Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 264514, 8 pages
http://dx.doi.org/10.1155/2015/264514

Research Article

Banknote Validation through an Embedded RFID Chip and an NFC-Enabled Smartphone

Mohamed Hamdy Eldefrawy and Muhammad Khurram Khan

Center of Excellence in Information Assurance, King Saud University, P.O. Box 92144, Riyadh 11653, Saudi Arabia

Correspondence should be addressed to Mohamed Hamdy Eldefrawy; meldefrawy@ksu.edu.sa

Received 14 August 2014; Accepted 17 November 2014

Academic Editor: Jinhui Zhang

With the new, state-of-the-art printing devices and equipment, there has been rapid growth in the counterfeiting of banknotes. Traditional security features on banknotes are easy targets for counterfeiters, and they can easily imitate the original banknotes with fake ones. Conventional methods for validating currency require specialized devices for the authentication of banknotes. However, cost and lack of mobility of sophisticated banknote validation devices are big problems for general consumers. Modern digital solutions are attempting to complement the traditional security features through embedding radio frequency identification (RFID) chips in the banknotes, for example, Euro currency. Unfortunately, the requirement of specialized RFID readers for banknote validation impedes their widespread proliferation among consumers. To overcome this problem, a new method of banknote validation using an RFID chip and an NFC-enabled smartphone is presented. The consumer sends a banknote validation request to the Monetary Agency ($\mathscr{MA}$) using her or his smartphone and an Internet connection. The $\mathscr{MA}$ replies by sending a random challenge to the consumer's smartphone. The RFID chip in the banknote receives the challenge, via the NFC, and calculates an equivalent response to the $\mathscr{MA}$'s challenge. If any of the messages are incorrect, authentication is denied. By the proposed method, consumers can easily and instantly check the originality of currency notes with the $\mathscr{MA}$ using their smartphones and an Internet connection. The proposed system is less expensive, computationally, than regular methods and preserves the privacy of people who carry banknotes.

1. Introduction

Counterfeiting money has become an enormous problem around the world. Traditional security features on banknotes, for example, holograms, are easily prone to counterfeiting. Existing techniques do not provide realistic solutions because of complexity of the sophisticated devices that are used for banknote validation. Recently, RFID chips have been used on banknotes to complement the existing security features printed on the banknotes. The new digital solutions embed the banknote's serial number in the attached RFID chips. Robust solutions require appending cryptographic methods to stop forgery and counterfeiting. RFID devices have been experimentally assessed and tested as a means for confronting the problem of counterfeit currency notes.

RFID systems are comprised of RF tags and RF tag readers. RFID tags are small, wireless microchips that are used to spot their attached targets. RFID tags generally can be classified into two categories; that is, (1) RFID tags with a power source are delivered dynamically to a reader and identified as "active tags" and (2) powerless devices, which are prompted by a reader, are identified as "passive tags" [1–3]. The reader is a machine that identifies and retrieves the RFID information from the card [4, 5]. The reader challenges the tag by generating a radio frequency wave, and the tag answers the reader with an equivalent response [6]. The reader delivers the tag's answers to a final host (server). The server obtains the tag's record and recovers the tag's complete information from its response. Near-field communication (NFC) is an emerging area of communication for connecting RFID tags; hence NFC standards are based on existing RFID standards, including ISO/IEC 14443. [7]. The NFC protocol establishes a radio communication channel with NFC-enabled devices by putting them in close proximity, normally no more than a few centimeters. With the improvement of computing and digital printing technology, the counterfeit industry recently has grown exponentially. An accepted counterfeiting technique is digital printing using computer scanners and high-resolution printers. Although banknotes already contain security attributes, such as holograms, foil lines, special threads, microprinting, special inks, and watermarks [6], additional protection is required. The aim of this paper is to offer a comprehensive solution against the use of counterfeit banknotes using RFID chips embedded in currency notes. The proposed technique will allow individuals to verify banknotes using a portable token (e.g., their smartphones) without going to a facility or making personal or direct contact with an agency. In the proposed system, the consumer does not need to have specialized RFID readers; rather he or she can use an NFC-enabled smartphone for this purpose. The capability of using smartphones for detecting counterfeit money will, in turn, lead to their widespread use for this purpose by consumers. It will influence wide-ranging consumers to validate their currency by their smartphones extensively without the need for any complicated currency validation tools. The proposed protocol provides a set of required security features, and it guarantees low communication and computational costs in terms of number of communications required between the reader-tag and the mathematical operations, respectively. The analysis shows that the proposed protocol achieved the required performance goal and the security goal. The rest of the paper is organized as follows. Section 2 discusses the related work, Section 3 illustrates the security requirements, Section 4 proposes our currency validation protocol, Section 5 analyzes the security attributes and evaluates performance, and Section 6 presents our conclusions.

