Noname manuscript No.
(will be inserted by the editor)

AES and SNOW 3G are feasible choices for a 5G phone from energy and throughput perspective

Mohsin Khan · Valtteri Niemi

Received: date / Accepted: date

Abstract The aspirations for a 5th generation (5G) mobile network are high. It has a vision of unprecedented data-rate and extremely pervasive connectivity. To cater such aspirations in a mobile phone, many existing efficiency aspects of a mobile phone need to be reviewed. We look into the matter of required energy to encrypt and decrypt the huge amount of traffic that will leave from and enter into a 5G enabled mobile phone. In this paper, we present an account of the power consumption details of the efficient hardware implementations of AES and SNOW 3G. We also present an account of the power consumption details of LTE protocol stack on some cutting edge hardware platforms. Based on the aforementioned two accounts, we argue that the energy requirement for the current encryption systems AES and SNOW 3G will not impact the battery-life of a 5G enabled mobile phone by any significant proportion.

Keywords 5G · Cryptosystem · ASIC

1 Introduction

To facilitate our discussion, we need to know what are the data that will be encrypted and decrypted in a 5G phone. We also need to know where and how many times the encryption and decryption will take place across the protocol stack on the phone. But 5G is not yet a reality. We do not have exact answers to these questions. So, we assume things that will still be applicable in a 5G network and argue on the basis of these assumptions. We turn to the LTE network to make the assumptions. In an LTE phone, the data that leave and enter the phone can be broadly classified into three categories. The first one are the control signals in between the phone and the core network. The second one are the control signals in between the phone and the radio network. And the third one are the user data which the user sends from and receive at it's application layer. Both of the first two categories are both privacy and integrity protected. For the third category, only the privacy is protected. Also note that, from volume point of view, the bulk share of data belong to the third category. And comparing to the the third category, the cryptographic computational need required for the data of first and second categories is negligible. And the user data in an LTE phone is only once encrypted and decrypted across the protocol stack in PDCP layer. In an LTE phone this encryption is done an ASIC. For a 5G phone, we assume that the user data will remain as the major share of the total data leaving and entering the phone. And the cryptographic computational need for the total amount of control signals will be negligible in comparison with that of user data. And that the user data will only once be encrypted somewhere across the protocol stack. From hardware point of view it will be in an ASIC. In order to have a pessimistic estimation, we assume that integrity protection of user data will be introduced in 5G. Based on these assumptions, we will look into the cryptographic energy requirements and also the total energy requirements across the whole protocol stack. Then we will scale up the data-rate from 100 Mbps to 1 Gbps and see how much extra pressure it puts on the battery of the phone in comparison with other energy hungry aspects of the phone like display and radio signalling.

Mohsin Khan
University of Helsinki
E-mail: mohsin.khan@helsinki.fi

Valtteri Niemi
University of Helsinki
E-mail: valtteri.niemi@helsinki.fi

According to [1], there are two encryption schemes in the 4th generation cellular network (LTE) developed by 3GPP. One is EEA1 in which the stream cipher SNOW 3G is used. The other is EEA2 in which the block cipher AES is used. According to the LTE architecture, there are three different connections are two encryption systems used to encrypt the user data traffic in 3GPP-defined cellular networks across the radio layer. As the data rate of the cellular networks has increased steadily throughout the history of the networks, researchers have focused on implementing these cryptosystems both in hardware and software to achieve the required throughput. Looking up in the existing literature, it has been found that there exists implementations of these two cryptosystems that can achieve the required throughput even for a 5G network, that is at least 1 Gbps. However, there is no concrete account available of the power consumption of these implementations that enables the readers to estimate the energy share of the task of encryption across the entire protocol stack. We have studied, collected and rendered the relevant information available in the literature into this single article in an easily comprehensible and comparable manner and make a case that the energy share of data encryption is too low to think of any alternative lightweight encryption for 5G enabled mobile phone.

2 Encryption is time consuming

It has been identified that encryption is the most time consuming process across the downlink (DL) of layer 2 (L2) in a mobile phone when traditional hardware acceleration concepts have been used. In a study [**?**] published in 2009, the authors in their experiment have found that 68 percent of the execution time spent in the L2 DL in LTE phone was consumed by deciphering when AES has been used considering the state-of-the-art mobile platform of the time. They also showed that instead of traditional hardware acceleration concepts more sophisticated hardware accelerators for the L2 are needed to supply enough computational power required in LTE and next generation mobile devices. However, they do not give any account of the case where SNOW 3G has been used. Nevertheless, other studies suggest that AES and SNOW 3G has very similar kind of throughput properties in the state of the art implementations. In a study in [**?**] conducted in 2010 on the L2 DL layer (MAC,PDCP,RLC) layer, it has has been shown that by an sDMA, the authors did not mention anything about the achieved throughput but said that, it is enough for an LTE terminal. However, to achive this required throughput, the implementation consumed 9.5 mW of power whereas AES and SNOW 3G each required .5 and .57 mW of power respectively. Which means the encryption/decryption consumes around 5 percent of the power budget of L2 DL. (see in figure 6)AES

Whereas, a very recent study done in 2014, presented in [**?**], conducted on the UDP/IP layer, shows that (in Table II) an ASIC implementation consumes 14.62 nano Joule of energy for a Kilobyte data in this layer. Which means it takes $(14.62/8) * 1000 = 1827$ micro Joule of energy for 1 Giga bit data while providing throughtput of 2.24 Gbps.

3 AES

Since the adoption of Rijndael as AES by NIST, there have been number of hardware implementations of AES to achieve efficiency and high throughput. The below table gives a picture

So far the best power figure is found in [**?**]. The implementation is scalable. Interestingly the power figure doesn't increase linearly with the number of AES engines used. Let us assume that the required data rate in 5G is 1 Gbps. So, the timing requirement is: 7.45 nano seconds per byte.

According to figure 9 in [**?**], it will take roughly $.02 * 5 = .1mW$ for 1Gbps throughput. Because SAME has throughput of 114Mbps. And it achieves $5.5Mbps/\mu J$. Which means it spends $114/5.5 = 20.72\mu J = .02mW$. Now, by scaling up by 10 times, it will spend $.02 * 10 = .2mW$ to achieve 1.14Gbps throughput

Comparing the best figure from the above table with [**?**], we see that ciphering takes $186/1827 = .1$ or 10 percent energy of data communication on a ASIC packet processor.

In the study in [**?**], it was found that encryption was taking 5 or 6 percent of the power budget. However, as because other aspects of the protocol stack could be made more efficient, the power budget of encryption/decryption has increased.

So, with the current best implementation of the encryptor/decryptor hardware engine, in near future the power budget will only increase. However, now we need to check if 10 percent of the power budget for encryption will be good enough for a 5G phone or not.

References

1. 3GPP, Article title, Journal, Volume, page numbers (year)
2. Author, Article title, Journal, Volume, page numbers (year)
3. Author, Book title, page numbers. Publisher, place (year)