Supplementary material: Generalized Bitcoin-Compatible Channels

A. Additional material to generalized channel protocol

We now formally describe the protocol for generalized channels Π described on high level in Section III of the paper. The protocol internally uses a secure adaptor signature scheme $\Xi_{R,\Sigma} = (\mathsf{pSign}, \mathsf{Adapt}, \mathsf{pVrfy}, \mathsf{Ext})$ for the ledger signature scheme Σ and a relation R. We assume that statement/witness pairs of R are public/secret key of Σ. More precisely, we assume there exists a function ToKey that takes as input a statement $Y \in L_R$ and outputs a public key pk. The function is s.t. the distribution of $(\mathsf{ToKey}(Y), y)$, for $(Y, y) \leftarrow \mathsf{GenR}$, is equal to the distributions of $(pk, sk) \leftarrow \mathsf{Gen}$. We emphasize that both ECDSA and Schnorr based adaptor signatures, that we presented in Section -G of this supplementary material, satisfy this condition (ECDSA, the ToKey simply drops the NIZK, for Schnorr ToKey is the identity function). We discuss how to modify our protocol if this assumption does not hold in Remark 1 below the formal protocol description. Before we present our protocols, we introduce some conventions.

We assume that each party $P \in \mathcal{P}$ maintains a set Γ^P of all open channels together with auxiliary information about the channel (such as the funding transaction, latest commit transaction and corresponding revocation secret etc.). In addition to the channel set, we assume that each party maintains a set Θ^P containing all revoked commit transactions and corresponding revocation secretes. Similarly to the the formal description of the ideal functionality, we make use of a arrow notation for sending and receiving messages. Moreover, our formal description excludes some natural check an honest party should make. Those checks are define as a protocol wrapper in Section -D of this supplementary material.

In order to distinguish between the communication between parties and input/outputs from/to the environment, we use lowercase letter for the former and uppercase typewriter typestyle for the latter. So for example "CREATE" denotes a message from the environment while "createInfo" denotes a protocol message.

Generalized channel protocol

Below, we abbreviate $Q := \gamma.\mathsf{otherParty}(P)$ for $P \in \gamma.\mathsf{users}$.

Create

Party P upon $(\texttt{CREATE}, \gamma, tid_P) \xleftarrow{t_0} \mathcal{E}$:

1) Set $id := \gamma.\mathsf{id}$, generate $(R_P, r_P) \leftarrow \mathsf{GenR}$, $(Y_P, y_P) \leftarrow \mathsf{GenR}$ and send $(\text{createInfo}, id, tid_P, R_P, Y_P) \xhookrightarrow{t_0} Q$.
2) If $(\text{createInfo}, id, tid_Q, R_Q, Y_Q) \xhookleftarrow{t_0+1} Q$, create:
$$[\texttt{TX}_\texttt{f}] := \texttt{GenFund}((tid_P, tid_Q), \gamma)$$
$$[\texttt{TX}_\texttt{c}] := \texttt{GenCom}([\texttt{TX}_\texttt{f}], I_P, I_Q, 0)$$
$$[\texttt{TX}_\texttt{s}] := \texttt{GenSplit}([\texttt{TX}_\texttt{c}].\mathsf{txid} \| 1, \gamma.\mathsf{st})$$
for $I_P := (pk_P, R_P, Y_P)$, $I_Q := (pk_Q, R_Q, Y_Q)$. Else stop.
3) Compute $s_\texttt{c}^P \leftarrow \mathsf{pSign}_{sk_P}([\texttt{TX}_\texttt{c}], Y_Q)$, $s_\texttt{s}^P \leftarrow \mathsf{Sign}_{sk_P}([\texttt{TX}_\texttt{s}])$ and send $(\text{createCom}, id, s_\texttt{c}^P, s_\texttt{s}^P) \xhookrightarrow{t_0+1} Q$.
4) If $(\text{createCom}, id, s_\texttt{c}^Q, s_\texttt{s}^Q) \xhookleftarrow{t_0+2} Q$, s.t. $\mathsf{pVrfy}_{pk_Q}([\texttt{TX}_\texttt{c}], Y_P; s_\texttt{c}^Q) = 1$ and $\mathsf{Vrfy}_{pk_Q}([\texttt{TX}_\texttt{s}]; s_\texttt{s}^Q) = 1$, $s_\texttt{f}^P \leftarrow \mathsf{Sign}_{sk_P}([\texttt{TX}_\texttt{f}])$ and send $(\text{createFund}, id, s_\texttt{f}^P) \xhookrightarrow{t_0+2} Q$. Else stop.
5) If $(\text{createFund}, id, s_\texttt{f}^Q) \xhookleftarrow{t_0+3} Q$, s.t. $\mathsf{Vrfy}_{pk_Q}([\texttt{TX}_\texttt{f}]; s_\texttt{f}^Q) = 1$, $\texttt{TX}_\texttt{f} := ([\texttt{TX}_\texttt{f}], \{s_\texttt{f}^P, s_\texttt{f}^Q\})$ and $(\text{post}, \texttt{TX}_\texttt{f}) \xhookrightarrow{t_0+3} \mathcal{L}$. Else parse $(\theta_P, \theta_Q) := \gamma.\mathsf{st}$, create tx such that $\mathsf{tx.Input} := tid_P$, $\mathsf{tx.Output} := \theta_P$, $\mathsf{tx}.w \leftarrow \mathsf{Sign}_{pk_P}([\mathsf{tx}])$ and $(\text{post}, \mathsf{tx}) \xhookrightarrow{t_0+3} \mathcal{L}$.
6) If $\texttt{TX}_\texttt{f}$ is accepted by $\mathcal{L}$ in round $t_1 \leq t_0 + 3 + \Delta$, set $\texttt{TX}_\texttt{c} := ([\texttt{TX}_\texttt{c}], \{\mathsf{Sign}_{sk_P}([\texttt{TX}_\texttt{c}]), \mathsf{Adapt}(s_\texttt{c}^Q, y_P)\})$, $\texttt{TX}_\texttt{s} := ([\texttt{TX}_\texttt{s}], \{s_\texttt{s}^P, s_\texttt{s}^Q\})$, store $\Gamma^P(\gamma.\mathsf{id}) := (\gamma, \texttt{TX}_\texttt{f}, (\texttt{TX}_\texttt{c}, r_P, R_Q, Y_Q, s_\texttt{c}^P), \texttt{TX}_\texttt{s})$ and $(\texttt{CREATED}, id) \xhookrightarrow{t_1} \mathcal{E}$.

Update

Party P upon $(\texttt{UPDATE}, id, \vec{\theta}, t_\mathsf{stp}) \xhookleftarrow{t_0} \mathcal{E}$

1) Generate $(R_P, r_P) \leftarrow \mathsf{GenR}$, $(Y_P, y_P) \leftarrow \mathsf{GenR}$ and send $(\text{updateReq}, id, \vec{\theta}, t_\mathsf{stp}, R_P, Y_P) \xhookrightarrow{t_0} Q$.

Party Q upon $(\text{updateReq}, id, \vec{\theta}, t_\mathsf{stp}, R_P, Y_P) \xhookleftarrow{\tau_0} P$

2) Generate $(R_Q, r_Q) \leftarrow \mathsf{GenR}$ and $(Y_Q, y_Q) \leftarrow \mathsf{GenR}$.
3) Set $t_\mathsf{lock} := \tau_0 + t_\mathsf{stp} + 4 + \Delta$, extract $\texttt{TX}_\texttt{f}$ from $\Gamma^P(id)$ and
$$[\texttt{TX}_\texttt{c}] := \texttt{GenCom}([\texttt{TX}_\texttt{f}], I_P, I_Q, t_\mathsf{lock})$$
$$[\texttt{TX}_\texttt{s}] := \texttt{GenSplit}([\texttt{TX}_\texttt{c}].\mathsf{txid} \| 1, \vec{\theta})$$
where $I_P := (pk_P, R_P, Y_P)$, $I_Q := (pk_Q, R_Q, Y_Q)$.
4) Sign $s_\texttt{s}^Q \leftarrow \mathsf{Sign}_{sk_Q}([\texttt{TX}_\texttt{s}])$, send $(\text{updateInfo}, id, R_Q, Y_Q, s_\texttt{s}^Q) \xhookrightarrow{\tau_0} P$, $(\texttt{UPDATE–REQ}, id, \vec{\theta}, t_\mathsf{stp}, \texttt{TX}_\texttt{s}.\mathsf{txid}) \xhookrightarrow{\tau_0+1} \mathcal{E}$.

Party P upon $(\text{updateInfo}, id, h_Q, Y_Q, s_\texttt{s}^Q) \xhookleftarrow{t_0+2} Q$

5) Set $t_\mathsf{lock} := t_0 + t_\mathsf{stp} + 5 + \Delta$, extract $\texttt{TX}_\texttt{f}$ from $\Gamma^Q(id)$ and
$$[\texttt{TX}_\texttt{c}] := \texttt{GenCom}([\texttt{TX}_\texttt{f}], I_P, I_Q, t_\mathsf{lock})$$
$$[\texttt{TX}_\texttt{s}] := \texttt{GenSplit}([\texttt{TX}_\texttt{c}].\mathsf{txid} \| 1, \vec{\theta}),$$
for $I_P := (pk_P, R_P, Y_P)$ and $I_Q := (pk_Q, R_Q, Y_Q)$. If $\mathsf{Vrfy}_{pk_Q}([\texttt{TX}_\texttt{s}]; s_\texttt{s}^Q) = 1$, $(\texttt{SETUP}, id, \texttt{TX}_\texttt{s}.\mathsf{txid}) \xhookrightarrow{t_0+2} \mathcal{E}$. Else stop.

6) If $(\texttt{SETUP-OK}, id) \xleftarrow{t_1 \le t_0+2+t_{\mathsf{stp}}} \mathcal{E}$, compute $s_{\mathtt{c}}^P \leftarrow \mathsf{pSign}_{sk_P}([\mathtt{TX}_{\mathtt{c}}], Y_Q) s_{\mathtt{s}}^P \leftarrow \mathsf{Sign}_{sk_P}([\mathtt{TX}_{\mathtt{s}}])$ and send $(\text{updateComP}, id, s_{\mathtt{c}}^P, s_{\mathtt{s}}^P) \xhookrightarrow{t_1} Q$. Else stop.

Party Q

7) If $(\text{updateComP}, id, s_{\mathtt{c}}^P, s_{\mathtt{s}}^P) \xleftarrow{\tau_1 \le \tau_0+2+t_{\mathsf{stp}}} P$, s.t. $\mathsf{pVrfy}_{pk_P}([\mathtt{TX}_{\mathtt{c}}], Y_Q; s_{\mathtt{c}}^P) = 1$ and $\mathsf{Vrfy}_{pk_P}([\overline{\mathtt{TX}}_{\mathtt{s}}]; s_{\mathtt{s}}^P) = 1$, output $(\texttt{SETUP-OK}, id) \xhookrightarrow{\tau_1} \mathcal{E}$. Else stop.
8) If $(\texttt{UPDATE-OK}, id) \xleftarrow{\tau_1} \mathcal{E}$, pre-sign $s_{\mathtt{c}}^Q \leftarrow \mathsf{pSign}([\mathtt{TX}_{\mathtt{c}}], Y_P)$ and send $(\text{updateComQ}, id, s_{\mathtt{c}}^Q) \xhookrightarrow{\tau_1} P$. Else send $(\text{updateNotOk}, id, r_Q) \xhookrightarrow{\tau_1} P$ and stop.

Party P

9) In round $t_1 + 2$ distinguish the following cases:
   - If $(\text{updateComQ}, id, s_{\mathtt{c}}^Q) \xleftarrow{t_1+2} Q$, s.t. $\mathsf{pVrfy}_{pk_Q}([\mathtt{TX}_{\mathtt{c}}], Y_P; s_{\mathtt{c}}^Q) = 1$, output $(\texttt{UPDATE-OK}, id) \xhookrightarrow{t_1+2} \mathcal{E}$.
   - If $(\text{updateNotOk}, id, r_Q) \xleftarrow{t_1+2} Q$, s.t. $(R_Q, r_Q) \in R$, add $\Theta^P(id) := \Theta^P(id) \cup ([\mathtt{TX}_{\mathtt{c}}], r_Q, Y_Q, s_{\mathtt{c}}^P)$ and stop.
   - Else, execute the procedure $\texttt{ForceClose}^P(id)$ and stop.
10) If $(\texttt{REVOKE}, id) \xleftarrow{t_1+2} \mathcal{E}$, parse $\Gamma^P(id)$ as $(\gamma, \mathtt{TX}_{\mathtt{f}}, (\overline{\mathtt{TX}}_{\mathtt{c}}, \bar{r}_P, \bar{R}_Q, \bar{Y}_Q, \bar{s}_{\mathtt{Com}}^P), \overline{\mathtt{TX}}_{\mathtt{s}})$ and update the channel space as $\Gamma^P(id) := (\gamma, \mathtt{TX}_{\mathtt{f}}, (\mathtt{TX}_{\mathtt{c}}, r_P, R_Q, Y_Q, s_{\mathtt{c}}^P), \mathtt{TX}_{\mathtt{s}})$, for $\mathtt{TX}_{\mathtt{s}} := ([\mathtt{TX}_{\mathtt{s}}], \{s_{\mathtt{s}}^P, s_{\mathtt{s}}^Q\})$ and $\mathtt{TX}_{\mathtt{c}} := ([\mathtt{TX}_{\mathtt{c}}], \{\mathsf{Sign}_{sk_P}([\mathtt{TX}_{\mathtt{c}}]), \mathsf{Adapt}(s_{\mathtt{c}}^Q, y_P)\})$., and send $(\text{revokeP}, id, \bar{r}_P) \xhookrightarrow{t_1+2} Q$. Else, execute $\texttt{ForceClose}^P(id)$ and stop.

Party Q

11) Parse $\Gamma^Q(id)$ as $(\gamma, \mathtt{TX}_{\mathtt{f}}, (\overline{\mathtt{TX}}_{\mathtt{c}}, \bar{r}_Q, \bar{R}_P, \bar{Y}_P, \bar{s}_{\mathtt{Com}}^Q), \overline{\mathtt{TX}}_{\mathtt{s}})$. If $(\text{revokeP}, id, \bar{r}_P) \xleftarrow{\tau_1+2} P$, s.t. $(\bar{R}_P, \bar{r}_P) \in R$, $(\texttt{REVOKE-REQ}, id) \xhookrightarrow{\tau_1+2} \mathcal{E}$. Else execute $\texttt{ForceClose}^Q(id)$ and stop.
12) If $(\texttt{REVOKE}, id) \xleftarrow{\tau_1+2} \mathcal{E}$ as a reply, set

$$\Theta^Q(id) := \Theta^Q(id) \cup ([\overline{\mathtt{TX}}_{\mathtt{c}}], \bar{r}_P, \bar{Y}_P, \bar{s}_{\mathtt{Com}}^Q)$$
$$\Gamma^Q(id) := (\gamma, \mathtt{TX}_{\mathtt{f}}, (\mathtt{TX}_{\mathtt{c}}, r_Q, R_P, Y_P, s_{\mathtt{c}}^Q), \mathtt{TX}_{\mathtt{s}}),$$

for $\mathtt{TX}_{\mathtt{s}} := ([\mathtt{TX}_{\mathtt{s}}], \{s_{\mathtt{s}}^P, s_{\mathtt{s}}^Q\})$, $\mathtt{TX}_{\mathtt{c}} := ([\mathtt{TX}_{\mathtt{c}}], \{\mathsf{Sign}_{sk_Q}([\mathtt{TX}_{\mathtt{c}}]), \mathsf{Adapt}(s_{\mathtt{c}}^P, y_Q)\})$, and send $(\text{revokeQ}, id, \bar{r}_Q) \xhookrightarrow{\tau_1+2} P$. In the next round $(\texttt{UPDATED}, id) \xhookrightarrow{\tau_1+3} \mathcal{E}$ and stop. Else, in round $\tau_1 + 2$, execute $\texttt{ForceClose}^Q(id)$ and stop.

Party P

13) If $(\text{revokeQ}, id, \bar{r}_Q) \xleftarrow{t_1+4} Q$ s.t. $(\bar{R}_Q, \bar{r}_Q) \in R$, then set $\Theta^P(id) := \Theta^P(id) \cup ([\overline{\mathtt{TX}}_{\mathtt{c}}], \bar{r}_Q, \bar{Y}_Q, \bar{s}_{\mathtt{Com}}^P)$ and $(\texttt{UPDATED}, id) \xhookrightarrow{t_1+4} \mathcal{E}$. Else execute $\texttt{ForceClose}^P(id)$ and stop.

Close

Party P upon $(\texttt{CLOSE}, id) \xleftarrow{t_0} \mathcal{E}$

1) Extract $\mathtt{TX}_{\mathtt{f}}$ and $\mathtt{TX}_{\mathtt{s}}$ from $\Gamma^P(id)$ and set:

$$[\overline{\mathtt{TX}}_{\mathtt{s}}] := \mathtt{GenSplit}(\mathtt{TX}_{\mathtt{f}}.\mathsf{txid} \| 1, \mathtt{TX}_{\mathtt{s}}.\mathsf{Output})$$

2) Compute $s_{\mathtt{s}}^P \leftarrow \mathsf{Sign}_{sk_P}([\overline{\mathtt{TX}}_{\mathtt{s}}])$ and send $s_{\mathtt{s}}^P \xhookrightarrow{t_0} Q$.
3) If $s_{\mathtt{s}}^Q \xleftarrow{t_0+1} Q$ s.t. $\mathsf{Vrfy}_{pk_Q}([\overline{\mathtt{TX}}_{\mathtt{s}}]; s_{\mathtt{s}}^Q) = 1$, set $\overline{\mathtt{TX}}_{\mathtt{s}} := ([\overline{\mathtt{TX}}_{\mathtt{s}}], \{s_{\mathtt{s}}^P, s_{\mathtt{s}}^Q\})$ and send $(\text{post}, \overline{\mathtt{TX}}_{\mathtt{s}}) \xrightarrow{t_0+1} \mathcal{L}$. Else, execute $\texttt{ForceClose}^P(id)$ and stop.
4) Let $t_2 \le t_1 + \Delta$ be the round in which $\overline{\mathtt{TX}}_{\mathtt{s}}$ is accepted by $\mathcal{L}$. Set $\Gamma^P(id) := \bot$, $\Theta^P(id) := \bot$ and send $(\texttt{CLOSED}, id) \xhookrightarrow{t_2} \mathcal{E}$.

Punish

Party P upon $\texttt{PUNISH} \xleftarrow{t_0} \mathcal{E}$:

For each $id \in \{0,1\}^*$ s.t. $\Theta^P(id) \neq \bot$:

1) Parse $\Theta^P(id) := \{([\mathtt{TX}_{\mathtt{c}}^{(\mathrm{i})}], r_Q^{(i)}, Y_Q^{(i)}, s^{(i)})\}_{i \in m}$ and extract γ from $\Gamma^P(id)$. If for some $i \in [m]$, there exist a transaction tx on $\mathcal{L}$ such that $\mathsf{tx}.\mathsf{txid} = \mathtt{TX}_{\mathtt{c}}^{(\mathrm{i})}.\mathsf{txid}$, then parse the witness as $(s_P, s_Q) := \mathsf{tx}.\mathsf{Witness})$, where $\mathsf{Vrfy}_{pk_P}([\mathsf{tx}]; s_P) = 1$, and set $y_Q^{(i)} := \mathsf{Ext}(s_P, s^{(i)}, Y_Q^{(i)})$.
2) Define the body of the punishment transaction $[\mathtt{TX}_{\mathtt{pun}}]$ as:

$$\mathtt{TX}_{\mathtt{pun}}.\mathsf{Input} := \mathsf{tx}.\mathsf{txid} \| 1,$$
$$\mathtt{TX}_{\mathtt{pun}}.\mathsf{Output} := \{(\gamma.\mathsf{cash}, \mathsf{One\text{-}Sig}_{pk_P})\}$$

3) Sign $s_y \leftarrow \mathsf{Sign}_{y_Q^{(i)}}([\mathtt{TX}_{\mathtt{pun}}]), s_r \leftarrow \mathsf{Sign}_{r_Q^{(i)}}([\mathtt{TX}_{\mathtt{pun}}]), s_P \leftarrow \mathsf{Sign}_{pk_P}([\mathtt{TX}_{\mathtt{pun}}])$, and set $\mathtt{TX}_{\mathtt{pun}} := ([\mathtt{TX}_{\mathtt{pun}}], s_y, s_r, s_P)$. Then $(\text{post}, \mathtt{TX}_{\mathtt{pun}}) \xhookrightarrow{t_0} \mathcal{L}$.
4) Let $\mathtt{TX}_{\mathtt{pun}}$ be accepted by $\mathcal{L}$ in round $t_1 \le t_0 + \Delta$. Set $\Theta^P(id) := \bot$, $\Gamma^P(id) := \bot$ and output $(\texttt{PUNISHED}, id) \xhookrightarrow{t_1} \mathcal{E}$.

Subprocedures

$\mathtt{GenFund}(\vec{tid}, \gamma)$:
Return $[\mathsf{tx}]$, where $\mathsf{tx}.\mathsf{Input} := \vec{tid}$ and $\mathsf{tx}.\mathsf{Output} := \{(\gamma.\mathsf{cash}, \mathtt{Multi\text{-}Sig}_{\gamma.\mathsf{users}})\}$.

$\mathtt{GenCom}([\mathtt{TX}_{\mathtt{f}}], (pk_P, R_P, Y_P), (pk_Q, R_Q, Y_Q), t)$:
Let $(c, \mathtt{Multi\text{-}Sig}_{pk_P, pk_Q}) := \mathtt{TX}_{\mathtt{f}}.\mathsf{Output}[1]$ and denote

$$\varphi_1 := \mathtt{Multi\text{-}Sig}_{\mathsf{ToKey}(R_Q), \mathsf{ToKey}(Y_Q), pk_P},$$
$$\varphi_2 := \mathtt{Multi\text{-}Sig}_{\mathsf{ToKey}(R_P), \mathsf{ToKey}(Y_P), pk_Q},$$
$$\varphi_3 := \mathtt{CheckRelative}_{\Delta} \wedge \mathtt{Multi\text{-}Sig}_{pk_P, pk_Q}.$$

Return $[\mathsf{tx}]$, where $\mathsf{tx}.\mathsf{Input} = \mathtt{TX}_{\mathtt{f}}.\mathsf{txid} \| 1$, $\mathsf{tx}.\mathsf{Output} := (c, \varphi_1 \vee \varphi_2 \vee \varphi_3)$ and set $\mathsf{tx}.\mathsf{TimeLock}$ to t if $t > \mathsf{now}$ and to 0 otherwise.

$\mathtt{GenSplit}(tid, \vec{\theta})$:
Return $[\mathsf{tx}]$, where $\mathsf{tx}.\mathsf{Input} := tid$ and $\mathsf{tx}.\mathsf{Output} := \vec{\theta}$.

$\texttt{ForceClose}^P(id)$:
Let t_0 be the current round.
1) Extract $\mathtt{TX}_{\mathtt{c}}$ and $\mathtt{TX}_{\mathtt{s}}$ from $\Gamma(id)$.
2) Wait until round $t_1 := \max\{t_0, \mathtt{TX}_{\mathtt{c}}.\mathsf{TimeLock}\}$ and send $(\text{post}, \mathtt{TX}_{\mathtt{c}}) \xhookrightarrow{t_1} \mathcal{L}$.
3) Let $t_2 \le t_1 + \Delta$ be the round in which $\mathtt{TX}_{\mathtt{c}}$ is accepted by the blockchain. Wait for Δ rounds to $(\text{post}, \mathtt{TX}_{\mathtt{s}}) \xrightarrow{t_2+\Delta} \mathcal{L}$.
4) Once $\mathtt{TX}_{\mathtt{s}}$ is accepted by $\mathcal{L}$ in round $t_3 \le t_2 + 2\Delta$, set $\Theta^P(id) := \bot$ and $\Gamma^P(id) := \bot$ and output $(\texttt{CLOSED}, id) \xhookrightarrow{t_3} \mathcal{E}$.

Remark 1. *In the protocol described in this section, we assume statement/witness pairs of R are valid keys pair. This assumption can be eliminated by modifying our protocol as follows. When creating a new commit transaction, each party samples the publishing pair $(Y_P, y_P) \leftarrow \mathsf{GenR}$ and chooses a random revocation secret r_P. Thereafter, it computes a hash of both secrets as $h_P := \mathcal{H}(r_P)$ and $H_P := \mathcal{H}(y_P)$ and*

*sends Y_P **and the hash values** h_P, H_P to the other party. In addition, it proves in zero knowledge the consistency of Y_P and H_P. The punishment mechanism for party P in the commit transaction then expects (i) a preimage of h_P (ii) a preimage of H_P and (iii) valid signature w.r.t. pk_Q.*

Theorem 2. *Let Σ be a* SUF–CMA *secure signature scheme, R a hard relation and $\Xi_{R,\Sigma}$ a secure adaptor signature scheme. Then for any ledger delay $\Delta \in \mathbb{N}$, the protocol Π UC-realizes the ideal functionality $\mathcal{F}(3,1)$.*

B. Towards fungibility

When designing applications using blockchains, one metric to keep in mind is *fungibility* of transactions, which, on high level, requires all output scripts on the ledger to look the same. This is a way how to prevent miner blocking certain applications, e.g. refusing to include any transaction belonging to an off-chain channel. To this end, off-chain protocol designs aim to (i) use signature verification only and (ii) reduce the number of required signature for each transaction.

Threshold cryptography is a very useful tool when it comes to combining signatures. For example, the number of required signature in a funding transaction of a payment channel can be reduced to one by leveraging a 2-of-2 threshold signature scheme. On a high level, such scheme allows two parties to jointly generate a key pair and jointly generate signatures under those keys. Importantly, both parties have to participate in the signing process to produce a valid signature. Hence, for the cost of a more complex off-chain protocol, funding transaction cannot be distinguished from a basic transaction that assigns coins to a public key.

In order to achieve the same for our generalized channel construction, we need a 2-of-2 threshold variant of an adaptor signature scheme. Intuitively, such scheme allows two parties to jointly generate a pre-signature that (i) could be completed by an adopter knowing a witness of the statement embedded in the signature and (ii) once completed, would be a valid signature 2-of-2 signature. Let us emphasize that concrete constructions (for both ECDSA and Schnorr) already exists in the blockchain literature [3, 4, 6]. However, a formal definition of the primitive and proofs of the schemes are missing. We leave this as an interesting problem for future research.

The Lightning network uses *combined* signatures, a primitive formalized in [1], to achieve fungibility of transaction needed for the punishment mechanism. Note that if one uses standard signatures only, a punishing party has to sign the transaction under (i) her own signing key to authenticate herself and (ii) revocation secret key to prove that the other party misbehaved. On high level, a combined signature scheme allows to combine those two signatures into one while preserving the security guarantees of both involved parties.

C. Simplifying functionality description

The formal description of the functionality $\mathcal{F}(T,k)$ as presented in Appendix D of the paper is simplified. Namely, several natural checks that one would expect an ideal functionality to make when receiving a message are excluded from its description. For example a functionality should ignore a message that is malformed (e.g. missing or additional parameters), requests an update of a channel that was never created, etc. We define all those check using a wrapper $\mathcal{W}_{\text{checks}}(T,k)$.

Functionality wrapper: $\mathcal{W}_{\text{checks}}(T,k)$

Below, we abbreviate $\mathcal{F} := \mathcal{F}(T,k)$.
Create: Upon $(\texttt{CREATE}, \gamma, tid) \overset{\tau_0}{\hookleftarrow} P$, where $P \in \gamma.\mathsf{users}$, check if: $\Gamma(\gamma.\mathsf{id}) = \bot$ and there is no channel γ' with $\gamma.\mathsf{id} = \gamma'.\mathsf{id}$ being created; γ is valid according to the definition given in Section III of the paper; $\gamma.\mathsf{st} = \{(c_P, \texttt{One–Sig}_{pk_P}), (c_Q, \texttt{One–Sig}_{pk_Q})\}$ for $c_P, c_Q \in \mathbb{R}^{\geq 0}$; and there exists $(t, id, i, \theta) \in \mathcal{L}.\texttt{UTXO}$ such that $\theta = (c_P, \texttt{One–Sig}_P)$ for $(id, i) := tid$;[a] If one of the above checks fails, drop the message. Else proceed as $\mathcal{F}$.
Update: Upon $(\texttt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}}) \overset{\tau_0}{\hookleftarrow} P$ check if: $\gamma := \Gamma(id) \neq \bot$; $P \in \gamma.\mathsf{users}$; there is no other update being preformed; let $\vec{\theta} = (\theta_1, \dots \theta_\ell) = ((c_1, \varphi_1), \dots, (c_\ell, \varphi_\ell))$, then $\sum_{j \in [\ell]} c_i = \gamma.\mathsf{cash}$ and $\varphi_j \in \mathcal{L}.\mathcal{V}$ for each $j \in [\ell]$. If not, drop the message. Else proceed as $\mathcal{F}$.
Upon $(\texttt{SETUP–OK}, id) \overset{\tau_2}{\hookleftarrow} P$ check if: you accepted a message $(\texttt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}}) \overset{\tau_0}{\hookleftarrow} P$, where $t_2 - t_0 \leq t_{\mathsf{stp}} + T$ and the message is a reply to the message $(\texttt{SETUP}, id, \vec{tid})$ sent to P in round τ_1 such that $\tau_2 - \tau_1 \leq t_{\mathsf{stp}}$[b]. If not, drop the message. Else proceed as $\mathcal{F}$.
Upon $(\texttt{UPDATE–OK}, id) \overset{\tau_0}{\hookleftarrow} P$, check if the message is a reply to the message $(\texttt{SETUP–OK}, id)$ sent to P in round τ_0. If not, drop the message. Else proceed as $\mathcal{F}$.
Upon $(\texttt{REVOKE}, id) \overset{\tau_0}{\hookleftarrow} P$, check if the message is a reply to either the message $(\texttt{UPDATE–OK}, id)$ sent to P in round τ_0 or the message $(\texttt{REVOKE–REQ}, id)$ sent to P in round τ_0. If not, drop the message. Else proceed as $\mathcal{F}$.
Close: Upon $(\texttt{CLOSE}, id) \overset{\tau_0}{\hookleftarrow} P$, check if $\gamma := \Gamma(id) \neq \bot$ and $P \in \gamma.\mathsf{users}$. If not, drop the message. Else proceed as $\mathcal{F}$.
All other messages are dropped.

[a] In case more channels are being created at the same time, then none of the other creation requests can use of the tid.
[b] What we formally mean by "reply" is explained in Appx. C of the paper.

D. Simplifying the protocol descriptions

Similarly as the descriptions of our ideal functionality, the description of the protocol Π presented in Section -A excludes many natural checks that we would want an honest party to make. Let us give a few examples of requests which an honest party drops if received from the environment: (i) The environment sends a malformed message to a party P (e.g. missing or additional parameters); (ii) A party P receives an instruction to create a channel γ but $P \notin \gamma.\mathsf{users}$; (iii) A party P receives an instruction to create a channel using the UTXO defined by tid but this UTXO is not spendable by P etc. We define all those check as a wrapper $\mathcal{W}_{\text{checksP}}$.

Protocol wrapper: $\mathcal{W}_{\text{checksP}}$

Party $P \in \mathcal{P}$ proceeds as follows:
Create: Upon $(\texttt{CREATE}, \gamma, tid) \overset{\tau_0}{\hookleftarrow} \mathcal{E}$ check if: $P \in \gamma.\mathsf{users}$; $\Gamma^P(\gamma.\mathsf{id}) = \bot$ and there is no channel γ' with $\gamma.\mathsf{id} = \gamma'.\mathsf{id}$ being created; γ is valid according to the definition given in Section III of the paper; $\gamma.\mathsf{st} = \{(c_P, \texttt{One–Sig}_{pk_P}), (c_Q, \texttt{One–Sig}_{pk_Q})\}$ for $c_P, c_Q \in \mathbb{R}^{\geq 0}$; there exists $(t, id, i, \theta) \in \mathcal{L}.\texttt{UTXO}$ such that

$\theta = (c_P, \texttt{One–Sig}_P)$ for $(id, i) := tid$. If one of the above checks fails, drop the message. Else proceed as in Π.
Update: Upon $(\texttt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}}) \xleftarrow{\tau_0} \mathcal{E}$ check if: $\gamma := \Gamma^P(id) \neq \perp$; there is no other update being preformed; let $\vec{\theta} = (\theta_1, \dots \theta_\ell) = ((c_1, \varphi_1), \dots, (c_\ell, \varphi_\ell))$, then $\sum_{j\in[\ell]} c_i = \gamma.\mathsf{cash}$ and $\varphi_j \in \mathcal{L}.\mathcal{V}$ for each $j \in [\ell]$. If on of the checks fails, drop the message. Else proceed as in Π. Upon $(\texttt{SETUP–OK}, id) \xleftarrow{\tau_2} \mathcal{E}$ check if: you accepted a message $(\texttt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}}) \xleftarrow{\tau_0} \mathcal{E}$, where $t_2 - t_0 \leq t_{\mathsf{stp}} + T$ and the message is a reply to the message $(\texttt{SETUP}, id, \vec{tid})$ you sent in round τ_1 such that $\tau_2 - \tau_1 \leq t_{\mathsf{stp}}$[a]. If not, drop the message. Else proceed as in Π.
Upon $(\texttt{UPDATE–OK}, id) \xleftarrow{\tau_0} \mathcal{E}$, check if the message is a reply to the message $(\texttt{SETUP–OK}, id)$ you sent in round τ_0. If not, drop the message. Else proceed as in Π.
Upon $(\texttt{REVOKE}, id) \xleftarrow{\tau_0} \mathcal{E}$, check if the message is a reply to either $(\texttt{UPDATE–OK}, id)$ or $(\texttt{REVOKE–REQ}, id)$ you sent in round τ_0. If not, drop the message. Else proceed as in Π.
Create: Upon $(\texttt{CLOSE}, id) \xleftarrow{\tau_0} \mathcal{E}$, check if $\gamma := \Gamma^P(id) \neq \perp$. If not, drop the message. Else proceed as in Π.
All other messages are dropped.

[a]What we formally mean by "reply" is explained in Appx. C of the paper.

E. Security proof

In this section we provide a proof for Theorem 2. In our proof, we provide the code for a simulator, that simulates the protocol $\Pi^{\mathcal{L}(\Delta,\Sigma)}(\Xi_{R,\Sigma})$ in the ideal world having access to the functionalities $\mathcal{L}$ and $\mathcal{F}$. The main challenge in providing a simulation in UC proofs usually arises from the fact that the simulator is not given the secret inputs of the parties in the protocol, which makes it difficult to provide a simulated transcript that is indistinguishable to a transcript of a real protocol execution. However, in our setting, parties do not obtain any secret inputs, but only receive commands from the environment $\mathcal{E}$ and hence the only challenge that arises during simulation is handling different behavior of malicious parties. For this reason, we omit the simulation for the case where both parties are honest in the protocol. Furthermore, due to the same reason, as long as the protocol can be simulated in the ideal world, the ideal and real world executions are indistinguishable. We emphasize that the security of the protocol and its realizability relies on the correctness and security properties of underlying adaptor signature scheme, namely unforgeability and witness extractability and adaptability.