2. Related Work

Several research scientists have attempted to develop secure communication protocols for detecting counterfeit money using lightweight RFIDs. RFIDs facilitate non-line-of-sight and very rapid examining of unique IDs. It allows practical handling of unique identifiers in open-loop supply chains. Generally, identifiers can be symbolized in barcodes or holograms as well, but a line-of-sight communication would be required, and they must be read one by one in a very exhaustive process. RFID chips can obtain a single factory programmed ID that is locked after writing, making it unchangeable. The number of chips is limited and requires trusted chip authorities who do not produce duplicate IDs. They should be made in a random distribution instead of used sequential numbers inside a certain number-space, making it essentially impervious to unauthorized disclosures of the legal ID. Preventing counterfeiting by tracking and tracing possessions across the supply chain utilizes central or connected databases by detecting any abnormal trace patterns of RFID tags. There are two fundamental categories of RFID authentication schemes, that is, the use of digital signature-based protocols and challenge-response protocols. However, in the challenge-response authentication, we could have a mutual authentication with a symmetric scheme as well as a one-sided authentication with an asymmetric scheme. To prevent counterfeiting, the authenticity of the service distributed is verified alongside the delivery chain and possibly at the end-users as well. However, many checkpoints are not online. Also, public key cryptography offers different options between complexity on the tag and complexity in the infrastructure. Therefore public key cryptography is an attractive alternative to symmetric key systems, in particular for open and offline systems. However, cryptographic tags have cost and performance limitations due to their additional hardware and the processing time required. The following subsection illustrates some of the schemes that have been presented and their weaknesses. Hash-based access control (HAC), proposed by Weis et al. [5, 8], uses a one-way hashing to latch the RFID tags. A latched tag uses a hash of a random key to be its meta-ID. When latched, a tag reacts to every inquiry by its fixed meta-ID. HAC is vulnerable to location tracking attacks because the meta-ID is stationary at any time when a tag is needed. Randomized access control (RAC) stops this tracking vulnerability, but it is susceptible to tag impersonation attacks since a captured tag's answer can be repeated. In addition, it does not grant backward untraceability since the tag's ID is stationary. Lane et al. disclosed a method and apparatus for authenticating currency wherein the currency contains a foundation, such as paper, and an implanted RFID transponder [9]. An implanted RFID transponder or electronic watermark could include several sequencing levels of electronic passwords, which could be used to defend the host currency from any illegal alteration. In addition, such smart RFID tags may, *outstandingly*, classify an original certificate and its related information. The validating organization can use a public/private electronic product code (EPC) database as a facility to authenticate documents by the authenticating agency. The smart EPC could be used as an anticounterfeit system to facilitate a third party's request in order to offer services, profits, or monetary payments to validate documents and stop the counterfeiting of money.

Pareskevakos presented a system and method for currency authentication [10]. In Pareskevakos's system, the currency is authenticated by evaluating the classifying information taken from the banknote itself, such as the note's correlated serial number, to identify information in a directory related to invalid currency, such as fake currency. If the extorted classifying information matches information on the directory, the note is considered original. Optical character recognition could be used to extract the classifying information.

Ohkubo et al. presented an inexpensive hash chain method to revise the tag's secret data and grant forward security [11, 12]. It was intended to classify a communication party while guaranteeing privacy. However, it is susceptible to replay attacks [9], and, consequently, it allows an intruder to masquerade as a tag without any knowledge of the hidden information on the tag.

Henrici and Müller (HM) proposed a one-way hash function to countermeasure tag-tracing violations by enhancing the privacy of the location. The tag answers a reader's inquiry with double hashes and renews its saved values after a legal validation. This proposition still allows an amount of tag tracing because a tag replies with the identical answer before its legitimate validation. In addition, forward security cannot be guaranteed since an intruder can analyze prior sessions' tag identifiers from the tag's present identifier with the random number of the server.

