Quantum cryptographic primitives using graph states

Peter P. Rohde[1]
[1] *BTQ Technologies*

CONTENTS

I. STABILISER STATES

The Pauli group on n qubits, $\mathcal{P}_n$, comprises arbitrary kronecker products of n Pauli operators,

$$\sigma_0 \equiv I,\, \sigma_1 \equiv X,\, \sigma_2 \equiv Y,\, \sigma_3 \equiv Z, \tag{1.1}$$

with phase $\{\pm 1, \pm i\}$,

$$\begin{aligned}\mathcal{P}_1 &= \{\pm 1, \pm i\} \times \{I, X, Y, Z\},\\ \mathcal{P}_n &= \mathcal{P}_1^{\otimes n}.\end{aligned} \tag{1.2}$$

Stabilisers for an n-qubit stabiliser state form a commutative subgroup of $\mathcal{P}_n$, which we will express as,

$$S_i = p_i \bigotimes_{j=1}^{n} X_j^{x_{i,j}} Z_j^{z_{i,j}}, \tag{1.3}$$

for the ith stabiliser. Here $x_{i,j}, z_{i,j} \in \{0,1\}$ are binary coefficients indicating the presence (1) or absence (0) of X or Z operators respectively, and $p_i \in \{\pm 1, \pm i\}$ are phase factors. Note that X and Z form a generating set of operators for $\mathcal{P}$ where $XZ = -iY$. Hence the x and z binary coefficients capture all four Pauli matrices.

An n-qubit stabiliser state $|\psi\rangle$ is fully characterised by n independent stabilisers, where $|\psi\rangle$ is the simultaneous $+1$ eigenstate of all S_i,

$$S_i \,|\psi\rangle = |\psi\rangle \;\forall\, i. \tag{1.4}$$

Stabilisers are not unique. Since,

$$S_i S_j \,|\psi\rangle = S_i \,|\psi\rangle = S_j \,|\psi\rangle = |\psi\rangle\,, \tag{1.5}$$

any product of stabilisers is also a stabiliser, $S_k = S_i S_j$.

Each stabiliser can be expressed as a binary vector,

$$S_i \cong [\mathbf{x}_i | \mathbf{z}_i | p_i], \tag{1.6}$$

where $\mathbf{x}_i$ ($\mathbf{z}_i$) is a row vector of $x_{i,j}$ ($z_{i,j}$).

A stabiliser set can be represented as a $(2n+1) \times n$ binary matrix,

$$[\mathbf{X}|\mathbf{Z}|\mathbf{P}], \tag{1.7}$$

known as the *tableau matrix.*

The Clifford group is the set of unitary operations that commute with the Pauli group and hence map stabiliser states to stabiliser states. Equivalently, stabiliser states can be considered the class of states accessible via Clifford operations acting on computational basis states. Clifford operations acting on stabiliser states are efficiently classically simulatable, related by conjugation (Gottesman, 1998). Since,

$$\begin{aligned}S\,|\psi\rangle &= |\psi\rangle\,,\\ USU^\dagger U\,|\psi\rangle &= U\,|\psi\rangle\,,\end{aligned} \tag{1.8}$$

this implies the stabiliser S' of a stabiliser state $|\psi\rangle$ evolved by Clifford operation U is,

$$\begin{aligned}S' &= USU^\dagger,\\ S'U\,|\psi\rangle &= U\,|\psi\rangle\,.\end{aligned} \tag{1.9}$$

A. Properties of stabilisers & stabiliser states

Add the tableau representation of the 3-qubit Bell state.

Since a stabiliser state $|\psi\rangle$ is the simultaneous eigenstate of its stabilisers, measuring a stabiliser S_i as an observable necessarily and deterministically yields the $+1$ measurement outcome and leaves the state unchanged.

