Improvement on RFID Credit Card: Security with Controllable RFID Tags and Encryption Algorithm

CSC 463 Project

University of Victoria

Saige Liu
V00812068

Yubing Ding
V00801106

Kit Ming Yau
V00759389

ABSTRACT

Since 1971, the ancestor of passive RFID, Mario Cardullo's device, be demonstrated, people has found a new technique to facilitate daily life. While more passive RFID has been implemented in real life, the concern of security risk has been raised. This project intends to find a new way to protect information from RFID hackings. We combine a physical switch and software encryption together in the design, and evaluate our idea through research.

1. INTRODUCTION

Radio-frequency identification(RFID) using electromagnetic field to identify tags on the objects automatically. There are two types of tags, passive tags and active tags, both can store electrical information. Passive tags have no internal power source and are powered by electromagnetic energy transmitted from its RFID reader. Passive tags are cheap and widely used for applications such as access control, object tracking and management. Active tags have its own battery which allows them to continuously broadcast signals. They are used in accurate and real-time tracking, and can be functioned under high-speed environments. Active tags have a larger read range compared to passive ones, but they are much more expensive [1].

The original design of RFID is active reader with passive tag. Low cost and developed techniques let passive RFID becomes the most popular one. However, these days more people has questioned its security. Years ago, Hong Kong decides to use smart ID card in 2018 to replace old ID cards which issued between 2003 and 2007[4]. Lawmakers has raised security doubts on using RFID technology on these smart ID cards, because personal information will be sending into air which everyone can access it with specific hacking techniques [3].

For this project, we aimed to provide a better way to improve the security of RFID. We select passive RFID for this research. We test different ways of upgrading the security, both in physical world and software. By combining varies of ideas, we build our best solution for protecting personal information in passive RFID.

2. DESIGN GOAL

Passive RFID has four parts, application, RFID reader, antenna and transponder. Figure 1 below illustrates the whole system.

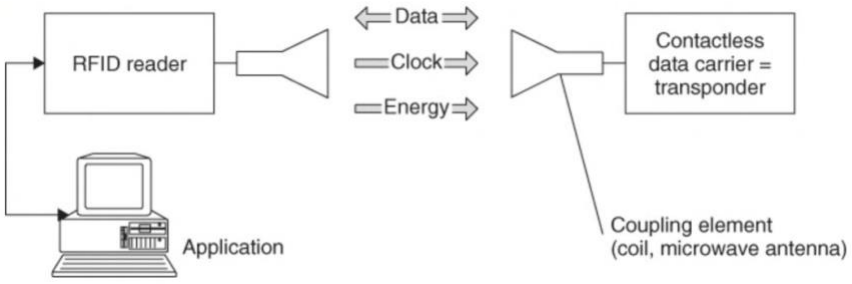


Figure 1: RFID reader and contactless smart card in practical use [2]

Common RFID hacking are RFID spoofing, tag cloning, side channel attacks, SQL injection, cross site scripting, buffer overflow, glue code, RFID viruses and worms. Most of them can be minimized by metal card shields [5]. Card shields are inconvenient if there are too many cards, but this gives us the idea that we can avoid hacking by simply block the signal in the physical world. There is a paper posted by Microsoft in 2010 showing that it is practical to place switches on passive tags to visualize hacking and even prevent it effectively [6]. Figure 2 is the idea card tag that has been designed.

Figure 2: Alternative RFID tag using switches [6]

We also tried to find a way to protect privacy in software. It is a high-risk for data can be access without authorization. Our design is inspired by key lock pair, encrypted data can only be retrieved by specific key. Details are demonstrated in section 4. Encryption algorithm.

3. The physical design: Controllable Two Chips RFID tag

A credit card usually contains a magnetic stripe and an EMV chip. Currently more credit cards have been renovated to have a RFID chip inside. The credit card information in a RFID chip could be easily stolen, by powering up the antenna inside credit card to retrieve information. Even the information is encoded, it can still be decrypted.

