基于签密的多方认证邮件协议

王彩芬, 贾爱库, 刘军龙, 于成尊
(西北师范大学数学与信息科学学院计算机科学系, 甘肃兰州 730070)

摘 要: 签密方案可以在一个逻辑步骤内同时实现签名和加密, 可以有效地减少运算. 本文在已有的两方签密方案的基础上结合组可验证的签密方案, 提出了一种新的、可用于多方认证邮件协议的签密方案, 进而设计出了异步的一对多的认证邮件协议, 并证明了该协议的公平性与非否认性. 文中还通过与已有协议进行比较, 阐述了新协议的优点.

关键词: 公平交换协议; 一对多的认证邮件协议; 签密; 公平性; 非否认性
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2005) 11-2070-04

Multi-party Certified Mail Protocol Based on Signcryption

WANG Cai-fen, JIA Ai-ku, LIU Jun-long, YU Cheng-zun
(*College of Mathematics and Information Science, Northwest Normal University, Lanzhou, Gansu 730070, China*)

Abstract: A new signcryption scheme is developed based on Domain-verifiable signcryption. The scheme simultaneously fulfills both signature and encryption in a single logical step at a lower computational cost. In particular, it can be used by certified mail protocol, and based on the scheme a multi-party certified mail protocol is proposed, its fairness and non-repudiation are proved.

Key words: fair exchange; one-to-more certified mail protocol; signcryption; fairness; non-repudiation

1 引言

认证邮件协议(certified mail)是指一个发送方要将消息 m 与接收方收到该消息后的证据进行交换的协议. 在[ISO1388-197]标准中, 认证邮件协议中至少包括两个参加者: 一个消息发送方, 一个消息接收方. 认证邮件协议作为公平交换协议的一种, 除了满足公平交换协议中的性质外, 还应满足在文献[1]中提出的单调性、第三方的不可见性、保密性、实际的可信任模型、高效性以及时间终止性的性质.

认证邮件协议是非对称的, 即接收方只有接收到某些信息后才发送一个表示已经接收的信息. 这与公平交换有些不同, 公平交换涉及两个项的同时交换. 所以认证邮件协议的设计以及性质与公平交换会略有不同, 但不会发生冲突.

与公平交换协议相同可以将认证邮件按照第三方在协议中的作用分为: 使用在线第三方的协议[2,3], 使用脱线的第三方的协议[4~7]. 按照参与方的个数又分为只有两个参与方和多个参与方的协议. 现有的协议多数都是只有两个参与方的协议, 多个参与方的协议比较少[8~11]. 在已有的多方或双方协议中为了保证公平性多数协议使用了传统密码基础如: 签名、加密或可验证加密. Asokan 在文献[4,5]提出很有效的、乐观的公平交换协议, 当将其应用到认证邮件协议时, 在文献[5]的(异步)方案中当参与双方都是诚实的情况下, 仍然需要 5 个信息的传送, 并且为了保证公平性, 一些消息允许被 TTP 撤销. 文献[4]中的协议由于使用了分割-选择的可验证托管, 效率不高. 在文献[8]中对多方协议进行了分类有环状拓扑结构以及矩阵拓扑结构的协议. 为了满足认证邮件协议的高效性, 我们将在认证邮件协议中使用最近提出的签密方案[12](signcryption).

2 签密方案

签密方案首先由 Zheng 在文献[12]中提出, 它是一种新的密码基础, 可以在一个逻辑步骤内同时实现签名和加密. 签密要比签名然后再加密计算量小、效率高. 在文献[12]中 Zheng 提出了两个签密方案, 在解签密的过程需要使用接收者的私钥 x_b, 这样只有接收者能够验证签名的正确性. 这样的方案使用起来有一定的局限性. 为了解决 Zheng 方案中的问题, Bao 和 Deng[13]提出了修改方案, 在解签密中不需要接收者的私钥, 但该方案计算量比较大, 在文献[14]中 Gamage, Leiwo 和 Zheng 对 Bao 和 Deng 方案又进行了修改, 该方案即保持了运算量小的优点, 同时不需要得到密文以及接收方的私钥, 任何第三方可以验证签名的有效性并确定消息的来源. 然而, 这些方案不能直接在认证邮件协议中使用, 为此我们在文献[14]中的方案的基础上结合 Seo 和 Kim[15]提出的组可验证的签密方案(Domain-verifiable signcryption), 提出新的、可用于多方认证邮件协议中的签密方案.