Stabilisers define constraints on the collective measurement outcomes of qubits. Consider the 3-qubit Bell state,

$$|\psi\rangle = (|000\rangle + |111\rangle)/\sqrt{2}. \tag{1.10}$$

This has stabilisers,

$$\begin{aligned} S_1 &= XXX, \\ S_2 &= ZZI, \\ S_3 &= IZZ. \end{aligned} \tag{1.11}$$

The S_1 stabiliser implies that upon measuring all qubits individually on the X basis the product of the measurement outcomes is $+1$. Similarly, the S_2 and S_3 stabilisers tell us that upon measuring the two qubits associated with Z operators in the Z basis the measurement outcomes multiply to $+1$.

B. Proofs-of-quantumness

Let Alice prepare an n-qubit stabiliser state $|\psi\rangle$ and give it to Bob. As the state description (stabiliser set) is only known to Alice, only Alice can prepare copies of $|\psi\rangle$. Hence the instance of $|\psi\rangle$ can be regarded as unique by Alice.

If Alice subsequently challenges Bob to report measurement results on $|\psi\rangle$, where the challenges are chosen from the stabiliser set $\{S_i\}$ known only to Alice, correct responses by Bob act as a zero-knowledge proof that Bob possesses $|\psi\rangle$. In this context, 'zero-knowledge' refers to 'quantumness', i.e Bob proves possession of a quantum state without sharing any quantum information, requiring only classical communication.

Since stabilisers form a compact representation of the respective stabiliser state, n such challenges to Bob provides a complete proof of possession of state $|\psi\rangle$, requiring only $O(n)$ query complexity. However, as the challenge questions reveal stabilisers, a complete proof of n correct stabiliser measurements implies Bob upon completion possesses a complete description of the state, implying a single-use property. Similarly, if Eve intercepts these queries she may subsequently reproduce $|\psi\rangle$ and spoof further queries.

C. Zero Knowledge Proof of Quantumness

* A general construction of ZKPoQ: step-by-step performed by both parties Alice and Bob.

II. R1CS CONSTRAINT SYSTEMS

*This section will give a more detail explanations about the R1CS and why can we build a ZKPs from it!

A. R1CS

An R1CS constraint is of the form,

$$(\mathbf{a}\cdot\mathbf{s})\times(\mathbf{b}\cdot\mathbf{s}) = (\mathbf{c}\cdot\mathbf{s}), \tag{2.1}$$

where $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{s}$ are vectors over a field $\mathcal{F}$, $\cdot$ denotes the vector dot-product, and s is a solution to the constraint system.

For a system of such constraints, we have,

$$(\mathbf{A}\cdot\mathbf{s})\times(\mathbf{B}\cdot\mathbf{s}) = (\mathbf{C}\cdot\mathbf{s}), \tag{2.2}$$

where $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ are matrices whose rows are of the form Eq. (2.1), one row for every constraint, which must all be simultaneously satisfied. Here $\mathbf{a}\times\mathbf{b}$ denotes element-wise vector multiplication.

B. Quadratic Arithmetic Programs

* QAPs are the primary reason ZK-SNARKs are able to be succinct?

* Succinct?

C. Why can we build a ZKPs from R1CS?

* ZK-SNARKs is built step-by-step from R1CS to QAP to the formal ZKPs construction. Can we do the same with ZKPoQ, going from constraints on the stabilisers to .... to the general definition of ZKPoQ.

III. STABILISERS STATES AS R1CS

Defining an R1CS relative the binary field, $\mathcal{F} = \mathrm{GF}(2)$, a stabiliser is equivalent to a single R1CS constraint, and a stabiliser set to an R1CS constraint system.

IV. PRIMITIVES

The following primitives afforded by stabiliser states apply both locally and non-locally as multi-qubit constraints are enforced by entanglement. This facilitates distributed constraints in a multi-party context.

