Pixel: Multi-signatures for Consensus

Manu Drijvers, DFINITY; Sergey Gorbunov, Algorand and University of Waterloo; Gregory Neven, DFINITY; Hoeteck Wee, Algorand and CNRS, ENS, PSL

https://www.usenix.org/conference/usenixsecurity20/presentation/drijvers
Abstract

In Proof-of-Stake (PoS) and permissioned blockchains, a committee of verifiers agrees and sign every new block of transactions. These blocks are validated, propagated, and stored by all users in the network. However, posterior corruptions pose a common threat to these designs, because the adversary can corrupt committee verifiers after they certified a block and use their signing keys to certify a different block. Designing efficient and secure digital signatures for use in PoS blockchains can substantially reduce bandwidth, storage and computing requirements from nodes, thereby enabling more efficient applications.

We present Pixel, a pairing-based forward-secure multi-signature scheme optimized for use in blockchains, that achieves substantial savings in bandwidth, storage requirements, and verification effort. Pixel signatures consist of two group elements, regardless of the number of signers, can be verified using three pairings and one exponentiation, and support non-interactive aggregation of individual signatures into a multi-signature. Pixel signatures are also forward-secure and let signers evolve their keys over time, such that new keys cannot be used to sign on old blocks, protecting against posterior corruptions attacks on blockchains. We show how to integrate Pixel into any PoS blockchain. Next, we evaluate Pixel in a real-world PoS blockchain implementation, showing that it yields notable savings in storage, bandwidth, and block verification time. In particular, Pixel signatures reduce the size of blocks with 1500 transactions by 35% and reduce block verification time by 38%.

1 Introduction

Blockchain technologies are quickly gaining popularity for payments, financial applications, and other distributed applications. A blockchain is an append-only public ledger that is maintained and verified by distributed nodes. At the core of the blockchain is a consensus mechanism that allows nodes to agree on changes to the ledger, while ensuring that changes once confirmed cannot be altered.

In the first generation of blockchain implementations, such as Bitcoin, Ethereum, Litecoin, the nodes with the largest computational resources choose the next block. These implementations suffer from many known inefficiencies, low throughput, and high transaction latency [17, 27, 49]. To overcome these problems, the current generation of blockchain implementations such as Algorand, Cardano, Ethereum Casper, and Dfinity turn to proofs of stake (PoS), where nodes with larger stakes in the system—as measured, for instance, by the amount of money in their account—are more likely to participate in choosing the next block [21, 24, 29, 32, 34, 39, 47]. Permissioned blockchains such as Ripple [54] and Hyperledger Fabric [4] take yet another approach, sacrificing openness for efficiency by limiting participation in the network to a selected set of nodes.

All PoS-based blockchains, as well as permissioned ones, have a common structure where the nodes run a consensus sub-protocol to agree on the next block to be added to the ledger. Such a consensus protocol usually requires nodes to inspect block proposals and express their agreement by digitally signing acceptable proposals. When a node sees sufficiently many signatures from other nodes on a particular block, it appends the block to its view of the ledger.

Because the consensus protocol often involves thousands of nodes working together to reach consensus, efficiency of the signature scheme is of paramount importance. Moreover, to enable outsiders to efficiently verify the validity of the chain, signatures should be compact to transmit and fast to verify. Multi-signatures [35] have been found particularly useful for this task, as they enable many signers to create a compact and efficiently verifiable signature on a common message [15, 40, 58, 59].

The Problem of Posterior Corruptions. Chain integrity in a PoS blockchain relies on the assumption that the adversary controls less than a certain threshold (e.g., a third) of the total stake; an adversary controlling more than that fraction...
may be able to fork the chain, i.e., present two different but equally valid versions of the ledger. Because the distribution of stake changes over time, however, the real assumption behind chain integrity is not just that the adversary currently controls less than a threshold of the stake, but that he never did so at any time in the past.

This assumption becomes particularly problematic if stake control is demonstrated through possession of signature keys, as is the case in many PoS and permissioned blockchains. Indeed, one could expect current stakeholders to properly protect their stake-holding keys, but they may not continue to do so forever, especially after selling their stake. Nevertheless, without additional precautions, an adversary who obtains keys that represent a substantial fraction of stake at some point in the past can compromise the ledger at any point in the future. The problem is further aggravated in efficient blockchains that delegate signing rights to a small committee of stakeholders, because the adversary can gain control of the chain after corrupting a majority of the committee members.

Referred to by different authors as long-range attacks [20], costless simulation [52], and posterior corruptions [12], this problem is best addressed through the use of forward-secure signatures [3, 9, 41, 46]. Here, each signature is associated with the current time period, and a user’s secret key can be updated in such a way that it can only be used to sign messages for future time periods, not previous ones. An adversary that corrupts an honest node can therefore not use the compromised key material to create forks in the past of the chain.

1.1 Our Results

We present the Pixel signature scheme, which is a pairing-based forward-secure multi-signature scheme for use in PoS-based blockchains that achieves substantial savings in bandwidth and storage requirements. To support a total of $T$ time periods and a committee of size $N$, the multi-signature comprises just two group elements and verification requires only three pairings, one exponentiation, and $N - 1$ multiplications. Pixel signatures are almost as efficient as BLS multi-signatures, as depicted in Figure 1, but also satisfy forward-secure; moreover, like in BLS multi-signatures, anybody can non-interactively aggregate individual signatures into a multi-signature.

Our construction builds on prior forward-secure signatures based on hierarchical identity-based encryption (HIBE) [14, 18, 22, 26] and adds the ability to securely aggregate signatures on the same message as well as to generate public parameters without trusted set-up.

We achieve security in the random oracle model under a variant of the bilinear Diffie-Hellman inversion assumption [11, 14]. At a very high level, the use of HIBE techniques allows us to compress $O(\log T)$ group elements in a tree-based forward-secure signature into two group elements, and secure aggregation allows us to compress $N$ signatures under $N$ public keys into a single multi-signature of the same size as a single signature.

To validate Pixel’s design, we compared the performance of a Rust implementation [1] of Pixel with previous forward-secure tree-based solutions. We show how to integrate Pixel into any PoS blockchain. Next, we evaluate Pixel on the Algorand blockchain, showing that it yields notable savings in storage, bandwidth, and block verification time. Our experimental results show that Pixel is efficient as a stand-alone primitive and in use in blockchains. For instance, compared to a set of $N = 1500$ tree-based forward-secure signatures (for $T = 2^{32}$) at 128-bit security level, a single Pixel signature that can authenticate the entire set is 2667x smaller and can be verified 40x faster (c.f. Tables 1 and 3). Pixel signatures reduce the size of Algorand blocks with 1500 transactions by $\approx 35\%$ and reduce block verification time by $\approx 38\%$ (c.f. Figures 3 and 4).

1.2 Related Work

Multi-signatures can be used to generate a single short signature validates that a message $m$ was signed by $N$ different parties [6, 10, 13, 31, 35, 43, 44, 48, 50]. Multi-signatures based on the BLS signature scheme [13, 15, 16, 53] are particularly well-suited to the distributed setting of PoS blockchains as no communication is required between the signers; anybody can aggregate individual signatures into a multi-signature. However, these signatures are not forward-secure.

Tree-based forward-secure signatures [9, 36, 41, 46] can be used to meet the security requirements, but they are not very efficient in an $N$-signer setting because all existing constructions have signature size at least $O(N\log T)$ group elements, where $T$ is an upper bound on the number of time periods. Some schemes derived from hierarchical identity-based encryption (HIBE) [14, 18, 22] can bring that down to $O(N)$ group elements, which is still linear in the number of signers.

The only forward-secure multi-signature schemes that appeared in the literature so far have public key length linear in the number of time periods $T$ [45] or require interaction between the signers to produce a multi-signature [55], neither of which is desirable in a blockchain scenario. The forward-secure multi-signature scheme of Yu et al. [61] has signature length linear in the number of signers, so is not really a multi-signature scheme.

Combining the generic tree-based forward-secure signature scheme of Bellare-Miner [9] with BLS multi-signatures [13, 16] gives some savings, but still requires $O(T)$ “certificates” to be included in each multi-signature. Batch verification [8] can be used to speed up verification of the certificates to some extent, but does not give us any space savings. Compared with existing tree-based forward-secure signatures in [9, 36, 41, 46], our savings are two-fold:

- we reduce the size of the signature set for $N$ commit-


| scheme                          | key update | sign | verify | $|\sigma|/|pk|/|sk|$ | forward security |
|-------------------------------|------------|------|--------|-----------------|-----------------|
| BLS multi-signatures [13, 15, 53] | –          | 1 exp| 2 pair | 1               | $O(1)$          |
| Pixel multi-signatures (this work) | 2 exp | 4 exp| 3 pair + 1 exp | 2               | $O((\log T)^2)$ |

Figure 1: Comparing our scheme with BLS signatures. Here, “exp” and “pair” refer to number of exponentiations and pairings respectively. $T$ denotes the maximum number of time periods. We omit additive overheads of $O(\log T)$ multiplications. The column “key update” refers to amortized cost of updating the key for time $t$ to $t+1$. The columns $|\sigma|$, $|pk|$, and $|sk|$ denote the sizes of signatures, public keys, and secret keys, respectively, in terms of group elements. Aggregate verification for $N$ signatures requires an additional $N - 1$ multiplications over basic verification.

- we reduce the verification time from $O(N)$ exponentiations to $O(1)$ exponentiation and $O(N)$ multiplications.

13 Paper Organization

The rest of this paper is organized as follows:

- In Section 2, we give a high level technical description of our new pairing-based forward-secure multi-signature scheme.
- In Sections 4 and 5, we describe the scheme in details. We prove the security of the construction in the random oracle model under a variant of a bilinear Diffie-Hellman inversion problem.
- In Section 6, we explain how to apply Pixel to PoS blockchains to solve posterior corruptions.
- In Section 7, we evaluate the efficiency savings for storage, bandwidth, and block verification time from using Pixel on the Algorand PoS blockchain.

