
REWOLUCJA STANU
FANTASTYCZNE WPROWADZENIE DO INFORMATYKI KWANTOWEJ
ALICE
pomysł: Piotr Gawron, scenariusz: Michał Cholewa, rysunki: Katarzyna Kara


ALICE

Piotr Gawron, Michał Cholewa, Katarzyna Kara
Rewolucja stanu – fantastyczne wprowadzenie do informatyki kwantowej

Autor części naukowej: *Piotr Gawron*

Autor scenariusza: *Michał Cholewa*

Rysunki: *Katarzyna Kara*

Projekt okładki: *Katarzyna Kara*

Redakcja i korekta: *Anna Askaldowicz*

Skład: *Piotr Gawron* z wykorzystaniem systemu LaTeX

Przygotowanie do druku: *Natalia Kara*

W części drugiej książki wykorzystano rysunki i kod źródłowy pochodzący z poniższych źródeł:
`https://openclipart.org/detail/15831/stylized-atom`
`https://openclipart.org/detail/1953/minimalist-monitor-and-computer`
`http://www.texample.net/tikz/examples/angles-quotes/`
`http://qutip.org/`

Publikacja finansowana ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Publikacja zrealizowana przy wsparciu Fundacji na rzecz Nauki Polskiej w ramach projektu SKILLS w trzeciej edycji konkursu eNgage 2015

ISBN: 978-83-926054-1-6

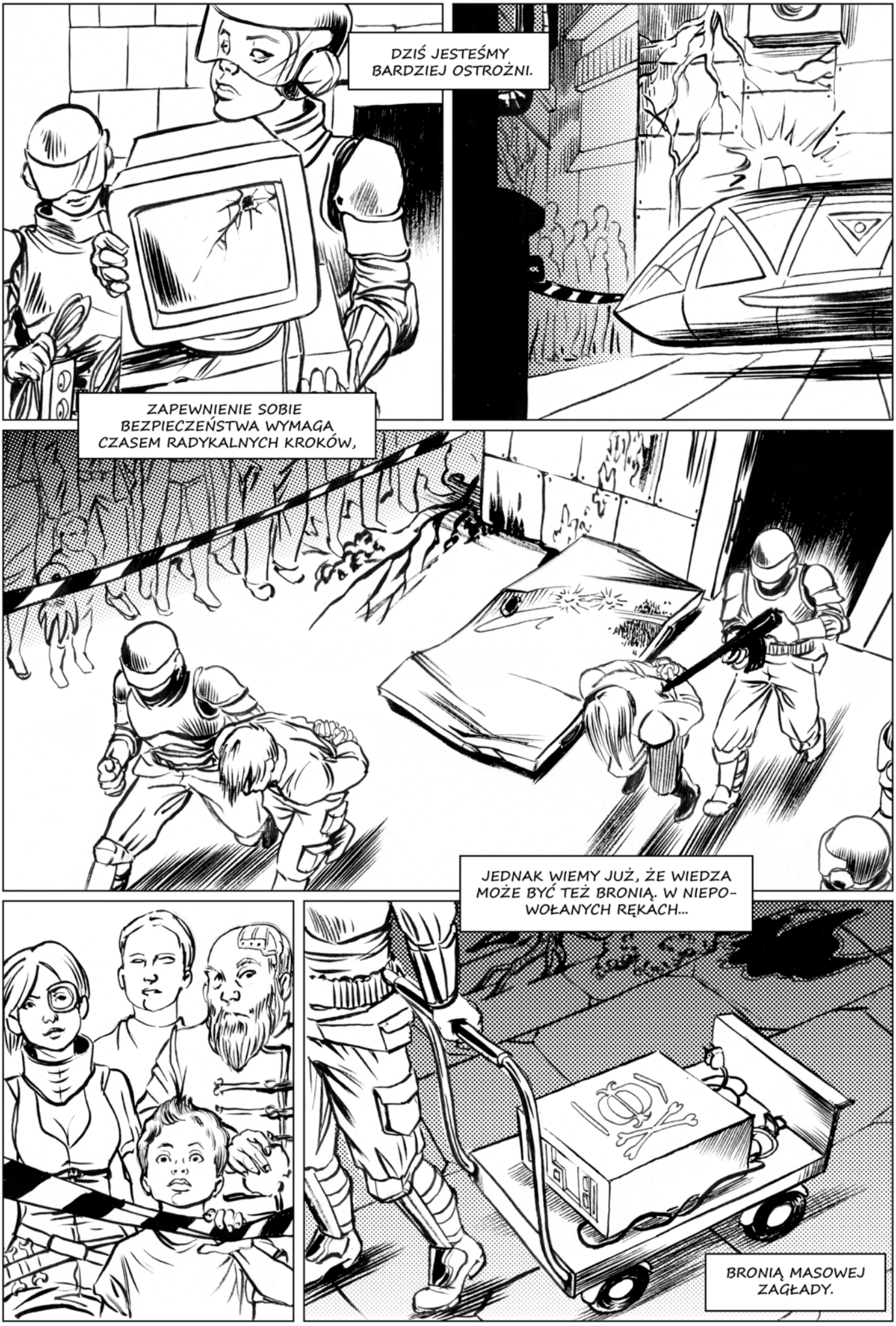
Spis treści

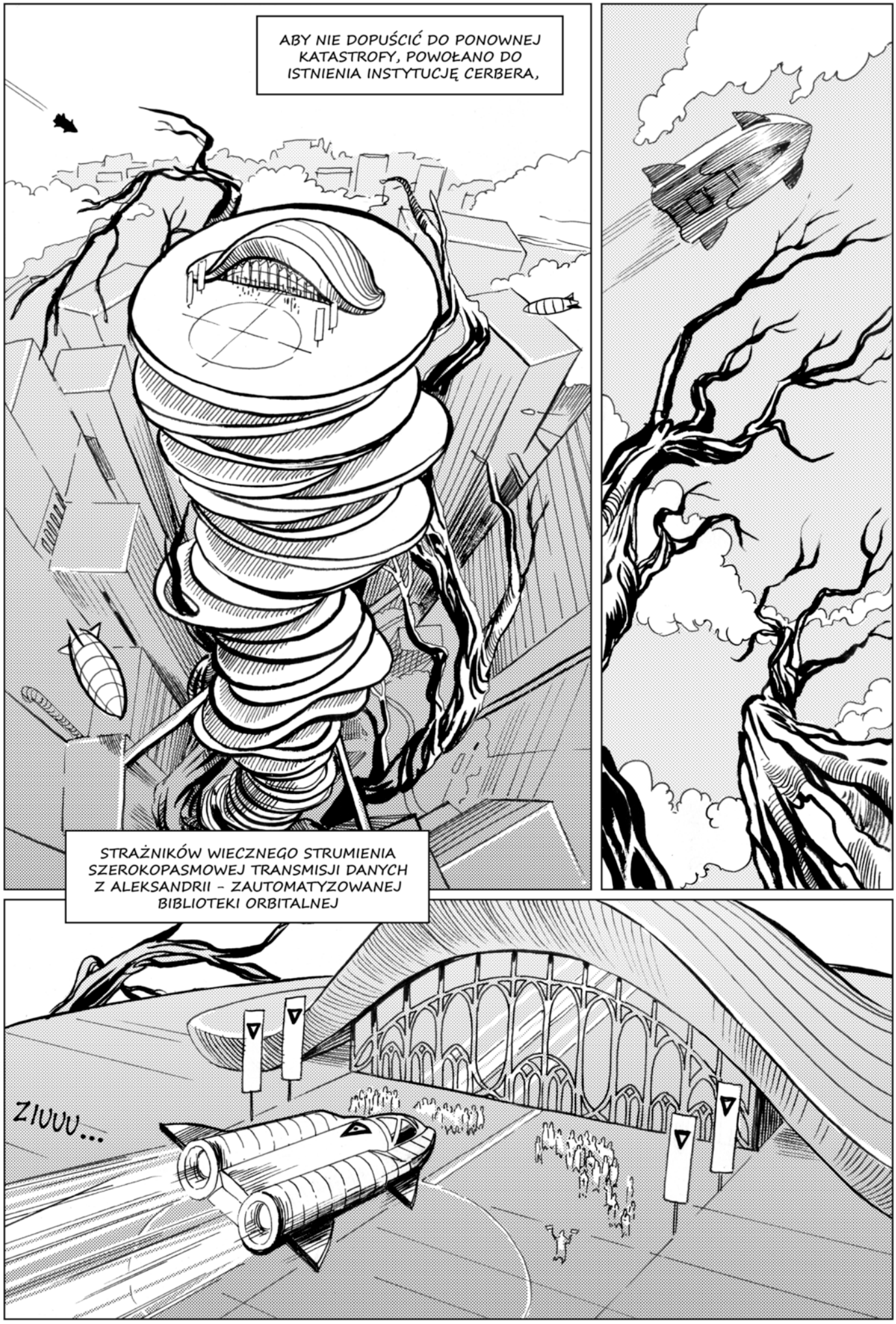
Część I

Fantastyczne wprowadzenie


PODOBNO KIEDYŚ ŚWIAT BYŁ INNY.
ODWRÓCILIŚMY SIĘ OD NATURY, NIE INTERESOWAŁ NAS HARMONIJNY ROZWÓJ.
ZIUUU...


STWORZYLIŚMY SPOŁECZEŃSTWO INFORMACYJNE POZBAWIONE JAKIEJKOLWIEK KONTROLI.
DOSTĘP DO CAŁEJ ZNANEJ NAM WIEDZY MIELI WSZYSCY – PRZYWÓDCY, NAUKOWCY, ARTYŚCI...
... GŁUPCY, TERRORYŚCI I ZBRODNIARZE.
CI OSTATNI DOPROWADZILI NAS DO UPADKU – I ŚMIERCI MILIARDÓW.
NEW
FLYSUIT
ALICE


DZIŚ JESTEŚMY BARDZIEJ OSTROŻNI.
ZAPEWNIENIE SOBIE BEZPIECZEŃSTWA WYMAGA CZASEM RADYKALNYCH KROKÓW,
JEDNAK WIEMY JUŻ, ŻE WIEDZA MOŻE BYĆ TEŻ BRONIĄ. W NIEPOWOŁANYCH RĘKACH...
BRONIĄ MASOWEJ ZAGŁADY.


ABY NIE DOPUŚCIĆ DO PONOWNEJ KATASTROFY, POWOŁANO DO ISTNIENIA INSTYTUCJĘ CERBERA,
STRAŻNIKÓW WIECZNEGO STRUMIENIA SZEROKOPASMOWEJ TRANSMISJI DANYCH Z ALEKSANDRII – ZAUTOMATYZOWANEJ BIBLIOTEKI ORBITALNEJ
ZIUUU...


CERBER
X25
I ZARAZEM JEDYNYCH POWIERNIKÓW KLUCZY DO KWANTOWEGO ZAMKA OTWIERAJĄCEGO SKARBNICĘ NIEBEZPIECZNEJ WIEDZY.

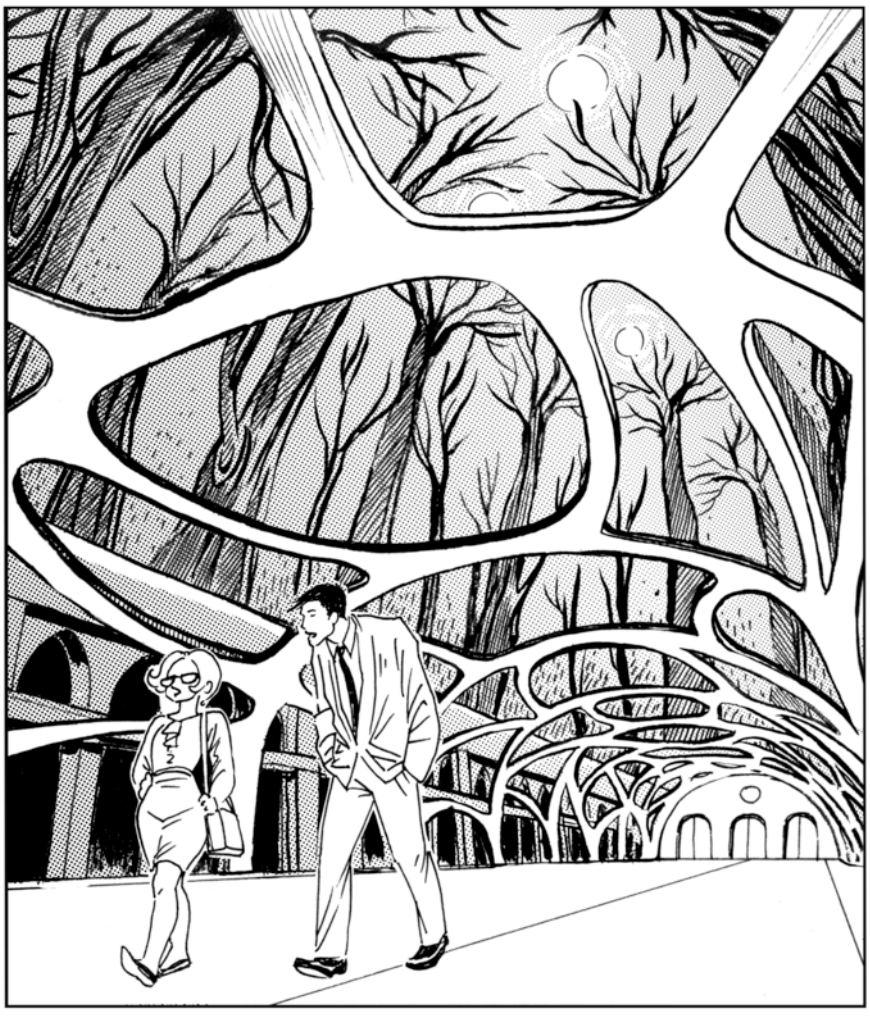

BYLI TACY, KTÓRZY NIE MOGLI POGODZIĆ SIĘ Z TYM STANEM RZECZY. STAWIALI OPÓR.
NAJCZĘŚCIEJ – NIESKUTECZNIE I KRÓTKO.
PRZETRWALI TYLKO CI NAJBARDZIEJ PRZEBIEGLI.
OSACZENI...


... ALE WCIĄŻ GOTOWI PODJĄĆ NAWET DESPERACKIE KROKI,
BYLE TYLKO ZBURZYĆ PORZĄDEK.

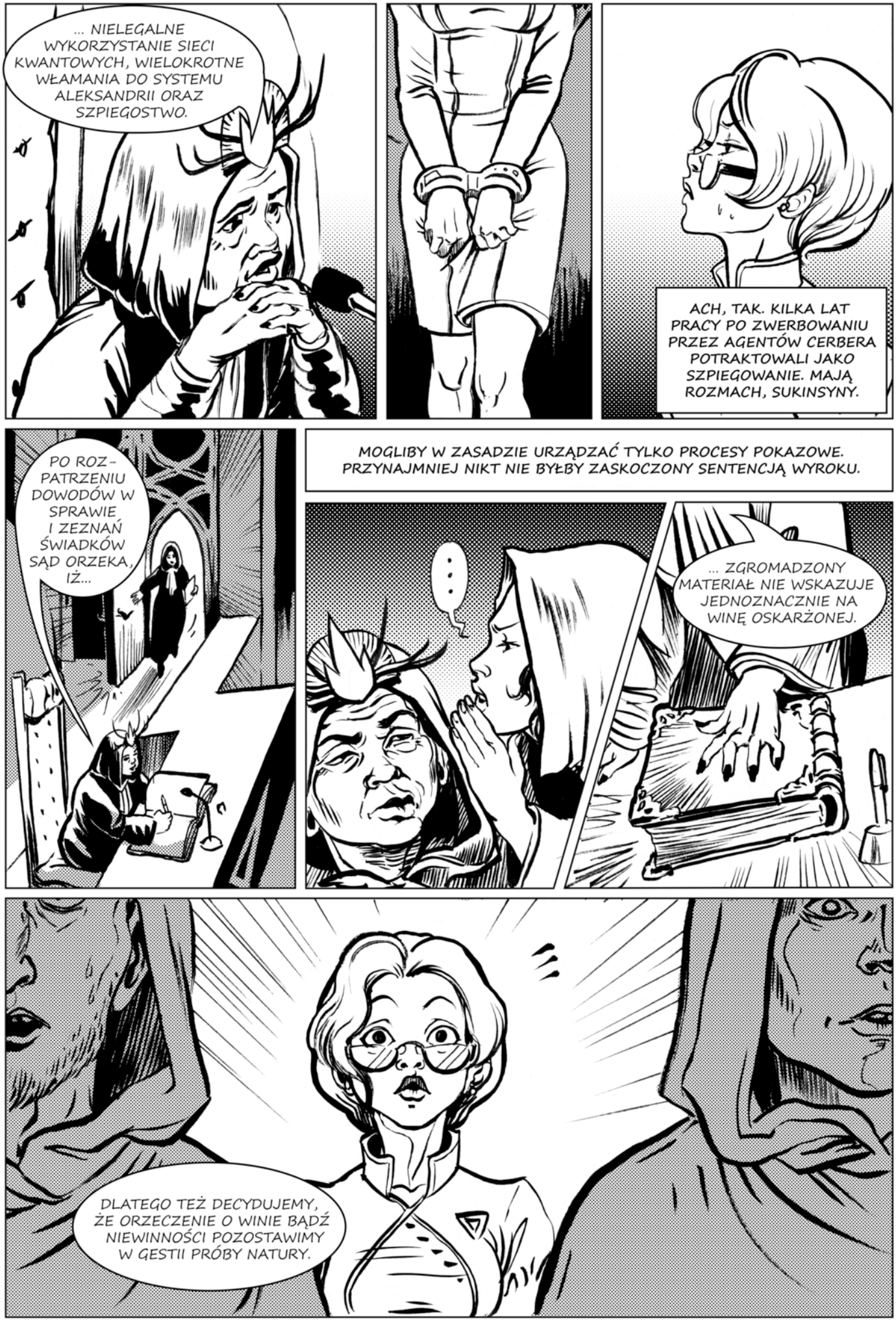

JEDNAK CHOĆ NIE COFNĄ SIĘ PRAWIE PRZED NICZYM...
... DALEKO IM DO ZWYCIĘSTWA.

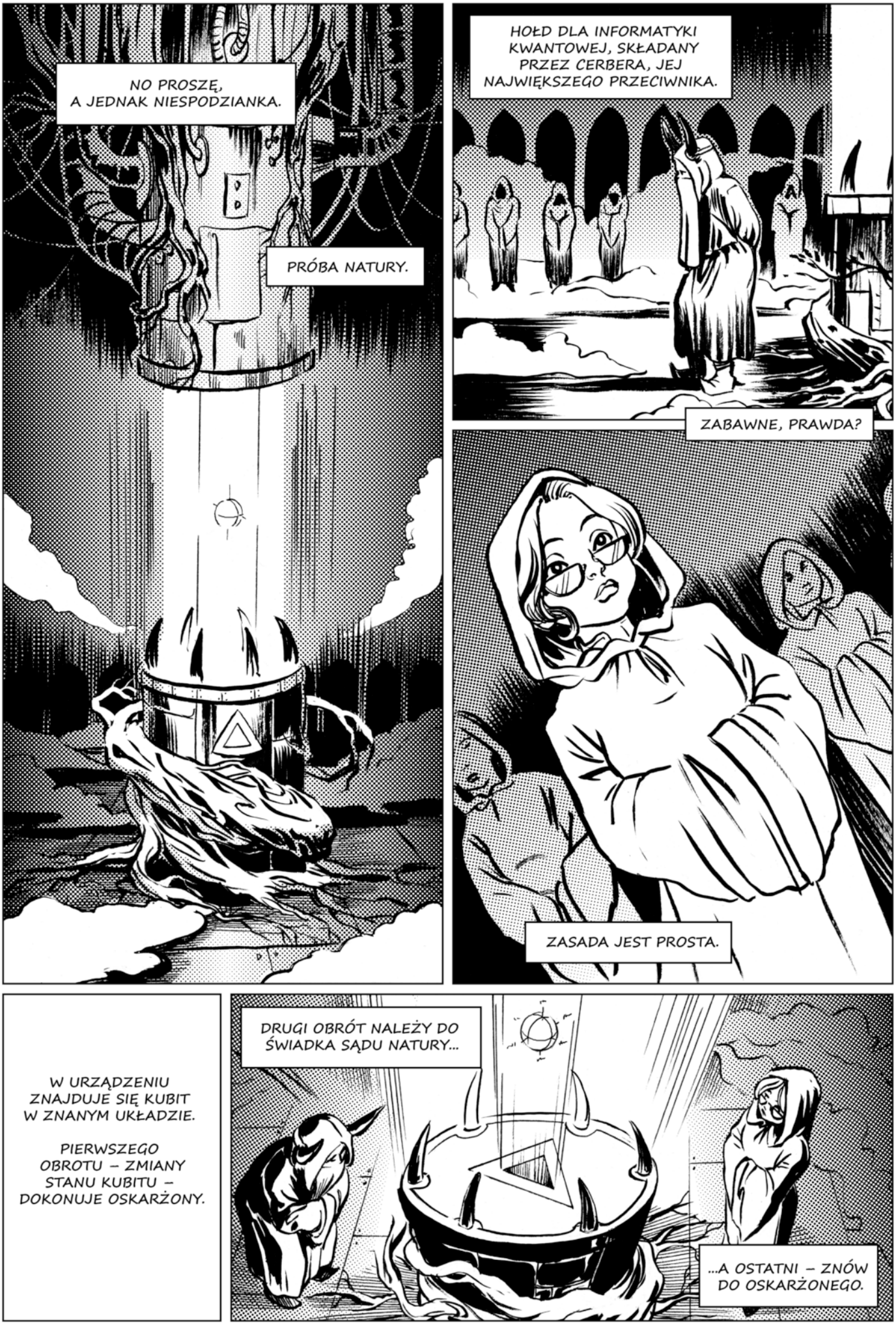
ROZDZIAŁ I

EVE




ZABAWNE – MAM WRAŻENIE, ŻE DO TEJ PORY IRRACJONALNIE WIERZYŁAM W SPRAWIEDLIWOŚĆ.
ZAPOMNIAŁAM NIESTETY, ŻE SĄD TO TYLKO NARZĘDZIE W RĘKU WŁADZY, A CERBER MOŻE MIEĆ WŁASNĄ DEFINICJĘ SPRAWIEDLIWOŚCI.
PROSZĘ WSTAĆ! NASTĄPI ODCZYTANIE WYROKU.
PRZEKONAŁAM SIĘ O TYM OCZYWIŚCIE WÓWCZAS, GDY PRZESTAŁAM JUŻ BYĆ UŻYTECZNA.
CÓŻ, KARA ŚMIERCI JAKO METODA REDUKCJI ETATÓW JEST PRZYNAJMNIEJ... WIDOWISKOWA.
OSKARŻONEJ ZARZUCA SIĘ DZIAŁALNOŚĆ W GRUPACH INFORMACYJNEGO TERRORYZMU...


