A New Scheme for Anonymous Secure Group Communication

Xukai Zou, Mingrui Qi, and Yan Sui
Computer and Information Science Department
Indiana University Purdue University at Indianapolis
Indianapolis IN 46202, USA
Email:{xkzou,qim,ysui}@cs.iupui.edu
Feng Li
Computer and Information Technology Department
Indiana University Purdue University at Indianapolis
Indianapolis IN 46202, USA
Email:fengli@iupui.edu

***Abstract*— Anonymity is an important feature in many two party communication systems. Its main meaning is that either the message sender or the receiver (or both) is unidentifiable to other users, even between themselves. Many mechanisms have been proposed to hide the identity of the sender, receiver, or both. Similarly, anonymity is an important feature in multi-party computing environments, but, little research has been conducted on this topic even though many secure group communication schemes have been proposed. In this paper, we highlight the concepts of anonymity for secure group communication and propose to extend a recently invented innovative group key management mechanism, Access Control Polynomial [1], to multiple-party group communication. This newly extended scheme can not only enforce anonymous group membership and group size but also implement secure and anonymous group communication. The experimental results and comparison with existing schemes show that the new scheme is elegant, flexible, efficient and practical. The paper also summarizes and classifies typical existing anonymous group communication schemes.**

Keywords: Secure Group Communication (SGC), Anonymity, Anonymous Secure Group Communication, Secret set, Access Control Polynomial (ACP).

I. Introduction

With the rapid growth and public acceptance of the Internet as a means of communication and information dissemination, concerns about privacy and censorship on the Internet have correspondingly grown. Anonymous communication is critical for protecting the identity of participants in many Internet applications, such as private e-Commerce, anonymous bulletin boards, online trading [2]. Anonymity is commonly defined as ensuring that a user may use a resource or service without disclosing his/her identity [3]. Imagine Alice wants to send a message to Bob, but does not want anyone including Bob himself to know who sent it. Imagine Bob wants to receive messages, but does not want anyone including Alice to know he received it. This requirement for anonymity can provide protection of a user's identity. This is particularly important in applications such as E-voting [4].

Traditionally, the research on anonymity has been focused on two-party communication. Further, three typical anonymities have been extensively studied: sender anonymity, receiver anonymity, and relationship anonymity (also called unlinkability). Such studies are lacking, however, in that anonymity is not only an issue in two-party communication environments, but also in multi-party computing environments where secure group communication (SGC) and selective differentiated access to data among multiple entities are two fundamental security functions [5]. In such an environment, hiding group membership and group size are important anonymous features. Such group-oriented anonymity issues in SGC have not, to date, obtained much investigation even though the group key management issue for SGC has been extensively explored [6], [7], [8], [9], [10].

In this paper, we extend our newly invented Access Control Polynomial (ACP) mechanism [1] to multi-party anonymous communication. This newly extended scheme can enforce anonymous group membership and group size, while at the same time realize secure and anonymous group communication. The experimental results and comparison with existing schemes show that the new scheme is elegant, flexible, efficient and practical. The paper also highlights the concepts of anonymity for secure group communication and summarizes and classifies typical existing anonymous group communication schemes.

The remainder of this paper is organized as follows. Section II gives definitions for different anonymities and summarizes related work on anonymity in both two-party communication and multi-party communication. Section III describes Secure Lock and Secret Set in multi-party communication in detail. Our ACP based anonymity scheme is proposed in Section IV. The comparison of the ACP based scheme with typical existing schemes is presented in Section V, which also includes some experimental results. Finally, we conclude the paper and discuss the future work in Section VI.

II. Definitions and Related work

In this section, we first summarize some definitions of anonymity for two-party communication which have appeared in literature. Then, we define anonymity in group communication.

Definition 2.1: Sender Anonymity: A particular message is not linkable to any sender and no message is vice versa linkable to a particular sender [11].

Definition 2.2: Receiver/recipient Anonymity: A certain message cannot be linked to any recipient and that no message is linkable to a particular recipient [11].

Compared with sender anonymity, receiver anonymity is easier to achieve [12]. Many more protocols satisfying the requirement of receiver anonymity are discussed than those of sender anonymity.

Definition 2.3: Unlinkability/Relationship Anonymity: The sender and the recipient cannot be identified as communicating with each other, though it may be clear they are participating in some form of communication [11].

