced or stolen it can be immediately disabled, preventing unauthorised personnel listening to private conversations or viewing sensitive information.

It is of national importance for a country's security-critical services to have a radio network that is not vulnerable to eavesdropping and outside manipulation, made up of devices that cannot be cloned. The secure design of the HURDLE cipher has ensured the integrity and confidentiality of a growing number of safety-critical networks over the past 10 years, with consequent benefits to national security, to safety, and to the reliable operations of the systems they support.

5. Sources to corroborate the impact (indicative maximum of 10 references)

[1] Supporting statement from the former Chair of ETSI SAGE (Security Algorithms Group of Experts) and Chair of ETSI Project TETRA WG 6 (the TETRA security group), 11 October 2013. Copy available on request. [Quality and authorship of underpinning research; link to impact.]

[2] Supporting statement from the President of the International Association of Cryptologic Research, 11 May 2013. Copy available on request. [Quality of underpinning research.]

[3] Supporting statement from the Chief Executive of the TETRA+ Critical Communications Association, October 2013. Copy available on request. [Authorship of research; link between research and impact; reach and significance of impact]

[4] ETSI EN 300 392-7 V2.1.1 (2001-02), Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security, European Telecommunications Standards Institute, 2001. http://www.etsi.org. Copy available on request. [Link between research and impact]

[5] TETRA Industry Group fact sheet "TETRA Around the World" (copy available on request) and http://www.tetrahealth.info/worldlintro.htm Retrieved 9 October 2013. [Reach of impact.]

[6] TETRA Industry Group, FAQs – Who uses TETRA and Why? http://www.tetrahealth.info/pages/FAQs_WhoUses.html Retrieved 9 October 2013. [Reach and significance of impact.]

[7] The TETRA Pocket Guide. http://pocketguide.tetra-association.com/english/ Retrieved May 2012. [Reach and significance of impact.]