Received June 2, 2021, accepted June 27, 2021, date of publication July 1, 2021, date of current version July 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3093925

Forward-Secure Multi-User Aggregate Signatures Based on zk-SNARKs

JEONGHYUK LEE[1], JIHYE KIM[2], (Member, IEEE), AND HYUNOK OH[1], (Member, IEEE)
[1]Department of Information Systems, Hanyang University, Seoul 04763, South Korea
[2]Department of Electrical Engineering, Kookmin University, Seoul 02707, South Korea

Corresponding authors: Jihye Kim (jihyek@kookmin.ac.kr) and Hyunok Oh (hoh@hanyang.ac.kr)

This work was supported in part by the Institute of Information Communications Technology Planning Evaluation (IITP) grant funded by the Korean government (MSIT) (No.2021-0-00518, High performance blockchain privacy preserving techniques based on commitment, encryption, and zero-knowledge proofs, 50%, No.2021-0-00532, Blockchain scalability solutions supporting high performance/capacity transactions, 30%, No.2021-0-00727, A Study on Cryptographic Primitives for SNARK, 10%, No.2021-0-00528, Development of Hardware-centric Trusted Computing Base and Standard Protocol for Distributed Secure Data Box, 5% and No.2021-0-00590, Decentralized High Performance Consensus for Large-Scale Blockchains, 5%).

ABSTRACT As a solution to mitigate the key exposure problems in the digital signature, the forward security has been proposed. The forward security guarantees the integrity of the messages generated in the past despite leaks of a current time period secret key by evolving a secret key on each time period. In this paper, we propose a new forward secure aggregate signature scheme utilizing recursive zk-SNARKs (zero knowledge Succinct Non-interactive ARguments of Knowledge). Our proposal has constant complexities in key/signature sizes, signature generation, and verification time. The proposed forward secure signature scheme can aggregate signatures generated by multiple users as well as a single user. The security of the proposed scheme is formally proven under zero-knowledge assumption and random oracle model. The experiment results show that our signature scheme yields 12 s for signing time, 1 ms for verification time, 25 s for aggregation time, with the 1.6 KB secret key size and signature size independent of the number of time periods.

INDEX TERMS Aggregate signature, digital signature, forward security, recursive proof composition, zero-knowledge proof, zk-SNARK.

I. INTRODUCTION

A digital signature is used widely in many of fields as an authentication such as IoT, blockchain, etc. [1]–[3]. However, the digital signature has a key managing issue since if the secret key is exposed, a signature can be forged. The forward security which assigns a different signing key to each time period alleviates a problem induced by the key exposure. After the security notion is firstly proposed by Anderson [4], several forward secure signature schemes have been devised [5]–[11] for decades. However, these works have a limitation in that the maximum time period T should be fixed in setup for the constant public key size. It causes the necessity of remaking the signing key and the public key when the maximum time period T ends. To avoid the problem, the maximum time period T is set to a large value.

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

However, it results in the inefficiency of the signature scheme of which complexities are dependent on the maximum time period [5]–[7]. For instance, Abdalla's construction [6] has $O(T)$ time complexity in setup, signing, and the verification. Although recent optimization of Abdalla's construction [12] reduces signing cost to $O(1)$ with some setup time trade-off, the verification cost remains $O(T)$. While the verification time is constant in several works [7], [9], [13], still one of the metrics is dependent on the maximum time period in every approach.

In the different view of the signature, aggregation is a useful tool for alleviating a storage problem. Specifically, the aggregate signature is used in blockchain applications to reduce the space required for the signature storage, and it mitigates the burden of blockchain network caused by the immense size of the transactions [14]. Although there exist many aggregate signature schemes to merge the signatures [15]–[19], only a few researches support an aggregation

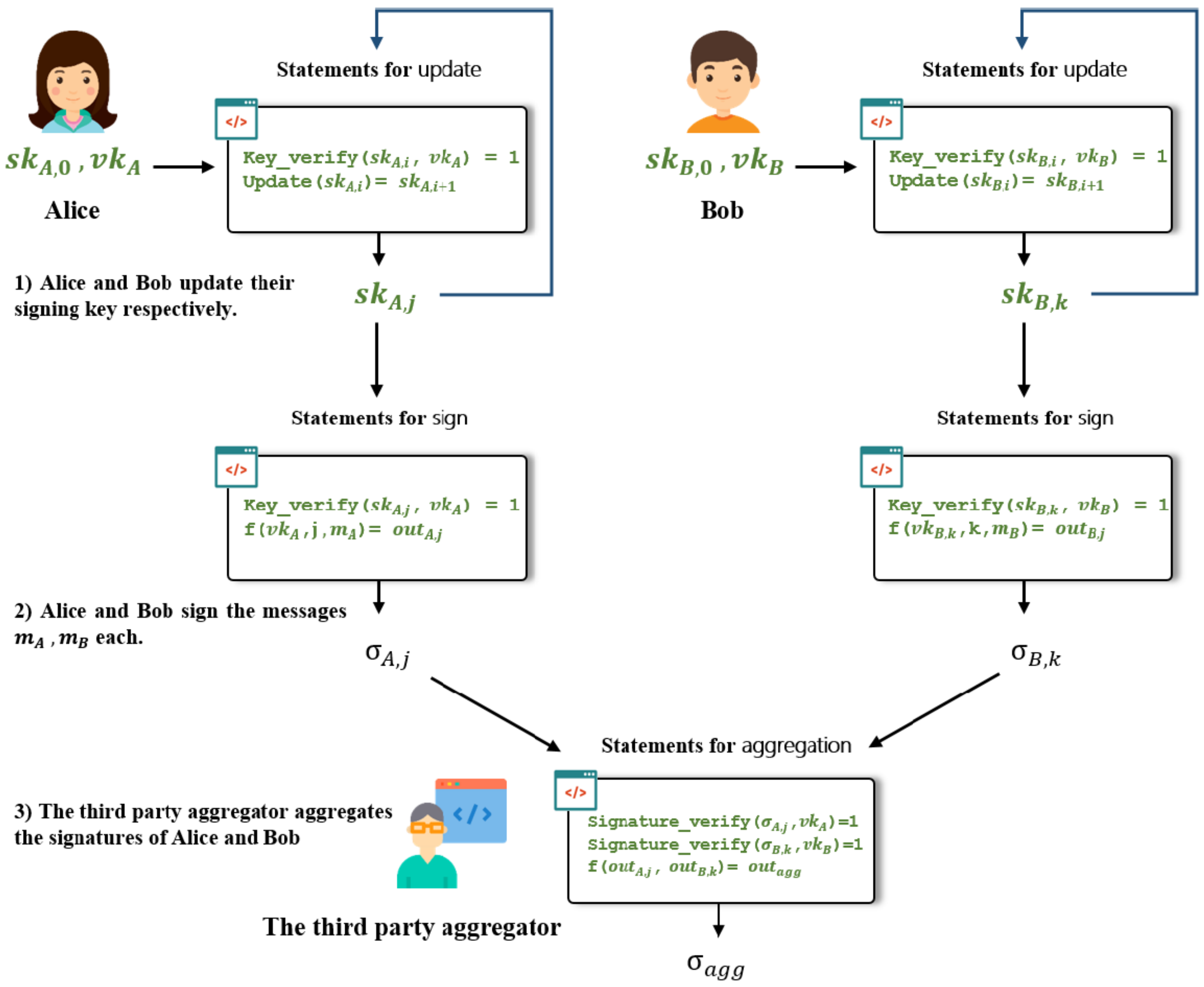
Statements for update
$sk_{A,0}$, vk_A
Alice
Key_verify($sk_{A,i}$, vk_A) = 1
Update($sk_{A,i}$)= $sk_{A,i+1}$
1) Alice and Bob update their signing key respectively.
$sk_{A,j}$
Statements for update
$sk_{B,0}$, vk_B
Bob
Key_verify($sk_{B,i}$, vk_B) = 1
Update($sk_{B,i}$)= $sk_{B,i+1}$
$sk_{B,k}$
Statements for sign
Key_verify($sk_{A,j}$, vk_A) = 1
f(vk_A,j,m_A)= $out_{A,j}$
Statements for sign
Key_verify($sk_{B,k}$, vk_B) = 1
f($vk_{B,k}$,k,m_B)= $out_{B,j}$
2) Alice and Bob sign the messages m_A , m_B each.
$\sigma_{A,j}$
$\sigma_{B,k}$
Statements for aggregation
3) The third party aggregator aggregates the signatures of Alice and Bob
Signature_verify($\sigma_{A,j}$,vk_A)=1
Signature_verify($\sigma_{B,k}$,vk_B)=1
f($out_{A,j}$, $out_{B,k}$)= out_{agg}
The third party aggregator
σ_{agg}

FIGURE 1. Basic structure of our proposal.

of forward secure signatures [20]–[24]. However, the aggregate signature schemes are able to either aggregate signatures generated from a single user [20]–[23] or multi-user signatures at which period is equivalent [20]–[23]. This requirement makes difficult to be deployed in a decentralized environment where the time periods are often not synchronized. In this paper, we propose a forward secure multi-user aggregate signature scheme where all the complexities are totally independent of the time period T. The aggregation supports different messages and different users flexibly applicable for the decentralized environment. In our construction, we use a simulation extractable zk-SNARK (zero-knowledge Succinct Non-interactive Argument of Knowledge) [25]–[28] as a building block of the signature scheme. The zk-SNARK enables proving arbitrary statements and the arbitrariness of the statements facilitates the removal of restrictions in existing signature schemes. That is, it is able to consider zk-SNARK proof as a signature if the proof proves the statements that suit the requirement of the signature. Naively, we can have an idea to construct a forward secure signature scheme by proving following statements.