Besides the above three forms of anonymity, other forms have also been studied, such as Node Anonymity [12], Proxy Anonymity [13], [14], [12], Unobservability [11], Full/Complete/Unconditional anonymity [15], [16], Computational anonymity [17], Provable anonymity [18], Pseudo-anonymity [15], and K-Anonymity [19], [20], [21]. Many mechanisms to implement different anonymities have also been proposed, such as Proxy Service [22], Mixnet [23], Remailers [24], [25], [26], [27], Anonymizer[13], Babel [28], TAZ / Rewebber [29], Onion Routing [30], Crowds [31], and Freedom Network [32], MASK [33], Dining Cryptographers [34], Identity Escrow [35], P-signatures [36], and K-Anonymous System [20], [37], [38], [39]. A recent survey on (two-party) anonymity can be found in [40].

In group communication scenarios, every member in the group is, in general, a sender and also a receiver (for the messages targeted at the group). Thus, anonymity in such a setting takes on different meanings and moreover poses different challenges in terms of implementation and applications. We define the following group communication anonymities.

Definition 2.4: Group Membership Anonymity: For a given set of all potential group members, any member can test their own membership in the set. Apart from the group manager, no one member can test another's membership in the set.

More strict definition requires that exactly no one be able to test another's membership [39].

Definition 2.5: Group Size Anonymity: For a given set of all potential group members, except for the group manager, no one can determine the exact number of members in the set.

In [41], the authors proposed the concept of Secret Set where for a given set of all potential group members, any member can test its membership in the set but can determine neither the other set members nor the cardinality of the set[1].

As is evident, Secret Set is thus equivalent to group membership anonymity plus group size anonymity.

Definition 2.6: Anonymous secure group communication: For a given set of all potential group members, any member can test their membership but cannot determine the membership of other members nor the size of the set. In addition, non-set member cannot understand the communication among the set members.

Secure lock [43] was the first anonymous secure group communication scheme developed but it suffers from an efficiency problem (See Section V for its efficiency analysis). In paper [44], a Secure Anonymous Group Infrastructure (called Secure and Anonymous multicast SAM) was proposed. In SAM, there are multiple SAM servers: any group participant joins a SAM server and remains anonymous to outsiders and also to other participants belonging to other SAM servers. The multicast messages are transmitted to SAM servers, which then deliver the messages to their own participants. Several secret set schemes have been proposed such as in [41], [45].

In papers [46], [47], [48], the concept of anonymous membership broadcasting (AMB) was introduced. In AMB, given a set of receivers, a sender broadcasts the secret identity of a receiver in such a way that only the right receiver can determine that he is in fact the intended receiver, while the others cannot [46]. Furthermore, a w-anonymous membership broadcast (w-AMB) is defined as any coalition of at most w users, excluding the intended receiver, has no information about the identity of the intended receiver [47]. The Cover-Free based AMB scheme proposed in [46] is a 1-ABM scheme and papers [47], [48] proposed several w-AMB schemes (where w is a system parameter and chosen during system setup). As can be observed, AMB (or w-AMB) is a specific case of secret set.

To give a flavor of group-oriented anonymity and its implementation mechanisms, we briefly introduce two typical group-oriented anonymous schemes in the following section.

III. Secure Lock and Secret set

A. Secure Lock

Secure Lock was proposed in [43]. This lock is, in fact, a single value computed from the multiple encrypted keys using the Chinese Remainder Theorem (CRT). The Secure Lock scheme works as follows: Suppose each member m_i in the universal group G has its public and private key pair (P_i, S_i). A central entity (e.g. a server) determines a sequence of $n = |G|$ pairwise relatively prime numbers $N_1, \cdots, N_n$. These numbers are assigned to group members $m_1, \cdots, m_n$ respectively. All the N_i are made public. When a group of members $\S = \{m_{i_1}, \cdots, m_{i_\ell}\}$ wants to form an anonymous

[1]Another concept related to secret set is *secure set membership*, which means that a participant holding set elements can create a representation of its set to prove knowledge of set elements to others [42]. Based on the NP-complete problem 3SAT, the authors in [42] proposed a cryptographic primitive for the secure set membership problem.

secure communicating group, the central server selects a random key k and first establishes the following congruences[2]:

$$\begin{aligned} Ł &\equiv E_{P_{i_1}}(k)\ (mod\ N_{i_1}) \\ &\vdots \\ Ł &\equiv E_{P_{i_\ell}}(k)\ (mod\ N_{i_\ell}) \end{aligned} \tag{3.1}$$

Then, the server computes Ł by applying the CRT. Integer Ł will be the lock for the encrypted keys $E_{P_{i_j}}(k)$, and is sent along with the random key k as $(Ł, \{k\}_k)$[3]. When a receiver, such as m_{i_j}, receives the above packet, he/she can compute $E_{P_{i_j}}(k)$= Ł $\bmod N_{i_j}$, then obtains $k = D_{S_{i_j}}(E_{P_{i_j}}(k))$ using his/her private key, and finally decrypts the random key k using k. If the decryption discloses k, then m_{i_j} knows that he is in the group and the group key is k. Otherwise, the member is not in the group (or the message was altered). Once group members get to know they are in the group and get the group key k, they can perform group communication which is securely protected by the group key k

It is clear that the CRT value Ł hides group membership, in addition, by introducing *decoys* (i.e., some additional random congruences) in EQ (3.1)), the group size is hidden. Here "group size" means exact size; the attacker will actually know the upper bound of the group size.