To prevent information getting revealed, we present a new RFID system that contains two protection layers: the physical layer and the digital encryption layer. The physical design of controllable RFID credit card has two chips. Either of the chip is connected to the antenna, so when put the RFID tag closes to the reader, only one chip is powered up. By switching the controller, chip A is disconnected and chip B is connected to the antenna, then chip B is powered up. When someone try to copy your RFID credit card information, he/she can only copy the digital information in one chip, not both. The data in both chips combined together is the real credit card information.

3.1 Mock-up Stage

To present our idea, we made a two circuits RFID tag prototype as shown in Figure 3. The materials used are copper coil winded around by 0.08mm copper wires, a LED light and two chips that contain different data.

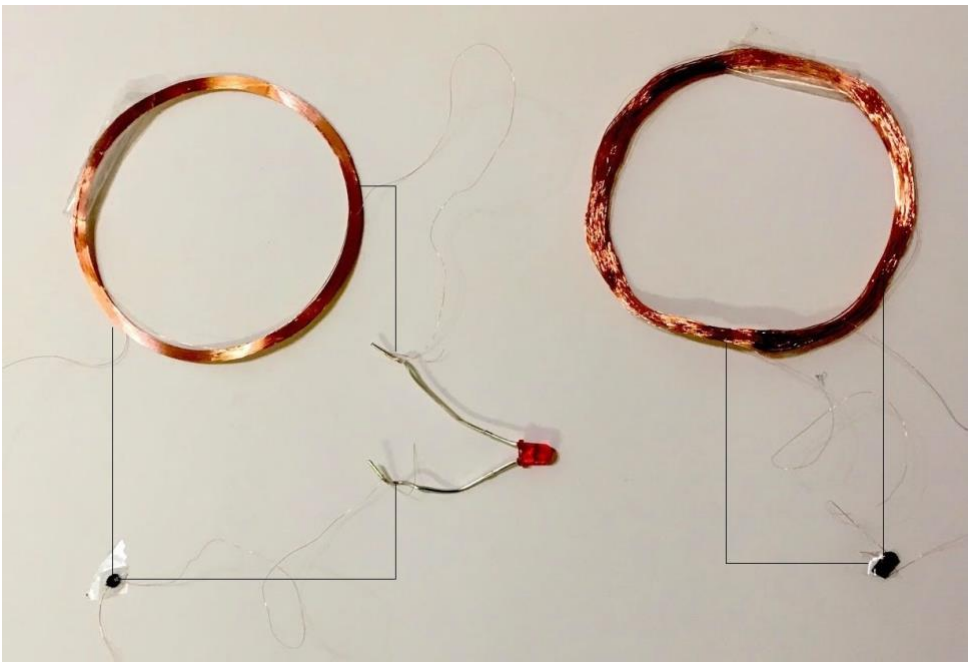


Figure 3: Initial design

One antenna connects a chip and a LED light, the other antenna connects the second chip. When the RFID tag on the left approaches reader, LED lights up and information in this chip is transferred to the reader. Similarly, when the RFID tag on the right approach the reader, digital information stored in chip is sent to reader.

3.2 RFID tag with LED light in real experiment

Adding LED light to present the RFID tag status is a common use in the RFID design world. Here is an instruction posted in 2008. As shown in Figure 4, the RFID tag contains cardboards, conductive copper tape, capacitor, low current LED and insulation tape. RFID IC chip is used in this experiment as shown in Figure 5. [13]

Cardboards are for the tag holder, conductive copper tape is used to build the RFID antenna, capacitor adjusts the capacitance to match coil inductance, and low current LED shows whether the RFID tag is activated. When build the antenna, each loop could not be connected, use insulation tape to separate the current flow.

