Optimality of approximate encryption schemes

Ashwin Nayak

University of Waterloo, and

Perimeter Institute for Theoretical Physics

Joint work with

Paul Dickinson, Leonard Schulman

Encryption of quantum states

- To encrypt qubit state ρ,
  map to completely mixed state ½ I

- Scheme
  - Pick random Pauli $U \in \{ I, X, Y, Z \}$
  - Apply U to state $\rho \rightarrow U\rho U^*$

$$\rho \rightarrow \tfrac{1}{4} (\rho + X\rho X + Y\rho Y + Z\rho Z)$$

- Fact: above operation maps every state ρ to ½ I

Size of key

- Picked one of 4 Paulis: 2^2 bits to encrypt 2-dim state

- Scheme generalizes to *n* quantum bits
  - Apply independently chosen random Pauli to each qubit
  - $d^2 = (2^n)^2$ operators for $d = 2^n$ dimensional states

- Theorem [BR'03, AMTdW'00, Jain'05, NS'06]

  d^2 unitaries are required for perfect randomization of d-dimensional states

- Relaxed notion [HLSW'04]

  Target state close to completely mixed

Approximate encryption

- **Theorem** [HLSW'04]

  If randomized state is ε close to completely mixed state

  $O(d \log d / \varepsilon^2)$

  unitary operators suffice

  key length = $n + \log n + O(\log(1/\varepsilon))$

  Closeness in trace norm

  $$\| M \|_{tr} = \mathrm{Tr} \sqrt{M^* M}$$

  characterizes distinguishability via measurements

- **Efficient, explicit scheme** [AS'04]
  - Same parameters, or
  - With $O(d/\varepsilon^2)$ unitaries, but cipher text has extra $2 \log d$ bits

Key size for approximate encryption

- Observation [DN'06]

  Improved efficient scheme

  $O(d / \varepsilon^2)$ unitary operators,

  i.e., $n + 2 \log (1/\varepsilon) + 4$ bits of key suffice

  (No increase in length of cipher text)

  Unitary operators used: Pauli operators

- This talk [DN'06; NS, ongoing]

  $\Omega(d / \varepsilon)$ Pauli operators are necessary

  $n + \log (1/\varepsilon) - O(1)$ bits of key are necessary

Lower bound for key length

- Kind of randomizing map studied
- Connection to pseudo-randomness
- Lower bound for sample space of pseudo-random distribution

Kind of randomizing map

- Consider n qubit states; dimension $d = 2^n$

- Randomizing map defined by a distribution π over n-qubit Pauli operators

$$R(\rho) = \sum_s \pi_s P_s \rho P_s^*$$

- n-qubit Pauli operators:

$$P = P_1 \otimes P_2 \otimes \cdots \otimes P_n$$

where each $P_i \in \{ I, X, Y, Z \}$

Single qubit Pauli operators

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y = iXZ = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

- Form an orthogonal basis for matrices

  $(A,B) = Tr(B^*A)$

- Unitary, Hermitian, self-inverse

  $X^* = X, \quad X^2 = I,$ etc.

- X, Y, Z anti-commute: $XY = -YX$, etc.

Higher dimensions

- *n*-qubit Pauli ↔ 2*n*-bit strings

  $(a,b) \leftrightarrow i^{|a \cap b|} X^a Z^b$

  where $X^a = X^{a_1} \otimes X^{a_2} \otimes \ldots$, etc.

- Phase irrelevant
- Form an orthogonal basis for matrices
- Unitary, Hermitian, self-inverse

- Commutation

  $$(X^a Z^b)(X^u Z^v) = (-1)^{(a,b)\circ(u,v)} (X^u Z^v)(X^a Z^b)$$

  $(a,b)\circ(u,v) = a\cdot v + b\cdot u$ "symplectic inner product"

Randomizing map

- Randomizing map defined by a distribution π over *2n*-bit strings

$$R(\rho) = \sum_{(a,b)} \pi(a,b) \; X^a Z^b \rho Z^b X^a$$

- If π were uniform over all *2n*-bit strings, *R* would be perfectly randomizing

- More efficient maps are constructed from sparse, *pseudo-random* subsets of strings

- We will connect arbitrary approximately randomizing maps back to pseudo-random distributions

Connection to pseudo-randomness

- Randomizing map

  $R(\rho) = \sum_{(a,b)} \pi(a,b) \; X^a Z^b \rho Z^b X^a$

- Let V be the random variable over $2n$-bit strings corresponding to π

- Let M be an n by $2n$ boolean matrix, representing the n independent generators of a pure *stabilizer state*

