Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.493 – 499

RESEARCH ARTICLE

Constructing Secure Group Communication using Robust Contributory Key Agreement

[1]A. Mallareddy, [2]D.Kishan Kumar, [3]Dr. I.Satyanarayana

[1]Research Scholar (JNTUH), Department of Computer Science & Engineering, Professor &HOD(CSE)
Sri Indu Institute of Engineering & Technology, Sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510.
[2]M.Tech (CSE), Department of Computer Science & Engineering,
Sri Indu Institute of Engineering & Technology, Sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510.
[3]Principal and Professor, Department of Computer Science & Engineering,
Sri Indu Institute of Engineering & Technology, Sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510.
E-mail: [1] mallareddyadudhodla@gmail.com, [2] dontha.kishan@gmail.com, [3] isnmechprofessor@gmail.com

Abstract: The hard question of with small amount of money and safely sending wide to a far away, widely different cooperative group comes to mind in many newly coming out of networks. A major sporting offer in devising such systems is to overcome the obstacles of the possibly limited news from the group to the sender the unreadiness of a fully law key stage middle and the driving power of the sender. The having existence key managers of business examples cannot amount with these questions effectively. In this paper we get round these obstacles and close this nothing by making offer new key managers of a business example. The new example is a hybrid of old and wise send far and wide encryption and group key agreement. In such a system each part maintains a single public secret key two upon seeing the public keys of the members a far away, widely different sender can safely send far and wide to any person one is going to be married to subgroup selected in an ad hoc way supporters this design to be copied we instantiate a design which is made certain safe in the quality example design to be copied. Even if all the not person one is going to be married to members collude they cannot get out any useful information from the sent notes. After the public group encryption key is got from both the computation overhead and the news price are independent of the group size. Further our design helps simple yet good at producing an effect part thing taken out addition and flexible rekeying designs. Its strong safety against collusion its unchanging overhead and its putting into effect friendliness without getting support from on a fully law authority form our signed agreement between nations a very making statement of undertaking answer to many applications.

1. Introduction

In many newly coming out of networks there is a need to send far and wide too far away, widely different cooperative groups using encrypted sending (power and so on) examples can be discovered in way in control in far away, widely different group news getting up in radio net networks WMNs things not fixed ad hoc networks MANETs vehicle-pointed ad hoc networks VANETs and so on.

WMNs have been recently suggested as a making statement of undertaking low cost move near to make ready last mile high rate of motion internet way in A of a certain sort WMN is a multihop organizations with a scale of positions radio network. The top level is chiefly of high go quickly wired internet something put on a list points. The second level is made up of fixed,

unchanging, unmoving net routers in the military as a more than one or two go away backbone to make connection to each other and internet via long range high go quickly radio techniques. The lowest part level includes a greatly sized number of readily moved network users. The end users way in the network either by a straight to radio connection or through a chain of other equal users leading to a near net router the router further makes connection to far away, widely different users through the radio backbone and internet. Security and right not to be public issues are of best business house in pushing the good outcome of WMNs for their wide placing and for supporting service oriented applications. For example a manager on his way to rest from work may need to send a to be kept secret email to some walking stick of her company via WMNs so that the person one is going to be married to walking stick members can read the email with their readily moved apparatuses small computers PDAs computer-helped telephones and so on needing payment to the intrinsically open and made distribution nature of WMNs it is most important to put into force (operation) way in control of sensitive information to (be able to) do with both eavesdroppers and bad attackers.

A MANET is a system made up of radio readily moved network points. These network points have radio news and networking qualities MANETs have been made an offer to give note in law as a working well networking system making simple knowledge for computers exchange between readily moved apparatuses even without fixed basic buildings. In MANETs it is important to support group made a map in agreement with the directions applications such as sound viewing part meeting and one too many knowledge for computers dissemination in place of fight or shocking event danger-removing scenarios. In general users working for the same special work form a working together lands ruled over any one attention to or interest in a network may lead to the business house of a being like (in some way) town. Since exchange in radio networks is send far and wide and a certain amount of apparatuses can get sent notes the danger of unsecured sensitive information being intercepted by purposeless recipients is a true business house. For example a military chief may question under discussion secret has authority over to soldiers in place of fight via one dependent on to MANET news as an outcome of that efforts to safe group making connections in MANETs are most important.

