# Pseudonym and Privacy Using Quantum Key Distribution (QKD) in E-business

**Sharipah Setapa, Norazah Abd Aziz, Mohd Aminudin Mohd Khalid, Muhammad Reza Zaba, Azimah A bd Kadir**

**Summary**
Pseudonym ID now play important role in electronic e-commerce and e-service. For e-business payment gateway is the key to establish and serve customer need and payment. Customer will communicate without using their true identity in order to protect privacy. In spite of this, there is certain weakness in pseudonym because it is traceable and linked it with a user true identity. In classical way to generate a pure random number is impossible since the program was used is deterministic. QKD technique guarantees a secure communication with a pure randomly identical key between two parties. This paper focus on the pseudonym ID by using QKD to make the identity of user is untraceable and less linkable from the perspective of user identity privacy.

***Keywords***
*Privacy, Pseudonym, untraceable, linkable*

## 1. Introduction

Internet has a widespread and it allowed products information apply to be presented to the world. With that, e-business is been established. In order to handle a transaction, a payment gateway is used to authorize the payments [1]. It is involved security because it exchanges confidential information. Threats to privacy are a main concern to consumer. A user will use a pseudonym to conceal the identity when a user places an order and transaction. There are good reasons for a user to use pseudonym such as:

- To avoid interfere with career
- To protect personal life from outsider

If the pseudonym can be link it with any bad activity, from the legal perspective it will not protect user from any legal action [2]. Privacy is needed because of three factors which are money, reduce risk and provide trust [3]. Trust it is necessary to attract user or customer. Without trust business will be collapsed. User can registered telephone number as a pseudonym ID to communicate. But the availability to trace and link user identity is higher compare with DNA and account bank as a pseudonym [4]. This is because registered telephone number is advertised. Due to that a new pseudonym concept of privacy-enabling personalization is needed. In order to make the identity of user is untraceable and less linkable an anonymizer and infrastructure of QKD system is needed.

Manuscript received August 5, 2011
Manuscript revised August 20, 2011

## 2. Anonymity

As an internet user our online activities are been monitored, logged, detected without prior notification. This is a form of intervention to user privacy. Any context when the user conducts or execute online the ordering is linkable to user true identity transaction or place the order is linkable from user true identity.
Encryption method is used to protect the content, but it does protect the particular owner's of the communication [5]. For this, anonymity method is to use to hide the internet user identity. One type of anonymity method uses pseudonym to protect user identity. It may be a good or bad based on user. If they use to deliver something that is not good, it will make an investigator a very difficult situation to trace the owner. However anonymity is difficult or tedious to preserve when payments, physical goods and non-electronic services are being exchanged [6]. The anonymity is getting higher if the pseudonym use seldom. This will make the context with the data is reduced. Other things is the frequency of changing the pseudonym if higher, the less it can be linked with user.

## 3. Pseudonym

Pseudonym been introduced as a technical concept in cryptography to achieve anonymity and unlinkability. There are 5 categories pseudonym which are:

- Person pseudonym,
- Member (role) pseudonym
- Relationship pseudonym
- Session pseudonym
- Transaction pseudonym [7]

Digital pseudonym such as public key is generated by user. When using pgp there are two key which public and private key. In email, users send the email and encrypt it using public key. Recipient will decrypt it using private key [8]. The key is random but it is not one time key or one time pseudonym.
Different messages can be linked with same identity. By exploiting a trivial HTTP to channel the attack, hackers have successfully stolen credit card numbers from online store's database. By retrieving the information such as

names, account number, email address and transaction histories, it means a fixed names or account number (pseudonym) can be link with the user identity. As a result this will create a bad publicity, lost of customer's trust and reduce order to the company [9]. The most important thing customer will declined to interact with the online database website which have been hacked due to breach of their privacy. Although customer is using pseudonym ID to interact, but normal and fixed pseudonym can be trace. Cookies and history can give away the username used by the person on the desktop. Table 1 showing window username use such as xxx_1 and administrator. Users play two roles as shown in table 1.

Table 1: Using Cookie to trace the identity of the user

| *Window Username using cookie* |
|---|
| Cookie:xxx_1@website |
| SYSTEM |

Fig. 1 Payment gateway with Client ID

When user place the order the identity of user is changing from window username. User will use payment gateway to place the order with different name from user machine such as abc123 as shown in figure 1. At first glance this doesn't give any information to us, until it can be linked with database, invoice or company's information about who is abc123. Cookies and history is also used to know the date and website was accessed by user which is not transparent to everybody. But in ebay's website, information of seller and item is listed which is transparent to public as shown in figure 2.