2 Technical Overview

Our construction builds on prior forward-secure signatures based on hierarchical identity-based encryption (HIBE) [14, 18, 22, 26] and adds the ability to securely aggregate signatures on the same message as well as to generate public parameters without trusted set-up.

Overview of our scheme. Starting with a bilinear group $(G_1, G_2, G_t)$ with $e : G_1 \times G_2 → G_t$ of prime order $q$ and generators $g_1, g_2$ for $G_1, G_2$ respectively, a signature on $M \in \mathbb{Z}_q$ at time $t$ under public key $g_2^t$ is of the form:

$$\sigma = (\sigma', \sigma'') = (h^t \cdot F(t, M)^{r'}, g_2^{r'}) \in G_1 \times G_2$$

where the function $F(t, M)$ can be computed with some public parameters (two group elements in $G_1$ in addition to $h \in G_1$) and $r$ is fresh randomness used for signing. Verification relies on the relation:

$$e(\sigma', g_2) = e(h, y) \cdot e(F(t, M), \sigma'')$$

and completeness follows directly:

$$e(\sigma', g_2) = e(h^t \cdot F(t, M)^{r'}, g_2)$$

$$= e(h^t, g_2) \cdot e(F(t, M)^{r'}, g_2)$$

$$= e(h, g_2^t) \cdot e(F(t, M), g_2^t)$$

$$= e(h, y) \cdot e(F(t, M), \sigma'')$$.

Note that $e(h, y)$ can be precomputed to save verification computation.

Given $N$ signatures $\sigma_1, \ldots, \sigma_N \in G_1 \times G_2$ on the same message $M$ at time $t$ under $N$ public keys $g_2^{r_1}, \ldots, g_2^{r_N}$, we can produce a multi-signature $\Sigma$ on $M$ by computing the coordinate-wise product of $\sigma_1, \ldots, \sigma_N$. Concretely, if $\sigma_i = (h_i, g_2^{r_i}, F(t, M)^{r_i}, g_2^{r_i})$, then

$$\Sigma = (h_1^{r_1} \cdot \cdots \cdot h_N^{r_N} \cdot F(t, M)^r, g_2^t)$$

where $r' = r_1 + \cdots + r_N$. To verify $\Sigma$, we first compute a single aggregate public key that is a compressed version of all $N$ individual public keys

$$apk \leftarrow y_1 \cdot \cdots \cdot y_N,$$

and verify $\Sigma$ against $apk$ using the standard verification equation.

How to generate and update keys. To complete this overview, we describe a simplified version of the secret keys and update mechanism, where the secret keys are of size $O(T)$ instead of $O((\log T)^2)$. The construction exploits the fact that the function $F$ satisfies

$$F(t, M) = F(t, 0) \cdot F^{M}$$

for some constant $F'$. This means that in order to sign messages at time $t$, it suffices to know

$$\tilde{sk}_t = \{h^t \cdot F(t, 0)^{r'}, F^{r'}, g_2^{r'}\}$$
from which we can compute \((h^t \cdot F(t, M)^r \cdot g_2^t)\).

The secret key \(sk_t\) for time \(t\) is given by:

\[
\tilde{sk}_t, \tilde{sk}_{t+1}, \ldots, \tilde{sk}_T
\]
generated using independent randomness. To update from the key \(sk_t\) to \(sk_{t+1}\), we simply erase \(sk_t\). Forward security follows from the fact that an adversary who corrupts a signer at time \(t\) only learns \(sk_t\) and, in particular, does not learn \(sk_{t'}\) for \(t' < t\), and is unable to create signatures for past time slots.

To compress the secret keys down to \(O((\log T)^2)\) without increasing the signature size, we combine the tree-based approach in [22] with the compact HIBE in [14]. Roughly speaking, each \(sk_t\) now contains \(\log T\) sub-keys, each of which contains \(O(\log T)\) group elements and looks like an "expanded" version of \(sk_t\). (In the simplified scheme, each \(sk_t\) contains \(T - t + 1\) sub-keys, each of which contains three group elements.)

Security against rogue-key attacks. The design of multi-signature schemes must take into account rogue-key attacks, where an adversary forges a multi-signature by providing specially crafted public keys that are correlated with the public keys of the honest parties. We achieve security against rogue-key attacks by having users provide a proof of possession of their secret key [13, 53]; it suffices here for each user to provide a standard BLS signature \(y\) on its public key \(y\) (cf. the proof \(\pi\) in the key generation and verification algorithms in Section 5.2).

Avoiding trusted set-up. Note that the common parameters contain uniformly random group elements \(h, h_0, \ldots, h_{\log T}\) in \(G_2\) which are used to define the function \(F\). These elements can be generated using an indifferentiable hash-to-curve algorithm [19, 60] evaluated on some fixed sequence of inputs (e.g. determined by the digits of pi), thereby avoiding any trusted set-up.

2.1 Discussion

Related works. The use of HIBE schemes for forward secrecy originates in the context of encryption [22] and has been used in signatures [18, 26], key exchange [33] and proxy re-encryption [30]. Our signature construction is quite similar to the forward-secure signatures of Boyen et al. [18] and achieves the same asymptotic complexity; their construction is more complex in order to achieve security against untrusted updates. The way we achieve aggregation is similar to the multi-signatures in [43].

Alternative approaches to posterior security. There are two variants of the posterior attack: (i) a short-range variant, where an adversary tries to corrupt a committee member prior to completion of the consensus sub-protocol, and (ii) a long-range variant as explained earlier. Dfinity [34], Ouroboros [39] and Casper [21] cope with the short-range attacks by assuming a delay in attacks that is longer than the running time of the consensus sub-protocol. For long-range attacks, Casper adopts a fork choice rule to never revert a finalized block, and in addition, assumes that clients log on with sufficient regularity to gain a complete up-to-date view of the chain. We note that forward-secure signatures provide a clean solution against both attacks, without the need for fork choice rules or additional assumptions about the adversary and the clients.

Application to permissioned blockchains. Consensus protocols, such as PBFT, are also at the core of many permissioned blockchains (e.g. Hyperledger), where only approved parties may join the network. Our signature scheme can similarly be applied to this setting to achieve forward secrecy, reduce communication bandwidth, and produce compact block certificates.

3 Preliminaries

Let \(G_1, G_2, G_3\) be multiplicative groups of prime order \(q\) with a non-degenerate pairing function \(e : G_1 \times G_2 \rightarrow G_3\). Let \(g_1\) and \(g_2\) be generators of \(G_1\) and \(G_2\), respectively.

In analogy with the weak bilinear Diffie-Hellman inversion problem \(\ell\-wBDHI\) [14], which was originally defined for Type-1 pairings (i.e., symmetric pairings where we have \(G_1 = G_2\)), we define the following variant for Type-3 pairings denoted \(\ell\-wBDHI\):

\[
\begin{align*}
\text{Input:} & \quad A_1 = g_1^\alpha, A_2 = g_1^{(\alpha^2)}, \ldots, A_\ell = g_1^{(\alpha^\ell)}, \\
& \quad B_1 = g_2^\alpha, B_2 = g_2^{(\alpha^2)}, \ldots, B_\ell = g_2^{(\alpha^\ell)}, \\
& \quad C_1 = g_3^\gamma, C_2 = g_3^{\gamma^2}, \\
\text{for } & \quad \alpha, \gamma \in \mathbb{Z}_q \\
\text{Compute:} & \quad e(g_1, g_2)^{\gamma \alpha^{\ell+1}}
\end{align*}
\]

The advantage \(\text{Adv}_{\ell\-wBDHI}(A)\) of an adversary \(A\) is defined as its probability in solving this problem.

As shown in [14], the assumption holds in the generic bilinear group model, with a lower bound of \(\Omega(\sqrt{q/\ell})\) (with a matching attack in [25]). Concretely, for the BLS12-381 pairing-friendly curve with \(\ell = 32\), the best attack has complexity roughly \(2^{125}\).

Alternatively, our scheme could be proved secure under a variant of the above assumption where the adversary has to output \(g_1^{(\alpha^{\ell+1})}\) given as input \(A_1, \ldots, A_\ell, B_1, \ldots, B_\ell\) and given access to an oracle \(\psi : g_2^3 \rightarrow g_1^3\). Because of the \(\psi\) oracle, this assumption is incomparable to the \(\ell\-wBDHI\) assumption described above.
4 Forward-Secure Signatures

We begin by describing a forward-secure signature scheme, and then extend the construction to a multi-signature scheme in Section 5.

4.1 Definition

We use the Bellare-Miner model [9] to define syntax and security of a forward-secure signature scheme. A forward-secure signature scheme $\mathcal{FS}$ for a message space $\mathcal{M}$ consists of the following algorithms:

**Setup**: $pp \leftarrow \text{Setup}(T)$. All parties agree on the public parameters $pp$. The setup algorithm mainly fixes the distribution of the parameters given the maximum number of time periods $T$. The parameters may be generated by a trusted third party, through a distributed protocol, or set to “nothing-up-my-sleeve” numbers. The public parameters are taken to be an implicit input to all of the following algorithms.

**Key generation**: $(pk, sk_1) \leftarrow \text{Kg}$. The signer runs the key generation algorithm on input the maximum number of time periods $T$ to generate a public verification key $pk$ and an initial secret signing key $sk_1$ for the first time period.