2.1 Seo 和 Kim 的组签密方案

公共参数 p: 大素数
q: $p-1$ 的大素因子
g: z_n^* 中阶为 q 的元
hash: 单向 hash 函数
KH: 有钥的单向 hash 函数
(E, D) 使用对称钥的加、解密算法

收稿日期: 2004-07-20; 修回日期: 2005-07-29
基金项目: 甘肃省自然科学基金(No. 3ZS051-A25-042); 西北师范大学网络安全重点学科基金

x_a: Alice 的私钥, y_a: Alice 的公钥 $y_a = g^{x_a} \bmod p$

B_i 是签密接收方, 其中 $i \in \{1, 2, \cdots, n\}$ 它的公/私钥对为:

$x_{B_i}, x_{B_i} \in Z_q^*$, B_i 的私钥, B_i 的公钥 y_{B_i}, $y_{B_i} = g^{x_{B_i}} \bmod p$

签密过程

Alice 作如下计算: Alice 随机选择 $x \in Z_q^*$

$k_i = hash(y_{B_i}^x \bmod p)$, $i = 1, 2, \cdots, n$

$k = hash(g^x \bmod p)$, $c_i = E_{k_i}(m_i)$, $i = 1, 2, \cdots, n$,

$r_i = KH_k(m_1, \cdots, c_i, \cdots, m_n)$

$s = x/(r_1 r_2 \cdots r_n + x_a) \bmod q$

Alice 将$(c_1, \cdots, c_n, r_1, \cdots, r_n, s)$ 发送给 B_i.

解签密:

$y = (y_a g^{r_1 \cdots r_n})^s \bmod p$

$k_i = hash(y^{x_{B_i}} \bmod p)$, $k = hash(y)$

$m_i = D_{k_i}(c_i)$,

B_i 接收签名当且仅当$KH_k(m_1, \cdots, c_i, \cdots, m_n) = r_i$.

2.2　改进后的签密方案

签密方案中涉及 Alice 和 n 个参与方 $R_i(i = 1, 2, \cdots, n)$以及完全可信的第三方(TTP), Alice 要将消息 m 发送给接收方 $R_i(i = 1, 2, \cdots, n)$. Alice 产生签密, $R_i(i = 1, 2, \cdots, n)$ 进行验证. 公共参数与文献[15]中的相同.

参与者的公/私钥对:

x_a: Alice 的私钥, y_a: Alice 的公钥 $y_a = g^{x_a} \bmod p$,

$x_{R_i}, x_{R_i} \in Z_q^*$ R_i 的私钥, R_i 的公钥 y_{R_i}, $y_{R_i} = g^{x_{R_i}} \bmod p$

可信第三方的私/公钥对为 x_T / y_T, $y_T = g^{x_T} \bmod p$

将要传递的邮件为 m, $M = \mathrm{hash}(m)$,

签密过程: Alice 作如下计算: Alice 随机选择 $x \in Z_q^*$

$k = hash(y_T^x \bmod p)$,　　$k_i = hash(y_{R_i}^x \bmod p)$

$y = g^x \bmod p$　　$k' = hash(y)$

$c = E_{k'}(m)$,　　$c_i = E_{k_i}(m)$, $i = 1, 2, \cdots, n$

$r = hash(y, c, M)$　　$r_i = KH_{k'}(y, c_i, M)$

$s = x/(r r_1 r_2 \cdots r_n + x_a) \bmod q$

Alice 将$(c, c_i, r, r_1, \cdots, r_n, s, M)$发送给 R_i.