Let us now explain the necessity of the adaptor signature properties in more detail. Clearly, if the environment or malicious parties are able to generate signatures on behalf of honest parties, we create an adversary that can use them in order to win the unforgeability game of the adaptor signature scheme. Therefore, only the simulator can generate valid signatures on behalf of the honest parties (the environment can do so only upon guessing the correct signing keys, which happens only with negligible probability). Witness Extractability is necessary in order to punish the dishonest party who has published an old commit transaction. Hence, if a malicious party can publish a valid signature for which the extract algorithm Ext, in step 1 of the simulation for the punish procedure, does not output a correct witness, we can build an adversary that can win the witness extractability game of the adaptor signature scheme. Further, adaptability is required in order to complete the pre-signature of the new commit transaction. Therefore, if a malicious party can generate a pre-signature that cannot be adapted, in step 8 of the simulation for the update procedure, we can build an adversary who can break the pre-signature adapatbility property. Last but not least, the signatures generated upon adapting a pre-signature are valid according to correctness and hence the punish transaction generated in step 3 of the simulation for the punish procedure, is signed correctly and will get accepted by the blockchain.

Remark 2. *In the following proof, we use the witness extracted from an adaptor signature as a signing secret key. We note that the proof extends naturally to the case where the witness is used as a hash preimage even though this requires an additional zero-knowledge proof, which guarantees consistency of the hash value and the preimage.*

Simulator for creating generalized channels

Let $T_1 = 3$.

Case A is honest and B is corrupted

Upon A sending $(\texttt{CREATE}, \gamma, tid_A) \xhookrightarrow{\tau_0} \mathcal{F}$, if B does not send $(\texttt{CREATE}, \gamma, tid_B) \xhookrightarrow{\tau} \mathcal{F}$ where $|\tau_0 - \tau| \leq T_1$, then distinguish the following cases:

1) If B sends $(\text{createInfo}, id, tid_B, R_B, Y_B) \xhookrightarrow{\tau_0} A$, then send $(\texttt{CREATE}, \gamma, tid_B) \xhookrightarrow{\tau_0} \mathcal{F}$ on behalf of B.
2) Otherwise stop.

Do the following:

1) Set $id := \gamma.\mathsf{id}$, generate a revocation public/secret pair $(R_A, r_A) \leftarrow \mathsf{GenR}(pp)$, generate publishing public/secret pair $(Y_A, y_A) \leftarrow \mathsf{GenR}(pp)$ and send $(\text{createInfo}, id, tid_A, R_A, Y_A) \xhookrightarrow{\tau_0} B$.
2) If you receive $(\text{createInfo}, id, tid_B, R_B, Y_B) \xhookleftarrow{\tau_0+1} B$, create the body of the funding, the first commit and split transactions:
$$[\texttt{TX}_\texttt{f}] := \texttt{GenFund}((tid_A, tid_B), \gamma)$$
$$[\texttt{TX}_\texttt{c}] := \texttt{GenCom}([\texttt{TX}_\texttt{f}], I_A, I_B, 0)$$
$$[\texttt{TX}_\texttt{s}] := \texttt{GenSplit}([\texttt{TX}_\texttt{c}].\mathsf{txid} \| 1, \gamma.\mathsf{st})$$
where $I_A := (pk_A, R_A, Y_A)$ and $I_B := (pk_B, R_B, Y_B)$. Else stop.
3) Pre-sign $[\texttt{TX}_\texttt{c}]$ w.r.t. Y_B and sign $[\texttt{TX}_\texttt{s}]$,
$$s_\texttt{c}^A \leftarrow \mathsf{pSign}_{sk_A}([\texttt{TX}_\texttt{c}], Y_B)$$
$$s_\texttt{s}^A \leftarrow \mathsf{Sign}_{sk_A}([\texttt{TX}_\texttt{s}])$$
and $(\text{createCom}, id, s_\texttt{c}^A, s_\texttt{s}^A) \xhookrightarrow{\tau_0+1} B$.
4) If you receive $(\text{createCom}, id, s_\texttt{c}^B, s_\texttt{s}^B) \xhookleftarrow{\tau_0+2} B$, s.t.
$$\mathsf{pVrfy}_{pk_B}([\texttt{TX}_\texttt{c}], Y_A; s_\texttt{c}^B) = 1$$
$$\mathsf{Vrfy}_{pk_B}([\texttt{TX}_\texttt{s}]; s_\texttt{s}^B) = 1$$
sign the funding transaction $s_\texttt{f}^A \leftarrow \mathsf{Sign}_{sk_A}([\texttt{TX}_\texttt{f}])$ and $(\text{createFund}, id, s_\texttt{f}^A) \xhookrightarrow{\tau_0+2} B$. Else stop.
5) If you $(\text{createFund}, id, s_\texttt{f}^B) \xhookleftarrow{\tau_0+3} B$ s.t. $\mathsf{Vrfy}_{pk_B}([\texttt{TX}_\texttt{f}]; s_\texttt{f}^B) = 1$, define $\texttt{TX}_\texttt{f} := ([\texttt{TX}_\texttt{f}], \{s_\texttt{f}^A, s_\texttt{f}^B\})$ and $(\text{post}, \texttt{TX}_\texttt{f}) \xhookrightarrow{\tau_0+3} \mathcal{L}$.

Else parse $(\theta_A, \theta_B) := \gamma.\mathsf{st}$, create tx such that $\mathsf{tx.Input} := tid_A$, $\mathsf{tx.Output} := \theta_A$, $\mathsf{tx}.w \leftarrow \mathsf{Sign}_{pk_A}([\mathsf{tx}])$ and $(\text{post}, \mathsf{tx}) \overset{\tau_0+3}{\hookrightarrow} \mathcal{L}$ and stop.

6) If $\mathtt{TX_f}$ is accepted by $\mathcal{L}$ in round $\tau_1 \leq \tau_0 + 3 + \Delta$, add

$$\Gamma^A(\gamma.\mathsf{id}) := (\gamma, \mathtt{TX_f}, (\mathtt{TX_c}, r_A, R_B, Y_B, s_{\mathsf{c}}^A), \mathtt{TX_s}),$$

where $\mathtt{TX_s} := ([\mathtt{TX_s}], \{s_{\mathsf{s}}^A, s_{\mathsf{s}}^B\})$ and

$$\mathtt{TX_c} := ([\mathtt{TX_c}], \{\mathsf{Sign}_{sk_A}([\mathtt{TX_c}]), \mathsf{Adapt}(s_{\mathsf{c}}^B, y_A)\}).$$

Simulator for updating generalized channels

Let $T_1 = 2$ and $T_2 = 1$ and let $|\vec{tid}| = 1$.

Case A is honest and B is corrupted

Upon A sending $(\mathtt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}}) \overset{\tau_0}{\hookrightarrow} \mathcal{F}$, proceed as follows:

1) Generate new revocation public/secret pair $(R_P, r_P) \leftarrow \mathsf{GenR}$ and a new publishing public/secret pair $(Y_P, y_P) \leftarrow \mathsf{GenR}$ and send $(\text{updateReq}, id, \vec{\theta}, t_{\mathsf{stp}}, R_A, Y_A) \overset{\tau_0^A}{\hookrightarrow} B$.
2) Upon $(\text{updateInfo}, id, h_B, Y_B, s_{\mathsf{s}}^B) \overset{\tau_0^A+2}{\hookleftarrow} B$, set $t_{\mathsf{lock}} := \tau_0^A + t_{\mathsf{stp}} + 5 + \Delta$, extract $\mathtt{TX_f}$ from $\Gamma^B(id)$ and

$$[\mathtt{TX_c}] := \mathtt{GenCom}([\mathtt{TX_f}], I_A, I_B, t_{\mathsf{lock}})$$
$$[\mathtt{TX_s}] := \mathtt{GenSplit}([\mathtt{TX_c}].\mathsf{txid} \| 1, \vec{\theta}),$$

for $I_A := (pk_A, R_A, Y_A)$ and $I_B := (pk_B, R_B, Y_B)$. If $\mathsf{Vrfy}_{pk_B}([\mathtt{TX_s}]; s_{\mathsf{s}}^B) = 1$, send $(\mathtt{SETUP}, id, \mathtt{TX_s}.\mathsf{txid}) \overset{\tau_0^A+2}{\hookrightarrow} \mathcal{E}$. Else stop.
3) If A sends $(\mathtt{SETUP\text{–}OK}, id) \overset{\tau_1^A \leq \tau_0^A+2+t_{\mathsf{stp}}}{\hookleftarrow} \mathcal{F}$, compute $s_{\mathsf{c}}^A \leftarrow \mathsf{pSign}_{sk_A}([\mathtt{TX_c}], Y_B) s_{\mathsf{s}}^A \leftarrow \mathsf{Sign}_{sk_A}([\mathtt{TX_s}])$ and send $(\text{update–commitA}, id, s_{\mathsf{c}}^A, s_{\mathsf{s}}^A) \overset{\tau_1^A}{\hookrightarrow} B$.
4) In round $\tau_1^A + 2$ distinguish the following cases:
   - If you receive $(\text{update–commitB}, id, s_{\mathsf{c}}^B) \overset{\tau_1^A+2}{\hookleftarrow} B$ and if B has not sent $(\mathtt{UPDATE\text{–}OK}, id) \overset{\tau_1^A+1}{\hookrightarrow} \mathcal{F}$, then send $(\mathtt{UPDATE\text{–}OK}, id) \overset{\tau_1^A+1}{\hookrightarrow} \mathcal{F}$ on behalf of B. If $\mathsf{pVrfy}_{pk_B}([\mathtt{TX_c}], Y_A; s_{\mathsf{c}}^B) = 0$, then stop.
   - If you receive $(\text{updateNotOk}, id, r_B) \overset{\tau_2^P+2}{\hookleftarrow} B$, where $(R_B, r_B) \in R$, add $\Theta^A(id) := \Theta^A(id) \cup ([\mathtt{TX_c}], r_B, Y_B, s_{\mathsf{c}}^A)$, instruct $\mathcal{F}$ to stop and stop.
   - Else, execute the simulator code for the procedure $\mathtt{ForceClose}^A(id)$ and stop.
5) If A sends $(\mathtt{REVOKE}, id) \overset{\tau_1^A+2}{\hookrightarrow} \mathcal{F}$, then parse $\Gamma^A(id)$ as $(\gamma, \mathtt{TX_f}, (\overline{\mathtt{TX}}_{\mathsf{c}}, \bar{r}_A, \bar{R}_B, \bar{Y}_B, \bar{s}_{\mathtt{Com}}^A), \overline{\mathtt{TX}}_{\mathsf{s}})$ and update the channel space as $\Gamma^A(id) := (\gamma, \mathtt{TX_f}, (\mathtt{TX_c}, r_A, R_B, Y_B, s_{\mathsf{c}}^A), \mathtt{TX_s})$, for $\mathtt{TX_s} := ([\mathtt{TX_s}], \{s_{\mathsf{s}}^A, s_{\mathsf{s}}^B\})$ and $\mathtt{TX_c} := ([\mathtt{TX_c}], \{\mathsf{Sign}_{sk_A}([\mathtt{TX_c}]), \mathsf{Adapt}(s_{\mathsf{c}}^B, y_A)\})$. Then send $(\text{revokeP}, id, \bar{r}_A) \overset{\tau_1^A+2}{\hookrightarrow} B$. Else, execute the simulator code for the procedure $\mathtt{ForceClose}^A(id)$ and stop.
6) If you receive $(\text{revokeB}, id, \bar{r}_B) \overset{\tau_1^A+4}{\hookleftarrow} B$ and if B has not sent $(\mathtt{REVOKE}, id) \overset{\tau_1^B+2}{\hookrightarrow} \mathcal{F}$, then send $(\mathtt{REVOKE}, id) \overset{\tau_1^B+2}{\hookrightarrow} \mathcal{F}$ on behalf of B. Check if $(\bar{R}_B, \bar{r}_B) \in R$, then set

$$\Theta^B(id) := \Theta^A(id) \cup ([\overline{\mathtt{TX}}_{\mathsf{c}}], \bar{r}_B, \bar{Y}_B, \bar{s}_{\mathtt{Com}}^A)$$

Else execute the simulator code for the procedure $\mathtt{ForceClose}^A(id)$ and stop.

Case B is honest and A is corrupted

Upon A sending $(\text{updateReq}, id, \vec{\theta}, t_{\mathsf{stp}}, h_A) \overset{\tau_0}{\hookrightarrow} B$, send $(\mathtt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}}) \overset{\tau_0}{\hookrightarrow} \mathcal{F}$ on behalf of A, if A has not already sent this message. Proceed as follows:

1) Upon $(\text{updateReq}, id, \vec{\theta}, t_{\mathsf{stp}}, R_A, Y_A) \overset{\tau_0^B}{\hookleftarrow} A$, generate $(R_B, r_B) \leftarrow \mathsf{GenR}$ and $(Y_B, y_B) \leftarrow \mathsf{GenR}$.
2) Set $t_{\mathsf{lock}} := \tau_0^B + t_{\mathsf{stp}} + 4 + \Delta$, extract $\mathtt{TX_f}$ from $\Gamma^A(id)$ and

$$[\mathtt{TX_c}] := \mathtt{GenCom}([\mathtt{TX_f}], I_A, I_B, t_{\mathsf{lock}})$$
$$[\mathtt{TX_s}] := \mathtt{GenSplit}([\mathtt{TX_c}].\mathsf{txid} \| 1, \vec{\theta})$$

where $I_A := (pk_A, R_A, Y_A)$, $I_B := (pk_B, R_B, Y_B)$.
3) Compute $s_{\mathsf{s}}^B \leftarrow \mathsf{Sign}_{sk_B}([\mathtt{TX_s}])$, send $(\text{updateInfo}, id, R_B, Y_B, s_{\mathsf{s}}^B) \overset{\tau_0^B}{\hookrightarrow} A$.
4) If you $(\text{updateComP}, id, s_{\mathsf{c}}^A, s_{\mathsf{s}}^A) \overset{\tau_1^B \leq \tau_0^B+2+t_{\mathsf{stp}}}{\hookleftarrow} A$ then send $(\mathtt{SETUP\text{–}OK}, id) \overset{\tau_1^B}{\hookrightarrow} \mathcal{F}$ on behalf of A, if A has not sent this message.
5) Check if $\mathsf{pVrfy}_{pk_P}([\mathtt{TX_c}], Y_Q; s_{\mathsf{c}}^P) = 1$ and $\mathsf{Vrfy}_{pk_P}([\mathtt{TX_s}]; s_{\mathsf{s}}^P) = 1$.
6) If B sends $(\mathtt{UPDATE\text{–}OK}, id) \overset{\tau_1^B}{\hookrightarrow} \mathcal{F}$, pre-sign $s_{\mathsf{c}}^B \leftarrow \mathsf{pSign}([\mathtt{TX_c}], Y_A)$ and send $(\text{updateComQ}, id, s_{\mathsf{c}}^B) \overset{\tau_1^B}{\hookrightarrow} A$. Else send $(\text{updateNotOk}, id, r_B) \overset{\tau_1^B}{\hookrightarrow} A$ and stop.
7) Parse $\Gamma^B(id)$ as $(\gamma, \mathtt{TX_f}, (\overline{\mathtt{TX}}_{\mathsf{c}}, \bar{r}_B, \bar{R}_A, \bar{Y}_A, \bar{s}_{\mathtt{Com}}^B), \overline{\mathtt{TX}}_{\mathsf{s}})$. If you $(\text{revokeP}, id, \bar{r}_A) \overset{\tau_1^B+2}{\hookleftarrow} A$, send $(\mathtt{REVOKE}, id) \overset{\tau_1^B+2}{\hookrightarrow} \mathcal{F}$ on behalf of A, if A has not sent this message.

   Else if you do not receive $(\text{revokeP}, id, \bar{r}_A) \overset{\tau_1^B+2}{\hookleftarrow} A$ or if $(\bar{R}_A, \bar{r}_A) \notin R$, execute the simulator code of the procedure $\mathtt{ForceClose}^B(id)$ and stop.
8) If B sends $(\mathtt{REVOKE}, id) \overset{\tau_1^B+2}{\hookrightarrow} \mathcal{F}$, then set

$$\Theta^B(id) := \Theta^B(id) \cup ([\overline{\mathtt{TX}}_{\mathsf{c}}], \bar{r}_A, \bar{Y}_A, \bar{s}_{\mathtt{Com}}^B)$$
$$\Gamma^B(id) := (\gamma, \mathtt{TX_f}, (\mathtt{TX_c}, r_B, R_A, Y_A, s_{\mathsf{c}}^B), \mathtt{TX_s}),$$

for $\mathtt{TX_s} := ([\mathtt{TX_s}], \{s_{\mathsf{s}}^A, s_{\mathsf{s}}^B\})$ and $\mathtt{TX_c} := ([\mathtt{TX_c}], \{\mathsf{Sign}_{sk_B}([\mathtt{TX_c}]), \mathsf{Adapt}(s_{\mathsf{c}}^A, y_B)\})$. Then $(\text{revokeB}, id, \bar{r}_B) \overset{\tau_1^B+2}{\hookrightarrow} A$ and stop. Else, in round $\tau_1^B + 2$, execute the simulator code of the procedure $\mathtt{ForceClose}^B(id)$ and stop.

Simulator for closing generalized channels

Let $T_1 = 1$.

Case A is honest and B is corrupted

Upon A sending $(\mathtt{CLOSE}, id) \overset{\tau_0}{\hookrightarrow} \mathcal{F}$, if B does not send $(\mathtt{CLOSE}, id) \overset{\tau}{\hookrightarrow} \mathcal{F}$ where $|\tau_0 - \tau| \leq T_1$, then distinguish the following cases:

1) If B sends $s_{\mathsf{s}}^B \overset{\tau_0}{\hookrightarrow} A$, then send $(\mathtt{CLOSE}, id) \overset{\tau_0}{\hookrightarrow} \mathcal{F}$ on behalf of B.
2) Otherwise execute the simulator code of the procedure $\mathtt{ForceClose}^A(id)$ and stop.

1) Extract $\mathtt{TX_f}$ and $\mathtt{TX_s}$ from $\Gamma^A(id)$. Create the body of the final split transaction $[\overline{\mathtt{TX}}_{\mathsf{s}}]$ as follows

$$[\overline{\mathtt{TX}}_{\mathsf{s}}] := \mathtt{GenSplit}(\mathtt{TX_f}.\mathsf{txid} \| 1, \mathtt{TX_s}.\mathsf{Output})$$

2) Compute the signature $s_{\mathtt{s}}^A \leftarrow \mathsf{Sign}_{sk_A}([\overline{\mathtt{TX}}_{\mathtt{s}}])$ and send $s_{\mathtt{s}}^A \overset{\tau_0}{\hookrightarrow} B$.
3) If you receive $s_{\mathtt{s}}^B \overset{\tau_0+1}{\hookleftarrow} B$, s.t. $\mathsf{Vrfy}_{pk_B}([\overline{\mathtt{TX}}_{\mathtt{s}}]; s_{\mathtt{s}}^B) = 1$, set $\overline{\mathtt{TX}}_{\mathtt{s}} := ([\overline{\mathtt{TX}}_{\mathtt{s}}], \{s_{\mathtt{s}}^A, s_{\mathtt{s}}^B\})$ and send $(\mathrm{post}, \overline{\mathtt{TX}}_{\mathtt{s}}) \overset{\tau_0+1}{\longrightarrow} \mathcal{L}$. Else, execute the simulator code for the procedure $\mathtt{ForceClose}^A(id)$ and stop.
4) Let $\tau_2 \leq \tau_1 + \Delta$ be the round in which $\overline{\mathtt{TX}}_{\mathtt{s}}$ is accepted by the blockchain. Set $\Gamma^A(id) = \bot$, $\Theta^A(id) = \bot$.

Simulator for punishment of generalized channels

Case A is honest and B is corrupted

Upon A sending $\mathtt{PUNISH} \overset{\tau_0}{\hookrightarrow} \mathcal{F}$, for each $id \in \{0,1\}^*$ such that $\Theta^P(id) \neq \bot$ do the following:

1) Parse $\Theta^A(id) := \{([\mathtt{TX}_{\mathtt{c}}^{(\mathtt{i})}], r_B^{(i)}, Y_A^{(i)}, s^{(i)})\}_{i \in m}$ and extract γ from $\Gamma^A(id)$. If for some $i \in [m]$, there exist a transaction tx on $\mathcal{L}$ such that $\mathsf{tx.txid} = \mathtt{TX}_{\mathtt{c}}^{(\mathtt{i})}.\mathsf{txid}$, then parse the witness as $(s_A, s_B) := \mathsf{tx.Witness})$, where $\mathsf{Vrfy}_{pk_A}([\mathsf{tx}]; s_A) = 1$, and set $y_B^{(i)} := \mathsf{Ext}(s_A, s^{(i)}, Y_B^{(i)})$.
2) Define the body of the punishment transaction $[\mathtt{TX}_{\mathtt{pun}}]$ as:

$$\mathtt{TX}_{\mathtt{pun}}.\mathsf{Input} := \mathsf{tx.txid} \| 1,$$
$$\mathtt{TX}_{\mathtt{pun}}.\mathsf{Output} := \{(\gamma.\mathsf{cash}, \mathtt{One\text{–}Sig}_{pk_A})\}$$

3) Compute the signatures $s_y \leftarrow \mathsf{Sign}_{y_B^{(i)}}([\mathtt{TX}_{\mathtt{pun}}]), s_r \leftarrow \mathsf{Sign}_{r_B^{(i)}}([\mathtt{TX}_{\mathtt{pun}}]), s_A \leftarrow \mathsf{Sign}_{pk_A}([\mathtt{TX}_{\mathtt{pun}}])$, and set $\mathtt{TX}_{\mathtt{pun}} := ([\mathtt{TX}_{\mathtt{pun}}], s_y, s_r, s_A)$. Then $(\mathrm{post}, \mathtt{TX}_{\mathtt{pun}}) \overset{\tau_0}{\hookrightarrow} \mathcal{L}$.
4) Let $\mathtt{TX}_{\mathtt{pun}}$ be accepted by $\mathcal{L}$ in round $\tau_1 \leq \tau_0 + \Delta$. Set $\Theta^A(id) = \bot$, $\Gamma^A(id) = \bot$.

Simulator for $\mathtt{ForceClose}^P(id)$

Let τ_0 be the current round
1) Extract $\mathtt{TX}_{\mathtt{c}}$ and $\mathtt{TX}_{\mathtt{s}}$ from $\Gamma(id)$.
2) Wait until round $\tau_1 := \max\{\tau_0, \mathtt{TX}_{\mathtt{c}}.\mathsf{TimeLock}\}$ and send $(\mathrm{post}, \mathtt{TX}_{\mathtt{c}}) \overset{\tau_1}{\hookrightarrow} \mathcal{L}$.
3) Let $\tau_2 \leq \tau_1 + \Delta$ be the round in which $\mathtt{TX}_{\mathtt{c}}$ is accepted by the blockchain. Wait for Δ rounds to $(\mathrm{post}, \mathtt{TX}_{\mathtt{s}}) \overset{\tau_2+\Delta}{\longrightarrow} \mathcal{L}$.
4) Once $\mathtt{TX}_{\mathtt{s}}$ is accepted by the blockchain in round $\tau_3 \leq \tau_2 + 2\Delta$, set $\Theta^P(id) = \bot$ and $\Gamma^P(id) = \bot$.

F. Proof of the ECDSA-based Adaptor Signature

In Section IV of the paper, we presented our ECDSA-based adaptor signature scheme and explained the main ideas of our security proof. We now provide the formal proof of Theorem 1 which we recall here the following completeness.

Theorem 1. *Assuming that the positive ECDSA signature scheme Σ_{ECDSA} is* SUF–CMA*-secure and R'_g is a hard relation, the adaptor signature scheme $\Xi_{R_g,\Sigma_{\mathsf{ECDSA}}}$ as defined in Figure 6 of the paper is secure in ROM.*

As a first step we prove that our ECDSA adaptor signature scheme satisfies pre-signature adaptability. In fact, we prove a slightly stronger statement; namely, that any valid pre-signature adapts to a valid signature with probability 1.

Lemma 1 (Pre-signature adaptability)**.** *The adaptor signature scheme $\Xi_{R'_g,\Sigma_{\mathsf{ECDSA}}}$ satisfies pre-signature adaptability.*

Proof. Let us fix arbitrary $(I_Y, y) \in R'_g$, $m \in \{0,1\}^*$, $X \in \mathbb{G}$ and $\tilde{\sigma} = (r, \tilde{s}, K, \pi) \in \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{G} \times \mathbb{G} \times \{0,1\}^*$. Let

$$\tilde{K} := g^{\mathcal{H}(m)\tilde{s}^{-1}} X^{r\tilde{s}^{-1}} \quad \text{and } r = f(K).$$

Assuming that $\mathsf{pVrfy}_X(m, I_Y; \tilde{\sigma}) = 1$, we know that there exists $k \in \mathbb{Z}_q$ s.t. $\tilde{K} = g^k$ and $K = Y^k$ for $(Y, \pi_Y) := I_Y$. Moreover,

By definition of Adapt, we know that $\mathsf{Adapt}(\tilde{\sigma}, y) = (r, s)$ for $s := \tilde{s} \cdot y^{-1}$. Hence, we have

$$\begin{aligned} f(g^{\mathcal{H}(m)s^{-1}} X^{rs^{-1}}) &= f((g^{\mathcal{H}(m)\tilde{s}^{-1}} X^{r\tilde{s}^{-1}})^y) \\ &= f(\tilde{K}^y) = f(K) = r. \end{aligned}$$

□

Lemma 2 (Pre-signature correctness)**.** *The adaptor signature scheme $\Xi_{R_g,\Sigma_{\mathsf{ECDSA}}}$ satisfies pre-signature correctness.*

Proof. Let us fix arbitrary $x, y \in \mathbb{Z}_q$ and $m \in \{0,1\}^*$, and define $X := g^x$, $Y := g^y$, $\pi_Y \leftarrow \mathsf{P}_g(Y)$ and $I_Y := (Y, \pi_Y)$. For $\tilde{\sigma} = (r, \tilde{s}, K, \pi) \leftarrow \mathsf{pSign}_x(m, I_Y)$ it holds that $\tilde{K} = g^k$, $K = Y^k$, $r = f(K)$ and $\tilde{s} = k^{-1}(\mathcal{H}(m) + rx)$. Set

$$\tilde{K} := g^{\mathcal{H}(m)\tilde{s}^{-1}} g^{r\tilde{s}^{-1}x} = g^k.$$

By correctness of NIZK_Y we know that $\mathsf{V}_Y((\tilde{K}, K), \pi) = 1$ and hence we have $\mathsf{pVrfy}_X(m, I_Y; \tilde{\sigma}) = 1$. By Lemma 1, this implies that $\mathsf{Vrfy}_X(m; \sigma) = 1$ for $\sigma = (r, s) := \mathsf{Adapt}(\tilde{\sigma}, y)$. By definition of Adapt, we know that $s = \tilde{s} \cdot y^{-1}$ and hence

$$\mathsf{Ext}((r, s), (r, \tilde{s}), I_Y) = s^{-1} \cdot \tilde{s} = (\tilde{s}^{-1} \cdot y^{-1}) \cdot \tilde{s} = y.$$

□

Lemma 3 (aEUF–CMA security)**.** *Assuming that the positive ECDSA signature scheme Σ_{ECDSA} is* SUF–CMA*-secure and R'_g is a hard relation, the adaptor signature scheme $\Xi_{R_g,\Sigma_{\mathsf{ECDSA}}}$ as defined in in Figure 6 of the paper is* aEUF–CMA *secure.*

Proof. We prove unforgeability for the ECDSA-based adaptor signature scheme by reduction to strong unforgeability of positive ECDSA signatures. We consider an adversary $\mathcal{A}$ who plays the $\mathsf{aSigForge}$ game, then we build a simulator $\mathcal{S}$ who plays the strong unforgeability experiment for the ECDSA signature scheme and uses $\mathcal{A}$'s forgery in $\mathsf{aSigForge}$ to win its own experiment. $\mathcal{S}$ has access to the signing oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ and the random oracle $\mathcal{H}^{\mathsf{ECDSA}}$, which it uses to simulate oracle queries for $\mathcal{A}$, namely random ($\mathcal{H}$), signing ($\mathcal{O}_{\mathrm{S}}$) and pre-signing ($\mathcal{O}_{\mathrm{pS}}$) queries.

The main challenges in the oracle simulations arise when simulating $\mathcal{O}_{\mathrm{pS}}$ queries, since $\mathcal{S}$ can only get full signatures from its own signing oracle and hence needs a way to transform those full signatures into pre-signatures for $\mathcal{A}$. In order to do so, the simulator faces two challenges, namely 1) $\mathcal{S}$ needs to learn the witness y for statement Y for which the pre-signature is supposed to be generated and 2) $\mathcal{S}$ needs to simulate the zero knowledge proof π which proves randomness consistency in the pre-signature.

More concretely, upon receiving a $\mathcal{O}_{\mathrm{pS}}$ query from $\mathcal{A}$ on input a message m and an instance $I_Y = (Y, \pi_Y)$, the

simulator queries its Sign oracle to obtain a full signature on m. Further, $\mathcal{S}$ needs to learn a witness y, s.t. $Y = g^y$, in order to transform the full signature into a pre-signature for $\mathcal{A}$. We make use of the extractability property of the zero knowledge proof π_Y, in order to extract y and consequently transform a full signature into a valid pre-signature. Additionally, since a valid pre-signature contains a zero knowledge proof for L_{exp}, the simulator has to simulate this proof without knowledge of the corresponding witness. In order to do so, we make use of the zero knowledge property, which allows for simulation of a proof for a statement without knowing the corresponding witness.

G_0

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$m \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(I_Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, I_Y)$
$\sigma \leftarrow \mathcal{A}(\tilde{\sigma}, I_Y)$
$b := \mathsf{Vrfy}_{pk}(m; \sigma^*)$
return $(m \notin \mathcal{Q} \wedge b)$

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, I_Y)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

Game G_0: This game corresponds to the original aSigForge game, where the adversary $\mathcal{A}$ has to come up with a valid forgery for a message m of his choice, while having access to oracles $\mathcal{H}$, $\mathcal{O}_{\mathrm{pS}}$ and $\mathcal{O}_{\mathrm{S}}$. Since we are in the random oracle model, we explicitly write the random oracle code $\mathcal{H}$.

$$\Pr[G_0 = 1] = \Pr[\mathsf{aWitExt}_{\mathcal{A}, \Xi_{R_g}, \Sigma_{\mathsf{Sch}}}(n) = 1]$$

G_1

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(I_Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m^*, I_Y)$
$\sigma^* \leftarrow \mathcal{A}(\tilde{\sigma}, I_Y)$
if $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma^*$
  Abort
$b := \mathsf{Vrfy}_{pk}(m^*; \sigma^*)$
return $(m^* \notin \mathcal{Q} \wedge b)$

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, I_Y)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

Game G_1: This game works exactly as **G_0** with the exception that upon the adversary outputting a forgery σ^*, the game checks if completing the pre-signature $\tilde{\sigma}$ using the witness y results in σ^*. In that case, the game aborts.

Claim: Let Bad_1 be the event that **G_1** aborts, then $\Pr[\mathsf{Bad}_1] \leq \nu(n)$.

Proof: This proof is analogous to the proof of **G_1** in lemma 8. ■

Since games **G_1** and **G_0** are equivalent except if event Bad_1 occurs, it holds that $\Pr[\boldsymbol{G_1} = 1] \leq \Pr[\boldsymbol{G_0} = 1] + \nu_1(n)$, where ν_1 is a negligible function in n.

G_2

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(I_Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m^*, I_Y)$
$\sigma^* \leftarrow \mathcal{A}(\tilde{\sigma}, I_Y)$
if $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma^*$
  Abort
$b := \mathsf{Vrfy}_{pk}(m^*; \sigma^*)$
return $(m^* \notin \mathcal{Q} \wedge b)$

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
  Abort
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, I_Y)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

Game G_2: This game only applies changes to the $\mathcal{O}_{\mathrm{pS}}$ oracle as opposed to the previous game. Namely, during the $\mathcal{O}_{\mathrm{pS}}$ queries, this game extracts a witness y by executing the algorithm K on inputs the statement Y, the proof π_Y and the list of random oracle queries H. The game aborts, if for the extracted witness y it does not hold that $((Y, \pi_Y), y) \in R'_g$.

Claim: Let Bad_2 be the event that **G_2** aborts during an $\mathcal{O}_{\mathrm{pS}}$ execution, then it holds that $\Pr[\mathsf{Bad}_2] \leq \nu_2(n)$ where ν_2 is a negligible function in n.

Proof: According to the *online extractor* property of the zero knowledge proof, for a witness y extracted from a proof π_Y of statement Y such that $\mathsf{Vrfy}(Y, \pi_Y) = 1$, it holds that $((Y, \pi_Y), y) \in R'_g$ except with negligible probability in the security parameter. ■

Since games **G_2** and **G_1** are equivalent except if event Bad_2 occurs, it holds that $\Pr[\boldsymbol{G_2} = 1] \leq \Pr[\boldsymbol{G_1} = 1] + \nu_2(n)$.

G_3

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(I_Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m^*, I_Y)$
$\sigma^* \leftarrow \mathcal{A}(\tilde{\sigma}, I_Y)$
if $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma^*$
  Abort
$b := \mathsf{Vrfy}_{pk}(m^*; \sigma^*)$
return $(m^* \notin \mathcal{Q} \wedge b)$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
  Abort
$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $(r, \tilde{s}, K, \pi_{\mathsf{S}})$

Game G_3: This game extends the changes of the previous game to the $\mathcal{O}_{\mathrm{pS}}$ oracle by first creating a valid full signature σ by executing the Sign algorithm and then converting σ into a pre-signature using the extracted witness y. Further, the game calculates the randomness $\tilde{K} = g^k$ and $K = \tilde{K}^{y^{-1}}$ from σ and simulates a zero knowledge proof π_{S} using $\tilde{K}$ and K.

Due to the *zero knowledge* property of the zero knowledge proof, the simulator can produce a proof π_{S} which is computationally indistinguishable from a proof $\pi \leftarrow P_{dh}((\tilde{K}, K), k)$. Hence, this game is indistinguishable from the previous game and it holds that $\Pr[\boldsymbol{G_3} = 1] \leq \Pr[\boldsymbol{G_2} = 1] + \nu_3(n)$, where ν_3 is a negligible function in n.

