Truly Anonymous Paper Submission and Review Scheme

Chun-I Fan\textsuperscript{1}, Ming-Te Chen\textsuperscript{2}, and Lung-Hsien Chen\textsuperscript{3}
Department of Computer Science and Engineering
National Sun Yat-sen University
70, Lienhai Rd., Kaohsiung 804, Taiwan
TEL: +886-7-5252000 ext. 4346
FAX: +886-7-5254301
Email\textsuperscript{1}: cifan@faculty.nsysu.edu.tw
Email\textsuperscript{2}: ecsemtnchen@gmail.com
Email\textsuperscript{3}: rryan.chen@gmail.com

Abstract

Due to the flush development of academic research, a great deal research results have been published in conference proceedings and journals. However, these articles need to be inspected by some professionals in specific fields. It is the most important that it must keep fair during the entire process of reviewing. However, the privacy of reviewers will be leaked out because that the reviewers must sign their comments on the reviewed papers. The leakage of the reviewers’ privacy will affect the fairness of paper reviewing. In addition, the authors need to show their names to the editor of conference proceedings or journals such that it may also make the inspecting results unfair. Unfortunately, the solutions proposed in the literature cannot cope with the problems of fairness well. Therefore, in order to eliminate the drawbacks of the previous schemes, we will deeply analyze the paper review procedure to find the possible reasons that bring about these unfair results. Furthermore, we will present a generic idea, which is independent of the underlying cryptographic components, to achieve the fairness property and other requirements in a paper review scheme.

1. Introduction

Now there are many papers about all kinds of topics in academic research to be published by diversiform conference proceedings and journals every year. The authors always attempt to submit their papers to the conferences and journals whose topics match the contents of their papers. A traditional physical “paper review system” contains three types of participants, i.e., authors, an editor of a conference proceeding or journal, and a group of reviewers, and it operates according to the following procedures and assumptions:

1. The editor of a conference proceeding or journal announces a publication schedule and information such as the topics of the conference or the journal, the deadline for paper submission, the date for notification of acceptance, the format of a submitted paper and so on.
2. The author of a paper submits her/his paper with her/his name to the conference or journal.
3. The editor receives the paper and she/he starts to check whether the paper matches the topics. After the due date of submission, the paper will be processed into the next stage if it passed the above verification. Otherwise, it will be returned to the author.
4. A group of reviewers will help the editor reviewing the papers. Nowadays this group is composed of the researchers in the same or similar research filed. The editor allocates some reviewers and invites them to review the paper. But the editor will hide the name of the author while allocating the paper.
5. The selected reviewers reply the invitation of the editor and receive the paper if they are willing to review it. Therefore, a lot of research people in the same research society inspect their papers each other.
6. The reviewers send their comments and results of the inspection back to the editor.
7. Finally, the editor collects all comments of the reviewers and then notifies the author whether the paper is accepted or not.


\textsuperscript{*}This work was supported in part by the National Science Council of the ROC (Taiwan) under grant NSC96-2221-E-110-071-MY3 and NSC97-2219-E-110-002.
Thus, we can divide the paper review procedure into three phases: (1) paper submission, (2) paper allocation and review, and (3) result decision. There are some drawbacks that we have found in the traditional paper review system as follows:

1. No Fairness: According to the steps described previously, the editor can know who the author of a paper is. Thus, the final result may be influenced by the personal attributes of the author such as the author’s institution or name. In the paper allocation phase, the editor may assign a paper which was written by his friends or a famed researcher to the reviewers who verifies the paper loosely. Moreover, the paper may be accepted more easily by the editor.

2. Privacy Leakage:
   2.1 Assume that a paper is not accepted by the editor. The rejected paper can be re-submitted to another conference or journal by its author. But the editor has known who the author of the paper is, and she/he may reveal it to someone else. Hence, the reviewers of the next conference or journal may have the name of the author of the paper before reviewing it.
   2.2 The editor knows the relationship between the reviewers and their comments on a paper. She/He is able to convince the author that someone has reviewed the paper.

   It is not good to let the editor know everything. As shown in [12], it has been widely believed that Anonymous Reviewing helps fairness of paper review, and the openly stated criticism might have some influences upon the reviewers’ careers. A common known truth is that some researchers, especially those who are at the beginning of their careers, may disincline to write negative review comments as it could hamper future promotions. In our point of view, we think that it also is necessary to keep reviewers anonymous such that the editor cannot get any evidence to convince anyone else of the fact of reviewing. In [3], it shows that the reviewer’s recommendations are frequently biased. Anonymous Submission may solve this problem. In this paper, we will present an anonymous paper review scheme with both submission and reviewing anonymity.