In 2007, a mutual authentication protocol for RFID was researched by Chien and Chen [13]. A challenge-response technique was presented to stop replay attacks. The server record contains images of previous and fresh tag keys to prevent denial-of-service attacks. The authentication key and the access-key are renewed cooperatively subsequent to a valid authentication to give backward untraceability. However, the system authorizes backward and forward traceability, since an intruder who exposes a tag could recognize a tag's earlier exchanges from the prior communications and can examine the tag's upcoming dealings. Furthermore, an intruder can impersonate an authorized server to a tag by obtaining the tag's private values.

Duc et al. demonstrated a synchronized connection method for the RFID tag of the EPCGlobal-Class-1-Gen-2 [14]. It considers a pseudo-random number producer and a CRC check. It is not able to counter replay attacks prior to the subsequently valid authentication. Critically, a DoS attack can get a server and a tag out of synchronization [15]. It cannot present backward intractability if the fixed EPC and the access-key PIN are disclosed [13].

Song and Mitchell presented a scheme by utilizing the challenge-response approach to avoid tag impersonation attacks and replay attacks [5]. It uses random challenge values to give unpredictable tag responses. To circumvent denial-of-service attacks in case of a lack of synchronization in the shared private updating, the back-end server saves the updated values with their earlier values for the next validations. If the validation and authentication process is successful, subsequently, the tag and the server will update their common private values using swapped random numbers, thereby achieving untraceability. A main attribute of the algorithm is that a random number produced by a tag acts as a short-term private value for the tag. An alternative attribute is that a tag only requires saving identification, which is a cryptohash function of a bit-string allocated to the tag. The scheme was intended to decrease the use of complicated cryptographic functions and to replace them with straightforward functions, such as bit-wise exclusive-or and left and right shift registers to join data sequences. Security threats to RFID protocols also are discussed in [5, 11, 16–18], and the use of RFID μ-chips for detecting counterfeit money is discussed in [18–25].

2.1. RFID μ-Chip. Improvement of low-cost RFIDs was initiated in 1998 as an authentication enclosure integrated circuit to help avert the counterfeiting of currency [26]. Each μ-chip IC has a 128-bit, exclusive identifier that is configurationally part of the chip. The μ-chips function at an operating frequency of 2.45 GHz. The normal time for the exchange of messages to and from the reader and the μ-chip is about 20 ms [15]. Maximum reading distance between the reader and the tag is about 30 cm in the free space. With an area of 0.4 mm^2, μ-chips can be implanted in the currency and transmit defined information over a low-range space. Also, the fabrication of chips per silicon wafer is roughly twice that of the typical 0.7 mm^2 RFID chips. The smaller chip is called the powder large-scale integrated (LSI) chip, which also saves a 128-bit identification.

Table 1: Banknote data storage format in Juels and Pappu's scheme.

RFID	
Cell γ ispublicly readable and keyed-writable	Cell δ is keyed-readable and keyed-writable
$C = \mathrm{Enc}(PK_L, \sum \| S, r)$	r
Optical	
S	$\sum = \mathrm{Sign}(SK_B, S \| \mathrm{den})$

Powder LSI chips contain basically the identical constituents as the μ-chip, but they are cuddled into minor pieces. A main reason for the added efficiency was the use of what is named "90-nanometer silicon-on-insulator" (SOI) expertise. SOI allows processors to execute better and use less power than those formed by traditional methods as it separates transistors with an insulator. The insulator decreases the absorption of electrical energy into the surrounding medium and maintains the transistors separated which stops interference between transistors and lets them be grouped more closely together, making the chip smaller in size [27].

2.2. Juels and Pappu's Scheme. In [25], Juels and Pappu proposed a scheme that allows the verification of banknotes, which allows a law enforcement agency $\mathscr{L}$ to legally track interesting banknotes. They identified four entities that are involved in treating banknotes; that is, (1) a central bank that is authorized to produce and issue banknotes is denoted by $\mathscr{B}$, (2) a law enforcement agency that is able to trace the flow of banknotes is denoted by $\mathscr{L}$, (3) the merchant is denoted by $\mathscr{M}$, and (4) the consumer is denoted by $\mathscr{C}$. $\mathscr{B}$ creates the banknotes and has a signing key pair (SK_B, PK_B) for Sign$(\cdot)$. $\mathscr{L}$ is the banknote tracing agency, and it has an encryption key pair (SK_L, PK_L) for Enc$(\cdot)$. $\mathscr{M}$ checks the received banknotes in a trade and has the responsibility of notifying $\mathscr{L}$ when a forgery is detected. The Juels-Pappu banknote protection scheme (RBPS) uses RFID μ-chips (tags) to prevent counterfeiting the banknote. They used two data sources on the currency, that is, the visual or ocular data issued on the currency, for example, the PDF417 2D bar code, and the digital data saved on an RFID tag with keyed-reading and keyed-writing abilities. Table 1 presents two data sources on currency (a bill).

