Practical Evaluation of Cryptographic Configurations for Packet TM/TC

André Adelsbach[1]**, Carlo Harpes**[1]**, Gian-Paolo Calzolari**[2]**, Stefano Zatti**[2]**, Daniel Fischer**[2]

[1] ***Telindus S.A., Security, Audit and Governance Services***
81-82, route d'Arlon, L-8009 Strassen, Luxembourg

[2] ***European Space Agency / European Space Operations Centre***
Robert-Bosch-Str. 5, 64293 Darmstadt, Germany

ABSTRACT

In recent years, the need for communication security - even in civil space missions - has been widely recognized and accepted. Therefore, the integration of cryptographic building blocks, such as encryption schemes and message authentication codes (MACs), is an active area of research within agencies and international forums like the CCSDS.

In this paper we discuss several evaluation criteria to assess the suitability of encryption and authentication schemes for use in Packet Telemetry and Telecommand protocols. Based on these evaluation criteria we define evaluation metrics, which are suitable to compare state-of-the-art cryptographic algorithms in the context of Packet Telemetry and Telecommand Protocols. Our theoretical analysis is complemented by practical evaluation, comparing the computational complexity of cryptographic algorithms.

1 INTRODUCTION

In recent years, the need for communication security - even in civil space missions - has been widely recognized and accepted. New applications, such as joy-sticking of instruments by principal investigators and new threats, such as the decreasing costs for hardware allowing cheap “rogue” ground stations to be established, are further pushing the need for secure space communication. Therefore, the integration of cryptographic building blocks, such as encryption schemes and message authentication codes (MACs), is an active area of research within agencies and international forums like the CCSDS.

Maliciously corrupted data that goes undetected often may have catastrophic impact. Obviously, corrupted telecommands may result in loss of spacecraft, but in addition corrupted telemetry or scientific data may lead operators to wrong decisions. Therefore, the need for authentication techniques is pressing, given the increasing threats. Similarly, confidentiality of telecommands and telemetry has become a critical requirement for several missions, pushing the need for encryption of packet telecommand and telemetry.

Both, agencies and the CCSDS, started an initiative to analyze suitable candidate algorithms on a theoretical basis and on assessing the different options (layers of the protocol stack) for the integration of encryption and authentication, leading to important documents, such as [1]. In addition, the research community started addressing the challenge of cryptography in packet TM/TC protocols (cf. [2], [3]) and produced first results in this context.

This paper presents preliminary results of an ongoing study performed for ESOC. The goal of this study is to perform a thorough theoretical and practical evaluation of selected cryptographic configurations (localization of security mechanisms, combinations of algorithms, key-sizes etc.) in the context of packet TM/TC protocols. In this paper the focus will be mainly on the evaluation metrics and the results of a first preliminary evaluation of cryptographic algorithms for packet TM/TC.

1.1 Contribution

The main contribution presented in this paper is the definition of evaluation metrics for encryption and authentication schemes in the context of packet TM/TC protocols and preliminary results on our evaluation of cryptographic algorithms based on the defined metrics. In addition our work complements the aforementioned analyses regarding two crucial aspects:

1. **New Cryptographic Algorithms -** The assessments we encountered in previous work mostly address the traditional, well-known encryption schemes (e.g. AES-CBC or AES-OFB) and message authentication codes such (e.g. CBC-MAC or CFB-MAC). However, especially in recent years we have been able to witness a tremendous development of new cryptographic algorithms, including advanced modes of operation for authenticated encryption and offering provable security. Further important developments are efficient, provably secure message authentication codes. We present an overview over recent developments in the area of cryptography and point out interesting relevant cryptographic research. In our future evaluation we explicitly include recently proposed algorithms, such as modes of operation for authenticated encryption.
2. **Practical Evaluation -** Previous work mostly focused on the theoretical evaluation of cryptographic algorithms. Another distinguishing feature of our evaluation is the practical evaluation, e.g. of the computational complexities of cryptographic algorithms, which is a crucial aspect in limited computational environments of spacecrafts.