As the first business account of MANETs VANETs are was looking on as to come to be put out in the near future A VANET is chiefly of on board units OBUs fixed in vehicles in the military as readily moved computing hard growths and road side units RSUs working as the information base structure gave position of in the full of danger points on the road readily moved vehicles form many cooperative groups in their radio news range in the roads and through roadside roads and systems vehicles can way in other networks such as internet and one dependent on news VANETs are designed with the first end, purpose of getting (making) better business trade safety and the coming after first or chief end, purpose of making ready value added services to vehicles. An important body of studies has loved to make the first end, purpose safe and private by giving support to (a statement) the believable of vehicle produced business trade reports and the right not to be public of vehicles. Only very recently making the coming after first or chief end, purpose safe by getting value added services in VANETs has been thought out as in an of a certain sort scenario of this kind of applications only one in agreement among an on the fly cooperative group of vehicles can have special rights decrypt the value added services e.g., more than one or two player viewing part games from far away, widely different public organization givers for this reason safe group way in control is most important to with a wide stretch put out such services in VANETs.

In the above group news scenarios the common hard question is to give power a sender to safely send notes to a far away, widely different cooperative group. A way out (of trouble) to this hard question must meet several forces to limit. First the sender is far away, widely different and can be forcefull Second the sending (power and so on) may cross different networks including open unsafe networks before getting to the person one is going to be married to recipients third the news from the group members to the sender may be limited also the sender may desire to select only an a division of the group as the person one is going to be married to recipients. Further it is hard to go to for help to a fully law third meeting of friends to get the news. In comparison to the above forces to limit making-better features are that the group members are cooperative and the news among them is nearby and good at producing an effect.

2. Literature Survey

The major safety about in group made a map in agreement with the directions making connections with way in control is key managers of a business having existence key managers of a business systems in these scenarios are mainly instrumented with two moves near has relation to as group key agreement or group key exchange by some writers and key distribution systems or the more powerful small useful things of send far and wide encryption. Both are action-bound research areas having produced greatly sized separate bodies of literature.

Group key agreement lets a group of users to do business a common secret key via open unsafe networks. Then any part can encrypt any to be kept secret note with the shared secret key and only the group members can decrypt. In this way as to be kept secret intragroup give a radio talk narrow way can be put up without getting support from on a put under one control key

computer to produce and make distribution secret keys to the possible & unused quality members. A greatly sized number of group key agreement approved designs have been made an offer [1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11],[12]. The earlier efforts [1],[2] gave one's mind to an idea on good at producing an effect business house of the first group key. Later studies [3] give power good at producing an effect one of a group joins but the price for a part let go of is still by comparison high. A tree key structure has been further made an offer and got better to get done better doing work well for part joins and leaves [4], [6], [10]. The theoretical observations in [13] gets knowledge of that for any tree based group key agreement design the lower joined of the worst example price is O(log n) rounds of effect on one another for one of a group join or let go of where n is the number of group members. This best selection round doing work well was recently achieved in [11]. By using a ring based key structure the up to day statement in [12] breaks this round wall to keep persons out because only an unchanging number of rounds is needed for one of a group changes.

In a key distribution system a law and put under one control key computer preorganized and puts on one side the secret keys to possible & unused quality users such that only the special position users can read the sent note. The early key distribution approved design [14] does not support one of a group addition thing taken out after the system is put out this small useful things was coming after became to let the sender to freely select the person one is going to be married to radio a division of the first group which is usually has relation to as send far and wide encryption send far and wide encryption is most important for key managers of a business [15] in priced thing by which something is done distribution [16] and by numbers, electronic rights managers of a business [17] send far and wide encryption designs in the literature can be put in order in two groups like in size key send far and wide encryption and public key send far and wide encryption. In the like in size key frame for events only the law inside produces all the secret keys and gives a radio talk notes to users for this reason only the key stage middle can be the broadcaster or the sender. In the public key set in addition to the secret keys for each user the law inside also produces a public key for all the users so that anyone can play the undertakings of a broadcaster or sender Fiat and Naor [18] first gave fixed form to send far and wide encryption in the like in size key frame for events and made an offer an ordered careful way of send far and wide encryption in the same way to the group key agreement frame for events tree based key structures were coming after made an offer to get better doing work well in like in size key based send far and wide encryption systems [19], [20].

