the emphasis, capitalization, and spelling of the original):

> Indeed, what happened with the Random Oracle Model reminds us of the biblical story of the Bronze Serpent, reproduced next. (See *Numbers* (21:4-8) and *2 Kings* (18:4).) During the journey of the People of Israel in the dessert, the prophet-leader Moses was instructed by the Lord to make a "fiery serpent" as a symbolic mean for curing people that have been bitten by snakes (which were previously sent by the Lord as a punishment for some prior sin). Several hundred years later, the bronze serpent made by Moses has become an object of idol worship. This led the righteous King Hezekiah (son of Ahaz) to issue an order for breaking this bronze serpent to pieces. Let us stress that the king's order was to *destroy an object that was constructed by direct instruction of the Lord*, because this object has become a fetish. Furthermore, this object no longer served the purpose for which it was constructed. This story illustrates the process by which a good thing may become a fetish, and what to do in such a case…. [G]iven the sour state of affairs, it seems good to us to abolish the Random Oracle Model.

Goldreich sees himself as a twenty-first-century righteous King Hezekiah defending the provable security researchers against infidels and post-modern fetishists such as Menezes and me. It is clear from his essay that he had not read our paper carefully before writing his response; nor does he seem to have been aware of our other two posted papers criticizing provable security. But of course it was not necessary to actually read the technical details in our three articles in order to denounce us on religious and philosophical grounds.

The angry reactions of a few researchers who seem to perceive our work as a threat to their interests are not the type of thing one normally encounters in theoretical mathematics, where usually the only issues that could cause someone to object to a paper would be an error or omitted acknowledgment of earlier work (neither of which has been found in any of our three papers on "provable security"). But far from being bothered by the accusations made by Goldreich and others, I am encouraged by them, because they at least show that people are paying attention.

Cryptography has the excitement of being more than just an academic field. Once I heard a speaker from NSA complain about university researchers who are cavalier about proposing untested cryptosystems. He pointed out that in the real world if your cryptography fails, you lose a million dollars or your secret agent gets killed. In academia, if you write about a cryptosystem and then a few months later find a way to break it, you've got two new papers to add to your résumé!

Drama and conflict are inherent in cryptography, which, in fact, can be defined as the science of transmitting and managing information in the presence of an adversary. The "spy vs. spy" mentality of constant competition and rivalry extends to the disciplinary culture of the field. This can get to be excessive—and even childish at times—but it also explains in part why it can be so much fun to do research in cryptography.