Smart Grid 智能电网, 2015, 5, 20-26
Published Online February 2015 in Hans. http://www.hanspub.org/journal/sg
http://dx.doi.org/10.12677/sg.2015.51003

Hans汉斯

Smart Grid Payment Scheme Based on Ring Signature and Certificateless Signature

Wei Wang, Haipeng Qu, Peng Shang, Shasha Shi

College of Information Science and Engineering, Ocean University of China, Qingdao Shandong
Email: quhaipeng@ouc.edu.cn

Received: Jan. 4th, 2015; accepted: Jan. 19th, 2015; published: Jan. 22nd, 2015

Abstract

With the continuous development of smart grid technologies in recent years, while smart meter system provides more accurate control and measurement of electrical loads, it has brought information disclosure risks to the user. Researchers have proposed some algorithms, which anonymize user information through the password techniques; but these algorithms have drawbacks that anonymity is not complete, the calculation amount is large, and interactions are complex. This paper puts forward a payment scheme based on ring signature and certificateless signature to protect the privacy of users while completing electricity data collection and payment correctly. The scheme uses anonymous payment algorithm to make a trusted third party only produce the private key of user part. It achieves unconditional anonymity, and reduces computational spending at the whole process and thus has a good practical value.

Keywords

Smart Grid, Ring Signature, Certificateless Signature

基于环签名及无证书签名的智能电网缴费方案

王　玮，曲海鹏，尚　鹏，石沙沙

信息科学与工程学院，中国海洋大学，山东 青岛
Email: quhaipeng@ouc.edu.cn

收稿日期：2015年1月4日；录用日期：2015年1月19日；发布日期：2015年1月22日

摘　要

随着近几年智能电网技术的不断发展，智能电表系统在提供更为精准的电力负载控制与计量的同时，也给电力用户的隐私带来了信息泄露的风险。研究者已经提出了一些算法，通过密码技术对用户信息进行匿名化，但这些算法存在匿名性不彻底、计算开销大、交互复杂等缺点。本文提出一个基于环签名以及无证书签名的缴费方案，在保护用户信息不泄露的前提下控制通过智能电表完成用电数据采集并进行正确缴费的过程。方案中使用匿名缴费算法使可信第三方只能产生用户部分私钥，实现无条件匿名，整个过程计算开销较小，具有较好的实际应用价值。

关键词

智能电网，环签名，无证书签名

1. 引言

在经济全球化的今天，节能环保、低碳持久的经济战略使得智能电网概念应运而生。但是与此同时，智能电网也面临着新的风险，尤其是用户使用时产生的安全与隐私问题。在智能电网中，由于用户的用电数据是由智能电表自动收集并将具体用电信息反馈至服务提供商，恶意攻击者可以从智能电表收集到的大量用电数据中推测出该用户的日常生活规律。例如：不同的家用电器在不同时间的用电量就能够较为准确的反映出用户的行为信息。

针对严重的用户隐私泄露问题，学者们提出了不同的方案进行保护。文献[1]是从智能电表的安全性着手考虑，阐述了如何在第三方托管协议的协助下成功设计出匿名电表的身份标识，直接从数据出口智能电表处实现在发送用户的实时用电量情况下的匿名性。文献[2]-[4]分别根据同态加密技术的特性、语义支持的互联网技术、可信平台技术设计了极为有效的信息聚合方法，通过用户隐私感知架构以及规模化、灵活化的智能电表配置、实时准确的通信框架，采用多种技术保护智能电网中的用户隐私问题。文献[5] [6]主要研究智能电表的硬件安全，根据智能电表的硬件特点制定相关的适用策略，从硬件的角度实现用户隐私保护。文献[7]和文献[8]都是从用户的行为进行考虑。文献[7]提出的方案中运用了数论的思想，以零知识、承诺的概念为突破口，证明了一个既能依据动态的计价标准进行缴费又能保证用户的用电情况不被泄露的方法，这样用户在缴费的过程中可以不必担心隐私的泄露，安全进行缴费活动。文献[8]是从恶意用户的角度观察问题，针对恶意的用户进行不正当用电行为(窃电)情况，使用基于线性系统方程思想的检测方案，该方法能够在正确检查用户是否窃电的前提下，保证用户的用电数据信息不会被泄露，达到用户隐私保护的目的。

