May 2016

Improved Attribute-based Encryption with Fpga for Automatic Appliance Control Application in Smart Grid

Xueqing Wang
University of Wisconsin-Milwaukee

IMPROVED ATTRIBUTE-BASED ENCRYPTION WITH FPGA FOR AUTOMATIC APPLIANCE CONTROL APPLICATION IN SMART GRID

by

Xueqing Wang

A Thesis Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Master of Science

in Engineering

at

The University of Wisconsin-Milwaukee

May 2016

ABSTRACT
IMPROVED ATTRIBUTE-BASED ENCRYPTION WITH FPGA FOR AUTOMATIC APPLIANCE CONTROL APPLICATION IN SMART GRID

by
Xueqing Wang

The University of Wisconsin-Milwaukee, 2016
Under the Supervision of Professor Weizhong Wang

In this thesis, the author describes the privacy violation issues in smart grid with Automatic Appliance Control applications, and explains the security threats related to it. The smart grid is a sensitive and sophisticated system in real life operation. A mass of data including the remote control commands and users' energy consumptions is transmitted between the utility companies and other devices in the smart grid such as the substations, smart meters, smart home appliances and much more. Without efficient cryptographic methods, an adversary may hack into the data or the remote control commands and extrapolates a resident's activity model. Therefore, the Attribute-Based Encryption (ABE) is proposed to provide protection through generating the secret key of user based on a set of attributes which is used to identify different users in the smart grid. And the ciphertext, which is the encrypted remote command, obtains the access policy for decryption. However, ABE algorithm requires long computational time especially a large quantity of attributes are required in a smart grid. The idea of improved ABE system with FPGA is proposed to solve the problem. But the FPGA is only conceptual idea in this thesis and future work of it will be done by other co-worker.

TABLES OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my supervisor, Dr. Weizhong Wang, who has provided me with valuable academic advising, and guidance for this thesis. Without his enlightening instructions, impressive kindness, and patience, this thesis would not have been completed. I would extend my thanks to my Program Committee: Dr. Guangwu Xu and Dr. Lingfeng Wang for their conducive comments on this thesis.

I would also like to express my sincerest gratitude to my family for their encouragement and support to go through the hard time with me.

I. Introduction and Problem Definition

1. Background

The electricity grid is a network of power generations, substations, transmission lines, transformers and other devices to deliver electricity from suppliers to consumers. By introducing the two-way digital communication technology to the grid, the smart grid is proposed which is embedded with computer-based remote control and automation so that the electrical grid has the capability to respond digitally to the change of electricity demand [1]. Many factors are taken into consideration to build a smart grid system such as reliability, economy, efficiency, security and safety [7].

With the widespread utilization of Internet of Things (IoT) in smart grid, different energy-related devices from power infrastructures to home appliances and smart meters are interconnected through the internet in the smart grid system. Through IoT, utility companies have the capability to find out new approaches based on the data collected by the these digitalized smart meters to enhance system reliability, to reduce energy losses, and to reduce customers' electricity expenses for their daily lives and so on. There is no doubt that a large amount of data including power consumptions, control commands and alarms will be transferred between the utilities and customers. Among all the devices in the smart grid, the automatic appliance control (AAC) application becomes one of the most visible and convenient applications. These data collected from AAC applications could be used in improper ways rather than the original purposes for which they are collected. A third party or

person can extrapolate the customers' live schedules and personal behavior modes [2, 11]. For example, sending remote AAC command to open or shut down the heater when temperatures reaches to particular Celsius / Fahrenheit degree could highly indicate the presence or absence of the residents at that time, which may leads to sever privacy violations. Therefore, proper privacy protection designs to hide the AAC commands and costumers' information are strongly demanded for AAC applications in smart grid system. A simple smart grid structure is shown in figure. 1.

