Generalized Adaptor Signature Scheme: From Two-Party to N-Party Settings

Kaisei Kajita[1], Go Ohtake[1], and Tsuyoshi Takagi[2]

[1] Japan Broadcasting Corporation, Tokyo, Japan
kajita.k-bu@nhk.or.jp
[2] the University of Tokyo, Tokyo, Japan

Abstract. Adaptor signatures have attracted attention as a tool to address scalability and interoperability issues in blockchain applications, for example, such as atomic swaps for exchanging different cryptocurrencies. Adaptor signatures can be constructed by extending of common digital signature schemes that both authenticate a message and disclose a secret witness to a specific party. In Asiacrypt 2021, Aumayr et al. formulated the two-party adaptor signature as an independent cryptographic primitive. In this study, we extend the their adaptor signature scheme formulation to N party adaptor signature scheme, present its generic construction, and define the security to be satisfied. Next, we present a concrete construction based on Schnorr signatures and discuss the security properties.

1 Introduction

1.1 Background

An adaptor signature was first proposed by Andrew Poelstra et al. [26, 27] in 2017 as the concept of Scriptless Script and later formulated as an independent cryptographic primitive by Aumayr et al. [1]. Adaptor signatures have recently attracted attention as a tool to address issues such as scalability and interoperability for blockchain applications. An adaptor signature scheme is constituted as an extension of a digital signature scheme through a dialogue between two parties: a signer and a secretary. First, the signer generates a pre-signature based on a certain mathematical condition. The conditions are defined by a computationally hard algebraic relation between the public information and the secret information, such as the discrete logarithm problem or the preimage of a hash function. Next, the secretary, who possesses a secret witness for the above conditions, fits the pre-signature to create a valid adaptor signature. Once the valid adaptor signature is completed, the secret information is disclosed to the signer. A valid adaptor signature is a digital signature that is verifiable in the original signature scheme. Particularly in blockchain applications, a miner will not know that an ordinary signature is the output of an adaptor signature scheme and will simply verify it. At the same time, the two parties involved in generating the adaptor signature can embed conditions that are not restricted to the blockchain's scripting language. Thus, adaptor signatures can be used in off-chain payment instruments such as a payment channel network (PCN) [11, 1], which is an off-chain payment method, and an atomic swap [26, 14], which is a P2P transaction between different cryptocurrencies. Moreover, they can be used in scriptless blockchain applications. A PCN is a second-layer technology created to accelerate the transaction processing of cryptocurrencies [13].

Adaptor signature is a signature scheme that can be adapted from a signature called a pre-signature to a normal signature without using a signing key by using a computationally difficult algebraic relation (Hard Relation), and is mainly used in two applications: Payment Channel Network (PCN) [11, 1], an off-chain payment method, and Atomic Swap [26, 14], a P2P transaction between different cryptocurrencies. To date, adaptor signatures have mainly been considered for applications like PCNs and atomic swaps, which are implemented via a dialoge between two parties. Accordingly, all existing studies on adaptor signature schemes have been based on this two-party case.

1.2 Related Works

As the adaptor signature was originally formulated as an independent cryptographic primitive by Aumayr et al., here, we mainly introduce related works that sought to analyze and improve adaptor signatures as cryptographic primitives.

Erwig et al. [10] proposed method for a general conversion method from IDs to adaptor signatures, following the work of Aumayr et al. Indeed, since that work, various adaptor signature schemes have been proposed as cryptographic primitives [11, 35, 19, 41]. The adaptor signature constructed by Aumayr et al. was based on the Schnorr signature [30]. Lattice-based [11], homomorphic mapping-based [35], and code-based [19] signatures have been proposed as schemes that satisfy quantum security resistance. Along this line, Esgin et al. constructed a lattice-based adaptor signature (LAS) based on the Dilithium signature [8]. Tairi et al. constructed a homomorphic mapping-based adaptor signature by applying the Fiat-Shamir transformation [12] from the CSI-FiSh variant to the Schnorr type identification protocol [30, 35]. An optimized version (O-IAS) was then proposed by [35]. Klamti et al. proposed a sign-based adaptor signature [19]. They used algebraic relations that were defined from the syndrome decoding problem to construct an adaptor signature based on Debris-Alazard et al.'s sign-based signature scheme of hash-and-sign [6].

On the security side, Erwig et al. [10] proposed an adapter signature with re-randomizable keys to securely store secret information via algebraic relations with respect to the signing key. Dai et al. [5] strengthened the existing security definition, added a new security definition, and improved the security model of adapter signatures. As for efficiency, Tu et al. [38] constructed an efficient adapter signature based on ECDSA by generating zero-knowledge proofs in the pre-signature stage in a batch and offline.

As noted above, atomic swaps [7, 15, 38, 16] and payment channel networks (PCNs) [25, 36, 3, 35, 24, 2, 33, 21, 39, 23, 29] use adapter signatures and have been actively studied in terms of various practical aspects. Both applications rely on technology to exchange secret information for signatures, which is precisely the functionality provided by adapter signatures. Note again that adapter signatures were originally designed to solve scalability and interoperability issues in blockchain applications, and they have various other applications [20, 31, 4]. Liu et al. [20] proposed a data sharing protocol on a blockchain, which is based on adapter signatures and zero-knowledge proofs (NIZK).

Regarding the functionality of adapter signatures, Sui et al. [33] proposed a two-party, sequentially linkable ring adapter signature (2P-CLRAS) to construct a PCN compatible with Monero, a privacy-preserving cryptocurrency. They constructed 2P-CLRAS from a sequential adapter signature (CAS) by using a new cryptographic primitive called a Verifiable Consecutive One-Way Function (VCOF). This led to the proposal of MoNet, a two-way, Monero-compatible PCN. Qin et al. [28] proposed a blind adapter signature (BAS) based on blind signature schemes to construct a new privacy-preserving payment channel hub (PCH), BlindHub, and a privacy-preserving bidirectional PCN protocol, BlindChannel, in a PCH that supports off-chain payments between senders and receivers via an intermediary (called a tumbler). Hu and Chen [17] also proposed an anonymous, fair transaction scheme for electronic resources by using a new BAS technology. To reduce the PCN's computational complexity, Zhou et al. proposed a new cryptographic primitive called a verifiable timed adapter signature. Thvagarajan et al. [37] proposed a scheme that is similar to the adapter signature, called a lockable signature, which does not require computationally difficult algebraic relations. Lockable signatures provide an effective signature scheme for constructing PCNs and can be seen as a special case of adapter signatures. Finally, as elaborated below, Ji et al. [18] proposed multi-adapter signatures and threshold adapter signatures based on the Schnorr signature and Dilithium schemes, respectively.

1.3 Our contribution

As explained above, adapter signatures have various applications that are akin to conventional digital signatures, yet the current two-party setting has proven insufficient. In this paper, we introduce a novel concept, the N-party adapter signature, to address this limitation. To accomplish this, we first propose a formal security model for three-party adapter signatures and demonstrate a specific construction example using Schnorr signatures. Then, we rigorously establish that the proposed scheme precisely satisfies the defined security model. Following the discussion on three-party scenarios, we delve into the security and concrete constructions for N-party scenarios. The security proofs are demonstrated inductively by leveraging the established security among three parties.

Technical Contributions The paper's technical contributions include the generalization of constructing pre-signatures for pre-signatures. This allows the formation of concatenated adapter signatures from two- to N-party settings. The mechanism for creating this "pre-signature of a pre-signature" is enabled by the additivity that appears in the syntax of adapter signatures. We call our algorithm for this "pre-signature of a pre-signature" the PreAdapt algorithm. Furthermore, we provide rigorous security proofs. It is evident that if security holds for three-party adapter signatures, then it easily extends to N-party settings. However, the proof of security for three-party settings cannot be trivially derived from that of two-party settings, because of differences in the form of pre-signatures and the addition of a pre-adaptation oracle. Finally, we derive the reduction loss to demonstrate the computational gap incurred by extending from two- to N-party settings.

Comparison with Existing Multi-Party Settings As explained above, our contribution lies in extending adapter signatures to multi-party settings and investigating the gap with respect to two-party settings. Ji et al. [18] proposed a multi-adapter signature scheme, but their multi-party setting differs from ours. In their setting, users who are performing pre-signatures exist "simultaneously" and the resulting n pre-signatures are aggregated into one via signature aggregation techniques before being sent to Alice, the secretary. Thus, Ji et al. considered n signers, and this extension could also be of interest in blockchain applications. In real-world applications, however, protocols that end in a single round trip are rare, and scenarios often involve routing or proxies, where someone else intervenes, or where Alice needs to forward messages to someone else. Therefore, our multi-party setting is more generalized. That is, given an initial pre-signer Bob, we consider the scenario of non-simultaneously receiving n users from Bob, who then passes on the pre-signatures sequentially. Eventually, the nth user performs adaptation to obtain a regular signature. At each handover, the execution of an "Extract" operation to obtain the secret witness enables the fair exchange desired in the two-party setting. Accordingly, we expect our approach to be applicable in data sharing and supply chain management, among other applications.

1.4 Two-party adaptor signatures

An adaptor signature scheme is essentially a two-step signing algorithm that is bound to a secret: a partial signature is first generated such that it can be completed only by a party knowing a certain secret, with the complete signature revealing that secret. More precisely, we define the adapter signature scheme with respect to a digital signature scheme Σ and a hard relation R. For any statement $Y \in L_R$, a signer holding a secret key can produce a pre-signature w.r.t. Y on any message m. Such a pre-signature can be adapted into a valid signature on m if and only if the adapter knows a witness for Y. Moreover, it must be possible to extract a witness for Y given the pre-signature and the adapted signature.

The adaptor signature scheme AS is constructed using a digital signature scheme $\Sigma = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ and a computationally intractable algebraic relation $(Y, y) \subseteq R$. Let $(Y, y) \leftarrow \mathsf{GenR}(\lambda)$ be a PPT algorithm that takes the security parameter λ as input and generates a pair comprising public and secret information related by an algebraic relation. For instance, when using the discrete logarithm problem, let $\mathbb{G} = \langle g \rangle$ be a cyclic group of prime order q, as defined in the previous section. In this case, the computationally intractable algebraic relation R_g is defined as $R_g = \{(Y, y) | Y = g^y\} \subseteq \mathbb{G} \times \mathbb{Z}_q$. Other constructions, such as those based on lattice problems, may also exist, and the definition is tailored to the computational assumptions underlying the constructed adapter signature's security.

Syntax of Two-Party Adaptor Signatures The adapter signature $\mathsf{AS}_{R,\Sigma} = (\mathsf{PreSign}, \mathsf{PreVrfy}, \mathsf{Adapt}, \mathsf{Ext})$ is defined by four algorithms as follows. Note that the public key, private key, public information, and secret information used below are pre-prepared via $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(\lambda)$ and $(Y, y) \leftarrow \mathsf{GenR}(\lambda)$. First, the pre-signature generation algorithm $\hat{\sigma} \leftarrow \mathsf{PreSign}((\mathsf{pk}, \mathsf{sk}), Y, M)$ takes as input a pair of public and private keys $(\mathsf{pk}, \mathsf{sk})$, the public information Y, and a message M, and it outputs the pre-signature $\hat{\sigma}$. The pre-verification algorithm $1/0 \leftarrow \mathsf{PreVrfy}(Y, \mathsf{pk}, \hat{\sigma}, M)$ takes as input public information Y, the public key pk, the pre-signature $\hat{\sigma}$, and the message M, and it outputs 1 if the signature σ is accepted, or 0 otherwise. The adaptation algorithm $\sigma := \mathsf{Adapt}((Y, y), \mathsf{pk}, \hat{\sigma}, M)$ takes as input a pair comprising the public information Y and secret information y, the public key pk, the pre-signature $\hat{\sigma}$, and the message M, and it outputs a signature σ via a DPT algorithm. Finally, the extraction algorithm $y' / \perp \leftarrow \mathsf{Ext}(Y, \hat{\sigma}, \sigma)$ s.t. $(Y, y') \in R$ takes as input the public information Y, pre-signature $\hat{\sigma}$, and signature σ, and it outputs y' satisfying $(Y, y') \in R$ if $\hat{\sigma}$ and σ are correct, or $\perp$ otherwise. With adapter signatures, a user who receives a pre-signature $\hat{\sigma}$ can obtain secret information from any $(\hat{\sigma}, \sigma)$ pair by adapting (Adapt) the secret information and pre-signature. For the security of the original two-party adaptor signatures, see the Appendix B.2..

2 Three-Party Adaptor Signatures.

In this section, we describe a three-party adapter signature scheme to prepare for our later N-party construction. The original adapter signature scheme initially involves two entities, the secretary and the signer. However, in the proposed three-party scheme presented here, we consider three entities: U_1 as the secretary, U_2 as the main signer, and U_3 as a sub-signer. In this configuration, the sub-signer U_3 generates a pre-signature; the main signer U_2 generates another pre-signature for the same message, based on the pre-signature generated by U_3; and finally, the secretary U_1 performs adaptation to transform the pre-signature into a (normal) signature. At this point, it is evident that the adapted (normal) signature does not reveal the presence of U_2 or U_3, thus providing anonymity for the signers. We now define two primitives that serve as the foundation for constructing the adapter signature. The first primitive is a digital signature scheme $\Sigma = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$, where U_2 and U_3 possess pairs of public and private keys, denoted as $(\mathsf{pk}_2, \mathsf{sk}_2)$ and $(\mathsf{pk}_3, \mathsf{sk}_3)$, respectively. The signatures generated using these keys are represented as $\sigma_2 \leftarrow \mathsf{Sign}(\mathsf{pk}_2, \mathsf{sk}_2, M)$

and $\sigma_3 \leftarrow (\mathsf{pk}_3, \mathsf{sk}_3, M)$. Then, the second primitive is a hard relation R with statement/witness pairs (Y, y) (as defined at the beginning of Appendix A).

Syntax of three-party adaptor signatures. A three-party adapter signature scheme w.r.t. a hard relation R and a signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ comprises six algorithms, $\Xi_{R,\Sigma} = (\mathsf{PreSign}, \mathsf{PreVrfy}, \mathsf{PreAdapt}, \mathsf{Adapt}, \mathsf{PreExt}, \mathsf{Ext})$, with syntax defined as follows. $\hat{\sigma}_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3),\ Y_2, M)$ is a PPT algorithm that takes as input a public key pk_3, a secret key sk_3, a statement $Y_2 \in R$, and a message $M \in \{0,1\}^*$, and outputs a pre-signature $\hat{\sigma}_3$. $b = \mathsf{PreVrfy}(Y_1, (\mathsf{pk}_2, \mathsf{pk}_3), (\hat{\sigma}_2), \hat{\sigma}_3), M)$ is a DPT algorithm that takes as input a statement $Y_1 \in R$, public keys $(\mathsf{pk}_2, \mathsf{pk}_3)$, pre-signatures $(\hat{\sigma}_2, \hat{\sigma}_3)$, and a message M, and outputs a bit b. $\mathsf{PreAdapt}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3, M)$ is a PPT algorithm[3] that takes as input a pair of hard relations, (Y_2, y_2), a statement Y_1, a public key pk_3, a pair of keys $(\mathsf{sk}_2, \mathsf{pk}_2)$, a pre-signature $\hat{\sigma}_3$, and a message M; then, it outputs a pre-signature $\hat{\sigma}_2$. $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \hat{\sigma}_2, M)$ is a DPT algorithm that takes as input a pair of a statement and a witness, (Y_1, y_1), a public key pk_2, a pre-signature $(\hat{\sigma})$, and a message M. $\mathsf{PreExt}(Y_2, \hat{\sigma}_3, \hat{\sigma}_2)$ is a DPT algorithm that takes as input a public statement Y_2 and pre-signatures $(\hat{\sigma}_3, \hat{\sigma}_2)$, and outputs either a witness y_2' such that $(Y_2, y_2') \in R$, or $\perp$. $\mathsf{Ext}(Y_1, \hat{\sigma_2}, \sigma_2)$ is a DPT algorithm that takes as input a public statement Y_1, a pre-signature $\hat{\sigma}_2$, and an (original) signature σ_2, and outputs either a witness y_2' such that $(Y_1, y_1') \in R$, or $\perp$.

Given these algorithm definitions, we have the following definition of pre-signature correctness for three parties.

Definition 1 (Pre-signature correctness for three parties) *For any message $M \in \{0,1\}^*$ and $(Y_2, y_2), (Y_3, y_3) \in R$, the three-party adapter signature scheme $\mathsf{AS}_{R,\Sigma}$ satisfies pre-signature correctness if the following holds:*

$$\Pr\left[\begin{array}{l|l} \mathsf{PreVrfy}_{U_2}(Y_2, \mathsf{pk}_3, \hat{\sigma}_3, M){=}1; & (\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3){\leftarrow}\mathsf{Gen}(1^\lambda); \\ \mathsf{Vrfy}(\mathsf{pk}_3, M, \sigma_2){=}1; & (Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda); \\ (Y_2, y_2') \in R; & \hat{\sigma}_3{\leftarrow}\mathsf{PreSign}_{U_3}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M); \\ \mathsf{PreVrfy}_{U_1}(Y_1, (\mathsf{pk}_2, \mathsf{pk}_3), & \hat{\sigma}_2{\leftarrow}\mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \\ \qquad (\hat{\sigma}_2, \hat{\sigma}_3), M) = 1; & \qquad \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3, M); \\ \mathsf{Vrfy}(\mathsf{pk}_2, M, \sigma_1) = 1; & y_2' = \mathsf{PreExt}_{U_3}(Y_2, \hat{\sigma}_3, \hat{\sigma}_2); \\ (Y_1, y_1') \in R & \sigma_2 = \mathsf{Adapt}_{U_1}((Y_1, y_1), \mathsf{pk}_2, \hat{\sigma}_2, M); \\ & y_1' / \perp = \mathsf{Ext}_{U_2}(Y_1, (\hat{\sigma}_2, \sigma_2)); \end{array}\right] = 1.$$

[3] The $\mathsf{PreAdapt}$ algorithm simultaneously performs internal processing of the Adapt and $\mathsf{PreSign}$ algorithms. While it includes elements of a DPT algorithm because of this simultaneous processing, the overall procedure involves probabilistic steps when generating pre-signatures. Therefore, it is defined as a PPT algorithm.