The serial number and the value of a banknote are denoted by S and den, respectively. Juels-Pappu RBPS involves the following procedure.

(1) Banknote Creation

$\mathscr{B}$ calculates $\sum_i = \mathrm{Sign}(SK_B, S_i \| \mathrm{den}_i)$ and prints the serial number S_i and the signature $\sum_i$ on a banknote.

$\mathscr{B}$ picks a random value r and puts it in the δ-cell.

$\mathcal{B}$ does $\mathrm{Enc}(PK_L, \sum_i \| S_i, r_i)$ in the γ-cell.

$\mathcal{B}$ evaluates the key $D_i = h(\sum_i)$ for a banknote.

$\mathcal{B}$ adjusts the reading/writing facilities as below: the γ-cell ispublicly readable and writable with a D_i as an access-key; the δ-cell is readable/writable with an access-key D_i.

(2) Banknote Verification

$\mathcal{M}$ examines the optical region to get S_i and $\sum_i$ and then calculates an access-key $D_i = h(\sum_i)$.

$\mathcal{M}$ reads C_i from the γ-cell and reads r with a key from the δ-cell.

$\mathcal{M}$ validates $C_i \stackrel{?}{=} \mathrm{Enc}(PK_L, \sum_i \| S_i, r_i)$.

(3) Banknote Anonymity

$\mathcal{M}$ selects r' in a random way and keyed-writes it into the δ-cell.

$\mathcal{M}$ computes $C = \mathrm{Enc}(PK_L, \sum_i \| S_i, r')$ and keyed-writes it into the γ-cell.

(4) Banknote Tracking

$\mathcal{L}$ gets C_i from the γ-cell.

$\mathcal{L}$ does $C = \mathrm{Dec}(SK_L, C_i)$ to get $(\sum_i \| S_i)$.

$\mathcal{L}$ validates a signature $(S_i \| \mathrm{den}_i) \stackrel{?}{=} \mathrm{Veri}(PK_B \| \sum_i)$ to obtain the serial number S_i for tracking.

Unless all of these steps in currency validation and banknote anonymity are successful, the merchant must inform $\mathcal{L}$. Juels-Pappu RBPS is vulnerable to data recovery, the cookies threat, access-key tracking, denial-of-service attack, and cipher-text tracking, as shown in [7].

3. Security Requirements

In this section, a number of advantageous security attributes as well as security threats to RFID protocols are discussed [5, 11, 16–18].

3.1. Nonrepudiation. Typically, "nonrepudiation" refers to the capability of ensuring that a communication party cannot deny the authenticity of the receipt security credentials that have been originated by the main server. Consequently, the RFID tags are not able to deny what they receive from the server.

3.2. Freshness. Encryption materials must be fresh and different from the reprocessing of previous keying material.

3.3. Known-Key Security. A protocol output should come with an exclusive shared secret. If a shared secret is compromised, it should have no effect on the other shared secrets.

3.4. Server Impersonation. An opponent, with knowledge of a tag internal condition, is able to masquerade as a legitimate server to the tag.

3.5. Timeliness. The process has to be accomplished in a planned amount of time and message exchange should be in a limited session.

3.6. Monitoring. Administration deals with keeping track of banknotes in exchange.

3.7. Replay Attack. In such an attack, the intruder reprocesses exchanged messages from prior communication sessions to perform the replay attack.

4. Currency Validation Protocol

RFID μ-chips have had a significant impact on security, especially in the detection of counterfeit currency [18–25]. However, those systems do not provide a high confidence level in terms of security and accuracy. The RFID μ-chip holds a 128-bit storage, including the note's serial number, which cannot be easily duplicated. However, there is concern that success in duplication of a serial number will lead to mass counterfeiting and failure to detect counterfeit notes. In the proposed work, an NFC-enabled smartphone was used to verify the authenticity of a banknote with high confidence in the accuracy. A key element of the present technique is the step of requiring the μ-chip on the banknote to do a calculation in response to a challenge that includes a random question.

