中山大学学报（自然科学版）
第29卷 第2期 ACTA SCIENTIARUM NATURALIUM Vol.29 №.2
1990年 UNIVERSITATIS SUNYATSENI 1990

强安全密码协议

姚卿达 李连弟 陈卫民
（计算机软件研究所） （计算机科学系）

摘 要

本文研究了著名的Dolev和Yao的级联协议和印章协议的强安全性，提出了强安全密码协议概念，并取得了一些新的结论.

关键词 协议，级联，印章，强安全，密码

1976年 Diffie和Hellman〔Diff76〕提出公开钥密码思想以来，关于公开钥密码系统的研究已有许多工作.然而，一个好的公开钥密码系统并不能保证有一个好的密码协议.因此，研究公开钥密码系统的同时，有必要开展对密码协议安全性的探讨.

1981年在22届IEEE计算机科学基础年会上，Dolev和Yao首次提出级联协议和印章协议两个模型，并研究了这两类协议(针对主动破坏者，包括心急破坏者)的安全性.本文在前人工作的基础上，提出了强安全密码协议概念，取得了一些结论.

1 级联协议和印章协议

1.1 级联协议(cascade protocol)

定义 1 双方级联协议P被一系列有穷串描述

$$\tilde{\rho}_i \in \{Z_1, Z_2, Z_3\}^*,\ 1 \leqslant i \leqslant t; \qquad \tilde{\sigma}_j \in \{Z_1, Z_2, Z_4\}^*,\ 1 \leqslant j \leqslant t$$

这里$t' = t$或$t-1$．对每一对不同的用户X和Y，令$\rho_i(X,Y)$,$\sigma_j(X,Y)$分别表示符号Z_1，Z_2，Z_3，Z_4为EX，EY，DX，DY代替的串$\tilde{\rho}_i$，$\tilde{\sigma}_j$.

定义 2 令P是由$\{\tilde{\rho}_i, \tilde{\sigma}_j \mid 1 \leqslant i \leqslant t, 1 \leqslant j \leqslant t'\}$描述．定义

$$N_1(X,Y) = \rho_1(X,Y); \qquad N_{2j}(X,Y) = \sigma_j(X,Y) N_{2j-1}(X,Y),\ 1 \leqslant j \leqslant t';$$
$$N_{2i+1}(X,Y) = \rho_{i+1}(X,Y) N_{2i}(X,Y),\ 1 \leqslant i < t.$$

当X希望发送明文M给Y的时候，互相交换的消息就是$N_i(X,Y)$,这里$i = 1,2,\cdots,t+t'$.

定义 3 令P是由$\{\tilde{\rho}_i, \tilde{\sigma}_j\}$说明的级联协议．定义

$$\Sigma_1(Z) = E \cup \{DZ\}; \qquad \Sigma_2 = \{\rho_i(A,B) \mid \text{对所有} A \neq B \text{和} i \geqslant 2\};$$
$$\Sigma_3 = \{\sigma_i(A,B) \mid \text{对所有} A \neq B \text{和} i \geqslant 1\}$$

我们说P是不安全的，如果存在某个$\tau \in \{\Sigma_1(Z) \cup \Sigma_2 \cup \Sigma\}_3^*$使得

本文1988年9月5日收到

$$\overline{\tau N_i(X,Y)}=\lambda$$

对某个$N_i(X,Y)$成立；否则，P是安全的．特别地，我们说P是抵抗心急破坏者不安全的，如果存在某个$\tau\in\{\Sigma_1(Z)\cup\Sigma_3\}^*$ 使得

$$\overline{\tau N_i(X,Y)}=\lambda$$

对某个$N_i(X,Y)$成立；否则，P是抵抗心急破坏者安全的．

定义4　令$\pi\in\{E,D\}^*$是一个串，A是用户名．说π对于A具有平衡性质如果

$$DA\in lt(\pi)\text{ 蕴涵 }EA\in lt(\pi)$$

定义5　令X，Y是2个不同的用户名，双方级联协议$P=\{\tilde{\rho}_i,\tilde{\sigma}_j\}$是平衡级联协议如果

1)对每个$i\geq 2$，$\rho_i(X,Y)$对于X具有平衡性质；2)对每个$j\geq 1$，$\sigma_j(X,Y)$对于Y具有平衡性质．

这里，$\rho_i(X,Y)$，$\sigma_j(X,Y)$是归约形．

定理1[1]（级联协议特征定理）双方级联协议$P=\{\tilde{\rho}_i,\tilde{\sigma}_j\}$是安全的，当且仅当

1) $lt[\rho_1(X,Y)]\cap\{EX,EY\}\neq\phi$；　　2) P是平衡的．

定理2[1] 令X,Y是2个不同的用户名．双方级联协议$P=\{\tilde{\rho}_i,\tilde{\sigma}_j\}$是抵抗心急破坏者安全的，当且仅当对每个$K\geq 1$