解签密过程: R_i 与 TTP 作如下计算

$y = (y_a g^{r r_1 \cdots r_n})^s \bmod p$

$k_i = hash(y^{x_{R_i}} \bmod p)$, $k = hash(y^{x_T} \bmod p)$

$m = D_{k_i}(c_i)$, $m = D_k(c)$

R_i 接收签名当且仅当$KH_{k'}(y, c_i, M) = r_i$, 然后可以解密得到消息 m 并可以通过$M = \mathrm{hash}(m)$验证 m 与 M 的一致性. 任何其他的第三方可以通过$(c, c_i, r, r_1, \cdots, r_n, s, M)$ 计算 $y = (y_a g^{r r_1 \cdots r_n})^s \bmod p$ 以及检查$KH_{k'}(y, c_i, M) = r_i$ 是否成立来验证签名的正确性以及消息来源于 Alice, 在验证过程中不需要得到明文.

在改进的签密方案中, 若攻击者企图伪造等价于解有限域上离散对数问题; 又因为 M 是经过单向 hash 函数作用于 m 得到的, 所以若企图从 M 得出 m 也是不可行的; 再根据签密中使用的加、解密算法的的安全性可以知道攻击者不可能直接解密得到消息 m.

与已有的签密方案比较, 文献[12]、[14]针对只有一个签密方和一个解签密方的签密方案, 我们改进后的签密方案适应于一组用户; 文献[15]中的方案是针对有 n 个用户的一个组提出的签密方案, 同一组中的成员要想验证, 必须拥有$(c_1, c_2, \cdots, c_n, r_1, r_2, \cdots, r_n, s)$, 而且该方案不能用于认证邮件协议中. 在我们改进后的签密方案中, 不考虑 TTP(因为在协议中只有必要的时候 TTP 才被使用), 若方案中有 n 个参与方, 那么在改进的签密方案中签密时需要 $n + 1$ 个指数运算(模), 解签密时共需要 $3n$ 个指数运算(模). 这与文献[15]中的效率是相同的. 但在我们的方案中 Alice 传递给每个参与方的信息量小, 同时我们的方案中每个接收方还可以利用 M 与解密得到的 m 一起检验 m 的正确性.

在认证邮件协议中使用改进的签密方案时, 首先只将$(c, r, r_1, \cdots, r_n, s, M)$ 发送给 R_i, R_i 可以验证签名的正确性以及消息来源于 Alice, 因为在 c 中使用可信第三方的公钥计算 k, 因此 k 只能由可信第三方计算, 从而使 R_i 不能解密直接得到 m, R_i 只能得到 M, 这与认证邮件协议的性质是相符合的. 为了使 c 与 M 相联系, 使 $r = hash(y, c, M)$. 修改后的方案应用在多方认证邮件协议中可以有效的提高协议的效率, 同时也能保证协议的公平性、非否认性.

3　一对多的认证邮件协议

一对多认证邮件协议是指在协议中一方将邮件发送给多个接收者. 在文献[11]中给出只有三步的一对多认证邮件协议, 但该协议在解决争议时需要联系 TTP, 这是不符合实际的. 我们的协议由三个子协议组成, 交换协议、恢复协议和终止协议.

协议中的假设: 在协议中使用的签密方案以及签名方案是安全的; 在协议中, 假定两个参与者之间的通信信道是不可恢复的即: 在信道中传输的数据有可能被丢失或被改变. 每个参与者与 TTP 之间的通信信道是可达的即: 信道中的数据总会被传送到.

协议中使用的记号:

Alice: E-mail 的发送者, 它的公/私钥对与改进的签密方案中的相同. $R = \{R_1, \cdots, R_n\}$ 邮件接收者集合, 每个 $R_i(i \in \{1, \cdots, n\})$ $R_i \in R$ 的公/私钥对与改进的签密方案中的相同.

