

PDF - DESIGN AND IMPLEMENTATION OF PROVABLE SECURITY FOR CRYPTO-CURRENCIES - researchcub.info  
In this project, the discussed issue is designing and implementing Cryptocurrencies security System using Simulink.

Two main techniques were used in this project which is scrambling and AES-128 encryption algorithm.

Finally the two techniques were compared in terms of degree of confidentiality and quality of output currency. It

was found that scrambling algorithm produces a better quality audio signal compared to AES encryption which

gave a very low quality audio due to unresolved accumulated delays. Furthermore AES encryption gives better

security solutions compared to scrambling techniques. In AES it almost infeasible to decrypt the currency without

having the proper key and brute force attacks are very difficult with AES. Brute force attacks of AES may be

feasible in the coming years through the quantum computers. **Chapter 1 Introduction**

### ***1.1 Background of the Project***

The concern about money security started from the very beginning (creation of universe), this concern

started when people first started having money and willing to share among themselves. The

monetary channel in which this shared money is going through is subject to leakage and as a result

insecurity, so people started thinking of a way to share their money without worrying about their data to

be compromised by an unauthorized party. First they invented a very basic way to protect the privacy of their

money such as Caesar's cipher, these basic ciphers later on evolved into a very cumbersome and complex

ways to protect the confidentiality of the money such as, DES, 3DES, AES, RSA and many other

algorithms. According to Brandau(2008), although most of monetary systems employ some sort of

security mechanism but always there is a security leakage in most of those systems, therefore currency encryption

is used in order to ensure that the currency transmitted from one end to another in Real-Time communication

systems such as, GSM, VOIP, Telephone and Analog Radio arrives safely without being compromised.

## **DESIGN AND IMPLEMENTATION OF PROVABLE SECURITY FOR CRYPTO-CURRENCIES**

**The complete project material is available and ready for download. All what you need to do is to order for the complete material. The price for the material is NGN 3,000.00.**

**Make payment via bank transfer to Bank: Guaranteed Trust Bank, Account name: Emi-Aware technology, Account Number: 0424875728**

**Bank: Zenith Bank, Account name: Emi-Aware technology, Account Number: 1222004869**

**or visit the website and pay online. For more info: Visit <https://researchcub.info/payment-instruct.html>**

**After payment send your depositor's name, amount paid, project topic, email address or your phone number (in which instructions will sent to you to download the material) to +234 70 6329 8784 via text message/ whatsapp or Email address: [info@allprojectmaterials.com](mailto:info@allprojectmaterials.com).**

**Once payment is confirmed, the material will be sent to you immediately.**

**It takes 5min to 30min to confirm and send the material to you.**

**For more project topics and materials visit: <https://researchcub.info/> or For enquiries: [info@allprojectmaterials.com](mailto:info@allprojectmaterials.com) or call/whatsapp: +234 70 6329 8784**

**Regards!!!**