**Key update**: $sk_{t+1} \leftarrow \text{Upd}(sk_t)$. The signer updates its secret key $sk_t$ for time period $t$ to $sk_{t+1}$ for the next period using the key update algorithm. The scheme could also offer a “fast-forward” update algorithm $sk_{t'} \leftarrow \text{Upd}'(sk_t, t')$ for any $t' > t$ that is more efficient than repetitively applying $\text{Upd}$.

**Signing**: $\sigma \leftarrow \text{Sign}(sk_t, M)$. On input the current signing key $sk_t$ and message $M \in \mathcal{M}$, the signer uses this algorithm to compute a signature $\sigma$.

**Verification**: $b \leftarrow \text{Vf}(pk, t, M, \sigma)$. Anyone can verify a signature $\sigma$ on a message $M$ for time period $t$ under public key $pk$ by running the verification algorithm, which returns 1 to indicate that the signature is valid and 0 otherwise.

**Correctness**

Correctness requires that for all messages $M \in \mathcal{M}$ and for all time periods $t \in [T]$ it holds that

$$\Pr[\text{Vf}(pk, t, M, \text{Sign}(sk_t, M)) = 1] = 1$$

where the coin tosses are over $pp \leftarrow \text{Setup}(T)$, $(pk, sk_1) \leftarrow \text{Kg}$, and $sk_i \leftarrow \text{Upd}(sk_{i-1})$ for $i = 2, \ldots, t$.

Moreover, if the scheme has a fast-forward update algorithm, then the keys it produces must be distributed identically to those produced by repetitive application of the regular update algorithm. Meaning, for all $t, t' \in [T]$ with $t < t' \leq T$ and for all $sk_t$ it holds that $sk_{t'} \leftarrow \text{Upd}'(sk_t, t')$ follows the same distribution as $sk_t$ produced as $sk_t \leftarrow \text{Upd}(sk_{t-1})$ for $i = t+1, \ldots, t'$.

**Security**

Unforgeability under chosen-message attack for forward-secure signatures is defined through the following game. The experiment generates a fresh key pair $(pk, sk_1)$ and hands the public key $pk$ to the adversary $A$. The adversary is given access to the following oracles:

**Key update.** If the current time period $t$ (initially set to $t = 1$) is less than $T$, then this oracle updates the key $sk_t$ to $sk_{t+1}$ and increases it.

**Signing.** On input a message $M$, this oracle runs the signing oracle with the current secret key $sk_t$ and message $M$, and returns the resulting signature $\sigma$.

**Break in.** The experiment records the break-in time $\bar{t} \leftarrow t$ and hands the current signing key $sk_t$ to the adversary. This oracle can only be queried once, and after it has been queried, the adversary can make no further queries to the key update or signing oracles.

At the end of the game, the adversary outputs its forgery $(t^*, M^*, \sigma^*)$. It wins the game if $\sigma^*$ verifies correctly under $pk$ for time period $t^*$ and message $M^*$, if it never queried the signing oracle on $M^*$ during time period $t^*$, and if it queried the break-in oracle, then it did so in a time period $\bar{t} > t^*$.

We define $A$’s advantage $\text{Adv}_{\mathcal{FS}}^\text{cma}(A)$ as its probability in winning the above game.

We also define a selective variant of the above notion, referred to as $\text{sfu-cma}$, where the adversary first has to commit to $\bar{t}, t^*$, and $M^*$. More specifically, $A$ first outputs $(\bar{t}, t^*, M^*)$, then receives the public key $pk$, is allowed to make signature and key update queries until time period $t = \bar{t}$ is reached, at which point it is given $sk_{t}$ and outputs its forgery $\sigma^*$.

4.2 Encoding time periods

Following [22], we associate time periods with all nodes of the tree according to a pre-order traversal. Prior tree-based forward-secure signatures [9,46] associate time periods with the only leaf nodes; using all nodes allows us to reduce the amortized complexity of key updates from $O(\log T)$ exponentializations to $O(1)$ exponentializations.

Recall that a tree of depth $\ell - 1$ has $2^{\ell} - 1$ nodes, which then correspond to time periods in $[2^\ell - 1]$. We will identify the nodes of the tree of depth $\ell - 1$ with strings in $\{1, 2\}^{\leq \ell - 1}$ where 1 denotes taking the left branch and 2 denotes taking the right branch. We work with $\{1, 2\}$ instead of $\{0, 1\}$ for technical reasons: roughly speaking, in the scheme, we need to work with strings of length exactly $\ell - 1$, which we obtain by padding strings in $\{1, 2\}^{\leq \ell - 1}$ with zeroes.

We can also describe the association explicitly as a bijection between $t = t_1 \| t_2 \| \ldots \in \{1, 2\}^{\leq \ell - 1}$ and $t \in [2^\ell - 1]$ for
any integer \( \ell \) given by
\[
\tau(t) = 1 + \sum_{i=1}^{\lceil \ell \rceil} (1 + 2^{\ell-i}(t_i - 1))
\]

For instance, for \( \ell = 3 \), this maps \( \varepsilon, 1, 11, 12, 2, 21, 22 \) to \( 1, 2, 3, 4, 5, 6, 7 \). The inverse of the bijection can be described as
\[
\tau(1) = \varepsilon \\
\tau(t) = \tau(t - 1) + 1 \text{ if } |\tau(t - 1)| < \ell - 1 \\
\tau(t) = \bar{t} + 2 \text{ if } |\tau(t - 1)| = \ell - 1
\]
where \( \bar{t} \) is the longest string such that \( \bar{t} \) is a prefix of \( \tau(t - 1) \).

The bijection induces a natural precedence relation over \( \{1, 2\}^{\leq \ell - 1} \) where \( t \preceq t' \) if \( t \) is a prefix of \( t' \) or exists \( \bar{t} \) s.t. \( \bar{t} \) is a prefix of \( t \) and \( \bar{t} + 2 \) is a prefix of \( t' \). We also write \( t, t + 1 \) corresponding to \( t, \bar{t} + 1 \).

Next, we associate any \( t \in \{1, 2\}^{\leq \ell - 1} \) with a set \( \Gamma_t \subset \{1, 2\}^{\leq \ell - 1} \) given by
\[
\Gamma_t := \{ t \} \cup \{ \bar{t} + 2 : |\bar{t} + 2| \text{ prefix of } t \}
\]
that corresponds to the set containing \( t \) and all the right-hand siblings of nodes on the path from \( t \) to the root, which also happens to be the smallest set of nodes that includes a prefix of all \( t' \succeq t \). For instance, for \( \ell = 3 \), we have
\[
\Gamma_1 = \{1, 2\}, \Gamma_{11} = \{11, 12, 2\}, \Gamma_{12} = \{12, 2\}.
\]

The sets \( \Gamma_t \) satisfy the following properties:
- \( t' \preceq t \) iff there exists \( u \in \Gamma_t \) s.t. \( u \) is a prefix of \( t' \);
- For all \( t \), we have \( \Gamma_{t+1} = \Gamma_t \setminus \{ t \} \) if \( |t| = \ell - 1 \) or \( \Gamma_{t+1} = \Gamma_t \setminus \{ t \} \cup \{ |t| + 2 \} \) otherwise;
- For all \( t' \succeq t \), we have that for all \( u' \in \Gamma_t \), there exists \( u \in \Gamma_t \) such that \( u \) is a prefix of \( u' \).

The first property is used for verification and for reasoning about security; the second and third properties are used for key updates.

### 4.3 Construction

We assume the bound \( T \) is of the form \( 2^\ell - 1 \). We use the above bijection so that the algorithms take input \( t \in \{1, 2\}^{\leq \ell - 1} \) instead of \( t \in [T] \). The following scheme is roughly the result of applying the Canetti-Halevi-Katz technique to obtain forward security from hierarchical identity-based encryption (HIBE) [23] to the signature scheme determined by the key structure of the Boneh-Boyen-Goh HIBE scheme [14]; we describe the differences at the end of this subsection.

**Setup.** Let \( \mathcal{M} \) be the message space of the scheme and let \( H_q : \mathcal{M} \rightarrow \{0, 1\}^\kappa \) be a hash function that maps messages to bit strings of length \( \kappa \) such that \( 2^\kappa < q \). Apart from the description of the groups, the common system parameters also contain the maximum number of time slots \( T = 2^\ell - 1 \) and random group elements \( h, h_0, \ldots, h_t \in G_1 \). These parameters could, for example, be generated as the output of a hash function modeled as a random oracle.

**Key generation.** Each signer chooses \( x \in \mathbb{Z}_q \) and computes \( y \leftarrow g_x^y \). It sets its public to \( pk = y \) and computes its initial secret key \( sk_1 \leftarrow \{sk_e\} \) where \( sk_e = (g_x^e, h^x_{h_0}, h_{t+1}, \ldots, h_t) \) for \( r \in \mathbb{Z}_q \).

**Key update.** We associate with each \( w \in \{1, 2\}^k \) with \( k \leq \ell - 1 \) a key \( \tilde{sk}_w \) of the form
\[
\tilde{sk}_w = (c, d, e_{k+1}, \ldots, e_1)
\]
for \( r \in \mathbb{Z}_q \). Given \( \tilde{sk}_w \), one can derive a key for any \( w' \in \{1, 2\}^k \) which contains \( w \) as a prefix as
\[
(c', d', e_{k+1}', \ldots, e_1') = \left( c \cdot g_x^{e_2}, \ldots, e_{k+1} \cdot h_{k+1} \cdot \ldots, e_1 \cdot h_1 \right)
\]
for \( r' \in \mathbb{Z}_q \).

The secret key \( sk_t \) at time period \( t \) is given by
\[
sk_t = \{ \tilde{sk}_w : w \in \Gamma_t \},
\]
which, by the first property of \( \Gamma_t \), contains a key \( \tilde{sk}_w \) for a prefix \( w \) of all nodes \( t' \succeq t \).

