2009 Second International Conference on Computer and Electrical Engineering

ID Based Signature Schemes for Electronic Voting

Tulasi Menon
Dept. of Computer Science
Sri Venkateswara College of Engineering
Chennai-602105, India.
Email: libra.tm@gmail.com

R. Sindhuja
Dept. of Information Technology
Sri Venkateswara College of Engineering
Chennai-602105, India.
Email: sindhuravi89@rediffmail.com

***Abstract*—Electronic voting is being used increasingly in several areas of work. The existing protocols and systems for voting are fraught with difficulties and flaws, which allow malicious users to tamper with the votes. Votes have to be unforgeable, anonymous and verifiable. In this paper, we suggest the use of 2 ID-Based signatures for an e-voting system. We describe a designated verifier ring signature, which will ensure both the security of the vote, as well as voter anonymity. In order for the voter to check if his/her vote has been taken into account, we provide a receipt for the voter, from the voting authority, using a new ID-Based designated verifier signature. The receipt will not allow the voter to reveal their vote to someone else, thus ensuring the security of the voter.**

***Index Terms*—Electronic voting, Designated verifier signature, ID-Based signature, Ring signature**

I. Introduction

In the world of today, electronic voting is being used in many applications and spheres of life, for example in companies, national ballot, etc. Each of these have different forms and methods, from automated voting system to vote through networks. In practice, the electronic voting systems have a number of loopholes and flaws, which can lead to unfair results and dire consequences. A vital property of a vote is that nobody should be able to vote on behalf of another person, i.e a vote must be unforgeable. Moreover, nobody, not even the voting authority should know who a particular candidate has voted for, i.e. anonymity must be maintained. Another problem arises when trying to combine voting privacy with the ability of the voter to check the correctness of his own voting by means of a receipt. Most of the time, being in possession of a voting receipt implies that a dishonest third party may possibly force the voter to reveal his/her vote. To avoid this, most systems propose receipt-free voting protocols. But in that case, the main problem becomes the difficulty of the voter to ensure his/her vote was taken into account. This paper proposes a new voting scheme, where we use ring signatures for the voting, and designated verification to ensure that the user gets a receipt. For the voting process, we employ a designated verifier ring signature, which is our extension of the ring signature by Chow et al in [9]. Here, the group of board members or shareholders represents the voting group. They each sign a vote and designate the Voting Authority as the verifier, so that nobody else can view their vote. The Voting Authority can verify all the votes and check their authenticity, but, due to the property of ring signatures, all he/she can verify is that someone in the group sent the vote, but will not be able to pinpoint the exact person. As a result, the anonymity of the voters is maintained, at the same time, votes are well checked for authenticity. Thus, no person outside the voting group will be able to send a valid signature, nor will any person be able to forge this signature.

The usage of designated verifier protocols for a receipt was utilized by [4], but we employ an ID-based scheme, which is much more efficient and practical for applications like voting within a group like board of members in a company, where the IDs of various participants have already been set up. The advantage of using designated verification, is that, even though the user can obtain a valid receipt containing evidence that his/her vote has been taken into account, he/she cannot use this to reveal the vote to some third party. A designated verifier scheme provides a message signed in such a way that only one person, i.e. the designated verifier, will be able to check its validity. In this case, the voter will be the designated verifier, and the Receipt Generator will be the signer of the receipt.

The paper is organized as follows. In the next section we introduce the various preliminaries of elliptic curve cryptography. In the third section, we describe the ID based designated verifier ring signature scheme for voting and in the fourth section, the ID based designated verifier signature scheme for the

978-0-7695-3925-6/09 $26.00 © 2009 IEEE
DOI 10.1109/ICCEE.2009.123

receipt. In the fifth and final section, we give the conclusion.