- A public verification key and a secret signing key are well constructed.
- The secret signing key is connected with a message.
- The secret signing key is updated correctly.

Though all of the statements can be proven by simply including these statements in a zk-SNARK circuit, it is not enough for the forward secure signature since signing keys of all time periods are required as witnesses in the proof generation. Furthermore, it causes the inefficiency in that the circuit size increases proportional to the number of key updates. We resolve the issue by adopting PCD (Proof Carrying Data) [29] where a proof proves the verification result of the other proof to prove the update process without the previous signing key.

In Fig.1, we describe the flow of our forward secure aggregate signature construction. Sign, update, and aggregate algorithms are designed by subsuming zk-SNARK proof

TABLE 1. Performance and size comparison in forward secure signature schemes: T and l denote the maximum period and the message length.

	Ours	BM [5]	AR [6]	IR [7]	Boyen et al. [9]	KO17 [12]
Key generation time	$O(1)$	$O(lT)$	$O(lT)$	$O(lT)$	$O(\log T)$	$O(lT)$
Update time	$O(1)$	$O(l)$	$O(l)$	$O(lT)$	$O(1)$	$O(l)$
Signing time	$O(1)$	$O(T+l)$	$O(lT)$	$O(l)$	$O(\log T+l)$	$O(1)$
Verification time	$O(1)$	$O(T+l)$	$O(lT)$	$O(l)$	$O(1)$	$O(lT)$
Secret key size	$O(1)$	$O(l)$	$O(1)$	$O(1)$	$O(\log^2 T)$	$O(1)$
Verification key size	$O(1)$	$O(l)$	$O(1)$	$O(1)$	$O(\log T+l)$	$O(1)$
Signature size	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$

construction that proves required statements respectively. All the statements consist of verification of previous proof and additional computation. As described in 1) in Fig.1, when the initial signing key $sk_{A,0}$ and $sk_{B,0}$ are assumed to be composed of user secret value and the proof that proves a relation of user secret value and the verification key, the secret signing key can be updated recursively by proving statements for update. The statement stipulates that the verification result of the previous signing key is passed and the signing key of the next time period is generated correctly. By updating the signing key recursively, we can keep the circuit size constant regardless of how many times the signing key is updated. When the updated signing key $sk_{A,j}$ and the message m_A are given, the signature generation is conducted similar to the update. For instance, when Alice proves that the secret signing key for j period $sk_{A,j}$ is verified and the message m_A and the time period j is connected with the secret signing key, the proof can be a forward secure signature itself. In aggregation described in 3), the third party aggregator verifies $\sigma_{A,j}$ and $\sigma_{B,k}$ that are signatures of Alice and Bob in j,k time period respectively. The third party aggregator proves the verification results and the aggregation of two signatures. That is, if the verification of two signatures is converged into one zk-SNARK proof, it can be an aggregate signature itself. Since the aggregation needs only the public information required in the verification, it can be conducted publicly.

A. OUR CONTRIBUTIONS

1) GENERIC CONSTRUCTION OF A FORWARD SECURE SIGNATURE USING zk-SNARK

We propose a generic construction of the forward secure signature via zk-SNARKs. In our construction, any kind of simulation extractable zk-SNARK from the pre-processing SNARKs such as GM17 [25], and KLO20 [30] to universal structured reference string based SNARKs such as MBKM19 [31], GWC19 [32], and BBB+18 [33] can be utilized as a building block. Various zk-SNARK libraries including libsnark [34], and snarkjs [35] can be used in the signature construction freely.

2) $O(1)$ EFFICIENCY

We construct a forward secure signature of which complexities are independent of the time period. In fact, our scheme does not require any maximum time period in the scheme setup. In our forward secure signature, all of the metrics in setup, update, sign, and verify algorithms have $O(1)$ time and space complexities. Note that the verification key size, secret key size and the signature size are constant. Table 1 compares performance and space requirement of forward secure signature schemes [5]–[7], [9], [12]. While all metrics are constant in our signature scheme, the other schemes have at least one metric that is dependent on the maximum period T. Except Boyen *et al.* [9] and our scheme, at least one metric is $O(T)$ while the key size is not constant in [9].

3) MULTI-USER SIGNATURE AGGREGATION FOR ANY TIME PERIOD

We propose a generic aggregate construction that aggregates multi-user signatures removing all restrictions on the time period and the message. While the time period and the message should be fixed [24] or the time periods should be sequential in existing schemes [21], [23], our scheme can aggregate signatures of different messages generated by multi-user in unsequential time periods. In summary, our public aggregation technique not only allows the aggregation of multi-user signatures without any constraint of the time period, and the message but maintains $O(1)$ complexity in the signature size and the key size. Table 2 shows the aggregation possibility, the performance, and the size requirement in various forward secure aggregate signature schemes. While our scheme and MT07 can aggregate signatures in arbitrary periods, YNR12 and KO19 can aggregate signatures in consecutive periods. In addition, our scheme can aggregate signatures generated by multiple users while the other forward secure schemes can only aggregate signatures generated by a single user. YNR12 scheme can aggregate signatures by only a signer while the other schemes allow anyone to aggregate signatures.

In summary, we present a new forward secure signature methodology whose complexities are fully independent of the time period and its aggregation has high flexibility. Our new forward secure signature scheme can be utilized usefully in a decentralized environment where entities have their own time periods independently. However, we should bear zk-SNARK computation that is relatively heavier than other schemes to obtain a time period independent efficiency and the flexibility in the aggregation. Though the computation is independent

TABLE 2. Comparison of forward secure aggregate signature schemes where *n* indicates the number of aggregated signatures.

	Ours	MT07 [20]	YNR12 [23]	KO19 [21]
Aggregation period	Any	Any	Sequential	Sequential
Aggregation user	Multiple	Single	Single	Single
Public aggregation	Yes	Yes	No	Yes
Key generation time	$O(1)$	$O(T)$	$O(T)$	$O(lT)$
Update time	$O(1)$	$O(1)$	$O(1)$	$O(l)$
Signing time	$O(1)$	$O(1)$	$O(1)$	$O(lT)$
Aggregation time	$O(n)$	$O(n)$	$O(n)$	$O(n)$
Verification time	$O(n)$	$O(n)$	$O(n)$	$O(ln + lT)$
Verification key size	$O(1)$	$O(T)$	$O(T)$	$O(l)$
Signature size	$O(1)$	$O(1)$	$O(1)$	$O(1)$

of the time period and message length, it is reliant on zk-SNARK circuit size. Thus, we measure the actual performance of our signature scheme via the implementation.

We describe related works in section II. In section III, we explain preliminaries of our design and define the security notion. We demonstrate specific construction of our signature scheme in section IV. Section V presents an extension of our forward secure signature scheme to the forward secure multi-user aggregate signature. Section VI presents the security proofs of all constructions. Section VII analyzes the experiment results of our scheme. We draw a conclusion in section VIII.

II. RELATED WORK

The forward security notion is firstly introduced by Anderson [4] aiming to alleviate the damage from the key exposure problem. The forward security divides overall time periods into separate time period and utilizes a different secret key in each period. A subsequent secret key is derived from the one in the previous time period, and extracting the previous one from the current secret key is computationally hard. Because of the hardness of the extraction, a past signature cannot be fabricated even if the secret key in the current time period is exposed. Bellare and Miner [5] formalize the security notion and present the first practical forward secure signature scheme. After the formalization, many pieces of research try to improve the efficiency of forward secure signature since it is ideal that all the operations have $O(1)$ time complexity, $O(1)$ signature size and $O(1)$ key size respectively. Abdalla [6] reduces the secret key size from $O(l)$ to $O(1)$ where l is message length while maintaining all the time complexity of operations. While Kozlov *et al.* [8] design a forward secure signature scheme updating a key in $O(1)$ time complexity, it has a limitation in that its signing time complexity and verification time complexity are linear with overall time period T. Itkis and Reyzin [7] present a forward secure signature scheme whose signing and verification have the time complexity irrelevant to overall time period T while taking a trade-off in the update time. Malkin *et al.* [10] construct a generic forward secure signature scheme that has almost unbounded time period. Boyen *et al.* [9] propose the forward secure signature methodology whose signing key can be updated as an encrypted form. Kim and Oh [12] make AR [6] have the $O(1)$ signing time complexity with adding some computations in the setup time. Despite the results of many pieces of research, any research could not reach a methodology where all operations can be conducted in $O(1)$ time while maintaining $O(1)$ space. In a different view, several pieces of research resolve an issue that occurs when the forward security is applied to certificate-based cryptography. Lu and Li first apply the forward security notion into certificate-based cryptography, and they propose a forward secure certificate based signature scheme without a random oracle model [36]. They solve an issue that occurs when a certificated authority is malicious [37] and propose a certificate-based key-insulated signature that improves the security in certificate-based cryptography [38].

