Graph state digital signature scheme

CONTENTS

I. Graph states 1

II. Graph states signature scheme 1

III. Security proof 1

I. GRAPH STATES

* Definition via stabilisers.

* Transformation and measurement rules.

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.

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 $\varepsilon = 1/2^n$.