(1) Alice zvolí $(4+\delta)n$ posloupnost uniformně náhodných informačních bitů $a = (a_i)$ a $(4+\delta)n$ posloupnost instrukčních bitů $b = (b_i)$.
(2) Alice zakóduje a_i pomocí stavů $|0\rangle$ a $|1\rangle$, je-li $b_i = 0$, a pomocí $|+\rangle$ stavů $|-\rangle$, je-li $b_i = 1$, a pošle je Bobovi.
(3) Bob zvolí $(4+\delta)n$ posloupnost uniformně náhodných dekódovacích bitů $c = (c_i)$ a změří přijaté kubity v bázi $\{|0\rangle, |1\rangle\}$, je-li $c_i = 0$, a v bázi $\{|+\rangle, |-\rangle\}$, je-li $c_i = 1$.
(4) Bob poté zveřejní posloupnost c a Alice zveřejní posloupnost b.
(5) Alice a Bob zvolí $2n$ indexů, pro které $b_i = c_i$, a pro které by tedy hodnota naměřená Bobem měla být a_i. Takových indexů existuje dostatečně mnoho s velkou pravděpodobností kontrolovanou číslem δ.
(6) Uniformně náhodně poté Alice a Bob zvolí polovinu těchto indexů, na kterých veřejně ověří, zda rovnost opravdu platí. Tím získají představu o míře porušení, kterou je možné očekávat u zbylých bitů.
(7) Je-li očekávaná míra porušení přijatelná, použijí zbylé bity jako sdílený klíč (porušené bity opraví pomocí mechanismu samoopravného kódu).

Princip bezpečnosti protokolu ilustrujme na nejjednodušším útoku, při kterém útočník změří k jednotlivých kubitů v jedné z bazí $|0\rangle, |1\rangle$ nebo $|+\rangle, |-\rangle$. Volbu báze útočníka na daném kubitu označme e_i.

- Je-li napaden i-tý bit, zná útočník hodnotu bitu a_i z klíče, pokud $b_i = c_i = e_i$ a i nebylo vybráno ke kontrole. To je tedy v průměru v $k/8$ případech.
- Napadení i-tého bitu je naopak prozrazeno, pokud $b_i = c_i \neq e_i$, i bylo vybráno ke kontrole a kontrola odhalí nesrovnalost. Uvědomme si, že bit změření útočníkem v chybné bázi je v jedno z bázových stavů této chybné báze, a výsledkem měření ve správné bázi je tedy uniformně náhodný bit. Nesrovnalost je tedy odhalena průměrně v $k/16$ případech.

Pokud tedy test poruchy odhalí t chyb, lze očekávat, že útočník zná zhruba $2t$ bitů. Význam slova „zhruba“ odpovídá centrální limitní větě, resp. Chernoffovu odhadu.

Základním nedostatkem naší analýzy je předpoklad o podobě útoku. Je úkolem kvantové teorie informace získat horní odhad na množství informace získatelné jakýmkoli útokem v závislosti na pravděpodobnosti odhalení.