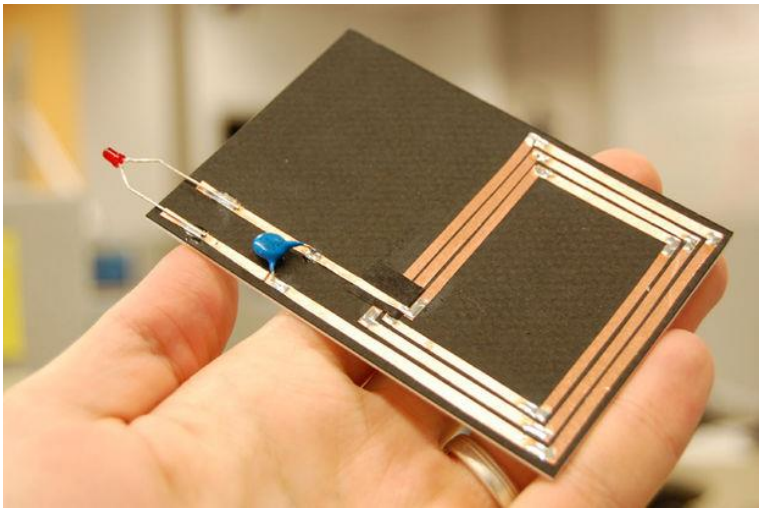


Figure 4: RFID tag with LED light. [13]

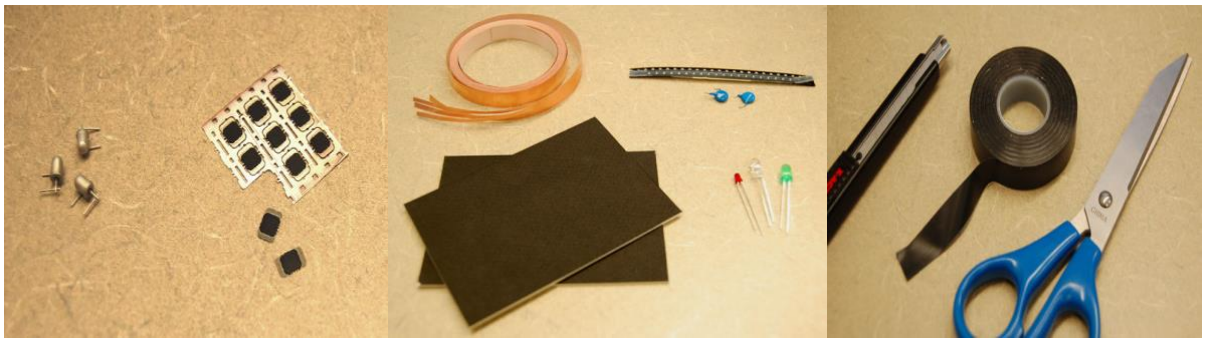


Figure 5: Common material for building RFID tag. [13]

3.3 Visible and controllable RFID tags research

In 2010, the University of Calgary students and Microsoft research published their research on visibility and controllability of RFID tags. [6] They presented a collection of alternative tag

designs. For example, as we discussed in the previous section, they installed a light-emitting diode on the circuit to enable visual feedback.

They also provided audible feedback and tactile feedback implemented by small pezzo speaker and vibro-tactile motor.

