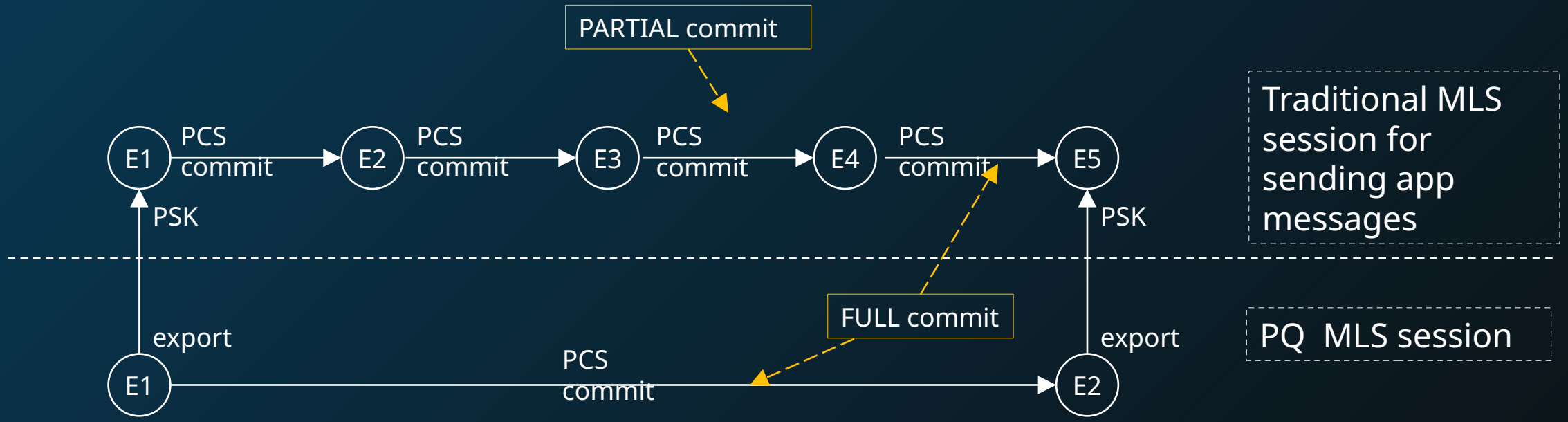
Amortized PQ MLS

Joël Alwen
Britta Hale
Marta Mularczyk
Xisen Tian

Amortized PQ MLS



- More flexible than a hybrid cipher suite

Changes to the Draft

- Renamed to “Hybrid PQ MLS” → “Amortized PQ MLS”

- New data formats bundling data from both MLS groups together.

```
struct {
  KeyPackage  t_key_package;
  KeyPackage pq_key_package;
} APQKeyPackage
```

```
struct {
  MLSPublicMessage  t_message;
  MLSPublicMessage pq_message;
} APQMLSPublicMessage
```

```
struct {.} APQMLSPrivateMessage
struct {.} APQWelcome
struct {.} APQGroupInfo
struct {.} APQPartialGroupInfo
```

Safe Application Interface

Interface is used by an application component, identified by component ID

APQMLS use:

- Safe Export Secret to export PSK and PSK ID
- Store APQInfo in a group context extension

APQMLS now fully compatible with the Safe API:

- Component ID set to 0x0006
- Correct function name SafeExportSecret
- Modify APQInfo in group context extensions using App Data Update proposal

PSK ID from Key Schedule

- Export PSK ID for PQ MLS group.
  - Use SafeExporterSecret() from the Safe Application Interface
    - See draft-ietf-mls-extensions v09

PQ MLS Group	Traditional MLS Group

`apq_exporter := SafeExporterSecret(0x0006);`
`apq_psk_id := DeriveSecret(apq_exporter, “psk_id”);`
	`PreSharedKeyID pskID;`
	`pskID.psktype := external(1);`
	`pskID.psk_id := apq_psk_id;`
	`pskID.psk_nonce := RandomBytes(KDF.Nh);`