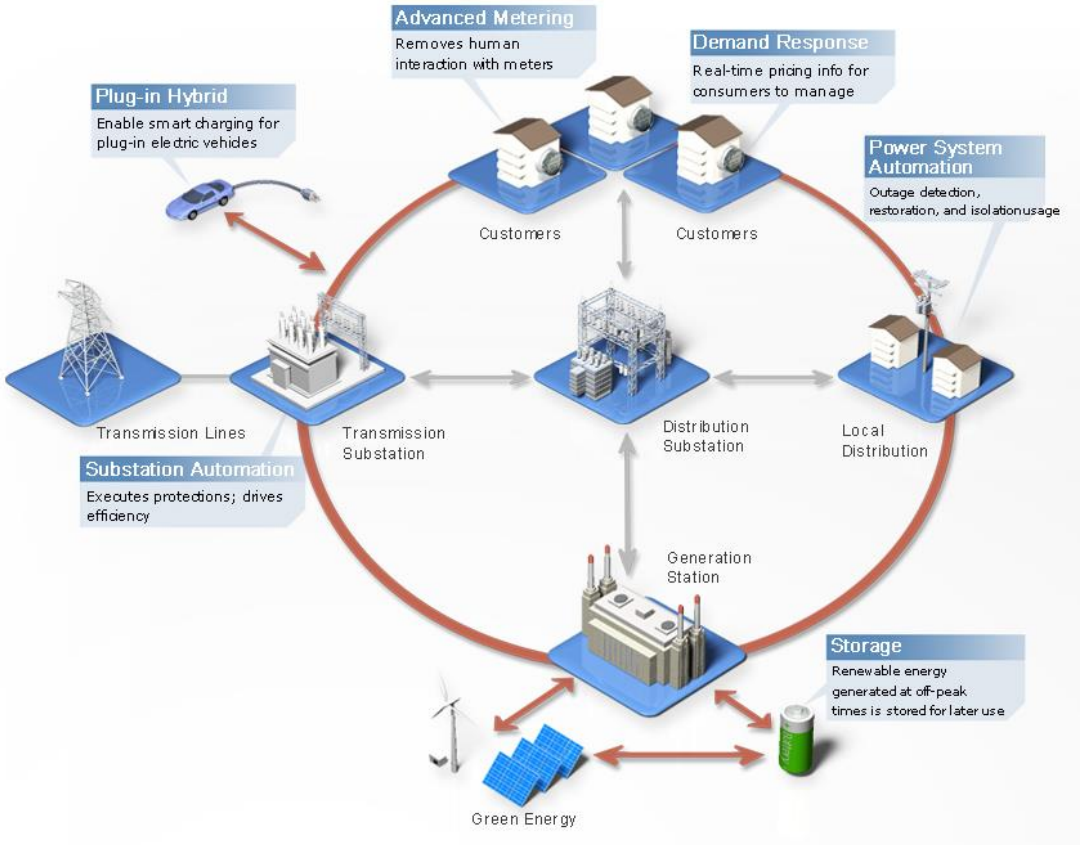

Figure.1 A simple illustration of smart grid network

2. Problem Description Related to ABE Methodology

From previous researches, a privacy encryption algorithm called attributed-based encryption (ABE) were applied to protect privacy in many fields [12-15], for instance, keeping privacy

data in cloud storage and smart phones, preserving patients' electronic medical records (EMR), securing data retrieval for decentralized disruption-tolerant military network (DTNs) and so forth. The concept of attribute-based encryption is a promising approach as it is embedded with the fine-grained access control, which facilities granting differential access rights to a series of users and realizes flexibility to specify the access rights of individual users [9]. In an attributed-based encryption system, the sender will generate the ciphertext with the master key (MK) and public keys (PK), and the user can only decrypt a ciphertext when user's private key matches with the ciphertext.

From a previous research, a privacy preservation protocol [2] was proposed for AAC applications in smart grids. This protection mechanism was built based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Rivest, Shamir, and Adleman (RSA) public key encryption algorithm. On the one hand, CP-ABE allows multicast from control center to various AAC applications. The sender's data access policy is embedded in ciphertext and a secret key (SK) is generated based on a set of user's attributes. On the other hand, RSA algorithm provides a more efficient encryption mechanism than CP-ABE that it can send back the encrypted response result from one AAC application to the control center. However, RSA can only handle the one-to-one data transfer, which is not practical for that among various AAC applications.

In order to realize the privacy protection for multicast, the CP-ABE is applied. However, there is an important challenge in utilizing the original CP-ABE system in AAC applications that CP-ABE requires long computational time for its operation. In this paper, we proposed an improved CP-ABE with field programmable gate arrays (FPGAs) [16] to solve this

challenge. In general, the FPGA is an integrated circuit designed to be configured by customers to satisfy the desired functionality requirements that are based on an array of configurable logic blocks (CLBs) connected through programmable interconnects [17-18]. The FPGA has been reconfigured as a strong tool to help deal with problems when using them in cryptographic applications. It offers many system advantages as algorithm agility, algorithm modification, high architecture efficiency, cost-efficiency and etc. [16]. The desired goal is to find out the part which requires the most computational time, and rebuild that algorithm through the FPGA so that the whole operation time for CP-ABE could be reduced for AAC applications in smart grid.