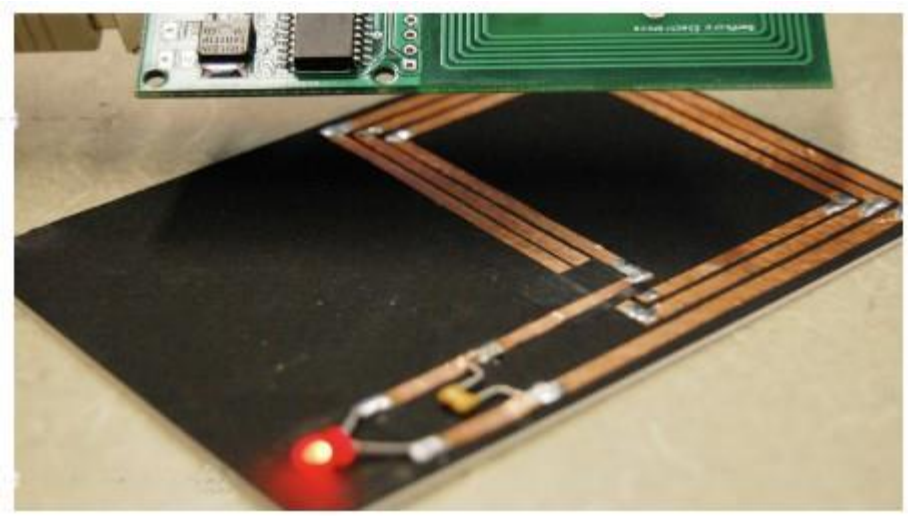


Figure 6: When reader approach the RFID tag, the LED lights up [6]

They investigated on how to make the tag controllable by end users. The main idea is that user can physically disconnect the antenna from the chip. They provided different mechanisms, the explicit control includes: toggle switch, push button, pressure-sensitive switch and touch-sensitive switch; the implicit control includes: tilt switch for tilt-sensitive tag and phototransistor to measure the surrounding light for light-sensitive tag.

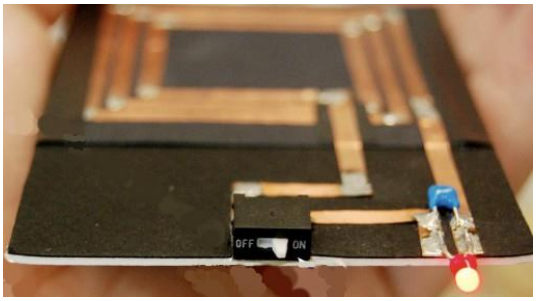


Figure 7: toggle switch active/deactive the RFID tag [6]

3.4 Finalized design in circuit diagram

It has been proved that it's possible to solder LED and toggle switch on RFID tags. To complete the whole design, the initial mock up design needs a switch that can control two circuits simultaneously. SPDT(single pole double throw) switch has three terminals: one common pin and two pins competing for connection to common. [14]

The following Figure 8 is the circuit diagram based on mock up and investments in section 3.2 and 3.3. Our design extends the controllable tag idea by commanding two circuit at the same time, thus enhance the protection of private information.

In this circuit diagram, SPDT switching between connecting chip A to its antenna and connecting chip B to its antenna.

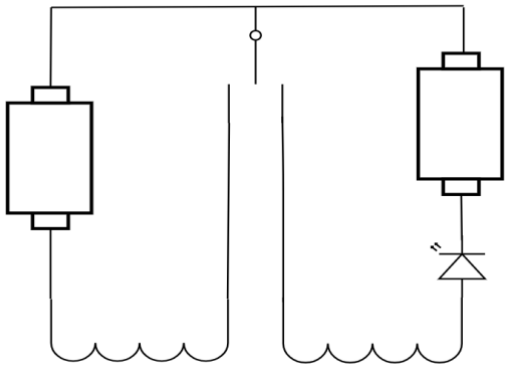


Figure 8: initial circuit diagram based on mock up

Digging more in the electronic area, we find that two antennas are not necessary. The typical LED resistance is low when placed forward bias. While placed reversely, there is no current pass through. Since the LED resistance is low, an identical antenna can power both chip A and chip B

with low current LED. A more simplified electrical diagram is created as shown in Figure 9. The SPDT switches connection between chip A to antenna and chip B to antenna.