To perform a regular update of \( sk_t \) to \( sk_{t+1} \), the signer uses the second property of \( \Gamma_t \). Namely, if \( |t| < \ell - 1 \), then the signer looks up \( \tilde{sk}_t = (c, d, e_{t+1}, \ldots, e_1) \in sk_t \), computes
\[
\tilde{sk}_{t+1} = (c, d, e_{t+2}, e_{t+2}, \ldots, e_1),
\]
and derives \( \tilde{sk}_w \) from \( \tilde{sk}_t \) using Equation (2). The signer then sets \( sk_{t+1} \leftarrow \{\tilde{sk}_{t+1}\} \cup \{\tilde{sk}_{t+1} \} \) and securely deletes \( sk_t \) as well as the re-randomization exponent \( r' \) used in the derivation of \( \tilde{sk}_{t+1} \).

If \( |t| = \ell - 1 \), then the signer simply sets \( sk_{t+1} \leftarrow sk_t \setminus \{\tilde{sk}_1\} \) and securely deletes \( sk_t \).

To perform a fast-forward update of its key to any time \( t' \geq t \), the signer derives keys \( \tilde{sk}_{w'} \) for all nodes \( w' \in \Gamma_{t'} \setminus \Gamma_t \) by applying Equation (2) to the key \( sk_w \in sk_t \) such that \( w' \) is a prefix of \( w \), which must exist due to the third property of \( \Gamma_t \). The signer then sets \( sk_{t'} \leftarrow \{\tilde{sk}_{w'} : w' \in \Gamma_{t'} \} \) and securely deletes \( sk_t \) as well as all re-randomization exponents used in the key derivations.
To generate a signature on message $M \in \mathcal{M}$ in time period $t \in \{1, 2, \ldots, t-1\}$, the signer looks up $sk_t = (c, d, e_{t+1}, \ldots, e_t) \in sk_t$, chooses $r' \leftarrow Z_q$, and outputs

$$(\sigma_1, \sigma_2) = \left(d' \cdot e_{t}^{H_t(M)}, (h_0 \cdot \prod_{j=1}^{t} h_j^{r_j} \cdot h_t^{H_t(M)})^{r'}, c \cdot g_2^{r'}\right).$$

### Verification

Anyone can verify a signature $(\sigma_1, \sigma_2) \in \mathbb{G}_1 \times \mathbb{G}_2$ on message $M$ under public key $pk = y$ in time period $t$ by checking whether

$$e(\sigma_1, g_2) = e(h, y) \cdot e(h_0 \cdot \prod_{j=1}^{t} h_j^{r_j} \cdot h_t^{H_t(M)}, \sigma_2).$$

Note that the pairing $e(h, y)$ can be pre-computed from the public key ahead of time, so that verification only requires two pairing computations.

### Differences from prior works

We highlight the differences between our scheme and those in [14, 18, 22], assuming some familiarity with these prior constructions.

- We rely on asymmetric bilinear groups for efficiency, and our signature sits in $\mathbb{G}_2 \times \mathbb{G}_1$ instead of $\mathbb{G}_2^2$. This way, it is sufficient to give out the public parameters $h_0, \ldots, h_t$ in $\mathbb{G}_1$ (which we can then instantiate using hash-to-curve with trusted setup) instead of having to generate “consistent” public parameters $(h_1, h_t') = (g_1^y, g_2^y) \in \mathbb{G}_1 \times \mathbb{G}_2$.

- Our key-generation algorithm also deviates from that in the Boneh-Boyen-Goh HIBE, which would set

$$pk = e(g_1, g_2)^t, h = g_1, \tilde{sk}_t = (g_t^x, g_t^y h_0, h_1', \ldots, h_t').$$

In our scheme, $pk = g_2^t$ lies in $\mathbb{G}_2$ instead of $\mathbb{G}_1$ and is therefore smaller. Setting $h$ to be random instead of $g_1$ also allows us to achieve security under weaker assumptions. In fact, setting $h = g_1$ and $pk = g_2^t$ would yield an insecure scheme in symmetric pairing groups where $g_1 = g_2$, since $h^x = g_1^y = g_2^y = pk$.

### 4.4 Correctness

We say that a secret key $sk_t$ for time period $t$ is well-formed if $sk_t = \{\tilde{sk}_w : w \in \Gamma_t\}$, where each $\tilde{sk}_w$ is of the form of Equation (1) for an independent uniformly distributed exponent $r' \leftarrow Z_q$. We first show that all honestly generated and updated secret keys are well-formed, and then proceed to the verification of signatures.

The key $sk_t$ is trivially well-formed for $t = 1$, i.e., $t = e$, as can be seen from the key generation algorithm. We now show that $sk_t$ is also well-formed after a regular update from time $t$ to $t+1$ and after a fast-forward update from $t$ to $t' > t$.

In a regular update, assume that $sk_t$ is well-formed. If $|t| = \ell - 1$, then the update procedure sets $sk_{t+1} \leftarrow sk_t \setminus \{sk_t\}$, which by the second property of $\Gamma_t$ and the induction hypothesis means that $sk_{t+1}$ is also well-formed. If $|t| < \ell - 1$, the update procedure adds keys $\tilde{sk}_{t1}$ and $\tilde{sk}_{t2}$ and removes $\tilde{sk}_t$ from $sk_t$, which by the second property of $\Gamma_t$ indeed corresponds to $\{w \in \Gamma_t\}$.

Moreover, $sk_{t1}$ is derived from $\tilde{sk}_t = sk_{t1} \leftarrow (c, d, e_{t+1}, \ldots, e_t)$ as $\tilde{sk}_{t1} \leftarrow (c, d, e_{t+1}, e_{t+2}, \ldots, e_t)$, which satisfies Equation (1) with randomness $r$ that is independent from all other keys in $sk_{t+1}$ because $\tilde{sk}_t \not\in sk_{t+1}$. Similarly, $\tilde{sk}_{t2}$ satisfies Equation (1) because it is generated as

$$c' = c \cdot g_2'^r = g_2^{r'},$$
$$d' = d' \cdot e_{t+1}^r (h_0 \cdot \prod_{j=1}^{t} h_j^{r_j} \cdot h_{t+1}^{H_{t+1}(M)})^{r'},$$
$$= h^x (h_0 \cdot \prod_{j=1}^{t} h_j^{r_j} \cdot h_{t+1}^{H_{t+1}(M)})^{r'},$$
$$e_{t+1}' = e_{t+1} \cdot h_{t+1}' = h_{t+2}' \cdot \cdots \cdot h_{t+1}' = h_{t+1}'^{r'},$$
$$e'_{t+1} = e'_{t+1} \cdot h_{t+1}' = h_{t+1}'^{r'}$$

satisfying Equation (1) with randomness $r + r'$, which is independent of the randomness of other keys in $sk_{t+1}$ due to the uniform choice of $r'$.

For the fast-forward update procedure, one can see that if $sk_f$ is well-formed, then the updated key $sk_{t'f}$ for $t' > t$ is still well-formed as well. Indeed, by adding the keys for nodes in $\Gamma_t \setminus \Gamma_f$ and removing those for $\Gamma_f \setminus \Gamma_t$, we have that $sk_{t'f}$ contains keys $\tilde{sk}_w$ for all $w \in \Gamma_f$. The randomness independence is guaranteed by the random choice of $r'$ in Equation (2). In the optimized variant, all keys still have independent randomness because one key $\tilde{sk}_{w'} \in sk_{t'f}$ will have the same randomness $r$ as some key $\tilde{sk}_w \in sk_f$ where $w$ is a prefix of $w'$. That randomness is independent from all other keys in $sk_{t'f}$, however, because the key $\tilde{sk}_w$ does not occur in $sk_{t'f}$. Indeed, by the definition of $\Gamma_{t'}$, one can see that $\Gamma_{t'}$ cannot have elements $w \neq w'$ with $w$ a prefix of $w'$.

To see why signature verification works, observe that a signature for time period $t$ and message $M$ is computed from a key $\tilde{sk}_t = (c, d, e_{t+1}, \ldots, e_t)$ in a well-formed key $sk_t$. The
left-hand side of the verification equation is therefore

$$e(\sigma_1, g_2) = e\left( d \cdot e_t^{H_0(M)}, (h_0 \prod_{j=1}^{[k]} h_j^{H_t(M)}) r', g_2 \right)$$

$$= e\left( h^r (h_0 \prod_{j=1}^{[k]} h_j^{H_t(M)}) r', g_2 \right)$$

$$= e(h \cdot g_2) \cdot e\left( h_0 \prod_{j=1}^{[k]} h_j^{H_t(M)} g_2 \right)$$

$$= e(h, y) \cdot e\left( h_0 \prod_{j=1}^{[k]} h_j^{H_t(M)}, \sigma_2 \right).$$

4.5 Security

Theorem 1. For any fu-cma adversary $A$ against the above forward-secure signature scheme in the random-oracle model for $T = 2^\ell - 1$ time periods, there exists an adversary $B$ with essentially the same running time and advantage in solving the $\ell$-wBDHI$_2$ problem

$$Ad_{G_1 \times G_2}^{\ell \cdot wBDHI_2}(A) \approx 1 - \frac{1}{T} \cdot q_H \cdot Ad_{FS}^{fu-cma}(A) - \frac{q_H^2}{2} \cdot q_H,$$

where $q_H$ is the number of random-oracle queries made by $A$.

We refer the interested reader to Appendix A for the full proof of security.