Due to the involvement of public key systems and the Chinese Remainder Theorem, the secure lock scheme is inefficient and not scalable.

B. Secret Set

Molva and Tsudik defined secret set as a group of members in which any user can test their membership in the group but can determine neither the other group members nor the size of the group. Secret set provides a fundamental structure for mutually suspicious entity group communication [41]. Further studies of secret sets can be found in [45]. We briefly introduce secret set techniques below.

- Public key based technique [41]. Assume each member m_i has its public and private key pair (P_i, S_i). A secret set §=$\{m_{i_1}, \cdots, m_{i_\ell}\}$ can be constructed by creating and broadcasting the following membership representation message: $P_{i_1}(txt_{i_1}), P_{i_2}(txt_{i_2}), \cdots, P_{i_\ell}(txt_{i_\ell})$, where txt_{i_j} denotes some unambiguous indication that m_{i_j} is a member of the secret set.
- Secret key based technique [41]. Assume each member m_i has a shared secret key s_i with the central server. A secret set §=$\{m_{i_1}, \cdots, m_{i_\ell}\}$ can be constructed by creating and broadcasting the following membership representation message: $s_{i_1}(txt_{i_1}), s_{i_2}(txt_{i_2}), \cdots, s_{i_\ell}(txt_{i_\ell})$.
- Chinese Remainder Theorem based technique [41]. The above two methods have drawbacks in that the size of secret set can be exposed and a member in the secret set needs to perform multiple decryptions to know he is in the secret set and the non-member needs to perform m decryptions to know he is not in the secret set. The following Chinese Remainder Theorem based technique will solve this problem[4]. Assume that each member m_i is assigned a public number N_i which is relatively prime to all other N_j, $DP_1, DP_2, \cdots, DP_w$ are decoyed public keys, and $DN_1, DN_2, \cdots, DN_w$ are decoyed random numbers and are relatively prime to all N_i. A secret set §=$\{m_{i_1}, \cdots, m_{i_\ell}\}$ can be constructed by computing s using the CRT and broadcasting s as membership representation.

$$\begin{aligned} s &\equiv E_{P_{i_1}}(k)\ (mod\ N_{i_1}) \\ &\vdots \\ s &\equiv E_{P_{i_\ell}}(k)\ (mod\ N_{i_\ell}) \\ s &\equiv E_{DP_1}(k)\ (mod\ DN_1) \\ &\vdots \\ s &\equiv E_{DP_l}(k)\ (mod\ DN_l) \end{aligned} \tag{3.2}$$

- Bit vector [41]. The binary vector is an optimal representation of secret set. Assuming the total number of members is n, the bit vector will also have n bits. Suppose each member m_i has a Diffie-Hellman public exponent g^{a_i} and the central server has its Diffie-Hellman public exponent g^c. Then the secret set can be constructed by setting the ith bit of the bit vector to:
  $MEMBER(m_i) = MSB(g^{ca_i})$, if $m_i \in$ secret set
  $MSB(g^{ca_i}) \oplus 1$, otherwise.
  where $MSB(y)$ denotes the leftmost (most significant) bit of y.
  If, instead of Diffie-Hellman public exponent, each member m_i has a shared secret key S_i with the central server, then the bit vector will be:
  $MEMBER(m_i) = MSB(S_i)$, if $m_i \in$ secret set
  $MSB(S_i) \oplus 1$, otherwise.
- Addition based technique [45]. The authors of paper [45] proposed an addition based secret set technique. Similar to the above techniques, each member m_i is assigned a secret key S_i ($\leq q$, $q \geq 2$ is a natural number). For a secret set §, the central server computes the membership representation message $t_1, t_2, \cdots, t_n$ where $t_i \leq q$, computes $r_i = S_i + t_i \bmod q$, $(i = 1, 2, \cdots, n)$ and delivers the secret set representation $r = (r_1, r_2, \cdots, r_n)$ to all members.