2. Related Works

Vincent Naessens, Liesje Demuyck, and Bart De Decker presented a fair anonymous submission and review system in 2006 [12]. Anonymous credentials were used as basic blocks. They claimed that anonymous credentials allow for anonymous yet accountable transactions between users and organizations. In [12], the authors presented a simplified version of the Idemix anonymous credential system [4][9].

The scheme of [12] presented a framework about an anonymous paper review system and [12] also showed that anonymous reviewing and anonymous submission can help the fairness of paper review. But it allows each attendant to use a pseudonym to keep anonymous in the protocol. It is not a good idea to achieve the anonymity property since the author of each paper needs to register a pseudonym with an organization. The registration may break the anonymity of the author if the organization is not trusted.

In addition, the editor in the protocol may record the messages of allocation for each paper in the paper review phase such that she/he can convince others of the reviewers’ identities of the paper. The scheme contains too many functions such that its structure is relatively complicated and it may be impractical for implementation.

3. Preliminaries

3.1 Partially Blind Signatures

Our anonymous paper review scheme adopts the functions of a partially blind signature scheme. In this subsection we will define a generic partially blind signature scheme. In the scenario of issuing a partially blind signature, the signer and a user are assumed to agree on a piece of common information, denoted as info. In some applications, info may be decided by the signer, while in some other applications it may just be sent from the user to the signer. Here we discuss the first case that info is decided by the signer only. Normally, a generic partially blind signature protocol [1][2][6][7][8] contains four phases: blinding, signing, unblinding, and verifying, which are described below.

1. Blinding: A user blinds a message and sends the blinded message to the signer to request the signer to sign it.
2. Signing: After receiving the blinded message, the signer signs the blinded message and the common information info by using its signing function and sends the signing result back. The signing result is called the partially blind signature since the common information info is clear to the signer.
3. Unblinding: The user unblinds the partially blind signature and then gets a signature of the signer on the combination of the original message and the common information info.
4. Verifying: Finally, the user or others can verify the signature by using the verifying formula with the parameters containing the signature, the message, and the common information info.

Now we introduce the functions that used in a generic partially blind signature scheme. Let $M$ be the underlying set of messages, $R$ be a finite set of random strings, $W$ be a finite set of strings with the predefined format which is negotiated by the signer and all users in advance. There are six elements $(G, B, S, H, U, V)$ in a generic partially blind signature scheme. They are defined as follows:

1. $G$: A probabilistic polynomial-time algorithm which takes a security parameter $k$ as the input and outputs a public and secret key pair $(PK, SK)$.
2. $H$: $M → M$ is a public one-way hash function.
3. $S$: $M × W → M^k$ is the signing function which is kept secret by the signer where $k$ is a positive integer. Given a message $m ∈ M$ and a common information $w ∈ W$, it is computationally infeasible to form $S(H(m), w)$ or modify $m$ and $w$ embedded in $S(H(m), w)$ without $S$, where $S(H(m), w)$ is called the signer’s signature on message $m$ and the common information $w$. 
4. \( V: M^k \times M \times W \rightarrow \{\text{TRUE}, \text{FALSE}\} \) is the public verification formula. \( V(t, H(m), w) = \text{TRUE} \) if and only if \( t \) is the signature of the signer on \( m \) with the common information. Therefore, \( V(S(H(m), w), H(m), w) \) is always true for each \( m \in M \) and \( w \in W \).

5. \( B: M \times R \rightarrow M \) is the blinding function. Select a random string \( r \in R \), which is prepared to be a blinding factor and kept secret by some user. The user takes \( r \) to form the blinded message \( B(H(m), r) \). Anyone cannot decide \( H(m) \) from the blinded message without the blinding factor \( r \).

6. \( U: M^k \times R \rightarrow M^k \) is the unblinding function. For each \( m \in M \), \( r \in R \), \( w \in W \), \( U \) can be used to shuck the blinding factor to get the signature on the clear message \( m \) and \( w \) such that \( U(S(B(H(m), r), w), r) = S(H(m), w) \). It is also impossible to decide \( S(H(m), w) \) from \( S(B(H(m), r), w) \) without \( r \).

