AES and SNOW 3G are not too Heavy for 5G Mobile Phones

Mohsin Ali Khan, Valtteri Niemi
Department of Computer Science
University Of Helsinki
Helsinki, Finland

November 10, 2016

Abstract

An account of the power consumption details of the cutting edge hardware implementations of AES and SNOW 3G is presented. It also gives an account of the power consumption details of LTE protocol stack on some cutting edge hardware platforms. It shows from the aforementioned accounts that the current encryption systems SNOW 3G and AES will not pose any significant threat of too high energy consumption to achieve the required 1 Gbps data rate in a 5G mobile phone.

1 Introduction

EEA1 (SNOW 3G) and EEA2 (AES) 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 not too high 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)

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

AES Implementations									
Year	Tech	Ref	TP (Gbps)	Gates (K)	Clock Speed (MHz)	Power (mW)	Scalable (Y/N)	Throughput per Kilo Gates in Gpbs	Energy per Gbit in μJoule
2001	.11μ	[**?**]	2.6	21.3	0	-	Y	0.122	-
2001	.11μ	[**?**]	.311	5.4	0	-	Y	0.0576	-
2001	-	[**?**]	.24	4	0	-	Y	0.06	-
2006	.18μ	[**?**]	.570	-	48	20.34	Y	-	35684
2006	.35μ	[**?**]	.569	-	48	192.5	Y	-	338312
2007	.18μ	[**?**]	.384	21	120	-	Y	0.018	-
2009	.18μ	[**?**]	1.16	19.47	-	-	Y	0.056	-
2009	.09μ	[**?**]	1.86	15.25	450	.78	Y	0.015	419
2011	–	[**?**]	.114	–	300	.02	Y	-	186.18
2012	.18μ	[**?**]	1.6	58.445	125	22.85	Y	-	14281

So far the best power figure is found in [**?**]. The implementation is scal-

able. 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.