Popular Science Summary

When you make a phone call to someone, what you said will be transmitted from your mobile phone through the open air to a base station, and the base station forwards the messages to the one you want to talk to. I believe that you do not want your talk heard by any third person, no matter he is malicious or just curious. The weakest sub-link along the message transmission path lies over the air, as it is open to everyone and a malicious or curious person, let us call him an attacker, may be able to eavesdrop or even manipulate your talk. As a consequence, the messages should be specially protected over the air to ensure that the attacker will know nothing even if he captures the messages, and not be able to manipulate the messages without notice. Such a goal is achieved by encrypting your messages and adding special tags using some specific cryptographic algorithms, also called ciphers.

There are three standardised ciphers used in 4G for this purpose, named AES, SNOW 3G, and ZUC. All people (with mobile phones) around the world are using (at least one of) these three ciphers, though they might not notice it: these ciphers are typically put into the devices during the manufacturing phase and the encryption is performed automatically by the devices. AES, SNOW 3G, and ZUC provide sufficient security and speeds in 4G for protecting our message transmission.

How about the situation in 5G?

When we come to 5G, the innovate network architecture and high performance demands introduce higher requirements on these ciphers. Firstly, they should be more secure since attackers in the future can potentially have very strong capabilities and can possibly recover your messages, due to the development of quantum computing. Moreover, these ciphers should run much faster in some specific environments since we will be able to enjoy much higher speeds in 5G. Therefore, it is crucial to investigate whether the ciphers we are using today (in 4G) can satisfy these new requirements; and if necessary, design new ones particularly targeting these goals. This is exactly the primary motivation and content of this thesis.

What we did?

Analysing Existing Ciphers. We investigated the security of two of the three ciphers that we are using today in 4G, i.e., SNOW 3G and ZUC, to check if they can satisfy the new security requirements in 5G. We found some theoretical attacks against them, which

provided some reference information to the standardisation organisation (i.e., 3GPP) for choosing good candidates for 5G. But we do not have to worry about these attacks at this moment, because their costs are much beyond an attacker's practical capability today, and furthermore, the attacker will not be able to get enough data for launching such attacks.

Designing New Ciphers. We also designed new ciphers, called SNOW-V and SNOW-Vi as an extreme performance variant, particularly targeting the 5G requirements regarding security and speeds. They can be viewed as successors of SNOW 3G but with much stronger security and higher speeds. They have been submitted to the standardisation organisation for consideration of usage in 5G, and they are currently under evaluation.

Analysing Local Pseudorandom Generators. When using ciphers for encryption or more advanced applications, some random numbers are usually needed. You might think from the intuition that it is easy to generate a random number, but it is actually not so for an electronic device. There are special cryptographic constructions called pseudorandom generators (PRGs) for achieving this goal. We investigated the security of one particular type of PRGs that are very efficient in implementation, which are called local PRGs. We developed some analysis methods that can help choose secure parameters if these PRGs were to be used in practice.