A. Parity constraints on single-qubit measurement outcomes

Stabiliser,

$$S_i = p_i \bigotimes_{j=1}^{n} X_j^{x_{i,j}} Z_j^{z_{i,j}}, \tag{4.1}$$

imposes a parity-conservation constraint on single-qubit measurement outcomes,

$$p_i \prod_{i=1}^{n} M(X_j^{x_{i,j}} Z_j^{z_{i,j}}) = 1, \tag{4.2}$$

where $M(O) = \pm 1$ is the measurement outcome of observable O.

That is, upon measuring the string of single-qubit Pauli operators in a stabiliser the product of their measurement outcomes is a constant enforced by the stabiliser. A stabiliser does not impose any constraints on the measurement outcomes from a distinct sequence of Pauli operators.

B. Proof of quantum state possession

Measuring any stabiliser, which in general requires entangling measurements, necessarily yields

$$M(S_i) = 1, \forall\, i, \tag{4.3}$$

outcomes while leaving $|\psi\rangle$ unchanged.

If Alice knows $|\psi\rangle$ and challenges Bob to randomly measure $\pm S_i$, if Bob correctly reports all $M(\pm S_i)$ this proves to Alice his measurements reflect that of $|\psi\rangle$. The likelihood of guessing all measurement outcomes asymptotically vanishes,

$$P(n) = \frac{1}{2^n}. \tag{4.4}$$

C. No-cloning

$|\psi\rangle$ cannot be copied unless its stabilisers are, but can be infinitely reproduced if all S_i are known. Hence, if Alice privately prepares a state and transfers it to Bob she has confidence only a single copy of $|\psi\rangle$ exists.

V. EXAMPLES

A. Quantum key distribution (QKD)

Consider the BB84 QKD protocol. Alice prepares n separable qubits as randomly chosen basis states in the X or Z basis, also chosen randomly.

Let,

$$m_i^{(A)} \in \{-1, +1\} \tag{5.1}$$

denote Alice's chosen basis state for the ith qubit, similarly defined for Bob's measured basis state, $m_i^{(B)}$. And let,

$$b_i^{(A)} \in \{0 \equiv X, 1 \equiv Z\}, \tag{5.2}$$

denote Alice's encoding basis, likewise for Bob with $b_i^{(B)}$.

Hence, the ith qubit prepared by Alice has a stabiliser form,

$$S_i \in \{Z_i, -Z_i, X_i, -X_i\}, \tag{5.3}$$

chosen uniformly at random, with implied I_j operators for all $j \neq i$.

The tableau representation can therefore be considered as having diagonal $\mathbf{X}$ and $\mathbf{Z}$ blocks, where $\mathbf{P}$ denotes the respective basis state,

$$\begin{aligned} \mathbf{X} &= \mathrm{diag}(x_i), \\ \mathbf{Z} &= \mathrm{diag}(z_i), \\ \mathbf{P} &= \mathrm{diag}(m_i^{(A)}). \end{aligned} \tag{5.4}$$

The $\mathbf{X}$ and $\mathbf{Z}$ blocks now capture encoding basis, while the $\mathbf{P}$ encodes the basis state via the respective ± 1 eigenvalue.

Since all stabilisers have a non-trivial operator at location i we have, $x_i = \bar{z}_i$,

$$\mathbf{X} + \mathbf{Z} = \mathbf{I}. \tag{5.5}$$

Stabiliser $S_i = \{\pm X, \pm Z\}$ imposes a measurement constraint on each qubit, where all constraints are independent.

The tableau block matrices of the state prepared by Alice are now structured as,

$$\begin{aligned} x_{i,i} &= \bar{b}_i^{(A)} m_i^{(A)}, \\ z_{i,i} &= b_i^{(A)} m_i^{(A)}, \end{aligned} \tag{5.6}$$

where $\bar{b} = (1 - b)$ is the binary complement.

