Securing a Web-Based Anti-counterfeit RFID System

Belal Chowdhury[1], Morshed Chowdhury[2], and Jemal Abawajy[2]

[1] Melbourne Institute of Technology, Melbourne 3000, Australia
bchowdhury@mit.edu.au
[2] Deakin University, Melbourne 3125, Australia
{muc,Jemal}@deakin.edu.au

Abstract. The use of RFID (Radio Frequency Identification) technology can be employed for automating and streamlining safe and accurate brand identification (ID) uniquely in real-time to protect consumers from counterfeited products. By placing brand tags (RFID tags) on brands at the point of manufacture, vendors and retailers can trace products throughout the supply chain. We outline a Web-based Anti-counterfeit RFID System (WARS) to combat counterfeit branding. Despite these potential benefits, security, and privacy issues are the key factors in the deployment of a web-based RFID-enabled system in anti-counterfeiting schemes. This paper proposes an asymmetric cryptosystem to secure RFID transmission in retail supply chain using Elliptic Curve Cryptographic (ECC) techniques. The uses of ECC techniques provide greater strength than other current cryptosystems (such as RSA, and DSA) for any given key length, enables the use of smaller key size, resulting in significantly lower memory requirements, and faster computations, thus, making it suitable for wireless and mobile applications, including handheld devices.

Keywords: Asymmetric Cryptography, ECC, RFID, WARS and Counterfeit.

1 Introduction

Counterfeiting is a significant and growing problem worldwide, occurring both in less and well developed countries. Considering the countries worldwide, almost five percent of all products are counterfeited [1], [2]. Counterfeiting continues to increase globally because of the high margins achieved through counterfeiting by manufacturers and the demand for trade name goods at value prices by consumers [3]. The problem of counterfeiting is further magnified because of the opening of huge new economies in Eastern Europe and Asia [4]. In the past, counterfeit goods were easy to identify because these products typically represented luxury goods made with shoddy materials and sold in limited venues such as open-air markets in large, cosmopolitan cities as New York and Los Angeles. Today, however, counterfeiting impacts virtually every product category: from fake foods, beverages and everyday household products to pharmaceuticals, auto parts and consumer electronics [5]. Counterfeiting refers to the unauthorized production of goods protected by

T. Zia et al. (Eds.): SecureComm 2013, LNICST 127, pp. 342–355, 2013.

trademarks, copyrights, or patents. Due to the technological advancements in materials and processing techniques, many counterfeit goods have found their way to legitimate bricks-and-mortar retail stores, such as Walmart, and Target, in developed and developing countries. Many successful brands also become victims of the worldwide phenomenon of counterfeiting, where cheap impersonations of the brands are distributed by the counterfeiters. Nowadays, the brand counterfeiting context is increasingly dominated by the unconstrained presence of fake brands [6]. Therefore, this topic has generated a substantial body of scholarly discussion, research and thought [7].

The majority of the research on counterfeiting has focused attention on the demand side of counterfeiting [8], [9], [10] that is consumer accomplices who engage in aberrant consumer behaviour [11], [12] and deliberately purchase counterfeit goods with scant research addressing the supply side [13]. It can be argued that counterfeiters are good marketers because they have found a need and are finding a way to fulfill it [14]. To develop techniques that effectively combat the problem of counterfeiting, it is necessary to determine and identify the existence of the segment(s) of consumer accomplices who purchase counterfeit goods.

The economic and social consequences of counterfeiting are enormous. It is estimated that brand holders lose approximately $600 billion of revenue annually due to counterfeiting and make up approximately seven percent of world trade [15].In the USA economy, the cost of counterfeiting is estimated to be up to $200 billion per year [16]. A large majority of these products include clothing, luxury goods, entertainment equipment, medicines and pharmaceutical products, handbags, automotive parts and high tech products. Manufacturers of affected products have a direct loss in sale revenues; this is often directly related to losses in tax revenues, and may also result in job losses. Furthermore, counterfeit goods are everywhere on the Internet and if a brand has revenue generating capability or brand credibility, it will surely be counterfeited and sold online. Online auction sites and business-to-business websites also provide the ideal online medium for counterfeit sales that worth billions. Michael Danel, the secretary general of the World Customs Organization identified that if terrorism did not exist, counterfeiting would be the most important criminal act of the early 21st century.