2.1 Concrete Construction of Three-Party Adaptor Signatures

In this section, we extend the two-party adapter signature defined in Section 1.4 to describe a specific instantiation of the Schnorr-based three-party adapter signature scheme outlined in Fig. 1. For Schnorr signatures Σ_{Sch} and a hard relation $R_g := \{(Y, y)|Y = g^y\}$, we show the concrete construction of an N-party adapter signature scheme $\mathsf{N\text{-}AS}_{R_g,\Sigma_{\mathsf{Sch}}}$ for the case of $N = 3$. Here, $H(\cdot)$ denotes any cryptographic hash function, and $\mathbb{Z}_q^*$ denotes the set of all integers from 1 to q, excluding 0. First, we denote the three entities in this scheme as U_1, U_2, and U_3. In the construction of the three-party adapter signature, an algorithm's subscript (e.g., $\mathsf{PreSign}_{U_3}$) corresponds to the entity executing the algorithm, and a subscript in an argument (e.g., Y_2 in $\mathsf{PreSign}_{U_3}$ or 3 in $\hat{\sigma}_3$) corresponds to the entity that initially owns (or generates) that value.

2.2 Security Definitions for Three-Party Adaptor Signature Scheme

We now define the security definitions from two-party adaptor signature scheme. Existential unforgeability under chosen message attack in the context of three-party adaptor signatures (3-aEUF-CMA) is an extension of the unforgeability (Definition 10 in Appendix B.2) for adaptor signatures to the three-party setting. In the three-party case, because the content of signatures depends on which entity generates them, we need to consider unforgeability for two separate dialogues involving all three entities, as classified into two cases. First, for unforgeability between entities U_3 and U_2, U_3 generates pre-signatures via the PreSign algorithm, and the attacker attempts to forge signatures via the signature/pre-signature oracle. Second, for unforgeability between U_1 and U_2, U_2 generates pre-signatures via the PreAdapt algorithm, and the attacker tries to forge signatures via the signature/pre-adaptation oracle. We define 3-aEUF-CMA as follows:

Definition 2 (Existential unforgeability for three parties) *A three-party adaptor signature scheme $\mathsf{3\text{-}AS}_{R,\Sigma}$ is 3-aEUF-CMA secure if for any PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, there exists a negligible function $\mathsf{negl}(\lambda)$ such that*

$$\Pr[\mathsf{3\text{-}aSigForge}_{\mathcal{A}_1,\mathsf{3\text{-}AS}_{R,\Sigma}}(\lambda) = 1] + \Pr[\mathsf{3\text{-}aSigForge}_{\mathcal{A}_2,\mathsf{3\text{-}AS}_{R,\Sigma}}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$$

where the experiments $\mathsf{3\text{-}aSigForge}_{\mathcal{A}_1,\mathsf{3\text{-}AS}_{R,\Sigma}}$ and $\mathsf{3\text{-}aSigForge}_{\mathcal{A}_2,\mathsf{3\text{-}AS}_{R,\Sigma}}$ are as defined in the figure Table 1.

Regarding pre-signature adaptability for three-party adapter signatures, as with unforgeability, we need to consider different cases depending on which signer is considered the malicious attacker. Here, we assume that only one entity, either U_2 or U_3, attempts to adapt the pre-signature. This is because, in three-party adapter signatures with two consecutive dialogues, integrity between entities cannot be guaranteed if there are multiple attackers. Accordingly, we have the following definition.

Definition 3 (Pre-signature adaptability for three parties) *For any message $M \in \{0, 1\}^*$, any statement/witness pair $(Y_1, y_1), (Y_2, y_2) \in R$, and any key*

Fig. 1. Concrete construction: Schnorr-based three-party adaptor signatures.

U_1: $\underline{(Y_1, y_1) \leftarrow \mathsf{GenR}(\lambda);}$

$$y_1 \leftarrow \mathbb{Z}_q^*,\ Y_1 := g^{y_1},$$
return Y_1 to U_2.

U_2: $\underline{(\mathsf{sk}_2, \mathsf{pk}_2) \leftarrow \mathsf{KeyGen}(\lambda),}$ $\underline{(Y_2, y_2) \leftarrow \mathsf{GenR}(\lambda);}$

$$\mathsf{sk}_2 := x_2 \leftarrow \mathbb{Z}_q,\ \mathsf{pk}_2 = X_2 := g^{x_2} \in \mathbf{G},$$
$$y_2 \leftarrow \mathbb{Z}_q^*,\ Y_2 := g^{y_2},$$
return Y_2 to U_3 and pk_2 to U_1, U_3.

U_3: $\underline{(\mathsf{sk}_3, \mathsf{pk}_3) \leftarrow \mathsf{KGen}(\lambda);}$

$$\mathsf{sk}_3 := x_3 \leftarrow \mathbb{Z}_q,\ \mathsf{pk}_3 = X_3 := g^{x_3} \in \mathbf{G},$$
return pk_3 to U_1, U_2.

U_3: $\underline{\hat{\sigma}_3 \leftarrow \mathsf{PreSign}_{U_3}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M);}$

$$k \leftarrow \mathbb{Z}_q,\ r_3 := \mathcal{H}(X_3 || g^k Y_2 || M),$$
$$s_3 := k + r_3 \cdot x_3,\ \hat{\sigma}_3 := (r_3, s_3),$$
return $(\hat{\sigma}_3, M)$ to U_1, U_2.

U_2: $\underline{0/1 {=} \mathsf{PreVrfy}_{U_2}(Y_2, \mathsf{pk}_3, \hat{\sigma}_3, M);}$

return 1
if $r_3 = \mathcal{H}(X_3 || g^{s_3} \cdot X_3^{-r_3} \cdot Y_2 || M)$.

U_2: $\underline{\hat{\sigma}_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3, M);}$

$$k' \leftarrow \mathbb{Z}_q,\ r_2 := \mathcal{H}\left(X_2 || g^{k'} Y_1 || M\right),$$
$$s_2 := k' + r_2 \cdot x_2,\ s_3' := s_3 + y_2,$$
$$\hat{\sigma}_2 = (r_2, s_2, s_3'),$$
return $(\hat{\sigma}_2, \hat{\sigma}_3, M)$ to U_1, and $\hat{\sigma}_2$ to U_3.

U_1: $\underline{b = \mathsf{PreVrfy}_{U_1}(Y_1, Y_2, \mathsf{pk}_2, \mathsf{pk}_3, \hat{\sigma}_2, \hat{\sigma}_3, M);}$

return 1 if $r_3 {=} \mathcal{H}(X_3 || g^{s_3} X_3^{-r_3} Y_2 || M)$
and $r_2 {=} \mathcal{H}(X_2 || g^{s_2} X_2^{-r_2} Y_1 || M)$.

U_1: $\underline{\sigma_2 = \mathsf{Adapt}_{U_1}((Y_1, y_1), \mathsf{pk}_2, \hat{\sigma}_2, M);}$

$$s_1 := s_2 + y_1,\ \sigma_2 = (r_2, s_1),$$
return σ_2 to U_2.

U_2: $\underline{y_1' / \perp = \mathsf{Ext}_{U_2}(Y_1, (\hat{\sigma}_2, \sigma_2));}$

$$y_1' := s_1 - s_2,$$
return y_1' if $(Y_1, y_1') \in R$, otherwise,
return $\perp$.

U_3: $\underline{y_2' / \perp = \mathsf{PreExt}_{U_3}(Y_2, \hat{\sigma}_3, \hat{\sigma}_2);}$

$$y_2' := s_3' - s_3,$$
return y_2' if $(Y_2, y_2') \in R$, otherwise,
return $\perp$.

Table 1. Experiment c

$\mathsf{3\text{-}aSigForge}_{\mathcal{A}_1,\mathsf{3\text{-}AS}_{R,\Sigma}}(\lambda)$

$Q := \emptyset$
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$\sigma_3^* \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M^*)$
$\sigma_2^* \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$\sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$
return $(M^* \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2^*, M^*))$

$\mathsf{3\text{-}aSigForge}_{\mathcal{A}_2,\mathsf{3\text{-}AS}_{R,\Sigma}}(\lambda)$

$Q := \emptyset$
$(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_2^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\mathsf{pk}_3)$
$\sigma_3^* \leftarrow \mathsf{PreSign}_{U_3}((\mathsf{pk}_3, \mathsf{sk}_3), Y_3, M^*)$
$\sigma_{n-1} \leftarrow \mathcal{A}_2^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\sigma_3^*, Y_2)$
return $(M^* \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M)$
$Q := Q \cup \{M\}$
return σ_2

$\mathcal{O}_S^{A_i}(M)$	$\mathcal{O}_{pS}(M, Y_2)$
$\sigma_i \leftarrow \mathsf{Sign}(\mathsf{sk}_i, M)$	$\sigma_3 \leftarrow \mathsf{PreSign}(\mathsf{sk}_3, Y_2, M)$
$Q := Q \cup \{M\}$	$Q := Q \cup \{M\}$
return σ_i	**return** σ_3

pairs $(\mathsf{pk}_2,\ \mathsf{sk}_2)$, $(\mathsf{pk}_3,\ \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$, *a three-party adaptor signature scheme* $\mathsf{3\text{-}AS}_{R,\Sigma}$ *is pre-signature adaptable if following conditions (i) and (ii) below are satisfied.*
(i) If the sub-signer U_3 *is an adversary, for any pre-signature* $\hat{\sigma}_3 \leftarrow \{0,1\}^*$ *with* $\mathsf{PreVrfy}_{U_2}\ (Y_2, \mathsf{pk}_3, \hat{\sigma}_3, M) = 1$, *then we have*

$$\mathsf{Vrfy}(\mathsf{pk}_3, M, \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3, M)){=}1.$$

(ii) If the main-signer U_2 *is an adversary, for any pre-signatures* $\hat{\sigma}_3 \leftarrow \mathsf{PreSign}_{U_3}($ $(\mathsf{pk}_3,\ \mathsf{sk}_3), Y_2, M)$ *and* $\hat{\sigma}_2 \leftarrow \{0,1\}^*$ *with* $\mathsf{PreVrfy}_{U_1}(Y_1, (\mathsf{pk}_2, \mathsf{pk}_3), (\hat{\sigma}_2, \hat{\sigma}_3), M) = 1$, *we have*

$$\mathsf{Vrfy}(\mathsf{pk}_2, M, \mathsf{Adapt}_{U_1}((Y_1, y_1), \mathsf{pk}_2, \hat{\sigma}_2, M)) = 1.$$

Finally, we consider an extension of witness extractability, as defined below. Here, we again perform a case analysis based on which of the three entities forges extraction of the secret information, specifically for U_1 or U_2 as the attacker.

However, the entity performing such extraction is limited to one of U_1 or U_2. In this case, the attacker extracting the witness is an entity that receives the pre-signature, just as in the two-party case, so is U_3 never the attacker.

Definition 4 (Witness extractability for three parties) *A three-party adaptor signature scheme* $\mathsf{3\text{-}AS}_{R,\Sigma}$ *is witness extractable if for every PPT adversary* $\mathcal{A}$ *there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\Pr[\mathsf{3\text{-}aWitExt}_{\mathcal{A}_\infty,\mathsf{3\text{-}AS}_{R,\Sigma}}(\lambda)=1]+\Pr[\mathsf{3\text{-}aWitExt}_{\mathcal{A}_\in,\mathsf{3\text{-}AS}_{R,\Sigma}}(\lambda)=1]\leq\mathsf{negl}(\lambda)$$

where those experiments $\mathsf{3\text{-}aWitExt}_{\mathcal{A}_\infty,\mathsf{3\text{-}AS}_{R,\Sigma}}$ *and* $\mathsf{3\text{-}aWitExt}_{\mathcal{A}_\in,\mathsf{3\text{-}AS}_{R,\Sigma}}$ *are as defined in Figure 2.*

Fig. 2. Experiments for witness extractability

$\mathsf{3\text{-}aWitExt}_{\mathcal{A}_1,\mathsf{3\text{-}AS}_{R,\Sigma}}(\lambda)$

1 : $Q := \emptyset$
2 : $(\mathsf{sk}_2,\mathsf{pk}_2)(\mathsf{sk}_3,\mathsf{pk}_3)\leftarrow\mathsf{KeyGen}(1^\lambda)$
3 : $(M^*,Y_1,Y_2)\leftarrow\mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2,\mathsf{pk}_3)$
4 : $\hat{\sigma}_3^*\leftarrow\mathsf{PreSign}_{U_3}((\mathsf{pk}_3,\mathsf{sk}_3),Y_2,M^*)$
5 : $\hat{\sigma}_2^*\leftarrow\mathsf{PreAdapt}_{U_2}((Y_2,y_2),Y_1,\mathsf{pk}_3,(\mathsf{sk}_2,\mathsf{pk}_2),\sigma_3,M^*)$
6 : $\sigma_1\leftarrow\mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\hat{\sigma}_2^*,\hat{\sigma}_3^*,Y_1,Y_2)$
7 : $y_1' := \mathsf{Ext}(Y_1,\sigma_1,\hat{\sigma}_2^*)$
8 : $\mathbf{return}(M^*\notin Q\wedge(Y_1,y_1')\notin R\wedge\mathsf{Vrfy}(\mathsf{pk}_2,\sigma_1,M^*))$

$\mathsf{3\text{-}aWitExt}_{\mathcal{A}_2,\mathsf{3\text{-}AS}_{R,\Sigma}}(\lambda)$

1 : $Q := \emptyset$
2 : $(\mathsf{pk}_3,\mathsf{sk}_3)\leftarrow\mathsf{Gen}(1^\lambda)$
3 : $(M^*,Y_2)\leftarrow\mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot)}(\mathsf{pk})$
4 : $\hat{\sigma}_3^*\leftarrow\mathsf{PreSign}((\mathsf{pk}_3,\mathsf{sk}_3),Y_2,M^*)$
5 : $\hat{\sigma}_2\leftarrow\mathcal{A}_2^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\hat{\sigma}_3^*)$
6 : $y_2' := \mathsf{Ext}(Y_2,\hat{\sigma}_2,\sigma_3^*)$
7 : $\mathbf{return}\ (M^*\notin Q\wedge(Y_2,y_2')\notin R'\wedge\mathsf{Vrfy}(\mathsf{pk}_3,\hat{\sigma}_2,M^*))$

$\mathcal{O}_{pA}(Y_i,Y_{i+1},M)$

1 : $\hat{\sigma}_2\leftarrow\mathsf{PreAdapt}_{U_2}((Y_2,y_2),Y_1,\mathsf{pk}_3,(\mathsf{sk}_2,\mathsf{pk}_2),\hat{\sigma}_3,M)$
2 : $Q := Q\cup\{M\}$
3 : $\mathbf{return}\ \hat{\sigma}_2$

$\mathcal{O}_{pS}(M,Y_i)$	$\mathcal{O}_S^{\mathcal{A}_1}(M)$	$\mathcal{O}_S^{\mathcal{A}_2}(M)$
1 : $\hat{\sigma}_{i+1}\leftarrow\mathsf{PreSign}(\mathsf{sk}_{i+1},Y_i,M)$	*1*: $\sigma_i\leftarrow\mathsf{Sign}(\mathsf{sk}_{i+1},M)$	*1*: $\sigma_i\leftarrow\mathsf{Sign}(\mathsf{sk}_{i+1},M)$
2 : $Q := Q\cup\{M\}$	*2*: $Q := Q\cup\{M\}$	*2*: $Q := Q\cup\{M\}$
3 : $\mathbf{return}\ \hat{\sigma}_{i+1}$	*3*: $\mathbf{return}\ \sigma_i$	*3*: $\mathbf{return}\ \sigma_i$

2.3 Security Proofs for Three-Party Adaptor Signature Scheme

Theorem 1 *If a Schnorr signature scheme Σ_{Sch} is SUF-CMA-secure, and R_g is a computationally hard algebraic relation, then $\text{3-AS}_{R_g,\Sigma_{\mathsf{Sch}}}$ in Fig. 1 is secure in the ROMl.*

Lemma 1 (Pre-signature adaptability for three parties) *The Schnorr-based adaptor signature scheme $\text{3-AS}_{R_g,\Sigma_{\mathrm{Sch}}}$ satisfies pre-signature adaptability for three parties.*

Lemma 2 *For any $\sigma_2 := (r_2, s_1) \in \mathbb{Z}_q \times \mathbb{Z}_q$ and any $y_1 \in \mathbb{Z}_q$,*

$$\mathsf{Adapt}_{U_1}(\mathsf{Adapt}_{U_1}((r_2, s_1), y_1), -y_1) = \sigma.$$

Proof. By the definition of Adapt, for any $r_2, s_1, y_1 \in \mathbb{Z}_q$, we have

$$\begin{aligned}\mathsf{Adapt}_{U_1}(\mathsf{Adapt}_{U_1}((r_2, s_1), y_1), -y_1) &= \mathsf{Adapt}((r_2, s_1 + y_1), -y_1)\\ &= (r_2, s_1 + y_1 + (-y_1))\\ &= (r_2, s_1).\end{aligned}$$

In particular, this lemma implies that, by knowing a witness y, we can not only adapt a valid pre-signature with respect to g^{y_1} into a valid signature but also vice versa.

Lemma 3 (3-aEUF-CMA security.) *Assuming that the Schnorr digital signature scheme Σ_{Sch} is SUF-CMA secure and R_g is a hard relation, the three-party adaptor signature scheme $\text{3-AS}_{R_g,\Sigma_{\mathrm{Sch}}}$, as defined in Fig.1, is 3-aEUF-CMA secure.*

Before formally proving this lemma, we discuss the main idea behind the proof intuitively. The goal is to reduce the forgery resistance of the three-party adapter signature scheme to the strong resistance of the standard Schnorr scheme. In the three-party scheme, we have two cases to consider: an adversary A_1 between U_1 and U_2, or an adversary A_2 between U_2 and U_3, where the adversary wins the 3-aSigForge experiment as a PPT attacker. We design an adversary (or simulator) S for this purpose. First, case (i) can be proved by using almost the same game-hopping steps as in the proof of the two-party adapter signature scheme [Lemma 4 (aSigForge) in [1]], so we skip the proof here. Next, for case (ii), the proof follows a completely different approach from the two-party case. The technical challenge is that A_1 can access not only the interaction between U_1 and U_2 but also the information exchanged between U_2 and U_4 that A_2 had. Specifically, A_2 has access to previous pre-signatures.

Proof. We consider two cases, (i) and (ii) as explained above, and we perform several game hops in each case to prove Lemma 3. For case (i), we follow a similar procedure to the proof of unforgeability in the original two-party scenario of Lemma 4 in [1]. Then, for case (i), we demonstrate each game hop and reduction loss via a sketch proof.

For case (i), we have the following game definitions for strongSigForge and G_0 to G_4.

Game G_0**:** The original $\mathsf{3\text{-}aEUF\text{-}CMA}$ game, $\mathsf{3\text{-}aSigForge}_{\mathcal{A}_2,\mathsf{AS}_{R,\Sigma}}$.
Game G_1**:** An abort game for when the adversary forges a pre-signature for the challenge public statement Y^* without knowing the secret witness s^*.
Game G_2**:** An abort game for when queries to the oracle overlap.
Game G_3**:** A game where the pre-signature oracle returns a regular signature.
Game G_4**:** A game where the pre-signature given to the adversary is turned into a regular signature.
Game $\mathsf{strongSigForge}$**:** A $\mathsf{SUF\text{-}CMA}$ game for regular signatures.

