基于 Clifford 半群上共轭搜索问题的密钥建立协议*)

黄华伟　肖国镇

(西安电子科技大学信息保密研究所　西安 710071)

摘　要　本文采用更广泛的半群作为平台，推广了 Iris Anshel 等提出的代数密钥建立协议模型。在定义了 Clifford 半群上的多重同时共轭搜索问题(MSCSP)后，给出了基于此问题的密钥建立协议。在理论上证明了若 Clifford 半群上的多重同时共轭搜索问题(MSCSP)是困难的，那么可以利用 MSCSP 来构造密钥建立协议，从而说明利用半群作为平台构建密钥建立协议是可能的。本文也提供了一种新的利用辫群的思路，即考虑利用辫群上的强半格(许多辫群按照一定规则形成的无交并)构成的 Clifford 半群来构建密码协议，以弥补单个辫群可能存在的安全缺陷。

关键词　密钥建立协议，Clifford 半群，多重同时共轭搜索问题(MSCSP)

A Key Establishment Protocol Based on Conjugacy Search Problem in Clifford Semigroups

HUANG Hua-Wei　XIAO Guo-Zhen

(Research Inst. of Information Security&Privacy, Xidian Univ., Xi'an 710071)

Abstract　This paper improves on an algebraic key establishment protocol presented by Iris Anshel et al. In our protocol, semigroup instead of group is adopted. After defining the multiple simultaneous conjugacy search problem (MSCSP) in Clifford semigroups, we give a key establishment protocol based on MSCSP. It is proved that if the MSCSP in some Clifford semigroups is hard, we can use this class Clifford semigroups to construct key establishment protocols. Hence it is possible to make use of semigroups as a platform to construct key establishment protocols. This paper also suggests a method of using braid group. We may make use of the strong semilattice of braid groups (the disjoint unions formed by many braid groups according to some rules) to construct cryptological protocol and remedy the possible secure bug of a simple braid group.

Keywords　Key establishment protocol, Clifford semigroup, Multiple simultaneous conjugacy search problem (MSCSP)

密码协议是一种分布式算法，是指两个或两个以上实体为达到一个特定的安全目标，执行一系列有明确动作规定的步骤。密钥建立协议是为了以后的密码学用途使一个秘密密钥对两方或更多方都可用的过程。目前主要的公钥密码系统和相应的协议大都基于有限群[1]，而且大多数的方法都是基于有限域上的算术。许多学者都希望找到可用于密码学的新的代数结构，一部分学者提出了基于非交换群的公钥算法和协议(如文[2])。

Iris Anshel 等 1999 年[3]提出了一个基于非交换群的代数密钥建立协议模型。利用在适当选择的群上多重同时共轭搜索的困难性问题(MSCSP)，文[3]给出一个具体的密钥建立协议。作者利用两个非交换的单向函数来计算出一个共同的换位子。他们发现利用辫群很有可能实现这些协议。之后，文[4]利用辫群上的单向函数构造了一个具体可行的 Diffie-Hellman 型密钥协商协议。这些方法的简易性激发了许多学者探索基于辫群的公钥密码体制。但是经过仔细研究后发现，也许是辫群过于丰富的结构导致了许多攻击辫群密码协议的特殊方法，例如长度攻击等[5~7]。辫群中的共轭困难问题是大部分辫群密码协议的基石，最近的一些结果表明解决辫群共轭困难问题并不像预料的那样难[8]。现在已经发现一些解决辫群共轭搜索问题的确定算法有可能是多项式时间的[9](没有证明)。越来越多的理论和实验结果表明辫群不是构建密码协议的好的平台。因此，最近一些学者利用其他非交换群代替辫群或者采用辫群中其他的困难问题代替共轭搜索问题，如文[10]。