... NIELEGALNE WYKORZYSTANIE SIECI KWANTOWYCH, WIELOKROTNE WŁAMANIA DO SYSTEMU ALEKSANDRII ORAZ SZPIEGOSTWO.
ACH, TAK. KILKA LAT PRACY PO ZWERBOWANIU PRZEZ AGENTÓW CERBERA POTRAKTOWALI JAKO SZPIEGOWANIE. MAJĄ ROZMACH, SUKINSYNY.
PO ROZ-PATRZENIU DOWODÓW W SPRAWIE I ZEZNAŃ ŚWIADKÓW SĄD ORZEKA, IŻ...
MOGLIBY W ZASADZIE URZĄDZAĆ TYLKO PROCESY POKAZOWE. PRZYNAJMNIEJ NIKT NIE BYŁBY ZASKOCZONY SENTENCJĄ WYROKU.
...
... ZGROMADZONY MATERIAŁ NIE WSKAZUJE JEDNOZNACZNIE NA WINĘ OSKARŻONEJ.
DLATEGO TEŻ DECYDUJEMY, ŻE ORZECZENIE O WINIE BĄDŹ NIEWINNOŚCI POZOSTAWIMY W GESTII PRÓBY NATURY.


NO PROSZĘ,
A JEDNAK NIESPODZIANKA.
PRÓBA NATURY.
HOŁD DLA INFORMATYKI KWANTOWEJ, SKŁADANY PRZEZ CERBERA, JEJ NAJWIĘKSZEGO PRZECIWNIKA.
ZABAWNE, PRAWDA?
ZASADA JEST PROSTA.
W URZĄDZENIU ZNAJDUJE SIĘ KUBIT W ZNANYM UKŁADZIE.
PIERWSZEGO OBROTU – ZMIANY STANU KUBITU – DOKONUJE OSKARŻONY.
DRUGI OBRÓT NALEŻY DO ŚWIADKA SĄDU NATURY...
...A OSTATNI – ZNÓW DO OSKARŻONEGO.


NASTĘPNIE ŚWIADKOWIE DOKONUJĄ UROCZYSTEGO POMIARU STANU KUBITU. JEŻELI KUBIT JEST W UKŁADZIE POCZĄTKOWYM – OSKARŻONY JEST UZNAWANY ZA NIEWINNEGO.
JEŻELI NIE... CÓŻ.
SZANSE NA TO, ŻE POMIAR BĘDZIE DLA OSKARŻONEGO POMYŚLNY, TO DOKŁADNIE PÓŁ NA PÓŁ.
CHYBA ŻE...
... JEST SIĘ KWANTOWYM HAKEREM.
WTEDY PRÓBA NATURY TO W ZASADZIE FORMALNOŚĆ.
NATURA ZADECYDOWAŁA!
NIEWINNA!
TYLE ŻE LUDZIE CERBERA WIEDZĄ, ŻE JESTEM KWANTOWYM HAKEREM. DOSKONALE WIEDZĄ. DLATEGO MNIE ZWERBOWALI.
CO PROWADZI DO INTERESUJĄCEGO PYTANIA:
DLACZEGO NAGLE PRZESTALI CHCIEĆ MNIE SKAZAĆ?

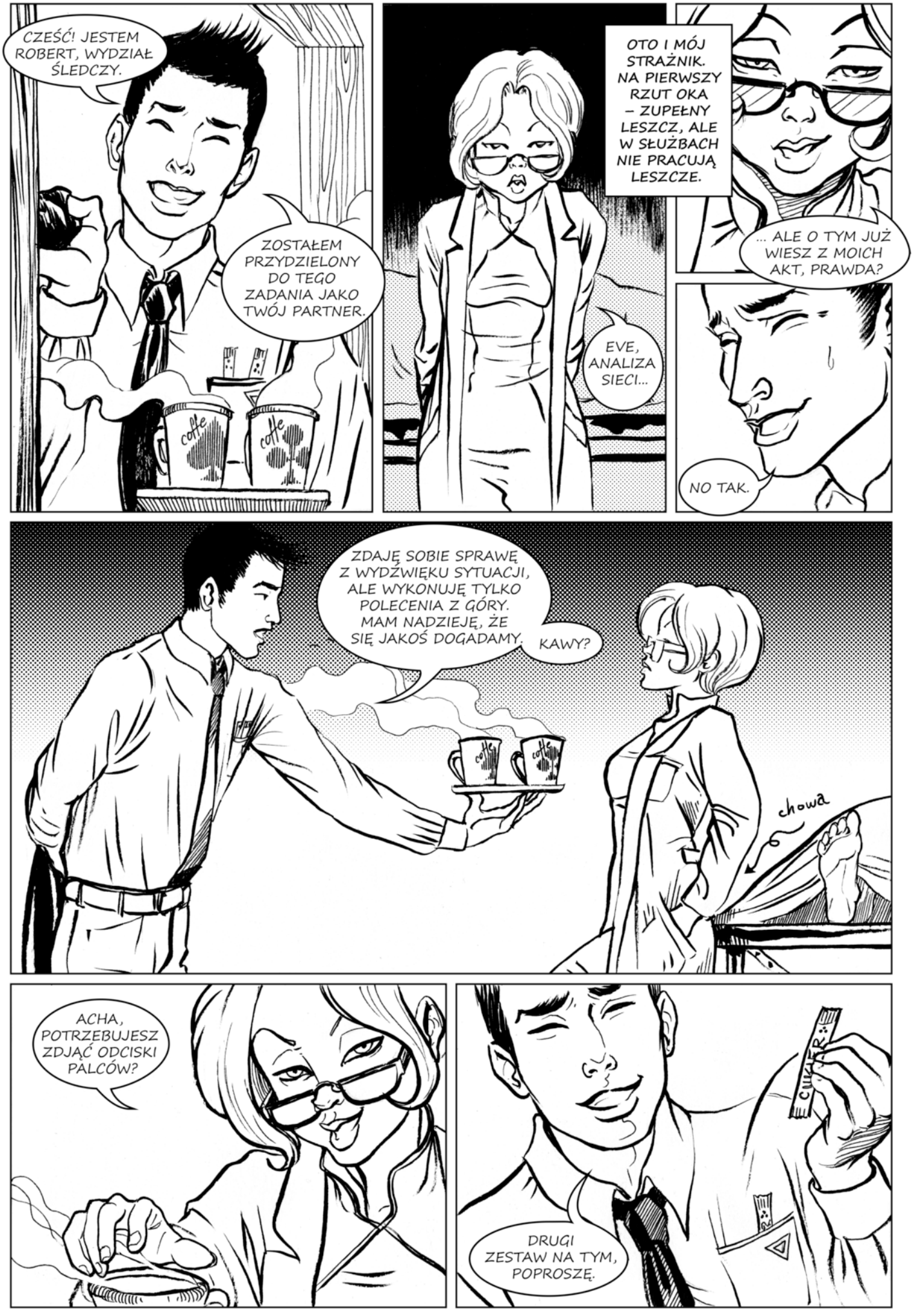

CIESZĘ SIĘ, ŻE WYNIK PRÓBY NATURY OKAZAŁ SIĘ POMYŚLNY DLA PANI...
GABINET PIERWSZEGO ADMINISTRATORA. PRZYPROWADZILI MNIE TU Z SALI PRÓBY NATURY TAK SZYBKO, ŻE NIE ZDĄŻYŁAM NAWET POMACHAĆ MOIM OSKARŻYCIELOM.
... I DLA NAS.
PEWNIE NADAL DYSKUTUJĄ Z JEJ GRUBAWĄ EKSCELENCJĄ SĄDEM.
NIE UKRYWAM, ŻE WIDZĘ W TYM SZCZĘŚLIWY ZBIEG OKOLICZNOŚCI – AKTUALNIE, OCZYSZCZONA Z ZARZUTÓW,
MA PANI OKAZJĘ PRZYSŁUŻYĆ SIĘ CERBEROWI.
NATURALNIE, WASZA EKSCELENCJO.
CO ZA ZASKOCZENIE.


OTÓŻ PRZED KILKOMA DNIAMI MIAŁ MIEJSCE PEWIEN... INCYDENT.
KTOŚ USIŁOWAŁ DOKONAĆ ZAMACHU NA MOJĄ OSOBĘ, W DODATKU W OBECNOŚCI WIELKIEGO ARCHIWISTY.
BARDZO KŁOPOTLIWA SYTUACJA.
CZY TO NIE SPRAWA DLA SŁUŻBY BEZPIECZEŃSTWA?
SUW
hmm...?
W NORMALNEJ SYTUACJI TAK BY BYŁO.
JEDNAK ZAMACHOWIEC BYŁ, PODOBNIE JAK PANI, OSOBĄ... ... SZCZEGÓLNĄ.
HAKER KWANTOWY!
ALE... PO CO HAKER MIAŁBY DOKONAĆ ZAMACHU?
I TO W TEN SPOSÓB?
POZWOLĘ SOBIE WIĘC SPYTAĆ, SKĄD TEN NAGŁY PRZYPŁYW ZAUFANIA?
JA TEŻ JESTEM HAKEREM KWANTOWYM, PRACUJĘ DLA CERBERA OD PIĘCIU LAT – CO NIE PRZESZKODZIŁO POSTAWIĆ MNIE W STAN OSKARŻENIA...
ZAPOMINA SIĘ PANI!
...WASZA EKSCELENCJO.


POPRZESTAŃMY NA TYM, ŻE OSKARŻENIA BYŁY WYSTARCZAJĄCO PRZEKONUJĄCE.
ACH, STARE DOBRE GIERKI WEWNĘTRZNE. CIEKAWE, KOMU NASTĄPIŁAM NA ODCISK. A MOŻE PO PROSTU ZACHCIAŁO IM SIĘ DEMONSTRACJI SIŁY?
NA SZCZĘŚCIE CHWILOWO TĘ KWESTIĘ MOŻEMY UZNAĆ ZA NIEBYŁĄ. I OBY TAK POZOSTAŁO.
TYMCZASEM OTRZYMUJE PANI DANE DOTYCZĄCE ŚLEDZTWA I NOWE UPRAWNIENIA.
PROSZĘ NIE POZWOLIĆ SIĘ ZATRZYMYWAĆ.
ACHA, I JESZCZE JEDNO...
PRZYDZIELILIŚMY PANI OFICERA SŁUŻBY BEZPIECZEŃSTWA.
OCZYWIŚCIE WYŁĄCZNIE DO POMOCY W ŚLEDZTWIE.


KWADRANS PÓŹNIEJ...
LABORATORIUM
DZIĘKI NATURZE, ŻE PANIĄ UNIEWINNIONO, PANNO EVE!
NIE WĄTPILIŚMY...
DZIĘKUJĘ. MIŁO SŁYSZEĆ, ŻE KTOŚ NIE WĄTPIŁ.
DOPIERO CO DOSTARCZONO NAM CIAŁO I RZECZY OSOBISTE TERRORYSTY, NIE ZDĄŻYLIŚMY NAWET ZACZĄĆ OZNACZAĆ...
ZAJMĘ SIĘ TYM, PROSZĘ SIĘ NIE PRZEJMOWAĆ.


ZANIOSĘ TO TYLKO DO ARCHIWUM I ZARAZ PANI POMOGĘ!
NATURALNIE.
YOKO
PAMIĘĆ KWANTOWA. WYPALONA. RÓWNIE DOBRZE KTOŚ MÓGŁ JĄ TU PODRZUCIĆ. TYLKO PO CO?
CO MY TU JESZCZE MAMY... ZAPAŁKI, ZEGAREK... A TO CO?
SKRZYP
PHILIP? ALICE WCIĄGNĘŁA GO ZNOWU?
NIE, TO NIEMOŻLIWE, NIE DAŁBY SIĘ.
ALBO COŚ BYM O TYM WIEDZIAŁA.


CZEŚĆ! JESTEM ROBERT, WYDZIAŁ ŚLEDCZY.
ZOSTAŁEM PRZYDZIELONY DO TEGO ZADANIA JAKO TWÓJ PARTNER.
OTO I MÓJ STRAŻNIK. NA PIERWSZY RZUT OKA – ZUPEŁNY LESZCZ, ALE W SŁUŻBACH NIE PRACUJĄ LESZCZE.
EVE, ANALIZA SIECI...
... ALE O TYM JUŻ WIESZ Z MOICH AKT, PRAWDA?
NO TAK.
ZDAJĘ SOBIE SPRAWĘ Z WYDŹWIĘKU SYTUACJI, ALE WYKONUJĘ TYLKO POLECENIA Z GÓRY. MAM NADZIEJĘ, ŻE SIĘ JAKOŚ DOGADAMY.
KAWY?
chowa
ACHA, POTRZEBUJESZ ZDJĄĆ ODCISKI PALCÓW?
CUKIER
DRUGI ZESTAW NA TYM, POPROSZĘ.


CO ZA MIŁA SYTUACJA.
NIE WIADOMO, JAK DOKONAŁ INFILTRACJI CERBERA ANI KTO MU POMAGAŁ.
KOBIETA, KAWA I TRUP...
MĘŻCZYZNA OKOŁO 20 LAT, BRAK ODCISKÓW PALCÓW W BAZIE. USTALAMY JEGO TOŻSAMOŚĆ I EWENTUALNE POWIĄZANIA Z SIATKĄ PRZESTĘPCZĄ.
I PO CO MU BYŁA PAMIĘĆ KWANTOWA.
ON RACZEJ NAM TEGO JUŻ NIE POWIE.
DLATEGO POTRZEBUJEMY CIEBIE.
TAK MIĘDZY NAMI ... CZYTAŁEM AKTA TWOJEJ SPRAWY I UWAŻAM, ŻE TO IDIOTYZM PRÓBOWAĆ POZBYĆ SIĘ JEDYNEGO KWANTOWEGO HAKERA, JAKIM DYSPONUJEMY.
KTOŚ CIĘ TU CHYBA BARDZO NIE LUBI.
TWOJA TROSKA PRAWIE MNIE WZRUSZA.
PRZEPRASZAM.
WIEM, ŻE TUŻ PO PROCESIE TO MOŻE BRZMIEĆ GŁUPIO...
OWSZEM, BRZMI.
JAK SIĘ DENERWUJĘ, TO MÓWIĘ DUŻO I BEZ ZASTA-NOWIENIA.


ROZUMIEM, ŻE TO WSZYSTKO, CO ZNALEŹLI PRZY ZAMACHOWCU... SPORO TEGO.
I JAK ZWYKLE – BAŁAGAN NA STOLE I BAŁAGAN W KATALOGU.
WŁAŚNIE MIAŁAM SIĘ ZA TO ZABIERAĆ.
ACH...
JEŚLI CHCESZ SIĘ PRZYDAĆ, TO PODAJ ETYKIETY.
JASNE!
MOŻE JAKOŚ SIĘ DOGADAMY.
ALE NICZEGO NIE OBIECUJĘ.
PEWNIE, ROZUMIEM. DZIĘKI.
SKĄD TA MINA? NIE PRZEPADASZ ZA TĄ ROBOTĄ?
KOGO ONI MI PRZYDZIELILI?
TROCHĘ TAK, A TROCHĘ ZWYCZAJNIE BOLI MNIE GŁOWA. PRZEPRASZAM.
Eve
bert
tanaka


NASTĘPNEGO DNIA...
ZNOWU TUTAJ? MASZ TYM RAZEM COŚ INTERESUJĄCEGO?
NIE. PO PROSTU UZNAŁEM, ŻE WARTO TO PRZEJRZEĆ.
ZNOWU?
MAM WRAŻENIE, ŻE PRZEOCZYLIŚMY COŚ ISTOTNEGO.
MAMY MOŻE JAKIEŚ NAGRANIE TEGO ATAKU? W KOŃCU BYLI TAM KAMERZYŚCI...
NIESTETY, TO BYŁA AKURAT TAJNA CZĘŚĆ OBRZĄDKU, TRANSMITOWANA TYLKO W WIELKIEJ SALI I NIENAGRYWANA.
JA PRZESŁUCHAŁAM ŚWIADKÓW I WSZYSCY MÓWIĄ TO SAMO. DUSIŁ GOŁYMI RĘKAMI, WYGLĄDAŁO TO NA NAPAD FURII.
NIKT GO NIE KOJARZYŁ, ALE NA OBRZĘDACH KRĘCI SIĘ TYLU BRACI ZAKONNYCH, ŻE NAWET ICH TO NIE ZANIEPOKOIŁO.
NIC. OSOBIŚCIE NADAL PODEJRZEWAM, ŻE PRACOWAŁ DLA ALICE, ALE WEDŁUG KARTOTEKI JEST CZYSTY JAK ŁZA.
MASZ MOŻE COŚ NA TEMAT JEGO TOŻSAMOŚCI?
NA WSZELKI WYPADEK ZLECIŁEM SEKCJĘ I BADANIE NA NARKOTYKI.
ACH, BAZY DANYCH WYDZIAŁU ŚLEDCZEGO, TAKIE UŻYTECZNE..
DAJ SPOKÓJ. ALICE TO NIE BYLE GRUPKA KWANTOWYCH HAKERÓW. SĄ DOBRZE ZORGANIZOWANI I...
ZAUWAŻYŁEŚ, ŻE GOŚĆ W OGÓLE NIE MIAŁ BRONI?
NIE JESTEM ZASKOCZONY.
Z BRONIĄ BYŁOBY MU O WIELE TRUDNIEJ PRZEBIĆ SIĘ PRZEZ KONTROLĘ BEZPIECZEŃSTWA.
ZAWODOWY ZABÓJCA?
NIE WIEM.
DBAJĄ O SWOICH, WIEM. ZBIERAJ SIĘ.
DOKĄD? PO CO?


TA WYPALONA PAMIĘĆ KWANTOWA NIE DAJE MI SPOKOJU.
A NIE WPUSZCZĄ MNIE DO TERMINALA BEZ MOJEGO DROGIEGO WSPÓŁPRACOWNIKA.
WIEM, TO UCIĄŻLIWE.
TO PRAWDA.
NIE MAM WPŁYWU NA PROCEDURY. PRZEPRASZAM.
NIE PRZEJMUJ SIĘ.
PRZYNAJMNIEJ MASZ JAKĄŚ FUNKCJĘ. INACZEJ BYŁBYŚ NIEPRZYDATNY.
PRZESADA. KRYPTOGRAFIA KWANTOWA TO METODA ZABEZPIECZANIA DANYCH. SAME DANE NIE MUSZĄ BYĆ SZKODLIWE.
PEWNIE PRZED UPADKIEM LUDZIE TEŻ TAK MYŚLELI...
ALE TO NIE KRYPTOGRAFIA NAS WTEDY ZAŁATWIŁA. PO PROSTU KTOŚ UŻYŁ JEJ W ZŁYM CELU.
PRZEZ DŁUGI CZAS NAWET NIE WIEDZIAŁEM, ŻE MAMY TU TERMINALE KWANTOWE.
A JAK SĄDZISZ, W JAKI SPOSÓB MIELIBYŚMY WALCZYĆ Z ALICE NA JEJ GRUNCIE?
SZCZERYMI CHĘCIAMI?
A TE WSZYSTKIE MĄDROŚCI O PATRZENIU W OTCHŁAŃ I TAK DALEJ?
A NIE SĄDZISZ, ŻE ZAWSZE SIĘ TACY ZNAJDĄ?
OCZYWIŚCIE. DLATEGO CERBER ZATRUDNIŁ MNIE.


WOW! NIE WIEDZIAŁEM, ŻE...
TAK TO WYGLĄDA?
WIDZIAŁEM SPORO TERMINALI KWANTOWYCH. WSZYSTKIE BYŁY ZDECYDOWANIE MNIEJ OKAZAŁE.
BO TO CENTRUM OBLICZEŃ KWANTOWYCH, A NIE TYLKO TERMINAL.
TUTAJ ODSZYFROWYWANY JEST SYGNAŁ ALEKSANDRII.
ALE PRZECIEŻ SYGNAŁ IDZIE SZEROKOPASMOWO. KAŻDY, KTO MA KLUCZ, MOŻE GO ODCZYTAĆ NA DOWOLNYM TERMI-NALU.
PO PIERWSZE, JAK SAM ZAUWAŻYŁEŚ, POTRZEBA KLUCZA. A KWANTOWYCH KLUCZY NIE MOŻNA SKOPIOWAĆ – CO NAJWYŻEJ MOŻNA JE TELEPORTOWAĆ, WIĘC LICZBA KOPII JEST STAŁA.


U NAS W KATEDRZE SĄ ZALEDWIE DWA, JEDEN TUTAJ I DRUGI U PIERWSZEGO ADMINISTRATORA.
FUU...
Q01231
NATURALNIE WIĘC STARAMY SIĘ ICH PILNOWAĆ.
I ONE ODSZYFROWUJĄ SYGNAŁ ALEKSANDRII?
ALEŻ SKĄD.
ontakt z Aleksandrią : przesył danych prawidłow
SAMO SZYFROWANIE TO PROSTY ALGORYTM VERNAMA, ALE KLUCZE TRZYMAMY W WEWNĘTRZNEJ SIECI.
TYLKO DLA AUTORYZOWANYCH TERMINALI?
DOKŁADNIE.
PO DRUGIE, KIEDY JUŻ MAMY SYGNAŁ, TUTAJ SIĘ GO SEGREGUJE.
R38
ALEKSANDRIA NADAJE PRAKTYCZNIE WSZYSTKO, CO LUDZKOŚĆ WIEDZIAŁA PRZED KATAKLIZMEM.
CERBER MUSI TO PRZEBRAĆ I ZADECYDOWAĆ, CO UDOSTĘPNI LUDZIOM, A CO ZACHOWA.


NIE CHCIELIBYŚMY NA PRZYKŁAD, ŻEBY KAŻDY MÓGŁ PRZECZYTAĆ, JAK ZROBIĆ BOMBĘ BIO, PRAWDA?
JEDEN RAZ WYSTARCZY.
A TERAZ, JEŚLI POZWOLISZ..
CO ROBISZ?
klik klik
RZECZY ABSOLUTNIE NIELEGALNE.
DISCONNECTED
CHOLERA!
TROCHĘ ICH NIE DOCENIŁAM.
KOGO?
ALICE, OCZYWIŚCIE!
POWINNAM BYŁA PRZEWIDZIEĆ, ŻE ZLIKWIDUJĄ MOJĄ FURTKĘ DO ICH SIECI.


CO SIĘ WŁAŚCIWIE STAŁO?
MIAŁAM WEJŚCIE DO SIECI ALICE. CHCIAŁAM GO UŻYĆ, ŻEBY TROCHĘ POWĘSZYĆ...
I JUŻ NIE MASZ?
... SĄDZIŁAM, ŻE BYŁO LEPIEJ UKRYTE.
CO TERAZ?
JESTEŚ ŚLEDCZYM OD NIEDAWNA, CO? JAK SAM WIDZISZ, ZAWIODŁA NAS DROGA NA SKRÓTY...
... WIĘC BĘDZIEMY MUSIELI ZAŁATWIĆ SPRAWĘ TRADYCYJNIE.