The reduction loss for the above is as follows, and it can be directly obtained from the original two-party scenario:

$$\begin{aligned} &\Pr[\mathsf{3\text{-}aSigForge}_{A_2,\mathsf{3\text{-}AS}}(\lambda)=1] \\ &= \Pr[G_0=1] \\ &\le \Pr[G_1=1]+v_1(\lambda) \\ &\le \Pr[G_2=1]+v_1(\lambda)+v_2(\lambda) \\ &= \Pr[G_3=1]+v_1(\lambda)+v_2(\lambda) \\ &\le \Pr[G_4=1]+v_1(\lambda)+v_2(\lambda) \\ &= \Pr[\mathsf{strongSigForge}_{S^{A_2},\mathsf{3\text{-}AS}}(\lambda)=1]+v_1(\lambda)+v_2(\lambda), \end{aligned} \tag{1}$$

where v_1 and v_2 are the negligible functions in λ.

Next, for case (ii), we have $\mathsf{3\text{-}aSigForge}_{\mathcal{A}_2,\mathsf{AS}_{R,\Sigma}}$.

Game $\mathbf{G}_0$**:** This game, which is formally defined in Table 2, corresponds to the original $\mathsf{3\text{-}aSigForge}$, where the adversary A_1 has to produce a valid forgery for a message m of his choice, while having access to a pre-signature oracle $\mathcal{O}_{\mathrm{pS}}$, a signature oracle $\mathcal{O}_{\mathrm{S}}$, and a pre-adaptation oracle $\mathcal{O}_{\mathrm{pA}}$. Since we are in the ROM, the adversary (as well as all of the scheme's algorithms) also has access to a random oracle $\mathcal{H}$. The simulator S wins if $b=1$ and $M^* \notin Q$.

$$\Pr[\mathsf{3\text{-}aSigForge}_{\mathcal{A}_2,\mathsf{AS}_{R,\Sigma}}(\lambda)=1] = \Pr[\mathbf{G}_0=1]. \tag{2}$$

Game $\mathbf{G}_1$**:** This game, which is formally defined in Table 14, works exactly like $\mathbf{G}_0$ with the following exception. When the adversary outputs a forgery σ_1^*, the game $\mathbf{G}_1$ checks whether completion of the pre-signature $\hat{\sigma}_2$ by using the secret value y_1 yields σ_1^*. If so, the game aborts. The difference between $\mathbf{G}_0$ and $\mathbf{G}_1$ is recorded in Table 3.

Claim for Game $\mathbf{G}_1$. Let Bad_1 be the event that $\mathbf{G}_1$ aborts. Then, $\Pr[\mathsf{Bad}_1] \le v_1(\lambda)$, where v_1 is a negligible function in λ.

Proof. Using adversary A_1, we construct a simulator S that solves a relation R_g and reduces it to a hard relation.

1. The simulator S generates a key pair $(\mathsf{sk}_2,\mathsf{pk}_2) \leftarrow \mathsf{Gen}(1^n)$ to simulate queries to the oracles $\mathcal{H},\mathcal{O}_S,\mathcal{O}_{pS},\mathcal{O}_{pA}$ of adversary A_1, where the oracles' behavior follows G_1.

Table 2. Formal definition of game $\mathbf{G_0}$

$\mathbf{G}_0$

$Q := \emptyset$
$H := [\perp]$
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_1^*, y_1^*)(Y_2^*, y_2^*) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2^*, M^*)$
$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2^*, y_2^*), Y_1^*, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$\sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1^*, Y_2^*)$
return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M)$
$Q := Q \cup \{M\}$
return σ_2

$\mathcal{O}_S^{\mathcal{A}_1}(M)$

$\sigma_1 \leftarrow \mathsf{Sign}((\mathsf{pk}_1, \mathsf{sk}_1), M)$
$Q := Q \cup \{M\}$
return σ_1

$\mathcal{O}_{pS}(M, Y_2)$

$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M)$
$Q := Q \cup \{M\}$
return σ_3

$\mathcal{H}(x)$

if $\mathcal{H}[x] = \perp$
$H[x] \leftarrow \mathbb{Z}_q$
return $\mathcal{H}[x]$

2. Upon receiving a challenge message M^* from an adversary A, S calculates $\sigma_2 \leftarrow PreSign((pk_2, sk_2), Y_1^*, M^*)$ and returns a pair (σ_2, Y^*) to A_1.
3. When an adversary A outputs a forged signature σ_1^* and Bad_1 occurs (i.e., $Adapt(\sigma_2, y_1) = \sigma_1^*$), S can obtain $(Y_1^*, y_1^*) \in R$ by executing $y_1^* \leftarrow \mathsf{Ext}(\sigma_1^*, \sigma_2, Y_1^*)$ (because of pre-signature correctness).
4. A challenge public statement Y_1^* is an instance of the hard relation R and follows the output distribution of Gen_R. From the perspective of an adversary A, $Y_1 \approx Y_1^*$, and G_0 and G_1 are thus indistinguishable.

Therefore, the probability that the simulator S breaks the hard relation R_g is equal to the probability of Bad_1 occurring.

Because games $\mathbf{G}_1$ and $\mathbf{G}_0$ are equivalent except if event Bad_1 occurs, it holds that

$$\Pr[\mathbf{G}_0 = 1] \leq \Pr[\mathbf{G}_1 = 1] + v_1(\lambda), \tag{3}$$

where v_1 means the probability of breaking the hard relation R.

Game $\mathbf{G}_2$: This game, which is formally defined in Table 15, behaves similarly to the previous game, with the only difference being in the $\mathcal{O}_{\mathrm{pS}}$ oracle. In this game, the $\mathcal{O}_{\mathrm{pS}}$ oracle first makes a copy of the list H before executing the algorithm $\mathsf{PreSign}$. Then, it extracts the randomness used during the $\mathsf{PreSign}$ algorithm, and checks whether, before the signing algorithm's execution, a query of the form $\mathsf{pk}_3||K||M$ or $\mathsf{pk}_3||K \cdot Y_2||M$ was made to $\mathcal{H}$ by checking whether $H'[\mathsf{pk}_3||K||M] \neq \perp$ or $H'[\mathsf{pk}_3||K \cdot Y_2||M] \neq \perp$. If such a query was made, the game aborts. The difference between $\mathbf{G}_1$ and $\mathbf{G}_2$ is recorded in Table 4.
Claim for Game $\mathbf{G}_2$. Let Bad_2 be the event that $\mathbf{G}_2$ aborts in $\mathcal{O}_{pS}$. Then $\Pr[\mathsf{Bad}_2] \leq v_2(\lambda)$, where v_2 is a negligible function in n.

Table 3. Difference between $\mathbf{G_0}$ and $\mathbf{G_1}$

$\mathbf{G}_1$
$1: Q := \emptyset$
$2: H := [\perp]$
$3: (\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$4: (Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$5: M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$6: \sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M^*)$
$7: \sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$8: \sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$
$9:$ if $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*$, abort.
$10:$ return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

Table 4. Difference between $\mathbf{G_1}$ and $\mathbf{G_2}$

$\mathcal{O}_{pS}(M, Y_2)$
1: $H' := H$
2: $\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M)$
3: $(r_3, s_3) := \sigma_3$
4: $K := g^s \mathsf{pk}_3^{-r_3}$
5: if $H'[\mathsf{pk}_3 \| K \| M] \neq \perp$
6: $\quad \wedge H'[\mathsf{pk}_3 \| K \cdot Y_2 \| M]$
7: $\quad$ abort
8: $Q := Q \cup \{M\}$
9: return σ_3

Proof. $\mathsf{PreSign}$, Sign, and $\mathsf{PreAdapt}$ compute $K = g^k$ by using a uniformly random k from $\mathbb{Z}_q$. Bad_2 occurs when queries $\mathsf{pk}_3 \| K_3 \| M$ and $\mathsf{pk}_3 \| (K_3 \cdot Y_2) \| M$ have not been generated before. As the adversary A is a PPT algorithm, the number of queries to each oracle $\mathcal{H}, \mathcal{O}_S, \mathcal{O}_{pS}, \mathcal{O}_{pA}$ is polynomial. The signature oracle $\mathcal{O}_S$, pre-signature oracle $\mathcal{O}_{pS}$, and pre-adaptation oracle $\mathcal{O}_{pA}$ use the above k when computing $K = g^k$. Let the numbers of queries to the oracles $\mathcal{H}, \mathcal{O}_S, \mathcal{O}_{pS}, \mathcal{O}_{pA}$ be l_1, l_2, l_3, l_4, respectively. Then,

$$\begin{aligned}\Pr[Bad_2] &= \Pr[\mathcal{H}'[pk_3 || K_3 || M] \neq \perp \vee \mathcal{H}'[pk_3 || (K_3 \cdot Y_2) || M] \neq \perp] \\ &\leq \frac{2(l_1 + l_2 + l_3 + l_4)}{q} =: v_2'(\lambda),\end{aligned}$$

where l_1, l_2, l_3, l_4 are polynomials in λ, making v_2' is negligible. In total, there are $l_1 + l_2 + l_3 + l_4$ chances out of q, and two of them are for K and $K \cdot Y$. Therefore,

$$\Pr[G_1 = 1] \leq \Pr[G_2 = 1] + v_2'(\lambda).$$

Game $\mathbf{G}_3$: This game, which is formally defined in Table 16, behaves similarly to the previous game, but with several differences in the oracle $\mathcal{O}_{\mathrm{pA}}$. In this game, $\mathcal{O}_{\mathrm{pA}}$ first makes a copy of the list H before executing $\mathsf{PreAdapt}$. Afterward, it extracts the randomness values r_2, s_2, and s_3' that were used in the $\mathsf{PreAdapt}$ algorithm. For r_2 and s_2, it checks whether, before the signing algorithm's execution, a query of the form $\mathsf{pk}_2 \| K_2 \| M$ or $\mathsf{pk}_2 \| K_2 \cdot Y_1 \| M$ was made to $\mathcal{H}$ by checking whether $H'[\mathsf{pk}_2 \| K_2 \| M] \neq \perp$ or $H'[\mathsf{pk}_2 \| K_2 \cdot Y_1 \| M] \neq \perp$. If such a query was made, the game aborts. The difference between $\mathbf{G}_2$ and $\mathbf{G}_3$ is recorded in Table 5.

Regarding s_3', it is used when extracting the witness y_2' ($y_2' := s_3' - s_3$). The adversary checks whether its forged witness y_2' corresponds (by chance) to the challenge statement Y_2^* on the oracle side. (The same verification performed by

Table 5. Difference between game $\mathbf{G_2}$ and game $\mathbf{G_3}$

$\mathbf{G}_3$	$\mathcal{O}_{pA}(M,(Y_2,Y_2),\sigma_3)$
$1: Q := \emptyset,\ S := \emptyset$	$1: H' := H$
$2: H := [\bot],$	$2: \sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2,y_2),Y_1,\mathsf{pk}_3,$ $(\mathsf{sk}_2,\mathsf{pk}_2),\sigma_3,M)$
$3: (\mathsf{pk}_2,\mathsf{sk}_2)(\mathsf{pk}_3,\mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$	$3: (r_2,s_2,s_3') := \sigma_2$
$4: (Y_1,y_1)(Y_2,y_2) \leftarrow \mathsf{GenR}(1^\lambda)$	$4: K_2 := g^{s_2}\cdot \mathsf{pk}_2^{-r_2}$
$5: M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2,\mathsf{pk}_3)$	$5: y_2' = s_3' - s_3\ (\because (r_3,s_3) := \hat{\sigma}_3)$
$6: \sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3,\mathsf{sk}_3),Y_2,M^*)$	$6:$ if $H'[\mathsf{pk}_2\Vert K_2\Vert M] \neq \bot$
$7: \sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2,y_2),$ $Y_1,\mathsf{pk}_3,(\mathsf{sk}_2,\mathsf{pk}_2),\sigma_3,M^*)$	$7: \quad \wedge\ H'[\mathsf{pk}_2\ \ K_2\cdot Y_1\Vert M] \neq \bot$
$8: \sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\sigma_2^*,\sigma_3^*,Y_1,Y_2)$	$8: \quad \wedge\ s_3' \in S$
$9:$ if $\mathsf{Adapt}((Y_1,y_1),\mathsf{pk}_2,\sigma_2,M) = \sigma_1^*,$	$9: \quad \wedge\ (Y_2^*,y_2') \in R^*$
$10: \vee\ y_1^* \leftarrow \mathsf{Ext}(Y_1^*,\mathsf{PreAdapt}_{U_2}((Y_2^*,y_2^*),Y_1^*,$ $\mathsf{pk}_3,(\mathsf{sk}_2,\mathsf{pk}_2),\hat{\sigma}_3^*,M),\sigma_2^*$	$10:$ abort
$11:$ then abort	$11: Q := Q \cup \{M\}$
$12:$ return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3,\sigma_2,M^*))$	$12: S := S \cup \{s_3'\}$
	$13:$ return σ_2

the simulator in $\mathbf{G_1}$ is performed here on the oracle side.) In other words, on the side of the pre-adaptation oracle $\mathcal{O}_{pA}$, if y_2' is computed from $\sigma_3' = (r_3,s_3)$ and $\sigma_2 = (r_2,s_2,s_3')$ as $y_2' = s_3' - s_3$, and if $(Y_2^*,y_2') \in R^*$, then the game aborts. While it aborts if a valid witness y_2' for the challenge statement Y_2^* exists, a separate list S is prepared because of possible overlapping queries.

If A_1 uses a challenge M^* as an oracle query, this can be determined by checking whether $M \notin \mathcal{Q}$; similarly, if A_1 uses $M(\neq M^*)$ and a challenge Y_1^* as oracle queries, this can be determined by the Adapt algorithm in line 39 of $\mathbf{G}_3$. For the case where A_1 uses $M(\neq M^*)$ and a challenge Y_2^*, however, further consideration is needed. Therefore, on the simulator side, S executes the algorithm $y_1' \leftarrow \mathsf{Ext}(Y_1,\hat{\sigma}_2,\sigma_2)$. If the forged σ_2^* output by A_1 corresponds to the legitimate witness y_1^* derived from the challenge Y_1^* when $\sigma_2' \leftarrow \mathsf{PreAdapt}$ is computed using $M(\neq M^*)$ and the challenge Y_2^*, then the game aborts. This probability is bounded by the probability of breaking the hard relation, at most.

Claim for Game $\mathbf{G_3}$. Let Bad_3 be the event that $\mathbf{G}_3$ aborts in $\mathcal{O}_{pA}$. Then $\Pr[\mathsf{Bad}_3] \leq v_3(\lambda)$, where v_3 is a negligible function in n.

Proof. We first note that $\mathsf{PreSign}$, Sign, and $\mathsf{PreAdapt}$ compute $K = g^k$ by choosing k uniformly at random from $\mathbb{Z}_q$. As A is PPT, the number of queries it can make to $\mathcal{H}$, $\mathcal{O}_{mathrmS}$, $\mathcal{O}_{\mathrm{pS}}$, and $\mathcal{O}_{\mathrm{pA}}$ is also polynomially bounded. Let l_1', l_2', l_3', l_4' be the numbers of queries made to $\mathcal{H}$, $\mathcal{O}_{mathrmS}$, $\mathcal{O}_{\mathrm{pS}}$, and $\mathcal{O}_{\mathrm{pA}}$ respectively. Furthermore, to address the case where A_1 uses $M(\neq M^*)$ and the challenge Y_2^*, S executes the algorithm $y_1' \leftarrow \mathsf{Ext}(Y_1,\hat{\sigma}_2,\sigma_2)$. If the forged σ_2^* output by A_1 corresponds to a legitimate witness y_1^* derived from the challenge Y_1^* when $\sigma_2' \leftarrow \mathsf{PreAdapt}$ is computed using $M(\neq M^*)$ and the challenge Y_2^*, then the game aborts. As with G_1, this probability is bounded by the probability of breaking the hard relation, which is denoted as v_1. Then, we have the following:

$$\begin{aligned}\Pr[\mathsf{Bad}_3] &= \Pr[H'[\mathsf{pk}_3||K_3||M] \neq \perp \wedge H'[\mathsf{pk}_3||K_3 \cdot Y_2||M] \neq \perp] + v_1(\lambda)\\ &\leq 2\frac{l'_1 + l'_2 + l'_3 + l'_4}{q} + v_1(\lambda) = v'_3(\lambda) + v_1(\lambda),\end{aligned}$$

where v'_3 is a negligible function because l'_1, l'_2, l'_3, l'_4 are polynomial in λ and v_1 is the advantage of hard relation's advantage.

$$\therefore \Pr[G_2 = 1] \leq \Pr[G_3 = 1] + v_1(\lambda) + v'_3(\lambda). \tag{4}$$

Game $\mathbf{G}_4$: In this game, which is formally defined in Table 17, upon an $\mathcal{O}_{pS}$ query, the game produces a valid full signature $\tilde{\sigma} = (r, s) = (H(pk||K||m), k + rs \cdot k)$ and adjusts the global list H as follows. It assigns the value stored at position $pk||K||m$ to $H[pk||K \cdot Y||m]$ and samples a fresh random value for $H[pk||K||m]$. These changes make the full signature $\tilde{\sigma}$ "look like" a pre-signature to the adversary A, because it obtains the value $H[pk||K||m]$ upon querying the random oracle on $pk||K \cdot Y||m$. The adversary can only notice the changes in this game if the random oracle was previously queried on either $pk||K||m$ or $pk||K \cdot Y||m$. This case is captured in the previous game, and it thus holds that $\Pr[G_3 = 1] = \Pr[G_4 = 1]$.

Table 6. Difference between game $\mathbf{G_3}$ and game $\mathbf{G_4}$

$\mathcal{O}_{pS}(M, Y_2)$

$H' := H$

$\sigma_3 \leftarrow \mathsf{Sign}((\mathsf{pk}_3, \mathsf{sk}_3), M)$

$(r_3, s_3) := \sigma_3$

$K := g^s \mathsf{pk}_3^{-r_3}$

if $H'[\mathsf{pk}_3||K||M] \neq \perp$

$\quad \wedge H'[\mathsf{pk}_3||K \cdot Y_2||M]$

$\quad$ abort

$x := \mathsf{pk}_3||K_3||M$

$H'[\mathsf{pk}_3||K_3 \cdot Y_2||M] := H[x]$

$H[x] \leftarrow \mathbb{Z}_q$

$Q := Q \cup \{M\}$

return σ_3

Game $\mathbf{G}_5$: This game, which is formally defined in Table 18, aims to appear like a pre-signature to the adversary upon an $\mathcal{O}_{pA}$ query. However, because a pre-signature's structure differs from that of a regular signature, adversaries may notice the changes in this game, unlike with $\mathbf{G_4}$. Therefore, to simulate $\hat{\sigma}_2 = (r_2, s_2, s'_3)$, where the first two components are indistinguishable from a regular signature $\sigma_2 = (r_2, s_1)$ and s'_3 is just random noise, we need to perform a similar procedure to that in $\mathbf{G_4}$, ensuring that $\sigma_2 = (r_2, s_1)$ remains indistinguishable and replacing s'_3 with a random value. The difference between $\mathbf{G}_4$ and $\mathbf{G}_5$ is recorded in Table 7. When using a randomly chosen s'_3 to extract y'_2, the probability that y'_2 corresponds to the challenge Y_2^* is bounded by the advantage of breaking the hard relation, denoted as v_1. Hence, $\Pr[G_4 = 1] = \Pr[G_5 = 1] + v_1(\lambda)$ holds.

