Title	Privacy-preserving advance power reservation
Author(s)	Chim, TW; Yiu, SM; Hui, LCK; Li, VOK
Citation	IEEE Communications Magazine, 2012, v. 50 n. 8, p. 18-23
Issued Date	2012
URL	http://hdl.handle.net/10722/192722
Rights	©2012 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE

Privacy-Preserving Advance Power Reservation

T. W. Chim, S. M. Yiu, Lucas C. K. Hui, and Victor O. K. Li, The University of Hong Kong

ABSTRACT

Smart grid is considered to be the next generation power system. Integrating information and communication technology, power electronics, and power system technologies, smart grid reduces excess power generation by better matching power generation with customer demands, and facilitates renewable power generation by closely monitoring renewable energy source status. Such a large-scale network may be subject to various attacks. In particular, authentication and user privacy preservation are considered two major security concerns. In this article, we first highlight the importance of smart grid security. Next we introduce a new power request paradigm in which a customer is allowed to submit a power usage plan in advance. We then propose a secure and privacy-preserving power request scheme as a solution to this problem. To achieve the privacy-preserving property, our scheme employs two cryptographic techniques: anonymous credential and blind signature. We conclude this article by discussing the security and performance issues of our proposed scheme.

INTRODUCTION

Smart grid is considered to be the next generation power supply network. It is regarded as environmentally friendly because of two reasons. First, through the communication network of the system, the actual electricity demands of customers can be obtained in advance to reduce excess electricity generation. Second, it facilitates renewable energy power generation. Due to the intermittent nature of renewable generation such as solar and wind power, increased renewable penetration causes instability in the power grid. Smart grid, with its sensor and communication network, allows the system to better anticipate problems and make appropriate control decisions, thereby improving system stability.

The smart grid project was initiated by the European Union in 2003 [1]. At around the same time, the U.S. Electric Power Research Institute started the IntelliGrid project [2] while the U.S. Department of Energy started the Grid 2030 project [3]. Under the Energy Independence and Security Act of 2007, the National Institute of Standards and Technology (NIST) is responsible for coordinating the development of a framework for information management to achieve interoperability of smart grid devices. In early 2010, NIST released a report [4] that describes the potential components of a smart grid. Building a smart grid power system is an important engineering project in most developed or developing countries.

To facilitate our discussion, we simplify a smart grid into three basic layers (Fig. 1):

- Power generators
- Substations (part of the transmission network)
- Electric appliances being connected to a smart meter

The smart meter will send demand information (e.g., power usage plan) in advance to the control center through wired or wireless networks (e.g., the Internet). If accepted, the control center will adjust the power generation accordingly.

The security of a power supply system is also a major issue in any country. It is a potential target for terrorists. The future design of a smart grid system tends to make use of public Internet connections (e.g., from smart meters to substations). As such, a smart grid may be more easily affected by computer worms or viruses like the Stuxnet virus [5] which infected Iran's nuclear installations in 2010. Thus, before a smart grid system is deployed, it is critical to make sure that it is fully secure. In fact, the security problems have been actively discussed within the community (e.g., [4]). For the generator-to-substation communications (i.e., the closed system in the old days), some security measures are already in place in the extended version of SCADA [8]. On the other hand, not much research has been done on the substation-to-consumer communications yet.

There are two major security problems, sender authentication and user privacy preservation, for these communications as described in [6, 7]. Power request (or the power usage plan) will be sent by smart meters to the corresponding substation. Authentication of the sender is needed before the request is sent to the control center; otherwise, a trivial denial of service attack can easily be launched. While authentication is necessary, the privacy of the sender must be preserved. Otherwise, by observing the power usage plan of a family, it is easy to know when the family is not at home [6]. Obtaining this

0163-6804/12/$25.00 © 2012 IEEE

information enables a criminal to break into one's apartment at the right moment. Similar concern also applies to commercial customers who do not want others to know when their offices are empty.