1) $lt[N_k(X,Y)]\cap\{EX,EY\}\neq\phi$；　　2) $\sigma_k(X,Y)$对于Y具有平衡性质．

1.2 印章协议(name-stamp protocol)

定义6　双方印章协议P由一系列串描述

$$\tilde{\rho}_i\in(F-\{Z_2\})^*,\quad \sigma_j\in(F-\{Z_1\})^*$$

这里$F=\{Z_1,Z_2,\cdots,Z_s\}$，$1\leq i\leq t$，和$1\leq j\leq t'(t'=t$或$t-1)$．令$\rho_i(X,Y)$和$\sigma_j(X,Y)$表示$Z_1,Z_2,\cdots Z_s$各自被$DX,DY,EX,EY,iX,iY,dX,dY,d$代替后的串$i$和$j$．令$N_1(X,Y)=\rho_1(X,Y),N_2(X,Y)=\sigma_1(X,Y)N_1(X,Y),N_3=\rho_2(X,Y)N_2(X,Y),\cdots,N_{2i}(X,Y)=\sigma_i(X,Y)N_{2i-1}(X,Y),N_{2i+1}(X,Y)=\rho_{i+1}(X,Y)N_{2i}(X,Y),\cdots$．要求$N_i(X,Y)$不含任何$d_A$．

$\{N_i(X,Y)M\}$是X和Y之间传递的报文序列．

定义7　令X，Y，Z是3个不同的用户．双方印章协议P是不安全的，如果存在串$\tau\in\Sigma Z^*$，$P\{N_i(X,Y)\}$使得$\bar{\tau}=\lambda$，集合ΣZ，P定义为

$$\Sigma Z,\ P=\{\rho_i(A,B)\mid\text{所有}A\neq B,\ \text{所有}i\leq 2\}\cup\{\sigma_j(A,B)\mid\text{所有}A\neq B,\ \text{所有}j\}\cup\{E_A,i_A,d_A,d\mid\text{所有}A\}\cup\{DZ\}.$$

否则，P是安全的．

定理3[2] 协议P是不安全的，当且仅当存在串$\tau\in\Sigma'Z,P\{\rho_1(X,Y)\}$使得$\bar{\tau}=\lambda$，这里

$$\Sigma'Z,P=\{\rho_i(A,B)\mid A,B\in\{X,Y,Z\},A\neq B,i\geq 2\}$$
$$\cup\{\sigma_j(A,B)\mid A,B\in\{X,Y,Z\},A\neq B\}$$
$$\cup\{E_A,i_A,d_A,d\mid A=X,Y,Z\}\cup\{D_2\}.$$

定理4[3] 设有$K\geq 1$使得印章协议的安全K-特征存在．

〔3〕的结论表明不存在印章协议特征定理，但〔2〕给出了一个$O(n^2)$的印章协议全性判别算法。

算法过程是：第一步，构造一架非确定有穷状态自动机A：

①状态0是（唯一）初始状态和状态1是（唯一）接受状态，（输入）字母表是$\Sigma=\Sigma Z\cup\Sigma X\cup\Sigma Y$；

②从状态0到状态1建一有向路径，其标号对应于$\rho_1(X,Y)$；

③对每个输入字母（算子）$\sigma\in\Sigma Z$，建一从0到0的自回标号为σ；

④对每个$\rho_i(A,B)$，$1\leqslant i\leqslant t$和$\{A,B\}\subseteq\{X,Y,Z\}$，建一从0到0的回路，使其各边依次被$\rho_i$的字母标记；

⑤对每个$\sigma_j(A,B)$，$1\leqslant i\leqslant t'$和$\{A,B\}\subseteq\{X,Y,Z\}$，建一从0到0的回路，使其各边依次被$\sigma_j$的字母标记。