Table 7. Difference between game $\mathbf{G_4}$ and game $\mathbf{G_5}$

$\mathbf{G}_5$	$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$
$Q := \emptyset,\ \boxed{S := \emptyset}$	$H' := H$
$H := [\perp],$	$\boxed{\sigma_2 \leftarrow \mathsf{Sign}((\mathsf{pk}_2, \mathsf{sk}_2), M)}$
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$	$\boxed{(r_2, s_2) := \sigma_2}$
$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$	$s'_3 \leftarrow \mathbb{Z}_q$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$	if $s'_3 \in S$, abort
$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M^*)$	$K_2 := g^{s_2} \cdot \mathsf{pk}_2^{-r_2}$
$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2),$ $Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$	$y'_2 = s'_3 - s_3\ (\because (r_3, s_3) := \hat{\sigma}_3)$
$\sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$	if $H'[\mathsf{pk}_2 \vert\vert K_2 \vert\vert M] \neq \perp$
if $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*,$	$\wedge\ H'[\mathsf{pk}_2\ \ K_2 \cdot Y_1 \vert\vert M] \neq \perp$
$\vee\ y_1^* \leftarrow \mathsf{Ext}(Y_1^*, \mathsf{PreAdapt}_{U_2}((Y_2^*, y_2^*), Y_1^*,$ $\mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3^*, M), \sigma_2^*$	$\wedge\ s'_3 \in S$
then abort	$\wedge\ (Y_2^*, y'_2) \in R^*$
return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$	abort
	$x := \mathsf{pk}_2 \vert\vert K_2 \vert\vert M$
	$H[\mathsf{pk2} \vert\vert K_2 \cdot Y_1 \vert\vert M] := H[x]$
	$H[x] \leftarrow \mathbb{Z}_q$
	$\boxed{(r_2, s_2, s'_3) := \hat{\sigma}_2}$
	$Q := Q \cup \{M\}$
	$S := S \cup \{s'_3\}$
	return σ_2

Game $\mathbf{G}_6$: In this game, which is formally defined in Table 19, the pre-signature generated upon A outputting the message M is created by modifying a full signature to a pre-signature.

The simulator S modifies the pre-signatures passed to adversary A_1 to pre-signatures converted from regular signatures. Specifically, from regular signatures σ'_2 and σ'_3, S creates $\sigma_2 = \text{Adapt}(\sigma'_2, -y_1)$ and $\sigma_3 = \text{Adapt}(\sigma'_3, -y_1)$. The difference in this transformation lies in k_2 and k_3 becoming $k'_2 = k_2 - y_1$ and $k'_3 = k_3 - y_2$; however, because k is uniformly random, it is indistinguishable, and A_1 cannot determine whether a signature is a pre-signature or a regular signature. This transformation can be viewed as k being modified to $k' = k - y_2$. Because k is chosen uniformly at random, and because, according to Lemma 2, the adversary's view is identical between this game and previous game, it holds that $\Pr[G_5 = 1] = \Pr[G_6 = 1]$.

Table 8. Difference between game $\mathbf{G_5}$ and game $\mathbf{G_6}$

$\mathbf{G}_6$

$Q := \emptyset$, $S := \emptyset$

$H := [\perp]$,

$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$

$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$

$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$

$\sigma_2', \sigma_3' \leftarrow \mathsf{Sign}((\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3), M^*)$

$(r_2', s_2') := \sigma_2', (r_3', s_3') := \sigma_3'$

$\sigma_2 := \mathsf{Adapt}(\sigma_2', -y_1)$

$\sigma_3 := \mathsf{Adapt}(\sigma_3', -y_2)$

$Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$

$\sigma_1' \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$

if $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*$,

$\vee\ y_1^* \leftarrow \mathsf{Ext}(Y_1^*, \mathsf{PreAdapt}_{U_2}((Y_2^*, y_2^*), Y_1^*,$
$\mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3^*, M), \sigma_2^*$

then abort

return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

Game strongSigForge: In analogous fashion, we seek to establish the existence of a simulator that can faithfully reproduce G_6 while harnessing the capabilities of A_1 to achieve success in the **strongSigForge** game. Here, we succinctly delineate how the simulator responds to oracle queries. For a comprehensive formal exposition of the simulator, refer to Table 9.

Signature queries: When the adversary A_1 queries oracle $\mathcal{O}_S$ with an input M, the simulator S forwards M to oracle $\mathcal{O}_{\text{Sign}}^{Sch}$ and relays the response to A_1.

Random oracle queries: When A_1 queries oracle $\mathcal{H}$ with input x, if $\mathcal{H}[x] = \perp$, then S queries $\mathcal{H}^{Sch}(x)$; otherwise, it returns $\mathcal{H}[x]$.

Pre-signature queries: 1. When A_1 queries oracle $\mathcal{O}_{pS}$ with input (M, Y_2), S forwards M to oracle $\mathcal{O}_{\text{Sign}}^{Sch}$ and receives a signature $\sigma_3 = (r_3, s_3)$ $(r_3 = \mathcal{H}^{Sch}(pk_3||K_3||M))$. 2. If oracle $\mathcal{H}$ was previously queried on $(pk_3||K_3||M)$ or $(pk_3||K_3 \cdot Y_2||"M")$, S aborts. 3. S programs the random oracle $\mathcal{H}$ such that queries made by A_1 on input $(pk_3||K_3 \cdot Y_2||"M")$ are answered with the value $\mathcal{H}^{Sch}(pk_3||K_3||M)$, and queries on input $(pk_3||K_3||M)$ are answered with $\mathcal{H}^{Sch}(pk_3||K_3 \cdot Y_2||M)$. 4. S returns σ_3 to A_1.

Pre-Adaptation queries: 1. When A_1 queries oracle $\mathcal{O}_{pA}$ with input (M, Y_1, Y_2, σ_2), S forwards M to oracle $\mathcal{O}_{\text{Sign}}^{Sch}$ and receives a signature $\sigma_2 = (r_2, s_2)$ $(r_2 = \mathcal{H}^{Sch}(pk_2||K_2||M))$. 2. If oracle $\mathcal{H}$ was previously queried on $(pk_2||K_2||M)$ or $(pk_2||K_2 \cdot Y_1||"M")$, S aborts. 3. S programs the random oracle $\mathcal{H}$ such that queries made by A_1 on input $(pk_2||K_2 \cdot Y_1||"M")$ are answered with the value $\mathcal{H}^{Sch}(pk_2||K_2||M)$, and queries on input $(pk_2||K_2||M)$ are answered with $\mathcal{H}^{Sch}(pk_2||K_2 \cdot Y_1||M)$. 4. S returns σ_2 to A_2.

Challenge Phase: S selects $(Y_1, y_1)(Y_2, y_2) \leftarrow GenR(1^n)$ and runs A_1 on pk_2, pk_3 and Y_1, Y_2. If A_1 outputs a challenge message M^*, then S queries the Sign^{Sch} oracle with input M^*. If A_1 outputs a forged signature σ^*, then S outputs (M^*, σ^*) as its own forgery.

The main difference between the simulation and G_6 lies in the syntax. Instead of generating public and secret keys and calculating the algorithm Sign_{sk} and random oracle $\mathcal{H}$, the simulator S uses its own oracles Sign^{Sch} and $\mathcal{H}^{Sch}$. Thus, S perfectly simulates G_6. We still need to demonstrate that S can use the forgery output by A_1 to win the **strongSigForge** game.

Claim for strongSigForge. *(M^*, σ^*) is a valid forgery of* **strongSigForge**.

Proof. We show that (M^*, σ^*) is never output by the oracle $\mathsf{Sign}^{\text{Sch}}$. This proof follows similar reasoning to the two-party case. First, the simulated adversary has not made any queries to O_S, O_{pS}, or O_{pA} for the challenge message M^*. From Game G_1 and Lemma 2, the adversary outputs a forgery σ that is equal to a signature σ' output by $\mathsf{Sign}^{\text{Sch}}$ during the challenge phase with only a negligible probability (i.e., the probability of breaking the hard relation). In this case, the simulation is aborted. Therefore, $\mathsf{Sign}^{\text{Sch}}$ never outputs σ for M, and (M^*, σ^*) is thus a valid forgery for the game **strongSigForge**.

As S provides a perfect simulation of G_6, from games $\mathbf{G_0}$ to $\mathbf{G_6}$, we have the following:

$$
\begin{aligned}
&\Pr[\mathsf{3\text{-}aSigForge}_{\mathcal{A}_2,\mathsf{AS}_{R_g,\Sigma}}(\lambda) = 1] \qquad (5)\\
&= \Pr[\mathbf{G}_0 = 1] \leq \Pr[G_1 = 1] + v_1(\lambda)\\
&\leq \Pr[G_2 = 1] + v_1(\lambda) + v_2'(\lambda)\\
&= \Pr[G_3 = 1] + 2v_1(\lambda) + v_2'(\lambda) + v_3'(\lambda)\\
&= \Pr[G_4 = 1] + 2v_1(\lambda) + v_2'(\lambda) + v_3'(\lambda)\\
&= \Pr[G_5 = 1] + 3v_1(\lambda) + v_2'(\lambda) + v_3'(\lambda)\\
&= \Pr[G_6 = 1] + 3v_1(\lambda) + v_2'(\lambda) + v_3'(\lambda)\\
&= \Pr[\mathsf{strongSigForge}_{S^{A_2},\mathsf{3\text{-}AS}}(\lambda) = 1] + 3v_1(\lambda) + v_2'(\lambda) + v_3'(\lambda).
\end{aligned}
$$

Then, from Equations (1) and (5), the overall reduction loss for three-party unforgeability is as follows:

$$\Pr[\mathsf{3\text{-}aSigForge}_{\mathcal{A}_1,\mathsf{AS}_{R_g,\Sigma}}(\lambda) = 1] + \Pr[\mathsf{3\text{-}aSigForge}_{\mathcal{A}_2,\mathsf{AS}_{R_g,\Sigma}}(\lambda) = 1] \leq \mathsf{negl}(\lambda).$$

Lemma 4 (Witness extractability for three parties.) *Assuming that the Schnorr digital signature scheme Σ_{Sch} is SUF-CMA secure and R_g is a hard relation, the three-party adaptor signature scheme $\mathsf{3\text{-}AS}_{R_g,\Sigma_{\text{Sch}}}$, as defined in Fig. 1, is witness extractable.*

As with the three-party unforgeability in Lemma 3, we reduce the witness extractability of the adapter signature to the SUF-CMA security of the Schnorr signature. That is, we demonstrate the existence of a simulator S when a PPT

Table 9. Formal definition of game **strongSigForge**

$\mathcal{S}^{\mathsf{Sign}^{\mathrm{Sch}},\mathcal{H}^{\mathrm{Sch}}}$

$Q := \emptyset,\ S := \emptyset$
$H := [\perp]$
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$\sigma'_2, \sigma'_3 := \mathsf{Sign}^{\mathrm{Sch}}(M)$
$(r'_2, s'_2) := \sigma'_2, (r'_3, s'_3) := \sigma'_3$
$\sigma_2 := \mathsf{Adapt}(\sigma'_2, -y_1)$
$\sigma_3 := \mathsf{Adapt}(\sigma'_3, -y_2)$
$Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$\sigma'_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot),\mathcal{O}_{pA}(\cdot)}(\sigma^*_2, \sigma^*_3, Y_1, Y_2)$
if $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma^*_1$
$\vee\ y^*_1 \leftarrow \mathsf{Ext}(Y^*_1, \mathsf{PreAdapt}_{U_2}((Y^*_2, y^*_2), Y^*_1,$
$\mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}^*_3, M), \sigma^*_2$
then abort
return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$H' := H$
$\sigma_2 := \mathsf{Sign}^{\mathrm{Sch}}(M)$
$(r_2, s_2) := \sigma_2$
$s'_3 \leftarrow \mathbb{Z}_q$
if $s'_3 \in S$, abort
$K_2 := g^{s_2} \cdot \mathsf{pk}_2^{-r_2}$
$y'_2 = s'_3 - s_3\ (\because (r_3, s_3) := \hat{\sigma}_3)$
if $H'[\mathsf{pk}_2||K_2||M] \neq \perp$
$\wedge\ H'[\mathsf{pk}_2\ \ K_2 \cdot Y_1||M] \neq \perp$
$\wedge\ s'_3 \in S$
$\wedge\ (Y^*_2, y'_2) \in R^*$
abort
$x := \mathsf{pk}_2||K_2||M$
$H[\mathsf{pk}_2||K_2 \cdot Y_1||M] := \mathcal{H}^{\mathrm{Sch}}(x)$
$H[x] := \mathcal{H}^{\mathrm{Sch}}(\mathsf{pk}_2||K_2 \cdot Y_1||M)$
$(r_2, s_2, s'_3) := \hat{\sigma}_2$
$Q := Q \cup \{M\}$
$S := S \cup \{s'_3\}$
return σ_2

$\mathcal{O}_S^{\mathcal{A}_1}(M)$

$\sigma_1 := \mathsf{Sign}^{\mathrm{Sch}}(M)$
$(r_2, s_1) := \sigma_1$
$K_1 := g^{s_1 \mathsf{pk}_2^{-r_2}}$
$x := \mathsf{pk}_2||K_1||M$
$H[x] := \mathcal{H}^{\mathrm{Sch}}(x)$
$Q := Q \cup \{M\}$
return σ_1

$\mathcal{O}_{pS}(M, Y_2)$

$H' := H$
$\sigma_3 := \mathsf{Sign}^{\mathrm{Sch}}(M)$
$(r_3, s_3) := \sigma_3$
$K := g^s \mathsf{pk}_3^{-r_3}$
if $H'[\mathsf{pk}_3||K||M] \neq \perp$
$\wedge H'[\mathsf{pk}_3||K \cdot Y_2||M]$
abort
$x := \mathsf{pk}_3||K_3||M$
$H[\mathsf{pk}_3||K_3 \cdot Y_2||M] := \mathcal{H}^{\mathrm{Sch}}(x)$
$H[x] := \mathcal{H}^{\mathrm{Sch}}(\mathsf{pk}_3||X_3 \cdot Y_2||M)$
$Q := Q \cup \{M\}$
return $\hat{\sigma}_3$

$\mathcal{H}(x)$

if $\mathcal{H}[x] = \perp$
$H[x] \leftarrow \mathcal{H}^{\mathrm{Sch}}(x)$
return $\mathcal{H}[x]$

adversary $A = (A_1, A_2)$ wins the 3-aWitExt game, indicating successful forgery of the signature.

Because the PPT adversary acts as the witness extractor, in the case of two-party witness extractability, we consider the scenario where a user corresponding to the secretary becomes the adversary. Under the three-party conditions, however, either the secretary U_1, who may receive the public statement, or the main signer U_2, can potentially become the adversary. Therefore, as with Lemma 3, we consider two cases (i) and (ii).

The strategy involves sending the adversary a complete signature and behaving as if that signature were a valid pre-signature. However, in the pre-signature simulation in aWitExt, unlike in aSigForge, the adversary outputs the public statement Y along with the message M, so the game does not select pairs (Y, y). Therefore, S cannot convert a full signature to a pre-signature by executing Adapt$(\sigma, -y)$ with the secret witness y.

Thus, to enable this transformation even without knowing y, we program a random oracle in which the values of $H(g^x|K|m)$ and $H(g^x|KY|m)$ are swapped (where the simulator knows $K = g^k$, g^x, and Y). Here, if at least one of $g^x|K|m$ or $g^x|KY|m$ has been queried to H before, the random oracle cannot be programmed. However, because A is PPT and k is uniformly randomly chosen from $\mathbb{Z}_q$, the probability that these values have been queried to H before is negligibly low.

Now, by considering the above points, we can outline the proof of three-party unforgeability.

Proof. As noted above, we divide Lemma 4 into two cases, (i) and (ii), and we perform several game hops in each case to prove the lemma. For case (i), we can follow a similar procedure to the proof of unforgeability in the original two-party scenario in Lemma 5 of [1] and in Lemma 3. Hence, we demonstrate each game hop and reduction efficiency as follows.

Case (i). For case (i), we have the following game definitions for $\mathbf{G}_0$ to $\mathbf{G}_4$ and strongSigForge.

Game $\mathbf{G}_0$: A three-party adapter signature game, $\mathsf{3\text{-}aWitExt}_{\mathcal{A}_2,\mathsf{AS}_{R_g,\Sigma}}$.

Game $\mathbf{G}_1$: An abort game for when queries to the oracle from A_2 overlap for $H'[\mathsf{pk}||K||M]$ and $H'[\mathsf{pk}||K \cdot Y||M]$

Game $\mathbf{G}_2$: A game where the pre-signature oracle returns a regular signature

Game $\mathbf{G}_3$: A game where the same modifications as for $\mathbf{G_1}$ are applied to S. The game aborts if S has already queried $H^{'}[\mathsf{pk}||K||M]$ and $H^{'}[\mathsf{pk}||K{\cdot}Y||M]$.

Game $\mathbf{G}_4$: A game where the same modifications as for $\mathbf{G_2}$ are applied to S. The game passes regular signatures to A instead of pre-signatures.

Game strongSigForge: A SUF-CMA game for regular signatures.

The reduction loss for the above is as follows and can be directly obtained from the original two-party scenario:

$$\begin{aligned}
&\Pr[\mathsf{3\text{-}aWitExt}_{\mathcal{A}_2,\mathsf{3\text{-}AS}_{R_g,\Sigma_{\text{Sch}}}}(\lambda) = 1] \\
&= \Pr[\mathbf{G}_0 = 1] \\
&\leq \Pr[\mathbf{G}_1 = 1] + v(\lambda) \\
&= \Pr[\mathbf{G}_2 = 1] + v(\lambda) \\
&= \Pr[\mathbf{G}_3 = 1] + v(\lambda) + v(\lambda) \\
&\leq \Pr[\mathbf{G}_4 = 1] + 2v(\lambda) \\
&= \Pr[\mathsf{strongSigForge}_{S^{\mathcal{A}_2},\mathsf{3\text{-}AS}_{R_g,\Sigma_{\text{Sch}}}}(\lambda) = 1] + 2v(\lambda),
\end{aligned} \tag{6}$$

where v is a negligible function in λ.