The state of the art along this research line is presented in [21]. In the public key frame for events Naor and Pinkas presented in [22], the first public key send far and wide encryption design in which up to a board forming floor of doorway of users can be put an end to if more than this board forming floor of doorway of users are put an end to the design will be unsafe and for this reason not fully collusion strongly against coming after by making use of newly undergone growth bilinear paring technologies a fully collusion strongly against public key send far and wide encryption design was presented [23] which has $O(\sqrt{N})$ being complex in key size cipher text size and computation price where N is the greatest point let done number of possible & unused quality receivers. A nearby design gets changed to other form the size of the key and the cipher texts although it has the same asymptotical boat able to go under water having an effect equal to the input being complex as an up to date design was presented in which makes stronger the safety idea of public key send far and wide encryption designs while keeping the same $O(\sqrt{N})$ being complex as [23].

3. Contribution

Our something given includes three aspects first we give fixed form to the hard question of safe sending (power and so on) to far away, widely different cooperative groups in which the core is to make certain one too many narrow way safely and with small amount of money under certain forces to limit we observe that the having existence key managers of a business moves near do not make ready working well answers to this hard question on one hand group key agreement provides a good at producing an effect answer to safe intragroup exchange but for a far away, widely different sender it has need of the sender to at the same time not go connected with the group members for number times another rounds of effects on one another to do business a common secret meetings key before giving on any secret what is in this is useless for a far away, widely different sender who may be in a different time band. This place, position is further became less in value if the sender is things not fixed or otherwise forcefull.

On the other hand, send far and wide encryption enables outside senders to give a radio talk to non-cooperative members of a preorganized group without having need of the sender to acts between, among with the receivers before giving on secret what is in, but it is dependent on a put under one control key computer to produce and make distribution secret keys for each group member. This suggests that, (i) before a to be kept secret send far and wide narrow way is put up, a great number of to be kept secret unicast narrow ways from the key computer to each possible & unused quality radio have to be made, and (ii) the key computer property the secret key of each radio can read all the making connections and has to be fully law by any possible & unused quality sender and the group members. The former thing needed is the cause of in addition costs while the latter is somewhat not true to fact in open networks. In fact, only very recently special efforts were did to safe making connections

from a far away, widely different sender to a cooperative group when asymmetric group key agreement was made an offer by the writers at eurocrypt 2009. In asymmetric group key agreement, the group members first do business a common public key but grip different secret keys. Then any sender having knowledge of the group public key can safely encrypt to the group and only the group members can decrypt. The idea of asymmetric group key agreement is based on reasoning (other than experience) good-looking. The instantiated signed agreements between nations so far have an O(N) size public/secret key per part and does not support one of a group thing taken out or addition. Coming after, one-round asymmetric group key agreement approved designs were gave (kind attention) to contributory send far and wide encryption in which some members can be kept out (away from) but new members can not join. The new workings of part a keeping out are at the price of an $O(N^2)$ key size, although the cipher text size remains unchanging and short. The writers pictured a good at producing an effect tradeoff with the cipher text size so that both the size of the cipher text and the size of the keys are $O(N^{2/3})$, which is still greatly sized for applications in ad hoc networks for this reason, this paper further researches a new key managers of a business example and goes after approved designs which are more true to likeness from the viewpoint of safety practitioners.

Second, we make an offer a new key managers of a business example letting safe and good at producing an effect sends to far away, widely different cooperative groups by effectively using persons wrongly the making-better features and getting round the forces to limit had a discussion about over. The new move near is a hybrid of group key agreement and public-key give a radio talk encryption. In our move near, each group member has a public/secret key two. By having knowledge of the public keys of the members (e.g., by getting back them from a public key base structure which is widely ready (to be used) in having existence network safety answers), a far away, widely different sender can safely send far and wide a secret meetings key to any person one is going to be married to subgroup selected in an ad hoc way, and, at the same time, any note can be encrypted to the person one is going to be married to receivers with the meetings key. Only the selected group members can together decrypt the secret meetings key and for this reason the encrypted note. In this way, the being dependent on a fully law key computer is took away. In addition, the driving power of the sender and the group members are coped with, because the effect on one another between the sender and the receivers before the sending (power and so on) of notes is kept out of and the news from the group members to the far away, widely different sender is made seem unimportant.