ROZDZIAŁ II

BRETT


MUSIAŁAM Z POWROTEM DOSTAĆ SIĘ DO SIECI ALICE. DOWIEDZIEĆ SIĘ, CO CHCIELI OSIĄGNĄĆ.
NO I OCZYWIŚCIE MUSIAŁAM ZNALEŹĆ PHILIPA.
PHIL, SŁODKI GŁUPKU, JAK MOGŁEŚ DAĆ SIĘ W TO WKRĘCIĆ?
NIE SPODZIEWAŁAM SIĘ, ŻE MOJA FURTKA DO SYSTEMU ZOSTANIE WYKRYTA TAK SZYBKO.
ILE RAZY JEJ UŻYŁAM? RAZ? DWA? NAJWYRAŹNIEJ WYSTARCZYŁO.
TERAZ TRZEBA JĄ ODZYSKAĆ.
A ODKURZANIE KONTAKTÓW TO ŻMUDNA I NIEPEWNA ROBOTA.
LICHO WIE, KTO JEST JESZCZE LOJALNY.


NIEKTÓRZY BYLI.
ALE NIE POTRAFILI POMÓC W WEJŚCIU DO SIECI ALICE.
W SPRAWIE PHILIPA TEŻ ZRESZTĄ NIE.
KROK PO KROKU...
... BEZPIECZNE OPCJE SIĘ KOŃCZYŁY.
BYĆ MOŻE TRZEBA BĘDZIE WYJŚĆ Z CIENIA.


WIESZ, EVE, MASZ MASĘ KONTAKTÓW ZWIĄZANYCH Z ALICE...
KILKA.
JESZ JAK DZIECKO.
UNIK?
NIEKONIECZNIE CHCĘ ROZMAWIAĆ O MOICH KONTAKTACH.
NIE, NIE! ZUPEŁNIE NIE O TO MI CHODZI!
WIĘC – O CO?
NO... TY KIEDYŚ BYŁAŚ W TEJ GRUPIE, PRAWDA?
WSZYSTKO JEST W AKTACH.
ANALITYCY CERBERA TWIERDZĄ, ŻE KONTAKT Z ALEKSANDRIĄ...
NIE, NIE WSZYSTKO.
WIADOMO, ŻE BYŁAŚ. NIE MA ANI SŁOWA O TYM, DLACZEGO PRZESTAŁAŚ BYĆ.
RÓŻNICE POGLĄDÓW.
NA TERRORYZM?
ALICE TO NIE TERRORYŚCI.
PO PROSTU UWAŻAJĄ, ŻE INFORMACJA POWINNA BYĆ DOSTĘPNA DLA WSZYSTKICH.
KAŻDA INFORMACJA. ŻE DZIELENIE SIĘ WIEDZĄ TO NACZELNY PRZYWILEJ CZŁOWIEKA.
W PEWNYM SENSIE TRUDNO ICH NIE ZROZUMIEĆ.
TAK... TYLKO PAMIĘTAJ, DO CZEGO TAKIE MYŚLENIE DOPROWADZIŁO.


KRYPTOGRAFIA KWANTOWA DAWAŁA PEŁNĄ PRYWATNOŚĆ. CAŁKOWITĄ WOLNOŚĆ OD JAKIEGOKOLWIEK NADZORU.
A MY NARZUCAMY KONTROLĘ.
WŁAŚNIE. LUDZIE ALICE WIERZĄ, ŻE ZNÓW DOROŚLIŚMY DO WOLNOŚCI – JA NIE.
RÓŻNICA POGLĄDÓW, JAK MÓWIŁAM.
JAK SIĘ NAJADŁEŚ, TO CHODŹ.
DOKĄD?
DO PRACY.
ZRELAKSUJ SIĘ, KUP SOBIE DRINKA, POPATRZ NA TANCERKI. TO NIE ZAJMIE WIĘCEJ NIŻ KILKA MINUT.
I, COKOLWIEK SIĘ ZDARZY, NIE IDŹ ZA MNĄ.
Toxic CLUB
WOLAŁBYM TAM Z TOBĄ PÓJŚĆ.
TAKI ATAWIZM.
BRETT CIĘ NIE ZNA, PRZY TOBIE NIE BĘDZIE CHCIAŁ GADAĆ.


BRETT. JEDEN Z KILKUNASTU INFORMATORÓW ALICE W MIEŚCIE.
JESTEŚ PEWNA, ŻE TO BEZPIECZNE?
JESTEM PEWNA, ŻE TO NIEBEZPIECZNE. INACZEJ ZACZĘŁABYM OD TEGO MIEJSCA.
DAM SOBIE RADĘ.
POTRZYMAJ MI TO
NAPRAWDĘ ŚWIETNIE.
NAJEMNIK. ALICE MU PŁACI, WIĘC JEST LOJALNY. PRAWDOPODOBNIE ZARAPORTUJE MOJĄ WIZYTĘ JAKIEŚ PIĘĆ MINUT PO TYM, JAK WYJDĘ.
NIE MA CIĘ NA LIŚCIE GOŚCI, PANIENKO.
ZAWIADOM PANA BRETTA, ŻE PRZYSZŁA EVE.
NIEKTÓRZY NIE MUSZĄ SIĘ WPISYWAĆ NA LISTĘ. IDŹ, NIE MAM CAŁEGO DNIA.
ALE W SWOIM CZASIE BYŁ MI WINIEN KILKA PRZYSŁUG. MOŻE TO COŚ DA.
STAF
ONLY
HMMM... BRAMKI TAKIE JAK W KWATERZE CERBERA.
CIEKAWE, CZY W OGÓLE WIE, DO CZEGO SŁUŻĄ, CZY ZAINSTALOWAŁ JE, BO SŁYSZAŁ, ŻE SĄ WAŻNE?


NIE ZMIENIŁ SIĘ ZBYTNIO.
BRETT! KOPĘ LAT!
EVE. SŁYSZAŁEM, ŻE NIE ŻYJESZ.
... I NOSI KLUCZ PRZY SOBIE.
PLOTKI, PLOTKI.
TWOI OCHRONIARZE SĄ WIDOCZNIE NIE NAJLEPIEJ POINFORMOWANI.
I TAK BYM CIĘ PRZECIEŻ WPUŚCIŁ. SIADAJ.
NAPIJESZ SIĘ?
DOPIERO KIEDY BĘDZIEMY OBLEWALI UBICIE INTERESU.
KONKRETNA JAK ZAWSZE.
NIE CHCĘ MARNOWAĆ TWOJEGO CZASU.
DLACZEGO W OGÓLE MIAŁBYM CHCIEĆ ROBIĆ INTERESY Z MARTWĄ HAKERKĄ CERBERA?
DLATEGO ŻE MNIE LUBISZ.
I DLATEGO ŻE JESTEŚ OSOBĄ PRAKTYCZNĄ.


A DOBICIE ZE MNĄ TARGU BĘDZIE CI SIĘ BARDZO OPŁACAŁO.
ZAMIENIAM SIĘ W SŁUCH.
POTRZEBUJĘ WEJŚĆ DO SIECI ALICE. RACZEJ JEDNORAZOWO I RACZEJ NA KRÓTKO.
PROSISZ O DUŻO.
O NIC, CZEGO NIE MÓGŁBYŚ DOSTARCZYĆ, BRETT. I WIERZ MI, NIE BĘDZIESZ ŻAŁOWAŁ.
WIDZISZ, EVE, JESTEM OCZYWIŚCIE PEWIEN, ŻE MASZ W ZANADRZU DOBRĄ OFERTĘ...
ALE JA TU MUSZĘ ŻYĆ.
NAPRAWDĘ UWAŻASZ, ŻE ALICE OCHRONI CIĘ LEPIEJ NIŻ CERBER?
ALEŻ SKĄD!
UWAŻAM PO PROSTU, ŻE CERBER MA MOJE BEZPIECZEŃSTWO W GŁĘBOKIM POWAŻANIU.
ZAPŁACI, A JAKŻE – PO CZYM ZAJMIE SIĘ WAŻNIEJSZYMI SPRAWAMI. A JA TU ZOSTANĘ.


NIE WIERZYSZ W LOJALNOŚĆ CERBERA WOBEC SWOICH?
A TY IM WIERZYSZ? PO TYM, CO CI ZROBILI?
krok...
WIERZĘ, ŻE MIELI POWODY.
A TY? UFASZ ALICE?
POWIEDZIELI CI CHOCIAŻ, JAK TO DZIAŁA?
O CO CHODZI Z KRYPTOGRAFIĄ KWANTOWĄ?
CZY WCISNĘLI TYLKO GARŚĆ IDEALISTYCZNYCH BZDUR?
SZARP
UFAM, ŻE MI ZAPŁACĄ. POWIEDZIELI, JAK TEGO UŻYWAĆ, JEŚLI BĘDĘ CHCIAŁ SIĘ Z NIMI SKONTAKTOWAĆ.
RESZTA MNIE NIE OBCHODZI.
NIE SĄDZĘ, ŻEBY CERBER POWIEDZIAŁ MI WIĘCEJ.
WIESZ, JESTEŚMY PRZYJACIÓŁMI. MOŻEMY SIĘ DOGADAĆ.


WYTŁUMACZĘ CI WSZYSTKO... CZEGO BĘDZIESZ SOBIE ŻYCZYŁ.
WSZYSTKO?
ALEŻ...
OCZYWIŚCIE, ŻE...
WSZYSTKO...
TO MOŻE POWIESZ MI, DLACZEGO UWAŻASZ, ŻE NABIORĘ SIĘ NA TAK TANIĄ SZTUCZKĘ?
SZTUCZKĘ?
NAPRAWDĘ MAM CI WYJAŚNIAĆ?
PO PIERWSZE – ZACZĘŁAŚ SIĘ PRZYMILAĆ ZUPEŁNIE BEZ POWODU, A WIEM, ŻE NIGDY TEGO NIE ROBISZ.
PO DRUGIE – ZDAJESZ SIĘ BEZZASADNIE UWAŻAĆ, ŻE MAM NA CIEBIE TAKĄ OCHOTĘ, ŻEBY RYZYKOWAĆ PRZEZ TO ŻYCIEM.


PO TRZECIE WRESZCIE... CAŁY CZAS GMERASZ MI PRZY ŁAŃCUSZKU KLUCZA.
PYCH
BAM
ZROZUM, BRETT...
NIE, TO TY ZROZUM. NIE MASZ NIC, CO UZNAŁBYM ZA WARTE RYZYKA.
W ZASADZIE POWINIENEM CIĘ ROZWALIĆ NA MIEJSCU.
gulp...
BRETT...
ALE PAMIĘTAM, ŻE JESTEM CI NADAL DŁUŻNY PRZYSŁUGĘ, WIĘC PO PROSTU ZNIKAJ STĄD I RACZEJ NIE WRACAJ.
OCHRONIARZ ODPROWADZI CIĘ DO WYJŚCIA.


PYCH
CO SIĘ STAŁO?
WYCHODZIMY!
HEJ, EVE!


ROZUMIEM, ŻE ROZMOWA NIE POSZŁA TAK, JAK POWINNA?
SKĄD TEN POMYSŁ?


OCHRONIARZ WYRZUCIŁ CIĘ Z BUDYNKU.
DOKŁADNIE NA TO LICZYŁAM. MAMY JAKIEŚ PIĘĆ MINUT.
JAK TO... ?
UKRADŁAM MU KLUCZ DO SIECI.


BRETT NIC NIE WIE O INFORMATYCE KWANTOWEJ. INACZEJ NIE NOSIŁBY KLUCZA NA SZYI.
POTRZEBOWAŁAM TYLKO PRZEZ CHWILĘ BYĆ NA TYLE BLISKO, ŻEBY TELEPORTOWAĆ JEGO ZAWARTOŚĆ NA MOJĄ WŁASNĄ KARTĘ...
SPLĄTANĄ Z KLUCZEM, KTÓRY ZOSTAWIŁAM Z TOBĄ.
A KONIECZNE DO ODSZYFROWANIA INFORMACJE ZOSTAŁY ZAPISANE KLASYCZNIE NA MOIM ZEGARKU.
BRETT ZABEZPIECZYŁ SIĘ BARDZO PORZĄDNIE, ALE JEGO BRAMKI NIE POZWALAJĄ WYPROWADZIĆ TYLKO INFORMACJI KWANTOWEJ. A JA JĄ JUŻ MIAŁAM W SPLĄTANYM KUBIKU W TORBIE.
MUSIAŁAM WIĘC PRZESZMUGLOWAĆ TYLKO DANE Z ZEGARKA, ALE ONE Z KOLEI NIE BYŁY KWANTOWE.
I WSZYSTKO TO ZAPLANOWAŁAŚ?
OWSZEM. ALE MAMY MAŁO CZASU.
ZA CHWILĘ BRETT SPRÓBUJE WEJŚĆ W SIEĆ ALICE, ŻEBY ZARAPORTOWAĆ, CO SIĘ WYDARZYŁO I ODKRYJE, ŻE JEGO KLUCZ JEST PUSTY.
PUSTY?
TAK, BO KLUCZ TELEPORTOWAŁAM DO SIEBIE. TEGO SIĘ NIE DA PO PROSTU SKOPIOWAĆ. W KAŻDYM RAZIE MUSIMY SIĘ BARDZO SPIESZYĆ.
WIESZ, TO MOŻE JA POSTOJĘ NA WARCIE. JAKBYŚ MIAŁA...
ŚWIETNIE, NIE BĘDZIESZ MI ZAGLĄDAŁ PRZEZ RAMIĘ.

klik

ZOBACZYMY... PRZEDE WSZYSTKIM PHIL.

CONNECTED

JAK NA RAZIE NIEŹLE.

O, JAK MIŁO Z ICH STRONY... ZNIEŚLI MÓJ DOSTĘP, ALE MOJA SKRZYNKA KONTAKTOWA Z PHILIPEM ZOSTAŁA. MOŻE NIE UDAŁO SIĘ JEJ ODKRYĆ. TYM LEPIEJ DLA MNIE.

O ZAMACHU ANI SŁOWA, ALE PRZYNAJMNIEJ PHIL WRZUCIŁ SWÓJ ADRES. HMM, TANOTH, STREFA ZEWNĘTRZNA... STRASZNE SLUMSY, ALE PRZYNAJMNIEJ WIEM, DOKĄD PÓJŚĆ.

tap tap

TERAZ JESZCZE...

IRVING: MIAŁEŚ NIE UŻYWAĆ TEGO KANAŁU, BRETT.

OCHO, CO ZA SZYBKA REAKCJA!

Z DRUGIEJ STRONY... MYŚLĄ, ŻE JESTEM BRETTEM. MOŻE DZIĘKI TEMU UDA SIĘ...

COŚ Z NICH WYCIĄGNĄĆ.

KIEDY NIE WIE SIĘ NIC, POZOSTAJE TYLKO BLEF.

ZOBACZYMY, CZY SIĘ NA TO ZŁAPIĄ.

BRETT: PRZYSZŁA DZIŚ DO MNIE EVE. PRÓBOWAŁA WZIĄĆ MNIE NA SPYTKI.

BRETT: BEZ PRZERWY WYPYTYWAŁA O ZAMACH W KATEDRZE. WYDAJE SIĘ SPORO WIEDZIEĆ. NA RAZIE KAZAŁEM JEJ PRZYJŚĆ JUTRO. CO ZALECACIE?

IRVING: NIC NIE WIE.

IRVING: UTRZYMUJ KONTAKT.
NA RAZIE NIECH NADAL WIERZY,
ŻE TO BYŁ ZAMACH.

BRETT: BĘDĘ MUSIAŁ COŚ JEJ DAĆ, PRĘDZEJ CZY PÓŹNIEJ.

NO, IRVING, KIMKOLWIEK JESTEŚ, POWIEDZ COŚ JESZCZE.

DISCONNECTED

CHOLERA, BRETT SIĘ ZORIENTOWAŁ.


OWOCNY WIECZÓR.
DOWIEDZIAŁAŚ SIĘ CZEGOŚ O NASZYM ZAMACHOWCU?
O TAK. NA PRZYKŁAD, ŻE TO NIE BYŁ ZAMACHOWIEC.
JAK NIE ZAMACHOWIEC, TO KTO?
JESZCZE NIE WIEM.
DOBRANOC.
DOBRANOC.
KWADRANS PÓŹNIEJ
TAXI!
MIEJMY NADZIEJĘ, ŻE PHILIP BĘDZIE COŚ WIEDZIAŁ. ALBO PRZYNAJMNIEJ BĘDZIE MÓGŁ MNIE NAPROWADZIĆ NA WŁAŚCIWY TROP.
TAXI
TAXI
ALBO ŻE W OGÓLE TAM BĘDZIE...

ROZDZIAŁ III

ALICE


TANOTH.
WSPANIAŁE MIEJSCE DO ŻYCIA.
STREFA WYSOKIEGO ZAGROŻENIA BIOLOGICZNEGO, WSZĘDZIE TOKSYCZNE WYZIEWY, NIE MÓWIĄC O ZWYKŁEJ MIĘDZYLUDZKIEJ WROGOŚCI.
BRAWO, PHIL.
WZIĘCIE BRONI NIE BYŁO NAJGORSZYM POMYSŁEM.
UCHYLONE DRZWI... TO NIE JEST DOBRY ZNAK.

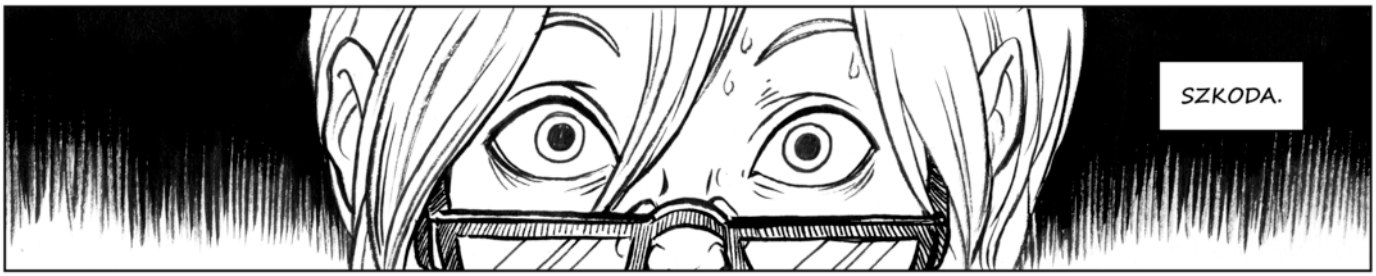

A ŚLADY PRZESZUKANIA TO ZNAK JESZCZE GORSZY.
O NIE...
PHIL?...
NIE, NIE, NIE!


DWÓCH.
NIE...
NIE SĄ TU PRZYPADKIEM, ZBYT PEWNIE IDĄ.
KROKI ...
CZY TO MOJA KOLEJ?
CZY ZABIJĄ MNIE TU, PRZY CIELE PHILIPA?
SKRZYP...
W PEWIEN SPOSÓB BYŁOBY TO WŁAŚCIWE...
ALE NIE.
KROK PIERWSZY.


WYKORZYSTAĆ ELEMENT ZASKOCZENIA.
ZRYW..
BAM!
KROK DRUGI: ZEMŚCIĆ SIĘ ZA PHILA.
KROK TRZECI...
hu hu hu
BACH
O, SZLAG!


NIE DAĆ SIĘ ZASKOCZYĆ PRZECIWNIKOWI.
DAŁAM SIĘ PODEJŚĆ.
KOSZTOWNY BŁĄD.


ZAPEWNE OSTATNI.


SZKODA.


BAM!


CO DO...?
EVE, JESTEŚ TUTAJ?
WSZYSTKO W PORZĄDKU?
DAWNO SIĘ TAK NIE CIESZYŁAM Z WIDOKU KOGOŚ ZE ŚLEDCZEGO.


SKĄD WIEDZIAŁEŚ, GDZIE JESTEM?
PRZECIEŻ MAM CIĘ NADZOROWAĆ. TO CHYBA JASNE, ŻE POJECHAŁEM ZA TOBĄ.
ACH, PRAWDZIWY MONITORING. CIEKAWE, CZY MIESZKANIE TEŻ MI NASZPIKOWALI KAMERAMI.
KTO TO BYŁ?
PHIL. PRZYJACIEL. KOCHANEK
ZNAJOMY. KONTAKT, NA KTÓRY LICZYŁAM.
TO MIŁO, ŻE NIE PYTA, DLACZEGO NIE POWIEDZIAŁAM MU WCZEŚNIEJ.
PRZYKRO MI.
NIE MASZ POWODÓW.
JA MAM POWODY. MOŻE GDYBYM NIE CHOWAŁA MEDALIKA, PHIL BY ŻYŁ. MOŻE ARESZTOWANY, ALE JEDNAK BY ŻYŁ.
ZAWIOZĘ CIĘ DO DOMU.
NIE MA SENSU TU ZOSTAWAĆ, EKIPA WYCZYŚCI WSZYSTKO.
DOPILNUJĘ, ŻEBYŚ MIAŁA PEŁNY DOSTĘP DO RAPORTÓW.
DZIĘKI.


JESTEŚ PEWNA, ŻE NIE CHCESZ ZOBACZYĆ LEKARZA?
TAXI
JESTEM.
LEDWO MNIE SZTURCHNĄŁ.
JAKBY CO... TO DZWOŃ.
JASNE.


uh...
PRAWIE JEDENASTA. CZUJĘ SIĘ JAK TRUP. CÓŻ, MOGŁAM BYĆ MARTWA.
CERBER JUŻ SIĘ DOBIJA, CHOĆ TYLKO WIRTUALNIE. DZIWNE, ŻE NIE PRZYSŁALI ZBROJNEJ GRUPY.
O. DZIEŃ WOLNEGO. WSPANIAŁOMYŚLNE. GDYBYM WIEDZIAŁA, CZĘŚCIEJ DAWAŁABYM SIĘ NAPADAĆ.
ZOSTAŁA MI PO TOBIE FOTOGRAFIA ZE SKAZĄ I TROCHĘ WSPOMNIEŃ, DAWNY PRZYJACIELU.
ALE JESZCZE NIE PORA NA ODPOCZYNEK.
TERAZ, SKORO PHIL NIE ŻYJE, NIE POTRZEBUJE OCHRONY. POTRZEBUJE ZEMSTY.


A KTÓŻ WYMIERZY JĄ LEPIEJ NIŻ CERBER, KIEDY ODKRYJE, ŻE PHIL BYŁ POWIĄZANY ZE SPRAWĄ ADMINISTRATORA?
MAM NADZIEJĘ, ŻE DOBRZE OBLICZYŁAM CZAS.
DOKŁADNIE TAK JAK MYŚLAŁAM. PUSTO.
uf...
NIE... TO NIE... TO NIE TO...
O, JEST.
SPIS WSZYSTKIEGO, CO ZNALEŹLIŚMY PRZY NASZYM DENACIE.
NO, DOPIERO TERAZ WSZYSTKIEGO...
PANI EVE?
... OCZYWIŚCIE NIC NIE MOŻE PÓJŚĆ IDEALNIE GŁADKO...


