ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

GROUP KEY AGREEMENT WITH LOCAL CONNECTIVITY USING JAVA

C. Pretty Diana Cyril[1], P.Sathya Moorthy[2], V.Vijaykrishnan[3], Dr.S.Saravanakumar[4]
Research Scholar, Department of CSE, St. Peter's University, Chennai, India[1].
Final Year, Department of IT, Loyola Institute of Technology, Chennai, India[2, 3].
Professor, Department of IT, SVEC, Chennai, India[4].

Abstract:-
In this paper, we have a tendency to tend to check a gaggle key agreement draw back where a user is barely conscious of his neighbours whereas the property graph is unfair. In our draw back, there is not any centralized information for users.A gaggle key agreement with these choices is very acceptable for social networks. Below our setting, we have a tendency to tend to construct two economical protocols with passive security. We have a tendency to tend to accumulate lower bounds on the spherical quality for this sort of protocol, that demonstrates that our constructions unit spherical economical. Finally, we have a tendency to tend to construct associate actively secure protocol from a passively secure one.

1. INTRODUCTION

K extra parties to firmly share a secret key. Starting from Diffie Hellman [21] for the two-party case, this subject has been extensively studied inside the literature. However, the bulk the protocols assume a complete property. Another draw back is networks like Face book, Skype, we tend to chat and Google+, that the cluster key of a given cluster cannot be changed a user is just connected of them unit friends. But they'll still be connected indirectly through the friend network. Of course, we've got an inclination to can still regard them as directly connected by concerning the intermediate users as routers. However, this is {often|this can be} often quite altogether completely different from a directly affiliation. First, indirectly connected users may not have the final public data of each different (e.g., Public key certificate). Second, indirectly connected users may not acknowledge the existence of 1 another (e.g., in our college union example, one educational in one department may not acknowledge another educational throughout a completely completely different department). Third, a message between a pair of indirectly connected users travels a extended time than that between directly connected users.We tend to study the cluster key agreement with degree discretionary property graph, where each user is just aware of his neighbours and has no information concerning the existence of other users. Further, he has no information concerning the constellation.Beneath escape downside is not easy. Further, computationally secure KPS is just well-known for the two- party case and additionally the trilateral case. KPS with a gaggle size larger than 3 remains open.

A broadcast secret writing is also a mechanism that al- lows a sender to send a gaggle key to a specific set of users. This might be thought of a gaggle key agreement of one message that is sent by the sender. In a passing bilateral key primarily based broadcast secret writing, the sender is also a mounted authority. Throughout this case, the user key size is combinatorially lower finite. To boot, it's secure only against a restricted kind of users. in AN passing public key broadcast secret writing , the key size downside is waived.But one still must set the brink for the amount of unhealthy users.Jointly the ciphertext size depends on the amount of users and so may be large (e.g., it's O(√n) certain n users). Further, users unit initialized by a central authority that won't desired in our setting.

2. PRELIMINARIES

Notations we've an inclination to will use the following notions. For a bunch S, x ← S samples x from S uniformly randomly; Function μ : N → R is negligible if for any polynomial p(x), limn→∞ μ(n)p(n) = zero. PPT stands for probabilistic polynomial time.[n] denotes the. Set. H(X) = − x PX (x) log PX (x) is that the entropy of random variable X and H(X|Y) = − PXY (x, y) log PX Y| (x|y) .x,y is the conditional mutual data between X and Y , once Z is given. Identity Two ensembles square measure indistinguishable if no economical algorithmic program can tell them apart. This notion was first projected by Goldwasser and Micali [24] simply just in case of cryptography. Generally, it had been thanks to Yao [40]. Definition 1: Ensembles X = Z≥1 and Y = Z≥1 square measure indistinguishable if for any PPT formula D, |Pr[D(XZ) = 1] − Pr[D(YZ) = 1]| is negligible. In a cryptological system, Z typically is that the protection parameter and implicitly made public. For example, in AN extremely RSA system, Z is that the bit length of the modulus N .Identity Two ensembles ar indistinguishable if no economical algorithmic program can tell them