Meanwhile, several kinds of research introduce aggregation technique to existing forward secure signature schemes to reduce the space required to store multiple signatures [21], [22]. Ma and Tsudik [20] firstly construct a forward secure aggregate signature, however, the methodology has $O(T)$ verification key space complexity. Although Ma [22] evolves BM [5] and AR [6] into a forward secure aggregate signature scheme that has a constant size of verification key, the scheme is ascertained insecure by Kim and Oh [21]. Yavuz *et al.* [23] propose the aggregation technique that can be conducted by only a single addition. However, the technique has a drawback in that the verification key size is linear with T. Kim and Oh [21] devise the aggregation technique where the verification key size is irrelevant to overall time period T. However, these techniques [21], [23] only allow the aggregation of single-user signatures whose time periods are consecutive.

We use a simulation extractable zk-SNARK [25]–[28] as a building block of signature scheme where many zk-SNARK schemes work in pairing-based environment [25], [28], [39], [40]. Gennaro *et al.* [41] firstly propose a non-interactive argument system where a general function is supported. Groth [40] reduces the number of verification equations from three to one and the number of elements in a proof from eight to three. Groth and Maller [25] propose a simulation extractable zk-SNARK firstly maintaining the proof size as three. However, Groth and Maller construction supports SAP (Square Arithmetic Program) representation only that incurs double size of common reference string compared with QAP (Quadratic Arithmetic Program) representation. Several researches try to develop SE-SNARK that can be represented as QAP representation. Bowe and Gabizon [26] construct QAP based SE-SNARK that has five proof elements. Lipmaa [27] reduces the proof size required in QAP representation to four, and Kim *et al.* [28] have three proof elements in QAP representation and a single verification equation.

We use PCD (Proof Carrying Data) as a specific building block of our construction. PCD is a special case of zk-SNARK, and the proof proves the result of verification of other proofs recursively. Chiesa and Tromer define the notion firstly [42], and Bitansky *et al.* [29] devise the recursive proof composition where any zk-SNARK can be used as a building block. Ben-Sasson *et al.* [43] enhance the practicality of the notion via using 2-cycles of pairing friendly elliptic curves. In addition, Bowe *et al.* [44] propose the recursive proof composition that does not require a trusted setup using Bulletproof [33] and Sonic [31] as building blocks. Chiesa *et al.* [45] not only grant the transparency as Bowe's construction [44] but enable the recursive proof composition to work in post-quantum environments.

III. BACKGROUND

A. NOTATION

We write $y \leftarrow x$ for substitution x on y. We write $y \leftarrow S$ for sampling y from S if S is a set. We write $y \leftarrow A(x)$ for a probabilistic algorithm on input x returning output y. When a probabilistic algorithm $A(x)$ has a private input r, we denote $A(x; r)$. We state $f(\lambda)$ is *negligible* if $f(\lambda) \approx 0$. We denote a concatenation as $||$. Given a scheme Π, its all operations are denoted by $\Pi.\mathsf{name}$. Let $\mathcal{R}$ be a relation generator that given a security parameter λ in unary returns a polynomial time decidable relation $R \leftarrow \mathcal{R}(1^\lambda)$. We denote $\mathcal{R}_\lambda$ as the set of relations that $\mathcal{R}(1^\lambda)$ outputs. We call ϕ the instance and w the witness for $(\phi, w) \in R$. We denote all of $\mathcal{A}$'s inputs and outputs for an algorithm $\mathcal{A}$ by $trans_{\mathcal{A}}$.

B. CRYPTOGRAPHIC ASSUMPTION

We use a hash extractability assumption [46] stated as below.

Definition 1: A hash function H is extractable for a PPT adversary $\mathcal{A}$ when there exists an extractor ε such that, for large enough security parameter λ and auxiliary input $\mathsf{aux} \in \{0,1\}^{poly(\lambda)}$, the adversary $\mathcal{A}$ wins the game below with *negligible* probability.

We define $\mathbf{Adv}^{Hash-ext}_{H,\varepsilon,\mathcal{A}}(\lambda) = \Pr[\mathcal{G}^{Hash-ext}_{H,\varepsilon,\mathcal{A}}(\lambda)]$ where the game $\mathcal{G}^{Hash-ext}_{H,\varepsilon,\mathcal{A}}$ is defined in Algorithm 1.

The hash extraction game needs the function Check which allows the verifier to check the well-formedness of hashes received from the adversary [47].

C. SIMULATION EXTRACTABLE zk-SNARK

We adopt a simulation extractable zero-knowledge succinct non-interactive arguments of knowledge (SE-SNARK) [25] as a building block of our signature scheme. A formal definition of SE-SNARK is described as follows.

Algorithm 1 Hash Extraction Game $\mathcal{G}^{Hash-ext}_{H,\varepsilon,\mathcal{A}}$

```
$\mathcal{G}^{Hash-ext(\lambda)}_{H,\varepsilon,\mathcal{A}}$
    $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$
    $(\sigma; x_e) \leftarrow (\mathcal{A}||\mathcal{E})(\mathsf{pp}, \mathsf{aux})$
    $\mathcal{A}$ wins if $\exists x$ such that $H(\mathsf{pp}, x) = \sigma \wedge \sigma \neq H(\mathsf{pp}, x_e)$ and
    there is a PPT algorithm $\mathsf{Check}(pp, \sigma)$ that returns 1 if $\exists x$
    such that $H(\mathsf{pp}, x) = \sigma$ and 0 otherwise.
```

Definition 2: A zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARK) for $\mathcal{R}$ is a set of quadruple algorithms $\Pi = (\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify}, \mathsf{SimProve})$ as follows.

- Setup is a PPT setup algorithm that takes as input a relation $R \in \mathcal{R}_\lambda$ and returns a common reference string crs and a simulation trapdoor τ.
- Prove is a PPT algorithm that takes as input a common reference string crs, an instance ϕ and a witness w for $(\phi, w) \in R$, and returns a proof π.
- Verify is a deterministic polynomial time algorithm which takes as input a common reference string crs, an instance ϕ and a proof π, and returns 0 (reject) or 1 (accept).
- $\mathsf{SimProve}$ is a PPT algorithm which takes as input a common reference string crs, a simulation trapdoor τ, and an instance ϕ. The algorithm returns a simulated proof π.

zk-SNARK Π satisfies completeness, knowledge soundness, zero-knowledge, and succinctness as described below.

1) PERFECT COMPLETENESS

Perfect completeness stipulates that a prover with a witness who is given a true statement can convince a verifier.

For all $\lambda \in \mathbb{N}$, for all $R \in \mathcal{R}_\lambda$ and for all $(\phi, w) \in R$:

$$\Pr[(crs, \tau) \leftarrow \mathsf{Setup}(R); \pi \leftarrow \mathsf{Prove}(crs, \phi, w) : \mathsf{Verify}(crs, \phi, \pi) = 1] = 1 \quad (1)$$

2) COMPUTATIONAL SOUNDNESS

Computational knowledge soundness states that the prover must know a witness and the witness should be extracted efficiently from a knowledge extractor. Proof of knowledge requests every adversarial prover $\mathcal{A}$ to generate an accepting proof, there must be an extractor $\chi_{\mathcal{A}}$ which outputs a valid witness taking a same input of $\mathcal{A}$. Formally, we define $\mathbf{Adv}^{sound}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}(\lambda) = \Pr[\mathcal{G}^{sound}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}(\lambda)]$ where $\mathcal{G}^{sound}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}$ is defined as follows.

An argument system Arg is considered computationally sound if for any PPT adversary adversary $\mathcal{A}$, there exists a PPT extractor $\chi_{\mathcal{A}}$ where $\mathbf{Adv}^{sound}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}(\lambda) \approx 0$.

Algorithm 2 Knowledge Soundness Game $\mathcal{G}^{sound}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}$

```
$\mathcal{G}^{sound}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}(\lambda)$
  $R \leftarrow \mathcal{R}(1^\lambda)$
  $(crs, \tau) \leftarrow \mathsf{Setup}(R)$
  $(\phi, \pi) \leftarrow \mathcal{A}(crs)$
  $w \leftarrow \chi_{\mathcal{A}}(trans_{\mathcal{A}})$
  $\mathcal{A}$ wins if $\mathsf{Verify}(crs, \phi, \pi) = 1$ and $(\phi, w) \notin R$ and fails otherwise.
```

Algorithm 3 Zero-Knowledge Game $\mathcal{G}^{zk}_{Arg,\mathcal{A}}$

```
$\mathcal{G}^{zk}_{Arg,\mathcal{A}}(\lambda)$
  $R \leftarrow \mathcal{R}(1^\lambda)$
  $(crs, \tau) \leftarrow \mathsf{Setup}(R)$
  $b \leftarrow \{0, 1\}$
  if $b = 0$ then
    $P^b_{crs,\tau}(\phi_i, w_i)$ returns $\pi_i$ where $\pi_i \leftarrow \mathsf{Prove}(crs, \phi, w)$ and $(\phi_i, w_i) \in R$
  else
    $P^b_{crs,\tau}(\phi_i, w_i)$ returns $\pi_i$ where $\pi_i \leftarrow \mathsf{SimProve}(crs, \phi, \tau)$ and $(\phi_i, w_i) \in R$
  end if
  $b' \leftarrow \mathcal{A}^{P^b_{crs,\tau}(\phi_i, w_i)}$
  $\mathcal{A}$ wins if $b = b'$ and fails otherwise.
```

3) PERFECT ZERO-KNOWLEDGE

Perfect zero-knowledge stipulates that a proof does not disclose any information about the witness besides the truth of the instance. The statement is certified by a simulator which cannot access a witness but has some trapdoor information that allows simulating proofs. Formally, we define $\mathbf{Adv}^{zk}_{Arg,\mathcal{A}}(\lambda) = 2\Pr[\mathcal{G}^{zk}_{Arg,\mathcal{A}}(\lambda)] - 1$ such that the game $\mathcal{G}^{zk}_{Arg,\mathcal{A}}$ is defined as follows.