In this paper, we will first review the basic concept of AAC applications that used in smart grid, and set up the AAC application model for our case simulation. Next, we introduce a detailed algorithm of Ciphertext-Policy Attribute-Based Encryption and explain pros and cons of CP-ABE. Then, the improved CP-ABE protection mechanism will be proposed to realize multicast among the AAC applications and to reduce the whole operation time. Finally, we tested our improved cryptography mechanism on the ARM based embedded system (detailed ARM info), and illustrate the operation time for different numbers of attributes.

II. Review of Automatic Appliance Control Application

1. Literature review of Automatic Appliance Control

The automatic appliance control applications are becoming more and more popular nowadays

such as air-conditioner, dishwasher, lights, even the smart phones and so on. AAC has been employed in the following areas: 1) automatic control for home appliances; 2) remote control service supported by utility companies via internet; and 3) electricity demand-response from smart grid [2, 4]. Among these applications, the control commands and data showing current status are transferred remotely through public communication systems, for example, the internet and telecommunications. More detailed descriptions for AAC appliances are shown below. From these descriptions of AAC applications, it can be clearly know that the AAC application can be employed in the smart grid system for better performance such as improving the efficient and safety of the system.

(1) AAC in Home Appliances Home automation, also known as smart home, becomes a popular tendency utilized in residence homes and buildings. Composed of hardware, communication system and electronic interfaces, the automation system achieves great success through remote control on environment protection, convenience, safety and real-time monitoring of living consumptions such as electric bills and water fees [19-21]. The functionality of safety mentioned here refers to checking security system's status of the home/building, for example, informing the current temperature of the home/building, whether the lights are on or not and much more. Undoubtedly, personal activity patterns are embedded inside the control commands resulting in privacy leakage.

(2) ***Remote Appliance Control Services*** Considering the growth of personal computers, mobile devices, internet and wireless technology and convenience, some utilities provide remote control on home appliances via secure channels such as internet and wireless technology, or even GSM (Global System for Mobile Communications) technology and

other technologies to offer a better use of electricity for customers. For example, the user can turn on or off the air-conditioner remotely depending on the user's desire. Furthermore, with the use of remote AAC services, safe operation and control can be achieved in smart grid. In many cases, fast response is required because of serious emergencies, for instance, when the power grid cannot supply sufficient electricity to all customer loads, some insignificant customers are needed to be disconnected rapidly from the grid network in case of large areas of blackout [2, 4, 11, 21-23].

(3) ***Demand Response*** Demand response (DR) provides an effective approach to balance the supply and customer loads during periods of peak energy consumption in real time. The customers play an important role for the operation of the smart grid that customers can comply with the requests of DR by monitoring the electricity usage at different time of a day through methods including smart meter technologies and offering various time-based rate pricing such as critical peak pricing, real-time pricing and so on. Taking the direct load control program as an example. It enables power companies to shut down customers' appliances remotely during periods of peak demand in exchange of lower bills and safe system operation for smart grid. The customers' appliances can be smart appliances such as air conditioners and water heaters. [2, 4, 11, 24-25]

2. Models of Automatic Appliance Control

The smart grid system is a network of various power devices, which makes the network become huge and sophisticated. Therefore, an appropriate AAC model is necessary to analyze

the effect of ABE system in smart grid. As introduced before, the two-way intelligent communication technology is utilized in smart grid system which enables controls and responses from/to different devices in the system are efficient and safe. Taking efficiency, scalability and functionality into account, it is necessary to apply multicast technique into smart grid network system since multicast provides one-to-many communications in the system [2, 4]. In real life applications, multicast can be utilized in DR programs considering the fact that the control center needs to send messages to quantities of remote appliances simultaneously.

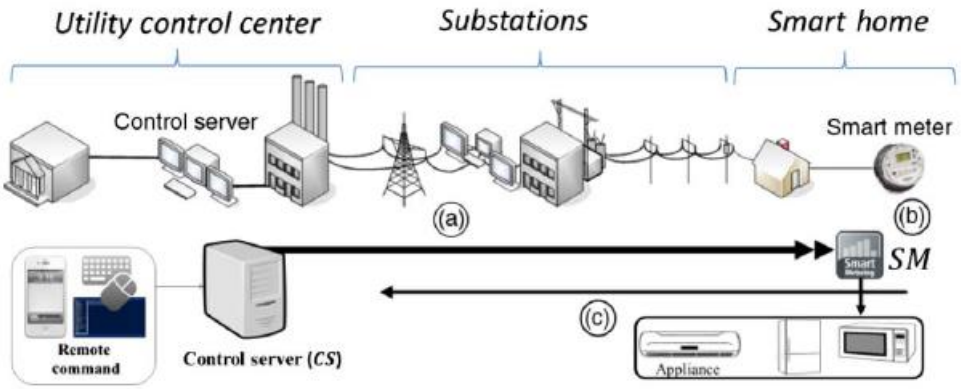

Figure.2 System AAC application model embedded with ABE cryptography [2]