IV. ACP based anonymous secure group communication scheme

As can be seen from the above descriptions, secure lock implements anonymous secure group communication, but it is inefficient. SAM tries to provide an architecture for

[2] $E_{P_i}(x)$ (or $D_{S_i}(x)$) denotes encrypting (or decrypting) value x using public key encryption (or decryption) algorithm under public key P_i (or private key S_i)

[3] $\{x\}_k$ denotes encrypting x using some symmetric encryption algorithm under key k

[4] The public key encryption can be replaced by secret key encryption if pairwise shared secret keys are assumed.

anonymous secure group communication, but fails in providing rigorous anonymity. Secret set schemes can implement anonymous group membership and group size, but cannot support secure group communication. In this section, we first introduce an innovative construction of an Access Control Polynomial (ACP), recently published in INFOCOM 2008 [1]. Then we extend the ACP mechanism to anonymous multiple party communication, which enforces both anonymous group (membership and size) and secure communication among the members of the anonymous group.

A. Access Control Polynomial [1]

As in the above secret key based secret set scheme, we assume that every valid member m_i in the system is assigned a secret key S_i (a random positive integer less than *q*). This secret is only known to the member and the central server. We also assume that *q* is a large prime from which a finite field F_q is formed and $f : \{0,1\}^* \rightarrow \{0,1\}^\ell$ (where $\ell = \lceil log(q) \rceil$) is a cryptographic hash function.

An *access control polynomial* (ACP) is a polynomial over $F_q[x]$ and defined as follows.

$$A(x) = \prod_{i \in \S} (x - f(S_i, z)) \tag{4.3}$$

where $\S$ denotes the secret set under consideration and z is a random integer from F_q and made public. In addition, z is changed every time *A*(*x*) is computed. It is evident that $A(x)$ is equated to 0 when x is substituted with $f(S_i, z)$ by a valid user with S_i in set $\S$; otherwise, $A(x)$ is a random value if other numbers or invalid users' secret keys are used in the substitution.

B. Extension of ACP to anonymous secure group communication

We extend the ACP mechanism by simply introducing *decoys* in access control polynomial $A(x)$.

In order to transmit the information about the membership of the secret set $\S$ and a secret key K used by the secret set, the central server computes and broadcasts the following information: $(z, P(x), \{K\}_K)$ where

$$P(x) \ = A(x)(x - D_1)(x - D_2) \cdots (x - D_w) + K \tag{4.4}$$

In EQ (4.4), $D_1, D_2, \cdots, D_w$ are *decoys*, and K is hidden, mixed with the constant of $A(x)$. From this public information, any secret member m_i with S_i can obtain the secret key *K*, by:

$$K \ = \ P(f(S_i, z)) \tag{4.5}$$

and verify both K and its membership by decrypting $\{K\}_K$ to disclose K. However, outsiders or non secret set members will get a random value other than K if they substitute an invalid S_j in EQ (4.5). Once the secret set members get K, they can conduct secure group communication by encrypting/decrypting their communications with K.

As a result, the new scheme guarantees:

- a secret set member can determine his/her membership in the secret set;
- a secret set member can get the secret key for secure group communication among the secret set;
- the size of the secret set is indeterminable due to the inclusion of random number of decoys in $P(x)$;
- outsiders and other members cannot know the membership or the size of the secret set;
- except knowledge of his/her own membership, a secret set member does not know the membership of others or the size of the secret set;
- all members, but m_i, even though they collude, have no information on the membership of m_i.

Theorem 4.1: The extended ACP-based scheme is solid in terms of anonymity and security of multiple party group communication.

Proof: In terms of anonymity, due the decoys introduced in $A(x)$, an attacker or a malicious member may guess a D_j which recovers and verifies K. However, he/she cannot determine members of the secret set. Furthermore, an attacker may guess a correct S_{i_j} which discloses K, but he/she cannot determine member m_{i_j} since he/she does not know that S_{i_j} is associated with m_{i_j} and also cannot discern whether S_{i_j} is a decoy. In terms of group communication security, the probability of obtaining group key K by guessing or brute-force attacks is changed/increased to $(n + d)/q$ from n/q, where n is the number of the members in the group, d the number of introduced decoys, and q the large prime forming the finite field F_q. We can, however, select a larger prime q' for anonymous secure group communication so that $(n + d)/q' \leq n/q$. Thus, the extended mechanism is not less secure than the original ACP scheme; the only penalty is that it slightly lowers performance. The detail security proof of the ACP mechanism can be found in [1]. ■

V. Comparisons and discussions

In this section, we first compare the proposed ACP based scheme with typical existing group-oriented anonymous schemes and then present some experimental results.

A. Comparisons

1) Secret set schemes. As is evident from the above description, the secret set is only used for anonymous membership and set size, but the new ACP-based mechanism can also distribute the secret key. Moreover, the bit vector is the most efficient method for secret set, but it assigns orders to the members and the total number of members must be known to the members[5]. In contrast, the new ACP-based scheme allows for a random number of members and there is no need for such ordering[6].
2) Anonymous membership broadcasting schemes (AMB). As mentioned in the related work, papers [46], [47],

[5]These requirements are true for other techniques, except for that based on Chinese Remainder Theorem.