本文从理论上探索了利用半群作为平台构建密钥建立协议的可能性。首先，我们采用更广泛的半群作为平台，推广了 Iris Anshel 等提出的一个代数密钥建立协议模型。然后，我们定义了 Clifford 半群上的多重同时共轭搜索问题(MSCSP)，并给出了基于此问题的密钥建立协议。在理论上证明了若 Clifford 半群上的多重同时共轭搜索问题(MSCSP)是困难的，那么可以用利用 MSCSP 来构造密钥建立协议。

1　Iris Anshel 代数密钥建立协议的推广

本节对文[3]中的代数密钥建立协议模型进行了推广。

我们的协议基于一个五元组 $(U,V,\beta,\gamma_1,\gamma_2)$，其中 U 和 V 都是半群，并且

$\beta:U\times U\to V,\gamma_i:U\times V\to V(i=1,2)$

是满足下列性质的可计算的函数：

(ⅰ)对任意 $x,y_1,y_2\in U,\beta(x,(y_1\cdot y_2))=\beta(x,y_1)\cdot\beta(x,y_2)$。

(ⅱ)对任意 $x,y\in U,\gamma_1(x,\beta(y,x))=\gamma_2(y,\beta(x,y))$。

*)本文得到国家自然科学基金项目(No. 60473028)和"十五"军事通信预研项目(No. 41001040102)的资助。黄华伟　博士，研究方向：计算机密码学、半群代数理论及编码学等。

(ⅲ)假设 $x\in U$ 是秘密元，$y_1,y_2,\cdots,y_k\in U$ 以及 $\beta(x,y_1),\beta(x,y_2),\cdots,\beta(x,y_k)$ 是公开的，那么确定秘密 x 是不可行的。

分别指定公开的有限生成的子半群 $S_A,T_B\subseteq U$ 给用户 A 和 B。假设 S_A 的生成元集为 $\{s_1,s_2,\cdots,s_m\}$，T_B 的生成元集为 $\{t_1,t_2,\cdots,t_m\}$。

下面给出这节的主要协议。

第一步　用户 A,B 分别选择秘密元 $a\in S_A,b\in T_B$。

第二步　用户 A 计算、传送 $\beta(a,t_i),(i=1,2,\cdots,n)$ 给用户 B。同时，用户 B 计算、传送 $\beta(b,s_i),(i=1,2,\cdots,m)$ 给用户 A。

第三步　用户 A,B 分别计算 $\beta(b,a),\gamma_1(a,\beta(b,a))$ 以及 $\beta(a,b),\gamma_2(b,\beta(a,b))$。他们的共享密钥为 $\kappa=\gamma_1(a,\beta(b,a))=\gamma_2(b,\beta(a,b))$。

协议的有效性证明如下。

由性质(ⅲ)知，尽管传送信息是在公开信道上进行，秘密元素 a 和 b 仍然是安全的。性质(ⅰ)确保用户 A 能够计算 $\beta(b,a)$ 和 $\gamma_1(a,\beta(b,a))$。同样，用户 B 能够计算 $\beta(a,b)$ 和 $\gamma_2(b,(\beta(a,b))$。根据性质(ⅱ)，

$\kappa=\gamma_1(a,\beta(b,a))=\gamma_2(b,\beta(a,b))$，

这样就建立了共享密钥。

上面的协议是文[3]中对应的代数密钥建立协议的推广。在文[3]中，U 和 V 都限制在幺半群(含单位元的半群)上，S_A,T_B 也限制在子幺半群上。但是，我们发现单位元的存在对协议本身并无影响。我们的这个协议是采用了更广泛的平台，U 和 V 是半群，而 S_A,T_B 是 U 上的子半群。此协议可以看做是构建密钥建立协议的一个代数模型，要应用此模型，必须找到合适的半群以及合适的困难问题。