- Proposition 1

  If R is ε-approximately randomizing,
  then $M \circ V$ is ε-close to uniform (in L_1 distance).

n-qubit Stabilizer states

- Stabilizer group G

  group generated by a set of commuting Pauli operators

- Stabilizer subspace
  - common +1 eigenspace of all operators in G
  - dimension = 2^{n-k} if G does not contain –I, and is generated by k independent generators

- Stabilizer state
  - pure state in 1-dimensional subspace stabilized by group G of order 2^n
  - G is generated by n independent commuting Paulis

Properties of Stabilizer states I

Let $|\psi\rangle$ be a stabilizer state, P any Pauli operator.
Then, $P|\psi\rangle$ is either parallel to $|\psi\rangle$ or perpendicular.

Proof: If P commutes with every stabilizer generator g, then

$$g\,P|\psi\rangle = P\,g|\psi\rangle = P|\psi\rangle$$

So $P|\psi\rangle$ lies in the stabilizer subspace. Since the subspace is one dimensional…

If not, then for some generator g

$$\langle\psi|P|\psi\rangle = \langle\psi|gP|\psi\rangle = -\langle\psi|Pg|\psi\rangle = -\langle\psi|P|\psi\rangle.$$

So $P|\psi\rangle$ is perpendicular to $|\psi\rangle$.

Properties II

- If $P \leftrightarrow (a,b)$,
  $P|\psi\rangle$ is parallel to $|\psi\rangle$ iff $M\circ(a,b) = 0^n$.

- Let $|\psi\rangle$ be a stabilizer state, P and Q any Pauli operators.
  Then, $P|\psi\rangle$ and $Q|\psi\rangle$ are either parallel or perpendicular.

- If $P \leftrightarrow (a,b)$, $Q \leftrightarrow (u,v)$, then
  $P|\psi\rangle$ and $Q|\psi\rangle$ are parallel iff $M\circ(a,b) = M\circ(u,v)$.

Properties III

- For an n-bit string s, let $|\psi_s\rangle = P|\psi\rangle$, for some P such that $M \circ (a,b) = s$.

- Since M has full rank, the states $|\psi_s\rangle$ form an orthonormal basis for n-qubit states

Proposition 1

$R(\rho) \quad = \quad \sum_{(a,b)} \pi(a,b) \quad X^a Z^b \rho Z^b X^a.$

V : random variable over $2n$-bit strings given by π.

M : n by $2n$ matrix representing a stabilizer state.

Then, if R is ε-approximately randomizing, then
$M \circ V$ is ε-close to uniform (in L_1 distance).

Proof: Consider state $|\psi\rangle$ generated by M.

Image under R = mixture of orthogonal states $|\psi_s\rangle$.

Trace distance from completely mixed = distance of the distribution over $s = M \circ V$.

Lower bound for key length

- Kind of randomizing map studied
- Connection to pseudo-randomness
- Lower bound for sample space of pseudo-random distribution

Lower bound for sample space

Given *V* : any random variable over $2n$-bit strings.

For any n by $2n$ boolean matrix M, rows orthogonal with respect to symplectic inner product, $M \circ V$ is ε-close to uniform (in L_1 distance).

Proposition 2

Sample space of V has size at least $\Omega(2^n/\varepsilon)$.

Implication:

Distribution π has support over the same number of Pauli operators

Proof sketch for Proposition 2

Consider *M* of the following form:

- The first $(n\text{–}m)$ rows are the same number of standard basis vectors for Z_2^{2n}.

- The next row is chosen so that it determines the parity of an arbitrary subset of $2m$ bits, different from the first $(n\text{–}m)$.

- The remaining rows are immaterial.

Proof sketch…

Pseudo-randomness condition on V implies

- The first $(n\text{–}m)$ bits of V are near uniform.

- (Informally) $2m$ bits of V are ε-biased, even conditioned on those first bits.

  (parity of every subset of bits is almost uniform)

- Let $m = \log(1/\varepsilon)$.

  Conditioned on any value of the first $(n\text{–}m)$ bits of V, the size of sample space is $\geq 2^{2m} = 2^m/\varepsilon$

- Net size of sample space $\geq 2^{n-m} \cdot 2^m/\varepsilon = 2^n/\varepsilon$.

Concluding remarks

- $\Omega(2^n/\varepsilon^2)$ unitary operators likely optimal
  Under investigation

- Explicit scheme takes time $\tilde{O}(n^2)$ with $\tilde{O}(n^4)$ preprocessing
  Faster encryption possible?

- Perfect encryption $\leftrightarrow$ Unitary orthogonal basis
  Characterization for approximate encryption?