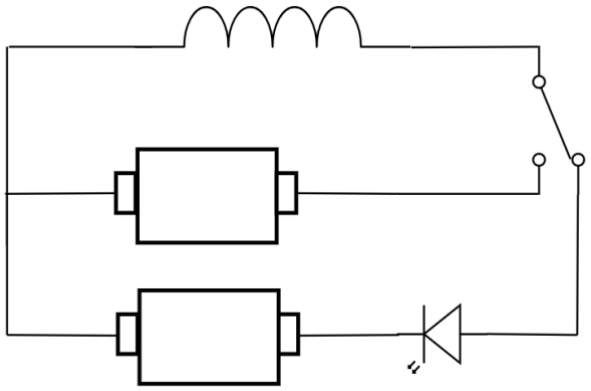


Figure 9: Controllable two chips RFID tag

3.5 Coupling method and Signal Frequency.

There are four types of coupling methods: close coupling, capacitive coupling, inductive coupling and radiative coupling. Inductive coupling which uses the magnetic field to match the reader and tag, is used in this design. [15]

Inductive coupling depends on magnetic field of the reader, and only occurs in the near-field. The electrical flow through the reader's antenna produce a magnetic field. When the tag's antenna is within the magnetic field, it generates a current in the circuit to power up chip and LED. When using inductive coupling, increase the amount of current generated in the tag is possible by increasing the number of loops of coils.

LF and HF passive RFID tag both support inductive coupling. Most credit card are using HF(13.56 MHz) standard. Our design is also using HF(13.56MHz) as the wave frequency.

The strength of the magnetic field is proportional to 1/r^3, r is the radial distance from the reader antenna. To enable inductive coupling, the tag should be placed at least 0.16 times the wavelength away from the reader. [16]

We have the wavelength frequency formula

$\lambda = v/f$

Where: λ = Wavelength of light, meters

v = Velocity of light (c = 3.0 x 108 m, for speed of light if not otherwise defined)

f = frequency of light, Hz

With wave frequency equals to 13.56 megahertz, wave speed 3x10^8 m/s, we get the wavelength equals to 22.12389m.

0.16 x 22.12389 = 3.5398 meters

Using inductive coupling method and 13.56 MHz, the RFID tag should be placed less than approximately 3.5 meter from the reader.

4. The encryption algorithm

Based on our design, there are two individual RFID tags in each card which are connected by one circuit. When a new card issued, the information is cached for encryption. Most of encryption function in language library are irreversible, but our design needs an algorithm to generate key for decryption. We develop our own algorithm (Crypt::random_str_appending_encrypt($input)) to encrypt by appending random string on original data. For example our algorithm receives ‘Hello World!’ as input string, and it

(Crypt::genSalt()) generates a random salt ‘3)pM5’ with the random appending position 7 (Crypt::random_append_position($input)). The random salt is appended after the seventh character which is the position after ‘W’. The output of the encryption should be ‘Hello W3)pM5orld!’. This output updates the input string for further appending, while the appended information is stored as the decryption key. This process designed to repeat till the string size is greater than 1024 in this case.

When the algorithm encrypted the input to greater than 1024 characters, the algorithm should contain two data string in the memory. The encrypted data string should looks like a random generated string, and the decryption key contains information for removing appended strings. To reinforce the protection of data, we encode the two data strings differently. Our algorithm encode the encrypted data string in ASCII code(Crypt::string_to_ascii($string)), while the decryption key is encoded in BASE64(Crypt::genSalt()).

The two data strings are now ready to be written into the RFID tags. Since both tags are powered by the same circuit, switching controller helps to ensure the data strings goes to the right tags. The data strings are sent to the RFID reader, and then be written into the RFID tags. When both tags contains data string, a checking is required to ensure both the encrypted data and decryption key exist in the same card.