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Goldwasser and Micali [24] simply just in case of cryptography. Generally, it had been thanks to Yao [40]. Definition 1: Ensembles X = Z≥1 and Y = Z≥1 ar indistinguishable if for any PPT formula D, |Pr[D(XZ) = 1] − Pr[D(YZ) = 1]| is negligible. In a science system, Z typically is that the protection parameter and implicitly made public. As AN example, in an exceedingly} very RSA system, Z is that the bit length of the modulus N. Decisional Diffie-Hellman assumption Let p, letter of the alphabet be a pair of huge primes and q|(p − 1). Let G be the subgroup of ∗Zp of order letter of the alphabet and g be a generator of G. The decisional Diffie-Hellman assumption is as follows. Definition 2: The decisional Diffie-Hellman assumption (DDH) holds if (g, gx , gy , gxy) and (g, gx , gy , gz) ar in- distinguishable once x, y, z ← Zq . The following lemmas are going to be merely proved by a hybrid reduction and it appeared in [15]. Lemma 1: [15] Let n ∈ N. Then, beneath the DDH assumption, ∪ and one ≤ i < j ≤ n} ∪ ar indistinguishable, where aij (1 ≤ i < j ≤ n) and a1, • • • , associate ar all uniformly random from Zq.

3. FORMAL MODEL

3.1 Syntax

Let U = be the universe of users United Nations agency ar connected by associate rudderless connected graph G U . Assume the set of neighbours for i ∈ U is Ui ⊆ U .We have a tendency to tend to assume user i is tuned in to Ui.We'll define a key agreement on any rudderless connected subgraph G = (V, E) of GU . The set of neighbours of i in G is denoted by Ni(G). The protocol permits users in V to agree on a shared key.Each user i at intervals the protocol can entirely send messages to his neighbours Ni(G). Since user i has no information regarding users excluding Ui, we have a tendency to tend to ought to facilitate him to figure out Ni(G). Toward this, we have a tendency to tend to assume that there's a basic description of G (denoted by basic(G)) mere with Ui and basic(G), user i will be able to merely verify Ni(G). basic(G) is about by the protocol instigator and it will appear at intervals the first incoming message of any user (other than the initiator) in G, that for simplicity will not be mentioned another time later. The syntax is as follows. Definition 3: Let U = be the universe of users connected by associate rudderless connected graph GU, where user i incorporates a neighbour set Ui. Cluster key agreement is that the conditional entropy of X given Y . I(X; Y) = H(X) − H(X|Y) is that the mutual data between X and Y ; I(X; Y |Z) = H(X|Z)−H(X|Y Z)

Π with a locality property is also a mechanism with the following parts. Setup(1Z). Upon 1Z, a system parameter sp is generated. for each i ∈ U, a public key P Ki and a private key SKi ar generated. (sp, P renowned to user i. Key Agreement. For associate afloat connected subgraph G = (V, E) of GU , initiated by some I ∈ V with input basic(G), users in V move with their neighbours in G and eventually all of them derive a cluster key sk. The protocol is complete: if users in V follow the protocol, they derive identical sk. As associate example, let GU be a connected social network and G be a university college union administrative unit organizes its members on GU .Each educator has his own friend list Ui in GU. Given the name "faculty union", educator i will be able to verify Ni(G), assumptive that he's tuned in to that administrative unit in his friend list may well be a school member and administrative unit is not (this ar progressing to be a extremely reasonable assumption). Presently if a school member desires the union to reckon a union key. He can send the request "faculty union key" to his union neighbours and move with them, administrative unit then continue the similar interaction with their own union neighbors, and so on. Finally, union members can get a bunch key.