文献[9]使用群签名和同态加密算法实现用户计费问题。由可信第三方负责分发用户以及服务提供商密钥。用户计算电费总和，通过服务提供商的公钥进行同态加密，再用私钥对同态加密结果进行群签名。服务提供商将用户发送过来的电费数额与计算得到的电费数额进行比较，如果不一致，由可信第三方解决纠纷。该方案中主要存在三个问题：首先可信第三方的权利过大，由可信第三方规定群中用户，当它使某一用户加入特定的群后，将通知服务提供商并发送用户相应的密钥。如果可信第三方中出现恶意攻击者，由于可信第三方熟知用户的密钥，其恶意攻击者便可以伪造用户的消息进行签名。其次，群签名的实现需要一个群管理者，恶意的群管理者的陷门信息将会揭露群中具体签名人员的身份，匿名不够彻底。最后，群签名的过程主要有初始化过程、群成员加入过程、签名过程、验证过程以及打开过程，在签名过程中还使用了同态加密技术，而同态加密有大量的计算开销，整个方案的实施代价较高。

本文通过研究智能电网中造成用户隐私泄露的途径，分析得到环签名的无条件匿名性以及不可伪造

性在智能电表传输信息过程中能有效保护用户的具体用电数据，很好地保护用户隐私。同时，为了削弱可信第三方的权利，无证书密码系统中的可信第三方不直接生成用户的私钥，只发送部分私钥，用户可以根据部分私钥计算自己的最终私钥。基于这样的思想，本论文提出结合环签名以及无证书的签名技术、在智能电网中完成正确缴费的同时保护用户隐私安全的方案。

2. 方案设计

该方案主要包括 4 个实体：智能电表、用户、可信第三方(密钥产生中心 KGC)以及服务供应商。KGC 是一个既被服务供应商又被用户信任的机构，负责密钥的分发并对用户身份进行管理。当缴费过程中出现用户计算费用与服务提供商计算费用不一致时，由 KGC 解决冲突。智能电表将用户的用电量定时发给用户以及服务供应商。服务供应商从智能电表中收集用电数据，向用户收取相应的费用。用户从智能电表中得到数据后计算费用并向服务供应商缴纳。

2.1. 概述

该方案主要包括以下过程，如图 1 所示。

该方案包括以下算法：

1) **Setup：** KGC 建立系统。根据用户的地理位置确定用户所在的群组以及用户对应的服务提供商。

2) **Exract：** KGC 产生并分发用户的 tag (由 KGC 加密并且签名的用户 id)，用户的部分私钥，服务供应商的密钥。

3) **Protocol：**

a) 智能电表按照一定的时间间隔周期性地将用电数据发送给用户，用户通过服务提供商的计费价目表进行费用计算，同时用户自己选择一个秘密值，和从 KGC 中得到的部分私钥计算得到属于自己的私钥，将计算出的电费和从 KGC 得到的 tag 一起用 KGC 的公钥进行加密并进行无证书签名，该签名与计算费用再由群公钥进行加密，然后进行环签名。将该结果发送至智能电表。

b) 智能电表收到用户发来的信息后，将该结果与用户使用电量和环信息发送至服务供应商。首先服务提供商验证签名的有效性，通过智能电表发送的用电数据计算费用，对比与私钥解密出来的用户提交的费用是否一致。如果一致，完成本次缴费，否则，由 KGC 解决不一致问题。

c) 当用户缴纳费用与服务提供商计算费用不一致时，服务提供商将费用以及环签名结果发送至 KGC，KGC 得到信息后，对比计算费用，找到计算错误的用户 tag，再通过解密得到用户 id。KGC 根据 id 信息通知该用户重新进行缴费工作。

