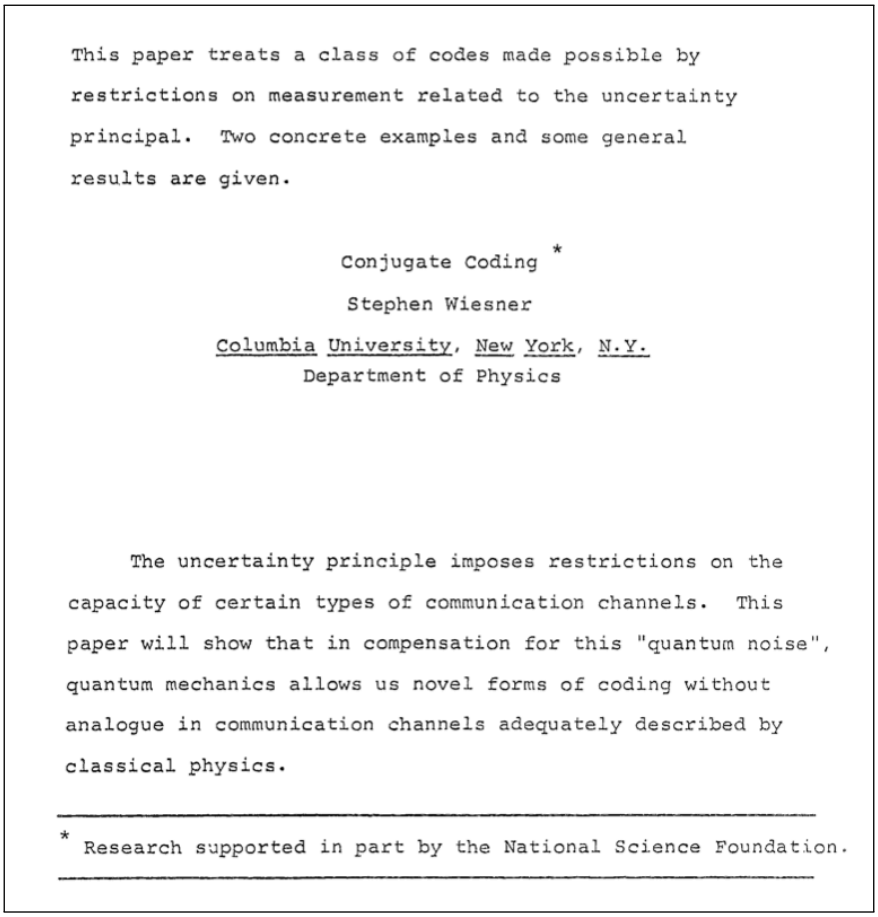
כסף קוונטי

1 קצת היסטוריה

הרעיון של כסף קוונטי הוצע על ידי סטיבן ויזנר, Stephen Wiesner, בסוף שנות השישים או בתחילת שנות השבעים. ויזנר וצ'רלס בנט הכירו בלימודיהם לתואר הראשון בברנדייס, ושמרו על קשר גם כשעברו ללימודים מתקדמים באוניברסיטאות שונות. באחת מפגישותיהם סיפר ויזנר לבנט על הרעיון: להשתמש בתורת הקוונטים כדי ליצור שטרות שקשה לזייף. המאמר לא התקבל לפרסום בתחילה, ובמשך שנים הרעיון כמעט שלא זכה לתשומת לב.



This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

Conjugate Coding *

Stephen Wiesner

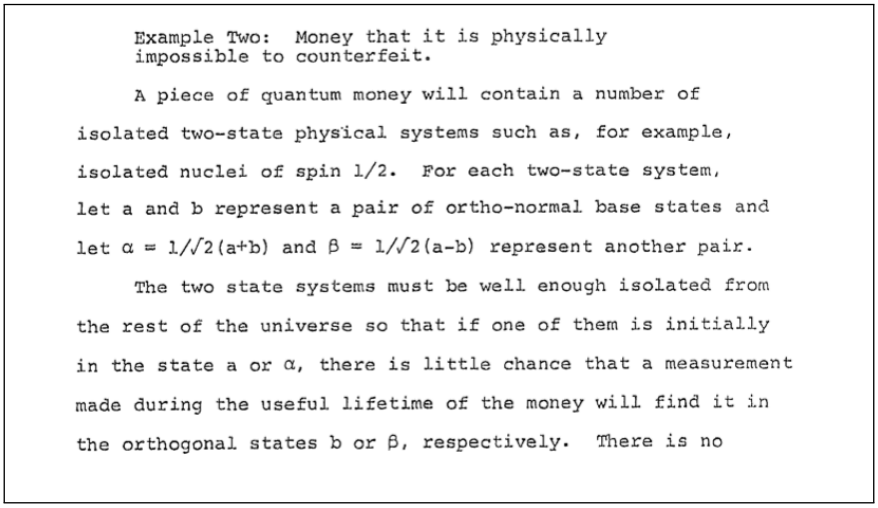
Columbia University, New York, N.Y.
Department of Physics