Overall, the AAC model for our system is shown in figure. 2. It composes of three parts: the control center (CS), the communication channels and the smart meters (sm_i). The control center refers to utility control center that sends remote commands to users and receives the feedback from the users which are the smart meters in this model. The smart meters receive remote control commands from utilities and other users to control the smart appliances.

For simplification, we assume only one smart meter sm_i is registered in a residence. To identify every smart meter in our system, we use the address of the residence. The address can be expressed as a set of attributes which can be changed depending on real cases, for

example $\hat{A} = \{attr_1 =$ "street name",attr$_2$="house number", $attr_3 =$ "ZIP code", $attr_4 =$ city name",attr$_5$="$state$" }, and we can add more attributes to make the smart meters response more accurately.

In our AAC system, the control center multicasts a command list M embedded with a set of control commands ({…,C_j, ...} to smart meters to smart meters. The smart meter can figure out whether the message is designated for it or not by checking its unique attributes set with the C_j's access policy. And smart meters give the feedback back to utility control center after executing command C_j. Furthermore, the smart meters can communicate between themselves if needed.

III. Overview of Ciphertext-Policy Attribute-Based Encryption

1. The CP-Attribute-Base Encryption System

Introduced by Sahai and Waters [8], the attribute-based encryption is a cryptography approach which reconsiders the scheme of traditional public key cryptography. Traditionally, a message is encrypted by using the user's public key,

There are mainly two algorithms of ABE: the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and the Key-Policy Attributed-Based Encryption (KP-ABE) [5]

A. Bilinear Maps

The bilinear map provides an effective computational theory for computation of attribute-based encryption. Defining $\mathbb{G}_1$ and $\mathbb{G}_2$ to be two cyclic multiplication groups with the same order of *p*. The bilinear map *e* is then defined as: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. And the bilinear map *e* is efficiently computable for $\forall u, v \in \mathbb{G}_1$. So it should have the following property:

1). Bilinear: for all $u, v \in \mathbb{G}_1$ and $a, b \in Z_p$, we have $e(u^a, v^b) = e(uv)^{ab}$.

2). Non-degenerate: for the generator *g* of $\mathbb{G}_1$, we have $e(g,g) \neq 1$.

B. Access Trees of Attributed-Based Encryption

From the name of encryption system, it is clearly shows that the ciphertexts that need to be encrypted consist of series of descriptive attributes. Therefore, an access tree is introduced that the a leaf represents one unique attribute, and the intermediate node is used as a threshold gate, for example "AND" and "OP" gates. Therefore, the subscribers can access the ciphertext only if their keys match with node of the access tree. The access tree has the symbolic representation of *T*. And a detailed illustration of the ABE access tree is shown below:

1) **Setup** The main function for setup procedure is to generate the master key (MK) and public key (PK) for ciphertext encryption. Define a security parameter of κ to determine the group size for bilinear map, by which the ABE system sets up the bilinear map calculation that is discussed in part A of this chapter, and a universal set of attributes is $U = \{1, 2, ..., n\}$. For each attribute i from this universal set, a number t_i is chosen randomly from Z_p, and *r* is chosen randomly in Z_p (pairings). Then the master key is generated:

$$t_1, t_2, \dots, t_{|U|}, y \tag{1}$$

And the public parameters PK become:

$$T_1 = g^{t_1}, T_2 = g^{t_2}, \ldots, T_{|U|} = g^{t_{|U|}}, Y = e(g,g)^y \quad (2)$$

The public key PK is open to all parties from the entire system, but the master key is owned by the authority party.

2) **Key Generation** By employing master key MK and public key PK, this procedure produces the private keys for users , which is held by the user only and used to decrypt the message encrypted with a set of attributes of γ. The basic algorithm is firstly defining a random polynomial q_x for each node *x* in the access tree T under a top-down manner starting from the root node *r*.