The effect of counterfeiting is always greater than the value of the counterfeit product itself. By damaging consumers’ perception of the performance, reliability, and safety of branded devices, counterfeiting tarnishes brand image, customer loyalty, and satisfaction. Actions to limit counterfeits can arise from both supply and demand side, considering the tactics companies employ to deter counterfeits [16] and the motivations that make a counterfeit an interesting option for some customers [17], [18]. Also, there is no single solution to this problem; anti-counterfeiting strategies should be multifaceted. The anti-counterfeiting strategies are possible by the use of mobile/wireless technology to combat counterfeiting. The application of these principles can be facilitated by the use of the wireless technology such as Radio Frequency Identification (RFID) [19]. Today's advanced technology is capable of uniting brand tags (RFID) and data processing into a single integrated system.

A Web-based Anti-counterfeit RFID System (WARS) can be used to automate and streamline safe and accurate brand identification (ID) uniquely in real-time by product marketing managers and to protect consumers from counterfeited products [20]. By placing brand tags (RFID tags) on brand items at the point of manufacture, manufacturers can trace products throughout the supply chain. The retail industry can use an online application, such as WARS at the point of sale to document the authenticity of their brand products at retail in real-time. The brand tags can store the unique product IDs and the product information can be stored in an associated (i.e., manufacturers) database. If the brand is not properly tagged or the brand tag is not associated (i.e., the product information is missing) with the database, then the retailers know the product is counterfeit. Additionally, by placing brand tags at the point of manufacture, not only can brands be traced throughout the supply chain, but it can also prevent counterfeit brands from entering into the supply chain.

These RFID-based systems can collect and organize data exponentially faster and more accurately. The unique ID number on standard RFID tags (e.g., passive) can be used to verify the authenticity of the products to which they are attached. As in the distribution chain, RFID-based systems in retail can greatly aid in reducing the cost of keeping accurate inventory data. With minimum staff and less time, retailers can keep accurate inventories. They can spend more time providing service to customers rather than counting product. In addition, the accuracy of the real time inventory data enables product marketing managers to ensure that hot selling items are properly stocked and to ensure replenishment order for these items are placed as quickly as possible. The RFID-based systems enable the product marketing managers to identify slow moving items quickly and to take corrective action to goose demand through promotional or advertising activity before a ‘fire sale’ is needed. Thus RFID systems help managers to maintain their margins. These systems are, also, a significant aid in deterring theft in retail environments. RFID enable brand tags to trigger alarms when they are removed from the store without a due process. In the past several decades, RFID-based systems have been successfully deployed for anti-theft purposes.

Despite these potential benefits, security, privacy and system deployment issues are the key factors in the deployment of a RFID-enabled system in anti-counterfeiting schemes and imposes significant threat on overall profitability [21]. Since a RFID-enabled web-based anti-counterfeiting systems use a wireless communication system, retailers or vendors and network servers need a strong security system (such as public-key cryptography) and mutual authentication protocol in their conversation [22]. Over the past three decades, public key cryptography such as RSA (Rivest, Shamir and Adelman) and DSA (Digital Signature Algorithm) has become a mainstay for secure communications. It provides the foundation for both key management and digital signatures. Public key cryptography is used to distribute the secret keys in key management and to authenticate the origin of data and protect the integrity of that data in digital signatures. However, over the past two decades, new techniques such as Elliptical Curve Cryptography (ECC) have been developed for better performance and higher security than these public key techniques [23].

One of the protocol proposed by Beller, Chang, and Yacobi [24], which provides mutual authentication and key agreement between users and servers with lower computational burden on the user side. This is important since the retailers usually communicate using a small, portable handset (e.g., smart phone) with limited power and processing capability. In this paper we will examine and propose a solution using ECC to address the security issues relating to RFID-enabled anti-counterfeiting systems.

The paper is structured as follows: Section 2 illustrates the application of a real-time Web-based Anti-counterfeit RFID System (WARS) to curb counterfeit branding. Section 3 discusses the Security issues and outlines the proposed solutions of WARS. Section 4 discusses the verification processes of counterfeit branding. Section 5 illustrates the practical implication of WARS and ECC. Section 6 concludes the paper.