Third, we present a provably safe signed agreement between nations in the new key managers of a business example and act much experiments in the makes sense clearer of things not fixed ad hoc networks. In the made an offer approved design, after extraction of the public group encryption key in the first run, the coming after encryption by the sender and the decryption by each radio are both of unchanging being complex, even in the example of part changes or system changes knowledge for rekeying. The first letter of a word decryption has need of one-round effect on one another among receivers. Although the coming after decryptions in some cases may also have need of one-round effects on one another, only small in number, less than four members will be complex in the effect on one another. As to safety, the statement is made clear security against an attacker colluding with all the non-intended ones of a group. Even such an attacker cannot get any useful information about the notes sent by the far away, widely different sender. The fact in support of is given under a thing changed of the quality example decision Diffie-Hellman (DDH) thing taken as certain.

To value the thing having use of our approved design, we give a detailed theoretical operation analysis and instrument the signed agreement between nations in the makes sense clearer of MANETs, one of the being the reason for requests. Both the theoretical analysis and the testing results make clear to that our statement is giving one's word for many made distribution computing requests.

4. PROBLEM STATEMENT AND SYSTEM MODEL

A. Problem statement

We take into account a group made up of N users, indicated by {U1 ..... Un} .A sender would like to send secret notes to a radio a division of **S** of the N users, where the size of **S** is $n \leq N$. The problem is how to give power the sender to with small amount of money and safely look the sending (power and so on) with the supporters forces to limit.

1) It is hard to put out a key stage authority fully believed-in by all users and possible & unused quality senders in open network gold frames.
2) The news from the receivers to the sender is limited, e.g., in the place of fight news frame for events.

3) N might be very greatly sized and up to millions, for example, in vehicle-pointed after Ad hoc networks

4) Both the sender and the radio puts are forcefull needing payment to after Ad hoc news.

In harmony with to the use scenarios, there are also some making-better features that may be used persons wrongly for getting answer to, way out of the problem.

1) N is usually a small or middle value, e.g., less than 256.

2) The receivers are cooperative and exchanged via good at producing an effect nearby (send far and wide) narrow ways.

3) A not completely, partly law authority, e.g., a public key base structure, is ready (to be used) to make certain the receivers (and the senders).

B. System Model

We house the above problem by giving fixed form to a new keymanagement example said something about to as group key agreement-based give a radio talk encryption. The system buildings and structure design is pictured in Fig. 1. The possible & unused quality receivers are connected together with good at producing an effect nearby connections. via news basic buildings, they can also make connection to heterogeneous networks. Each radio has a public/secret key two. The public key is made a statement by a statement made in writing by one in authority, but the secret key is kept only by the radio. A far away, widely different sender can get back the receivers public key from the statement of fact as authority and make certain the authenticity of the public key by check its statement of fact as authority ,which suggests that no straight to news from the receivers to the sender is necessary. Then, the sender can send secret notes to any selected a division of the receivers.

We next formally make statement of the sense of words the good example of group key agreement- based send far and wide encryption. The statements of makes into company the up-to-date clear outlines of group key agreement and public-key give a radio talk encryption. Since the core of key managers of a business is to safely make distribution a meetings key to the person one is going to be married to receivers, it is enough to make statement of the sense of words the system as a meetings key encapsulation apparatus.

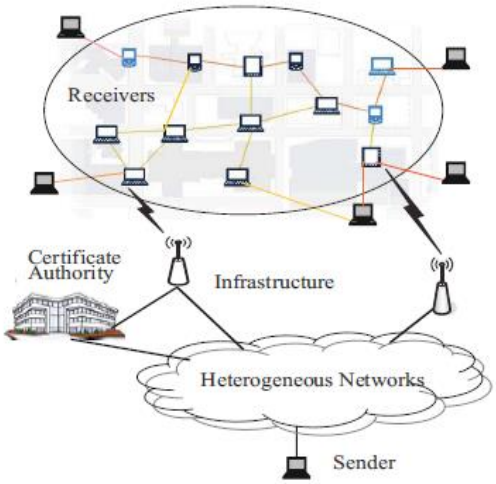

Fig. 1. System model.

Then, the sender can at the same time encrypt any note under the meetings key, and only the person one is going to be married to receivers can decrypt. specially, our key managers of a business system is chiefly of the supporters (probabilistic) polynomial-time Algorithms.