R': 表示已经给 Alice 发送收到邮件密文的接收者 R 的子集

m: Alice 将要发送的邮件

$A \rightarrow B$: X 表示 A 给 B 发送消息 X

$A \Rightarrow R$: X 表示 A 对集合 R 广播消息 X

协议中 Alice 的计算过程: Alice 采用上述改进的签密方案计算得到$(c, c_i, r, r_1, \cdots, r_n, s, M)$.

协议描述如下:

如果参与协议的每一方都是诚实的, 则只要执行如下的交换协议即可.

交换协议

$\mathrm{Alice} \Rightarrow R$: $m1 = (c, r, r_1, \cdots r_n, s, M)$

$R_i \rightarrow$ Alice: $sig_{R_i}(m1)$, where $R_i \in R$, $i \in \{1, \cdots, n\}$

Alice⇒R': $c_i = E_{k_i}(m)$, $i \in \{1, \cdots, |R'|\}$

$R_i \rightarrow$ Alice: $sig_{R_i}(m)$, $R_i \in R'$

恢复子协议

如果 R_i 在给 Alice 发送签名后没有收到邮件或者它没有发送签名但是希望得到邮件 m, R_i 可以使用如下的 R_i 恢复子协议, 请求TTP 的帮助; 或者若 R_i 已经收到邮件 m, 但 Alice 没有收到 R_i 发送的证据 $sig_{R_i}(m)$, 则 Alice 执行它的恢复子协议.

R_i 的恢复子协议

$R_i \rightarrow$ TTP: $sig_{R_i}(m1)$, $m1$

IF 已经执行 abort 子协议或恢复子协议 Then 终止

Else recovered= true,

TTP $\rightarrow$ R_i: m

TTP $\rightarrow$ Alice: $s_T = sig_{TTP}(sig_{R_i}(m1))$

TTP 收到请求后首先检查协议的状态, 若协议已经执行了 abort 子协议或者恢复子协议则TTP 终止, 否则 TTP 检查 R_i 的签名, 若正确 TTP 计算 $y = (y_a g^{r_1 \cdots r_n})^s \bmod p$ 得到密钥 k 并对密文 c 解密得到 m, 然后检验 hash$(m) = M$ 是否成立, 若正确, 则分别将 m 和 s_T 给 R_i 和 Alice, s_T 作为 R_i 收到邮件的证据. 否则, TTP 通过验证 $y = (y_a g^{r_1 \cdots r_n})^s \bmod p$、$KH_{k'}(y, c_i, M) = r_i$ 是否成立确认 $m1$ 来源于 Alice 且为 Alice 的签名, 以及 $sig_{R_i}(m1)$的正确性来检查 $R_i \in R'$ 是否成立, 若成立, 则 TTP 执行如下步骤, 表示 Alice 试图欺骗:

TTP $\rightarrow$ R_i: sig_{TTP}(fail)

TTP $\rightarrow$ Alice: sig_{TTP}(fail)

若 $R_i \in R'$ 不成立, 则TTP 什么也不做.

Alice 的恢复子协议

Alice $\rightarrow$ TTP: $m1$, $sig_{R_i}(m1)$

IF 已经执行 abort 或 recover 子协议 Then 终止

Else recovered= true

TTP $\rightarrow$ R_i: m

TTP $\rightarrow$ Alice: $sig_{TTP}(m1)$

在该子协议中 Alice 将 $m1$ 以及 R_i 的签名发送给 TTP, TTP 首先检查协议是否已经执行了 abort 或 recover 子协议, 若已执行, 则终止, 否则, TTP. 检查 Alice 发送的消息是否正确, TTP 计算 $y = (y_a g^{r_1 \cdots r_n})^s \bmod p$ 并检查 $r = hash(y, c, M)$ 若都正确, 则 TTP 计算 k、解密 c 将邮件 m 发送给 R_i, 将其 sig_{TTP}签名发送给 Alice, 以后可以作为 R_i 收到邮件的证据.