1.2 Approach and Outline

The overall approach taken by the project is as follows:

1. We review several evaluation criteria, such as computational overhead, communication overhead, error propagation/expansion and synchronization that determine the performance and suitability of cryptographic algorithms in the context of packet TM/TC protocols. By prioritization/weighting these criteria based on the characteristics of the communication links, payload characteristics, etc we define three evaluation metrics: Telemetry Encryption Metric, Telecommand Authentication Metric and Telecommand Encryption Metric.
2. Based on the defined metrics, we analyze cryptographic configurations, including recently proposed algorithms and assess their suitability for packet TM/TC protocols.

In addition to theoretical analysis our evaluation covers practical measurements of computational complexity. This is an important feature of our evaluation, because it proves the practicability of strong cryptography in the context of packet TM/TC protocols.

In Section 2 we discuss the evaluation criteria for cryptographic algorithm and propose evaluation metrics for TM encryption, TC Authentication and TC Encryption by proposing suitable weightings of the evaluation criteria. In Section 3 we present a short review of recent cryptographic algorithms and in 4 we present preliminary evaluation results of the ongoing ESOC study “Consultancy on Cryptographic Design”. In Section 5 we review related work and we conclude in Section 6.

2 EVALUATION CRITERIA

We consider the following criteria to be of medium to high importance when applied in the context of packet TM/TC protocols. In the following we do not consider those criteria in detail that have been rated as “low important” in the context of space communications, such as parallelizability, support of variable key sizes, stateful vs. not stateful and key agility.

2.1.1 General Criteria

Below we discuss general evaluation criteria. Here, by “general” we refer to criteria, applicable to any cryptographic building block, no matter whether encryption scheme or authentication scheme.

- **Intellectual Property Rights (IPR):** When considering a cryptographic algorithm for a certain application, it is important to have a clear view on the intellectual property rights associated with the algorithm, i.e., whether it is covered by a patent and, if covered by a patent, what the license conditions are.
- **Performance in implementations:** This criterion addresses the question, whether the cryptographic algorithm can be efficiently implemented on a wide range of platforms (H/W and S/W). This mainly concerns the
    - **computational complexity**, i.e., the complexity and number of operations (XOR, addition, multiplication, shifts, etc) being used by the cryptographic algorithms.

  - **memory complexity**, i.e., the memory required by the algorithm during its operation.

  For application in space environments, the performance is a crucial criterion, because the cost of space approved processors and memory is significantly higher than COTS hardware.

- **Security:** This criterion addresses the question whether security properties of the cryptographic algorithm have been proven rigorously based on meaningful definitions, mathematical abstractions and cryptographic assumptions. If possible, provably secure algorithms should be preferred over algorithms, whose security has not been proven.. Security proofs of cryptographic algorithms should be based on well-analyzed cryptographic assumptions - the weaker the underlying cryptographic assumptions underlying the security proof, the better.
  If an algorithm has not been proven secure, one should make sure that it has been thoroughly peer-reviewed by the cryptographic research community (see "availability of specifications" below) and that the best known attacks are still far from being feasible and do not indicate a serious conceptual weakness of the algorithm.
  Finally, supported security parameters such as the key-length have to be in line with the long lifetime of space communication standards and of space missions in order to guarantee security of the cryptographic algorithm over its whole lifetime.

- **Availability of specifications:** Availability of the algorithm's specification is important, because it guarantees that the algorithm can be reviewed, both by the implementer and the cryptographic community. A cryptographic algorithm should be published and undergone thorough peer-review in the research community such that design flaws and security issues can be identified.

- **Standardization:** Open standardization of cryptographic algorithms guarantees that the algorithm has been specified rigorously and peer-reviewed by the standardization body. Furthermore, compliance to standards fosters availability and interoperability of COTS components, reduces the price of components and improves reliability of implementations.

- **Size of inner state:** This criterion addresses the size of the inner state that has to be generated and maintained by a cryptographic algorithm. This criterion is of importance, because shielded memory is a significant cost factor in spacecrafts.

- **Online vs. offline:** Offline schemes require the size of the message (or the complete message itself) to be known before they can start, whereas online schemes do not require the size of the message (or the complete message itself) to be known a-priori. Online schemes can process data on-the-fly without knowing when it will stop.
  Importance of this criterion depends also on the localization of the encryption/authentication scheme within the packet TM/TC protocol stack, because PDUs such as space packets have variable sizes, while the size of transfer frames is fixed, i.e., always known a-priori.