CHCIAŁAM ZDAĆ MEDALIK, KTÓRY POBRALIŚMY Z ROBERTEM DO ANALIZY. BYŁO PUSTO, WIĘC SIĘ ROZGOŚCIŁAM.
MEDALIK? JAKI MEDALIK?
NIECH TO NIE BĘDZIE TEN JEDYNY PRZYPADEK W PAŃSKIEJ KARIERZE, KIEDY AKURAT NIE JEST PAN ROZTARGNIONY...
SPRAWA ATAKU NA PIERWSZEGO ADMINISTRATORA, RZECZY ZNALEZIONE PRZY NAPASTNIKU?
POBRALIŚMY TO JAKIŚ CZAS TEMU, ZROBILIŚMY BADANIA, ODNOSZĘ.
ZUPEŁNIE ZAPOMNIAŁEM! KTÓREGOŚ DNIA WŁASNEJ GŁOWY ZAPOMNĘ, HA, HA...
NO, A JEDNAK SIĘ UDAŁO...
OCH, TO PRZECIEŻ NIC WAŻNEGO. DO WIDZENIA!
CHWILECZKĘ, PROSZĘ PANI!
TAK?
POKWITOWANIE ZDANIA DOWODU! PROSZĘ!
Cerber Center
UFF. PORA SIĘ ZWIJAĆ, ZANIM ZBYT WIELU LUDZI MNIE TU ZOBACZY.

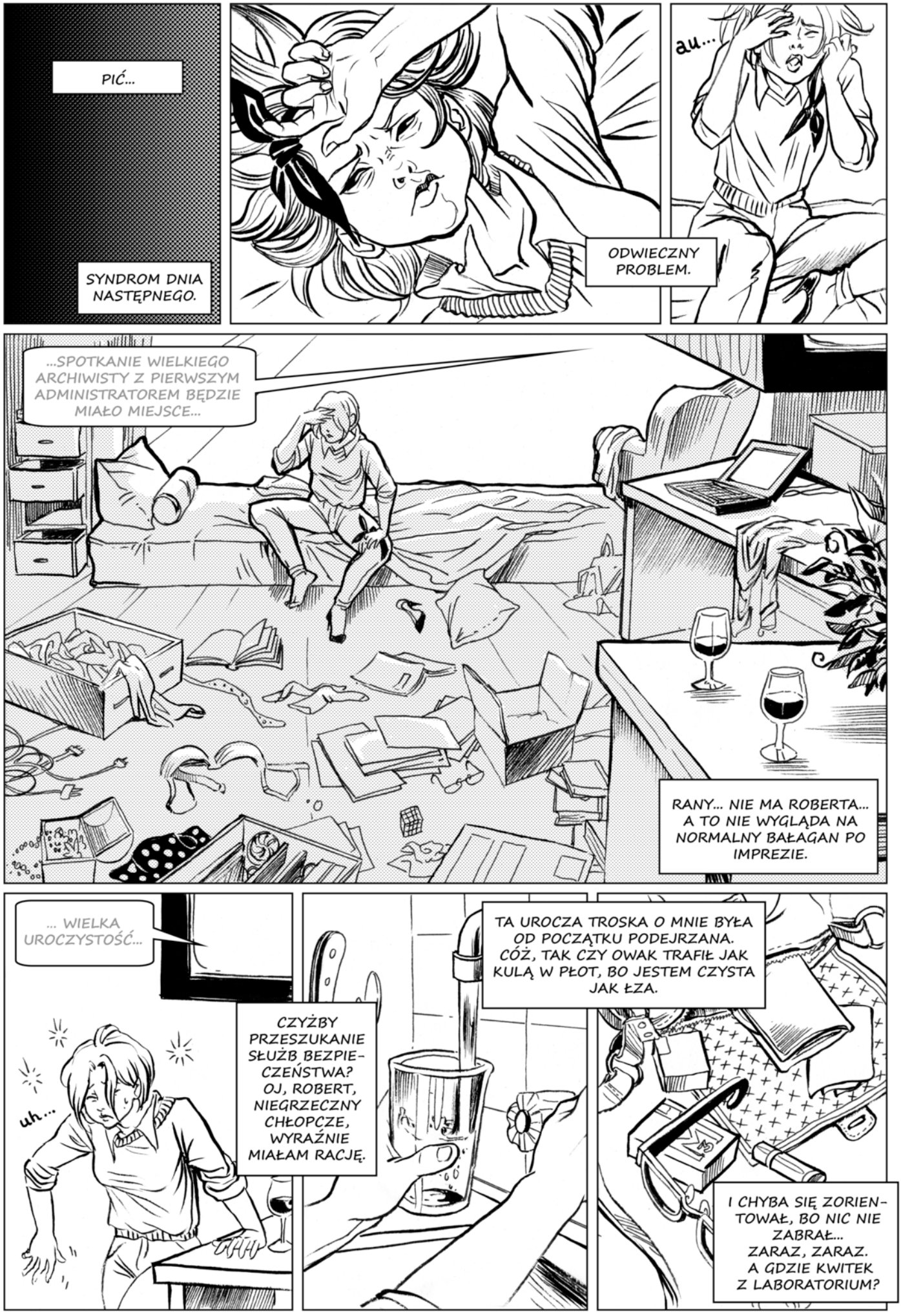

ZDJĘCIE DOWODU
WIESZ JUŻ COŚ WIĘCEJ O TYM ZABÓJSTWIE Z TANOTH?
WŁAŚNIE PRZEBIJAMY SIĘ PRZEZ ANALIZĘ MIEJSCA ZBRODNI, LABORATORIUM JEST W TRAKCIE SEKCJI.
PODRZUCĘ CI WYNIKI, JAK TYLKO BĘDZIEMY MIELI JE ZEBRANE W RAPORT.
POWIEDZMY, OOO... SZÓSTEJ?
BĘDĘ WDZIĘCZNA, ROBERCIE.
CO ZA TROSKLIWOŚĆ. W SUMIE NAWET MIŁE.
KILKA GODZIN PÓŹNIEJ...
CHCE PRZYJŚĆ OSOBIŚCIE, WIĘC ZAPEWNE WIEŚCI NIE SĄ NAJLEPSZE. ZRESZTĄ CZEGO TU OCZEKIWAĆ – OBAJ NIEDOSZLI CYNGLE NIE ŻYJĄ.
QUBIT, ZŁAŹ ZE STOŁU
ODERWIJ SIĘ OD ZIEMI I JEJ PROBLEMÓW W NOWYM „SKY-FLIGHT"! TEN CAŁKOWICIE ZATWIERDZONY PRZEZ CERBERA PRODUKT...


OCHO, PUNKTUALNY JAK DO URZĘDU.
KWIATKI? SERIO?
NIE MAM DOŚWIADCZENIA, NIE WIEM, CO SIĘ PRZYNOSI REKONWALESCENTOM.
DOSTAŁAM JEDNEGO KOPNIAKA!
ATAWIZM, PAMIĘTASZ?
KAWA! DZIĘKI!
COŚ ZA COŚ.
DAWAJ WYNIKI ŚLEDZTWA.
JEST ZDENERWOWANY. CIEKAWE, CO ODKRYLI.
KIEDY GO ZNALAZŁAŚ
TWÓJ KONTAKT, PHILIP JONAS, NIE ŻYŁ PRAWDOPODOBNIE OD GODZINY.
ŚLADY NA CIELE WSKAZUJĄ, ŻE PRZED ŚMIERCIĄ BYŁ TORTUROWANY. NIE WIEMY CZEMU.
PRZY TYCH DWÓCH, NA KTÓRYCH TRAFIŁAŚ, NIE ZNALEŹLIŚMY NICZEGO, CO MÓGŁBY IM DAĆ.
JEDNAK SKORO BYŁ INFORMATOREM, MÓGŁ COŚ WIEDZIEĆ.
TRUDNO POWIEDZIEĆ CO, ALE...
LICZYŁAM NA INFORMACJE O ALICE.
O TYM ZAMACHU, KTÓRY NIE BYŁ ZAMACHEM.
WSZYSTKO W PORZĄDKU?
NIE.
W SUMIE – NIC, CO POWIEM, JUŻ MU NIE ZASZKODZI. NIE ŻYJE.


TO BYŁ... PRZYJACIEL. RAZEM BYLIŚMY W ALICE. I RAZEM STAMTĄD ODESZLIŚMY.
TYLKO JA TRAFIŁAM DO CERBERA, A ON PRZESTAŁ SIĘ ANGAŻOWAĆ W TEN KONFLIKT. NIE ZGADZAŁ SIĘ Z ŻADNĄ ZE STRON.
ZACHOWALIŚMY WEJŚCIA DO SIECI ALICE I SKRZYNKĘ, ŻEBY MÓC UTRZYMYWAĆ KONTAKT.
UŻYŁAM JEJ PO RAZ PIERWSZY DOPIERO W TYM ŚLEDZTWIE.
ROZUMIEM.
NIE ROZUMIESZ.
BYŁAŚ OFIARĄ ATAKU, O MAŁO NIE ZGINĘŁAŚ, ALE KIEDY ZADZWONIŁEM, ZAPYTAŁAŚ O ZABÓJSTWO W TANOTH. TO BYŁO DLA CIEBIE WAŻNIEJSZE.
MYŚLĘ WIĘC, ŻE JAKIŚ TAM OBRAZ SYTUACJI MAM...
ZDECYDOWANIE NIE POWINNAM SIĘ TAK ODSŁANIAĆ.
WINA?
CZEMU NIE?
BO TO GŁUPI POMYSŁ. ALE Z DRUGIEJ STRONY – CO GORSZEGO MOŻE SIĘ STAĆ?
ZA CIEBIE, PHIL. TERAZ MUSZĘ CIĘ OPŁAKAĆ. POTEM PRZYJDZIE CZAS NA ZEMSTĘ.

ROZDZIAŁ IV

ROBERT


PIĆ...
SYNDROM DNIA NASTĘPNEGO.
au...
ODWIECZNY PROBLEM.
...SPOTKANIE WIELKIEGO ARCHIWISTY Z PIERWSZYM ADMINISTRATOREM BĘDZIE MIAŁO MIEJSCE...
RANY... NIE MA ROBERTA... A TO NIE WYGLĄDA NA NORMALNY BAŁAGAN PO IMPREZIE.
... WIELKA UROCZYSTOŚĆ...
uh...
CZYŻBY PRZESZUKANIE SŁUŻB BEZPIECZEŃSTWA? OJ, ROBERT, NIEGRZECZNY CHŁOPCZE, WYRAŹNIE MIAŁAM RACJĘ.
TA UROCZA TROSKA O MNIE BYŁA OD POCZĄTKU PODEJRZANA. CÓŻ, TAK CZY OWAK TRAFIŁ JAK KULĄ W PŁOT, BO JESTEM CZYSTA JAK ŁZA.
I CHYBA SIĘ ZORIENTOWAŁ, BO NIC NIE ZABRAŁ... ZARAZ, ZARAZ. A GDZIE KWITEK Z LABORATORIUM?


TYLKO PO CO MU KWITEK?
... SAM PIERWSZY ADMINISTRATOR ZDECYDOWAŁ SIĘ NIE ZAMYKAĆ CEREMONII POMIMO NIEDAWNEGO ATAKU...
ŻEBY MNIE OSKARŻYĆ O ZATAJENIE DOWODU?
BZDURA. TO ZA MAŁO, ŻEBY MI ZASZKODZIĆ.
Hsss...
CHYBA ŻE CHODZI...
... O COŚ...
... ZUPEŁNIE INNEGO.


MAM WRAŻENIE, ŻE PRZEOCZYLIŚMY COŚ ISTOTNEGO
SKĄD TA MINA? NIE PRZEPADASZ ZA TĄ ROBOTĄ?
TROCHĘ TAK, A TROCHĘ ZWYCZAJNIE BOLI MNIE GŁOWA. PRZEPRASZAM.
ACH, BAZY DANYCH WYDZIAŁU ŚLEDCZEGO, TAKIE UŻYTECZNE.
BYŁAM ŚLEPA.
UKRADŁAM MU KLUCZ DO SIECI.
PRZECIEŻ MAM CIĘ NADZOROWAĆ. TO CHYBA JASNE, ŻE POJECHAŁEM ZA TOBĄ.
WINA?
JEST ZDENERWOWANY, CIEKAWE CO UKRYWA.
A GDZIE KWITEK Z LABORATORIUM?


MOŻE JESZCZE NIE JEST ZA PÓŹNO. MOŻE JESZCZE MAM CZAS...
DZIEŃ DOBRY, PA...
ROBERT. TEN ŚLEDCZY, Z KTÓRYM PRACUJĘ.
BYŁ TU?
TA-AK. WŁAŚNIE SIĘ PANI Z NIM MINĘŁA. POJECHAŁ, ZDAJE SIĘ, DO BIUR.
ZABRAŁ TYLKO...
WIEM, CO ZABRAŁ.
I WIEM, DOKĄD JEDZIESZ.
hu hu hu
LĄDOWISKO. JEDYNE MIEJSCE POZA STREFĄ ZAKŁÓCANIA ŁĄCZNOŚCI.

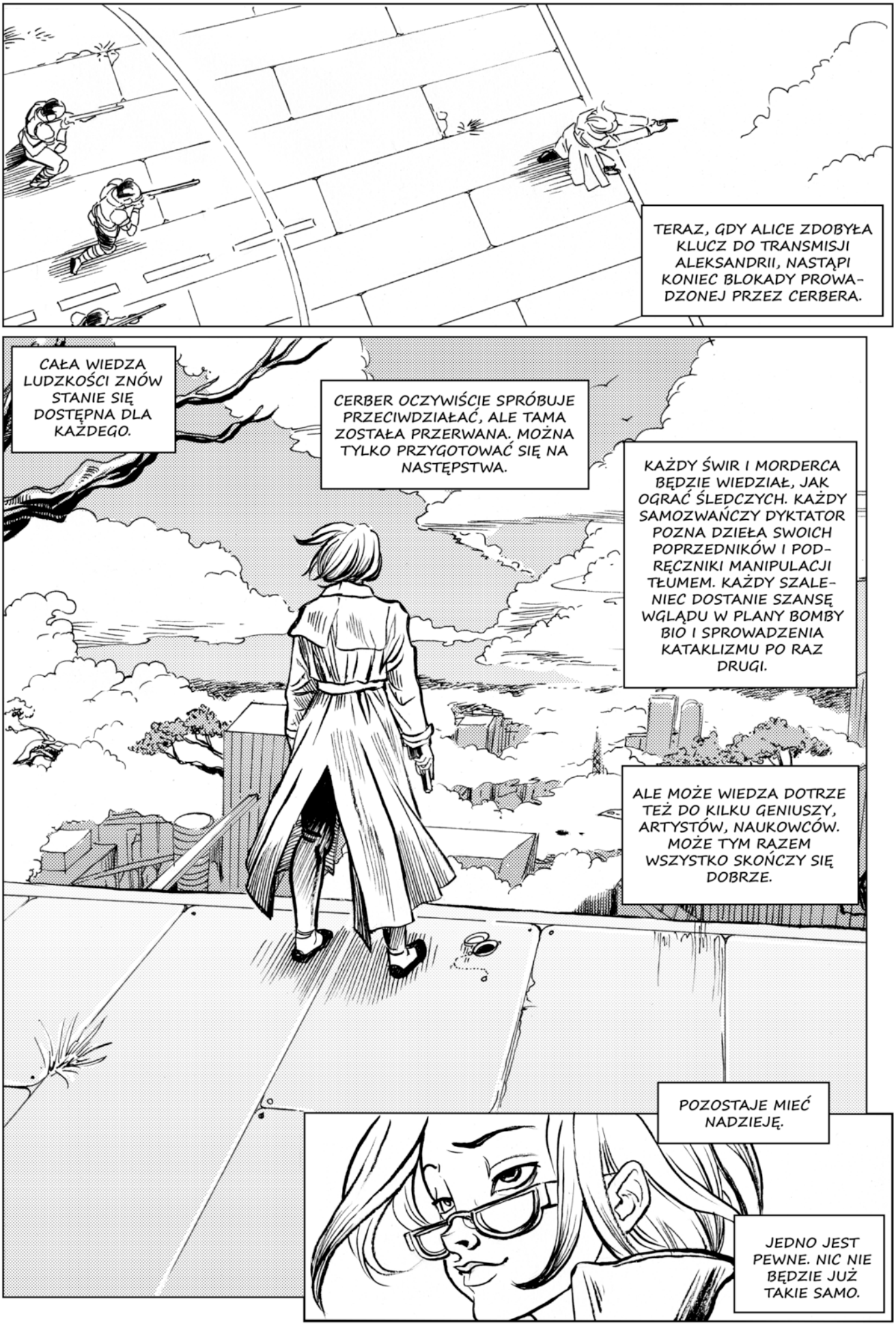

NA CO CZEKA? MOŻE JESZCZE NIE POSŁAŁ?
ROBERT!
W ZASADZIE WOLĘ „BOB"!
OD POCZĄTKU CHODZIŁO CI O TEN MEDALIK, PRAWDA?
DRUGA CZĘŚĆ DANYCH TELEPORTACJI KLUCZA PIERWSZEGO ADMINISTRATORA?
NAPRAWDĘ MUSISZ PYTAĆ?
NIE.
JAK ZAWSZE NAJSŁABSZYM PUNKTEM SYSTEMU OKAZALI SIĘ LUDZIE.


WIEDZIELISMY, ŻE PIERWSZY ADMINISTRATOR JEST PRÓŻNY.
UZNALIŚMY W ALICE, ŻE ATAK W CZASIE CEREMONII TO IDEALNA OKAZJA, ŻEBY WYKRAŚĆ KLUCZ I PODRZUCIĆ CERBEROWI FAŁSZYWY TROP – ZAMACH SZALEŃCA.
SPLĄTANE PAKIETY KUBITÓW, OBEJŚCIE BRAMEK DZIĘKI WYPALENIU INFORMACJI KLASYCZNEJ NA NIEPOZORNYM MEDALIKU...
PRZYZNAJĘ – BAŁEM SIĘ, ŻE SIĘ ZORIENTUJESZ, KIEDY U BRETTA ZROBIŁAŚ TO SAMO.
NIE WIEDZIAŁAM, ŻE TEN DEBIL, PIERWSZY ADMINISTRATOR, NOSI KLUCZ PRZY SOBIE.
DOPIERO DZISIAJ SIĘ POŁAPAŁAM.
TEŻ NIE MOGŁEM W TO UWIERZYĆ.
CÓŻ. TERAZ MA PUSTY KLUCZ.
OWSZEM. ALE NIE BYŁO LEKKO. DWA LATA PRZYGOTOWAŃ – A POCZĄTEK OPERACJI MAŁO ZACHĘCAJĄCY.
ATAK NA PIERWSZEGO ADMINISTRATORA WYGLĄDAŁ AUTENTYCZNIE.


ALE NIE UDAŁO SIĘ WYELIMINOWAĆ CIEBIE, BO PROCES NIE ZAKOŃCZYŁ SIĘ PRZED AKCJĄ – I CERBER NAGLE ZMIENIŁ ZDANIE CO DO SWOJEJ HAKERKI.
POTEM ZNIKNĄŁ MEDALIK, WIĘC NIE MOGLIŚMY DOKOŃCZYĆ ZADANIA ANI USTAWIĆ PHILIPA JAKO WROGA CERBERA.
DOPRAWDY, STRASZNE.
POCZĄTKOWO MYŚLAŁEM, ŻE TEN WISIOREK PO PROSTU ZGINĄŁ, ALE KIEDY TAK ROZPACZLIWIE ZACZĘŁAŚ SZUKAĆ PHILA...
TO TY GO ZABIŁEŚ?
ALICE UZNAŁA, ŻE TO JEDYNY SPOSÓB, ŻEBYŚ UZNAŁA, ŻE NIE MA SENSU DŁUŻEJ CHOWAĆ MEDALIKA. BYŁEM PRZECIWNY TEMU ROZWIĄZANIU. NIE MUSISZ MI WIERZYĆ.
TO PROSTE PYTANIE.
NIE. I NAPRAWDĘ CHOLERNIE MI PRZYKRO.


JASNE.
CO TERAZ?
krok
NIE POZWOLĘ CI NICZEGO WYSŁAĆ.
ŻARTUJESZ CHYBA.
PRZEKAZAŁEM DANE JESZCZE ZANIM ZAMIENILIŚMY CHOĆ SŁOWO.
ZBYT CIĘ SZANUJĘ, ŻEBY Z TYM CZEKAĆ.
dzyń
Krok


I NA TYM, OBAWIAM SIĘ, MOJA ROLA SIĘ KOŃCZY.
DO ZOBACZENIA W NOWYM ŚWIECIE!
Fuu...
ROBERT!
BUM
BUM


TERAZ, GDY ALICE ZDOBYŁA KLUCZ DO TRANSMISJI ALEKSANDRII, NASTĄPI KONIEC BLOKADY PROWADZONEJ PRZEZ CERBERA.
CAŁA WIEDZA LUDZKOŚCI ZNÓW STANIE SIĘ DOSTĘPNA DLA KAŻDEGO.
CERBER OCZYWIŚCIE SPRÓBUJE PRZECIWDZIAŁAĆ, ALE TAMA ZOSTAŁA PRZERWANA. MOŻNA TYLKO PRZYGOTOWAĆ SIĘ NA NASTĘPSTWA.
KAŻDY ŚWIR I MORDERCA BĘDZIE WIEDZIAŁ, JAK OGRAĆ ŚLEDCZYCH. KAŻDY SAMOZWAŃCZY DYKTATOR POZNA DZIEŁA SWOICH POPRZEDNIKÓW I PODRĘCZNIKI MANIPULACJI TŁUMEM. KAŻDY SZALEŃIEC DOSTANIE SZANSĘ WGLĄDU W PLANY BOMBY BIO I SPROWADZENIA KATAKLIZMU PO RAZ DRUGI.
ALE MOŻE WIEDZA DOTRZE TEŻ DO KILKU GENIUSZY, ARTYSTÓW, NAUKOWCÓW. MOŻE TYM RAZEM WSZYSTKO SKOŃCZY SIĘ DOBRZE.
POZOSTAJE MIEĆ NADZIEJĘ.
JEDNO JEST PEWNE. NIC NIE BĘDZIE JUŻ TAKIE SAMO.

Część II

Informatyka kwantowa

Rozdział 5

Wstęp

Dlaczego?

Kiedy byłem uczniem liceum, czytałem wiele tekstów popularnonaukowych. Niektóre z nich rozumiałem, niektóre – nie. Jednak jeśli dany tekst dotyczył mechaniki kwantowej – nigdy nie zdarzyło się, żebym go zrozumiał. Od tamtego czasu minęło kilkanaście lat, z których większość spędziłem na zgłębianiu tematu informatyki kwantowej. Jednakże kiedy dziś czytam tekst popularyzatorski poświęcony mechanice lub informatyce kwantowej... Nadal go nie rozumiem. A to dlatego, że – parafrazując Galileusza –

„*Natura jest pisana językiem matematyki*",

a publikacje popularnonaukowe... No cóż, językiem potocznym. Dlatego, drogi Czytelniku, postanowiłem trzymać się Galileuszowej maksymy i zamiast decydować się na popularyzatorski styl – przedstawić w niniejszej książce pewną minimalną ilość wiedzy matematycznej i fizycznej, która pozwoli Ci zrozumieć podstawy mechaniki i informatyki kwantowej.

Dla kogo?