3.2 Universal Designated-Verifier Signatures (UDVS)

In addition to a generic partially blind signature scheme, we use another technique called Universal Designated-Verifier Signatures (UDVS) [15][16]. A UDVS scheme is a digital signature scheme with an additional functionality which allows any holder of a signature to designate the signature to any desired designated-verifier such that the designated-verifier can verify that the message was signed actually by the signer but the verifier cannot use this signature to convince anyone else of this fact because her/his secret key allows her/him to forge the same signature without the signer’s cooperation. Hence, UDVS protects the privacy of signature holders from dissemination of signatures by verifiers. A UDVS scheme is made up by eight algorithms and a Verifier Key-Registration Protocol, \( P_{KR} \). All of these algorithms may be randomized. The functions of a UDVS scheme and the security notions are defined as follows.

1. Common Parameter Generation \( GC \): On inputting a security parameter \( k \), it outputs a string \( cp \) that consists of common scheme parameters.

2. Signer Key Generation \( GKS \): On inputting a common parameter string \( cp \), it outputs a key pair \( (SK_{Ri}, PK_{Ri}) \) for the signer \( i \).

3. Verifier Key Generation \( GKV \): On inputting a common parameter string \( cp \), it outputs a key pair \( (SK_V, PK_V) \) for the verifier.

4. Signing \( S \): On inputting a secret key \( SK_{Ri} \), and a message \( m \), it outputs a publicly-verifiable \( (PV) \) signature \( \sigma \) of the signer \( i \).

5. Public Verification \( V \): On inputting a signer’s public key \( PK_{Ri} \) and a string pair \( (m, \sigma) \) consisting of the message and corresponding signature, it outputs a verification result \( d \in \{\text{TRUE}, \text{FALSE}\} \).

6. Designation \( DV \): On inputting a signer’s public key \( PK_{Ri} \), a verifier’s public key \( PK_V \), and a message/PV-signature pair \( (m, \sigma) \), it outputs a designated-verifier \( (DV) \) signature \( \hat{\sigma} \).

7. Designated Verification \( VDV \): On inputting a signer’s public key \( PK_{Ri} \), a verifier’s secret key \( SK_V \), and a message/DV-signature pair \( (m, \hat{\sigma}) \), it outputs a verification result \( d \in \{\text{TRUE}, \text{FALSE}\} \).

8. Verifier Key-Registration \( P_{KR} \): A Verifier \( (VER) \) wishes to register a verifier’s public key with a Key Registration Authority \( (KRA) \). On inputting a common string \( cp \), \( VER \), and \( KRA \) sends messages alternately to each other. Then \( KRA \) outputs a \( (PK_V, Auth) \) pair where \( PK_V \) is a verifier’s public key and \( Auth \) is an authorization decision of the key-registration authority.

There are two major properties in UDVS, where one is unforgeability and the other is non-transferability privacy.

1. Unforgeability: A UDVS scheme consists of two types of unforgeability properties. The first property is \( PV \)-Unforgeability where the definition of the property is the same as the typical unforgeability notion under CMA (chosen-message attack) for the standard signature scheme which consists of \( GC, GKS, S \) and \( V \). The second one is \( DV \)-Unforgeability which makes it difficult for an attacker to forge a \( DV \)-signature \( \sigma' \) on a new message \( m' \) that can pass the \( DV \)-verification with a given designated-verifier’s public key \( PK_V \).

2. Non-Transferability Privacy: The goal of this property for a UDVS scheme is to protect the actual signer’s privacy. It prevents a designated-verifier from using the \( DV \)-signature on message \( m \) to convince someone that the signature on message \( m \) is signed by the actual signer.

3.3 The Requirements

In order to construct a secure anonymous review system, we collect the following security requirements.

1. Anonymity: The anonymity property is quite important in the paper review system. It is related to the fairness property and can be divided into several parts as follows:
   - Author—Editor: The author needs to blind her/his name when she/he submits her/his paper to the editor. The editor does not know who the author of the paper is such that she/he will allocate it to reviewers more fairly.
   - Author—Reviewer: The author also should cover her/his name to the reviewers. If her/his identity were known by the reviewers, the reviewers may be influenced when they give their comments.
   - Reviewer—Author: While a reviewer’s identity is not disclosed, she/he can inspect the paper more fairly. She/He will not be asked to give a good/bad comment by coercers, bribers, or the authors.

