有半信任方(STNP)的多方交换协议

郑 东[1],张方国[2],陈克非[1],尤晋元[1]
(1. 上海交通大学计算机科学系,上海 200030;2. 西安电子科技大学 ISDN 重点实验室,西安 710071)

摘 要: Frankin 和 Tsudik 在 FC'98 中给出了两个多方交换协议,此协议是关于多方交换的公平交换协议,本文发现了对其中第一个协议(SUCEX-1)的攻击,指出该协议是一个不公平交换协议,并给出了此协议的一种改进形式.

关键词: 电子商务; 公平交换; 协议; 攻击
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2001) 01-0118-02

Multi-Item Fair Exchange with Semi-Trusted Neutral Party

ZHENG Dong[1], ZHANG Fang-guo[2], CHEN Ke-fei[1], YOU Jin-yuan[1]
(1. *Dept. of Computer Science and Engineering, Shanghai Jiaotong Univ., Shanghai* 200030, *China*;
2. *Key Lab. On ISDN, Xidian Univ., Xi'an* 710071, *China*)

Abstract: In FC'98, Frankin and Tsudik Proposed two protocols for n-party multi-unit fair exchange. In this paper, an attack on its protocol SUCCX-1 is presented, and in the meanwhile, an improved protocol is given.

Key words: electronic commerce; fair exchange; protocol; attack

1 引言

近年来,电子商务中的公平交换问题已受到人们的广泛关注,这是由于电子商务中的很多业务是物品交换.即使是购买商品,实际上也是一种交换,是支票(或钱币)与所买物品的交换.公平交换协议应当不损坏遵守协议运行规则的主体的利益,关于两个主体的公平交换已有很多结果,但对于多个主体之间公平交换的研究却很少. Frankin 和 Tsudik 在 FC'98 中给出了两个多方交换的协议,此协议是关于多方/单项交换的协议(分别称作 SUCEX-1, SUCEX-2),本文指出了协议 1 (SUCEX-1)是一个不公平的协议,并给出了一种攻击方法及改进的协议.

2 多方公平交换

设$\{K_1, \cdots, K_d\}$是多个主体要相互交换的具有给定单位的物品.

定义 1[2] 单位-循环交换(图 1): n 个主体的单位循环交换是一个长为 n 的交换圈,对每个 $i \le n$,对应的主体 P_i 提供一个单位的 K_i 给 P_{i+1},同时接收 P_{i-1}向他提供的一个单位的 K_{i-1}.

多项交换要求的基本性质

(1)如果所有主体是诚实的,则每个主体 P_i 能够得到所有预先期望的 K_{i-1}; (2)如果所有 P_i 是诚实的,则 Z(半-信任的中性参与方)不能得到任何秘密 K_j, $(j = 1, 2, \cdots, n)$; (3)设 $P = P_1, \cdots, P_n$, $\forall S = P - P_k (0 < k \le n)$.

如果所有属于 S 的主体和 Z 都是诚实的,则 (a) P_k 能够得到一个秘密 K_{k-1},当有仅当 $\forall P_i \in S$, P_i 能够得到 K_{i-1},即诚实的主体能够得到应交换的"物品". (b)任何不诚实的 P_k 都得不到属于其它主体的秘密 $K_j, j \ne k$.

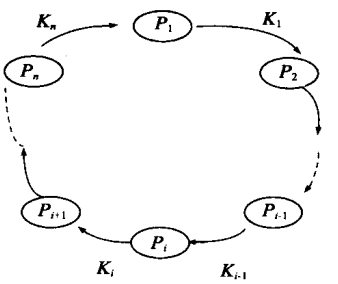

图 1 多方/单位交换

在下文中,需要满足性质 $F_n(X_1, f(X_2), \cdots, f(X_n)) = f(X_1, \Lambda, X_n)$ 的函数对 (F_n, f). 例如,可以取:

$$F_n = (X_1^2)\, X_2 \cdots X_n, f = X^2 \bmod N$$

其中, N 是两个不同大素数的乘积.

3 对协议 SUCEX-1 的攻击及其改进

在文献[2]中,作者给出了两个单项循环交换的协议(SUCEX-1, SUCEX-2),但 SUCEX-1 是有漏洞的,在此协议中,任何一个不诚实的主体 P_k 可以欺骗诚实的主体 P_{k+1}. 为叙述方便,先介绍文[2]中的单位循环交换协议 SUCEX-1:

协议的初始假设:每个主体 P_i 拥有秘密 K_i 且知道所有的 $f(K_j)$, $(0 < j \le n)$.