第二步，简化自动机A，并令简化自动机A的状态集合$S=\{0,1,\cdots S\}$。

第三步，用下述算法计算A的瓦解关系C：

①$C\leftarrow\{(i,i)\mid 0\leqslant i\leqslant s\}$，$Q\leftarrow C$；〔注释：$C$的各个新对进入状态对队列$Q$一次〕

While $Q\neq\phi$ do

②从Q中删除第一对(i,j)；

③如果$(j,k)\in C$和$(i,k)\notin C$ 那么把(j,k)放进C和Q；

④如果$(k,i)\in C$和$(k,j)\notin C$ 那么把(k,j)放进C和Q；

⑤如果$k\xrightarrow{\alpha}i$和$j\xrightarrow{\tau}l$和 $\overline{\sigma\tau}=\lambda$和$(k,l)\notin C$那么把$(k,l)$放进$C$和$Q$ od；

第四步，如果$(0,1)\in C$，则协议P是不安全的；否则，P是安全的。

2 强安全密码协议

我们知道，安全的级联协议和安全的印章协议是使破坏者无法从中获取明文M的。但一个破坏者可以通过截获发送者发出的消息，使其不能到达接收者手中，并注入假的或其它有害信息M'来扰乱通信的双方，以达到破坏目的。且糟糕的是收一发双方往往都不知道协议中传递的消息已被窜改，因而发生误会，造成严重后果。

假情报注入问题在公开钥密码系统中尤为突出，因为加密算法是公开的，任何人都可以向任何一方发送用接收方加密算法加密的清息M'。

举一个简单的例子。假设一家W公司老板A同他的股票经纪人B之间用公开钥密码系统通信。通信协议是：①$(X,EY(M),Y)$,②$(Y,EX(\text{“}OK\text{”}),X)$。意思是，发送方给接收方发送用接收方加密算法加密的消息M，接收方回送用发送方加密算法加密的“OK”表示已收到消息。显然，任何第三方都无法从这个协议的执行过程中获取明文M，但该协议没有抵抗假情报渗透的能力，比方说一家想吞并W公司的U公司就可以用假情报的方法达到其目的。U公司只要截获A向B发送的一条消息$(A,EB(M),B)$，使其不能到达B，然后自己冒充A向B发送$(A,EB(\text{“抛出本公司股票的51\%”},B)$（由于$EB$公开，所以$U$是有能力发送这条消息的），$B$接收到消息后，按照协议向$A$回送$(B,EA(\text{“}OK\text{”}),A)$。$A$收到回话后得知$B$确有消息收到，但是并不知道原来的消息已被截获而替换成

了有害内容。为了防止这种破坏行为的发生，保证通信的安全畅通进行，我们引入了强安全密码协议概念。

定义 8　一个双方级联协议（或印章协议）$P=\{\widetilde{\rho}_i, \widetilde{\sigma j}\mid 1\leqslant i\leqslant t, 1\leqslant j\leqslant t'\}$是强安全的，如果$P$是安全的并且对任何2个不同的用户$X$和$Y$，存在$i,j,1\leqslant j\leqslant i\leqslant t$使得对某个$\sigma_1\in E\cup\{DX\}$（或$\sigma_1\in E\cup\{DX\}\cup\{d\}$），$\sigma_2\in E\cup\{DX\}$（或$\sigma_2\in E\cup\{DY\}\cup\{d\}$），有

$$\sigma_1 N_{2i}(X,Y) = \overline{\sigma_2 N_{2j-1}(X,Y)} = \lambda$$

强安全密码协议定义的背景涵义是，为了防止假情报渗透，要求收方在接到消息M以后给发方回送一张收条，表示消息M已收到，而且这张收条应该是与M内容密切相关的，因为只有这样发方才知道收方收到的确实是M而不是任何其它的M'。

对强安全密码协议的研究得到下述结论。

结论 1　不存在强安全的双方级联协议。

结论表明：如果级联协议是安全的，那么它抵抗假情报渗透是无能为力的。也就是说，对于级联协议破坏者或者可以发现明文，或者可以用假的或有害的情报扰乱通信的一方或双方而不会被任一方发觉。

结论 2　不存在抵抗心急破坏者的强安全双方级联协议。

结论表明：都是从抵抵心急破坏者安全的协会中也找不出能有效抵抗假情报渗透级联协议。

结论 3　存在强安全双方印章协议.或更准确地说，协议：1) $(A, EB(MA)', B)$；2) $(B, EA(M), A)$是强安全的。

结论表明：用上述协议的1)、2)进行通信，既能防止报文内容被敌方译获，又能及时发觉后来策划的任何假情报渗透的阴谋。

以下证明结论

2.1　准备工作

引理 1　任给2个对于A具有平衡性质的归约形$\overline{\pi_1}, \overline{\pi_2}$，则$\overline{\pi_1\pi_2}$对于$A$也具有平衡性质。