2.2. 匿名缴费算法

在文献[10]-[13]中主要介绍环签名的思想并且分析环签名的特性；文献[14]-[16]主要介绍无证书签名的基本思想及其特点。本文提出的方案主要结合环签名方案[11]以及无证书的签名方案[17]进行设计，具体实现如下：

1) **Setup：** 加法群 G 和乘法群为 $G1$ 的阶均为素数 q，P 是 G 的生成元，双线性对为 e：$G\times G\to G1$，$g=e(P,P)$，定义哈希函数如下：

$$H_1:\{0,1\}^*\to Z_q^*$$

$$H_2:\{0,1\}^*\times\{0,1\}^*\times G1\times G\times G1\times G1\to Z_q^*$$

$$H_3:G1\to Z_q^*$$

$$H_4:\{0,1\}^*\to G$$

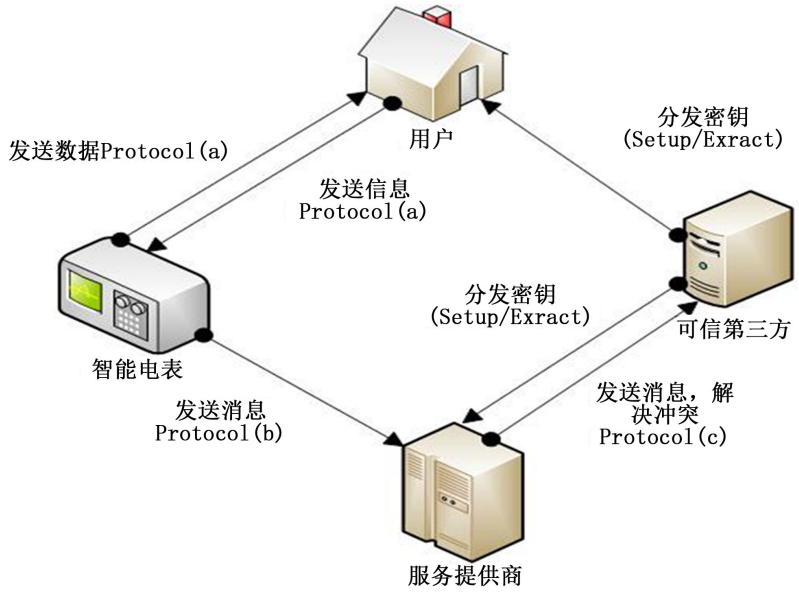

Figure 1. The flow chart of anonymous payment scheme
图 1. 本方案流程图

随机选择一个私钥 $s \in Z_q^*$，计算群公钥为 $PK_K = SP$。得到公钥后进行系统参数发布，KGC 将公钥通过安全的信道发送至用户以及服务提供商。KGC 将用户 *id* 进行加密并且签名形成 *tag*，同时利用 *tag* 值计算用户的部分私钥：

$$SK_u = \left(\frac{1}{(s+D_u)}\right)P$$

其中 $D_u = H_1(tag)$，最后将 *tag* 以及部分私钥 SK_u 也通过安全信道发送给用户。

2) **Extract**：用户选择一个随机的值 $s \in Z_q^*$，用户的公钥计算为：

$$PK_u = (P_1, P_2)$$

其中 $P_1 = g^m$， $P_2 = H_3(P_1)(PK_K + D_u P)$。用户从 KGC 处收到部分私钥验证：

$$e(SK_u, PK_K + D_u P) \bmod q = g$$

该等式成立，则用户私钥确立为：

$$SK = (m, SK_u)$$

该验证过程如下：

$$\begin{aligned} & e(SK_u, PK_K + D_u P) \bmod q \\ &= e\left(\left(\frac{1}{(s+D_u)}\right)P, PK_K + D_u P\right) \bmod q \\ &= e(P,P)^{\frac{(s+D_u)}{(s+D_u)}} \bmod q = g \end{aligned}$$