[6]In the ACP-based scheme, the numbers in subscript are purely for description purpose.

TABLE I
COMPLEXITIES OF SECURE LOCK AND ACP[&]

	Secure Lock	ACP
Generation of Ł or $P(x)$	$O(n^2B_1^2)^* + O(nB_1^3)^{\#}$	$O(n^2B_2^2)$
Given $B_1 = 1024, B_2 = 128$	$O(2^{20}n^2) + O(2^{30}n)$	$O(2^{14}n^2)$
Key computation	$O(nB_1^2)^{\%} + O(B_1^3)^{\$}$	$O(nB_2^2)$
Given $B_1 = 1024, B_2 = 128$	$O(2^{20}n) + 2^{30}$	$O(2^{14}n)$
Message length	$O(nB_1)$	$O(nB_2)$
Given $B_1 = 1024, B_2 = 128$	$O(2^{10}n)$	$O(2^7n)$

*: the CRT computation. #: the n public encryptions of the key.
%: getting $E_{P_{i_j}}(k)$ by division. $: getting k by public decryption.
&: Ignore the complexity of $f(S_i, z)$ since its complexity depends on the hash function selected and, in general, a hash function does not pose an efficiency problem.

TABLE II
EXPERIMENTAL RESULTS OF SECURE LOCK AND ACP

Group	Generation of Ł or $P(x)$ (ms)		Key Computation (ms)	
Size	Secure Lock	ACP	Secure Lock	ACP
10	22.122448	3.607294	32.548145	0.160141
50	334.4157	11.172215	35.519367	0.2505174
100	1248.3452	25.149284	35.745132	0.48382694
150	2715.346	45.294716	37.36742	0.7251202
200	4739.1973	71.207054	38.873844	0.96511495
250	7328.6416	102.26748	40.622406	1.2320576
300	10508.015	138.02417	42.16938	1.4394373
350	14244.455	187.28809	44.092808	1.6779447
400	18545.045	225.84566	45.835262	1.9190532
450	23349.342	278.32162	47.28901	2.161534
500	28807.654	336.43692	48.277184	2.4009411

and [48] proposed and implemented AMB. The new ACP-based scheme can also support AMB if only the intended receiver's ID is included in the construction of $A(x)$ (besides decoys). In particular, the new ACP based scheme is secure against collusion of any number of users.

3) Anonymous secure group communication schemes. As for secure lock, it is based on public key cryptosystems. In contrast, the new ACP-based mechanism employs polynomial and secret key cryptosystems. Thus, the ACP based scheme can use a 128-bit number to get stronger security than secure lock using at least 1024-bit numbers. This is because 80-bit symmetric systems, 160-bit hash functions, and 1024-bit RSA all have comparable security [49]. In this sense, the new ACP-based scheme will be more efficient than secure lock.

Let us discuss the efficiencies of the ACP mechanism and Secure Lock in detail. From paper [1], we know that the time complexity for generating $P(x)$ is $O(n^2)$ multiplications (with modulus) and the key computation time is $O(n)$ multiplications. The complexity for modular multiplications is $O(B^2)$ bit operations [50], where B is the bit length of the operands. As for Secure Lock, the complexity for public key encryption is $O(B^3)$ [50]. Since there are n public key encryptions, the total running time for public key encryptions is $O(nB^3)$ (in bit operations). The complexity for CRT computation is $O(n^2B^2)$ (See Corollary 5.5.6 in book [51]). Thus, the total running time for computing Ł (which is nB bits)is $O(nB^3) + O(n^2B^2)$. As for computing the key from Ł, its complexity is $O(nB^2) + O(B^3)$. Ignoring the key and membership verification (which is the same for both methods), the complexities are summarized in Table I.

B. Experiment

To demonstrate the performance of our scheme, we implemented both the ACP-based scheme and the secure lock scheme. A java program was developed to measure the computation time of the core message generation and key computation. The program is written in JAVA and utilizes JAVA's BigInteger and crypto classes. It runs on a DELL Laptop with single Intel Conroe 1.86GHz CPU and 1G memory. The ACP scheme uses 128-bit numbers and secure lock uses 1024-bit numbers.

For the ACP-based scheme, we generate a 128-bit random prime q to form the field F_q in which to perform our polynomial arithmetic. The one way function is chosen as $a^{s \oplus z} mod q$ where a is a primitive root of q. We use the typical *Square and Multiply* technique for exponentiation.