3.2 Security definition

Before formally method the protection, we have a tendency to tend to introduce the following notions. ΠAi i this can be associate instance (or session) in user i and Ai is that the instance id that differentiates it from various instances within the same statAi .This can be the internaluser.State of instance ΠAi.sidAii this can be the session image of instance i ΠAi . i i Its precise utility ar progressing to be mentioned at intervals the specification of partnering later. Pid neighbours Ai i .usually |this can be} often the set of neighbours that ΠAiiIs directly interacting kAi .This can be the cluster key with.Derived by ΠAi . i i By partnering, we have a tendency to tend to would really like to capture the intuition that a pair of partnered instances ought to attend thesameAj protocol execution. Formally, a pair of instances ΠAii and Πj ar directly partnered if Aj Ai 1.2. iS ∈(sid pidAii j , sid andAjj) j = ∈ 1pid, wherever ; re S may be a Boolean perform that can be made public w.r.t. the concrete protocol. Condition (1) intends to mention that ΠAi interacts with user j which ΠAj interacts with user i i. This condition implicitly implies that j j which i ar neighbors. Condition. Intends to mention that ΠAii and ΠAjj have consistent session identifiers and thence they are together execution the agreement. If uses i and j don't seem to be neighbors, we have a tendency to ar ready to generalize the partnership as follows. ΠAii and ΠAjj subgraph G of GU and request to execute the key agreement on it. He could corrupt users and obtain their long-standing time secrets. He can request to urge the cluster key of any session. If he's associate active wrongdoer, he could launch a man-in-the-middle attack. at intervals the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

formalized by allowing A to adaptively access the set of oracles that ar maintained by a contest.

3.3 Efficiency

Now we tend to contemplate the potency live of a bunch key agreement.The wide celebrated measures area unit computation value, communication quality and spherical com- plexity. The computation value of a user sometimes is outlined as the range of long operations like a standard involution. The communication quality is outlined because the total traffic length of the protocol. To outline the spherical quality, we tend to assume the protocol takings in rounds .The amount of spherical within which a protocol taking is named its round quality.

4. PASSIVELYSECURE CONSTRUCTIONS

In this section, we tend to gift 2 passively secure constructions.We tend to assume that at the start of the protocol, all parties in G area unit already notified the key agreement event (and in order that they will begin the protocol simultaneously).We tend to decision it a beginning assumption. This assumption is required solely to count the spherical quality. It's been implicitly assumed by several protocols within the literature (e.g., [17]). In our constructions, while not this assumption, a user won't begin till he receives the initial message whereas the entire protocol starts from associate degree leader. Below this, the passive security of our protocols remains unchanged however the spherical quality becomes larger. It'd be surprising: if a user in our setting is solely aware of his neighbors, however will all users be notified of the key agreement event before the protocol starts? We tend to remark that the protocols during this section area unit solely passively secure and ultimately they have to be created actively secure. In Section six, this can be done through a two-stage protocol: stage zero could be a pre processing stage that notifies every party of the key agreement event (starting from associate degree initiator) associate degreed stage one could be a real transformation from a passively secure protocol to an actively secure one, wherever the beginning assumption has been enforced in stage-0. We will initial gift the constructions for a graph G that's a tree. Then, we are going to extend them to a general connected graph. The primary construction is thought to be a bunch Diffie-Hellman with an area property. The second construction basically could be a personal coin moving protocol protected by a Diffie-Hellman key. Once G could be a tree: the primary theme Let p, letter be massive primes with letter|p− one and g be a generator of the cluster G of order q in Zp. ∗ Assume that p, q, g are all public. Let (Eρ, Dρ) be a centrosymmetric coding theme with a secret key ρ. Let G = (V, E) be associate degree directionless connected graph for is formally delineate . However, it'd be helpful to relinquish additional explanations here. The protocol contains 3 stages. ,ı,~4,~,s, ,A 4,, 7, s ı,~,2,~s, ss Selective Service Systems sss A4 ,ı,s ,~7.,~,s, , ,ı,~1,~s,s sssss s s,ıı, ,~~,36,~,~,ss, ss s ss militia s7sA ss7 ,s6s ss sAss5ı, ,~ 5 ~, .A,s 5,7=1A,8 A , κ ,,7,ı,ı ~,~,κλ,~~,s,,s ,cs. In Stage one, every A sends to every of his neighbouri: his own temporary Diffie-Hellman (DH) public key yet because the incorporate temporary DH public key of users within the subtree A (excluding A) of node i. Specifically, A ∈ V sends (AAi, AA) to every neighbour i, wherever he defines AA = gaA by taking a secret aA ← Zq and AAi is ready as follows. If user A could be a leaf, AAi = 1. Q Generally, AAi = j∈NA\ Aj AjA , that is iteratively outlined beginning from leaf users. For instance, A7,6 = A4A4,7 · A8A8,7 · A5A5,7 and toward this, node 7 should initial receive (A8,7, A8) from node eight, (A4,7, A4) from node four and (A5,7, A5) from node five. This might want many rounds within the protocol. For instance, (A4,7, A4) is sent to node seven in the 3th spherical in Stage one whereas (A5,7, A5) is shipped to node seven within the first spherical. Later, we are going to show within the completeness that AAi is really the merchandise of Aj for all j within the subtree A (excluding A) of node i (where we tend to regard G as a tree unmoving at i). as an example, A7,6 = A1A2A3A4A5A8A9 and A6,7 = A5,7 = 1. In Stage 2, every A sends to every of his neighbour i: a partial cluster secret that is a incorporate result of DH keys of all indirectly connected user combines such that every pair has a user in the subtree A of node i, wherever this partial cluster secret is shipped below the coding of the pairwise DH key between A and that i. Specifically, user A prepares associate degreed sends an encrypted LAi to every neighbour i, wherever the coding uses the Diffie-Hellman key ρAi = gaAai between i and A. Here LAi is ssss,ı,~ 4,~s,, ,[L] ssss ss ı,ı,,~,~32~,~,s,s,s ssssss s[sL seven,6s] 4s,7s,s [,s ı,s, ~,57,~ .,s, 7 ,[L 8,7,] , ss,ı~,1,~s,s sss L .] ı,~,κ,~s, s s s,ı~,λ~,,s ,ı~,6~,,s,s ,ı~,5,~s,