Poniższa książka jest przeznaczona dla młodych ludzi zainteresowanych matematyką, fizyką i informatyką. Od Czytelnika wymagam zatem znajomości zagadnień matematycznych na poziomie programu liceum ogólnokształcącego – szczególnie notacji matematycznej i prostych zdolności rachunkowych. Podsumowując: jeżeli potrafisz dokonywać operacji na liczbach rzeczywistych, rozumiesz pojęcie układu współrzędnych, znasz podstawy trygonometrii i elementarne pojęcia rachunku prawdopodobieństwa, to bez większego problemu poradzisz sobie ze zrozumieniem treści, które tu przedstawię.

Co, gdzie, jak?

Celem tego tekstu jest dostarczenie Ci, Czytelniku, narzędzi niezbędnych do zrozumienia podstaw informatyki kwantowej. Narzędzia, o jakich tu mowa, to podstawowe definicje i struktury matematyczne, których – choćby elementarne – zrozumienie jest niezbędne, by osiągnąć założony cel. Pozwoli Ci to zyskać pewną intuicję dotyczącą mechaniki kwantowej. Mam nadzieję, że po przeczytaniu tej książki będziesz w stanie zrozumieć rachunek matematyczny opisujący zjawisko teleportacji kwantowej, kwantowej dystrybucji klucza oraz prostą grę kwantową.

Niniejsza książka składa się z czterech głównych części:

- tego wstępu,
- wprowadzenia do podstaw mechaniki kwantowej,
- rozdziału o informatyce kwantowej
- oraz dodatku matematycznego.

Materiał zawarty w dodatku matematycznym przedstawiony został w sposób uproszczony, co oznacza, że pozwoliłem sobie pominąć w nim wiele ważnych dla matematyka szczegółów. Jednakże zawarta w nim wiedza matematyczna wystarczy, aby wykonywać podstawowe obliczenia informatyki kwantowej. Slang matematyczny, którego używam w tekście, wywodzi się z języka opisu mechaniki kwantowej i przez to może nieco różnić się od języka, którego zwykle używają matematycy – dlatego też na końcu książki znajdziesz skorowidz.

Podziękowania

Podziękowania należą się moim współautorom: rysowniczce Katarzynie Karze, bez której talentu artystycznego to dzieło nie mogłoby powstać, oraz pisarzowi i scenarzyście Michałowi Cholewie, twórcy trzymającej w napięciu fabuły. Dziękuję też tutaj instytucjom, które wsparły nasz projekt finansowo i organizacyjnie: Fundacji na rzecz Nauki Polskiej oraz Instytutowi Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk; i wreszcie – organizatorom konwentów Polcon 2015, Imladris 2015, Falkon 2015, Liskon 2016 oraz Dni Fantastyki 2016, dzięki których uprzejmości mieliśmy przyjemność wygłosić na tych imprezach prelekcje na temat projektu „Rewolucja stanu”.

Piotr Gawron

Rozdział 6

Mechanika kwantowa

Mechanika kwantowa opisuje zachowania bardzo małych cząstek fizycznych, czyli np. fotonów lub elektronów albo kwantowych bitów – qubitów[1]. Na potrzeby niniejszej książki przyjmiemy, że nie będą nas interesować ich właściwości fizyczne, a tylko pewne abstrakcyjne stany, w jakich mogą się znajdować. Stany te numerujemy zazwyczaj przy użyciu liczb naturalnych: 0, 1, 2 itd. Mogą one opisywać polaryzację fotonu, energię elektronu na orbicie atomu, drgania sieci krystalicznej lub jeszcze inne właściwości układów kwantowych.

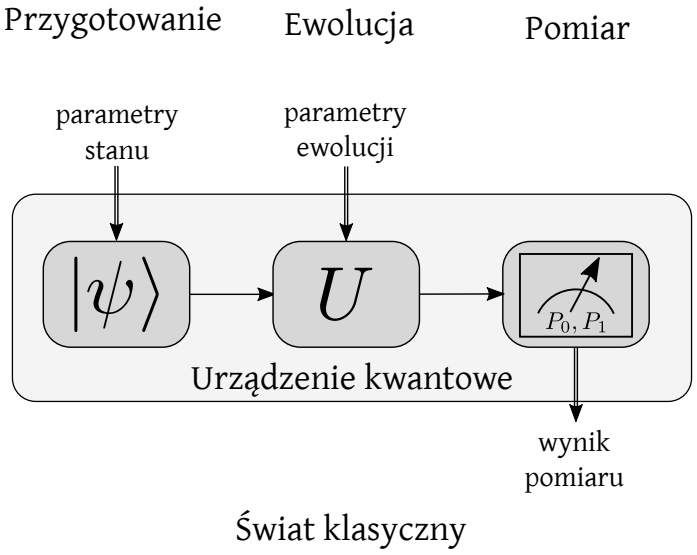
Informatyków często nie interesuje, w jaki sposób właściwości fizyczne układów są wykorzystywane do zapisu informacji klasycznej w komputerze klasycznym – a zauważmy, że do tego celu może zostać wykorzystana magnetyzacja powierzchni na talerzu dysku twardego, napięcie elektryczne w obwodzie w procesorze czy wartość prądu w przewodzie elektrycznym. Dlatego też informatyków kwantowych nie musi interesować, w jaki sposób informacja kwantowa jest fizycznie zapisana w komputerze kwantowym.

Gdy mówimy o mechanice kwantowej, a zatem również o informatyce kwantowej, posługujemy się fizycznym pojęciem *doświadczenia*. Doświadczenie – w znaczeniu, jakie będziemy nadawać mu w niniejszym tekście – składa się z trzech etapów:

- przygotowania,
- ewolucji,
- pomiaru i interpretacji wyników.

W interesującym nas kontekście możemy opisać poszczególne etapy doświadczenia następująco: przygotowujemy stan kwantowy, dokonujemy ewolucji kwantowej tego stanu i – na koniec – dokonujemy pomiaru kwantowego (patrz: Rysunek 6.1).

[1]Przez niektórych autorów określanych spolszczoną nazwą kubitów.



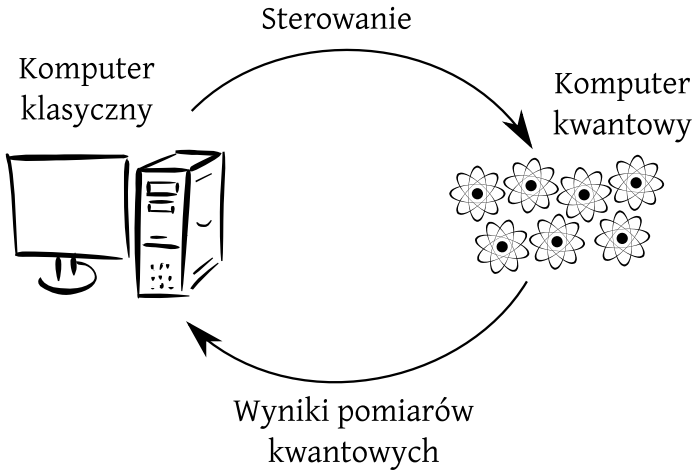
Rysunek 6.1: Schematyczna reprezentacja doświadczenia kwantowego.

Zauważmy, że w podobny sposób wykonujemy w informatyce obliczenia klasyczne: przygotowujemy dane (stan początkowy); następnie wykonujemy program (ewolucja) i odczytujemy wynik (pomiar). Współczesne komputery wykonują te trzy etapy jako przeprowadzane nieustannie obliczenia. Nie obserwujemy tych etapów podczas codziennych interakcji z komputerem, więc nie zauważamy w sposób świadomy powyższego schematu działania.

Każde urządzenie informatyczne działające w oparciu o zasady informatyki kwantowej – lub, w skrócie, komputer kwantowy – musi być wyposażone zarówno w podukład kwantowy, jak i podukład klasyczny, czyli jakąś formę komputera klasycznego, np. elektronicznego. Komputer klasyczny będzie w takim urządzeniu odpowiadał za sterowanie układem kwantowym, komunikację ze światem zewnętrznym oraz interpretację wyników działania komputera kwantowego. Schemat konstrukcji i działania komputera kwantowego sprzężonego z komputerem klasycznym przedstawiono na Rysunku 6.2.

W przypadku bardziej złożonym – kiedy chcemy opisać sieć komputerów kwantowych i jej wykorzystanie – mówimy zazwyczaj również o użytkownikach tej sieci, którzy mają do dyspozycji komputery kwantowe i klasyczne oraz kwantowe i klasyczne połączenia sieciowe. Na potrzeby opisu w literaturze przedmiotu nadaje im się umowne imiona: „Alicja" (użytkownik A), „Bob" (użytkownik B) oraz „Ewa" (podsłuchujący)[2]. Dwie pierwsze osoby próbują się komunikować, a ostatnia próbuje im w tym przeszkodzić. Nietrudno zauważyć, że w komiksie dość swobodnie nawiązujemy do tej konwencji.

[2]Po angielsku – odpowiednio „Alice", „Bob" i „Eve". Imiona „Alice" i „Bob" są używane, bo można je oznaczyć literami A i B. Natomiast „Eve" pochodzi od angielskiego słowa *eavesdropping*, czyli podsłuchiwanie.



Rysunek 6.2: Schematyczna reprezentacja działania kwantowego urządzenia informatycznego. Komputer klasyczny steruje komputerem kwantowym, komputer kwantowy zwraca wyniki pomiarów do komputera klasycznego.

6.1 Formalizm matematyczny

Mechanika kwantowa jest opisywana przy pomocy formalizmu (języka) matematycznego, który wykorzystuje liczby zespolone, wektory oraz macierze. Bez jego zrozumienia nie jest zatem możliwe zrozumienie samej mechaniki kwantowej. Jednakże w niniejszej książce najpierw skupimy się na przedstawieniu pojęć ściśle związanych z mechaniką i informatyką kwantową; natomiast opis formalizmu matematycznego znajduje się w Dodatku zamieszczonym na końcu. Uznałem bowiem, że nie chcę Cię, Czytelniku, zmuszać do nauki materiału matematycznego, skoro jeszcze nie znasz powodów, dla których opanowanie tego formalizmu jest Ci niezbędne. Oczywiście można zacząć od lektury Dodatku – a jeśli się na nią nie zdecydujesz, zachęcam do zerkania do niego, ilekroć nie będziesz rozumieć jakiegoś pojęcia lub symbolu matematycznego.

6.2 Stan

Stanem w mechanice kwantowej nazywamy wektor

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix},$$

który możemy zapisać również w bazie obliczeniowej w postaci

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{n-1} |n-1\rangle .$$

Chcemy, aby $\alpha_i \in \mathbb{C}$ dla $i = 0, 1, \ldots, n-1$, tzn. współczynniki wektora, były liczbami zespolonymi oraz aby $\||\psi\rangle\| = |\alpha_0|^2 + |\alpha_1|^2 + \ldots + |\alpha_{n-1}|^2 = 1$, tzn. aby norma euklidesowa wektora wynosiła 1.

Liczby $\alpha_i \in \mathbb{C}$ nazywamy *amplitudami prawdopodobieństwa* stanu kwantowego. Gdy jedna z tych liczb jest równa 1, możemy powiedzieć – nieformalnie – że układ kwantowy jest w stanie odpowiadającym tej liczbie. Na przykład jeżeli $\alpha_0 = 1$, mówimy, że układ kwantowy jest w stanie $|0\rangle$.

Jeżeli żadna z liczb α_i nie jest równa 1, to znaczy, że przynajmniej dwie amplitudy prawdopodobieństwa są niezerowe. Wówczas mówimy, że układ jest w *superpozycji* stanów. Przykładowo: jeżeli mamy układ z $n = 3$ i $\alpha_0 = \alpha_2 = 1/\sqrt{2}$, tzn. nasz stan zapisujemy jako $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|2\rangle$, to mówimy, że stan jest w superpozycji stanu $|0\rangle$ oraz $|2\rangle$.

6.3 Qubit

Elementarnym obiektem w informatyce kwantowej jest *qubit*, który jest najprostszym układem kwantowym. Stan qubitu opisuje wektor o dwóch elementach zespolonych.

W celu opisania stanu qubitu zwyczajowo wybieramy bazę obliczeniową:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Wówczas dowolny stan $|\psi\rangle$ qubitu tworzy liniową kombinację wektorów bazowych

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

z $|\alpha|^2 + |\beta|^2 = 1$ oraz $\alpha, \beta \in \mathbb{C}$.

Liczby α i β są zespolone, zatem aby je zapisać, potrzebujemy czterech liczb rzeczywistych. Jednak ponieważ zachodzi warunek $|\alpha|^2 + |\beta|^2 = 1$, jedną z potrzebnych nam liczb możemy wyliczyć z pozostałych trzech. Wynika z tego, iż dowolny stan qubitu może być opisany przez trzy liczby rzeczywiste. Taki przykładowy opis jest zadany równaniem

$$|\psi\rangle = e^{\mathrm{i}\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{\mathrm{i}\phi}\sin\frac{\theta}{2}\,|1\rangle\right),$$

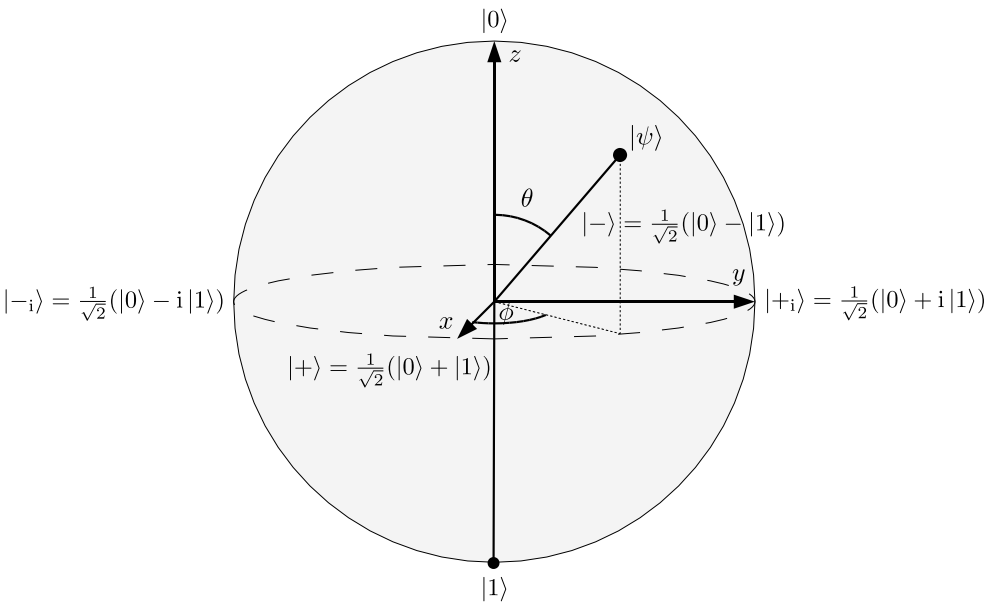
gdzie $\gamma, \theta, \phi \in \mathbb{R}$. Współczynnik $e^{\mathrm{i}\gamma}$ nazywamy *fazą globalną*. Jak się później przekonamy, nie ma on większego znaczenia, więc zawsze możemy przyjmować, że równa się on 1, czyli $\gamma = 0$. Zatem w efekcie dostajemy taką oto postać wzoru stanu qubitu:

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{\mathrm{i}\phi}\sin\frac{\theta}{2}\,|1\rangle\,.$$

Liczby rzeczywiste θ i ϕ mogą być interpretowane jako współrzędne punktu na trójwymiarowej sferze o promieniu 1. Sferę taką nazywamy *sferą Blocha*. Będziemy ją bardzo często wykorzystywać do wizualizacji operacji na qubicie.

Jeżeli dwa stany różnią się o fazę globalną, to fizycznie te stany są takie same. Zatem każdy stan możemy również pomnożyć przez dowolną liczbę w postaci $e^{\mathrm{i}\gamma}$, nie zmieniając tego stanu.

Sfera Blocha



Rysunek 6.3: Sfera Blocha.

Sfera Blocha[3] (Rysunek 6.3) jest wygodną reprezentacją graficzną qubitu. Zazwyczaj rysujemy ją w taki sposób, że stan $|0\rangle$ oznaczamy u góry, stan $|1\rangle$ u dołu, $|-_{\mathrm{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}\,|1\rangle)$ po lewej stronie, $|+_{\mathrm{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}\,|1\rangle)$ – po prawej, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ z przodu, a $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ z tyłu.

W dalszej części tekstu zostanie opisane, w jaki sposób bramki kwantowe działają na qubit – a odwzorowania zostaną zaprezentowane właśnie na sferze Blocha.

[3]Od nazwiska fizyka Feliksa Blocha.

6.4 Stany wielosystemowe

Dwa qubity

Operacją matematyczną, która odpowiada złączeniu układów dwóch qubitów, jest iloczyn Kroneckera. Jeśli dane są stany dwóch qubitów $|\psi\rangle$ i $|\phi\rangle$:

$$|\psi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle\,, |\phi\rangle = \begin{bmatrix}\gamma\\ \delta\end{bmatrix} = \gamma\,|0\rangle + \delta\,|1\rangle\,,$$

to ich łączny stan zapisujemy następująco:

$$|\psi\rangle \otimes |\phi\rangle = \begin{bmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{bmatrix} = \alpha\gamma\,|0\rangle \otimes |0\rangle + \alpha\delta\,|0\rangle \otimes |1\rangle + \beta\gamma\,|1\rangle \otimes |0\rangle + \beta\delta\,|1\rangle \otimes |1\rangle\,,$$

bądź w skrócie:

$$|\psi\phi\rangle = \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle\,.$$

Jak widać, etykiety 00, 01, 10 oraz 11 odpowiadają liczbom 0, 1, 2 oraz 3 zapisanym binarnie. Zatem stan $|\psi\phi\rangle$ możemy zapisać jako:

$$|\psi\phi\rangle = \alpha\gamma\,|0\rangle + \alpha\delta\,|1\rangle + \beta\gamma\,|2\rangle + \beta\delta\,|3\rangle\,.$$

Zapiszmy teraz nowy stan:

$$|\Phi\rangle = c_0\,|0\rangle + c_1\,|1\rangle + c_2\,|2\rangle + c_3\,|3\rangle$$

i zastanówmy się, czy istnieją takie liczby c_0, c_1, c_2, c_3, dla których nie da się znaleźć takich $\alpha, \beta, \gamma, \delta$, które spełniają układ równań

$$c_0 = \alpha\gamma,\ c_1 = \alpha\delta,\ c_2 = \beta\gamma,\ \text{oraz}\ c_3 = \beta\delta.$$

Weźmy pod uwagę stan $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |3\rangle)$ i dla uproszczenia opuśćmy czynnik $\frac{1}{\sqrt{2}}$. Wtedy mamy $c_0 = c_3 = 1$ oraz $c_1 = c_2 = 0$. Załóżmy, że nasz stan możemy zapisać w postaci $\alpha\gamma\,|0\rangle + \alpha\delta\,|1\rangle + \beta\gamma\,|2\rangle + \beta\delta\,|3\rangle$. Wówczas uzyskujemy układ równań:

$$\alpha\gamma = 1,\ \alpha\delta = 0,\ \beta\gamma = 0,\ \beta\delta = 1.$$

Zauważmy, że $\alpha, \beta, \gamma, \delta \geqslant 0$, co wynika z tego, że $|\alpha|^2 + |\beta|^2 = 1$ oraz $|\delta|^2 + |\gamma|^2 = 1$. Zatem aby spełnić pierwszy warunek $\alpha = \gamma = 1$; aby spełnić drugi warunek $\delta = 0$. Jednakże z czwartego warunku wynika, że $\delta = 1$. Zatem otrzymujemy sprzeczność. Wnioskujemy z tego, że stanu $\left|\Phi^+\right\rangle$ nie da się zapisać jako iloczynu Kroneckera dwóch stanów. Stan $\left|\Phi^+\right\rangle$ nazywamy *stanem Bella*[4]. Ma on wyjątkowo istotne znaczenie w informatyce kwantowej.

[4]Od nazwiska fizyka Johna S. Bella.

Wiele układów kwantowych

Gdy mamy do dyspozycji n układów kwantowych w stanach

$$|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle,$$

każdy o jakimś dowolnym wymiarze $d_1, d_2, \ldots, d_n$, wówczas możemy opisać je jako jeden łączny układ, którego stan ma $d_1 \times d_2 \times \cdots \times d_n$ współczynników. Operacją matematyczną, która w sposób zbiorczy opisuje takie połączenie wielu układów, jest iloczyn Kroneckera. Jeżeli układy nie są ze sobą związane (splątane), to stan takiego układu jest opisany przez łączny stan

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle.$$

Splątanie kwantowe

Splątanie kwantowe jest zjawiskiem, które dotyczy tylko i wyłącznie obiektów podlegających prawom mechaniki kwantowej. Dwa lub więcej układów, które miały okazję ze sobą oddziaływać w przeszłości, może być splątane. Matematycznie definicja splątania dwóch układów jest następująca: jeżeli danego stanu $|\phi\rangle$, który opisuje stan dwóch układów, nie możemy zapisać jako $|\psi_1\rangle \otimes |\psi_2\rangle$ dla jakichkolwiek $|\psi_1\rangle$ oraz $|\psi_2\rangle$, to jest on *splątany*. Jeżeli natomiast istnieją takie $|\psi_1\rangle$ oraz $|\psi_2\rangle$, że $|\phi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, to stan nazywamy *separowalnym*. Jak widać, wspomniany wcześniej stan Bella $|\Phi^+\rangle$ jest stanem splątanym.

Splątanie wielu układów kwantowych jest problemem znacznie bardziej złożonym. Jeżeli mamy np. trzy układy, to pierwsze dwa mogą być splątane ze sobą, ale nie z trzecim, jak na przykład w stanie

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |1\rangle.$$

Wszystkie trzy układy mogą być ze sobą splątane na różne sposoby. Przykładowo stany

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

oraz

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

są splątane w całkowicie różny sposób – przy czym wytłumaczenie tego faktu wykracza poza zakres tej książki.

Stany splątane mają bardzo nieintuicyjne właściwości. Nawet jeżeli cząstki będące w stanie splątanym są bardzo odległe od siebie, nadal pozostają ze sobą związane. Będziemy mieli okazję zaobserwować ten efekt, gdy będzie mowa o pomiarze stanów splątanych.

6.5 Ewolucja kwantowa

Ewolucja kwantowa to nazwa, którą opisujemy zmianę stanu kwantowego w czasie. Zakładamy, że mamy pewien stan w chwili 0, a dzięki ewolucji kwantowej uzyskujemy stan w chwili 1. Zwróćmy tutaj uwagę na pewien fakt dotyczący stanów kwantowych: norma stanu kwantowego wynosi zawsze 1. Normę tę utożsamiamy z prawdopodobieństwem całkowitym. Zatem jeżeli chcemy, by prawdopodobieństwo całkowite było zachowane, oznacza to, że chcemy, by matematyczny opis ewolucji zachowywał normę wektora stanu. Norma wektora jest zachowywana wyłącznie przez obroty i symetrie. Taki opis matematyczny ewolucji dają nam macierze unitarne. Dla uproszczenia opisu pomijamy tutaj kwestię wymiarów macierzy i wektorów stanów. Oczywiście wymiary muszą być tak dobrane, by można było mnożyć odpowiadające sobie nawzajem wymiarami macierze i wektory.