In the experiments, the program generates 10,000 random numbers less than q as keys S for 10,000 users. For each experiment, the program selects different group sizes and then m random values $S_1, \cdots, U_m$ from the pre-generated keys for the users in the group such as $U_1, \cdots, U_m$. Then a random number less than q is generated as z. $S_1 \cdots S_m$ and z, together with a random session key, are used to calculate the coefficients of the polynomial $P(x)$. To evaluate the core performance, we did not add decoys for either secure lock or ACP schemes. The session key recovery is as follows: A user computes $f(s, z) = a^{s \oplus z} \ mod \ q$ and substitutes $f(s, z)$ into the polynomial he received and gets the session key. Each step of the computation will reduce the result to the field of F_q to increase efficiency.

For the secure lock scheme, we select RSA public key cryptosystem and use RSA classes contained in bcprov-jdk16-145.jar. The package is a Java implementation of cryptographic algorithms from Bouncy Castle Crypto (http://www.bouncycastle.org). we generate 10000 public primes and RSA objects. The primes are 1024 bits long and generated randomly. We use a random 128-bit number as session key K.

The experimental results are shown in Table II and also in Figures 1, 2, and 3 (**Notes:** the figure are drawn in logarithmic scale for y-coordinate). From the table and figures, it can be observed that the experimental results validate our theoretical analysis in Table I and prove the ACP-based mechanism is more efficient than the secure lock scheme approximately 100 times faster in term of membership representation generation (i.e. Ł or $P(x)$) and approximately 10 times better in terms of key computation and message length.

C. Applications

As mentioned in the introduction, anonymous secure group communication is critical for protecting the identity of par-

ticipants in many Internet applications. One such emerging application is Wireless Access in Vehicular Environments (WAVE) via Vehicular Ad Hoc Networks (VANET), where vehicle drivers (along with service providers) communicate/share important road, traffic and weather-related information in order to enhance driving safety and shorten travel time. Standards for vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) infrastructure have previously been proposed; among these is IEEE 1609.2–the IEEE Trial-Use Standard for Security Services for Applications and Management Messages for WAVE [52]. In vehicular environments, one of the most important issues is the need to maintain users' privacy [53]. Indeed, unless a user can be assured that their personal/private information (e.g., their real identity) can be kept private, they will most likely be unwilling to use such V2V communications for fear of their identity being stolen or of possibly being tracked by police and issued traffic tickets. The embracing of anonymity and anonymous secure group communication techniques is certainly a possible solution that would serve to protect users' privacy. Some preliminary work on privacy and anonymity in VANETs has been initiated such as traceable anonymous certificate (TAC) [54] recently proposed by the IEEE Internet Engineering Task Force and group-based anonymous communication schemes [55]. In this regard, the proposed extended ACP scheme could have both important research implications and practical applications in this area.

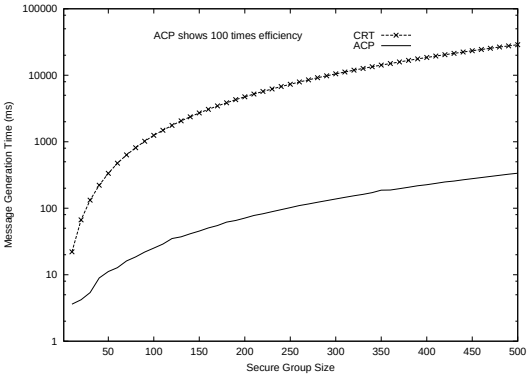

Fig. 1. Membership representation generation time.

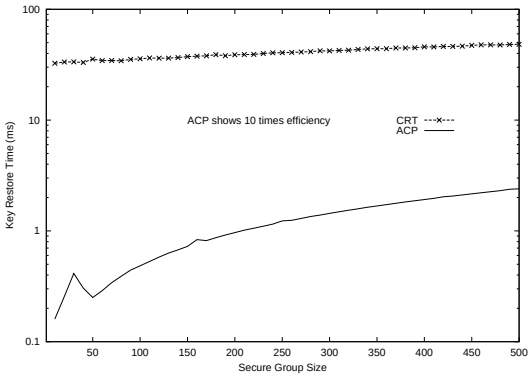

Fig. 2. Key computation time.

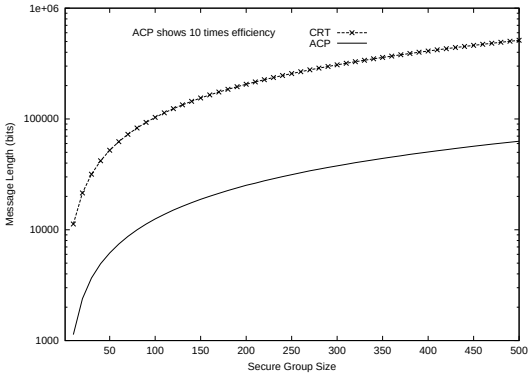

Fig. 3. Communication complexities in terms of message length in bits.