5 Forward-Secure Multi-Signatures

To obtain a multi-signature scheme, we observe that the component-wise product $(\Sigma_1, \Sigma_2) = (\prod_{i=1}^{[k]} \sigma_{i,1}, \prod_{i=1}^{[k]} \sigma_{i,2})$ of a number of signatures $(\sigma_{1,1}, \sigma_{1,2}), \ldots, (\sigma_{n,1}, \sigma_{n,2})$ satisfies the verification equation with respect of the product of public keys $Y = y_1 \cdot \ldots \cdot y_n$. This method of combining signatures is vulnerable to a rogue-key attack, however, where a malicious signer chooses his public key based on that of an honest signer, so that the malicious signer can compute valid signatures for their aggregated public key. The scheme below borrows a technique due to Ristenpart and Yilek [53] using proofs of possession (denote by $\pi$ below) to prevent against these types of attack.

5.1 Definitions

In addition to the algorithms of a forward-secure signature scheme in Section 4.1, a forward-secure multi-signature scheme $FMS$ in the key verification model has a key generation that additionally outputs a proof $\pi$ for the public key:

- **Key generation**: $(p, \pi, sk_1) \leftarrow Kg$. The key generation algorithm generates a public verification key $pk$, a proof $\pi$, and an initial secret signing key $sk_1$ for the first time period.

and additionally has the following algorithms:

**Key verification**: $b \leftarrow KVf(pk, \pi)$. The key verification algorithm returns 1 if the proof $pk$ is valid for $pk$ and returns 0 otherwise.

**Key aggregation**: $apk \leftarrow KAgg(pk_1, \ldots, pk_n)$. On input a list of individual public keys $(pk_1, \ldots, pk_n)$, the key aggregation returns an aggregate public key $apk$, or $\bot$ to indicate that key aggregation failed.

**Signature aggregation**. $\Sigma \leftarrow SAgg((pk_1, \sigma_1), \ldots, (pk_n, \sigma_n), t, M)$. Anyone can aggregate a given list of individual signatures $(\sigma_1, \ldots, \sigma_n)$ by different signers with public keys $(pk_1, \ldots, pk_n)$ on the same message $M$ and for the same period $t$ into a single multi-signature $\Sigma$.

**Aggregate verification**. $b \leftarrow AVf(apk, t, M, \Sigma)$. Given an aggregate public key $apk$, a message $M$, a time period $t$, and a multi-signature $\Sigma$, the verification algorithm returns 1 to indicate that all signers in $apk$ signed $M$ in period $t$, or 0 to indicate that verification failed.

**Correctness.** Correctness requires that $KVf(pk, \pi) = 1$ with probability one if $(pk, \pi, sk_1) \leftarrow Kg$ and that for all messages $M \in M$, for all $n \in \mathbb{Z}$, and for all time periods $t \in \{0, \ldots, T - 1\}$, it holds that $AVf(apk, t, M, \Sigma) = 1$ with probability one if $(pk_i, \pi_i, sk_{i,1}) \leftarrow Kg$, $apk \leftarrow KAgg(pk_1, \ldots, pk_n)$, $sk_{i,j} \leftarrow Upd(sk_{i,j-1})$ for $i = 1, \ldots, n$ and $j = 2, \ldots, t$, $\sigma_i \leftarrow Sign(sk_{i,j}, M)$ for $i = 1, \ldots, n$, and $\Sigma \leftarrow SAgg((pk_1, \sigma_1), \ldots, (pk_n, \sigma_n), t, M)$.

**Security.** Unforgeability (fu-cma) is defined through a game that is similar to that described in Section 4.1. The adversary is given the public key $pk$ and proof $\pi$ of an honest signer and access to the same key update, signing, and break-in oracles. However, at the end of the game, the adversary’s forgery consists of a list of public keys and proofs $(pk_1^*, \pi_1^*, \ldots, pk_n^*, \pi_n^*)$, a message $M^*$, a time period $t^*$, and a multi-signature $\Sigma^*$. The forgery is considered valid if

- $pk \in \{pk_1^*, \ldots, pk_n^*\}$,
- the proofs $\pi_1^*, \ldots, \pi_n^*$ are valid for public keys $pk_1^*, \ldots, pk_n^*$ according to $KVf$,
- $\Sigma^*$ is valid with respect to the aggregate public key $apk^*$ of $(pk_1^*, \ldots, pk_n^*)$, message $M^*$, and time period $t^*$,
- $t > t^*$,
- and $A$ never made a signing query for $M^*$ during time period $t^*$.
5.2 Construction

Let $H_{G_1} : \{0,1\}^* \rightarrow G_1^*$ be a hash function. The multi-signature scheme reuses the key update and signature algorithms from the scheme from Section 4.3, but uses different key generation and verification algorithms, and adds signature and key aggregation.

**Key generation.** Each signer chooses $x \leftarrow Z_q$ and computes $y \leftarrow g_1^x$ and $y' \leftarrow H_{G_1}(\text{PoP}, y)$, where PoP is a fixed string used as a prefix for domain separation. It sets its public key to $pk = y$, the proof to $\pi = y'$, and computes its initial secret key as $sk_1 \leftarrow h^x$.

**Key verification.** Given a public key $pk = y$ with proof $\pi = y'$, the key verification algorithm validates the proof of possession by returning 1 if

$$e(y', g_2) = e(h, y)$$

and returning 0 otherwise.

**Key aggregation.** Given public keys $pk_1 = y_1, \ldots, pk_n = y_n$, the key aggregation algorithm computes $Y = \prod_{i=1}^n y_i$ and returns the aggregate public key $apk = Y$.

**Signature aggregation.** Given signatures $\sigma_1 = (\sigma_{1,1}, \sigma_{1,2}), \ldots, \sigma_n = (\sigma_{n,1}, \sigma_{n,2}) \in G_1 \times G_2$ on the same message $M$, the signature aggregation algorithm outputs

$$\Sigma = (\Sigma_1, \Sigma_2) = (\prod_{i=1}^n \sigma_{i,1}, \prod_{i=1}^n \sigma_{i,2}) .$$

**Aggregate verification.** Multi-signatures are verified with respect to aggregate public keys in exactly the same way as individual signatures with respect to individual public keys. Namely, given a multi-signature $(\Sigma_1, \Sigma_2) \in G_1 \times G_2$ on message $M$ under aggregate public key $apk = Y$ in time period $t$, the verifier accepts if and only if $apk \neq \bot$ and

$$e(\Sigma_1, g_2) = e(h, Y) \cdot e(h_0 \cdot \prod_{j=1}^t h_j \cdot H_{G_1}(M), \Sigma_2) .$$

5.3 Security

**Theorem 2.** For any fu-cma adversary $A$ against the above forward-secure multi-signature scheme for $T = 2^t - 1$ time periods in the random-oracle model, there exists an adversary $B$ with essentially the same running time that solves the $\ell$-wBDH$_3$ problem with advantage

$$\text{Adv}_{\text{\ell-wBDH}_3^*}^{G_1 \times G_2}(B) \geq \frac{1}{T} \cdot q_H \cdot \text{Adv}_{\text{fu-cma}}^{\text{SS}}(A) - \frac{q_H^2}{2^t} ,$$

where $q_H$ is the number of random-oracle queries made by $A$.

We defer the interested reader to Appendix B for proof details.

6 Pixel in PoS-based Blockchains

In this section, we describe how to integrate Pixel into PoS-based blockchains that rely on forward-secure signatures to achieve security against posterior corruptions. We summarize systems that rely on forward-secure signatures, abstract how signatures are used in these systems, and explain how to apply Pixel.

**PoS Blockchains Secure under Posterior Corruptions.** Ouroboros Genesis and Praos rely on forward-secure signatures to protect against posterior corruptions [5,29,38]. These blockchains require users to rotate key and assume secure erasures. Thuderella is a blockchain with fast optimistic instant confirmation [51]. The blockchain is secure against posterior corruptions assuming that a majority of the computing power is controlled by honest players. Similarly, the protocol relies on forward-secure signatures. Pixel can be applied in all these blockchains to protect against posterior attacks and potentially reduce bandwidth, storage, and computation costs in instances where many users propagate many signatures on the same message (e.g., a block of transactions). Ouroboros Crypsinous uses forward-secure encryption to protect against the same attack [37]. Snow White shows that under a mild setup assumption, when nodes join the system they can access a set of online nodes the majority of whom are honest, the system can defend against posterior corruption attack [28]. The system does not rely on forward-secure signatures.

**Background on PoS Blockchains.** A blockchain is an append-only public ledger to which anyone can write and read. The fundamental problem in blockchains is to agree on a block of transactions between users. In Proof-of-Stake protocols, users map the stake or tokens they own in the system to “voting power” in the agreement protocol. Various types of PoS systems exist that use different formulas for determining the weight of each vote. For instance, in bounded PoS protocols, users must explicitly lock some amount $A$ of their tokens to participate in the consensus. The weight of each vote is $A/Q$, where $Q$ is the total number of locked tokens who’s users wish to participate in the agreement. Users that misbehave are punished by a penalty applied to their locked tokens.

To tolerate malicious users, all PoS protocols run a Byzantine sub-protocol to agree on a block of transactions. The system is secure, assuming that that majority (often 2/3) of the tokens participating in the consensus is honest. Each block is valid if a majority of committee members, weighted by their stake, approved it.

**Pixel Integration.** In order to vote on a block $B$, each member of the sub-protocol signs $B$ using Pixel with the current block number. The consensus is reached when we see a collection of $N$ committee member signatures $\sigma_1, \ldots, \sigma_N$ on the
same block \( B \), where \( N \) is some fixed threshold. Finally, we will aggregate these \( N \) signatures into a single multi-signature \( \Sigma \), and the pair \((B, \Sigma)\) constitute a so-called block certificate and the block \( B \) is appended to the blockchain.

