云计算中基于公平的安全判定相等协议的身份认证方案*

刘婷婷[1]，王文彬[2]
（1. 信息工程大学，河南 郑州 450012；2. 61660 部队，北京 100840）

摘　要：云用户与云之间的双向认证是云计算中用户访问云中资源和数据的重要前提。为解决云计算环境下基于口令的身份认证方式存在的问题，并保证海量用户环境下认证的效率，对一个常数复杂性的判定口令相等的百万富翁协议进行了改进，提出了一个公平的安全双方判定相等协议，可以公平且秘密地比对认证方与被认证方所拥有口令的一致性。在上述协议的基础上，基于具有语义安全的加法同态算法——Bresson 算法，实现了一个保护云用户和云服务提供者双方隐私的身份认证方案，最后，证明了该身份认证方案在判定相等方面的正确性，并给出了方案的安全性分析。

关键词：云计算；公平的安全双方判定相等协议；Bresson 算法；身份认证
中图分类号：TP309.2　　**文献标志码**：A　　**文章编号**：1001－2486(2013)05－0120－04

An authentication scheme based on fair equality-determination protocol in cloud computing

LIU Tingting[1], *WANG Wenbin*[2]
(1. Information Engineering University, Zhengzhou 450012, China; 2. Unit 61660, Beijing 100840, China)

Abstract: Mutual authentication between the user and the cloud is an essential requirement for the user to access the public cloud in cloud computing. In order to solve the problems of password-based identity authentication scheme in the cloud computing environment and to improve the efficiency of authentication in the environments of mass users, a fair equality-determination protocol was presented by developing an equality-determination protocol of constant complexity. The protocol proposed can compare the passwords between the user and the cloud fairly and secretly. Based on the protocol, a two-party privacy-protected identity authentication scheme based on semantically secure algorithm-Bresson algorithm was further presented. Finally, the correctness of the scheme was proved and its security was analyzed.

Key words: cloud computing; fair equality-determination protocol; Bresson algorithm; identity authentication

随着云计算技术的不断进步以及云计算中心的商业化运营，云端服务器存储了大量的用户敏感数据，而用户必须通过网络访问这些数据，因此如何在不安全的网络环境下完成对用户身份的认证是云计算急需解决的问题[1]。而基于口令认证无疑是最为简便、最为常用的一种方式。在基于口令的身份认证系统中，用户拥有一个身份鉴别码(ID)以及与之相应的口令，认证服务器存储的是与用户 ID 和与之对应的口令相关的认证数据，通常是哈希值或者加密的密文。在认证过程中，用户 ID 和口令被发送给认证服务器，服务器通过一定处理并与所存储的认证数据相比较来判断用户身份的合法性。然而，这种方式中密码通常是以明文或者哈希值在网络上传输，容易被黑客截获或破解；同时，恶意的认证服务器很容易破解用户口令，从而威胁用户其他信息系统安全(用户习惯于在不同的信息系统中使用相同的口令)。

安全双方计算主要解决网络上的双方在彼此不知道对方拥有数据具体信息的情况下比较双方数据的关系问题。本文在改进了一个安全双方计算协议的基础上，从保护双方隐私的角度出发，设计了一个基于安全多方计算的身份认证方案，方案的优点在于：(1)用户私有的密码不以明文或简单的哈希值传输，通过公钥加密，确保密码传输中的安全性；(2)保护双方私有数据，可以防止针对认证服务器的密文攻击；(3)方案利用随机数，可以防止中间人攻击；(4)降低传统基于口令认证方式中用户端的安全劣势。

* **收稿日期**：2013－01－12
基金项目：国家科技重大专项课题资助项目(2012ZX03002003)
作者简介：刘婷婷(1984—)，女，山东济南人，博士研究生，E-mail：ann320120@yahoo.com.cn；
王文彬(通信作者)，男，博士，工程师，E-mail：buptwwb@yahoo.com.cn