Then, the degree d_x of the polynomial q_x for each node *x* is assigned: $d_x = k_x - 1$, and k_x is the threshold value for the node *x*. Start from the root node *r*, assigning the polynomial $q_r(0) = \mathrm{y}$ and degree *d*, and set d_r other points for q_r randomly for the complete q_r definition.

Finally, as for the rest non-root node *x*, the polynomial is assigned to be $q_x(0) = q_{parent(x)}(index(x))$, where $q_{parent(x)}$ is the parent for node x and $\mathrm{index}(x)$ represents the unique ordering number given by its parent node. Similar to what is done for root node, randomly choose d_x other points for q_x to complete the definition of q_x. By following the algorithm, the secret keys can be obtained:

$$\mathrm{SK} = \{D_x = g^{\frac{q_x(0)}{t_i}}\} \quad (3)$$

where t_i is the master key for attribute *i* generated before.

3) **Encryption** A set of attributes γ, the public key PK, and a message M are used as input for encryption. And the encrypted ciphertext E becomes:

$$\mathrm{E} = \{\gamma, E' = MY^s, \{E_i = T_i^s\}_{i\in\gamma}\} \tag{4}$$

where *s* is a random number in Z_p.

4) **Decryption** Specifically, a recursive algorithm is invoked for ciphertext decryption. The decryption algorithm is defined as $DecryptNode(E, SK, x)$ which obviously shows that encrypted ciphertext E, the secret key SK, and the node *x* are taken as input.

- If the node *x* is a leaf node:

① If $i \in \gamma, DecrytNode(E, SK, x) = \perp$

② If $i \in \gamma, DecrytNode(E, SK, x) = e(SK_x, E_i) = e\left(g^{\frac{q_x(0)}{t_i}}, g^{s-t_i}\right) = e(g,g)^{q_x(0)\cdot s}$ (5)

- If the node χ is not a leaf node, then the recursive algorithm changes to: For all nodes *z* which are the children nodes of *x*, the function F_z is called as:

$$F_z = DecrytNode(E, SK, z) \tag{6}$$

And set S_x with an arbitrary k_x-sized set of children nodes *z* so that $F_z \neq \perp$. If no such set can be found, then the node is not satisfied and the function returns $\perp$.

For the case that the node is satisfied, we have the function:

$$\begin{aligned} F_x &= \prod_{z\in S_x} F_z^{\Delta_{i,S'_x(0)}} = \prod_{z\in S_x} (\mathrm{e(g,g)}^{s\cdot q_z(0)})^{\Delta_{i,S'_x(0)}} \\ &= \prod_{z\in S_x} (\mathrm{e(g,g)}^{s\cdot q_{parent(x)}(index(z))})^{\Delta_{i,S'_x(0)}} \\ &= \prod_{z\in S_x} \mathrm{e(g,g)}^{s\cdot q_x(i)\cdot\Delta_{i,S'_x(0)}} = e(g,g)^{q_x(0)\cdot s} \end{aligned} \tag{7}$$

And returns the result to F_x, where $i = index(z)$, $S'_x = \{index(z): z \in S_x$ and the Lagrange coefficient $\Delta_{i,S'_x(0)} = \prod_{j\in S, j\neq i} \frac{x-j}{i-j}$.

The decryption function is called starting from the root of the tree, therefore, the algorithm becomes $\mathrm{DecryptNode}(\mathrm{E}, \mathrm{SK}, \mathrm{r}) = \mathrm{e}(\mathrm{g}, \mathrm{g})^{ys} = Y^s$ when the ciphertext matches with the access tree. And as we have already known in Encryption procedure, then we can decrypt the ciphertext as follows:

$$\frac{E'}{DecryptNode(E,SK,r)} = \frac{MY^s}{Y^s} = M \tag{8}$$

the message is then recovered and can be read by users who satisfy the decryption policy.

2. Advantages of ABE System.

The human society has turned into the information age that we can create and develop things based via high technical products such as computers, smart phones, internet and much more. Without sufficient protection, information can be easily violated by a third party. For example, the idea of new product of a company can be stole by its adversaries which results in quantities of economic losses for this company.

The primitive encryption schemes are employed that a sender encrypts the message for every target user to provide confidentiality to the remote communications via internet, Bluetooth and other digital communications. However, it brings serious defects that the sender needs to know the identities of all intended receivers and both of the sender and receivers share the same secret keys of the encryption. In real life, it is difficult to recognize the identities for all expected receivers that need to access the messages. Meanwhile, the communication systems are normally huge and complicated that vast numbers of users are installed [5, 8-9, 27]. Take the smart grid system as an example, the utility company remotely send control command to remotely shut down numbers of nonessential smart appliances

during the period of peak power consumption, so that the utility companies can provide sufficient power to the system without building additional power plants.

