Contemporary Engineering Sciences, Vol. 2, 2009, no. 11, 543 - 552

Transversal Struture Based Key Establishment Protocols

Gunjan Srivastava

MNNIT Allahabad
gunjansri21@gmail.com

S. D. Dixit

J. K. Institute of Applied Physics
University of Allahabad

Abstract. In this paper, we study various shared key establishment protocols using algebraic machinery (viz presentation theory of groups and transversals in groups) which are based on Diffie-Hellman spirit. We develop a cryptosystem using transversal structure in groups.

Keywords: Diffie Hellmann, Group based cryptography, Transversals, Presentation theory, Free groups

1. Introduction

The most commonly used cryptosystem R.S.A and few others used today in its strength depend on the complexity in finite Abelian groups. Although, till today the security of these protocols are not threatened, but with the advent of quantum computers, it might be threatened in future. It appears prudent, therefore to explore the possibility of enhancing these protocols in its spirit. The extraordinary complexity in the combinatorial problems in the presentation theory of groups, prompts us to develop protocols based on these problems and which in spirit is the same as that in Diffie-Hellman. This idea has been explored in [16] and also in the seminal work of Anshel etal [1,2] . We search for other similar protocols and study them (specially the algebra behind these protocols) together with the existing ones also.

This paper is organised as follows. In section 2, we discuss the principle of secret shared key protocol. Section 3 centers arround introduction of protocol algebra based on the spirit of Diffie Hellmann. The section 4 contains some basic concepts in combinotorial group theory based cryptography. Dehn fundamental problems which play an important role in deciding the security of group based cryptography are discussed in section 5. A protocol which is generalization (and indeed more secure) of the Ko-Lee protocol and which is based on conjugacy search problem is discussed in section 6. In section 7, we describe as to how group action can be used to devlop protocols. Finally the most important section in this article is the section 8 in which it is shown as to how the concepts in transversals in group theory can be used to develop efficient and secure cryptosystem. The multilevel cryptographic protocols can also be used in succession to the transversal structure based cryptography.

2. **Preliminaries**

Encryption - Decryption using secret shared key

Once Alice and Bob agree on a secret shared key, they enter into a realm of symmetric key cryptography. There are various encrypting and decrypting procedures depending on the algebra of key and message spaces.

Example 2.1. *The hash function based encryption and decryption is based on the algebra of group* $\mathbb{Z}_2^n = (0,1)^n$. *More precisely, let* S *be a set of key space of sufficiently large size. Let* $H : S \to \mathbb{Z}_2^n$ *be any (public) injective function (called a Hash function)from the key space* S *to the strings of zeros and ones of length* n, *where* n *is as large as computer can afford or at least* $\log_2 |S|$, *if* S *is finite. Suppose that Alice and Bob have arrived on a shared secret key* k *(by some means). Then Alice encrypts a message* $m \in \mathbb{Z}_2^n$ *by*

$$E(m) = m \oplus H(k)$$

where $\oplus$ *is the addition modulo* 2. *Further, Bob decrypts the message by*

$$DE(m) = m \oplus H(k) \oplus H(k) = m.$$

It may be noted that, in general $\mathbb{Z}_2^n$ *can be replaced by a large group* G.

3. **Diffie-Hellman key spirit**

Based on the spirit of the paper [6] in which Diffie and Hellman used an excellent idea to establish a shared secret key between Alice and Bob through a non secure channel. We introduce the following definition

Definition 3.1. *A septuple* $(U, V, W, X, \beta, \gamma_1, \gamma_2)$ *where* V *and* W *are monoids,* U *and* X *are sets,* β *a map from* $U \times V$ *to* W*,* γ_1 *and* γ_2 *are maps from* $U \times W$ *to* X *is called a Diffie-Hellman protocol algebra if*
(i) $\beta(u, v_1v_2) = \beta(u, v_1)\beta(u, v_2)\ \forall u, v_1, v_2, v \in V$*,*
(ii)$\gamma_1(u, \beta(\acute{u}, v)) = \gamma_2(\acute{u}, \beta(u, v))\ \forall u, \acute{u} \in U$
(iii) It is computationally feasible to find $\beta(u, v)\ \forall\ u\ \in U, v \in V$ *and also* $\gamma_1(u, w)$ *and* $\gamma_2(u, w)\ \forall u \in U$ *and* $w \in W$*.*
(iv)It is computationally infeasible to find u *from the knowledge of* $\beta(u, v)$ *and* v*.*