1　相关研究

1.1　身份认证技术

常用的身份认证方法包括主体特征认证、公钥证书认证机制和口令认证。

1)主体特征认证

主体特征认证是指利用个人特征进行认证的方式 ,具有很高的安全性。目前已有的方法包括:视网膜扫描、声音验证、指纹和手型识别器。这些识别系统能够监测指纹、签名、声音等物理特征。但这些系统价格昂贵、可靠性差。

2)公钥认证机制

公钥认证泛指所有应用公钥加密和签名的公钥基础设施(PKI)。PKI 包括公开密钥密码技术、数字证书、认证机构、注册机构和关于公开密钥的安全策略等基本成分组成。公钥认证机制可以有效并且非常安全地解决身份认证问题,但过于完整,过于庞大,成本高昂,技术复杂。

3)口令认证

口令认证是指认证双方相互约定代码,在验证时,被认证方如果能提供该约定的代码,即通过认证,然后协商一个安全的会话密钥。基于口令的方案可以避免复杂的密钥管理 ,无需额外的公钥设施或者安全硬件。因此,虽然这种机制容易受到字典攻击,中间人攻击,但还是以其方便性而得到了广泛的应用。目前已经有许多基于口令实现的方案[3-5]。

1.2　安全双方计算

安全双方计算协议也称为百万富翁协议,首先由 Yao[6] 提出。该协议主要解决如下问题:两个百万富翁想知道谁拥有更多的财富,但是不想让对方知道财富的进一步信息。将该问题简化为如下的模型:Alice 知道整数 i 且 Bob 知道整数 j,协议结束后,Alice 和 Bob 都知道 $i \geqslant j$ 或 $i < j$,但都没有得到关于 i 和 j 的进一步信息。很多研究都只倾向于必须分出谁更富有的通用解决方案[7-8]及提高现有方案的效率[9],没给出相等情况的比较协议。而如何秘密比较 $i = j$ 即拥有相当财富的情况后来被发现有很大的用途,这就是人们所熟知的社会主义百万富翁问题[10]。

社会主义百万富翁问题假设 Alice,Bob 分别拥有秘密输入 a,b(以下都只考虑秘密输入为整数的情况),他们希望不泄露秘密输入信息而比较出 a,b 是否相等。

1.3　Bresson 算法

Bresson 算法是由 Bresson 等提出的一个公钥密码算法[11]。该算法通过对明文加入随机数进行加密得到密文对,然后由得到的密文对进行变换求商得到明文。Bresson 算法可以被用来解决组密钥交换等问题,是被证明了的具有语义安全的加法同态算法[12]。

在基于语义安全的加同态密码体制中,设加密算法为 E,解密算法为 D,其中加密密钥公开,解密密钥保密。明文空间 $M \subseteq Z$,E 满足下面两个性质:

1)语义安全性:对任意两个消息 $m_1, m_2 \in M$,不存在多项式时间算法区分 $E(m_1), E(m_2)$;

2)加法同态性:对任意消息 $m_1, m_2 \in M$,任意 $k \in Z$,若 $m_1 + m_2 \in M$,且 $km_1 \in M$,则 $D(E(m_1)E(m_2)) = m_1 + m_2$ 且 $D(E(m_1)^k) = km_1$。

2　一个公平的安全双方判定相等协议

令 Alice 是认证方,可认为是云端管理员,而 Bob 是被认证方,可认为是云用户。Alice 需验证 Bob 的口令是否正确,以授权其对云服务或资源的访问权。

文献[8]将文献[2]中的一个常数复杂性的百万富翁协议做了改进并推广得出如下的安全双方判定相等协议。

设加密算法 E,解密算法 D 满足基于语义安全的加法同态性。

输入:Alice 拥有秘密输入为 a;Bob 拥有秘密输入为 b;

输出:$a = b$ 或者 $a \neq b$;

协议步骤:

Step1:Alice 用自己的公钥计算 $c = E(a)$ 发给 Bob;