In this article, we first introduce a new power request paradigm. We then propose a scheme to solve the security problems. Our solution can preserve the privacy of the customers not only from third parties, but also from the substation and the power operator. At the same time, our scheme provides authentication to prevent hackers abusing the system. The core techniques used in the scheme are two cryptographic primitives: anonymous credential and blind signatures. The scheme is also able to compute the charges of each customer based on the amount of electricity requested during peak and non-peak hours despite the fact that the authentication is done anonymously.

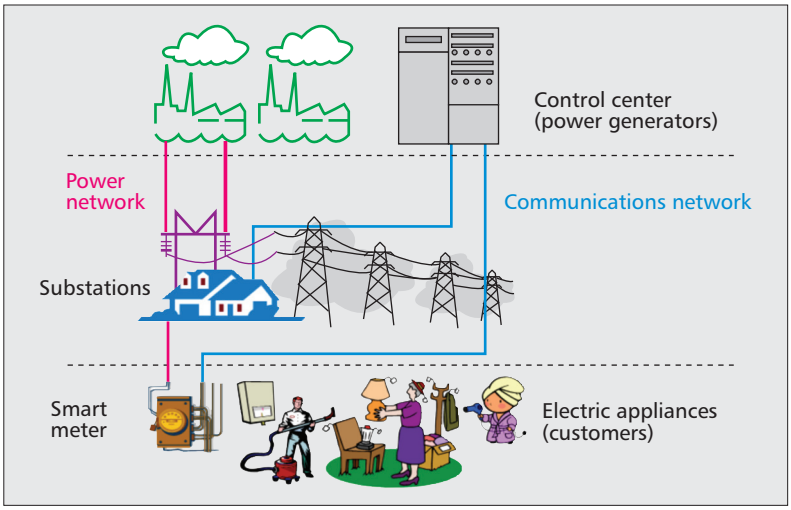

Figure 1. *A simplified smart grid architecture.*

The New Power Request Paradigm

Presently, a customer does not need to request power because a traditional power system tries to estimate the electricity demand (the load) and generates enough electricity to satisfy the load. Spinning reserves[1] are used to cover any potential shortfall due to an underestimate of the load. Any excess generation due to an overestimate of the load and the spinning reserves lead to waste. The impact is even worse for those generators operating on fossil fuel due to the pollutants released into the environment.

Smart grid may alleviate this problem. Power is generated based on customers' demands. How can the power operators know customers' demands? The answer is that customers need to request power supply. Of course, it does not make sense to require a customer to request power each time he/she needs to turn on a small electric appliance such as a mobile phone charger. Normally, the power operator tries to maintain a basic power level that can satisfy most customers' average needs. Then when a customer thinks that he/she needs more power to turn on heavily loaded electric appliances such as heaters or air-conditioners sometime in the future, he/she is required to make additional power requests. These requests can be sent at different time periods such as one day ahead or one week ahead, but not in real time.

Reference [9] is the first scheme that allows customers to make power requests in a privacy-preserving manner. They introduced the problem and proposed a solution, but the power request model is not realistic. They assume that a customer makes an additional power request every time the basic power level cannot fulfill his/her needs. That is, a customer may need to make numerous power requests throughout a day. This is not practical and may cause a significant burden on the smart grid communication network. Also, the customer may find it inconvenient to wait for a certain network delay before the power operator can adjust the power level to satisfy his/her needs.

A more realistic power request model is as follows. A customer is required to submit a power usage plan in advance. Such a plan can be on a daily basis. The customer can tell the power operator the time he/she needs additional power together with the amount throughout the day (e.g., 160 units of power for operating an air conditioner from 7:00 p.m. to 11:00 p.m., 120 units of power for operating a washing machine from 8:00 p.m. to 9:00 p.m.). In the future, this can be made automatic by the smart meter, which communicates with all household appliances and stores the usage profile of the customer, then predicts the power usage for the day based on some artificial intelligence techniques. The power operator then adjusts the schedule of power generation accordingly. In fact, this power request model is not new and was mentioned in [10]. According to this work, the power operator tries to minimize the risk of power generation mismatch (especially those by renewable energy sources) by collecting power plans one day or one week ahead. Such power plans may be power usage plans from customers.