2 Web-Based Anti-counterfeit RFID System

RFID is an advanced emerging technology that elegantly provides a solution to leading global brands in multiple industries including retail, pharmaceuticals, electronics, entertainment, aviation, IT and many more. WARS represent one of the most promising approaches to curb counterfeit branding. WARS mainly consist of smart brand tags, a RFID Reader and retailer's IT system. It can be embedded into the retailer's web portal (i.e., dashboard) to identify the authenticity of the brand tags. Each unique brand tag can be passive, semi-passive or active [25]. Passive tags can be used for both reading/writing capabilities by the RFID reader and do not need an internal power (i.e., battery). They get energized by the reader device and have a read range from 10 mm to almost 10 meters [26]. Passive tags are cheap, ranging from $0.25c to $0.40c each and life expectancy is unlimited. Thereby, we suggest the use of passive brand tags (13.56 MHz ISO 15693 tag) with the read range of one meter attached to each brand at the point of manufacture. The main components of the WARS are shown in Figure 1.

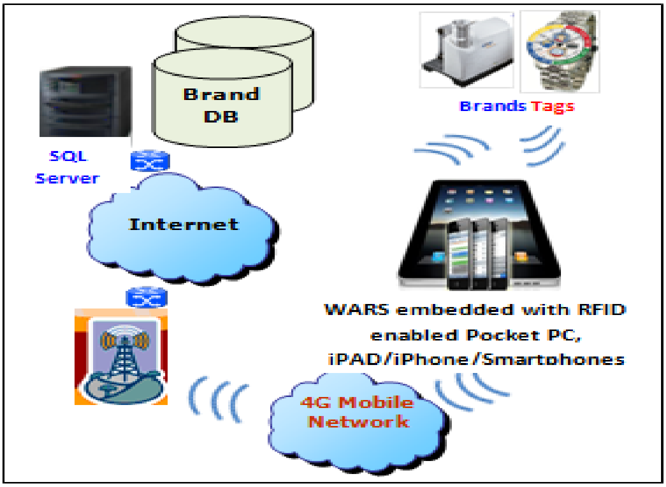
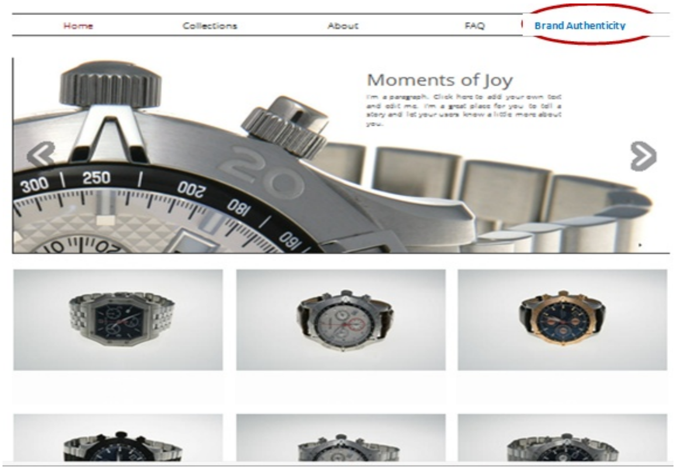

Brand DB
SQL Server
Brands Tags
Internet
WARS embedded with RFID enabled Pocket PC, iPAD/iPhone/Smartphones
4G Mobile Network

Fig. 1. Main components of WARS

The passive brand tag antenna picks up radio-waves or electromagnetic energy beamed at it from an RFID reader device attached to mobile devices (e.g., iPad, iPhone or smartphone) and enables the chip to transmit the brand's unique ID and other information to the reader device, allowing the product to be remotely identified [20]. A mobile device-based RFID reader will ensure that the identity of the brand product is passed to the device (e.g., iPhone) and automatically logged into an integrated database server (e.g., SQL server) using a wireless network. The RFID reader can also request any additional information from the brand tag that is encoded on it [26]. The reader converts the radio waves reflected back from the brand tag into digital information [27] then passed onto WARS (embedded in a smartphone/iPhone) for processing. The brand database can also link with other databases through Internet for retrieving specific brand information.

As the retail industry currently faces counterfeit branding issues, multi-layer RFID architecture can establish an infrastructure to address such a challenge, to automate and simplify the functionality for tracking and detecting brands wirelessly. Figure 2 shows a retailer's mobile-based web portal (i.e., dashboard) integrated with WARS. By clicking '**Brand Authenticity'** tab on the dashboard will enable WARS.