Fig. 2 Individual information regarding price and seller information [9]

With a clientID which is unidentified and unobservable while did the transaction user will think that their privacy is secure. During registration an ID is created and all personnel information is stored in one located area. This is like centralized architecture which enables the public to access the information.

Certain pseudonym is combined with time stamp but it can be predicted, although it takes a lot time to know what is the pseudonym been use by user. A pseudonym needs to change from time and time whether manually or automatically. Reputation data for different pseudonym is only one global database. This can enable intruder to trace the identity of the user.

In internet environment especially in e-business or e-service, almost user will communicate using pseudonym which is choosen by user without random parameter. It is based on user's creativity, provided it is traceable by the creator and also able to hide their real name.

Three elements which are order confirmation, payment gateway interface and transaction database interface are use in e-business over encrypted channel using SSL. Another aspect of privacy is transaction as shown in Figure 3[10]. This transaction can be linked with other transaction if further analyses have been done. Unlinkability only happens when none of this transaction is linkable [11].

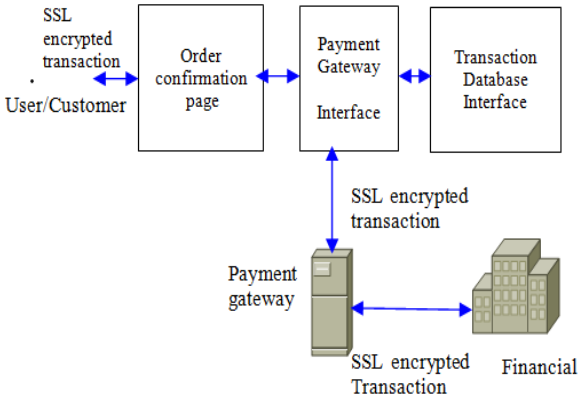


Fig. 3 Transaction interface which provide linkability

## 3.1 Transaction

Microsoft, Symantec, SANS, hacker will post the security issue in internet. On some occasion privacy is less prioritized over security. The result of privacy has direct impact on the individual. Thieves will use personal information to trade user payment record and manipulate it. .User e-transaction carries a lot of related information about individual which can be linked with another transaction. During e-transaction it is important to ensure unlinkability. E-business uses web browser, which enable user to view the source code on the web hypertext markup language (HTML) format using notepad or web editor and etc. This is another method form of less privacy system.

### 3.1.1 Transaction processing

Although user interact using pseudonym, but transaction status can be tracked by the organization. Threat which comes from internal is more dangerous because it betray

the internal user trust of the organization. Ethics such as integrity is been violate [12].
User will think the transaction process is safe. Such Application has a weakness, there are cases that the information was disclosed accidentally and temporary file remain in the system and can be accessed by other user. For web application, it is better for temporary file's path to be placed in other than web document root directory.

3.1.2 Transaction database interface
Database is a heart of the web where information regarding customer is store. Security is new to database and this cause a vulnerabilities. Database interface is a focus for the attack as shown in figure 3 [13]. Sometimes technology gives the advantages of the intruder to retrieve information easily using the weakness of input validation which not been validate properly. By send unusual input attacker can gain access to database or which not practice the input validation. The input validation can reduce and defend from any malicious attack. It is suggests all information regarding username, credit card, personal information are not keep in one database, in order to minimize the risks.

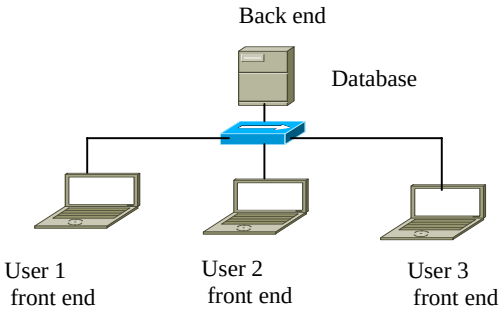


Fig. 4 Front end and Back end

In internet, million of computers are connected through TCP ports 80 or 443 to the World Wide Web. User information is retrieve using this port because firewalls have to let web traffic go in. This gives the opportunity to attack encrypted information in the encrypted stream by intruder.
The shared secret can be a password or passphrase. The different is how strong it can protect a user. A pseudonym also can be a shared secret which can be use an identity for user to communicate. In ordinary privacy enhancement system such as client and e-service provider, pseudonym ID is used to protect user identity so that user is anonymous to e-service provider. The weakness of pseudonymn ID which been address above is due the method commonly used to create pseudonym ID is too structured and thus predictable.
Current pseudonym ID is generated using HASH function which using user identity and timestamp as input to HASH function to change the value of pseudonym ID for each communication session so that it is less linkable to user identity. However, timestamp method is fixed, structured and predictable which enable hacker to trace the linkability. This exposes the system to identity theft attack.

