What Does it Mean that PRIMES is in P?

Popularization and Distortion Revisited

Boaz Miller

Published in *Social Studies of Science* 39(2): 257–288.

ABSTRACT In August 2002, three Indian computer scientists published a paper entitled 'PRIMES is in P' online. It presents a 'deterministic algorithm' which determines in 'polynomial time' if a given number is a prime number. The story was quickly picked up by the general press, and by this means spread through the scientific community of complexity theorists, where it was hailed as a major theoretical breakthrough. This is despite scientists regarding the media reports as vulgar popularizations. When the paper was published in a peer-reviewed journal only 2 years later, the three scientists had already received wide recognition for their accomplishment. Current sociological theory challenges the ability to clearly distinguish on independent epistemic grounds between distorted and non-distorted scientific knowledge. It views the demarcation lines between such forms of presentation as contextual and unstable. In my paper,
I challenge this view. By systematically surveying the popular press coverage of the 'PRIMES is in P' affair, I argue – against the prevailing new orthodoxy – that distorted simplifications of scientific knowledge are distinguishable from non-distorted simplifications on independent epistemic grounds. I argue that in the 'PRIMES is in P' affair, the three scientists could ride on the wave of the general press-distorted coverage of their algorithm, while counting on their colleagues' ability to distinguish genuine accounts from distorted ones. Thus, their scientific reputation was unharmed. This suggests that the possibility of the existence of independent epistemic standards must be incorporated into the new SSK model of popularization.

Keywords computer science, distortion, mathematical proof, popularization, science and media, social epistemology

In August 2002, three Indian computer scientists, Professor Manindra Agrawal and his two students Neeraj Kayal and Nitin Saxena, from the Indian Institute of Technology Kanpur (IIT) published a paper entitled 'PRIMES is in P' online. It presented a 'deterministic algorithm' which determines in 'polynomial time' if a given number is a prime number (the AKS algorithm). The story was quickly picked up by *The New York Times* (*NYT*) and the rest of the general press, and by this means it spread through the relevant scientific communities of complexity theorists and number theorists, where it was hailed as a major theoretical breakthrough.

By the time the paper was published in a peer-reviewed journal, 2 years after its initial publication on the Internet, Agrawal and his students had already received wide recognition for their accomplishment.

The general media usually show little interest in theoretical developments in computer science or mathematics, important as they may be, but in this case, the general media devoted a surprising amount of attention to the story. However, the media's interpretation of the meaning and implications of the new algorithm was very different from that of specialists in the relevant fields, who regarded the media's interpretation as distorted.

How come a theoretical development in computer science received this much attention from the general press? In what ways was the interpretation by the press of the AKS algorithm different from that of the scientists? Did the Indian scientists have an interest in this press coverage? Can we determine which one of the interpretations of the AKS algorithm is the 'correct' interpretation? Why is it that the three scientists' choice to publish their result on the Internet and in a popularized manner in the general press rather than a peerreviewed journal did not damage their scientific reputation among their peers?

Current sociological theory challenges the ability to clearly distinguish on independent epistemic grounds between genuine and simplified scientific knowledge, as well as between faithful simplifications and distortions. It views the demarcation lines between such forms of presentation as largely contextual and unstable. In this paper, I challenge the epistemological assumptions that underpin and enable the current model of popularization. I give a systematic survey and analysis of the popular press coverage of the 'PRIMES is in P' affair in the English language. I argue that when dealing with popularization, it is not necessarily true that distorted accounts of knowledge cannot be distinguished from faithful simplifications on independent and recognizable epistemic grounds. Additionally, the demarcation lines between distorted and non-distorted representations of scientific knowledge are not as open to political manipulation as the new sociological view of popularization suggests.

The existence of such independent epistemic grounds will explain, in turn, the ability of Agrawal and his students to simultaneously communicate distorted and non-distorted accounts of their discovery to different audiences, without damaging their scientific reputations. If independent grounds for distinguishing distorted from non-distorted accounts did not exist, it would be very likely that Agrawal and his students' choice to disseminate their results on the Internet and through the popular media would have damaged their reputations and negatively affected their careers. This is because not only did Agrawal and his students violate the social norms of the scientific community by turning to the popular media and communicating their research results directly to the public, but these media reports were also inconsistent with the consensual views among specialists. Therefore they stood in contrast to their cognitive interests. As I will show, although scientists first learned about Agrawal and his students' achievements from the media, he and his team received full recognition of their achievement from their colleagues. I will argue that this is because scientists were able to identify the ‘genuine science’ within the media’s distorted accounts.[1]

Generally speaking, my case study supports the view that while the various interests of the actors involved affect the different representations of scientific knowledge in different media, distorted simplifications of scientific knowledge are distinguishable from non-distorted simplifications on independent epistemic grounds. Furthermore, because such independent epistemic standards exist, scientists are able to communicate different contents to different target audiences in order to promote their interests.

My paper links up with other work that tries to show, with various degrees of success, that the metaphysical and epistemological assumptions underpinning SSK theories hinder them from providing adequate social explanations of science even in terms of their own standards.[2] My paper may also be considered as part of what Collins and Evans call a ‘third wave’ science study. I rely on current SSK theory of popularization to explain the events of the ‘PRIMES is in P’ affair (hereinafter ‘PRIMES’). However, similarly to Collins and Evans, who (hesitantly) claim that science is not entirely reducible to politics (2002: 245, 286 n 27), my paper calls for a reform to the current theory of popularization by acknowledging that scientific knowledge is at least partly constrained by non-political factors, and that this fact should be used as an explanatory resource in social explanations of scientific affairs.

This paper consists of five sections. The first section (Between Popularization, Simplification and Distortion) presents the current theory about popularization and challenges the view that distorted simplifications cannot be clearly distinguished from non-distorted ones. The second section (‘PRIMES is in P’ – Necessary Scientific Background) provides scientific background from the theory of computation that is necessary for understanding the meaning and significance of the AKS algorithm in its scientific context. The third section (The General Press Coverage of ‘PRIMES is in P’) systematically surveys the general press coverage of the ‘PRIMES is in P’ paper. In that section, I analyse the explicit as well as the implicit ways in which the general press gave a false impression of the implications of the AKS algorithm to lay readers. The fourth section (The Shared Interests of the Scientists and the Press in Distortion) analyses the interests that the scientists and the press had in the media coverage of PRIMES. In that section, I identify three interests – visibility, recognition and priority – which the scientists had in the general media coverage of their algorithm. The fifth section (Popularization and Distortion Revisited) addresses possible criticisms of my argument and discusses its methodological significance and generalizability to other sciences.

Between Popularization, Simplification and Distortion

Roughly speaking, two views regarding popularization of scientific knowledge may be identified in the literature: the traditional model and the new model. They differ on three main points. First, the traditional model assumes that audiences are atomistic uninformed assimilators of information, with little or no collective internal structure (Whitley, 1985: 3). Traditionally, 'science is the active disseminator and the fountain of meaning and agency, the public are merely the passive receivers and repositories' (Michael, 1996: 109).

Second, popularization is traditionally viewed as external to the knowledge production and validation process, which is left to non-scientists. Scientists' dissemination of scientific knowledge to audiences of non-scientists is viewed as a subsidiary activity that does contribute to a researcher's reputation, or may even in fact damage it (Whitley, 1985: 3).

Third, the traditional model holds an idealized notion of pure genuine scientific knowledge that it contrasts to popularized knowledge. Any differences between genuine and popularized sciences are assumed to be caused by distortion or degradation by journalists and the lay public (Hilgartner, 1990: 519). Traditional communication studies therefore search for ways to improve accuracy and balance in science reporting and to avoid sensationalism and distortion (Lewenstein, 1995: 407).[3]

The new view of popularization in the sociology of science challenges each of these three assumptions. First, the new model recognizes diversity within the public and its attitudes towards science. Sociological research shows that members of different publics construct different self-perceptions of their interest in and knowledge of science as part of their social identity. They can also critically reflect on their own epistemological standards (Michael, 1996).

In addition, the public consists of a number of readily identified audiences, some of which are important for scientific research. Some members of the public are scientists from other fields. Some belong to professional occupations, such as engineering, which claim legitimacy for their use of science. Some are university students, from which future researchers can be recruited, and some, for example policy-makers, wield power to make decisions regarding scientific research. All of these types of audience treat popularized scientific knowledge differently, and to these different types of audience scientists deliver different types of knowledge (Whitley, 1985: 5).

Second, according to the new model, popularization has an active part in the process of producing and generating knowledge. The mechanisms are twofold. First, in order to gain general support from society and lay decision-makers, scientists need to simplify scientific knowledge, popularize it and emphasize its practical value (Whitley, 1985: 19). Second, affecting the view of and gaining support from outsiders, such as decision-makers or the general public, may tip the scales in scientific controversies within a scientific community. Naturally, such external audiences learn and form their views of scientific knowledge from the popularized accounts that scientists provide to them.

How does popularization feed back into the scientific community? This is done by giving references to popularized sources in scholarly publications, thus legitimizing them as good science (Hilgartner, 1990: 523–24). Another way is through public or private communication between scientists and science journalists, where scientists learn from journalists and media reports about recent developments in their field before they appear in scholarly journals (Lewenstein, 1995: 411–24). The crucial point is that scientists form judgments and shape their beliefs and expectations about scientific factual claims based on popularized sources.

According to the new model, what underpins and enables these processes is the fact that scientific knowledge is produced in a social process of negotiations. As Whitley puts it:

> ‘Facts’ are socially constructed cognitive objects, liable to reinterpretation and change, which become established through negotiations and extensive communication among scientists. The exposition of research results to scientific audiences is a crucial component of these processes which affects what comes to constitute knowledge in that field at that time. Expository practices are not epistemologically neutral. (Whitley, 1985: 11; footnote omitted)

This picture challenges the third assumption of the traditional model about the categorical distinction between genuine and distorted scientific knowledge. The new model rejects any notion that scientific knowledge completely transcends social context. Since the distinction between genuine and distorted accounts assumes such a transcendental account, the new model rejects it too. As Lewenstein puts this:

> … a technical paper presented at a small conference is no more ‘science’ than a multimedia extravaganza presented on an IMAX screen or at Disney World’s EPCOT Center. Both are attempts to use rhetoric to present understandings of the natural world to particular audiences. (Lewenstein, 1995: 408)

According to the new model, knowledge always takes form in a particular social context. Knowledge is always tied with epistemic standards that are used to validate it. These epistemic standards are social norms, which are always situated within a particular epistemic community and its unique way of living. Different epistemic communities may offer different yet equally valid forms of knowledge (Wynne, 1996).[4]

The new model holds that epistemic standards are determined by contingent matters and relative to an epistemic community or even to an individual scientist. On Lewenstein’s view, for example, epistemic standards are in constant flux. Throughout their work, scientists happen to encounter different reports from various sources, popularized and non-popularized, and form ideas about them in an accidental fashion. In turn, these scientists produce other reports, which are consumed by other actors and so on:

> People take in lots of information, filter it in various ways and base their judgements on a range of issues running from salience and importance through time of day and state of hunger … . Theory suggests that *each reader would make a different judgement, based on completely contingent factors*. No model attempting to predict the value of different types of communications can work. (Lewenstein: 1995, 415; emphasis in the original)

As Broks (2006: 125) nicely puts it, Lewenstein conceptualizes scientific knowledge as part of a *web* in which 'press conferences, lab reports, news programmes, emails, grant proposals, policy documents and seminars are interconnected and feeding into each other'. An alternative conceptualization is a *continuum* of forms of representation of scientific knowledge, in which specialist accounts are on one extreme and non-specialist accounts are on another (Whitley, 1985: 7–8; Hilgartner, 1990: 525–28). The important point for this paper is that neither conceptualization invokes global or independent epistemic standards to determine whether a given account is a distortion or not. This is always determined locally based on contingent standards.