VI. Conclusion

This paper presented an elegant construction of secret set based on access control polynomials. Furthermore, the new scheme also supports anonymous secure group communication and offers many desirable features. The experiment and comparison showed the newly extended ACP-based scheme is both efficient and practical.

References

[1] X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," *Proceedings of INFOCOM'08, Phoenix, AZ, USA*, pp. 1211–1219, Apr. 2008.

[2] Y. Guan, X. Fu, R. Bettati, and W. Zhao, "An optimal strategy for anonymous communication protocols," in *In Proc. 22nd IEEE International Conference on Distributed Computing Systems (ICDCS 2002)*, 2002.

[3] I. O. for Standardization (ISO), "Information technology-security techniques-evaluation criteria for it security," ISO/IEC 15408, 2005.

[4] D. Evans and N. Paul, "Election security: perception and reality," *IEEE Security & Privacy*, vol. 2, no. 1, pp. 24–31, 2004.

[5] X. Zou, B. Ramamurthy, and S. S. Magliveras, Eds., *Secure Group Communications over Data Networks*. New York, NY, USA, ISBN: 0-387-22970-1 (The ebook ISBN: 0-387-22971-X): Springer, Oct. 2004.

[6] F. Liu and X. Cheng, "LKE: A self-configuring scheme for location-aware key establishment in wireless sensor networks," *IEEE Transactions On Wireless Communications*, 2007.

[7] W. H. D. Ng, M. Howarth, Z. Sun, and H. Cruickshank, "Dynamic balanced key tree management for secure multicast communications," *IEEE Transactions on Computers*, vol. 56, no. 5, pp. 577–589, May 2007.

[8] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Computing Surveys*, vol. 35, no. 3, pp. 309–329, 2003.

[9] W. Trappe, Y. Wang, and K. J. R. Liu, "Resource-aware conference key establishment for heterogeneous networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 13, no. 1, pp. 134 – 146, Feb. 2005.

[10] Z. Yu and Y. Guan, "A key pre-distribution scheme using deployment knowledge for wireless sensor networks," *Proceedings of the 4th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pp. 261–268, 2005.

[11] A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology," Draft, July 2007.

[12] Q. Lu, S. Zhou, and Y. Fu, "Analyzing anonymous communication technology," *Journal of UEST of China*, vol. 33, no. 2, pp. 162–165, Apr. 2004.

[13] Unknown, "The anonymizer," http://www.anonymizer.com/.

[14] Z. M. Mao, C. D. Cranor, F. Douglis, M. Rabinovich, O. Spatscheck, and J. Wang, "A precise and efficient evaluation of the proximity between web clients and their local dns servers," in *Proceedings of the General Track: 2002 USENIX Annual Technical Conference, June 10-15, 2002, Monterey, California, USA*, 2002, pp. 229–242.

[15] M. Bishop, R. Crawford, B. Bhumiratana, L. Clark, and K. N. Levitt, "Some problems in sanitizing network data," in *15th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE 2006), 26-28 June 2006, Manchester, United Kingdom*, 2006, pp. 307–312.

[16] J. Ren, T. Li, and Y. Li, "Anonymous communications in overlay networks," *Proceedings of IEEE Military Communications Conference, 2008 (MILCOM 2008), San Diego, CA, USA, 16-19 Nov. 2008*, pp. 1–6, 2008.

[17] D. Chaum and E. van Heyst, "Group signatures," *Advances in Cryptology ł EUROCRYPT 91, Lecture Notes in Computer Science*, vol. 547, pp. 257–265, 1991.

[18] N. Koblitz and A. Menezes, "Another look at "provable security"," Cryptology ePrint Archive, Report 2004/152, 2004.

[19] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," in *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, CA, May 1998.

[20] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[21] Z. Teng and W. Du, "Comparisons of k-anonymization and randomization schemes under linking attacks," in *Proceedings of the 6th IEEE International Conference on Data Mining (ICDM 2006), 18-22 December 2006, Hong Kong, China*, 2006, pp. 1091–1096.

[22] A. Shubina and S. Smith, "Using caching for browsing anonymity," *ACM SIGEcom Exchanges*, vol. 4, no. 2, September 2003.

[23] M. Burnside and A. D. Keromytis, "Low latency anonymity with mix rings," in *Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings*, 2006, pp. 32–45.

[24] J. Helsingius, "Don't try to control the network because it's impossible anyway," *IC Magazine, NTT Publishing*, Dec 1994.

[25] E. Hughes, "A cypherpunk's manifesto," Mar 1993.

[26] L. Cottrell, "Mixmaster and remailer attacks," 1994.