3) **Protocol**：

a) 用户从智能电表得到自己的用电数据情况，根据服务提供商公布的电价说明进行计算，得到用电实际费用 *fee*，将 *fee* 与 *tag* 用群公钥进行加密，同时用自己的私钥进行无证书签名。

用户随机地选择 $l_1, l_2 \in Z_q$，并且进行以下计算：

令： $L_1 = g^{l_1}$， $L_2 = g^{l_2}$

$$h = H_2\left(fee, tag, PK_u, g^{l_1}, g^{l_2}\right)$$

$$M = \left(\frac{\left(l_1 + \left(H_2\left(fee, tag, PK_u, g^{l_1}, g^{l_2}\right)\right)\right)}{H_3\left(P_1\right)}\right) SK_u$$

$$V = m\left(H_2\left(fee, tag, PK_u, g^{l_1}, g^{l_2}\right)\right) + l_2$$

通过计算，该用户对此消息的签名为(M,V,h)。该签名与 fee 通过服务提供商的公钥加密进行环签名。假设匿名范围中成员的集合为 $U=\{tag_1, tag_2, \cdots, tag_u\}$，签名者随机选取一个值 $A \in G$，计算 $c_{k+i} = H_2\left(U \| fee \| e(A,P)\right)$ 产生环序列，随机选择 $T_i \in G$，并且计算 $c_{i+1} = H_2\left(U \| fee \| e(T_i,P) e\left(c_i, H_4\left(tag_i\right), PK_i\right)\right)$，$i = 0,1,2,\cdots,k+1,\cdots,u-1$；$T_k = A - c_k SK_k$，则环签名的结果为$\left(c_0, T_0, T_1, \cdots, T_{u-1}\right)$。最终将该结果发送给智能电表。智能电表收到用户发送的信息之后，将该消息与用户的用电数据以及环信息打包发送给服务提供商。

b) 服务供应商进行收费。服务提供商接收智能电表发送的信息，通过用电量以及对应计价方法计算用户实际使用费用，验证环签名的有效性，输入 fee，U，环签名结果，计算 c_{i+1}。若 $c_0 = c_u$，则说明环签名有效，否则拒绝该消息。将服务提供商计算费用与智能电表发送费用进行比较，如果一致，则完成本次缴费，否则，将该信息发送给 KGC，由 KGC 解决冲突。

c) KGC 解决冲突。当 KGC 收到由服务供应商发送的信息后，由 KGC 验证：

$$h = H_2\left(fee, tag, PK_u, L_1, L_2\right)$$

该等式成立，则证明无证书签名有效。其中：

$$P_2 = H_3\left(P_1\right)\left(PK_K + D_u P\right)$$

$$L_1 = e\left(M, P_2\right) g^{-h}$$

$$L_2 = g^V P_1^{-h}$$

最后，KGC 通过私钥解密后获取用户的 id，找到缴费不成功的用户并通知该用户重新完成缴费。

3. 安全性分析

针对本文提出的在智能电网中的缴费方案，从以下几个方面对其安全性进行了整体分析：

1) **匿名性：**根据该方法无法推算出签名者的实际身份。在签名过程中所使用的参数是根据一定的规则进行首尾相接而组成的环状，整个的签名过程完全不需要群管理员进行参与，所以根本无法通过陷门信息获得签名者的具体信息。恶意攻击者即使非法获得了所有可能签名者的私钥，能够成功找出该签名者的概率也很小，不会超过 u （u 为所有签名者的个数)。

2) **不可伪造性：**恶意攻击者在无法获取群成员私钥的情况下，即便通过其他手段从产生环签名的模型中得到了关于任何消息的签名也不可能成功伪造出一个合法的签名。

3) **可操作性：**在整个签名过程中，实际的签名者可以从所有用户中随机任意选择出参与该签名过程的用户，生成一个环签名方案，但不需要通知那些被选中的用户。

4) **机密性：**KGC 只能生成用户的部分私钥，用户的最终私钥由部分私钥以及用户选取的秘密值组成，从而减少 KGC 的恶意行为的发生，保证的用户私钥的机密性。