Upon completing the protocol and comparing measurement bases we have the constraint,

$$m_i^{(B)} = \begin{cases} m_i^{(A)}, & b_i^{(A)} = b_i^{(B)} \\ \mathrm{Ber}(1/2), & b_i^{(A)} \neq b_i^{(B)} \end{cases},$$

where $\mathrm{Ber}(1/2) \in \{-1, +1\}$ is a Bernoulli random variable with $p = 1/2$.

The binary vector,

$$\mathbf{c} = \mathbf{b}^{(A)} \times \mathbf{b}^{(B)}, \tag{5.7}$$

is a mask indicating which bases were consistent between Alice and Bob.

Consider the subset of consistent measurement basis ($c_i = 1$). Now $\mathbf{c}$ masks out a sub-matrix of the original tableau matrix,

$$\mathbf{P} \cdot \mathbf{c} = \mathbf{m}^{(B)} \cdot \mathbf{c}, \tag{5.8}$$

which defines the correctness constraint on the subset of qubits where Alice and Bob employ the same basis. Note that,

$$\mathbf{P} \cdot \mathbf{c} = \mathbf{m}^{(A)} \cdot \mathbf{c}, \tag{5.9}$$

holds by definition.

For inconsistent measurement basis we have,

$$\mathbb{P}(\mathbf{P}\cdot\bar{\mathbf{c}}=\mathbf{m}^{(B)}\cdot\bar{\mathbf{c}})=\frac{1}{\sqrt{2^{|\bar{\mathbf{c}}|}}}, \tag{5.10}$$

where $|\mathbf{c}|$ denotes Hamming weight.

Any set,

$$W=(\mathbf{b}^{(A)},\mathbf{b}^{(B)},\mathbf{m}^{(A)},\mathbf{m}^{(B)}) \tag{5.11}$$

satisfying Eq. (5.8) acts as a witness for an instance of the QKD protocol.

B. Quantum authentication

$HMP4$ states,

$$\begin{aligned}|\alpha(x)\rangle&=\frac{1}{2}\sum_{i=1}^{4}(-1)^{x_i}\,|(i-1)_2\rangle\\&=\frac{1}{2}[\beta_1\,|00\rangle+\beta_2\,|01\rangle+\beta_3\,|10\rangle+\beta_4\,|11\rangle]\end{aligned} \tag{5.12}$$

where $x\in\{0,1\}^4$, $(\cdot)_2$ denotes base-2 representation, and $\beta_i=(-1)^{x_i}$.

$HMP4$ condition for verification,

$$b=\begin{cases}x_1\oplus x_{2+m}, & a=0\\ x_{3-m}\oplus x_4, & a=1\end{cases},$$

where we say $(x,m,a,b)\in HMP_4$ if this condition is satisfied, the verification constraint. Here Alice holds x and m, while Bob provides a and b.

C. Interactive proofs of quantumness (IPQ)

The interactive IPQ protocol based on TCFs generates bit-string superpositions from an underlying lattice construction, whose measurement by a prover provide a proof for the verifier.

Consider a superposition of two bit-strings,

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|x\rangle+|y\rangle), \tag{5.13}$$

where $x,y\in\{0,1\}^n$ and $x\neq y$.

Define the subsets of bits,

$$s_{a,b}=\{i\,|\,(x_i,y_i)=(a,b)\}_{i\in\{1,\dots,n\}}. \tag{5.14}$$

We introduce stabilisers:

$$\begin{aligned}&S=Z_i,\ \forall\, i\in s_{0,0},\\&S=-Z_i,\ \forall\, i\in s_{1,1},\\&S=\bigotimes_{i\in s_{0,1}\cup s_{1,0}}X_i,\\&S=\bigotimes_{i\in s_{0,1}\cup s_{1,0}}Z_{(s_{0,1}\cup s_{1,0})_1}Z_i,\end{aligned} \tag{5.15}$$

D. Quantum anonymous broadcasting

GHZ state,

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle^{\otimes n}+|1\rangle^{\otimes n}). \tag{5.16}$$

Stabilisers,

$$\begin{aligned}&S_1=X^{\otimes n},\\&S_i=Z_{i-1}\otimes Z_i,\quad 2\leq i\leq n.\end{aligned} \tag{5.17}$$

S_1 enforces a parity constraint upon measuring all qubits in the X basis,

$$\prod_{i=1}^{n}M(X_i)=1, \tag{5.18}$$

where $M(X_i)=\pm1$ is the measurement outcome of the X_i observable.