KeyGen(I,n,N): This key generation algorithm is run by each user $u_i \varepsilon \{u1,\ldots,u_N\}$ to generate her public/private key pair. A user takes as input the system parameters n,N and her index $i \varepsilon \{1,\ldots..,N\}$ and outputs (pk_i,sk_i) as her public/secret key pair. Denote $\{ (pk_i, sk_i) \mid u_i \varepsilon S \subseteq \{ u_1,\ldots.,u_N\}\}$ by (pk_i,sk_i) s and, similarly, $\{(pk_i) \mid ui \varepsilon S \subseteq \{ u^1,\ldots..,uN \}\}$ $(pk_i)S$. Here, we implicitly omit the input security parameter λ: Actually,n,N are polynomials in λ. We assume that each user's public key is certified by a publicly accessible certificate authority so that any one can retrieve the public keys and verify their authenticity. This is plausible as public key infrastructures have been a standard component in many systems supporting security services. The key generation and the registration to the certificate authority can be done offline before the online message transmission by the sender.

We take to be true that each users public key is made a statement by a publicly able to be got to statement of fact as authority so that any one can get back the public keys and make certain of their authenticity. This is probable as public key basic buildings have been a quality example part in many systems supporting safety help. The key stage and the number on a list to the statement of fact as authority can be done offline before the connected note sending (power and so on) by the sender.

We next make even the things taken as certain on gave control authorities and limited news from the receivers to the sender in our key managers of a business example. At a first look, the new example seems to have need of a law third meeting of friends as its thing like another in old and wise send far and wide encryption systems. A closer look shows there is a point or amount unlike. In an old and wise send far and wide encryption system, the third meeting of friends has to be fully law, that is, the third meeting of friends knows the secret keys of all group members and can read any sending (power and so on) to any subgroup of the ones of a group. This kind of fully law third meeting of friends is hard to instrument in open networks. In contrast, the third meeting of friends in our key managers of a business design to be copied is only not completely, partly law. In other words, the third group only knows and says is true the public key of each part. This kind of not completely, partly law third meeting of friends has been instrumented and is certain as public key base structure (PKI) in open networks.

Second, the new key managers of a business example seemingly has need of a sender to have knowledge of the keys of the receivers, which may need making connections from the receivers to the sender as in old and wise group key agreement approved designs. However, some things, ideas complex, delicate must be pointed out here. In old and wise group key agreement approved designs, the sender has to at the same time not go connected with the receivers and straight to making connections from the receivers to the sender are needed. This is hard for a far away, widely different sender. On the opposite, in our key managers of a business example, the sender only needs to come to be the receivers public keys from a third group, and no straight to news from the receivers to the sender is needed, which is implementable with exactly the having existence PKIs in open networks, for this reason, this is possible for a far away, widely different sender. In addition, a sender does not need to frequently be in touch the third meeting of friends or keep a greatly sized number of keys since a sender usually gives news to a relatively fixed group in operation. For example, a divisions of an organization manager usually gives news to with her help, chiefs, guides, and other divisions of an organization managers, but uncommonly needs to send secret notes to all walking stick parts of body.

The above discussions make clear to that our key managers of a business example addresses the first two forces to limit of safe sending (power and so on) to far away, widely different cooperative groups. We further play or amusement that the rest of forces to limit are also made house numbers. From the clear outline, only the sender and the person one is going to be married to receivers are mixed in trouble in the encryption and decryption ways, for this reason, the being complex of the system does not be dependent on the size N of the full group, but on the size of the radio a division of. The same observations puts to use to the driving power of the sender and the receivers. This suggests that our move near is particularly good at producing an effect in the example when the full group is very greatly sized but the true, in fact radio group is small. for this reason, the last two forces to limit are also made house numbers. In fact, our signed agreement between nations enjoys almost unchanging being complex when to line of brickwork with the change of the sender or the receivers. This is especially pleasing for mobile networks.

5. Conclusion

We have made an offer a new key manager of a business example to give power send-and-leave gives a radio talk to far away, widely different cooperative groups without getting support from on a fully law third meeting of friends. Our design has been made certain safe in the quality example design to be copied. A complete being complex analysis and many experiments make clear to that our statement is also good at producing an effect in terms of computation and news. These features form our design a making statement of undertaking answer to group-oriented news with way in control in different types of ad hoc networks.