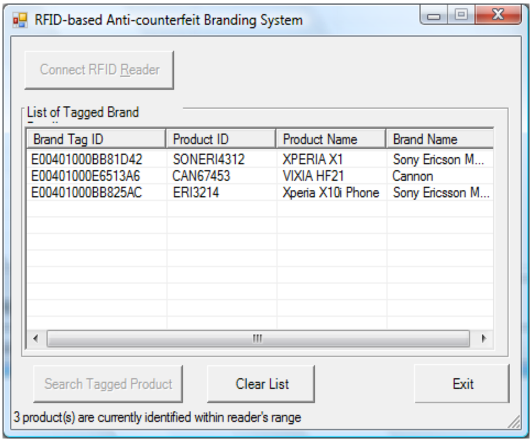


Moments of Joy

I'm a paragraph. Click here to add your own text and edit me. I'm a great place for you to tell a story and let your users know a little more about you.

Fig. 2. Retailer's web portal (dashboard)

Figure 3 shows the windows based WARS application, which can be embedded with a mobile device for capturing brand information (e.g., product ID, product name, or brand name) automatically and wirelessly. The WARS application identifies every product uniquely with a brand ID embedded in brand items through RFID-enabled mobile devices. A brand tag only contains a unique ID and perhaps other information (e.g. product and brand name), which a WARS application uses to retrieve a product record stored in the retail branding database (e.g., SQL server). A WARS can also be linked to other (e.g., brand manufacturer) databases.



Brand Tag ID	Product ID	Product Name	Brand Name
E00401000BB81D42	SONERI4312	XPERIA X1	Sony Ericson M...
E00401000E6513A6	CAN67453	VIXIA HF21	Cannon
E00401000BB825AC	ERI3214	Xperia X10i Phone	Sony Ericsson M...

3 product(s) are currently identified within reader's range

Fig. 3. WARS application for automatic brand detection

In case of counterfeit branding issues, a retailer or vendor can use WARS for detecting and determining the right brands. After running the WARS application, the retail staff needs to connect RFID reader first by clicking “Connect RFID Reader” button. Then detect brand product(s) by clicking “Search Tagged Product” button.

When the required brand items are in the mobile device-based RFID readers energizing field, the WARS application beeps, indicating that the identified brand is not counterfeited and displays the brand information (e.g., tag ID, product name, and brand name) in real-time in the list box as shown in Figure 3.

In case of counterfeit brand items, the WARS pop-up an error message, “Brand information is not found”.

3 Security of WARS

Counterfeit branding has been an issue in many industries that affect only the bottom line and a company’s reputation. High value luxury goods, such as handbags, wristwatches, and other products, are among the most susceptible to counterfeiting. The brand holders spend large amounts of money to trace and eliminate the counterfeit products and the people responsible to ensure that counterfeit products don’t sully their brands.

Most of the security threats in retail supply chain are attributed to the security of the communication channel between authentic RFID-enable reader devices (e.g., smart phone) and the brand (RFID) tags through the air interface (i.e., wireless communication). A brand tag reading occurs when a reader device generates a radio frequency “interrogation” signal that communicates with the brand tag (e.g., a tagged camera), triggering a response from the brand tag [28]. Since RFID-enabled anti-counterfeit systems uses open air space as a communication channel (wireless), the content (such as brand name) of the communication may be exposed to an eavesdropper, or system services can be used fraudulently. Further with respect to

Read/Write (reprogrammable) tags, unauthorized alteration of brand data can be the possibility in the supply chain. As a result, security is the key issue which presents a host of challenges for the successful implementation of RFID-enabled anti-counterfeit branding systems. To address RFID security issues, we propose a separate security layer, which ensures a reliable proper security measures such as authenticity, confidentiality and intractability over the wireless communication channel [9] in the RFID-enable anti-counterfeiting architecture. The security layer implements a strong cryptographic algorithm such as ECC initially proposed by other researches [29].The security measures are as follows:

1) Attaching a brand tag (RFID) to the high value product – Brand tags can be attached to or is permanently embedded in each high value products (such as a wristwatch) at the point of manufacture to prevent counterfeit products from entering the supply chain. Including a digital signature in these brand tags can create authentication schemes that are extremely difficult for counterfeiters to circumvent. This will add an extra layer of security, which ensures that the counterfeiters cannot duplicate the signature as it is an effective measure to prevent a repudiation of service.

2) Strong cryptographic techniques and mutual authentication to protect high-value products - Cryptography is the science of keeping information secure. It provides confidentiality, authentication, integrity and non-repudiation. Cryptography can be classified into two categories: s*ymmetric* and a*symmetric*. In symmetric key cryptography, both parties share the same key for encryption as well as the corresponding decryption. Assymetric key cryptography uses pairs of keys – a public key, is used for encryption and its corresponding, intrinsically linked private/secret key is used for decryption. Both public and private keys can be used interchangeably.