Defined as LAi = (Πj∈NA\LjA) · (Πj∈NA AjA) aA , that once more is outlined iteratively ranging from leaf users. as an example, L7,6 = L4,7L8,7L5,7 · (A4,7A8,7A5,7A6,7)a7.Here,LAi is computed providing every product term LjA has been received by A. Later, we are going to show within the completeness that LAi is that the product of all Diffie-Hellman key gajau , wherever j is within the subtree A (including A) of node i and u is bigoted as long as (j, u) f∈ E and j f= u. For Instance,L8,7 = ga8(a1+···+a6)+a9(a1+···+a7) In Stage 3, every user computes the cluster key mistreatment his own secret and also the partial cluster secrets he received in stage 2. Specifically, every user key letter aA . For instance, in Fig. 3,A

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

sk A =(L militia · AsAa2) L3,2A3a,22 · L4,2Aa42, 2. Later we L1,2A1,2 · will show within the completeness that gajau for (j, u) $f\in$ E and j $f=$ u. sk Since is that the product of sk will not all rely upon A, it's a shared key among all users. With the notions of AA, AAi and LAi, we will currently handily reveal the look plan of our protocol (Fig. 4). Use G . three as associate degree example. Roughly, we tend to will style the protocol such that sk is the product of all gajau for any combine of users (j, u) United Nations agency don't seem to be neighboursin G (here excluding neighboring (j, u) is for the safety proofQ purpose solely and can be even soon). That is, sk = (j,u)$f\in$E,j$f=$u g ajau . To admit user A to figure sk, we tend to intend to partition Ω = (j, u) $f\in$ E, j $f=$ u according to his neighboursand himself. Take A = seven as associate degree example. His neighbour's area unit four, 5, 6, κ. Partition Ω = Ω4 ∪ Ω5 ∪ Ω6 ∪ Ωκ ∪ Ω7. Here Ω4 is outlined because the set of all.