Przejście ze stanu w chwili 0 $|\psi_{t=0}\rangle$ do stanu w chwili 1 $|\psi_{t=1}\rangle$ jest zadane przez $|\psi_{t=1}\rangle = \mathbf{U}\,|\psi_{t=0}\rangle$, gdzie $\mathbf{U}$ jest macierzą unitarną.

Powyższe, pozornie trywialne, równanie opisuje zachowanie wszystkich układów kwantowomechanicznych, w tym oczywiście komputerów kwantowych. W informatyce kwantowej macierze unitarne przeważnie nazywamy *bramkami kwantowymi*.

Zauważmy od razu pewną charakterystyczną cechę mechaniki kwantowej, wynikającą z powyższego równania: pamiętając, że macierz odwrotna $\mathbf{U}^{-1}$ do macierzy unitarnej zawsze istnieje i jest jej sprzężeniem hermitowskim $\mathbf{U}^{\dagger}$, możemy zapisać to równanie odwrócone w czasie: $|\psi_{t=0}\rangle = \mathbf{U}^{\dagger}\,|\psi_{t=1}\rangle$. Dlatego też mówimy, że ewolucja kwantowa jest *odwracalna w czasie*.

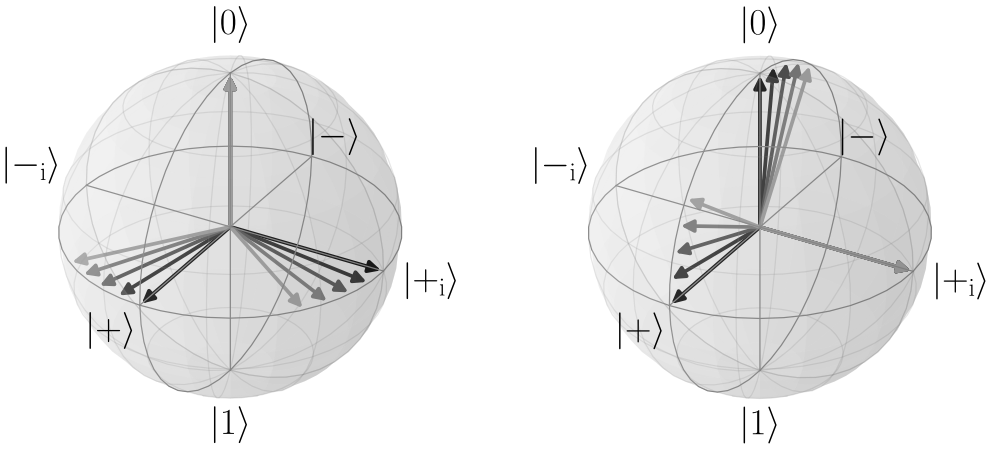
6.6 Bramki kwantowe

Bramek kwantowych jest nieskończenie wiele – jednakże my, mimo ich mnogości, skupimy się tylko na bramkach działających na jeden lub dwa qubity. Bramki te wystarczają do tego, by zbudować dowolny komputer kwantowy lub kwantowe urządzenie komunikacyjne. Są one zatem najciekawsze z punktu widzenia informatyka kwantowego.

Bramki jednoqubitowe

Dla jednego qubitu możemy zapisać wiele różnych bramek kwantowych. Na początek zdefiniujmy bramkę obrotu wokół osi y o kąt γ:

$$\mathbf{R_y}(\gamma) = \begin{bmatrix} \cos(\frac{\gamma}{2}) & \sin(\frac{\gamma}{2}) \\ -\sin(\frac{\gamma}{2}) & \cos(\frac{\gamma}{2}) \end{bmatrix},$$



(a) Bramka $\mathbf{R_z}(\beta)$ dokonująca obrotu wokół osi z łączącej $|0\rangle$ z $|1\rangle$.

(b) Bramka $\mathbf{R_y}(\gamma)$ dokonująca obrotu wokół osi y łączącej $|+_{\mathrm{i}}\rangle$ z $|-_{\mathrm{i}}\rangle$.

Rysunek 6.4: Działanie bramek $\mathbf{R_z}(\beta)$ – panel (a) oraz $\mathbf{R_y}(\gamma)$ – panel (b) na stanach $|0\rangle$, $|+\rangle$, $|+_{\mathrm{i}}\rangle$ (czarne strzałki). Wartości β oraz γ rosną zgodnie z przechodzeniem kolorów strzałek od ciemniejszych do jaśniejszych i wynoszą $(0{,}05\pi, 0{,}1\pi, 0{,}15\pi, 0{,}2\pi)$.

bramkę obrotu wokół osi z o kąt β:

$$\mathbf{R_z}(\beta) = \begin{bmatrix} e^{\frac{\mathrm{i}\beta}{2}} & 0 \\ 0 & e^{\frac{-\mathrm{i}\beta}{2}} \end{bmatrix}$$

oraz bramkę zmieniającą fazę globalną o czynnik α:

$$\mathbf{Ph}(\alpha) = \begin{bmatrix} e^{\mathrm{i}\alpha} & 0 \\ 0 & e^{\mathrm{i}\alpha} \end{bmatrix}.$$

Działanie bramek $\mathbf{R_z}(\beta)$ oraz $\mathbf{R_y}(\gamma)$ zostało pokazane na Rysunku 6.4. Bramka $\mathbf{Ph}(\alpha)$ zmienia tylko globalną fazę, zatem nie można jej działania zaobserwować na sferze Blocha.

Dowolna bramka działająca na jednym qubicie może być zapisana jako złożenie czterech bramek: zmiany fazy oraz trzech obrotów, w postaci opisanej przez cztery liczby rzeczywiste $\alpha, \beta, \gamma, \delta$:

$$\begin{aligned}\mathbf{U}(\alpha,\beta,\gamma,\delta) =& \mathbf{Ph}(\alpha)\mathbf{R_z}(\beta)\mathbf{R_y}(\gamma)\mathbf{R_z}(\delta) = \\ =& \begin{bmatrix} e^{\mathrm{i}\alpha} & 0 \\ 0 & e^{\mathrm{i}\alpha} \end{bmatrix} \begin{bmatrix} e^{\frac{\mathrm{i}\beta}{2}} & 0 \\ 0 & e^{\frac{-\mathrm{i}\beta}{2}} \end{bmatrix} \begin{bmatrix} \cos\left(\frac{\gamma}{2}\right) & \sin\left(\frac{\gamma}{2}\right) \\ -\sin\left(\frac{\gamma}{2}\right) & \cos\left(\frac{\gamma}{2}\right) \end{bmatrix} \begin{bmatrix} e^{\frac{\mathrm{i}\delta}{2}} & 0 \\ 0 & e^{\frac{-\mathrm{i}\delta}{2}} \end{bmatrix}.\end{aligned}$$

Pierwszy obrót to obrót wokół osi z, drugi – wokół osi y, a trzeci – ponownie wokół z.

Bramki kwantowe mają swoje oznaczenia graficzne. Bramkę jednoqubitową oznacza się jako prostokąt, wewnątrz którego zapisana jest nazwa bramki. Przykład takiej bramki kwantowej jest pokazany na Rysunku 6.5.

Rysunek 6.5: Rysunek przedstawiający bramkę jednoqubitową **U**. Pojedyncza linia przechodząca przez bramkę oznacza qubit. Stan wejściowy do bramki – po lewej stronie, wyjściowy – po prawej.

Bramki jednoqubitowe

Kilka spośród wszystkich bramek kwantowych ma swoje ustalone nazwy, które są często wykorzystywane w informatyce kwantowej. Poniżej prezentujemy ich przegląd, zawierający informację o tym, jak wygląda macierz danej bramki, jak działa ona na ogólny stan $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, a także interpretację jej działania na sferze Blocha.

Bramka identyczność nie zmienia stanu qubitu. Oznaczamy ją przez **I**. Jej macierz zawiera jedynki na diagonali i zera poza diagonalą:

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Działanie identycznością na stan jest trywialne:

$$\mathbf{I}(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle.$$

Bramka negacji bitu oznaczana jest przez **X**. Jej macierz jest następująca:

$$\mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

a działanie polega na zamianie stanu $|0\rangle$ na $|1\rangle$ i odwrotnie. Zatem gdy te stany bazy obliczeniowej są w superpozycji, bramka **X** zamienia pomiędzy nimi amplitudy prawdopodobieństwa:

$$\mathbf{X}(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle.$$

Bramka negacji fazy, oznaczana przez **Y**, ma następującą postać macierzową:

$$\mathbf{Y} = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}.$$

Jej działanie polega na wzajemnej zamianie stanów $|+\rangle$ oraz $|-\rangle$. Jej działanie na superpozycję stanów bazy obliczeniowej jest następujące:

$$\mathbf{Y}(\alpha|0\rangle + \beta|1\rangle) = \alpha\mathrm{i}|1\rangle - \beta\mathrm{i}|0\rangle,$$

ale ponieważ możemy pomnożyć ten stan przez fazę globalną $\mathrm{i} = e^{\frac{\mathrm{i}\pi}{2}}$, nie zmieniając stanu, to otrzymujemy $\beta|0\rangle - \alpha|1\rangle$.

Bramka negacji fazy i bitu oznaczana jest przez $\mathbf{Z}$, a jej macierz jest następująca:

$$\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Bramka ta zamienia ze sobą stany $|+_\mathrm{i}\rangle$ oraz $|-_\mathrm{i}\rangle$. Jej działanie na superpozycji wektorów bazy obliczeniowej jest następujące:

$$\mathbf{Z}(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|0\rangle - \beta\,|1\rangle\,.$$

Zauważmy, że bramki $\mathbf{X}$, $\mathbf{Y}$ oraz $\mathbf{Z}$ mają ciekawą własność:

$$\mathbf{X}^2 = \mathbf{Y}^2 = \mathbf{Z}^2 = \mathrm{i}\mathbf{XYZ} = \mathbf{I}.$$

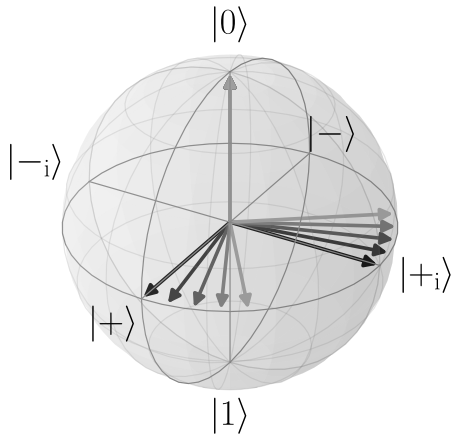
Bramki zmiany fazy to rodzina bramek $\mathbf{R}(\phi)$ zależnych od parametru rzeczywistego ϕ. Postać macierzowa tych bramek jest następująca:

$$\mathbf{R}(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathrm{i}\phi} \end{bmatrix}.$$

Ich działanie zmienia fazę względną pomiędzy stanami bazy obliczeniowej:

$$\mathbf{R}(\phi)(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|0\rangle + e^{\mathrm{i}\phi}\beta\,|1\rangle\,.$$

Rysunek 6.6 przedstawia działanie tej rodziny bramek.



Rysunek 6.6: Wizualizacja działania bramek $\mathbf{R}(\phi)$ na stanach $|0\rangle$, $|+\rangle$, $|+_\mathrm{i}\rangle$ (czarne strzałki). Wartości ϕ rosną w miarę rozjaśniania się kolorów strzałek i wynoszą $(0{,}05\pi, 0{,}1\pi, 0{,}15\pi, 0{,}2\pi)$.

Bramka Hadamarda jest oznaczana symbolem $\mathbf{H}$, a jej postać macierzowa jest następująca:

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Bramka ta jest często pierwszym krokiem wielu algorytmów i protokołów kwantowych, gdyż przeprowadza ona stany bazy obliczeniowej do ich superpozycji w następujący sposób:

$$\mathbf{H}\left|0\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right) = \left|+\right\rangle,$$
$$\mathbf{H}\left|1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right) = \left|-\right\rangle.$$

Bramki kontrolowane

W przypadku bramek dwuqubitowych możemy stworzyć bramki kontrolowane. O bramkach tych mówimy, iż jeden qubit kontroluje bramkę, a na drugi nakładana jest dana bramka $\mathbf{U}$. Bramka kontrolowana „kontrolowane $\mathbf{U}$" działa w następujący sposób: jeżeli qubit kontrolujący jest w stanie $|1\rangle$, to nałóż wybraną bramkę $\mathbf{U}$ na qubit docelowy; jeżeli qubit kontrolujący jest w stanie $|0\rangle$, to nie rób nic.

Bramkę taką możemy zapisać w postaci

$$\mathbf{CU}_1^2 = \left|0\right\rangle\!\left\langle 0\right| \otimes \mathbf{I} + \left|1\right\rangle\!\left\langle 1\right| \otimes \mathbf{U},$$

gdzie indeks dolny oznacza numer qubitu kontrolującego, a górny kontrolowanego. Jeżeli bramka $\mathbf{U}$ ma postać macierzową

$$\mathbf{U} = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix},$$

to kontrolowana bramka $\mathbf{U}$ ma postać

$$\mathbf{CU}_1^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix},$$

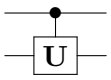
a jej działanie można zapisać jako:

$$\begin{aligned} \mathbf{CU}_1^2 \left|0\right\rangle \otimes \left|0\right\rangle &= \left|0\right\rangle \otimes \left|0\right\rangle, \\ \mathbf{CU}_1^2 \left|0\right\rangle \otimes \left|1\right\rangle &= \left|0\right\rangle \otimes \left|0\right\rangle, \\ \mathbf{CU}_1^2 \left|1\right\rangle \otimes \left|0\right\rangle &= \left|1\right\rangle \otimes \mathbf{U}\left|0\right\rangle, \\ \mathbf{CU}_1^2 \left|1\right\rangle \otimes \left|1\right\rangle &= \left|1\right\rangle \otimes \mathbf{U}\left|1\right\rangle. \end{aligned}$$

Na Rysunku 6.7 pokazana jest graficzna reprezentacja bramki „kontrolowane $\mathbf{U}$".

Jeżeli chcemy natomiast, by w bramce kontrolowanej qubit kontrolujący był drugi, a kontrolowany pierwszy, to możemy uzyskać taki efekt, korzystając z następującej postaci bramki:

$$\mathbf{CU}_2^1 = \mathbf{I} \otimes \left|0\right\rangle\!\left\langle 0\right| + \mathbf{U} \otimes \left|1\right\rangle\!\left\langle 1\right|.$$



Rysunek 6.7: Rysunek przedstawiający bramkę kontrolowaną **U**. Linie przechodzące przez bramkę oznaczają qubity. Kropka oznacza qubit kontrolujący, a kwadrat – bramkę, która jest kontrolowana.

Bramka CNOT

Jednym z bardzo użytecznych przykładów bramek kontrolowanych jest bramka „kontrolowane **X**", czyli $\mathbf{CNOT}_1^2$, która ma następującą postać macierzową:

$$\mathbf{CNOT}_1^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Działanie tej bramki można opisać następująco: jeżeli qubit kontrolowany jest w stanie $|0\rangle$, to zaneguj stan qubitu docelowego:

$$\begin{aligned} \mathbf{CNOT}_1^2 |0\rangle \otimes |0\rangle &= |0\rangle \otimes |0\rangle, \\ \mathbf{CNOT}_1^2 |0\rangle \otimes |1\rangle &= |0\rangle \otimes |1\rangle, \\ \mathbf{CNOT}_1^2 |1\rangle \otimes |0\rangle &= |1\rangle \otimes |1\rangle, \\ \mathbf{CNOT}_1^2 |1\rangle \otimes |1\rangle &= |1\rangle \otimes |0\rangle. \end{aligned}$$

Rysunek 6.8 pokazuje reprezentację graficzną tej bramki.

Rysunek 6.8: Rysunek przedstawiający bramkę $\mathbf{CNOT}_1^2$. Linia przechodząca przez bramkę oznacza qubity. Kropka oznacza qubit kontrolujący, a kółko z krzyżykiem – bramkę **X**.

Bramka SWAP

Bramka **SWAP** służy do zamiany stanów dwóch qubitów. Można ją zrealizować jako ciąg trzech bramek: $\mathbf{CNOT}_1^2\mathbf{CNOT}_2^1\mathbf{CNOT}_1^2$, tak jak to przedstawiono na Rysunku 6.9. Postać macierzowa bramki **SWAP** jest następująca:

$$\mathbf{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Rysunek 6.9: Rysunek po lewej przedstawia ciąg bramek $\mathbf{CNOT}_1^2\mathbf{CNOT}_2^1\mathbf{CNOT}_1^2$, który realizuje bramkę **SWAP** – oznaczaną jak na rysunku po prawej.

Łączenie bramek szeregowo

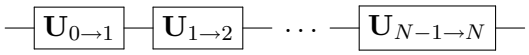
Jeżeli ewolucja kwantowa $\mathbf{U}$ jest podzielona w czasie na kolejne etapy, tzn. na przykład rozpoczyna się od bramki kwantowej $\mathbf{U}_{0\to1}$, która przeprowadza stan z chwili 0 do chwili 1; następnie wprowadza bramkę kwantową $\mathbf{U}_{1\to2}$, która przeprowadza stan z chwili 1 do chwili 2 itd. ..., aż do bramki $\mathbf{U}_{(N-1)\to N}$, która przeprowadza stan z chwili $N-1$ do chwili N – to taki szereg ewolucji zapisujemy jako iloczyn macierzy:

$$\mathbf{U} = \mathbf{U}_{(N-1)\to N}\mathbf{U}_{(N-2)\to(N-1)}\cdots\mathbf{U}_{1\to2}\mathbf{U}_{0\to1}.$$

W takim przypadku jako wynik otrzymujemy też szereg stanów

$$|\psi_1\rangle = \mathbf{U}_{0\to1}|\psi_0\rangle\,,\ |\psi_2\rangle = \mathbf{U}_{1\to2}|\psi_1\rangle\,,\ldots,\ |\psi_N\rangle = \mathbf{U}_{(N-1)\to N}|\psi_{N-1}\rangle\,,$$

które odpowiadają kolejnym chwilom w czasie. Rysunek 6.10 przedstawia szeregowe łączenie bramek.



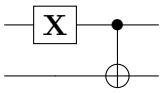
Rysunek 6.10: Szeregowe łączenie bramek kwantowych.

Łączenie bramek równolegle

Jeżeli mamy układ kwantowy składający się z wielu qubitów, to albo każdy z nich może ewoluować oddzielnie, albo niektóre – bądź wszystkie – mogą ewoluować łącznie. Dodatkowo ewolucja niektórych (bądź wszystkich) qubitów może być trywialna, tzn. niezmieniająca stanu.

Aby można było połączyć bramki szeregowo, muszą one działać na układ składający się z takiej samej liczby qubitów. Nie można łączyć bramek $\mathbf{X}$ i $\mathbf{CNOT}_1^2$ szeregowo, gdyż ich macierzy nie można pomnożyć, ponieważ mają różne wymiary. Zatem w takim przypadku musimy rozszerzyć bramkę $\mathbf{X}$ tak, by działała na dwa qubity. Wykorzystujemy do tego iloczyn Kroneckera i macierze identyczności. Jeżeli chcemy uzyskać ciąg bramek kwantowych taki, w którym na początku działamy bramką $\mathbf{X}$ na pierwszy qubit, a następnie bramką $\mathbf{CNOT}_1^2$ na qubity: pierwszy – kontrolujący i drugi – docelowy,

to rozszerzamy bramkę $\mathbf{X}$ tak, by na drugi qubit działała trywialnie do postaci $\mathbf{X} \otimes \mathbf{I}$. Pokazano to na Rysunku 6.11.



Rysunek 6.11: Graficzna reprezentacja operacji $\mathbf{CNOT}_1^2(\mathbf{X} \otimes \mathbf{I})$.

Obwody kwantowe

Łączenie bramek szeregowo i równolegle możemy przedstawić graficznie na tzw. *obwodzie kwantowym* – czyli rysunku, na którym każda linia obwodu oznacza qubit, a każda bramka jest zaznaczona na odpowiednim qubicie lub kilku qubitach. Czas w obwodzie biegnie od lewej do prawej. Przykładem obwodu kwantowego jest przedstawiony poniżej proces uzyskiwania stanu splątanego ze stanu separowalnego.

Tworzenie stanu splątanego ze stanu separowalnego

Ponieważ wiemy, jak łączyć bramki szeregowo i równolegle, możemy teraz stworzyć stan splątany ze stanu separowalnego. Zaczynamy od następującego stanu:

$$|\psi_{t=1}\rangle = |0\rangle \otimes |0\rangle \,.$$

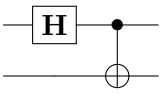
Następnie nakładamy bramkę Hadamarda na pierwszy qubit:

$$|\psi_{t=2}\rangle = (\mathbf{H} \otimes \mathbf{I})\,|\psi_{t=1}\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle)\,.$$

Na koniec nakładamy bramkę $\mathbf{CNOT}_1^2$, w której pierwszy qubit jest kontrolującym, a drugi – docelowym:

$$|\psi_{t=3}\rangle = \mathbf{CNOT}_1^2\,|\psi_{t=2}\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)\,.$$

Otrzymujemy w ten sposób stan maksymalnie splątany – stan Bella $|\Phi^+\rangle$. Obwód kwantowy realizujący tę operację jest przedstawiony na Rysunku 6.12.



Rysunek 6.12: Przykład obwodu kwantowego, który ze stanu $|00\rangle$ tworzy stan Bella $|\Phi^+\rangle$.

6.7 Pomiar

W naszym schemacie – obejmującym przygotowanie stanu, ewolucję i pomiar – ten ostatni stanowi łącze pomiędzy światem kwantowym a klasycznym. Tylko i wyłącznie poprzez pomiar kwantowy układu kwantowego możemy się o nim czegoś dowiedzieć. Ważnym jest, aby pamiętać, że pomiar bezpowrotnie zmienia stan kwantowy. Pomiar nie jest odwracalny.

Matematycznie *pomiar kwantowy* jest opisany przez zbiór ponumerowanych lub poindeksowanych macierzy pomiaru:

$$\mathcal{P} = \{\mathbf{P}_0, \mathbf{P}_1, \ldots, \mathbf{P}_{n-1}\}.$$

Macierze pomiaru są macierzami rzutowymi, co oznacza, że dla każdej macierzy $\mathbf{P}_i$ mamy:

$$\mathbf{P}_i^2 = \mathbf{P}_i\mathbf{P}_i = \mathbf{P}_i.$$

Wymagamy, aby dla każdej pary macierzy o różnych indeksach $i \neq j$ zachodziło:

$$\mathbf{P}_i\mathbf{P}_j = \mathbf{0},$$

czyli aby iloczyn macierzy pomiarów dla różnych wyników był macierzą zerową. Ponadto chcemy, aby suma macierzy pomiaru dawała macierz identycznościową:

$$\mathbf{P}_0 + \mathbf{P}_1 + \ldots + \mathbf{P}_{n-1} = \mathbf{I}.$$

Zauważmy, że z każdą macierzą pomiaru związany jest pewien indeks, np.: $0, 1, \ldots, n-1$. Indeks ten nazywamy *wynikiem pomiaru kwantowego*.