The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

* Research supported in part by the National Science Foundation.

בשנת 1979 נפגשו בנט וז'יל ברסאר, Gilles Brassard, בזמן כנס FOCS בפוארטו ריקו. ליתר דיוק, ברסאר שחה בים כשבנט, שאותו לא הכיר אז אישית, ניגש אליו וסיפר לו על השטרות הקוונטיים של ויזנר. ברסאר תיאר

זאת לימים כאחד הרגעים המוזרים והקסומים בחייו המקצועיים. השיחה הזו הובילה לשיתוף פעולה ולרעיונות יסוד בקריפטוגרפיה קוונטית. מאמרו המקורי של ויזנר, שכותרתו Conjugate Coding, פורסם לבסוף בשנת 1983.



Example Two: Money that it is physically impossible to counterfeit.

A piece of quantum money will contain a number of isolated two-state physical systems such as, for example, isolated nuclei of spin 1/2. For each two-state system, let a and b represent a pair of ortho-normal base states and let $\alpha = 1/\sqrt{2}(a+b)$ and $\beta = 1/\sqrt{2}(a-b)$ represent another pair.

The two state systems must be well enough isolated from the rest of the universe so that if one of them is initially in the state a or α, there is little chance that a measurement made during the useful lifetime of the money will find it in the orthogonal states b or β, respectively. There is no

2 מהו כסף קוונטי?

הרעיון הוא לצרף לשטר מצב קוונטי, לצד מידע קלאסי כמו מספר סידורי. את המידע הקלאסי אפשר להעתיק, אבל את המצב הקוונטי הלא־ידוע אי אפשר לשכפל באופן מושלם. כך אפשר לקוות לבסס את ההגנה מפני זיוף על חוקי הפיזיקה, ולא רק על הקושי לייצר נייר, דיו או סימנים מיוחדים.

עם זאת, משפט אי־השכפול לבדו אינו הוכחת ביטחון. זייפן אינו חייב ליצור עותקים מושלמים: די שייצר שני שטרות שיעברו את בדיקת הבנק. בנוסף, צריך להגדיר אילו פעולות מותר לו לבצע מול הבנק. כפי שנראה, לפרט האחרון יש השפעה מכרעת על הביטחון.

2.1 הסכמה של ויזנר

לסכמה יש פרמטר ביטחון n. כדי להנפיק שטר, הבנק בוחר מספר סידורי $s \in \{0,1\}^n$ שטרם הונפק, וכן מחרוזת סודית אחידה

$$q = (q_1, \ldots, q_n) \in \{0, 1, +, -\}^n.$$

הסימנים במחרוזת מתארים את ארבעת המצבים המוכרים לנו. הבנק מכין את המצב

$$|\psi_q\rangle = |q_1\rangle \otimes |q_2\rangle \otimes \cdots \otimes |q_n\rangle ,$$

ומוסר את השטר

$$\text{note} = (s, |\psi_q\rangle).$$

ברשומות הבנק נשמר הזוג (s,q). המספר הסידורי גלוי, אבל המחרוזת q נשארת סודית.

כדי לבדוק שטר, הבנק מחפש את המספר הסידורי ברשומותיו. אם הוא אינו מופיע, הבנק פוסל את השטר. אחרת, לכל $i \in \{1,\dots,n\}$, הוא מודד את הקיוביט המתאים בבסיס שנקבע על ידי q_i: בבסיס החישובי אם $q_i \in \{0,1\}$, ובבסיס $\{|+\rangle, |-\rangle\}$ אם $q_i \in \{+,-\}$. הבנק מאשר את השטר רק אם בכל הקואורדינטות התקבלה התוצאה הצפויה. נבחין כי שטר חוקי עובר את הבדיקה בהסתברות 1, והמצב שלו אינו משתנה.

