Another Look at Non-Frameability in Group Signatures for Anonymous Auctions

Cao Shiqi*[1] and Keita Emura†[1,2]

[1.]Kanazawa University, Japan.
[2.]AIST, Japan.

June 9, 2026

Abstract

In addition to anonymity and traceability, which are the primary security properties of group signatures, non-frameability is also defined (Bellare-Shi-Zhang, CT-RSA 2005). This property guarantees that even an adversary colluding with all authorities (the opener and the issuer) cannot produce a signature that frames an honest user, and it is regarded as a security notion that protects users. In this short note, we introduce a new perspective on non-frameability, namely that it can also protect the authorities, and we examine its significance in the context of anonymous auctions, a well-known application of group signatures. We show that non-frameability serves as an effective countermeasure against situations in which a winning bidder falsely claims not to have placed a bid and accuses the organizer of forgery.

1 Introduction

In a group signature scheme [7], a verifier can check the validity of a signature without identifying the signer, thereby ensuring anonymity. At the same time, a group manager can identify the signer by using its own secret key. Owing to these functionalities, anonymity and traceability are widely recognized as the primary security properties of group signatures. Indeed, in the BMW (Bellare-Micciancio-Warinschi) model [3], which formalizes the standard security notions for group signatures, it is shown that satisfying full anonymity and full traceability encompasses all previously defined security requirements. The BMW model considers a static-group setting, meaning that all members' signing keys are generated when the group public key is generated, and member join or revocation after that point is not supported. Moreover, the two roles of issuing signing keys and opening signatures are both assigned to a single authority (the group manager).

To address these limitations, the BSZ (Bellare-Shi-Zhang) model [4] introduces a dynamic-group setting, in which new members can be added after the group public key has been generated. It also separates the managerial roles by defining a signing-key issuer and a signature opener. This separation enables a more precise trust-level setting in each authority. For example, in the anonymity game, the adversary may collude with the issuer, while in the traceability game, the adversary

*This work was done when the first author, Cao Shiqi, was with Kanazawa University. She is currently a master student at Japan Advanced Institute of Science and Technology.

†Corresponding Author: k-emura@se.kanazawa-u.ac.jp

may collude with the opener. In other words, anonymity must remain secure even against a malicious issuer, and traceability must remain secure even against a malicious opener. Independently and concurrently, the KY (Kiayias-Yung) model [11] was proposed, which also considers dynamic groups and separates the authorities.

Furthermore, several extensions have been studied, including revocable group signatures [5, 10, 12, 13, 15], which incorporate member revocation, as well as fully dynamic models [6] and their everlasting variants [9], which support both member join and revocation after the group public key has been generated.[1]

Non-Frameability. Besides anonymity and traceability, another well-known security notion for group signatures is non-frameability. As mentioned earlier, anonymity and traceability are widely regarded as the primary security properties of group signatures. However, in the BSZ model [4], where non-frameability was introduced, it is positioned as one of the Three Key Requirements, standing alongside anonymity and traceability as an equally important security property. Specifically,

> *We formulate three key requirements, namely anonymity, traceability and non-frameability.* [4]

Intuitively, non-frameability guarantees that even if all entities other than a particular signer, including the issuer and the opener, collude, they still cannot generate a valid group signature that opens to that non-colluding signer. It is important to emphasize here that, unlike in the anonymity and traceability games, the adversary is allowed to collude with both authorities. In the BSZ paper, the trust assumptions regarding the authorities are described as follows.

> *We consider different levels of trust in each authority, namely that it may be uncorrupt (trusted), partially corrupt (its secret key is available to the adversary but it does not deviate from its prescribed program) or fully corrupt (the adversary controls it entirely, so that it may not follow its program). In order to protect group members against dishonest authorities to the maximum extent possible, we formulate security requirements to require the lowest possible level of trust in each authority.* [4]

It summarizes the trust levels of the authorities for each security notion. In light of this background, non-frameability can be regarded as a security property defined as a security guarantee that must hold even when all authorities act as adversaries, and it is therefore positioned fundamentally as a notion that protects users (i.e., signers).

Our Contribution. In this short note, we introduce a new perspective on non-frameability, viewing it as a security property that also protects the authorities, and we examine its significance in the context of anonymous auctions, a widely recognized application of group signatures. Specifically, we show that non-frameability serves as an effective countermeasure against situations in which a winning bidder falsely claims not to have placed a bid and accuses the organizer of forgery.