2. Uniqueness: None can claim that she/he is the author of a paper except that she/he is the actual one of it.

3. Comments Unforgeability: The comments can only be written by the reviewers. They cannot be forged.

4. Honesty: When a user submits her/his paper, she/he cannot be a reviewer of her/his own paper.
4. Proposed Anonymous Paper Review Scheme

We make use of the generic partially blind signature scheme, an anonymous secure channel [5][11], and a universal designated-verifier signature scheme [15][16] to design the anonymous paper review protocol. There are four parties in the protocol: a timestamp server, authors, an editor, and a group of reviewers where the authors get timestamp signatures from the timestamp server and submit their papers to the editor and the reviewers examine the quality of the papers. The editor decides whether the paper is accepted according to the responses and comments of the reviewers.

In order to make the protocol more simple, we assume that there is only one author for each paper. Our protocol is also suitable for that there are many authors of a paper. The protocol consists of four phases: preparing, submitting papers, dispatching papers, inspecting, and declaring the result, which are described in the followings.

Notations:

- $m$: the paper that an author wants to submit.
- $ID_i$: the identity of author $i$.
- $M$: the message space.
- $PK_{TS}$: the public key of the timestamp server.
- $SK_{TS}$: the secret key of the timestamp server.
- $H(\cdot)$: a one-way hash function.
- $ST_{SK}(\cdot)$: the signing function of the timestamp server based on a generic partially blind signature with key $SK$.
- $VT_{PK}(\cdot)$: the verifying function of the timestamp server based on the generic partially blind signature with key $PK$.
- $B_T(\cdot)$: the blinding function of the timestamp server.
- $U_T(\cdot)$: the unblinding function of the timestamp server.
- $PK_E$: the public key of the editor.
- $SK_E$: the private key of the editor.
- $E_{PK}(\cdot)$: an encrypting function with key $PK$.
- $D_{SK}(\cdot)$: a decrypting function with key $SK$.
- $S_{SK}(\cdot)$: a signing function with key $SK$.
- $V_{PK}(\cdot)$: a verifying function with key $PK$.
- $PK_{R_i}$: the public key of the $i$-th reviewer.
- $SK_{R_i}$: the secret key of the $i$-th reviewer.
- $VD_{SK}(\cdot)$: the $DV$-signature verifying function with private key $SK$ in a UDVS scheme.
- $DV_{PK}(\cdot)$: the designating function with the public key $PK$ of the designated-verifier in the UDVS scheme.
- $A_m$: the abstract of a paper $m$.
- $C_i$: the decision of reviewer $i$ for inspecting a paper, i.e., “YES” or “NO”.
- $Time$: the string of time created by the timestamp server.
- $Comment_i$: the comment that reviewer $j$ sends to the editor.

Candidate pool: the reviewers whose decision for inspecting a paper is “YES”.

1. Preparing Phase:

In the preparing phase, we have some steps to do and they are shown as follows.

(a) An author $ID_i$ chooses a random string $r$ as a blinding factor.
(b) Let $m$ be the paper of the author. She/He uses the blinding factor $r$ to compute the blinded message $\alpha = B_T(H(m||ID_i), r)$ and sends $\alpha$ to the timestamp server.
(c) Then the timestamp server sets the string of current time, $Time$, according to its clock. It signs $\alpha$ and $Time$ with the private key $SK_{TS}$ by computing $Z = ST_{SK_E}(\alpha, Time)$.
(d) The timestamp server sends $Z$ and $Time$ to the author.
(e) The author uses her/his blinding factor $r$ and $U_T$ to unblind $Z$ and then obtains $S = U_T(Z, r)$. The 4-tuple $(S, m, ID_i, Time)$ is valid since $VT_{PK_E}(S, H(m||ID_i), Time) = TRUE$. Thus, the author gets a paper credential $Sig = (S, m, ID_i, Time)$.

2. Submitting Paper:

This phase is shown as follows.

(a) The author encrypts her/his own paper $m$, which does not contain any identification information of the author, and sends it to the editor via an anonymous channel.
(b) After receiving the encrypted paper $E_{PK_E}(m)$, the editor decrypts it with her/his private key $SK_E$ to get the paper $m$. The editor does not know who the real author of $m$ is.

3. Dispatching Paper:

When the editor obtains paper $m$, she/he needs to select some reviewers to inspect it. But it is an important issue that how the editor chooses them. We hope to prevent the reviewers from being bullied by the author. Hence, the followings are our dispatching steps, which also are shown as follows.