3 ניסיונות זיוף ללא גישה לבנק

3.1 לנחש את המחרוזת הסודית

נניח שאנחנו מכירים מספר סידורי חוקי, ובוחרים באקראי מחרוזת $\tilde{q} \in \{0,1,+,-\}^n$. ההסתברות לנחש בדיוק את q היא 4^{-n}. אבל זו אינה ההסתברות שהשטר שהכנו יעבור את הבדיקה: גם מצב שונה מהמצב הנכון עשוי להתקבל.

בקואורדינטה אחת, בהסתברות $1/4$ ניחשנו את המצב הנכון, בהסתברות $1/4$ ניחשנו את המצב האורתוגונלי לו, ובהסתברות $1/2$ בחרנו מצב מהבסיס האחר. לכן הסתברות הקבלה היא

$$\frac{1}{4}\cdot 1 + \frac{1}{4}\cdot 0 + \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{2}.$$

מאי־התלות בין הקואורדינטות, השטר כולו מתקבל בהסתברות 2^{-n}. גם זו הסתברות זעירה כאשר n גדול, אבל חשוב להבחין בין ניחוש התיאור הסודי לבין מעבר של בדיקה קוונטית.

3.2 משטר אחד לשני שטרות

נגדיר כעת את משחק הזיוף שבו נתמקד. הזייפן מקבל שטר חוקי אחד $(s, |\psi_q\rangle)$, ומנסה להפיק שני שטרות הנושאים את אותו מספר סידורי. הוא מנצח אם **שניהם** עוברים את בדיקת הבנק. מותר לו לבצע כל פעולה קוונטית, ואף ליצור שזירה בין שני השטרות. בשלב זה אין לו גישה לבדיקות ביניים של הבנק. ההסתברות נלקחת על בחירת השטר, על האקראיות של הזייפן ועל תוצאות המדידות.

נתחיל מהתקפה פשוטה. נמדוד את כל הקיוביטים בבסיס החישובי, ונקבל מחרוזת $r \in \{0,1\}^n$. נכין שני שטרות שבכל אחד מהם המצב

$$|r\rangle = |r_1\rangle \otimes \cdots \otimes |r_n\rangle .$$

אם $q_i \in \{0,1\}$, אז $r_i = q_i$, ושני השטרות עוברים את הבדיקה בקואורדינטה הזו בוודאות. אם $q_i \in \{+,-\}$, כל אחד משני העותקים של $|r_i\rangle$ עובר את הבדיקה בהסתברות $1/2$. שני העותקים הוכנו במצב מכפלה, ולכן ההסתברות ששניהם יעברו היא $1/4$. בסך הכול, בקואורדינטה אחת נקבל

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{4} = \frac{5}{8},$$

ולכן הסתברות הניצחון בהתקפה הזו היא

$$\left(\frac{5}{8}\right)^n.$$

אפשר לעשות טוב יותר. הסתברות הניצחון האופטימלית במשחק הזיוף שהגדרנו היא

$$\left(\frac{3}{4}\right)^n.$$

זהו חסם על כל התקפה קוונטית, גם כזו שפועלת במשותף על כל הקיוביטים, וקיימת התקפה שמשיגה אותו. לא נוכיח כאן את התוצאה; היא הוכחה על ידי Molina, Vidick and Watrous. החסם הזה תלוי במודל: הוא אינו מתיר לזייפן לפנות לבנק במהלך ההתקפה.

4 מה בדיוק הבנק מחזיר?

כשמתחילים לחשוב על שימוש בשטרות, עולות שאלות נוספות. האם צריך לפנות לבנק כדי לבדוק כל תשלום? מה עושים עם שטר שאושר? ומה עושים עם שטר שנפסל? האם מחזירים אותו, מחרימים אותו, או מחליפים אותו בשטר חדש?