证明　设$D_A\in lt(\pi_1)$且$D_A\in lt(\pi_2)$，因π_1，π_2皆对于A具有平衡性质，所以$E_A\in lt(\pi_1)$且$EA\in lt(\pi_2)$。故可令

$$\pi_1=\phi_1 E_A\phi_2,\ \pi_2=\mu_1 E_A\mu_2,\quad \phi_1,\phi_2,\mu_1,\ \mu_2\in\Sigma^*$$

有

$$\overline{\pi_1\pi_2}=\overline{\phi_1 E_A\phi_2\mu_1 E_A\mu_2}$$

要$E_A\notin lt\ (\overline{\pi_1\pi_2})$，除非$\phi_2\mu_1$形如$D_A W D_A$。即$\phi_2$形如$D_A$且$\mu_1$形如$W_2 D_A$。这与$\pi_1$，$\pi_2$为归约形的假设相矛盾。故$\overline{\pi_1\pi_2}$对于$A$具平衡性质。

引理 2　令Z是用户名和P是平衡级联协议，则对于$(\Sigma_1(Z)\cup\Sigma_2\cup\Sigma_3)^*$中的每个串$\phi$，$\overline{\phi}$对于每个$A\neq Z$具有平衡性质。

证明　显然对于A具有平衡性质。由于P是平衡级联协议，所以，对(A,B)　$i\geqslant 2$，$A\neq B$对于A具有平衡性质，又$\sigma_i(A,B)\in\{EA,EB,DB\}$出现$DA$，所以$\sigma_i(A,B)$对于$A$具有平衡性质。综上，任何$\pi\in\Sigma_1(Z)\cup\Sigma_2(Z)$对于$A\neq Z$具有平衡性质。再结合引理1，即可证得引理2。

定义 9 令ϕ是一串。ϕ的一个子串π称作是A-子串，对某个X，$Y\neq A$，下述之一为真：1）$\phi=\phi_1DX\pi DY\phi_2$；2）$\phi=\phi_1DX\pi$；3）$\phi=\pi DY\phi_2$。

定义10 串ϕ是强A-平衡的如果每个A-子串π对于A具有平衡性质。

引理 3 令ϕ是强A-平衡串，1）如果$\phi=\phi_1DB\phi_2$且$B\neq A$，则ϕ_1和ϕ_2都是强A-平衡的；2）如果$\phi=\phi_1\phi_2$和$EA\notin lt(\phi_2)$，则ϕ_1是强A-平衡的。

引理 4 令τ，v是任何归约形强A-平衡。如果$(lt(\tau)\cup lt(v))\cap\{E_A, D_A\}\neq\phi$，则$\overline{\tau v}\neq\lambda$。

引理3、4证明见文献〔1〕。

引理 5 如果串ϕ_1和ϕ_2是强A-平衡的归约串，则串$\phi_1\phi_2$也是强A-平衡的。

证明 易知，π是串$\phi_1\phi_2$的一个A-子串仅当π形如下面三式之一：①$\pi_1$②$\pi_2$③$\pi_1\pi_2$，这里π_1为ϕ_1的某A-子串，π_2为ϕ_2的某A-具有平衡性质。显然，π_1，π_2对于A具有平衡性质。由引理1可推出$\pi_1\pi_2$对于A也具有平衡性质。故任给串$\phi_1\phi_2$的一个A-子串π，π对于A具有平衡性质。

引理 6 令$MY=\{\sigma_i(X,Y)|$对所有的i和所有的用户$X\}$。如果MY的每个元素对于Y都具有平衡性质，则对每个串

$$\phi\epsilon(MY\cup E\cup\{DX|X\neq Y\})^* \qquad (1)$$

ϕ是强Y-平衡的。

证明 显然，任给$\sigma\epsilon MY\cup E\cup\{DX|X\neq Y\}$，$\sigma$是强$Y$-平衡的，结合引理5，知对每个串式(1)成立，$\phi$是强$Y$-平衡的。