Step2:Bob 随机选择整数 u_1, v_1, w_1,使 $|v_1 - w_1| < u_1$ 且 $u_1 > 0$,并用 Alice 的公钥计算 $X_1 = c^{u_1}E(v_1)$,$Y_1 = E(u_1 b + w_1)$ 发送给 Alice;

Step3:Alice 解密 $D(X_1) = u_1 a + v_1$,$D(Y_1) = u_1 b + w_1$,若 $D(X_1) > D(Y_1)$,则 $a \geqslant b$,否则,若 $D(X_1) < D(Y_1)$,则 $a \leqslant b$;

Step4:Alice 通知 Bob 再随机选择整数 u_2, v_2, w_2,使 $|v_2 - w_2| < u_2, u_2 > 0$ 且 $(v_2 - w_2)(v_1 - w_1) < 0$,并用 Alice 的公钥计算 $X_2 = c^{u_2}E(v_2)$,$Y_2 = E(u_2 b + w_2)$ 发送给 Alice;

Step5:Alice 解密 $D(X_2) = u_2 a + v_2$,$D(Y_2) = u_2 b + w_2$,若 $D(X_2) > D(Y_2)$,则 $a \geqslant b$,否则,若 $D(X_2) < D(Y_2)$,则 $a \leqslant b$;

Step6:Alice 分析两次比较的结果,若 $(D(X_1) - D(Y_1)) \oplus (D(X_2) - D(Y_2)) = 1$,则 $a = b$;

Step7：Alice 把比较结果告知 Bob。

根据整个判定相等协议过程可知，Alice 实际上是占有优势的一方，虽然文献[8]证明了协议的计算安全性，但是显然 Alice 要拥有更多的密文资源；如果云端管理员 Alice 存在恶意，那么云用户 Bob 将得不到正确的结果，这些对于 Bob 来讲是不公平的。为此，基于文献[8]给出的协议，本文改进得到一个公平的安全双方判定相等协议如下，以保护云用户的权益。

Step1′：Alice 用自己的公钥计算 $c=E(a)$ 发给 Bob；

Step2′：Bob 随机选择整数 u_1，v_1，w_1，使 $|v_1-w_1|<u_1$ 且 $u_1>0$，并用 Alice 的公钥计算 $X_1=c^{u_1}E(v_1)$，$Y_1=E(u_1b+w_1)$ 发送给 Alice；

Step3′：Alice 解密 $D(X_1)=u_1a+v_1$，$D(Y_1)=u_1b+w_1$，若 $D(X_1)>D(Y_1)$，则 $a\geqslant b$，否则，若 $D(X_1)<D(Y_1)$，则 $a\leqslant b$；

Step4′：Alice 再随机选择整数 u_2，v_2，w_2，使 $|v_2-w_2|<u_2$，$u_2>0$ 且 $v_2-w_2<0$，并用 Bob 的公钥计算 $X_2=c^{u_2}E(v_2)$，$Y_2=E(u_2b+w_2)$ 发送给 Bob；

Step5′：Bob 解密 $D(X_2)=u_2a+v_2$，$D(Y_2)=u_2b+w_2$，若 $D(X_2)>D(Y_2)$，则 $a\geqslant b$，否则，若 $D(X_2)<D(Y_2)$，则 $a\leqslant b$；

Step6′：Alice 将 $D(X_1)-D(Y_1)$ 利用 Bob 公钥加密后发送给 Bob；

Step7′：Bob 将 $D(X_2)-D(Y_2)$ 利用 Alice 公钥加密后发送给 Alice；

Step8′：Alice 和 Bob 分别解密分析比较的结果，若 $(D(X_1)-D(Y_1))\oplus(D(X_2)-D(Y_2))=1$，则 $a=b$，否则 $a\neq b$；

3 一种保护双方隐私的身份认证方案

为了避免口令在不安全网络上的传输，且保护认证双方的口令隐私，采用第 2 部分设计的公平的判定相等协议，可以秘密地比对认证与被认证端所拥有口令的一致性，从而达到身份认证的目的。由于任何口令都可表示成一串二进制比特串，而任何比特串都可以化为一个整数，因此，比较口令的一致性就转化为两个数的比较。本部分以公平的判定相等协议为基础，实现了一个基于 Bresson 算法的保护双方隐私的身份认证方案，并对其正确性和安全性进行了验证。