3.1. **Key Establishment Protocol.** (i)A Diffie-Hellmann Protocol Algebra is made public.
(ii) Alice selects an element $u \in U$ as her private key and sends the pair $(v, \beta(u, v))$ to Bob.
(iii) Bob then selects an element $\acute{u} \in U$ as private key and sends $(v, \beta(\acute{u}, v))$ to Alice.
(iv)Alice computes $\gamma_1(u, \beta(\acute{u}, v))$, Bob computes $\gamma_2(\acute{u}, \beta(u, v))$.
The shared secret Key is

$$k = \gamma_1(u, \beta(\acute{u}, v)) = \gamma_2(\acute{u}, \beta(u, v)).$$

Some examples of of key establishment on this algebra are given below:

Example 3.1. ***Diffie hellman key protocol*** *Let* G *be a monoid. Take* $U = \mathbb{N} \cup \{0\}$*,* $V = W = X = G$*.*
Define the following mappings:
(i) β *a map from* $U \times V$ *to* W *as*

$$\beta(n, g) = g^n,$$

(ii) γ_1 *and* γ_2 *are maps from* $U \times W$ *to* X *as*

$$\gamma_1(n, h) = h^n = \gamma_2(n, h) = \beta(n, h)$$

for $n \in \mathbb{N} \cup \{0\}$ *and* $h \in G$ *It can be shown that all the conditions of Diffie Hellmann protocol Algebra are satisfied.*

Example 3.2. *Let* G *be a nilpotent group of class* 2*. Take* $U = V = W = X = G$*.*
Define the following mappings:
(i) β *a map from* $U \times V$ *to* W *as*

$$\beta(u, v) = u^{-1}vu$$

(ii) γ_1 *and* γ_2 *are maps from* $U \times W$ *to* X *as*

$$\gamma_1 = \gamma_2 = \beta.$$

Then since $[u, v] = u^{-1}v^{-1}uv$ *is a member of center of* G *it follows that*

$$\beta(u, \beta(\acute{u}, v)) = \beta(\acute{u}, \beta(u, v)).$$

Here the conjugacy search problem even if the group presented is known to be nilpotent of class 2*, appears to be infeasible and therefore difficult for adversary to decrypt.*

Example 3.3. *Let* G *be a group. Consider a subset* A *of* G *such that* $[A, A] \subseteq Z(G)$*, where* $[A, A] = \{u^{-1}v^{-1}uv : u, v \in A\}$ *and* $Z(G)$ *is a center of* G*. Take* $U = A, V = W = X = G$*, and define the mappings as*

$$\beta(a, g) = g^a = a^{-1}ga. \text{ and}$$

$$\gamma_1 = \gamma_2 = \beta.$$

The conditions (i), (ii) and (iii) in the definition 3.1 are satisfied while condition (iv) follows from the fact that the conjugacy search problem for certain presentations of groups is infeasible. A platform group for such a protocol is relatively free nilpotent group $F_n/[[F_n, F_n], F_n]$ *of class* 2*,* F_n *being a free group of rank* n*.*

Remark 3.2. *The Diffie Hellman protocol algebra as above is a generalization of the protocol due to Ko etal [7].It may be noted that the evesdroper in this protocol will have to face the membership search problem which is undecidable in certain platform groups.*

4. Some basic concepts in combinatorial group theory based cryptography

4.1. **Free Groups.** Let X be a set. We denote by $X^{-1} = \{x^{-1} : x \in X\}$, the set X^{-1} is one-one correspondance through the map $x \to x^{-1}$ and $F(X)$ the free group on X. A word w in X is a finite arrangement of symbols in $X \cup X^{-1}$ given by

$$w = x^{\epsilon_1}{}_{\alpha_1} x^{\epsilon_2}{}_{\alpha_2} \dots x^{\epsilon_r}{}_{\alpha_r}, where\ x_{\alpha_i} \in X, \epsilon_i = \pm 1$$

We have also a symbol ϕ called the empty word.The above word w is called freely reduced word for each i, if either $\alpha_i \neq \alpha_{i+1}$ or $\alpha_i = \alpha_{i+1}$ but $\epsilon_i \neq -\epsilon_{i+1}$. The empty word is also termed as a freely reduced word.