In the traditional power supply paradigm, customers are not subjected to privacy leakage. Recall that a power operator installs a kWh meter at each customer's home. This kWh meter records the total amount of electricity used by the customer who is then charged accordingly after each billing period (say at the end of each month). What the power operator knows is the total amount of electricity used by the customer. However, in the new power request paradigm, besides the total amount of electricity used, the power request information also contains a customer's electricity usage pattern. For example, by observing the power usage plan of a family, it is easy to know when the family is not at home. If a criminal obtains this information, the family is susceptible to being burglarized. Therefore, privacy concern is critical for such a new power request paradigm.

Besides protecting the privacy of customers, how to ensure the effectiveness of the power request mechanism is another important issue. Normally, a certain charge should be imposed on a customer whenever he/she makes an additional power request. Otherwise, a customer may

[1] *Spinning reserve is the additional generating capacity that is available by increasing the output of the generators already connected to the power grid.*

Customers do not want to reveal their private information to the power operator. Besides, the communication channels from the smart meters to the control center and from the substations to the control center could be the public Internet and is always considered unsafe.

simply make excessive power requests no matter whether he/she will use the power requested or not. As a result, excessive power is generated. Therefore, we assume that a customer will be charged according to the amount of additional power requested in the power usage plan.

Nowadays, power operators usually encourage customers to shift some heavy power usage to non-peak hours. This can help to reduce the peak of power generation which in turn can limit the impact of air pollutants to the environment. Therefore, it is a natural trend to require a customer to take this into account when submitting power usage plans. In fact, this can be done easily by charging a customer more for power requests made during peak hours than that during non-peak hours. Our proposed scheme will allow the charging to follow different charging profiles.

Security Problems and Requirements

In a smart grid, a smart meter is installed in each customer's home. Therefore, it is natural to assume that it takes up the role of forwarding customers' power usage plans to the power operator. The control center can be a single server located inside the power plant or distributed servers located at different geographical locations for load balancing and to avoid a single point of failure.

In this article, we focus on the challenge of the trustworthiness of the parties involved. From the power operator's point of view, its control center and substations are more trusted than the customers since the control center and substations are usually physically protected. Smart meters, on the contrary, are not physically protected and can be compromised by dishonest customers or even by hackers who can then abuse the system. From the customers' point of view, the power operator as well as its control center and substations are only semi-trusted. They perform security operations honestly, but since they know the electricity usage pattern of the customers, they may induce private information of the customers (e.g., when they are at home). As such, customers do not want to reveal their private information to the power operator. Besides, the communication channels from the smart meters to the control center and from the substations to the control center could be the public Internet and is always considered unsafe.

We target designing a system to resolve the following four security problems:

Message authentication: Every power usage plan sent by any smart meter should be checked to confirm that it is from a valid user. Authentication is the basis of the system. Without it, anyone can abuse the system easily.

Identity privacy preservation: The real identity of the customer during the power usage plan submission phase should be unknown to everyone (including the power operator) to protect the privacy of customers.

Request message confidentiality: The information in any power usage plan should not be known by any third party in order to protect the privacy of the customers.

Traceability: The total amount of power requested by each customer in a certain period of time should be known by the power operator (i.e., its control center) as a lump sum so that the power operator can check whether the amount of power requested is close to the actual amount of power used. If the amount of power requested is far more than the actual amount of power used, excess power will be generated. On the contrary, if the amount of power requested is far less than the actual amount of power used, system instability will be caused. Thus, a customer should be subjected to additional charge under both cases.