- **Key Agility:** Key agility refers to the efficiency of context switches in case the same algorithm (engine) is applied in parallel to different message streams, using different keys or if re-keying is required in short intervals. This criterion is related to the size of inner state of a cryptographic algorithm.

2.1.2 Criteria for Encryption Schemes

While the criteria discussed in the previous section are applicable to several classes of cryptographic algorithms (e.g. encryption algorithms, MAC algorithms, digital signature schemes), the following criteria are mainly applicable to evaluate encryption schemes.

- **Symmetric vs. Asymmetric:** Asymmetric encryption schemes come with a significantly higher computational complexity, but allow for easier key distribution. However, in the context of space applications we consider the drawback of a high computational complexity to outweigh the gain due to easier key distribution.

- **Stream Cipher vs. Block Cipher:** Can the encryption scheme operate on variable length bit strings or on fixed length strings (one block) only. As protocol data units are usually bigger than usual block sizes (64, 128 bit) of block ciphers, the use of stream ciphers is mandatory. Note, however, that stream ciphers can be constructed by using block ciphers in dedicated modes of operation (see Section 3).

- **Synchronous vs. Self-Synchronization:** This distinction mainly applies to stream ciphers. Decryption of synchronous stream ciphers does not depend on the ciphertext prefix received before. If a bit of the ciphertext stream is lost or added during transmission, sender and receiver are out of synchronization, resulting in wrong decryption. Self-synchronization refers to the ability of an encryption scheme (mainly stream ciphers) to recover from such errors in the ciphertext stream, which may be induced by the communication channel.

- **Error propagation / error expansion:** This criterion refers to the number of decrypted bits affected by an error in the ciphertext. If error-correction coding is applied before encryption, a high error-expansion rate strongly impacts the error-correction capabilities, since decryption expands a single error on the communication to several errors in the decrypted bit-stream. As in most encryption localizations options that are under closer consideration apply error-correction coding after encryption, the weighting of error propagation / error expansion is rather low.
- **Block padding:** Does encryption require input messages of a certain size (e.g., multiple of the block cipher's block size) or is it possible to operate on messages of arbitrary length. If the encryption algorithm requires messages of a certain size, encryption of messages may require padding of the message, which implies a message expansion and additional overhead on the communication link. Especially for short messages, such as TC messages, block padding may induce a significant communication overhead. Therefore, we consider this criterion to be of high importance for TC encryption, while for TM encryption we consider it to be of medium importance, since usual TM PDUs are longer than TC PDUs. (cf. Table 1)
- **Message expansion:** Does the encryption scheme require additional information to be attached to the ciphertext (such as IVs?). This criterion impacts the overhead introduced by the encryption.
- **Random access:** Is it possible to decrypt any position of the ciphertext, without decrypting the whole prefix of the ciphertext?
- **Authenticated Encryption:** Does the encryption scheme provide secure authentication in addition to confidentiality? See Section 3 for more details.

2.1.3 Criteria for Authentication Schemes

Below we summarize evaluation criteria that are specific to authentication schemes:

- **Symmetric vs. Asymmetric:** It is important to distinguish symmetric authentication schemes (message authentication codes) from asymmetric ones (signature schemes). The advantage of digital signature schemes is that key-management is easier and that these schemes offer non-repudiation, which means that the receiver of an authenticated message can prove that a specific message has been authenticated (signed) by a certain party. In symmetric authentication schemes this cannot be achieved, because sender and receiver share the same key, i.e., the receiver may have authenticated the message himself. However, again the asymmetric algorithms suffer from significant computation overhead. [1]
- **Size of authenticator:** The size of the authenticator (MAC or digital signature) is important to judge the communication overhead induced by the authentication scheme. This is an important evaluation criterion – especially for short messages – because it may induce a significant overhead on the communication link.

2.2 Evaluation Metrics

After a first analysis of packet TM/TC protocols we propose a weighting of the evaluation criteria as summarized in the Table 1 and Table 2 below. The weighting scale ranges from 1 to 10, where 1 is the lowest weight and 10 is the highest weight.