II. Preliminaries

Bilinear pairing is an important primitive for many cryptographic schemes. Here, we describe some of its key properties.Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of order q for some large prime q, where $\mathbb{G}_1$ is a cyclic additive group and $\mathbb{G}_2$ is a related multiplicative group. A pairing, which can be either a modified Weil pairing or a Tate pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following properties:

- *Bilinearity:* Given $P, Q, R \epsilon \mathbb{G}_1$, we have $\hat{e}(P, Q + R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$ and $\hat{e}(P + Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$. Hence for any $a, b \epsilon \mathbb{Z}_q^*, \hat{e}(aP, bQ) = \hat{e}(abP, Q) = \hat{e}(P, Q)^{ab}$.
- *Non-Degeneracy:* There exists a $P \epsilon \mathbb{G}_1$ such that $\hat{e}(P, P) \neq 1$.
- *Computability:* If $P, Q \epsilon \mathbb{G}_1, \hat{e}(P, Q)$ can efficiently be computed.

Definition 1. *Given a generator P of a group $\mathbb{G}$ and a 3-tuple (aP, bP, cP), the Decisional Diffie-Hellman problem (DDHP) is to decide if c = ab.*

Definition 2. *Given a generator P of a group $\mathbb{G}$ and a 2-tuple (aP, bP), the Computational Diffie-Hellman problem (CDHP) is to compute abP.*

Definition 3. *We define G as a Gap Diffie-Hellman (GDH) group if $\mathbb{G}$ is a group such that DDHP can be solved in polynomial time but no algorithm can solve CDHP with non-negligible advantage within polynomial time.*

III. Related Work

Considerable amount research has been involved in proposing efficient cryptographic protocols for practical applications like electronic voting systems. In 2006, David Wagner[3] proposed and discussed in detail several cryptographic protocols for improving electronic voting systems, and compared and contrasted the ideas based on accuracy, privacy and usability. Ratna Dutta et al. in 2004 [6], gave a detailed survey on the various existing pairing based cryptographic protocols. In 2004, Emmanuel Dall'Olio and Olivier Markowitch discussed the use of a designated verifier signature-like protocol in [4] for generating receipts in an electronic voting system.

Since the introduction of DVS , there have been a lot of work on it and its variants. Jakobsson et al. [5] proposed a stronger version of DVS, strong designated verifier signature (SDVS), in which only the verifier can verify the validity of a signature designated to him since the verification requires the secret key of the designated verifier. Steinfeld et al. proposed the notion of universal designated verifier signature (UDVS), in which the holder of a signature can designate any third party as the designated verifier for checking the validity of the signature, but in the meanwhile, the designated verifier still could not convince others the source of the signature. Laguillaumie et al. studied other variants of designated verifier signatures , i.e. multi-designated verifiers signatures and etc. Saeednia, Kremer and Markowitch proposed Efficient Designated Verifier Signature Schemes[7] in 2004. Susilo et al. [10] studied DVS schemes in the identity-based setting and proposed an identity-based SDVS scheme based on bilinear Diffie-Hellman (BDH) assumption. Huang et al. also proposed a strong DVS scheme and an identity-based SDVS scheme based on Diffie-Hellman key exchange, which has very short signature size. Kang et al. proposed another identity-based SDVS scheme which is secure based BDH assumption. In 2008, Bin Wang[1] proposed a strong id-based designated verifier signature scheme with the added feature of non-delegatability.

At Asiacrypt 2001, Rivest, Shamir and Tauman first introduced the concept and the need for ring signatures. In 2002, Fangguo Zhang and Kwangjo Kim designed one of the first ID-based ring signature scheme using bilinear pairing. In 2003,Chih-Yin Lin and Tzong-Chen Wu introduced another scheme, which improved the computational efficiency of by using fewer pairings. Later in the year, Chunming Tang,Zhuojun Liu and Mingsheng Wang showed that Lin-Wu's scheme was unreasonable and developed their own scheme. A year later, Sherman S.M Chow, S.M Yiu and Luvas C.K Hui designed a highly efficient signature scheme, with only two pairings. Recently, in 2007, Jianhong Zhang and Cheng Ji bettered this, and developed a scheme that uses no pairings at all.In addition to these, there are several others, like Jun Shao, Zhenfu Cao and Licheng Wang , and Victor K. Wei and Tsz Hon Yuen who developed ID-based threshold ring signatures. Another related signature scheme is the ID-based Proxy ring signature, which was developed by several authors, including Wu Lei and Li Daxing , Amit K Ashwati and Sunder Lal and others.