This line of analysis emphasizes the political dimension of knowledge. Both Hilgartner and Bucchi argue that without epistemic 'gold standards' for evaluating scientific knowledge, the process of determining what is 'genuine' science and what is not becomes *political*. A decontextualized scientific report (if one can be imagined) would neither be genuine nor distorted. Rather, based on their interests at a given time, scientists determine whether a given account with its degree of simplification is a distortion. Scientists enjoy the exclusive social authority to demarcate 'real science' from 'popularized science', and 'faithful simplifications' from mere 'distortions'. Therefore, in order to preserve this authority in accord with their political interests, scientists can label some representations of scientific knowledge as 'appropriate representations' and others as 'distorted accounts', while blaming, for example, the media for the distortion (Hilgartner, 1990: 320; Bucchi, 1996: 377–78). Generally speaking, as a political resource, scientists maintain strict boundaries between science and non-scientific forms of knowledge. Science, so they argue, is governed by superior epistemic standards of prediction and control. In their view, the superiority of scientific knowledge entitles them to social authority in the form of expertise in public matters to which scientific knowledge is relevant (Wynne, 1996).

Bucchi stresses that the distinction between appropriate scientific dissemination and distorted spectacles is a political resource available to scientists. It is used, for example, to exclude colleagues or other actors from the public arena (Bucchi, 1996: 387). Scientists who mainly communicate popularized accounts to the general public are typically ostracized by their colleagues, especially if they have not yet gained the reputation of serious scholars. This is because popularizers undermine scientists' exclusive hegemony on the construction of scientific facts (Gregory & Miller, 1998: 82–3). On the other hand, scientists themselves learn about fields outside their own from reports in the popular media and other simplified accounts. When it suits their purposes, scientists refer to such accounts in their specialized publications, thus treating them as appropriate representations (Hilgartner, 1990: 520–24). Furthermore, when it suits their purposes, they use media reports to set epistemological standards for the closure of scientific controversies. In some cases, media reports are used as a significant resource for reaching collective agreement on what experiments would
count as successful replications (Simon, 2001: 388–89).

Under the new model, then, various representations of scientific content exist in the different media. These representations may be labelled as popularizations and used to discredit certain viewpoints and individuals in a scientific community. Alternatively, they may be labelled as appropriate representations and used to legitimate certain views and claims within a scientific community. It is because popularized content by itself is indistinguishable on independent epistemic grounds from non-popularized content that scientists are able to put similar representations of scientific content to opposing uses in different circumstances.

While my case study supports the new model's view about the generative role of popularization and the active role of different types of audiences, it challenges the view that the difference between genuine knowledge, faithful simplification and distorted simplification is purely or at least largely political. As a basis for my analysis I would like to address two points with regard to the new model.

First, I would like to challenge an implicit assumption that underpins the new model, which is that scientists enjoy an exclusive epistemological authority on the definition of science in society. In my view, when scientists operate outside their field, their knowledge is subject to different epistemic standards. Scientists often do not decide what counts as science outside their own field. Law, for example, has its own standards for distinguishing scientific from non-scientific knowledge and ascertaining the reliability of scientific evidence.[5] Even when scientists' views about what science is do matter outside their field, they do not control the standards by which nonscientists evaluate scientific claims. For example, scientists do not control the media's standards for what is worthy of publication. Therefore if scientists want their research to appear in the general media – and I will show that many of them do have such an interest – they need to play along and present their research in the most attractive way for the media. Scientists are not the only actors, and perhaps not the main actors, who set standards for what is presented and gets recognition as science in the public arena.

Second, as the new model rejects the distinction between genuine and distorted knowledge, it uses terms such as 'distortion' and 'popularization' interchangeably. These words are also usually scare-quoted, to indicate their fictitious reference. While the new model does not require a conceptual analysis of these terms, my account does. I will use the term 'distortion' for accounts that mislead their readers and make them form wrong beliefs. As Adler notes, distortion has an element of wilfulness or intellectual neglect, which excludes innocent misconstrual. Distorters may take advantage of existing epistemic norms within a given epistemic community, which, when applied to a report, will probably cause it to be misconstrued (Adler: 2007: 383). I will use the term 'simplification' to denote reports that present the original account in a less detailed, less jargon-laden or generally less complex form. Note that a simplification is not necessarily a distortion. A report can omit certain details, for example, without giving its reader a wrong impression. I will use the term 'popularization' mainly to denote distorted simplifications.

I suggest that scientific and non-scientific epistemic standards are different from each other, and are relatively stable. As my example will show, scientists achieve political goals by adjusting the different accounts of knowledge they produce to these different standards, not by defining these standards and playing with them. In the section 'The General Press Coverage of 'PRIMES is in P"', I will give a detailed analysis of how the media distorted the meaning of the 'PRIMES is in P' paper. In order to do so, I will first need to give a brief technical background of the subject.

'PRIMES is in P' – Necessary Scientific Background

As I will show later, the 'PRIMES is in P' paper was susceptible to media distortion as terms that are used in it, such as 'deterministic' and 'probabilistic', have different meanings and implications in the scientific and ordinary contexts. In addition, in computational theory two distinct problems exist with regard to prime numbers, PRIMES and Integer Factorization Problem (IFP), and the media reports have tended to confuse them. In this section, I will explain the significance of the 'PRIMES is in P' paper, as understood by specialists who are familiar with this problem. This background is needed to understand my argument in later sections of this paper. Readers who are familiar with the theory of computation may skip to the conclusion of this section.[6]

Complexity Class P

In the theory of computation, problems that can be solved by computers are grouped into complexity classes according to the time it takes a computer to solve them. The time is not measured in seconds or minutes, but as a function of the length of the input; specifically, the relationship between the growth of the time function and the growth of the length of the input.

For example, two important complexity classes are *P* and *EXP*. To class *P* belong all the problems that can be solved in polynomial time by a deterministic algorithm (an explanation of what a deterministic algorithm is will be given in the next subsection). In other words, the time it takes to solve problems in the complexity class *P* is a polynomial function[7] of the length of the input.[8] In contrast, to class *EXP* belong problems that are solved by a deterministic algorithm whose time to solution is an exponential function of the length of the input.[9] The difference between these two classes is the rate growth of the functions. While polynomial functions grow relatively slowly with the growth of their input, exponential functions grow very fast. Therefore, problems that belong to complexity class *P* are regarded as problems that can be solved in reasonable time. In contrast, problems that belong to the complexity class *EXP* are considered to be problems that cannot be solved in reasonable time.

For example, let us suppose that problem *K* with an input of the length of x characters can be solved by a computer in x^2 seconds. Because the function x^2 is a polynomial, problem *K* belongs to complexity class *P*. Then, if the length of the input is 10 characters, it will take the computer 10^2 □□100 seconds – less than 2 minutes – to solve. If the length of the input is 100 characters, it will take the computer 100^2 □□10,000 seconds – about 3 hours – to solve. In contrast, let us assume that problem *L* with an input of the length of *x* characters is solvable in 2^x seconds. Because the function 2^x is exponential, problem *L* belongs to complexity class *EXP*. Then, if the length of the input is 10 characters, it will take the computer 2^{10} □□1,024 seconds – about 17 minutes – to solve it. However, if the length of the input is 100 characters, it will take the computer 2^{100} seconds – more than billions of years(!) – to solve it. It is important to notice that such problems are considered unsolvable, in principle, in reasonable time, regardless of the actual computing speed of contemporary computers. Even if we had computers that were, for example, 100 times faster than current computers, because of the fast growth of the running time function, if we slightly increased the length of the input, it would still take billions of years to solve problems that belong to complexity class *EXP*.[10]

Probabilistic and Deterministic Algorithms

Another distinction is made in the theory of computation between problems that have a deterministic algorithm for solving them and problems that are solved by probabilistic algorithms. If an algorithm is deterministic, then it means that it reaches the same and right answer every time it is run. In contrast, if an algorithm is probabilistic, its output depends on its 'tossing a coin' during its run. It does not necessarily give the same answer every time, and there is a chance that it will reach a wrong answer. This distinction has theoretical significance in the theory of computation. However, from a practical point of view, probabilistic algorithms are *as reliable* as deterministic algorithms. This is because we can run an algorithm as many times as we want to achieve as high a degree of confidence as we want. For example, let us suppose that an algorithm *A* is used to solve a problem *p, and* that if the correct answer to *p* is negative, *A* has a probability of ½ for giving an incorrect positive answer. However, if the correct answer to *p* is positive, *A* will always give the correct positive answer. If we run *A* 100 times, for instance, and get the same positive answer every time, there is a
probability of only $\frac{1}{2^{100}}$ that the answer we have is incorrect. This is an extremely low probability, lower, for example than the probability that a meteor will hit you before you finish reading this sentence.

In addition, it is important to notice that when *deterministic* algorithms are used in practice, they are not 100% accurate. This is because there is the possibility that there is a bug in the program that implements them, or a bug in the compiler that was used to compile them, or in the operating system used to run them, or in the hardware used to run the operating system, or that there will be an electrical fluctuation that will change the content of the memory of the computer, or that a cosmic ray will hit the computer and change the content of its memory, and so on. In other words, from a practical point of view, there is no difference between the reliability of deterministic algorithms and probabilistic algorithms (Sipser, 1997: 335–36). To sum up, probabilistic algorithms are as reliable for any practical use as deterministic algorithms. Probabilistic algorithms are treated differently from deterministic algorithms mainly by theorists, who are not interested in their practical use, but in their mathematical properties.