   Asymmetric cryptography has proved to be so useful that it has become a common part of everyday life. Emerging technologies such as e-commerce web site uses a secure server employs asymmetric cryptography to secure online transactions. In this paper, we suggest an Asymmetric cryptography - the core technology behind digital signatures and authentication, offers the robust protection that can combat counterfeit branding.

3.1 Asymmetric Cryptography

Asymmetric cryptography uses a combined public and private key to encrypt messages and digital signatures. Although asymmetric cryptography offers superior security, it is by nature also demanding, complex, and costly to implement. Most of the public-key cryptosystems such as RSA and DSA are used for performing asymmetric authentication. The strength of technology provided by asymmetric cryptography is directly proportional to the key length used. As the key gets longer, the computational and software complexity also get longer. ECC can be an emerging alternative to public-key cryptosystems, and can be used to create faster, smaller, and more efficient cryptographic keys [30]. The countries like United States, United Kingdom, Canada and some NATO member countries have adopted some form of ECC for future systems to protect classified information between their governments. The United States Department of Defense aims at replacing almost 1.3 million existing equipment over the next 10 years that uses ECC for key management and digital signatures [23].

3.2 Elliptic Curve Cryptography

ECC is a public key encryption technique based on elliptic curve theory in cryptography was first proposed by Victor Miller and Neal Koblitz in 1985. ECC provides higher strength per bit than any other current cryptosystem (such as RSA, DSA, etc.), thus, making it suitable for wireless and mobile applications, including smartcards and handheld devices. The advantage of elliptic curve over the other public key systems such as RSA, DSA etc. is the key strength. The following table 1 summarizes the comparison of the key strengths ECC and other public key schemes [23].

Table 1. Comparison of the key strengths between RSA/DSA and ECC

RSA/DSA Key Size (bits)	ECC Key Size (bits)
1024	160
2048	224
3072	256
7680	384
15360	512

The above table shows that a 244-bit ECC key has the equivalent strength of a 2048-bit RSA key for security; a 384-bit ECC key matches a 7680-bit RSA key. So, it is clear that greater strength for any given key length enables the use of smaller key size, bandwidth savings, lower computational loads and memory requirements, and hence faster computations [23][30].

ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. An elliptic curve E over a field R of real numbers, is defined by an equation, $\mathbf{E : y^2 + a_1xy + a_3y}$ as shown in Figure 4. Where a_1, a_3 are real numbers belong to R, x and y take on values in the real numbers.

An elliptic curve represents a looping line intersecting two axes as shown in the following figure. ECC is based on properties of a mathematical equation derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is quite difficult to identify the number, even the original point and the result are known.

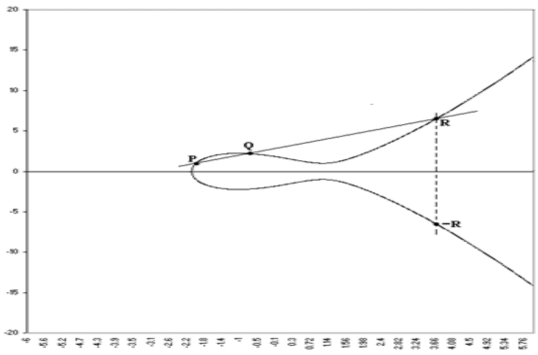


Fig. 4. Graph of the elliptic curve function

We propose an ECC public key [16] cryptosystem to communicate between two parties - sender and receiver. Both sender and receiver must agree to use an elliptic curve Ep (s,r) to communicate the messages, where p is a prime number. The sender (S) selects a large random number α, which is less than the order of Ep (s,r) and a random point A and C on the elliptic curve. The sender computes $S_1 = \alpha(C + A)$ and $S_2 = \alpha A$. S keeps the random number α, and the point A as his/her private keys and publishes S_1 and S_2 as a general public keys.

Similarly, the receiver (R) selects a large random number β and a point B on the elliptic curve. He/she computes $R_1 = \beta(C+B)$ and $R_2 = \beta B$. R keeps the random number β and the point B as his/her private keys and publishes R_1 and R_2 as general public keys. After publishing the public keys, the communicating parties again calculate the following quantities and publish them as their specific public keys of each other.

- The sender calculates $\mathbf{S_R = \alpha R_2}$ and publishes it as his/her specific public key for receiver.
- The receiver calculates $\mathbf{R_S = \beta S_2}$ and publishes it as his/her specific public key for sender.