We first examined prior works on anonymous auctions constructed using group signatures [14, 16, 18–22] to determine whether they discuss a perspective of non-frameability similar to ours. In all of the papers we explored, anonymity is employed as the mechanism for protecting bidders' privacy, and traceability is employed as the mechanism for identifying the winning bidder, which together justify the use of group signatures. The work of Trevathan et al. [20] requires exculpability, a property implied by non-frameability in group signatures. Liu et al. [14] require what they call no framing, meaning that even the authorities cannot impersonate the winning bidder. However,

[1] The BSZ model is sometimes referred to as a partially dynamic model to distinguish it from fully dynamic models.

none of these papers address the perspective we advocate in this note, namely that non-frameability serves as a security notion for protecting the authorities.

Related Work. Security notions encompassed by non-frameability include exculpability [1] and framing resistance [8]. The KY model [11], proposed independently and concurrently with the BSZ model, also defines a notion of framing. Moreover, non-frameability is defined in the fully dynamic model [6], which extends the BSZ framework. Unframeability is likewise defined in set pre-constrained group signatures [2]. To the best of our knowledge, none of these works discuss the perspective we advocate in this paper, namely that non-frameability can be viewed as a security notion for protecting the authorities. Based on these observations, we conclude that another look at non-frameability, viewed from the perspective of protecting the authorities, provides an additional viewpoint that does not appear to have been explored in prior work, to the best of our knowledge.

2 Group Signatures and Non-Frameability

In this section, we present the definitions of group signatures and non-frameability in the BSZ model. For the other security notions, the reader is referred to the BSZ paper [4]. A group signature scheme GS consists of eight algorithms $(\mathsf{GKg}, \mathsf{UKg}, \mathsf{Join}, \mathsf{Iss}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Open}, \mathsf{Judge})$ defined as follows.

Definition 1 (Syntax of Group Signatures)**.**

GKg: *The group key generation algorithm takes a security parameter $k \in \mathbb{N}$ as input, and outputs a group public key* gpk*, an issuer key* ik*, and an opening key* ok*.*

UKg: *The personal user key generation algorithm (for an entry i) takes a security parameter $k \in \mathbb{N}$, and outputs a user public key* $\mathsf{upk}[i]$ *and a user secret key* $\mathsf{usk}[i]$*.*

Join, Iss: *The group joining protocol (for an entry i) is defined by non-interactive algorithms* Join *and* Iss*. Each algorithm takes an incoming message and current state information, and outputs an outgoing message, updated state information, and the result (accept, reject, cont). If the issuer accepts, the i-th entry of the registration table* reg*,* $\mathsf{reg}[i]$*, stores final stare information output by* Iss*. If i accepts, the final state output by* Join *is a signing key* $\mathsf{gsk}[i]$*.*

GSig: *The signing algorithm takes* gpk*,* $\mathsf{gsk}[i]$*, a message to be signed $m \in \{0,1\}^*$ as input, and outputs a group signature σ.*

GVf: *The verification algorithm takes* gpk*, $m \in \{0,1\}^*$, and σ as input, and outputs 0 or 1.*

Open: *The opening algorithm takes* gpk*,* ok*,* reg*, m, and σ as input, and outputs an integer $i \geq 0$ and a proof τ. If $i \geq 1$, it indicates that there is a group member whose entry identity is i generated σ. If $i = 0$, then it indicates there is no member who generated σ.*

Judge: *The judge algorithm takes* gpk*, an integer j,* $\mathsf{upk}[j]$*, m, and a valid group signature σ on m, and τ as input, and outputs 0 or 1.*

Definition 2 (Non-Frameability)**.** *We define the following experiment* $\mathsf{Exp}^{\mathsf{nf}}_{\mathsf{GS},\mathcal{A}}(k)$*. Let $\mathcal{A}$ be an adversary and $\mathcal{C}$ be the challenger.*

1. *$\mathcal{C}$ runs* $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \leftarrow \mathsf{GKg}(1^k)$*, and gives* $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$ *to $\mathcal{A}$. Initialize the set of corrupted users* $\mathsf{CU} := \emptyset$ *and the set of honest users* $\mathsf{HU} := \emptyset$*.*

2. *$\mathcal{A}$ is allowed to access the five oracles* $(\mathsf{SndToU}, \mathsf{WReg}, \mathsf{GSig}, \mathsf{USK}, \mathsf{CrptU})$.