(a) The editor signs the abstract $A_m$ of the paper $m$ with the private key to generate $Sig_{A_m} = S_{SK_E}(H(A_m))$.
(b) Then she/he encrypts $A_m$ and $Sig_{A_m}$ with the public key of each reviewer $i$ by computing $EN_{A_m, R_i} = E_{PK_{R_i}}(A_m, Sig_{A_m})$.
(c) She/He sends $EN_{A_m, R_i}$ to each reviewer $i$ and asks her/him to return the decision about inspecting this paper.
(d) Reviewer $i$ decrypts $EN_{A_m, R_i}$ and reads the abstract $A_m$ of the paper. She/He can also check the correctness of $Sig_{A_m}$ via $V_{PK_E}$.
(e) Reviewer $i$ sets the decision $C_i$ which may be “YES” or “NO”. Here we ask the author to set her/his decision as “NO” if she/he also is a reviewer.
(f) Reviewer $i$ signs $C_i$ and $A_m$ to generate a $PV$-signature $\beta_i = S_{SK_{R_i}}(H(A_m||C_i))$.
(g) Finally, reviewer $i$ designates the editor to be the designated-verifier by computing $\tilde{\beta}_i = DV_{PK_E}(\beta_i)$. She/He sets $\delta_i = (\tilde{\beta}_i, (A_m, C_i))$ subsequently and sends it to the editor.
(h) The editor verifies $\delta_i$ by using the $DV$-signature verifying function $VD_{PV}$ with $PK_{R_i}$ and $SK_E$ and then checks the decision of the reviewer. If the decision of the reviewer is “YES”, the editor will add the reviewer to the candidate pool.
(i) After all reviewers finishing step c) to step g), the editor chooses some reviewers in the candidate pool randomly and go to next phase, i.e., 4).

4. Inspecting and Declaring the Result:

In the phase, the editor will decide whether the paper can be accepted or not according to the comments of the selected reviewers. The identities of the reviewers inspecting the paper cannot be known by the anyone else. Hence, we make use of a UDVS scheme to help achieving this goal.

(a) The editor sends the ciphertext $E_{PK_{R_j}}(m, Sig_m)$ to each selected reviewer $j$, where $Sig_m$ is the signature of $m$ signed by the editor.

(b) The selected reviewers decrypt $EN_{m, R_j}$ to get $m$ and check whether $Sig_m$ is valid or not by $V_{PK_E}$. Each of them writes down her/his comment $\text{comment}_j$ and signs on it with $m$, i.e., each selected reviewer $j$ computes $\gamma_j = SK_{R_j}(H(m||\text{comment}_j))$.

(c) They generate their $DV$-signatures $\gamma_j = DV_{PK_E}(\gamma_j)$ for all $j$ and assign the editor to be the designated-verifier. And they send back $\varepsilon_j = (\gamma_j, (m, \text{comment}_j))$ for all $j$ to the editor.

(d) The editor verifies each $\varepsilon_j$ via $VDV$ with $PK_{R_j}$ and $SK_E$.

(e) After all selected reviewers send back their own $\varepsilon_j$'s, the editor can decide whether the paper $m$ can be accepted according to the comments of the reviewers.

(f) The result of inspecting paper $m$ will be published by the editor. The author of the paper $m$ must show her/his paper credential $Sig$, which has been obtained in the first phase, to tell the editor that she/he is the actual author of the paper $m$ when the paper $m$ is accepted.

5. Security Analysis

In this section, we will explain why our protocol satisfies all requirements shown in subsection 3.3 of Section III.

1. Anonymity:

The author’s identity is blinded in the preparing phase. The author chooses a blinding factor to hide her/his name. Nobody can know who the actual author is before the paper is accepted. Therefore, her/his identity will not be revealed during the review scheme.

(a) Author → Editor: The author’s network address is kept secret by using an anonymous channel when she/he submits her/his paper to the editor. The editor only receives an anonymous paper without any unnecessary information. Therefore, it is successful to keep the author anonymous to the editor.

(b) Author → Reviewer: The reviewers get the same message as the editor received in the submitting paper phase. There is only an anonymous paper which does not contain the author’s identity. The author is also anonymous to the reviewers.