3.1 基于 Bresson 算法的隐私保护身份认证方案

假设 Alice 是认证者，拥有的口令为 a；Bob 是被认证者，拥有的口令为 b；

Step1：Bob 向 Alice 发送认证请求；

Step2：Alice 随机地选取两个比较大的素数 p，q，满足：$N=pq$，$p=2p_0+1$，$q=2q_0+1$，p_0，q_0 也为素数，G 为模 N^2 的二次剩余循环群，Alice 再随机选择 $\alpha\in\mathbf{Z}_{N^2}^*$ 和 $\beta\in[1,ord(G)]$（其中：$\alpha\neq kN$，k 为整数），并使 $g_1=\alpha^2 \bmod N_1^2$，$h_1=g_1^{\beta_1} \bmod N_1^2$，Alice 将 (N_1,g_1,h_1) 作为自己的公钥公开，将 β_1 作为对应的私钥保存。

Step3：Bob 根据 Bresson 算法要求，选取 (N_2,g_2,h_2) 作为自己的公钥公开，将 β_2 作为对应的私钥保存。

Step4：Alice 在 $Z_{N_1^2}$ 中随机选择数 r_1，计算 $c=(g_1^{r_1} \bmod N_1^2, h_1^{r_1}(1+aN_1) \bmod N_1^2)$。Alice 将 c 发送给 Bob；

Step5：Bob 随机选择整数 u_1，v_1，w_1，使 $v_1-w_1<u_1$ 且 $u_1>0$，$v_1-w_1>0$，Bob 再随机选取数 r_2，用 Alice 的公钥计算：$X_1=(g_1^{r_1r_2u_1} \bmod N_1^2, h_1^{r_1r_2u_1}(1+(u_1a+v_1)N_1) \bmod N_1^2)$，$Y_1=(g_1^{r_2} \bmod N_1^2, h_1^{r_2}(1+(u_1b+w_1)N_1) \bmod N_1^2)$，并发送给 Alice；

Step6：Alice 解密：

$$D(X_1)=\left[\frac{h_1^{r_1r_2u_1}[1+(u_1a+v_1)N_1^2] \bmod N_1^2}{g_1^{r_1r_2u_1\beta_1} \bmod N_1^2}-1\right] \bmod N_1^2/N_1$$
$$=u_1a+v_1 \bmod N_1^2$$
$$D(Y_1)=\left[\frac{h_1^{r_2}[1+(u_1b+w_1)N_1] \bmod N_1^2}{g^{r_2\beta_1} \bmod N_1^2}-1\right] \bmod N_1^2/N_1$$
$$=u_1b+w_1 \bmod N_1^2$$

若 $D(X_1)>D(Y_1)$，则 $a\geqslant b$，否则，若 $D(X_1)<D(Y_1)$，则 $a\leqslant b$；

Step7：Alice 再随机选择整数 u_2，v_2，w_2，使 $|v_2-w_2|<u_2$，$u_2>0$ 且 $v_2-w_2<0$。Alice 再随机选取数 r_3，利用 Bob 的公钥计算：

$X_2=(g_2^{r_1r_3u_2} \bmod N_2^2, h^{r_1r_3u_2}(1+(u_2a+v_2)N_2) \bmod N_2^2)$，$Y_2=(g_2^{r_3} \bmod {N_2}^2, h_2^{r_3}(1+(u_2b+w_2)N_2) \bmod N_2^2)$，Alice 将 X_2，Y_2 发送给 Bob；

Step8：Bob 解密：$D(X_2)=u_2a+v_2 \bmod N_2^2$，$D(Y_2)=u_2b+w_2 \bmod N_2^2$；若 $D(X_2)>D(Y_2)$，则 $a\geqslant b$，否则，若 $D(X_2)<D(Y_2)$，则 $a\leqslant b$；