If a Z_i gate is applied to any qubit this flips the sign of the collective constraint, independent of which qubit Z_i was applied to, enforcing anonymity.

VI. GRAPH STATES

For a graph $G=(E,V)$ let $\rho(G)$ be the respective graph state.

We have the one-way property that given G one can prepare and infinitely reproduce $\rho(G)$,

$$G\to\rho(G), \tag{6.1}$$

but given $\rho(G)$ one cannot obtain G,

$$\rho(G)\not\to G, \tag{6.2}$$

If G is revealed $\rho(G)$ can be verified by measuring all its stabilisers with $+1$ outcome. The likelihood of obtaining all $+1$ outcomes for a graph $G'\neq G$ scales as $1/2^n$ for $n=|V|$, the statistical security of the commitment $\rho(G)$.

A. Digital signatures

Let $\mathcal{X}_n$ denote the uniform distribution of random graphs with n vertices where all edges exist with probability $p = 1/2$. Hence the edge-sets $E(\mathcal{X}_n)$ have maximum entropy.

Using a graph with $2m+n$ qubits let the secret key be $G \in \mathcal{X}_{2m+n}$ and $\rho(G)$ be the public key. Hence,

$$\begin{aligned}\texttt{KeyGen} &: \{G \in \mathcal{X}_{2m+n}, \rho(G)\},\\ \texttt{SecKey} &: G,\\ \texttt{PubKey} &: \rho(G).\end{aligned} \tag{6.3}$$

Alice can infinitely reproduce $\rho(G)$ to provide to any number of parties.

We pair the first $2m$ qubits to encode m message bits, 2 qubits per message bit.

Taking $\rho(G)$, to verify Alice's message he measures each qubit pair in the bases (Z, Y) for $m = 0$ or (Y, Z) for $m = 1$.

Qubits measured in Z are eliminated while Y measurements perform an edge complement on the subgraph induced by the random subset of vertices that qubit is connected to.

Thus the measurements for each message bit implement one of two possible random edge complementations.

Upon performing all message bit measurements Bob has a reduced n-qubit random graph as a function of the message, $\rho(G'(m))$ (where $|V(G')| = n$), also with maximum edge set entropy.

Alice knows the reduced graph $G'(m)$ itself, which can be efficiently computed given knowledge of G, whereas Bob knows neither G nor G', always perceiving maximum entropy graphs.

Alice's signature is the disclosure of $G'(m)$, which Bob can verify by measuring the respective stabilisers with $+1$ outcome. He has statistical security scaling as $\varepsilon = 1/2^n$.

Bob's knowledge of G' does not allow him to know G (the private key), since they are both maximum entropy and related by random edge complementations.

We have both a binding and hiding property for the signature. Non-repudiation here arises from all random signature graphs G' being distinct. Collisions (i.e multiple messages reducing to the same random graph) provide opportunity for repudiation. The collision rate scales inverse exponentially with n.

Thus by pre-sharing an $2m + n$ qubit random graph with Bob, Alice can sign an m bit classical message with n bit statistical security.

There are no hardness assumptions, only information-theoretic ones.

Message information is not block-encoded, rather all message bits are collectively encoded into the reduced state G' under a random, maximum-entropy code.

This is a general signature scheme affording arbitrary parameterisation of m and n with information-theoretic security given by n.

