Graph state digital signature scheme

CONTENTS

I. GRAPH STATES

* Definition via stabilisers:

$$S_j = X_j \bigotimes_{k \in n(j)} Z_k, \quad \forall\, j \in V(G). \tag{1.1}$$

* Transformation and measurement rules. (**??**)

* Graph transformation rules for Z and Y measurements:

$$\begin{aligned} P^{(Z)}_{j,\pm} \left|G\right\rangle &= U^{(Z)}_{j,\pm} \left|G - j\right\rangle, \\ P^{(Y)}_{j,\pm} \left|G\right\rangle &= U^{(Y)}_{j,\pm} \left|\tau_j(G) - j\right\rangle, \end{aligned} \tag{1.2}$$

where $\tau_j(G)$ denotes local complementation of the neighbourhood of vertex j in G,

$$\tau_j(G) = G \oplus [j + n(j)], \tag{1.3}$$

using XOR arithmetic on the edge set of G.

* Respective local corrections for Z and Y measurements:

$$\begin{aligned} U^{(Z)}_{j,+} &= I, \\ U^{(Z)}_{j,-} &= \bigotimes_{k \in n(j)} Z_k, \\ U^{(Y)}_{j,+} &= \bigotimes_{k \in n(j)} \sqrt{-iZ_k}, \\ U^{(Y)}_{j,-} &= \bigotimes_{k \in n(j)} \sqrt{iZ_k}, \end{aligned} \tag{1.4}$$

II. GRAPH STATES SIGNATURE SCHEME

* Describe one-way interpretation: $G \to \rho(G)$.

* Describe commit-reveal interpretation.

* Random graph construction.

* Describe protocol.

* How encoding via pairwise measurements works.

* Local correction rules:

The local correction rules for Pauli measurements are neighbourhood dependent. We would like local corrections to reveal to information about the random partitions associated with measurement qubits. This requires that all local corrections be uniform.

III. SECURITY PROOF

* Proof that adjacency matrix exponentially converges to uniform and separable random edge set.

* Argue that this affords information theoretic security, parameterised by statistical security $\varepsilon = 1/2^n$.

REFERENCES