Step9：Alice 将 $D(X_1)-D(Y_1)=a_1$ 利用 Bob 公钥加密后发送给 Bob；

$A_1=g_2^{r_1} \bmod {N_2}^2$，$B_1=h_2^{r_1}(1+a_1N_2) \bmod N_2^2$

Step10：Bob 将 $D(X_2)-D(Y_2)=a_2$ 利用 Alice 公钥加密后发送给 Alice；

$A_2=g_1^{r_2} \bmod {N_1}^2$，$B_2=h_1^{r_2}(1+a_2N_1) \bmod {N_1}^2$

Step11：Alice 和 Bob 分别解密

$$a_1 = \frac{B_1 / A_1^{\beta_2} - 1 \bmod N_2^2}{N_2}$$

$$a_2 = \frac{B_2 / A_2^{\beta_1} - 1 \bmod N_1^2}{N_1}$$

分析比较的结果,若 $a_1 \oplus a_2 = 1$,则 $a = b$;

Step12:Alice 分析,若 $a_1 \oplus a_2 = 1$ 允许 Bob 访问资源,否则,拒绝访问。

3.2　正确性分析

定理 1　$\begin{cases} \text{if } D(X_1) > D(Y_1), \text{then } a \geqslant b \\ \text{if } D(X_1) < D(Y_1), \text{ then } a \leqslant b \end{cases}$

证明　因 $D(X_1) = u_1 a + v_1, D(Y_1) = u_1 b + w_1$,且有 $|v_1 - w_1| < u_1, u_1 > 0$,因此可得

$(D(X_1) - D(Y_1))/u_1 = (a - b) + (v_1 - w_1)/u_1, |(v_1 - w_1)/u_1| < 1$,

所以当 $a \neq b, a, b$ 为整数,则 $|a - b| \geqslant 1$,因此

若 $a - b \geqslant 1 > 0$,则 $D(X_1) > D(Y_1)$

若 $a - b \leqslant -1 < 0$,则 $D(X_1) < D(Y_1)$

当 $a = b$ 时,则 $D(X_1) - D(Y_1)$ 与 $v_1 - w_1$ 符号一致。

定理 2　if $(D(X_1) - D(Y_1)) \oplus (D(X_2) - D(Y_2)) = 1$, then $a = b$。

证明　若 $(D(X_1) - D(Y_1)) \oplus (D(X_2) - D(Y_2)) = 1$

由 $D(X_1) = u_1 a + v_1, D(Y_1) = u_1 b + w_1, D(X_2) = u_2 a + v_2, D(Y_2) = u_2 b + w_2$ 可得

$(D(X_1) - D(Y_1)) \oplus (D(X_2) - D(Y_2))$
$= [u_1(a - b) + v_1 - w_1] \oplus [u_2(a - b) + v_2 - w_2]$

若 $a = b$,由于 $(v_2 - w_2)(v_1 - w_1) < 0$ 成立,$(D(X_1) - D(Y_1)) \oplus (D(X_2) - D(Y_2)) = 1$;

由于 $(D(X_1) - D(Y_1)) \oplus (D(X_2) - D(Y_2)) = 1$,即当 $D(X_1) > D(Y_1)$ 时,$D(X_2) < D(Y_2)$;当 $D(X_1) < D(Y_1), D(X_2) > D(Y_2)$。可知 $D(X_2) > D(Y_2), a > b$ 或 $a = b$;$D(X_2) < D(Y_2)$,同理可得 $a < b$ 或 $a = b$,综上知 $a = b$。

3.3　保护双方隐私的身份认证方案的安全性分析

本节所提保护双方隐私的身份认证方案的安全性是有保证的:

(1)Bob,即被认证方接收到 $c = E(a)$ 后,因为 Bresson 算法加密过程是语义安全的,所以 Bob 无法从中获得任何有关 a 的信息,这就有效地避免了被认证方的试探性攻击,同时也确保了双方口令在网络传输过程中的安全。