Game G_4: In this game, upon receiving the challenge message m^* from $\mathcal{A}$, the game creates a full signature by executing the Sign algorithm and transforms the resulting signature into a pre-signature in the same way as in the previous game during the $\mathcal{O}_{\mathrm{pS}}$ execution. Hence, the same indistinguishability argument as in the previous game holds in this game as well and it holds that $\mathsf{Adv}^{\mathcal{A}}_{\boldsymbol{G_4}} \leq \mathsf{Adv}^{\mathcal{A}}_{\boldsymbol{G_3}} + \nu_3(n)$, where ν_3 is a negligible function in n.

G_4

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(I_Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\sigma \leftarrow \mathsf{Sign}_{sk}(m^*, I_Y)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m^*) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\tilde{\sigma} := (r, \tilde{s}, K, \pi_{\mathsf{S}})$
$\sigma^* \leftarrow \mathcal{A}(\tilde{\sigma}, I_Y)$
if $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma^*$
  Abort
$b := \mathsf{Vrfy}_{pk}(m^*; \sigma^*)$
return $(m^* \notin \mathcal{Q} \wedge b)$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
  Abort
$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $(r, \tilde{s}, K, \pi_{\mathsf{S}})$

□

Having shown that the transition from the original aSigForge game (Game $\boldsymbol{G_0}$) to Game $\boldsymbol{G_4}$ is indistinguishable, it remains to show that there exists a simulator that perfectly simulates $\boldsymbol{G_4}$ and uses $\mathcal{A}$ to win the strongSigForge game. In the following we describe in a concise way the simulator code.

Simulation of oracle queries

Signing queries: Upon $\mathcal{A}$ querying the oracle $\mathcal{O}_{\mathrm{S}}$ on input m, $\mathcal{S}$ forwards m to its oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ and forwards its response to $\mathcal{A}$.

Random Oracle queries: Upon $\mathcal{A}$ querying the oracle $\mathcal{H}$ on input x, if $H[x] = \perp$, then $\mathcal{S}$ queries $\mathcal{H}^{\mathsf{ECDSA}}(x)$, otherwise the simulator returns $H[x]$.

Pre-Signing queries: 1) Upon $\mathcal{A}$ querying the oracle $\mathcal{O}_{\mathrm{pS}}$ on input (m, I_Y), the simulator extracts y using the extractability of NIZK, forwards m to oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ and parses the signature that is generated as (r, s).

2) $\mathcal{S}$ generates a pre-signature from (r, s) by computing $\tilde{s} := s \cdot y$.

3) Finally, $\mathcal{S}$ simulates a zero knowledge proof π_{S}, proving that K and $\tilde{K}$ have the same exponent. The simulator outputs $(r, \tilde{s}, K, \pi_{\mathsf{S}})$.

Challenge phase: 1) Upon $\mathcal{A}$ outputting the message m^* as the challenge message, $\mathcal{S}$ generates $(I_Y, y) \leftarrow \mathsf{GenR}(1^n)$, forwards m^* to the oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ and parses the signature that is generated as (r, s).

2) The simulator generates the required pre-signature $\tilde{\sigma}$ in the same way as during $\mathcal{O}_{\mathrm{pS}}$ queries.
3) Upon $\mathcal{A}$ outputting a forgery σ^*, the simulator outputs (m^*, σ^*) as its own forgery.

$\mathcal{S}^{\mathsf{Sign}^{\mathsf{ECDSA}},\mathcal{H}^{\mathsf{ECDSA}}}(pk)$

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$m^* \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(I_Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\sigma \leftarrow \mathsf{Sign}^{\mathsf{ECDSA}}(m^*, I_Y)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m^*) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\tilde{\sigma} := (r, \tilde{s}, K, \pi_{\mathsf{S}})$
$\sigma^* \leftarrow \mathcal{A}(\tilde{\sigma}, I_Y)$
return (m^*, σ^*)

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}^{\mathsf{ECDSA}}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

if $H[x] = \perp$
$H[x] \leftarrow_{\$} \mathcal{H}^{\mathsf{ECDSA}}(x)$
return $H[x]$

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
  Abort
$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $(r, \tilde{s}, K, \pi_{\mathsf{S}})$

We emphasize that the main difference between the simulation and $\boldsymbol{G_4}$ are syntactical, namely instead of generating the public and secret keys and calculating the algorithm Sign_{sk} and the random oracle $\mathcal{H}$, the simulator $\mathcal{S}$ uses its oracles $\mathsf{Sign}^{\mathsf{ECDSA}}$ and $\mathcal{H}^{\mathsf{ECDSA}}$.

It remains to show that the forgery output by $\mathcal{A}$ can be used by the simulator to win the strongSigForge game.

Claim: (m^*, σ^*) constitutes a valid forgery in game strongSigForge.

Proof: In order to prove this claim, we have to show that the tuple (m^*, σ^*) has not been output by the oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ before. Note that the adversary $\mathcal{A}$ has not previously made a query on the challenge message m^* to either $\mathcal{O}_{\mathrm{pS}}$ or $\mathcal{O}_{\mathrm{S}}$. Hence, $\mathsf{Sign}^{\mathsf{ECDSA}}$ is only queried on m^* during the challenge phase. As shown in game $\boldsymbol{G_1}$, the adversary outputs a forgery σ^* which is equal to the signature σ output by $\mathsf{Sign}^{\mathsf{ECDSA}}$ during the challenge phase only with negligible probability. Hence, $\mathsf{Sign}^{\mathsf{ECDSA}}$ has never output σ^* on query m^* before and consequently (m^*, σ^*) constitutes a valid forgery for game strongSigForge. ■

From the games $\boldsymbol{G_0} - \boldsymbol{G_4}$ we get that $\Pr[\boldsymbol{G_0} = 1] \leq \Pr[\boldsymbol{G_4} = 1] + \nu_1(n) + \nu_2(n) + 2\nu_3(n)$. Since $\mathcal{S}$ provides a perfect simulation of game $\boldsymbol{G_4}$, we obtain:

$$\begin{aligned}\mathsf{Adv}^{\mathcal{A}}_{\mathsf{aSigForge}} &= \Pr[\boldsymbol{G_0} = 1] \\ &\leq \Pr[\boldsymbol{G_4}] + \nu_1(n) + \nu_2(n) + 2\nu_3(n) \\ &\leq \mathsf{Adv}^{\mathcal{S}}_{\mathsf{strongSigForge}} + \nu_1(n) + \nu_2(n) + 2\nu_3(n).\end{aligned}$$

Lemma 4 (Witness Extractability)**.** *Assuming that the positive ECDSA scheme Σ_{pECDSA} is* SUF–CMA*-secure and R'_g is a hard relation, the adaptor signature scheme $\Xi_{R'_g,\Sigma_{\mathsf{pECDSA}}}$ as defined in in Figure 6 of the paper is witness extractable.*

Proof. Before providing the formal proof of witness extractability, we give the main intuition behind this proof. In general this proof is very similar to the proof of lemma 3. Our goal is to reduce the witness extractability of $\Xi_{R'_g,\Sigma_{\mathsf{pECDSA}}}$ to the strong unforgeability of the positive ECDSA signature scheme. In other words, assuming that there exists a PPT adversary $\mathcal{A}$ who wins the aWitExt experiment, we design a PPT adversary $\mathcal{S}$ that wins the strongSigForge experiment.

During the reduction, the main challenge arises during the simulation of pre-sign queries. This simulation is done exactly as in the proof of lemma 3. However, unlike in the aSigForge experiment, in aWitExt, $\mathcal{A}$ outputs the statement I_Y for relation R'_g alongside the challenge message m^*, meaning that the game does not choose the pair (I_Y, y). Therefore, $\mathcal{S}$ does not learn the witness y and hence cannot transform a full signature to a pre-signature by computing $\tilde{s} := s \cdot y$. Fortunately, it is possible to extract y from the zero-knowledge proof embedded in I_Y. After extracting y, the same approach used in order to simulate the pre-sign queries can be taken here as well.

Game $\boldsymbol{G_0}$: This game corresponds to the original aWitExt game, where the adversary $\mathcal{A}$ has to come up with a valid signature σ for a message m of his choice, a given pre-signature $\tilde{\sigma}$ and a given statement/witness pair $((Y, \pi_Y), y)$, while having access to oracles $\mathcal{H}$, $\mathcal{O}_{\mathrm{pS}}$ and $\mathcal{O}_{\mathrm{S}}$, such that $((Y, \pi_Y), \mathsf{Ext}(\sigma, \tilde{\sigma}, (Y, \pi_Y))) \notin R'_g$. Since we are in the random oracle model, we explicitly write the random oracle code $\mathcal{H}$.

$$\Pr[G_0 = 1] = \Pr[\mathsf{aWitExt}_{\mathcal{A},\Xi_{R_g},\Sigma_{\mathsf{Sch}}}(n) = 1]$$

Game $\boldsymbol{G_1}$: This game only applies changes to the $\mathcal{O}_{\mathrm{pS}}$ oracle as opposed to the previous game. Namely, during the $\mathcal{O}_{\mathrm{pS}}$ queries, this game extracts a witness y by executing the algorithm K on inputs the statement Y, the proof π_Y and the list of random oracle queries H. The game aborts, if for the extracted witness y it does not hold that $((Y, \pi_Y), y) \in R'_g$.
Claim: Let Bad_1 be the event that $\boldsymbol{G_1}$ aborts during an $\mathcal{O}_{\mathrm{pS}}$ execution, then it holds that $\Pr[\mathsf{Bad}_1] \leq \nu_1(n)$, where ν_1 is a negligible function in n.
Proof: According to the *online extractor* property of the zero knowledge proof, for a witness y extracted from a proof π_Y for statement Y such that $\mathsf{Vrfy}(Y, \pi_Y) = 1$, it holds that $((Y, \pi_Y Y), y) \in R'_g$ except with negligible probability. ■
Since games $\boldsymbol{G_1}$ and $\boldsymbol{G_0}$ are equivalent except if event Bad_1

occurs, it holds that $\Pr[\boldsymbol{G_0} = 1] \leq \Pr[\boldsymbol{G_1} = 1] + \nu_1(n)$, where ν_1 is a negligible function in n.

$\boldsymbol{G_0}$

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m, I_Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, I_Y)$
$\sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma})$
$y' := \mathsf{Ext}(\sigma, \tilde{\sigma}, I_Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m; \sigma)$
$b_2 := m \notin \mathcal{Q}$
$b_3 := (I_Y, y') \notin R'_g$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{H}(x)$

if $H(x) = \bot$
$H(x) \leftarrow_{\$} \mathbb{Z}_q$
return $H(x)$

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, I_Y)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\boldsymbol{G_1}$

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m^*, I_Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m^*, I_Y)$
$\sigma^* \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma})$
$y' := \mathsf{Ext}(\sigma^*, \tilde{\sigma}, I_Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m^*; \sigma^*)$
$b_2 := m^* \notin \mathcal{Q}$
$b_3 := ((I_Y), y') \notin R'_g$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{H}(x)$

if $H(x) = \bot$
$H(x) \leftarrow_{\$} \mathbb{Z}_q$
return $H(x)$

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
Abort
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, I_Y)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

Game $\boldsymbol{G_2}$: This game extends the changes to $\mathcal{O}_{\mathrm{pS}}$ from the previous game. In the $\mathcal{O}_{\mathrm{pS}}$ execution, this game first creates a valid full signature σ by executing the Sign algorithm and converts σ into a pre-signature using the extracted witness y. Further, the game calculates the randomness $\tilde{K} = g^k$ and $K = \tilde{K}^{y^{-1}}$ from σ and simulates a zero knowledge proof π_{S} using $\tilde{K}$ and K. Due to the *zero knowledge* property of the zero knowledge proof, the simulator can produce a proof π_{S} which is indistinguishable from a proof $\pi \leftarrow \mathsf{P}_{dh}((\tilde{K}, K), k)$. Hence, this game is indistinguishable from the previous game. It holds that $\Pr[\boldsymbol{G_1} = 1] \leq \Pr[\boldsymbol{G_2} = 1] + \nu_2(n)$, where ν_2 is a negligible function in n.

$\boldsymbol{G_2}$

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m^*, I_Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m^*, I_Y)$
$\sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma})$
$y' := \mathsf{Ext}(\sigma^*, \tilde{\sigma}, I_Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m^*; \sigma^*)$
$b_2 := m^* \notin \mathcal{Q}$
$b_3 := (I_Y, y') \notin R$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{H}(x)$

if $H(x) = \bot$
$H(x) \leftarrow_{\$} \mathbb{Z}_q$
return $H(x)$

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
Abort
$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $(r, \tilde{s}, K, \pi_{\mathsf{S}})$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

Game $\boldsymbol{G_3}$: In this game we apply the exact same changes made in game $\boldsymbol{G_1}$ in oracle $\mathcal{O}_{\mathrm{pS}}$ to the challenge phase of the game. During the challenge phase, this game extracts a witness y by executing the algorithm K on inputs the statement Y, the proof π_Y and the list of random oracle queries H. The game aborts, if for the extracted witness y it does not hold that $((Y, \pi_Y), y) \in R'_g$.

$\boldsymbol{G_3}$

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m^*, I_Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
Abort
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, I_Y)$
$\sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma})$
$y' := \mathsf{Ext}(\sigma^*, \tilde{\sigma}, I_Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m^*; \sigma^*)$
$b_2 := m^* \notin \mathcal{Q}$
$b_3 := ((Y, \pi_Y), y') \notin R'_g$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{H}(x)$

if $H(x) = \bot$
$H(x) \leftarrow_{\$} \mathbb{Z}_q$
return $H(x)$

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
Abort
$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $(r, \tilde{s}, K, \pi_{\mathsf{S}})$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

Claim: Let Bad_2 be the event that $\boldsymbol{G_3}$ aborts during the challenge phase, then it holds that $\Pr[\mathsf{Bad}_2] \leq \nu_1(n)$, where ν_1 is a negligible function in n.

Proof: This proof is analogous to the proof of $\boldsymbol{G_1}$ in the proof of lemma 4. ■

Since games $\boldsymbol{G_2}$ and $\boldsymbol{G_3}$ are equivalent except if event Bad_2 occurs, it holds that $\Pr[\boldsymbol{G_2} = 1] \leq \Pr[\boldsymbol{G_3} = 1] + \nu_1(n)$, where ν_1 is a negligible function in n.

$\boldsymbol{G_4}$

$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m^*, I_Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
  Abort
$\sigma \leftarrow \mathsf{Sign}_{sk}(m^*)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m^*) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\tilde{\sigma} := (r, \tilde{s}, K, \pi_{\mathsf{S}})$
$\sigma^* \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma})$
$y' := \mathsf{Ext}(\sigma^*, \tilde{\sigma}, I_Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m^*; \sigma^*)$
$b_2 := m^* \notin \mathcal{Q}$
$b_3 := ((Y, \pi_Y), y') \notin R'_g$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

if $H(x) = \perp$
  $H(x) \leftarrow_{\$} \mathbb{Z}_q$
return $H(x)$

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
  Abort
$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $(r, \tilde{s}, K, \pi_{\mathsf{S}})$

Game $\boldsymbol{G_4}$: In this game we apply the exact same changes made in game $\boldsymbol{G_2}$ in oracle $\mathcal{O}_{\mathrm{pS}}$ to the challenge phase of the game. In the challenge phase, this game first creates a valid full signature σ by executing the Sign algorithm and converts σ into a pre-signature using the extracted witness y. Further, the game calculates the randomness $\tilde{K} = g^k$ and $K = \tilde{K}^{y^{-1}}$ from σ and simulates a zero knowledge proof π_{S} using $\tilde{K}$ and K. Due to the *zero knowledge* property of the zero knowledge proof, the simulator can produce a proof π_{S} which is indistinguishable from a proof $\pi \leftarrow \mathsf{P}_{dh}((\tilde{K}, K), k)$. Hence, this game is indistinguishable from the previous game. It holds that $\Pr[\boldsymbol{G_3} = 1] \leq \Pr[\boldsymbol{G_4} = 1] + \nu_3(n)$, where ν_3 is a negligible function in n.

$\mathcal{S}^{\mathsf{Sign}^{\mathsf{ECDSA}}, \mathcal{H}^{\mathsf{ECDSA}}}(pk)$

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(m^*, I_Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
  Abort
$\sigma \leftarrow \mathsf{Sign}^{\mathsf{ECDSA}}(m^*)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m^*) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\tilde{\sigma} := (r, \tilde{s}, K, \pi_{\mathsf{S}})$
$\sigma^* \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma})$
return (m^*, σ^*)

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}^{\mathsf{ECDSA}}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

if $H(x) = \perp$
  $H(x) \leftarrow_{\$} \mathcal{H}^{\mathsf{ECDSA}}(x)$
return $H(x)$

$\mathcal{O}_{\mathrm{pS}}(m, I_Y)$

parse I_Y as (Y, π_Y)
$y := \mathsf{K}(Y, \pi_Y, H)$
if $((Y, \pi_Y), y) \notin R'_g$
  Abort
$\sigma \leftarrow \mathsf{Sign}^{\mathsf{ECDSA}}(m)$
parse σ as (r, s)
$\tilde{s} := s \cdot y$
$u := \mathcal{H}(m) \cdot s^{-1}$
$v := r \cdot s^{-1}$
$\tilde{K} := g^u X^v$
$K := \tilde{K}^{y^{-1}}$
$\pi_{\mathsf{S}} \leftarrow \mathsf{S}((\tilde{K}, K), 1)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $(r, \tilde{s}, K, \pi_{\mathsf{S}})$

□

Having shown that the transition from the original aWitExt game (Game $\boldsymbol{G_0}$) to Game $\boldsymbol{G_4}$ is indistinguishable, it remains to show that there exists a simulator that perfectly simulates $\boldsymbol{G_4}$ and uses $\mathcal{A}$ to win the strongSigForge game. In the following we describe in a concise way the simulator code.

Simulation of oracle queries

Signing queries: Upon $\mathcal{A}$ querying the oracle $\mathcal{O}_{\mathrm{S}}$ on input m, $\mathcal{S}$ forwards m to its oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ and forwards its response to $\mathcal{A}$.

Random Oracle queries: Upon $\mathcal{A}$ querying the oracle $\mathcal{H}$ on input x, if $H[x] = \perp$, then $\mathcal{S}$ queries $\mathcal{H}^{\mathsf{ECDSA}}(x)$, otherwise the simulator returns $H[x]$.

Pre-Signing queries: 1) Upon $\mathcal{A}$ querying the oracle $\mathcal{O}_{\mathrm{pS}}$ on input (m, I_Y), the simulator extracts y using the extractability of NIZK, forwards m to oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ and parses the signature that is generated as (r, s).
2) $\mathcal{S}$ generates a pre-signature from (r, s) by computing $\tilde{s} := s \cdot y$.
3) Finally, $\mathcal{S}$ simulates a zero knowledge proof π_{S}, proving that it knows the exponent of K and $\tilde{K}$. The simulator outputs $(r, \tilde{s}, K, \pi)$.

Challenge phase: 1) Upon $\mathcal{A}$ outputting the message (m^*, I_Y) as the challenge message, $\mathcal{S}$ extracts y using the extractability of NIZK, forwards m^* to the oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ and parses the signature that is generated as (r, s).

2) The simulator generates the required pre-signature $\tilde{\sigma}$ in the same way as during $\mathcal{O}_{\mathrm{pS}}$ queries.
3) Upon $\mathcal{A}$ outputting a forgery σ, the simulator outputs (m^*, σ^*) as its own forgery.

We emphasize that the main difference between the simulation and $\boldsymbol{G_4}$ are syntactical, namely instead of generating the public and secret keys and calculating the algorithm Sign_{sk} and the random oracle $\mathcal{H}$, the simulator $\mathcal{S}$ uses its oracles $\mathsf{Sign}^{\mathsf{ECDSA}}$ and $\mathcal{H}^{\mathsf{ECDSA}}$.

It remains to show that the signature output by $\mathcal{A}$ can be used by the simulator to win the strongSigForge game.

Claim: (m^*, σ^*) constitutes a valid forgery in game strongSigForge.

Proof: In order to prove this claim, we have to show that the tuple (m^*, σ^*) has not been output by the oracle $\mathsf{Sign}^{\mathsf{ECDSA}}$ before. Note that the adversary $\mathcal{A}$ has not previously made a query on the challenge message m^* to either $\mathcal{O}_{\mathrm{pS}}$ or $\mathcal{O}_{\mathrm{S}}$. Hence, $\mathsf{Sign}^{\mathsf{ECDSA}}$ is only queried on m^* during the challenge phase. If the adversary outputs a forgery σ^* which is equal to the signature σ output by $\mathsf{Sign}^{\mathsf{ECDSA}}$ during the challenge phase, the extracted y would be in relation with the given public value I_Y. Hence, $\mathsf{Sign}^{\mathsf{ECDSA}}$ has never output σ^* on query m^* before and consequently (m^*, σ^*) constitutes a valid forgery for game strongSigForge. ∎

From the games $\boldsymbol{G_0} - \boldsymbol{G_4}$ we get that $\Pr[\boldsymbol{G_0} = 1] \leq \Pr[\boldsymbol{G_4} = 1] + 2\nu_1(n) + \nu_2(n) + \nu_3(n)$. Since $\mathcal{S}$ provides a perfect simulation of game $\boldsymbol{G_4}$, we obtain:

$$\begin{aligned}\mathsf{Adv}_{\mathsf{aWitExt}} &= \Pr[\boldsymbol{G_0} = 1] \\ &\leq \Pr[\boldsymbol{G_4} = 1] + 2\nu_1(n) + \nu_2(n) + \nu_3(n) \\ &\leq \mathsf{Adv}^{\mathcal{S}}_{\mathsf{strongSigForge}} + 2\nu_1(n) + \nu_2(n) + \nu_3(n).\end{aligned}$$

G. Schnorr-based Adaptor Signature

In this section we recall the Schnorr-based adaptor signature construction put forward by Poelstra [5], and formally prove that it satisfies our security definitions.

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of prime order q and let $R_g \subseteq \mathbb{G} \times \mathbb{Z}_q$ be a relation defined as $R_g := \{(Y, y) \mid Y = g^y\}$. The adaptor signature construction is defined with respect to the Schnorr signature scheme Σ_{Sch} for the group $\mathbb{G}$ and the relation R_g. We implicitly assume that all algorithms of the scheme (and the adversary) are parameterized by public parameters $pp := (g, q)$ and have access to a random oracle $\mathcal{H}\colon \{0,1\}^* \to \mathbb{Z}_q$.

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

To extend Schnorr signatures to an adaptor signature scheme, we need a method to produce pre-signatures that depend on the statement Y and reveal the corresponding witness y once the full signature is published. To this end, the r-component of a pre-signature is computed as $\mathcal{H}(X \| g^k Y \| m)$, and s is computed as in standard Schnorr. To adapt a pre-signature into a complete signature, we need to adjust the randomness in s to make it consistent with the randomness $k + y$ used in the r-component. This is done by adding y to s, where y is a value s.t. $g^y = Y$. Clearly, given s and the fixed s-component, we can then efficiently compute the witness y. We formally define the Schnorr-based adaptor signature scheme $\Xi_{R_g, \Sigma_{\mathsf{Sch}}}$ in Fig. 1.

$\mathsf{pSign}_{sk}(m, Y)$
$k \leftarrow_{\$} \mathbb{Z}_q$
$r := \mathcal{H}(X \| g^k Y \| m)$
$\tilde{s} := k + r \cdot sk$
return $(r, \tilde{s})$

$\mathsf{Ext}(\sigma, \tilde{\sigma}, Y)$
$(r, s) := \sigma, (\tilde{r}, \tilde{s}) := \tilde{\sigma}$
$y' := s - \tilde{s}$
if $(Y, y') \in R$
then return y'
else return $\perp$

$\mathsf{pVrfy}_{pk}(m, Y; \tilde{\sigma})$
$(r, \tilde{s}) := \tilde{\sigma}$
$r' := \mathcal{H}(pk \| g^{\tilde{s}} \cdot pk^{-r} \cdot Y \| m)$
return $(r = r')$

$\mathsf{Adapt}(\tilde{\sigma}, y)$
$(r, \tilde{s}) := \tilde{\sigma}$
$s := \tilde{s} + y$
return (r, s)

Fig. 1. Schnorr-based adaptor signature scheme $\Xi_{R_g, \Sigma_{\mathsf{Sch}}}$.

Theorem 3. *If the Schnorr signature scheme Σ_{Sch} is* SUF–CMA*-secure and R_g is a hard relation, then $\Xi_{R_g, \Sigma_{\mathsf{Sch}}}$ from Fig. 1 is a secure adaptor signature scheme in the ROM.*

Remark 3. *We note that Σ_{Sch} is* SUF–CMA*-secure under the assumption that the discrete logarithm problem is hard [2]. However, since we prove the* aEUF–CMA*-security of $\Xi_{R_g, \Sigma_{\mathsf{Sch}}}$ by a reduction to* SUF–CMA*-security of Σ_{Sch}, we state the* SUF–CMA*-security of Σ_{Sch} in Theorem 3.*

In order to prove Theorem 3, we reduce both the unforgeability and the witness extractability of the adaptor signature scheme to the strong unforgeability of the standard Schnorr signature scheme. We first provide a high level overview of the main technical challenges and thereafter present the full proof.

Suppose there exists a PPT adversary $\mathcal{A}$ that wins the aSigForge (resp. aWitExt) experiment, then we design a PPT adversary (also called the simulator) $\mathcal{S}$ that breaks the SUF–CMA security. The main technical challenge in both reductions is that $\mathcal{S}$ has to answer queries (m, Y) to $\mathcal{O}_{\mathrm{pS}}$ by $\mathcal{A}$. This has to be done with access to the Schnorr signing oracle, but without knowledge of sk and the witness y. Thus, we need a method to "transform" full signatures into valid pre-signatures without knowing y, which seems to go against the aEUF–CMA-security (resp. witness extractability).

To address this difficulty, we will use the programmability of the random oracle. Concretely, upon a pre-sign query by $\mathcal{A}$

on some message m, the simulator forwards this message to its own signing oracle and sends the resulting full signature back to $\mathcal{A}$. To "convince" $\mathcal{A}$ that the reply looks like a valid pre-signature, we program the random oracle for RO queries made to verify the pre-signatures. This is possible since the pre-signature and signature verification differ only in the inputs to the hash function.

Finally, let us briefly explain why we need that the underlying signature scheme is strongly unforgeable. In the reduction, $\mathcal{S}$ needs to simulate a pre-signature on the target message m for which a successful $\mathcal{A}$ will later produce a forgery. As described above, this is achieved by querying the underlying Schnorr signature oracle on message m. When $\mathcal{A}$ returns a full signature for m as its forgery, $\mathcal{S}$ can only use this forgery to break the strong unforgeability of Schnorr.

Theorem 1. *Assuming that the Schnorr signature scheme Σ_{Sch} is* SUF–CMA*-secure and R_g is a hard relation, the adaptor signature scheme $\Xi_{R_g,\Sigma_{\mathsf{Sch}}}$ as defined in Fig. 1 is secure in ROM.*

As a first step we prove that our Schnorr adaptor signature scheme satisfies pre-signature adaptability. In fact, we prove a slightly stronger statement; namely, that any valid pre-signature adapts to a valid signature with probability 1.

Lemma 5 (Pre-signature adaptability)**.** *The adaptor signature scheme $\Xi_{R_g,\Sigma_{\mathsf{Sch}}}$ satisfies pre-signature adaptability.*

Proof. Let us fix arbitrary $y \in \mathbb{Z}_q$, $m \in \{0,1\}^*$, $pk \in \mathbb{G}$ and $(r, \tilde{s}) \in \mathbb{Z}_q \times \mathbb{Z}_q$. Let us define $Y := g^y$ and $s := \tilde{s} + y$. Assuming that $\mathsf{pVrfy}_{pk}(m, Y; (r, \tilde{s})) = 1$, we have

$$\begin{aligned} r &= \mathcal{H}(pk \| g^{\tilde{s}} pk^{-r} Y \| m) \\ &= \mathcal{H}(pk \| g^{\tilde{s}+y} pk^{-r} \| m) \\ &= \mathcal{H}(pk \| g^{s} pk^{-r} \| m) \end{aligned}$$

which implies that $\mathsf{Vrfy}_{pk}(m; (r, s)) = 1$. □

Lemma 6 (Pre-signature correctness)**.** *The adaptor signature scheme $\Xi_{R_g,\Sigma_{\mathsf{Sch}}}$ satisfies pre-signature correctness.*

Proof. Let us fix arbitrary $x, y \in \mathbb{Z}_q$ and $m \in \{0,1\}^*$, and define $X := g^x$ and $Y := g^y$. For $\tilde{\sigma} = (r, \tilde{s}) \leftarrow \mathsf{pSign}_x(m, Y)$ it holds that $r = \mathcal{H}(X \| g^k \cdot Y \| m)$ and $\tilde{s} = k + rx$, for some $k \in \mathbb{Z}_q$. Since

$$\mathcal{H}(X \| g^{\tilde{s}} X^{-r} Y \| m) = \mathcal{H}(X \| g^{k+rx} g^{-xr} Y \| m) = r,$$

we have $\mathsf{pVrfy}_X(m, Y; \tilde{\sigma}) = 1$. By Lemma 5, this implies that $\mathsf{Vrfy}_X(m, Y; \sigma) = 1$ for $\sigma = (r, s) := (r, \tilde{s} + y) = \mathsf{Adapt}_X(\tilde{\sigma}, y)$. Finally,

$$\mathsf{Ext}((r, s), (r, \tilde{s}), Y) = s - \tilde{s} = (\tilde{s} + y) - \tilde{s} = y$$

which completes the proof.

□

Before we prove that the Schnorr-based adaptor signature scheme satisfies unforgeability, we make the following simple but useful observation.

Lemma 7. *For any $\sigma := (r, s) \in \mathbb{Z}_q \times \mathbb{Z}_q$ and any $y \in \mathbb{Z}_q$ it holds that*

$$\mathsf{Adapt}(\mathsf{Adapt}(\sigma, y), -y) = \sigma.$$

Proof. By definition of Adapt, for any $r, s, y \in \mathbb{Z}_q$ we have

$$\begin{aligned} \mathsf{Adapt}(\mathsf{Adapt}((r, s), y), -y) &= \mathsf{Adapt}((r, s + y), -y) \\ &= (r, s + y + (-y)) = (r, s) \end{aligned}$$

□

This lemma, in particular, implies that knowing a witness y one can not only adapt a valid pre-signature w.r.t. g^y into a valid signature but also the other way round.

Lemma 8 (aEUF–CMA security)**.** *Assuming that the Schnorr signature scheme Σ_{Sch} is* SUF–CMA*-secure and R_g is a hard relation, the adaptor signature scheme $\Xi_{R_g,\Sigma_{\mathsf{Sch}}}$ as defined in Fig. 1 is* aEUF–CMA *secure.*

Before we give the formal proof, let us give some intuition about the main ideas of the proof. Our goal is to reduce the unforgeability of the adaptor signature scheme to the strong unforgeability of the standard Schnorr signature scheme, i.e. we assume that there exists a PPT adversary $\mathcal{A}$ winning the aSigForge experiment and design a PPT adversary (also called the simulator) $\mathcal{S}$ winning the strongSigForge experiment. The main technical challenge in the reduction is the simulation of pre-sign queries. Since the reduction has access to the Schnorr signing oracle, it may ask for a full signature on the given message. However, it is not immediately clear how this helps to produce a pre-signature w.r.t. a given statement *without* knowing a witness. In fact, this might seem to go against the intuition that it is infeasible to transform a valid pre-signature to a full signature and vice versa without knowing a corresponding witness.

We make use of the fact that the reduction simulates not only the sign and pre-sign queries but also the queries to the random oracle. The main trick in simulating pre-sign queries is to simply forward the full signature to the adversary and "convince" him that it is a valid pre-signature. In more detail, we program the random oracle such that queries made during pre-signature verification are answered as if they were queries made during signature verification and vice versa. This is possible since the pre-signature and signature verification differ only in the string being hashed.

Let us emphasize that no oracle programming is needed for the pre-signature on the forgery message m. This is because the statement/witness pair (Y, y) is chosen by the reduction simulating the aSigForge experiment. The reduction can hence ask the Schnorr signing oracle for a signature σ on the message m and adapt it into a valid pre-signature $\tilde{\sigma}$ itself by executing $\mathsf{Adapt}(\sigma, -y)$. Now if the adversary outputs a valid signature σ', there are two options. Either $\sigma' \neq \sigma$, in which case the reduction learns a valid strongSigForge forgery, or $\sigma' = \sigma$, in which case the reductions failed. However, the latter case happens only with negligible probability since it implies that the adversary, given statement Y, found a witness y and hence broke the hardness of the relation R_g.

Proof. We prove the lemma by defining several game hops.

Game G_0: This game corresponds to the original aSigForge, where the adversary $\mathcal{A}$ has to come up with a valid forgery for a message m of his choice, while having access to pre-sign oracle $\mathcal{O}_{\mathrm{pS}}$ and sign oracle $\mathcal{O}_{\mathrm{S}}$. Since we are in the ROM, the adversary (as well as all the algorithms of the scheme) has additionally access to a random oracle $\mathcal{H}$.

$$\Pr[G_0 = 1] = \Pr[\mathsf{aWitExt}_{\mathcal{A},\Xi_{R_g},\Sigma_{\mathsf{Sch}}}(n) = 1]$$

Game G_1: This game works exactly as G_0 with the following exception. When the adversary outputs a forgery σ, the game checks if completing the pre-signature $\tilde{\sigma}$ using the secret value y results in σ. If yes, the game aborts.

G_0

$1: \mathcal{Q} := \emptyset$
$2: H := [\bot]$
$3: (sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$4: m \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$5: (Y, y) \leftarrow \mathsf{GenR}(1^n)$
$6: \tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$7: \sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma}, Y)$
$8: b := \mathsf{Vrfy}_{pk}(m; \sigma)$
$9:$ **return** $(m \notin \mathcal{Q} \wedge b)$

$\mathcal{H}(x)$
$1:$ **if** $H[x] = \bot$
$2:$ $H[x] \leftarrow_{\$} \mathbb{Z}_q$
$3:$ **return** $H[x]$

$\mathcal{O}_{\mathrm{pS}}(m, Y)$
$1: \tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$2: \mathcal{Q} := \mathcal{Q} \cup \{m\}$
$3:$ **return** $\tilde{\sigma}$

$\mathcal{O}_{\mathrm{S}}(m)$
$1: \sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$2: \mathcal{Q} := \mathcal{Q} \cup \{m\}$
$3:$ **return** σ

G_1

$1: \mathcal{Q} := \emptyset$
$2: H := [\bot]$
$3: (sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$4: m \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$5: (Y, y) \leftarrow \mathsf{GenR}(1^n)$
$6: \tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$7: \sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma}, Y)$
$8:$ **if** $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma$
$9:$ Abort
$10: b := \mathsf{Vrfy}_{pk}(m; \sigma)$
$11:$ **return** $(m \notin \mathcal{Q} \wedge b)$

$\mathcal{H}(x)$
$1:$ **if** $H[x] = \bot$
$2:$ $H[x] \leftarrow_{\$} \mathbb{Z}_q$
$3:$ **return** $H[x]$

$\mathcal{O}_{\mathrm{pS}}(m, Y)$
$1: \tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$2: \mathcal{Q} := \mathcal{Q} \cup \{m\}$
$3:$ **return** $\tilde{\sigma}$

$\mathcal{O}_{\mathrm{S}}(m)$
$1: \sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$2: \mathcal{Q} := \mathcal{Q} \cup \{m\}$
$3:$ **return** σ

Claim: Let Bad_1 be the event that G_1 aborts. Then $\Pr[\mathsf{Bad}_1] \leq \nu_1(n)$, where ν_1 is a negligible function in n.