Consider the set $F(X)$ of freely reduced words. The product in $F(X)$ is defined by juxtaposition and free reduction (free reduction means whenever we arrive at a consecutive $x_\alpha{}^\epsilon x_\alpha{}^{-\epsilon}$ in the product, we remove it). This makes $F(X)$ a group where identity is the empty word ϕ. The group $F(X)$ is called the free group on X. If X contains n elements we say that it is a free group

of rank n and denote it by F_n. A freely reduced word given in above equation is said to be cyclically reduced if either $x_{\alpha_r} \neq x_{\alpha_1}$ or $x_{\alpha_r} = x_{\alpha_1}$ but $\epsilon_r \neq -\epsilon_i$. Every word in $F(X)$ is a conjugate to a (not necessarily unique) cyclically reduced word.

4.2. **Presentation of Groups.** A presentation of a group is an ordered pair $(X; R)$ also written as $\langle X; R\rangle$ where X is a set and R is a set of words in X. Every presentation determines the group $G = F(X)/\langle R\rangle$, where $\langle R\rangle$ is the normal subgroup of $F(X)$ generated by R of which it is called presentation. Indeed every group has a presentation.
G is said to be relatively free if the subgroup $\langle R\rangle$ is fully invariant in $F(X)$ in the sense that $\alpha(\langle R\rangle) \subseteq \langle R\rangle$ for all endomorphism α of $F(X)$. One of the important properties of relatively free group $G = F[X]/\langle R\rangle$ is that every map from the generating set $\{x.\langle R\rangle : x \in X\}$ to G can be extended uniquely to an endomorphism of G.

5. Fundamental problems of Dehn

Motivated from the problems in topology, Dehn introduced the following problems known as Dehn Fundamental problems in the presentation theory of groups. Efficient algorithms to solve these problems are desired for cryptographic use. However, for secure communication, other variants of these problems such as conjugacy search problems and membership search problems are more important. The compexities involved in these problem make the communication quite secure.

5.1. **Word Problem.** Let $\langle X; R\rangle$ be a presentation of a group G.

"Do we have an algorithm by which we can decide in finite number of steps whether a word $w \in F(X)$ defines the identity of the group?" More precisely,: Do we have an algorithm by which we can decide in finite number of steps if $w \in \langle R\rangle$, the normal subgroup of $F(X)$ generated by R?
However, in some presentation of groups such as a Braid group with standard presentations, small cancellation groups or equivalently groups having Dehn presentation or equivalently hyperbolic groups it is possible to design efficient algorithm for solving word problems. Such groups are termed as Platform groups.

5.2. **Conjugacy Problem.** Given a presentation $\langle X; R\rangle$ of a group G, "Do we have an algorithm by which we can decide in finite number of steps whether

two words w_1, w_2 in $F(X)$ define conjugate words in G?"
Note that an algorithm for conjugacy problem also gives an algorithm to solve word problem.

5.3. **Isomorphism problem.** Given two presentations $\langle X; R\rangle$ and $\langle Y; S\rangle$ of groups G and $\acute{G}$ respectively.
"Do we have an algorithm by which we can decide in finite number of steps whether a group G having a presentation $\langle X; R\rangle$ is isomorphic to the group $\acute{G}$ having presentation $\langle Y; S\rangle$?"

5.4. **Conjugacy search problem.** Given a presentation $\langle X; R\rangle$ of a group G and the information that g and h are conjugate in G.
"Do we have an algorithm by which in finite number of steps we can find a $u \in G$ such that $g^u = u^{-1}gu = h$?". It may be noted that for a recursively presented groups with solvable word problem has a recursive algorithm which is quite insufficient and indeed exponential times.