Proposed Scheme to Solve Security Problems

In this section, we propose a secure and privacy-preserving scheme to solve the security problems mentioned. Roughly speaking, our scheme can be divided into four simple modules: *system startup*, *credential request*, *power usage plan submission*, and *reconciliation*. Let us describe each of them in more details.

System Startup

Recall that in a public key infrastructure (e.g., RSA), each party is assigned a public and private key pair. Its public key is assumed to be known by everyone, while its private key is only known by itself. When A wants to send a message to another party B, A encrypts the message using B's public key. B can then use its private key to recover the message. Also, A uses its private key to generate a digital signature on the message, and B can use A's public key to verify it.

In our scheme, during system startup, the control center assigns itself an RSA public and private key pair for it to sign credentials and for customers to encrypt messages to it. The public key is assumed to be known by everyone while the private key is only known by itself. Whenever a new smart meter is registered, it will be assigned a unique identity for identification purposes.

Credential Request

Our scheme is credential-based as the one proposed in [9]. A credential serves the same purpose as a ticket. At the beginning of each month, customers need to request a certain amount of credentials from the control center for power usage plan submission in the whole month. Customers are authenticated using their real identities in this module. Each customer (with the help of his/her smart meter) sends credential signing requests to the control center. Each credential is of the format $<CID, DOI>$. CID is a unique credential identity for each credential; DOI indicates the date that the credential is issued. By presenting a credential, a customer can request V points of additional power supply (the concept of points is explained in the next subsection).

In our scheme, all credentials are generated by customers. To make a credential anonymous, a customer first blinds it using a blinding factor (i.e., mixes it with some random components so that one cannot recognize its original content based on the blind version) and sends it to the

control center. The control center signs the credential using its private key and sends it back to the customer. The customer performs some computation to remove the blinding factor in order to obtain control center's signature on the real credential. Interested readers may refer to any cryptographic textbook about the actual mathematical operation involved. To prevent a customer from generating an invalid credential (e.g., *CID* being used before or *DOI* being outdated), a customer has to generate n times more credentials using different *CID*s and blinding factors, where n is predetermined by the control center. For each n credentials, the control center randomly challenges the customer to open (n – 1) of them and verify the details in them. If the information in all the opened credentials is valid, the control center signs the remaining one using its private key. Otherwise, the control center signs nothing and returns an error message to the customer. The control center computes and records the number of credentials N_{total} it has signed for that customer. Recall that the control center's public key is assumed to be known by everyone, while its private key is only known to itself. Thus, its signature can be verified by everyone, but can only be generated by it. Also note that although all credentials are known by the customers during generation, it will not cause any security problem because a credential is valid only if it contains the control center's signature.

To ease readers' understanding, we summarize the flow of this module in Fig. 2.