## 4. Construction Pseudonym with Quantum Key Distribution

A QKD system consists of a quantum channel and classical channel. It can be used to generate and distribute secret key together with classical algorithm such as Rivest, Shamir and Adleman (RSA) and key management using Diffie-Hellman. QKD generates and exchanges the secret keys in optical fiber, by using Quantum mechanics and exchanging photons, a secret key will be created. The beauty here is that quantum mechanics guarantee that the key cannot be copied or intercepted [14] [15]. Any changes to the photon will make the properties of photon changed
In the classical method without using QKD, to generate a pure random number is impossible since the program was used is deterministic. One of the possible alternatives is to solve the predictability of pseudonym by using method provided by QKD network. In order to create pseudonym id based on quantum key the, QKD technology will be used with the pseudonym which is priory create in classical way. The characteristic of QKD network enable incorporation of random process that will complicate the traceability of user identity as shown in figure 4.

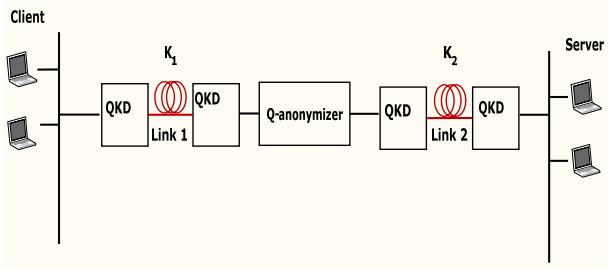


Fig. 5 Q-anonymizer to anonymize user identity [16]

In figure 4 the process begins as below:

- Client will send a request for private communication to Q-anonymizer in order to communicate with server
- Client will request $K_1$ from its QKD and key $ID_1$ to Q-anonymizer
- Q-anonymizer will retrieve $k_1$ by using Key $ID_1$ from its QKD
- Q-anonymizer will request $K_2$ and send the key $ID_2$ to server
- After initialization step, the q-anonymizer will react

as shown below

- Upon receive key ID, q-anonymizer will retrieve $K_1$ through link 1. Communication will establish between client and q-anonymizer.
- Server will receive key ID from q-anonymizer. Using Key ID, server will retrieve $K_2$ from QKD system through link 2. Communication will establish between q-anonymizer and server. $K_1$ and $K_2$ is combined with pseudonym (usual) such as social security number, DNA, telephone number, in order to get quantum network based pseudonym ID.

## 5. Conclusions

Unlinkability and anonymiser is dependable on each other. Privacy needs unlinkability and anonymizer to implement it need anonymizer. Infrastructure is used to support anonymizer. Pseudonym is a choice for the person who did not want his/her family, colleagues to know his activity or interest. It gives total- freedom for them to express something or do e-business. Percentage of the pseudonym to be easy to link with the user is dependable on infrastructure used because pseudonym alone still can be linked and need a secure infrastructure that have the capability to provide randomness without depending to timestamp in order to achieve anonymity and unlinkability. The structure of pseudonym which been study by intruder will make the anonymity decreases.

What we recommend is a system with a virtual transaction using one time pseudonym and database. A key which is one time key, session and random should explored in order to provide that unlinkability pseudonym together with the database. Another way to hide our identity is to possibly reduce our communication using internet except for important things. Although this suggestion may seem conventional this is the best option to do that until one time pseudonym, one time random and one time database is achieved. QKD is not a total solution in the security. It is a piece of the security project and depends on conventional network for encryption, transferring and storing of data.

## References


[1] Wikpedia, “Payment Gateway”. [Online]. Available: http://en.wikipedia.org/wiki/payment_gateway. [Accessed: Oct. 13, 2010]. (General Internet site)

[2] Moira Allen, “Should you Use Pseudonym,” 2001. [Online]. Available: http://www.writing-world.com/rights/pseudonym.shtml. [Accessed: Oct. 13, 2010]. (General Internet site)

[3] Data Protection Technical Guidance Note: Privacy Enhancing Technologies (PETs), Information Commissioner’s Office (ICO), April 2006. [Online]. Available: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf [Accessed:Oct 6, 2010]. (General Internet site)

[4] Privacy Design in the U-ATM, chapter 6

[5] Michael A.Caloyannides, “Privacy Protection and Computer Forensics,” Second edition, Artech House, Computer Security Series, 2004.