While reading the tag, RFID antenna powers up the tags and RFID reader can read the data within a certain range. RFID reader is designed to handle multiple tags with the collision avoidance algorithm. Like other wireless connections, congestion window in tags are set after

being notified by the reader that the system is busy. Our design has a controller on the circuit which ensure only one RFID tag is activating. This improves the accuracy for reading and the security of the card by limiting the number of tags that a reader can read. The reader receives two input data strings within 2 seconds(Crypt::begin()). So the reader and the terminal for processing have to cache the first input for 2 seconds then flush cache. For our code(Crypt::operate()), the PHP code stored these strings into SESSION for maximum 5 seconds as we have to input strings manually. While with the help of circuit switching, the time allowance should be shortened, the reaction time for switching the controller should be limited to 1.5 seconds. As the decryption key is BASE64 encoding and the data is ASCII encoding, they can be distinguished by the algorithm. Users do not need to tap in specific orders. Decryption (Crypt::random_str_appending_decrypt($text, $salt)) begins if and only if two input are cached and their format matched with data and key pair. Then the two data string are decoded and decrypted by removing appended strings. The original text string is now recovered and can be used for further authorization.

[RFID security] Encryption & Decryption Code in PHP

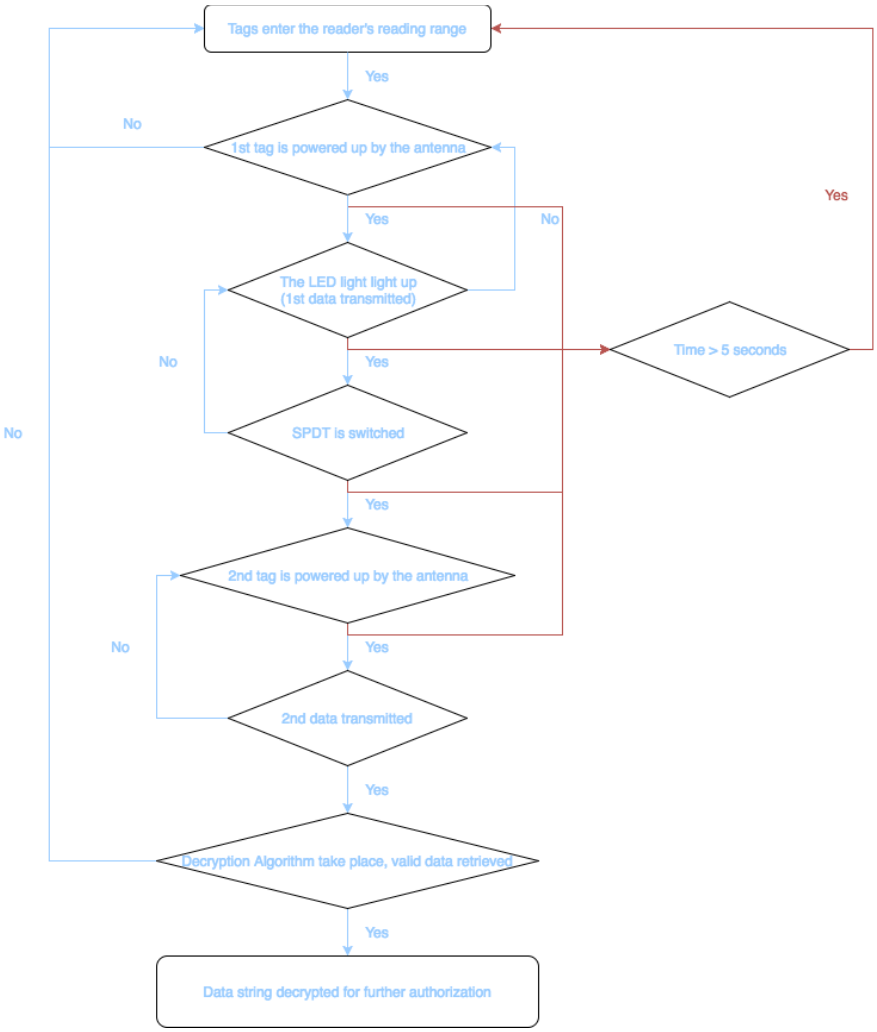
```
<?php if(!session_id()) session_start();

error_reporting(0);

class Crypt{

	public function begin(){
	(isset($_SESSION['expire']) && $_SESSION['expire'] < time()) ? (session_unset('input')) :
$_SESSION['expire']=time()+5;
	if(!isset($_SESSION['input'])) $_SESSION['input'] = array();
	array_push($_SESSION['input'], $_POST['text']);
	Crypt::operate();
	}

	public function check(){
	print_r($_POST);
	print_r($_SESSION);
	}

	public function genSalt() {
		$charset =