The Difference between PRIMES *and* IFP

In the theory of computation, a distinction is drawn between two distinct mathematical problems. The first problem is *PRIMES*. *PRIMES* is defined as the problem of finding whether a given number is a prime number.[11] (A prime number is a natural number that has only two natural number divisors, which are one and the prime number itself.) In contrast, *IFP* is defined as finding the *factors* of a number.[12] For example, given the number 6, the output of an algorithm which solves *PRIMES* will be ‘not prime’, because 6 is not a prime number. In contrast, given the number 6, the output of an algorithm which solves *IFP* will be ‘2 and 3’, because 2 and 3 are the factors of 6 (2·3 □□6). Of course, a solution for *IFP* entails also a solution for *PRIMES*, because if we know the factors of a number, we immediately know if it is prime or not. However, a solution for *PRIMES does not* entail a solution for *IFP* – when an algorithm that solves *PRIMES* gives us an answer we know whether or not the input number is prime, but we do not know its factors. *PRIMES* is a decision problem, namely an algorithm that solves it gives us the answer ‘yes’ or ‘no’. In contrast, *IFP* is a calculation problem, namely an algorithm that solves it gives us numbers that are the solution to a mathematical calculation problem.

Now, in the paper ‘PRIMES is in P’, Agrawal and his students describe an algorithm that is (1) deterministic and (2) solves *PRIMES* (3) in polynomial time, hence the title ‘PRIMES is in P’. Before their paper, the question of whether *PRIMES* was in *P* or not had been a long-lasting open theoretical problem, hence the wide attention they got from their peers.

It is also important to emphasize that the AKS algorithm which was presented in the ‘PRIMES is in P’ paper *solves the problem PRIMES and not the problem IFP*. In other words, it determines if a given number is prime or not, but does not find its factors. *Currently, there is no known algorithm that solves IFP in polynomial time.*

It is also important to mention that a *probabilistic* algorithm that solves *PRIMES* in polynomial time had already been introduced in 1976 by Miller and improved by Rabin in 1981, and has been widely used since. Since, as aforementioned, probabilistic algorithms are as reliable as deterministic ones, the AKS algorithm did not have any practical implication (Sipser, 1997: 339–43).[13]

The Rivest–Shamir–Adelman Encryption Algorithm

The Rivest–Shamir–Adelman (RSA) algorithm is an encryption algorithm that is widely used on the Internet, among other places. If two participants want to use RSA to exchange encrypted data, each of them must possess two types of key: a private key, which is known only to each of them alone, and a public key, which is known to everybody. If I want to exchange encrypted messages with someone, all I need to give that person is my public key. The public encryption key is like a key that can lock a box, but cannot unlock it once it is locked. Using my public key, the other person will be able to encrypt messages to me, but once the message is encrypted, only I will be able to decipher it, because I am the only one who knows my private key.

What is the connection between RSA and prime numbers? In RSA, part of my public key is a number *n*, which is the product of two large prime numbers, *p* and *q*. In order to verify that *p* and *q* are in fact prime, the probabilistic Miller–Rabin algorithm, which solves the *PRIMES* problem in polynomial time, is used. As mentioned earlier, the fact that the Miller–Rabin algorithm is probabilistic does not affect its reliability whatsoever, and therefore it does not compromise the strength of the encryption. In RSA, my private key is computable from my public key, but not in reasonable time. If somebody other than me wants to compute my private key from my public key in order to break the encryption, he must factor *n* in reasonable time. In other words, he needs to have a polynomial time algorithm for solving *IFP*. However, since currently there is no known algorithm for solving *IFP* in polynomial time, the RSA encryption algorithm is currently unbreakable in reasonable time. Since the AKS algorithm solves *PRIMES* and not *IFP*, it cannot be used to break RSA encryption (Cormen et al., 2001: 881–87).

Conclusion

To sum up this section, this is the state of affairs from the point of view of computational theorists. In the theory of computation, a distinction exists between problems that can be solved in reasonable time and those that cannot. In addition, a theoretical distinction exists between deterministic and probabilistic algorithms, but this distinction has no practical implications when algorithms are put to use. Two problems exist in the theory of computation with regard to prime numbers, *PRIMES* and *IFP*. The AKS algorithm, which was presented in the 'PRIMES is in P', is a deterministic algorithm that solves *PRIMES*, but not *IFP*, in reasonable time. There had already been at that time a probabilistic algorithm – the Miller–Rabin algorithm – that solves *PRIMES* in reasonable time. As the Miller–Rabin algorithm is reliably used for establishing RSA-based encryption systems on the Internet, the introduction of the AKS algorithm does not change the way data are encrypted on the Internet. In order to break this encryption, an algorithm that solves *IFP* in reasonable time is needed. Currently, no such algorithm exists.

The General Press Coverage of 'PRIMES is in P'

In a paper in *Notices of the American Mathematical Society*, Folkmar

TABLE 1
‘PRIMES is in P’ timetable

4 August 2002	Agrawal and his team email a draft of their paper to 15 expert mathematicians and computer scientists
7 August 2002	Agrawal and his team publish their paper on the Internet
8 August 2002	*The New York Times* publishes an article about their paper
9 August 2002–26 August 2002	Several other local and international newspapers pick up the story and publish articles about the paper
30 October 2002	Agrawal gives a talk at Clay Mathematics Institute in Cambridge, MA, and receives the Clay Research Award
31 October 2002–11 November 2002	Agrawal gives talks at MIT, Harvard University and Princeton University
4 November 2002	*The Wall Street Journal* publishes an article about Agrawal’s talks.
November 2002–March 2003	The popular press publishes a few additional articles about the paper
24 January 2003	The paper is accepted for publication by the peer-reviewed journal *Annals of Mathematics*
27 May 2003	Agrawal receives the International Centre for Theoretical Physics (ICTP) prize
September 2004	*Annals of Mathematics* publishes the paper
24 April 2006	Agrawal and his team win the Gödel Prize for their paper in *Annals of Mathematics*

Bornemann, a mathematician at the Technische Universität München, depicts the process of discovery and reception of the AKS algorithm and the basic mathematical ideas on which it is based. According to Bornemann, on Sunday 4 August 2002, Agrawal and his two students sent a pre-print version of their paper to 15 experts by email. On Monday, Carl Pomerance, a world-renowned expert in number theory, confirmed the result, and informed the reporter Sara Robinson from the *The New York Times* (*NYT*). On Tuesday, Agrawal and his students made their paper available online (Bornemann, 2003: 545). On Thursday 8 August 2002, an article by Sara Robinson was published in the Science section of the *NYT* under the title ‘New Method Said to Solve Key Problem in Math’. The first paragraph of the article says:

> Three Indian computer scientists have solved a longstanding mathematics problem by devising a way for a computer to tell *quickly and definitively* whether a number is prime – that is, whether it is evenly divisible only by itself and 1. (Robinson, 2002: A20; emphasis added)

The words ‘quickly and definitely’ are prone to two different interpretations in two different contexts. Understood in their theoretical context, ‘quickly’ means ‘belonging to complexity class *P*’ and ‘definitively’ means ‘deterministic’. However, in ordinary language, ‘quickly’ is the opposite of ‘slowly’ and ‘definite’ is the opposite of ‘indefinite’. This gives to the lay reader the false impression that, until that time, there had been no ‘quick and definite’ algorithm for checking whether a number is prime (recall that the Miller–Rabin method does just that). Then the article states:

> Prime numbers play a crucial role in cryptography, so devising fast ways to identify them is important. Current computer recipes, or algorithms, are fast, but have a small chance of giving either a wrong answer or no answer at all. The new algorithm – by Manindra Agrawal, Neeraj Kayal and Nitin Saxena of the Indian Institute of Technology in Kanpur – guarantees a correct and timely answer. (Robinson, 2002: A20)

As before, the term ‘small chance’ has also very different meaning in the theoretical context and in the ordinary language context. As opposed to the actual state of affairs, the lay reader gets the impression that until now, there has been no reliable way to identify prime numbers. On the different interpretations of the terms in the article by mathematicians and the lay public, Bornemann remarks:

> The … *New York Times* article celebrated the result as a triumph, but opaquely by choosing to simplify to a ridiculous extent: polynomial running time became ‘quickly’; deterministic became ‘definitively’. The article thus reads as follows: three Indians obtained a breakthrough because the computer could now say ‘quickly and definitively’ if a number is prime. On the other hand, the new algorithm has no immediate application, because the already existing methods are faster and do not err in practice. ‘Some breakthrough,’ readers would say to themselves. (Bornemann, 2003: 550–51)

Another way in which the *NYT* article creates a false impression to the lay reader is by the juxtaposition of the issue of cryptography next to the sentence about the fact that previous algorithms have a ‘small chance’ for error. It is true that prime numbers play a ‘crucial role in cryptography’, but the article does not state what role. The word ‘so’ implies a causal relation between cryptography and the need to identify prime numbers, neglecting the fact that there already exists an efficient and reliable way – in the ordinary sense of these words – to achieve this task. By juxtaposing these two pieces of information, and by taking into account that the lay reader will misinterpret the meaning of ‘small chance’, the article creates a false impression to the lay reader. Without saying this specifically, the article gives the idea that until now there have been some problems with cryptography algorithms – perhaps they were not reliable enough because they sometime made mistakes – and that the new algorithm is going to fix this problem.

The *NYT* article was followed by several other reports in the general media. The *NYT* article was first picked up by the Indian media. On 9 August the Indian daily English newspaper *The Hindu* published the article, only changing the title to ‘New Algorithm by Three Indians’, thus changing the emphasis to matters of national pride (Anonymous, 2002).[14] On 9 August 2002 an article was published on the Internet sites CNET and ZDNET with the title ‘Prime efforts may boost encryption’ (Junnarkar, 2002). In this article, the AKS algorithm is depicted as a possible improvement upon the popular and widely used RSA encryption algorithm, since old primality tests had a 'miniscule probability of producing a wrong answer' while the new algorithm 'is believed to generate correct results each and every time'. In fact, in this article, Agrawal is quoted as saying: 'Our algorithm is slower than the fastest-known primality testing algorithms. The satisfying part of our algorithm is that it is completely deterministic as opposed to earlier ones that may make an error – even though rarely' (Junnarkar, 2002).

In other words, what was only implied in the *NYT* article – namely, that the new AKS algorithm is important because of its possible practical use in cryptography, became explicit. Agrawal's own words, which have two very different interpretations in the theoretical versus common language context, seem to strengthen this conclusion, since the article does not mention that the fact that previous algorithms 'make an error – even though rarely' is just a theoretical characterization of these algorithms, which does not have any bearing on the practical reliability of these algorithms for encryption.