Case (ii). For case (ii), we have the following game definitions for $\mathbf{G}_0$ to $\mathbf{G}_6$ and strongSigForge.

Game $\mathbf{G}_0$: A three-party adapter signature game, $\mathsf{3\text{-}aWitExt}_{\mathcal{A}_1,\mathsf{AS}_{R_g,\Sigma}}$. The changes from 3-aWitExt to G_0 involve recording the hash values in the game's random oracle, namely the addition of $H := [\perp]$. The reduction between the games is $\Pr[\mathsf{3\text{-}aWitExt}_{\mathcal{A}_1,\mathsf{3\text{-}AS}_{R_g,\Sigma_{\text{Sch}}}}(\lambda) = 1] = \Pr[\mathbf{G}_0 = 1]$.

Game $\mathbf{G}_1$: A game that aborts if queries to the pre-signature oracle from A_2 overlap for $H'[\mathsf{pk}_2||K||M]$ and $H'[\mathsf{pk}_2||K \cdot Y_1||M]$. The modification from G_0 to G_1 is that, in the pre-signature oracle $\mathcal{O}_{pS}$, if either the pre-signature's format or the normal Schnorr signature's format has already been queried to the random oracle $\mathcal{H}$, the game aborts. Let Bad_1 denote the event that G_1 aborts. Let ℓ denote the total number of queries to each oracle. Because ℓ is a polynomial in λ and v is a negligible function, the reduction between the games is as follows:

$$\begin{aligned}
\Pr[\mathsf{Bad}_1] &= \Pr[H'[\mathsf{pk}_2||K||M] \neq \perp \wedge H'[\mathsf{pk}_2||K \cdot Y_1||M] \neq \perp] \\
&\leq 2\frac{\ell}{q} := v_1(\lambda),
\end{aligned}$$

where v_1 is negligible in λ. Therefore, we obtain $\Pr[G_0 = 1] \leq \Pr[G_1 = 1] + v_1(\lambda)$.

Game $\mathbf{G}_2$: A game that aborts if queries from A to the pre-adaptation oracle overlap. The modification from G_1 to G_2 is that, in the pre-adaptation oracle $\mathcal{O}_{pA}$, if either the pre-signature's format or the normal Schnorr signature's format has already been queried to the random oracle $\mathcal{H}$, the game aborts. Similarly to G_1, the reduction between the games is as follows:

$$\Pr[G_1 = 1] \leq \Pr[G_2 = 1] + v_2(\lambda),$$

where v_2 is negligible in λ.

Game $\mathbf{G}_3$: A game whose pre-signature oracle returns a regular signature. In this game G_3, the pre-signature oracle $\mathcal{O}_{pS}$ outputs the signature σ instead of a pre-signature $\tilde{\sigma}$. The value of $H[\mathsf{pk}||K||M]$ is set to $H[\mathsf{pk}||K \cdot Y||M]$, and $H[\mathsf{pk}||K||M]$ is set to a new random value by the random oracle.

The adversary A cannot distinguish full signatures and pre-signatures, but it can only notice the change in this game if the random oracle has been queried on either $\mathsf{pk}||K||M$ or $\mathsf{pk}||K \cdot Y||M$. However, as this case is covered in G_1, the reduction loss is $\Pr[G_2 = 1] = \Pr[G_3 = 1]$.

Game $\mathbf{G}_4$: A game where the pre-adaptation oracle returns regular signatures. In this game G_4, the pre-adaptation oracle $\mathcal{O}_{pA}$ generates a regular signature σ instead of a pre-signature $\tilde{\sigma}$. However, because this oracle's form differs from that of a pre-signature oracle, some adjustments are necessary. These adjustments can be made similarly to those for the unforgeability game G_3. First, the value of $H[\mathsf{pk}||K||M]$ is set to $H[\mathsf{pk}||K \cdot Y||M]$, and $H[\mathsf{pk}||K||M]$ is set to a new random value by the random oracle. As in Game G_3 above, the adversary A cannot distinguish full signatures and pre-signatures but can only notice the change in this game if the random oracle has been queried on either $\mathsf{pk}||K||M$ or $\mathsf{pk}||K \cdot Y||M$. Again, this case is covered in G_1.

Next, the adversary's output forged witness y_2' is checked against the challenge statement Y_2^* (by chance) or on the oracle side. If y_2' does not correspond to Y_2^*, the game aborts. The probability here is equal to the probability of breaking the hard relation v_3. Therefore, the reduction loss is $\Pr[G_3 = 1] \leq \Pr[G_4 = 1] + v_3(\lambda)$, where v_3 is negligible in λ.

Game $\mathbf{G}_5$: A game that applies the same modifications as in $\mathbf{G_1}$ and $\mathbf{G}_2$ to S. The game aborts if S has already queried $H^{'}[\mathsf{pk}||K||M]$ and $H^{'}[\mathsf{pk}||K \cdot Y||M]$. The reduction loss is $\Pr[G_4 = 1] \leq \Pr[G_5 = 1] + v_1(\lambda) + v_2(\lambda)$.

Game $\mathbf{G}_6$: A game that applies the same modifications as in $\mathbf{G}_3$ and $\mathbf{G}_4$ to S. The game passes regular signatures instead of pre-signatures to A. The reduction loss is $\Pr[G_5 = 1] \leq \Pr[G_6 = 1] + v_3(\lambda)$.

Game strongSigForge: The SUF-CMA game for regular signatures. In this game, unlike in 3-aEUF-CMA security, the adversary A_1 outputs a message M^* and public statements Y_1^*, Y_2^* as the challenge messages. Therefore, to convert full signatures into pre-signatures, the random oracle's output is programmed such that full signatures become regular signatures and vice versa. As a result, although regular Schnorr signatures are sent to the adversary, it can behave as if those signatures are valid pre-signatures, thus fully simulating Game G_6. Note that we will give a formal, detailed proof of this in the full version of this paper. Hence, the reduction is $\Pr[G_6 = 1] = \Pr[\mathsf{strongSigForge} = 1]$.

Finally, from the above discussion, the reduction efficiency for case (ii) is as follows:

$$
\begin{aligned}
&\Pr[\mathsf{3\text{-}aWitExt}_{\mathcal{A}_1,\mathsf{3\text{-}AS}_{R_g,\Sigma_{\mathrm{Sch}}}}(\lambda)=1]\\
&=\Pr[\mathbf{G}_0=1]\\
&\le \Pr[\mathbf{G}_1=1]+v_1(\lambda)\\
&\le \Pr[\mathbf{G}_2=1]+v_1(\lambda)+v_2(\lambda)\\
&=\Pr[\mathbf{G}_3=1]+v_1(\lambda)+v_2(\lambda)\\
&\le \Pr[\mathbf{G}_4=1]+v_1(\lambda)+v_2(\lambda)+v_3(\lambda)\\
&\le \Pr[\mathbf{G}_5=1]+2v_1(\lambda)+2v_2(\lambda)+v_3(\lambda)\\
&\le \Pr[\mathbf{G}_6=1]+2v_1(\lambda)+2v_2(\lambda)+2v_3(\lambda)\\
&=\Pr[\mathsf{strongSigForge}_{S^{A_1},\mathsf{3\text{-}AS}_{R_g,\Sigma_{\mathrm{Sch}}}}(\lambda)=1]+2v_1(\lambda)+2v_2(\lambda)+2v_3(\lambda).
\end{aligned}
$$

3 N-Party Adaptor Signatures

In this section, we extend the two-party adapter signatures defined in Section 1.4 to construct an N-party adapter signature scheme $\mathsf{N\text{-}AS}_{R,\Sigma}$. Here, we denote the N entities as $U_1,\cdots,U_i,\cdots,U_n$. Each entity is classified into one of three types: U_n as the entity that generates the initial pre-signature, U_1 as the entity that finally adapts from pre-signatures to a regular signature, and U_i as all the other entities. In constructing N-party adapter signatures, we assume the same digital signature scheme and computationally hard algebraic relation used in the two-party case. Additionally, the subscripts for each algorithm (e.g., U_n in $\mathsf{PreSign}_{U_n}$) correspond to the entity executing the algorithm, and the subscripts for each argument (e.g., i in Y_i or n in σ_n) correspond to the entity that initially owns (or generates) that value.

Syntax of Proposed N-Party Adaptor Signatures Setup. U_1 executes the algebraic relation generation algorithm $(Y_1,y_1)\leftarrow\mathsf{GenR}(1^n)$; the U_i $(2\le i<n)$ execute the key generation algorithm $(\mathsf{sk}_i,\mathsf{pk}_i)\leftarrow\mathsf{KeyGen}(\lambda)$ and the algebraic relation generation algorithm $(Y_i,y_i)\leftarrow\mathsf{GenR}(1^n)$; and U_n executes the key generation algorithm $(sk_n,pk_n)\leftarrow\mathsf{KeyGen}(\lambda)$.
Pre-signing: $\sigma_n\leftarrow\mathsf{PreSign}_{U_n}((\mathsf{pk}_n,\mathsf{sk}_n),Y_{n-1},M)$**.** The pre-signing algorithm $\mathsf{PreSign}_{U_n}$ is executed by U_n and takes as input the key pair $(\mathsf{pk}_n,\mathsf{sk}_n)$ of U_n, the public information Y_{n-1} of U_{n-1}, and the message M; then, it outputs the pre-signature σ_n. Note that all entities except U_1 generate pre-signatures, but because entities other than U_1 and U_n generate pre-signatures with the $\mathsf{PreAdapt}$ algorithm, only U_n executes this pre-signing algorithm.
Pre-verification: $0/1\leftarrow\mathsf{PreVrfy}_{U_i}(\{Y_j\}_{j=i}^{n-1},\{\mathsf{pk}_j\}_{j=i+1}^{n},\{\sigma_j\}_{j=i+1}^{n},M)$**.** The pre-verification algorithm $\mathsf{PreVrfy}_{U_i}$ is executed by the U_i $(1\le i<n)$. It takes as input the public information $(Y_i,\ldots,Y_{n-1})$ from U_i to U_{n-1}, the pre-signatures $(\sigma_{i+1},\ldots,\sigma_n)$ and public keys $(\mathsf{pk}_{i+1},\ldots,\mathsf{pk}_n)$ generated by U_{i+1} to U_n, and

the message M, and it performs pre-signature verification. It outputs 1 if the signature is accepted, or 0 otherwise.

Pre-adaptation: $\sigma_i \leftarrow \mathsf{PreAdapt}_{U_i}((Y_i, y_i), Y_{i-1}, \mathsf{pk}_{i+1}, (\mathsf{sk}_i, \mathsf{pk}_i), \sigma_{i+1}, M)$**.** The pre-adaptation algorithm $\mathsf{PreAdapt}_{U_i}$ is executed by the U_i $(2 \le i < n)$. It takes as input the algebraic relation pair (Y_i, y_i) of U_i, the public information Y_{i-1} of U_{i-1}, the public key pk_{i+1} of U_{i+1}, the key pair $(\mathsf{sk}_i, \mathsf{pk}_i)$ of U_i, the pre-signature σ_{i+1} generated by U_{i+1}, and the message M; then, it outputs the pre-signature σ_i.

Adaptation: $\sigma_1 \leftarrow \mathsf{Adapt}_{U_1}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M)$: The adaptation algorithm Adapt_{U_1} is executed by U_1. It takes as input the algebraic relation pair (Y_1, y_1) of U_1, the public key pk_2 of U_2, the signature σ_2 generated by U_2, and the message M, and it outputs the signature σ_1.

Extraction: $y_{i-1} \leftarrow \mathsf{Ext}_{U_i}(Y_{i-1}, \sigma_i, \sigma_{i-1})$: The extraction algorithm Ext_{U_i} is executed by the U_i $(2 \le i \le n)$. It takes as input the public information Y_{i-1} of U_{i-1} and the signatures σ_i and σ_{i-1} generated by U_i and U_{i-1}, respectively, and it outputs the secret information y_{i-1}.

The N-party adaptor signature scheme $\mathsf{N\text{-}AS}_{R,\Sigma}$ satisfies the following correctness.

Definition 5 (Pre-signature correctness for N parties) *For any message $M \in \{0,1\}^*$ and $(Y_1, y_1) \dots (Y_{n-1}, y_{n-1}) \in R$, the N-party adaptor signature scheme $\mathsf{N\text{-}AS}_{R,\Sigma}$ satisfies pre-signature correctness for N parties if the following holds:*

$$\Pr\left[\begin{array}{l|l} & \{\mathsf{sk}_j, \mathsf{pk}_j\}_{j=2}^{n} \leftarrow \mathsf{Gen}(1^\lambda); \\ \mathsf{PreVrfy}_{U_i}(\{Y_j\}_{j=i}^{n-1}, & \{Y_j, y_j\}_{j=1}^{n-1} \leftarrow \mathsf{GenR}(1^\lambda); \\ \quad \{\mathsf{pk}_j, \sigma_j\}_{j=i+1}^{n}, M) = 1; & \sigma_n \leftarrow \mathsf{PreSign}_{U_n}((\mathsf{pk}_n, \mathsf{sk}_n), Y_{n-1}, M); \\ \mathsf{Vrfy}(\mathsf{pk}_i, M, \sigma_{i-1}) = 1; & \sigma_i \leftarrow \mathsf{PreAdapt}_{U_i}((Y_i, y_i), Y_{i-1}, \\ (Y_{i-1}, y'_{i-1}) \in R & \qquad \mathsf{pk}_{i+1}, (\mathsf{sk}_i, \mathsf{pk}_i), \sigma_{i+1}, M); \\ & y_{i-1} := \mathsf{Ext}_{U_i}(Y_{i-1}, \sigma_i, \sigma_{i-1}); \\ & \sigma_1 := \mathsf{Adapt}_{U_1}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) \end{array}\right] = 1.$$

3.1 Concrete Construction of Schnorr-Based N-Party Adaptor Signatures

Here, we extend the three-party adapter signature scheme defined in Section 2 to describe a specific instantiation of the Schnorr-based N-party adapter signature scheme given in Fig. 3. For Schnorr signatures Σ_{Sch} and a hard relation $R_g := \{(Y, y) | Y = g^y\}$, we show the concrete construction of the N-party adapter signature scheme $\mathsf{N\text{-}AS}_{R_g, \Sigma_{\mathsf{Sch}}}$.

Fig. 3. Concrete construction: Schnorr-based N-party adaptor signatures.

U_1: $\underline{(Y_1, y_1) \leftarrow \mathsf{GenR}(\lambda);}$

$$y_1 \leftarrow \mathbb{Z}_q^*,\ Y_1 := g^{y_1},$$
return Y_1 to U_2.

U_2: $\underline{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \mathsf{KeyGen}(\lambda),}$
$\underline{(Y_i, y_i) \leftarrow \mathsf{GenR}(\lambda);}$

$$\mathsf{sk}_i := x_i \leftarrow \mathbb{Z}_q,\ \mathsf{pk}_i = X_2 := g^{x_i} \in \mathbf{G},$$
$$y_i \leftarrow \mathbb{Z}_g^*,\ Y_i := g^{y_i},$$
return Y_i to U_{i+1} and pk_i to U_{i-1}, U_{i+1}.

U_n: $\underline{(\mathsf{sk}_n, \mathsf{pk}_n) \leftarrow \mathsf{KGen}(\lambda);}$

$$\mathsf{sk}_n := x_n \leftarrow \mathbb{Z}_q^*,\ \mathsf{pk}_n = X_n := g^{x_n} \in \mathbf{G},$$
return pk_n to U_i.

U_n: $\underline{\hat{\sigma}_n \leftarrow \mathsf{PreSign}_{U_n}((\mathsf{pk}_n, \mathsf{sk}_n), Y_{n-1}, M);}$

$$k_n \leftarrow \mathbb{Z}_q,\ r_n := \mathcal{H}(X_n || g^{k_n} Y_{n-1} || M),$$
$$s_n := k_n + r_n \cdot x_n,\ \hat{\sigma}_n := (r_n, s_n),$$
return $(\hat{\sigma}_n, M)$ to U_{n-1}.

U_i: $(1 \le i \le n-1)$:
$\underline{0/1 \leftarrow \mathsf{PreVrfy}_{U_i}\left(\{Y_j\}_{j=i}^{n-1}, \{\mathsf{pk}_j\}_{j=i+1}^{n}, \{\sigma_j\}_{j=i+1}^{n}, M\right);}$

For $1 \le i \le n-1$, $i+1 \le j \le n$,

return 1 if $r_j = \mathcal{H}\left(X_j || g^{s_j} \cdot X_j^{-r_j} \cdot Y_{j-1} || M\right)$.

$U_i(2 \le i \le n-1)$:
$\underline{\hat{\sigma}_i \leftarrow \mathsf{PreAdapt}_{U_i}\left((Y_i, y_i), Y_{i-1}, \mathsf{pk}_{i+1}, (\mathsf{sk}_i, \mathsf{pk}_i), \sigma_{i+1}, M\right);}$

$$k_i \leftarrow \mathbb{Z}_q,\ r_i := \mathcal{H}\left(X_i || g^{k_i} Y_{i-1} || M\right),$$
$$s_i := k_i + r_i \cdot x_i,\ s'_{i+1} := s_{i+1} + y_i,$$
$$\hat{\sigma}_i = (r_i, s_i, s'_{i+1}),$$
return $\{\hat{\sigma}_j\}_{j=i}^{n}$ and M to U_{i-1} and $\hat{\sigma}_i$ to U_{i+1}.

U_1: $\underline{\sigma_1 = \mathsf{Adapt}_{U_1}((Y_1, y_1), \mathsf{pk}_2, \hat{\sigma}_2, M);}$

$$s_1 := s_2 + y_1,\ \sigma_1 := (r_2, s_1),$$
return σ_1 to U_2.

U_2: $\underline{y'_1 / \perp = \mathsf{Ext}_{U_2}(Y_1, (\hat{\sigma}_2, \sigma_1));}$

$$y'_1 := s_1 - s_2,$$
return y'_1, If $(Y_1, y'_1) \in R$, otherwise, return $\perp$.

$U_i(2 < i \le n)$:
$\underline{y'_{i-1} / \perp = \mathsf{PreExt}_{U_i}(Y_{i-1}, \hat{\sigma}_i, \hat{\sigma}_{i-1});}$

For $2 < i \le n$, $y'_{i-1} := s'_i - s_i$.
return y'_{i-1}, if $(Y_{i-1}, y'_{i-1}) \in R$, otherwise, return $\perp$.