4.1. Notation. We used the coming notation in the illustration of the protocol.

$\mathcal{U}$: regular consumer (user);

$\mathcal{MA}$: *Monetary Agency;*

$h(\cdot)$: public cryptographic one-way hash function;

$h_A(\cdot)$: first hash function;

$h_B(\cdot)$: second hash function;

s_i: banknote i serial number;

sd_i: seed initial value for banknote i;

$sd_i(t)$: seed number t for the tth authentication (current seed) for banknote i;

AC_i: authentication counter for banknote i;

(x_t, y_t): nested hashing progress, random challenge, values for tth authentication;

$h_B^{y_t}(h_A^{x_t}(sd_i(t)))$: hashing the current seed number t by $h_A(\cdot)$ for x_t times followed by an $h_B(\cdot)$ hashing for y_t times;

$\|$: concatenation operation.

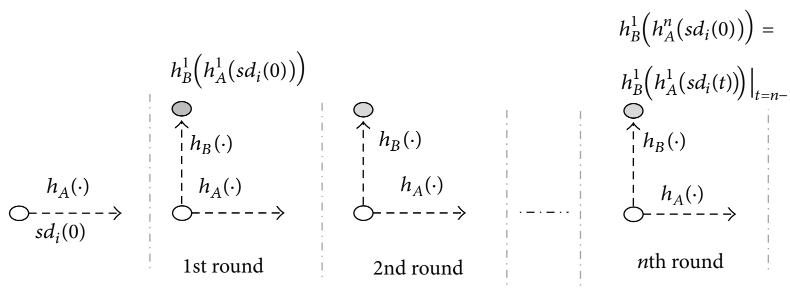

FIGURE 1: Challenge-response internal function based on two different types of hashes.

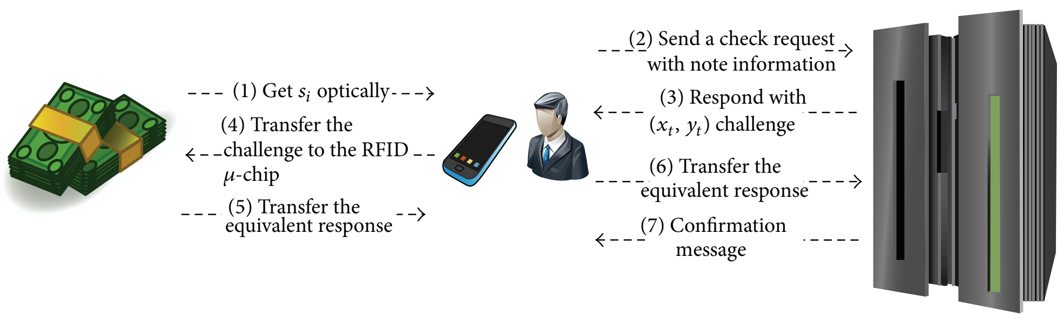

FIGURE 2: Framework and operations of the proposed scheme.

4.2. Description of the Protocol. The aim of the proposed scheme is to use a zero-knowledge proof instead of using public key cryptography. Two dissimilar hashes, $h_A(\cdot)$ and $h_B(\cdot)$, were included to satisfy the algorithm's challenge-response function [24], as depicted in Figure 1.

We integrated two dissimilar one-way hashes, $h_A(\cdot)$ and $h_B(\cdot)$, to preset our algorithm challenge-response function [10], as shown in Figure 1. Hence, $\mathscr{MA}$ sends refreshed challenge indexes (x_t, y_t) to $\mathscr{U}$ for the tth authentication. Then, $\mathscr{U}$ prompts those indexes to her or his token to be transferred to the μ-chip using RFID communication. The μ-chip responds with the corresponding response to the user's smartphone over the RFID channel. The smartphone transfers the μ-chip's response to $\mathscr{MA}$ for validation. With the result of the validation, the server confirms the validity of the banknote. Both $\mathscr{U}$ and $\mathscr{MA}$ have the same initial seed value.

4.3. Currency Creation. (1) As shown in Table 2, $\mathscr{MA}$ embeds the two RFID μ-chips (i.e., γ and δ chips) [25, 28] in the currency that contains a tamperproof primary value (the bill seed) sd_i and issues the serial number on the banknote.