Later that year, an article in *The New York Times Magazine* reinforced this false interpretation of the AKS algorithm contributing to increased Internet security, and even to the war against terror (!):

> Encryption programs used by banks and governments rely on increasingly large primes – up to 300 digits, these days – to keep criminals and terrorists at bay. This new algorithm could guarantee primes so massive they would afford almost perfect online security. (Thompson, 2002: 107)

On 14 August 2002, an article was published on The Australian Broadcasting Corporation (ABC) Internet news site. This article also gave a wrong interpretation of the new algorithm, emphasizing its practical applicability for improving the RSA encryption algorithm, saying that existing algorithms for primality check were either inefficient or 'carry a small degree of inaccuracy'. The article explained that the new algorithm was able to determine if a given number was prime, but not to factor a number. The article concluded with the commentary of Mr Adam Spencer, 'a mathematician by training', saying: 'If someone was to develop a program that was able to factor numbers, the whole security process of data would collapse' (Kingsley, 2002).

The ABC article managed to distinguish the *PRIME* problem from the *IFP* problem, but this was not the case for all the articles about the AKS algorithm. On 19 August 2002, the Israeli daily newspaper *Haaretz,* a highquality broadsheet, published an article with the sensational title 'The Prime Numbers Will be Identified, the Code will Be Broken'. The article, which references the *NYT* article from 8 August 2002, states that if the new algorithm developed by the three Indians really works, 'it will be able to serve as an effective tool for breaking digital codes'. By confusing the *IFP* problem with the *PRIMES* problems, the article states that the current RSA encryption used on the Internet cannot be broken because 'current methods for determining the primality of numbers are either too slow or not certain', and concludes: 'it will be shortly made clear if this is indeed a development which undermines the ability to encrypt digital data' (Brizon, 2002). About a week later, the newspaper published a correction article by Dr Tamir Tassa, a mathematician from The Open University of Israel, with the title 'With all Due Respect to the Deterministic Algorithm in Polynomial Time, the Code Will not Be Broken'. This article interpreted the AKS algorithm in its theoretical context (note also the use of mathematical jargon in the title!), explaining the reliability of the existing Miller–Rabin probabilistic algorithm for checking primality and distinguishing *PRIMES* from *IFP* (Tassa, 2002).

Between 20 October and 3 November 2002, Agrawal held a series of talks at MIT, Harvard University, Clay Mathematics Institute in Boston, and Princeton University. Following this series of talks, an article was published in *The Wall Street Journal.* The article's subtitle states 'Will Manindra Agrawal Bring about the End of the Internet as We Know It?'. The article states that Agrawal found an algorithm for determining if a number is prime, and suggests that just another small step is needed to find an algorithm for factoring a large number – a development that would break Internet encryption. Describing the attention Agrawal got from computer scientists and mathematicians, the article states:

> Prof. Agrawal's work involved only testing whether a number is prime, not the factoring problem. Still, there are enough connections and similarities between the two that mathematicians and computer scientists from all over the East Coast flew in to hear Prof. Agrawal on a whirlwind tour last week through the likes of M.I.T., Harvard and Princeton. (Gomes, 2002: B1)

The article connects the wide academic attention Agrawal got to the fact that his algorithm might be used for breaking Internet encryption. However, a reading of the abstract of the paper Agrawal presented at MIT suggests that the academic interest in his work was purely theoretical:

> Testing if a given number is prime is a fundamental and well-studied problem of computational number theory. There are several algorithms known for it that are efficient in various ways: deterministic polynomial time under ERH (Miller), randomized polynomial time (Rabin, SolovayStrassen, Adleman-Huang), and deterministic 'slightly' superpolynomial time. However, till recently, there was no unconditional deterministic polynomial time algorithm known for the problem. In this talk, we present the first such algorithm.[15]

Note that this abstract does not mention anything about Internet encryption or the *IFP* problem. It deals only with the *PRIMES* problem in relation to its classification to complexity classes. Of course, I am not denying that the overall interest in algorithms concerning prime numbers has to do with their use in encryption. However, as opposed to *The Wall Street Journal*'s allegation, 'connections and similarities' between *PRIMES* and *IFP* were not presented at Agrawal's talks.

An article in *The Economist* from 29 March 2003 with the title 'Primed to Go: Mathematicians are Discussing Ways to Make Code-Breaking Easier' is written along the same lines as *The Wall Street Journal* and states the following:

> There is still some way to go before any of this work actually threatens cryptography. That is because quick and dirty techniques for testing primality already exist. Unlike Dr Agrawal's method, and its slower predecessors, these sometimes make mistakes, falsely attesting that a number is prime. But because such mistakes are rare, they are tolerable. However, if Dr Agrawal's primality test can be extended to factoring numbers, it would mean a rejigging of modern cryptography. Then the spooks and bankers really would be worried (Anonymous, 2003: 89).

The word 'because' in the beginning of the second sentence creates an alleged connection of cause and effect between the fact the AKS algorithm does not yet pose a threat to Internet security and the probabilistic nature of the existing Miller–Rabin algorithm for testing primality. However, from the point of view of computational theorists, this is false. Recall that the existing Miller–Rabin algorithm is used for encryption and not for code breaking, and the fact that it is probabilistic is a theoretical characterization of it, and has nothing to with its reliability for practical use.

The popular press, therefore, misinterpreted the AKS algorithm, its significance and its implications. While mathematicians and computational theorists understood it as a *theoretical* breakthrough, the popular press emphasized its alleged *practical* significance for encryption on the Internet. The press misinterpreted the term 'probabilistic' when used to refer to algorithms as meaning 'having a tangible probability of error in the practical domain of encryption'. By doing so it concluded that the former probabilistic Miller–Rabin algorithm for checking primality was unreliable. It therefore interpreted the new AKS algorithm either as an algorithm that could improve current encryption on the Internet by making it more reliable, or as an algorithm that could be used for breaking the current method of encryption. Both of these contradictory interpretations are false from the point of view of specialists familiar with the problem.

A question then arises about what caused the popular press to misinterpret the significance of the 'PRIMES is in P' paper. In the next section, I will argue that this misinterpretation served both the interests of the popular press as well as the interest of the scientists who made the discovery. I will argue that the fact that the relevant scientific community had strict epistemic standards for evaluating the paper in question and distinguishing a correct from a distorted understanding of it, explains how Agrawal and his team were able to have different interpretations delivered simultaneously to different audiences through different communication channels, achieving maximal exposure without risking their scientific reputation.

The Shared Interests of the Scientists and the Press in Distortion

Gregory and Miller identify several characteristic, or 'news values', which make stories appealing to media consumers. Stories about events that happen on a large scale have more news value than those that happen on a small scale. Stories relevant to readers' lives, or stories about matters on which readers already have knowledge or opinions, have relatively high news value. Exclusive stories have more news value than stories that are widely accessible. Bad news is more newsworthy than good news. Readers have more interest in stories that happen in their own back yards than those that happen far away. Last, stories from reliable sources have more news value than stories from dubious sources.

As Gregory and Miller observe, with the exception of having what is perceived as a reliable source, scientific stories typically lack news value: they usually happen on a small scale; they touch on aspects that are foreign to people's lives; stories about scientific discoveries are usually not exclusive; their immediate negative or positive impact is not clear; and they are often universal and not local (Gregory & Miller, 1998: 110–14). News reports about science therefore try to be as relevant and meaningful as possible: they make bold claims; they lack nuance; they emphasize the potential application and outcomes of scientific results; and they connect scientific results to matters that are close to the readers' world (Gregory & Miller, 1998: 116).

News values are a set of epistemic standards that are external to the scientific community. Scientists determine what knowledge of science the general public will have only to a small extent. So do science journalists. News editors, who have no particular loyalties to science as an enterprise, largely determine which stories get published, and they typically publish what they believe the public wants to read (Gregory & Miller, 1998: 109).

If scientists have interest in the general media's coverage of their work, as I will argue they do, they must cooperate with the media's epistemic standards. At the same time, since their fellow scientists are also media consumers, they will not want the media reports to discredit their work in their colleagues' eyes. But when distortion is easily distinguished from genuine scientific knowledge, they needn't worry about this so much. They can enjoy both worlds.

These observations are important in analysing the PRIMES affair. When asked by his fellow mathematicians about his impression of the popular media coverage of his discovery, Agrawal politely advised, 'leave aside the general public coverage' (Bornemann, 2003: 550). However, although Agrawal was reluctant to comment about it to his colleague, he did cooperate with the popular media coverage.

Agrawal's cooperated in a twofold manner. First, he gave interviews to reporters from the popular media. As I will show, it is likely that some of the journalists' misconceptions originated from these interviews. Second, on the webpage where they published their original 'PRIMES is in P' paper, Agrawal and his students published several links to media reports about their paper, including the first *NYT* report.[16]

When interviewed by *The Wall Street Journal*, Agrawal made the following statement regarding his motivation to find a deterministic polynomial algorithm for solving *IFP* (recall that, if found, such an algorithm can be used to break the popular Internet RSA encryption system):

> 'Factoring is a natural problem. And natural problems should have a natural complexity to them. But this … is not natural complexity. This looks very strange. There must be something more natural than this out there.' (Agrawal, quoted in Gomes, 2002: B1)

To the lay reader, such a statement may seem reasonable. However, to a specialist, it makes less sense, because the word 'natural' used in this context is vague and ambiguous. The term 'natural problem' does not refer to any particular class of problems. Does a 'natural problem' involve natural numbers? Perhaps, or perhaps not. Likewise, the term 'natural complexity' is not associated with any of the known complexity classes. At most, for a specialist, this statement may express some vague intuition and nothing more. However, to the lay reader, to the extent Agrawal is quoted correctly, this statement provides the missing speculative link between the actual AKS algorithm and 'putting the Internet on alert'.