IV. An ID based Designated Ring Signature Scheme for Voting

Define $\mathbb{G}_1$,$\mathbb{G}_2$ and $\hat{e}(\cdot, \cdot)$ as in Section 2 where $\mathbb{G}_1$ is a GDH group. $H(\cdot)$ and $H_0(\cdot)$ are two cryptographic

hash functions where $H : \{0,1\}^* \longrightarrow \mathbb{G}_1$ and $H_0 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$.

- **Setup:** The Voting Authority, VA randomly chooses $x \ \epsilon_R \ \mathbb{Z}_q^*$, keeps it as the master secret key and computes the corresponding public key $P_{pub} = xP$. The system parameters are: $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, P, P_{pub}, H(\cdot), H_0(\cdot)\}$.
- **KeyGen:** The signer with identity $ID \ \epsilon \ \{0,1\}^*$ submits ID to VA. The VA sets the signers public key Q_{ID} to be $H(ID)\epsilon\mathbb{G}_1$, computes the signers private signing key S_{ID} by $S_{ID} = xQ_{ID}$. Then VA sends the private signing key to the signer via a secure channel.
- **Sign:** Let $L = \{ID_1, ID_2, , ID_n\}$ be the set of all identities of n users. The actual signer, indexed by s (i.e. his/her public key is $Q_{ID_s} = H(ID_s)$), carries out the following steps to give an ID-based designated ring signature on behalf of the group L to the verifier, indexed by v (i.e. his/her public key is $Q_{ID_v} = H(ID_v)$).
  - Choose $l \ \epsilon \ \mathbb{Z}_q^*$, compute $Y = lP$ and $k = \hat{e}(lQ, P_{pub})$.
  - Compute $Z = lH_1(ID_V) + lQ \ \forall \ i \ \epsilon\{1, 2, ..., n\}$.
  - Choose $U_i \ \epsilon_R \ \mathbb{G}_1$, compute $h_i = H_0(m\|L\|U_i\|k) \ \forall \ i \ \epsilon\{1, 2, ..., n\} \ \setminus \ \{s\}$.
  - Choose $r'_s \ \epsilon_R \ \mathbb{Z}_q^*$, compute $U_s = r'_s Q_{ID_s} - \Sigma_{i \neq s}\{U_i + h_i Q_{ID_i}\}$.
  - Compute $h_s = H_0(m\|L\|U_s\|k)$ and $V = (h_s + r'_s)S_{ID_s}$.
  - Output the signature on m as $\sigma = \{\bigcup_{i=1}^{n}\{U_i\}, V\}$.
- **Verify:**A verifier can check the validity of a signature $\sigma = \{\bigcup_{i=1}^{n}\{U_i\}, V\}$ for the message m and a set of identities L as follows.
  - Compute $h_i = H_0(m\|L\|U_i\|k) \ \forall \ i \ \epsilon\{1, 2, ..., n\}$.
  - Check whether $\hat{e}(P_{pub}, \Sigma_{i=1}^{n}(U_i + h_i Q_{ID_i})) = \hat{e}(P, V)$.
  - Accept the signature if it is true, reject otherwise.
  - The correctness of the above verification process is given as follows:

$$\hat{e}(P_{pub}, \Sigma_{i=1}^{n}(U_i + h_i Q_{ID_i}))$$
$$\Rightarrow \hat{e}(xP, r'_s Q_{ID_s} - U_s + U_s + h_s Q_{ID_s})$$
$$\Rightarrow \hat{e}(xP, r'_s Q_{ID_s} + h_s Q_{ID_s})$$
$$\Rightarrow \hat{e}(P, x \cdot (r'_s + h_s) Q_{ID_s})$$
$$\Rightarrow \hat{e}(P, (h_s + r'_s) S_{ID_s})$$
$$\Rightarrow \hat{e}(P, V)$$

The group of voters is considered for generating a designated verifier ring signature. An important feature of this signature is that the actual voter maintains his anonymity to the VA as the VA is assured only that the vote has been generated by someone in the group and not who exactly has voted.

