Professor Adi Shamir, Hon DSc

Wednesday, 18 January 2023, am

Chancellor:

I am delighted to introduce our honorary graduand this morning, one of the founders of modern cryptography: PROFESSOR ADI SHAMIR.

Professor Shamir is one of the most respected cyber security researchers in the world. It was in 2016, while he was acting as a high level scientific advisor in cyber security to the European Commission, that he met Professor Maple, who leads the University's EPSRC-NCSC Academic Centre of Excellence in Cyber Security Research. Given that Adi has spent most of his academic career in his home country, Carsten felt he should explain that while the University of Warwick was only just over 50 years old it was recognised as a leading global institution. Adi's response was simply "I know; you do know that I was at Warwick, Carsten?" Carsten was aware of the great work that had taken place in mathematics and cryptography since the 1970s, but until this point was unaware of Adi's time here.

Professor Shamir completed his BSc in Mathematics at Tel Aviv University in 1973, and his MSc and his PhD in Computer Science at the Weizmann Institute in Israel (where he is now Borman Professor of Computer Science). It was after this, in 1976, that he came to Warwick as a post-doctoral researcher, supervised by Professor Mike Paterson in the Computer Science Department.

The following year, he left Warwick for MIT and it was here, in 1977, that his most famous invention took place. Together with colleagues

Leonard Adleman and Ronald Rivest, Professor Shamir invented the Rivest-Shamir-Adleman (RSA) algorithm – still the best known and commonly used public key encryption and signature scheme, enabling us, for instance, to shop online safely using our credit cards. The three colleagues subsequently founded the RSA Data Security Company, which was bought by EMC in a multi-billion dollar deal in 2006. Of course, it's very common for academic ventures to be traded in multi-billion dollar deals!!

Despite the significance of his work with Rivest and Adleman, Adi did not rest on his laurels. His sole-authored work on how to share a secret in 1979 has garnered over seventeen and a half thousand citations, and is the basis of some of the work being undertaken by researchers at the University and at the Turing Institute, in collaboration with HSBC. In 1984 Professor Shamir presented a new cryptographic scheme, that enabled any pair of users to communicate securely and to verify each other. This work has also left an indelible mark on the research landscape and has attracted almost ten thousand citations. Over dinner in Vilnius at the aforementioned European Commission advisory group meeting, Adi had mentioned to Carsten some new joint work that identified and exploited a vulnerability in the Phillips Hue smart lightbulb that was about to be published. Carsten gave this some thought and explained that perhaps this attack might be able to be executed at scale – of course Professor Shamir and his co-authors had thought of this and had used a standard drone, flown hundreds of metres away from office buildings, which forced all the Hue lamps installed in them to blink SOS in morse code! His research achievements are too numerous and wide-reaching to mention here, but his contributions continue to this day. Indeed earlier this week he presented some new joint work to researchers at the University which involves compromising facial recognition systems. Making a small fraction of the weightings in the system creates errors only on specific persons which are preselected by the attacker, with almost no effect on the correctness of its decisions for

other persons. In the work they explained that they had manipulated a system so that Morgan Freeman and Scarlett Johansson were declared to be the same person more than 90% of the time, without reducing the network's accuracy on everyone else. It's not often, based upon appearance, people fail to distinguish these two actors!

Professor Shamir's groundbreaking research has earned him a host of prizes and honours, in Israel and internationally: for example, the Vatican Pontifical Academy Pius XI Gold Medal, 1992; the Turing Award (with Adelman and Rivest) in 2002, and in 2017, the 33rd Japan Prize in the field of electronics, information and communication. He was elected to the Israeli Academy of Science in 1998, the US National Academy of Science in 2005 and as a Foreign Member of the Royal Society in 2018. He holds honorary degrees from the Ecole Normale Supérieure and the University of Waterloo. He visited us here in 2019 to give a number of talks to students and faculty, as well as participating in a conference. The graduate research students were particularly grateful for the time and interest provided by Professor Shamir, and have commented on how useful the advice received had been. It is a testament to Adi's approachability that he gave so much of his time so freely to these students embarking on their career. So for all of us working in this field, and his contribution to and influence on the work at Warwick, it is a particular pleasure to welcome Professor Shamir back today.

Chancellor: in the name of the Senate, I present to you for admission to the degree of Doctor of Science, *honoris causa*, PROFESSOR ADI SHAMIR.