**Registering public keys.** Each user who wishes to participate in consensus needs to register a participation signing key. A user first samples a Pixel key pair and generates a corresponding PoP. The user then issues a special transaction (signed under her spending key) registering the new participation key. The transaction includes PoP. PoS verifiers who are selected to run an agreement at round \( r \), check (a) validity of the special transaction, and (b) validity of PoP. If both checks pass, the user’s account is updated with the new participation key. From this point, if selected, the user signs on blocks using Pixel.

**Vote generation.** To generate a vote on a block number \( t \), users first update their keys to correspond to the round number. Subsequently, they sign the block using the correct secret key and propagate the signature to the network.

**Propagating and aggregating signatures.** Individual committee signatures will be propagated through the network until we see \( N \) committee member signatures on the same block \( B \). Note that Pixel supports non-interactive and incremental aggregation: the former means that signatures can be aggregated by any party after broadcast without communicatiing with the original signers, and the latter means that we can add a new signature to a multi-signature to obtain a new multi-signature. In practice, this means that propagating nodes can perform intermediate aggregation on any number of committee signatures and propagate the result, until the block certificate is formed. Alternatively, nodes can aggregate all signatures just before writing a block to the disk. That is, upon receiving enough certifying votes for a block, a node can aggregate \( N \) committee members’ signatures into a multi-signature and then write the block and the certificate to the disk. To speed up verification of individual committee member signatures, a node could pre-compute \( e(h, y) \) for the \( y \)'s corresponding to the users with the highest stakes.

**Key updates.** When using Pixel in block-chains, time corresponds to the block number or sub-steps in consensus protocols. Naively, when associating time with block numbers, this means that all eligible committee members should update their Pixel secret keys for each time a new block is formed and the round number is updated. Assume for simplicity that each committee member signs at most one block (if not, simply append a counter to the block number and use that as the time). If a user is selected to be on the committee at block number \( t \), it should first update its key to \( sk_t \) (Pixel supports “fast-forward” key updates from \( sk_t \) to \( sk_{t'} \) for any \( t' > t \)), and as soon as it signs a block, updates its key to \( sk_{t+1} \) and then propagates the signature. In particular, there is no need for key updates when a user is not selected to be on the committee.

7 **Evaluation on Algorand Blockchain**

In order to measure the concrete efficiency gains of Pixel, we evaluate it on the Algorand blockchain \([56, 57]\).

**Algorand Overview.** Algorand is a Pure PoS (PPOS) system, where each token is mapped to a single vote in the consensus without any explicit bonding \([56, 57]\). Some users may opt-out from participation, in which case their tokens are excluded from the total number of participating tokens (i.e., the denominator in the weight). Each user maintains an account state on-chain that specifies her spending key, balance, consensus participation status, participation key, and other auxiliary information. A user wishing to perform a transaction must sign it with her corresponding secret key. Users run a Byzantine consensus algorithm to agree on a block of transactions following the high-level structure we outlined in the previous section. We call a block certificate to denote a collection of votes above a certain threshold approving a block. All users in the network validate and store block certificate (and the corresponding transactions) on disk. We refer to a node as a computer system running Algorand client software on the user’s behalf.

**Verifier Vote Structure and Block Certificates.** In Algorand, each valid vote for a block proposal includes (a) a proof that the verifier was indeed selected to participate in the consensus at round \( r \), and (b) a signature on the block proposal. In more detail, each vote includes the following fields:

- Sender identifier which is represented by a unique public key registered on-chain (32 bytes).
- Round and sub-step identifiers (8 bytes).
- Block header proposal (32 bytes).
- A seed used as an input to a VRF function for cryptographic sortition (32 bytes).
- VRF credential that proves that the sender was indeed chosen to sign on the block (96 bytes).
- Forward-secure signature authenticating the vote (256 bytes).

Overall, each vote is about 500 bytes (including some additional auxiliary information), half of which is for the forward-secure signature.

Algorand has two voting sub-steps for each round. In the first sub-step, a supporting set (of expected size 3000) of verifiers is chosen to vote on a block proposal. In the second sub-step, a certifying set (of expected size 1500) of verifiers
is chosen to finalize the block proposal. All verifiers’ votes propagate in the network during the agreement, but only the certifying votes are stored long-term and sufficient to validate a block in the future. Larger recovering set (of expected size 10000) is chosen during a network partition for recovery.

**Algorand’s Existing Solution to Posterior Corruptions.** Algorand solves posterior corruptions using forward-secure signatures instantiated with a $d$-ary certificate tree [9], which we call BM-Ed25519 for convenience. The root public key of an Ed25519 signature scheme is registered on-chain, and keys associated with the leaves (and subsequently used to sign at each round) are stored locally by the potential verifiers. For each block at round $r$ a verifier must (a) produce a valid certificate chain from the root public key to the leaf associated with $r$, and (b) signature of the vote under the leaf key. Algorand assumes secure erasures and that users delete old keys from their nodes. BM-Ed25519 is instantiated with 10000-ary tree of depth 2. BM-BLS is instantiated using the same parameters with public keys in $G_1$ and signatures in $G_2$.

**Table 1:** Total size of signature sets using various forward-secure signature schemes for $2^{32}$ time periods. BM-Ed25519 is instantiated using Algorand’s parameters with 10,000-ary tree of depth 2. BM-BLS is instantiated using the same parameters with public keys in $G_1$ and signatures in $G_2$.

**Storage Savings.** In Table 1, we compare the sizes of signature sets that are propagated (for supporting and verifying votes) and stored (for verifying votes) by all participating nodes. We instantiate BM-Ed25519 with Algorand parameters of 10000-ary and depth 2. For BM-BLS we place the public key in $G_1$ and signatures in $G_2$. Since BLS supports aggregation of signatures, we can compress all signatures in a certificate chain and the signature of the block into 96 B (note that the public key in the certificate chain cannot be compressed and adds an additional 96 B per signature). Furthermore, we can compress all signatures across votes. Pixel signatures authenticating a block with 1500 signatures are 2667x and 1003x times smaller than signature sets using BM-Ed25519 and BM-BLS, respectively. In Figure 3, we show long-term blockchain storage improvements using Pixel signatures. We evaluate storage assuming various number of transactions in each block. Each transaction in Algorand is about 232 bytes. We also assume that the entire expected number of certifying verifiers (1500) are selected for each block. Given today’s block confirmation time of just under 4.3 seconds per block, Algorand blockchain should produce 10^8 blocks every ≈ 50 days and 10^9 blocks every ≈ 13 years. Pixel signatures improve blockchain size by about 40% and 20% on blocks packed with 1500 and 5000 transactions, respectively. This improvement translates to smaller overall storage requirements and faster catch-up speed for new nodes.

**7.1 Efficiency Evaluation**

Pixel signatures can serve as a replacement of BM-Ed25519 in Algorand following the same design as outlined Section 6.

<table>
<thead>
<tr>
<th>Sig. set size</th>
<th>BM-Ed25519</th>
<th>BM-BLS</th>
<th>Pixel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>256 B</td>
<td>192 Bytes</td>
<td>144 B</td>
</tr>
<tr>
<td>1500</td>
<td>375 KB</td>
<td>141 KB</td>
<td>144 B</td>
</tr>
<tr>
<td>3000</td>
<td>750 KB</td>
<td>281 KB</td>
<td>144 B</td>
</tr>
<tr>
<td>10000</td>
<td>2.4 MB</td>
<td>938 KB</td>
<td>144 B</td>
</tr>
</tbody>
</table>

**Figure 2:** Performance figures of the Pixel signature scheme algorithms, and the size of public keys, signatures, and secret keys when using a BLS12-381 curve. $N$ denotes the amount of signatures and keys aggregated, respectively. Maximum number of time periods is $T = 2^{32} - 1$.

| $pk \in G_1$ | keygen | key update | sign $\sigma$ | aggregate $(N = 1500)$ | verify agg. $(N = 1500)$ | aggregate $(N = 1500)$ | verify agg. $(N = 3000)$ | $|pk|$ | $|\sigma|$ | $|sk_1|$ |
|---------------|--------|------------|--------------|------------------------|-------------------------|------------------------|------------------------|------|-------|-------|
| 1.03 ms       | 1.8 ms | 2.8 ms     | 7.2 ms       | 6.7 ms                 | 13.9 ms                | 8.3 ms                | 48 B                   | 144 B | 43 kB |

Table 2: Total size of signature sets using various forward-secure signature schemes for $2^{32}$ time periods. BM-Ed25519 is instantiated using Algorand’s parameters with 10,000-ary tree of depth 2. BM-BLS is instantiated using the same parameters with public keys in $G_1$ and signatures in $G_2$. Verification time. In Pixel, the signature set corresponds to a single multi-signature.
Figure 3: Size of blockchain measured for different total number of blocks. The top two plots assume average of 1500 transactions per block and the bottom plots assume 5000 transactions per block. All plots assume average of 1500 certifying votes per block.

![Blockchain size](image)

Table 2: Total bandwidth to propagate a set of 4500 signatures during consensus to agree on a block of transactions.

<table>
<thead>
<tr>
<th>Number of connections</th>
<th>BM-Ed25519</th>
<th>Pixel</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>4.4 MB</td>
<td>2.5 MB</td>
</tr>
<tr>
<td>10</td>
<td>11 MB</td>
<td>6.2 MB</td>
</tr>
<tr>
<td>100</td>
<td>109.9 MB</td>
<td>61.8 MB</td>
</tr>
</tbody>
</table>

Table 3: Total runtime to verify signature sets authenticating a block. Pixel verification includes the time to aggregate public keys.