若 $U=C=S$ 为辫群，$S_A,T_B\subseteq S$ 为有限生成的子群。函数 $\beta:S\times S\to S$ 被定义为：$\beta(x,y)=x^{-1}yx$。函数 $\gamma_1,\gamma_2:S\times S\to S$ 被定义为：$\gamma_1(u,v)=\gamma_2(u,v)=u^{-1}v$。那么，容易验证性质(ⅰ)，(ⅱ)和(ⅲ)都成立，上面的这个协议就是文[3]中的基于辫群上多重同时共轭搜索的困难性问题(MSCSP)的密钥建立协议。

本文找到了一类可以应用于此协议的半群，即 Clifford 半群。基于的问题是 Clifford 半群上的多重同时共轭搜索问题(MSCSP)。在接下来的两节中，我们证明了若 Clifford 半群上的多重同时共轭搜索问题(MSCSP)是困难的，那么可以用利用 MSCSP 来构造类似的密钥建立协议。

2　Clifford 半群上的多重同时共轭搜索问题(MSCSP)

这一节首先给出了 Clifford 半群的相关概念及结论，然后定义了 Clifford 半群上的多重同时共轭搜索问题。

令 S 为半群，$a\in S$ 称为正则的，如果对任意 $x\in S,a=axa$；S 是正则的，如果它的所有元素都是正则的。正则半群 S 称为逆半群，如果任意 $a\in S$ 都有一个唯一的逆元，即存在一个唯一的元 $a^{-1}\in S$ 使得 $aa^{-1}a=a,a^{-1}aa^{-1}=a^{-1}$。令 $e\in S,e$ 称为幂等的，如果 $e^2=e$。通常 $E(S)$ 表示 S 中所有幂等元集合。正则半群 S 称为 Clifford 半群，如果它的幂等元都是中心的，即 $ex=xe$ 对任意 $e\in E(S)$ 和 $x\in S$ 都成立。根据文[11]，我们知道正则半群是逆半群当且仅当它的所有幂等元构成一个交换子半群。因此，Clifford 半群是一类特殊的逆半群。

引理[11]　令 S 为逆半群。那么下列各条成立：

(1)对任意 $a\in S,(a^{-1})^{-1}=a$；

(2)对任意 $a\in S,aa^{-1},a^{-1}a\in E(S)$；

(3)对任意 $a,b\in S,(ab)^{-1}=b^{-1}a^{-1}$。

半群 S 上的格林关系 L,R 定义为：aLb 当且仅当 $S^1a=S^1b,aRb$ 当且仅当 $aS^1=bS^1$。这里 S^1 的定义如下：若 S 有单位元，$S^1=S$；若 S 无单位元，$S^1=SU\{1\}$(1 为添加的单位元)。显然，L 和 R 都是等价关系。在逆半群中，aLb 当且仅当 $a^{-1}a=b^{-1}b,aRb$ 当且仅当 $aa^{-1}=bb^{-1}$。因此，逆半群的每个 L 类和每个 R 类都有唯一的幂等元。若 S 为 Clifford 半群，则对任意 $a\in S$ 都有 $a^{-1}a=aa^{-1}$ 成立，从而 $L=R$(详见文[11])。

每个群都有唯一的幂等元，即单位元 1，但是一个半群通常有许多幂等元且可能无单位元。易知，每个群都是 Clifford 半群，但是 Clifford 半群不一定是群。因此，所有 Clifford 半群的集合真包含所有群的集合。

例[12]　令 $D=\{(z,n)\mid z\in Z,n\in N\}$，在 D 上定义乘法如下：

$$\forall(z_1,n_1),(z_2,n_2)\in D,(z_1,n_1)(z_2,n_2)=(z_1+z_2,\max\{n_1,n_2\})$$

容易验证，D 关于此乘法是交换 Clifford 半群。对任意 $(z,n)\in D,(z,n)^{-1}=(-z,n)$，且 (z,n) 所在的 L 类 $L_{(z,n)}$ 包含的唯一幂等元为 $(0,n)$。D 的幂等元集 $E(D)=\{(0,n)\mid n\in N\}$。