The argument system is considered perfect zero-knowledge if $\mathbf{Adv}^{zk}_{Arg,\mathcal{A}}(\lambda) = 0$ for all PPT adversaries $\mathcal{A}$.

4) SIMULATION-EXTRACTABILITY

Simulation-Extractability stipulates that any adversary $\mathcal{A}$ who can access a simulated proof for a false instance cannot forge the proof to another proof for a false instance. In a simulation extractable zk-SNARK, the adversary cannot generate a new valid proof even if the adversary acquire proofs of other statements.

Formally, we define $\mathbf{Adv}^{proof-ext}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}(\lambda) = \Pr[\mathcal{G}^{proof-ext}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}(\lambda)]$ where the game $\mathcal{G}^{proof-ext}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}$ is defined as follows.

Compared to the knowledge soundness game described in Algorithm 2, the adversary can access the simulated proof via $\mathsf{SimProve}$ queries additionally. zk-SNARK is considered simulation extractable if there exists an extractor $\chi_{\mathcal{A}}$, for any PPT adversary $\mathcal{A}$, where $\mathbf{Adv}^{proof-ext}_{Arg,\chi_{\mathcal{A}},\mathcal{A}}(\lambda) \approx 0$.

Proof-Carrying Data: Proof-carrying data (PCD) [42], [48] is a cryptographic primitive that guarantees the validity

Algorithm 4 Simulation Extractable Knowledge Soundness Game $\mathcal{G}^{proof-ext}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}$

```
$\mathcal{G}^{sound}_{Arg,\mathcal{A},\chi_{\mathcal{A}}}(\lambda)$
  $R \leftarrow \mathcal{R}(1^\lambda)$, $Q \leftarrow 0$
  $(crs, \tau) \leftarrow \mathsf{Setup}(R)$
  repeat
    $\pi_i \leftarrow \mathsf{SimProve}(crs, \tau, \phi_i)$
    $Q \leftarrow Q \cup \{\phi_i, \pi_i\}$
  until $(\phi, \pi) \leftarrow \mathcal{A}^{\mathsf{SimProve}_{crs,\tau}}(crs)$
  $w \leftarrow \chi_{\mathcal{A}}(trans_{\mathcal{A}})$
  $\mathcal{A}$ wins if $\mathsf{Verify}(crs, \phi, \pi) = 1$, $(\phi, w) \notin R$ and $(\phi, \pi) \notin Q$ and fails otherwise.
```

of all previous proofs via the recursive proof composition. It is a special case of zk-SNARK where the relation R is composed of some functions that are required for the verification of other proofs. To guarantee the verification result of the other proof in the proof circuit, the instance ϕ includes a proof set $\vec{\pi}$ and inputs needed for the verification of the proof additionally. It has a proof size independent of the number the recursion, and it has $O(1)$ verification time regardless of the number of recursion. PCD inherits all the properties of zk-SNARK such as the completeness, the knowledge soundness and zero-knowledge. The concrete proofs of these properties are described in Ben-Sasson *et al.*'s work [43].

D. FORWARD SECURE SIGNATURES

A forward secure signature scheme is a key evolving digital signature algorithm. All of the operations are divided into time period t and a signer signs a message using a different signing key which is issued at each time period. A key update is conducted by a one-way update function that computes a secret key for the new time period from the secret key at the current time period. A formal definition of the forward secure signature is as follows.

Definition 3: A forward secure signature is a set of four algorithms $\mathsf{FSS} = (\mathsf{Keygen}, \mathsf{Update}, \mathsf{Sign}, \mathsf{Verify})$ where

- Keygen takes as input a security parameter λ and returns a key pair sk_0, vk the initial signing key and the verification key and the time period j.
- Update takes as input a secret key sk_j, the time period j and returns the secret key sk_{j+1} and the next time period $j + 1$.
- Sign takes as input a message m, the secret key sk_j, the time period j, the verification key vk and returns σ_j that is a signature for time period j.
- Verify takes as input a message m, the time period j, the verification key vk, the signature σ and returns 1 if the σ is valid signature or 0, otherwise.

We define the security of FSS similarly to the existing works [5]–[7], [9]. The only difference is that we do not assume the maximal period anymore. Informally, an adversary who wants to succeed a valid signature forgery executes

Algorithm 5 Forward Security Game $\mathcal{G}^{fwsec}_{\mathsf{FSS},\mathcal{F}}(\lambda)$

```
$\mathcal{G}^{fwsec}_{\mathsf{FSS},\mathcal{F}}(\lambda)$
  $(sk_0, 0, vk) \leftarrow \mathsf{Keygen}(\lambda)$
  $j \leftarrow 0$
  repeat
    $j \leftarrow j+1$; $sk_j \leftarrow \mathsf{Update}(sk_{j-1}, j-1, vk)$; $d \leftarrow \mathcal{F}^{\mathsf{Sign}(\cdot,j)}(\mathsf{cma}, vk)$
  until $d = \mathsf{breakin}$
  $(m^*, b, \sigma) \leftarrow \mathcal{F}(\mathsf{forge}, sk_j)$
  if $\mathsf{Verify}(m^*, b, vk, \sigma) = 1$ and $m^*$ was not queried of $\mathsf{Sign}(\cdot, b)$ and $0 \le b < j$ then
    return 1 else return 0
  end if
```

chosen message attack cma until a secret signing key of the current time period is leaked. The adversary succeeds a valid forgery if the adversary generates a signature of the previous time period on a new message.

Formally, we define $\mathbf{A}dv^{fwsec}_{\mathsf{FSS},\mathcal{F}}(\lambda) = \Pr[\mathcal{G}^{fwsec}_{\mathsf{FSS},\mathcal{F}}(\lambda)]$ where the game $\mathcal{G}^{fwsec}_{\mathsf{FSS},\mathcal{F}}$ is defined in Algorithm 5.

The adversary $\mathcal{F}$ works in three phases: the chosen message attack cma phase, the break-in phase, breakin, the forgery phase forge. FSS is considered as forward secure if $\mathbf{A}dv^{fwsec}_{\mathsf{FSS},\mathcal{F}}(\lambda) \approx 0$ for any PPT adversary $\mathcal{F}$ where the execution time is at most t and the number of signing queries is at most q_{sig}.

E. FORWARD SECURE MULTI-USER AGGREGATE SIGNATURES

We extend the forward secure signature notion to a forward secure multi-user aggregate signature that supports the aggregation of multi-user signatures whose messages and time periods are different. A formal definition is as follows.

Definition 4: A forward secure multi-user aggregate signature FSMAS is a set of six algorithms by including additional algorithms in FSS. The additional algorithms are defined as follows.

- Agg takes as input a multi-user signature set $((m_1, j_1, vk_1, \sigma_1), \ldots, (m_n, j_n, vk_n, \sigma_n))$ and returns an aggregate signature σ_{agg}.
- AggVerify takes as input a set $(m_1, j_1, vk_1), .., (m_n, j_n, vk_n)$, the aggregate signature σ_{agg} and returns 1 if σ_{agg} is a valid signature or 0, otherwise.

We define the security of forward secure multi-user aggregate signature similar to Algorithm 5. An adversary $\mathcal{F}$ can freely choose all of the user verification keys $\vec{vk} = (vk_1, \ldots, vk_n)$ except the verification key of one honest user vk^*. When the adversary $\mathcal{F}$ is given the verification key of the honest user vk^*, the adversary tries to forge an aggregate signature that involves the signature of the honest user. An adversary $\mathcal{F}$ can access a sign oracle and an update oracle freely, and can request break-in query also. Since the aggregation is allowed to everyone, the

Algorithm 6 Forward Security Game of FMSAS $\mathcal{G}^{fwsec}_{\mathsf{FSMAS},\mathcal{F}}(\lambda)$

```
$\mathcal{G}^{fwsec}_{\mathsf{FSMAS},\mathcal{F}}(\lambda)$
  $(sk^*_0, 0, vk^*) \leftarrow \mathsf{Keygen}(\lambda)$
  $j \leftarrow 0$
  repeat
    $j \leftarrow j+1$; $sk^*_j \leftarrow \mathsf{Update}(sk^*_{j-1}, j-1, vk^*)$; $d \leftarrow \mathcal{F}^{\mathsf{Sign}(\cdot,j)}(\mathsf{cma}, vk^*)$
  until $d = \mathsf{breakin}$
  $((m_1, j_1, vk_1, ), \ldots, (m^*, b, vk^*), \ldots, (m_n, j_n, vk_n)), \sigma^*_{agg})$
  $\leftarrow \mathcal{F}(\mathsf{forge}, sk^*_j)$
  if $\mathsf{AggVerify}((m_1, j_1, vk_1), \ldots, (m_n, j_n, vk_n), \sigma^*_{agg}) = 1$ and $vk^* \in \{vk_1, \ldots, vk_n\}$ and $m^*$ was not queried of $\mathsf{Sign}(\cdot, b)$ and $0 \le b < j$ then
    return 1 else return 0
  end if
```

adversary does not need to request an oracle of aggregation. If the adversary outputs an aggregate signature σ^*_{agg} where $\mathsf{AggVerify}((m_1, j_1, vk_1), \ldots, (m_n, j_n, vk_n), \sigma^*_{agg}) = 1$ and the aggregate signature includes the signature of m^* that was not queried of $\mathsf{Sign}(\cdot, b)$ and $0 \le b < j$ and $vk^* \in \vec{vk}$, then the adversary wins the forgery game. A formal security notion is described in Algorithm 6. Formally, we define $\mathbf{A}dv^{fwsec}_{\mathsf{FSMAS},\mathcal{F}}(\lambda) = \Pr[\mathcal{G}^{fwsec}_{\mathsf{FSMAS},\mathcal{F}}(\lambda)]$ where the game $\mathcal{G}^{fwsec}_{\mathsf{FSMAS},\mathcal{F}}$ is defined in Algorithm 6.