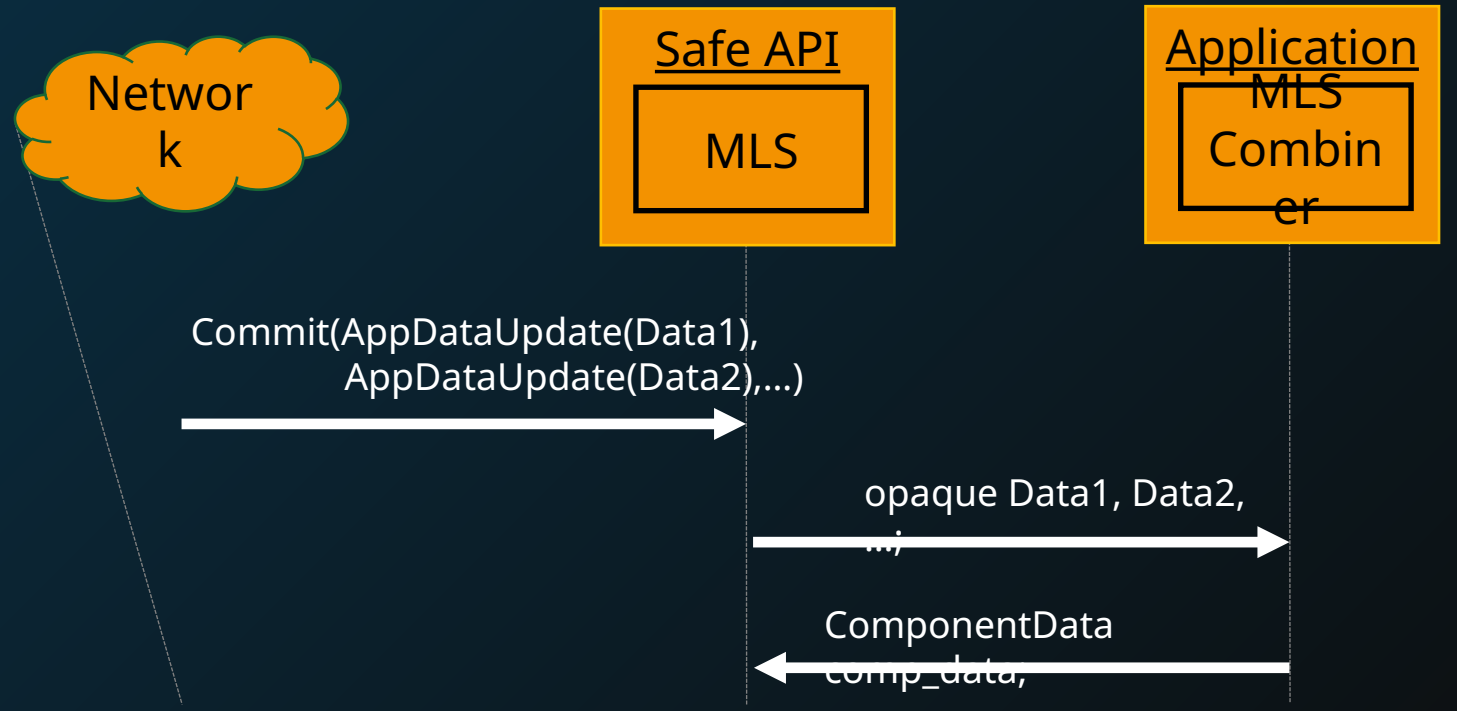
Updating APQMLS State Using Safe API

AppDataUpdate proposal from Safe API

- Structure – opaque update data

Integration with APQMLS:

```
struct {
    APQUpdateType update_type;
    select (update_type) {
        case full_update:
            APQInfo new_apq_info;
        case new_t_epoch:
            uint64 new_t_epoch;
        case new_pq_epoch:
            uint64 new_pq_epoch;
} APQInfoUpdate;
```



PQ Authenticity Guarantees

Clarified PQ authenticity guarantees:

> *Note that an active attacker with access to a CRQC can become a group member by impersonating members in the moment they are added. As such, the authenticity guarantees outlined above only hold as long as the adversary is passive during the addition of new group members.*