The encryption and decryption processes are as follow:

Encryption: If R wants to communicate the message M then all the characters of the message are coded to the points on the elliptic curve using the code table, which is agreed upon by the both S and R. Then each message point is encrypted to a pair of cipher points E_1,E_2 . R uses a random number γ, which is different for the encryption of different message points.

$$\mathbf{E_1 = \gamma C}$$
$$\mathbf{E_2 = M + (\beta + \gamma)\, S_1 - \gamma\, S_2 + S_R}$$

After encrypting all the message character, the receiver converts the pair of points of each message point into the text characters using the code table. Then he/she sends the cipher text to S in the public channel (i.e., air).

Decryption: After receiving the cipher text, S converts the cipher text into the points on the elliptic curve and recognizes the points E_1 and E_2 of each character. Then he/she decrypts the message as follows.

$$\mathbf{M = E_2 - (\alpha E1 + \alpha R_1 + R_S)}$$

An asymmetric scheme (using ECC) for security of WARS is shown in the following Figure 5.

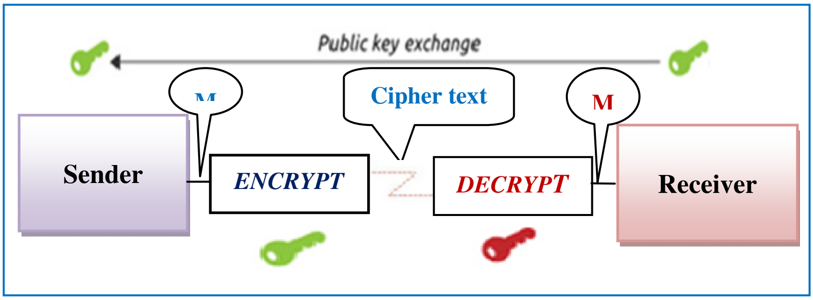


Fig. 5. An asymmetric encryption (ECC) algorithm for secure communication

4 How Does WARS Work Using ECC?

The manufacturer embeds a brand tag (i.e., smart RFID tag) in each of its brand at the point of manufacture. Each brand tag contains a private key and a certificate that has the approval of luxury products (such as handbags, wristwatches, and other products) manufacturers, as well as identifying information about the brand, such as the name, description, etc. Retailers or vendors can use WARS at the point of purchase to verify the authenticity of high value products. The following steps are needed to verify counterfeit bands with retailers IT system using ECC:

a) A RFID-based smart phone (i.e., WARS) enables the brand tag to transmit brand’s unique ID and pass it to the retailer’s web-based IT (i.e., host) system.

b) The retailer’s host system first requests a certificate (a random number along with a public key). The host then combines that number with the public key to create a challenge message, which the host sends back to the brand tag.

c) The brand tag uses its securely stored private key to compute the elliptic curve digital signature of the challenge message and sends this digital signature back to the host.

d) Using the corresponding public key, the host verifies the signature by decrypting random number is shown in the Figure 6.

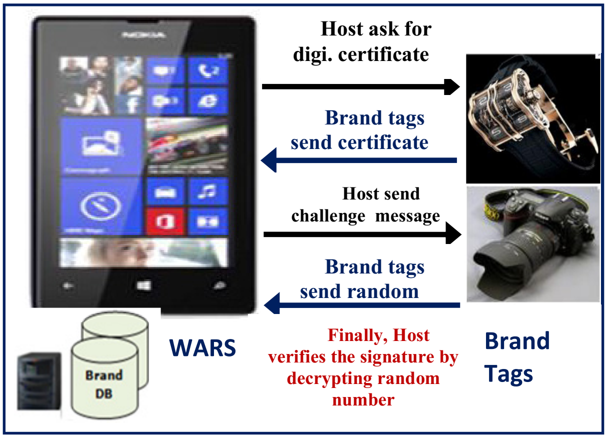

Host ask for digi. certificate
Brand tags send certificate
Host send challenge message
Brand tags send random
Finally, Host verifies the signature by decrypting random number
WARS
Brand DB
Brand Tags

Fig. 6. Verification processes of counterfeit branding

Only an authentic brand with knowledge of the private key can produce a correct digital signature. Using the verification result, the host decides whether to authenticate the brand to respond to RFID-enabled reader device. The host can also determine whether brand ID and other information are correct for use with the host and could also use the brand to track.

