On the Security of New Key Exchange Protocols Based on the Triple Decomposition Problem

M. M. Chowdhury

Abstract: We show that two new key exchange protocols with security based on the triple decomposition problem may have security based on the MSCSP.

1 Introduction

Recently a new key exchange primitive based the triple DP (decomposition problem) is proposed in [1] and the triple DP is defined in [1] as finding the decomposition of a given element into three elements (that are not known).

One purpose of inventing the above scheme of [1] is its security is based on hard problems in braid groups such that a linear algebraic attack is not possible. It is claimed in [1] that the security of the new scheme is based on the triple DP in any G. If G is a group / the private keys are invertible then we show that the scheme in [1] is based on the CSP (conjugacy search problem) or the MSCSP (multiple simultaneous CSP) hence the algorithms in [1] are no more secure than using other key agreement algorithms using the CSP or MSCSP and hence the new scheme in [1] can be attacked feasibly using linear algebra if using braid groups (or the new scheme can be attacked with any algorithm that gives solutions of the CSP or MSCSP). There is a linear algebraic method to find solutions of the MSCSP which has been used to attack the braid key exchange protocol of Anshel-Anshel-Goldfeld [2] and this attack can be used to attack the new scheme with linear algebra.

2 Description of the New Protocols Based on the Triple Decomposition Problem

In this section the protocols are described using original portions of sections 2 and 3 taken from the preprint [1] (hence the protocols are described as exactly as in [1]).

2.1 Suggested Subgroup Parameters

In this section the protocols are described using original portions of sections 5 taken from the preprint [1] (hence the parameters are described as exactly as in [1]).

3 Security Of the Protocols based on the Triple Decomposition Problem

If G is a group (it is suggested in [1] that G may be a group an example given in [1] for G is the braid group) or the private keys are invertible then we can show the following. In this section we give our new result that the security

Figure 1:

Figure 2:

Figure 3:

Figure 4:

Figure 5:

of the new protocols in [1] is based on a system of equations (1 & 2 below), MSCSP or the CSP in G.

3.1 The First Protocol

Compute $O_1 = pqr = (b_1y_1)(y_1^{-1}b_2y_2)(y_2^{-1}b_3) = b_1b_2b_3$
Compute $O_1^{-1}pqJ_Ir = O_1^{-1}(b_1y_1)(y_1^{-1}b_2y_2)J_I(y_2^{-1}b_3)$
$= (b_3^{-1}b_2^{-1}b_1^{-1})b_1b_2J_Ib_3$
$= b_3^{-1}J_Ib_3$ for $1 \leq I \leq K_1$

$$b_3^{-1}J_Ib_3 \text{ for } 1 \leq I \leq K_1 \tag{1}$$

For some integer K_1 and J_I (J_I may be braids) chosen by the attacker.
Compute $pT_IqrO_1^{-1} = (b_1y_1)T_I(y_1^{-1}b_2y_2)(y_2^{-1}b_3)O_1^{-1}$
$= b_1T_Ib_2b_3(b_3^{-1}b_2^{-1}b_1^{-1}) = b_1T_Ib_1^{-1}$ for $1 \leq I \leq K_2$