Abort 子协议

若 Alice 决定终止协议, 向 TTP 请求, 执行如下的 Abort 子协议

A $\rightarrow$ TTP: $m1$

IF 已经执行 abort 或 recover 子协议 Then 终止

Else aborted= true

TTP $\rightarrow$ Alice: sig_{TTP}(abort)

TTP $\rightarrow$ R_i: sig_{TTP}(abort)

只有 Alice 执行 Abort 子协议, 若 Alice 决定终止协议, 向 TTP 请求, 若TTP 接受请求, 则TTP 分别向 Alice 和 R_i 发送协议终止的标志.

4 协议的执行与公平性分析

如果协议中各方都是诚实的, 则只需要执行交换子协议. 在交换子协议中 Alice 对集合 R 广播消息 $m1$, 收到消息 $m1$ 后 R_i 可以验证消息的来源以及签名, 若都正确则 R_i 发送收到密文的证据, Alice 验证后将 c_i 发送给 R_i, R_i 计算 $y = (y_a g^{r_1 \cdots r_n})^s \bmod p$ 以及 $k_i = hash(y^{x_{R_i}} \bmod p)$, 然后解密得到邮件 m, 并检验 hash$(m) = M$ 是否成立, 若都成立则发送 $sig_{R_i}(m)$. 在协议执行过程中 Alice 可以通过执行 Abort 子协议终止协议的执行; R_i 在发送完$sig_{R_i}(m1)$后或者没有发送该签名但仍然希望执行协议时, 可以执行 R_i 的恢复子协议; 若 Alice 发送 c_i 之后没有收到R_i 的签名, 可以通过执行 Alice 的恢复子协议, 请求TTP 的帮助. 协议不要求参与各方时钟的同步, 每个参与方都可以单方面终止协议而不破坏公平性.

如前所述认证邮件协议应该满足多种性质, 以下证明协议满足最主要和最基本的性质即公平性和非否认性.

结论 1 一对多认证邮件协议满足公平性, 在协议执行的任何时刻, 没有哪个参与方处于有利地位.

证明: 如果所有的参与方都是诚实的, 在成功地执行完交换协议后每个 R_i 收到消息m, Alice 收到 $sig_{R_i}(m)$, $R_i \in R'$.

如果某个参与者试图欺骗, Alice 和 R_i 可以执行恢复子协议. 若是Alice 试图发送错误的消息 m, R_i 通过检查是否 $h(m) = M$ 成立, 若不成立 R_i 可以终止协议或者通过恢复子协议来得到正确的消息 m.

如果 Alice 试图通过公布小于 R' 的集合R'', 使得 $R_i(R' \setminus R'')$ 不能得到消息m 的密文, 在这种情况下 Alice 只有 R_i 收到 $m1$ 的证据, 公平性成立. 如果 R_i 想要得到消息m 可以执行恢复子协议, 在这种情况下公平性仍然成立.

如果 $R_i \in R'$ 试图通过发送错误的 $sig_{R_i}(m)$ 进行欺骗, Alice 可以执行恢复子协议得到 TTP 的签名, 用以代替 R_i 的承诺值. 公平性仍然成立.

综上述知, 结论成立.

5 争议的解决

在认证邮件协议中有可能出现两种情况的争议, 一是发送方的抵赖即接收方声明收到由发送方发送的邮件, 但发送方否认曾发送了邮件; 二是接收方的抵赖即发送方声明曾给接收方发送了邮件, 但接收方否认曾收到由发送方发送的邮件. 为了解决协议结束后出现的争议, 需要一个仲裁者, 当出现争议时发送方和接收后方分别将相关证据出示给仲裁者, 由仲裁者验证证据的正确性, 从而解决出现的问题. 以下分别说明我们协议中争议的解决过程.