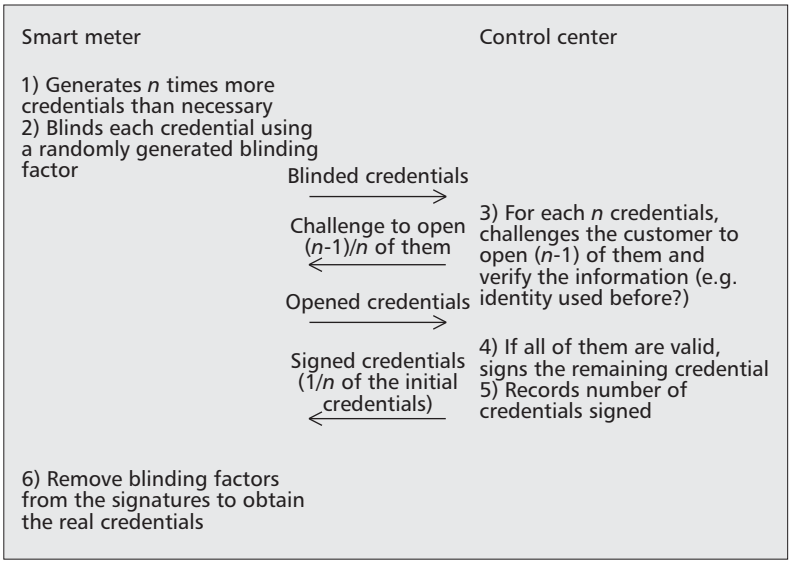

Figure 2. *Summary of credential request module.*

Power Usage Plan Submission

This module can be executed at different time periods, say one day or one week ahead of actual power usage. Note that to preserve customers' privacy, this module is run anonymously and customers do not have to authenticate themselves. As such, the control center cannot tell who the sender of a certain power usage plan is.

To submit a power usage plan, after communicating with appliances in the house, the smart meter of a customer first summarizes and constructs a power usage scheduling table like the one shown in Table 1.

Time	Additional power units required
07:01–08:00	100
08:01–09:00	120
19:01–23:00	160

Table 1. *Sample power usage scheduling table.*

The smart meter then downloads the up-to-date charging profile from the control center. This charging profile indicates different charging ratios among different hours. For example, a power operator may charge a customer twice as much if he/she requests additional power during peak hours, as mentioned earlier. As a result, a customer may need to issue twice the number of credentials (i.e., twice the number of points) to request the same amount of additional power units during peak hours as during non-peak hours.

After that, the smart meter attaches enough credentials. Let us consider the example in Table 1. Assume that the power operator charges customers twice as much during the peak hours from 19:01 to 07:00 the next day. That is, a customer will be charged 1 point for each power unit from 07:01 to 19:00, while he/she will be charged 2 points for each power unit the rest of the time. Also, we assume that by presenting a credential, a customer can request for 20 points of additional power. Then based on the above example, the customer has to present $100/20 + 120/20 + 160/20 \times 2 = 27$ credentials.

Next the smart meter encrypts the power usage scheduling table as well as the credentials symmetrically using a randomly generated session key and encrypts that session key asymmetrically using the control center's public key. The whole encrypted block is then transmitted to the control center.

Upon receiving the message, the control center obtains the session key using its private key and obtains the power usage scheduling table as well as the credentials using the decrypted session key. It then validates each credential by checking against its own signature and ensuring DOI is not outdated. If all validations are successful, the control center schedules the generators and the power level in different districts at appropriate times. Also, it records the credential identities CIDs into its local database so that the same set of credential identities cannot be reused. The control center then schedules appropriate control decisions to adjust the amount of power generated.

To ease readers' understanding, we summarize the flow of this module in Fig. 3.

Reconciliation

At the end of each billing period, reconciliation will be carried out. Note that similar to the registration module, this module is not anonymous. Customers need to be authenticated using their

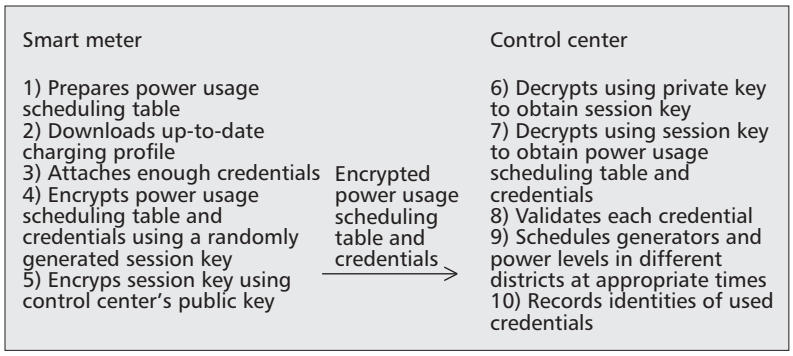

Figure 3. *Summary of a power usage plan submission module.*

real identities in this phase. During this phase, the smart meter of a customer sends all the credentials that have not been used to the control center. The control center then checks the credentials as usual, counts the total number of unused credentials N_{unused}, and computes the total number of used credential N_{used}as $N_{\text{total}} - N_{\text{unused}}$. As such, the customer needs to pay for the $(N_{\text{total}} - N_{\text{unused}})$ points of additional power requested.