(2)Alice,即认证方接收并解密 $D(X_1) = u_1 a + v_1, D(Y_1) = u_1 b + w_1$,自己只知道 a,则根据已有条件计算不出 b 的取值;在接收并解密 $D(X_2) = u_2 a + v_2, D(Y_2) = u_2 b + w_2$ 后也不知道 b 的取值为多少;即使 Alice 将两次得到的信息联立起来,有 6 个未知数,只有 4 个已知条件,所以也无法从中解出 b 的值,因此确保了对被认证方口令信息的隐私保护。

(3)方案在 Step4、Step5、Step7、Step9、Step10 中多次利用随机数加密,可以有效防止中间人攻击。

(4)方案基于一个公平的安全相等判定协议,双方可以安全地得知口令是否一致,且被认证方先得知信息,并将安全凭证 $A_2 = g_1^{r_2} \bmod N_1^2, B_2 = h_1^{r_2}(1 + a_2 N_1) \bmod N_1^2$(Step10)发送给认证方,降低了云计算环境下基于口令认证技术中用户端的安全劣势。

4　结束语

本文在分析一个高效的安全双方相等判定协议的基础上,提出了一个公平的安全双方相等判定协议,并基于 Bresson 算法实现了一种保护双方隐私的身份认证方案,提高了云计算环境下基于口令认证的安全性。该方案拥有如上很多优点,但也存在效率上的问题,这将是我们后续需要解决的问题。另外,探索安全双方计算问题在特殊领域(如云计算环境下保护隐私的双方协同)的应用问题也将是一个新的研究热点。

参考文献(References)

[1]　冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报, 2011, 22(1):71 - 83.
FENG Dengguo, ZHANG Min, ZHANG Yan, et al. Study on cloud computing security[J]. Journal of Software, 2011, 22(1):71 - 83. (in Chinese)

[2]　秦波,秦慧,周克复,等. 常数复杂性的百万富翁协议[J]. 西安理工大学学报, 2005, 21(2):149 - 152.
QIN Bo, QIN Hui, ZHOU Kefu, et al. Millinaires' s protocol with constant complexity[J]. Journal of Xi'an University of Technology, 2005, 21(2):149 - 152. (in Chinese)

[3]　Bellovin S M, Merrit M. Encrypted key exchange: password-based protocols secure against dictionary attacks [C]// Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, IEEE Computer Society, 1992: 72 - 84.

[4]　Gong L, Mark T, Lomas A, et al. Protecting poorly chosen secrets from guessing attacks[J]. IEEE Journal on Selected Areas in Communications, 1993, 11 (5):648 - 656.

[5]　Ding Y, Horster P. Undetectable on-line password guessing attacks[J]. ACM Operating Systems Reviews, 1995, 29 (4): 77 - 86.

(下转第 139 页)

(1)由于没有涡流产生,图中互感梯度不随时间变化,其大小接近导电导磁材料封装时电流平沿的互感梯度值。

(2)间隙 d 越小,封装厚度 t 越大,则互感梯度越大。$d=1, t=6$ 曲线互感梯度最大。减小封装与线圈的间隙 d,增加封装厚度 t,导磁材料的磁场加强效果更好。因此可以采用硅钢叠片,当叠片厚度足够小的时候可以尽量减小材料的电导率,使得封装内的感应涡流被削弱,从而充分利用其导磁性能[7]。

3　结论

以螺旋线圈炮为例,对四种不同属性的封装材料和封装尺寸对互感梯度的影响做出了分析和比较,结论如下:

(1)线圈炮互感梯度受到封装材料电导率和磁导率的双重制约。电导率决定了封装中感应涡流的大小;磁导率决定了对磁场的加强程度。

(2)线圈炮互感梯度与封装结构有关。减小封装与线圈的间距,导磁材料的磁场加强效果更好,而导电材料的涡流效应也更明显;增加封装的厚度,导磁材料可以更好地增强磁场,但导电材料由于电阻更小,涡流效应更明显。

(3)为了实现互感梯度的最大化,可以在减小封装与驱动线圈间距并增加封装厚度的情况下使用高磁导率的硅钢片制作封装,硅钢片的厚度应该尽量小,从而削弱涡流效应。

参考文献(References)

[1] Engel T G,et al. Efficiency and scaling of constant inductance cradient DC electromagnetic launchers[J]IEEE Trans. Magn., 2006,42(8): 2043-2051.