Table 1 Preliminary weighting of properties for encryption schemes in packet TM/TC protocols

Criterion	TM Encryption	TC Encryption
Security	10	10
Computational Complexity	9	7
Memory Complexity	7	7
Size of inner state	5	5
Key Agility	2	2
IPR	4	4

[1] As an example a RSA signature for a 2048 byte message using a 1024 bit key requires 2462.19 microseconds, whereas computation of a SHA-1 HMAC authentication code requires only 4.2 microseconds. (see Section 4.2 for details about the benchmarking platform)

Publicly specified	9	9
Standardized	8	8
Offline	2	2
Asymmetry - easier key distribution	4	4
Asymmetry – higher computational complexity	9	7
Error propagation / error expansion	3	3
Block padding	6	8
Message Expansion	8	8
Random Access	4	4
Authenticated Encryption	6	8

Table 2 Preliminary weighting of properties for authentication schemes in packet TC protocols

Criterion	TC Encryption
Security	10
Computational Complexity	7
Memory Complexity	7
Size of inner state	5
Key Agility	2
IPR	4
Publicly specified	9
Standardized	8
Offline	2
Asymmetry - easier key distribution	4
Asymmetry – higher computational complexity	7
Asymmetry – non-repudiation	2
Size of authenticator	9

3 STATE OF THE ART CRYPTOGRAPHIC ALGORITHMS

Our evaluation includes the classical modes of operation for encryption ECB, CBC, CFB, OFB and CTR as specified in [9].

For authentication we identified the following interesting candidate algorithms that we will analyze in future work in more detail: CMAC, UMAC, HMAC, TTMAC (Two-Track MAC), EMAC. In order to get an indication of the practicability of digital signature schemes for authentication of packet TM/TC communication, we consider elliptic curve algorithms like EC-DSA.

For usage in packet telecommand communication, where risk analyses indicate a need for both confidentiality and authentication we will in addition consider modes of operation for authenticated encryption, such as CCM (Counter with CBC-MAC), EAX, GCM (Galois Counter Mode), OCB (Offset Codebook), and CWC (Carter-Wegman and Counter Mode).

An authenticated encryption scheme (AE) is a cryptographic mechanism that transforms a message *m* into a ciphertext *c* in order to protect its privacy *and* authenticity. Authenticated encryption can be achieved by *“**generic composition**”* of an encryption scheme and an authentication scheme: first the message is encrypted using the encryption scheme and a symmetric encryption key and afterwards the ciphertext is authenticated using the authentication scheme and a symmetric authentication key.[2]

4 EVALUATION

The following sub-sections give a summary of first preliminary results achieved in the so far.

[2] Here, it is important to note that for generic composition the encryption key and the authentication key have to be different.

4.1 Theoretical evaluation

Considering classical encryption modes of operation, our first results indicate that CTR mode of operation has substantial advantages: high efficiency, error expansion supports messages of arbitrary length (no block padding required) and provides provable security on the weak assumption that the underlying block cipher is a pseudo-random permutation.

First reviews of relevant publications indicate that message authentication codes based on block ciphers are more suitable for short messages than those based on hashing, because block lengths of block ciphers are shorter than sizes of hash function outputs.[3] Future work will analyze this in more detail.

Regarding authenticated encryption one distinguishes ***one-pass*** and ***two-pass*** authenticated encryption schemes [9]: one-pass schemes only require a single pass over the data to achieve both privacy and authenticity, whereas two-pass schemes require two passes over the data – one to achieve privacy and the second to achieve authenticity.

Efficiency of two-pass AE schemes is only slightly better than that of generically composed encryption and authentication schemes [9]. The speed-up is mainly due to the use of one key instead of two separate keys, which also reduces the number of keys that have to be exchanged and managed. Typically, the computation complexity of one-pass schemes is approximately half the complexity of two-pass schemes.

However, since one-pass AE schemes are subject to pending patents, standardization bodies like *“802.11 WG i”* or NIST have preferred two-pass schemes like CCM or EAX over one-pass schemes like OCB. In the context of space communication, the advantages of one-pass schemes in terms of computation complexity may outweigh the costs to license a one-pass algorithm. This has to be evaluated in more detail.

4.2 Practical evaluation results

The computational benchmarking of encryption schemes has been implemented based on the Crypto++ Library. Benchmarking has been performed for fixed, randomly generated keys and fixed, randomly generated plaintexts. The benchmarking results have been measured on a Pentium IV 3.2 GHz PC, running Windows XP Professional. In order to obtain stable benchmarking results, encryptions have been repeated 1000 times and the average time required for encryption has been used for benchmarking purposes.