(2) The validation counting value for each note is kept in the issuer/authenticator's server $\mathscr{MA}$.

(3) The issuer/authenticator's server $\mathscr{MA}$ does not need to indicate the bill's serial number.

(4) The issuer/authenticator's server $\mathscr{MA}$ ensures that the γ-cell is unreadable and self-writable and that the δ-cell is openly readable and only writable by γ.

4.4. Currency Validation. (1) When an individual consumer or $\mathscr{U}$ receives a banknote and wishes to check its validity, $\mathscr{U}$ uses the NFC smartphone to read the information on μ-chip message number 1 and to automatically send a request to the issuer/authenticator's server message, that is, number 2. The message communication is shown in Figure 2.

TABLE 2: Banknote data storage format in the proposed scheme.

RFID	
Cell γ is unreadable and self-writable	Cell δ is publicly readable/only writable by γ
$sd_i(t)$	$h_B^{y_t}(h_A^{x_t}(sd_i(t)))$
Optical	
S	

(2) Then the issuer/authenticator's server $\mathscr{MA}$ verifies the value and serial number and, upon correction of values, it corresponds with a random challenge (x_t, y_t) for the next authentication round $(t+1)$th message number 3 that requires a calculation by the RFID μ-chip embedded in the banknote. This calculation is done by hashing $(sd_i(t))$ by $h_A(\cdot)$ x_t times to get $(sd_i(t+1)) = (h_A^{x_t}(sd_i(t)))$ and define it for the current seed and afterwards hash this current seed by $h_B(\cdot) y_t$ times to get $h_B^{y_t}(h_A^{x_t}(sd_i(t)))$ to be transferred to δ-cell, $(\gamma) \rightarrow (\delta)$, which is publicly readable. This challenge is sent to the smartphone and transferred to the banknote's μ-chip, as shown in Figure 2, message number 4.

(3) The server $\mathscr{MA}$ receives and digests the response for the $(t+1)$th authentication in step message number 5 and message number 6. If $\mathscr{MA}$ receives the correct response, it sends a confirmation or authentication through message number 7.

4.5. Currency Secrecy. The knowledge of δ which obtains $h_B^{y_t}(h_A^{x_t}(sd_i(t)))$, which is openly readable, cannot reveal any

Table 3: Comparison of the presented scheme and related schemes in terms of computational costs.

		DPLK [14]	CC [13]	SM [5]	Proposed
$\mathscr{TAG}$	Operations	$4F$	$4F$	$3F$	$(x_t + y_t)\,F = 2F\|_{x_t=y_t=1}$
$\mathscr{MA}$	Operations	$(k+3)\,F$	$(k+3)\,F$	$(k+1)\,F$	$(x_t + y_t)\,F = 2F\|_{x_t=y_t=1}$

F: a computationally complex function (such as a CRC or a hash function).
k: an integer that satisfies $1 \le k \le 2N$.
N: the number of tags.

information about the banknote. In each authentication session, the equivalent reply value must be distorted.

4.6. Currency Tracing. The proposed scheme allows standard and nonspecialist consumers to identify fake banknotes by using their smartphones. Individual consumers can report fake banknotes to the administration $\mathscr{MA}$. Consequentially, the capability of identifying fake currency is fully achieved.

5. Security, Performance Analysis, and Comparison

The algorithm we presented can obstruct the off-line guessing attack; thus it leads to strong answers, anchored in strong hash functions. The prevention of counterfeiting comes by detecting and eliminating banknote forgeries and the production of fake bills over a random generation of serial numbers. In the following subsections, a security analysis of the proposed scheme is illustrated [29, 30].

5.1. Nonrepudiation Attack. To circumvent the nonrepudiation attack, the authentication parties $\mathscr{U}$ and $\mathscr{MA}$ must update their shared secret value, $(sd_i(t+1)) = (h_A^{x_t}(sd_i(t)))$, one time per round. Consequently, the client updating will be used as the host's next verifier, and vice versa, so that any unauthorized modification of the exchanged vectors will be detected by the authentication party.

5.2. Freshness. The authentication credentials should be fresh; that is, material that has been used should not be reused. This is to be done by maintaining the randomization of the generated challenges and, consequently, the equivalent response.

