What I have kept in mind while selecting the papers to retell was that, firstly, you as a listener learn something new or interesting along the way, and secondly, having constructed these short reviews, I also understand the concepts the authors are covering better. The topic of my personal research touches upon the subject of so-called zero-knowledge proofs, which is a mathematical construct that allows one to prove possession of some secret or property without revealing any details about this secret or property. Say, for instance, you are at the bar and the bartender asks if you are 18 or not. In a typical scenario you would most likely take out your passport or ID-card and show it to them, but, as you may understand, you are giving away much more information, than is necessary, such as your birthdate, for example. Zero-knowledge proofs provide you with a way to prove to the bartender that you are indeed 18 revealing nothing but the fact, or, as I would say, revealing only a single bit of information: true or false, over 18 or under 18. Just to be clear, you would give a bartender some proof, they will look at it and either accept or reject it. And the key that makes it all possible, which is discussed in the papers to come, is that you allow the bartender to make a mistake, meaning accepting you when you are under 18, but only with a very small probability. Think of numbers like ten to the minus twenty.

The first paper is entitled "The Knowledge Complexity of Interactive Proof Systems" released in 1989, a seminal work by the three authors: Shafi Golwasser, Silvio Micali and Charles Rackoff, who have basically with this paper laid the foundation of the zero-knowledge proofs to be. The authors explain the intention behind and give the definition of the notion of interactive proof systems and emphasize the importance of probability in cryptographic protocols, representing these systems. The authors provide us with comprehensive analysis of the previous work done in the field, and discuss examples of interactive proof systems for various mathematical tasks, mostly proving some number properties, which is typical for cryptography as it relies heavily on probability and number theories. A full description of a particular zero-knowledge proof for a special property of a number, called quadratic residuosity, is presented and thoroughly analyzed in a separate section. This particular number property is what we would classify as "not efficiently recognizable", which basically means that no computer can deterministically decide if a number has this property or not, and the authors thus were

first to construct a zero-knowledge proof for a property which is not known to be efficiently recognizable.

The second paper I would like to discuss is a 2019 paper by Ariel Gabizon, Zachary J. Williamson and Oana Ciobotaru titled "PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge". The authors present what's called a SNARK construction, which expands to Succinct Non-interactive ARgument of Knowledge. Basically, SNARK is the more precise name for a notion of proof I was talking about earlier, and the authors provide a concrete construction for such proof and call it PLONK. This paper is of particular interest primarily because PLONK along with its variations is one of the most widely deployed SNARKs today. Back to the paper, the authors first give a brief analysis of their protocol, which shows advantages of the protocol over its predecessors along with some useful metrics, such as time needed to construct a proof, and head right to mathematics underlying the protocol. The article is pretty descriptive in that every lemma comes with its proof and there are a lot of lemmas. The authors wrap up with a complete description of the protocol which utilizes all mathematical methods acquired up to this point.

In conclusion I'd just say that you may think what I'm talking about in this review is not applicable to our today's life. But remember: these exact techniques are already being used in many-many voting systems all over the world, not to say about its heavy use is cryptocurrencies, such as Ethereum or Monero. The two papers I have chosen to review play very important role in the development of ways to algorithmically prove arbitrary statements without revealing any information but what is being proven. And also, please note that I have left out an enormous amount of detail and used a lot of simplifications in order to keep my message clear during the retelling. Thank you.