בסכמה שתיארנו רק הבנק יודע לבדוק שטרות, משום שרק הוא מחזיק במידע הסודי. זהו כסף קוונטי עם מפתח פרטי. כסף קוונטי שאפשר לאמת באופן פומבי הוא נושא אחר, שלא נעסוק בו כאן. נתמקד בשאלה שנראית תחילה כמו פרט מנהלי: מה הבנק עושה בשטר לאחר הבדיקה?

4.1 לא כדאי להחזיר שטר שנפסל

נניח שהבנק מודד את כל הקיוביטים בבסיסים הסודיים, ומחזיר את השטר גם אם הוא נפסל. נראה כיצד לנצל זאת כדי ללמוד את q.

נתחיל משטר חוקי, וננסה ללמוד קואורדינטה אחת, q_i. נחליף רק את הקיוביט הזה במצב מועמד $|t\rangle$, כאשר $t \in \{0,1,+,-\}$, ונשלח את השטר לבדיקה. שאר הקיוביטים נשארים חוקיים, ולכן ההכרעה תלויה רק בקואורדינטה ששינינו. אם $t = q_i$, הבנק מאשר בוודאות. אם המצב המועמד אורתוגונלי למצב הנכון, הוא פוסל בוודאות. אם הם שייכים לבסיסים שונים, הוא מאשר בהסתברות $1/2$.

נבדוק כל מועמד עד שנקבל דחייה, או עד שיעבור c בדיקות רצופות. **לפני כל בדיקה מכינים מחדש את המצב המועמד בקוורדינטה הזו.** אחרת, אישור ראשון כבר היה משחזר את הקיוביט הנכון, והבדיקות הבאות לא היו בודקות עוד את הניחוש שלנו. גם אחרי דחייה אפשר להמשיך, משום שהבנק מחזיר את השטר ושאר הקיוביטים לא השתנו.

המועמד הנכון עובר תמיד. לכל אחד משני המועמדים מהבסיס האחר יש הסתברות 2^{-c} לעבור את כל הבדיקות, והמועמד האורתוגונלי נפסל מיד. לכן ההסתברות שנזהה לא נכון קוורדינטה כלשהי חסומה על ידי

$$2n\,2^{-c}.$$

אחרי שזיהינו קוורדינטה, נתקן אותה ונעבור לבאה. לכל $0 < \delta < 1$, בחירה של

$$c = \left\lceil \log_2\left(\frac{2n}{\delta}\right) \right\rceil$$

נותנת הסתברות הצלחה לפחות $1-\delta$, תוך לכל היותר $4nc = O(n\log(n/\delta))$ פניות לבנק. כאן חסם האיחוד מתייחס לשגיאה הראשונה בתהליך; כל עוד לא טעינו, שאר השטר נשאר חוקי.

4.2 גם החזרת שטר שאושר עלולה להספיק

נניח כעת שהבנק מחרים כל שטר שנפסל, אבל מחזיר את אותו שטר כשהוא מאושר. ההתקפה הקודמת מסוכנת מדי: ניסיון לא מוצלח אחד גומר לנו את השטר. ובכל זאת, אפשר ללמוד את המחרוזת הסודית בהסתברות גבוהה.

הרעיון מזכיר את ניסוי הפצצה של אליצור--ויידמן: במקום להפריע לשטר בבת אחת, נבצע הרבה הפרעות קטנות, ובין הפרעה להפרעה ניתן לבנק לבדוק אותו. האישור של הבנק מחזיר את השטר למצב החוקי, בעוד שמידע על המצב מצטבר בקיוביט עזר שנשאר אצלנו. זו התקפה אדפטיבית, המבוססת על תוצאות בדיקות קודמות. נעבור לנתח את המקרה הזה ב-סעיף 5.

5 התקפה בעזרת סיבובים קטנים

5.1 בדיקה אם קיוביט מסוים נמצא במצב פלוס

נתמקד בקוורדינטה i, ונכתוב $|\phi\rangle = |q_i\rangle$. נרצה לבדוק אם $|\phi\rangle = |+\rangle$. נכין קיוביט עזר במצב $|0\rangle$. נבחר מספר **זוגי** c, ונגדיר

$$\theta = \frac{\pi}{2c}, \qquad R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

נחזור על שלושת הצעדים הבאים c פעמים:

1. נפעיל את הסיבוב R_θ על קיוביט העזר.

2. נפעיל CNOT, כאשר קיוביט העזר הוא הבקרה והקיוביט שבשטר הוא המטרה.