3.2 Security of N-party Adaptor Signature Scheme

We now extend the security definitions of Section 2.2 to define the security properties that the N-party adaptor signatures, as defined in Section 3, should satisfy.

First, existential unforgeability against chosen-plaintext attacks for N-party adapter signatures (N-aEUF-CMA) extends the unforgeability definition for adapter signatures (Definition 10) to N parties. Here, because the signature content depends on the generating entity, it is necessary to consider unforgeability for n entities with $n-1$ interactions each. Hence, we consider two cases. The first case is unforgeability between U_n and U_{n-1}. In this case, U_n generates a pre-signature via the PreSign algorithm, and the adversary attempts to forge signatures via the signature/pre-signature oracle. The second case is unforgeability between U_i and U_{i+1} for $1 \leq i \leq n-2$. Here, U_{i+1} generates a pre-signature via the PreAdapt algorithm, and the adversary attempts to forge signatures via the signature/pre-adaptation oracle. We define N-aEUF-CMA as follows.

Table 10. Experiment $\mathsf{N\text{-}aSigForge}_{\mathcal{A},\mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda)$

$\mathsf{N\text{-}aSigForge}^{i}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda)$

$1: Q := \emptyset,\ (\mathsf{sk}_{i+1}, \mathsf{pk}_{i+1}) \leftarrow \mathsf{Gen}(1^{\lambda})$
$2: (Y_i, y_i) \leftarrow \mathsf{GenR}(1^{\lambda})$
$3: (M, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pA}(\cdot,\cdot,\cdot)}(\{\mathsf{pk}_j\}_{j=i+1}^{n}, \{Y_j\}_{j=i}^{n-1})$
$4: \sigma_{i+1} \leftarrow \mathsf{PreAdapt}_{U_{i+1}}((Y_i, y_i), Y_{i-1}, \mathsf{pk}_{i+1}, (\mathsf{sk}_i, \mathsf{pk}_i), \sigma_{i+1}, M)$
$5: \sigma_i \leftarrow \mathcal{A}_2^{\mathcal{O}_S(\cdot),\mathcal{O}_{pA}(\cdot,\cdot,\cdot)}(\{\sigma_j\}_{j=i+1}^{n}, \mathsf{st})$
$6: \textbf{return } (M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_{i+1}, \sigma_i, M))$

$\mathsf{N\text{-}aSigForge}^{n-1}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda)$

$1: Q := \emptyset,\ (\mathsf{sk}_n, \mathsf{pk}_n) \leftarrow \mathsf{Gen}(1^{\lambda})$
$2: (Y_{n-1}, y_{n-1}) \leftarrow \mathsf{GenR}(1^{\lambda})$
$3: (M, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\mathsf{pk}_n, Y_{n-1})$
$4: \sigma_n \leftarrow \mathsf{PreSign}_{U_n}((\mathsf{pk}_n, \mathsf{sk}_n), Y_{n-1}, M)$
$5: \sigma_{n-1} \leftarrow \mathcal{A}_2^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\sigma_n, \mathsf{st})$
$6: \textbf{return } (M \notin Q \wedge \mathsf{Vrfy}_{U_n}(\mathsf{pk}_n, \sigma_{n-1}, M))$

$\mathcal{O}_{pA}(M, (Y_i, Y_{i+1}), \sigma_{i+2})$

$1: \sigma_i \leftarrow \mathsf{PreAdapt}_{U_i}((Y_i, y_i), Y_{i-1}, \mathsf{pk}_{i+1}, (\mathsf{sk}_i, \mathsf{pk}_i), \sigma_{i+1}, M)$
$2: Q := Q \cup \{M\}$
$3: \textbf{return } \sigma_i$

$\mathcal{O}_S(M)$	$\mathcal{O}_{pS}(M, Y_{n-1})$
$1: \sigma_i \leftarrow \mathsf{Sign}(\mathsf{sk}_i, M)$	$1: \sigma_n \leftarrow \mathsf{PreSign}(\mathsf{sk}_n, Y_{n-1}, M)$
$2: Q := Q \cup \{M\}$	$2: Q := Q \cup \{M\}$
$3: \textbf{return } \sigma_i$	$3: \textbf{return } \sigma_n$

Definition 6 (Existential unforgeability for N parties) *An N-party adaptor signature scheme* $\mathsf{N\text{-}AS}_{R,\Sigma}$ *is* $\mathit{N\text{-}aEUF\text{-}CMA}$ *secure if for any PPT adversary* $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_{N-1})$*, there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\sum_{i=1}^{N-2} \Pr[\mathsf{N\text{-}aSigForge}_{\mathcal{A}_i, \mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda) = 1] + \Pr[\mathsf{N\text{-}aSigForge}_{\mathcal{A}_{N-1}, \mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda) = 1]$$
$$\leq \mathsf{negl}(\lambda)$$

where the experiments $\mathsf{N\text{-}aSigForge}_{\mathcal{A}_i, \mathsf{N\text{-}AS}_{R,\Sigma}}$ *and* $\mathsf{N\text{-}aSigForge}_{\mathcal{A}_{N-1}, \mathsf{N\text{-}AS}_{R,\Sigma}}$ *are as defined in the Table 10.*

Regarding pre-signature adaptability for N-party adapter signatures, as with unforgeability, it is necessary to consider separate cases depending on which signer is considered as the malicious attacker. Here, we consider U_i $(2 \leq i \leq n)$ as the entity attempting to adapt the pre-signature. This is because N-party adapter signatures entail $n-1$ consecutive interactions, so the legitimacy between entities cannot be guaranteed when two or more attackers are present.

Definition 7 (Pre-signature adaptability for N parties) *For any message* $M \in \{0,1\}^*$*, algebraic relation pairs* $\{Y_j, y_j\}_{j=1}^{n-1} \in R$*, and public keys* $\{\mathsf{pk}_j\}_{j=2}^{n}$*, the N-party adaptor signature scheme* $\mathsf{N\text{-}AS}_{R,\Sigma}$ *satisfies pre-signature adaptability for N parties if the following requirements hold. (i) When* U_n *is the attacker, for any randomly chosen pre-signature* $\sigma_n \leftarrow \{0,1\}^*$ *satisfying* $\mathsf{PreVrfy}_{U_{n-1}}(\mathsf{pk}_n, M, Y_{n-1}, \sigma_n) = 1$*, we have*

$$\mathsf{Vrfy}_{U_n}(M, \mathsf{pk}_n, \mathsf{PreAdapt}_{U_{n-1}}((Y_{n-1}, y_{n-1}), Y_{n-2}, \mathsf{pk}_n, (\mathsf{sk}_{n-1}, \mathsf{pk}_{n-1}), \sigma_n, M)) = 1.$$

(ii) When U_i $(2 \leq i < n)$ *is the attacker, for any* $\sigma_n \leftarrow \mathsf{PreSign}_{U_n}((\mathsf{pk}_n, \mathsf{sk}_n), Y_{n-1}, M)$ *and* $\sigma_i \leftarrow \{0,1\}^*$ *satisfying* $\mathsf{PreVrfy}_{U_i}(\{Y_j\}_i^{n-1}, \{\mathsf{pk}_j\}_{j=i+1}^n, \{\sigma_j\}_{j=i+1}^n, M) = 1$*, the following conditions hold: for* $2 < i < n$*,*

$$\mathsf{Vrfy}_{U_n}(M, \mathsf{pk}_n \mathsf{PreAdapt}_{U_{n-1}}((Y_{n-1}, y_{n-1}), Y_{n-1}, \mathsf{pk}_n, (\mathsf{sk}_{n-1}, \mathsf{pk}_{n-1}), \sigma_n, M)) = 1,$$

and for $i = 2$*,*

$$\mathsf{Vrfy}_{U_n}(M, \mathsf{pk}_i, \mathsf{Adapt}_{U_{i-1}}((Y_i, y_i), Y_{i-1}, \mathsf{pk}_i, \sigma_i, M)) = 1.$$

Next, we consider the extension of witness extractability. Again, depending on which entity among the N parties extracts secret information—i.e., when U_i is the attacker for $1 \leq i < n-1$, or when U_n is the attacker—we need to distinguish these cases. Note, however, that the entity extracting secret information is limited to the U_i $(1 \leq i \leq n-1)$.

Definition 8 (Witness extractability for N parties) *The N-party adaptor signature scheme* $\mathsf{N\text{-}AS}_{R,\Sigma}$ *is witness extractable if for every PPT adversary* $\mathcal{A}$ *there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\sum_{i=1}^{n-2} \Pr[\mathsf{N\text{-}aWitExt}^{1 \leq i < n-1}_{\mathcal{A}_i, \mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda) = 1] + \Pr[\mathsf{N\text{-}aWitExt}^{i=n-1}_{\mathcal{A}_{N-1}, \mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda) = 1]$$
$$\leq \mathsf{negl}(\lambda),$$

for experiments $\mathsf{N\text{-}aWitExt}^{1\leq i<n-1}_{\mathcal{A}_i,\mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda)$ *and* $\mathsf{N\text{-}aWitExt}^{i=n-1}_{\mathcal{A}_{n-1},\mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda)$.

Table 11. Experiment $\mathsf{N\text{-}aWitExt}_{\mathcal{A},\mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda)$

$\mathsf{N\text{-}aWitExt}^{1\leq i<n-1}_{\mathcal{A}_i,\mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda)$

1: $Q := \emptyset$, $(\mathsf{sk}_{i+1}, \mathsf{pk}_{i+1}) \leftarrow \mathsf{Gen}(1^\lambda)$
2: $(M, Y_i, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pA}(\cdot,\cdot)}(\mathsf{pk}_{i+1}, Y_{i+1})$
3: $\sigma_{i+1} \leftarrow \mathsf{PreAdapt}_{U_{i+1}}((Y_{i+1}, y_{i+1}), Y_i, \mathsf{pk}_{i+2}, (\mathsf{sk}_{i+1}, \mathsf{pk}_{i+1}), \sigma_{i+2}, M)$
4: $\sigma_i \leftarrow \mathcal{A}_2^{\mathcal{O}_S(\cdot),\mathcal{O}_{pA}(\cdot,\cdot)}(\sigma_{i+1}, \mathsf{st})$
5: $\mathbf{return}(Y_i, \mathsf{Ext}_{U_{i+1}}(Y_i, \sigma_i, \sigma_{i+1}) \wedge M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_{i+1}, \sigma_i, M))$

$\mathsf{N\text{-}aWitExt}^{i=n-1}_{\mathcal{A}_{n-1},\mathsf{N\text{-}AS}_{R,\Sigma}}(\lambda)$

1: $Q := \emptyset$, $(\mathsf{sk}_{n-1}, \mathsf{pk}_{n-1}) \leftarrow \mathsf{Gen}(1^\lambda)$
2: $(M, Y_{n-1}, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\mathsf{pk}_{n-1})$
3: $\hat{\sigma}_{n-1} \leftarrow \mathsf{PreSign}(\mathsf{sk}_{n-1}, Y_{n-1}, M)$
4: $\sigma_n \leftarrow \mathcal{A}_2^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\hat{\sigma}_{n-1}, \mathsf{st})$
5: $\mathbf{return}\ (Y_{n-1}, \mathsf{Ext}_{U_n}(\sigma_n, \sigma_i, Y) \wedge M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_{n-1}, \sigma_n, M))$

$\mathcal{O}_{pA}(Y_i, Y_{i+1}, M)$

1: $\sigma_{i+1} \leftarrow \mathsf{PreAdapt}_{U_{i+1}}((Y_{i+1}, y_{i+1}), Y_i, \mathsf{pk}_{i+2}, (\mathsf{sk}_{i+1}, \mathsf{pk}_{i+1}), \sigma_{i+2}, M)$
2: $Q := Q \cup \{M\}$
3: $\mathbf{return}\ \sigma_{i+1}$

$\mathcal{O}_S(M)$	$\mathcal{O}_{pS}(M, Y_i)$
1: $\sigma_i \leftarrow \mathsf{Sign}(\mathsf{sk}_{i+1}, M)$	*1* : $\sigma_{i+1} \leftarrow \mathsf{PreSign}(\mathsf{sk}_{i+1}, Y_i, M)$
2: $Q := Q \cup \{M\}$	*2* : $Q := Q \cup \{M\}$
3: $\mathbf{return}\ \sigma_i$	*3* : $\mathbf{return}\ \sigma_{i+1}$

3.3 Security Proofs for N-Party Adaptor Signature Scheme

In this section, we demonstrate that N-party adapter signatures based on Schnorr signatures satisfy the security properties defined above. Note that each proof is a straightforward extension of the corresponding proof given for the three-party case in Section 2.3.

Theorem 2 *If the Schnorr signature scheme Σ_{Sch} is SUF-CMA secure, and R_g is a computationally hard algebraic relation, then $\mathsf{N\text{-}AS}_{R_g,\Sigma_{\mathsf{Sch}}}$ in Fig. 3 is secure in the random oracle model.*

To demonstrate the validity of Theorem 2, it suffices to show that it satisfies Definitions 5, 6, 7, and 8. Each of these properties has already been proven for the three-party case, and it is then trivial that they hold for the N-party case.

Regarding pre-signature correctness and pre-signature adaptability for N parties, it is sufficient to demonstrate that the two verification procedures Vrfy and $\mathsf{PreVrfy}_{U_i}$ hold in the N-party construction.

Finally, regarding existential unforgeability and witness extractability for N parties, we can apply similar case-by-case reasoning as in the three-party case. In the three-party scenario, we considered an attacker A_2 between U_2 and U_3 as case (i) and an attacker A_1 between U_1 and U_2 as case (ii). The same approach can be used for the N-party scenario: we consider an attacker A_{n-1} between U_{n-1} and U_n as case (i), and an attacker A_i between U_i and U_{i+1} as case (ii), with iteration over $1 \leq i \leq n-2$. This straightforward extension yields the desired results.

4 Conclusion

In this paper, we explored a general extension of adapter signature schemes that previously applied for two parties. First, we extended the two-party adapter signature scheme to three parties and presented the security requirements that the extended scheme should satisfy. We also provided a specific construction example using Schnorr signatures. Then, we demonstrated that the resulting Schnorr-signature-based, three-party adapter signature scheme satisfies all the defined security properties. Furthermore, by extending the scheme to N parties, we showed a general construction method for N-party adapter signatures and again provided a specific construction example using Schnorr signatures. This illustrates the ease of extending from three to N parties.

References

1. Aumayr, L., Ersoy, O., Erwig, A., Faust, S., Hostáková, K., Maffei, M., Moreno-Sanchez, P., and Riahi, S.: *Generalized channels from limited blockchain scripts and adaptor signatures*, Asiacrypt (2021).
2. Aumayr, L., Thyagarajan, S. A., Malavolta, G., Moreno-Sanchez, P., and Maffei, M.: *Sleepy channels: Bi-directional payment channels without watchtowers*, ACM CCS (2022).
3. Bagaria, V., Neu, J., and Tse, D.: *Boomerang: Redundancy improves latency and throughput in payment-channel networks*, FC (2020).
4. Chen, Y., Liu, J. N., Yang, A., Weng, J., Chen, M. R., Liu, Z., and Li, M.: *PACDAM: Privacy-Preserving and Adaptive Cross-Chain Digital Asset Marketplace*, IEEE Internet of Things Journal (2023).
5. Dai, W., Okamoto, T., and Yamamoto, G.: *Stronger security and generic constructions for adaptor signatures*, Indocrypt (2022).
6. Debris-Alazard, T., Sendrier, N., and Tillich, J.-P.: *Wave: A new code-based signature scheme*, Cryptology ePrint Archive, 2018/996 (2018).
7. Deshpande, A. and Herlihy, M.: *Privacy-preserving cross-chain atomic swaps*, FC (2020).
8. Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and Stehle, D.: *CRYSTALS–Dilithium: Digital Signatures from Module Lattices*, CHES (2018).
9. Erwig, A., Faust, S., Hostáková, K., Maitra, M., and Riahi, S.: *Two-party adaptor signatures from identification schemes*, PKC (2021).
10. Erwig, A. and Riahi, S.: *Deterministic Wallets for Adaptor Signatures*, ESORICS (2022).

11. Esgin, M. F., Ersoy, O., and Erkin, Z.: *Post-quantum adaptor signatures and payment channel networks*, ESORICS (2020).
12. Fiat, A. and Shamir, A.: *How to prove yourself: Practical solutions to identification and signature problems*, Eurocrypt (1986).
13. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., and Gervais, A.: *Sok: Layer-two blockchain protocols*, FC (2020).
14. Han, R., Lin, H., and Yu, J.: *On the optionality and fairness of atomic swaps*, The 1st ACM Conference on Advances in Financial Technologies (2019).
15. Hoenisch, P. and del Pino, L. S.: *Atomic swaps between bitcoin and monero*, arXiv preprint arXiv:2101.12332 (2021).
16. Hoenisch, P., Mazumdar, S., Moreno-Sanchez, P., and Ruj, S.: *LightSwap: An Atomic Swap Does Not Require Timeouts at both Blockchains*, DPM (2022).
17. Hu, X., and Chen, H.: *Design and Analysis of an Anonymous and Fair Trading Scheme for Electronic Resources with Blind Adaptor Signature* 6th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI) (pp. 1-5). IEEE (2023).
18. Ji, Y., Xiao, Y., Gao, B., and Zhang, R.: *Threshold/Multi Adaptor Signature and Their Applications in Blockchains*, Electronics, 13(1), 76. 2023.
19. Klamti, J. B. and Hasan, M. A.: *Post-Quantum Two-Party Adaptor Signature Based on Coding Theory*, Cryptography (2022).
20. Liu, Z., Yang, A., Zeng, H., Jiang, C., and Ma, L.: *A Generalized Blockchain-Based Government Data Sharing Protocol*, Security and Communication Networks (2023).
21. Madathil, V., Thyagarajan, S. A., Vasilopoulos, D., Fournier, L., Malavolta, G., and Moreno-Sanchez, P.: *Cryptographic Oracle-Based Conditional Payments*, NDSS (2023).
22. Malavolta, G., Moreno-Sanchez, P., Schneidewind, C., Kate, A., and Maffei, M.: *Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability*, NDSS (2019).
23. Minaei, M., Chatzigiannis, P., Jin, S., Raghuraman, S., Kumaresan, R., Zamani, M., and Moreno-Sanchez, P.: *Unlinkability and Interoperability in Account-Based Universal Payment Channels*, FC (2023).
24. Mirzaei, A., Sakzad, A., Yu, J., and Steinfeld, R.: *Fppw: A fair and privacy preserving watchtower for bitcoin*, FC (2021).
25. Moreno-Sanchez, P., Blue, A., Le, D.V., Noether, S., Goodell, B., and Kate, A.: *DLSAG: non-interactive refund transactions for interoperable payment channels in monero*, FC (2020).
26. Poelstra, A.: *Scriptless Scripts. Presentation Slides*, `https://download.wpsoftware.net/bitcoin/wizardry/mw-slides/2017-05-milan-meetup/slides.pdf.` (accessed 2023-08-17).
27. Poelstra, A. and Nick, J.: *Adaptor Signatures and Atomic Swaps from Scriptless Scripts*, `https://github.com/ElementsProject/scriptless-scripts/blob/master/md/atomic-swap.md` (2017).
28. Qin, X., Pan, S., Mirzaei, A., Sui, Z., Ersoy, O., Sakzad, A., Esgin, M. F., Liu, J. K., Yu, J., and Yuen, T. H.: *Blindhub: Bitcoin-compatible privacy-preserving payment channel hubs supporting variable amounts*, IEEE S&P (2023).
29. Riahi, S., and Litos, O. S. T.: *Bitcoin Clique: Channel-free Off-chain Payments using Two-Shot Adaptor Signatures*, Cryptology ePrint Archive (2024).
30. Schnorr, C.-P.: *Efficient identification and signatures for smart cards*, CRYPTO (1990).