定义 1　令 S 为 Clifford 半群。共轭搜索问题(CSP)是：假设 $a,b\in S$ 且存在 $x\in S$ 使得 $x^{-1}ax=b$，找出至少一个满足这种条件的 x。

定义 2　令 S 为 Clifford 半群。多重同时共轭搜索问题(MSCSP)是：假设 $a_1,\cdots,a_r,x^{-1}a_1,x,\cdots,x^{-1}a_rx\in S$，找出至少一个满足这种条件的 x。

显然，这两个定义是群上(多重同时)共轭搜索问题概念的自然推广。

辫群作为 Clifford 半群的一个特例，其上的(多重同时)共轭搜索问题被认为是困难的(虽然近来发现一些解决辫群共轭搜索问题的确定算法有可能是多项式时间的，但仍没有证明)。

令 $C=\{S\mid S$ 是 Clifford 半群$\}$，记 $M=\{S\in C\mid S$ 上的 MSCSP 是困难的$\}$。既然$\{$所有辫群$\}\subseteq M$，我们有 $M\neq\varnothing$。容易证明，上文例中的 $D\notin M$。

3　基于 Clifford 半群的密钥建立协议

本节基于 Clifford 半群上多重同时共轭搜索问题(MSCSP)，构建密钥建立协议。这个协议是第 1 节的代数协议模型的具体应用，推广了文[3]中基于群的密钥建立协议。

令半群 $U=V=S\in M$ 为可计算的 Clifford 半群。分别指定公开的有限生成的子半群 $S_A,T_B\subseteq U$ 给用户 A 和 B：

$$S_A=\langle s_1,s_2,\cdots,s_m\rangle,T_B=\langle t_1,t_2,\cdots,t_n\rangle。$$

函数 $\beta:S\times S\to S$ 被定义为共轭作用：

$$\beta(x,y)=x^{-1}yx。$$

函数 $\gamma_1,\gamma_2:S\times S\to S$ 分别被定义为：

$$\gamma_1(u,v)=u^{-1}v,\gamma_2(u,v)=v^{-1}u.$$

定理　五元组 $(S,S,\beta,\gamma_1,\gamma_2)$ 满足第 1 节代数密钥建立协议模型中的性质(ⅰ)，(ⅱ)，(ⅲ)。

证明　令 $x,y_1,y_2\in S$。由逆半群的定义以及引理(2)，知对任意 $a\in S$

$aa^{-1}a=a, a^{-1}aa^{-1}=a^{-1}$ 且 $a^{-1}a, aa^{-1}\in E(S)$。

另一方面，既然是 Clifford 半群，它的所有幂等元都是中心的。因此，

$$\begin{aligned}\beta(x,(y_1\cdot y_2))&=x^{-1}(y_1\cdot y_2)x\\&=x^{-1}xx^{-1}(y_1\cdot y_2)xx^{-1}x\\&=x^{-1}(xx^{-1}y_1)\cdot(y_2xx^{-1})x\\&=x^{-1}(y_1xx^{-1})\cdot(xx^{-1}y_2)x\\&=(x^{-1}y_1x)\cdot(x^{-1}xx^{-1}y_2x)\\&=(x^{-1}y_1x)\cdot(x^{-1}y_2x)\\&=\beta(x,y_1)\cdot\beta(x,y_2)。\end{aligned}$$

这证明了性质(ⅰ)。

令 $x,y\in S$。计算 $\gamma_1(x,\beta(y,x))=x^{-1}\cdot(y^{-1}xy)=x^{-1}y^{-1}xy$。由引理(1)和(3)，可得

$$\begin{aligned}\gamma_2(y,\beta(x,y))&=[\beta(x,y)]^{-1}\cdot y\\&=(x^{-1}yx)^{-1}\cdot y\\&=x^{-1}y^{-1}(x^{-1})^{-1}\cdot y\\&=x^{-1}y^{-1}xy。\end{aligned}$$

