Analysis of Human Identification Protocols

Josef Pieprzyk, Queensland University of Technology

Human identification protocols are challenge-response protocols that rely on human computational ability to reply to random challenges from the server based on a public function of a shared secret and the challenge to authenticate the human user. One security criterion for a human identification protocol is the number of challenge-response pairs the adversary needs to observe before it can deduce the secret. In order to increase this number, protocol designers have tried to construct protocols that cannot be represented as a system of linear equations or congruences.

In the talk, we take a closer look at different ways from algebra, lattices and coding theory to obtain the secret from a system of linear congruences. We then show examples of human identification protocols from literature that can be transformed into a system of linear congruences. The resulting attack limits the number of authentication sessions these protocols can be used before secret renewal.