To check against whether a customer requested roughly the same amount of power as he/she used, the power operator may use a traditional kWh meter to collect the monthly power consumption, and the system will compare the consumption with the points computed above to see whether they are comparable. If there is a big difference between them, an extra charge can be added to the monthly bill of the customer. However, one point to note is that since the power operator imposes different charging profiles during peak hours and during non-peak hours, kWh meters have to be adjusted accordingly so that they can put a heavier weight to the electricity used during peak hours (e.g., the recording plate rotates at a higher speed).

Performance Analysis on Proposed Scheme

In this section, we first evaluate our scheme according to the security requirements listed earlier (we skip the formal security proof here due to space limitations). Next, we discuss some performance issues such as signature generation time and the impact of V (the number of points represented by each credential).

As mentioned earlier, we target designing a system to resolve four security problems: message authentication, identity privacy preservation, request message confidentiality, and traceability. Let us consider them one by one.

Message authentication: At the registration phase, a customer needs to authenticate him/herself using the private key signature before requesting any signing of credentials. So when the customer presents the signed credentials during the power requesting phase, he also proves him/herself authenticated.

Identity privacy preservation: Customers only reveal their identities in registration and reconciliation modules. In the power usage plan submission module, when the customer presents the credentials, the control center cannot relate them with the customer. Due to the properties of the blind signature, the credential identity is only known by the owner. The credentials do not reveal the identity of the customers either.

Request message confidentiality: Before sending out the power usage plan, the smart meter first encrypts the power usage scheduling table as well as the credentials symmetrically using a randomly generated session key and encrypts that session key asymmetrically using the control center's public key. Thus, no one except the control center can decrypt the message. Confidentiality of the power usage plan is thus preserved.

Traceability: In registration and reconciliation modules, a customer needs to present his/her identity (i.e., not anonymous) to the control center. The total amount of points used by each customer over a certain period of time (say a month) can be known by the control center. The customer can then be properly charged at the end of the charging period.

Regarding the signature generation time, according to [9], signing 10,000 credentials using a consumer PC with Intel Core 2 Duo CPU, T5870 @ 2.00 GHz and with 1024 bits (2048 bits) RSA needs only about 1 min (10 min). Also, this process can be done in a batch mode during non-peak hours. Therefore, it should not cause a burden to the control center.

Now let us investigate the impact of V (the number of points each credential represents) to our scheme. Assume that at a certain power usage plan submission process, a customer has to submit a total of P points. Without loss of generality, assume that each credential represents V points. The number of credentials the customer has to submit is $\lceil P/V \rceil$. Obviously this leads to some waste to both the customer and the power operator and this waste is bounded by V points. For example, if $P = 93$ and $V = 20$, the waste becomes 7 points. In fact, this waste is related to some unnecessary additional power request. To the customer, he/she needs to pay the necessary charge for it. To the power operator, it needs to generate excess electricity. Nevertheless, one may notice that if V is close to the basic unit of P (e.g., $V = 1$ if P takes an integer value), this waste can be minimized. However, it should also be noted that the smaller the value of V, the more credentials a customer has to present in the power usage plan submission module. This in turn leads to higher communication overhead and higher credential generation overhead at the control center. Therefore, developers should take into consideration this trade-off when adopting our scheme in their system.

Conclusions

In this article, we briefly introduce what a smart grid is. We then introduce a power request paradigm in which a customer is allowed to submit a power usage plan in advance and highlighted the importance of smart grid security. Next we propose a secure and privacy-preserving power request scheme based on the techniques of anonymous credential and blind signature. Credentials are generated by the customer but

are blindly signed by the control center. Our scheme fulfills two seemingly contradictory security requirements:

- All customers' privacy including their electricity usage pattern is preserved from anyone including the control center.
- All customers' power requests are properly authenticated.