Proof: We prove this claim using a reduction to the hardness of the relation R_g. More concretely, we construct a simulator $\mathcal{S}$ breaking the hardness the relation assuming he has access to an adversary $\mathcal{A}$ that causes G_1 to abort with non-negligible probability. The simulator gets a challenge Y^*, upon which it generates a key pair $(sk, pk) \leftarrow \mathsf{Gen}(1^n)$ in order to simulate $\mathcal{A}$'s queries to the oracles $\mathcal{H}$, $\mathcal{O}_{\mathrm{pS}}$ and $\mathcal{O}_{\mathrm{S}}$. This simulation of the oracles works as described in G_1. Eventually, upon receiving the challenge message m from $\mathcal{A}$, $\mathcal{S}$ computes a pre-signature $\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y^*)$ and returns the pair $(\tilde{\sigma}, Y^*)$ to the adversary who outputs a forgery σ. Assuming that Bad_1 happened (i.e. $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma$), we know that due to the correctness property, the simulator can extract y^* by executing $\mathsf{Ext}(\sigma, \tilde{\sigma}, Y^*)$ to obtain a valid statement/witness pair for the relation R_g, i.e. $(Y^*, y^*) \in R_g$.

First, we note that the view of $\mathcal{A}$ is indistinguishable to his view in G_1, since the challenge Y^* is an instance of the hard relation R_g and hence equally distributed to the public output of GenR. Hence the probability of $\mathcal{S}$ can breaking the hardness of the relation is equal to the probability of the Bad_1 event. By our assuption, this is non-negligible with is the contradiction with the hardness of R_g. ■

Since games G_1 and G_0 are equivalent except if event Bad_1 occurs, it holds that $\Pr[G_0 = 1] \leq \Pr[G_1 = 1] + \nu_1(n)$.

Game G_2: This game behaves like the previous game with the only differences being in the $\mathcal{O}_{\mathrm{pS}}$ oracle. In this game, the $\mathcal{O}_{\mathrm{pS}}$ oracle makes a copy of the list H before executing the algorithm pSign_{sk}. Afterwards the it extracts the randomness used during the pSign_{sk} algorithm, and checks if before the execution of the signing algorithm a query of the form $pk\|K\|m$ or $pk\|K \cdot Y\|m$ was made to $\mathcal{H}$ by checking if $H'[pk\|K\|m] \neq \bot$ or $H'[pk\|K \cdot Y\|m] \neq \bot$. If so the game aborts.

G_2

$1: \mathcal{Q} := \emptyset$
$2: H := [\bot]$
$3: (sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$4: m \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$5: (Y, y) \leftarrow \mathsf{GenR}(1^n)$
$6: \tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$7: \sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma}, Y)$
$8:$ **if** $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma$
$9:$ Abort
$10: b := \mathsf{Vrfy}_{pk}(m; \sigma)$
$11:$ **return** $(m \notin \mathcal{Q} \wedge b)$

$\mathcal{H}(x)$
$1:$ **if** $H[x] = \bot$
$2:$ $H[x] \leftarrow_{\$} \mathbb{Z}_q$
$3:$ **return** $H[x]$

$\mathcal{O}_{\mathrm{pS}}(m, Y)$
$1: H' := H$
$2: \tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$3: (r, s) := \tilde{\sigma}$
$4: K := g^s \cdot pk^{-r}$
$5:$ **if** $(H'[pk\|K\|m] \neq \bot$
$6:$ $\vee H'[pk\|K \cdot Y\|m] \neq \bot)$
$7:$ Abort
$8: \mathcal{Q} := \mathcal{Q} \cup \{m\}$
$9:$ **return** $\tilde{\sigma}$

$\mathcal{O}_{\mathrm{S}}(m)$
$1: \sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$2: \mathcal{Q} := \mathcal{Q} \cup \{m\}$
$3:$ **return** σ

Claim: Let Bad_2 be the event that G_2 aborts in $\mathcal{O}_{\mathrm{pS}}$. Then $\Pr[\mathsf{Bad}_2] \leq \nu_2(n)$, where ν_2 is a negligible function in n.

Proof: We first recall that pSign_{sk} and Sign_{sk} compute $K = g^k$ by choosing k uniformly at random from $\mathbb{Z}_q$. Since $\mathcal{A}$ is PPT, the number of queries it can make to $\mathcal{H}$, $\mathcal{O}_{\mathrm{S}}$ and $\mathcal{O}_{\mathrm{pS}}$ is also

polynomially bounded. Let l_1, l_2, l_3 be the number of queries made to $\mathcal{H}$, $\mathcal{O}_{\mathrm{S}}$ and $\mathcal{O}_{\mathrm{pS}}$ respectively, then we have:

$$\begin{aligned}\Pr[\mathsf{Bad}_2] &= \Pr[H'[pk\|K\|m] \neq \perp \vee H'[pk\|K\cdot Y\|m] \neq \perp] \\ &\leq 2\frac{l_1+l_2+l_3}{q} =: \nu_2(n)\end{aligned}$$

Since l_1, l_2, l_3 are polynomial in the security parameter, ν_2 is a negligible function. ■

Since games $\boldsymbol{G_2}$ and $\boldsymbol{G_1}$ are equivalent except if event Bad_2 occurs, it holds that $\Pr[G_1 = 1] \leq \Pr[G_2 = 1] + \nu_2(n)$.

Game $\boldsymbol{G_3}$: In this game, upon an $\mathcal{O}_{\mathrm{pS}}$ query, the game produces a valid full signature $\tilde{\sigma} = (r, s) = (\mathcal{H}(pk\|K\|m), k + rsk)$ and adjusts the global list H as follows: It assigns the value stored at position $pk\|K\|m$ to $H[pk\|K\cdot Y\|m]$ and samples a fresh random value for $H[pk\|K\|m]$. These changes make the full signature $\tilde{\sigma}$ "look like" a pre-signature to the adversary, since upon querying the random oracle on $pk\|K\cdot Y\|m$, $\mathcal{A}$ obtains the value $H[pk\|K\|m]$. The adversary can only notice the changes in this game, in case the random oracle has been previously queried on either $pk\|K\|m$ or $pk\|K\cdot Y\|m$. This case has been captured in the previous game and hence it holds that $\Pr[G_2 = 1] = [G_3 = 1]$.

$\boldsymbol{G_3}$

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$m \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$\sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma}, Y)$
if $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma$
  Abort
$b := \mathsf{Vrfy}_{pk}(m; \sigma)$
return $(m \notin \mathcal{Q} \wedge b)$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, Y)$

$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{Sign}_{sk}(m)$
$(r, s) := \tilde{\sigma}$
$K := g^s \cdot pk^{-r}$
if $(H'[pk\|K\|m] \neq \perp$
  $\vee\, H'[pk\|K\cdot Y\|m] \neq \perp)$
  Abort
$x := pk\|K\|m$
$H[pk\|K\cdot Y\|m] := H[x]$
$H[x] \leftarrow_{\$} \mathbb{Z}_q$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

Game $\boldsymbol{G_4}$: In this game the pre-signature in generated upon $\mathcal{A}$ outputting the message m is generated by modifying a full signature to a pre-signature. In other words upon receiving the full signature $\sigma = (r, s)$, where $s = k + xr$ and $r = \mathcal{H}(g^x\|g^k\|m)$ and given the pair (Y, y), the game can modify the signature to the pre-signature by setting $\tilde{\sigma} = \mathsf{Adapt}(\sigma, -y)$. One way to see this transformation is that k is modified to $k' = k - y$.

$\boldsymbol{G_4}$

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$m \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\sigma' \leftarrow \mathsf{Sign}_{sk}(m)$
$(r, s) := \sigma'$
$\tilde{\sigma} := \mathsf{Adapt}(\sigma, -y)$
$\sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma}, Y)$
if $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma$
  Abort
$b := \mathsf{Vrfy}_{pk}(m; \sigma)$
return $(m \notin \mathcal{Q} \wedge b)$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, Y)$

$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{Sign}_{sk}(m)$
$(r, s) := \tilde{\sigma}$
$K := g^s \cdot pk^{-r}$
if $(H'[pk\|K\|m] \neq \perp$
  $\vee\, H'[pk\|K\cdot Y\|m] \neq \perp)$
  Abort
$x := pk\|K\|m$
$H[pk\|K\cdot Y\|m] := H[x]$
$H[x] \leftarrow_{\$} \mathbb{Z}_q$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

Since k is chosen uniformly at random and according to Lemma 7, the view of the adversary is identical in this game and the previous game and hence it holds that $\Pr[G_3 = 1] = [G_4 = 1]$.

$\mathcal{S}^{\mathsf{Sign}^{\mathsf{Sch}},\mathcal{H}^{\mathsf{Sch}}}(pk)$

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$m \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$(Y, y) \leftarrow \mathsf{GenR}(1^n)$
$\sigma' := \mathsf{Sign}^{\mathsf{Sch}}(m)$
$(r, s) := \sigma'$
$\tilde{\sigma} := \mathsf{Adapt}(\sigma, -y)$
$\sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma}, Y)$
return (m, σ)

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma := \mathsf{Sign}^{\mathsf{Sch}}(m)$
$(r, s) := \sigma$
$K := g^s \cdot pk^{-r}$
$x := pk\|K\|m$
$H[x] := \mathcal{H}^{\mathsf{Sch}}(x)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, Y)$

$H' := H$
$\tilde{\sigma} := \mathsf{Sign}^{\mathsf{Sch}}(m)$
$(r, s) := \tilde{\sigma}$
$K := g^s \cdot pk^{-r}$
if $H'[pk\|K\|m] \neq \perp$
  or $H'[pk\|K\cdot Y\|m] \neq \perp$
  Abort
$x := pk\|K\|m$
$H[pk\|K\cdot Y\|m] := \mathcal{H}^{\mathsf{Sch}}(x)$
$H[x] := \mathcal{H}^{\mathsf{Sch}}(pk\|K\cdot Y\|m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

Having shown that the transition from the original aSigForge game (Game $\boldsymbol{G_0}$) to Game $\boldsymbol{G_4}$ is indistinguishable, it remains to show that there exists a simulator that perfectly simulates $\boldsymbol{G_4}$ and uses $\mathcal{A}$ to win the strongSigForge game. In the following we describe in a concise way the simulator code.

Simulation of oracle queries

Signing queries: Upon $\mathcal{A}$ querying the oracle $\mathcal{O}_{\mathrm{S}}$ on input m, $\mathcal{S}$ forwards m to its oracle $\mathsf{Sign}^{\mathsf{Sch}}$ and forwards its response to $\mathcal{A}$.

Random Oracle queries: Upon $\mathcal{A}$ querying the oracle $\mathcal{H}$ on input x, if $H[x] = \perp$, then $\mathcal{S}$ queries $\mathcal{H}^{\mathsf{Sch}}(x)$, otherwise the simulator returns $H[x]$.

Pre-Signing queries: 1) Upon $\mathcal{A}$ querying the oracle $\mathcal{O}_{\mathrm{pS}}$ on input (m, Y), $\mathcal{S}$ forwards m to its oracle $\mathsf{Sign}^{\mathsf{Sch}}$ and receives the signature $\tilde{\sigma} = (r, s)$ where $r = \mathcal{H}^{\mathsf{Sch}}(pk\|K\|m)$.
2) If $\mathcal{H}$ has been previously queried on the input $(pk\|K\|m)$ or $(pk\|K \cdot Y\|m)$, $\mathcal{S}$ aborts.
3) $\mathcal{S}$ programs the random oracle $\mathcal{H}$ such that queries of $\mathcal{A}$ on the input $pk\|K \cdot Y\|m$ are answered with the value of $\mathcal{H}^{\mathsf{Sch}}(pk\|K\|m)$ and queries on the input $pk\|K\|m$ are answered with the value of $\mathcal{H}^{\mathsf{Sch}}(pk\|K \cdot Y\|m)$.
4) The simulator returns $\tilde{\sigma}$ to $\mathcal{A}$.

Challenge Phase: 1) Upon $\mathcal{A}$ outputting the message m as the challenge message, $\mathcal{S}$ chooses values $(Y, y) \leftarrow \mathsf{GenR}(1^n)$ and queries the $\mathsf{Sign}^{\mathsf{Sch}}$ oracle on input m. Let $\sigma' = (r, s)$ be the response, then $\mathcal{S}$ returns $\tilde{\sigma} = (r, s - y)$ to $\mathcal{A}$.
2) Upon $\mathcal{A}$ outputting a forgery σ, the simulator outputs (m, σ) as its own forgery.

We emphasize that the main difference between the simulation and $\boldsymbol{G_4}$ are syntactical, namely instead of generating the public and secret keys and calculating the algorithm Sign_{sk} and the random oracle $\mathcal{H}$, the simulator $\mathcal{S}$ uses its oracles $\mathsf{Sign}^{\mathsf{Sch}}$ and $\mathcal{H}^{\mathsf{Sch}}$. Therefore $\mathcal{S}$ perfectly simulates $\boldsymbol{G_4}$.

It remains to show that the forgery output by $\mathcal{A}$ can be used by the simulator to win the strongSigForge game.

Claim: (m, σ) constitutes a valid forgery in game strongSigForge.

Proof: In order to prove this claim, we have to show that the tuple (m, σ) has not been output by the oracle $\mathsf{Sign}^{\mathsf{Sch}}$ before. Note that the adversary $\mathcal{A}$ has not previously made a query on the challenge message m to either $\mathcal{O}_{\mathrm{pS}}$ or $\mathcal{O}_{\mathrm{S}}$. Hence, $\mathsf{Sign}^{\mathsf{Sch}}$ is only queried on m during the challenge phase. As shown in game $\boldsymbol{G_1}$ and according to Lemma 7, the adversary outputs a forgery σ which is equal to the signature σ' output by $\mathsf{Sign}^{\mathsf{Sch}}$ during the challenge phase only with negligible probability (in this case the simulation aborts). Hence, $\mathsf{Sign}^{\mathsf{Sch}}$ has never output σ on query m before and consequently (m, σ) constitutes a valid forgery for game strongSigForge. ■

From the games $\boldsymbol{G_0} - \boldsymbol{G_4}$ we get that $\Pr[\boldsymbol{G_0} = 1] \leq \Pr[\boldsymbol{G_4} = 1] + \nu_1(n) + \nu_2(n)$. Since $\mathcal{S}$ provides a perfect simulation of game $\boldsymbol{G_4}$, we obtain: $\mathsf{Adv}^{\mathcal{A}}_{\mathsf{aSigForge}} \leq \mathsf{Adv}^{\mathcal{S}}_{\mathsf{strongSigForge}} + \nu_1(n) + \nu_2(n)$.

□

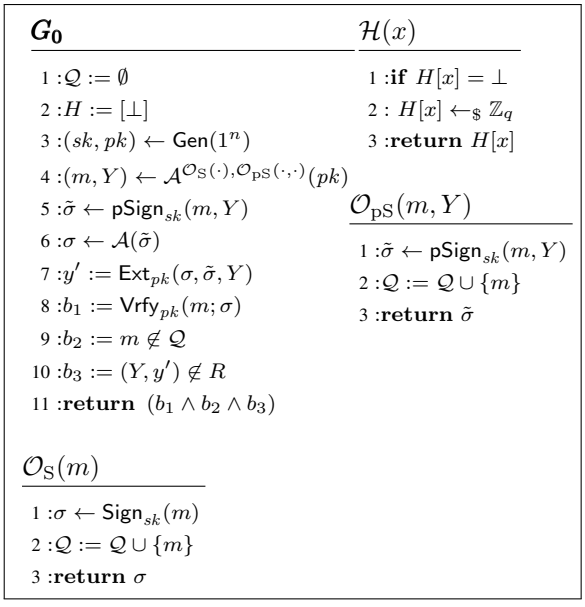
Lemma 9 (Witness Extractability)**.** *Assuming that Schnorr signature scheme Σ_{Sch} is SUF–CMA-secure and R_g is a hard relation, the adaptor signature scheme $\Xi_{R_g, \Sigma_{\mathsf{Sch}}}$ as defined in Fig. 1 is witness extractable.*

Proof. Before giving the formal proof, we first provide the main intuition. In general this proof is very similar to the proof of Lemma 8. Our goal is to reduce the witness extractability of the adaptor signature scheme to the strong unforgeability of the standard Schnorr signature scheme. More concretely, under the assumption that there exists a PPT adversary $\mathcal{A}$ winning the aWitExt experiment, we design a PPT adversary $\mathcal{S}$ that wins the strongSigForge experiment.

The simulation of pre-sign queries is done exactly as in the proof of Lemma 8. However, unlike in the aSigForge experiment, in aWitExt $\mathcal{A}$ outputs the public value Y alongside the challenge message m, meaning that the game does not choose the pair (Y, y). Therefore, $\mathcal{S}$ does not learn the witness y and hence cannot transform a full signature to a pre-signature by executing $\mathsf{Adapt}(\sigma, -y)$. Fortunately, we can do this transformation without knowledge of y by using the same random oracle programmability as in the $\mathcal{O}_{\mathrm{pS}}$ oracle. More concretely, $\mathcal{S}$ can program the random oracle such that queries made during pre-signature verification are answered as if they were queries made during signature verification and vice versa. In other words the values $\mathcal{H}(g^x\|K\|m)$ and $\mathcal{H}(g^x\|KY\|m)$ (where $K = g^k$, g^x and Y are known to the simulator) are swapped in the random oracle.

We note that it is not possible to program the random oracle if at least one of the values $g^x\|K\|m$ or $g^x\|KY\|m$ have already been queried to $\mathcal{H}$. However, since $\mathcal{A}$ is PPT, and k is chosen uniformly at random from $\mathbb{Z}_q$ (during the signing and pre-signing processes) where q is exponential in n, the probability that one of these values have previously been queried to $\mathcal{H}$ is negligible in the security parameter n.

□



Game $\boldsymbol{G_0}$: This game corresponds to the original aWitExt, where the adversary $\mathcal{A}$ has to come up with a valid forgery for a message m of his choice such that extracting the secret value given the forgery and the pre-sinature is not in relation with the corresponding public key. $\mathcal{A}$ has access to oracles $\mathcal{H}$, $\mathcal{O}_{\mathrm{pS}}$ and $\mathcal{O}_{\mathrm{S}}$, and since we are in the random oracle model, we explicitly write the random oracle code $\mathcal{H}$.

G_1

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m, Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$\sigma \leftarrow \mathcal{A}(\tilde{\sigma})$
$y' := \mathsf{Ext}_{pk}(\sigma, \tilde{\sigma}, Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m; \sigma)$
$b_2 := m \notin \mathcal{Q}$
$b_3 := (Y, y') \notin R$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, Y)$

$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
parse $\tilde{\sigma}$ as (r, s)
$K := g^s \cdot pk^{-r}$
if $H'[pk\|K\|m] \neq \perp$
or $H'[pk\|K \cdot Y\|m] \neq \perp$
Abort
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

Game G_1: This game behaves like G_0 with the only differences being in the $\mathcal{O}_{\mathrm{pS}}$ oracle. First a copy of the list H is stored before executing the algorithm pSign_{sk} in the oracle $\mathcal{O}_{\mathrm{pS}}$. Upon computing the pre-signature, the game extracts the randomness used during the pSign_{sk} algorithm, and checks if before the execution of the signing algorithm a query of the form $pk\|K\|m$ or $pk\|K \cdot Y\|m$ was made to $\mathcal{H}$. This is done by checking if $H'[pk\|K\|m] \neq \perp$ or $H'[pk\|K \cdot Y\|m] \neq \perp$. If so the game aborts.

Claim: Let Bad_1 be the event that G_1 aborts in $\mathcal{O}_{\mathrm{pS}}$, then $\Pr[\mathsf{Bad}_1] \leq \nu(n)$, where ν is a negligible function in n.

Proof: We first recall that pSign_{sk} and Sign_{sk} compute $K = g^k$ by choosing k uniformly at random from $\mathbb{Z}_q$. Since $\mathcal{A}$ is PPT, the number of queries it can make to $\mathcal{H}$, $\mathcal{O}_{\mathrm{S}}$ and $\mathcal{O}_{\mathrm{pS}}$ are also polynomially bounded. Let l_1, l_2, l_3 be the number of queries made to $\mathcal{H}$, $\mathcal{O}_{\mathrm{S}}$ and $\mathcal{O}_{\mathrm{pS}}$ respectively, then we have:

$$\begin{aligned}\Pr[\mathsf{Bad}_1] &= \Pr[H'(pk\|K\|m) \neq \perp \\ &\quad \vee H'(pk\|K \cdot Y\|m) \neq \perp] \\ &\leq 2\frac{l_1 + l_2 + l_3}{q} \leq \nu(n)\end{aligned}$$

■

Since games G_1 and G_0 are equivalent except if event Bad_1 occurs, it holds that $\Pr[G_0 = 1] \leq \Pr[G_1 = 1] + \nu_1(n)$.

Game G_2: In this game, upon an $\mathcal{O}_{\mathrm{pS}}$ query, the game produces a valid full signature such that $\tilde{\sigma} = (r, s) = (\mathcal{H}(pk\|K\|m), k + rsk)$ and modifies the global list H as follows: It sets the value stored at position $pk\|K\|m$ to $H[pk\|K \cdot Y\|m]$ and samples a fresh random value for $H[pk\|K\|m]$. These changes make the full signature $\tilde{\sigma}$ look like a pre-signature to the adversary, since upon querying the random oracle on $pk\|K \cdot Y\|m$, $\mathcal{A}$ obtains the value $H[pk\|K\|m]$. The adversary can only notice the changes in this game, in case the random oracle has been previously queried on either $pk\|K\|m$ or $pk\|K \cdot Y\|m$. This case has been captured in the previous game and hence it holds that $\Pr[G_1 = 1] = \Pr[G_2 = 1]$.

G_2

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m, Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$\sigma^* \leftarrow \mathcal{A}(\tilde{\sigma}, Y)$
if $\mathsf{Adapt}(\tilde{\sigma}, y) = \sigma$
Abort
$y' := \mathsf{Ext}_{pk}(\sigma, \tilde{\sigma}, Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m; \sigma)$
$b_2 := m \notin \mathcal{Q}$
$b_3 := (Y, y') \notin R$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, Y)$

$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{Sign}_{sk}(m)$
parse $\tilde{\sigma}$ as (r, s)
$K := g^s \cdot pk^{-r}$
if $H'[pk\|K\|m] \neq \perp$
or $H'[pk\|K \cdot Y\|m] \neq \perp$
Abort
$x := pk\|K\|m$
$H[pk\|K \cdot Y\|m] := H[x]$
$H[x] \leftarrow_{\$} \mathbb{Z}_q$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

G_3

$\mathcal{Q} := \emptyset$
$H := [\perp]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m, Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
parse $\tilde{\sigma}$ as (r, s)
$K := g^s \cdot pk^{-r}$
if $H'[pk\|K\|m] \neq \perp$
or $H'[pk\|K \cdot Y\|m] \neq \perp$
Abort
$\sigma \leftarrow \mathcal{A}(\tilde{\sigma}, Y)$
$y' := \mathsf{Ext}_{pk}(\sigma, \tilde{\sigma}, Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m; \sigma)$
$b_2 := m \notin \mathcal{Q}$
$b_3 := (Y, y') \notin R$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\mathrm{pS}}(m, Y)$

$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{Sign}_{sk}(m)$
parse $\tilde{\sigma}$ as (r, s)
$K := g^s \cdot pk^{-r}$
if $H'[pk\|K\|m] \neq \perp$
or $H'[pk\|K \cdot Y\|m] \neq \perp$
Abort
$x := pk\|K\|m$
$H[pk\|K \cdot Y\|m] := H[x]$
$H[x] \leftarrow_{\$} \mathbb{Z}_q$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

Game G_3: In this game, we apply the exact same changes made in game G_1 in oracle $\mathcal{O}_{\mathrm{pS}}$ to the challenge phase of the game. First a copy of the list H is stored before executing the algorithm pSign_{sk} during the challenge phase of the game. Upon computing the pre-signature, the game extracts the randomness used during the pSign_{sk} algorithm, and checks if before the execution of the pre-signing algorithm a query of the form $pk\|K\|m$ or $pk\|K \cdot Y\|m$ was made to $\mathcal{H}$. This is done by checking if $H'[pk\|K\|m] \neq \perp$ or $H'[pk\|K \cdot Y\|m] \neq \perp$. If so the game aborts.

Claim: Let Bad_2 be the event that $\boldsymbol{G_2}$ aborts in $\text{Game}_3(n)$ during the challenge phase, then $\Pr[\mathsf{Bad}_2] \leq \nu(n)$, where ν is a negligible function in n.

Proof: This proof is analogous to the proof of claim -G. ■

Since games $\boldsymbol{G_3}$ and $\boldsymbol{G_2}$ are equivalent except if event Bad_2 occurs, it holds that $\Pr[\boldsymbol{G_2} = 1] \leq \Pr[\boldsymbol{G_3} = 1] + \nu(n)$.

Game $\boldsymbol{G_4}$: In this game, we apply the exact same changes made in game $\boldsymbol{G_2}$ in oracle $\mathcal{O}_{\text{pS}}$ to the challenge phase of the game. As explained before the adversary receives a full signature but by programming the random oracle, from $\mathcal{A}$'s point of view the signature looks like a pre-signature. It holds that $\Pr[\boldsymbol{G_4} = 1] = \Pr[\boldsymbol{G_3} = 1]$.

$\boldsymbol{G_4}$

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m, Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\text{S}}(\cdot), \mathcal{O}_{\text{pS}}(\cdot,\cdot)}(pk)$
$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{Sign}_{sk}(m)$
parse $\tilde{\sigma}$ as (r, s)
$K := g^s \cdot pk^{-r}$
if $H'[pk \| K \| m] \neq \bot$
or $H'[pk \| K \cdot Y \| m] \neq \bot$
Abort
$x := pk \| K \| m$
$H[pk \| K \cdot Y \| m] := H[x]$
$H[x] \leftarrow_{\$} \mathbb{Z}_q$
$\sigma \leftarrow \mathcal{A}(\tilde{\sigma}, Y)$
$y' := \mathsf{Ext}_{pk}(\sigma, \tilde{\sigma}, Y)$
$b_1 := \mathsf{Vrfy}_{pk}(m; \sigma)$
$b_2 := m \notin \mathcal{Q}$
$b_3 := (Y, y') \notin R$
return $(b_1 \wedge b_2 \wedge b_3)$

$\mathcal{O}_{\text{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

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

$\mathcal{O}_{\text{pS}}(m, Y)$

$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{Sign}_{sk}(m)$
parse $\tilde{\sigma}$ as (r, s)
$K := g^s \cdot pk^{-r}$
if $H'[pk \| K \| m] \neq \bot$
or $H'[pk \| K \cdot Y \| m] \neq \bot$
Abort
$x := pk \| K \| m$
$H[pk \| K \cdot Y \| m] := H[x]$
$H[x] \leftarrow_{\$} \mathbb{Z}_q$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

Having shown that the transition from the original aWitExt game (Game $\boldsymbol{G_0}$) to Game $\boldsymbol{G_4}$ is indistinguishable, it remains to show that there exists a simulator that perfectly simulates $\boldsymbol{G_4}$ and uses $\mathcal{A}$ to win the strongSigForge game. In the following we describe in a concise way the simulator code.

Simulation of oracle queries

Signing queries: Upon $\mathcal{A}$ querying the oracle $\mathcal{O}_{\text{S}}$ on input m, $\mathcal{S}$ forwards m to its oracle $\mathsf{Sign}^{\mathsf{Sch}}$ and forwards its response to $\mathcal{A}$.

Random Oracle queries: Upon $\mathcal{A}$ querying the oracle $\mathcal{H}$ on input x, if $H[x] = \bot$, then $\mathcal{S}$ queries $\mathcal{H}^{\mathsf{Sch}}(x)$, otherwise the simulator returns $H[x]$.

Pre-Signing queries: 1) Upon $\mathcal{A}$ querying the oracle $\mathcal{O}_{\text{pS}}$ on input (m, Y), $\mathcal{S}$ forwards m to its oracle $\mathsf{Sign}^{\mathsf{Sch}}$ and receives the signature $\tilde{\sigma} = (r, s)$ where $r = \mathcal{H}^{\mathsf{Sch}}(pk \| K \| m)$.
2) If $\mathcal{H}$ has been previously queried on the input $(pk \| K \| m)$ or $(pk \| K \cdot Y \| m)$, $\mathcal{S}$ aborts.
3) $\mathcal{S}$ programs the random oracle $\mathcal{H}$ such that queries of $\mathcal{A}$ on the input $pk \| K \cdot Y \| m$ are answered with the value of $\mathcal{H}^{\mathsf{Sch}}(pk \| K \| m)$ and queries on the input $pk \| K \| m$ are answered with the value of $\mathcal{H}^{\mathsf{Sch}}(pk \| K \cdot Y \| m)$.
4) The simulator returns $\tilde{\sigma}$ to $\mathcal{A}$.

Challenge Phase: 1) Upon $\mathcal{A}$ outputting the message and public value (m, Y) as the challenge message, $\mathcal{S}$ queries the $\mathsf{Sign}^{\mathsf{Sch}}$ oracle on input m. Let $\sigma = (r, s)$ be the response where $r = \mathcal{H}^{\mathsf{Sch}}(pk \| K \| m)$, then $\mathcal{S}$ again programs the random oracle $\mathcal{H}$ such that queries of $\mathcal{A}$ on the input $pk \| K \cdot Y \| m$ are answered with the value of $\mathcal{H}^{\mathsf{Sch}}(pk \| K \| m)$ and queries on the input $pk \| K \| m$ are answered with the value of $\mathcal{H}^{\mathsf{Sch}}(pk \| K \cdot Y \| m)$.
2) Upon $\mathcal{A}$ outputting a forgery σ, the simulator outputs (m, σ) as its own forgery.

$\mathcal{S}^{\mathsf{Sign}^{\mathsf{Sch}}, \mathcal{H}^{\mathsf{Sch}}}(pk)$

$\mathcal{Q} := \emptyset$
$H := [\bot]$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m, Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\text{S}}(\cdot), \mathcal{O}_{\text{pS}}(\cdot,\cdot)}(pk)$
$H' := H$
$\tilde{\sigma} \leftarrow \mathsf{Sign}^{\mathsf{Sch}}(m)$
parse $\tilde{\sigma}$ as (r, s)
$K := g^s \cdot pk^{-r}$
if $H'[pk \| K \| m] \neq \bot$
or $H'[pk \| K \cdot Y \| m] \neq \bot$
Abort
$x := pk \| K \| m$
$H[pk \| K \cdot Y \| m] \leftarrow_{\$} \mathcal{H}^{\mathsf{Sch}}(x)$
$H[x] \leftarrow_{\$} \mathcal{H}^{\mathsf{Sch}}(pk \| K \cdot Y \| m)$
$\sigma \leftarrow \mathcal{A}(\tilde{\sigma}, Y)$
return (m, σ)

$\mathcal{O}_{\text{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}^{\mathsf{Sch}}(m)$
parse σ as (r, s)
$K := g^s \cdot pk^{-r}$
$x := pk \| K \| m$
$H[x] \leftarrow \mathcal{H}^{\mathsf{Sch}}(x)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{H}(x)$

if $H[x] = \bot$
$H[x] \leftarrow_{\$} \mathcal{H}^{\mathsf{Sch}}(x)$
return $H[x]$

$\mathcal{O}_{\text{pS}}(m, Y)$

$H' := H$
$\sigma \leftarrow \mathsf{Sign}^{\mathsf{Sch}}(m)$
parse $\tilde{\sigma}$ as (r, s)
$K := g^s \cdot pk^{-r}$
if $H'[pk \| K \| m] \neq \bot$
or $H'[pk \| K \cdot Y \| m] \neq \bot$
Abort
$x := pk \| K \| m$
$y := pk \| K \cdot Y \| m$
$H[y] \leftarrow_{\$} \mathcal{H}^{\mathsf{Sch}}(x)$
$H[x] \leftarrow_{\$} \mathcal{H}^{\mathsf{Sch}}(y)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

We emphasize that the main difference between the simulation and $\boldsymbol{G_4}$ are syntactical, namely instead of generating the public and secret keys and calculating the algorithm Sign_{sk} and the random oracle $\mathcal{H}$, $\mathcal{S}$ uses its oracles $\mathsf{Sign}^{\mathsf{Sch}}$ and $\mathcal{H}^{\mathsf{Sch}}$.

It remains to show that the signature output by $\mathcal{A}$ can be used by the simulator to win the strongSigForge game.

Claim: (m, σ) constitutes a valid forgery in game strongSigForge.

Proof: In order to prove this claim, we have to show that the tuple (m, σ) has not been output by the oracle $\mathsf{Sign}^{\mathsf{Sch}}$ before. Note that the adversary $\mathcal{A}$ has not previously made a query on the challenge message m to either $\mathcal{O}_{\mathrm{pS}}$ or $\mathcal{O}_{\mathrm{S}}$. Hence, $\mathsf{Sign}^{\mathsf{Sch}}$ is only queried on m during the challenge phase. If the adversary outputs a forgery σ which is equal to the signature $\tilde{\sigma}$ output by $\mathsf{Sign}^{\mathsf{Sch}}$ the adversary loses the game because this would not be valid signature given the programmed random oracle. Hence, $\mathcal{A}$ must output a valid signature $\sigma \neq \tilde{\sigma}$ and $\mathsf{Sign}^{\mathsf{Sch}}$ has never output σ on query m before, consequently (m, σ) constitutes a valid forgery for game $\mathsf{strongSigForge}$. ■

From the games $\boldsymbol{G_0} - \boldsymbol{G_4}$ we get that $\Pr[\boldsymbol{G_0} = 1] \leq \Pr[\boldsymbol{G_4} = 1] + 2\nu(n)$. Since $\mathcal{S}$ provides a perfect simulation of game $\boldsymbol{G_4}$, we obtain: $\mathsf{Adv}^{\mathcal{A}}_{\mathsf{aSigForge}} \leq \mathsf{Adv}^{\mathcal{S}}_{\mathsf{strongSigForge}} + 2\nu(n)$.

Generalized Bitcoin-Compatible Channels

Diff of current and previous submission.