3. נשלח את השטר לבנק, ונשמור אצלנו את קיוביט העזר. אם השטר נפסל, ההתקפה נכשלת. אם הוא אושר, נקבל אותו בחזרה ונמשיך לסיבוב הבא.

לבסוף נמדוד את קיוביט העזר בבסיס החישובי.

5.2 המקרה שבו המצב הוא פלוס

נשים לב כי כשהקיוביט הראשון הוא הבקרה והשני הוא המטרה:

$$\mathrm{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$$

על כן $X|+\rangle = |+\rangle$, ולכן השער המבוקר אינו משנה את קיוביט המטרה ואינו יוצר שזירה. לכל מצב של קיוביט העזר מתקיים

$$\mathsf{CNOT}((\alpha|0\rangle + \beta|1\rangle) \otimes |+\rangle) = (\alpha|0\rangle + \beta|1\rangle) \otimes |+\rangle .$$

לכן השטר מאושר בכל סיבוב, וקיוביט העזר רק צובר סיבובים:

$$R_\theta^c|0\rangle = R_{\pi/2}|0\rangle = |1\rangle .$$

התוצאה הסופית היא 1 בוודאות, והשטר נשאר חוקי.

5.3 המקרים שבהם המצב הוא אפס או אחת

נניח תחילה ש־ $|\phi\rangle = |0\rangle$. אם קיוביט העזר מתחיל את הסיבוב במצב אפס, אחרי הסיבוב והשער המבוקר נקבל

$$\cos\theta\ |0\rangle \otimes |0\rangle + \sin\theta\ |1\rangle \otimes |1\rangle .$$

הבנק מצפה לאפס בקיוביט שבשטר. הוא מאשר בהסתברות $\cos^2\theta$, ובהתניה באישור, המצב המשותף חוזר להיות $|0\rangle \otimes |0\rangle$. לכן אפשר לחזור על אותו ניתוח בכל סיבוב.

אם $|\phi\rangle = |1\rangle$, המצב אחרי הסיבוב והשער המבוקר הוא

$$\cos\theta\ |0\rangle \otimes |1\rangle + \sin\theta\ |1\rangle \otimes |0\rangle ,$$

ומתקבל אותו ניתוח בדיוק. בשני המקרים, ההסתברות שכל הבדיקות יאושרו היא

$$\cos^{2c}\theta.$$

בהתניה בכך, קיוביט העזר מסיים במצב אפס. הסיכון שהשטר ייפסל חסום על ידי

$$1-\cos^{2c}\theta = 1-(1-\sin^2\theta)^c \le c\sin^2\theta \le c\theta^2 = \frac{\pi^2}{4c}.$$

ככל שנבחר יותר סיבובים קטנים, הסיכון יקטן.

5.4 המקרה שבו המצב הוא מינוס

זהו המקרה שדורש קצת תשומת לב. מכיוון ש־ $X|-\rangle = -|-\rangle$, השער המבוקר מפעיל למעשה את Z על קיוביט העזר:

$$\mathsf{CNOT}((\alpha|0\rangle+\beta|1\rangle)\otimes|-\rangle) = (\alpha|0\rangle-\beta|1\rangle)\otimes|-\rangle\,.$$

השטר נשאר חוקי ומאושר תמיד, אבל קיוביט העזר עובר בכל סיבוב את הפעולה ZR_θ.

למה 5.1. *עבור המטריצות*

$$R_\theta = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}, \qquad Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

מתקיים

$$ZR_\theta Z = R_{-\theta}.$$

בפרט,

$$(ZR_\theta)^2 = I.$$

הוכחה. כפל ב־ Z מימין מחליף את סימן העמודה השנייה, וכפל ב־ Z משמאל מחליף את סימן השורה השנייה. לכן

$$\begin{aligned} ZR_\theta Z &= \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}\\ &= \begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix} = R_{-\theta}. \end{aligned}$$

מכאן

$$(ZR_\theta)^2 = (ZR_\theta Z)R_\theta = R_{-\theta}R_\theta = I.$$

אפשר להבין את הזהות גם גאומטרית: במישור הממשי, Z הוא שיקוף ביחס לציר האופקי. שיקוף, סיבוב בזווית θ, ושיקוף בחזרה הופכים את כיוון הסיבוב, ולכן מתקבל סיבוב בזווית $-\theta$. □

נחזור לניתוח שלנו. מכיוון שבחרנו את c זוגי, הפעולה הכוללת על קיוביט העזר היא

$$(ZR_\theta)^c = I,$$

ולכן הוא חוזר למצבו ההתחלתי, $|0\rangle$.