5 Practical Implication of WARS and ECC

A drawback of existing anti-counterfeiting measures (such as barcodes) is the low achievable degree of automation when checking the originality of a product. With existing schemes, large-scale checks, for example required in retail warehouses, are not feasible. RFID helps to address this problem, and provides the possibility to implement extensible, secure protection mechanisms in the retail supply chain. A RFID-based real-time automatic Anti-counterfeit RFID System (WARS) can be implemented in retail supply chain for combating counterfeit branding. Retailers or vendors would use WARS at the point of purchase to authenticate the brands [32].

As ECC employs both public and private key, a counterfeiter cannot derive one key based on knowledge of the other key. Thus, only brand tags that know the private key can respond correctly to a retailer’s IT systems (i.e., host) challenge and the host system can determine this knowledge using only the corresponding public key. If a counterfeiter cannot obtain the private key, then the host can assume that any brand responding correctly is authentic.

In case of corrupt retailers or vendors, customer can verify the brand authenticity via SMS (Short Message Service), which is getting popular now-a-days and almost been used everywhere. Using SMS, consumers can send messages; make purchases and receive notification, all on a mobile device. For example, financial services institutions, such as banks, and credit card companies, are experiencing high rates of customer adoption and usage of SMS-based mobile banking services as the services become available on all mobile telephone technologies [33].

Upon purchasing a brand, customers can find an item specific code, such as brand serial number. Then, they text the code to manufacturer using their mobile phone and receive a reply confirming that the brand is genuine or warning that it may be counterfeited.

6 Conclusions and Future Work

In this paper we have outlined, and designed a Web-based Anti-counterfeit RFID System (WARS) to curb counterfeit branding. The authors have shown the application and practical implication of the above system. Efforts are being made to develop the complete system (i.e., WARS) for use in retail sectors to prevent counterfeiting. We also propose a separate security layer in WARS architecture to address RFID security issues and propose a reliable proper security measures such as authenticity, confidentiality and intractability using asymmetric cryptosystem (ECC) over the wireless communication. The advantage of elliptic curve over the other public key systems such as RSA, DSA etc, is the key strength, which provides greater security and more efficient performance.

The security and implementation properties of the ECC seem to be over the highest cryptographic strength per bit among all existing public-key systems. The RSA-based protocols have significant problems in terms of the bandwidth and storage requirements. For example, a 244-bit ECC key has the equivalent strength of a 2048-bit RSA key for security; a 384-bit ECC key matches a 7680-bit RSA key. So, it is clear that ECC is an emerging alternative to public-key cryptosystems, and has the smaller key sizes result in smaller system parameters, smaller public-key certificates, bandwidth savings, faster implementations, and lower power requirements. Thus, the use of the ECC in wireless communication system is highly recommended to combat counterfeit branding.

Nevertheless, implementation of such a security system requires specialized knowledge and a significant investment in hardware and software development, has prevented most manufacturers from employing it.

However, as the microprocessors available to counterfeiters wanting to hack these systems continue to become faster and cheaper, a key length that seemed adequate a few years ago may no longer offer adequate security. For this reason, effective asymmetric implementations have been too costly for all but the most high-end applications.

Finally the implementation of the proposed system could be an interesting area of future research.

References

1. International Anti-counterfeiting Coalition, IACC (2005)
2. International Intellectual Property Institute, IIPI (2003)
3. Amine, L.S., Magnusson, P.: Cost-benefit models of stakeholders in the global counterfeiting industry and marketing response strategies. Multinational Business Review, 1–23 (2007)