Our evaluation results justify a clear preference for AES-based encryption schemes, because their computational overheads are even lower than those of the DES-based. Double- and Triple-DES based encryption schemes come with a significantly higher computational overhead.

Furthermore, the benchmarking results show that the computational complexity of AES-256 based encryption schemes is only 23 – 30 % higher than that of AES-128 based encryption scheme. We conclude that AES-256 based encryption schemes are an option for missions with very high security requirements and that the resulting overhead is moderate.

5 RELATED WORK

In [11], an analysis on localization options for encryption and authentication in Packet Telemetry and Telecommand is presented, which complements the results presented in this paper.

At the time of writing the CCSDS book “Recommendation for Encryption Algorithms” was in draft status. Based on the previous “Encryption Algorithm Trade Study”, the draft book proposes a standard symmetric block-cipher encryption for civilian space missions. The hope of using standard algorithms is to support the selection of strong cryptographic

[3] https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf

algorithms, improve interoperability and to foster potential rewards of economies of scale by allowing use of standard "off-the-shelf" products.

The document version (January 2006), current at the time of writing, considers AES [5] in CTR mode mandatory, whereas other NIST modes may be optionally employed. The rationale for the choice of AES is that it is publicly specified and is available without licensing or patent restrictions. Furthermore, it went through a thorough public evaluation process by the cryptographic research community and can be implemented efficiently in both software and hardware. In addition it supports different key sizes (128-, 192-, 256-bits). The rationale for CTR mode is its efficiency and the fact that no padding of the plaintext is required. Therefore, CTR is considered suitable for links with limited bandwidth and encryption of short plaintexts.

The CCSDS draft book "Recommendation for Authentication Algorithms" (January 2006) is based on a prior trade study "Authentication/Integrity Algorithm Issues" (August 2005) that reviews existing MAC and digital signature algorithms.

As a minimum base-line the CCSDS draft book requires implementation of the HMAC message authentication code [6] as the minimum compatible baseline among CCSDS missions. HMAC-96, i.e. truncation of HMAC to 96 bits, is not mandatory for CCSDS compliance, but may be used to reduce the communication overhead. The draft book does not encourage the use of SHA-1 for HMAC due to recent attacks reported in [12]. However, we want to stress that recent security proofs show that usage of SHA-1 is not affected by the attacks reported in [7].

If digital signatures are being used by a mission, the Digital Signature Algorithm (DSA) must be supported [8]. In addition, other digital signature schemes, specified in the Digital Signature Standard (DSS), such as RSA Digital Signature or ECDSA (Elliptic Curve Digital Signature Algorithm), may be used.

Spinsante, Chiaraluce and Gambi [3] address the quantitative performance evaluation of AES-based encryption and authentication when applied to TM and TC data structures. More concretely, the authors discuss the "impact of residual errors, introduced by the channel and not compensated by the coding layer of the TC or TM architectures." Towards this end, the authors investigate the interactions between encryption and authentication on the one side and FEC (Forward Error Correction) as defined in the Packet TM and TC protocols on the other side.

For telecommand authentication the authors evaluate CBC-MAC based on AES and CFB-MAC based on AES. The paper analyses the MAC's susceptibility/robustness to random errors. We do not consider this to be a suitable criterion to evaluate authentication algorithms: a single bit-error should cause verification of any reasonable MAC to fail – in fact it is the security requirement of a good MAC that its validation will fail as soon as one bit of the message or MAC flipped.
In any case error correction should be applied before verification of the message authentication codes. Therefore, there will be no interference between message authentication and error correction.

In addition the authors evaluate TM encryption. More concretely, the authors focus on AES in OFB and CFB modes of operation and analyze the effects of residual errors on these encryption modes of operation. OFB mode of operation is known to be well-suited for encryption of noisy channels, because a single bit-error in the ciphertext results only in a single bit-error in the decrypted plaintext, i.e. OFB mode of operation does not suffer from error-propagation. CFB is a self-synchronizing stream cipher, but it suffers from error propagation and synchronization takes longer (approximately n/r blocks, where n is the block size of the block cipher and r is the size of the shift-register of the CFB design. The simulation results presented in the paper favor the adoption of OFB mode for Telemetry encryption.