如果接收方 R_i 声明收到由 Alice 发送的邮件 m, 但 Alice 否认曾发送了邮件, 那么 R_i 必须给仲裁者提供证据: m, $m1$, c_i 或者 m, $m1$, $s_T = sig_{TTP}(sig_{R_i}(m1))$, 仲裁者计算 y $(y_a g^{r_1 \cdots r_n})^s \bmod p$ 并检查是否$r = hash(y, c, M)$ 和 $KH_{k'}(y, c_i, M) = r_i$ 以及 hash$(m) = M$ 是否成立来确认$m1$, c_i 来源于 Alice 和 M 与 m 的一致性, 或者仲裁者计算 $y = (y_a g^{r_1 \cdots r_n})^s \bmod p$ 并检查是否$r = hash(y, c, M)$ 成立来确认 $m1$ 来源于 Alice

ice 以及 hash(m) = M 是否成立来说明M 与m 的一致性, 和 s_T 是否是TTP 正确的签名说明邮件 m 是由 TTP 发送的. 若都成立, 且 Alice 不能提供 sig_{TTP}(abort), 则仲裁者确认接收方是正确的, 否则, 说明TTP 的行为不当. 如果其中有一项不成立, 则仲裁者拒绝 R_i 的要求, 说明 R_i 试图欺骗.

如果 Alice 声明接收方 R_i 收到了邮件m, 但 R_i 否认, 那么Alice 必须给仲裁者提供证据: m, $m1$, $sig_{R_i}(m1)$, $sig_{R_i}(m)$ 或者 m, $m1$, $sig_{R_i}(m1)$, $sig_{TTP}(m1)$, 仲裁者验证签名 $sig_{R_i}(m1)$, $sig_{R_i}(m)$或者 $sig_{R_i}(m1)$, $sig_{TTP}(m1)$ 的正确性, 若都成立, 且 R_i 没有 sig_{TTP}(abort), 则仲裁者确认发送方是正确的. 如果其中有一项不成立, 则仲裁者拒绝 Alice 的要求, 说明 Alice 试图欺骗.

结论 2　上述过程也说明了我们的协议满足非否认性的要求.

6　结束语

与其他协议比较我们的协议具有如下优点:

• 文献[11]中的协议执行第一步后接收方无法确认密文中消息的正确性, 我们使用改进的签密方案设计的协议可以避免这种缺陷.

• 因在提出的协议中使用改进后的签密方案, 在 R_i 收到 $m1$ 和 c_i 后能同时验证签名的正确性以及密文来源于发送方, 其他文献中的协议都是使用分开的签名和加密, 需要分别验证, 所以我们的协议执行效率高, 虽然效率有所提高但协议的安全性不会降低, 具体说明如下: 在交换子协议中 Alice 对集合 R 广播消息$m1$, 收到消息 $m1$ 后 R_i 可以验证消息的来源以及签名, 由签密方案的安全性 R_i 不可能直接从$m1$ 得到邮件, 若 R_i 验证相关消息都是正确的, 则 R_i 发送收到密文的证据, Alice 验证 R_i 发送的收到密文的证据后, 将 ci 发送给 R_i, R_i 计算 $y = (y_a g^{r_1 \cdots r_n})^s \bmod p$ 以及 $k_i = hash(y^{x_{R_i}} \bmod p)$, 然后解密得到邮件 m, 并检验 hash(m) = M 是否成立, 若都成立则 R_i 发送$sig_{R_i}(m)$表示收到正确邮件的证据.

• 在提出的协议中当某个 R_i 需要向 TTP 求助时, 没有限定一定要 $R_i \in R'$, 即使 $R_i \in R'$ 不成立, 只要 R_i 给 TTP 提供正确的信息, R_i 和 Alice 都能得到各自所需的消息, 所以协议避免了文献[11, 8]中只有固定集合 R' 中的参与方得到邮件 m 的局限.

• 我们的协议中通信信道的假设是较弱的, 协议的执行是异步的.

参考文献:

[1] Giuseppe Ateniese, Breno de Medeiros, Michael T Goodrich. TRICERT: A Distributed Certified E-Mail Scheme[A]. Proc of NDSS'01[C]. San Diego, CA: The Internet Society, 2001. 30- 39.