[2] 王莹, 肖峰. 电炮原理[M]. 北京: 国防工业出版社, 1995: 94.
WANG Ying, Xiao Feng. Principle of electric gun [M]. Beijing: National Defense Industry Press, 1995: 94. (in Chinese)

[3] 汤蕴璆, 梁艳萍. 电机电磁场的分析与计算[M]. 北京: 机械工业出版社, 2010: 169, 12, 92.
TANG Yunqiu, LIANG Yanping. Analysis and calculation of electromagnetic field in motor [M]. Beijing: Machinery Industry Press, 2010: 169, 12, 92. (in Chinese)

[4] Nunnally C W, et al. Results from a 750 kJ computer controlled sequentially-fired pulse forming network[J]. IEEE Trans. Magn., 2006,42(8): 419-422.

[5] Engel T G, et al. Development of a medium-bore high-efficiency helical coil electromagnetic launcher [J]. IEEE Transactions on Plasma Science, 2004, 42(5): 1893-1895.

[6] 杨栋, 沈志. 螺旋线圈电磁发射器径向受力仿真与电枢设计[J]. 电工电能新技术, 2011,30(3): 47 - 50.
YANG Dong, SHEN Zhi. Simulation of the helical coil electromagnetic launcher's radial force and the design of armature[J]. Advance Technology of Electrical Engineering and Energy, 2011,30(3): 47 - 50. (in Chinese)

[7] 刘守豹,阮江军. 封装对轨道炮电感梯度的影响[J]. 电工电能新技术, 2009,28(4): 42 - 45.
LIU Shoubao, RUAN Jiangjun. Influence of shielding on rail gun induction gradient[J]. Advance Technology of Electrical Engineering and Energy, 2009,28(4): 42 - 45. (in Chinese)

(上接第 123 页)

[6] Yao A. Protocols for secure computation[C]//Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS), IEEE, 1982, 160 - 164.

[7] Goldreich O, Micali S, Wigderson A. Proofs that yield nothing about their validity-or-all languages in NP have zero-knowledge proof systems[J]. Journal of the ACM, 1991, 8(1): 691 - 729.

[8] 肖倩,罗守山,陈萍,等. 半诚实模型下安全多方排序问题的研究[J]. 电子学报,2008, 36(4):709 - 714.
XIAO Qian, LUO Shoushan, CHEN Ping, et al. Research on the problem of secure multi-party ranking under semi-honest model[J]. Chinese Journal of Electronics,2008, 36(4):709 - 714. (in Chinese)

[9] 李顺东,戴一奇,游启民. 姚氏百万富翁问题的高效解决方案[J]. 电子学报,2005,33(5):769 - 773.
LI Shundong, DAI Yiqi, YOU Qimin. An efficient solution to yao's millionaires' problem [J]. Chinese Journal of Electronics, 2005,33(5):769 - 773. (in Chinese)

[10] Boudot F, Schoenmakers B, Traor′e J. A fair and efficient solution to the socialist Millionaires' problem[J]. Discrete Applied Mathematics, 2001, 111(SI):23 - 36.

[11] Bresson E, Catalano D, Pointcheval D. A simple public key cryptosystem with a double trapdoor decryption mechanism and its applications [J]. Aciacrypt 2003, LNCS 2894, Berlin: Springer-Verlag, 2003:37 - 54.

[12] Bresson E, Chevassut P, et al. Provably secure authenticated group Diffie-Hellman key exchange[J]. ACM Transactions on Information and System Security, 2007, 10(3): 421 - 454.