[27] G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: design of a type iii anonymous remailer protocol," in *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, May 2002, pp. 2–15.

[28] C. Gülcü and G. Tsudik, "Mixing e-mail with Babel," in *Proceedings of the Network and Distributed Security Symposium - NDSS '96*. IEEE, February 1996, pp. 2–16.

[29] I. Goldberg and D. Wagner, "Taz servers and the rewebber network: Enabling anonymous publishing on the world wide web," *First Monday*, vol. 3, no. 4, Apr 1998.

[30] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," *Journal on Selected Areas in Communications*, vol. 16, no. 4, May 1998.

[31] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for web transactions," *ACMTransactions on Information and System Security*, vol. 1, no. 1, 1998.

[32] P. Boucher, A. Shostack, and I. Goldberg, "Freedom systems 2.0 architecture," White Paper, Dec. 2000.

[33] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Mask: anonymous on-demand routing in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2376–2385, Sep 2006.

[34] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, pp. 65–75, 1988.

[35] J. Kilian and E. Petrank, "Identity escrow," in *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, ser. Lecture Notes In Computer Science, vol. 1462, 1998, pp. 169–185.

[36] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "Non-interactive anonymous credentials," Cryptology ePrint Archive, Report 2007/384, 2007.

[37] L. von Ahn, A. Bortz, and N. J. Hopper, "K-anonymous message transmission," in *Proceedings of the 10th ACM conference on Computer and Communications Security*, Washington D.C., USA, 2003, pp. 122–130.

[38] G. Yao and D. Feng, "A new k-anonymous message transmission protocol," in *WISA*, 2004, pp. 388–399.

[39] P. Wang, P. Ning, and D. S. Reeves, "A k-anonymous communication protocol for overlay networks." in *Proceedings of the 2nd ACM symposium on Information, computer and communications security (ASIACCS)*, F. Bao and S. Miller, Eds. ACM, 2007, pp. 45–56.

[40] M. Edman and B. Yener, "On anonymity in an electronic society: A survey of anonymous communication systems," *Computing Surveys (CSUR)*, vol. 42, no. 1, pp. 1–35, 2009.

[41] R. Molva and G. Tsudik, "Secret sets and applications," *Information Processing Letters*, vol. 65, pp. 47–55, 1998.

[42] M. de Mare and R. N. Wright, "Secure set membership using 3SAT," in *Proceedings of the 8th International Conference on Information and Communications Security (ICICS), Raleigh, NC, USA, December 4-7*, 2006, pp. 452–468.

[43] G. H. Chiou and W. Chen, "Secure broadcasting using the Secure Lock," *IEEE Transactions on Software Engineering*, vol. 15, no. 8, pp. 929–934, Aug. 1989.

[44] N. Weiler, "Secure anonymous group infrastructure for common and future internet applications," *Proceedings 17th Annual Computer Security Applications Conference (ACSAC)*, pp. 401–410, 2001.

[45] A. D. Santis and B. Musucci, "On secret set schemes," *Information Processing Letters*, vol. 74, no. 5-6, pp. 243–251, June 2000.

[46] H. Wang and J. Pieprzyk, "A combinatorial approach to anonymous membership broadcast," *Lecture Notes on Computer Sciences (LNCS)*, vol. 2387, pp. 162–170, 2002.

[47] A. D. Santis and B. Masucci, "Anonymous membership broadcast schemes," *Designs, Codes and Cryptography*, vol. 32, pp. 135–151, 2004.

[48] H. v. Tilborg, J. Pieprzyk, R. Steinfeld, and H. Wang, "New constructions of anonymous membership broadcasting schemes," *Advances in Mathematics of Communications*, vol. 1, no. 1, pp. 29–44, 2007.

[49] A. K. Lenstra, "Key length," *Handbook of Information Security, Editor-in-Chief, Hossein Bidgoli*, vol. 2, pp. 617–635, 2005.

[50] D. R. Stinson, *Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC, November 2005. [Online]. Available: http://www.amazon.fr/exec/obidos/redirect?tag=citeulike06-21&path=ASIN/1584885084

[51] E. Bach and J. Shallit, "Algorithmic number theory, volume I: Efficient algorithms," *The MIT Press*, 1996.

[52] IEEE, "1609.2-2006 IEEE Trial-Use Standard for Wireless Access in Vehicular Environments," *http://www.safetyonline.com/product.mvc/16092-2006-IEEE-Trial-Use-Standard-for-Wirele-0001*.

[53] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: a secure and privacypreserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, pp. 3442–3456, 2007.

[54] I. E. T. Force, "Traceable anonymous x.509 certificate (TAC)," *http://tools.ietf.org/html/draft-ietf-pkix-tac-04*.

[55] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON 2009)*, pp. 1–9, 2009.