协议步骤如下: (1)首先假设每个主体 P_i 秘密生成一个随机数 $R_i \in_R Z_q$,并计算 R_i^{-1},然后, P_i 向 P_{i+1}秘密发送 R_i. (2)每个 P_i 计算下列两项:

收稿日期:1999-09-06;修回日期:2000-02-26
基金项目:国家自然科学基金(No. 69773013, 69973031)

$A_i = F_n(K_i, f(K_1), \cdots, f(K_{i-1}), f(K_{i+1}), \cdots, f(K_n))$

$C_i = K_i \cdot R_i^{-1}$ 并向 Z 发送 $< A_i, C_i, f(R_i) >$ (3) Z 计算 $C = C_1 \cdots C_n$,

$$F_{n+1}(C, f(R_1), \cdots, f(R_n)) = f(K_1 R_1^{-1} \cdots K_n R_n^{-1}, R_1 \cdots R_n) = f(K_1 \cdots K_n)$$

并判断下式:

$$A_i = A_j \quad ? \ (\text{for all } 0 < i, j \le n)$$

$$F_{n+1}(C, f(R_1), \cdots, f(R_n)) = A_i \ ?$$

若对所有的 $1 \le i, j \le n$,上述等式成立,则进行步骤 4,否则,输出 ERROR,并终止运行协议或要求重新运行协议. (4) Z 向所有 P_i 广播 $C = \{C_j \mid 0 < j \le n\}$, P_i 能够计算出 $K_{i-1} = R_{i-1} \cdot C_{i-1} = R_{i-1} \cdot K_{i-1} \cdot R_{i-1}^{-1}$.

上述协议并不是公平的协议,它允许任何一个不诚实的主体 P_k 欺骗诚实的主体 P_{k+1}. 看下面的攻击:

假设某主体 P_k 是不诚实的,他想欺骗 P_{k+1},做法如下:

(1) P_k 和其它主体一样,秘密生成一个随机数 $R_k \in_R Z_q$ 并计算 R_k^{-1},向 P_{k+1} 秘密发送 R_k. (2) 除 P_k 外,其它每个 P_i 正确计算下列两项:

$A_i = F_n(K_i, f(K_1), \cdots, f(K_{i-1}), f(K_{i+1}), \cdots, f(K_n))$

$C_i = K_i \cdot R_i^{-1}$

并向 Z 发送 $< A_i, C_i, f(R_i) >$. P_k 正确计算 A_k,但并不如实计算 $C_k, f(R_k)$,而是取一随机数 $N \in_R Z_q$ 及 N 的逆元 N^{-1},并计算: $C'_k = K_k N^{-1} R_k^{-1}$,然后向 Z 发送 $< A_k, C'_k, f(NR_k) >$.

在此情况下,仍然有

$A_i = A_j, 0 < i, j \le n$

$F_{n+1}(C', f(R_1), \cdots f(NR_k), \cdots, f(R_n)) = A_i$

$(C' = C_1 \Lambda C_{k-1} C'_k C_{k+1} \Lambda C_n)$

即 Z 误认为所有的主体都正确运行了协议,并向所有的主体广播 $c = \{C_1, \Lambda, C_{k-1}, C'_k, C_{k+1}, \Lambda, C_n\}$,除 P_{k+1} 外,其余每个主体 P_i 都可以得到 $K_{i-1} = R_{i-1} \cdot C_{i-1} = R_{i-1} \cdot K_{i-1} \cdot R_{i-1}^{-1}$,但 P_{k+1} 得不到 K_{k+1},这是由于在集合 $c = \{C_1, \Lambda, C_{k-1}, C'_k, C_{k+1}, \Lambda, C_n\}$ 中, P_{k+1} 找不到 $C_k (0 < i \le n)$ 满足 $f(C_i \cdot R_j) = f(K_{i-1})$.

改进的协议如下:

(1) P_j 和其它主体一样,秘密生成一个随机数 $R_j \in_R Z_q$ 并计算 R_j^{-1},向 P_{j+1} 秘密发送 R_j; (2) 每个 P_i 计算下列两项:

$A_i = F_n(K_i, f(K_1), \cdots, f(K_{i-1}), f(K_{i+1}), \cdots, f(K_n))$

$C_i = K_i \cdot R_i^{-1}$, $E_i = f(R_i)$, $D_i = f(R_i R_{i-1})$

并向 Z 发送 $< A_i, C_i, E_i, D_i >$ (3) Z 计算下列式子: $C = C_1 \cdots C_n$,

$$F_{n+1}(C, f(R_1), \cdots, f(R_n)) = f(K_1 R_1^{-1} \cdots K_n R_n^{-1} R_1 \cdots R_n) = f(K_1 \cdots K_n)$$