(c) Reviewer → Author: When a reviewer gives her/his comments on the author’s paper to the editor, she/he uses the UDVS scheme [15][16] to protect her/his own anonymity. The reviewer is the signer of the comments and the signature designator. She/He designates that the editor is the only verifier to check the designated-verifier signature which produced by the reviewer. But the editor can also use her/his secret key to generate the $DV$-signature which is the same as the one produced by the reviewer. When the author receives the comments published by the editor, she/he cannot know who the reviewer is. The editor cannot prove that the $DV$-signature $\gamma_j$ was produced by the reviewer $j$. Thus, the reviewer’s identity is unknown to the author.

The author’s name cannot be known before the paper is accepted by the editor. An author can submit her/his paper to any conference or journal with privacy protection. Owing to the anonymity property, the editor will allocate the paper to reviewers more fairly in the dispatching paper phase. The editor does not have any other information about the author such that she/he can just follow the legal processes of dispatching paper. During the view process of each reviewer, she/he can give her/his comments just depending on the professional knowledge without being influenced by the reputation of the author. Also, the reviewer is only responsible to the editor and she/he is anonymous to other people including the author. She/He is not afraid to write negative comments about the author to offend the author. In the inspecting phase, the editor receives the $DV$-signature $\gamma_j$ from the reviewer $j$. She/He cannot convince the author that $\gamma_j$ was made by the reviewer. We take advantages of UDVS such that the editor (the designated verifier) can produce the same signature $\gamma_j$. Finally, the editor decides whether the paper is accepted only depending on the comments received from the reviewers. It will be more fair.

2. Uniqueness:

To modify $(m||ID_i)$ and $Time$ in $Sig$ produced in the first phase is infeasible since the timestamp server has signed on them. Thus, an attacker cannot forge a signature containing $m$ and an earlier time $Time$ to impersonate the actual author. A pilferer may have the same paper to get $Sig'$ and submits it to another conference or journal, but she/he will be detected when she/he shows her/his $Sig'$ and $ID_i$. The $Time$ in $Sig'$ is always later than $Time$ in $Sig$. Hence, the paper only be owned by a unique author or a unique group of authors.

3. Comment Unforgeability

In a UDVS scheme [15][16], the unforgeability is concluded. The unforgeability of a UDVS scheme contains $DV$-signature unforgeability and $PV$-signature unforgeability. We make use of the two unforgeabilities to achieve comment unforgeability by adopting a secure UDVS scheme which satisfies the two properties.

4. Honesty:

In the dispatching paper phase, we show the abstract of the
paper to all reviewers to ask them to return their decisions about inspecting the paper. The editor chooses some reviewers whose decisions are “YES”. Here, we ask the author of the paper to set her/his decision as “NO”. Therefore, if she/he set her/his \( C \) = “YES” and was selected by the editor, the editor can detect it in the final phase. When the author shows her/his identity to declare that the accepted paper was written by herself/himself, the editor can check whether the author is one of the selected reviewers.

6. Conclusions

In this paper, we have proposed an anonymous paper review scheme which can make paper review more fair. We make use of a partially blind signature scheme and a universal designated-verifier signature scheme as the underlying key techniques to construct the proposed anonymous paper review scheme with the anonymity property. The anonymity property in the proposed scheme can help the scheme to achieve the most important property, i.e., fairness. Therefore, the attendants in our scheme can more fairly do their jobs without worrying about anything. All characteristics of our scheme are summarized as follows:

1. The proposed scheme protects the privacy of authors and reviewers.
2. It can be realized and implemented easily.
3. The proposed idea is independent of the underlying partially blind signature scheme and UDVS scheme and we can use any secure partially blind signature and UDVS schemes to implement it.
4. It is suitable for different types of review schemes.

Finally, the comparisons among our scheme, the previous protocol [12], and traditional paper review system are shown in Table 1.

References


<table>
<thead>
<tr>
<th>Table 1. Comparisons</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
</tr>
<tr>
<td>Ours</td>
</tr>
<tr>
<td>T¹</td>
</tr>
<tr>
<td>[12]</td>
</tr>
</tbody>
</table>

✓: Satisfied; ×: Not satisfied; △: Satisfied under some strong assumption

P1: Author Anonymity to Reviewer
P2: Reviewer Anonymity to Author
P3: Author Anonymity to Editor
P4: Comment Unforgeability
P5: Uniqueness
P6: Honesty

¹: Traditional paper review system
²: The editor may reveal the author’s identity
³: The editor may reveal the reviewers’ identities
⁴: It needs a fully trusted third party to guarantee the property.