IV. CONSTRUCTION

A. MAIN IDEA

In this section, we describe a formal construction of the proposed scheme. We represent intuition of our construction first then specify details of the construction. Verification of forward secure signature [5]–[7] checks whether the signature satisfies the following properties.

- A verification key is generated from a secret signing key which is implied in the signature.
- The signing key is updated correctly corresponding to a time period.
- The signing key is connected to a correct message with the time period.

While it is not easy to construct a signature scheme which satisfies the above properties simultaneously, it is more straightforward to devise a circuit to satisfy the above properties by stating them. Even if more properties are required, it is not difficult to include them in a circuit. Hence, we devise a relation circuit to efficiently represent each property in zk-SNARKs.

In key generation, a signing and verification key pair is generated with a proof which proves a connectivity between the signing key and the verification key. When the secret signing key is updated, the existing key is checked and it is updated through one-way hash function. In a sign relation, the secret key should be checked against the verification key,

Algorithm 7 Relation

```
update_relation($s_{j'}, j', vk; \pi_j, s_j, j$)
    if $j = 0$ then
        $vk = H(s_j||r)$
    else
        $j' = j + 1$
        $\Pi$.verify($\pi_j, s_j, j, vk, crs$) = 1
        $s_{j'} = H(s_j)$
    end if
sign_relation($\phi_{sig}; \pi_j, s_j, j, vk$)
    $\Pi$.verify($\pi_j, s_j, vk, crs$) = 1
    $\phi_{sig} = H(m||j||vk)$
```

and a signature is a hash output of the message, the time period, and the verification key. When aggregation of signatures is required, a circuit checks two signatures to be aggregated and generates a single hash output from two input data.

B. FORWARD SECURE SIGNATURE CONSTRUCTION

We provide a formal construction of the proposed forward secure signature scheme. Note that we use simulation-extractable zk-SNARK Π as a building block in our signature scheme. We assume that a common reference string *crs* is hard-coded as an integer value in algorithm. Algorithm 7 describes zk-SNARK relation of update and signing process. In key generation (a time period j is set to 0), a proof that proves a correlation of the signing key and the verification key is generated. update$_{\text{relation}}$ describes a key generation relation and update relation. If the time period j' is 0, the proof proves that the verification key vk is a hash output of signing key s_j. When the signer updates the signing key (the time period $j' > 0$), the signer proves that a verification output of π_j which proves correctness of s_j is 1 and an updated signing key $s_{j'}$ is hash output of s_j. As described in sign$_{\text{relation}}$, the signer should prove verification of the proof π_j. Then the signer proves that the committed value ϕ_{sig} is a hash output of a message m, the time period j and the verification key vk.

Algorithm 8 shows an overall construction of our proposed forward secure signature. Let H be a collision-resistant hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^l$ where l is a bit length of hash function output. In Setup, this algorithm takes as input a relation for update R_{update}, and relation for sign R_{sig}. The algorithm generates all common reference strings for relations and hardcodes crs_{update}, crs_{sig} into the algorithms respectively.

Keygen takes a security parameter λ as input. The algorithm sets an initial secret signing key s_0 from $\mathbb{Z}_p$ randomly and yields a verification key vk which is a hash output of concatenation of s_0 and the random value r. An initial time period j is set to 0. The algorithm computes a proof π_{init} which proves the correctness of verification key vk based on update_relation. Keygen sets (s_j, π_j) to sk_j and outputs sk_j, j, vk. Update takes as input a previous signing key sk_j, time

Algorithm 8 Forward Secure Signature (FSS) Scheme

```
Setup($R_{update}, R_{sig}$)
    $crs_{update} \leftarrow \Pi$.setup($R_{update}$)
    $crs_{sig} \leftarrow \Pi$.setup($R_{sig}$)
    return $crs_{update}, crs_{sig}$
Keygen($\lambda$)
    $s_0 \overset{\$}{\leftarrow} \mathbb{Z}_l^*$
    $r \overset{\$}{\leftarrow} \mathbb{Z}_l^*$
    $vk \leftarrow H(s_0||r)$
    $j \leftarrow 0$
    $\pi_{init} \leftarrow \Pi$.prove($s_j, j, vk, crs_{update}$)
    $sk_j \leftarrow (s_j, \pi_{init})$
    return $sk_j, j, vk$
Update($sk_j, j, vk$)
    if $\Pi$.verify($\pi_j, s_j, j, vk, crs_{update}$) = 1 then
        $j' \leftarrow j + 1$
        $s_{j'} \leftarrow H(s_j)$
    else
        abort
    end if
    $\pi_{j'} \leftarrow \Pi$.prove($s_{j'}, j', vk, crs_{update}; \pi_j, s_j, j$)
    delete $sk_j$
    $sk_{j'} \leftarrow (s_{j'}, \pi_{j'})$
    return $sk_{j'}, j'$
Sign($m, sk_j, j, vk$)
    if verify($\pi_j, s_j, j, vk, crs_{update}$) = 1 then
        $\phi_{sig} \leftarrow H(m||j||vk)$
        $\pi_{sig} \leftarrow \Pi$.prove($\phi_{sig}, crs_{sig}; \pi_j, s_j, j, vk$)
    else
        abort
    end if
    type $\leftarrow 0$
    $\sigma \leftarrow (\pi_{sig}, \phi_{sig}$, type)
    return $\sigma$
Verify($m, j, vk, \sigma$)
    Check $\phi_{sig} = H(m||j||vk)$
    $b \leftarrow \Pi$.verify($\pi_{sig}, \phi_{sig}, crs_{sig}$)
    return $b$
```

period j, and verification key vk. The algorithm verifies the proof π_j that implies the correctness of signing keys in all previous periods first. If it is verified, it updates the signing key by computing a new signing key s_{j+1} that is a hash output of s_j. Update generates a proof π_{j+1} for update_relation taking $s_{j+1}, j + 1, vk$ as input and π_j, s_j, j as witness then deletes the previous signing key sk_j. The algorithm outputs the updated signing key sk_{j+1} and the new time period $j + 1$. Sign takes as input a message m, a signing key sk_j, a time period j, and a verification key vk. If the proof π_j which proves validity of s_j on update_relation is verified, ϕ_{sig} that is a hash output of $m||j||vk$ is generated. The algorithm makes a proof π_{sig} taking ϕ_{sig} as input based on sign_relation.

Algorithm 9 Agg Relation

```
agg_relation($\phi_{agg}$; $\sigma_i$, $\sigma_j$)
  Parse $\sigma_i$ as ($\phi_i$, $\pi_i$, type$_i$)
  Parse $\sigma_j$ as ($\phi_j$, $\pi_j$, type$_j$)
  if type$_i$ $= 0$ then
      $crs \leftarrow crs_{sig}$
  else
      $crs \leftarrow crs_{agg}$
  end if
  $\Pi$.verify($\pi_i, \phi_i, crs$) $= 1$
  $\Pi$.verify($\pi_j, \phi_j, crs_{sig}$) $= 1$
  $\phi_{agg} = H(\phi_i || \phi_j)$
```

And then type that reveals the type of signatures is 0. The algorithm finally outputs $\sigma = (\phi_{sig}, \pi_{sig}, \text{type})$. Since the normal signature verification and the aggregate signature verification have different relations, the type of signature should be available to a verifier (and an aggregator) for efficient aggregation. Though a secret signing key is connected with a message directly in the normal signature scheme, our scheme connects a message m with the verification key vk to support aggregation of multi-user signatures.

Verify first checks the correctness of ϕ_{sig} by computing $H(m||j||vk)$. Verify calls Π.verify and returns b which is a verification result of π_{sig} taking input ϕ_{sig}.

V. EXTENDED CONSTRUCTION

A. FORWARD SECURE AGGREGATE SIGNATURE CONSTRUCTION

Algorithm 9 represents a relation for the signature aggregation. We assume that the aggregation proceeds one by one repeatedly regardless of the signature's time period, message, and verification key. The intuitive idea of the aggregation is that a proof can be an aggregate signature if the proof proves verification of the multiple signatures. For instance, when Alice wants to aggregate Bob's two signatures which have different time periods and messages, she can aggregate two signatures by verifying signatures respectively and proving the verification process. As described in Algorithm 9, an aggregator verifies two signatures then generates a hash value that implies all the components of signatures (the message, the time period, and the verification key).

