1. List of team members.
Sathya Kanth Vardhanapu

2. The exact title of your project (it can be different than a corresponding project topic proposed by the instructor; it should take into account the exact scope of your project).
Anti-Counterfeiting of Integrated Circuits: RFID Tags as a Countermeasure

3. Introduction and motivation. Placement of the problem in the broader research area. Why is this project worth working on? Why is it original? Why is it practical?
To counterfeit means to make an imitation or copy of something and pass it off as the genuine piece. This is a prevalent problem, in the sense that it is done with various products ranging from electronics, clothes, vehicles, and any form of a consumer product. Counterfeiting is primarily:

- Imitating without obtaining permission or rights from the original manufacturer.
- Not following the standards set by the original manufacturer, in terms of performance, design and other factors.
- Producing a good, and labelling it as 'By Original Company' while it isn't from the original company.
- A defective product or a used product scrapped by the original manufacturer sold by the counterfeiter after modification as a new or a working model.

There are various ways to define counterfeiting, but either way it is of major concern to the security of the device and the consumers. "An Integrated Circuit is a semiconductor wafer on which thousands or millions of tiny resistors, capacitors, and transistors are fabricated.", as taken from Wikipedia. In terms of security and counterfeiting, the primary focus is on software. Then we have the hardware, which is usually taken for granted. As once the hardware is compromised, most people wouldn't notice it or wouldn't consider that this is one area of major concern which could compromise security.

Security threats to ICs are primarily done in terms of Counterfeiting, Reverse Engineering, and Tampering. For instance, Peter Picone, a resident of Massachusetts was caught selling counterfeit ICs which were indirectly to be used in US Navy submarines. This is a matter of national security, which endangers the lives of millions of people. Counterfeiting can be countered by using RFID tags. RFID tags are usually low cost devices. The general idea being that RFID tags are used to identify products. As in they are primarily used as an authentication method. An RFID tag comprises of an antenna, a tag-chip, and a memory unit. Also, many approaches have already been discussed or covered in the software domains. There are relatively fewer resources for security attacks in Hardware domains. One of the first steps to anti-counterfeiting is detection, which means the identification of a device, if it is genuine or not. With the aid of RFID tags, this is possible. As there have been many attempts before, and not many successful, each catering to anti-counterfeiting of one or two types of counterfeit ICs. An analysis made in terms of current implementations and various detection methods and prevention and protection measures would be of use to research and contribute in terms of a safer digital world.

4. List of alternative solutions (protocols/algorithms/implementations) you are planning to explore.

I would look at the following:
a. Various ways in which RFID tags are used for Anti-Counterfeiting.
Any other implementations by semiconductor companies.

5. Tentative list of evaluation criteria.
a. Complexity
b. Costs
c. Current implementations by semiconductor companies
d. Efficiency
e. Vulnerabilities
g. Implementation security.
h. Type of technology implemented on.
i. Risk factor based on where Counterfeiting is done in ICs.

6. Mutual dependencies among various evaluation criteria.
Mutual dependencies would be based on the types of IC counterfeiting and severity of the risk involved the techniques proposed might vary. There might be certain trade-offs.

7. Detailed description of problems/hypotheses you are planning to investigate.
Counterfeiting of ICs: How it is done, and in what are the types.
Semiconductor companies: What are the major problems the semiconductor companies face with counterfeiting of ICs?
Preventive measures: Assuming that there is prior knowledge of how the attacks will be made. Listing and detailing preventive measures.
Detection measures: To detect after an attack is made or a vulnerability which already exists.
Protection measures: To provide solutions to secure the devices.
Cost to company and field returns: Analysing the costs involved and what it would mean if there were field returns in case of a defective model already in production.

8. A tentative list of questions you will be seeking an answer to.
a. Counterfeiting of ICs, what are the ways to do this and how to prevent this?
b. What steps have the Semiconductor companies taken in order to aid in keeping the security intact? Who are the big players in the market?
c. What are the vulnerabilities in existing implementations and how can we rectify it?
d. RFID tags and how authentication and data protection can be achieved with this.
e. Latest technologies in the market. In ASICs and FPGAs.