   $\mathsf{SndToU}(i, M_{in})$**:** *$\mathcal{A}$ runs the group joining protocol as the issuer. If $i \notin \mathsf{HU}$, then the oracle runs $(\mathsf{upk}[i], \mathsf{usk}[i]) \leftarrow \mathsf{UKg}(1^k)$, and adds i to* HU*. The oracle runs the* Join *algorithm that takes M_{in} and state information $(\mathsf{gpk}, \mathsf{upk}[i], \mathsf{usk}[i])$ of i, and gives the output to $\mathcal{A}$.*

   $\mathsf{WReg}(i, \rho)$**:** *Set $\mathsf{reg}[i] = \rho$.*

   $\mathsf{GSig}(i, m)$**:** *If either $i \notin HU$ or $\mathsf{gsk}[i] = \epsilon$, output $\perp$. Otherwise, return the result of $\mathsf{GSig}(\mathsf{gpk}, \mathsf{gsk}[i], m)$.*

   $\mathsf{USK}(i)$**:** *Return $(\mathsf{gsk}[i], \mathsf{usk}[i])$.*

   $\mathsf{CrptU}(i, \mathsf{upk})$**:** *If $i \in \mathsf{HU} \cup \mathsf{CU}$, then return $\perp$. Add i to* CU *and set $\mathsf{upk}[i] = \mathsf{upk}$.*

3. *$\mathcal{A}$ outputs (m, σ, i, τ). If all the followings hold, then output 1, and 0 otherwise.*

   (a) $\mathsf{GVf}(\mathsf{gpk}, m, \sigma) = 1$

   (b) $i \in \mathsf{HU}$, $\mathsf{gsk}[i] \neq \epsilon$, *and* $\mathsf{Judge}(\mathsf{gpk}, i, \mathsf{upk}[i], m, \sigma, \tau) = 1$

   (c) $\mathcal{A}$ did not query $\mathsf{USK}(i)$ *or* $\mathsf{GSig}(i, m)$.

The advantage of $\mathcal{A}$ is defined as $\mathsf{Adv}^{\mathsf{nf}}_{\mathsf{GS},\mathcal{A}}(k) = \Pr[\mathsf{Exp}^{\mathsf{nf}}_{\mathsf{GS},\mathcal{A}}(k) = 1]$. *We say that* GS *provides non-frameability if* $\mathsf{Adv}^{\mathsf{nf}}_{\mathsf{GS},A}(k)$ *is negligible for all probabilistic polynomial-time adversaries $\mathcal{A}$.*

In a model where the issuer generates $\mathsf{gsk}[i]$ and hands it to user i, an adversary $\mathcal{A}$ possessing the issuer key ik can easily break non-frameability. In the BSZ model, the use of an interactive join protocol enables the definition of secret information known only to the user, $\mathsf{usk}[i]$, thereby ensuring that even the issuer does not learn all the values contained in $\mathsf{gsk}[i]$.

3 Another Look at Non-Frameability in Anonymous Auctions

Anonymous Auctions with Group Signatures. We begin by describing the workflow of an anonymous auction constructed using group signatures. Essentially, the identity of bidders is hidden by the anonymity of the underlying group signature scheme, while the winner can be identified through traceability. This design principle is common to all group-signature-based anonymous auctions of which we are aware [14, 16, 18–22]. An anonymous auction consists of four parties: the organizer, the bidders, the registration authority, and the verifier. The organizer corresponds to the opener in a group signature scheme, the bidders correspond to the users, the registration authority corresponds to the issuer, and the verifier corresponds to the signature verifier. The procedures executed in each phase among these entities are outlined below.

Given $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok}) \leftarrow \mathsf{GKg}(1^k)$, the organizer holds ok, and the registration authority holds ik. The description that follows adheres to the syntax of the BSZ model, although the setting can be adapted depending on the model. For example, the verifier may be any entity other than the organizer, even if the organizer possesses the opening key. In the BSZ model, an anonymity adversary is allowed to collude with the issuer, so the registration authority may also serve as the verifier. In models where the authorities are not separated, the organizer and the registration authority are represented by the same entity. Precisely, the organizer plays the roles of the registration authority in the BMW model [3] that does not provide non-frameability.