Algorithm 10 shows a whole construction of aggregation. AggSetup takes as input a relation R_{agg} that is described in Algorithm 9, and generates a common reference string for aggregation crs_{agg} and it is hardcoded in the algorithm. The aggregate algorithm Agg takes as input n signature sets $(m_1, j_1, vk_1, \sigma_1), \ldots, (m_n, j_n, vk_n, \sigma_n)$ where m_i,j_i,vk_i are the message, the time period, and the verification key, respectively. The algorithm first checks the validity of ϕ_{sig_i} value of all σ_i by computing $H(m_i||j_i||vk_i)$ then verifies first two signatures by running Π.verify with crs_{sig}. After they are verified, the algorithm generates a new signature value ϕ_{agg} which is a hash output of $(\phi_{sig_1}||\phi_{sig_2})$. The algorithm proves

Algorithm 10 Aggregation Construction

```
AggSetup($R_{agg}$)
  $crs_{agg} \leftarrow \Pi$.setup($R_{agg}$)
  return $crs_{agg}$
Agg(($m_1, j_1, vk_1, \sigma_1$), ..., ($m_n, j_n, vk_n, \sigma_n$))
  parse $\sigma_i$ as ($\phi_{sig_i}, \pi_{sig_i}$, type$_i$)
  Check all $\phi_{sig_i} = H(m_i||j_i||vk_i)$
  $b_1 \leftarrow \Pi$.verify($\pi_{sig_1}, \phi_{sig_1}, crs_{sig}$)
  $b_2 \leftarrow \Pi$.verify($\pi_{sig_2}, \phi_{sig_2}, crs_{sig}$)
  if $b_1 \&\& b_2 = 1$ then
      $\phi_{agg} \leftarrow H(\phi_{sig_1}||\phi_{sig_2})$
      $\pi_{agg} \leftarrow \Pi$.prove($\phi_{agg}, crs_{agg}; \sigma_1, \sigma_2$)
      type $\leftarrow 1$
  end if
  if $n < 3$ then $\sigma_{agg} \leftarrow (\phi_{agg}, \pi_{agg}, \text{type})$
      return $\sigma_{agg}$
  else
      for $i \leftarrow 3$ to $n$ do
          $\sigma_{old} \leftarrow (\phi_{agg}, \pi_{agg})$
          $b_1 \leftarrow \Pi$.verify($\pi_{agg}, \phi_{agg}, crs_{agg}$)
          $b_2 \leftarrow \Pi$.verify($\pi_i, \phi_i, crs_{sig}$)
          if $b_1 \& b_2 \neq 1$ then abort
          else
              $\phi_{agg} \leftarrow H(\phi_{agg}||\phi_i)$
              $\pi_{agg} \leftarrow \Pi$.prove($\phi_{agg}, crs_{agg}; \sigma_{old}, \sigma_i$)
              type $\leftarrow 1$
              $\sigma_{agg} \leftarrow (\phi_{agg}, \pi_{agg}, \text{type})$
          end if
      end for
  end if
  return $\sigma_{agg}$
AggVerify(($m_1, j_1, vk_1$), ..., ($m_n, j_n, vk_n$), $\sigma_{agg}$)
  parse $\sigma_{agg}$ as ($\phi_{agg}, \pi_{agg}$)
  $\phi_{sig_1} \leftarrow H(m_1||j_1||vk_1)$
  $\phi_{sig_{old}} \leftarrow \phi_{sig_1}$
  for $i \leftarrow 2$ to $n$ do
      $\phi_{sig_i} \leftarrow H(m_i||j_i||vk_i)$
      $\phi_{sig_{old}} \leftarrow H(\phi_{sig_{old}}||\phi_{sig_i})$
  end for
  if $\phi_{sig_{old}} = \phi_{agg}$ then
      $b \leftarrow \Pi$.verify($\phi_{agg}, crs_{agg}$)
  end if
  return $b$
```

the aggregation result according to algorithm 9. If more than two signatures are aggregated, the aggregator verifies the previous aggregate signature with crs_{agg} and input signature σ_i with crs_{sig}. Similarly to the above aggregation, the aggregator generates a hash output value ϕ_{agg} and proves the verification results repeatedly. The algorithm returns aggregate signature $(\phi_{agg}, \pi_{agg}, \text{type})$ lastly.

A verification algorithm AggVerify takes n messages, time periods, verification keys and the aggregate signature σ_{agg}. A verifier first checks the validity of ϕ_{agg} in σ_{agg} using the hash-chain computation, and verifies the aggregate signature using Π.verify.

VI. SECURITY PROOF

Proof Idea: We construct our signature scheme based on an extractable hash assumption described in Algorithm 1. By designing a hash extraction adversary $\mathcal{A}$ that utilizes a signature forgery $\mathcal{F}$ as a subroutine to succeed in the extraction of a hash pre-image, we prove the forward security of our signature scheme. Intuitively, the adversary $\mathcal{A}$ acquires a trapdoor of a proof in the setup phase and the trapdoor enables the adversary $\mathcal{A}$ to generate a simulated proof in the query phase. Finally, the adversary $\mathcal{A}$ that has a witness extractor of the proof extracts the hash pre-image from the proof where the forgery $\mathcal{F}$ outputs as a signature. We describe the formal security proof as follows.

Theorem 1: Let FSS be our key evolving signature scheme. Then for parameters modulus size λ, the execution time t, the common reference generation time t_{crs}, and the number of sign queries q_{sig},

$$\mathbf{Adv}^{fwsec}_{\mathsf{FSS},\mathcal{F}}(\lambda) \le \mathbf{Adv}^{Hash-ext}_{H,\varepsilon,\mathcal{A}}(\lambda) \tag{2}$$

where $t' = t + t_{crs}$

Theorem 2: Let FSMAS be our forward secure multi-user aggregate signature scheme. Then for parameters modulus size λ, the execution time t, the common reference generation time t_{crs}, and the number of sign queries q_{sig},

$$\mathbf{Adv}^{fwsec}_{\mathsf{FSMAS},\mathcal{F}}(\lambda) \le \mathbf{Adv}^{Hash-ext}_{H,\varepsilon,\mathcal{A}}(\lambda) \tag{3}$$

where $t' = t + t_{crs}$

A. PROOF OF THEOREM 1

We construct an adversary $\mathcal{A}$ that conducts a hash extraction game described in Algorithm 1. The adversary $\mathcal{A}$ utilizes the adversary $\mathcal{F}$ which executes $\mathcal{G}^{fwsec}_{\mathsf{FSS},\mathcal{F}}(\lambda)$ experiment described in Algorithm 5 as a subroutine. We suppose the adversary $\mathcal{F}$ succeeds with $\mathbf{Adv}^{fwsec}_{\mathsf{FSS},\mathcal{F}}(\lambda)$ in execution time t.

1) INITIAL KEY GENERATION

The adversary $\mathcal{A}$ gets a hash value σ from the challenger, and then set σ to vk. The adversary runs Setup and acquires common reference strings crs_{update}, and crs_{sig}. Note that since the adversary has a trapdoor of the common reference string, the adversary can generate simulated proof using Π.SimProve. Unusually, the adversary does not need to choose an initial secret signing key s_0, since the correctness of vk is guaranteed by a simulated proof which deceives a relation between vk and the blank input. The adversary runs subroutine $\mathcal{F}$ taking as input vk, crs_{update}, and crs_{sig}.

2) INTERACTIVE QUERY PHASE

- **Update query**: When $\mathcal{F}$ requests to update the signing key, $\mathcal{A}$ runs Π.SimProve and acquires a simulated proof on any arbitrary signing key at the queried time period. Since the simulated proof can prove any relation of false input, $\mathcal{A}$ can update the signing key fraudulently.
- **Sign query**: $\mathcal{A}$ generates a signature dishonestly without the secret signing key when $\mathcal{A}$ receives a sign query (a message m, time period j). $\mathcal{A}$ sets $H(m||j||vk)$ as ϕ_{sig} and generates a simulated proof π_{sig}. Finally $\mathcal{A}$ outputs a signature where $\sigma = (\pi_{sig}, \phi_{sig}, \mathsf{type})$ to $\mathcal{F}$.
- **Break-in query**: $\mathcal{A}$ randomly chooses a secret signing key s_b that is unrelated to the previous signing key and the vk. Likewise the above, relation between s_b and vk is proven by simulated proof π_b. $\mathcal{A}$ outputs current time period signing key s_b and π_b to $\mathcal{F}$.

3) FINAL FORGERY

When $\mathcal{F}$ acquires a signing key s_b and π_b where b is the time period at break-in, $\mathcal{F}$ outputs forged signature $(\pi_{sig^*}, \phi_{sig^*}, \mathsf{type})$ on a new message m^* where m^* was not queried of $\mathsf{Sign}(\cdot, j)$ and $0 \le j < b$. After receiving the forged signature set, $\mathcal{A}$ runs extractor $\mathcal{E}$ and extracts a secret signing key s_j which is a witness of π_{sig^*}. The adversary $\mathcal{A}$ can compute a pre-image of s_b through hashing s_j repeatedly.

4) SUCCESS PROBABILITY

We analyze a probability of above execution. Note that we do not need to guess the time period of break-in since all the signing keys are irrelevant to the signing key at the time period of break-in via the simulated proof. Likewise, there is no probability to fail responding the sign query because all the queries can be responded through the simulated proof. Therefore, a success probability of $\mathcal{A}$ converges on the success probability of extractor $\mathcal{E}$ completely.