An examination of Agrawal and his students' web page shows a conscious use of this medium. Their site contains three main sections, which target roughly three types of audience. Two sections, the first and third, have already been mentioned. The first section contains a link for downloading their original 'PRIME is in P' paper. This is obviously intended for the specialist audience of mathematicians and computer scientists. The third section is the list of links to popular reports about the algorithm. The other section, the second on the page, contains a link to a list of Frequently Asked Questions (FAQ) about 'Prime is in P' compiled by Anton Stiglic (2005).[17]

This FAQ targets an audience of people who are interested in theoretical computer science, but are not professional academics, such as students, software engineers and amateur mathematicians. It aims at explaining the principles of the AKS algorithm and its importance. Specifically, it aims at clarifying common misconceptions about the algorithm, such as the confusion between *PRIMES* and *IFP*, as the following excerpt from it shows:

> Q13. Does this result have any impact in cryptography at all?
>
> Not in any obvious ways. Certain algorithms need to generate prime numbers in order to construct cryptographic keys, but algorithms to accomplish this which can be executed very efficiently already existed before the result in [1]. The most commonly used ones have a probability of error, but this error can be made to be arbitrarily small … and thus they give us practically the same assurance as the algorithm proposed in
> P. These algorithms that are commonly used in practice are actually faster than the ones proposed in [1]. The result in [1] is a very important one in complexity theory, but probably have no (practical) impact in cryptography. (Stiglic, 2005)

If we compare this statement with Agrawal's statement in *The Wall Street Journal* we get quite a different impression. While according to this statement, AKS has no impact on cryptography, at least 'not in any obvious way',[18] the impression we get from the article in *The Wall Street Journal* and the other articles in the general press is that just another small step is needed for AKS to be used to break Internet cryptography.

The conclusion of this comparison is clear. Different messages were simultaneously delivered to different types of audiences through different communication channels. It seems that it was very difficult for Agrawal to receive wide exposure in the popular media without implying that his algorithm has practical implications for Internet security. On the other hand, Agrawal could count on his colleagues to immediately recognize the real significance of the paper, which is purely theoretical, and simply dismiss the general media reports about the algorithm as popularized distortions. In other words, *as it lacked news value on its own, it was very unlikely that the general media would report only a theoretical breakthrough in computer science if it had not been implied that this breakthrough has practical implications for Internet security.*[19] *On the other hand, these reports in the general media did not compromise Agrawal's prestige among his peers because they could clearly distinguish genuine knowledge from distortion.* This example shows that, as opposed to Bucchi's claim (1996: 378), such simultaneous communication at different levels does not necessarily mean that barriers between genuine and popularized knowledge cannot be drawn sharply. Rather, it implies the contrary.

What did Agrawal and his team have to gain from the general media coverage of their algorithm? Or in other words: What were their interests in such coverage? What may explain their choice to publish their result on the Internet and to turn to the general media before pursuing regular channels of peer reviewed publications? An analysis of this case points to three interests: *visibility*, *recognition* and *priority*.[20]

Visibility

The popular media is an ideal means of getting as much exposure as possible. The first article in the *NYT* was a great promotion that attracted the attention of mathematicians and computer scientists. Within the first day that their paper was available online, it was downloaded by about 30,000 people (Kingsley, 2002).[21] Within the first 10 days of being online, the dedicated webpage had more than 2 million hits and 300,000 downloads of the paper itself (Bornemann, 2003: 546). The coverage of the paper in the general media was the trigger, or at least a major catalyst, for this extremely vast interest.

Another important reason for turning to the general media is to enhance the number of citations of a paper. A study that compared the number of references in the *Science Citation Index* of papers in the *New England Journal of Medicine* that were covered by the *NYT* with the number of citations of similar papers that were not covered shows that papers in the journal that were covered received a disproportionate number of scientific citations in each of the 10 years after they appeared (Phillips et al., 1991).[22] It is reasonable to assume that the first paper about the 'PRIMES is in P' paper in the *NYT* was the most influential, because that newspaper is believed to set the tone for other general papers and magazines (Phillips et al., 1991: 1180).

As of June 2008, *Google Scholar* counts about 126 references to the original 'PRIMES is in P' article that was published on the Internet in 2002,[23] and 367 references[24] to the peer-reviewed paper published in 2004 in *Annals of Mathematics*.[25] The above study suggests that without the *NYT* publication, it would have been lower.

Recognition

In this case recognition is a direct result of visibility, and the epistemic standards of evaluation of the relevant scientific community were rigid and well defined. Namely, there is a consensus among professional mathematicians and theoretical computer scientists about what constitutes a mathematical proof.[26] Moreover, Agrawal and his students' paper was short – only eight pages long. Unlike other proofs, the mathematics that it used was relatively simple and accessible to an advanced undergraduate maths student (Bornemann, 2003: 545).[27] Thus, Agrawal and his team did not need to wait for the long and tedious peer review process. Thousands of professional mathematicians and computer scientists downloading the paper and checking the proof were better than any peer review process. Of course, not all cases are like that, and visibility does not always result in recognition.

Another important aspect of recognition is prizes. An article on the Internet news site *rediff.com* reports that 'IIT Kanpur Director Sanjay Dhande was elated at the news that created headlines in *The New York Times*'. A few sentences later it adds: 'He was confident about Agrawal getting nominated for the world's top honours in mathematics, considering his latest feat' (Pradhan, 2002). The connection between media coverage and recognition in the form of awards was not concealed to IIT Kanpur director Dhande, and indeed on 30 October 2002, less than 3 months after the initial publication of Agrawal's paper on the Internet, and before his paper was published in any peer-reviewed journal, Agrawal won the Clay Research Award at the Clay Mathematics Institute in Cambridge, MA. In May 2003 he won the International Centre for Theoretical Physics (ITTC) Prize. In April 2006, after the paper appeared in *Annals of Mathematics* in September 2004, Agrawal won the prestigious Gödel Prize, which is given only to papers published in peer-reviewed publications.

Priority

Computer science is a field with very rapid developments. It may be the case that by the time a paper is published in a peer-reviewed journal, it is already outdated. The publication of 'PRIMES is in P' in a peer-reviewed journal (*Annals of Mathematics*) (Agrawal et al., 2004) occurred more than 2 years after the paper appeared online. It was almost 9 months from the moment the paper was accepted to the moment it was published. The slow process of peer review is incompatible with the fast pace of the field. As Odlyzko, writing before the publication of the paper in *Annals of Mathematics*, observes:

> The [peer-reviewed] journal version will probably be the main one cited in the future, but will likely have little influence on the development of the subject. Within weeks of the distribution of the Agrawal–Kayal–Saxena article, improvements on their results had been obtained by other researchers, and future work will be based mainly on those. Agrawal, Kayal, and Saxena will get proper credit for their breakthrough. However, although their paper will go through the conventional journal peer review and publication system, that will be almost irrelevant for the intellectual development of their area. (Odlyzko, 2003: 311)

Because of the dynamic nature of this field, it is plausible to assume that scientists in it will give prime importance to the issue of priority. Publishing a paper on the Internet is the best way to win a priority race. Because there is a consensus among scientists about what constitutes a mathematical proof and presenting such a proof was all that was required to achieve acceptance of their claim, Agrawal and his team had nothing to lose by their Internet publication and their use of the general media, only to be acknowledged as the first to find a deterministic polynomial algorithm for PRIMES.

Popularization and Distortion Revisited

A debate exists about the question of media popularization. The question is whether there is ‘genuine knowledge’ in contrast to ‘distorted knowledge’. In this paper I have shown that in the PRIMES affair, the general media did give a distorted account of the AKS algorithm, its importance and implications. These modes of distortion, several of which were usually used together, are summarized in Table 2.

In the usual case, a reader who is familiar with the relevant scientific discourse could find a kernel of truth in a media report, or at least identify the genuine fact on which the distorted account is based. However, in rare cases, there is no interpretation, not even one extremely liberal and charitable, under which statements in the media report may be considered to be even partly true. This is the case that corresponds to mode of distortion no. 6 (Table 2). The example that is quoted in no. 6 is the only case I have found during my research in which a newspaper published a correction.

Viewed from the perspective of computation and number theorists, the distorted accounts in this case could be distinguished from faithful representations on stable and recognizable epistemic grounds. The existence of these stable communal epistemic grounds explains Agrawal and his students’ ability to deliver different accounts, distorted and non-distorted, to different audiences, thus achieving both visibility and professional recognition at the same time. In this case, the standards of the scientific community *clearly and rigidly defined the borderline between genuine scientific knowledge and distorted simplifications*.

TABLE 2
Modes of distortion by the media of the 'PRIMES is in P' paper

No.	Mode of distortion	Examples
1	Using terms which have different meaning in ordinary language context and in scientific context	'The new algorithm – by Manindra Agrawal, Neeraj Kayal and Nitin Saxena of the Indian Institute of Technology in Kanpur – guarantees a *correct* and *timely* answer' (Robinson, 2002: A20; emphasis added)
2	Neglecting to mention facts that are relevant for understanding the significance of the discovery	Many reports ignored the fact that a reliable algorithm for testing primality is already used in RSA encryption
3	Obscuring the difference between similar but not identical things	Obscuring the difference between *PRIMES* and *IFP*
4	Mentioning two facts which are true in themselves, but juxtaposing them or making a logical connection between them in a way that creates a false impression that they are connected	'RSA, a popular encryption algorithm used in securing Internet commerce, is built on the assumption that when prime numbers … are large enough, they're nearly impossible to generate and determine. … But a new algorithm, developed at the Indian Institute of Technology in Kanpur by Manindra Agrawal and his students Neeraj Kayal and Nitin Saxena, is believed to generate correct results each and every time' (Junnarkar, 2002)
5	Using speculative language, for example, like 'possibly' or 'may', phrasing sentences in the form of a question, and so on, while the speculations are unfounded	'Prime Efforts May Boost words Encryption' (Junnarkar, 2002); 'Will Manindra Agrawal bring about the end of the Internet as we know it?' (Gomes, 2002: B1)
6	Making false statements	'It will be shortly made clear if this is indeed a development which undermines the ability to encrypt digital data' (Brizon, 2002)

I have argued that the existence of independent epistemic standards for evaluating knowledge claims explains the turn of events in my case study. One may argue, however, that my case study supports only a weaker claim than the one I have made, namely that researchers in a particular community are able to distinguish knowledge claims that adhere to their community consensus, where a consensus exists, from knowledge claims that depart from it. Hence, so this objection goes, what I call the independent epistemic standards merely turn out to be the standards of the particular community.[28]

My response to this worry is threefold. First, even if we grant only my weaker claim, it still calls for a significant reform to the new model of popularization. Recall that according to the new model, scientists' ability to label different accounts as legitimate or distorted science in different social circumstances is a political resource available to them to maintain their hegemony on the construction of scientific facts. This assumed ability is used to explain how certain claims gain the social status of knowledge. In order to effectively use this ability, the community's epistemic standards need to be *flexible and easily redefinable*. The new sociological model of popularization suggests that when encountering a scientific report in the general media, individual scientists can make ad hoc changes to their epistemic standards either to legitimize or discredit the report according to their social interests. If, however, epistemic standards are rigid and constrained by the pre-existing community consensus, scientists cannot legitimize or discredit reports as they wish. It follows that scientists cannot maintain their hegemony on the construction of scientific facts as effectively as the new model suggests. This seems to seriously impair the potential explanatory potential of the new model.