5. AN ACTIVELY SECURE CONSTRUCTION

We gift a construction of associate actively secure protocol Πr from a passively secure one Π. Our construction consists of 2 stages. Stage zero is to line up the session info and satisfy the beginning assumption. Stage one is that the actual transformation of Π that primarily authen- ticates every message in Π employing a signature. To raised perceive the protocol, we tend to give some explanations as follows. In Stage 0, besides satisfying the beginning assumption, we are going to establish a worldwide session symbol and also the session symbol between any 2 neighbouring users. Will be necessary as a user can solely access his neighbours. Toward this, associate leader I initial takes a random θI ← n and then sends θI|θI|I ton his neighbors. His neighbour i will be able to conjointly take θi ← and send θI|θi|i to his own neighbors. Generally, once a user j is initial contacted, he can take θj ← n and send θI|θj|j to his own neighbors. Here θI primarily plays as a world session symbol. The session between 2 neighboursi, j will be known victimization θI|θi|θj . In Stage one, the purpose is to execute the protocol Π genuinely. Specifically, if user i needs to send m to His θI permits neighbour j to j , notice he sends the session θI|m|sig tos i p(θrIocess|i|j|θ i the |θj|m message). Here andis authenticated: if sigsi (θIli|j|θi|θji lis corrupted, no security is possible;m) permits user j to ensure that m If i am uncorrupted, the recentness of j|θj (as user j chooses θj randomly) implies that the signature is fresh. In the remaining of this section, we are going to prove the safety of Πr . Toward this, we'd like to formally outline the session symbol. We tend to outline sidAi = ∪ atomic number 28 ∪ }. From our protocol description, i θI is well- outlined for ΠAi i to user i can begin with θI and can be directed to ΠAii with θI ∈ sidAi i (only one ΠAi i in user i with this property exists). This can be vital as we tend to should coordinate totally different neighbor instances with ΠAii . Finally, ∪ ⊆Ai i sidand Ai Π ∩ sidAj j areAj . Notedirectly that partnered a continual if i j θI can cause a user to unremarkably reject.

However, if a standard leader samples a continual θI , this happens with chance solely 2−n, which might be ignored; if associate assaulter reuses θI , the reject suggests that that the attack fails. The security plan of our construction is as follows. Essentially, we wish to argue that if Π is passively secure, then Πr is actively secure. Initial of all, in any execution of Π with all users uncorrupted, we will assume that users see the same θI which any 2 neighboursi, j see the same θi|θj. This is true as every message at Stage one in Πr is attended with a signature containing input θI|θi|θj|i|j. underneath this assumption, if there's associate soul Ar breaking Or , we tend to show a way to build associate soul A breaking Π. The strategy of A is to simulate the execution of Πr and run Ar against it. In turn, A mimics the action of Ar to attack Π. Specifically, whenever Ar requests a brand new execution of Or , A problems associate Execute question in Π and obtains a transcript tr. He tries to simulate or specified the transcript of Π in stage one in Πr is strictly If this can be true, the cluster key in Πr and also the cluster key in Π area unit identical. Thus A will break the privacy of Π if Ar will this for or. To insert try into or. The most tasks for A are to answer the Send queries from Ar for a Stage-1 message. To do this, every Send oracle generates the output θI|m|σ unremarkably except that the Π message m is taken from tr. Upon a question Send (j, Aj, θ∗|m|σ) from i, A verifies whether or not (σI∗ , σ, m) is consistentI along with his user Record (σI, θi, θj) and m in tr. If yes, it is assured that i and j area unit within the same session and m isn't modified. So again, A simulates the oracle output unremarkably except the Π message is taken from tr. If no, the attack of Ar is detected then A will safely reject. As a result, A can smoothly simulate a Πr execution for Ar and inherit his success. We tend to gift this formally within the following.

Theorem 5: Let Π be a passively (contributively) secure cluster key agreement with (P K , i SK i) = cypher. Assume that (sig, ver) is existentially unforgeable. Then, Πr is associate actively (contributively) secure cluster key agreement .Proof. We tend to prove that if there exists soul Ar that breaks the active security of Πr , then we tend to will construct soul A that breaks the passive security of Π. Upon parameter follows. He takes sp and the description of (v,s) unremarkably for G U , i A does. Then, as i every ∈ U he provides sp, GU

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

execution of Πr with Ar as follows. Initial of all, we tend to assume Ar ne'er makes associate Execute question as it is replaced a sequence of Send queries. Let the amount of initiating Send queries by Ar be finite by ν. Then, A takes t ← [ν]. Denote the tth initiation Send question by alphabetic character.

