

Entanglement-Based Version of BB84

CSS codes protocol

1. Alice creates n random check bits, a random m -bit key k , and two random n -bit strings v and w . She encodes $|k\rangle$ in the code $\text{CSS}_{v,w}(C_1, C_2)$. She also encodes n qubits as $|0\rangle$ or $|1\rangle$ according to the check bits.
2. She randomly selects n positions out of $2n$ and puts the check qubits at these positions and the encoded qubits in the remaining positions.
3. Alice selects a random classical bit string $b = (b_1, b_2, \dots, b_{2n})$ of length $2n$. Whenever the bit b_i is 1, she applies a Hadamard transformation (2.28) to her half of the corresponding qubit pair.
4. She sends the other half of all qubit pairs to Bob.
5. Bob receives the qubits and publicly announces this fact.
6. Alice announces b, v and w and the positions of the check qubits.
7. Bob applies a Hadamard transformation to those qubits for which $b_i = 1$.
8. Bob measures the n check qubits in the computational basis $\{|0\rangle, |1\rangle\}$ to estimate the error rate. If more than t errors occur, they abort the protocol.
9. If the number of errors is below t , Bob decodes the remaining n qubits from $\text{CSS}_{v,w}(C_1, C_2)$.
10. Bob measures his qubits to obtain the shared secret key k .

The Calderbank–Shor–Steane (CSS) code is now defined as follows: Suppose we have two classical linear error correction codes, an $[n, k_1]$ code C_1 and an $[n, k_2]$ code C_2 such that $C_2 \subset C_1$ and C_1 and C_2^\perp both correct up to t errors. Using these two classical codes we can define a quantum error correction code, the *CSS code of C_1 over C_2* , denoted $\text{CSS}(C_1, C_2)$. It is an $[n, k_1 - k_2]$ quantum code that is capable of correcting errors on up to t qubits. The construction works as follows: for any codeword $x \in C_1$, we define the quantum state

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle, \quad (\text{B.6})$$

where $+$ is the bitwise addition modulo 2 and $|C_2|$ denotes the cardinality of C_2 (which is 2^{k_2} , since this is the number of codewords of C_2).

hence, $|x + C_2\rangle$ and $|x' + C_2\rangle$ are orthonormal states. The quantum code $\text{CSS}(C_1, C_2)$ is defined to be the vector space spanned by $\{|x + C_2\rangle\}_{x \in C_1}$. Since the number of cosets of C_2 in C_1 is $|C_1|/|C_2|$, the dimension of this vector space is $|C_1|/|C_2| = 2^{k_1 - k_2}$, and therefore $\text{CSS}(C_1, C_2)$ is an $[n, k_1 - k_2]$ quantum code.

Equivalent Prepare-And-Measure version of BB84

Secure BB84

1. Alice creates $4n$ random bits.
2. Alice encodes each of the bits either in the computational or in the Hadamard basis according to another random $4n$ -bit string b .
3. Alice sends the resulting qubits to Bob.
4. Alice chooses a random $x_k \in C_1$.
5. Bob receives the qubits, publicly announces this fact, and measures each of the qubits either in the computational or in the Hadamard basis, chosen at random.
6. Alice announces b .
7. Alice and Bob discard those bits where they have used different bases. After this step, there are about $2n$ bits left. Alice randomly chooses n of these bits to serve as check bits and tells Bob the position of these bits.
8. Alice and Bob publicly compare the check bits. If they find more than t errors, they abort the protocol. Otherwise, they continue and Alice is left with the n -bit string x , and Bob with n -bit string $x + e$.
9. Alice announces $x - x_k$. Bob subtracts this from his string and corrects it with the code C_1 to obtain x_k .
10. Alice and Bob compute the coset to which x_k belongs in order to obtain the final key k .

Brouwer-Zimmerman Algorithm for finding the Minimum Distance of a given Linear Code $[n, k]$ given its Generator Matrix:

1.8.2 **Algorithm** Compute the minimum distance of a given linear (n, k) -code C .

Input: A systematic generator matrix $\Gamma_1 = (I_k \mid A_1)$ of C .

Output: The minimum distance $\text{dist}(C)$.

- (1) $m := 2$
- (2) $k_1 := k$
- (3) **repeat**
- (4) Apply Gaussian elimination and possibly permutations of the columns to the matrix A_{m-1} from $\Gamma_{m-1} = \left(A'_{m-1} \mid \begin{array}{c|c} I_{k_{m-1}} & A_{m-1} \\ \hline 0 & 0 \end{array} \right)$ to obtain a generator matrix $\Gamma_m = \left(A'_m \mid \begin{array}{c|c} I_{k_m} & A_m \\ \hline 0 & 0 \end{array} \right)$
- (5) **until** $\text{rank}(A_m) = 0$
- (6) $C_0 := \{0\}$
- (7) $i := 0$
- (8) **repeat**
- (9) $i := i + 1$
- (10) $C_i := C_{i-1} \cup \bigcup_{j=1}^m \{v \cdot \Gamma_j \mid v \in \mathbb{F}(q)^k, \text{wt}(v) = i\}$
- (11) $\overline{d}_i := \min\{\text{wt}(c) \mid c \in C_i, c \neq 0\}$
- (12) $\underline{d}_i := \sum_{\substack{j=1 \\ k-k_j \leq i}}^m (i+1) - (k - k_j)$
- (13) **until** $\overline{d}_i \leq \underline{d}_i$
- (14) **return** \overline{d}_i

□

Problem in the construction of the quantum code $CSS(C1, C2)$:

Let $k_2 < k_1$.

We can now try to construct a quantum code $CSS(C1, C2)$ as follows:

- 1) Start with an appropriate $k_1 \times n$ Generator matrix G_1
- 2) From G_1 , construct the linear code $C_1 = [n, k_1]$
- 3) Use the Brouwer-Zimmermann algorithm to find the minimum distance d_1 of C_1
- 4) From G_1 obtain an appropriate $k_2 \times n$ Generator matrix G_2
- 5) From G_2 , construct the linear code $C_2 = [n, k_2]$ such that C_2 is contained in C_1
- 6) From C_2 , construct its dual code C_2^\perp
- 7) Use the Brouwer-Zimmermann algorithm to find the minimum distance d_2 of C_2^\perp

Statement of the Problem:

How do we choose G_2 from G_1 such that $d_2 = d_1$ as required for the $CSS(C_1, C_2)$ code?