[6] Yang Wang et.al, “PLA-based Runtime Dynamism in Support of Privacy-Enhanced Web Personalization”, Proceedings of the 10th International Software Product Line Conference, Baltimore, MD, IEEE Press, 2006.

[7] Gerrit Bleumeer, Henk C.A.Van Tilborg, Encyclopedia of Cryptography and Security, International Federation for Information processing, Pseudonyms, 10.1007/0-387-23483-7_327,2005, [Online]. Available: http://www.springerlink.com/content/j64q39216t0235g1/fulltext.htm. [Accessed: Oct 11 2010]. (General Internet site)

[8] Andreas Pfitzmann, Marit Kohntopp, Adam Shostack, “Anonymity, Unobservability and Pseudonymity-A proposal for Terminalogy,” Draft v0.6 November 26 2000.

[9] http://www.ebay.com.my

[10] Stuart McClure, Saumil Shah, Shreeraj Shah, “Web Hacking Attacks and Defense,” Addison-Wesley,2003

[11] Ben Laurie, “Privacy”, www.apache-ssl.org/privacy.pdf, September 26, 2004 [Accessed:Oct 21, 2010]. (General Internet site)

[12] Sean M.price , “Security Weaknesses of System and Application Interfaces Used to Process Sensitive Information,” Information Security Management Handbook, Auerbach Publications, 2009. [Online].Available: http://www.infosectoday.com/Articles/Security_Weaknesses_Interface.htm. [Accessed:Oct 19, 2010]. (General Internet site)

[13] MSDN, “Delivering your application,” Chapter 8 [Online]. Available: http://msdn.microsoft.com/en-us/library/aa188209(office.10).aspx. [Accessed:Oct 21, 2010]. (General Internet site)

[14] [14] Andrea Pasquinucci, Quantum Cryptography Pros & Cons, UCCI IT

[15] [15] Alan Mink, Sheila Frankel and Ray Perlner, National Institute of Standard and Technology (NIST), 100 Bureau Dr., Gaithersburg, MD 20899, International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009

[16] [16] Chip Elliot, Building the Quantum Network, New Journal of Physics, 12 July 2002

**Sharipah Setapa** has received degree in bachelor of Computer and Communication engineering from Universiti Sains Malaysia (USM), Malaysia. She currently working in MIMOS Berhad

**Norazah Abd Aziz** graduated from the University Technology Malaysia in Computer Science. Currently, she is pursuing study in Master of Science degree at University Putra Malaysia. Her primary research area is in information security and trusted computing. Presently, she is a researcher at MIMOS Berhad and involved in trusted computing development projects

Received Bachelor of Engineering (Information Engineering) from Tokyo Institute of Technology in year 2000. Currently serves as Staff Researcher in Mimos Berhad in the area of key management and cryptographic engineering.

**Muhammad Reza Z'aba** received the PhD in Information Technology (Information Security) at Queensland University of Technology, Australia in 2010. He is currently a Staff Researcher at MIMOS Berhad. His research interest include cryptography particularly in the design and analysis of block ciphers.

**Azimah Abdul Kadir** is an industrial experienced and a practitioner in the field of Intellectual Property Management and Commercialization. She holds a Master in Intellectual Property under the Law Faculty of the National University of Malaysia (UKM). She is currently the Head of the Intellectual Property Management Department (IPMD) of MIMOS Berhad, a government owned Research Institute under the Ministry of Science, Technology and Innovation of Malaysia.

She has served a Malaysian MNC automotive industry in the Intellectual Property Management field for 13 years prior to joining MIMOS.

In MIMOS, she introduced and developed the Intellectual Property Strategies and Policies for the ICT intangible asset management, commercialisation and valuation of ICT intellectual properties for MIMOS and its Technology Recipient Companies. She is currently the Intellectual Property Strategist and trainer on innovation creation framework for MIMOS technology clusters namely, Advanced Mathematics, Information Security, Psychometrics, MEMS and Nano, Micro Energy, Product and Software Development, Advanced Informatics and Surveillance, Wireless Communication, Microelectronics and Wafer Fabrication.

She has co-invented 7 patent pending in the field of Information Security and Advanced Informatics.