V. An ID based Designated Signature Scheme for Generation of Receipts

Define $\mathbb{G}_1$,$\mathbb{G}_2$ and $\hat{e}(\cdot,\cdot)$ as in Section 2 where $\mathbb{G}_1$ is a GDH group. $H(\cdot)$ and $H_0(\cdot)$ are two cryptographic hash functions where $H : \{0,1\}^* \longrightarrow \mathbb{G}_1$ and $H_0 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$.

- **Setup:** The Receipt Generator, RG randomly chooses $x \ \epsilon_R \ \mathbb{Z}_q^*$, keeps it as the master secret key and computes the corresponding public key $P_{pub} = xP$. The system parameters are: $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, P, P_{pub}, H(\cdot), H_0(\cdot)\}$.
- **KeyGen:** The signer with identity $ID \ \epsilon \ \{0,1\}^*$ submits ID to RG. The RG sets the signers public key Q_{ID} to be $H(ID)\epsilon\mathbb{G}_1$, computes the signers private signing key S_{ID} by $sk_{ID} = xQ_{ID}$. Then RG sends the private signing key to the signer via a secure channel.
- **Sign:** Given the signer's key pair (sk_{ID_S}, ID_S), the verifier's identity ID_D and a message m, the signer should perform the following steps:
  - Picks random numbers $r_A, w_A \ \epsilon \ Z_q^*$ and computes $R_A = e(Q_{ID_D}, r_A \cdot P)$.
  - Computes $V_A = e(sk_{ID_S}, Q_{ID_D})$ and $h_A = H_0(ID_S, ID_D, R_A, V_A, m)$.
  - Computes $Z_A = r_A \cdot P + (h_A + w_A) \cdot sk_{ID_S}$.
  - The signature is $\sigma_{DV} = \{R_A, w_A, Z_A\}$.
- **Verify:** Given the signer's identity ID_S, the verifier's key pair (sk_{ID_D}, ID_D), the signed message m and the corresponding signature σ_{DV}, the correctness of the signature can be verified as follows:
  - Computes $V_A = e(Q_{ID_S}, sk_{ID_D})$ and $h_A = H_0(ID_S, ID_D, R_A, V_A, m)$.
  - Returns 1 if and only if $e(Q_{ID_D}, Z_A) = R_A \cdot e(sk_{ID_D}, (h_A + w_A) \cdot Q_{ID_S})$.
  - The correctness of the above verification process is given as follows:

$$V_A = e(Q_{ID_S}, sk_{ID_D})$$
$$\Rightarrow e(Q_{ID_S}, xQ_{ID_D})$$
$$\Rightarrow e(xQ_{ID_S}, Q_{ID_D})$$
$$\Rightarrow e(sk_{ID_S}, Q_{ID_D}) = V_A$$

$$e(Q_{ID_D}, Z_A)$$
$$\Rightarrow e(Q_{ID_D}, r_A P + (h_A + w_A) sk_{ID_S})$$

$$\Rightarrow R_A \cdot e(Q_{ID_D}, (h_A + w_A) \cdot sk_{ID_S})$$
$$\Rightarrow R_A \cdot e(sk_{ID_D}, (h_A + w_A) \cdot Q_{ID_S})$$