1. Registration Phase

- The bidders prove to the registration authority that they are eligible to participate in the auction. Since this procedure is independent of the group signature scheme, we omit the details.
- If the bidder's eligibility is confirmed, the registration authority and the bidder execute the group-joining protocol $(\mathsf{Join}, \mathsf{Iss})$, and the bidder obtains the signing key gsk. In a static-group setting, the registration authority simply sends gsk to the bidder.

2. Bidding Phase

   - The bidder uses their signing key gsk to generate a group signature on the bid value and submits it to the verifier.
   - The verifier uses gpk to check that the bid was submitted by a legitimate participant. Note that, due to the anonymity property of the group signature, the verifier cannot identify the bidder.

3. Winner Determination Phase

   - The verifier determines the winning bid from the submitted bid values and sends the corresponding group signature to the organizer.
   - The organizer uses ok to identify the winning bidder.

In an anonymous auction constructed using group signatures, bidders can submit their bids without revealing their identities, thereby hiding who bid what amount, while allowing only the organizer to identify the winning bidder.

Role of Non-Frameability: A Current Prospective. As a natural motivation, suppose that the organizer prefers the auction to be won at a higher price. If a group signature scheme that does not satisfy non-frameability is used, the following attack becomes possible:

- The organizer impersonates a particular bidder and submits an excessively high bid.
- The impersonated bidder cannot deny having placed the bid, due to the anonymity property.

Such an attack may illustrate the necessity of non-frameability. If the group signature scheme satisfies non-frameability, it guarantees that even the organizer, even when colluding with the registration authority, cannot impersonate the winning bidder. In other words, it cryptographically prevents the scenario described above, in which an entity that is not the actual winning bidder is nevertheless identified as the winner and consequently forced to pay the winning price.

From the above, non-frameability can first be viewed as a form of security that protects users (the bidders). Nevertheless, one might argue that:

- An organizer who impersonates a bidder would lose public trust, and no one would participate in future auctions.
- From this perspective, the organizer has no incentive to impersonate a bidder in the first place.

Thus, one might think that non-frameability is unnecessary if social deterrents are sufficient to prevent the organizer from impersonating bidders, even without cryptographic guarantees. It is therefore natural to ask whether there is a more appropriate interpretation of the significance of non-frameability in anonymous auctions.

Role of Non-Frameability: A New Prospective. We now present a new perspective in which non-frameability acts as a security property that protects the organizer and the registration authority. Consider an anonymous auction that uses a group signature scheme that does not satisfy non-frameability, and suppose that the winning bidder claims:

- I did not place this bid, and perhaps the organizer impersonated me.

Of course, the opening result identifies this bidder, and the correctness of the opening procedure is verified by the Judge algorithm, which proves that the organizer has performed the opening correctly. However, as long as there remains the possibility that the organizer could generate a group signature on behalf of the bidder, it should be noted that this verification does not establish that the organizer did not impersonate the bidder. Here, we exclude the case in which the bidder colludes with the organizer and the registration authority, as this would trivially yield a group signature that opens to the bidder.

A winning bidder may have various motivations for making such a claim, such as dissatisfaction with the winning price or simply a change of mind. Moreover, if cancellations of winning bids were allowed, one could even imagine manipulating the winning price by placing casual bids at arbitrary amounts. Even if the rules prohibit cancellation, the organizer may still suffer reputational damage if there is no evidence to refute the allegation that the organizer impersonated the bidder.

If the group signature scheme satisfies non-frameability, the organizer can assert that:

- It is cryptographically guaranteed that even the organizer cannot generate a group signature on behalf of a bidder, even when colluding with the registration authority.

In other words, non-frameability serves as effective evidence against false accusations made by the winning bidder. For this reason, we argue that non-frameability can also be interpreted as a security property that protects the organizer.