Second, a stable communal consensus, where one exists, is itself an intriguing social fact that requires an explanation. How and why does such a consensus emerge and why is it maintained? A desideratum for a robust theory of popularization is to be able to explain the different outcomes, such as a change or lack of change in a community's consensus, in similar cases in which scientists turn to the media. In particular, when does a scientist's mere choice to turn to the media threaten the community to which she belongs and cause its members, for example, to penalize the deviating scientist by delegitimizing the factual claims in question? What distinguishes the cold fusion affair, in which media reports allegedly constructed scientists' epistemic expectations (Lewenstein, 1995; Simon, 2001)[29] from the PRIMES affair, where this was not the case? The new model does not seem to give us answers to these questions, whereas the introduction of the existence of independent and recognizable epistemic standards may explain the stability of a consensus in some cases.

Specifically, adherence to such standards may adequately explain why certain popularization episodes have so little influence on the shared beliefs of experts, while other episodes seem to have lasting effects on the course of scientific research. Of course, it is not sufficient simply *to assume* that such independent epistemic standards exist. If the stability and instability of communal consensus is to be explained, subsequent sociological accounts of scientific knowledge will need to tell us when it is legitimate to make such an assumption and what it includes. The modest goal of the current study is to underscore the need for this kind of shift in explanatory strategy, rather than to propose a full-blown methodological alternative.[30]

Third, the claim that the epistemic standards reflect merely local consensus overlooks an important aspect of my case study. The subject matter of Agrawal and his students' claim was not restricted to the inner discourse of an esoteric group of number theorists. Rather, it was also a claim about what computers, material artefacts in the world, are capable and not capable of doing and at what speed. According to many of the newspapers reports, the AKS algorithm could be used to break the commonly used RSA encryption on the Internet. Specialists, on the other hand, regarded this claim as false. To date, there have been no reported cases in which the AKS algorithm was successfully used to break RSA encryption in order to steal, for example, credit card numbers that are used in online transactions. To date, then, in spite of opposing predictions in the general media, Web users can still safely use their credit cards and access their bank accounts online. What explains this ability? Why hasn't the Internet collapsed, as predicted by some media reports? How are the inner social norms and conventions of an esoteric group of number theorists translated to the social norms and conventions governing online commerce? If we assume that the epistemic standards of the esoteric community of number theorists are more than merely social norms, and that they are independent of the social settings in some way – that they are constrained by some physical and logical necessities, for example – the fact that the general media's apocalyptic predictions about the collapse of the Internet have been proven false is easily explained. If we do not assume that, then we need a much more complex explanation that refers only to social norms. The current sociological model of popularization does not provide us with such an explanation, and I doubt very much if it can.

My claim is that the possibility of the existence of independent epistemic standards needs to be added to the explanatory toolbox of the new model of popularization. Cases such as PRIMES cannot be adequately explained otherwise. Indeed, the absence of this assumption may reveal an explanatory lacuna in other case studies as well. For example, Sommer (2006) examines the discovery of a Neanderthal skeleton by French archaeologist Marcellin Boule in 1908. Boule interpreted the Neanderthal skeleton as a 'cousin' of modern humans, namely as having a common ancestry but not as a direct ancestor. Sommer, who relies on the new model (2006: 216) suggests that Boule chose this interpretation because it was susceptible to two opposing popularized interpretations. The first interpretation suited the worldview of the secular progressivist French press, and the second was 'Church friendly' (2006: 231). Sommer does not examine, however, the extent to which the anatomical and paleontological beliefs of scientists of the time constrained the possible interpretations of the skeleton to begin with. If my argument in this paper is correct, a complete explanation of the case should have addressed this as well.

While the possibility of the existence of independent epistemic standards is a nice thing to have in the explanatory toolbox of the new model, I do not argue that it should always be used. I do not claim that independent epistemic standards always exist, nor that when they exist, they always explain the outcome of a scientific affair. Moreover, I do *not* claim that when independent epistemic standards exist, they necessarily correspond to the standards of the relevant scientific community. I call for a reform to the current model of popularization, not a return to old models of explanation, in which scientists' true beliefs are explained by their truth, and false beliefs are explained by 'external' social factors.[31]

Developing such a theory of popularization exceeds the scope of this paper, the main aim of which is to point out the need for such a theory. Nevertheless, I would like to make a few preliminary remarks about the generalizability of this case study. The case study I presented in this paper was from theoretical computer science. However, the social mechanism I have identified and the distinction between genuine and distorted scientific knowledge is relevant to other cases as well. For example, a discovery of a new large asteroid is not news. If the asteroid is about to hit Earth, however, this is news. Therefore, in order to reach the general media, a scientist has every interest in overestimating as much as possible the chances that this newly discovered asteroid will hit Earth. Similarly, in the cold fusion affair, it is doubtful if Fleischmann and Pons would have reached the general press had they not claimed the discovery of an extremely cheap energy source.[32]

At first glance, the PRIMES case study may seem different from perhaps more typical cases of popularization in that it involves popularization of mathematical knowledge, for which there are arguably rigid and stable epistemological standards. This suggestion is problematic for two reasons. First, a principled distinction between mathematical and other forms of scientific knowledge conflicts with the epistemological commitments of the proponents of the new model. From its early days, SSK theory has denied any such principled distinction, arguing that the same kind of sociological analysis applies both to the 'hard' and 'soft' sciences (Collins, 1983: 278).[33] Proponents of the new model of popularization embrace this view, and regard the new model as part of the research programme that was set forward by the early SSK scholarship (Whitley, 1985: 6; Hilgartner, 1990: 522–24; Lewenstein, 1995: 407). Therefore, they cannot simply explain away PRIMES as an unrepresentative exception to their model.

Second, as I have mentioned, the claims in the PRIMES affair are also about what computers, which are material artefacts in the world, are capable of doing.[34] In this sense, they are similar, for example, to physicists' claims about what certain objects in the world can do, which are also expressed in mathematical language. What distinguishes this case from others, in my opinion, is that in PRIMES, the relevant scientific community required no empirical demonstration to secure the knowledge claim. Agrawal and his team were not required, for example, to code a computer program that solves PRIMES and test its performance. Presenting a proof was enough. In computational theory, empirical demonstration in the form of coding a program and running it is considered irrelevant for supporting claims. This is not the case in other branches of computer science. For example, in computational linguistics, it is not enough to develop a new algorithm for speech recognition; it must also be empirically shown that it correctly recognizes speech. Computational computer scientists' confidence in the correctness of their claims without need to empirically demonstrate them may have many explanations. But, the enormous past success in easily implementing theoretical results such as the RSA encryption algorithm and the Miller–Rabin primality testing algorithm surely has something to do with it.

In the cold fusion affair, in contrast, repeatable empirical demonstrations were required to establish the claim. Scientists who were trying to replicate Fleischmann and Pons' experiment and produce cold fusion learned many details about the experimental design from the media (Lewenstein, 1995; Simon, 2001), and so media reports obviously played a major role in mediating the knowledge claims at stake. However, note that this analysis of the role of the media shifts the focus to explaining why certain experiments failed or succeeded. This brings us back to notions of accuracy in reporting and distortion, which are associated with the old model, and not so much to social factors such as the prestige and reputation of the informants.

If this is the case, then, it seems that when replications are required and performed, such as in the cold fusion affair, or when experiments are irrelevant for establishing claims, such as in PRIMES, it is likely that the media will play a minor role, if any, in the construction of scientific knowledge. It seems more plausible that the media will play a more crucial role in constructing scientific knowledge in cases where scientists report certain empirical results, but attempts to replicate their experiment or reproduce their results are *not* performed due to various reasons such as cost and lack of resources. These are of course tentative suggestions that call for more sociological research.

Conclusion

In this paper I have systematically surveyed and analysed the popular press coverage of the 'PRIMES is in P' affair. I have argued – against the prevailing new orthodoxy – that without assuming that distorted simplifications of scientific knowledge are distinguishable from non-distorted simplifications on independent epistemic grounds, the turn of events in the PRIMES case study cannot be adequately explained. This suggests that the possibility of the existence of independent epistemic standards must be incorporated into the new SSK model of popularization.

Notes

I would like to thank the following people: Yves Gingras for his excellent SSK seminar and helpful advice; Anjan Chakravartty, Omer Levy, Isaac Record, Eran Tal and Tamir Tassa for their comments on earlier versions of this paper; the participants in the IHPST Work-inProgress Seminar for their helpful feedback, especially Joseph Berkovitz, Lucia Dacome, Mark Solovey and Marga Vicedo; the anonymous reviewers and especially Michael Lynch for their criticisms and suggestions for improvement; my wife, Meital Pinto, for her support and inspiration; and my mother, Leah Miller, who was the first person I know to read about the PRIMES paper in the newspaper and ask me about it.

[1] The literature about popularization covers both the popularization of scientific knowledge and practice. With regard to scientific practice, it is argued that the media conveys to lay audiences an idealized account of the scientific method, which hides the intricate process of social conflicts and negotiations through which scientific knowledge is constructed. Because of this idealized account of the scientific method, lay people ascribe a high degree of reliability to scientists' claims (Gregory & Miller, 1998: 90–91). Within the scope of this paper, I only address the question of the popularization of

scientific knowledge, but not of scientific practice. In other words, I address the question of what beliefs lay readers come to form from popularized reports about what scientists claim to have done. I do not address the question of the warrant that lay readers have or should have for these beliefs, although, of course, in general these two questions are not isolated.

