Principles of Cryptocurrency Design

Appunti ed Esercizi

Francesco Pasquale

12 marzo 2024

1 Il protocollo di Dolev-Strong

Consideriamo il protocollo di Dolev-Strong [1] per il problema Byzantine Broadcast.

Algorithm 1 Dolev-Strong Protocol for Byzantine Broadcast

1: ROUND 0. Ogni nodo i inizializza un insieme vuoto $\mathcal{E}_i = \emptyset$.
2: La sorgente (il nodo 1) riceve in input b e invia $\langle b \rangle_1$ a tutti i nodi.
3: PER OGNI ROUND $r = 1, \ldots, f$. Ogni nodo i:
4: Per ogni messaggio $\langle \hat{b} \rangle_{1,j_1,j_2,\ldots,j_{r-1}}$ con r firme distinte (inclusa quella
5: della sorgente) ricevuto nel Round $r-1$:
6: SE $\hat{b} \notin \mathcal{E}_i$:
7: Aggiungi $\hat{b}$ a $\mathcal{E}_i$;
8: Firma il messaggio $\langle \hat{b} \rangle_{1,j_1,j_2,\ldots,j_{r-1}}$;
9: Invia il messaggio firmato $\langle \hat{b} \rangle_{1,j_1,j_2,\ldots,j_{r-1},i}$ a tutti i nodi;
10: ROUND $f+1$. Ogni nodo i:
11: Per ogni messaggio $\langle \hat{b} \rangle_{1,j_1,j_2,\ldots,j_f}$ con $f+1$ firme distinte (inclusa quella
12: della sorgente) ricevuto nel Round f:
13: SE $\hat{b} \notin \mathcal{E}_i$, aggiungi $\hat{b}$ a $\mathcal{E}_i$;
14: SE $\mathcal{E}_i$ contiene un solo elemento, allora OUTPUT l'elemento in $\mathcal{E}_i$,
15: Altrimenti OUTPUT 0

Esercizio 1. Alle linee 4 e 11 del protocollo ogni nodo onesto verifica, oltre al *numero* di firme distinte presenti (r firme per messaggi arrivati nel round $r-1$), che fra le firme ci sia anche la firma della sorgente. Descrivere un attacco al protocollo che i nodi corrotti potrebbero mettere in atto se i nodi onesti non verificassero la presenza della firma della sorgente.

Esercizio 2. Supponete che c'è un *bug* nell'implementazione del sistema di firme digitali usato nel protocollo che consente a un nodo corrotto di falsificare le firme dei nodi onesti. Descrivere un attacco al protocollo che i nodi corrotti possono mettere in atto in questo caso.

Riferimenti bibliografici

[1] Danny Dolev and H. Raymond Strong. Authenticated algorithms for Byzantine agreement. *SIAM Journal on Computing*, 12(4):656–666, 1983.