5) **不可关联性：**KGC 将用户信息 id 进行加密并签名，服务提供商、恶意攻击者无法获取用户的信息，无法将用户与其具体的用电数据进行关联，从而不能分析出用户的生活规律；同时 KGC 不能获取用

户的用电信息，从而也不能将用户信息与用电数据进行关联，这样保证了不泄露用户的隐私。

6) **正确性：**为了完成正确的缴费行为，需要满足的条件是在验证签名的有效性的同时双方计算的费用一致。当双方的计算费用不一致时，服务提供商通过 KGC 进行公平解决，由 KGC 确认缴费不一致行为的发生，根据用户信息通知用户进行重新缴费。

根据以上安全性的分析，该方案确实实现了在智能电网中保护用户隐私的前提下，完成智能电表全部用电数据的存储以及服务供应商与用户之间的正确缴费。

4. 方案比较

文献[9] (下文称：群签名方案)与本文提出的方案的特点对比如表 1 所示。

- 群签名方案中对于 KGC 赋予的权利过大。KGC 的职责主要有：规定用户所属的群，计算群公钥，向用户本人、服务提供商发送密钥信息以及最终当用户与服务提供商费用结算不一致时进行纠纷解决。当 KGC 中出现恶意攻击者，并且恶意攻击者知道用户的密钥信息，根据密钥信息，该攻击者可以伪造用户的签名。在本方案里，KGC 只计算部分私钥，由用户选择一个秘密值，与 KGC 发送的部分私钥共同计算得到最终的私钥，然后生成相应的公钥。这样，用户密钥信息的生成是由用户与 KGC 共同参与完成的，KGC 就成为了半可信的(semi-honest)，有效削弱了 KGC 的权利。
- 群签名方案的群签名技术无法做到无条件匿名。群管理员的陷门信息将会揭露群中具体签名者的身份，若群管理员怀有恶意，那么群中成员的身份信息将会泄露。本文提出的方案，不需要管理员、签名者用自己的私钥和任意个环成员的公钥对消息进行签名，只需要验证是否为环成员所签。恶意攻击者即使知道环成员中所有人的私钥，也无法确定具体是由哪个成员进行的签名，实现了无条件的匿名。
- 群签名方案的实现代价较大。群签名的过程主要有初始化过程、群成员加入过程、签名过程、验证过程以及打开过程，在签名过程中还使用了同态加密技术，而同态加密有大量的计算开销，本方案使用的环签名技术主要有密钥生成过程、签名过程以及签名验证过程，无证书的签名技术主要计算用户的部分私钥。另外在整个环签名过程中，实际的签名者可以从所有用户中随机任意选择出参与该签名过程的用户，生成一个环签名方案，并且不需要通知那些被选中的用户。
- 最后考虑到用户缴费过程中可能出现的收费不一致问题，利用 KGC 进行校验，可以迅速准确的找到问题用户，达到了准确收费的要求。用户的身份 id 仅由 KGC 存储，整个缴费过程中，用户的身份信息都是经过 KGC 加密并签名的，只有 KGC 拥有。若用户身份信息遭到泄露，将可以确定是 KGC 出现问题并追究责任，本方案从用户身份信息以及用户用电信息两方面进行了安全保护。

综上所述：本方案的优势在于削弱了 KGC 的权利，匿名过程更加彻底、实现的代价更小。

Table 1. Characteristics of scheme comparison
表 1. 方案特点对比

特点	群签名方案	本方案
匿名性		具有无条件匿名性质，匿名过程更加彻底
可操作性		实现代价较小，无大量的计算需求
机密性		使用无证书签名，减小 KGC 的权利，增加机密性
正确性	√	√
不可关联性	√	√
不可伪造性	√	√

