Detecting Counterfeit-Money using RFID-enabled Mobile devices

Authors: **Mohamed Hamdy Eldefrawy**, **Muhammad Khurram Khan**
Center of Excellence in Information Assurance, King Saud University, Saudi Arabia

Student: **Prabhat Ranjan**, Telecom SudParis, Evry, France Date: 25/Feb/2016

SUMMARY

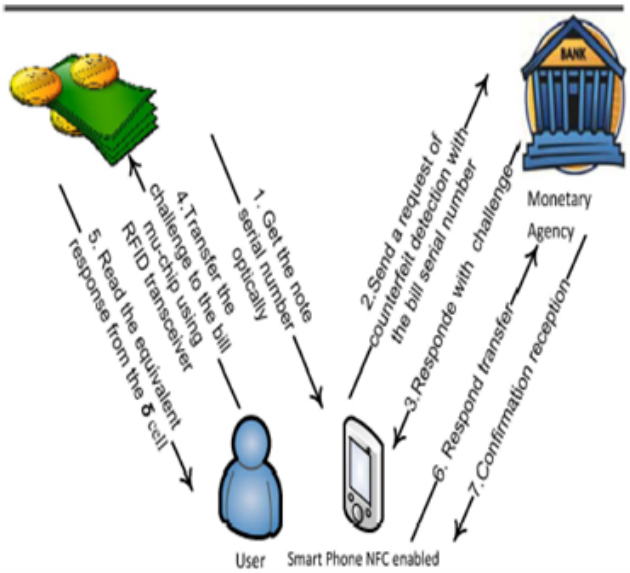
Counterfeit is way to represent the duplicity of real originality. Money counterfeiting causes more money to be circulated in the economy leading to a general rise in prices, inflation. If people have the secure method to check money then large amount of money can be detected and prevented before exchange. This article proposes an RFID counterfeit detection scheme and compares with two other counterfeit detection method which are presented to detect Counterfeit money and check the authenticity of the original notes by embedding the RFID chips on banknotes.

Juels and pappu's Scheme: Juels and pappu's Scheme uses 2 data source cell, public key cryptography, encryption with random key, ocular communication but it also includes some **limitation: data recovery attack, access-key tracking. Cypher-text tracking, etc.**

Yang et al.'s scheme: It uses 4 data source cell and multiple message exchange and computaion**. Limitation: Computational cost and complexity.**

Best algorithm: NFC enabled Smartphone RFID Protection: It uses two different one way Hash functions for challenge/response which increases different possibilities and creates more complexity.

Terminology: M A is Monetary agency, U is user, $h_A(.)$ and $h_B(.)$ is hash function sd_i is seed initial value and $sd_i(t)$ is t-the authentication.



Banknote Creation:
a)M A attach the banknote with 2 RFID µ-chips i.e δ-chips and y-chips which prints serial number on the banknote.
b)M A's do not sign note serial number
c)MA defines reading/writing i.e y-cell is unreadable and self-writable. δ-cell is publicly readable and writable by y-cell.

2)Bank verification
a) U scans the serial number to satisfy the privacy.
b)U sends an authentication request to MA over communication channel containing the bill serial number.
c)M A challenges the RFID mu-chips to produce authentication for t+1 th authentication value by using hashing function with user smart phone. Hashing($sd_i(t)$) with $h_A(.)$ to get $(sd_i(t+1))= (h_A(sd_i(t)))$ and the hash with $h_B(.)$ to get $h_B(h_A(sd_i(t)))$ and send to δ. δ->y;
d) M A receive the t+1 response and calculate it with own calculated value
e)Comparision true is authentication success

3)Banknote anonymity: d information, $h_B(h_A(sd_i(t)))$,didn't disclose any acquaintance about banknote.
4)Banknote tracking: Tracking is implicit and completely achieved
Benefits: simplicity, more secured, less message exchange, Non-specialist use friendly.

Benefits: simplicity, more secured, less message exchange, Non-specialist use friendly

Security: Prevent non-repudiation attack, Prevent forgery attack, Prevent data recovery attack