9. Procedure/experiments used for verifying the results of your investigation.
a. Go through the IEEE papers on Counterfeiting of ICs.
b. Analysis of existing preventive, protective measures by semiconductor companies.
c. Go through material online and list various vulnerabilities that still have to be addressed and what steps are being taken to address those. And why is it that the vulnerabilities are not addressed as of today, i.e., Are the costs too high or the limitations affect one aspect while solving another?
d. If there are any prototypes, research them and compare.
e. Public Key Cryptography can be implemented on an RFID, practicality aspect.

10. Time schedule, including intermediate goals to be achieved by the dates of progress reports: Oct. 26-27, Nov. 9-10, Nov. 23-24, Dec. 7-8.

October 28-29: History of Counterfeiting of ICs. Basic understanding of each type.
Nov 9-10 : RFID tags methods used to counter counterfeiting.
Nov 23-24 : Report on Semiconductor companies and their efforts. Type of technology used. Solutions for various problems faced by counterfeiting in the Industry.
Dec. 7-8 : Final Report.

11. A list of possible areas, where the specification can change depending on the progress of the project.
Based on new findings, there might be some change in the specifications and list of alternative solutions and table of contents in the index.

12. Tentative table of contents of your final report.
1. Abstract
2. Introduction
3. An overview of Counterfeiting: Prevention, Detection and Protection
4. Types of Integrated Circuits Counterfeiting
5. Existing methods for Anti-Counterfeiting.
6. RFID Tags-Why Choose it to Counter Counterfeiting?
7. Public Key Cryptography on RFID.
8. RFID Tags to Identify Counterfeit PCB boards.
9. Physically Unclonable Enabled RFID.
10. Semiconductor market: The big players and their efforts.
11. Other Countermeasures
12. Conclusions
13. Future Scope
14. Literature

13. List of literature.
[1] U. Guin et al., "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proc. IEEE* vol. 102, no. 8, pp. 1207-1228, Aug. 2014.

[2] H. Livingston, "Avoiding Counterfeit Electronic Components", *IEEE Trans. Compon. Packag. Technol.*, vol. 30, pp. 187-189, Mar. 2007.

[3] H. Huang et al., "The detection of counterfeit integrated circuit by the use of electromagnetic fingerprint", *Proc. 2014 Int. Symp. on Electromagnetic Compatibility.,* Gothenburg, Sweden, 2014, pp. 1118-1122.

[4] A.R. Desai et al., "Anti-counterfeit Integrated Circuits Using Fuse and Tamper-Resistant Time-stamp Circuitry," *IEEE 2013 Int. Conf. Technologies for Homeland Securities,* MA, 2013, pp. 480-485.

[5] S. Stanzione et al., "CMOS Silicon Physical Unclonable Functions Based on Intrinsic Process Variability," *Proc. IEEE J. Solid-State Circuits,* vol. 46, no. 6, pp. 1456-1463, Jun. 2011.

[6] K. Yang et al., “An RFID-based Technology for Electronic Component and System Counterfeit Detection and Traceability,” *IEEE 2015 Int. Conf. Technologies for Homeland Securities,* M, pp. 1-6.

[7] A.C. Baumgarten, “Preventing integrated circuit piracy using reconfigurable logic barriers,” M.S. Thesis, Dept. Comp. Eng., Iowa State Univ, Ames, 2009.

[8] A. Viejo. (2015, Oct. 13*). Microsemi and Athena Announce FPGA Cores with Strong DPA Countermeasures for Cryptography Users* [Online]. Available: http://www.design-reuse.com

[9] E. Asanghanwa. (2008). *Product Counterfeiting Made Easy. And Why it’s so Difficult to Prevent* [Online]. Available: http://citeseerx.ist.psu.edu

[10] J.R. Hamlet et al., “Deterrence of device counterfeiting, cloning, and subversion by substitution using hardware fingerprinting,” U.S. Patent 8848905 B1, Sep 30, 2014.

14. Anything else you consider important.