5.5. **Membership decision problem.** Let $\langle X; R\rangle$ be a presentation of a group G. Let $W_1, W_2, \ldots, W_n$ be elements of G.
"Do we have an algorithm by which we can decide in finite number of steps whether an element $w \in G$ is in subgroup generated by $\{W_1, W_2.....W_n\}$?"
One may note that even if word problem for a presentation of group is solvable, decision problem may not be solvable. For example, in Braid group $B_n, n \geq 6$ the word problem is solvable where as decision problem is not solvable. (e.g. for subgroup $H =< \sigma_1^2, \sigma_2^2, \sigma_4^2, \sigma_5^2 >= F_2 \times F_2$ [12].

6. A Protocol based on conjugacy search problem

Let G be a group having a presentation $\langle X; R\rangle$. Let $H = \langle\{a_1, a_2, \ldots, a_r\}\rangle$, $K = \langle\{b_1, b_2, \ldots, b_s\}\rangle$ and L=$\langle\{c_1, c_2, \ldots, c_t\}\rangle$ be subgroups with the condition that $[[a_j, b_j], c_k] = 1$, $\forall i, j$ and k. H, K and L may be taken to be maximal with these properties. The subgroups H and K are made public. Alice selects an elemant $a \in H$ as a word $a = a(a_1, \ldots, a_r)$ in $\{a_1, a_2, \ldots, a_r\}$ $keepsitprivateandmakes$(c, c^a) public, where $c \in L$ is expressed as a word $c = c(c_1, \ldots, c_t)$ and $c^a = a^{-1}ca$. Bob, then, selects an elemant $b \in K$ as a word $b = b(b_1, \ldots, b_s)$ and sends $c^b = b^{-1}cb$ to Alice. Since $[a, b]$ commutes with c, $c^{ab} = c^{ba}$. Thus $c^{ab} = c^{ba}$ is their shared key.

To break, the protocol, an adversary needs a solution to conjugacy search problem (A recursive search is exponential and so infeasible). Further there are group presentations in which conjugacy search problem is infeasible (e.g. Braid groups).

7. Group Actions and protocols

Definition 7.1. *Let X be a set and $F(X)$ be the free group on X. We define a protocol Algebra on the set X to be a quaraple $(\rho, *, \bullet, R)$ where ρ is a homomorphism from $F(X)$ to $AutF(X), *$ and $\bullet$ are actions of $F(X)$ on $F(X)$ and R is a subset of $F(X)$ (called a set of relators) such that*
(i) $w * \rho(u)(w) = u \bullet \rho(w)(u)\ \forall u, w \in F(X)$
(ii) R is an admissible set of relators with respect to $\rho, *, \bullet$ in the sense that they preserve R . More precisely
(a) $w_1 w_2^{-1} \in R$ and $uv^{-1} \in R$ implies that $\rho(w_1)(u)(\rho(w_2)(v))^{-1} \in R$
(b) $w_1 w_2^{-1} \in R$ and $uv^{-1} \in R$ implies that $w_1 * \rho(u)(w_1) \bullet (w_2 * \rho(v)(w_2)^{-1} \in R$
(iii) Knowing $\rho(\bar{w})(\bar{v_1}), \rho(\bar{w})(\bar{v_2}), ..., \rho(\bar{w})(\bar{v_r})$, it is computationally infeasible to find $\bar{w}$ where $\bar{w} = w.\langle R \rangle$

Example 7.1. *Let $X = \{x_1, x_2, \dots, x_n\}$. Define ρ from $F(X)$ to $AutF(X)$ by $\rho(w)(u) = w^{-1}uw$. The actions $*$ and $\bullet$ of $F(X)$ on $F(X)$ are given by $u * v = u^{-1}v$ and $u \bullet v = v^{-1}u$. Let*
$R_n = \left\{x_i x_{i+1} x_i x_{i+1}^{-1} x_i^{-1} x_{i+1}^{-1} : 1 \leq i \leq n-1\right\} \cup \left\{x_i x_j x_i^{-1} x_j^{-1} : |i-j| > 1\right\}$ be the set of standard relators of the Braid group B_n. Then $(\rho, *, \bullet, R)$ is a protocol algebra on X.