引理 7 如果τ，ϕ是任何两个归约形强Y-平衡串，并且$EY\epsilon lt(\phi)$，则

$$lt(\overline{\tau v})\cap\{EY,DY\}\neq\phi.$$

证明 通过对$n(n=\max\{|\tau|,|v|\})$归纳证明。

当$n=0$时，引理平凡成立。

当$n=1$时，$v=EY$，要使引理推翻必须$\tau=DY$，但这与τ是强Y-平衡串矛盾，所以此时引理仍然成立。

假设当$n<k$时，引理成立，即$lt(\overline{\tau v})\cap\{EY,DY\}\neq\phi$，这里$\max\{|\tau|,|v|\}<k$。现证当$n=k$时，$lt(\overline{\tau v})\cap\{EY,DY\}\neq\phi$。反证法，假定$lt(\tau v)\cap\{EX,DY\}=\phi$。由于$EY\epsilon lt(v)$，所以$DY\epsilon lt(\tau)$。又因为$\tau$为强$Y$-平衡串，故$EY\epsilon lt(\tau)$，从而又有$DY\epsilon lt(v)$。因此$\{EY,DY\}\subseteq lt(\tau)$和$\{EY,DY\}\subseteq lt(v)$。不妨假定$\tau=\tau_2DY^+\tau_1$，这里$lt(\tau_1)\cap\{EY,DY\}=\phi$，$EY\epsilon lt(\tau_2)$（$\tau=\tau_2EY^+\tau_1$情形类似讨论）。在这种情形$v=v_1EYv_2$，这里$v_1=\tau_1$。由于串$\tau$是强$Y$-平衡的，所以$\tau_2$应形如$\tau_3EX$，对某个$X\neq Y$，并且$EY\epsilon lt(\tau_3)$，（否则$\tau=\tau_3DXDY^+\tau_1$，这里$X\neq Y$，$EY$ $lt(\tau_1)$，这与$DY^+\tau_1$对于Y具有平衡性质矛盾）。于是，$\overline{\tau v}=\overline{\tau_3EXv_2}$。由于$\tau_3$含$EY$，所以必须$v_2=DXv_3$。$v_3$中含$DY$。故$\overline{\tau v}=\overline{\tau_3v_3}$。由于$\tau=\tau_3EXDY^+\tau_1$和$v=v_1EY^+DXv_3$都是强$Y$-平衡串，据引理3，$\tau_3$和$v_3$也是强$Y$-平衡串。因为$v_3$含$DY$，因此$v_3$也含$EY$。据归纳假定，$lt(\overline{\tau_3v_3})\cap\{EY,DY\}\neq\phi$，即$lt(\overline{\tau v})\cap\{EY,DY\}\neq\phi$，与假定矛盾。

2.2　结论的证明

结论1的证明　假设存在强安全的双方级联协议$P=\{\tilde{\rho}_i, \tilde{\sigma}_j | 1\leqslant i\leqslant t, 1\leqslant j\leqslant t'\}$则存在$i,j,1\leqslant j\leqslant i\leqslant t$，使得对某个$\sigma_1\epsilon E\cup\{DX\}$，$\sigma_2\epsilon E\cup\{DY\}$，有

$$\overline{\sigma_1 N_{2i}(X,Y)}=\overline{\sigma_2 N_{2j-1}(X,Y)}=\lambda$$

从而

$$lt(\overline{N_{2i}(X,Y)})\subseteq\{EX,DX,DY\} \quad (2)$$

$$lt(\overline{N_{2j-1}(X,Y)})\subseteq\{EY,DX,DY\} \quad (3)$$

记$N_{2i}(X,Y)=P_{2i}\rho_1(X,Y)$和$\overline{N_{2j-1}(X,Y)}=\overline{P_{2j-1}(X,Y)\rho_1(X,Y)}$，这里$P_{2i}$，$P_{2i-1}\epsilon(\Sigma_2\cup\Sigma_3)^*$假设$P$是安全的，将导致矛盾。

据特征定理（定理1），P必须是平衡的。

情形1　$EY\epsilon lt(\rho_1(X,Y))$：显然（2）要求$\overline{P_{2i}}$应当含有$DY$但不含$EY$，这与引理2矛盾。

情形2　$EX\epsilon lt(\rho_1(X,Y))$和$EY\epsilon lt(\rho_1(X,Y))$：在这种情形，(3)要求含有$DY$但不含$EX$，这与引理2矛盾。