Pomiar kwantowy działa w następujący sposób: jeżeli mamy dany pewien stan kwantowy $|\psi\rangle$ i zbiór macierzy pomiaru $\mathcal{P} = \{\mathbf{P}_0, \mathbf{P}_1, \ldots, \mathbf{P}_{n-1}\}$, to gdy wykonamy pomiar na tym stanie, uzyskamy wynik i z prawdopodobieństwem:

$$p_i = \|\mathbf{P}_i\,|\psi\rangle\|^2.$$

Nie można przewidzieć, który z wyników otrzymamy jako rezultat pomiaru; jest to proces całkowicie losowy. Możemy mówić tylko o prawdopodobieństwie otrzymania danego wyniku. Pomiar kwantowy zmienia stan układu. Gdy uzyskamy wynik i, wówczas stan układu po pomiarze zmienia się na:

$$|\psi_i\rangle = \frac{\mathbf{P}_i\,|\psi\rangle}{\sqrt{p_i}} = \frac{\mathbf{P}_i\,|\psi\rangle}{\|\mathbf{P}_i\,|\psi\rangle\|}.$$

Ponieważ norma jest nieujemna, zatem $\sqrt{p_i} = \sqrt{\|\mathbf{P}_i |\psi\rangle\|^2} = \|\mathbf{P}_i |\psi\rangle\|$.

Zauważmy, że istnieje wiele różnych pomiarów, które możemy wybrać dla danego stanu kwantowego. Przykładowo możemy wziąć pod uwagę jeden qubit i zdefiniować na nim dwa pomiary – pierwszy, składający się z macierzy

$$\mathbf{P}_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \ \mathbf{P}_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

i drugi, składający się z macierzy

$$\mathbf{Q}_{-_\mathrm{i}} = |-_\mathrm{i}\rangle\langle -_\mathrm{i}| = \frac{1}{2}\begin{bmatrix} 1 & \mathrm{i} \\ -\mathrm{i} & 1 \end{bmatrix}, \ \mathbf{Q}_{+_\mathrm{i}} = |+_\mathrm{i}\rangle\langle +_\mathrm{i}| = \frac{1}{2}\begin{bmatrix} 1 & -\mathrm{i} \\ \mathrm{i} & 1 \end{bmatrix}.$$

Warto zauważyć, że określiliśmy wyniki pomiaru zadanego przez macierze $\mathbf{Q}_i$ jako $+_\mathrm{i}$ oraz $-_\mathrm{i}$, a nie przy pomocy liczb naturalnych. Pozwala nam to na rozróżnienie wyników pomiaru pierwszego i drugiego.

Spójrzmy na Rysunek 6.13. Załóżmy, że mierzymy stan $|\psi\rangle = \sqrt{0{,}7}\,|0\rangle + \sqrt{0{,}3}\mathrm{i}\,|1\rangle$ przy użyciu pomiaru zadanego przez $\mathbf{P}_0, \mathbf{P}_1$. Wówczas wynik 0 otrzymujemy z prawdopodobieństwem

$$\begin{aligned} p_0 =& \left\| \mathbf{P}_0 \left(\sqrt{0{,}7}\,|0\rangle + \sqrt{0{,}3}\mathrm{i}\,|1\rangle \right) \right\|^2 = \left\| \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \sqrt{0{,}7} \\ \sqrt{0{,}3}\mathrm{i} \end{bmatrix} \right\|^2 = \\ =& \left\| \begin{bmatrix} \sqrt{0{,}7} \\ 0 \end{bmatrix} \right\|^2 = \left(\sqrt{|\sqrt{0{,}7}|^2 + |0|^2} \right)^2 = 0{,}7 \end{aligned}$$

lub – z prawdopodobieństwem $p_1 = 0{,}3$ – wynik 1. W pierwszym przypadku nasz stan zmieni się po pomiarze na $|\psi_0\rangle = |0\rangle$, a w drugim – na $|\psi_1\rangle = |1\rangle$.

Jednak jeżeli będziemy mierzyć ten sam stan $|\psi\rangle = \sqrt{0{,}7}\,|0\rangle + \sqrt{0{,}3}\mathrm{i}\,|1\rangle$ przy użyciu pomiaru zadanego przez $\mathbf{Q}_{-_\mathrm{i}}, \mathbf{Q}_{+_\mathrm{i}}$, to z prawdopodobieństwem $p_{-_\mathrm{i}} = \frac{5-\sqrt{21}}{10} \approx 0{,}958$ otrzymamy wynik $-_\mathrm{i}$, a z prawdopodobieństwem $p_{+_\mathrm{i}} = \frac{5+\sqrt{21}}{10} \approx 0{,}042$ otrzymamy wynik $+_\mathrm{i}$. W przypadku otrzymania pierwszego wyniku stan po pomiarze zmieni się na $|\psi_{-_\mathrm{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}\,|1\rangle)$, zaś w przypadku otrzymania drugiego – stan po pomiarze zmieni się na $|\psi_{+_\mathrm{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}\,|1\rangle)$.

Zastanówmy się nad jeszcze jednym pomiarem – *trywialnym* – składającym się tylko z macierzy jednostkowej $\{\mathbf{I}_?\}$. Oczywiście zbiór taki spełnia warunki, jakich spełnienia wymagamy od pomiaru, ale wykonanie go na dowolnym stanie po pierwsze nie daje nam żadnej informacji, a po drugie – nie zmienia mierzonego stanu. Wkrótce przekonamy się jednak, że taki pomiar ma pewne znaczenie.

Zobaczmy, jak wygląda pomiar stanu różniącego się tylko o globalną fazę $e^{\mathrm{i}\phi}\,|\psi\rangle$ od stanu $|\psi\rangle$. Prawdopodobieństwo zmierzenia wyniku i jest zadane przez $p_i = \left\| \mathbf{P}_i e^{\mathrm{i}\phi}\,|\psi\rangle \right\|^2$, zatem korzystając z własności normy euklidesowej,

$p_i = \left|e^{\mathrm{i}\phi}\right|^2 \|\mathbf{P}_i |\psi\rangle\|^2$. Ponieważ wiemy, że $\left|e^{\mathrm{i}\phi}\right| = 1$, to $p_i = \|\mathbf{P}_i |\psi\rangle\|^2$, co oznacza, że jest takie samo jak dla stanu $|\psi\rangle$. Zatem faza globalna nie wpływa na wyniki pomiarów.

Szeregowanie pomiarów

Tak samo jak bramki kwantowe, pomiary mogą być wykonywane jeden po drugim. Oczywiście trzeba brać pod uwagę, że pierwszy pomiar zmieni stan kwantowy i wynik drugiego pomiaru będzie zależał od wyniku pierwszego pomiaru.

Jeżeli wykonujemy ten sam pomiar wielokrotnie, to wynik, który otrzymaliśmy z pierwszego pomiaru, otrzymamy też w każdym następnym pomiarze. Weźmy zatem pod uwagę stan $|\psi\rangle$ oraz pomiar $\mathcal{P} = \{\mathbf{P}_0, \mathbf{P}_1, \ldots, \mathbf{P}_{n-1}\}$. Jeżeli dokonamy pomiaru tego stanu jednokrotnie i zmierzymy wynik i, to otrzymamy stan

$$|\psi_i\rangle = \frac{\mathbf{P}_i |\psi\rangle}{\|\mathbf{P}_i |\psi\rangle\|}.$$

Zmierzmy ten stan jeszcze raz i zobaczmy, jakie jest prawdopodobieństwo zmierzenia wyniku j:

$$p'_j = \|\mathbf{P}_j |\psi_i\rangle\|^2 = \left\| \frac{\mathbf{P}_j \mathbf{P}_i |\psi\rangle}{\|\mathbf{P}_i |\psi\rangle\|} \right\|^2.$$

Ponieważ $\mathbf{P}_j \mathbf{P}_i$ jest równe $\mathbf{0}$ dla różnych i i j, to prawdopodobieństwo zmierzenia za drugim razem wyniku innego niż za pierwszym wynosi 0. Natomiast prawdopodobieństwo zmierzenia za drugim razem tego samego wyniku co za pierwszym razem wynosi

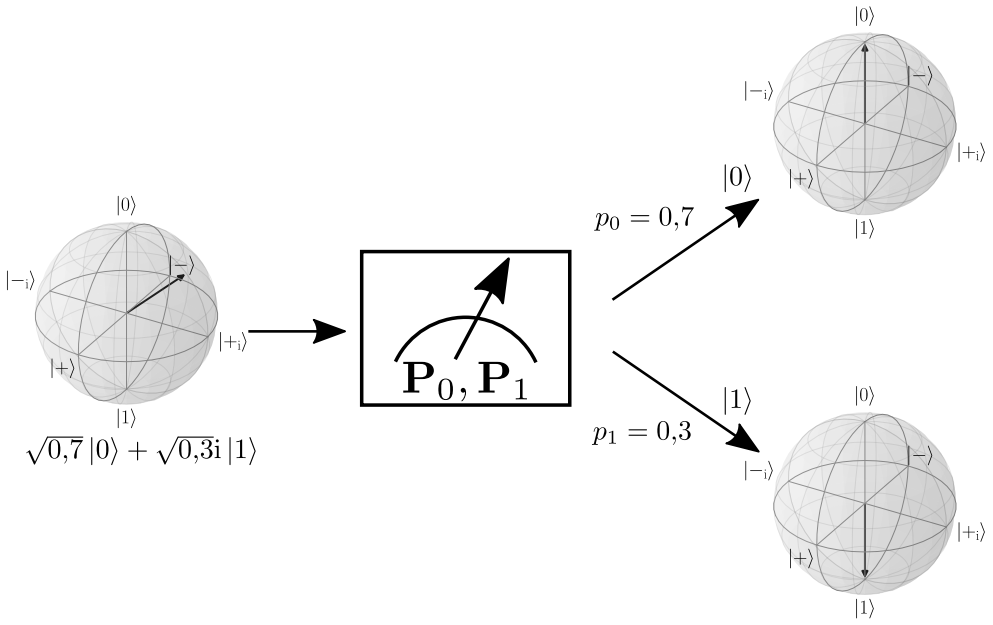
$$p'_i = \left\| \frac{\mathbf{P}_i \mathbf{P}_i |\psi\rangle}{\|\mathbf{P}_i |\psi\rangle\|} \right\|^2 = \left\| \frac{\mathbf{P}_i |\psi\rangle}{\|\mathbf{P}_i |\psi\rangle\|} \right\|^2 = \frac{1}{\|\mathbf{P}_i |\psi\rangle\|^2} \|\mathbf{P}_i |\psi\rangle\|^2 = 1.$$

Zatem widać, że jeżeli za pierwszym razem dokonaliśmy pomiaru $\mathcal{P}$ na stanie $|\psi\rangle$ i otrzymaliśmy wynik i oraz stan po pomiarze $|\psi_i\rangle$, to po dokonaniu tego samego pomiaru raz jeszcze na otrzymanym stanie uzyskamy ten sam wynik i. Zatem stan $|\psi_i\rangle$ pozostanie niezmieniony.

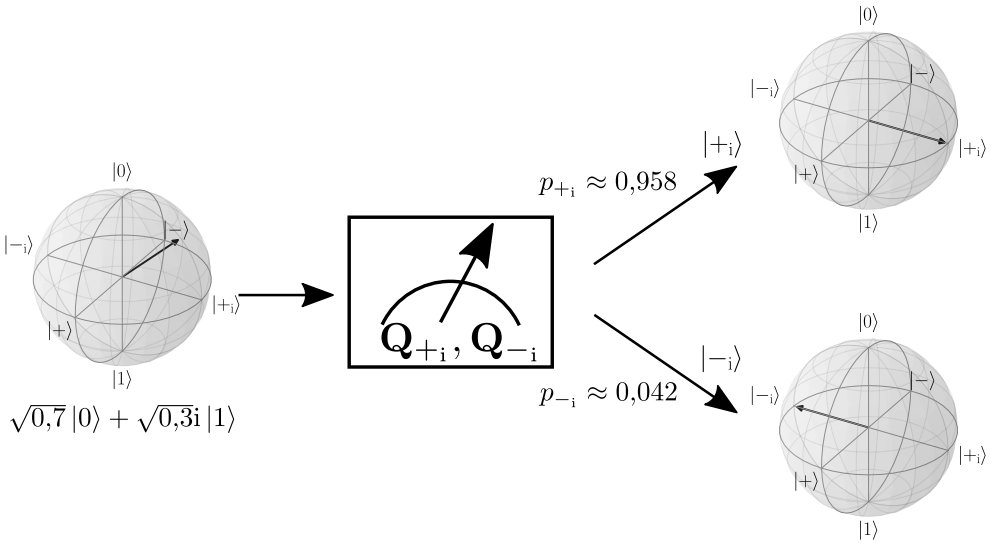
Pomiar częściowy stanu wielosystemowego

Zobaczmy teraz, co się dzieje, gdy dokonamy pomiaru częściowego stanu pierwszego qubitu na stanie złożonym z dwóch qubitów. Przez *pomiar częściowy* rozumiemy taki pomiar dokonywany na układzie wielu qubitów, że na części z nich dokonujemy pomiaru trywialnego, a na części – nietrywialnego.

Załóżmy, że mamy do dyspozycji stan $|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$ i wykonujemy pomiar $\mathcal{P} = \{\mathbf{P}_0 = |0\rangle\langle 0|, \mathbf{P}_1 = |1\rangle\langle 1|\}$ na pierwszym



(a) Pomiar z wykorzystaniem macierzy $\mathbf{P}_0 = |0\rangle\langle 0|\,, \mathbf{P}_1 = |1\rangle\langle 1|$.



(b) Pomiar z wykorzystaniem macierzy $\mathbf{Q}_{-\mathrm{i}} = |-_{\mathrm{i}}\rangle\langle -_{\mathrm{i}}|\,, \mathbf{Q}_{+\mathrm{i}} = |+_{\mathrm{i}}\rangle\langle +_{\mathrm{i}}|$.

Rysunek 6.13: Schemat dwóch różnych pomiarów kwantowych tego samego stanu $\sqrt{0{,}7}\,|0\rangle + \sqrt{0{,}3}\mathrm{i}\,|1\rangle$. W zależności od rodzaju pomiaru uzyskujemy inne wyniki z różnymi prawdopodobieństwami oraz inne stany po wykonaniu pomiaru. Takie zachowanie układów jest charakterystyczne dla mechaniki kwantowej.

qubicie oraz pomiar trywialny na drugim. Wówczas wynik 0 z pomiaru pierwszego qubitu uzyskujemy z prawdopodobieństwem

$$p_{0?} = \|\mathbf{P}_0 \otimes \mathbf{I}_? \, |\psi\rangle\|^2 = \left\| \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \right\|^2 = \left\| \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ 0 \\ 0 \end{bmatrix} \right\|^2 = |\alpha_{00}|^2 + |\alpha_{01}|^2.$$

Odpowiednio wynik 1 uzyskujemy z prawdopodobieństwem

$$p_{1?} = |\alpha_{10}|^2 + |\alpha_{11}|^2.$$

Stan po zmierzeniu 0 na pierwszym qubicie staje się

$$|\psi_{0?}\rangle = \frac{\alpha_{00} \, |00\rangle + \alpha_{01} \, |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} = |0\rangle \otimes \frac{\alpha_{00} \, |0\rangle + \alpha_{01} \, |0\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}},$$

a po zmierzeniu 1 – staje się

$$|\psi_{1?}\rangle = \frac{\alpha_{10} \, |10\rangle + \alpha_{11} \, |11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}} = |1\rangle \otimes \frac{\alpha_{10} \, |0\rangle + \alpha_{11} \, |1\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}.$$

Zobaczmy, co się stanie, gdy przeprowadzimy go na stanie Bella $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Wówczas mamy $\alpha_{00} = \alpha_{11} = \frac{1}{\sqrt{2}}$ oraz $\alpha_{01} = \alpha_{10} = 0$. Zatem zmierzenie 0 na pierwszym qubicie da nam stan po pomiarze $|00\rangle$, a zmierzenie 1 da nam stan $|11\rangle$. Czyli – jak widać – wynik pomiaru na pierwszym qubicie determinuje stan po pomiarze drugiego qubitu, a zatem również wynik pomiaru na drugim. Efekt taki jest utożsamiany ze splątaniem kwantowym i – jako taki – jest on bardzo istotny dla informatyki kwantowej.

6.8 Podsumowanie

W powyższym rozdziale wprowadziliśmy pojęcia stanu, bramki kwantowej i pomiaru kwantowego. Dzięki temu wiemy teraz, jak opisywane są układy kwantowe, jak zmieniają się w czasie i jak są odczytywane ich właściwości. W komputerach kwantowych te operacje wykonywane są cyklicznie po to, by implementować protokoły lub algorytmy kwantowe. W następnym rozdziale zobaczymy proste i bardziej złożone przykłady zastosowania mechaniki kwantowej w informatyce.

Rozdział 7

Informatyka kwantowa

Twierdzenie o zakazie klonowania

Możliwość kopiowania informacji zakodowanej w postaci ciągów bitów wydaje się być oczywista. Używając komputerów w życiu codziennym, ciągle kopiujemy strony www z serwerów na nasze urządzenia, kopiujemy programy z dysku komputera do pamięci operacyjnej lub po prostu kopiujemy zdjęcia dla znajomych i rodziny.

Informacja zapisana w postaci qubitów jest inna. Nie można jej skopiować. Właściwość tę opisuje twierdzenie o zakazie klonowania, które można przedstawić dla qubitów w sposób opisany poniżej.

Wyobraźmy sobie, że dana jest bramka kwantowa $\mathbf{U_c}$ działającą na dwóch układach kwantowych, która dla dowolnego stanu $|\psi\rangle$ działa następująco:

$$|\psi\rangle \otimes |\psi\rangle = \mathbf{U_c}(|\psi\rangle \otimes |0\rangle).$$

Oznacza to, że kopiuje ona nieznany stan $|\psi\rangle$ z układu pierwszego na układ drugi. Weźmy zatem dwa dowolne stany $|\psi_1\rangle$ oraz $|\psi_2\rangle$ i zapiszmy dla nich powyższe równanie:

$$\begin{aligned} |\psi_1\rangle \otimes |\psi_1\rangle &= \mathbf{U_c}(|\psi_1\rangle \otimes |0\rangle), \\ |\psi_2\rangle \otimes |\psi_2\rangle &= \mathbf{U_c}(|\psi_2\rangle \otimes |0\rangle). \end{aligned}$$

Policzmy teraz iloczyn skalarnym pomiędzy wektorami w górnym i dolnym równaniu:

$$(\langle\psi_1| \otimes \langle\psi_1|)(|\psi_2\rangle \otimes |\psi_2\rangle) = (\langle\psi_1| \otimes \langle 0|)\mathbf{U_c}^\dagger \mathbf{U_c}(|\psi_2\rangle \otimes |0\rangle).$$

Ponieważ $\mathbf{U_c}$ jest macierzą unitarną, możemy usunąć z równania $\mathbf{U_c}^\dagger \mathbf{U_c} = \mathbf{I}$, a następnie pogrupować składniki:

$$\langle\psi_1|\psi_2\rangle \otimes \langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle \otimes \langle 0|0\rangle\,.$$

Oczywiście $\langle 0|0\rangle = 1$, a iloczyn Kroneckera liczb jest równy iloczynowi tych liczb – zatem otrzymujemy:

$$\langle\psi_1|\psi_2\rangle^2 = \langle\psi_1|\psi_2\rangle\,.$$

To równanie ma dwa rozwiązania – dla $\langle\psi_1|\psi_2\rangle = 0$, czyli wektorów ortonormalnych, oraz $\langle\psi_1|\psi_2\rangle = 1$, czyli dla wektorów $|\psi_1\rangle = |\psi_2\rangle$. Wynika z tego, że możemy klonować stany tylko z ortonormalnego zbioru stanów. Ponieważ zbiór wszystkich stanów nie jest ortonormalny, zatem nie istnieje bramka unitarna, która pozwalałaby na klonowanie dowolnych stanów.

Twierdzenie to będzie nam potrzebne do zrozumienia podstaw działania kwantowego protokołu dystrybucji klucza kwantowego – podstawy kwantowej kryptografii – oraz kwantowych zamków.

7.1 Zamki kwantowe

Jak widać, klonowanie dowolnych stanów kwantowych jest niemożliwe. Można więc wyobrazić sobie proste zastosowanie tego faktu do tworzenia niepodrabialnych kluczy do zamków.

Wyobraźmy sobie klucz, który składa się z n qubitów, oraz zamek, który zawiera urządzenie elektroniczne, a także kwantowe urządzenie pomiarowe, które umie zmierzyć stan klucza. Zamek może zostać otwarty przez odpowiedni klucz i nie powinien być otwierany przez inny klucz.

Załóżmy teraz, że dany jest ciąg qubitów $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$, które stanowią klucz. Chcemy, aby każdy qubit był w jednym z następujących stanów:

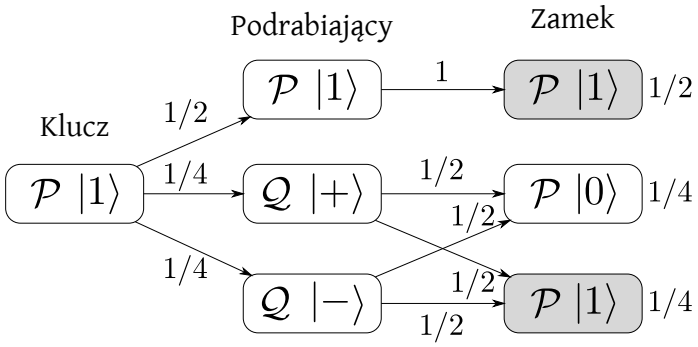
$$|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ lub } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Aby zbudować mechanizm zamka, potrzebujemy dwóch pomiarów: pierwszego $\mathcal{P} = \{\mathbf{P}_0 = |0\rangle\langle 0|, \mathbf{P}_1 = |1\rangle\langle 1|\}$ i drugiego $\mathcal{Q} = \{\mathbf{Q}_+ = |+\rangle\langle +|, \mathbf{Q}_- = |-\rangle\langle -|\}$. Wyniki pierwszego pomiaru będziemy oznaczać jako 0 i 1, a drugiego – jako + i −. Od razu widać, że pomiar $\mathcal{P}$ jest dopasowany do stanów $|0\rangle$ i $|1\rangle$ i potrafi je doskonale rozróżniać – co znaczy, że dla stanu $|0\rangle$ zwróci zawsze wynik 0, a dla stanu $|1\rangle$ zawsze zwróci wynik 1. Natomiast dla stanów $|+\rangle$ i $|-\rangle$ zwróci wyniki 0 lub 1 z prawdopodobieństwem $\frac{1}{2}$. Odpowiednio w przypadku pomiaru $\mathcal{Q}$ – jest on dopasowany do stanów $|+\rangle$ i $|-\rangle$, które rozróżnia doskonale, ale dla stanów $|0\rangle$ i $|1\rangle$ zwraca wyniki + i − z prawdopodobieństwem $\frac{1}{2}$.

