Final Project Report

Reports must be 6 pages in length, following the IEEE conference format. I recommend writing the report using LaTeX or similar system. Overleaf.com is handy for collaboration on the report.

Reports should include (tentative grade distribution):

1) Introduction, motivation, problem statement (5%)
2) Background, including references to relevant literature (10%)
3) Methodology, e.g. proposed architecture of the hardware or software tool you developed, algorithms used, etc. (40%)
4) Results (this will be specific to your project; if unsure what to include, consult Prof. Karam) (25%)
5) Discussion / conclusion (10%)
6) Novelty and presentation (organization, flow, grammar, etc.) (10%);

Will format later

I. INTRODUCTION

The concept of using the randomness of physical events as a security measure is present anywhere from the biometrics of a fingerprint to using lava lamps for encryption cite. Physically Unclonable Functions, hereafter referred to as PUFs, extend this concept into the field of hardware security.

A PUF is based on a physical system that's easy to evaluate and produces an output that looks like a random function, making it unpredictable even for an attacker with physical access. Due to variations in the process integrated circuits contain sufficient path delays to allow this variance to be used for identification purposes. This means there are no integrated circuits that would produce exactly identical responses to a given challenge cite.

In 2017 Intrinsic ID stated that it was working on BROADKEY, an attempt at hardware intellectual property protection using software alone. The purpose of this was to "secure the Internet of Things" without the need for security dedicated chips, allowing it to be installed at any point in the supply chain or even be retrofitted onto deployed devices cite. The chief executive officer of Intrinsic ID elaborated