***Abstract*—The widespread adoption of decentralized cryptocurrencies, such as Bitcoin or Ethereum, is currently hindered by their inherently limited transaction rate. One of the most prominent proposals to tackle this scalability issue are *payment channels* which allow mutually distrusted parties to exchange an arbitrary number of payments in the form of off-chain authenticated messages while posting only a limited number of transactions onto the blockchain. Specifically, two transactions suffice, unless a dispute between these parties occurs, in which case more on-chain transactions are required to restore the correct balance. Unfortunately, popular constructions, such as the Lightning network for Bitcoin, suffer from heavy communication complexity both off-chain and on-chain in case of dispute. Concretely, the communication overhead grows exponentially and linearly, respectively, in the number of applications that run in the channel.**

In this work, we introduce and formalize the notion of *generalized channels* for Bitcoin-like cryptocurrencies. Generalized channels significantly extend the concept of payment channels so as to perform off-chain any operation supported by the underlying blockchain. Besides the gain in expressiveness, generalized channels outperform state-of-the-art payment channel constructions in efficiency, reducing the communication complexity and the on-chain footprint in case of disputes to linear and constant, respectively.

We provide a cryptographic instantiation of generalized channels that is compatible with Bitcoin, leveraging *adaptor signatures* – a cryptographic primitive already used in the cryptocurrency literature but formalized as a standalone primitive in this work for the first time. We formally prove the security of our construction in the Universal Composability framework. Furthermore, we conduct an experimental evaluation, demonstrating the expressiveness and performance of generalized channels when used as building blocks for popular off-chain applications, such as channel splitting and payment-channel networks.

I. Introduction

Blockchain technologies have spurred increasing interest over the last years, enabling secure payments, and more generally computations, among mutually ~~distrustful~~ distrusting parties. At the core of them lies a decentralized consensus protocol, which establishes and maintains a distributed ledger that stores all transactions. An inherent drawback of their ~~dezentralized~~ decentralized approach, however, is its poor transaction throughput, which, for instance, in the case of Bitcoin is around ten transactions per second, three orders of magnitude lower than credit card networks. This severely limits the widespread adoption of blockchain technologies and their potential to cater for a large user base.

Among several recent proposals to tackle this scalability problem [18, 32, 4], payment channels [5] have emerged as one of the most promising and widely deployed solutions (see, e.g., the Lightning network [29] in Bitcoin and the Raiden Network [31] in Ethereum). A payment channel enables an arbitrary number of payments between users while committing only two transactions onto the blockchain, without compromising on security. In a bit more detail, focusing on Bitcoin and its Unspent Transaction Output (UTXO) model, a payment channel between Alice and Bob is first created by a single on-chain transaction that locks bitcoins into a multi-signature address controlled by both users. They can then pay to each other (possibly many times) by exchanging authenticated off-chain messages that represent an update of their share of coins in the multi-signature address. The payment channel is finally closed when a user decides to submit the last authenticated distribution of coins to the blockchain.

Payment channels serve as a building block for a variety of off-chain services, which aim at offering better connectivity, as establishing a different channel for each possible payee would be cumbersome and financially unsustainable (e.g., one would have to lock coins in each channel). For instance, payment channel networks (PCNs) [29, 25] link payment channels to each other, forming a graph through which payments can be routed along multi-hop paths. Payment channel hubs [20] offer a different connectivity solution, with an untrusted third party acting as proxy between any pair of users and yet unable to compromise either the security or the privacy of transactions. Payment channels also serve as building block for atomic swaps [19] where two users can atomically trade their coins.

On a technical level, the key challenge in designing Bitcoin-compatible payment channels is how to revoke old states: as previously mentioned, the distribution of coins in the channel changes over time due to payments between the end-points, which poses the problem of how to prevent one of the two parties from publishing an old, financially more advantageous, state on the blockchain. The state-of-the-art approach, put forward in the Lightning Network, is based on a punishment mechanism which allows the cheated party to claim all coins from the channel. The current cryptographic realization, however, suffers from two central drawbacks, which undermine its ability to cater for the growing number of applications built on top of them:

State duplication. In order to protect parties from each other, the state of the channel is duplicated. Each copy has a ~~built in~~ built-in punishment mechanism for one of the parties. State updates have to be propagated on both duplicates, leading to cumbersome and expensive protocols. This issue becomes even more pressing when users decide to use the same channel for multiple applications (e.g., [13]), which they need to update independently in parallel. For that, the channel is recursively split into *sub-channels* (with each additional application requiring a further sub-channel splitting), each of which again contains two copies of the state to faithfully point out the misbehaving user. This unfortunately makes

the number of transactions ruling the distribution of coins to grow exponentially in k where k is the number of off-chain applications built on top of each other.

Output-based revocation. Since each (sub-)channel can be used to process multiple applications, each corresponding (sub-)channel state may contain multiple outputs defining how coins can be spent. The current punishment approach follows a "punish-per-output" pattern which means that if an old state appears on the blockchain, the cheated party has to claim money from each output of the state separately, leading to a possibly large number of on-chain transactions, linear in the number of applications represented in the revoked state.

This state-of-affairs leads to the following question: *is it possible to design a simple, efficient, and expressive Bitcoin-compatible payment channel, i.e., one that reduces the channel state to be stored by each party as well as the revocation overhead on the blockchain to a minimum, while supporting a large class of off-chain applications?*

a) Our contributions: In this work, we give a positive answer to the above question, designing and formalizing a novel payment channel scheme. Concretely, our contributions are summarized below.

- We introduce the notion of *generalized channels*, which generalizes payment channels to support any application expressed in the scripting language of the underlying blockchain, thereby enhancing their expressiveness. One may view a generalized channel as a 2-party ledger for off-chain operations offering the same functionality as the underlying blockchain. Hence, our construction extends the concept offered by state channels for Ethereum [26, 12] to cryptocurrencies with limited ~~scirpting~~ scripting capabilities such as Bitcoin.
- We design a novel revocation mechanism, which relies on adaptor signatures [24], to avoid state duplication thereby reducing the number of states (and thus the communication complexity) of off-chain protocols from exponential to linear in the number of applications. Additionally, our revocation mechanism based on *punish-then-split* enables revocation through a single output (and thus a single transaction), thereby reducing the overhead on the blockchain from linear to constant.
- We provide a cryptographic instantiation of generalized channels based on ECDSA-based adaptor signatures as well as Schnorr-based adaptor signatures. Our cryptographic instantiation is thus supported by virtually all cryptocurrencies, including Bitcoin.
- We formalize the security and functionality of generalized channels as ideal functionalities in the Universal Composability (UC) framework [7] and prove the security of our construction in the UC framework. While doing so, we provide the first (game-based) security definition for adaptor signatures. We ~~beleive~~ believe that the formalization of adaptor signatures is of independent interest.
- We implemented our protocols and conducted an experimental evaluation, demonstrating how to use generalized channels to implement popular off-chain applications, like payment channel network and channel splitting, and characterizing the gains in performance as compared to the construction from the Lightning Network.

b) Organization: The rest of the paper is organized as follows. In Section II, we introduce the required background and overview our solution. In ~~?? C0d, we formally define~~ Section III, we describe our cryptographic instantiation of generalized channels ~~and our model in the UC framework~~. In Section IV, we introduce the adaptor signatures and the (game-based) security definitions. In ~~Section III, we describe our cryptographic instantiation of~~ Section V, we elaborate on our UC modeling approach. In Section VI, we show how generalized channels can be leveraged to build different off-chain applications. In Section VII, we analyze the performance of generalized channels. We conclude in Section VIII. –

II. Background and Solution Overview

A. Background and notation

Throughout this work, we use the following notation for *attribute tuples*. Let T be a tuple of values which we call attributes. Each attribute in T is identified using a unique keyword attr and referred to as $T.\mathsf{attr}$.

a) Outputs and transactions: In this work, we focus on blockchains based on the Unspent Transaction Output (UTXO) model, such as Bitcoin. In the UTXO model, coins are held in *outputs*. Formally, an output θ is an attribute tuple $(\theta.\mathsf{cash}, \theta.\varphi)$, where $\theta.\mathsf{cash}$ denotes the amount of coins associated to the output and $\theta.\varphi$ denotes the conditions that need to be satisfied to spend the output. The condition $\theta.\varphi$ can contain any script supported by the considered blockchain. We say that a user P controls or owns an output θ if $\theta.\varphi$ contains a signature verification w.r.t. the public key of P.

A *transaction* transfers coins across outputs meaning that it maps (possibly multiple) existing outputs to a list of new outputs. To avoid confusion, the existing outputs that fund the transactions are called *transaction inputs*. Formally, a transaction tx is an attribute tuple consisting of the following attributes $(\mathsf{tx.txid}, \mathsf{tx.Input}, \mathsf{tx.Output}, \mathsf{tx.Witness})$. The attribute $\mathsf{tx.txid} \in \{0,1\}^*$ is the identifier of the transaction and is calculated as $\mathsf{tx.txid} := \mathcal{H}([\mathsf{tx}])$, where $\mathcal{H}$ is a hash function modeled as a random oracle and $[\mathsf{tx}]$ is the *body of the transaction* defined as $[\mathsf{tx}] := (\mathsf{tx.Input}, \mathsf{tx.Output})$. The attribute $\mathsf{tx.Input}$ is a vector of strings identifying all inputs of tx. The attribute $\mathsf{tx.Output} = (\theta_1, \ldots, \theta_n)$ is a vector of new outputs. Finally, the attribute $\mathsf{tx.Witness} \in \{0,1\}^*$ contains the witness of the transaction allowing to spend the inputs.

To ease the readability, we illustrate the transaction flows throughout the paper ~~in the form of charts. Let us here~~ using charts. We now define and explain the symbols and notation used in the charts. A transaction is represented as a rectangle with rounded corners. Doubled edge rectangles represent transactions published on the blockchain, while single edge rectangles are transactions that could be published on the blockchain but they are not (yet). Transaction outputs are depicted as a box inside the transaction. The value of the

output is written inside the output box and the output condition is written above the arrow coming from the output.

Conditions of transaction outputs might be fairly complex and hence it would be cumbersome to spell them out above the arrows. Instead, for conditions that are used frequently, we define the following abbreviated notation. If the output script contains (among other conditions) signature verification w.r.t. some public keys $pk_1, \ldots, pk_n$, we write all the public keys *below* the arrow and the remaining conditions *above* the arrow. Hence, information below the arrow denotes "who owns the output" and information above denotes "additional spending conditions". If the output script contains a check of whether a given witness hashes to a predefined hash value h, we express this by simply writing the hash value h *above* the arrow. Moreover, if the output script contains a relative time lock, i.e. a condition that is satisfied if and only if at least t rounds passed since the transaction was published, we write the string "$+t$" *above* the arrow. Finally, if the output script φ can be parsed as $\varphi = \varphi_1 \vee \cdots \vee \varphi_n$ for some $n \in \mathbb{N}$, we add a diamond shape to the corresponding transaction output. Each of the subconditions φ_i is then written above a separate arrow. An example is given in Fig. 1.

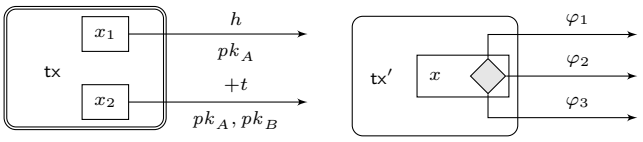


Fig. 1. (Left) Transaction $\mathtt{tx}$ is published on the blockchain. The output of value x_1 can be spent by a transaction containing a preimage of h and signed w.r.t. pk_A. The output of value x_2 can be spent by a transaction signed w.r.t. pk_A and pk_B but only if at least t rounds passed since $\mathtt{tx}$ was accepted by the blockchain. (Right) Transaction $\mathtt{tx}'$ is not published on the ledger. Its only output, which is of value x, can be spent by a transaction whose witness satisfies the output condition $\varphi_1 \vee \varphi_2 \vee \varphi_3$.

b) Payment channels: A payment channel enables several transactions between two users without committing every single transaction to the blockchain. The cornerstone of payment channels is depositing coins into an output controlled by two users, who then authorize new deposit balances in a peer-to-peer fashion while having the guarantee that all coins are refunded at a mutually agreed time. In a bit more detail, a payment channel has three operations: *open*, *update* and *close*.

First, assume that Alice and Bob want to create a payment channel with an initial deposit of x_A and x_B coins respectively. For that, Alice and Bob agree on a *funding transaction* (that we denote by $\mathtt{TX_f}$) that sets as inputs two outputs controlled by Alice and Bob holding x_A and x_B coins respectively and transfers them to an output controlled by both Alice and Bob. When $\mathtt{TX_f}$ is added to the blockchain, the payment channel between Alice and Bob is effectively open.

Assume now that Alice wants to pay $\alpha \leq x_A$ coins to Bob. For that, they create a new *commit transaction* $\mathtt{TX_c}$ representing the commitment from both users to the new channel state. The commit transaction spends the output of $\mathtt{TX_f}$ into two new outputs: (i) one holding $x_A - \alpha$ coins controlled by Alice; and (ii) the other holding $x_B + \alpha$ coins controlled by Bob. Finally, parties exchange the signatures on the commit transaction. At this point, Alice (resp. Bob) could add $\mathtt{TX_c}$ to the blockchain. Instead, they keep it locally in their memory and overwrite it when they agree on another commitment transaction $\overline{\mathtt{TX_c}}$ representing a newer channel state. This, however, leads to several commitment transactions that can possibly be added to the blockchain. Since all of them are spending the same output, only one can be accepted by the blockchain. Since it is impossible to prevent a malicious user from publishing an old commit transaction, payment channels require a mechanism that punishes such behavior.

Lightning Network [29], the state-of-the-art payment channel network for Bitcoin, implements such mechanism by introducing two commitment transactions per channel update, each of which contains a punishment mechanism for one of the users. In more detail (see also Fig. 2), the output of $\mathtt{TX_c^A}$ representing Alice's balance in the channel has a special condition. Namely, it can be spent by Bob if he presents a preimage of a hash value h_A or by Alice if certain number of rounds passed since the transaction was published. During a channel update, Alice chooses a value r_A, called the *revocation secret*, and presents the hash $h_A := \mathcal{H}(r_A)$ to Bob. Knowing h_A, Bob can create and sign the commit transaction $\mathtt{TX_c^A}$ with the ~~built in~~ built-in punishment for Alice (analogously for Bob and $\mathtt{TX_c^B}$). During the next channel update, parties first commit to the new state by creating and signing $\overline{\mathtt{TX_c^A}}$ and $\overline{\mathtt{TX_c^B}}$, and then *revoke* the old state by sending the revocation secrets to each other thereby enabling the punishment mechanism. If a malicious Alice now publishes the old commit transaction $\mathtt{TX_c^A}$, Bob can spent both of its outputs and hence claim all coins locked in the channel.

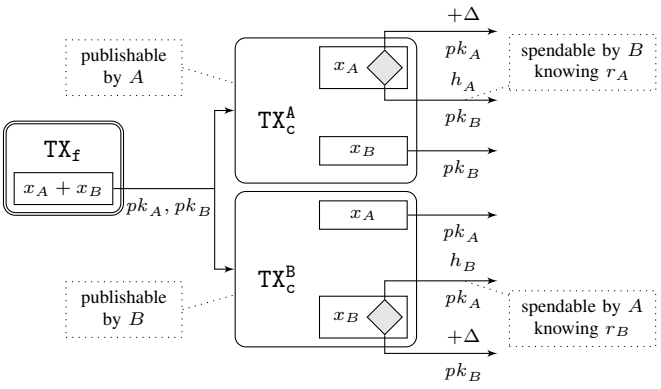


Fig. 2. A Lightning style payment channel where A has x_A coins and B has x_B coins. The values h_A and h_B correspond to the hash values of the revocation secrets r_A and r_B. The value of Δ upper bounds the time needed to publish a transaction on a blockchain.

B. Solution Overview

The goal of our work is to extend the idea of payment channels such that parties can perform essentially *any* operation that they could do on-chain and not only pay to each other. Technically, this means that we want the commit transaction to contain arbitrary many outputs with arbitrary

conditions (as long as they are supported by the underlying blockchain). The main question we need to answer when designing such channels, which we call *generalized channels*, is how to implement the revocation mechanism in this case.

a) Revocation per update: The first idea would be to extend the revocation mechanism of payment channels explained above such that *each output* of $\mathtt{TX}_c^A$ contains a punishment mechanism for Alice (analogously for Bob). This approach is taken by the Lightning network [29] whose channels support (multiple) hash-time lock payments.[1] While this solution works, it has several disadvantages: (i) If one party, say Alice, cheats and publishes an old commit transaction $\mathtt{TX}_c^A$, Bob has to spend all outputs of $\mathtt{TX}_c^A$ in order to punish Alice for her misbehavior. Although Bob could group some of them within a single transaction (up to the transaction size limit), he might be forced to publish multiple transactions thereby paying high transaction fees in order to punish Alice; (ii) such revocation mechanism requires a high on-chain footprint not only for $\mathtt{TX}_c^A$, but also for Bob to get the coins from the outputs. –

Our goal is to design a punishment mechanism whose on-chain footprint and potential transaction fees are independent of the channel state, i.e., the number and type of outputs in the channel. To this end, we propose the *punish-then-split* mechanism which separates the punishment mechanism from the actual outputs. In a nutshell, the commit transaction $\mathtt{TX}_c^A$ has now only one output dedicated to the punishment mechanism which can be spent (i) immediately by Bob, if he proves that the commit transaction was old (i.e. he knows the revocation secret r_A of Alice); or (ii) after certain number of rounds by a *split transaction* $\mathtt{TX}_s^A$ controlled by both parties and containing all the outputs of the channel (i.e. representing the channel state). Hence, if $\mathtt{TX}_c^A$ is published on the blockchain, Bob has some time to punish Alice if the commit transaction was old. If Bob does not use this option, any of the parties can publish the split transaction $\mathtt{TX}_s^A$ representing the channel state. Analogously for $\mathtt{TX}_c^B$.

b) One commit transactions per channel update: Another drawback of the Lightning style revocation mechanism is the need for two commit transactions for the same channel state. While this is not an issue for simple payment channels, for generalized channels it might cause redundancy in terms of communication and computational costs. This comes from the fact that generalized channels support arbitrary output conditions and hence can be used as a source of funding for, e.g., another off-chain channel as we discuss later in this work (see Section VI). Such off-chain channel would, however, have to "exist" twice. Once considering $\mathtt{TX}_c^A$ being eventually published on-chain and once considering $\mathtt{TX}_c^B$. Therefore, a natural goal is to construct generalized channels that require only one commit transaction.

The naive approach to design such a single commit transaction $\mathtt{TX}_c$ would be to simply "merge" the transactions $\mathtt{TX}_c^A$ and $\mathtt{TX}_c^B$. Such $\mathtt{TX}_c$ could be spent (i) by Alice if she knows Bob's revocation secret; (ii) by Bob if he knows Alice's revocation secret or (iii) by the split transaction $\mathtt{TX}_s$ representing the channels state after some time. This simple proposal does not work, however, since it allows parties to misuse the punishment mechanism as follows. A malicious Alice could publish an old commit transaction $\mathtt{TX}_c$ and since she knows Bob's revocation secret, she could immediately try to punish Bob. In order to prevent such undue punishment of honest Bob, we need to make sure that Alice can use the punishment mechanism only if it was Bob publishing $\mathtt{TX}_c$. In other words, our punishment mechanism built in $\mathtt{TX}_c$ requires the punishing party to prove that (i) this commit transaction was old and (ii) this commit transaction was published by the other party.

The main idea how to implement the requirement (ii), is to force the party publishing $\mathtt{TX}_c$ to reveal some secret, which we call *publishing secret*, that could be used by the other party as a proof. We achieve this by leveraging the concept of an *adaptor signature scheme* – a signature scheme that allows a party to *pre-sign* a message w.r.t. some statement Y of a hard relation.[2] Such pre-signature can be adapted into a valid signature by anyone knowing a witness for the statement Y. Moreover, knowing both the pre-signature and the adapted full signature, it is possible to extract a witness for Y. In our context, adaptor signatures allow parties of the generalized channels to express the following: "I give you my *pre-signature* on $\mathtt{TX}_c$ which you can turn into a valid signature and publish $\mathtt{TX}_c$ on-chain. But this will reveal your publishing secret to me."

To conclude, our solution, depicted in Fig. 3, requires only one commit transaction $\mathtt{TX}_c$ per update. The commit transaction has one output that can be spent (i) by Alice if she knows Bob's revocation secret r_B *and publishing secret* y_B; (ii) by Bob if he knows Alice's revocation secret r_A *and publishing secret* y_A or (iii) by the split transaction $\mathtt{TX}_s$ representing the channels state after some time. In the depicted construction we assume that that the statement/witness pairs used for the adaptor signature scheme are public/secret keys of the blockchain signature scheme. Hence, testing if a party knows a publishing secret can be done by requiring a valid signature w.r.t. this public key. Let use emphasize that public/secret keys can also be used for the revocation mechanism instead of the hash/preimage pairs. This is actually preferable since the punishment output script will only consist of signatures and thereby we require less complex scripting language.

III. Generalized Channel Construction

~~In this section we formalize the notion of~~

Before introducing the protocol for generalized channels ~~and their functionality. We first introduce~~, we overview the main cryptographic building blocks. Moreover, we establish some basic notation and ~~our security model which closely follows the previous works on off-chain channels [9, 10, 12]~~ present the security properties of interest.

[1] Hash-time lock payment is a conditional payment that is performed conditioned on the receiver presenting a preimage of a hash function before a certain time.

[2] On a high level, a statement/witness relation is hard, if given a statement Y is it computationally hard to find a witness y.

Sections III and V are swapped. Changes in the section about our protocol:
* moved here: necessary background and notation, informal security properties
* rewritten: high level protocol description
* new: pseudo-code description

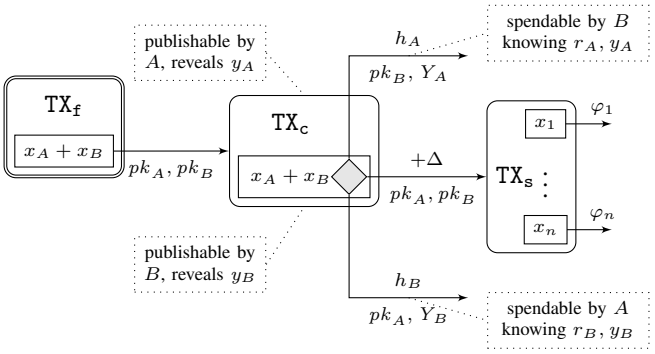


Fig. 3. A generalized channel in the state $((x_1, \varphi_1), \ldots, (x_n, \varphi_n))$. The values h_A and h_B correspond to the hash values of the revocation secrets r_A and r_B. The value of Δ upper bounds the time needed to publish a transaction on a blockchain. If $\mathtt{TX_c}$ is published by A, publishing secret y_A corresponding to Y_A is revealed. If $\mathtt{TX_c}$ is published by B, publishing secret y_B corresponding to Y_B is revealed.

Originally in section:"Adaptor signatures"

A. ~~Notation and security model~~Building blocks

~~To formally model the security of our channel construction~~

a) Digital signatures: A signature scheme consists of three algorithms $\Sigma = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$, where: (i) $\mathsf{Gen}(1^n)$ gets as input 1^n (n is the security parameter) and outputs the secret and public keys (sk, pk); (ii) $\mathsf{Sign}_{sk}(m)$ gets as input the secret key sk and a message $m \in \{0,1\}^*$ and outputs the signature σ; and (iii) $\mathsf{Vrfy}_{pk}(m; \sigma)$ gets as input the public key pk, a message m and a signature σ, and outputs a bit b.

A signature scheme must fulfill correctness, i.e. it must hold that $\mathsf{Vrfy}_{pk}(m; \mathsf{Sign}_{sk}(m)) = 1$ for all messages m and valid key pairs (sk, pk). In this work, we use ~~a synchronous version of the global UC framework (GUC)~~ signature schemes that satisfy the notion of strong existential unforgeability under chosen message attack (or SUF–CMA). On a high level, SUF–CMA guarantees that an adversary on input the public key pk and with access to a signing oracle, cannot produce a *new* valid signature on any message m.

b) Hard relation: We next recall the definition of a hard relation R with statement/witness pairs (Y, y). Let L_R be the associated language defined as $L_R := \{Y \mid \exists y \text{ s.t. } (Y, y) \in R\}$. We say that R is a *hard relation* if the following holds: (i) There exists a PPT sampling algorithm $\mathsf{GenR}(1^n)$ that on input 1^n outputs a statement/witness pair $(Y, y) \in R$; (ii) The relation is poly-time decidable; (iii) For all PPT ~~[8] which extends the standard UC framework [7] by allowing for a global setup. Monetary transactions are handled by a global ledger $\mathcal{L}(\Delta, \Sigma)$, where Δ is an upper bound on the blockchain delay (number of rounds it takes to publish a transaction)~~ $\mathcal{A}$ the probability of $\mathcal{A}$ on input Y outputting y is negligible.

c) Adaptor signature: An adaptor signature scheme wrt. a hard relation R and a signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ consists of four algorithms $\Xi_{R,\Sigma} = (\mathsf{pSign}, \mathsf{Adapt}, \mathsf{pVrfy}, \mathsf{Ext})$, where: (i) $\mathsf{pSign}_{sk}(m, Y)$ gets as input a secret key sk, message $m \in \{0,1\}^*$ and statement $Y \in L_R$, and outputs a pre-signature $\tilde{\sigma}$; (ii) $\mathsf{pVrfy}_{pk}(m, Y; \tilde{\sigma})$ gets as input a public key pk, message

New: introduced syntax for adaptor signatures

$m \in \{0,1\}^*$, statement $Y \in L_R$ and ~~Σ defines the signature scheme used by the blockchain.We denote by $\mathcal{P}$ the set of all parties participating in the protocols considered in this work.For more details about our model, we refer the reader to Appendix C.~~

~~We define a~~ pre-signature $\tilde{\sigma}$, and outputs a bit b; (iii) $\mathsf{Adapt}(\tilde{\sigma}, y)$ gets as input a pre-signature $\tilde{\sigma}$ and witness y, and outputs a signature σ; and (iv) $\mathsf{Ext}(\sigma, \tilde{\sigma}, Y)$ gets as input a signature σ, pre-signature $\tilde{\sigma}$ and statement $Y \in L_R$, and outputs a witness y such that $(Y, y) \in R$, or $\perp$. A secure adaptor signature scheme must, on a high level, satisfy the following properties: *existential unforgeability under chosen message attack* (or EUF–CMA) saying that no ppt adversary $\mathcal{A}$ is able to forge a signature for a fresh message m even if $\mathcal{A}$ knows a pre-signature on m w.r.t. a random statement $Y \in L_R$ (i.e., $\mathcal{A}$ does not know the corresponding y); *pre-signature adaptability* guaranteeing that any valid pre-signature w.r.t. Y can be completed given the correct witness y; and *witness extractability* ensuring that given a valid signature/pre-signature pair $(\sigma, \tilde{\sigma})$ for message/statement (m, Y), the Ext algorithm extracts the corresponding witness y. We formally define and construct an adaptor signature scheme in Section IV.

Originally in section "Generalized Channels"

B. Notation and security goals

A *generalized channel* γ as an attribute tuple $(\gamma.\mathsf{id}, \gamma.\mathsf{users}, \gamma.\mathsf{cash}, \gamma.\mathsf{st})$, where $\gamma.\mathsf{id} \in \{0,1\}^*$ is the identifier of the channel, $\gamma.\mathsf{users} \in \mathcal{P}^2$ defines the identities of the channel users, $\gamma.\mathsf{cash} \in \mathbb{R}^{\geq 0}$ represents the total amount of coins locked in this channel and $\gamma.\mathsf{st} = (\theta_1, \ldots, \theta_n)$ is the state of the channel composed of a list of *outputs*. Each output θ_i has two attributes: the value $\theta_i.\mathsf{cash} \in \mathbb{R}^{\geq 0}$ representing the amount of coins and the function $\theta_i.\varphi\colon \{0,1\}^* \to \{0,1\}$ representing the spending condition of the output. For convenience, we define a function $\gamma.\mathsf{otherParty}\colon \gamma.\mathsf{users} \to \gamma.\mathsf{users}$ defined as $\gamma.\mathsf{otherParty}(P) := Q$ for $\gamma.\mathsf{users} = \{P, Q\}$.

C. ~~Ideal Functionality~~

~~We capture the desired functionality of a~~ A generalized channel protocol ~~as an ideal functionality $\mathcal{F}$ interacting with parties from the~~ runs between parties from a set $\mathcal{P}$~~, with the adversary $\mathcal{S}$ (called the simulator) and observes the global ledger functionality $\mathcal{L}$. In a bit more detail, if a party wants to perform an action (such as open a new channel), it sends a message to $\mathcal{F}$ who executes the action and informs the party about the result. The execution might leak information to the adversary who may also influence the execution.The possible leakage and influence are modelled via the interaction with $\mathcal{S}$.Finally, $\mathcal{F}$ can observe the global ledgerand hence verify that a certain transaction appeared on-chain or that a given party owns certain amount of coins. The latter is done by checking if there exists an unspent output whose condition requires signature of (only) the given party P. We denote such script $\mathtt{One\text{-}Sig}_{pk_P}$~~.

~~As a first step towards defining our functionality, we identify the~~ We assume that all parties have access to a global *ledger*

$\mathcal{L}(\Delta, \Sigma)$, where Δ upper bounds the blockchain delay, i.e., how long it takes to process a transaction posted on the ledger, and Σ defines the signature scheme used by the blockchain. We formally define the ideal behavior of a generalized channelprotocol as an *ideal functionality* in Appendix D. Here we informally introduce the most important security and efficiency notions of interest~~that a functionality should provide. To this end, we use the following terminology. A~~

Originally in section "Generalized Channels"

Consensus on creation: Parties in γ.users ~~output the message UPDATED/CREATED. In addition a state st is called *enforced* on the ledger if a transaction with this state appears on the ledger.~~ **Consensus on creation:** ~~A~~ reach agreement whether the channel is created or not after an a-priori bounded number of rounds (the bound may depend on the blockchain delay Δ). Moreover, a channel γ ~~can be successfully created if and~~ is successfully created only if both parties in ~~the set~~ γ.users agree with the creation.

Consensus on update: Parties in γ.users reach agreement on channel update acceptance or rejection after an a-priori bounded number of rounds (the bound may depend on the blockchain delay Δ). Moreover, a channel γ ~~can be successfully updated if and~~ is successfully updated only if both parties in ~~the set~~ γ.users agree with the update.

Instant finality with punish: ~~If a channel γ is successfully updated to the state γ.st and this is the latest successful update, then an~~ An honest party $P \in \gamma$.users has the guarantee that either ~~γ.st~~ the current state of the channel can be enforced on the ledger, or P can enforce a state where she gets all γ.cash coins.[3]

Optimistic update: If both parties in γ.users are honest, a successful update takes a constant number of rounds (independent of the blockchain delay Δ). In other words, if both parties are honest, channel update is performed without any blockchain interaction.

~~Having the guarantees identified above in mind, we now design our ideal functionality $\mathcal{F}$. We assume that $\mathcal{F}$ maintains a set Γ, where it stores created channels in their latest state and the corresponding funding transaction tx. We sometimes treat Γ as a function which on input id outputs (γ, tx) s. t. $\gamma.\mathsf{id} = id$ if such channel exists and $\perp$ otherwise. To keep $\mathcal{F}$ generic, we parameterized it by two values T~~

C. *Protocol description*

We now present a concrete protocol for generalized channels that requires only one commit transaction, i.e., implements the punish-then-split mechanism. This is achieved by utilizing an adaptor signature scheme $\Xi_{R,\Sigma} = (\mathsf{pSign}, \mathsf{Adapt}, \mathsf{pVrfy}, \mathsf{Ext})$ for signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ used by the underlying ledger and a hard relation R. Our protocol consists of four subprotocols: Create, Update, Close and Punish. We present each subprotocol separately by providing both a high level as well as a pseudo-code description (cf. Fig. 5

[3]A state st is called *enforced* on the ledger if a transaction with this state appears on the ledger.

Rewritten: protocol description
New: added proof intuitions

). Throughout this section, we assume that statement/witness pairs of R used by $\Xi_{R,\Sigma}$ are also the public/secret keys of the signature scheme. We will later show how to design an ECDSA based adaptor signature that satisfies this condition We discuss how to modify our protocol if this assumption does not hold in the supplementary material [30].

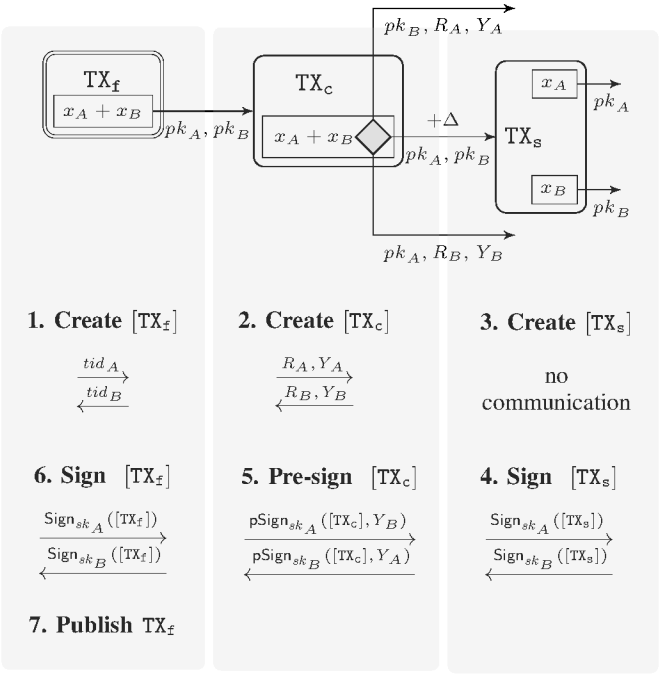


Fig. 4. Schematic description of the channel creation protocol.

a) Channel creation: In order to create a channel ~~creation might require more communication rounds than old staterevocation~~γ, the users of the channel, say A and B, have to agree on the body of the funding transaction $[\mathtt{TX_f}]$, mutually commit to the first channel state defined by $\gamma.\mathsf{st} = ((x_A, \mathtt{One\text{–}Sig}_{pk_A}), (x_B, \mathtt{One\text{–}Sig}_{pk_B}))$, and sign and publish the funding transaction $\mathtt{TX_f}$ on the ledger. Here $\mathtt{One\text{–}Sig}_{pk}$ represents the script that verifies that the transaction is correctly signed w.r.t. the public key pk. Once $\mathtt{TX_f}$ is published, the channel creation is completed. Looking at Fig. 4, one can summarize the creation process as a step-by-step creation of transaction bodies from left to right, and then a step-by-step signature exchange on the transaction bodies from right to left. Let us elaborate on this in more detail.