- **Simulation:** Given the signer's identity ID_S, the verifier's key pair (sk_{ID_D}, ID_D), and a message m, a simulated signature σ'_{DV} can be generated as follows:
  - Picks random $\alpha_D, \lambda_D \epsilon Z_q, Z_D \epsilon \mathbb{G}_1$ and computes $V_D = e(Q_{ID_S}, sk_{ID_D})$.
  - Computes $R_D = e(Q_{ID_D}, Z_D)e(sk_{ID_D}, -\lambda_D \cdot Q_{ID_S}), h_D = H_0(ID_S, ID_D, R_D, V_D, m)$.
  - Computes $w_D = (\lambda_D - h_D) mod q$.
  - The simulated signature is $\sigma'_{DV} = \{R_D, w_D, Z_D\}$.
  - The correctness of σ'_{DV} can be checked as follows:

    $$e(P, T_D + w_D \cdot sk_{ID_D})$$
    $$\Rightarrow e(P, \alpha_D \cdot P) = V_D$$

    $$e(Q_{ID_D}, Z_D)$$
    $$\Rightarrow R_D \cdot e(sk_{ID_D}, \lambda_D \cdot Q_{ID_S})$$
    $$\Rightarrow R_D \cdot e(sk_{ID_D}, (h_D + w_D) \cdot Q_{ID_S})$$

  A designated verifier signature on the receipt sent from the RG to the voter, ensures that only the actual voter can verify the authenticity of the receipt and no one else. Moreover, the actual voter cannot prove to anyone else the authenticity of the signature as it can be simulated by him.

VI. Conclusion

Thus, the two signatures for the electronic voting system have been described above. The voter, who is part of a group in a company, sends his vote, signed by the designated verifier ring signature scheme. The Voting Authority (VA) gets the vote, and verifies its authenticity by checking that it is really from some person in the group. The VA cannot find out the identity of the voter, due to the property of ring signatures, thus maintaining the anonymity of the voter. Once the voter has sent across his/her vote, he/she would want to ensure that their vote is taken into account. To show that a vote has been received, the Receipt Generator (RG) sends a receipt to the voter as soon as the vote has been cast. The RG knows only the ID of the voter, and sends the receipt, signed with a designated verifier signature, designated to the voter. The voter can verify the receipt, but does not have the power to convince any other person that the receipt is authentic. Thus, the system is strongly secure.

References

[1] Bin Wang *A non-delegatable identity-based strong designated verifier signature scheme*, In Cryptology ePrint Archive 2008, unpublished.

[2] Dan Boneh and Ben Lynn and Hovav Shacham, "Short Signatures from the Weil Pairing",*Journal of Cryptology*, pp. 297-319. Springer-Verlag LNCS, 2004.

[3] David Wagner, "Cryptographic Protocols for Electronic Voting", *Advances in Cryptology - CRYPTO 2006*, pp. 393, 2006.

[4] Emmanuel Dall'Olio and Olivier Markowitch, "Voting with Designated Verifier Signature-Like Protocol", *Proceedings of the IADIS International Conference WWW/Internet 2004*, Madrid, Spain, 2 Volumes, 2004.

[5] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo, "Designated verifier proofs and their applications", *Advances in Cryptology - EUROCRYPT 96*, volume 1070 of Lecture Notes in Computer Science, pp. 143 154. Springer, 1996.

[6] Ratna Dutta, Rana Barua and Palash Sarkar, "Pairing-Based Cryptographic Protocols: A Survey". [Online]. Available: eprint.iacr.org/2004/064.pdf

[7] Shahrokh Saeednia, Steve Kremer and Olivier Markowitch, "Efficient Designated Verifier Signature Schemes", *International conference on information security and cryptology*, Seoul, vol. 2971, pp. 40-54, 2004.

[8] Sherman S. M. Chow, "Identity-Based Strong Multi-Designated Verifiers Signatures", *Proceedings of Third European PKI Workshop: Theory and Practice*, EuroPKI 2006, Turin, Italy, vol. 4043/2006, pp. 257-259, 2006.

[9] Sherman S. M. Chow, Victor K.W. Wei, Joseph K. Liu and Tsz Hon Yuen, "Ring signatures without random oracles", *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, ASIACCS 2006, Taipei, Taiwan, pages 297-302, 2006.

[10] Willy Susilo, Fangguo Zhang, and Yi Mu, "Identity-based strong designated verifier signature schemes", *Proceedings of 9th Australasian Conference on Information Security and Privacy*, ACISP 2004, volume 3108 of Lecture Notes in Computer Science, pages 313-324. Springer, 2004.