并判断下式: $A_i = A_j \ ? \ E_i E_{i-1} = D_i \ ?$

$$F_{n+1}(C, f(R_1), \cdots, f(R_n)) = A_i \ ?$$

若对所有的 $1 \le i, j \le n$,上述等式成立,则进行步骤 4,否则,输出 ERROR,并终止运行协议或要求重新运行协议. (4) Z 向所有 P_i 广播 $C = \{C_j \mid 0 < j \le n\}$, P_i 可以计算出 $K_{j,i} = C_{j,i} \cdot R_{j,i}, j \in \overline{S_i}$;

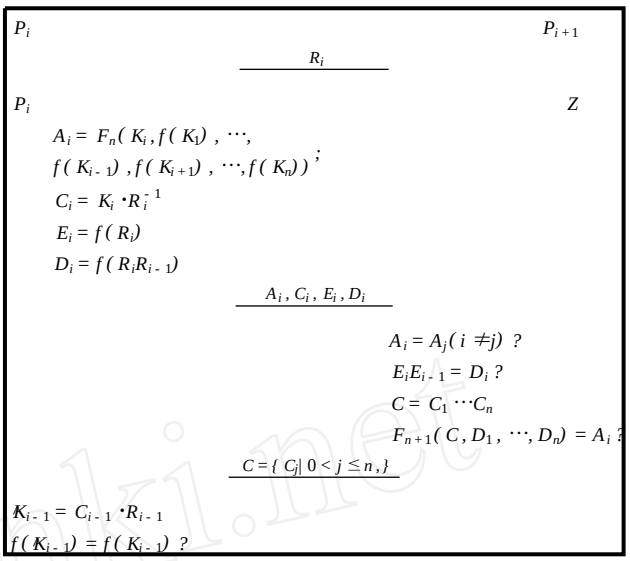

图 2　改进的多项交换协议

协议的安全性分析

(1) 若所有的主体是诚实的,则每个 P_i 通过计算 $K_{i-1} = R_{i-1} \cdot C_{i-1}$ 得到 K_{i-1}, (2) 假设只有一个主体 P_k 是不诚实的,则若他想得到 K_{k-1},必须如实发送 $< A_k, C_k, E_k, D_k) >$,这是由于 P_j 需要在协议的最后一轮得到 Z 的广播 $C = \{C_j \mid 0 < j \le n\}$,而 Z 只有在下列式子: $(0 < i \le n)$ $A_i = A_j \ ? \ E_i E_{i-1} = D_i \ ?$

$$F_{n+1}(C, f(R_1), \cdots, f(R_n)) = A_i \ ?$$

成立的条件下,才进行广播 $C = \{C_j \mid 0 < j \le n\}$.

等式 $E_{k+1} E_k = D_{k+1}$ 要求 P_k 正确发送 $E_k = f(R_k)$,等式 $F_{n+1}(C, f(R_1), \cdots f(R_n)) = A_j$ 要求 P_k 正确发送 $C_k = K_k \cdot R_k^{-1}$. 这就防止了原协议的漏洞. (3) P_j 只有 R_{j-1} 可以用于计算 K_{j-1},而得不到其它的 K_i.

4　结论

本文发现了文[2]中的公平交换协议 SUCEX-1 的漏洞,即找出了对此协议的成功攻击,并给出了改进的公平协议. 但此改进的协议仍然要求半-可信方 (STNP) Z 知道交换的拓扑结构,我们不知是否存在这样的公平协议,其交换的拓扑结构对 STNP 是保密的.

参考文献:

[1] N. Asokan, V. Schoup, and M. Waidner. Optimistic fair exchange of digital signatures. Research Report RZ 2892 (# 90840). IBM Research, December 1997M. Franklin, G. Tsudik. Secure group barter: Multi-party fair exchange with semi-trusted neutral parties [A]. Financial cryptography (FC '98): Proceedings [C], R. Hirschfeld (ed.), Springer-verlag, February 1998, LNCS 1465: 90 - 102.

[2] M. Franklin and M. Reiter. Fair exchange with a semi-trusted third party [A]. In ACM Conference on Computer and Communication Security [C], April 1997.

作者简介:

郑　东　1964 年出生,1999 年获西安电子科技大学密码学博士学位,现在上海交通大学计算机系从事博士后研究工作,研究方向是密码学与信息安全.