Step 1: To prepare $[\mathtt{TX_f}]$, parties need to inform each other about their funding sources, i.e., exchange the transaction identifiers tid_A and tid_B. Each party can then locally create $[\mathtt{TX_f}]$ with $\{tid_A, tid_B\}$ as input and output requiring the signature of both A and B. **Step 2:** Parties can now start committing to the initial channel state. To this end, ~~we give the power to the simulator to "speed-up" the process when possible. The parameter k defines the number of ways the channel state γ.st can be published on~~ each party $P \in \{A, B\}$ first generates a *revocation public/secret*

pair $(R_P, r_P) \leftarrow \mathsf{GenR}$ and *publishing public/secret* pair $(Y_P, y_P) \leftarrow \mathsf{GenR}$. The public values R_P and Y_P are sent to the ledger.As discussed in Section II, in this work we present a protocol realizing the functionality for $k = 1$ (see Fig. 3). Lightning style generalized channels (see Fig. 2) would be a candidate protocol for $k = 2$. Before we present $\mathcal{F}(T, k)$ formally, we discuss it on a high level and argue why it captures the aforementioned security and efficiency properties. In the text below, we abbreviate $\mathcal{F} := \mathcal{F}(T, k)$.

b) Create: If $\mathcal{F}$ receives a message of the form $(\mathtt{CREATE}, \gamma, tid_P)$ from both parties in γ.users within T rounds, it expects a channel funding transaction to appear on the ledger $\mathcal{L}$ other party. Each party can now locally generate the body of the commit transaction $[\mathtt{TX_c}]$ which spends $\mathtt{TX_f}$ and can be spent by a transaction satisfying one of these conditions:

Punish A**:** It is correctly signed w.r.t. pk_B, Y_A, R_A;
Punish B**:** It is correctly signed w.r.t. pk_A, Y_B, R_B;
Channel state: It is correctly signed w.r.t. pk_A and pk_B, and at least Δ rounds have passed since $\mathtt{TX_c}$ was published.

Steps 3+4: Using the transaction identifier of $\mathtt{TX_c}$, parties can generate and exchange signatures on the body of the split transaction $\mathtt{TX_s}$ which spends $\mathtt{TX_c}$ and whose output is equal to γ.st (i.e., the coins that are owned by A and B). **Step 5:** Parties are now prepared to complete the committing phase by *pre-signing* the commit transaction to each other. This means that party A executes the pSign_{sk_A} on message $[\mathtt{TX_c}]$ and statement Y_B and sends the pre-signature to B (analogously for B). **Step 6:** If valid pre-signatures are exchanged (validity is checked using the pVrfy algorithm), parties exchange signatures on the funding transaction and post it on the ledger in **Step 7**. If the funding transaction is accepted by the ledger, channel creation is successfully completed.

The question is what happen if one of the parties misbehaves during the creation process by aborting or sending a malformed message (w.l.o.g. let B be the malicious party). If the misbehavior happens before A sends her signature on $\mathtt{TX_f}$ (i.e., before step 6), party A can safely conclude that the creation failed. If the misbehavior happens during step 6, A is in a hybrid situation. She cannot post $\mathtt{TX_f}$ on-chain as she does not have B's signature which is needed to spend tid_B. However, since she already sent her signature on $\mathtt{TX_f}$ to B, she has no guarantee that B will not post $\mathtt{TX_f}$ later. In order to resolve this issue, our protocol instructs A to spend her outputs tid_A. Now within Δ rounds, tid_A is spent. Either by the transaction posted by A (in which case creation failed) or by $\mathtt{TX_f}$ posted by B (in which case creation succeeded). Such transaction must spend both funding sources (defined by transaction identifiers tid_P, tid_Q)and containing one output of the value γ.cash. If this is true, then $\mathcal{F}$ stores this transaction together with the

Security of Create: Since both parties have to sign the funding transaction, signature unforgeability guarantees that the creation can be successful only if both parties agree. As discussed above, an honest party can ensure that within fixed number of rounds the channel γ in the set Γ and informs both parties about the successful channel creation via the message $(\mathtt{CREATED}$. Since a $\mathtt{CREATE}$ message is required from both parties, "creation either succeeds or fails. Hence consensus on creation " holds.

Let us briefly argue that also instant finality holds after the channel creation, meaning that each of the two parties (alone) is able to unlock her coins from the channel at any time. The pre-signature adaptability property of Ξ guarantees that after a successful channel creation, each party P is able to adapt the pre-signature of the other party Q on $[\mathtt{TX_c}]$ by using the publishing secret value y_P (corresponding to Y_P). Party P can now sign $[\mathtt{TX_c}]$ herself and post $\mathtt{TX_c}$ on the ledger. Since parties never signed any other transaction spending $\mathtt{TX_f}$, the posted $\mathtt{TX_c}$ will be accepted by the ledger within Δ rounds.

Let us stress that parties have not revealed their revocation secrets, i.e, the values r_P and r_Q, to each other yet. None of the two parties is hence able to use the punishment mechanism of the published commit transaction. This implies that after Δ rounds, P can post the split transaction $\mathtt{TX_s}$ on the ledger by which she unlocks her x_P coins.

b) Update: The channel update is initiated by one of the parties P (called the *initiating party*) via a message $(\mathtt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}})$. The parameter id identifies the channel to be updated, $\vec{\theta}$ represents the new channel state and t_{stp} denotes the number of rounds needed by the parties to setup off-chain objects (e.g. new channels or hash-time lock contracts) that are being built on top of the channel via this update request. The update is structured into two phases: In order to update a created channel γ to a new state, represented by a vector of output scripts $\vec{\theta}$, parties have to (i) the prepare phase, and agree on the new commit and split transaction that represent the new state (ii) the revocation phase. Intuitively, the prepare phase models the fact that both parties first agree on the new channel state and get time to setup the off-chain objects on top of this new state. The revocation phase models invalidate the old commit transaction. Part (i) is very similar to the agreement on the initial commit and split transaction as described in the creation protocol (**Steps 2-5** in Fig. 4). There is one major difference coming from the fact that an update is only completed once the two parties invalidate the previous channel state the new channel state $\vec{\theta}$ can contain outputs that fund other off-chain applications (such as sub-channels).[4] In order to setup these applications, the identifier of the new split transaction is needed. To this end, parties first prepare the commit (**Steps 2+3**) to learn the desired identifier and set up all applications off-chain. Once this is done, which is signaled by $\mathtt{SETUP\text{-}OK}$, parties execute the second part of the committing phase (**Steps 4+5**). To realize part (ii) in which the punishment mechanism of the old commit transaction is activated, parties simply exchange the revocation secrets corresponding to the previous commit transaction which completes the update. Note that in this optimistic case when both parties are honest, update

[4] This is not the case during channel creation since we assume that the initial channel state consist of two accounts only.

is performed entirely off-chain. ~~We detail these two phases in the following.~~

~~The prepare phase starts when $\mathcal{F}$ receives a vector of transaction identifiers $\vec{tid} = (tid_1, \ldots, tid_k)$ from $\mathcal{S}$~~We now discuss what happens if one party misbehaves during the update.[5] ~~In the optimistic case it is completed within $3T + t_{\mathsf{stp}}$ rounds and ends when the initiating party P receives an `UPDATE_OK` message from $\mathcal{F}$. The setup phase can be aborted by both the initiating party P and the other party Q. In the ideal world this is achieved by P not sending the `SETUP_OK` and by Q not sending the `UPDATE_OK` message, respectively. This models two things. Firstly, the fact that Q might not agree with the proposed update and secondly, the fact that setting up off-chain objects might fail in which case~~ As long as none of the parties ~~want to abort the channel update. The abort may also result in a forceful closing of the channel via the subprocedure `ForceClose` (which we discuss further below).It happens when~~ pre-signed the new commit transaction, i.e., before **Step 5**, misbehavior simply implies update failure. A more problematic case is when the misbehavior occurs after at least one of the parties ~~has sufficient information to enforce the new state on-chain, while~~ pre-signed the new commit transaction. This happens, when one party pre-signs the new commit but the other does not; or when one party revokes the old commit and the other does not.

~~In order to complete the update,~~ In each of these situations, an honest party ends up in a hybrid state when the update is neither rejected nor accepted. To ensure that parties reach consensus on the update, our protocol instructs an honest party to perform a *force close* in this case. This means that the honest party posts the latest commit transaction it has on the ledger. This step guarantees that $\mathtt{TX}_{\mathtt{f}}$ is spent within Δ rounds. If the ~~revocation phase is executed. The functionality expects to receive the `REVOKE` message from both parties within $2T$ rounds, in which caseit updates the channel state in $\Gamma(id)$ accordingly and informs both parties about the successful updated via the message `UPDATED`. If one of the messages does not arrive, the subprocedure `ForceClose` is called.~~ transaction sending $\mathtt{TX}_{\mathtt{f}}$ is the new commit transaction, the update is successful. Otherwise, the update fails.

~~To conclude, the possibility for forceful closing guarantees the security property "consensus on update ". Moreover, in case both parties are honest, the duration of an successful update is independent of the ledger delay Δ, hence the efficiency property "optimistic update " is satisfied.~~ **Security of Update:** Since both parties have to pre-sign the new commit transaction, unforgeability of the adaptor signature scheme guarantees that the update is successful only if both parties agree. As discussed above, an honest party can ensure that within fixed number of rounds the channel update either succeeds or fails. Hence consensus on update holds.

c) ~~Close:~~ ~~Any of the two parties can request closure of~~ After a successful update, each party P possesses a pre-signature of the other party Q on the new commit transaction $\mathtt{TX}_{\mathtt{c}}$ which implies that P is able to complete Q's signature and post $\mathtt{TX}_{\mathtt{c}}$ on-chain. Assuming that the funding transaction of the channel ~~via the message (`CLOSE`, id), where id identifies the channel to be closed. In case both parties request closure within T rounds, *peaceful closure* is expected meaning that a transaction, spending the channel funding transaction and whose output corresponds to the latest channel state γ.st, should appear on $\mathcal{L}$ within Δ rounds. In case only one of the parties requests closing, the functionality executes the `ForceClose` subprocedure in which casesuch transaction is supposed to appear on $\mathcal{L}$ within 3Δ rounds. In both cases, if the funding transaction is not spent before a certain round, an `ERROR` message is returned.~~ $\mathtt{TX}_{\mathtt{f}}$ is not spent yet, $\mathtt{TX}_{\mathtt{c}}$ will be accepted by the ledger. Since party Q does not know the revocation secret of party P corresponding to $\mathtt{TX}_{\mathtt{c}}$, the only way how $\mathtt{TX}_{\mathtt{c}}$ can be spent is by publishing $\mathtt{TX}_{\mathtt{s}}$ representing the latest channel state. Hence, instant finality holds in this case. In the next paragraph we discuss what happens when the $\mathtt{TX}_{\mathtt{f}}$ is already spent by the time the new commit transaction is processed by the ledger. Namely, in this case instant finality cannot be guaranteed anymore, since $\mathtt{TX}_{\mathtt{c}}$ will not get accepted by the ledger. However, by using the punish procedure as described in the next paragraph, we ensure that honest parties get financially compensated in this situation.

c) Punish: ~~In order to guarantee "instant finality with punishments", parties continuously monitor the ledgerand apply the punishment mechanism if misbehavior is detected. This is captured by the functionality in the part "Punish" which is executed at the end of each round. The functionality checks if a~~ Since we are in the UTXO model, nothing can stop a corrupted party from publishing an old commit transaction, thereby spending the funding transaction of ~~some channelwas spent. If yes, then it expects one of the following to happen~~the channel. However, the way we designed the commit transaction enables the honest party to punish such malicious behavior and get financially compensated. If an honest party A detects that a malicious party B posted an old commit transaction $\overline{\mathtt{TX}}_{\mathtt{c}}$, it can react by publishing a *punishment transaction* which spends $\overline{\mathtt{TX}}_{\mathtt{c}}$ and assigns all coins to A. In order to make such punishment transaction valid, A must sign it under: (i) ~~a punish transaction appears on $\mathcal{L}$ within Δ rounds, assigning γ.`cash` coins to the honest party $P \in \gamma$.`users`; or~~ its secret key sk_A, (ii) ~~a transaction whose output corresponds to the latest channel state γ.st appears on $\mathcal{L}$ within 2Δ rounds, meaning that the channel is peacefully or forcefully closed. If none of the above is true, `ERROR` is returned.Hence, under the condition that no `ERROR` was returned, the security property "instant finality with punish" is satisfied.~~ B's publishing secret key $\bar{y}_B$, and (iii) B's revocation secret key $\bar{r}_B$. The knowledge of the revocation secret $\bar{r}_B$ follows from the fact that $\overline{\mathtt{TX}}_{\mathtt{c}}$ was old, i.e., parties revealed their revocation secrets to each other. The knowledge of the publishing secret $\bar{y}_B$ follows from the fact that it was B who published $\overline{\mathtt{TX}}_{\mathtt{c}}$. Let us elaborate on this in more detail.

Since $\overline{\mathtt{TX}}_{\mathtt{c}}$ was accepted by the ledger, it had to include a

[5] ~~For technical reasons, ideal functionality cannot sign transactions and thus it can also not prepare the transaction ids (which is the task of the simulator).~~

signature of A. The only signature A provided to B on $\overline{\mathtt{TX}}_c$ was a *pre-signature* w.r.t. Y_B. The unforgeability and witness extractability properties of Ξ guarantee that the only way B could produce a valid signature of A on $\overline{\mathtt{TX}}_c$ was by adapting the pre-signature thereby revealing the secret key $\bar{y}_B$ to A.

d) ~~Simplified formal description~~Close: ~~Since we do not aim to make any claims about privacy, we implicitly assume that every message that $\mathcal{F}$ receives/sends from/to~~ It remains to discuss how generalized channels are closed. The naive way to implement the closing procedure is to let parties publish the latest agreed upon commit transaction, i.e., perform a force close. However, due to the built-in punishment mechanism, parties have to wait for a certain number of rounds after such commit transaction is accepted by the ledger to publish the split transaction representing the latest channel state.

Our protocol uses a slightly more efficient solution which eliminates the redundant waiting time for honest parties. When parties want to close a channel, they first run a "final update". In short, the final update preserves the latest channel state but removes the punishment layer. More precisely, parties agree on a new split transaction that has exactly the same outputs as the last split transaction but spends the funding transaction $\mathtt{TX}_f$ directly (i.e., **Steps 2+5** from Fig. 4 are skipped). Once parties jointly sign the split transaction, they can publish it on the ledger and complete the channel closure. If the final update fails, parties close the channel using the force close procedure, i.e. they publish the latest commit transaction.

e) Psedu-code protocol description: We now present the pseudo-code description of our protocol in Fig. 5, in which we use the following arrow notation~~in formal description below~~. If we write $m \overset{t}{\hookrightarrow} P$, we mean "send the message m to party P in round t." and if we write $m \overset{t}{\hookleftarrow} P$, we mean "receive a message m from party P in round t". Moreover, in the protocol description, we abbreviate $\mathtt{One\text{-}Sig}_{pk_1} \wedge \cdots \wedge \mathtt{One\text{-}Sig}_{pk_n}$ by denoting it as $\mathtt{Multi\text{-}Sig}_{pk_1,\ldots,pk_n}$.

~~In summary, our functionality formally defined below satisfies the identified security and efficiency properties if no ERROR occurs. In case of an ERROR, all guarantees may be lost. Hence, we are interested only in those protocols realizing $\mathcal{F}$ that never output an ERROR.~~

~~Ideal Functionality $\mathcal{F}(T,k)$We abbreviate $Q := \gamma.\mathsf{otherParty}(P)$ for $P \in \gamma.\mathsf{users}$. Upon $(\mathtt{CREATE}, \gamma, tid_P) \overset{\tau_0}{\hookleftarrow} P$, let $\mathcal{S}$ define $T_1 \leq T$ and: If already received $(\mathtt{CREATE}, \gamma, tid_Q) \overset{\tau}{\hookleftarrow} Q$, where $\tau_0 - \tau \leq T_1$, wait if in round $\tau_1 \leq \tau + \Delta + T_1$ a transaction tx, with $\mathsf{tx.Input} = (tid_P, tid_Q)$ and $\mathsf{tx.Output} = (\gamma.\mathsf{cash}, \varphi)$, appears on the ledger $\mathcal{L}$. If yes, set $\Gamma(\gamma.\mathsf{id}) := (\gamma, \mathsf{tx})$ and $(\mathtt{CREATED}, \gamma.\mathsf{id}) \overset{\tau_1}{\hookrightarrow} \gamma.\mathsf{users}$. Else stop. Else store the message and stop.~~

~~Upon $(\mathtt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}}) \overset{\tau_0}{\hookleftarrow} P$, let $\mathcal{S}$ define $T_1, T_2 \leq T$, parse $(\gamma, \mathsf{tx}) := \Gamma(id)$ and proceed as follows: In round $\tau_1 \leq \tau_0 + T$, let $\mathcal{S}$ set $|\vec{tid}| = k$. Then $(\mathtt{UPDATE\text{-}REQ}, id, \vec{\theta}, t_{\mathsf{stp}}, \vec{tid}) \overset{\tau_1}{\hookrightarrow} Q$ and $(\mathtt{SETUP}, id, \vec{tid}) \overset{\tau_1}{\hookrightarrow} P$. If $(\mathtt{SETUP\text{-}OK}, id) \overset{\tau_2 \leq \tau_1 + t_{\mathsf{stp}}}{\hookleftarrow} P$, then $(\mathtt{SETUP\text{-}OK}, id) \overset{\tau_2+T_1}{\hookrightarrow} Q$. Else stop. If $(\mathtt{UPDATE\text{-}OK}, id) \overset{\tau_2+T_1}{\hookleftarrow} Q$, then $(\mathtt{UPDATE\text{-}OK}, id) \overset{\tau_2+2T_1}{\hookrightarrow} P$. Else distinguish: If Q honest or if instructed by $\mathcal{S}$, stop (update rejected). Else execute $\mathtt{ForceClose}(id)$ and stop. If $(\mathtt{REVOKE}, id) \overset{\tau_2+2T_1}{\hookleftarrow} P$, $(\mathtt{REVOKE\text{-}REQ}, id) \overset{\tau_2+2T_1+T_2}{\hookrightarrow} Q$. Else execute $\mathtt{ForceClose}(id)$ and stop. If $(\mathtt{REVOKE}, id) \overset{\tau_2+2T_1+T_2}{\hookleftarrow} Q$, set $\gamma.\mathsf{st} = \vec{\theta}$ and $\Gamma(id) := (\gamma, \mathsf{tx})$. Then $(\mathtt{UPDATED}, id, \vec{\theta}) \overset{\tau_2+2T_1+2T_2}{\hookrightarrow} \gamma.\mathsf{users}$ and stop. Else distinguish:~~

- ~~If Q honest, execute $\mathtt{ForceClose}(id)$ and stop.~~
- ~~If Q corrupt, and wait for Δ rounds. If tx still unspent, then set $\vec{\theta}_{old} := \gamma.\mathsf{st}$, $\gamma.\mathsf{st} := \{\vec{\theta}_{old}, \vec{\theta}\}$ and $\Gamma(id) := (\gamma, \mathsf{tx})$. Execute $\mathtt{ForceClose}(id)$ and stop.~~

~~Upon $(\mathtt{CLOSE}, id) \overset{\tau_0}{\hookleftarrow} P$, let $\mathcal{S}$ define $T_1 \leq T$ and distinguish: If you received $(\mathtt{CLOSE}, id) \overset{\tau}{\hookleftarrow} Q$, where $\tau_0 - \tau \leq T_1$, let $(\gamma, \mathsf{tx}) := \Gamma(id)$ and distinguish:~~

- ~~If in round $\tau_1 \leq \tau + T_1 + \Delta$ a transaction tx′, with $\mathsf{tx}'.\mathsf{Output} = \gamma.\mathsf{st}$ and $\mathsf{tx}'.\mathsf{Input} = \mathsf{tx.txid}$, appears on $\mathcal{L}$, set $\Gamma(id) := (\bot, \mathsf{tx})$, $(\mathtt{CLOSED}, id) \overset{\tau_1}{\hookrightarrow} \gamma.\mathsf{users}$ and stop.~~
- ~~If tx is still unspent in round $\tau + T_1 + \Delta$, output $(\mathtt{ERROR}) \overset{\tau+T_1+\Delta}{\hookrightarrow} \gamma.\mathsf{users}$ and stop.~~

~~Else wait for at most T_1 rounds to receive $(\mathtt{CLOSE}, id) \overset{\tau \leq \tau_0+T_1}{\hookleftarrow} Q$ (in that case option "Both agreed" is executed). If such message is not received, execute $\mathtt{ForceClose}(id)$ in round $\tau_0 + T_1$.~~

~~For each $(\gamma, \mathsf{tx}) \in \Gamma$ check if $\mathcal{L}$ contains tx′ with $\mathsf{tx}'.\mathsf{Input} = \mathsf{tx.txid}$. If yes, then distinguish: For $P \in \gamma.\mathsf{users}$ honest, the following must hold: in round $\tau_1 \leq \tau_0 + \Delta$, a transaction tx″ with $\mathsf{tx}''.\mathsf{Input} = \mathsf{tx}'.\mathsf{txid}$ and $\mathsf{tx}''.\mathsf{Output} = (\gamma.\mathsf{cash}, \mathtt{One\text{-}Sig}_{pk_P})$ appears on $\mathcal{L}$. Then $(\mathtt{PUNISHED}, id) \overset{\tau_1}{\hookrightarrow} P$, set $\Gamma(id) := \bot$ and stop. Either $\Gamma(id) = (\bot, \mathsf{tx})$ before round $\tau_0 + \Delta$ (channels was peacefully closed) or in round $\tau_1 \leq \tau_0 + 2\Delta$ a transaction tx″, with $\mathsf{tx}''.\mathsf{Output} \in \gamma.\mathsf{st}$ and $\mathsf{tx}''.\mathsf{Input} = \mathsf{tx}'.\mathsf{txid}$, appears on $\mathcal{L}$ (channel is forcefully closed). In the latter case, set $\Gamma(id) := (\bot, \mathsf{tx})$ and $(\mathtt{CLOSED}, id) \overset{\tau_1}{\hookrightarrow} \gamma.\mathsf{users}$. Otherwise $(\mathtt{ERROR}) \overset{\tau_0+2\Delta}{\hookrightarrow} \gamma.\mathsf{users}$.~~

~~Let τ_0 be the current round and $(\gamma, \mathsf{tx}) := \Gamma(id)$. If within Δ rounds tx is still an unspent transaction on $\mathcal{L}$, then $(\mathtt{ERROR}) \overset{\tau_0+\Delta}{\hookrightarrow} \gamma.\mathsf{users}$ and stop. Else, latest in round $\tau_0 + 3\Delta$, $m \in \{\mathtt{CLOSED}, \mathtt{PUNISHED}, \mathtt{ERROR}\}$ is output via Punish.~~

IV. Adaptor Signatures

Before we proceed to the formalization of adaptor signatures, we introduce the final building block that is require. Namely, we recall the definition of a *non-interactive zero-knowledge proof of knowledge* (NIZK) with online extractors as introduced in [14]. The online extractability property allows for extraction of a witness y for a statement Y from a proof π in the random oracle model and is useful for models where the rewinding proof technique is not allowed, such as UC. We need this property in order to prove

Building blocks: Digital Signature and Hard relation moved to section III. NIZK kept here.

New: Added pseudo-code description of our protocol.

Create channel

/ Initiate creation of γ with funding source id_P in round τ_0

$(R_P, r_P) \leftarrow \mathsf{GenR}, (Y_P, y_P) \leftarrow \mathsf{GenR}$

$(tid_P, R_P, Y_P) \xhookrightarrow{\tau_0} Q$

if $(tid_Q, R_Q, Y_Q) \xhookrightarrow{\tau_0+1} Q$ **then**

$[\mathtt{TX_f}] := \mathtt{GenFund}((tid_P, tid_Q), \gamma)$

$[\mathtt{TX_c}] := \mathtt{GenCom}([\mathtt{TX_f}], (pk_P, R_P, Y_P), (pk_Q, R_Q, Y_Q))$

$[\mathtt{TX_s}] := \mathtt{GenSplit}([\mathtt{TX_c}].\mathsf{txid}\|1, \gamma.\mathsf{st})$

$s_{\mathtt{c}}^P \leftarrow \mathsf{pSign}_{sk_P}([\mathtt{TX_c}], Y_Q), s_{\mathtt{s}}^P \leftarrow \mathsf{Sign}_{sk_P}([\mathtt{TX_s}])$

$(s_{\mathtt{c}}^P, s_{\mathtt{s}}^P) \xhookrightarrow{\tau_0+1} Q$

else stop

if $(s_{\mathtt{c}}^Q, s_{\mathtt{s}}^Q) \xhookrightarrow{\tau_0+2} Q \wedge \mathsf{pVrfy}_{pk_Q}([\mathtt{TX_c}], Y_P, s_{\mathtt{c}}^Q) \wedge \mathsf{Vrfy}_{pk_Q}([\mathtt{TX_s}], s_{\mathtt{s}}^Q)$ **then**

$s_{\mathtt{f}}^P \leftarrow \mathsf{Sign}_{sk_P}([\mathtt{TX_f}]), s_{\mathtt{f}}^P \xhookrightarrow{\tau_0+2} Q$

else stop

if $s_{\mathtt{f}}^Q \xhookrightarrow{\tau_0+3} Q \wedge \mathsf{Vrfy}_{pk_Q}([\mathtt{TX_f}], s_{\mathtt{f}}^Q)$ **then**

$\mathtt{TX_f} := ([\mathtt{TX_f}], s_{\mathtt{f}}^P, s_{\mathtt{f}}^Q), \quad \mathtt{TX_f} \xhookrightarrow{\tau_0+3} \mathcal{L}$

else spend tid_P

if within Δ rounds $\mathtt{TX_f}$ accepted by $\mathcal{L}$ **then**

Creation successful.

else stop

Update channel

/ Initiate update of γ with state $\vec{\theta}$ in τ_0

$(R_P, r_P) \leftarrow \mathsf{GenR}, (Y_P, y_P) \leftarrow \mathsf{GenR}$

$(\vec{\theta}, t_{\mathsf{stp}}, R_P, Y_P) \xhookrightarrow{\tau_0} Q$

if $(\vec{\theta}, t_{\mathsf{stp}}, R_Q, Y_Q) \xhookrightarrow{\tau_0+1} Q$ **then**

$[\mathtt{TX_c}] := \mathtt{GenCom}([\mathtt{TX_f}], (pk_P, R_P, Y_P), (pk_Q, R_Q, Y_Q))$

$[\mathtt{TX_s}] := \mathtt{GenSplit}([\mathtt{TX_c}].\mathsf{txid}\|1, \gamma.\mathsf{st})$

$s_{\mathtt{s}}^P \leftarrow \mathsf{Sign}_{sk_P}([\mathtt{TX_s}]), \quad s_{\mathtt{s}}^P \xhookrightarrow{\tau_0+1} Q$

else stop

if $s_{\mathtt{s}}^Q \xhookrightarrow{\tau_0+2} Q \wedge \mathsf{Vrfy}_{pk_Q}([\mathtt{TX_s}], s_{\mathtt{s}}^Q)$ **then**

if $\mathtt{SETUP\text{-}OK}$ in $\tau_1 \leq \tau_0 + 2 + t_{\mathsf{stp}}$ **then**

$s_{\mathtt{c}}^P \leftarrow \mathsf{pSign}_{sk_P}([\mathtt{TX_c}], Y_Q), \quad s_{\mathtt{c}}^P \xhookrightarrow{\tau_1} Q$

else stop

else stop

if $s_{\mathtt{c}}^Q \xhookrightarrow{\tau_1+1} Q \wedge \mathsf{Vrfy}_{pk_Q}([\mathtt{TX_f}], s_{\mathtt{f}}^Q)$ **then**

Let $\bar{r}_P$ be the revocation secret of the old state

$\bar{r}_P \xhookrightarrow{\tau_1+1} Q$

else $\mathtt{ForceClose}^P(\gamma.id)$

if $\bar{r}_Q \xhookrightarrow{\tau_1+2} Q \wedge (\bar{R}_Q, \bar{r}_Q) \in R$ **then**

Update successful.

else $\mathtt{ForceClose}^P(\gamma.id)$

Close channel

/ Let $\mathtt{TX_f}$ be the funding and $\mathtt{TX_s}$ the latest split txs of γ.

$[\overline{\mathtt{TX}}_{\mathtt{s}}] := \mathtt{GenSplit}(\mathtt{TX_f}.\mathsf{txid}\|1, \mathtt{TX_s}.\mathsf{Output})$

$s_{\mathtt{s}}^P \leftarrow \mathsf{Sign}_{sk_P}([\overline{\mathtt{TX}}_{\mathtt{s}}]), \quad s_{\mathtt{s}}^P \xhookrightarrow{\tau_0} Q$

if $s_{\mathtt{s}}^Q \xhookrightarrow{\tau_0+1} Q \wedge \mathsf{Vrfy}_{pk_Q}([\overline{\mathtt{TX}}_{\mathtt{s}}]; s_{\mathtt{s}}^Q) = 1$ **then**

$\overline{\mathtt{TX}}_{\mathtt{s}} := ([\overline{\mathtt{TX}}_{\mathtt{s}}], s_{\mathtt{s}}^P, s_{\mathtt{s}}^Q), \quad \overline{\mathtt{TX}}_{\mathtt{s}} \xhookrightarrow{\tau_0+1} \mathcal{L}$

Once $\overline{\mathtt{TX}}_{\mathtt{s}}$ accepted, Close successful.

else $\mathtt{ForceClose}^P(id)$

Punish

/ In every round τ_0 check the ledger and punish misbehavior

for every open channel γ **do**

Let $\{([\mathtt{TX}_{\mathtt{c}}^{(i)}], r_Q^{(i)}, Y_Q^{(i)}, s_P^{(i)})\}_{i \in m}$ be the set of all revoked commit transactions $[\mathtt{TX}_{\mathtt{c}}^{(i)}]$, with revocation secret $r_Q^{(i)}$, $Y_Q^{(i)}$ publishing value and pre-signature $s_P^{(i)}$

if $\exists \mathsf{tx} \in \mathcal{L}$ with $\mathsf{tx}.\mathsf{txid} = \mathtt{TX}_{\mathtt{c}}^{(i)}.\mathsf{txid}$ **then**

$(s_P, s_Q) := \mathsf{tx}.\mathsf{Witness}, \quad y_Q^{(i)} := \mathsf{Ext}(s_P, s_P^{(i)}, Y_Q^{(i)})$

$\mathtt{TX}_{\mathtt{pun}}.\mathsf{Input} := \mathsf{tx}.\mathsf{txid}\|1, \mathtt{TX}_{\mathtt{pun}}.\mathsf{Output} := (\gamma.\mathsf{cash}, \mathtt{One\text{-}Sig}_{pk_P})$

$s_y \leftarrow \mathsf{Sign}_{y_Q^{(i)}}([\mathtt{TX}_{\mathtt{pun}}]), \quad s_r \leftarrow \mathsf{Sign}_{r_Q^{(i)}}([\mathtt{TX}_{\mathtt{pun}}]),$

$s_P \leftarrow \mathsf{Sign}_{pk_P}([\mathtt{TX}_{\mathtt{pun}}])$

$\mathtt{TX}_{\mathtt{pun}} := ([\mathtt{TX}_{\mathtt{pun}}], s_y, s_r, s_P), \quad \mathtt{TX}_{\mathtt{pun}} \xhookrightarrow{\tau_0} \mathcal{L}$

Once $\mathtt{TX}_{\mathtt{pun}}$ accepted, channel closed.

Auxiliary procedures

$\mathtt{GenFund}(\vec{tid}, \gamma)$:

$\mathsf{tx}.\mathsf{Input} := \vec{tid}, \mathsf{tx}.\mathsf{Output} := \left(\gamma.\mathsf{cash}, \mathtt{Multi\text{-}Sig}_{\gamma.\mathsf{users}}\right)$

return tx

$\mathtt{GenCom}([\mathtt{TX_f}], (pk_P, R_P, Y_P), (pk_Q, R_Q, Y_Q))$:

$(c, \mathtt{Multi\text{-}Sig}_{pk_P, pk_Q}) := \mathtt{TX_f}.\mathsf{Output}[1]$

$\varphi_1 := \mathtt{Multi\text{-}Sig}_{R_Q, Y_Q, pk_P}, \varphi_2 := \mathtt{Multi\text{-}Sig}_{R_P, Y_P, pk_Q}$

$\varphi_3 := \mathtt{CheckRelative}_{\Delta} \wedge \mathtt{Multi\text{-}Sig}_{pk_P, pk_Q}$

$\mathsf{tx}.\mathsf{Input} := \mathtt{TX_f}.\mathsf{txid}\|1, \ \mathsf{tx}.\mathsf{Output} := (c, \varphi_1 \vee \varphi_2 \vee \varphi_3)$

return tx

$\mathtt{GenSplit}(tid, \vec{\theta})$:

$\mathsf{tx}.\mathsf{Input} := tid, \mathsf{tx}.\mathsf{Output} := \vec{\theta}$

return tx

$\mathtt{ForceClose}^P(\gamma.id)$

/ Let $\mathtt{TX_c}$ and $\mathtt{TX_s}$ be the latest commit and split txs of γ.

$\mathtt{TX_c} \xhookrightarrow{\mathtt{TX_c}.\mathsf{TimeLock}} \mathcal{L}$

if $\mathtt{TX_c}$ accepted by $\mathcal{L}$ at round τ **then**

$\mathtt{TX_s} \xhookrightarrow{\tau+\Delta} \mathcal{L}$

if $\mathtt{TX_s}$ accepted by $\mathcal{L}$ **then** γ closed.

Fig. 5. Protocol for generalized channels.

our ECDSA-based adaptor signature scheme secure. More formally, a pair (P, V) of PPTalgorithms is called a NIZK with an online extractor for a relation R, random oracle $\mathcal{H}$ and security parameter n if the following holds: (i) *Completeness*: For any $(Y, y) \in R$, it holds that $\mathsf{V}(Y, \mathsf{P}(Y, y)) = 1$ except with negligible probability; (ii) *Zero knowledge*: There exists a PPTsimulator S, which on input Y can simulate the proof π for any $(Y, y) \in R$. (iii) *Online Extractor*: There exist a PPTonline extractor K with access to the the sequence of queries to the random oracle and its answers, such that given (Y, π), the algorithm K can extract the witness y with $(Y, y) \in R$. It is shown in [14] how to instantiate such proof system.

A. Adaptor Signature Definition

Adaptor signatures have been introduced by the cryptocurrency community to tie together the authorization of a transaction and the leakage of a secret value. An adaptor signature scheme is essentially a two-step signing algorithm bound to a secret: first a partial signature is generated such that it can be completed only by a party knowing a certain secret, with the complete signature revealing such a secret. More precisely, we define an adaptor signature scheme with respect to a standard signature scheme Σ and a hard relation R. For any statement $Y \in L_R$, a signer holding a secret key is able to produce a *pre-signature* w.r.t. Y on any message m. Such pre-signature can be *adapted* into a valid signature on m if and only if the adaptor knows a witness for Y. Moreover, if such a valid signature is produced, it must be possible to extract a witness for Y given the pre-signature and the adapted signature.

Despite the fact that adaptor signatures have been used in previous works (e.g. [24] [15] [27]), none of these works has given a formal definition of the adaptor signature primitive and its security. As a consequence, in the following we provide the

Original definition in compressed form.