Ciphertext-Policy Attributed-Based Encryption (CP-ABE) provides solutions to these problems. As shown in the ABE algorithm in part 1 of Chapter III, the access policy is embedded in the ciphertext and the user's secret key is assigned based on a defined set of attributes which is kept by user only. With ABE system, user can decrypt the ciphertext only if the attributes associated with his or her secret key satisfy the access policy and the messages are protected without any privacy violations. Besides, ABE system utilizes multicast for communications between devices [4]. Multicast technology enables effective communications from one to many devices. Within a smart grid system, it is normal for the utilities to send the control commands to various devices in the same time. With multicast communication, utility companies respond quickly to trigger the protection actions when unexpected accidents happen in the smart grid system, for example large areas of blackout, loss on transmission lines, excess of power consumption during peak energy consumption periods and so on.

IV. Improved ABE System with FPGA

Traditionally, in order to meet the requirements of long and difficult design cycles, the Application Specific Integrated Circuit (ASIC) of the embedded systems are widely applied for system designs because of its high performance and low-power budget However, when the reconfigurable components are introduced in the 1980s, new

integrated circuits were developed which is known as the Field Programmable Gate Arrays (FPGAs). Generally speaking, Field Programmable Gate Arrays (FPGAs) are the semiconductor devices that are based on a matrix of configurable logic blocks connected via reconfigurable interconnects. There is no doubt that FPGAs has powerful functionality that enables users to reconfigure the circuits with faster design cycles using HDL (Hardware Description Language) according to their special preferences, rather than the designed and unchangeable circuits via ASICs [16-18].

With the technology development, the modern FPGAs become more powerful containing various logic gates and RAM blocks to support complex digital computations. Due to increasing trend of using FPGAs and its strong function, FPGAs are becoming more popular for cryptographic implementations which normally require huge and sophisticated computations during their operations [2, 26].

Theoretically, from the operation process of ABE system, with the increasing numbers of attributes involved in our AAC system, more calculations are required which results in longer computational time [27], and the computational time would be linearly proportional to the numbers of attributes defined for the system. Undoubtedly, in the consideration of efficiency and security, we would prefer a shorter operational time of the cryptography utilized in smart grid, for instance, fast response is necessary to balance the power supplied by utilities and customers' consumptions during periods of peak energy consumption in real time. Otherwise, large areas of blackouts may occur or additional power plants are needed to be installed to the smart grid which increases system costs such as the maintenance fees and cost of power supply.

From part B of Chapter III we can know that there are totally four steps for the ABE system operation. Instead of reconfiguring the design with all the four steps of ABE, we can test the operation time for each step, and then reconfigure the most time-consumption step with FPGA to reduce the computational time. In this paper, actually we only propose the basic idea of utilizing ABE system with FPGA and exam the ABE system to check the time-consuming parts which needs to be reconfigured. The FPGA part will be done by other co-workers in the future.

V. Real Simulation

The main target is to test the operation time of the ABE system and decide the part that needed to be reconfigured by FPGA. Two tools are used for the simulation, one is the Ubuntu desktop with Linux operation system and the ZedBoard Zynq-7000^{TM} embedded with the ARM core. Ubuntu desktop is chose to compile and run the ABE program before compiling it to the ZedBoard to guarantee the encryption program can operate under the Linux system. The encryption program is formed based on the Ciphertext-Policy Attribute-Based Encryption toolkit from Advanced Crypto Software Collection. By adding the command *gettimeofday()* to display the execution time in second for each of the four steps that are setup, key generation, encryption, and decryption. After the successful operation in Ubuntu, the ABE program is compiled to the Zedboard with its required libraries.

During the test, two sets of fifteen attributes are defined and two secret keys are generated based on their attributes and the detailed procedure of ABE operation is shown in

the Appendix. Assuming our AAC model of smart grid is built with in the United States that the abbreviations of 20 states are chosen as the address characters. The two secret keys are labeled as '*subsc1_priv_key*' and '*subsc2_priv_key*' and the control command file '*message.txt*' is created through *cat* command that the content can be justified depending on the request of control server (or utility companies in smart grid system). In real simulation the operation time is executed after each of the steps is done. The execution time is shown in table.1. It clearly shows that the key generation for two subscribers of ABE system occupy the most time for the entire operation procedure. Therefore, the encryption step needs to reconfigure with FPGA in the future.

