Cryptography in a Hitchhiker's Universe

Alexander W. Dent

Information Security Group, Royal Holloway, University of London
Egham Hill, Egham, Surrey, TW20 0EX, UK
a.dent@rhul.ac.uk

1 Introduction

The cryptographic universe is an uncertain place. Concrete security guarantees are currently beyond our ability to produce as we are unable to solve the fundamental problem of determining whether P=NP, and the related questions of whether one-way functions and permutations exist. An interesting characterisation of these possible different universes is given by Impagliazzo [2]. Most cryptographic analysis is conducted assuming we exist in a cryptomania world, but Pietrzak [3] has demonstrated the value of considering the limits of cryptography in other universes.

This article considers the limits of cryptography in three separate universes, whose existence is conjectured by Adams [1]. Since we cannot currently mathematically prove that we are not within these universe paradigms, this research has value.

2 Cryptography in a Finitely Improbable Universe

We begin by considering a universe in which finite amounts of improbability can be generated. It is well known that the generation of finite amounts of improbability would lead to some stupendous and intensely biological parties; what is less well-known is that would virtually wipe out war among planets that could afford to buy improbability generators. In the pre-improbability-generator days, countries would send encrypted messages to each other safe in the knowledge that no-one else could read them. These messages were frequently irreverent, saying things like "I think Belgium smells" and "The President of the United States is a poo-poo head".

Of course, the countries who couldn't read them would automatically assume that they were being talked about, and, despite frequent denials, that not-nice things were being said. The situation was compounded by the fact that it would often take centuries for these countries to decrypt their (by now) enemy's messages and find out that they weren't saying nasty things about their Aunty Mabel after all.

However, it doesn't take much imagination to see that, while it is fairly improbable that a computer would instantly decrypt a ciphertext, it is still a finite possibility. Indeed, it isn't even that unlikely when you compared it to, say, the success of "Achy-Breaky Heart". In this way it is easy to see that one can use a finite improbability generator to instantly read any message sent to anyone anywhere.

Undoubtedly, such a discovery would prompt a short period of intense violence, which would only stop when one country has the good sense to admit that they never liked Aunty Mabel that much anyway. After this, a planet would either stop writing things down[1] or become so incredibly relaxed about things that they wouldn't care what *anyone* said about Aunty Mabel.

It is also easy to see that a finite improbability generator cannot produce a code that cannot be broken by another improbability generator. To do so would require the first generator to produce something that was so improbable that not even all the other improbability generators in the world could ever produce such levels of improbability, even when working together. And no-one seems to be able to get the tea hot enough to do this.

[1] Such as the Galgazats of Christmas III, who haven't written anything down for over three hundred millennia. This has led to the creation of restaurants with very short, very memorable menus, and the complete obliteration of all lawyers. This is not considered a bad trade.

3 Cryptography in an Infinitely Improbably Universe

The existence of a machine capable of generating infinite improbability would provide an interesting challenge to cryptography. On one hand, it would allow for the creation of an encryption scheme which would resist attacks made by devices which can generate finite amounts of improbability. This would again allow governments to communicate securely and allow bureaucratic officials to again comment on the personal hygiene of Aunty Mabel with impunity. Hence, the existence of an infinite improbability generator is likely to increase tensions between nations once more.

On the other hand, cryptanalysis is also more interesting when one considers the existence of a device capable of generating infinite improbability. Such a device would not only be able to decrypt the message, but also tell you what the sender meant to say, what his boss thinks he said, and what he would have said if he hadn't felt a bit ill after that curry last night[2]. Furthermore, it would present all of these revelations in easy-to-swallow capsule form.

The effects of attacking an infinitely improbable encryption scheme with an infinitely improbably cryptanalytic machine are unknown. It is conjectured that the result of attacking a $\aleph_n$ infinitely improbable scheme with an $\aleph_m$ infinitely improbably machine would be an event that is $\aleph_{n+m}$ infinitely improbable. The only known example of an $\aleph_n$ infinitely improbable event for $n > 2$ was the relationship between David Copperfield and Claudia Schiffer.

4 Cryptography in a Bistromath Universe

The last of Adams' universes to be considered is the bistromath universe. In such a universe, the laws of mathematics behave differently depending on the location in which the mathematics occurs. This implies the existence of cryptographic schemes whose security depends on the location from which the message is sent or received.

It is well known that the mathematical laws are most flexible when the mathematician is within a restaurant. This explains why most mathematicians can sit in their offices for hours struggling with a problem, only to immediately solve the problem when they step out for a coffee. Particularly difficult problems are also more likely to be solved when proofs are sketched on the back of napkins.

From a cryptographic perspective, this implies that the best way to send, receive or intercept encrypted messages is from within a restaurant. For high security applications, this should be a restaurant with plush, red velour seating and a snooty maitre d'. This also means that the best way to cryptanalyse an encryption scheme is from within a restaurant, and for optimal alignment with the mathematical techniques used in the encryption scheme, within the same restaurant as the sender or receiver. This is a somewhat controversial theory with detractors claiming that the information security experts have not so much broken the fundamental hardness of the encryption scheme as they have read the message over the shoulder of the recipient (who is typically drunk by this stage).

The bistromath theory of cryptography has been heartily embraced by some sections of the existing cryptographic community, who have put in place experimental structures to enable cryptographers to do as much research as possible in expensive restaurants[3].

[2] It is well known that all important decisions are always made after a night out when you've had a curry and a few beers. The classic example of this is marriage, in which two people have a good night out and then inexplicably agree the next day to only sleep with one person for the rest of their lives. The K'yeks of Zargon, a pitiful race of cowardly creatures, have attempt to eliminate all excitement from their lives by banning curries.

[3] EU Project Number: IST-2002-507932 (ECRYPT)

5 Coming Attractions

If you have enjoyed our feature presentation, you'll be pleased to hear about upcoming attractions by the same author:

- The cryptanalysis of Human Interactive Protocol Systems. A controversial cryptanalysis of the paper of Shakira [4] which proves that HIPS do, in fact, lie.
- Anti-zero-knowledge. A protocol system which reveals everything that a prover knows except that which the verifier wants to hear. Ad-hoc anti-zero-knowledge protocols have been developed by most customer helpline services.
- Quantum key distribution based on social phenomena. This paper demonstrates how to distribute keys using quantum techniques but without using quantum objects. Instead of using quantum objects, the protocol instead uses the uncertainty that any man has about whether his first evening out with a woman counts as a date or not to transmit the keys.

Acknowledgements

The author would like to thank the anonymous J. Crap. reviewers for their suggestions.

References

1. Douglas Adams. The Hitchhikers Guide to the Galaxy. Pan Books, 1979.
2. Russell Impagliazzo. A personal view of average-case complexity. In *Structure in Complexity Theory Conference*, pages 134147, 1995.
3. Krzysztof Pietrzak. Composition Implies Adaptive Security in Minicrypt. In *Advances in Cryptology – Eurocrypt 2006*, pages 328–338, 2006.
4. Shakira. HIPS don't lie. Epic records, 2006.