5. 结论

为了保护用户在智能电网中的隐私安全，基于环签名和无证书签名的思想，本文提出了智能电网用户缴费方案。方案通过匿名缴费算法实现用户缴费过程中的无条件匿名，可以有效防止服务提供商根据缴费信息和用电量获取用户的行为信息。同时用户的私钥由用户选择随机数计算产生，服务提供商无法获取用户身份。该方案保证了服务提供商与用户的利益，保证了双方的正确缴费过程。匿名缴费算法实现过程中计算开销较小，运用于实际生活中的可行性更高，应用价值更大。

参考文献 (References)

[1] Rial, A., Leuven, K.U. & IBBT, Leuven, Belgium, G. (2010) Privacy-preserving smart metering technical report. MSRTR-2010-150, Microsoft Research, 49-60.

[2] The Smart Grid Interoperability Panel (2009) Smart grid cyber security strategy and requirements. Technical Report 7628, National Institute of Standards and Technology, Vol. 2.

[3] Lisovich, M.A. and Wicker, S.B. (2008) Privacy concerns in upcoming residential and commercial demand-response system. *Power Systems Conference*, 553-570.

[4] McDaniel, P. and McLaughlin, S. (2009) Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, **7**, 75-77.

[5] Wagner, A., Speiser, S., Raabe, O. and Harth, A. (2010) Linked data for a privacy-aware smart gird. 448-454.

[6] Lemay, M., Gross, G., Gunter, A. and Garg, S. (2007) United architecture for largr-scale attested metering. *International Conference on System Sciences*, 1503-1605.

[7] Alinas, S.S. and Li, M. (2012) Mesh and Ad Hoc Communications and Networks. 9*th Annual IEEE Communications Society Conference*, 18-21 June 2012, 605-613.

[8] Garcia, F. and Jacobs, B. (2010) Privacy-Friendly Energy-Metering via Homomorphic Encryption. *Workshop on Security and Trust Management*, 226-239.

[9] 龚凡 (2013) 基于群签名的智能电网用电量统计及电费的缴费方案. 硕士论文, 西安电子科技大学, 西安.

[10] Rivest, R.L., Shamir, A. and Tauman, Y. (2001) How to leak a secret. LNCS 2248. Spring-Verlag, Berlin, 552-565.

[11] Zhang, F. and Kim, K. (2002) ID based blind sighature and ring signature from pairings. Spring-Verlag, Berlin, 533-576.

[12] Bresson, E., Stern, J. and Szydlo, M. (2002) Thresh old ring signatures for ad-hoc groups. LNCS 2501. Spring-Verlag, Berlin, 465-480.

[13] 王文强, 陈少真 (2009) 一种基于身份的高效环签名方案. *计算机应用*, **11**, 10-14.

[14] Harn, L., Ren J. and Lin, C.L. (2009) Design of DL-based certificateless digital signatures. *Journal of System and Software*, **82**, 789-793.

[15] Duan, S.S. (2008) Certificateless undeniable signature scheme. *Information Sciences*, **178**, 742-755.

[16] Bessie, C.H., Zhang, Z.F. and Dong, X.T. (2007) Certificateless signature: A new security model and improved generic construction. *Designs, Codes and Cryptography*, **42**, 109-125.

[17] 梁红梅, 黄振杰 (2010) 高效无证书签名方案的安全性分析和改进. *计算机应用*, **3**, 685-687.

汉斯出版社为全球科研工作者搭建开放的网络学术中文交流平台。自2011年创办以来，汉斯一直保持着稳健快速发展。随着国内外知名高校学者的陆续加入，汉斯电子期刊已被450多所大中华地区高校图书馆的电子资源采用，并被中国知网全文收录，被学术界广为认同。

汉斯出版社是国内开源（Open Access）电子期刊模式的先行者，其创办的所有期刊全部开放阅读，即读者可以通过互联网免费获取期刊内容，在非商业性使用的前提下，读者不支付任何费用就可引用、复制、传播期刊的部分或全部内容。