4. Organisation for Economic Co-operation and Development, The economic impact of counterfeiting. Organisation for Economic Co-operation and Development, Paris (1998)
5. WHO, The Need for Global Standards and Solutions to Combat Counterfeiting (2012), `http://www.gs1.org/docs/GS1_Anti-Counterfeiting_White_Paper.pdf` (accessed on July 05, 2013)
6. Phau, I., Teah, M., Lee, A.: Targeting buyers of counterfeits of luxury brands: A study on attitudes of Singaporean consumers. Journal of Targeting, Measurement & Analysis for Marketing 17(1), 3–15 (2009)
7. Staake, T., Thiesse, F., Fleisch, E.: The emergence of counterfeit trade: a literature review Export. European Journal of Marketing 43(3-4), 320–349 (2009)
8. Bloch, P.H., Bush, R.F., Campbell, L.: Consumer “accomplices” in product counterfeiting. Journal of Consumer Marketing 10(4), 27–36 (1993)
9. Cordell, V.V., Wongtada, N., Kieschnick, R.L.: Counterfeit purchase intentions: Role of lawfulness attitudes and product traits as determinants. Journal of Business Research 35(1), 41–53 (1996)
10. Wee, C.H., Ta, S.J., Cheok, K.H.: Non-price determinants of intention to purchase counterfeit goods: An exploratory study. International Marketing Revie 12(6), 19–46 (1995)
11. Bush, R.F., Bloch, P.H., Dawson, S.: Remedies for product counterfeiting. Business Horizons 32(1), 59–65 (1989)
12. Siponen, M.T., Vartiainen, T.: Unauthorized copying of software and levels of moral development: Implications for research and practice. Information Systems Journal 14(4), 387–407 (2004)
13. Cottman, L.: It’s not the real thing. Security Management 36(12), 68–70 (1992); Cole, C.A.: Deterrence and consumer fraud. Journal of Retailing 65, 107–120 (1989)
14. Veloutsou, C., Bian, X.: A cross-national examination of consumer perceived risk in the context of non-deceptive counterfeit brands. Journal of Consumer Behavior 7(1), 3–20 (2008)
15. Richetto, D.: Advanced security prevents counterfeit products, Inside Secure - November 4 (2011)
16. Chaudhry, P.E., Cordell, V., Zimmerman, A.: Modeling anti-counterfeiting strategies in response to protecting intellectual property rights in a global environment (2005)
17. Phau, I., Prendergast, G.: ‘Custom-made fakes: A mutant strain of counterfeit products’. In: Proceedings of Globalisation of Business Conference, Cyprus, November 16-18 (1998b)
18. International Trademark Association, Addressing the Sale of Counterfeits on the Internet (2009), `http://www.inta.org/Advocacy/Documents/INTA%20Best%20Practices%20for%20Addressing%20the%20Sale%20of%20Counterfeits%20on%20the%20Internet.pdf` (accessed on July 05, 2013)
19. Chowdhury, B., Khosla, R., Chowdhury, M.: Real-time Secured RFID-based Smart Healthcare Management System. International Journal of Computer & Information Science (IJCIS) 9(3) (2008)
20. Shepard, S.: RFID Radio Frequency Identification. The McGraw-Hall Companies, Inc., USA (2005)
21. Cottman, L.: It’s not the real thing. Security Management 36(12), 68–70 (1992); Cole, C.A.: Deterrence and consumer fraud. Journal of Retailing 65, 107–120 (1989)
22. Die, W., van Oorschot, P.C., Wiener, M.J.: Authentication and authenticated key exchanges. Designs, Codes and Cryptography 2, 107–125 (1992)

23. National Security Agency, The Case for Elliptic Curve Cryptography (2009), http://www.nsa.gov/business/programs/elliptic_curve.shtml (accessed on July 09, 2013)
24. Beller, M.J., Chang, L.-F., Yacobi, J.: Privacy and authentication on a portable communications systems. IEEE Journal on Selected Areas in Communications 11(6), 821–829 (1993)
25. U.S. Government Accountability Office, "Radio Frequency Identification Technology in the Federal Government", 441 G Street NW, Room LM Washington, D.C. 20548 (2005)
26. Glover, B., Bhatt, H.: RFID Essentials. O'Reilly Media, Inc. 1005 Gravenstein Highway North, Sebastopol, CA 95472 (January 2006)
27. Denis, L.: What is WiFi? An Introduction to Wireless Networks for the Small/Medium Enterprise (SME), http://www.openxtra.co.uk/articles/wifiintroduction.php (accessed on February 10, 2007)
28. Bacheldor, B.: Strong sales growth expected for RFID tags, Manufacturers' Monthly (December 10, 2007), http://www.manmonthly.com.au/articles/Strong-salesgrowth-expected-for-RFID-tags_z138655.htm (accessed on February 11, 2011)
29. Enge, A.: Elliptic curves and their applications to cryptography. Kluwer Academic Publishers, Norwell (1999)
30. Menezes, J.: Elliptic Curve Public Key Cryptosystems. Kluwer Academic Publishers, Boston (1993)
31. Lopez, J., Dahab, R.: An overview of elliptic curve cryptography (May 2000)
32. Richetto, D.: Advanced security prevents counterfeit products, Inside Secure - November 4 (2011)
33. Riley, B., Schmidt, A., Tubin, G.: SMS in Financial Services: Accessing Your Customers on Their Terms, TowerGroup (2011), Research is available on the Internet at http://www.towergroup.com