לסיכום, קיבלנו בדיקה שתוצאתה 1 אם המצב הוא פלוס, ו־ 0 בכל אחד משלושת המצבים האחרים, בתנאי שהשטר לא נפסל בדרך. הסתברות הפסילה בכל אחת מארבע האפשרויות היא לכל היותר $\pi^2/(4c)$. בהתניה בהשלמת הבדיקה, התשובה נכונה והשטר חוקי.

5.5 ללמוד את כל המחרוזת

כדי לבדוק אם הקיוביט נמצא במצב אחר, נשנה זמנית את הבסיס כך שהמצב המועמד יהפוך לפלוס. אפשר לבחור את האופרטורים הבאים:

$$V_+ = I, \qquad V_- = Z, \qquad V_0 = H, \qquad V_1 = ZH.$$

לכל מועמד t מתקיים $V_t|t\rangle = |+\rangle$, והאופרטור מעביר את ארבעת מצבי הסכמה לאותם ארבעה מצבים, עד כדי פאזה כוללת.

בכל סיבוב נפעיל על הקיוביט שבשטר את V_t, נפעיל את השער המבוקר, ואז נבטל את שינוי הבסיס באמצעות $V_t^\dagger$ **לפני** שנשלח את השטר לבנק. כך הבנק עדיין בודק את המצב המקורי שלו. השער המבוקר שהפעלנו שקול לשער עם אופרטור מטרה $V_t^\dagger X V_t$, ולכן כל הניתוח הקודם חל באותה צורה.

נבדוק את המועמדים $+, -, 0$ לפי הסדר. אם אחת הבדיקות מחזירה 1, זיהינו את המצב. אם שלושתן מחזירות 0, המצב הוא $|1\rangle$. נאתחל מחדש את קיוביט העזר לפני כל בדיקה. נחזור על כך בכל n הקואורדינטות, כל עוד השטר לא נפסל.

יש לכל היותר $3n$ בדיקות, ולכן ההסתברות שהבנק יפסול את השטר בשלב כלשהו חסומה על ידי

$$\frac{3\pi^2 n}{4c}.$$

חסם האיחוד תקף גם כאן: לאחר כל היסטוריה של אישורים, השטר חוזר להיות חוקי והחסם על הבדיקה הבאה נשאר תקף. כדי להצליח בהסתברות לפחות $1-\delta$, נבחר את המספר הזוגי הקטן ביותר המקיים

$$c \geq \frac{3\pi^2 n}{4\delta}.$$

מספר הפניות לבנק הוא לכל היותר

$$3nc = O\left(\frac{n^2}{\delta}\right).$$

בסיום מוצלח למדנו את כל q ועדיין נשארנו עם שטר חוקי. כעת אפשר להכין כמה עותקים שרוצים.

6 מה למדנו על המודל?

אין כאן סתירה למשפט אי־השכפול או לחסם הזיוף שהזכרנו. הזייפן קיבל משאב נוסף: גישה חוזרת לבדיקת הבנק, המבוססת על מידע סודי שאינו ברשותו. הבדיקות מחזירות את השטר למצב החוקי, ומאפשרות לו לצבור מידע בלי להסתכן יותר מדי בכל צעד.

לכן לא מספיק לומר שהשטרות הם קוונטיים ושאי אפשר לשכפל מצב לא־ידוע. צריך להגדיר גם כיצד משתמשים בשטרות וכיצד מאמתים אותם. דרך לחסום את ההתקפות שתיארנו היא להחרים שטר שנפסל, ולהחליף שטר שאושר בשטר חדש בעל מספר סידורי ומחרוזת סודית חדשים, תוך ביטול המספר הסידורי הישן. כך אי אפשר לחזור שוב ושוב אל אותה בדיקה סודית. זו חסימה של ההתקפות המסוימות שהצגנו; הוכחת ביטחון מלאה דורשת להגדיר ולנתח את כל מודל השימוש.