To more clearly demonstrate that non-frameability can be interpreted as a security notion protecting the organizer, we explicitly describe the impersonation attack and the advantage is bounded by the advantage of non-frameability. Here, an adversary $\mathcal{A}$ produces a group signature σ and tries to claim that the authorities (the organizer and the registration authority) produce σ on behalf of a bidder who does not collude with the authorities. We construct an algorithm $\mathcal{B}$ that breaks non-frameability using $\mathcal{A}$ as follows. The non-frameability challenger $\mathcal{C}$ gives $(\mathsf{gpk}, \mathsf{ik}, \mathsf{ok})$ to $\mathcal{B}$. $\mathcal{B}$ sends gpk to $\mathcal{A}$ (this setting is natural since $\mathcal{A}$ does not collude with the authorities). For some $n \in \mathbb{N}$ ($n \geq 1$) and $i \in [n]$, $\mathcal{B}$ executes $\mathsf{SndToU}(i, M_{in})$ and then $i \in \mathsf{HU}$ and $\mathsf{upk}[i]$ is generated and published. Without loss of generality, let $i^* \in [n]$ be the identity of the target bidder to be claimed as impersonated. Finally, $\mathcal{A}$ produces (m, σ) where $\mathsf{GVf}(\mathsf{gpk}, m, \sigma) = 1$ and claims that $\mathcal{B}$ produces (m, σ) on behalf of the bidder i^*. Since $\mathcal{B}$ does not issue CrptU for all $i \in [n]$, $i^* \in \mathsf{HU}$. $\mathcal{B}$ runs $(i^*, \tau) \leftarrow \mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, \mathsf{reg}, m, \sigma)$. Then, $\mathsf{Judge}(\mathsf{gpk}, i^*, \mathsf{upk}[i^*], m, \sigma, \tau) = 1$ holds. $\mathcal{B}$ outputs (m, σ, i^*, τ) and breaks non-frameability. In other words, if $\mathcal{A}$ can produce a group signature that opens to an honest and non-colluding bidder and claims that the organizer impersonates the bidder, then non-frameability can be broken. To sum up, under the assumption that the underlying group signature scheme provides non-frameability, no adversary can make such a claim.

We would like to clarify the setting captured in the reduction. We explicitly exclude the case where the bidder colludes with the organizer and the registration authority, as this would trivially lead to a group signature that can be opened to the bidder. In the security proof, the adversary $\mathcal{A}$ does not obtain $\mathsf{gsk}[i^*]$, since the only way to add a user to the group is via the SndToU oracle, where the adversary in the non-frameability game plays the role of the issuer, and $i^* \in \mathsf{HU}$ is required. Under this setting, for a group signature on the highest bid that opens to a winning

bidder, the signature must have been generated either by the winner or by the organizer colluding with the winner. In both cases, the winner is necessarily involved in generating the signature. In addition, the adversary is not allowed to send a query $\mathsf{GSig}(i^*, m)$ where m is the challenge message generated by $\mathcal{A}$. This restriction ensures that, even if the organizer observes a signature $\mathsf{GSig}(i^*, m')$ for some m', the organizer cannot modify m' into a higher bid m. That is, even if the winner claims that they only submitted $\mathsf{GSig}(i^*, m')$ and attempts to argue that the organizer altered it into a higher bid $m > m'$, such a claim cannot be justified, as non-frameability guarantees that forging $\mathsf{GSig}(i^*, m)$ is infeasible unless the winner colludes with the organizer.

4 Conclusion

In this short note, we introduced a new perspective of non-frameability as a security property that protects the authorities, and we demonstrated that it is effective as a countermeasure when a winning bidder makes a false claim in an anonymous auction.

As information that helps participants decide whether they can safely take part in an anonymous auction, the organizer may emphasize that it is cryptographically guaranteed that the organizer cannot place bids by impersonating bidders. As future work, we plan to investigate, for example through questionnaires, whether the presence or absence of non-frameability actually influences users' decisions to participate in anonymous auctions.

Anonymous auction schemes that do not explicitly use group signatures are outside the scope of this study. Such schemes may define a security notion analogous to non-frameability, and examining this point is left for future work. Our analysis focused on anonymous auctions, a representative application of group signatures. As another direction, we will investigate whether non-frameability can similarly serve as a security property that protects authorities in other applications of group signatures.

Non-frameability appears to be related to non-repudiation. If the opening result of a group signature identifies a user i, and the opening proof π is accepted by the Judge algorithm, then no entity other than i can have produced the group signature due to non-frameability. This implies that user i indeed generated the signature, and that i cannot repudiate having done so. Actually, in the BSZ paper [4], it is written that

> *Non-frameability asks that the adversary be unable to create a judge-accepted proof that an honest user produced a certain valid signature unless this user really did produce this signature. (This implies the more usual formulation, namely that it cannot produce a signature that an honest opener would attribute to a user unless the latter really did produce it, because, if it could produce such a signature, it could also produce the judge-accepted proof. The latter is true because we give it the secret key of the opener).*

We expected that opening soundness [6, 17] would also be required in order to guarantee the soundness of the opening proof. Further investigation of this connection is an interesting direction for future work.

