COM-440, Introduction to Quantum Cryptography, Fall 2025

Security of Wiesner's scheme

1 An SDP formulation of simple counterfeiting attacks

We describe how the optimal success probability of a counterfeiting strategy may be represented by a semi-definite program.

1.1 A mathematical expression for the optimal counterfeiting strategy

Mathematically speaking, a simple counterfeiting attack is described by a quantum channel Φ with input from X, a 2-dimensional register containing the challenger's single-qubit money state, and output in $(\mathsf{Y}_1, \mathsf{Y}_2)$ two 2-dimensional registers that should contain the two copies. This channel takes a state $\rho \in \mathrm{D}(\mathcal{X})$ to a state $\Phi(\rho) \in \mathrm{D}(\mathcal{Y}_1 \otimes \mathcal{Y}_2)$, where $\mathrm{D}(\cdot)$ denotes the set of density matrices on some register.

In order to be physically realizable, at least in an idealized sense, the channel Φ must correspond to a completely positive and trace preserving linear mapping of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}_1 \otimes \mathcal{Y}_2)$. Conditioned on the bank having chosen the key k and prepared the money state $|\psi_k\rangle$, the probability of success for an attack described by Φ is given by $\langle \psi_k \otimes \psi_k | \Phi(|\psi_k\rangle\langle\psi_k|) | \psi_k \otimes \psi_k \rangle$. Averaging over the possible choices of k, the overall success probability of a counterfeiting attack is

$$\sum_{k=1}^{N} p_k \langle \psi_k \otimes \psi_k | \Phi(|\psi_k\rangle\langle\psi_k|) | \psi_k \otimes \psi_k \rangle. \tag{1.1}$$

The optimal success probability of a counterfeiting strategy is then the supremum of the probability (1.1), taken over all valid channels $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}_1 \otimes \mathcal{Y}_2)$.

1.2 Reformulation using the Choi-Jamiolkowski representation

Let us see how to model this as a semidefinite program. We first choose a standard basis $\{|1\rangle, \ldots, |d\rangle\}$, shared by the spaces $\mathcal{X}$, $\mathcal{Y}_1$, and $\mathcal{Y}_2$. With respect to this basis, the *Choi-Jamiołkowski representation* of a linear mapping $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}_1 \otimes \mathcal{Y}_2)$ is defined as

$$J(\Phi) = \sum_{1 \leq i,j \leq d} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j| \in \mathrm{L}(\mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{X}).$$

The operator $J(\Phi)$ uniquely determines Φ, and a well-known necessary and sufficient condition for $J(\Phi)$ to represent a valid channel (i.e., a completely positive and trace-preserving map) is that (i) $J(\Phi)$ is positive semidefinite, and (ii) $\mathrm{Tr}_{\mathcal{Y}_1 \otimes \mathcal{Y}_2}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}$. It is also easy to verify that

$$\langle \phi | \Phi(|\psi\rangle\langle\psi|) | \phi \rangle = \langle \phi \otimes \overline{\psi} | J(\Phi) | \phi \otimes \overline{\psi} \rangle$$

for any choice of vectors $|\psi\rangle \in \mathcal{X}$ and $|\phi\rangle \in \mathcal{Y}_1 \otimes \mathcal{Y}_2$, with complex conjugation taken with respect to the standard basis.

1.3 The semidefinite program

Combining the observations that have just been made with the expression (1.1), one finds that the optimal success probability of any simple counterfeiting strategy is given by the following semidefinite program:

Primal problem	Dual problem
maximize: $\mathrm{Tr}(QX)$	minimize: $\mathrm{Tr}(Y)$
subject to: $\mathrm{Tr}_{\mathcal{Y}_1\otimes\mathcal{Y}_2}(X) = \mathbb{1}_{\mathcal{X}}$	subject to: $\mathbb{1}_{\mathcal{Y}_1\otimes\mathcal{Y}_2}\otimes Y \geq Q$
$X \in \mathrm{Pos}\,\mathcal{Y}_1\otimes\mathcal{Y}_2\otimes\mathcal{X}$	$Y \in \mathrm{Herm}\,(\mathcal{X})$

where

$$Q = \sum_{k=1}^{N} p_k |\psi_k\otimes\psi_k\otimes\overline{\psi_k}\rangle\langle\psi_k\otimes\psi_k\otimes\overline{\psi_k}|.$$

The dual problem is obtained from the primal problem in a routine way, as described in the notes from last week. It may be verified that for this particular semidefinite program, the optimal values for the primal and dual problems are always equal, and are both achieved by feasible choices for X and Y.

1.4 Analysis of Wiesner's original scheme

We can now determine the optimal success probability of a counterfeiting attack against Wiesner's original scheme, by considering just the single-qubit scheme given by the ensemble $\mathcal{E} = \left\{\left(\frac{1}{4}, |0\rangle\right), \left(\frac{1}{4}, |1\rangle\right), f\left(\frac{1}{4}, |+\rangle\right), \left(\frac{1}{4}, |-\rangle\right)\right\}$. This ensemble yields the operator

$$Q = \frac{1}{4}\left(|000\rangle\langle 000| + |111\rangle\langle 111| + |+++\rangle\langle +++| + |---\rangle\langle ---|\right)$$

in the semidefinite programming formulation. We claim that the optimal value of the semidefinite program in this case is equal to 3/4. To show this we exhibit explicit primal and dual feasible solutions achieving the value $3/4$. For the primal problem the value 3/4 is obtained by the solution $X = J(\Phi)$ for Φ being the channel $\Phi(\rho) = A_0\rho A_0^* + A_1\rho A_1^*$, where

$$A_0 = \frac{1}{\sqrt{12}}\begin{pmatrix} 3 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad A_1 = \frac{1}{\sqrt{12}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 3 \end{pmatrix}.$$

For the dual problem, the value 3/4 is obtained by the solution $Y = \frac{3}{8}\mathbb{1}$, whose feasibility may be verified by computing $\|Q\| = 3/8$.