结论2的证明　反证法。假设存在抵抗心急破坏者的强安全双方级联协议$P=\{\tilde{\rho}_i, \tilde{\sigma}_j\}$，由定理2和定义3，有对每个$k\geqslant 1$

1) $lt(\overline{N_k(X,Y)})\cap\{EX,EY\}\neq\phi$,

2) $\sigma_k(X,Y)$对于Y具有平衡性质，及对某个i，j $1\leqslant j\leqslant i\leqslant t$，$\sigma_1\epsilon E\cup\{DX\}$和$\sigma_2\epsilon\{DY\}$有

3) $\overline{\sigma_1 N_{2i}(X,Y)}=\overline{\sigma_2 N_{2j-1}(X,Y)}=\lambda$

由1）和3），我们有

$$\{EX\}\subseteq lt(\overline{N_{2i}(X,Y)})\subseteq\{EX,DX,DY\},$$

$$\{EY\}\subseteq lt(\overline{N_{2j-1}(XY)})\subseteq\{EY,DX,DY\}.$$

据引理6，σ_1，$N_{2i}(X,Y)$和$N_{2j-1}(X,Y)$是强Y-平衡的。要使3）成立，据引理4，必须$(lt(\sigma_1)\cup lt(\overline{N_{2i}(X,Y)}))\cap\{EY,DY\}=\phi$，得出$lt(N_{2i}(X,Y))\cap\{EY,DY\}=\phi$，但

$$\overline{N_{2i}(X,Y)}=\overline{\sigma_i\rho_i\sigma_{i-1}\rho_{i-1}\cdots\sigma_{j+1}\rho_{j+1}\sigma_j N_{2j-1}(X,Y)}$$

而据引理6

$\overline{\sigma_i\rho_i\sigma_{i-1}\rho_{i-1}\cdots\sigma_{j+1}\rho_{j+1}\sigma_j}$和$\overline{N_{2j-1}(X,Y)}$是强$Y$-平衡的，现在

$EY\epsilon lt(\overline{N_{2j-1}(X,Y)})$，根据引理7，$lt(\overline{N_{2i}(X,Y)})\cap\{EY,DY\}\neq\phi$，矛盾。

结论3的证明　令$P=\{\rho_1,\sigma_1\}$，这里$\rho_1(X,Y)=EY_iX$，$\sigma_1(X,Y)=EXdXDY$。应

用印章协议安全性判别算法，最后得到C矩阵：

	0	1	2	3	4	5	6	7	8	9	10
0	1					1				1	
1		1								1	
2			1							1	
3	1			1		1				1	
4	1	1		1	1	1		1		1	
5	1					1				1	
6	1	1				1	1	1		1	
7	1	1				1		1		1	
8	1		1	1		1				1	
9	1					1				1	
10	1		1	1		1				1	1

由于$(0,1)\notin c$，知P是安全的，又取$\sigma_1=DX$，$\sigma_2=dDY$，有

$$\overline{\sigma_1 N_2(X,Y)}=\overline{DXEX}=\lambda=\overline{dDYEY_iX}=\overline{\sigma_2 N_1(X,Y)},$$

所以P是强安全双方印章协议。

3 结束语

关于强安全密码协议，我们认为至少有两点还有待于今后作进一步的探讨。

①强安全密码协议要求能否降低？我们要求收方在接到消息M后重新发回M，这从传输速率角度考虑是不理想的，能否引入一个单向函数$f(x)$，使收方在接到消息M后回送$f(M)$。发送方可自己计算$f(M)$，然后与收方发回的$f(M)$比较，判断收方是否收到M。

②我们所讨论的协议都是双方协议，而在网络通信中圆桌会议是经常发生的。如何将双方协议推广到多方协议是个重要的课题。

参 考 文 献

[1] Dolev D et al., *Inform. Theory*, IT-29(1983),2, 198～209

[2] Dolev D et al., *Inform. and Control*, 55(1982),57～68

[3] Book R V et al., *Theoretical Computer Science*, 39(1985), 2,3, 319～325

The Strong-secure Cryptography Protocol

Yao Qingda Li Liandi Chen Weimin*

Abstract

A strong-secure cryptography protocol against tampering with message in Public Key Cryptography has been introduced. The strong-secure characters of Dolev & Yao's well-known cascade protocol and name-stamp protocol have also been explored.

Keywords protocol, casade, name-stamp, strong-secure, cryptography

*Computer Software Institute