Definition 1 (Adaptor Signature Scheme)**.** An adaptor signature scheme wrt. a hard relation R and a signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ consists of four algorithms $\Xi_{R,\Sigma} = (\mathsf{pSign}, \mathsf{Adapt}, \mathsf{pVrfy}, \mathsf{Ext})$ with the following syntax: $\mathsf{pSign}_{sk}(m, Y)$ is a PPT algorithm that on input a secret key sk, message $m \in \{0,1\}^*$ and statement $Y \in L_R$, outputs a pre-signature $\tilde{\sigma}$; $\mathsf{pVrfy}_{pk}(m, Y; \tilde{\sigma})$ is a DPT algorithm that on input a public key pk, message $m \in \{0,1\}^*$, statement $Y \in L_R$ and pre-signature $\tilde{\sigma}$, outputs a bit b; $\mathsf{Adapt}(\tilde{\sigma}, y)$ is a DPT algorithm that on input a pre-signature $\tilde{\sigma}$ and witness y, outputs a signature σ; and $\mathsf{Ext}(\sigma, \tilde{\sigma}, Y)$ is a DPT algorithm that on input a signature σ, pre-signature $\tilde{\sigma}$ and statement $Y \in L_R$, outputs a witness y such that $(Y, y) \in R$, or $\perp$.

In addition to the standard signature correctness, an adaptor signature scheme has to satisfy *pre-signature correctness*. Informally, ~~it guarantees that~~ an honestly generated pre-signature wrt. a statement $Y \in L_R$ is a valid pre-signature and can be completed into a valid signature from which a witness for Y can be extracted.

Definition 2 (Pre-signature correctness)**.** An adaptor signature scheme $\Xi_{R,\Sigma}$ satisfies pre-signature correctness if for every $n \in \mathbb{N}$, every message $m \in \{0,1\}^*$ and every statement/witness pair $(Y, y) \in R$, the following holds:

$$\Pr\left[\begin{array}{c|l} \mathsf{pVrfy}_{pk}(m, Y; \tilde{\sigma}) = 1 \\ \wedge \\ \mathsf{Vrfy}_{pk}(m; \sigma) = 1 \\ \wedge \\ (Y, y') \in R \end{array} \middle| \begin{array}{l} (sk, pk) \leftarrow \mathsf{Gen}(1^n) \\ \tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y) \\ \sigma := \mathsf{Adapt}_{pk}(\tilde{\sigma}, y) \\ y' := \mathsf{Ext}_{pk}(\sigma, \tilde{\sigma}, Y) \end{array}\right] = 1.$$

We now define the security properties of an adaptor signature scheme. We begin with the notion of unforgeability which is similar to ~~the definition of~~ existential unforgeability under chosen message attacks but additionally requires that producing a forgery σ for some message m is hard even given a pre-signature on m w.r.t. a random statement $Y \in L_R$. Let us emphasize that allowing the adversary to learn a pre-signature on the forgery message m is crucial since for our applications unforgeability needs to hold even in case the adversary learns a pre-signature for m without knowing a ~~corresponding~~ witness for Y. We now formally define the existential unforgeablity under chosen message attack for adaptor signature (aEUF–CMA security for short)~~in Definition 3~~.

Definition 3 (aEUF–CMA security)**.** An adaptor signature scheme $\Xi_{R,\Sigma}$ is aEUF–CMA secure if for every PPT adversary $\mathcal{A}$ there exists a negligible function ν such that: $\Pr[\mathsf{aSigForge}_{\mathcal{A},\Xi_{R,\Sigma}}(n) = 1] \leq \nu(n)$, where the experiment $\mathsf{aSigForge}_{\mathcal{A},\Xi_{R,\Sigma}}$ is defined as follows:

$\mathsf{aSigForge}_{\mathcal{A},\Xi_{R,\Sigma}}(n)$
1 : $\mathcal{Q} := \emptyset$
2 : $(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
3 : $m \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
4 : $(Y, y) \leftarrow \mathsf{GenR}(1^n)$
5 : $\tilde{\sigma} \leftarrow \mathsf{pSign}_{pk\,sk}(m, Y)$
6 : $\sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot), \mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma}, Y)$
7 : **return** $(m \notin \mathcal{Q} \wedge \mathsf{Vrfy}_{pk}(m; \sigma))$

$\mathcal{O}_{\mathrm{S}}(m)$
1 : $\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
2 : $\mathcal{Q} := \mathcal{Q} \cup \{m\}$
3 : **return** σ

$\mathcal{O}_{\mathrm{pS}}(m, Y)$
1 : $\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
2 : $\mathcal{Q} := \mathcal{Q} \cup \{m\}$
3 : **return** $\tilde{\sigma}$

As discussed above, adaptor signatures guarantee that a valid pre-signature w.r.t. Y can be completed to a valid signature if and only if the corresponding witness y for Y is known. An additional property that we will require is that any valid pre-signature w.r.t. Y (possibly produced by a malicious signer) can be completed into a valid signature using the witness y with $(Y, y) \in R$. Notice that this property is stronger than the pre-signature correctness property from Definition 2, since we require that even maliciously produced pre-signatures can always be completed into valid signatures. The next definition formalizes the above discussion.

Definition 4 (Pre-signature adaptability)**.** An adaptor signature scheme Ξ_R satisfies pre-signature adaptability if for any $n \in \mathbb{N}$, any message $m \in \{0,1\}^*$, any statement/witness pair $(Y, y) \in R$, any key pair $(sk, pk) \leftarrow \mathsf{Gen}(1^n)$ and any pre-signature $\tilde{\sigma} \leftarrow \{0,1\}^*$ with $\mathsf{pVrfy}_{pk}(m, Y; \tilde{\sigma}) = 1$, we have: $\Pr[\mathsf{Vrfy}_{pk}(m; \mathsf{Adapt}(\tilde{\sigma}, y)) = 1] = 1$.

The ~~aEUF–CMA security together with the pre-signature adaptability ensure that a pre-signature for Y can be transferred into a valid signature if and only if the corresponding witness y is known. The~~ last property that we are interested in is *witness extractability*. Informally, it guarantees that a valid signature/pre-signatue pair $(\sigma, \tilde{\sigma})$ for message/statement (m, Y) can be used to extract the corresponding witness y.

Definition 5 (Witness extractability)**.** An adaptor signature scheme Ξ_R is *witness extractable* if for every PPT adversary $\mathcal{A}$, there exists a negligible function ν such that the following holds: $\Pr[\mathsf{aWitExt}_{\mathcal{A},\Xi_R}(n) = 1] \leq \nu(n)$, where the experiment $\mathsf{aWitExt}_{\mathcal{A},\Xi_{R,\Sigma}}$ is defined as follows

$\mathsf{aWitExt}_{\mathcal{A},\Xi_{R,\Sigma}}(n)$

$\mathcal{Q} := \emptyset$
$(sk, pk) \leftarrow \mathsf{Gen}(1^n)$
$(m, Y) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(pk)$
$\tilde{\sigma} \leftarrow \mathsf{pSign}_{pk\,sk}(m, Y)$
$\sigma \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{S}}(\cdot),\mathcal{O}_{\mathrm{pS}}(\cdot,\cdot)}(\tilde{\sigma})$
$y' := \mathsf{Ext}_{pk}(\sigma, \tilde{\sigma}, Y)$
return $(m \notin \mathcal{Q} \wedge (Y, y') \notin R$
$\quad \wedge \mathsf{Vrfy}_{pk}(m; \sigma))$

$\mathcal{O}_{\mathrm{S}}(m)$

$\sigma \leftarrow \mathsf{Sign}_{sk}(m)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return σ

$\mathcal{O}_{\mathrm{pS}}(m, Y)$

$\tilde{\sigma} \leftarrow \mathsf{pSign}_{sk}(m, Y)$
$\mathcal{Q} := \mathcal{Q} \cup \{m\}$
return $\tilde{\sigma}$

Let us stress that while the witness extractability experiment aWitExt looks fairly similar to the experiment aSigForge, there is one crucial difference; namely, the adversary is allowed to choose the forgery statement Y. Hence, we can assume that he knows a witness for Y so he can generate a valid signature on the forgery message m. However, this is not sufficient to win the experiment. The adversary wins *only* if the valid signature does not reveal a witness for Y.

Definition 6 (Secure Adaptor Signature Scheme)**.** An adaptor signature scheme $\Xi_{R,\Sigma}$ is secure, if it is aEUF–CMA secure, pre-signature adaptable and witness extractable.

B. ECDSA-based Adaptor Signature

In this section we present an ECDSA-based adaptor signature construction that provably satisfies our security definition. The construction presented here is similar to the construction put forward by [27], however some modifications are needed for the security proof. Note that while we present here an ECDSA-based adaptor signature scheme, we additionally show a scheme based on Schnorr signatures including correctness and security proofs in the ~~full version of this paper [16]~~ supplementary material [30].

Recall the ECDSA signature scheme ~~$\Sigma_{\mathsf{ECDSA}} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$~~ $\Sigma_{\mathsf{ECDSA}} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ for a cyclic group $\mathbb{G} = \langle g \rangle$ of prime order q. The key generation algorithm samples $x \leftarrow_{\$} \mathbb{Z}_q$ and outputs $g^x \in \mathbb{G}$ as the public key and x as the secret key. The signing algorithm on input a message $m \in \{0,1\}^*$, samples $k \leftarrow_{\$} \mathbb{Z}_q$ and computes $r := f(g^k)$ and $s := k^{-1}(\mathcal{H}(m) + rx)$, where $\mathcal{H}\colon \{0,1\}^* \to \mathbb{Z}_q$ is a hash function modelled as a random oracle and $f\colon \mathbb{G} \to \mathbb{Z}_q$.[5] (i.e., f is typically defined as the projection to the x-coordinate since in ECDSA the group $\mathbb{G}$ consists of elliptic curve points). The verification algorithm on input a message $m \in \{0,1\}^*$ and a signature (r, s) verifies that $f(g^{s^{-1}\mathcal{H}(m)} X^{s^{-1}r}) = r$. One of the properties of the ECDSA scheme is that if (r, s) is a valid signature for m, then so is $(r, -s)$. Consequently, Σ_{ECDSA} does not satisfy SUF–CMA security which we need in order to prove its security. In order to tackle this problem we build our adaptor signature from the *Positive ECDSA* scheme which guarantees that if (r, s) is a valid signature, then $|s| \leq (q-1)/2$. The positive ECDSA has already been used in other works such as [3, 23]. This slightly modified ECDSA scheme is not only assumed to be SUF–CMA but also prevents having two valid signatures for the same message after the signing process, which is useful in practice, e.g., for threshold signature schemes based on ECDSA. ~~We note that~~ As the ECDSA verification accepts valid positive ECDSA signatures~~and hence~~, these signatures can ~~also~~ be used in Bitcoin.

The adaptor signature scheme in [27] is presented ~~with respect to~~ w.r.t. a relation $R_g \subseteq \mathbb{G} \times \mathbb{Z}_q$ defined as $R_g := \{(Y, y) \mid Y = g^y\}$. The main idea of the construction is that a pre-signature (r, s) for a statement Y is computed by embedding Y into the r-component while keeping the s-component unchanged. This embedding ~~however~~ is rather involved~~in ECDSA~~, since the value s contains a product of k^{-1}, r and the secret key. More concretely, to compute the pre-signature for Y, the signer samples a random k and computes $K := Y^k$ and $\tilde{K} := g^k$. It then uses the first value to compute $r := f(K)$ and sets $s := k^{-1}(\mathcal{H}(m) + rx)$. To ensure that the signer uses the same value k in K and $\tilde{K}$, a zero-knowledge proof that $(\tilde{K}, K) \in L_Y := \{(\tilde{K}, K,) \mid \exists k \in \mathbb{Z}_q \text{ s.t. } g^k = \tilde{K} \wedge Y^k = K\}$ is attached to the pre-signature. We denote the prover of the NIZK as P_Y and the corresponding verifier as V_Y). The pre-signature adaptation is done by multiplying the value s with y^{-1}, where y is the corresponding witness for Y. This adjusts the randomness k used in s to ky, and hence matches with the r value.

[5] ~~Since in ECDSA, the group $\mathbb{G}$ consists of elliptic curve points, the function f is typically defined as the projection to the x-coordinate.~~

$\mathsf{pSign}_{sk}(m, I_Y)$

$x := sk$
$(Y, \pi_Y) := I_Y$
$k \leftarrow_{\$} \mathbb{Z}_q$
$\tilde{K} := g^k, K := Y^k$
$r := f(K)$
$\tilde{s} := k^{-1}(\mathcal{H}(m) + rx)$
$\pi \leftarrow \mathsf{P}_Y((\tilde{K}, K), k)$
return $(r, \tilde{s}, K, \pi)$

$\mathsf{pVrfy}_{pk}(m, I_Y; \tilde{\sigma})$

$X := pk$
$(Y, \pi_Y) := I_Y$
$(r, \tilde{s}, K, \pi) := \tilde{\sigma}$
$u := \mathcal{H}(m) \cdot \tilde{s}^{-1}$
$v := r \cdot \tilde{s}^{-1}$
$K' := g^u X^v$
$b_r := (r = f(K))$
$b := \mathsf{V}_Y((K', K), \pi)$
return $(b_r \wedge b)$

$\mathsf{Ext}(\sigma, \tilde{\sigma}, I_Y)$

$(r, s) := \sigma$
$(\tilde{r}, \tilde{s}, K, \pi) := \tilde{\sigma}$
$y' := s^{-1} \cdot \tilde{s}$
if $(I_Y, y') \in R'_g$
then return y'
else return $\perp$

$\mathsf{Adapt}(\tilde{\sigma}, y)$

$(r, \tilde{s}, K, \pi) := \tilde{\sigma}$
$s := \tilde{s} \cdot y^{-1}$
return (r, s)

Fig. 6. ECDSA-based adaptor signature scheme.

Unfortunately, it is not clear how to prove security for the above scheme for the following reason: Ideally, we would like to reduce both the unforgeability and the witness extractability of the scheme to the strong unforgeability of positive ECDSA. More concretely, suppose there exists a PPT adversary $\mathcal{A}$ that wins the aSigForge (resp. aWitExt) experiment, then we design a PPT adversary (also called the simulator) $\mathcal{S}$ that breaks the SUF–CMA security. The main technical challenge in both reductions is that $\mathcal{S}$ has to answer queries (m, Y) to $\mathcal{O}_{\mathrm{pS}}$ by $\mathcal{A}$. This has to be done with access to the ECDSA signing oracle, but without knowledge of sk and the witness y. Thus, we need a method to "transform" full signatures into valid pre-signatures without knowing y, which seems to go against the aEUF–CMA-security (resp. witness extractability).

Due to this reason, we slightly modify this scheme. In particular, we modify the hard relation for which the adaptor signature is defined. Let R'_g consist of *pairs* (Y, π), where $Y \in L_{R_g}$ is as above, and π is a non-interactive zero-knowledge proof of knowledge that $Y \in L_{R_g}$. Formally, we define $R'_g := \{((Y, \pi), y) \mid Y = g^y \wedge \mathsf{V}_g(Y, \pi) = 1\}$ and denote by P_g the prover and by V_g the verifier of the proof system for L_{R_g}. Clearly, due to the soundness of the proof system, if R_g is a hard relation, then so is R'_g.

It might seem that we did not make it any easier for the reduction to learn a witness needed for creating pre-signatures. However, we exploit the fact that we are in the ROM and the reduction answers adversary's random oracle queries. Upon receiving a statement $I_Y := (Y, \pi)$ for which it must produce a valid pre-signature, it uses the random oracle query table to extract a witness from the proof π. Knowing the witness y and a signature (r, s), the reduction can compute $(r, s \cdot y)$ and execute the simulator of the NIZK_Y to produce a consistency proof π. This concludes the protocol description and the main proof idea. We refer the reader to ~~the full version of this paper [16]~~ the supplemenatry material [30] for the detailed proof of the following theorem.

~~ECDSA-based adaptor signature scheme.~~

Theorem 1. *If the positive ECDSA signature scheme* Σ_{ECDSA} *is* SUF–CMA*-secure and* R'_g *is a hard relation,* $\Xi_{R'_g, \Sigma_{\mathsf{ECDSA}}}$ *from Fig. 6 is a secure adaptor signature scheme in the ROM.*

V. ~~Protocol description~~Security Model

~~We now present a concrete protocol, which we denote Π, that realizes the channel functionality $\mathcal{F}(T, k)$ for $T = 3$ and $k = 1$. This is achieved by utilizing an adaptor signature scheme $\Xi_{R,\Sigma} = (\mathsf{pSign}, \mathsf{Adapt}, \mathsf{pVrfy}, \mathsf{Ext})$ for signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$~~ To formally model the security of our channel construction, we use a synchronous version of the global UC framework (GUC) [8] allows for a global setup. Monetary transactions are handled by a global ledger $\mathcal{L}(\Delta, \Sigma)$, where Δ is an upper bound on the blockchain delay (number of rounds it takes to publish a transaction) and Σ defines the signature scheme used by the ~~underlying ledger and a hard relation R. Our protocol consists of four subprotocols: Create, Update, Close and Punish~~blockchain. For more details about our security model, which closely follows the model of [9, 10, 11], we refer the reader to Appendix C. Here we ~~explain~~ outline the main ideas of ~~the protocol. We refer the reader to ?? for the formal descriptions. To simplify the exposition of the discussion below, we assume here that statement~~our security analysis in the UC-model.

Our first step is to define an ideal behavior of a generalized channelprotocol as an *ideal functionality* $\mathcal{F}$. This ideal functionality specifies the input/~~witness pairs of R are valid key pairs of Σ.~~[5] output behavior of a generalized channelprotocol, its impact on the ledger and defines the possible influence of an adversary on the protocol execution (e.g., the power to delay protocol execution). Thereafter, we show that our generalized channelprotocol Π *emulates* the ideal functionality $\mathcal{F}$. On a high level, this means that any attack that can be performed on our protocol can be simulated as an attack on $\mathcal{F}$. Or put differently, we show that our protocol is at least as secure as the ideal functionality.

~~Schematic description of the channel creation protocol.~~

a) ~~Channel creation:~~ ~~In order to create a channel γ, users of the channel, let us denote them A and B, have to agree on the body of the funding transaction $[\mathtt{TX}_\mathtt{f}]$, mutually commit to the first channel state defined by $\gamma.\mathtt{st} = ((x_A, \mathtt{One\text{-}Sig}_{pk_A}), (x_B, \mathtt{One\text{-}Sig}_{pk_B}))$, and sign and publish the funding transaction $\mathtt{TX}_\mathtt{f}$ on the ledger. Once $\mathtt{TX}_\mathtt{f}$ is published, the channel creation is completed.Looking at Fig. 4 , one can summarize the creation process as a step-by-step creation of transaction bodies from left to right, and then step-by-step signature exchange on the transaction bodies from right to left. Let us elaborate on this in more detail.~~ The proof of emulation consists of two parts. We first design a *simulator* that translates an attack on the protocol into an attack on the ideal functionality. Thereafter, we show that no ppt *environment* can distinguish whether it is interacting with the real protocol and giving instructions to a real adversary (i.e., interacts with the *real world*), or if it is interacting with the ideal functionality and giving attack instruction to the simulator (i.e., interacts with the *ideal world*).

~~**Step 1:** To prepare $[\mathtt{TX}_\mathtt{f}]$, parties need to inform each other about their funding sources~~As the environment can observe the ledger when trying to distinguish the two worlds, the main technical challenge when designing a simulator is to ensure that the same transactions are posted on the ledger in the same round in both worlds. Moreover, the simulator instructs the ideal functionality to output message in the same round as the protocol would do. This guarantees that the environment cannot trivially distinguish between the two worlds because of timings or content of messages. We reduce the indistinguishability of the real and ideal world to the security of the primitives underlying our protocol, i.e., ~~exchange the transaction identifiers tid_A and tid_B. Each party can then locally create $[\mathtt{TX}_\mathtt{f}]$ with $\{tid_A, tid_B\}$ as~~

[5] ~~Statements in the ECDSA-based adaptor signature can be mapped to public keys by dropping the second coordinate, i.e., the zero-knowledge proof.~~

Sections III and V swapped. Changes in section about UC model:
* Ideal functionality moved to Appx. D
* New: UC proof strategy

input and output requiring signature of both A and B. **Step 2:** Parties can now start committing to the initial channel state. To this end, each party $P \in \{A, B\}$ first generates a *revocation public/secret* as $(R_P, r_P) \leftarrow$ GenR and *publishing public/secret* pair $(Y_P, y_P) \leftarrow$ GenR. The public values R_P and Y_P are sent to the other party. Each party can now locally generate the body of the commit transaction $[\mathtt{TX_c}]$ which spends $\mathtt{TX_f}$ and can be spent by a transaction satisfying one of the following conditions: It is correctly signed w. r. t. pk_B, Y_A, R_A; It is correctly signed w.r.t. pk_A, Y_B, R_B; It is correctly signed w.r.t. pk_A and pk_B, and at least security of the signature scheme, the hard relation and the adaptor signature scheme.

The definition of our generalized channelfunctionality $\mathcal{F}$ can be found in Appendix D. In the supplementary material [30], we formally state and prove the following theorem.

Theorem 2. *(Informal) Let Σ be a* SUF–CMA *secure signature scheme, R a hard relation and $\Xi_{R,\Sigma}$ a secure adaptor signature scheme. Then for any ledger delay $\Delta \in \mathbb{N}$, the protocol Π UC-realizes the ideal functionality $\mathcal{F}$*

Applications rewritten s.t. independent of UC formalism.

VI. Applications

Generalized channelscan be used as a building block for many different applications. In this section, we provide a generic guideline on how to build an application on top of a generalized channeland demonstrate it on concrete examples.

Assume that Alice and Bob already created a generalized channelγ and now they want to use it for several applications. For that, parties have to carry out the following steps.

Initialize: Parties agree on the new state $\vec{\theta}$ of γ and the upper bound t_{stp} on the time required to setup off-chain applications. Hence, for each application parties need to agree on (i) the amount of coins they want to invest in the application and the funding condition; technically, this means that parties define $\theta_i = (\theta_i.\mathsf{cash}, \theta_i.\varphi)$, and (ii) the value t_i denoting the maximal amount of rounds that it takes to setup the corresponding application. The value t_{stp} is defined as $\max_i t_i$, thereby defining the maximal amount of rounds that it takes to setup all the applications in parallel.

Steps 2+5Prepare: are skipped)Parties now start the update process using $\vec{\theta}$ and t_{stp}. Once parties jointly sign the split transaction, they can publish it on the ledger which completes the channel closurereach the point in the protocol, where they are instructed to setup applications, they proceed to the next step. Recall that at this point, both parties know the identifier of the split transaction tid representing the state $\vec{\theta}$.

a) Punish: Since we are in the UTXO model, nothing can stop a corrupt party from publishing old commit transactions. However, the way we designed the commit transaction enables the honest party to punish such malicious behavior and get financially compensated. If an honest party A detects that a malicious party B posted an old commit transaction $\mathtt{TX_c}$, it can react by publishing a *punishment transaction* which spends $\mathtt{TX_c}$ and assigns all coins to A. In order to make such punishment transaction valid, A must sign it under: (i) its secret key sk_A, (ii) **Setup:** The parties exchange the application-dependent information required to fulfill the conditions $\{\theta_i.\varphi\}$ according to the rules of each application, using tid as the funding source. Once completed, parties return $\mathtt{SETUP\text{-}OK}$. **Complete:** Parties complete the update process.

We now demonstrate how to use this generic process on concrete examples by describing their initialize and setup steps. To avoid repetition, for each example, we assume there is a channel γ between parties A and B 's publishing secret key y_B, owning α_A and (iii) B's revocation secret key r_B. The knowledge of the revocation secret r_B follows from the fact that $\mathtt{TX_c}$ was old, i.e. parties revealed their revocation secrets to each other. The knowledge of the publishing secret y_B follows from the fact that it was B who published $\mathtt{TX_c}$. Let us elaborate on this in more detail. Since $\mathtt{TX_c}$ was accepted by the ledger, it had to include a signature of A. The only signature α_B coins and their public keys are pk_A and pk_B, respectively.

a) Channel splitting [13]: As discussed earlier in this work, a generalized channelcan be split into multiple sub-channels that can be updated independently in parallel. Assume that A provided to B on $\mathtt{TX_c}$ was a *pre-signature* w.r.t. Y_B. The unforgeability and witness extractability properties of Ξ guarantee that the only way and B could produce a valid signature want to split their channel γ into two sub-channels γ_0 and γ_1 with the coin distributions (β_A, β_B) and $(\alpha_A - \beta_A, \alpha_B - \beta_B)$ respectively. They proceed as follows:

Initialize: Parties create two outputs each of which funds one of the sub-channels:

- $\theta_0.\mathsf{cash} := \gamma_0.\mathsf{cash}$, $\theta_0.\varphi := \mathtt{One\text{-}Sig}_{pk_A} \wedge \mathtt{One\text{-}Sig}_{pk_B}$
- $\theta_1.\mathsf{cash} := \gamma_1.\mathsf{cash}$, $\theta_1.\varphi := \mathtt{One\text{-}Sig}_{pk_A} \wedge \mathtt{One\text{-}Sig}_{pk_B}$

and set the value $t_{\mathsf{stp}} := 2$ for the required setup steps.

Setup: For each sub-channel, parties generate and sign the commit and split transactions representing the initial channel state. This procedure, explained in Section III, takes 2 rounds.

b) Payment-channel networks (PCNs) [29, 25, 24]: A payment-channel network (PCN) enables transitive payments between two users by leveraging a *path* of payment channels between the sender and the receiver. The Lightning Network implements a so-called multi-hop payment by means of a script called hash-time lock contract (HTLC). In particular, we denote by $\mathtt{CheckHash}_y$ an output condition that can be spent by providing a value r such that $H(r) = y$. Using the same HTLC to update each channel in the payment path, the Lightning Network ensures that the payment is correctly carried out. In a bit more detail, the receiver sends to the sender the value y and keeps locally the value r such that $H(r) = y$. Then, the payment starts by updating each channel from the sender to the receiver so that it locks the payment amount into an output that can be spent under the condition $\mathtt{CheckHash}_y$. When the channel with the receiver is updated accordingly, the receiver is sure that he can redeem the coins

by revealing r. In addition, if the receiver never reveals the value r, the sender eventually gets back the locked coins with a timeout t condition, denoted by $\texttt{CheckAbsolute}_t$.

The generalized channelconstruction presented in this work can be used to implement PCNs. In particular, assume a payment of β coins through a payment path formed by n generalized channels. For each channel γ in the path, an update with the following initialize and setup steps is performed.

Initialize: Parties exchange the hash value y, decide on the timeout value t, and create three outputs (one for the HTLC, one for the balance of A ~~on $\texttt{TX}_c$ was by adapting the pre-signature thereby revealing the secret key y_B to A~~and one for the balance B):

- $\theta_0.\texttt{cash} := \beta, \theta_0.\varphi := (\texttt{CheckHash}_y \wedge \texttt{One-Sig}_{pk_B}) \vee (\texttt{CheckAbsolute}_t \wedge \texttt{One-Sig}_{pk_A})$
- $\theta_1.\texttt{cash} := \alpha_A - \beta, \theta_1.\varphi := \texttt{One-Sig}_{pk_A}$
- $\theta_2.\texttt{cash} := \alpha_B, \theta_2.\varphi := \texttt{One-Sig}_{pk_B}$

Parties set the value $t_{\text{stp}} := 0$ as no setup is needed (each party has enough information to prepare the transactions locally).

~~In the full version of this paper [16] we prove the following theorem, which essentially says that the Π protocol is a secure realization, as defined according to the UC framework, of~~ After the successful update of all channels on the path, the ~~$\mathcal{F}(3,1)$ ideal functionality.Let Σ be a SUF-CMA secure signature scheme, R a hard relation and $\Xi_{R,\Sigma}$ a secure adaptor signature scheme. Then for any ledger delay $\Delta \in \mathbb{N}$, the protocol Π UC-realizes the ideal functionality $\mathcal{F}(3,1)$.~~ payment of β coins in the PCN is successfully set. A similar procedure can be carried out then to settle the payment when the receiver releases the value r such that $H(r) = y$.

New paragraph in Applications about virtual channels

a) Virtual Channels [1]: In a recent follow-up work [1], generalized channels have been used in order to build virtual channels over Bitcoin. The concept of virtual channels was first introduced in the work of Dziembowski et al. [12], in which the authors presented a construction over Ethereum. Let us shortly recall this concept. Assume Alice and Bob both have a channel with a party Ingrid, but not with each other. A virtual channel allows Alice and Bob to send off-chain payments to each other without having to communicate with Ingrid for each transaction. We refer the reader to [1] for more details.

VII. Performance Analysis

We created a proof of concept implementation for the `CREATE`, `UPDATE`, `CLOSE` and `PUNISH` operations. In a bit more detail, we utilized the `python-bitcoin-utils` library to create the required raw Bitcoin transactions encoded in the Bitcoin scripting language *Script*. Furthermore, we successfully deployed them on the Bitcoin testnet, demonstrating thereby the compatibility with the current Bitcoin network. The source code is publicly available ~~.~~[5] at https://github.com/generalized-channels/gc.

[5] ~~https://github.com/generalized-channels/gc~~

We evaluate the different operations for generalized channels using the following criteria: (i) the number of on- and off-chain transactions required in the protocols; (ii) the total amount of bytes that the on- and off-chain transactions sum up to; and (iii) the estimated cost (i.e. the transaction fee) for publishing the on-chain transactions required in each protocol. We remark that the transaction fee in Bitcoin is dependent on the transaction size. In our calculations, we use the price values valid at the time of writing: the average transaction fee is 14 satoshis per byte[5], or at the current exchange rate of 8869.67 USD per BTC[5], 0.00124 USD per byte.

A. Evaluation of multi-hop payments in PCNs

a) Single multi-hop payment: Let us evaluate the scenario, where we carry out one multi-hop payment, once on top of a Lightning channel and once on top of a generalized channel. To achieve this, we need three outputs, two containing the values for each of the parties and one for the HTLC.

A first difference is that in Lightning channels we need to store these outputs twice, once per commitment. If we were to update a channel to have one HTLC, we would require four off-chain transactions in the Lightning construction, two commitments with three outputs each and one transaction for the HTLC on each commitment. For the generalized channel construction, the number of transactions required for such an update is merely two, one for the commitment transaction and one for the split containing the three outputs. Note that, in the latter case, also the outputs need to be stored only once and that the HTLC does not require an additional transaction. The difference in off-chain transaction size is 1526 bytes for Lightning compared to 818 bytes for generalized channels.

A second difference is that, in ~~the Lightningcase, we need~~ Lightning, a punish mechanism is needed per output. Hence, ~~should~~ if an old commitment transaction ~~get~~ is published, we would require two additional on-chain transactions with a total of 923 bytes in Lightning compared to only two transactions with 663 bytes in the generalized channel construction (including ~~the~~ commitment transaction in both cases). The difference for this is 1.15 ~~USD~~ vs 0.82 USD.

b) Asymptotic analysis: Nodes ~~participating in a payment-channel network~~ in a PCN typically take part in several, ~~let us~~ say n, multi-hop payments at once instead of just one. In this case, the Lightning solution scales even worse, as it requires $2 + 2 \cdot n$ transactions or $706 + 2 \cdot n \cdot 410$ bytes of off-chain transactions. With generalized channels, we only need 2 transactions ~~with a size of~~ of size $695 + n \cdot 123$ bytes.

For punishment, the difference is even more pronounced, as we reduce the asymptotic complexity from linear to constant. Specifically, Lightning channels require $2 + n$ on-chain transactions of $513 + n \cdot 410$ bytes, which cost around $0.64 + n \cdot 0.51$ USD. In generalized channels, the cost for punishment is independent of the number of HTLCs that are constructed on top of the channel. It requires 2 transactions with 663 bytes

[5] ~~https://bitcoinfees.info/~~

[5] ~~https://coinmarketcap.com/currencies/bitcoin/~~

TABLE I
EVALUATION OF LIGHTNING (LC) AND GENERALIZED CHANNELS (GC)

Operations	on-chain			off-chain	
	# txs	size	cost	# txs	size
update (LC)	0	0	0	$2+2\cdot n$	$706+2\cdot n\cdot 410$
update (GC)	0	0	0	2	$695+n\cdot 123$
punish (LC)	$2+n$	$513+n\cdot 410$	$0.64+n\cdot 0.51$	0	0
punish (GC)	2	663	0.82	0	0

TABLE II
CHANNEL SPLITTING

	# txs per sub-channel	size
first split (LC)	4	1412
first split (GC)	2	695
n^{th} split (LC)	2^{n+1}	$353\cdot 2^{n+1}$
n^{th} split (GC)	2	695

resulting in a cost of 0.82 USD. These differences can be observed in Table I for direct comparison.

In Table I, both constructions carry n HTLCs. *# txs* refers to the total number of transactions needed either on-chain or off-chain, *size* refers to the total number of bytes in all required on-/off-chain transactions, respectively, *cost* is in USD and denotes the estimated cost of publishing the transactions.

B. Evaluation of channel splitting

The comparison between Lightning and generalized channels in the case of channel splitting is summarized in Table II. Performing a split in a Lightning channel setting has the drawback of not only doubling off-chain objects that are potentially used on these sub-channels, but also the amount of commitment transactions, i.e., we need to create commitments for the sub-channels on both commitments of the initial channel. So if we were to split a channel, the required number of commitment transactions is four (two for every commitment) for each sub-channel with a total of 1412 bytes. In our generalized channel construction it is just one commitment and one split transaction per sub-channel, which is 695 bytes.

Once a split is performed, the sub-channels are expected to behave as a normal channel. Say that we want to split one of these sub-channels again into two: in the Lightning solution there would now be eight commitments (two for each of the four commitments) per sub-channel. Observe that after every recursive split of a channel, the amount of commitment transactions for the new sub-channel doubles for the Lightning construction. In the generalized channel construction, instead, we only need to keep track of one commitment transaction per sub-channel, therefore the amount of new commitment transactions per split is constant and not exponential. The difference between storing one and eight commitment transactions is 695 bytes for the generalized vs. 2824 bytes for the Lightning construction, not even counting any potential off-chain objects that would need to be stored eight times in the latter case. The amount of transactions needed for updates doubles for every split as well. For n splits, the difference would be 2^{n+1} additional commitment transactions in the Lightning setting against one new commitment and one new split transaction in the generalized channel setting, per sub-channel.

VIII. CONCLUSION

Payment channels constitute ~~one of the most promising approaches~~ a promising approach to tackle the scalability issue of decentralized blockchains. Despite the conceptually appealing design, which in principle supports different types of off-chain applications, existing constructions for Bitcoin-like cryptocurrencies suffer from a heavy communication complexity ~~as well as~~ and on-chain footprint. This ~~fundamentally~~ undermines the potential of payment channels to serve as building block for a variegated multi-application off-chain ecosystem.