B. ZKPs for NP-complete graph problems

Consider a graph-theoretic problem in NP whose solution can be expressed in the form of a partitioning of G into k edge-disjoint spanning (i.e same vertex set) subgraphs,

$$G = \sum_{i=1}^{k} G_i, \tag{6.4}$$

whose solution can be verified from the properties of the partitions $\{G_i\}_i$.

Since the partitions G_i are edge-disjoint the degree of every vertex $v \in G$ is given by the sum of the respective vertex degrees in each partition,

$$d(v \in G) = \sum_{i=1}^{k} d(v \in G_i), \forall\, v, \tag{6.5}$$

affording verification of Eq. (6.4).

1. Interactive proof protocol

For given graph G known to both prover (P) and verifier (V) with witness $\{G_i\}_i$ known only to P we perform the following N times,

- P prepares and commits the witness (i.e solution) state,

  $$\rho_{\texttt{sol}} = \bigotimes_{i=1}^{k} \rho(G_{\pi_i}),\ \pi \in S_k \tag{6.6}$$

  with random ordering of the elements G_i.
- V challenges P by choosing a random vertex $v \in G$.
- P reveals the local neighbourhood of $v \in G_i$ for all partitions i.

2. Verification

Verification by V succeeds if for every iteration over N with independently chosen random challenge vertex v,

- $d(v \in G) = \sum_{i=1}^{k} d(v \in G_i)$.
- $\texttt{ngh}(v \in G) = \bigcup_{i=1}^{k} \texttt{ngh}(v \in G_i)$.
- The set of local neighbourhoods,

  $$W = \{\texttt{ngh}(v \in G_i)\}_i, \tag{6.7}$$

  satisfy the necessary and sufficient conditions for satisfying solutions of the respective NP graph problem,

  $$\texttt{Sat}_G(W) \to \{0, 1\}. \tag{6.8}$$

These properties can all be verified by measuring the respective stabilisers implied by the revealed local neighbourhoods of challenge vertex v in each partition G_i,

$$S_{v\in G_i} = X_{v\in G_i} \prod_{j\in\mathtt{ngh}(v\in G_i)} Z_j, \tag{6.9}$$

with all $+1$ measurement outcomes,

$$M(S_{v\in G_i}) = 1,\ \forall\, i. \tag{6.10}$$

For each iteration over N the likelihood of measuring all $+1$ outcomes for incorrect solutions is $1/2^k$, and the overall statistical security is,

$$\varepsilon = 1/2^{kN}. \tag{6.11}$$

3. Compatible NP-complete graph problems

a. Edge colouring For a k-colouring of graph G the solution can be expressed as k edge-disjoint subgraphs $G_i \subseteq G$ where each G_i contains the edges for colour i.

A valid edge-colouring implies all vertices in every graph partition have degree 0 or 1 (necessary and sufficient),

$$\mathtt{Sat}_G(W) = \begin{cases} 1, & d(v\in G_i) \in \{0,1\},\ \forall\, G_i \\ 0, & \text{otherwise} \end{cases}. \tag{6.12}$$

b. Perfect matchings In a perfect matching, M, every vertex is connected by exactly one edge (necessary and sufficient),

$$d(v\in M) = 1,\ \forall\, v \in G. \tag{6.13}$$

A perfect matching can be decomposed into $k = |V(G)|/2$ subgraphs each containing a single edge from the matching.

For vertex v exactly one subgraph G_i will exhibit $d(v \in G_i) = 1$ with all others having $d(v \in G_{j\neq i}) = 0$ and collectively sum to 1 (necessary and sufficient),

$$\mathtt{Sat}_G(W) = \begin{cases} 1, & \sum_{i=1}^{k} d(v\in G_i) = 1, \\ 0, & \text{otherwise} \end{cases}. \tag{6.14}$$

REFERENCES

Gottesman, Daniel (1998), “The heisenberg representation of quantum computers,” arXiv:quant-ph/9807006.