Jornada Matemática SPM/CIM em Teoria da Codificação, Informação e Criptografia

por Pedro Patrício

18 de Novembro de 2009

Decorreu, no dia 14 de Novembro de 2009, a Jornada Matemática SPM/CIM em Teoria da Codificação, Informação e Criptografia. Este eventou realizou-se no Hotel Quinta das Lágrimas, em Coimbra. A organização esteve a cargo de Pedro Patrício, do Departamento de Matemática da Universidade do Minho Estiveram presentes duas dezenas participantes.

Por razões de força maior, o Doutor Rogério Reis não pôde estar presente. Como tal, o programa científico sofreu alterações de última hora.

14:25 Sessão de boas vindas;

14:30 *O totobola e os códigos correctores de erros*, por António Machiavelo, Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto
Resumo: O problema de determinar o número mínimo de apostas num totobola (um jogo em vias de extinção...) com n jogos, de modo a garantir n-1 resultados correctos é um problema em aberto com fortes ligações aos códigos correctores de erros. Pretendemos dar um resumo do que se sabe e do que se desconhece sobre este problema, assim como falar de possíveis generalizações a outros jogos.

15:15 *Códigos convolucionais: um olhar através da teoria dos sistemas*, por Raquel Pinto, Departamento de Matemática da Universidade de Aveiro
Resumo: Os códigos de correcção de dados são um elemento chave na transmissão e armazenamento eficiente de informação. Em 1948, Claude Shannon mostrou, no seu célebre artigo The Mathematical Theory of Communication, que a introdução de redundância numa mensagem de forma apropriada (codificação) torna possível a detecção e correcção de erros originados na transmissão ou armazenamento desta (descodificação). Os códigos lineares (a blocos ou convolucionais) são os mais utilizados, já que possuem propriedades relevantes para uma implementação robusta. Nesta palestra vamo-nos centrar nos códigos convolucionais. Estes códigos foram introduzidos por Peter Elias em 1955. Em 1960, Massey and Sain relacionaram a teoria dos códigos convolucionais com a teoria dos sistemas, descrevendo um codificador convolucional como uma função de transferência de um sistema linear, invariante no tempo. Nesta palestra iremos analisar esta abordagem, a qual tem desempenhado um papel importante na investigação de códigos convolucionais.

16:00 *Segurança do RSA*, por Paulo Almeida, Departamento de Matemática da Universidade de Aveiro

Resumo: No sistema criptográfico RSA há uma chave pública em que uma das componentes é o produto de dois primos grandes (que não são publicados). Este sistema é seguro porque é considerado muito difícil factorizar um número enorme. Iremos descrever métodos de factorizaçãoo que surgiram após a invenção do RSA, e outros ataques a este sistema que ameaçam a sua segurança quando este é implementado de uma forma descuidada.

16:45 Pausa para Café

17:10 *Cryptographic security of individual instances*, por Luís Antunes, Departamento de Ciência de Computadores da Faculdade de Ciências da Universidade do Porto

Resumo: For symmetric cipher systems one can prove unconditional security against an opponent with unlimited computational power. The proof is based on the notion of entropy. However, this measure does not provide a satisfactory framework to the analysis of public key cryptosystems, always based on cryptographic assumptions. The problem is that Shannon's definition of information is a purely statistical notion, which ignores the computational difficulty of extracting the information. The public key and the cipher text together contain all the Shannon information concerning the plaintext, but the information is computationally inaccessible. So, we face this intriguing question: what is accessible information? In this talk we present a first attempt to answer this question based on algorithmic entropy also known as Kolmogorov complexity.

17:55 *Complete non-malleability from strong chosen-ciphertext security*, por Manuel Barbosa, Departamento de Informática da Universidade do Minho

Resumo: In this talk we establish a connection between two strong variants of standard security notions for public-key encryption schemes: indistinguishability under strong chosen-ciphertext attacks and complete non-malleability. Strong chosen-ciphertext attacks model adversaries who can maliciously replace public keys of users and subsequently ask for decryptions under unknown secret keys. We give the first precise definition of a strong decryption oracle, pointing out the subtleties in alternative approaches that can be taken. In particular, we specify how to deal with invalid ciphertext and/or public keys and the inherent ambiguity in the message that the oracle should return. We extend indistinguishability of ciphertexts, comparison-based non-malleability and simulation non-malleability under various attack models to allow strong decryption queries. We show that the known relations for the standard versions of these definitions naturally extend to their stronger versions. We examine the relation between our new definitions of non-malleability and the notion of complete non-malleability introduced by Fischlin (ICALP 05) and by Ventre and Visconti (PKC 2008). We conclude that they can be seen as alternative formulations of complete non-malleability. Furthermore, our discussion reveals that two different decryption oracle definitions co- exist in the original formulations, which makes them hard to relate to standard notions of security for encryption schemes. Finally, our characterisation of non-malleability via indistinguishability al-

lows us to construct a practical scheme which is secure against strong chosen-ciphertext attacks in the standard model, and therefore completely non-malleable. We also discuss the apparent contradiction between the existence of our construction and Fischlin's impossibility results for completely non-malleable schemes.

18:40 Considerações finais e encerramento do evento.

É de salientar uma participação activa do público que colocou questões e proferiu vários comentários às palestras realizadas.

O organizador não pode deixar de agradecer, mais uma vez, à SPM e ao CIM pelo convite para organizar um evento desta índole, onde se tentou aproximar investigadores que estudam teoria de informação de várias prespectivas.