31. Shao, W., Wang, J., Wang, L., Jia, C., Xu, S., and Zhang, S.: *Auditable Blockchain Rewriting in Permissioned Setting with Mandatory Revocability for IoT*, IEEE Internet of Things Journal (2023).
32. Sui, Z., Liu, J. K., Yu, J., and Qin, X.: *Monet: A fast payment channel network for scriptless cryptocurrency monero*, IEEE DCS (2022).
33. Sui, Z., Liu, J. K., Yu, J., Au, M. H., and Liu, J.: *AuxChannel: Enabling efficient bi-directional channel for scriptless blockchains*, ACM AsiaCCS (2022).
34. Tairi, E., Moreno-Sanchez, P., and Maffei, M.: *A^2L: Anonymous atomic locks for scalability in payment channel hubs*, IEEE S&P (2021).
35. Tairi, E., Moreno-Sanchez, P. and Maffei, M.: *Post-quantum adaptor signature for privacy-preserving off-chain payments*, FC (2021).
36. Thyagarajan, S. A., Malavolta, G., Schmidt, F., and Schröder, D.: *Paymo: Payment channels for monero*, Cryptology ePrint Archive, 2020/1441 (2020).
37. Thyagarajan, S. A. K. and Malavolta, G.: *Lockable signatures for blockchains: Scriptless scripts for all signatures*, IEEE S&P (2021).
38. Tu, B., Zhang, M., and Yu, C.: *Efficient ECDSA-Based Adaptor Signature for Batched Atomic Swaps*, ISC (2022).
39. Wang, X., Lin, C., Huang, X., and He, D.: *Anonymity-Enhancing Multi-Hop Locks for Monero-Enabled Payment Channel Networks*, IEEE Transactions on Information Forensics and Security (2023).
40. Zhou, X., He, D., Ning, J., Luo, M., and Huang, X.: *Efficient Construction of Verifiable Timed Signatures and its Application in Scalable Payments*, IEEE Transactions on Information Forensics and Security (2023).
41. Zhu, X., He, D., Bao, Z., Peng, C., and Luo, M.: *Two-Party Adaptor Signature Scheme Based on IEEE P1363 Identity-Based Signature*, IEEE Open Journal of the Communications Society (2023).

A Preliminaries

We first introduce the cryptographic primitives and notations used in this paper. We denote by $x \leftarrow X$ the uniform sampling of a variable x from a set X. Throughout this paper, λ denotes the security parameter, and all our algorithms run in polynomial time in λ. By writing $x \leftarrow A(y)$, we mean that, on input y, a probabilistic polynomial time (PPT) algorithm A outputs x. If A is a deterministic polynomial time (DPT) algorithm, then we use the notation $x := A(y)$. A function $\mathsf{negl} : \mathbb{N} \rightarrow \mathbb{R}$ is negligible in n if, for every $k \subset N$, there exists $n_0 \in N$ s.t. for every $n \geq n_0$ it holds that $|\mathsf{negl}(n)| \leq 1/n^k$.

We next recall the definition of a hard relation R with statement/witness pairs (Y, y). Let L_R be the associated language defined as $\{Y | \exists y \text{ s.t.} (Y, y) \in R\}$. We say that R is a hard relation if the following hold: (i) There exists a PPT sampling algorithm GenR that, on input 1^λ, outputs a statement/witness pair $(Y, y) \in R$; (ii) the relation is poly-time decidable; and (iii) for all PPT A on input Y, the probability of A outputting a valid witness y is negligible.

A.1 Digital Signatures

A digital signature scheme Σ comprises the three algorithms KGen, Sign, and Vrfy. The key generation algorithm $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(\lambda)$ takes a security parameter λ as an input and outputs a secret (signing) key sk and a public (verification) key pk. The signing algorithm $\sigma \leftarrow \mathsf{Sign}(M, \mathsf{pk}, \mathsf{sk})$ takes a message M, pk, and sk as inputs and outputs a signature σ. The verification algorithm $1/0 \leftarrow \mathsf{Vrfy}(M, \mathsf{pk}, \sigma)$ takes M, pk, and σ as inputs, and it outputs 1 if the signature is accepted, or 0 otherwise. In this paper, we use a signature scheme that satisfies $\mathsf{SUF\text{-}CMA}$ (strong existential unforgeability under chosen-message attack). $\mathsf{SUF\text{-}CMA}$ security guarantees that a PPT attacker with access to the signature oracle by entering his public key pk cannot generate a new valid signature for any message M.

A.2 Schnorr signatures

In this section, we introduce one of the most fundamental signature schemes, Schnorr signatures, for later use in concrete configurations. Schnorr signatures are the most intuitive and most compatible signature scheme with adapter signatures, because Poelstra [26] used them as a base when he first presented the concrete structure of adapter signatures.

First, let $\mathbb{G} =< g >$ be a cyclic group of prime order q, and let $R_q \subset \mathbb{G} \times \mathbb{Z}_q$ be a relation defined as $R_q := \{(Y, y) | Y = g^y\}$, where $\mathbb{Z}_q$ is the set of integers modulo q.

Next, we briefly recall the Schnorr signature scheme $\Sigma_{\mathrm{S}ch} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$. The key generation algorithm samples $x \leftarrow \mathbb{Z}_q$ uniformly at random and returns $X := g^x \in \mathbb{G}$ as the public key and x as the secret key. On an input message $m \in \{0,1\}^*$, the signing algorithm computes $r] = \mathcal{H}(X||g^k||m) \in \mathbb{Z}_q$ and $s := k + rx \in \mathbb{Z}_q$, for $k \leftarrow \mathbb{Z}_q$ chosen uniformly at random, and it outputs a signature $\sigma := (r, s)$. Finally, on an input message $m \in \{0,1\}^*$ and signature $(r, s) \in \mathbb{Z}_q \times \mathbb{Z}_q$, the verification algorithm verifies that $r = \mathcal{H}(X||g^s \cdot X^{-r}||m)$.

In this paper, Schnorr signatures are considered to satisfy $\mathsf{SUF\text{-}CMA}$. At a high level, $\mathsf{SUF\text{-}CMA}$ guarantees that a PPT adversary, given the public key pk and access to a signature oracle, cannot produce a new valid signature on any message m.

B Supplemental Material for Two-Party Adaptor Signatures

B.1 Correctness of Two-Party Adaptor Signatures

The adapter signature scheme $\mathsf{AS}_{R,\Sigma}$ satisfies the following correctness:

Definition 9 (Pre-signature correctness) *For any message $M \in \{0,1\}^*$ and $(Y, y) \in R$, the adapter signature scheme $\mathsf{AS}_{R,\Sigma}$ satisfies pre-signature correctness if the following holds:*

$$\Pr\left[\begin{array}{l|l} \mathsf{PreVrfy}(Y, \mathsf{pk}, \hat{\sigma}, M) = 1; & (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(1^\lambda); \\ \mathsf{Vrfy}(\mathsf{pk}, M, \sigma) = 1; & \hat{\sigma} \leftarrow \mathsf{PreSign}((\mathsf{pk}, \mathsf{sk}), Y, M); \\ (Y, y') \in R & \sigma := \mathsf{Adapt}((Y, y), \mathsf{pk}, \hat{\sigma}, M); \\ & y' := \mathsf{Ext}(Y, \hat{\sigma}, \sigma) \end{array}\right] = 1.$$

B.2 Security of Two-Party Adaptor Signatures

Here, we introduce the security of adapter signatures according to the definition by Aumayr et al. [1], which entails three properties. Below, $\mathsf{aEUF\text{-}CMA}$(existential unforgeability under chosen-message attack for adapter signatures) is defined in terms of the $\mathsf{EUF\text{-}CMA}$ security of a general digital signature, by considering a scenario in which an additional pre-signature is provided for a randomly chosen public statement $Y \in L_R$. This first property of existential unforgeability aims to ensure the unforgeability of signatures even when the adversary has a pre-signature for a specific message M.

$\mathsf{aEUF\text{-}CMA}$ security protects the signer. It is similar to $\mathsf{EUF\text{-}CMA}$ for digital signatures but additionally requires that production of a forgery σ for some message M is hard even given a pre-signature on M with respect to a random statement $Y \in L_R$. Note that it is essential to allow the adversary to learn a pre-signature on M because, for practical applications, signature unforgeability needs to hold even when the adversary learns a pre-signature for M without knowing a witness for Y.

Definition 10 (Existential unforgeability) *For any probabilistic polynomial-time (PPT) algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, consider the experiment $\mathsf{aSigForge}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda)$ in Table 12. If there exists a negligible function such that $\Pr[\mathsf{aSigForge}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$, then the adapter signature scheme $\mathsf{AS}_{R,\Sigma}$ is $\mathsf{aEUF\text{-}CMA}$ secure.*

Here, $\mathsf{aEUF\text{-}CMA}$ represents an for adaptively chosen-message attack under a chosen-message attack (CCA) security, and $\Pr[\mathsf{aSigForge}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda) = 1]$ represents the probability that the adversary $\mathcal{A}$ succeeds in the given experiment for the adapter signature scheme $\mathsf{AS}_{R,\Sigma}$ with security parameter λ. The above inequality means that if this probability is non-negligible, then the scheme is not $\mathsf{aEUF\text{-}CMA}$-secure.

Table 12. Experiment of $\mathsf{aSigForge}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda)$

$\mathsf{aSigForge}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda)$	$\mathcal{O}_S(M)$	$\mathcal{O}_{pS}(M,Y)$
$1: Q := \emptyset,\ (\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}(1^\lambda)$	$1: \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, M)$	$1: \hat{\sigma} \leftarrow \mathsf{PreSign}(\mathsf{sk}, Y, M)$
$2: (Y, y) \leftarrow \mathsf{GenR}(1^\lambda)$	$2: Q := Q \cup \{M\}$	$2: Q := Q \cup \{M\}$
$3: (M, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\mathsf{pk}, Y)$	$3:$ **return** σ	$3:$ **return** $\hat{\sigma}$
$4: \hat{\sigma} \leftarrow \mathsf{PreSign}(\mathsf{sk}, Y, M)$		
$5: \sigma \leftarrow \mathcal{A}_2^{\mathcal{O}_S(\cdot),\mathcal{O}_{pS}(\cdot,\cdot)}(\hat{\sigma}, \mathsf{st})$		
$6:$ **return** $(m \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}, \sigma, M))$		

The second property, called pre-signature adaptability, protects the verifier. It guarantees that any valid pre-signature w.r.t. Y (possibly produced by a malicious signer) can be completed as a valid signature by using a witness y with $(Y, y) \in R$. Note that this property is stronger than the pre-signature correctness property, because we require that even pre-signatures that were not produced by $\mathsf{PreSign}$ but are valid can still be completed as into valid signatures.

Definition 11 (Pre-signature adaptability) *For any message $M \in \{0,1\}^*$, any statement/witness pair $(Y, y) \in R$, any public key pk and any pre-signature $\hat{\sigma} \in \{0,1\}^*$ with $\mathsf{PreVrfy}(\mathsf{pk}, M, Y; \hat{\sigma}) = 1$, an adaptor signature scheme $\mathsf{AS}_{R,\Sigma}$ satisfies pre-signature adaptability if we have $\mathsf{Vrfy}(M, \mathsf{pk}; \mathsf{Adapt}(\hat{\sigma}, y)) = 1$.*

The last property of interest is witness extractability, which protects the signer. Informally, it guarantees that a valid signature/pre-signature pair $(\sigma, \hat{\sigma})$ for a message/statement pair (m, Y) can be used to extract a witness y for Y. Hence, a malicious verifier cannot use a pre-signature $\hat{\sigma}$ to produce a valid signature σ without revealing a witness for Y.

Definition 12 (Witness extractability) *An adaptor signature scheme $\mathsf{AS}_{R,\Sigma}$ is witness extractable if, for every PPT adversary $A = (A_1, A_2)$, there exists a negligible function $\mathcal{V}$ such that the following holds: $Pr[aWitExt_{A,\mathsf{AS}_{R,\Sigma}}(n) = 1] \leq \mathcal{V}(\lambda)$, where the experiment $aWitExt_{A,\mathsf{AS}_{R,\Sigma}}$ is defined as in Table 13.*

Table 13. Experiment $\mathsf{aWitExt}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda)$

$\mathsf{aWitExt}_{\mathcal{A},\mathsf{AS}_{R,\Sigma}}(\lambda)$
$1: Q := \emptyset,\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(1^\lambda)$
$2: (M, Y, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\mathsf{pk})$
$3: \hat{\sigma} \leftarrow \mathsf{PreSign}(\mathsf{sk}, Y, M)$
$4: \sigma \leftarrow \mathcal{A}_2^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot,\cdot)}(\hat{\sigma}, \mathsf{st})$
$5: \mathbf{return}\ (Y, \mathsf{Ext}(\mathsf{pk}, \sigma, \hat{\sigma}), T \notin R \wedge M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}, \sigma, M))$

$\mathcal{O}_S(M)$	$\mathcal{O}_{pS}(M, Y)$
$1: \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, M)$	$1: \hat{\sigma} \leftarrow \mathsf{PreSign}(\mathsf{sk}, Y, M)$
$2: Q := Q \cup \{M\}$	$2: Q := Q \cup \{M\}$
$3: \mathbf{return}\ \sigma$	$3: \mathbf{return}\ \hat{\sigma}$

This security definition above does not explicitly consider the existential unforgeability of pre-signatures (*pre-signature existential unforgeability*). However, by considering an experiment that omits steps 4 and 5 in Definition 10 and directly returns the pre-signature $\hat{\sigma}$, we can effectively address this aspect. Given the similarity between this modified experiment and Definition 10, we omit the detailed description here.

Finally, given the above definitions, we have the following definition of an adapter signature scheme's security.

Definition 13 *Suppose that the Schnorr signature scheme Σ_{Sch} is $\mathsf{SUF\text{-}CMA}$ and R_g is a hard relation. $\mathsf{N\text{-}AS}_{R_g,\Sigma_{\mathrm{Sch}}}$ in Fig. 3 is a secure three-party adapter* *signature scheme in the ROM if N-party pre-signature correctness, three-party existential unforgeability, N-party pre-signature adaptability, and N-party witness extractability are satisfied.*

C Security

C.1 Pre-signature adaptability for three-party

Lemma 5 (Pre-signature adaptability for three-party) *The Schnorr-based adaptor signature scheme* $\mathsf{3\text{-}AS}_{R_g,\Sigma_{\mathrm{Sch}}}$ *satisfies pre-signature adaptability for three-party.*

Proof. It is provable as well as the pre-signature adaptability of the 2-party. Two case divisions depending on which adaptability among the three parties is considered (i) when U_2 (main-signer) is adversary (ii) when U_3 (sub-signer) is adversary.

(i) If U_2 is an adversary, let $y_1, y_2 \in \mathbb{Z}_q$, $M \in \{0,1\}^*$, $\mathsf{pk}_2, \mathsf{pk}_3 \in \mathbb{G}$, and $\hat{\sigma}_2 = (r_2, \tilde{s}_2, s_3') \in \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q$. Define $s_1 := \tilde{s}_2 + y_1$. Assume $\mathsf{PreVrfy}_{U_1}(Y_1, (\mathsf{pk}_2, \mathsf{pk}_3), (\hat{\sigma}_2, \hat{\sigma}_3), M) = 1$, then

$$\begin{aligned} r_2 &= \mathcal{H}(\mathsf{pk}_2 || g^{\tilde{s}_2} \cdot \mathsf{pk}_2^{-r_2} \cdot Y_1 || M) \\ &= \mathcal{H}(\mathsf{pk}_2 || g^{\tilde{s}_2} + y_1 \cdot \mathsf{pk}_2^{-r_2} || M) \\ &= \mathcal{H}(\mathsf{pk}_2 || g^{s_1} \cdot \mathsf{pk}_2^{-r_2} || M), \end{aligned}$$

which implies $\mathsf{Vrfy}(\mathsf{pk}_1, \sigma_1 = (r_2, s_1), M) = 1 (\because r_2 = \mathcal{H}(\mathsf{pk}_3 || g^{s_1} \cdot \mathsf{pk}_3^{-r_2} || M)$.

(ii) If U_3 is an adversary, let $y_1, y_2 \in \mathbb{Z}_q$, $M \in \{0,1\}^*$, $\mathsf{pk}_2, \mathsf{pk}_3 \in \mathbb{G}$, $\hat{\sigma}_3 = (r_3, \tilde{s}_3) \in \mathbb{Z}_1 \times \mathbb{Z}_q$. Define $s_3' := \tilde{s}_3 + y_2$. Assume $\mathsf{PreVrfy}_{U_2}(Y_2, \mathsf{pk}_3, (r_3, \tilde{s}_3), M) = 1$, then

$$\begin{aligned} r_3 &= \mathcal{H}(\mathsf{pk}_3 || g^{\tilde{s}_3} \mathsf{pk}_3^{-r_3} Y_2 || M) \\ &= \mathcal{H}(\mathsf{pk}_3 || g^{\tilde{s}_3 + y_2} \mathsf{pk}_3^{-r_3} || M) \\ &= \mathcal{H}(\mathsf{pk}_3 || g^{s_3'} \mathsf{pk}_3^{-r_3} || M), \end{aligned}$$

which implies $\mathsf{Vrfy}(\mathsf{pk}_3, \hat{\sigma}_3 = (r_3, \hat{\sigma}_3), \hat{\sigma}_2 = (r_2, s_2, s_3') || M) = 1$ since $r_3 = \mathcal{H}(\mathsf{pk}_3 || g^{s_3'} \mathsf{pk}_3^{-r_3} || M)$ holds.

