I choose this dissertation for the reason of interest in Network Security Attack/Defense. The topic I want to talk about here is the "cost of attack and defense",which closely related to Security technology onto FPGA in my understanding。

In the Security Technology(EE5815),we learned a lot of algorithms and Number Theory about security technology. But as the study progressed, I gradually realized that security technology is not just create generation gap simply in technology,theory or principle.We have to consider comprehensive costs and even off-site factors.After all, the encryption algorithm is not "unbreakable", but the current computing power and algorithm is “not fast enough to break".

In the same era, the superiority of the algorithm on the defensive side of the mechanism is more important.Even if the defender's information gap advantage is eliminated, for example, the British caught the Enygma cipher machine of German,the attacker was still need time to follow in technologies, so a more flexible mindset was needed to compensate.After all, blue team defence against for all loophole of a house in general rather red team can win by seeking for just one .Take《The Imitation Game》as example，a film based on historical facts of World War II.Even with such a large cost and genius designed machine,”Christopher”,In the end, it was also cracked with the help of the German army's correspondence habits,which in fact a loophole in human nature rather than crush in machine performance.

Well, from the story,naturally we can find common features between information confrontation and frontal battlefield confrontation in the form of many competitions .In my view,algorithms for network offense and defense just like the tank in the Soviet-German rivalry. The cost effectiveness differentiation between offense and defense ,or the capacity of the offensive and defensive can reach taking the most limelight.

This shows that all Encryption algorithms will be broken in acceptable time(or evolve to some extent) with the the development of information technology and the increase of computing power .No matter it is asymmetric encryption,which achieve security in mechanism on the idea of a brilliant algorithm,in fact depend on characteristics of “K=g^xy mod p” in mathematics,which created a One-way trap door,Or just about something relatively easy to understand like Caesar or Polyalphabetic cipher.

Take DES and 3DES for example,which is proven that there is a possibility of breakthrough by recent computing power,will be Improved algorithm performance immediately.And means be replaced soon.We are always looking for more secure algorithms .

All this example are taken to explain that individual technical barriers and advantages can create local temporary advantages.Actually, confrontation is the sum of Hacker and Net Security competition in the cost of computing power/economically/time/number of devices .how much offensive and defensive capacity can be created in the same cost?That’s should be the important things.

In that case,the appeal of this dissertation for me is obvious.Based on the above mentioned,hardware acceleration of security algorithms on different function with dedicated circuits implemented by FPGA design,such as hashing,encryption ,digital signature scheme and so on.Then there is no doubt that we can decrease the cost of Offensive and Defensive in security.I believe that the experience in this dissertation will contribute to my comprehensive understanding in security algorithms as well as attack/defense.

To sum up the above,I’m very interested in the technology details in realizing these specific functions and want to try this dissertation.

What’s more,some experience and fundamental knowledge seems brings me some advantages in this topic,and thanks to Communication Engineering,I think I own a better frame mind in the different layer when learning and designing the Processor.

During the dissertation,I aims to improve research ability and enrich research experience in preparation for future PhD applications of destination Institution.So I want to apply for a position of RA to enhance my experience in security research especially in network attack/defense after graduation with dissertation completed.