**IMPLEMENTATION OF SYMMETRIC ALGORITHM MODIFICATION SYSTEM TO RESIST POWER BASED SIDE CHANNEL ATTACKS**

Project ID: 17-044

Individual Component Abstracts

Pathirana K.P.A.P Hangawaththa N.H.A.D.A  Lankarathne L.R.M.O

March 2017

B.Sc. Special (Honors) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

Member: Pathirana K.P.A.P

**Device implementation for extracting power consumption measurements**

The objective of this component is to implement a physical device that will enables us to take the power consumption readings from a particular target chip while it executing a cryptographic algorithm. An algorithm will be developed to take the power consumption reading to a computer by converting them in to digital files. The device will be based on the board arduino and board FPGA, and by connecting these parts, an AtMega8-16PU chip, AVR programmer, and couple of 22pF 680uF capacitors and 100 ohm resistors which will be able get the power consumption readings from the target chip. After that implementing algorithm on arduino environment, we can get the readings to a computer in a digital form. The final output of this component is to get a visual representation of the power consumption which indicate the power spike patterns of that particular cryptographic algorithm.

Member: Hangawaththa N.H.A.D.A

**Data classification, analysis and module training using machine learning**

The objective of the second component is to come up with a system which is fine-tuned to identify potential vulnerabilities in a cryptographic algorithm and suggests appropriate countermeasures which adds randomness to the identified patterns by analyzing the meter readings of the side channel information. Extracted power consumption measurements are first classified by selecting th subset of all available data in a linear manner procedure. All the data is preprocessed by formatting, fixing wrong data and sampling methods. Processes data is transformed to appropriate machine learning styles using techniques such as scaling, attribute decomposition and attribute aggregation. Using supervised and unsupervised learning styles, system is trained fluently to obtain the most accurate and reliable solution for the identified vulnerability. By using machine learning algorithms in similarity in functions such as regression, Bayesian and clustering, the final output is to improve the precision of the countermeasures for the identified vulnerabilities.

Member: Lankarathne L.R.M.O

**Automate Code embedding mechanism using machine learning and Artificial intelligence**

The objective of this component is to develop an automated mechanism to add suitable modifications to the analyzed algorithm according to the suggested countermeasures from the trained data analysis module. For this task we use machine learning techniques, AI techniques and expect to use open source tools like hadoop and shogun to achieve this task. Both supervised and unsupervised techniques will be used, supervised will enables us to get solutions from past learn data which means by deriving them from analyzed power consumption data in the past, while unsupervised will derive inferences from datasets and also to apply those suggested modification to the algorithm automatically. For the automation part, Artificial intelligence techniques are used to generate the required code to append to the algorithm. The expected outcome of the component is to give out an algorithm which will be able to resist side-channel-attacks while providing the same output (encrypted data) from the algorithm same as before.