Steps for ABE	Execution Time [s]
Setup	0.1759
Key Generation for Subscriber 1	18.0424
Key Generation for Subscriber 2	18.0412
Encryption	2.1789
Decryption	1.5746

Table.1 Execution time in seconds for four steps of ABE operation

However, there is still a defect about this ABE program that is the operation time of encryption does not linearly increase or decrease corresponding to the change of numbers of defined attributes. In real simulation, when the attributes are all expressed in words, for example, only use the first ten attributes of a subscriber (listed in Appendix), the execution time reduces to approximate 12 seconds. On the contrary, if the subscriber's secret key is only

generated based on the three attributes containing numbers inside, key generation execution time becomes about 17 seconds for each subscriber. This obeys the linear relationship between computational time and numbers of attributes. So it is still need to justify the ABE program in the future.

VI. Conclusion and Future Work

In this paper, we demonstrate the basic content of why choosing attribute-based encryption to prevent the privacy violations from third parties of AAC applications in smart grid. In the CP-ABE system we used here, the access policy is embedded within the ciphertext, and the user's secret key (SK) is generated a pre-defined set of attributes by using the address to identify different users in the smart grid system. A user can decrypts the encrypted control command only if the attributes associated with the secret key satisfy the access policy. Compared to traditional cryptography methods, the ABE guarantees a better approach for privacy preservation. The real simulation brings out the execution time based on our AAC model with 15 attributes for each subscriber that key generation requires the most computational time.

However, there are some future works need to be done. One is to solve the relationship between numbers of attributes and execution time. They should comply with linear relationship that only the number of attributes impacts the change of execution time. The type of attributes, for instance words or numbers, should not generate obvious time difference. The other one is that to solve the long computational time, the idea of employing FPGA to

reconfigure the ABE program is proposed in this thesis, but future work needs to be done to operate the reconfigured program on the ZedBoard and simulate the execution time for it.

Renerences

[1] *Office of Electricity Delivery & Energy Reliability*. "Technology Development-Smart Grid," [Online] Available at: https://www.smartgrid.gov/the_smart_grid/smart_grid.html.

[2] D. Li, Z. Aung, J.Williams, A. Sanchez. "P3: Privacy preservation protocol for appliance control application in smart grid," in *IEEE Internet of Things Journal*, vol. 1, issue 5, pp. 414-429, 2014 September.

[3] Olivier Monnier, "A smart grid with the Internet of Things," in *Texas Instruments*, slyb214, 2013 October.

[4] Q. Li, G. Cao. "Multicast authentication in the smart grid with one-time signature," in *IEEE Transactions on Smart Grid*, vol. 2, issue 4, pp. 686-696, 2011 May.

[5] X. Wang, J. Zhang, E.M. Schooler, M. Ion, "Performance evaluation of attribute-based encryption: toward data privacy in the IoT," in Communications (ICC), 2014 IEEE International Conference, pp. 725-730, 2014 June.

[6] A. M.-Markham, G. Danezis, K. Fu, P. Shenoy, D. Irwin. "Designing privacy-preserving smart meters with low-cost microcontrollers," [Online] Available at: https://eprint.iacr.org/2011/544.pdf.

[7] *National Energy Technology Laboratory (NETL)*, "Understanding the benefits of the smart grid," 2010 June, DOE/NETL-2010/1413.

[8] J. Bethencourt, A. Sahai, B. Waters. "Ciphertext-policy attribute-based encryption," [Online] Available at: https://www.cs.utexas.edu/~bwaters/publications/papers/cp-abe.pdf.

[9] V. Goyal, O. Pandey, A. Sahai, B. Waters. "Attribute-based encryption for fine-grained access control of encrypted data," [Online] available at: https://eprint.iacr.org/2006/309.pdf.

[10] S.Yu, C. Wang, K. Ren, W. Lou. "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *INFOCOM, 2010 Proceeding IEEE*, pp. 1-9, 2010 March.

[11] D. Li, Z. Aung, J.Williams, A. Sanchez. "P3: Privacy preservation protocol for appliance control application," in *Smart Grid Communications(SmartGridComm), 2012 IEEE Third International Conf*erence, pp. 294-299, 2014 November.

[12] M. Ambrosin, M. Conti, T. Dargahi. "On the feasibility of attribute-based encryption on

smartphone devices," in Cornel University Library, 2015 April.

[13] J. Hur, K. Kang. "Secure data retrieval for decentralized disruption-tolerant military networks," in *IEEE/ACM Transactions on Networking*, vol. 22, issue 1, pp. 16-26, 2012 August.