<table>
<thead>
<tr>
<th>Sig. set size</th>
<th>BM-Ed25519</th>
<th>Pixel</th>
<th>Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.18 ms</td>
<td>4.9 ms</td>
<td>27x slower</td>
</tr>
<tr>
<td>1500</td>
<td>270 ms</td>
<td>6.7 ms</td>
<td>40x faster</td>
</tr>
<tr>
<td>3000</td>
<td>540 ms</td>
<td>8.3 ms</td>
<td>65x faster</td>
</tr>
<tr>
<td>10000</td>
<td>1.8 sec</td>
<td>15.6 ms</td>
<td>115x faster</td>
</tr>
</tbody>
</table>

Block Verification Time Savings. Since verifying a Pixel multi-signature requires only 3 pairings in addition to multiplying all the public keys in the signature set, they are faster to verify than BM-Ed25519 signatures sets. Table 3 shows that a set of 3000 signatures can be verified about 65x faster. In Figure 4, we measure the overall savings on block verification time. Block verification time is broken into three main intervals: (a) time to verify vote signatures, (b) time to verify vote VRF credentials, and (c) time to verify transactions. In each interval, signature verification dramatically exceeds the time of any additional checks (e.g., check that the transaction amount is higher than the user’s balance). Blocks with 1500 and 5000 transactions can be verified 38% and 29% faster, respectively.

8 Conclusion

In this work, we focus on improving the speed and security of PoS consensus mechanisms via optimizing its core building block – digital signature scheme. We design a new pairing-based forward-secure multi-signature scheme, Pixel. We prove that Pixel is secure in the random oracle model under a variant of Diffie-Hellman inversion problem over bilinear groups. Pixel is efficient as a stand-alone primitive and results in significant performance and size reduction compared to the previous forward-secure signatures applied in settings where multiple users sign the same message (block). For
instance, compared to a set of 1500 tree-based forward-secure signatures, a single Pixel signature that can authenticate the entire set is 2667x smaller and can be verified 40x faster. We explained how to integrate Pixel to any PoS blockchains to solve posterior corruptions problem. We also demonstrate that Pixel provides significant efficiency gains when applied to Algorand blockchain. Pixel signatures reduce the size of Algorand blocks with 1500 transactions by \( \approx 35\% \) and reduce block verification time by \( \approx 38\% \).

Acknowledgments

We would like to thank Zhenfei Zhang for implementing Pixel as well as his help with Section 7. In addition, we thank Jens Groth, Nickolai Zeldovich, our shepherd Ari Juels, and the anonymous reviewers for useful feedback.

References


[34] Timo Hanke, Mahnush Movahedi, and Dominic Williams. Dfinity technology overview series, consensus system, 2018.


We show that the above scheme with mes-

A Security Proof of Forward-Secure Signatures

Proof. We prove the theorem in two steps. First, we show that the scheme is selectively secure when the message space \( M = \{0, 1\}^k \) and \( H_q \) is the identity function, meaning, interpreting a \( k \)-bit string as an integer in \( \mathbb{Z}_q \).

Step 1: sfu-cma. We show that the above scheme with message space \( M = \{0, 1\}^k \) and \( H_q \) the identity function is sfu-cma-secure under the \( \ell \)-wBDHI\(_3\) assumption by describing an algorithm \( B \) that, given a successful sfu-cma forger \( \mathcal{A}' \), solves the \( \ell \)-wBDHI\(_3\) problem. On input \( (A_1 = g_1^{a_1}, A_2 = g_1^{a_2}, \ldots, A_\ell = g_1^{a_\ell}, B_1 = g_2^a, B_2 = g_2^a, \ldots, B_\ell = g_2^a, C) \), algorithm \( B \) proceeds as follows.

It first runs \( \mathcal{A} \) to obtain \( (\bar{t}, \bar{t}^*, M^*) \). That is, \( \mathcal{A} \) receives \( s_k^q \) and produces a forgery on \( t^*, M^* \). Let \( w^* \in \{0, 1, 2\}^{\ell-1} \) such that \( w^* = w_1^* \cdots w_{\ell-1}^* = t^* \| 0^{\ell-1-|t^*|} \). It then sets the public key and public parameters as

\[
\begin{align*}
y & \leftarrow B_1, \\
h & \leftarrow g_1^a, A_t, \\
h_0 & \leftarrow g_1^a, \prod_{i=1}^{\ell-1} A_t^{-w_i^*} \cdot A_t^{-M^*}, \\
h_i & \leftarrow g_1^a, A_{t-i+1}^{-1} & \text{for } i = 1, \ldots, \ell,
\end{align*}
\]

where \( \gamma, \gamma_0, \ldots, \gamma_\ell \in \mathbb{Z}_q \).

By setting the parameters as such, \( B \) implicitly sets \( x = \alpha \) and \( h^* = A_1^\gamma, g_1^{a+1} \). The reduction allows us to achieve two goals:

- extract the value of \( h^* \) from a forgery on \( t^*, M^* \) (provided by \( \mathcal{A}' \)), allowing \( B \) to easily compute its \( \ell \)-wBDHI\(_3\) solution \( e(g_1, C)(a^\ell + 1) \);
- simulate \( \tilde{s}_k^w \) for all \( w' \in \{0, 1, 2\}^{\ell-1} \) which are not a prefix of \( w^* \); this would be useful for simulating both the signing and the break-in oracle.

Algorithm \( B \) responds to \( \mathcal{A}' \)’s oracle queries as follows.

**Key update.** There is no need for \( B \) to simulate anything beyond keeping track of the current time period \( t \).

**Signing.** We first describe how to answer a signing query for a message \( M \) in time period \( t \neq t^* \), and then describe the case that \( t = t^* \) and \( M \neq M^* \). Let \( w \in \{0, 1, 2\}^{\ell-1} \) be such that \( w = t^* \| 0^{\ell-1-|t^*|} \).

Case 1: \( t \neq t^* \). It is easy to see that \( t \neq t^* \implies w \neq w^* \). (This crucially uses the fact that \( t, t^* \in \{1, 2\}^k \).) Then, let \( w^* = w_1^* \cdots w_k^* \) denote the shortest prefix of \( w \) which is not a prefix of \( w^* \). Extending the notation of \( \tilde{s}_k^w \) to \( w^* \in \{0, 1, 2\}^{\ell-1} \), we describe how \( B \) can derive a valid key \( s_k^w \), from which it is straight-forward to derive both \( s_k^w \) and a signature for \( t, M \). Recall that \( s_k^w \) has the structure

\[
(c, d, e_{k+1}, \ldots, e_{\ell}) = \left(g_2^a, h^x(h_0 \prod_{i=1}^k h_i^{w_i^*})^y, h_{k+1}, \ldots, h_{\ell}\right)
\]

for a uniformly distributed value of \( r \). Focusing on the second
component $d$ first, we have that

$$d = h^\tau \left( h_0 \prod_{i=1}^{k} h_i \right)^r$$

$$= (g_1^{\tau} A_\tau)^{\alpha} \cdot \left( \left( \prod_{i=1}^{k} A_{\ell-i+1}^{\mu_i} \right) \prod_{i=k+1}^{\ell} g_1^{\tau} A_{\ell-i+1} \right)^r$$

$$= A_1^{\tau} g_1^{(\ell+1)} \cdot \left( s_1^{\gamma_i \sum_{i=k}^{\ell} w_i} A_{\ell-k+1}^{w_k} \prod_{i=k+1}^{\ell} A_{\ell-i+1}^{w_i} \right)^r,$$

where the third equality holds because $w_i = w_i^\gamma$ for $1 \leq i < k$ and $w_k \neq w_k^\gamma$. (Note that in the product notation $\prod_{i=k+1}^{\ell-1}$ above, we let the result of the product simply be the unity element if $k+1 > \ell-1$.) Let us denote the four factors between parentheses in the last equation as $F_1, F_2, F_3,$ and $F_4$, and denote their product as $F$. If we let

$$r \leftarrow r' + \frac{\alpha^\ell}{w_k^{\gamma} - w_k} \mod q$$

for a random $r' \in \mathbb{Z}_q$, then we have that

$$d = A_1^{\tau} g_1^{(\ell+1)} \cdot F' \cdot F^{w_k^{\gamma} - w_k}.$$  

The first and third factors in this product are easy to compute. The second factor would allow $B$ to compute the solution of the $\ell$-wBDH$_1$ problem as $e(g_1^{(\ell+1)}, C)$, so $B$ cannot simply compute it. The last factor $F^{w_k^{\gamma} - w_k}$ can be written as the product of

$$F_{1,k-k}^{\alpha^\ell} = A_{\ell-k+1}^{w_k^{\gamma} - w_k},$$

$$F_{2,k-k}^{\alpha^\ell} = A_{\ell-k+1}^{w_k^{\gamma} - w_k} = g_1^{-(\ell+1)},$$

$$F_{3,k-k}^{\alpha^\ell} = \prod_{i=k+1}^{\ell} A_{\ell-i+1}^{w_k^{\gamma} - w_k},$$

$$F_{4,k-k}^{\alpha^\ell} = A_{\ell-k+1}^{w_k^{\gamma} - w_k}.$$  

Because $1 \leq k \leq \ell-1$, it is clear that all but the second of these can be computed from $B$’s inputs, and that the second cancels out with the factor $g_1^{-(\ell+1)}$ in $d$, so that it can indeed compute $d$ this way. The other components of the key are also efficiently computable as

$$c = g_2^{\tau} \cdot B_k^{w_k^{\gamma} - w_k},$$

$$e_i = h^{\tau} \cdot A_{\ell-k+1}^{w_k^{\gamma} - w_k} \text{ for } i = k+1, \ldots, \ell$$

$$= h^{\tau} \cdot A_{\ell-i} \text{ for } i = 0, \ldots, \ell - k - 1.$$  

From this key ($c, d, e_{k+1}, \ldots, e_{\ell}$) for $w^\gamma$, $B$ can derive a key for $w$ and compute a signature as in the real signing algorithm.