$$b_1T_Ib_1^{-1} \text{ for } 1 \leq I \leq K_2 \tag{2}$$

For some integer K_2 and T_I chosen by the attacker. Observe the elements J_I are chosen from the A_3 (because of the commutativity conditions of the protocols) and the elements T_I are chosen from A_2. To find b_2 compute $b_2 = b_1^{-1}O_1b_3^{-1}$ and now Bob's private key is known and so the secret shared key can be constructed. Hence from the systems of equations 1 and 2 the security of the protocol can be based on the MSCSP [3] (which includes the CSP) hence we have shown that the security of the new protocol in [1] is based on solving the MSCSP twice. A very similar derivation show the security of the new protocol is also based on two MSCSP with the unknowns a_1 and a_3. An observation from the above is for any G the above the security of the protocol can also be based on (MSDSP) multiple simultaneous decomposition search problem for example (using the above computations) by solving the equations $b_1b_2J_Ib_3$ for $b_3, b_1T_Ib_2b_3$ for b_1 and then solving for b_2 using b_1 and b_3 and using the publicly known information (again there is a similar result using Alice's private keys) and not the triple decomposition problem. Observe that for the possible specific parameters suggested in [1] satisfy commutativity conditions such as B_2 commutes with A_2 etc. in addition to the required commutativity conditions which are necessary for the protocol to work. We can use these above additional commutativity conditions to show the security can be based on the CSP as follows. We can solve MSCSP for $a_1$and b_3 as described as above. Let $O_2 = uvw = a_1a_2a_3$.

To recover the common secret key compute
$O_2^{-1}a_1(O_1b_3^{-1})a_1^{-1}O_2 = a_3^{-1}a_2^{-1}(b_1b_2)a_2a_3 = a_3^{-1}(b_1b_2)a_3$,

$$a_3^{-1}(b_1b_2)a_3 \tag{3}$$

similarly
$O_1b_3^{-1}(a_1^{-1}O_2)b_3O_1^{-1} = b_1(a_2a_3)b_1^{-1}$

$$b_1(a_2a_3)b_1^{-1} \tag{4}$$

we can solve for above a_3, b_1 by solving the CSP with $b_1 b_2, a_2 a_3$ Or we can solve the 5,6 below for b_1 and a_3 as follows (so again the protocol can be based on the MSCSP).

Attacker selects V_I commuting with a_2 but not with a_3 or select $V_I \in B_1$
$O_2^{-1} a_1(V_I) a_1^{-1} O_2 = a_3^{-1} a_2^{-1}(V_I) a_2 a_3 = a_3^{-1} V_I a_3$

$$a_3^{-1} V_I a_3, \text{for } 1 \leq I \leq K_3 \tag{5}$$

similarly the attacker selects W_I commuting with b_2 but not with b_1 or select $V_I \in A_3$
$O_2 b_3^{-1}(W_I) b_3 O_2^{-1} = b_1 W_I b_1^{-1}$

$$b_1 W_I b_1^{-1} \text{ for } 1 \leq I \leq K_4 \tag{6}$$

The above result also holds when different subgroups are used that satisfy the additional commutativity conditions (described above) for an arbitrary G.

Observe that computing b_1 and b_3 from the MSCSP or CSP gives
$y_1 = b_1^{-1} p$, $y_2^{-1} = r b_3^{-1}$, hence $b_2 = (b_1^{-1} p) q (r b_3^{-1})$ (a_2 can be computed in a very similar way).

To defend against the attack in section 3.1 of reconstructing the secret shared key by solving the MSCSP the private keys of Alice, Bob are chosen so that they not invertible.

3.2 The Second Protocol

The derivation to show the second protocol can be based on the MSCSP is identical to the derivation for the first protocol except the elements J_I are chosen from S_{y_2}, the elements T_I are chosen from S_{y_1} etc. hence the above observations also applies to the second protocol. To defend against the attack in section 3.1 of reconstructing the secret shared key by solving the MSCSP all the elements in the private keys of Alice, Bob are chosen so that they are all not invertible.

4 Conclusion

We have shown that two new key exchange protocols with security based on the triple decomposition problem may have security based on the MSCSP or the MSDSP.

References

[1] A New Key Exchange Primitive Based on the Triple Decomposition Problem, Yesem Kurt, Cryptology eprint archive,http://eprint.iacr.org/2006/378

[2] A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem, 7th Australasian Conference on Information Security and Privacy-2002, LNCS 2384, Springer Verlag, pp. 176-189, 2002

[3] Ki Hyoung Ko, Tutorial on Braid Cryptosystems 3, PKC 2001,www.ipkc.org/pre_conf/pkc2001/PKCtp_k

[19] A New Key Exchange Protocol Based on the Decomposition Problem, V. Shilparin and A. Ushakov, http://eprint.iacr.org/2005/447

Appendix

We sketch the proof for the attacks considering the suggestion of 5.2.2 in [1]. We recover Bob's private key as follows.