[14] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, A. D. Rubin. "Self-protecting electronic medical records using attribute-based encryption," [Online] Available at: https://eprint.iacr.org/2010/565.pdf.

[15] H. Zhu, R. Huang, X. Liu, H. Li. "SPEMR: A new secure personal electronic medical recode scheme with privilege separation," in *Communications Workshops (ICC), 2014 IEEE International Conference*, pp. 700-705, 2014 June.

[16] T. Wollinger, J. Guajardo, C. Paar. "Security on FPGAs: State-of-the-Art implementations and attacks," in *ACM Transactions on Embedded Computing Systems*, vol. 3, No. 3, pp. 534-574, 2004 August.
.
[17] "Field-progrmmable gate array" from *Wikipedia, the free encyclopedia*. [Online] Available at: https://en.wikipedia.org/wiki/Field-programmable_gate_array.

[18] "Field programmable gate array (FPGA)," from *Xilinx Inc*. 2016. [Online] Available at: http://www.xilinx.com/training/fpga/fpga-field-programmable-gate-array.htm.

[19] "Control your applications over the internet," 2004 January. [Online] Available at: http://www.popularmechanics.com/technology/gadgets/a4775/1279916/.

[20] "Control your house lights (and more) with your iPhone," 2011. [Online] Available at: http://cybernetnews.com/control-lights-with-your-iphone/.

[21] "What is home automation and how does it work?" from *SafeWise*. [Online] Available at: http://www.safewise.com/home-security-faq/how-does-home-automation-work.

[22] K. Y. Lee, J.W. Choi. "Remote-controlled home automation system via Bluetooth home network," in *SICE 2003 Annual Conference*, volume 3, pp. 2824-2829, 2003 August.

[23] F. Baig, S. Beg, M. F. Khan. "Controlling home appliances remotely through voice command," in *International Journal of Computer Applications*, volume 48-NO. 17, 2012 June. [Online] Available at: https://arxiv.org/ftp/arxiv/papers/1212/1212.1790.pdf.

[24] M. Holladay. "Get ready for Smart Appliances," from *Green Building Advisor*, 2014 August. [Online] Available at: http://www.greenbuildingadvisor.com/blogs/dept/musings/get-ready-smart-appliances.

[25] “Demand Response,” from *Office of Electricity Delivery & Energy Reliability*. [Online] Available at: http://energy.gov/oe/technology-development/smart-grid/demand-response.
[26] T. Güneysu. “Utilizing hard cores of modern FPGA devices for high-performance cryptography”, *Journal of Cryptographic Engineering*, volume 1, issue 1, pp. 37-55, April 2011.

[27] N. Doshi, D. Jinwala. “Constant Ciphertext Length in CP-ABE” [Online] Available at: https://eprint.iacr.org/2012/500.pdf

APPENDIX:

Command Code for Attribute-Based Encryption Procedure

```
// Define attributes for 2 subscribers
// 1.(1) WI          (2) IL          (3) CA          (4) ID          (5) ND          (6) SD
//      (7) KS          (8) CO          (9) WY          (10) MT          (11) NM          (12) TX
//      (13) Zip = 2016       (14) Zip = 2015       (15) Zip = 2014

// 2.(1) MI          (2) IN          (3) PA          (4) NY          (5) VA          (6) NC
//      (7) KY          (8) AR          (9) MS          (10) AL          (11) GA          (12) SC
//      (13) Zip = 2016       (14) Zip = 2015       (15) Zip = 2012

./ cpabe-setup
./ ls                                   // setup PK, MK


./ cpabe-keygen -o subsc1_priv_key pub_key master_key \
    CHN PHL HKG NZL PAK THA India Uganda Japan Korea Iraq Cambodia \
    'Zip = 2016' 'Zip = 2015' 'Zip = 2014'
./ cpabe-keygen -o subsc2_priv_key pub_key master)key \
    USA GBR FRA AUS ITA BEL Peru Poland Norway Germany Denmark Brazil \
    'Zip = 2016' 'Zip = 2015' 'Zip = 2012'
./ ls

cat > message.txt

This message can only be read by the people who have the allowance.

(Ctrl+D to exit the content editing)
./ls
./cpabe-enc pub_key message.txt
    (WI) and ('Zip = 2015')
(Ctrl+D to exit)
./ls
message.txt.cpabe

./cpabe-dec subsc1_priv_key message.txt.cpabe
./ls
pub_key subsc1_priv_key message.txt
```