B. PROOF OF THEOREM 2

A proof of Theorem 2 is almost identical to the proof of Theorem 1. The adversary $\mathcal{F}$ forges an aggregate signature on behalf of forging the normal forward secure signature. Thus, all the proof procedure proceeds as subsection VI-A except for the final forgery. When $\mathcal{A}$ is given a forged aggregate signature, $\mathcal{A}$ should run the extractor $\mathcal{E}$ recursively until the extractor outputs the sk_j of signature on message m^* where $0 \le j < b$. Since the aggregate signature proves only the aggregation result, an inner proof which is a witness of the forged aggregate signature should be extracted n times in worst case (n is the number of aggregations). Thus the success probability of $\mathcal{A}$ converges on ϵ^n where ϵ is the success probability of extractor $\mathcal{E}$. Note that if the aggregation is performed balanced then n becomes $O(\log(N))$ where N denotes the total number of signatures in an aggregate signature and the success probability is $N\epsilon$.

VII. EXPERIMENT

In this section, we measure the performance of our forward secure signature. Basically, our forward secure signature scheme supports the aggregation of multi-user signatures regardless of their time periods, and all the efficiencies are not dependent on the time period. In particular, only zk-SNARK

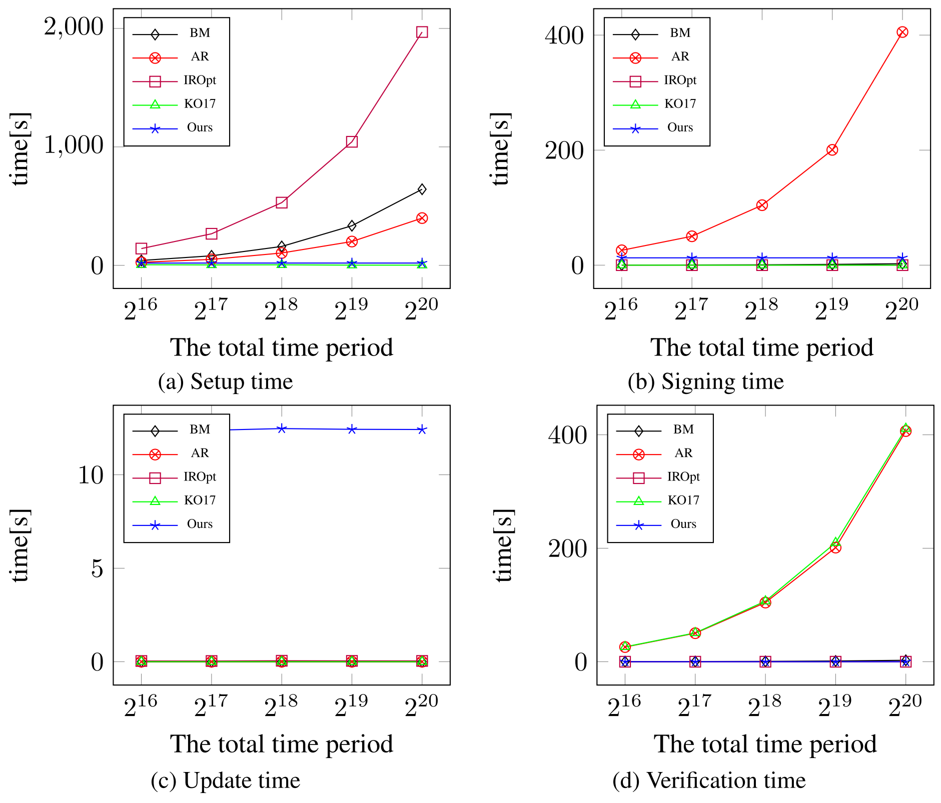

FIGURE 2. **Comparison of time performances with other forward secure signatures.**

circuit size affects the time efficiencies of our construction, and the performance of the construction can differ depending on the zk-SNARK proof scheme. We implement the forward secure signature scheme using Plonk [32] proposed by Aztec as the zero-knowledge proof scheme [49]. We compare the performance of our signature scheme with BM [5], AR [6], IR [7], KO17 [12], and KO19 [21]. The experiment is performed on Intel i7 4.2GHz desktop with 64GB RAM under Ubuntu 18.04.

Figure 2 represents the key setup time, the signing time, the update time, and the verification time of all comparative signatures by varying the total time period T. The security parameter is fixed to 2048 bits in cases of RSA-based signature schemes [5]–[7], [12], [21] and 256 bits in our case since the construction utilizes a pairing function. The message length is fixed to 160 bits in all cases.

As shown in Figure 2(a), the setup time is proportional to the total time periods T in BM, AR, and IR (optimized version). Specifically, the setup time of IROpt reaches about 2000 seconds when the total time period is 2^{20}. In case of KO17, while the time complexity is $O(lT)$ originally, the setup is optimized by using the RSA group order in the implementation. Our scheme has 19 seconds in all time periods cases. Figure 2(b) illustrates the signing time of the signature schemes. IROpt, KO17, and our signature scheme have a constant signing time. Note that it takes 12 seconds in our scheme where the circuit size affects the signing time. Meanwhile, BM and AR have a signing time that is proportional to total time periods T in the same manner, the signing time of AR takes more than those of BM since the computation in AR is composed of exponentiation. In case of the update time, as shown in Figure 2(c), all the signature schemes have a constant update time. Like in the case of the signing time, our update time is affected by the zk-SNARK circuit size and it takes 12 seconds identical to the signing time. Figure 2(d) illustrates the verification time of all signature schemes. Only IROpt and our signature scheme have a constant verification time. On the other hand, other signature schemes have a maximum period dependent verification time. Table 3 shows detailed data of the performance when $T = 2^{20}$, and the message bits $l = 160$.

Table 4 represents the experiment results on the forward secure aggregate schemes. We implement forward secure aggregate schemes via applying KO19 [21] technique to BM and AR respectively. The total time period, the message bits, and the security parameter are equivalent to Table 3 and the number of signatures is two. As shown in Table 4, the aggregation time in our signature scheme has a relatively heavy computation compared with the other forward secure signatures since a large size circuit is required like 1.6M gates for the aggregation. However, the verification time of the aggregate signature is equal to the single signature

TABLE 3. Performance experiment results in forward secure signature schemes.

		Ours	BM [5]	AR [6]	IR [7]	KO17 [12]
Key generation time		$19.407s$	$642.4375s$	$398.9233s$	$1970.0101s$	$4.4893s$
Update time		$12.874s$	$0.6ms$	$0.4ms$	$43ms$	$0.4ms$
Signing time		$12.555s$	$2.5412s$	$398.3939s$	$1ms$	$0.4ms$
Verification time		$1ms$	$2.5118s$	$389.2896s$	$0.2ms$	$389.3412s$
Signing key size	Secret key	$1.6KB$	$65KB$	$0.2KB$	$0.5KB$	$0.2KB$
	Public parameter	$654MB$				
Verification key size	Verification key	$32B$	$65KB$	$0.5KB$	$0.5KB$	$1KB$
	Public parameter	$1KB$				
Signature size		$1.6KB$	$0.5KB$	$0.2KB$	$0.3KB$	$0.5KB$

TABLE 4. Performance experiment results on aggregation.

	Ours	BM-FAS [21]	AR-FAS [21]
Setup time	$38.54s$	$1701.22s$	$1159.04s$
Signing time	$12.55s$	$2242.76s$	$3477.03s$
Aggregation time	$25.23s$	$0.004ms$	$0.004ms$
Aggregate signature verification time	$1ms$	$1680.63s$	$1739.39s$

verification. In addition, the circuit is optimizable using Halo technique [44] that performs the proof verification outside the proof circuit via the proof aggregation.

VIII. CONCLUSION

In this paper, we propose a new forward secure multi-user aggregate signature using zk-SNARK. Our new forward secure signature scheme supports all constant complexities and a flexible aggregation where all restrictions that exist in previous works are eliminated. Specifically, our signature scheme has constant complexities of setup time, update time, signing time and verification time. In terms of the size, signature and key sizes are also constant. Our signature scheme supports the aggregation of multi-user signatures with all different messages and different time periods. We use zk-SNARK as a building block of the forward secure signature scheme. Through the characteristic of zk-SNARK that proves any arbitrary relation in key evolving structure, we remove time period dependent operations and aggregate multi-user signatures flexibly. The security of the proposed scheme is formally proven in the random oracle model. Our experimental results demonstrate the practicality of our signature scheme. In future, we will extend our methodology to cover more properties such as group signatures, blind signatures, etc. and improve the performance in zk-SNARK computation.