'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890123456789_+-.,!@#$%^&*()|';
		$randString = "";
		$target = rand(3, 15);
		for ($i = 0; $i < $target; $i++) {
		$randString .= $charset[mt_rand(0, strlen($charset) - 1)];
		}
		return $randString;
	}

	public function operate(){
	if(count($_SESSION['input']) < 2)
		return 0;
	foreach($_SESSION['input'] as $input){
		if(base64_encode(base64_decode($input)) == $input)
		$salt = $input;
		else
		$text = html_entity_decode($input, ENT_QUOTES, 'UTF-8');
	}
	session_unset('input');
	if(!$text)
		echo "hashed string is missing.";
	elseif(!$salt)
		echo "decrypt key is missing.";
	else
		Crypt::random_str_appending_decrypt($text, $salt);
	}

	public function random_append_position($text){
	return (strlen($text) < 20) ? strlen($text) / 2 : mt_rand(0, strlen($text) - 1);
	//return mt_rand(0, strlen($text) - 1);
	}

	public function random_str_appending_encrypt($text){
	$key = '';
	$result = $text;
```

```
		$i = 0;
		while(strlen($result) < 1024){
			if($i > 0) $key .= ';';
			$position = Crypt::random_append_position($result);
			$salt = Crypt::genSalt();
			$key .= $position.':'.$salt;
			$result = substr_replace($result, $salt, $position, 0);
			$i++;
		}
		echo base64_encode($key);
		echo "\n";
		$ascii = Crypt::string_to_ascii($result);
		echo $ascii;
		}

		public function random_str_appending_decrypt($text, $salt){
		$key = base64_decode($salt);
		$salts = explode(';', $key);
		$i = 0;
		//print_r($salts);
		foreach($salts as $eachsalt){
			$temp = explode(':', $eachsalt);
			$thissalt[$i]['place'] = $temp[0];
			$thissalt[$i]['number'] = strlen($temp[1]);
			$i++;
		}
		$result = $text;
		for($j=$i-1;$j>=0;$j--){
			$result = substr_replace($result, "", $thissalt[$j]['place'], $thissalt[$j]['number']);
		}
		echo $result;

		}

		public function string_to_ascii($string){
	$ascii = '';
	for ($i = 0; $i < strlen($string); $i++)
		$ascii .= '&#'.ord($string[$i]).';';
	return($ascii);
		}
}
if($_POST["method"] == 'RanStrAppEn')
		Crypt::random_str_appending_encrypt($_POST['text']);
elseif($_POST["method"] == 'RanStrAppDe')
		Crypt::begin();
else
		Crypt::check();
?>
```