Case 2: $t = t^*, M \neq M^*$. For a signing query with $t = t^*$ but $M \neq M^*$, $B$ proceeds in a similar way, but derives the signature $(\sigma_1, \sigma_2)$ directly. Algorithm $B$ can generate a valid signature using a similar approach as above, but using the fact that $M \neq M^*$ instead of $w_k \neq w_k^\gamma$. Namely, letting $w = t[0^{\ell-1} - 1]$, $B$ computes a signature

$$\sigma_1 = h^{\tau} \cdot \left( h_0 \prod_{i=1}^{\ell-1} h_i \right)^r$$

$$= (g_1^{\tau} A_\tau)^{\alpha} \cdot \left( \left( \prod_{i=1}^{\ell-1} A_{\ell-i+1}^{w_i} \cdot A_{\ell-i}^{w_i} \right) \prod_{i=k+1}^{\ell} g_1^{\tau} A_{\ell-i+1} \right)^r,$$

$$= A_1^{\tau} g_1^{(\ell+1)} \cdot \left( s_1^{\gamma_i \sum_{i=k+1}^{\ell} w_i + \gamma M} \cdot A_{1}^{M-M^*} \right)^r,$$

by setting

$$r \leftarrow r' + \frac{\alpha^\ell}{M^*-M} \mod q$$

for $r' \in \mathbb{Z}_q$, so that $B$ can compute $(\sigma_1, \sigma_2)$ from its inputs $A_1, \ldots, A_\ell, B_1, \ldots, B_\ell$ similarly to the case that $t \neq t^*$.

**Break in.** Here, $B$ needs to simulate $sk_{t^*}$ where $t^* \neq t$. This in turn requires simulating $sk_{w^\gamma}$ for all $w \in \mathcal{G}_1$. By the first property of $\mathcal{G}_1$ (described in Section 4.2), all of these $w$ are not prefixes of $t^*$ and also not prefixes of $w^\gamma$, and we can therefore simulate $sk_w$ exactly as before.

**Forgery.** When $A'$ outputs a forgery $(\sigma_1', \sigma_2')$ that satisfies the verification equation

$$e(\sigma_1', g_2) = e(h, y) \cdot e(h_0 \cdot \prod_{i=1}^{\ell} h_i^{t^*} \cdot h_{t^*}^{M^*}, \sigma_2') ,$$

then there exists an $r \in \mathbb{Z}_q$ such that

$$\sigma_1' = h^{\tau} \cdot \left( h_0 \prod_{i=1}^{\ell} h_i^{t^*} \right)^r$$

$$\sigma_2' = g_2^r.$$  

From the way that $B$ chose the parameters $h, h_0, \ldots, h_\ell$, one can see that

$$\sigma_1' = A_1^{\tau} g_1^{(\ell+1)} \cdot (g_1^\gamma \cdot (s_1^{\gamma_i \sum_{i} w_i + Y M^*}) \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2'),$$

Note that we do not know $g_1^\gamma$, so we cannot directly extract $g_1^{(\ell+1)}$ from $\sigma_1'$. Instead, observe that we have

$$e(\sigma_1', C_2) = e(A_1^{\tau} g_1^{(\ell+1)} C_2) \cdot e(g_1^{(\ell+1)} C_2) \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2') \cdot e(C_1, \sigma_2'),$$

where $\sigma_1'$ is a forgery for $t^*$, and $\sigma_2'$ is a forgery for $t^*$. $B$ can then use $\sigma_1'$ and $\sigma_2'$ to break $sk_{t^*}$.
from which $B$ can easily compute its output $e(g_1^{(q_2+1)}, C_2) = e(g_1, g_2)^{(q_2+1)}$. It does so whenever $A'$ is successful, so that

$$\text{Adv}^{\text{sfu-cma} \cdot \text{w-BDH}\cdot}(B) \geq \text{Adv}^{\text{sfu-cma} \cdot \text{w-BDH}\cdot}(A') .$$

Step 2: fu-cma. Full fu-cma security for $M = \{0,1\}^*$ and with $H_q : M \rightarrow \{0,1\}^k$ modeled as a random oracle then follows because, given an fu-cma adversary $A$ in the random-oracle model, one can build a sfu-cma adversary $A'$ that guesses the the time period $t^*$ and index of $A$'s random-oracle query for $H_q(M^*)$, and sets $t = t^* + 1$. If $A'$ correctly guesses $t^*$, then it can use $sk_2$ to simulate $A$'s signature, key update, and break-in queries after time $t$, until $A$'s choice of break-in time $t'$, at which point it can hand over $sk_2$.

If $A'$ moreover correctly guesses the index of $H_q(M^*)$, and if $A$ never made colliding queries $H_q(M) = H_q(M')$ for $M \neq M'$, then $A$'s forgery is also a valid forgery for $A'$. Note that for $A$ to be successful, it must hold that $t' > t^*$, so it must hold that $t^* \geq t$. The advantage of $A'$ is

$$\text{Adv}^{\text{sfu-cma} \cdot \text{w-BDH}\cdot}(A') \geq \frac{1}{T \cdot q_H} \cdot \text{Adv}^{\text{sfu-cma} \cdot \text{w-BDH}\cdot}(A) - \frac{q_H}{2^k} ,$$

where $q_H$ is an upper bound on $A$'s number of random-oracle queries. Together with Equation (3), we obtain the inequality of the theorem statement.

B Security Proof of Forward-Secure Multi-signatures

Proof. We show how to construct a forger $A$ for the multi-signature scheme yields a forger $A'$ for the single-signer scheme of Section 4.3 such that

$$\text{Adv}^{\text{sfu-cma} \cdot \text{w-BDH}\cdot}(A') \geq \text{Adv}^{\text{sfu-cma} \cdot \text{w-BDH}\cdot}(A) .$$

The theorem then follows from Theorem 1.

Step 1: simulating $A$'s view. On input the parameters $(T, h, h_0, \ldots, h_n)$ and a public key $y$ for the single-signer scheme, the single-signer forger $A$ chooses $r \leftarrow \mathbb{Z}_q^*$ and stores $(y, \perp, g_1^r)$ in a list $L$. It computes $y' = y^r$ and runs $A$ on the same public parameters and target public key $pk = y$ and proof $\pi = y'$. Observe that $\pi$ is indeed a valid proof for $pk$ since $e(y', g_2) = e(H_{G_1}(\mathcal{P} \ell \mathcal{P}, y), y)$.

Algorithm $A'$ answers all of $A$'s key update, signing, and break-in oracle queries, as well as random-oracle queries for $H_q$, by simply relaying queries and responses to and from $A$'s own oracles. Queries to the random oracle for $H_{G_1}$ are answered as follows.

Random oracle $H_{G_1}$. On input $(\mathcal{P} \ell \mathcal{P}, z)$, $A'$ checks whether there already exists a tuple $(z, r, v) \in L$. If so, it returns $v$. If not, it chooses $r \leftarrow \mathbb{Z}_q^*$, computes $v = h^r$, adds a tuple $(z, r, v)$ to $L$ and returns $v, y$.

Step 2: extracting a forgery. When $A$ outputs its forgery

$$(pk_1^*, \pi_1^*, \ldots, pk_n^*, \pi_n^*), M^*, t', \Sigma^* ,$$

algorithm $A'$ first verifies the proofs $\pi_1^*, \ldots, \pi_n^*$ for public keys $pk_1^*, \ldots, pk_n^*$ and computes the aggregate public key $apk^*$, creating additional entries in $L$, if necessary. Let $pk_i^* = y_i = g_2^i$ and $\pi_i^* = \pi_i^*$. Looking ahead, if $pk_i^*$ passes key verification, then we have that $\pi_i^*(h^r)^{y_i}$ and since we know $r_i$, we will be able to "extract" $h^{y_i} \in G_1$.

If all keys are valid, then it holds that $\pi_i^* = H_{G_1}(\mathcal{P} \ell \mathcal{P}, y_i)^{y_i}$ for all $i = 1, \ldots, n$. Let $apk^* = Y$ be the aggregate public key. From the aggregate verification equation

$$e(\Sigma_1, g_2) = e(h, Y) \cdot e(h_0, \prod_{j=1}^{\ell} h_j^{y_j} h_{y_j}^{H_q(M^*)}, \Sigma_2^*)$$

and the fact that $Y = \prod_{i=1}^{\ell} y_i = y \cdot g_2^{\sum_{i=1}^{\ell} y_i d_{y_i}^{y_i}}$, we have that

$$e(\Sigma_1, g_2) = e(h, y_i) \cdot e(h, g_2)^{\sum_{i=1}^{\ell} y_i d_{y_i}^{y_i}} .$$

$$e(h_0, \prod_{j=1}^{\ell} h_j^{y_j} h_{y_j}^{H_q(M^*)}, \Sigma_2^*) \leftrightarrow e(\Sigma_1, h^{\sum_{i=1}^{\ell} y_i d_{y_i}^{y_i}}, g_2) = e(h, y_i) .$$

$$e(h_0, \prod_{j=1}^{\ell} h_j^{y_j} h_{y_j}^{H_q(M^*)}, \Sigma_2^*) .$$

For all $y_i \neq y$, $A'$ looks up the tuple $(y_i, r_i, v_i)$ in $L$. We know that $v_i = h^{r_i}$, and hence that $\pi_i^* = h^r_i$. By comparing the last equation above to the verification equation of the single-signer scheme, and by observing that $\pi_i^* = h^{r_i}$, we know that the pair

$$\sigma_1^* \leftarrow \Sigma_1 \cdot \prod_{i=1, i \neq y}^{\ell} y_i^{-1/r_i}$$

$$\sigma_2^* \leftarrow \Sigma_2$$

is a valid forgery for the single-signer scheme, so $A'$ can output $M^*, t', (\sigma_1^*, \sigma_2^*)$ as its forgery. \qed