Acknowledgment: The authors would like to thank the anonymous reviewers for their invaluable comments and suggestions. This work was partially supported by the Telecommunications Advancement Foundation.

References

[1] Giuseppe Ateniese and Gene Tsudik. Some open issues and new directions in group signatures. In *Financial Cryptography*, pages 196–211, 1999.

[2] James Bartusek, Sanjam Garg, Abhishek Jain, and Guru-Vamsi Policharla. End-to-end secure messaging with traceability only for illegal content. In *EUROCRYPT Part V*, pages 35–66, 2023.

[3] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *EUROCRYPT*, pages 614–629, 2003.

[4] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In *CT-RSA*, pages 136–153, 2005.

[5] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In *ACM CCS*, pages 168–177. ACM, 2004.

[6] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, and Jens Groth. Foundations of fully dynamic group signatures. In *Applied Cryptography and Network Security*, pages 117–136, 2016.

[7] David Chaum and Eugène van Heyst. Group signatures. In *EUROCRYPT*, pages 257–265, 1991.

[8] Lidong Chen and Torben P. Pedersen. New group signature schemes (extended abstract). In *EUROCRYPT*, pages 171–181, 1994.

[9] Yimeng He, San Ling, Khai Hanh Tang, and Huaxiong Wang. Everlasting fully dynamic group signatures. In *Applied Cryptography and Network Security*, pages 3–28, 2025.

[10] Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka, and Keisuke Tanaka. Fully anonymous group signature with verifier-local revocation. In *Security and Cryptography for Networks*, pages 23–42, 2018.

[11] Aggelos Kiayias and Moti Yung. Secure scalable group signature with dynamic joins and separable authorities. *Int. J. Secur. Networks*, 1(1/2):24–45, 2006.

[12] Benoît Libert, Thomas Peters, and Moti Yung. Group signatures with almost-for-free revocation. In *CRYPTO*, pages 571–589, 2012.

[13] Benoît Libert, Thomas Peters, and Moti Yung. Scalable group signatures with revocation. In *EUROCRYPT*, pages 609–627, 2012.

[14] Xin Liu, Qiu-Liang Xu, and Jiu-Qing Shang. A public auction scheme based on group signature. In *InfoSecu*, pages 136–142. ACM, 2004.

[15] Callum London, Daniel Gardham, and Constantin Catalin Dragan. Dynamic group signatures with verifier-local revocation. In *IEEE CSF*, pages 473–488, 2025.

[16] Khanh Quoc Nguyen and Jacques Traoré. An online public auction protocol protecting bidder privacy. In *ACISP*, pages 427–442, 2000.

[17] Yusuke Sakai, Jacob C. N. Schuldt, Keita Emura, Goichiro Hanaoka, and Kazuo Ohta. On the security of dynamic group signatures: Preventing signature hijacking. In *Public Key Cryptography*, pages 715–732, 2012.

[18] Kouichi Sakurai and Shingo Miyazaki. An anonymous electronic bidding protocol based on a new convertible group signature scheme. In *ACISP*, pages 385–399, 2000.

[19] Yanbin Sun, Yan Sun, Mingxing Luo, Lize Gu, Shihui Zheng, and Yixian Yang. Comment on Lee et al.'s group signature and e-auction scheme. *Inf. Syst. Frontiers*, 15(1):133–139, 2013.

[20] Jarrod Trevathan, Hossein Ghodosi, and Wayne Read. An anonymous and secure continuous double auction scheme. In *IEEE HICSS*, 2006.

[21] Cheng-Yi Tsai, Pi-Fang Ho, and Min-Shiang Hwang. A secure group signature scheme. *Int. J. Netw. Secur.*, 20(2):201–205, 2018.

[22] Ding Yong, Li Bin, and Zheng Zhaoxia. An electronic auction scheme based on group signatures and partially blind signatures. *Procedia Engineering*, 15:3051–3057, 2011. CEIS 2011.