The customers can even be charged based on the amount of electricity requested on top of different charging profiles across peak and non-peak hours. We remark that this may not be the best solution to the problem. We aim to introduce these security problems to readers and stimulate the interest of the community to investigate these problems further.

Acknowledgement

This research is supported in part by the HKU RCGAS Small Project Funding under Grant No. 201109176206 and the Collaborative Research Fund of the Research Grants Council of Hong Kong under Grant No. HKU10/CRF/10.

References

[1] SmartGrids, "European SmartGrids Technology Platform: Vision and Strategy for Europe's Electricity Networks of the Future," EC Directorate-General for Research, Sustainable Energy Systems, EUR 22040, 2006.
[2] Electric Power Research Institute, "Intelligrid," http://intelligrid.epri.com.
[3] U.S. Dept. of Energy, "Grid 2030: A National Vision for Electricity's Second 100 Years," 2003.
[4] Office of the National Coordinator for Smart Grid Interoperability, "NIST Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperatility Standards, Release 1.0," Jan 2010.
[5] Stuxnet.net, "All about Stuxnet," http://www.stuxnet.net.
[6] H. Khurana *et al.*, "Smart-Grid Security Issues," *IEEE Security and Privacy Mag.*, Feb 2010, pp. 81–85.
[7] The Smart Grid Interoperability Panel — Cyber Security Working Group, "Second Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements," Feb. 2010.
[8] Juniper Networks Inc., "Architecture for Secure SCADA and Distributed Control System Networks," 2009.
[9] J. C. L. Cheung *et al.*, "Credential-Based Privacy-Preserving Power Request Scheme for Smart Grid Network," *Proc. IEEE GLOBECOM '11*, Dec 2011.
[10] V. O. K. Li, F.F. Wu, and J. Zhong, "Communication Requirements for Risk-Limiting Dispatch in Smart Grid," *Proc. IEEE Wksp. Smart Grid Commun.*, Cape Town, South Africa, May 2010.

Biographies

T. W. Chim (twchim@cs.hku.hk) received his B.Eng., M.Phil., and Ph.D. degrees in information engineering, electrical and electronic engineering, and computer science, respectively, from the University of Hong Kong in 2002, 2004, and 2011, respectively. He is currently a post-doctoral fellow in the Department of Computer Science at the University of Hong Kong and being funded by Prof. Victor O.K. Li. His research interests include information security and network routing.

S. M. Yiu (smyiu@cs.hku.hk) obtained his Ph.D. in computer science from the Department of Computer Science, University of Hong Kong. He is currently an assistant professor in the same department. His research interests include information security, cryptography, and bioinformatics.

Lucas C. K. Hui [SM] (hui@cs.hku.hk) is the founder and honorary director of the Center for Information Security and Cryptography, and concurrently an associate professor in the Department of Computer Science, University of Hong Kong. His research interests include information security, computer crime, cryptographic systems, and electronic commerce security. He received his B.Sc. and M.Phil. degrees in computer science from the University of Hong Kong, and his M.Sc. and Ph.D. degrees in computer science from the University of California, Davis. He is a member of HKIE.

Victor O. K. Li [F'92] (vli@eee.hku.hk) is Chair Professor of Information Engineering and Associate Dean of Engineering at the University of Hong Kong. He received S.B., S.M., E.E., and Sc.D. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology in 1977, 1979, 1980, and 1981, respectively. Previously, he was a professor of electrical engineering at the University of Southern California (USC), Los Angeles, and director of the USC Communication Sciences Institute.

In registration and reconciliation modules, a customer needs to present his/her identity to the control center. The total amount of points used by each customer over a certain period of time can be known by the control center. The customer can then be properly charged at the end of the charging period.