Example 7.2. *Let $X = \{x_1, x_2, \dots, x_n, \dots,\}$. The quadraple $(\rho, *, \bullet, T_n)$ where $\rho, *$ and $\bullet$ are as in above example and $T_n = \left\{x_i^{-1} x_k x_i x_{k+1}^{-1} : k > i\right)$ is a standard set of relations in Thompson group P, is also a protocol algebra in the sense of the above definition 7.1. Similarly, $(\rho, *, \bullet, D_n)$ is a protocol algebra on $X = \{x_1, x_2, \dots, x_n\}$ where D_n is a subset of $F(X)$ such that $\langle X; D_n \rangle$ is a Dehn presentation.*

8. Transversals based cryptosystems

Definition 8.1. *Given a pair (G, H) where G is a group and H a subgroup of G, a subset S of G obtained by selecting one and only one member from each right coset of H in G with $e \in S$, is called right transversals to H in G. If S is right transversal to H in G, then we have right quasi group structure "o" on S given by*

$$\{xoy\} = S \cap Hx.y$$

Indeed every right quasi group can be embedded as a right transversal to a subgroup in a group with some universal properties [11]. If S is a right transversal to a subgroup H in a group G then there is a bijection from the set $T(G, H)$ of all right transversals to H in G to the set of all identity preserving maps from S to H. More precisely , any right transversal $\acute{S}$ to H in G is determined uniquely by a map $g : S \to H$ with $g(e) = 1$, the identity of H, in the sense

that $\acute{S} = \{g(x)x | x \in S\}$ *and the right quasi group structure* $\acute{o}$ *induced on* $\acute{S}$ *is given by*

$$g(x)x\acute{o}g(y)y = g(x\theta g(y)oy)(x\theta g(y)oy)$$

where $\acute{o}$ *is the induced right quasi group structure on* $\acute{S}$ *and*

$$\{x\theta g(y)\} = Hxg(y) \cap S$$

This further induces a right quasigroup structure o_g on S given by

$$xo_g y = x\theta g(y)oy$$

which is isomorphic to $(\acute{S}, \acute{o})$. There are certain family of group pairs (G, H) given by presentations (for example Braid groups ,Hyperbolic groups, Small evaluation groups, groups having Dehn presentations and other one relater groups) for which word problems, conjugacy problems, are solvable whereas conjugacy search problems and membership search problems have infeasible solution. They can be used as platform groups for public key cryptography. We propose, two key establishment protocols using transversals.
A pair (G, H) out of platform of groups together with a transversal S and a map $g : S \to H$ is made public. Alice selects a private key $m \in \mathbb{N}$ and makes g^m public. Bob selects a private key n and makes g^n public. Then both Alice and Bob would know $g^{mn} : S \to H$ and thereby the right quasi groups which can be used as multilevel index cryptography for the exchange of messages as string of symbols .It may be computationally infeasible for any one to decrypt it in certain groups where computing discrete log problem is infeasible. To make it more secure we can have the following protocols :

8.1. **Key establishment protocol 1.** (i) A triple (G, H, S) where G is a group, H is a subgroup and S a right transversal to H in G, is made public.
(ii) A map $g : S \to H$ with $g(e) = e$ is made public .
(iii) Alice chooses a map $A : S \to \mathbb{N}$ as a private key and makes public the map $g^A : S \to H$ given by

$$g^A(x) = g(x)^{A(x)}$$

(iv) Bob chooses a map $B : S \to \mathbb{N}$ as a private key and makes public the map $g^B : S \to H$ given by

$$g^B(x) = g(x)^{B(x)}$$

Alice, then, sends her message as a strings of alphabets in S by encrypting it through a right quasi group operation [4,8,9,10] determined by the map

$g^{BA} = g^{AB}$ (which she can0 compute using the Bob's public Key g^B and her own private key A) to Bob and then Bob can decrypt it using inverse transformations determined by that quasi group.
The complexity in determining the keys A on B is equivalent to that of computing log in the presentation theory of groups. This can be extraordinarily complex depending on the choice of platform groups.