5.3. Known-Key Security. The proposed protocol grants security against the known key. That is why each run of the protocol between authentication parties $\mathscr{U}$ and $\mathscr{MA}$ should make an exclusive shared key, which relies on random challenges. Even if an adversary has discovered some other earlier keys, he or she cannot guess a future key. Therefore, the protocol attains its goal against the adversary.

5.4. Server Impersonation. An opponent could demand a certain tag to renew its common secrets. The tag and the genuine server could then be unsynchronized with authentication counter AC_i and incapable of successful communication.

5.5. Timeliness. In the proposed protocol, we tried to decrease the number of swapped messages between authentication parties and the direct message exchange in real-time. In addition, the size of the messages was short.

5.6. Monitoring and Tracking. The trusted authority (i.e., issuer/authenticator's server $\mathscr{MA}$) has the full keying resources and sequentially achieves admittance to those associated keys, such that key-escrow is fully achieved. Thus, nonspecialist consumers have the ability to detect counterfeiting easily. Then the tracking capability is implicitly and completely achieved.

5.7. Preplay Attack. To avoid this attack, shared secrets should be revealed only to tags and the server. Also, challenge-response authentication addresses this threat.

5.8. Replay Attack. Gaining of unauthorized access by replaying reusable passwords is restricted by encoding passwords, which are used only once.

5.9. Forgery Attack. The algorithm we used has a high forgery-attack confrontation. The data recovery attack is banned provided that the second hash function $h_B(\cdot)$ is unbroken, and $h_B(\cdot)$ will not help a counterfeiter recover any information required to make a counterfeit copy with a certain serial number. However, in case of the failure of $h_B(\cdot)$ and obtaining the required information by the forger to generate multiple copies of given banknote with a serial number, $\mathscr{MA}$ will achieve a lack of synchronization with its counter AC_i.

5.10. Recovery Attack. As has been illustrated previously, the recovery attack cannot be executed in the survival of $h_B(\cdot)$, which is the blockade for any intruder who is attempting to acquire any hidden information. Also, it is important to note that no access-key is needed for hiding information. Table 3 [5] demonstrates a judgment between the presented algorithm and contemporary algorithms considering the number of operations required by each communication party.

6. Conclusions

In this paper, the currency counterfeiting problem has been addressed. Schemes for protecting electronic cash must include cryptomethods to deal with forgery and counterfeiting problems. A new banknote validation technique has been presented which is based on the use of an RFID μ-chip and an

NFC-enabled smartphone. A banknote is issued with a value, a serial number, and a secret seed message that is also saved on the $\mathscr{MA}$. A tamperproof RFID μ-chip is embedded in the currency note and includes the value, serial number, and secret message that is used for validation. The smartphone reads the information on the chip and requests the $\mathscr{MA}$ to validate the note. The $\mathscr{MA}$ transmits a challenge through an Internet connection and the μ-chip calculates an equivalent answer that is sent to the $\mathscr{MA}$. An approval or disapproval is then sent to the smartphone.

This possibility of using these devices to detect counterfeit money results in the extensive deployment of this technology among regular and nonspecialist end-users. It will encourage the general public to check for counterfeit money using smartphones without the need for any sophisticated and expensive optical devices. The presented validation technique satisfies the security requirements for banknote counterfeit detection. It has been compared with some related schemes with regard to computational efficiency and performance analysis. The comparisons showed that the proposed scheme is more efficient and effective than existing schemes.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] Y.-J. Huang, W.-C. Lin, and H.-L. Li, "Efficient implementation of RFID mutual authentication protocol," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 12, pp. 4784–4791, 2012.

[2] Y. J. Huang, C. C. Yuan, M. K. Chen, W. C. Lin, and H. C. Teng, "Hardware implementation of RFID mutual authentication protocol," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 5, pp. 1573–1582, 2010.

[3] M. H. Eldefrawy and M. K. Khan, "Detecting counterfeit-money using RFID-enabled mobile devices," in *Proceedings of the 7th International Conference for Internet Technology and Secured Transactions*, 2012.

[4] B. Glover and H. Bhatt, *RFID Essentials: O'Reilly Media*, Incorporated, 2006.

[5] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," in *Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec '08)*, pp. 140–147, April 2008.

[6] F. Thornton, B. Haines, A. M. Das, H. Bhargava, A. Campbell, and J. Kleinschmidt, *RFID Security*, Syngress Media Incorporated, 2006.