REFERENCES

[1] X. Yang, D. Fan, A. Ren, N. Zhao, and M. Alam, "5G-based user-centric sensing at C-band," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 3040–3047, May 2019.
[2] C. Meshram, A. Alsanad, J. V. Tembhurne, S. W. Shende, K. W. Kalare, S. G. Meshram, M. A. Akbar, and A. Gumaei, "A provably secure lightweight subtree-based short signature scheme with fuzzy user data sharing for human-centered IoT," *IEEE Access*, vol. 9, pp. 3649–3659, 2021.
[3] X. Yang, L. Guan, Y. Li, W. Wang, Q. Zhang, M. U. Rehman, and Q. H. Abbasi, "Contactless finger tapping detection at C-band," *IEEE Sensors J.*, vol. 21, no. 4, pp. 5249–5258, Feb. 2021.
[4] R. Anderson, "Invited lecture," in *Proc. 4th ACM Comput. Commun. Secur.*, 1997.
[5] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in *Proc. 19th Annu. Int. Cryptol. Conf.* Santa Barbara, CA, USA: Springer, Aug. 1999, pp. 431–448.
[6] H. Jingxin, "A new forward-secure digital signature scheme," in *Proc. Int. Workshop Anti-Counterfeiting, Secur. Identificat. (ASID)*, Apr. 2007, pp. 116–129.
[7] G. Itkis and L. Reyzin, "Forward-secure signatures with optimal signing and verifying," in *Proc. Annu. Int. Cryptol. Conf.* Santa Barbara, CA, USA: Springer, Aug. 2001, pp. 332–354.
[8] A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in *Proc. 3rd Int. Conf., SCN*. Amalfi, Italy: Springer, Sep. 2002, pp. 241–256.
[9] X. Boyen, H. Shacham, E. Shen, and B. Waters, "Forward-secure signatures with untrusted update," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006, pp. 191–200.
[10] T. Malkin, D. Micciancio, and S. Miner, "Efficient generic forward-secure signatures with an unbounded number of time periods," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Amsterdam, The Netherlands: Springer, Apr./May 2002, pp. 400–417.
[11] H. Krawczyk, "Simple forward-secure signatures from any signature scheme," in *Proc. 7th ACM Conf. Comput. Commun. Secur. (CCS)*, 2000, pp. 108–115.
[12] J. Kim and H. Oh, "Forward-secure digital signature schemes with optimal computation and storage of signers," in *Proc. 32nd IFIP TC 11 Int. Conf., SEC*. Rome, Italy: Springer, May 2017, pp. 523–537.
[13] S. Hohenberger and B. Waters, "New methods and abstractions for RSA-based forward secure signatures," in *Proc. 18th Int. Conf., ACNS*. Rome, Italy: Springer, Oct. 2020, pp. 292–312.
[14] K. Qiao, H. Tang, W. You, and Y. Zhao, "Blockchain privacy protection scheme based on aggregate signature," in *Proc. IEEE 4th Int. Conf. Cloud Comput. Big Data Anal. (ICCCBDA)*, Apr. 2019, pp. 492–497.
[15] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Warsaw, Poland: Springer, May 2003, pp. 416–432.
[16] D. R. Brown and S. A. Vanstone, "Aggregate signature schemes," U.S. Patent 8 185 744, May 22, 2012.
[17] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Inf. Sci.*, vol. 219, pp. 225–235, Jan. 2013.

[18] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in *Proc. 9th Int. Conf. Theory Pract. Public-Key Cryptogr.* New York, NY, USA: Springer, Apr. 2006, pp. 257–273.

[19] S. Chatterjee, D. Hankerson, E. Knapp, and A. Menezes, "Comparing two pairing-based aggregate signature schemes," *Des., Codes Cryptogr.*, vol. 55, nos. 2–3, pp. 141–167, May 2010.

[20] D. Ma and G. Tsudik, "Forward-secure sequential aggregate authentication," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 86–91.

[21] J. Kim and H. Oh, "FAS: Forward secure sequential aggregate signatures for secure logging," *Inf. Sci.*, vol. 471, pp. 115–131, Jan. 2019.

[22] D. Ma, "Practical forward secure sequential aggregate signatures," in *Proc. ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, 2008, pp. 341–352.

[23] A. A. Yavuz, P. Ning, and M. K. Reiter, "BAF and FI-BAF: Efficient and publicly verifiable cryptographic schemes for secure logging in resource-constrained systems," *ACM Trans. Inf. Syst. Secur.*, vol. 15, no. 2, pp. 1–28, Jul. 2012.

[24] M. Drijvers and G. Neven, "Forward-secure multi-signatures," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 261, Dec. 2019.

[25] J. Groth and M. Maller, "Snarky signatures: Minimal signatures of knowledge from simulation-extractable SNARKs," in *Proc. 37th Annu. Int. Cryptol. Conf.*, vol. 10402. Santa Barbara, CA, USA: Springer, Aug. 2017, pp. 581–612.

[26] S. Bowe and A. Gabizon, "Making Groth's zk-SNARK simulation extractable in the random oracle model," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 187, Feb. 2018.

[27] H. Lipmaa, "Simulation-extractable snarks revisited," Cryptol. ePrint Arch., Tech. Rep. 2019/612, 2019. [Online]. Available: https://eprint.iacr.org/index.html

[28] J. Kim, J. Lee, and H. Oh, "Qap-based simulation-extractable snark with a single verification," Cryptol. ePrint Arch., Tech. Rep. 2019/586, 2019. [Online]. Available: https://eprint.iacr.org/index.html

[29] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "Recursive composition and bootstrapping for SNARKS and proof-carrying data," in *Proc. 45th Annu. ACM Symp. Symp. Theory Comput. (STOC)*, 2013, pp. 111–120.

[30] J. Kim, J. Lee, and H. Oh, "Simulation-extractable zk-SNARK with a single verification," *IEEE Access*, vol. 8, pp. 156569–156581, 2020.

[31] M. Maller, S. Bowe, M. Kohlweiss, and S. Meiklejohn, "Sonic: Zero-knowledge SNARKs from linear-size universal and updatable structured reference strings," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 2111–2128.

[32] A. Gabizon, Z. J. Williamson, and O. Ciobotaru, "Plonk: Permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 953, Dec. 2019.

[33] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 315–334.

[34] (2014). *Libsnark*. Accessed: 2020. [Online]. Available: https://github.com/scipr-lab/libsnark

[35] J. Baylina. (2020). *Iden3/Snarkjs*. [Online]. Available: https://github.com/iden3/snarkjs

[36] J. Li, H. Teng, X. Huang, Y. Zhang, and J. Zhou, "A forward-secure certificate-based signature scheme," *Comput. J.*, vol. 58, no. 4, pp. 853–866, Apr. 2015.

[37] Y. Lu and J. Li, "A forward-secure certificate-based signature scheme with enhanced security in the standard model," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 3, pp. 1502–1522, 2019.

[38] J. Li, H. Du, and Y. Zhang, "Certificate-based key-insulated signature in the standard model," *Comput. J.*, vol. 59, no. 7, pp. 1028–1039, 2016.

[39] B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 238–252.

[40] J. Groth, "On the size of pairing-based non-interactive arguments," in *Proc. 35th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Vienna, Austria: Springer, May 2016, pp. 305–326.

[41] R. Gennaro, C. Gentry, B. Parno, and M. Raykova, "Quadratic span programs and succinct NIZKs without PCPs," in *Proc. 32nd Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Athens, Greece: Springer, May 2013, pp. 626–645.

[42] A. Chiesa and E. Tromer, "Proof-carrying data and hearsay arguments from signature cards," in *Proc. ICS*, vol. 10, 2010, pp. 310–331.

[43] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Scalable zero knowledge via cycles of elliptic curves," *Algorithmica*, vol. 79, no. 4, pp. 1102–1160, Dec. 2017.

[44] S. Bowe, J. Grigg, and D. Hopwood, "Halo: Recursive proof composition without a trusted setup," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 1021, Feb. 2020.

[45] A. Chiesa, D. Ojha, and N. Spooner, "Fractal: Post-quantum and transparent recursive proofs from holography," in *Proc. 39th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Zagreb, Croatia: Springer, May 2020, pp. 769–793.

[46] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proc. 3rd Innov. Theor. Comput. Sci. Conf. (ITCS)*, 2012, pp. 326–349.

[47] D. Fiore, C. Fournet, E. Ghosh, M. Kohlweiss, O. Ohrimenko, and B. Parno, "Hash first, argue later: Adaptive verifiable computations on outsourced data," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1304–1316.

[48] A. Chiesa and E. Tromer, "Proof-carrying data: Secure computation on untrusted platforms (high-level description)," *Next Wave, Nat. Secur. Agency's Rev. Emerg. Technol.*, vol. 19, no. 2, pp. 40–46, 2012.

[49] (2020). *Aztecprotocol/Barretenberg*. [Online]. Available: https://github.com/AztecProtocol/barretenberg.git

JEONGHYUK LEE received the B.S. degree in information systems engineering from Hanyang University, Seoul, South Korea, where he is currently pursuing the Ph.D. degree in information systems engineering. His current research interests focus on applied cryptography, in particular on provable security for cryptographic schemes, including protocols for public-key encryption, blockchain, and zero-knowledge proof systems.

JIHYE KIM (Member, IEEE) received the B.S. and M.S. degrees from the School of Computer Science and Engineering, Seoul National University, South Korea, in 1999 and 2003, respectively, and the Ph.D. degree in computer science from the University of California at Irvine, in 2008. She is currently an Associate Professor with the Department of Electrical Engineering, Kookmin University. Her research interests include network security, applied cryptography, and zero-knowledge proof.

HYUNOK OH (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in computer engineering from Seoul National University, Seoul, South Korea, in 1996, 1998, and 2003, respectively. He is currently a Full Professor with the Department of Information Systems, Hanyang University, Seoul. His research interests include applied cryptography, zero-knowledge proof, and blockchain.