从而 $\gamma_1(x,\beta(y,x))=\gamma_2(y,\beta(x,y))$，性质(ⅱ)成立。

最后，假设 $x\in S$ 是一个秘密元，而 $y_1,y_2,\cdots,y_k\in S, x^{-1}y_1x, x^{-1}y_2x,\cdots,x^{-1}y_kx\in S$ 是公开的。由于 $S\in M$，我们知道由这些信息确定 x 是不可行的，因此性质(ⅲ)成立。

下面，我们给出这节的主要协议。

第一步　用户 A，B 分别选择秘密元 $a\in S_A, b\in T_B$。

第二步　用户 A 计算、传送 $a^{-1}t_1a, a^{-1}t_2a,\cdots,a^{-1}t_na$ 给用户 B，用户 B 计算、传送 $b^{-1}s_1b, b^{-1}s_2b,\cdots,b^{-1}s_mb$ 给用户 A。

第三步　用户 A，B 分别计算

$$\beta(b,a)=b^{-1}ab, \gamma_1(a,\beta(b,a))=a^{-1}b^{-1}ab$$

以及

$$\beta(a,b)=a^{-1}ba, \gamma_2(b,\beta(a,b))=a^{-1}b^{-1}ab。$$

他们的共享密钥为 $\kappa=a^{-1}b^{-1}ab$。

我们给出协议有效性的详细证明如下。

假设 A 选定 $i_1,i_2,\cdots,i_p\in\{1,2,\cdots,m\}, k_1,k_2,\cdots,k_p\in Z$，把 $a=s_{i_1}^{k_1}\cdot s_{i_2}^{k_2}\cdots s_{i_p}^{k_p}$ 作为自己的秘密元；B 选定 $j_1,j_2,\cdots,j_q\in\{1,2,\cdots,n\}, k'_1,k'_2,\cdots,k'_q\in Z$，把 $b=t_{j_1}^{k'_1}\cdot t_{j_2}^{k'_2}\cdots t_{j_q}^{k'_q}$ 作为自己的秘密元。在 A 与 B 分别进行协议的第 2、3 步之后，A 知道了 $b^{-1}s_1b, b^{-1}s_2b,\cdots,b^{-1}s_mb$，B 知道了 $a^{-1}t_1a, a^{-1}t_2a,\cdots,a^{-1}t_na$。因此，A 可以计算出

$$\begin{aligned}&(b^{-1}s_{i_1}b)^{k_1}\cdot(b^{-1}s_{i_2}b)^{k_2}\cdots(b^{-1}s_{i_p}b)^{k_p}\\&=[\beta(b,s_{i_1})]^{k_1}\cdot[\beta(b,s_{i_2})]^{k_2}\cdots[\beta(b,s_{i_p})]^{k_p}\\&=\beta(b,s_{i_1}^{k_1})\cdot\beta(b,s_{i_2}^{k_2})\cdots\beta(b,s_{i_p}^{k_p})(\text{由于}\beta\text{满足(ⅰ)})\\&=\beta(b,s_{i_1}^{k_1}\cdot s_{i_2}^{k_2}\cdots s_{i_p}^{k_p})(\text{由于}\beta\text{满足(ⅰ)})\\&=\beta(b,a),\end{aligned}$$

接着计算 $\gamma_1(a,\beta(b,a))=\gamma_1(a,b^{-1}ab)=a^{-1}b^{-1}ab$。同理，B 可以计算出 $\beta(a,b)$，接着计算

$$\begin{aligned}\gamma_2(b,\beta(a,b))=\gamma_2(b,a^{-1}ba)&=(a^{-1}ba)^{-1}\cdot b\\&=a^{-1}b^{-1}(a^{-1})^{-1}b\\&=a^{-1}b^{-1}ab。\end{aligned}$$