C.2 Pre-signature correctness for three-party

Lemma 6 (Pre-signature correctness for three-party) *The Schnorr-based adaptor signature scheme* $\mathsf{3\text{-}AS}_{R_g,\Sigma_{\mathrm{Sch}}}$ *satisfies pre-signature correctness for three-party.*

Proof. We show that the six equations of definition 9 are satisfied under the conditions of the definition.

Correctness of $\mathsf{PreVrfy}_{U_2}(Y_2, \mathsf{pk}_3, \hat{\sigma}_3, M)$=1. Given $\hat{\sigma}_3 = (r_3, s_3)$ and $s_3 = k + r_3 x_3$,

$$g^{s_3} \cdot X_3^{-r_3} \cdot Y_2 = g^{k+r_3x_3} \cdot (g^{x_3})^{-r_3} Y_2 = g^k Y_2.$$

Therefore, $\mathsf{PreVrfy}_{U_2}(Y_2, \mathsf{pk}_3, \hat{\sigma}_3, M)$ computes

$$r_3 = \mathcal{H}(X_3||g^{s_3} \cdot g^k \cdot Y_2||M) = \mathcal{H}(X_3||g^{s_3} \cdot X_3^{-r_3} \cdot Y_2||M).$$

Correctness of $\mathsf{PreVrfy}_{U_3}(Y_1, \mathsf{pk}_2, \hat{\sigma}_2, M) = 1$. Given $\hat{\sigma}_2 = (r_2, s_2, s_3')$ and $s_2 = k' + r_2 x_2$,

$$g^{s_2} \cdot X_2^{-r_2} \cdot Y_1 = g^{k'+r_2x_2} \cdot (g^{x_2})^{-r_2} \cdot Y_1 = g^{k'} Y_1.$$

Therefore, $\mathsf{PreVrfy}_{U_3}(Y_1, \mathsf{pk}_2, \hat{\sigma}_2, M)$ computes

$$r_2 = \mathcal{H}(X_2||g^{s_2} \cdot g^{k'} \cdot Y_1||M) = \mathcal{H}(X_2||g^{s_2} \cdot X_2^{-r_2} \cdot Y_1||M).$$

Correctness of $(Y_2, y_2') \in R$. For $s_3' = s_3 + y_2$, U_3 gets $y_2' = s_3' - s_3 = (s_3 + y_2) - s_3 = y_2$.

$$\therefore (Y_1, y_1') \in R.$$

Correctness of $\mathsf{PreVrfy}_{U_1}(Y_1, (\mathsf{pk}_2, \mathsf{pk}_3), (\hat{\sigma}_2, \hat{\sigma}_3), M) = 1$. Given $\hat{\sigma}_2 = (r_2, s_2, s_3')$ and $\hat{\sigma}_3 = (r_3, s_3)$, return 1 if $r_3 = \mathcal{H}(X_3||g^{s_3} \cdot X_3^{-r_3} \cdot Y_2||M)$ and $r_2 = \mathcal{H}(X_2||g^{s_2} \cdot X_2^{-r_2} \cdot Y_1||M)$ hold. The above can be demonstrated similarly to the correctness of $\mathsf{PreVrfy}_{U_2}$ and $\mathsf{PreVrfy}_{U_3}$.

Correctness of $\mathsf{Vrfy}(\mathsf{pk}_2, M, \sigma_1)$=1. Given $\sigma_1 = (r_2, s_1)$,

$$\begin{aligned} g^{s_1} \cdot X_2^{-r_2} &= g^{s_2+y_1} \cdot (g^{x_2})^{-r_2} \ (\because s_1 = s_2 + y_1) \\ &= g^{k'+r_2x_2+y_1} \cdot (g^{x_2})^{-r_2} \ (\because s_2 = k' + r_2 x_2) \\ &= g^{k'+y_1} \\ &= g^{k'} Y_1 \ (\because Y_1 = g^{y_1}). \end{aligned}$$

Therefore,

$$r_2 = \mathcal{H}(X_2||g^{k'} Y_1||M) = \mathcal{H}(X_2||g^{s_1} X_2^{-r_2}||M).$$

Correctness of $(Y_1, y_1') \in R$. For $s_1 = s_2 + y_1$, U_2 gets $y_1' = s_1 - s_2 = (s_2 + y_1) - s_2 = y_1$.

$$\therefore (Y_1, y_1') \in R.$$

D Security Definitions of Games in Lemma 3.

In this section, we describe the formal definition of each game $\mathbf{G_1}$ through $\mathbf{G_6}$ in Case (ii) of Lemma 3.

Table 14. Formal definition of game $\mathbf{G_1}$

$\mathbf{G}_1$

$Q := \emptyset$
$H := [\perp]$
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M^*)$
$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$\sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$
if $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*$, abort.
return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_S^{\mathcal{A}_1}(M)$

$\sigma_1 \leftarrow \mathsf{Sign}((\mathsf{pk}_1, \mathsf{sk}_1), M)$
$Q := Q \cup \{M\}$
return σ_1

$\mathcal{O}_{pS}(M, Y_2)$

$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M)$
$Q := Q \cup \{M\}$
return σ_3

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M)$
$Q := Q \cup \{M\}$
return σ_2

$\mathcal{H}(x)$

if $\mathcal{H}[x] = \perp$
$H[x] \leftarrow \mathbb{Z}_q$
return $\mathcal{H}[x]$

Table 15. The formal definition of game $\mathbf{G_2}$

$\mathbf{G}_2$

$Q := \emptyset$
$H := [\perp]$
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M^*)$
$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$\sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$
if $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*$, abort.
return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_S^{\mathcal{A}_1}(M)$

$\sigma_1 \leftarrow \mathsf{Sign}((\mathsf{pk}_1, \mathsf{sk}_1), M)$
$Q := Q \cup \{M\}$
return σ_1

$\mathcal{O}_{pS}(M, Y_2)$

$H' := H$
$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M)$
$(r_3, s_3) := \sigma_3$
$K := g^s \mathsf{pk}_3^{-r_3}$
if $H'[\mathsf{pk}_3 || K || M] \neq \perp$
$\quad \wedge H'[\mathsf{pk}_3 || K \cdot Y_2 || M]$
$\quad$ abort
$Q := Q \cup \{M\}$
return σ_3

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M)$
$Q := Q \cup \{M\}$
return σ_2

$\mathcal{H}(x)$

if $\mathcal{H}[x] = \perp$
$H[x] \leftarrow \mathbb{Z}_q$
return $\mathcal{H}[x]$

Table 16. Formal definition of game $\mathbf{G_3}$

$\mathbf{G}_3$

$Q := \emptyset,\ S := \emptyset$

$H := [\bot],$

$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$

$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$

$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$

$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M^*)$

$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2),$
$\quad Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$

$\sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$

if $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*,$

$\vee\ y_1^* \leftarrow \mathsf{Ext}(Y_1^*, \mathsf{PreAdapt}_{U_2}((Y_2^*, y_2^*), Y_1^*,$
$\quad \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3^*, M), \sigma_2^*$

then abort

return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_{pS}(M, Y_2)$

$H' := H$

$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M)$

$(r_3, s_3) := \sigma_3$

$K := g^s \mathsf{pk}_3^{-r_3}$

if $H'[\mathsf{pk}_3 || K || M] \neq \bot$

$\quad \wedge H'[\mathsf{pk}_3 || K \cdot Y_2 || M]$

abort

$Q := Q \cup \{M\}$

return σ_3

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$H' := H$

$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3,$
$\quad (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M)$

$(r_2, s_2, s_3') := \sigma_2$

$K_2 := g^{s_2} \cdot \mathsf{pk}_2^{-r_2}$

$y_2' = s_3' - s_3\ (\because (r_3, s_3) := \hat{\sigma}_3)$

if $H'[\mathsf{pk}_2 || K_2 || M] \neq \bot$

$\quad \wedge\ H'[\mathsf{pk}_2\ \ K_2 \cdot Y_1 || M] \neq \bot$

$\quad \wedge\ s_3' \in S$

$\quad \wedge\ (Y_2^*, y_2') \in R^*$

abort

$Q := Q \cup \{M\}$

$S := S \cup \{s_3'\}$

return σ_2

$\mathcal{O}_S^{\mathcal{A}_1}(M)$

$\sigma_1 \leftarrow \mathsf{Sign}((\mathsf{pk}_1, \mathsf{sk}_1), M)$

$Q := Q \cup \{M\}$

return σ_1

$\mathcal{H}(x)$

if $\mathcal{H}[x] = \bot$

$H[x] \leftarrow \mathbb{Z}_q$

return $\mathcal{H}[x]$

Table 17. Formal definition of game $\mathbf{G_4}$

$\mathbf{G}_4$

$Q := \emptyset,\ S := \emptyset$
$H := [\perp],$
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M^*)$
$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2),$
$\quad Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$\sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$
$\text{if } \mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*,$
$\lor\ y_1^* \leftarrow \mathsf{Ext}(Y_1^*, \mathsf{PreAdapt}_{U_2}((Y_2^*, y_2^*), Y_1^*,$
$\quad \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3^*, M), \sigma_2^*$
$\quad \text{then abort}$
$\text{return } (M \notin Q \land \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$H' := H$
$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2), Y_1, \mathsf{pk}_3,$
$\quad (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M)$
$(r_2, s_2, s_3') := \sigma_2$
$K_2 := g^{s_2} \cdot \mathsf{pk}_2^{-r_2}$
$y_2' = s_3' - s_3\ (\because (r_3, s_3) := \hat{\sigma}_3)$
$\text{if } H'[\mathsf{pk}_2 || K_2 || M] \neq \perp$
$\quad \land\ H'[\mathsf{pk}_2\ \ K_2 \cdot Y_1 || M] \neq \perp$
$\quad \land\ s_3' \in S$
$\quad \land\ (Y_2^*, y_2') \in R^*$
$\quad \text{abort}$
$Q := Q \cup \{M\}$
$S := S \cup \{s_3'\}$
$\text{return } \sigma_2$

$\mathcal{O}_S^{\mathcal{A}_1}(M)$

$\sigma_1 \leftarrow \mathsf{Sign}((\mathsf{pk}_1, \mathsf{sk}_1), M)$
$Q := Q \cup \{M\}$
$\text{return } \sigma_1$

$\mathcal{O}_{pS}(M, Y_2)$

$H' := H$
$\sigma_3 \leftarrow \mathsf{Sign}((\mathsf{pk}_3, \mathsf{sk}_3), M)$
$(r_3, s_3) := \sigma_3$
$K := g^s \mathsf{pk}_3^{-r_3}$
$\text{if } H'[\mathsf{pk}_3 || K || M] \neq \perp$
$\quad \land H'[\mathsf{pk}_3 || K \cdot Y_2 || M]$
$\quad \text{abort}$
$x := \mathsf{pk}_3 || K_3 || M$
$H'[\mathsf{pk}_3 || K_3 \cdot Y_2 || M] := H[x]$
$H[x] \leftarrow \mathbb{Z}_q$
$Q := Q \cup \{M\}$
$\text{return } \sigma_3$

$\mathcal{H}(x)$

$\text{if } \mathcal{H}[x] = \perp$
$H[x] \leftarrow \mathbb{Z}_q$
$\text{return } \mathcal{H}[x]$

Table 18. Formal definition of game $\mathbf{G_5}$

$\mathbf{G_5}$

$Q := \emptyset$, $S := \emptyset$
$H := [\bot]$,
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$\sigma_3 \leftarrow \mathsf{PreSign}((\mathsf{pk}_3, \mathsf{sk}_3), Y_2, M^*)$
$\sigma_2 \leftarrow \mathsf{PreAdapt}_{U_2}((Y_2, y_2),$
$\quad Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$\sigma_1 \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$
if $\mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*$,
$\vee\ y_1^* \leftarrow \mathsf{Ext}(Y_1^*, \mathsf{PreAdapt}_{U_2}((Y_2^*, y_2^*), Y_1^*,$
$\quad \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3^*, M), \sigma_2^*$
$\quad$ then abort
return $(M \notin Q \wedge \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$H' := H$
$\sigma_2 \leftarrow \mathsf{Sign}((\mathsf{pk}_2, \mathsf{sk}_2), M)$
$(r_2, s_2) := \sigma_2$
$s_3' \leftarrow \mathbb{Z}_q$
if $s_3' \in S$, abort
$K_2 := g^{s_2} \cdot \mathsf{pk}_2^{-r_2}$
$y_2' = s_3' - s_3$ $(\because (r_3, s_3) := \hat{\sigma}_3)$
if $H'[\mathsf{pk}_2 || K_2 || M] \neq \bot$
$\quad \wedge\ H'[\mathsf{pk}_2\ \ K_2 \cdot Y_1 || M] \neq \bot$
$\quad \wedge\ s_3' \in S$
$\quad \wedge\ (Y_2^*, y_2') \in R^*$
$\quad$ abort
$x := \mathsf{pk}_2 || K_2 || M$
$H[\mathsf{pk2} || K_2 \cdot Y_1 || M] := H[x]$
$H[x] \leftarrow \mathbb{Z}_q$
$(r_2, s_2, s_3') := \hat{\sigma}_2$
$Q := Q \cup \{M\}$
$S := S \cup \{s_3'\}$
return σ_2

$\mathcal{O}_S^{\mathcal{A}_1}(M)$

$\sigma_1 \leftarrow \mathsf{Sign}((\mathsf{pk}_1, \mathsf{sk}_1), M)$
$Q := Q \cup \{M\}$
return σ_1

$\mathcal{O}_{pS}(M, Y_2)$

$H' := H$
$\sigma_3 \leftarrow \mathsf{Sign}((\mathsf{pk}_3, \mathsf{sk}_3), M)$
$(r_3, s_3) := \sigma_3$
$K := g^s \mathsf{pk}_3^{-r_3}$
if $H'[\mathsf{pk}_3 || K || M] \neq \bot$
$\quad \wedge H'[\mathsf{pk}_3 || K \cdot Y_2 || M]$
$\quad$ abort
$x := \mathsf{pk}_3 || K_3 || M$
$H'[\mathsf{pk}_3 || K_3 \cdot Y_2 || M] := H[x]$
$H[x] \leftarrow \mathbb{Z}_q$
$Q := Q \cup \{M\}$
return $\hat{\sigma}_3$

$\mathcal{H}(x)$

if $\mathcal{H}[x] = \bot$
$H[x] \leftarrow \mathbb{Z}_q$
return $\mathcal{H}[x]$

Table 19. Formal definition of game $\mathbf{G_6}$

$\mathbf{G}_6$

$Q := \emptyset,\ S := \emptyset$
$H := [\bot],$
$(\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3) \leftarrow \mathsf{Gen}(1^\lambda)$
$(Y_1, y_1)(Y_2, y_2) \leftarrow \mathsf{GenR}(1^\lambda)$
$M^* \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\mathsf{pk}_2, \mathsf{pk}_3)$
$\sigma_2', \sigma_3' \leftarrow \mathsf{Sign}((\mathsf{pk}_2, \mathsf{sk}_2)(\mathsf{pk}_3, \mathsf{sk}_3), M^*)$
$(r_2', s_2') := \sigma_2', (r_3', s_3') := \sigma_3'$
$\sigma_2 := \mathsf{Adapt}(\sigma_2', -y_1)$
$\sigma_3 := \mathsf{Adapt}(\sigma_3', -y_2)$
$Y_1, \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \sigma_3, M^*)$
$\sigma_1' \leftarrow \mathcal{A}_1^{\mathcal{O}_S(\cdot), \mathcal{O}_{pS}(\cdot), \mathcal{O}_{pA}(\cdot)}(\sigma_2^*, \sigma_3^*, Y_1, Y_2)$
$\text{if } \mathsf{Adapt}((Y_1, y_1), \mathsf{pk}_2, \sigma_2, M) = \sigma_1^*,$
$\lor\ y_1^* \leftarrow \mathsf{Ext}(Y_1^*, \mathsf{PreAdapt}_{U_2}((Y_2^*, y_2^*), Y_1^*,$
$\quad \mathsf{pk}_3, (\mathsf{sk}_2, \mathsf{pk}_2), \hat{\sigma}_3^*, M), \sigma_2^*$
$\quad \text{then abort}$
$\text{return } (M \notin Q \land \mathsf{Vrfy}(\mathsf{pk}_3, \sigma_2, M^*))$

$\mathcal{O}_{pA}(M, (Y_2, Y_2), \sigma_3)$

$H' := H$
$\sigma_2 \leftarrow \mathsf{Sign}((\mathsf{pk}_2, \mathsf{sk}_2), M)$
$(r_2, s_2) := \sigma_2$
$s_3' \leftarrow \mathbb{Z}_q$
$\text{if } s_3' \in S, \text{ abort}$
$K_2 := g^{s_2} \cdot \mathsf{pk}_2^{-r_2}$
$y_2' = s_3' - s_3\ (\because (r_3, s_3) := \hat{\sigma}_3)$
$\text{if } H'[\mathsf{pk}_2 || K_2 || M] \neq \bot$
$\quad \land\ H'[\mathsf{pk}_2\ \ K_2 \cdot Y_1 || M] \neq \bot$
$\quad \land\ s_3' \in S$
$\quad \land\ (Y_2^*, y_2') \in R^*$
$\quad \text{abort}$
$x := \mathsf{pk}_2 || K_2 || M$
$H[\mathsf{pk2} || K_2 \cdot Y_1 || M] := H[x]$
$H[x] \leftarrow \mathbb{Z}_q$
$(r_2, s_2, s_3') := \hat{\sigma}_2$
$Q := Q \cup \{M\}$
$S := S \cup \{s_3'\}$
$\text{return } \sigma_2$

$\mathcal{O}_S^{\mathcal{A}_1}(M)$

$\sigma_1 \leftarrow \mathsf{Sign}((\mathsf{pk}_1, \mathsf{sk}_1), M)$
$Q := Q \cup \{M\}$
$\text{return } \sigma_1$

$\mathcal{O}_{pS}(M, Y_2)$

$H' := H$
$\sigma_3 \leftarrow \mathsf{Sign}((\mathsf{pk}_3, \mathsf{sk}_3), M)$
$(r_3, s_3) := \sigma_3$
$K := g^s \mathsf{pk}_3^{-r_3}$
$\text{if } H'[\mathsf{pk}_3 || K || M] \neq \bot$
$\quad \land H'[\mathsf{pk}_3 || K \cdot Y_2 || M]$
$\quad \text{abort}$
$x := \mathsf{pk}_3 || K_3 || M$
$H'[\mathsf{pk}_3 || K_3 \cdot Y_2 || M] := H[x]$
$H[x] \leftarrow \mathbb{Z}_q$
$Q := Q \cup \{M\}$
$\text{return } \hat{\sigma}_3$

$\mathcal{H}(x)$

$\text{if } \mathcal{H}[x] = \bot$
$H[x] \leftarrow \mathbb{Z}_q$
$\text{return } \mathcal{H}[x]$