$s_1 b_1 s_1^{-1}(s_2 y_1 s_2^{-1})(s_2 y_1^{-1} s_2^{-1})(s_3 b_2 s_3^{-1})(s_4 y_2^{-1} s_4^{-1})(s_4 y_2 s_4^{-1})(b_3) =$
$s_1 b_1 s_1^{-1} s_3 b_2 s_3^{-1} b_3 = O_1$
$O_1^{-1} s_1 b_1 s_1^{-1}(s_2 y_1 s_2^{-1})(s_2 y_1^{-1} s_2^{-1})(s_3 b_2 s_3^{-1})(s_4 y_2 s_4^{-1})(s_4 H_I s_4^{-1})$
$(s_4 y_2^{-1} s_4^{-1})(b_3) = O_1^{-1} s_1 b_1 s_1^{-1} s_3 b_2 s_3^{-1} s_4 H s_4^{-1} b_3 = b_3^{-1} s_4 H_I s_4^{-1} b_3.$
Hence b_3 can be found by solving the MSCSP.
Then $y_2 = (s_4^{-1} r b_3^{-1} s_4)^{-1}$
Now select J_I form A_2.
$s_1 b_1 s_1^{-1}(s_2 y_1 s_2^{-1})(s_2 J_I s_2^{-1})(s_2 y_1^{-1} s_2^{-1})(s_3 b_2 s_3^{-1})(s_4 y_2 s_4^{-1})(s_4 y_2^{-1}$
$s_4^{-1})(b_3) O_1^{-1} =$
$s_1 b_1 s_1^{-1}(s_2 y_1 s_2^{-1})(s_2 J_I s_2^{-1})(s_2 y_1^{-1} s_2^{-1})(s_3 b_2 s_3^{-1})(s_4 y_2 s_4^{-1})(s_4 y_2^{-1} s_4^{-1})$
$(b_3)((s_1 b_1 s_1^{-1})(s_2 y_1 s_2^{-1})(s_2 y_1^{-1} s_2^{-1})(s_3 b_2 s_3^{-1})(s_4 y_2^{-1} s_4^{-1})(s_4 y_2 s_4^{-1})(b_3))^{-1} =$
$= s_1 b_1 s_1^{-1}(s_2 y_1 s_2^{-1})(s_2 J_I s_2^{-1})(s_2 y_1^{-1} s_2^{-1}) s_1 b_1^{-1} s_1^{-1}$
$= s_1 b_1 s_1^{-1}(s_2 J_I s_2^{-1}) s_1 b_1^{-1} s_1^{-1}$
Hence b_1 can be found by solving the MSCSP.
Then $y_1 = s_1 b_1^{-1} s_1^{-1} s_2^{-1} p s_2$
Then we can recover Bob's second private key as
$(s_2 y_1 s_2^{-1}) q (s_4 y_2 s_4^{-1}) = (s_3 b_2 s_3^{-1})$
Now we have Bob's private key, the shared key is recovered as
$a_1(s_1 x_1 s_1^{-1})(s_1 b_1 s_1^{-1})(s_1 x_1^{-1} s_1^{-1})(s_2 a_2 s_2^{-1})(s_3 x_2 s_3^{-1})(s_3 b_2 s_3^{-1})(s_3 x_2^{-1} s_3^{-1})$
$(s_4 a_3 s_4^{-1}) b_3 =$
$a_1(s_1 x_1 b_1 x_1^{-1} s_1^{-1})(s_2 a_2 s_2^{-1})(s_3 x_2 b_2 x_2^{-1} s_3^{-1})(s_4 a_3 s_4^{-1}) b_3 = shared\ key$
There are similar attacks for each of our above attacks.