因此 A 与 B 就建立了共享密钥

$$\kappa=\gamma_1(a,\beta(b,a))=\gamma_2(b,\beta(a,b))=a^{-1}b^{-1}ab。$$

注记：

(1)既然可能不是群，文[3]中的基于群论的密钥建立协议是这个协议的一个特例。因此，这个协议推广了文[5]中基于群论的密钥建立协议。

(2)攻击者要从公开信道截收到的信息中确定 a 和 b，面临的是解决 Clifford 半群 S 上的 MSCSP 困难性问题。即使敌手解决了 MSCSP 问题，求得 a' 和 b' 使 $(a')^{-1}t_ia'=a^{-1}t_ia(i=1,\cdots,n), (b')^{-1}s_jb'=b^{-1}s_jb(j=1,\cdots,m)$，如果 $a'\neq a$ 或 $b'\neq b$，那么敌手仍求不出共享密钥 κ。

(3)这个协议提供了一种新的利用辫群的思路，即考虑利用辫群上的强半格(许多辫群按照一定规则形成的无交并)构成的 Clifford 半群来构建密码协议，以弥补单个辫群可能存在的安全缺陷。

结束语　本文采用更广泛的任意半群作为平台，推广了 Iris Anshel 等在文[3]中提出的代数密钥交换协议模型。在定义了 Clifford 半群上的多重同时共轭搜索问题(MSCSP)后，给出了基于此问题的密钥建立协议。在理论上证明了若 Clifford 半群上的多重同时共轭搜索问题(MSCSP)是困难的，那么可以用利用 MSCSP 来构造密码协议，从而说明利用 Clifford 半群作为平台构建密码协议是可能的。如果能够找到适用这个协议的 Clifford 半群，必将在实际中有重要用途。

参 考 文 献

1 Koblitz N. Algebraic Aspects of Cryptography[M]. Berlin: Springer-Veralg, 1998

2 Wagner N R, Magyarik M R. A public key cryptosystem based on the word problem[A]. In: G. R. Blakely and D. Chaum, eds. Advances in Cryptology: Proceedings of Crypto 84 (Lect. Notes in Comp. Sci. 196)[C]. Berlin: Springer-Veralg, 1985. 19～36

3 Anshel I, Anshel M, Goldfeld D. An algebraic method for publickey cryptography[J]. Mathematical Research Letters, 1999, 6(3-4): 287～291

4 Ko K H, Lee S J, Cheon J H, Han J W, Kang J S, Park C. New Public-Key Cryptosystem Using Braid Groups[A]. Crypto 2000: Lect. Notes in Comp. Sci. 1880[C]. Berlin: Springer-Veralg, 2000. 166～183

5 Franco N, Gonzales-Meneses J. Conjugacy problem for braid groups and Garside groups[J]. J. Algebra, 2003, 266(1): 112～132

6 Hughes J. A linear algebraic attack on the AAFG1 braid group cryptosystem[A]. ACISP 2002: Lect. Notes in Comp. Sci. 2384[C]. Berlin: Springer-Veralg, 2002. 212～225

7 Cheon J, Jun B. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem[A]. CRYPTO2003: Lecture Notes in Comput. Sci. 2729[C]. Berlin: Springer-Veralg, 2003. 212～225

8 Birman J, Ko K, Lee S. The infimum, supremum, and geodesic length of a braid conjugacy class[J]. Adv. in Math, 2001, 164(1): 41～56

9 Gonzalez-Meneses J. Improving an algorithm to solve Multiple Simultaneous Conjugacy Problems in braid groups. http://xxx.lanl.gov/abs/math.GT/0212150, 2005-11-18

10 Shpilrain V, Ushakov A. Thompson's Group and Public Key Cryptography[A]. Applied Cryptography and Network Security 2005: Lect. Notes in Comp. Sci. 3531[C]. Berlin: Springer-Veralg, 2005. 151～163

11 Howie J M. An Introduction To Semigroup Theory[M]. London: Academic Press, 1976

12 Blyth T S. Dubreil-Jacotin inverse semigroups. Proc. Roy. Soc. Edinburgh. Sect. A71, 1973. 345～360