[7] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical NFC peer-to-peer relay attack using mobile phones," in *Proceedings of the 6th International Workshop on Radio Frequency Identification: Security and Privacy Issues (RFIDSec '10)*, pp. 35–49, 2010.

[8] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in Pervasive Computing*, pp. 50–59, 2004.

[9] K. Lane, W. Lane, and R. Stewart, "Hierarchical electronic watermarks and method of use," US7221258, 2007.

[10] T. G. Pareskevakos, "System and method for intelligent currency validation," US Patent no. US7724938, 2010.

[11] S. Cai, Y. Li, T. Li, and R. H. Deng, "Attacks and improvements to an RFID mutual authentication protocol and its extensions," in *Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec '09)*, pp. 51–58, March 2009.

[12] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags," in *Proceedings of the RFID Privacy Workshop*, 2003.

[13] H.-Y. Chien and C.-H. Chen, "Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards," *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 254–259, 2007.

[14] D. N. Duc, H. Lee, and K. Kim, "Enhancing security of EPCglobal Gen-2 RFID against traceability and cloning," White Paper, Auto-ID Labs Information and Communication University, 2006.

[15] D. Henrici and P. Müller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," in *Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications, Workshops (PerCom '04)*, pp. 149–153, March 2004.

[16] S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," in *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05)*, pp. 63–67, November 2005.

[17] T. Van Deursen and S. Radomirović, "Security of an RFID protocol for supply chains," in *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE '08)*, pp. 568–573, Xi'an, China, October 2008.

[18] P. Rizomiliotis, E. Rekleitis, and S. Gritzalis, "Security analysis of the Song-Mitchell authentication protocol for low-cost RFID tags," *IEEE Communications Letters*, vol. 13, no. 4, pp. 274–276, 2009.

[19] C.-L. Chen, Y.-Y. Chen, Y.-C. Huang, C.-S. Liu, C.-I. Lin, and T.-F. Shih, "Anti-counterfeit ownership transfer protocol for low cost RFID system," *WSEAS Transactions on Computers*, vol. 7, no. 8, pp. 1149–1158, 2008.

[20] I. Vajda and L. Buttyán, "Lightweight authentication protocols for low-cost RFID tags," in *Proceedings of the 2nd Workshop on Security in Ubiquitous Computing (Ubicomp '03)*, 2003.

[21] M. O. Lehtonen, F. Michahelles, and E. Fleisch, "Trust and security in RFID-based product authentication systems," *IEEE Systems Journal*, vol. 1, pp. 129–144, 2007.

[22] D. Huang and H. Kapoor, "Towards lightweight secure communication protocols for passive RFIDs," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09)*, pp. 1–9, IEEE, Rome, Italy, June 2009.

[23] P. Najera, J. Lopez, and R. Roman, "Real-time location and inpatient care systems based on passive RFID," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 980–989, 2011.

[24] S. K. Kwok, J. S. L. Ting, A. H. C. Tsang, W. B. Lee, and B. C. F. Cheung, "Design and development of a mobile EPC-RFID-based self-validation system (MESS) for product authentication," *Computers in Industry*, vol. 61, no. 7, pp. 624–635, 2010.

[25] A. Juels and R. Pappu, "Squealing Euros: privacy protection in RFID-enabled banknotes," in *Computer Aided Verification*, pp. 103–121, 2003.

[26] G. Andrechak and R. A. Wiens, *Hitachi μ-chip RFID Technology Compatible with Gamma Sterilization*, 2008.

[27] T. Hornyak, "RFID powder," *Scientific American*, vol. 298, no. 2, pp. 68–71, 2008.

[28] C.-N. Yang, J.-R. Chen, C.-Y. Chiu, G.-C. Wu, and C.-C. Wu, "Enhancing privacy and security in RFID-enabled banknotes," in *Proceedings of the IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA '09)*, pp. 439–444, August 2009.

[29] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, T.-H. Kim, and H. Elkamchouchi, "Mobile one-time passwords: two-factor authentication using mobile phones," *Security and Communication Networks*, vol. 5, no. 5, pp. 508–516, 2012.

[30] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, "One-time password system with infinite nested Hash chains," in *Security Technology, Disaster Recovery and Business Continuity*, vol. 122 of *Communications in Computer and Information Science*, pp. 161–170, Springer, Berlin, Germany, 2010.