6. CONCLUSION

We studied a bunch key agreement draw back, where a user is simply aware of his neighbours whereas the connectivity graph is unfair. To boot, users square measure initialized absolutely freelance of each various. A bunch key agreement throughout this setting is implausibly applicable for applications like social networks. we've got an inclination to try to made a pair of passively secure protocols with contributiveness and verified lower bounds on a spherical quality, demonstrating that our protocols square measure spherical economical. Finally, we've got an inclination to try to make associate actively secure protocol from a passively secure one. In our work, we've got an inclination to did not take under consideration the thanks to update the cluster key further expeditiously than merely running the protocol over again, once user membership's square measure resurgent. We've got an inclination to are not clear the thanks to do this. One can either propose algorithms to our current protocols (as Dutta and Barua [22] did for [17]) or construct a really new key agreement with these choices. We've got an inclination to go away it as associate open question.

REFERENCES

[1] Christo Ananth, H.Anusuya Baby, "Encryption and Decryption in Complex Parallelism", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 3, March 2014,pp 790-795

[2]D. Augot, R. Bhaskar, V. Issarny and D. Sacchetti, "An economical cluster Key Agreement Protocol for unplanned Networks", Proc. sixth IEEE Int'l Symp. On a World of Wireless Mobile and transmission Networks (WOWMOM 2005), pp. 576-580, 2005.

[3]A. Beimel and B. Chor, "Communication in Key Distribution Schemes", Proc. Advances in science (CRYPTO'λ3), vol. 773, pp. 444-455, 1994.

[4]R. Blom, "An best class of symmetric Key Generation Systems", Proc. Advances in Cryptology-EUROCRYPT'κ4, vol. 20λ, pp. 335-338, 1984.

[5]D. Boneh and M. K. Franklin, "An economical Public-key Traitor Tracing Scheme", Proc. Advances in science (CRYPTO'λλ), vol. 1666, pp. 338-353, 1999.

[6]D. Boneh, C. upper crust and B. Waters, "Collusion Resistant Broad- solid cryptography with Short Ciphertexts and private Keys", Proc. Advances in science (CRYPTO'05), vol. 3621, pp.

[7]D. Boneh, A. Sahai and B. Waters, "Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and private Keys", Proc. twenty fifth Int'l Conf. Theory and Application of science Techniques (EUROCRYPT'06), vol. 4004, pp. 573-592, 2006.

[8]D. Boneh and M. Naor, "Traitor Tracing with Constant Size Ciphertext", Proc. fifteenth ACM Conf. portable computer and Comm. Security, pp. 501-510, 2008.

[9]D. Boneh and A. Silverberg, "Applications of Multilinear Forms to Cryptography", trendy arithmetic, Vol. 324, yank Mathematical Society, pp. 71-90, 2003.

[10]C. Blundo, L. A.Mattos and D. R. Stinson, "Generalized Beimel- Chor Schemes for Broadcast cryptography and Interactive Key Distribution", Theory. Comp.Sci., vol. 200, no. 1-2, pp. 313-334, 1998.

[11]C. Blundo and A. Cresti, "Space requirements for Broadcast Encryption", Proc. Advances in science - EUROCRYPT 1994, vol. 950, pp. 287-298, 1995.

[12]C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences", Inf. Compute., vol. 146, no. 1, pp. 1-23, 1998.

[13]C. Boyd and J. M. Gonza´lez-Nieto, "Round-Optimal Contribu- tory Conference Key Agreement", Proc. Public Key Cryptography (PKC'03), vol. 2567, pp. 161-174, 2003.

[14]E. Bresson, O. Chevassut and D. Pointcheval, "Provably Au- thenticated cluster Diffie-Hellman Key Exchange The Dynamic Case", Proc. seventh Int'l Conf. Theory and Application of science and information Security (ASIACRYPT'01), vol. 224κ, pp. 290-309, 20

[15]E. Bresson, O. Chevassut and D. Pointcheval, "Dynamic cluster DiffieHellman Key Exchange beneath commonplace Assumptions", Proc. 21th Int'l Conf.