2. Reactions to constructivism can be divided into two main camps. Accounts that belong to the first camp deny some of the constructivists' premises and offer a rational or realist reconstruction of construction narratives, which they argue to be more plausible (Goldman, 1999: 225–30; Brown, 2001: 115–43; Giere & Moffatt, 2003). Accounts in the other camp, to which this paper belongs, accept constructivist premises and argue that constructivist explanations fail on their own terms. For example, Silva (2005) examines experiments in aerodynamics, and argues that discursive theory alone cannot explain the existence of a giant physical robotic model of a moth in these experiments, its role in producing knowledge and the different knowledge that would have been produced had computer simulations been used instead. This is because the theory lacks the necessary concepts to deal with the materiality of the model. Based on a field study of a nuclear physics laboratory, Giere (1988: chapter 5) argues that one cannot give an adequate social explanation to the physicists' behaviour without assuming the ontological reality in which they believe. Similarly, my case study suggests that the existence of independent epistemological standards needs to be assumed in order to adequately explain its outcome.
3. See Väliverronen (1993: 24–26) for a literature review of studies associated with the traditional model.
4. Following Kusch, I take epistemic standards to be a set of exemplars (in the Kuhnian sense) that are shared by members of an epistemic community. Justifying a claim is a dialectical process in which members of the epistemic community try to show that the relations between the content of the claim and the evidence for it are similar or analogous to one of the communally endorsed exemplars. A claim counts as knowledge when the community is satisfied that this is indeed the case (Kusch, 2002: 120–30). As I will show, however, my case study militates against Kusch's claim that epistemic standards are necessarily relative to an epistemic community, and that one epistemic community's epistemic standards cannot be said to be objectively better than another community's epistemic standards (Kusch, 2002: chapter 18).
5. For a critical review of the changing legal standards for evaluating scientific expert testimony in US courts see Haack (2003, chapter 9).
6. The following account is simplified from two leading university-level computer science textbooks (Sipser, 1997; Cormen et al., 2001). Therefore this account may be considered a 'canonical' account. The account I give is simplified in two main ways. First, it does not include any proofs, so the claims remain without their justifications. Second, mathematical jargon and technical notations are largely omitted. Though simplified, my account is not distorted. My ability to give such a simplified yet nondistorted account is consistent with my claim in this paper. (The fifth section of this paper (popularization and Distortion Revisited) I defend my choice to rely on this account when analysing the media reports.) Due to my own academic background in computer science I have 'interactional expertise' that allows me to serve as a translator (Collins & Evans, 2002: 254–58) between computer scientists and the readers of this paper.
7. A polynomial function is a function of the form $f(x)$ □□ a_nx^n □□ $a_{n-1}x^{n-1}$ □□... □□ a_1x □□ a_0, where $a_n \dots a_0$ are constants and n is a positive natural number. Examples for polynomial functions are $f(x)$ □□ $3x^2$, $f(x)$ □□ $5x^{27}$ □□ $12x^{20}$ □□ $8x^4$, and so on.
8. More precisely, let a be an algorithm, let x be the length of the input and let the function t denote the running time of the algorithm, then a belongs to complexity class P if and only if there exists a polynomial function p such that for all x, $t(x)$□$p(x)$.
9. An exponential function is a function of the form $f(x)$ □□ c^x, where c is a constant.
10. For a formal definition of complexity class P see Sipser (1997: 234–36).
11. A formal definition of *PRIMES* is: *PRIMES* □□ $\{n \mid n$ is a prime number$\}$.
12. A formal definition of *IFP* is: *IFP* □□ $\{x \mid x$ □□ pq, for integers $p, q>1\}$.

13. It is useful to note that for practical implications, the AKS algorithm runs significantly slower than the Miller–Rabin algorithm, although both of them run asymptotically in polynomial time. Therefore, for practical implementation, the Miller–Rabin algorithm is preferable to the AKS algorithm.
14. Other reports in the English-language Indian press are Pradhan (2002), Rajghatta (2002) and Ramachandran (2002). Ramachandran (2002) is the only exception of a paper from the popular press that I found during my research which gives an accurate and non-distorted account of the importance of the AKS algorithm in its scientific context.
15. See <http://theory.csail.mit.edu/toc-seminars/archives/2002/Agarwal-abs.html>.
16. The original web page was in the URL <http://www.cse.iitk.ac.in/news/primality.html>, but it was no longer available online after April 2005. However, it can still be accessed in the Internet Archive site in the following URL: <http://web.archive.org/web/20021017101338/http://www.cse.iitk.ac.in/news/primality. html>.
17. According to his homepage, Stiglic is a cryptologist who obtained his MSc in theoretical computer science from the Université de Montréal, and is also active at the 'Crypto and Quantum info Lab' at the School of Computer Science at McGill University <http://www.instantlogic.net>.
18. When making claims, scientists tend to use cautious and modest language. This may be explained inter alia by their adherence to the Popperian ethos, in which all knowledge claims are provisional and may be subject to future falsification. Other epistemic communities, such as the popular media, prefer a much more decisive language. As Beecher-Monas (2007) notes, in the legal system, this difference in tone has profound implications. While scientists tend to use cautious language, judges prefer the language of certainty. When encountering cautious language, judges often exclude scientific evidence as speculative. This shows their lack of understanding of the cultural norms of modesty and caution of the scientific community, and a failure to evaluate the evidence on its own stake (Beecher-Monas, 2007: 54–55).
19. In addition to being consistent with Gregory and Miller's analysis of news values, the plausibility of this claim is supported by historical research. Hughes (2007) describes the work of *Manchester Guardian* science journalist James G. Crowther in interwar Britain. While Crowther expressed interest in reporting about new developments in atomic physics and the discovery of new subatomic particles, his editor tended to perceive these issues as too complicated and lacking in interest for the newspaper's readership. Instead, he encouraged Crowther to inform readers about mundane issue such as 'eels, the physiological effects of manual labour, and dairy farming' (Hughes, 2007: 16). It was only Crowther's success in achieving priority in reporting about the developments in atomic physics and competing journals' consequent interest in these reports that persuaded his editor to approve their publication.
20. Fuller identifies a general interest of the scientific community in popularization. This is the interest in science's continued survival. The scientific community has an interest in popularized accounts in the media, because they help science gain the support of the public, but at the same time they do not provide the public with sufficient in-depth understanding of science to enable them to question scientists' work (Fuller, 1997: 32–33). Within the scope of this paper I will only discuss interests of individual scientists in popularization.
21. The ABC article states that the paper was published on the Internet on 7 August 2002, and 'within 24 hours' it was downloaded more than 30,000 times. The *NYT* article was published on 8 August 2002. So, because of the time difference between Kanpur and New York, if we take the words '24 hours' literally, and we start counting from the early morning of 7 August (Kanpur time), then these downloads occurred before the *NYT* article was published. However, if we start counting the hours from the evening of 7 August (Kanpur time), or do not take the words '24 hours' literally, then it turns out – and this is the plausible scenario in my opinion – that the *NYT* article did contribute significantly to the number of downloads. Otherwise, this enormous number cannot be

explained. The alternative explanation is that the rumour about the paper was spread by emails. However, if this was the case, members of the initial group of people that could spread this rumour had already had the article sent to them by email. It would have been more plausible that they would have forwarded the actual paper by email to their colleagues as well, saving them the need to download it from the Internet themselves. Therefore, it is much more plausible that the *NYT* article was responsible for the great number of downloads.

22. The researchers had a control group of articles published in a 3-month period in which the *NYT* was on strike, which militates against the possibility that the articles that appeared in that newspaper were simply the most important ones.
23. See <http://scholar.google.com/scholar?hl□en&lr□&q□%22%2Bwww.cse.iitk.ac.in%2Fnews%2Fprimality.*%22&btnG□Search>. The method I used was to count the number of references to the original URL in which the paper was first published.
24. See <http://scholar.google.com/scholar?hl□en&lr□&q□link:FRe2NnJZe0J:scholar.google.com/>.
25. Unfortunately, the *ISI Web of Science* gives inaccurate results about this paper. According to the Web of Science, the 2004 paper was cited only eight times! However, when I checked some of the citing papers that appeared on *Google Scholar*, I found that they did exist on the *Web of Science*, but for some reason did not appear among the papers citing the 2004 paper.
26. MacKenzie describes how the concept of proof in computer science and mathematics has changed in the second half of the 20th century, side-by-side with developments in computer technology. Within mathematics and computer science, he identifies two main subcultures that have emerged. One subculture sees proof as a logical manipulation of symbols in a formal language that can, at least potentially, be performed by a computer. The second subculture sees proofs as rigorous arguments that can convince a trained human mathematician. While subscribers to the former view will tend to regard proofs that appear in textbooks and academic papers, such as the proof that PRIMES is in P, as sketches of formal proofs, subscribers to the latter view will tend to regard formal proof as a partly adequate and idealized model of real, rigorous argument proofs (MacKenzie, 2001: 323–24). MacKenzie argues, however, that these two views are not incompatible enough for actual mathematical proofs to genuinely constitute what Galison (1997: chapter 9) calls a 'trading zone', namely a site where diverse cultures coordinate their practical activities while maintaining a distinct understanding of the meaning of what they do and what they exchange. Different types of proof that conform to different perceptions of what a proof is are allowed to live peacefully together in the mathematical literature and are rarely disputed (MacKenzie, 2001: 327–28). As MacKenzie points out, while there no one agreed-upon view among mathematicians about what exactly a mathematical proof is, 'this does not imply that "anything goes", that any arbitrary argument can count as a mathematical proof. What it suggests, rather, is that members of the relevant specialist mathematical community, in interaction with one another, come to a collective agreement as to what counts as a mathematical proof' (MacKenzie, 2001: 318). Moreover, MacKenzie's research did not find a case in which a mechanical proof disagreed about a theorem with an established rigorous proof that had preceded it (p. 323). We should also distinguish between disagreements on the nature of proof (epistemic standards) from disagreement on the truth and falsity of theorems (knowledge claims). For example, in the case of the four-colour theorem, which was controversially proven with the aid of a computer program, if we ignore the groundless rumours about a bug in the program that was used to prove it (MacKenzie, 2001: 139) then mathematicians do not dispute whether the theorem itself is true, only whether the method that was used to show its truth constitutes a proof.
27. Agrawal and his students' proof was an ordinary mathematical proof like the vast majority of mathematical proofs that appear in mathematical journals and textbooks. It did not involve the use of computers. Thus, unlike the proof of the four-colour theorem (see note 26), for example, which relied extensively on the use of computers, the proof that PRIMES is in P did not trigger debates about its validity. In addition, because

Agrawal and his students' proof was relatively short and non-complex, it did not trigger debates such as in the case of the proof of Fermat's last theorem, the length and complexity of which made it difficult to be verified.

28. I thank this journal's anonymous reviewer for pressing me to further explicate this point.
29. For an alternative interpretation of the cold fusion affair, see Solomon (2001: 129–32).
30. See Tucker (2003) for such a discussion of scientific consensus.
31. An example of the direction I am proposing is Solomon's Social Empiricism. Solomon argues that social empiricism can offer symmetrical explanations for true and false beliefs, which invoke empirical, social, theoretical and cognitive factors (Solomon, 2001: 117–20). For Solomon, empirical success is the main epistemic criterion for evaluating scientific theories (Solomon, 2001: chapter 2). The details of Solomon's account may, of course, be debated. One may wonder, for example, whether empirical success is or should be the main epistemic criterion for theory evaluation in all social contexts. In addition, it is not clear that empirical success is as independent of the social context as Solomon maintains. Nevertheless, the general principles of her overall framework may provide a promising avenue for developing a richer and more robust theory of popularization that accommodates the existence of independent epistemic standards and the ability to distinguish distorted from non-distorted scientific accounts.
32. As Pinch (1985) points out, scientists have a choice about how to put their claims. The more dramatic and less cautious they put them, the more they can gain in terms of reputation and recognition if their claims are ultimately accepted, and the more they can lose if their claims are ultimately not accepted.
33. For example, according to Bloor's influential Strong Programme, the status of logical necessity or a priori knowledge is given to knowledge claims (at least primarily) through social negotiations. Mathematical knowledge that has gained a secure status in the past can be occasionally challenged, and whether it retains its secure status is subject to a collective decision of the relevant epistemic community (Bloor, 1991: 84–156). Moreover, according to Bloor (1984), so-called objective epistemic standards, including mathematical rules of inference, are the intersubjective socially given meanings and categories in a given epistemic community, and are relative to it. Consequently, sociologists should analyse them in terms of the community's social structure and collective social interests.
34. More precisely, the claims are about what a Turing Machine, which is an abstract model of a computer, can do. A Turing Machine is considered equivalent in its asymptotic computational power to a digital computer because a digital computer can simulate a Turing Machine in polynomial time and vice versa (Hopcroft et al., 2001: 355–65).