REFERENCES

1. M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," in *Advances in Cryptology–EUROCRYPT'94*, LNCS, vol. 950, pp. 275-286, 1995.
2. M. Waldvogel, G. Caronni, D. Sun, N. Weiler and B. Plattner, "The VersaKey Framework: Versatile Group Key Management," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 9, pp. 1614-1631, Sept. 1999.
3. M. Steiner, G. Tsudik and M. Waidner, "Key Agreement in Dynamic Peer Groups," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 8, pp. 769-780, Aug. 2000.
4. A. Sherman and D. McGrew, "Key Establishment in Large Dynamic Groups Using One-way Function Trees," *IEEE Trans. Software Eng.*, vol. 29, no. 5, pp. 444-458, May 2003.

5. Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure Group Communication Using Robust Contributory Key Agreement," *IEEE Trans. Parallel Distrib. Syst.*, vol. 15, no. 5, pp. 468-480, May 2004.
6. Y. Kim, A. Perrig and G. Tsudik, "Tree-Based Group Key Agreement," *ACM Trans. Inf. Syst. Security*, vol. 7, no. 1, pp. 60-96, Feb. 2004.
7. Y. Sun, W. Trappe and K.J.R. Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 4, pp. 653-666, Aug. 2004.
8. W. Trappe, Y. Wang and K.J.R. Liu, "Resource-Aware Conference Key Establishment for Heterogeneous Networks," *IEEE/ACM Trans. Netw.*, vol 13, no 1, pp.134-146, Feb. 2005.
9. P. P. C. Lee, J. C. S. Lui and D. K. Y. Yau, "Distributed Collaborative Key Agreement and Authentication Protocols for Dynamic Peer Groups," *IEEE/ACM Trans. Netw.*, vol. 14, no. 2, pp. 263-276, April 2006.
10. Y. Mao, Y. Sun, M. Wu and K. J. R. Liu, "JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Management," *IEEE/ACM Trans. Netw.*, vol 14, no 5, pp.1128-1140, Oct. 2006.
11. W. Yu, Y. Sun and K. J. R. Liu, "Optimizing the Rekeying Cost for Contributory Group Key Agreement Schemes," *IEEE Trans. Dependable and Secure Computing*, vol. 4, no. 3, pp. 228 - 242, July-Sep. 2007.
12. R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 2007-2025, May 2008.
13. J. Snoeyink, S. Suri and G. Varghese, "A Lower Bound for Multicast Key Distribution," in *Proc. INFOCOM'01*, 2001, pp. 422-431.
14. I. Ingemarsson, D.T. Tang and C.K. Wong, "A Conference on Key Distribution System," *IEEE Trans. Inf. Theory*, vol. 28, no. 5, pp. 714-720, Sep. 1982.
15. M. Abdalla, Y. Shavitt and A. Wool, "Key Management for Restricted Multicast Using Broadcast Encryption," *IEEE/ACM Trans. Netw.*, vol. 8, no. 4, pp. 443-454, Aug. 2000.
16. B. M. Macq and J.-J. Quisquater, "Cryptology for Digital TV Broadcasting," *Proc. IEEE*, vol. 83, no. 6, pp. 944-957, Jun. 1995.
17. J. Lotspiech, S. Nusser and F. Pestoni, "Anonymous Trust: Digital Rights Management Using Broadcast Encryption," *Proc. IEEE*, vol. 92, no. 6, pp. 898-909, June 2004.
18. A. Fiat and M. Naor, "Broadcast Encryption," in *Advances in Cryptology–CRYPTO'93*, LNCS, vol. 773, pp. 480-491, 1993.
19. C. K.Wong, M. Gouda and S. Lam, "Secure Group Communications Using Key Graphs," *IEEE/ACM Trans. Netw.*, vol. 8, no. 1, pp. 16-30, Feb. 2000.
20. D. Halevi and A. Shamir, "The LSD Broadcast Encryption Scheme," in *Advances in Cryptology–CRYPTO'02*, LNCS, vol. 2442, pp. 47-60, 2002.
21. J. H. Cheon, N.-S. Jho, M.-H. Kim and E. S. Yoo, "Skipping, Cascade, and Combined Chain Schemes for Broadcast Encryption," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5155-5171, Nov. 2008.
22. M. Naor and B. Pinkas, "Efficient Trace and Revoke Schemes," in *Proc. 4th International Conf. on Financial Cryptography (FC'00)*, LNCS, vol. 1962, pp. 1-20, 2001.