Fischer, Engel and Merri [4] mainly discuss the localization of encryption and authentication in the TM/TC protocol family. Besides this discussion the paper presents a short discussion on cryptographic algorithms suitable for TM/TC encryption and authentication.

The paper focuses on symmetric cryptography, because they argue that the advantage of asymmetric cryptography (key management) is not so strong in the case of space missions, since symmetric keys can be set up before launch. In general we agree with this assessment, but asymmetric cryptography may, nevertheless, be useful to allow for end-to-end security, dynamic groups of users, in order to achieve non-repudiation or in scenarios where several parties are involved in the operation of a satellite.

Fischer et al. consider the use of CTR mode of operation favorable, because it is parallelizable, requires no padding and the IV (nonce) used in CTR mode is smaller (half the block size) than IVs in other modes of operation. For authentication the authors consider the use of OCB or EAX mode for authenticated encryption.

Our preliminary evaluation results indicate a preference for OCB, because it is a one-pass scheme and, as such, more efficient than EAX.

6 CONCLUSION AND FUTURE WORK

Based on our preliminary evaluation, we consider CTR mode of operation with an AES-128 block cipher to be a reasonable candidate for packet TM/TC encryption. Its main advantages are its efficiency and the fact that the CTR mode has no error expansion, supports messages of arbitrary length (no block padding required) and provides provable security based on the weak assumption that the underlying block cipher is a pseudo-random permutation.

Furthermore, the benchmarking results show that the computational complexity of AES-256 based encryption schemes is 23 – 30 % higher than that of AES-128 based encryption scheme. We conclude that AES-256 based encryption schemes are an option for missions with very high security requirements and that the resulting overhead is moderate.

Future work will address a more detailed analysis of the discussed cryptographic algorithms based on the presented evaluation metric.

7 REFERENCES

[1] CCSDS, “The application of CCSDS Protocols to Secure Systems”, CCSDS 350.0-G-2, Green Book, January 2006

[2] S. Spinsante, F. Chiaraluce and E. Gambi, “Evaluation of AES-based authentication and encryption schemes for Telecommand and Telemetry in satellite applications”, SpaceOps 2006, AIAA-2006-5558, SpaceOps 2006 Conference, 2006

[3] F. Chiaraluce, E. Gambi and S. Spinsante , “Numerical Verification of the Historicity of the ESA Telecommand Authentication Approach”, SpaceOps 2006, AIAA-2006-5580, SpaceOps 2006 Conference, 2006

[4] D. Fischer, T. Engel, M. Merri, “Approach to the integration of data security into the packet TM/TC standards;SpaceOps 2006 Conference, AIAA 2006-5804

[5] National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES), Federal Information Processing Standards Publication (FIPS PUB) 197, November 2001

[6] National Institute of Standards and Technology (NIST).The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication (FIPS PUB) 198, March 2002

[7] Mihir Bellare. New Proofs of NMAC and HMAC: Security without Collision-Resistance. Advances in Cryptology – Crypto 2006, LNCS 4117, Springer-Verlag, 2006. Full version available at http://www-cse.ucsd.edu/users/mihir.

[8] National Institute of Standards and Technology (NIST). The Digital Signature Standard (DSS), Federal Information Processing Standards Publication (FIPS PUB) 186/186-2, May 1994/January 2000

[9] National Institute of Standards and Technology (NIST). Recommendations for Block Cipher Modes of Operation, NIST Special Publication 800-38A, 2001

[10] Mihir Bellare, Phillip Rogaway, and David Wagner. The EAX Mode of Operation – A Two-Pass Authenticated Encryption Scheme Optimized for Simplicity and Efficiency. In Fast Software Encryption (FSE) 2004, full version available at http://www.cs.ucdavis.edu/~rogaway/papers/eax.html

[11] Daniel Fischer, Mario Merri and Thomas Engel. Introducing a generic security extension for the packet TM/TC protocol stack, 4th ESA International Workshop on Tracking, Telemetry and Command Systems for Space Applications, 2007

[12] X. Wang, D. Feng, X. Lai, and H Yu. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. Report 2004/199, Cryptology ePrint Archive, 2004.