[2] J Zhou, D Gollmann. Certified Electronic Mail[A]. Proc of Computer Ecurity-Esorics'96[C]. Rome, Italy: Springer verlag, 1996. 55- 61.

[3] R H Deng, L Gong, A A Lazar, W Wang. Practical protocols for certified electronic mail[J]. Journal of network and systems management, 1996, 4(3): 279- 297.

[4] N Asokan, Victor Shoup, Michael Waider. Optimistic fair exchange of digital signatures[J]. IEEE Journal On Selected Areas In Communications, 2000, 18(4): 593- 610.

[5] N Asokan, V Shoup, M Waidner. Asynchronous Protocols For Optimistic Fair Exchange[A]. Proc of 1998 IEEE symposium on security and privacy[C]. Oakland, USA: IEEE computer society press, 1998. 86- 99.

[6] M M Puigserver, J L F Gomila, L H Rotger. Certified Electronic Mail Protocol Resistant To A Minority Of Malicious Third Parties[A]. Proc Of IEEE INFOCOM 2000[C]. Tel Aviv, Israel: IEEE computer society press, 2000. 1401- 1405.

[7] L F Gomila, M Payeras-Capella, L H Rotger. An Efficient Protocol Certified Electronic Mail[A]. Proc of ISW'2000[C]. LNCS1975, Wollongong, NSW, Australia: Springer verlag, 2000. 237- 248.

[8] Matt Franklin, Gene Tsudik. Secure Group Barter: Multi-Party Fair Exchange With Semi-Trusted Neutral Parties[A]. Proc of Financial Cryptography'98[C]. LNCS1465, Anguilla, Springer-verlag, 1998. 90- 102.

[9] Steve Kremer, Olivier Markowitch. A Multi-Party Non-Repudiation Protocol[A]. Proceedings of the 3rd International Conference on Information Security and Cryptology (ICISC 2000)[C]. LNCS 2015, Seoul, Korea: Springer, 2001. 109- 122.

[10] N Asokan, M Schunter, M Waidner. Optimistic Protocols for Multi-Party Fair Exchange[R]. IBM Research Report RZ 2892, Zurich, November 1996.

[11] Josep L. Ferrer-Gomila, M Payeras-Capella, L Huguet-Roteger. A Realistic Protocol for Multi-Party Certified Electonic Mail[A]. Proc of ISC2002[C]. LNCS2433, Heidelberg, Germany: Springer, 2002. 210- 219.

[12] Y Zheng. Digital Signcryption or how to achieve cost(Signature and Encryption) ≪ cost(signature) + cost(encryption)[A]. Proc of Advance Cryptology-CRYPTO'97[C]. LNCS1294, California, USA: Springer-Verlag, 1997. 169- 179.

[13] F Bao, R H Deng. A signcryption scheme with signature directly verifiable by public key[A]. Proc of PKC'98[C]. LNCS, vol. 1431, Yokorhama, Japan: Springer verlag, 1998. 55- 59.

[14] C Gamage, J Leiwo, Y Zheng. Encrpted Message Authentication By Firewalls[A]. Proc of PKC'99[C]. LNCS 1560, Kamakura, Japan: Springer verlag, 1999. 69- 81.

[15] Moonseog, Kwangjo Kim. Electronic funds transfer protocol using domain verifiable signcryption scheme[A]. Proc of Information Security And Cryptology (ICISC'99)[C]. Seoul, Korea: Springer Verlag, 2000. 269- 277.

作者简介:

王彩芬　女, 1963 年生于河北省安国市, 1983 年获兰州大学数学力学系理学学士学位, 1998 年获兰州大学计算机科学系理学硕士学位, 2003 年获西安电子科技大学密码学专业工学博士学位, 现为西北师范大学数学与信息科学学院计算机科学系教授. 目前主要研究方向为信息安全、协议的设计及协议的形式化分析等, 在《计算机学报》《电子学报》《通信学报》等国内外刊物发表论文三十余篇. E-mail: wangcf@nwnu.edu.cn.