References

Adler, Jonathan (2007) 'Argumentation and Distortion', *Episteme* 4(3): 382–401. Agrawal, Manindra, Neeraj Kayal & Nitin Saxena (2002) 'PRIMES is in P'. Available at <http://web.archive.org/web/20060721061116/http://www.cse.iitk.ac.in/users/manindra/ primality_original.pdf> (accessed 23 November 2008).

Agrawal, Manindra, Neeraj Kayal & Nitin Saxena (2004) 'PRIMES is in P', *Annals of Mathematics* 160(2): 781–93.

Anonymous (2002) 'New Algorithm by Three Indians', *The Hindu* (9 August). Available at <http://www.hinduonnet.com/thehindu/2002/08/09/stories/2002080901331200.htm> (accessed 23 November 2008).

Anonymous (2003) 'Mathematicians are Discussing Ways to Make Code-Breaking Easier', *The Economist* 366(8317) (29 March): 89.

Beecher-Monas, Erica (2007) *Evaluating Scientific Evidence: An Interdisciplinary Framework for Intellectual Due Process* (Cambridge: Cambridge University Press).

Bloor, David (1984) 'A Sociological Theory of Objectivity', in S.C. Brown (ed.), *Objectivity and Cultural Divergence* (Cambridge: Cambridge University Press): 229–45.

Bloor, David (1991) *Knowledge and Social Imagery,* 2nd edn (Chicago, IL: University of Chicago Press).

Bornemann, Folkmar (2003) ‘PRIMES is in P: A Breakthrough for “Everyman”’, *Notices of the American Mathematical Society* 50(5): 545–52.

Brizon, Uriel (2002) ‘The Prime Numbers Will be Identified, the Code Will Be Broken’, *Haaretz* (19 August): 6. [In Hebrew]

Broks, Peter (2006) *Understanding Popular Science* (Maidenhead, Berks: Open University Press).

Brown, James R. (2001) *Who Rules in Science? An Opinionated Guide to the Wars* (Cambridge, MA: Harvard University Press).

Bucchi, Massimiano (1996) ‘When Scientists Turn to the Public: Alternative Routes in Scientific Communication’, *Public Understanding of Science* 5: 375–94.

Collins, Harry (1983) ‘The Sociology of Scientific Knowledge: Studies of Contemporary Science’, *Annual Review of Sociology* 9: 265–85.

Collins, Harry & Robert Evans (2002) ‘The Third Wave of Science Studies: Studies of Expertise and Experience’, *Social Studies of Science* 32(2): 235–96.

Cormen, Thomas, Charles E. Leiserson & Ronal L. Rivest (2001) *Introduction to Algorithms*, 2nd edn (Cambridge, MA: MIT Press).

Fuller, Steve (1997) *Science* (Buckingham, Bucks: Open University Press).

Galison, Peter (1997) *Image and Logic: A Material Culture of Microphysics* (Chicago, IL: University of Chicago Press).

Giere, Ronald N. (1988) *Explaining Science: A Cognitive Approach* (Chicago, IL: University of Chicago Press).

Giere, Ronald N. & Barton Moffatt (2003) ‘Distributed Cognition: Where the Cognitive and the Social Merge’, *Social Studies of Science* 33(2): 301–10.

Goldman, Alvin L. (1999) *Knowledge in a Social World* (New York: Oxford University Press).

Gomes, Lee (2002) ‘A Beautiful Mind from India is Putting the Internet on Alert’*, The Wall Street Journal* (4 November): B1.

Gregory, Jane & Steve Miller (1998) *Science in Public: Communication, Culture, and Credibility* (New York: Plenum Press).

Haack, Susan (2003) *Defending Science – within Reason: Between Scientism and Cynicism* (Amherst, NY: Prometheus Books).

Hilgartner, Stephen (1990) ‘The Dominant View of Popularization: Conceptual Problems, Political Uses’, *Social Studies of Science*, 20(3): 519–39.

Hopcroft, John E., Rajeev Motwani & Jeffrey D. Ullman (2001) *Introduction to Automata Theory, Languages, and Computation*, 2nd edn (Boston, MA: Addison-Wesley).

Hughes, Jeff (2007) ‘Insects or Neutrons? Science News Values in Interwar Britain’, in Martin W. Bauer & Massimiano Bucchi (eds), *Journalism, Science and Society: Science Communication between News and Public Relations* (New York: Routledge): 11–20.

Junnarkar, Sandeep (2002) ‘Prime Efforts May Boost Encryption’, *CNET News.com* (9 August). Available at <http://news.net.com/Prime-efforts-may-boost-encryption/2100- 1009_3-949170.html?tag=mncol> (accessed 14 January 2009).

Kingsley, Danny (2002) ‘A Prime Result’, *ABC Science Online* (14 August). Available at <http://www.abc.net.au/science/news/stories/s647647.htm> (accessed 23 November 2008).

Kusch, Martin (2002) *Knowledge by Agreement: The Programme of Communitarian Epistemology* (New York: Oxford University Press).

Lewenstein, Bruce V. (1995) ‘From Fax to Facts: Communication in the Cold Fusion Saga’, *Social Studies of Science* 25(3): 403–36.

MacKenzie, Donald A. (2001) *Mechanizing Proof: Computing, Risk and Trust* (Cambridge, MA: MIT Press).

Michael, Mike (1996) ‘Ignoring Science: Discourses of Ignorance in the Public Understanding of Science’, in Alan Irwin & Brian Wynne (eds), *Misunderstanding Science? The Public Reconstruction of Science and Technology* (Cambridge: Cambridge University Press): 107–25.

Odlyzko, Andrew (2003) ‘Alternatives to Peer Review I: Peer and Non-Peer Review’, in Fiona Godlee & Tom Jefferson (eds), *Peer Review in Health Sciences*, 2nd edn (London: BMJ Books): 309–11.

Phillips David P., Elliot J. Kanter, Bridget Bednarczyk & Patricia L. Tastad (1991) 'Importance of the Lay Press in the Transmission of Medical Knowledge to the Scientific Community', *New England Journal of Medicine* 325 (17 October): 1180–83.

Pinch, Trevor (1985) 'Towards an Analysis of Scientific Observation: The Externality and Evidential Significance of Observational Reports in Physics', *Social Studies of Science* 15(1): 3–36.

Pradhan, Aharat (2002) 'IIT Professor Makes Prime Mathematics Breakthrough', *Rediff.com* (10 August). Available at <http://www.rediff.com/news/2002/aug/10prime.htm> (accessed 23 November 2008).

Rajghatta, Chidanand (2002) 'India Still Has the Number on Maths', *The Times of India* (12 August). Available at <http://timesofindia.indiatimes.com/articleshow/18891466.cms> (accessed 23 November 2008).

Ramachandran, R. (2002) 'A Prime Solution', *Frontline: India's National Magazine* 19(17) (17 August). Available at <http://www.flonnet.com/fl1917/19171290.htm> (accessed 23 November 2008).

Robinson, Sara (2002) 'New Method Said to Solve Key Problem in Math', *The New York Times* (8 August): A20.

Silva, Michelle R. (2005) 'The Aerodynamics of Insects: The Role of Models and Matter in Scientific Experimentation', *Social Epistemology* 19(4): 325–37.

Simon, Bart (2001) 'Public Science: Media Configuration and Closure in the Cold Fusion Controversy', *Public Understanding of Science* 10(4): 383–402.

Sipser, Michael (1997) *Introduction to the Theory of Computation* (Boston, MA: PWS Pub.).

Solomon, Miriam (2001) *Social Empiricism* (Cambridge, MA: MIT Press).

Sommer, Marianne (2006) 'Mirror, Mirror on the Wall: Neanderthal as Image and "Distortion" in Early 20th-century French Science and Press', *Social Studies of Science* 36(2): 207–40.

Stiglic, Anton (2005) 'The PRIMES is in P little FAQ'. Available at <http://www.instantlogic.net/publications/PRIMES%20is%20in%20P%20little%20FAQ.htm> (accessed 23 November 2008).

Tassa, Tamir (2002) 'With all Due Respect to the Deterministic Algorithm in Polynomial Time, the Code Will not Be Broken', *Haaretz* (26 August): 6. [In Hebrew]

Thompson, Clive (2002) 'Outsider Math', *The New York Times Magazine* (15 December): 107.

Tucker, Aviezer (2003) 'The Epistemic Significance of Consensus', *Inquiry* 46(4): 501–21.

Väliverronen, Esa (1993) 'Science and the Media: Changing Relations', *Science Studies* 6(2): 23–34.

Whitley, Richard (1985) 'Knowledge Producers and Knowledge Acquirers: Popularisation as a Relation between Scientific Fields and Their Publics', in Terry Shinn & Richard Whitley (eds), *Expository Science: Forms and Functions of Popularisation, Sociology of the Sciences Yearbook,* vol. 9 (Dordrecht & Boston, MA: Reidel): 3–28.

Wynne, Brian (1996) 'Misunderstood Misunderstandings: Social Identities and the Public Uptake of Science', in Alan Irwin & Brian Wynne (eds), *Misunderstanding Science? The Public Reconstruction of Science and Technology* (Cambridge: Cambridge University Press): 19–46.

Boaz Miller is a PhD student at the Institute for the History and Philosophy of Science and Technology (IHPST), University of Toronto. He received an MA at IHPST and a BSc in Computer Science and 'Amirim' Interdisciplinary Honors Program from the Hebrew University of Jerusalem. He works in the areas of philosophy of science and social epistemology.

Address: IHPST, University of Toronto, 316 Victoria College, 91 Charles Street West, Toronto, Ontario, Canada M5S 1K7; email: boaz.miller@utoronto.ca; website: http://individual.utoronto.ca/boaz