There are open source encryption methods on GitHub, such as Php-Encryption [7] in PHP by defuse, Endecrypt [8] in node.js by dcodeIO, TashfeerClass [9] in PHP and Java language by tarekmahedy, Any-Key-Rot-Encryption-Decryption [10] in Python by gdegy and etc. These languages are common for web development, with the help of the Point of Sale eXtended

Markup Language (POSXML) [11], they can create web app for POS terminal. While in-shop system are mostly written in C/C++, RSA-Encryption [12] in C++ by ma-anjum95 could be considered. These algorithms are open sources, so it is recommended not to be implemented without modification.

5. Case Study



Unlike other security protocols in RFID, we need two tags for verification. Compare to credit card wireless payment and mobile payment, our design is more secure and need not to be relied

on other devices. This design can be used in high security facilities which need multiple identities authorizations. And unlike the Hash Lock protocol, our algorithm will not query the database before a valid information retrieved.

6. Conclusion

RFID is a quick matching method for object identifying, it is widely applied in different area. Passive RFID tags are used for wireless payment such as VISA Paywave. Though passive tags are less secure to the active tags, the security risks of this method have been raised. The information in RFID tags can be retrieved by mobile RFID readers anonymously, 2 or more step verifications should be considered as a protection. Our design helps preventing retrieve data from both tags without authorization, while authorization required both tags for original data retrieve. And our design does not require extra electronic devices or equipment for verification, it keeps users away from low battery anxiety.

Reference

[1]Finkenseller, Klaus. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition.* Chichester: John Wiley, 2010. Google books. Web. 5 Dec. 2017. https://books.google.ca

[2]Smiley, Suzanne. "Active RFID vs. Passive RFID: What's the Difference?" *RFID Insider.* atlasRFIDstore, 10 July 2017. Web. 5 Dec. 2017.

[3]Danny, Lee. "Lawmakers raise security doubts on using RFID technology in new Hong Kong smart ID cards." *South China Morning Post.* N.p., 07 Jan. 2015. 6 Dec. 2017

[4]SCMP Editorial. "Privacy crucial for new identity cards" *South China Morning Post*, 3 Dec. 2017. Web. 3 Dec. 2017.

[5]Grover, Amit. Berghel, Hal. "A Survey of RFID Deployment and Security Issues." *Journal of Information Processing Systems* 7 (2011): 561-580. KOREASCIENCE. Web. 6 Dec. 2017

[6]Marquardt, Nicolai, et al. Visible and Controllable RFID Tags, ACM, 2010, doi:10.1145/1753846.1753917.

[7]"Github - Defuse/Php-Encryption: Simple Encryption In PHP." *GitHub repository*. N.p., 2017. Web. 2 Dec. 2017. https://github.com/defuse/php-encryption

[8]"Github - Dcodeio/Endecrypt: Password Based En-/Decryption Of Arbitrary Data With And For Node.Js. Http://Dcode.Io." *GitHub repository*. N.p., 2013. Web. 2 Dec. 2017. https://github.com/dcodeIO/endecrypt

[9]"GitHub - tarekmahedy/TashfeerClass: simple php,Java class for text encryption and decryption with password" *GitHub repository*. N.p., 2014. Web. 2 Dec. 2017. https://github.com/tarekmahedy/TashfeerClass

[10]"GitHub - gdegy/any-key-rot-encryption-decryption: encrypt and decrypt any text with any key" *GitHub repository*. N.p., 2016. Web. 2 Dec. 2017. https://github.com/gdegy/any-key-rot-encryption-decryption

[11]"Posxml Protocol Specification Version 7.1 / Standard." *Voicecom.ee*. N.p., 2012. Web. 4 Dec. 2017. https://voicecom.ee/media/filer_public/2013/01/22/vcomt2appl_posxml_71_std.pdf

[12]“GitHub - ma-anjum95/RSA-Encryption: An implementation of RSA Public Key Encryption Algorithm with Key Generation, Encrypting and Decryption data.” *GitHub repository*. N.p., 2014. Web. 2 Dec. 2017. https://github.com/ma-anjum95/RSA-Encryption

[13] nmarquardt. "RFID Reader Detector And Tilt-Sensitive RFID Tag." *Instructables.* N.p., Web. 26 Nov. 2017. http://www.instructables.com/id/RFID-Reader-Detector-and-Tilt-Sensitive-RFID-Tag/

[14]Jimbo. “Switch Basic: poles and throws, open and closed” *sparkfun.* N.p., Web. 01 Dec. 2017.

[15]Smiley, Suzanne. “Operating Principles: Coupling” *RFID insider*. atlasRFIDstore, N.p., Web. 5 Dec. 2017.

[16]Mark, Roberti. “Why Can't RFID Systems Use 2.4 GHz Inductive Coupling to Communicate?” *RFID Journal.* N.p., Web. 6 Dec. 2017