In this work, we formalize for the first time the notion of *generalized channels* for Bitcoin-like cryptocurrencies, a generalization of the concept of payment channels that provides off-chain support for any operation ~~supported~~ allowed by the underlying blockchain. Besides the gain in expressiveness and the streamlined design of off-chain applications, generalized channels lead to a significant performance improvement, reducing the communication complexity and the on-chain footprint in case of disputes to linear and constant, respectively, in the number of applications leveraging the channel. Additionally, we provide a cryptographic instantiation of a generalized channel compatible with Bitcoin with provable security guarantees in the Universal Composability framework. To this end, we also introduce the first formalization of *adaptor signatures*, which we believe is of independent interest.

Generalized channels can be integrated today in the Lightning Network and other Bitcoin-compatible off-chain applications, thereby improving their performance. Most importantly, we believe generalized channels pave the way for the design of novel off-chain applications, such as Bitcoin-compatible virtual channels and more efficient and expressive payment channel hub constructions~~, a research direction we intend to explore in the near future.~~.

REFERENCES

[1] L. Aumayr et al. *Bitcoin-Compatible Virtual Channels*. Cryptology ePrint Archive, Report 2020/554. https://eprint.iacr.org/2020/554. 2020.

[2] C. Badertscher et al. "Bitcoin as a Transaction Ledger: A Composable Treatment". In: *CRYPTO 2017, Part I*. Ed. by J. Katz and H. Shacham. Vol. 10401. LNCS. Springer, Heidelberg, Aug. 2017, pp. 324–356.

[3] W. Banasik et al. "Efficient Zero-Knowledge Contingent Payments in Cryptocurrencies Without Scripts". In: *ESORICS 2016, Part II*. Ed. by I. G. Askoxylakis et al. Vol. 9879. LNCS. Springer, Heidelberg, Sept. 2016, pp. 261–280. DOI: 10.1007/978-3-319-45741-3_14.

[4] S. Bano et al. "Consensus in the Age of Blockchains". In: *CoRR* abs/1711.03936 (2017). arXiv: 1711.03936. URL: http://arxiv.org/abs/1711.03936.

[5] *Bitcoin Wiki: Payment Channels*. https://en.bitcoin.it/wiki/Payment_channels. 2018.

[6] D. Boneh et al. “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps”. In: *EUROCRYPT 2003*. Ed. by E. Biham. Vol. 2656. LNCS. Springer, Heidelberg, May 2003, pp. 416–432.

[7] R. Canetti. “Universally Composable Security: A New Paradigm for Cryptographic Protocols”. In: *42nd FOCS*. IEEE Computer Society Press, Oct. 2001, pp. 136–145.

[8] R. Canetti et al. “Universally Composable Security with Global Setup”. In: *TCC 2007*. Ed. by S. P. Vadhan. Vol. 4392. LNCS. Springer, Heidelberg, Feb. 2007, pp. 61–85.

[9] S. Dziembowski et al. “General State Channel Networks”. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*. 2018, pp. 949–966.

[10] S. Dziembowski et al. “Multi-party Virtual State Channels”. In: *EUROCRYPT 2019, Part I*. Ed. by V. Rijmen and Y. Ishai. LNCS. Springer, Heidelberg, May 2019, pp. 625–656. DOI: 10.1007/978-3-030-17653-2_21.

[11] S. Dziembowski et al. *PERUN: Virtual Payment Channels over Cryptographic Currencies*. Cryptology ePrint Archive, Report 2017/635. http://eprint.iacr.org/2017/635. 2017.

[12] S. Dziembowski et al. “Perun: Virtual Payment Hubs over Cryptocurrencies”. In: *2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019*. 2019, pp. 106–123.

[13] C. Egger et al. “Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’19. ACM, 2019, pp. 801–815.

[14] M. Fischlin. “Communication-Efficient Non-interactive Proofs of Knowledge with Online Extractors”. In: *CRYPTO 2005*. Ed. by V. Shoup. Vol. 3621. LNCS. Springer, Heidelberg, Aug. 2005, pp. 152–168.

[15] L. Fournier. *One-Time Verifiably Encrypted Signatures A.K.A. Adaptor Signatures*. https://github.com/LLFourn/one-time-VES/blob/master/main.pdf. 2019.

[16] *Generalized Bitcoin-Compatible Channels (Full Version)*. https://generalized-channels.github.io/.

[17] O. Goldreich. *Foundations of Cryptography: Volume 1*. New York, NY, USA: Cambridge University Press, 2006. ISBN: 0521035368.

[18] L. Gudgeon et al. *SoK: Off The Chain Transactions*. Cryptology ePrint Archive, Report 2019/360. https://eprint.iacr.org/2019/360. 2019.

[19] E. Heilman et al. *The Arwen Trading Protocols (Full Version)*. Cryptology ePrint Archive, Report 2020/024. https://eprint.iacr.org/2020/024. 2020.

[20] E. Heilman et al. *TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub*. Cryptology ePrint Archive, Report 2016/575. http://eprint.iacr.org/2016/575, accepted to the Network and Distributed System Security Symposium (NDSS) 2017. 2016.

[21] J. Katz et al. “Universally Composable Synchronous Computation”. In: *TCC 2013*. Ed. by A. Sahai. Vol. 7785. LNCS. Springer, Heidelberg, Mar. 2013, pp. 477–498. DOI: 10.1007/978-3-642-36594-2_27.

[22] A. Kiayias and O. S. T. Litos. *A Composable Security Treatment of the Lightning Network*. Cryptology ePrint Archive, Report 2019/778. https://eprint.iacr.org/2019/778. 2019.

[23] Y. Lindell. “Fast Secure Two-Party ECDSA Signing”. In: *CRYPTO 2017, Part II*. Ed. by J. Katz and H. Shacham. Vol. 10402. LNCS. Springer, Heidelberg, Aug. 2017, pp. 613–644.

[24] G. Malavolta et al. “Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability”. In: *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. 2019. URL: https://www.ndss-symposium.org/ndss-paper/anonymous-multi-hop-locks-for-blockchain-scalability-and-interoperability/.

[25] G. Malavolta et al. “Concurrency and Privacy with Payment-Channel Networks”. In: *ACM CCS 17*. Ed. by B. M. Thuraisingham et al. ACM Press, 2017, pp. 455–471.

[26] A. Miller et al. “Sprites: Payment Channels that Go Faster than Lightning”. In: *CoRR* abs/1702.05812 (2017). URL: http://arxiv.org/abs/1702.05812.

[27] P. Moreno-Sanchez and A. Kate. *Scriptless Scripts with ECDSA*. lightning-dev mailing list. https://lists.linuxfoundation.org/pipermail/lightning-dev/attachments/20180426/fe978423/attachment-0001.pdf.

[28] A. Poelstra. *Scriptless scripts*. https://download.wpsoftware.net/bitcoin/wizardry/mw-slides/2017-05-milan-meetup/slides.pdf. 2017.

[29] J. Poon and T. Dryja. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Draft version 0.5.9.2, available at https://lightning.network/lightning-network-paper.pdf. Jan. 2016.

[30] *Supplementary material to Generalized Bitcoin-Compatible Channels*. https://generalized-channels.github.io/.

[31] *Update from the Raiden team on development progress, announcement of raidEX*. https://tinyurl.com/z2snp9e. Feb. 2017.

[32] A. Zamyatin et al. *SoK: Communication Across Distributed Ledgers*. Cryptology ePrint Archive, Report 2019/1128. https://eprint.iacr.org/2019/1128. 2019.

New: summary of changes

A. Addressing previous reviews

We would like to thank the reviewers for their valuable comments and suggestions on our submission. We report below the revision conditions and summarize the changes we made to the paper in order to address them:

- Please provide a protocol description which is:

  - complete and clear, preferably in pseudocode, possibly with macros if procedures can and should be re-used in the exact same way as specified in create;
  - self-contained for readers unfamiliar with the UC framework.
- Include a security proof in the supplementary material that convinces the reviewers about the security guarantees of the protocol.

a) Structure of the paper: In Section III, we provide a full description of the protocol including pseudocode (see next point). In Section IV, we formalize Adaptor Signatures and show a construction from ECDSA. In Section V we give an overview of our security model. Finally we have moved the ideal functionality for generalized channelsis to Appendix D.

b) Protocol pseudocode: We give an intuitive description of all protocol parts in prose and further provide the pseudocode of the whole protocol in the main body of the paper. For sake of readability, we abstract in the pseudocode from the technicalities required for the UC proof. The UC components are only added in the supplementary material [30].

c) Reduce UC Dependency: We have reduced the focus on the UC-formalism and explained the different components of the paper such that readers who are not familiar with UC can understand and follow them. To this end, we added a high level explanation on how we proceed in order to prove the security of our protocol in the UC model Section V. We have also moved the Ideal Functionality to the Appendix. Furthermore, we rewrote the application section to remove the UC-formalism and mentioned an additional practical example.

d) Proofs: In Section III, we argue why our protocol satisfies the security properties and the formal UC proof is presented in supplementary material [30].

B. Related work

a) Adaptor signatures: Poelstra introduced the notion of adaptor signatures. In a nutshell, an adaptor signature (AS) is a modified version of a digital signature so that a valid signature can be created only given a witness for a cryptographic hardness assumption (e.g., discrete logarithm problem) [28]. Adaptor signatures have been proven useful in off-chain applications such as PCNs [24].

Given the utility of AS, there have been some attempts to formally use them. For instance, Malavolta et al. [24] use AS as building block to define and realize multi-hop payments in PCNs. However, they do not define AS as a stand alone primitive that can be then used in other works. Concurrent to our work, Fournier [15] attempts to formalize AS as an instance of one-time verifiable encrypted signatures. Yet, in their definition the adversary is not given a pre-signature on the challenge message in the unforgeability and extractability games. However, in applications including our generalized channels, the adversary learns a pre-signature on the message for which it wishes to forge a signature.

Boneh et al. [6] define the notion of verifiably encrypted signatures (VES). In this setting the signer wishes to show the verifier that she has signed a message correctly without revealing the signature. In another similar work, Banasik et al. [3] introduce a method that allows two parties (buyer and seller) to exchange a digital asset using cryptocurrencies that do not support Turing complete programs (smart contracts). Neither of the those works provide a construction that can realize the properties expected from an AS.

b) Generalized channels: The authors in [22] provide a formalization of the Lightning Network (LN) in the UC framework. This formalization is however tailored to the details of the current LN and cannot be leveraged to formalize generalized channels as we propose in this work. State channels enable to execute arbitrary computations off-chain [9, 10, 26]. Moreover, the authors have also provided a formal model in the UC framework. These constructions, however, require a highly expressive scripting functionality (e.g., as in Ethereum) that is not available in many cryptocurrency, including Bitcoin.

C. On the usage of the UC-Framework

To formally model the security of our construction, we use a synchronous version of the global UC framework (GUC) [8] which extends the standard UC framework [7] by allowing for a global setup. Since our model is essentially the same as in [9, 10], parts of this section are taken verbatim from there.

a) Protocols and adversarial model: We consider a protocol π that runs between parties from the set $\mathcal{P} = \{P_1, \ldots, P_n\}$. A protocol is executed in the presence of an *adversary* $\mathcal{A}$ that takes as input a security parameter 1^n (with $n \in \mathbb{N}$) and an auxiliary input $z \in \{0,1\}^*$, and who can *corrupt* any party P_i at the beginning of the protocol execution (so-called static corruption). By corruption we mean that $\mathcal{A}$ takes full control over P_i and learns its internal state. Parties and the adversary $\mathcal{A}$ receive their inputs from a special entity – called the *environment* $\mathcal{E}$ – which represents anything "external" to the current protocol execution. The environment also observes all outputs returned by the parties of the protocol.

b) Modeling time and communication: We assume a synchronous communication network, which means that the execution of the protocol happens in rounds. Let us emphasize that the notion of rounds is just an abstraction which simplifies our model and allows us to argue about the time complexity of our protocols in a natural way. We follow [10], which in turn follows [21], and formalize the notion of rounds via an ideal functionality $\mathcal{F}_{clock}$ representing "the clock". On a high level, the ideal functionality requires all honest parties to indicate that they are prepared to proceed to the next round before the clock is "ticked". We treat the clock functionality as a *global* ideal functionality using the GUC model. This means that all entities are always aware of the given round.

We assume that parties of a protocol are connected via authenticated communication channels with guaranteed delivery of exactly one round. This means that if a party P sends a message m to party Q in round t, party Q receives this message in beginning of round $t+1$. In addition, Q is sure

that the message was sent by party P. The adversary can see the content of the message and can reorder messages that were sent in the same round. However, it can not modify, delay or drop messages sent between parties, or insert new messages. The assumptions on the communication channels are formalized as an ideal functionality $\mathcal{F}_{GDC}$. We refer the reader to [10] its formal description.

While the communication between two parties of a protocol takes exactly one round, all other communication – for example, between the adversary $\mathcal{A}$ and the environment $\mathcal{E}$ – takes zero rounds. For simplicity, we assume that any computation made by any entity takes zero rounds as well.

c) Handling coins: We model the money mechanics offered by UTXO ~~crypotcurrencies~~cryptocurrencies, such as Bitcoin, via a *global* ideal functionality $\mathcal{L}$ using the GUC model. Our functionality is parameterized by a *delay parameter* Δ which upper bounded in the maximal number of rounds it takes to publish a valid transaction, and a signature scheme Σ. The functionality accepts messages from a fixed set of parties $\mathcal{P}$.

The ledger functionality $\mathcal{L}$ is initiated by the environment $\mathcal{E}$ via the following steps: (1) $\mathcal{E}$ instructs the ledger functionality to generate public parameter of the signature scheme pp; (2) $\mathcal{E}$ instructs every party $P \in \mathcal{P}$ to generate a key pair (sk_P, pk_P) and submit the public key pk_P to the ledger via the message $(\text{register}, pk_P)$; (3) sets the initial state of the ledger meaning that it initialize a set $\mathtt{TX}$ defining all published transactions.

Once initialized, the state of $\mathcal{L}$ is public and can be accessed by all parties of the protocol, the adversary $\mathcal{A}$ and the environment $\mathcal{E}$. Any party $P \in \mathcal{P}$ can at any time post a transaction on the ledger via the message $(\text{post}, \mathsf{tx})$. The ledger functionality waits for at most Δ rounds (the exact number of rounds is determined by the adversary). Thereafter, the ledger verifies the validity of the transaction and adds it to the transaction set $\mathtt{TX}$. The formal description of the ledger functionality follows.

Ideal Functionality $\mathcal{L}(\Delta, \Sigma)$

The functionality accepts messages from all parties that are in the set $\mathcal{P}$ and maintains a $\mathtt{PKI}$ for those parties. The functionality maintains the set of all accepted transactions $\mathtt{TX}$ and all unspent transaction outputs $\mathtt{UTXO}$. The set $\mathcal{V}$ defines valid output conditions.

Initialize public keys: Upon $(\text{register}, pk_P) \overset{\tau_0}{\hookleftarrow} P$ and it is the first time P sends a registration message, add (pk_P, P) to $\mathtt{PKI}$.

Post transaction: Upon $(\text{post}, \mathsf{tx}) \overset{\tau_0}{\hookleftarrow} P$, check that $|\mathtt{PKI}| = |\mathcal{P}|$. If not, drop the message, else wait until round $\tau_1 \leq \tau_0 + \Delta$ (the exact value of τ_1 is determined by the adversary). Then check if:

1) The id is unique, i.e. for all $(t, \mathsf{tx}') \in \mathtt{TX}$, $\mathsf{tx}'.\mathsf{txid} \neq \mathsf{tx}.\mathsf{txid}$.
2) All the inputs are unspent and the witness satisfies all the output conditions, i.e. for each $(tid, i) \in \mathsf{tx}.\mathsf{Input}$, there exists $(t, tid, i, \theta) \in \mathtt{UTXO}$ and $\theta.\varphi(\mathsf{tx}, t, \tau_1) = 1$.
3) All outputs are valid, i.e. for each $\theta \in \mathsf{tx}.\mathsf{Output}$ it holds that $\theta.\mathsf{cash} > 0$ and $\theta.\varphi \in \mathcal{V}$.
4) The value of the outputs is not larger than the value of the inputs. More formally, let $I := \{\mathtt{utxo} := (t, tid, i, \theta) \mid \mathtt{utxo} \in \mathtt{UTXO} \wedge (tid, i) \in \mathsf{tx}.\mathsf{Input}\}$, then $\sum_{\theta' \in \mathsf{tx}.\mathsf{Output}} \theta'.\mathsf{cash} \leq \sum_{\mathtt{utxo} \in I} \mathtt{utxo}.\theta.\mathsf{cash}$
5) The absolute time-lock of the transaction has expired, i.e. $\mathsf{tx}.\mathsf{TimeLock} \leq \mathsf{now}$.

If all the above checks return true, add (τ_1, tx) to $\mathtt{TX}$, remove the spent outputs from $\mathtt{UTXO}$, i.e., $\mathtt{UTXO} := \mathtt{UTXO} \setminus I$ and add the outputs of tx to $\mathtt{UTXO}$, i.e., $\mathtt{UTXO} := \mathtt{UTXO} \cup \{(\tau_1, \mathsf{tx}.\mathsf{txid}, i, \theta_i)\}_{i \in [n]}$ for $(\theta_1, \ldots, \theta_n) := \mathsf{tx}.\mathsf{Output}$. Else, ignore the message.

Let us emphasize that our ledger functionality is fairly simplified. In reality, parties can join and leave the blockchain system dynamically. Moreover, we completely abstract from the fact that transactions are published in blocks which are proposed by parties and the adversary. Those and other features are captured by prior works, such as [2], that provide a more accurate formalization of the Bitcoin ledger in the UC framework [7]. However, interaction with such ledger functionality is fairly complex. To increase the readability of our channel protocols and ideal functionality, which is the main focus on our work, we decided for this simpler ledger.

d) The GUC-security definition: Let π be a protocol with access to the global ledger $\mathcal{L}(\Delta, \Sigma)$ and the global clock $\mathcal{F}_{clock}$. The output of an environment $\mathcal{E}$ interacting with a protocol π and an adversary $\mathcal{A}$ on input 1^n and auxiliary input z is denoted as $\text{EXE}^{\mathcal{L}(\Delta,\Sigma),\mathcal{F}_{clock}}_{\pi,\mathcal{A},\mathcal{E}}(n, z)$. Let $\phi_{\mathcal{F}}$ be the ideal protocol for an ideal functionality $\mathcal{F}$ with access to the global ledger $\mathcal{L}(\Delta, \Sigma)$ and the global clock $\mathcal{F}_{clock}$. This means that $\phi_{\mathcal{F}}$ is a trivial protocol in which the parties simply forward their inputs to the ideal functionality $\mathcal{F}$. The output of an environment $\mathcal{E}$ interacting with a protocol $\phi_{\mathcal{F}}$ and a adversary $\mathcal{S}$ (sometimes also call *simulator*) on input 1^n and auxiliary input z is denoted as $\text{EXE}^{\mathcal{L}(\Delta,\Sigma),\mathcal{F}_{clock}}_{\phi_{\mathcal{F}},\mathcal{S},\mathcal{E}}(n, z)$.

We are now ready to state our main security definition which, informally, says that if a protocol π UC-realizes an ideal functionality $\mathcal{F}$, then any attack that can be carried out against the real-world protocol π can also be carried out against the ideal protocol $\phi_{\mathcal{F}}$.

Definition 7. We say that a protocol π *UC-realizes an ideal functionality $\mathcal{F}$ with respect to a global ledger $\mathcal{L} := \mathcal{L}(\Delta, \Sigma)$* and a global clock $\mathcal{F}_{clock}$ if for every adversary $\mathcal{A}$ there exists an adversary $\mathcal{S}$ such that we have

$$\left\{\text{EXE}^{\mathcal{L},\mathcal{F}_{clock}}_{\pi,\mathcal{A},\mathcal{E}}(n, z)\right\}_{\substack{n \in \mathbb{N}, \\ z \in \{0,1\}^*}} \overset{c}{\approx} \left\{\text{EXE}^{\mathcal{L},\mathcal{F}_{clock}}_{\phi_{\mathcal{F}},\mathcal{S},\mathcal{E}}(n, z)\right\}_{\substack{n \in \mathbb{N}, \\ z \in \{0,1\}^*}}$$

(where "$\overset{c}{\approx}$" denotes computational indistinguishability of distribution ensembles, see, e.g., [17]).

To simplify exposition, we omit the session identifiers *sid* and the sub-session identifiers *ssid*. Instead, we will use expressions like "message m is a reply to message m'". We believe that this approach improves readability.

Originally in section "Generalized Channels"

D. Ideal Functionality

We capture the desired functionality of a generalized channelprotocol as an ideal functionality $\mathcal{F}$ interacting with parties from the set $\mathcal{P}$, with the adversary $\mathcal{S}$ (called the simulator) and observes the global ledger functionality $\mathcal{L}$. In a bit more detail, if a party wants to perform an action (such as open a new channel), it sends a message to $\mathcal{F}$ who executes the action and informs the party about the result. The execution might

leak information to the adversary who may also influence the execution. The possible leakage and influence are modeled via the interaction with $\mathcal{S}$. Finally, $\mathcal{F}$ can observe the global ledger and hence verify that a certain transaction appeared on-chain or that a given party owns certain amount of coins. The latter is done by checking if there exists an unspent output whose condition requires signature of (only) the given party P. Recall that we denote such script $\texttt{One-Sig}_{pk_P}$.

We assume that $\mathcal{F}$ maintains a set Γ, where it stores created channels in their latest state and the corresponding funding transaction tx. We sometimes treat Γ as a function which on input id outputs (γ, tx) s.t. $\gamma.\mathsf{id} = id$ if such channel exists and $\perp$ otherwise. To keep $\mathcal{F}$ generic, we parameterized it by two values T and k – both of which must be independent of the blockchain delay Δ. On a high level, the value T upper bounds the maximal number of consecutive off-chain communication rounds between channel users. Since different parts of the protocol might require different amount of communication rounds, the upper bound T might not be reached in all steps. For instance, channel creation might require more communication rounds than old state revocation. To this end, we give the power to the simulator to "speed-up" the process when possible. The parameter k defines the number of ways the channel state $\gamma.\mathsf{st}$ can be published on the ledger. As discussed in Section II, in this work we present a protocol realizing the functionality for $k = 1$ (see Fig. 3). Lightning style generalized channels (see Fig. 2) would be a candidate protocol for $k = 2$. Before we present $\mathcal{F}(T, k)$ formally, we discuss it on a high level and argue why it captures the aforementioned security and efficiency properties identified in Section III. In the text below, we abbreviate $\mathcal{F} := \mathcal{F}(T, k)$.

a) Create: If $\mathcal{F}$ receives a message of the form $(\texttt{CREATE}, \gamma, tid_P)$ from both parties in $\gamma.\mathsf{users}$ within T rounds, it expects a channel funding transaction to appear on the ledger $\mathcal{L}$ within Δ rounds. Such transaction must spend both funding sources (defined by transaction identifiers tid_P, tid_Q) and containing one output of the value $\gamma.\mathsf{cash}$. If this is true, then $\mathcal{F}$ stores this transaction together with the channel γ in the set Γ and informs both parties about the successful channel creation via the message $\texttt{CREATED}$. Since a $\texttt{CREATE}$ message is required from both parties, "consensus on creation" holds.

b) Update: The channel update is initiated by one of the parties P (called the *initiating party*) via a message $(\texttt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}})$. The parameter id identifies the channel to be updated, $\vec{\theta}$ represents the new channel state and t_{stp} denotes the number of rounds needed by the parties to setup off-chain objects (e.g. new channels or hash-time lock contracts) that are being built on top of the channel via this update request. The update is structured into two phases: (i) the prepare phase, and (ii) the revocation phase. Intuitively, the prepare phase models the fact that both parties first agree on the new channel state and get time to setup the off-chain objects on top of this new state. The revocation phase models the fact that an update is only completed once the two parties invalidate the previous channel state. We detail these two phases in the following.

The prepare phase starts when $\mathcal{F}$ receives a vector of transaction identifiers $\vec{tid} = (tid_1, \ldots, tid_k)$ from $\mathcal{S}$.[5] In the optimistic case it is completed within $3T + t_{\mathsf{stp}}$ rounds and ends when the initiating party P receives an $\texttt{UPDATE-OK}$ message from $\mathcal{F}$. The setup phase can be aborted by both the initiating party P and the other party Q. In the ideal world this is achieved by P not sending the $\texttt{SETUP-OK}$ and by Q not sending the $\texttt{UPDATE-OK}$ message, respectively. This models two things. Firstly, the fact that Q might not agree with the proposed update and secondly, the fact that setting up off-chain objects might fail in which case parties want to abort the channel update. The abort may also result in a forceful closing of the channel via the subprocedure $\texttt{ForceClose}$ (which we discuss further below). It happens when one of the parties has sufficient information to enforce the new state on-chain, while the other does not.

In order to complete the update, the revocation phase is executed. The functionality expects to receive the $\texttt{REVOKE}$ message from both parties within $2T$ rounds, in which case it updates the channel state in $\Gamma(id)$ accordingly and informs both parties about the successful updated via the message $\texttt{UPDATED}$. If one of the messages does not arrive, the subprocedure $\texttt{ForceClose}$ is called.

To conclude, the possibility for forceful closing guarantees the security property "consensus on update". Moreover, in case both parties are honest, the duration of an successful update is independent of the ledger delay Δ, hence the efficiency property "optimistic update" is satisfied.

c) Close: Any of the two parties can request closure of the channel via the message $(\texttt{CLOSE}, id)$, where id identifies the channel to be closed. In case both parties request closure within T rounds, *peaceful closure* is expected meaning that a transaction, spending the channel funding transaction and whose output corresponds to the latest channel state $\gamma.\mathsf{st}$, should appear on $\mathcal{L}$ within Δ rounds. In case only one of the parties requests closing, the functionality executes the $\texttt{ForceClose}$ subprocedure in which case such transaction is supposed to appear on $\mathcal{L}$ within 3Δ rounds. In both cases, if the funding transaction is not spent before a certain round, an $\texttt{ERROR}$ message is returned.

d) Punish: In order to guarantee "instant finality with punishments", parties continuously monitor the ledger and apply the punishment mechanism if misbehavior is detected. This is captured by the functionality in the part "Punish" which is executed at the end of each round. The functionality checks if a funding transaction of some channel was spent. If yes, then it expects one of the following to happen: (i) a punish transaction appears on $\mathcal{L}$ within Δ rounds, assigning $\gamma.\mathsf{cash}$ coins to the honest party $P \in \gamma.\mathsf{users}$; or (ii) a transaction whose output corresponds to the latest channel state $\gamma.\mathsf{st}$ appears on $\mathcal{L}$ within 2Δ rounds, meaning that the channel is peacefully or forcefully closed. If none of the above is

[5] For technical reasons, ideal functionality cannot sign transactions and thus it can also not prepare the transaction ids (which is the task of the simulator).

true, ERROR is returned. Hence, under the condition that no ERROR was returned, the security property "instant finality with punish" is satisfied.

e) Simplified formal description: Since we do not aim to make any claims about privacy, we implicitly assume that every message that $\mathcal{F}$ receives/sends from/to a party is directly forwarded to $\mathcal{S}$. When $\mathcal{F}$ expects $\mathcal{S}$ to set certain values, such as the vector of tid's during the update process, and it does not do so, we implicitly assume that ERROR is returned. Moreover, we omit several natural checks that one would expect $\mathcal{F}$ to make. For example, messages with malformed or missing parameters should be ignored, channel instruction should be accepted only from channel users, etc. We formally define all those checks as a functionality wrapper $\mathcal{W}_{checks}$ in the supplementary material [30].

In summary, our functionality formally defined below satisfies the identified security and efficiency properties if no ERROR occurs. In case of an ERROR, all guarantees may be lost. Hence, we are interested only in those protocols realizing $\mathcal{F}$ that never output an ERROR.

Ideal Functionality $\mathcal{F}(T, k)$

We abbreviate $Q := \gamma.\mathsf{otherParty}(P)$ for $P \in \gamma.\mathsf{users}$.

Create

Upon $(\texttt{CREATE}, \gamma, tid_P) \xleftarrow{\tau_0} P$, let $\mathcal{S}$ define $T_1 \leq T$ and:

Both agreed: If already received $(\texttt{CREATE}, \gamma, tid_Q) \xleftarrow{\tau} Q$, where $\tau_0 - \tau \leq T_1$, wait if in round $\tau_1 \leq \tau + \Delta + T_1$ a transaction tx, with $\mathsf{tx.Input} = (tid_P, tid_Q)$ and $\mathsf{tx.Output} = (\gamma.\mathsf{cash}, \varphi)$, appears on the ledger $\mathcal{L}$. If yes, set $\Gamma(\gamma.\mathsf{id}) := (\gamma, \mathsf{tx})$ and $(\texttt{CREATED}, \gamma.\mathsf{id}) \xhookrightarrow{\tau_1} \gamma.\mathsf{users}$. Else stop.

Wait for Q: Else store the message and stop.

Update

Upon $(\texttt{UPDATE}, id, \vec{\theta}, t_{\mathsf{stp}}) \xleftarrow{\tau_0} P$, let $\mathcal{S}$ define $T_1, T_2 \leq T$, parse $(\gamma, \mathsf{tx}) := \Gamma(id)$ and proceed as follows:

1) In round $\tau_1 \leq \tau_0 + T$, let $\mathcal{S}$ define $\vec{tid}$ s.t. $|\vec{tid}| = k$. Then $(\texttt{UPDATE-REQ}, id, \vec{\theta}, t_{\mathsf{stp}}, \vec{tid}) \xhookrightarrow{\tau_1} Q$ and $(\texttt{SETUP}, id, \vec{tid}) \xhookrightarrow{\tau_1} P$.
2) If $(\texttt{SETUP-OK}, id) \xleftarrow{\tau_2 \leq \tau_1 + t_{\mathsf{stp}}} P$, then $(\texttt{SETUP-OK}, id) \xhookrightarrow{\tau_2 + T_1} Q$. Else stop.
3) If $(\texttt{UPDATE-OK}, id) \xleftarrow{\tau_2 + T_1} Q$, then $(\texttt{UPDATE-OK}, id) \xhookrightarrow{\tau_2 + 2T_1} P$. Else distinguish:
   - If Q honest or if instructed by $\mathcal{S}$, stop (update rejected).
   - Else execute $\texttt{ForceClose}(id)$ and stop.
4) If $(\texttt{REVOKE}, id) \xleftarrow{\tau_2 + 2T_1} P$, $(\texttt{REVOKE-REQ}, id) \xhookrightarrow{\tau_2 + 2T_1 + T_2} Q$. Else execute $\texttt{ForceClose}(id)$ and stop.
5) If $(\texttt{REVOKE}, id) \xleftarrow{\tau_2 + 2T_1 + T_2} Q$, set $\gamma.\mathsf{st} := \vec{\theta}$ and $\Gamma(id) := (\gamma, \mathsf{tx})$. Then $(\texttt{UPDATED}, id, \vec{\theta}) \xhookrightarrow{\tau_2 + 2T_1 + 2T_2} \gamma.\mathsf{users}$ and stop. Else distinguish:
   - If Q honest, execute $\texttt{ForceClose}(id)$ and stop.
   - If Q corrupt, and wait for Δ rounds. If tx still unspent, then set $\vec{\theta}_{old} := \gamma.\mathsf{st}$, $\gamma.\mathsf{st} := \{\vec{\theta}_{old}, \vec{\theta}\}$ and $\Gamma(id) := (\gamma, \mathsf{tx})$. Execute $\texttt{ForceClose}(id)$ and stop.

Close

Upon $(\texttt{CLOSE}, id) \xleftarrow{\tau_0} P$, let $\mathcal{S}$ define $T_1 \leq T$ and distinguish:

Both agreed: If you received $(\texttt{CLOSE}, id) \xleftarrow{\tau} Q$, where $\tau_0 - \tau \leq T_1$, let $(\gamma, \mathsf{tx}) := \Gamma(id)$ and distinguish:

- If in round $\tau_1 \leq \tau + T_1 + \Delta$ a transaction tx', with $\mathsf{tx}'.\mathsf{Output} = \gamma.\mathsf{st}$ and $\mathsf{tx}'.\mathsf{Input} = \mathsf{tx.txid}$, appears on $\mathcal{L}$, set $\Gamma(id) := (\bot, \mathsf{tx})$, $(\texttt{CLOSED}, id) \xhookrightarrow{\tau_1} \gamma.\mathsf{users}$ and stop.
- If tx is still unspent in round $\tau + T_1 + \Delta$, output $(\texttt{ERROR}) \xrightarrow{\tau + T_1 + \Delta} \gamma.\mathsf{users}$ and stop.

Wait for Q: Else wait for at most T_1 rounds to receive $(\texttt{CLOSE}, id) \xleftarrow{\tau \leq \tau_0 + T_1} Q$ (in that case option "Both agreed" is executed). If such message is not received, execute $\texttt{ForceClose}(id)$ in round $\tau_0 + T_1$.

Punish (executed at the end of every round τ_0)

For each $(\gamma, \mathsf{tx}) \in \Gamma$ check if $\mathcal{L}$ contains tx' with $\mathsf{tx}'.\mathsf{Input} = \mathsf{tx.txid}$. If yes, then distinguish:

Punish: For $P \in \gamma.\mathsf{users}$ honest, the following must hold: in round $\tau_1 \leq \tau_0 + \Delta$, a transaction tx'' with $\mathsf{tx}''.\mathsf{Input} = \mathsf{tx}'.\mathsf{txid}$ and $\mathsf{tx}''.\mathsf{Output} = (\gamma.\mathsf{cash}, \texttt{One-Sig}_{pk_P})$ appears on $\mathcal{L}$. Then $(\texttt{PUNISHED}, id) \xhookrightarrow{\tau_1} P$, set $\Gamma(id) := \bot$ and stop.

Close: Either $\Gamma(id) = (\bot, \mathsf{tx})$ before round $\tau_0 + \Delta$ (channels was peacefully closed) or in round $\tau_1 \leq \tau_0 + 2\Delta$ a transaction tx'', with $\mathsf{tx}''.\mathsf{Output} \in \gamma.\mathsf{st}$ and $\mathsf{tx}''.\mathsf{Input} = \mathsf{tx}'.\mathsf{txid}$, appears on $\mathcal{L}$ (channel is forcefully closed). In the latter case, set $\Gamma(id) := (\bot, \mathsf{tx})$ and $(\texttt{CLOSED}, id) \xhookrightarrow{\tau_1} \gamma.\mathsf{users}$.

Error: Otherwise $(\texttt{ERROR}) \xrightarrow{\tau_0 + 2\Delta} \gamma.\mathsf{users}$.

Subprocedure $\texttt{ForceClose}(id)$

Let τ_0 be the current round and $(\gamma, \mathsf{tx}) := \Gamma(id)$. If within Δ rounds tx is still an unspent transaction on $\mathcal{L}$, then $(\texttt{ERROR}) \xrightarrow{\tau_0 + \Delta} \gamma.\mathsf{users}$ and stop. Else, latest in round $\tau_0 + 3\Delta$, $m \in \{\texttt{CLOSED}, \texttt{PUNISHED}, \texttt{ERROR}\}$ is output via Punish.