8.2. **Key establishment protocol 2.** (i) A triple (G, H, S) where G is a group, H is a subgroup and S a right transversal to H in G, is made public .
(ii) A map $g : S \to H$ with $g(e) = e$ is made public .
(iii) Let K be a public subgroup of H such that $[K, K] \subseteq$ Z(H)
(iv) Alice chooses a map $\phi : S \to K$ as a private key and makes public the map $g(x)^{\phi(x)} : S \to H$ given by

$$g(x)^{\phi} = g(x)^{\phi(x)} = \phi(x)^{-1} g(x) \phi(x)$$

(v) Bob chooses $\psi : S \to K$ as a private key and makes public

$$g^{\psi}(x) = g(x)^{\psi(x)} = \psi(x)^{-1} g(x) \psi(x)$$

Since $[K, K] \subseteq Z(H)$

$$g^{\phi\psi} = g^{\psi\phi}$$

Alice, then, sends her message as a strings of alphabets in S by encrypting it through a right quasi group operation [4,8,9,10] determined by the map $g^{\psi\phi} = g^{\phi\psi}$ (which she can compute using the Bob's public Key g^{ψ} and her own private key A) to Bob and then Bob can decrypt it using inverse transformations determined by that quasi group.
The complexity of the determining the keys A and B is equivalent to that of computing log in the presentation theory of groups. This can be extraordinarily complexity depending on the choice of platform groups.

References

[1] I.Anshel, M.Anshel, B.Fisher, D.Goldfield (1999), Algebraic method of public key cryptography, Maths.Res.Lett.6.pp.287-291.

[2] I.Anshel, M.Anshel, B.Fisher, D.Goldfield, New Key agreement protocol in Braid group Cryptography, Topics in cryptography-CT-RSA 2001, Lecture Notes in Computer Sci. 2020, Springer 2001,pp13-27.

[3] Dehn, M.Uber Unendliche diskontinuieche Gruppen, Math. Ann. 71(1912), pp.116-144.

[4] J.Denes and Keedwell A.D.(1999), Some applications of non-associative algebraic systems in cryptology, Tech Rep. 99/ 03, Dept of Math, Univ. of Surrey.

[5] Derek F Holt and Bettina Eick Hand book of computational group theory, Chapman and Hall CRC.

[6] W.Diffie and M.E.Hellman, New Directions in Cryptography, IEEE, Transaction in Information Theory, IT 22(1976) pp.644-654.

[7] K.H.Ko, S.J.Lee, J.H.Cheon, J.W.Han, J.Kang, C.Park, New public cryptosystem using Braid groups, Advances in Cryptography- CRYPTO 2000 (Santa Barbara CA.), 166-183, Lecture notes in computer science, 1880, Springer, Berlin 2000,pp 166-183.

[8] C.Koscielny (1996), A method of constructing quasi group based stream ciphers, Int J Appl. Math Comp Sci., Vol6, No.1, pp 109-121.

[9] C Koscielny and G.L.Muller (1999), A quasigroup based public key cryptosystem. Int J.Appl. Math and Comp. Scit, Vol9, No4, pp 953-963.

[10] C Koscielny (2002), Generation of quasi groups for cryptographic application Int J Appl. Math Comp Sci., Vol12, No.4, pp 559-569.

[11] Lal.R (1996), Transversals in group , J.Algebra ,181, pp 70-81.

[12] K.A.Mihailova, The occurance problem for direct product of groups. Dokl. Abad. Nank SSSR 119 (1958), (Russian) pp 1103-1105.

[13] A.Myashibov and V.Shpilrain (2007), Group based cryptography, Lecture Notes Center deRecerca Mathematica.

[14] P.S. Novikov, On the algorithmic unsolvability of word problem in group theory, Trudy Mat.Inst.Steklov, no.44, Izdat, Abad, Nank SSR Maskow 1955.

[15] V. Shpilrain and Gabriel Zapata, Arxiv, Combinatorial group theory and public key cryptography, Math 0410068v1[Math CR]

[16] N.R.Wagner, M.R Magralik , A Public key cryptosystem based on the word problem. CRYPTO,1984, Lecture notes in coputer science, 196, Springer,Berlin,1985, pp 19-36

Received: July, 2009