Zatem jeżeli mechanizm zamka zna stany qubitów klucza, to może dokonywać odpowiednich dopasowanych pomiarów na ich stanach. Jeżeli przynajmniej jeden pomiar zwróci wynik, który nie jest oczekiwany, to znaczy, że klucz nie pasuje do zamka.

Co się więc stanie, jeżeli ktoś, mając w ręku klucz, chciałby go podrobić? Zakładamy, że osoba, która podrabia klucz, nie wie nic na temat tego, jakie pomiary są przeprowadzane w zamku, i oczywiście nie wie nic o stanach klucza.

Zatem jedyne, co może zrobić, to wybrać losowo pomiary i zmierzyć stany qubitów klucza. Wtedy z prawdopodobieństwem $\frac{1}{2}$ wybierze pomiar, który jest dopasowany do stanu qubitu zamka. Jeżeli zostanie wybrany niewłaściwy pomiar, to zamek wykryje błąd z prawdopodobieństwem $\frac{1}{2}$. Zatem z prawdopodobieństwem $\frac{3}{4}$ qubit podrobionego klucza zostanie poprawnie rozpoznany przez zamek (zobacz Rysunek 7.1). Jeżeli klucz będzie się składał z n qubitów, to prawdopodobieństwo otwarcia zamka podrobionym kluczem wynosi $\left(\frac{3}{4}\right)^n$ – czyli maleje wraz ze wzrostem liczby qubitów i dla dużej liczby qubitów jest bardzo małe.



Rysunek 7.1: Schemat obliczania prawdopodobieństwa prawidłowego zmierzenia stanu qubitu podrobionego klucza. Kolorem szarym oznaczono pomiary, które wykonuje zamek i które zwrócą oczekiwany wynik.

Jak widać, nie jest łatwo podrobić klucze kwantowe. Czy jednak istnieje możliwość ich wykradzenia? Tego dowiemy się pod koniec niniejszego rozdziału.

7.2 Gra w obracanie monety

Wersja klasyczna

Wyobraźmy sobie następującą grę, w której bierze udział dwoje graczy: Pi (Π) i Sigma (Σ)[1]. Gracze mają do dyspozycji monetę, która jest zamknięta w pudełku, więc nie mogą jej zobaczyć w trakcie gry; natomiast wiedzą, że na początku gry moneta jest odwrócona orłem do góry. Gra składa się z trzech ruchów: pierwszy wykonuje Pi, drugi – Sigma, trzeci – znowu Pi. Ruch polega na odwróceniu monety bądź pozostawieniu jej w takim stanie, w jakim była. Oczywiście to, jaki ruch wykona jeden z graczy, pozostaje tajemnicą dla drugiego. Po dokonaniu ostatniego ruchu pudełko zostaje otwarte i gracze mogą sprawdzić, czy moneta jest odwrócona orłem czy reszką do góry.

[1]Przybysze z Matplanety.

Pi wygrywa, jeśli moneta będzie w pozycji „orzeł", a Sigma – jeśli w pozycji „reszka".

Łatwo sprawdzić, że w tej grze nie istnieje strategia wygrywająca dla żadnego z graczy i najlepsze, co oboje mogą zrobić, to wylosować swoje ruchy. Wtedy dla każdego z nich szansa na wygraną wynosi 50% .

Wersja kwantowa

Zastanówmy się teraz, co się stanie, jeżeli gracze będą mieć do dyspozycji nie monetę, ale qubit. Żeby zamodelować taką sytuację, przypiszmy pozycji monety „orzeł" stan $|0\rangle$ oraz macierz pomiaru $\mathbf{P}_0 = |0\rangle\langle 0|$, a pozycji „reszka" stan $|1\rangle$ i operator pomiaru $\mathbf{P}_1 = |1\rangle\langle 1|$. Obrócenie monety – qubitu będzie wówczas odpowiadać bramce $\mathbf{X}$, a pozostawienie go w stanie, w jakim był – bramce $\mathbf{I}$. W tym schemacie ruchom wykonywanym przez graczy odpowiada czynność nałożenia bramki kwantowej na qubit – za pierwszym i trzecim razem przez Pi, a za drugim – przez Sigmę. Otworzeniu pudełka odpowiada pomiar kwantowy. Przykładową rozgrywkę można zatem zapisać w następujący sposób:

Stan początkowy to:

$$|\psi_{t=0}\rangle = |0\rangle\,.$$

Pi decyduje się nic nie robić:

$$|\psi_{t=1}\rangle = \mathbf{I}\,|0\rangle = |0\rangle\,.$$

Sigma decyduje się obrócić qubit:

$$|\psi_{t=2}\rangle = \mathbf{X}\,|0\rangle = |1\rangle\,.$$

Pi ponownie decyduje się nic nie robić:

$$|\psi_{t=3}\rangle = \mathbf{I}\,|1\rangle = |1\rangle\,.$$

Gracze dokonują pomiaru $\{\mathbf{P}_0, \mathbf{P}_1\}$ i otrzymują prawdopodobieństwa zmierzenia „orła" – wyniku pomiaru 0 – lub „reszki" – wyniku pomiaru 1:

$$p_0 = \||0\rangle\langle 0|\,|1\rangle\| = 0, \quad p_1 = \||1\rangle\langle 1|\,|1\rangle\| = 1.$$

Zatem Sigma wygrywa z prawdopodobieństwem 1. Nie znaczy to, że Sigma wygrywa tę grę zawsze; znaczy tylko tyle, że wygrywa w przypadku takiego ciągu ruchów. Jeśli ciąg ruchów będzie inny, np.. $\mathbf{X}$, $\mathbf{X}$, $\mathbf{I}$, może wygrać Pi.

Dajmy teraz Pi przewagę: ona będzie wiedzieć, że grają na qubicie, a Sigma nie będzie tego świadom. Zobaczmy teraz, co może zrobić Pi, jeżeli wie, że gra odbywa się z wykorzystaniem nie monety, ale qubitu. Nasz stan początkowy to znowu:

$$|\psi_{t=0}\rangle = |0\rangle\,.$$

Pi decyduje się użyć „tajnego" ruchu kwantowego i nakłada bramkę Hadamarda:

$$|\psi_{t=1}\rangle = \mathbf{H}\,|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

Załóżmy, że Sigma decyduje się obrócić qubit:

$$|\psi_{t=2}\rangle = \mathbf{X}\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

Jak widać, jego działanie nie zmienia teraz stanu qubitu. Zatem niezależnie od tego, czy nakłada on bramkę $\mathbf{X}$ lub $\mathbf{I}$, nie zmieni stanu qubitu. Następnie Pi znowu nakłada bramkę Hadamarda:

$$\begin{aligned}|\psi_{t=3}\rangle =& \mathbf{H}\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{\sqrt{2}}\left(\mathbf{H}\,|0\rangle + \mathbf{H}\,|1\rangle\right) = \\ =& \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) + \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right) = \\ =& \frac{1}{2}\left(|0\rangle + |1\rangle + |0\rangle - |1\rangle\right) = |0\rangle\end{aligned}$$

Gracze dokonują pomiaru $\{\mathbf{P}_0, \mathbf{P}_1\}$ i otrzymują prawdopodobieństwa

$$p_0 = \||0\rangle\langle 0|\,|0\rangle\| = 1, \quad p_1 = \||1\rangle\langle 1|\,|1\rangle\| = 0.$$

W efekcie Pi wygrywa, i to wygrywa niezależnie od działań Sigmy. Zatem możliwość wykorzystania większej liczby bramek kwantowych – takich, które nie mają odpowiedników klasycznych – daje przewagę jednemu z graczy.

7.3 Kwantowa dystrybucja klucza

Wyobraźmy sobie, że istnieją dwie osoby oddalone od siebie fizycznie, które chcą przesłać pomiędzy sobą pewną informację w postaci ciągu bitów. Informacja ta jest tajna i nie powinna zostać przechwycona przez osoby trzecie. Osobę nadającą nazywamy Pi, odbierającą – Sigmą, a próbującą przechwycić informację – Omegą (Ω).

Klasyczne rozwiązanie tego problemu polega na wykorzystaniu któregoś z algorytmów szyfrujących oraz klasycznego kanału informacyjnego. Wadą tego rozwiązania jest to, iż nie mamy pewności, czy algorytmy szyfrujące na pewno są bezpieczne. Nasza wiara w ich bezpieczeństwo wynika tylko i wyłącznie z przekonania, iż nie wiadomo, w jaki sposób szybko i efektywnie wykonywać pewne algorytmy, takie jak np. algorytm znajdowania dzielników liczb.

Szyfr Vernama

Istnieje szyfr pozwalający przesyłać informację całkowicie bezpiecznie. Jest to szyfr Vernama[2]. Jego idea jest bardzo prosta. Pi i Sigma współdzielą pewien tylko sobie znany ciąg losowych bitów, czyli klucz. Zakładamy, że Pi chce

[2]Od nazwiska Gilberta Vernama (1890–1960).

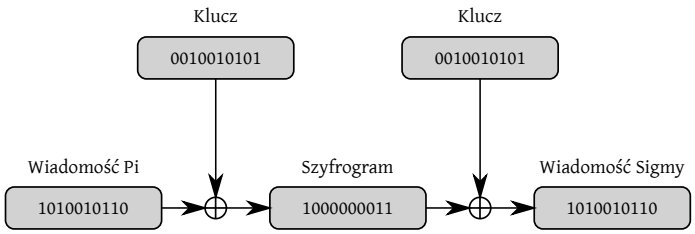
przesłać tajną wiadomość w postaci binarnej do Sigmy. Ażeby ukryć tę wiadomość przed Omegą, dla każdego bitu wiadomości dokonuje operacji XOR z odpowiednim bitem klucza. W ten sposób uzyskuje szyfrogram, który wysyła do Sigmy. Po otrzymaniu zaszyfrowanej wiadomości Sigma odwraca działanie Pi – tzn. dokonuje operacji XOR na każdym bicie szyfrogramu z odpowiednim bitem klucza i w ten sposób odzyskuje oryginalną wiadomość nadaną przez Pi.

Operacja XOR działa na dwóch bitach następująco: jeżeli oba bity są różne, to zwraca 1, jeżeli są równe – to zwraca 0. Możemy zatem stworzyć Tabelę 7.1 wejść i wyjść operacji XOR, w której dwie lewe kolumny odpowiadają argumentom operacji (wejściom), a prawa kolumna odpowiada wartościom (wyjściu).

we_1	we_2	wy
0	0	0
0	1	1
1	0	1
1	1	0

Tabela 7.1: Tabela argumentów i wartości operacji $\text{wy} = XOR(\text{we}_1, \text{we}_2)$.

Oznaczmy zatem tajną wiadomość Pi jako ciąg bitów $a_1, a_2, \ldots, a_n$, szyfrogram – jako $s_1, s_2, \ldots, s_n$, klucz jako $k_1, k_2, \ldots, k_n$, a wiadomość odczytaną przez Sigmę jako $b_1, b_2, \ldots, b_n$. Wówczas w procesie szyfrowania uzyskujemy szyfrogram ze wzoru $s_i = XOR(a_i, k_i)$ dla każdego $i = 1, 2, \ldots, n$. Sigma natomiast deszyfruje wiadomość, korzystając ze wzoru $b_i = XOR(s_i, k_i)$. Łatwo można sprawdzić, że dla każdego $i = 1, 2, \ldots, n$ $a_i = b_i$, co oznacza, że wiadomość otrzymana przez Sigmę jest tą, którą nadała Pi. Przykład takiego procesu szyfrowania i deszyfrowania jest pokazany na Rysunku 7.2.



Rysunek 7.2: Przykład działania szyfru Vernama. Symbol $\oplus$ oznacza operację XOR.

Jeżeli klucz jest całkowicie losowy, to dla Omegi, która nie zna klucza, szyfrogram także jest całkowicie losowy i nie niesie żadnej informacji o tajnej wiadomości.

Protokół BB84

Szyfr Vernama ma pewną wadę – wymaga on tego, by nadawca i odbiorca wiadomości korzystali z klucza kryptograficznego, który ma długość samej wiadomości oraz jest całkowicie losowy. Taki klucz – po pierwsze – trudno stworzyć, ponieważ nie jest łatwo wylosować całkowicie losowy ciąg bitów; a po drugie – dystrybuować pomiędzy nadawcę i odbiorcę. Rozwiązaniem problemu losowania i dystrybucji klucza jest protokół BB84[3], który wykorzystuje qubity i mechanikę kwantową do przygotowania i dystrybucji klucza kryptograficznego.

Podobnie jak w konstrukcji zamków i kluczy kwantowych, w protokole BB84 używamy czterech stanów jednoqubitowych:

$$|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ lub } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

oraz dwóch rodzajów pomiarów $\mathcal{P} = \{\mathbf{P}_0 = |0\rangle\langle 0|, \mathbf{P}_1 = |1\rangle\langle 1|\}$ i $\mathcal{Q} = \{\mathbf{Q}_+ = |+\rangle\langle +|, \mathbf{Q}_- |-\rangle\langle -|\}$.

Pi – nadawca – nadaje qubity w stanach wymienionych powyżej, natomiast Sigma – odbiorca – dokonuje wymienionych powyżej pomiarów. Zależność wyniku pomiaru od wysłanego stanu qubitu i od tego, jaki pomiar został na nim dokonany, przedstawia Tabela 7.2.

stan	pomiar	wynik pomiaru
$\|0\rangle$	$\mathcal{P}$	0
$\|1\rangle$	$\mathcal{P}$	1
$\|+\rangle$	$\mathcal{Q}$	+
$\|-\rangle$	$\mathcal{Q}$	−
$\|0\rangle$	$\mathcal{Q}$	+ lub − z $p_+ = p_- = \frac{1}{2}$
$\|1\rangle$	$\mathcal{Q}$	+ lub − z $p_+ = p_- = \frac{1}{2}$
$\|+\rangle$	$\mathcal{P}$	0 lub 1 z $p_0 = p_1 = \frac{1}{2}$
$\|-\rangle$	$\mathcal{P}$	0 lub 1 z $p_0 = p_1 = \frac{1}{2}$

Tabela 7.2: Zależność wyniku pomiaru od stanu i wybranego rodzaju pomiaru.

Jeżeli stan nadawany przez Pi nie jest dopasowany do pomiaru, to wynik jego pomiaru jest losowy, co pokazują ostatnie cztery wiersze tabeli. Dodatkowo po pomiarze stan początkowy zmienia się na stan odpowiadający wynikowi pomiaru. Fakt ten można wykorzystać do wykrywania podsłuchu podczas przesyłania qubitów. Pozwala to na stworzenie protokołu dystrybucji kluczy kwantowych składającego się z poniższych kroków:

[3]Zaproponowany w roku 1984 przez Charlesa Bennetta i Gilles'a Brassarda.

Krok 1 Pi wysyła sekwencję qubitów, z których każdy jest w losowo i niezależnie wybranym stanie: $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ lub $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Krok 2 Sigma dokonuje – również losowo i niezależnie – wyboru, który z dwóch pomiarów – $\mathcal{P}$ lub $\mathcal{Q}$ – przeprowadzi na każdym z qubitów z osobna.

Krok 3 Sigma zapisuje swój wybór i wyniki pomiarów.

Krok 4 Sigma wysyła do Pi w sposób jawny swój wybór pomiarów.

Krok 5 Pi przekazuje Sigmie informację, które pomiary były dopasowane do stanów nadanych qubitów.

Krok 6 Pi i Sigma dzielą qubity na dwie części: jedna zawiera te, które zostały zmierzone za pomocą dopasowanego pomiaru, a druga – te, które nie zostały zmierzone w ten sposób.

Możemy zauważyć, że średnio w połowie przypadków został użyty niedopasowany pomiar. Przypadki te muszą zostać odrzucone, gdyż wynik niedopasowanego pomiaru jest całkowicie losowy.

Jeżeli nie zaistniały przekłamania i nikt nie ingerował w proces transmisji, to ok. 50% qubitów zmierzonych przez Sigmę posiada ten sam stan, jaki został nadany przez Pi. Te właśnie qubity mogą zostać wykorzystane do stworzenia klucza kryptograficznego.

Krok 7 Pi i Sigma wybierają pewien wspólny podzbiór qubitów spośród tych, które zostały zmierzone przy użyciu dopasowanego pomiaru i w sposób jawny je porównują. Qubity te oczywiście będzie trzeba odrzucić, jako że zostały ujawnione.

Jeżeli nie doszło do podsłuchania transmisji qubitów, to porównanie powinno dać całkowicie zgodne wyniki. Wówczas Pi i Sigma przypisują stanom $|0\rangle$, $|-\rangle$ bit 0, a stanom $|1\rangle$, $|+\rangle$ bit 1. Zatem teraz Pi i Sigma posiadają wspólny losowy klucz kryptograficzny, którego mogą użyć do przekazania sobie zaszyfrowanej szyfrem Vernama wiadomości.

Jeżeli podczas wykonywania protokołu Pi i Sigma wykryli niezgodności, oznacza to, że qubity zostały już poddane pomiarowi przez osobę trzecią i nie należy ich używać do tworzenia klucza. W takim przypadku muszą zaniechać przesyłania tajnej informacji.

Zastanówmy się, jakie próby ataku może podjąć Omega. Nie może skopiować stanu qubitu i zmierzyć jego kopii, gdyż tego zabrania twierdzenie o zakazie klonowania. Może natomiast wpiąć się do kwantowego kanału transmisji i przechwytywać wszystkie qubity nadesłane przez Pi, dokonywać na nich pomiaru i następnie odsyłać do Sigmy. Taka technika podsłuchu jest bardzo łatwa do zdemaskowania, gdyż – nie wiedząc, jakie qubity zostały nadane –

Omega nie wie, jaki pomiar wybrać. Wybierając niewłaściwy pomiar, Omega doprowadza do zmiany stanów qubitów, co – po wymianie klucza – Pi i Sigma z łatwością wykryją. Omega może również przechwytywać tylko niektóre qubity i je mierzyć, ale wtedy nie uzyska całego klucza kryptograficznego, a jej działanie też może zostać wykryte.

Tabela 7.3 pokazuje, jak może przebiegać krótki proces ustalania klucza przez Pi i Sigmę, gdy Omega nie podsłuchuje. Natomiast w Tabeli 7.4 pokazano, co się dzieje, gdy Omega podsłuchuje komunikację kwantową.

Π_1	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
Σ_1	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$
Σ_2	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
bit	0	1	1				1		0			0		1				1	0	0

Tabela 7.3: Przykład realizacji protokołu BB84 bez podsłuchu. Oznaczenia wierszy: Π_1 – stany wysłane przez Pi, Σ_1 – pomiary wybrane przez Sigmę, Σ_2 – stany po pomiarze Sigmy, bit – bit klucza. Kolumny oznaczone na szaro wyróżniają przypadki, dla których stan qubitu nadanego przez Pi pokrywa się z qubitem zmierzonym przez Sigmę. We wszystkich przypadkach, w których Pi nadała qubit w stanie dopasowanym do pomiaru Sigmy, Sigma zmierzył odpowiedni stan – zatem Pi i Sigma nie mają powodu podejrzewać, że ktoś podsłuchiwał ustalanie klucza.

Π_1	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
Ω_1	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$
Ω_2	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
Σ_1	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{Q}$
Σ_2	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$

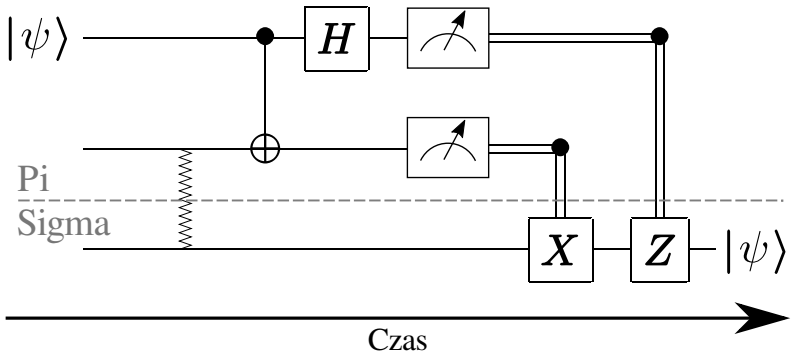
Tabela 7.4: Przykład realizacji protokołu BB84 z podsłuchem. Oznaczenia wierszy: Π_1 – stany wysłane przez Pi, Ω_1 – pomiary wybrane przez Omegę, Ω_2 – stany po pomiarze Omegi, Σ_1 – pomiary wybrane przez Sigmę, Σ_2 – stany po pomiarze Sigmy. Kolumny oznaczone na szaro wyróżniają przypadki, dla których stan qubitu nadanego przez Pi nie pokrywa się z qubitem zmierzonym przez Sigmę. Te przypadki wskazują Pi i Sigmie, że mogło dojść do podsłuchu.

Bezpieczeństwo protokołu BB84 zależy od naszej ufności w skuteczność mechaniki kwantowej – najlepiej potwierdzonej współczesnej teorii fizycznej – w przeciwieństwie do klasycznych protokołów kryptografii asymetrycznej, w przypadku której musimy zakładać, że nikt nie zna skutecznych metod faktoryzacji liczb lub liczenia logarytmu dyskretnego.

7.4 Teleportacja kwantowa

Wyobraźmy sobie, że Pi posiada qubit, którego stanu nie zna. Chce przesłać ten stan do Sigmy, ale nie ma możliwości przesłania do niego informacji kwantowej – tzn. stanów kwantowych. Może do niego natomiast przesłać informację klasyczną. Jeśli ma się tylko jedną kopię stanu, jest to oczywiście niemożliwe. Natomiast jeżeli Pi i Sigma współdzielą splątany stan Bella, to możliwe staje się przesłanie informacji klasycznej. Taki proces przesyłania stanu

kwantowego z wykorzystaniem stanu splątanego nazywamy protokołem *teleportacji kwantowej*. Schematyczna ilustracja tego protokołu jest przedstawiona na Rysunku 7.3. Pierwszy i drugi qubit znajduje się w posiadaniu Pi, natomiast trzeci qubit ma Sigma. Pierwszy qubit jest w stanie, który Pi chce przesłać, natomiast drugi i trzeci qubit są w stanie Bella $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.



Rysunek 7.3: Obwód teleportacji kwantowej. Linie poziome oznaczają qubity. Pionowa linia zygzakowata oznacza stan splątany. Linie podwójne oznaczają klasyczne bity. Pozioma linia przerywana oddziela układ Pi od układu Sigmy.

Ponieważ nie wiemy nic o stanie qubitu Pi, zapiszmy go w ogólnej postaci:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,.$$

Wówczas stan początkowy układu jest następujący:

$$\begin{aligned}
|\psi_{t=0}\rangle &= |\psi\rangle \otimes \left|\Phi^+\right\rangle = \\
&= |\psi\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right) = \\
&= \left(\alpha\,|0\rangle + \beta\,|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right) = \\
&= \frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle\right).
\end{aligned}$$

Pi nakłada teraz bramkę $\mathbf{CNOT}_1^2$ na swoje qubity i stan układu zmienia się na:

$$\begin{aligned}
|\psi_{t=1}\rangle &= (\mathbf{CNOT}_1^2 \otimes \mathbf{I})\frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle\right) = \\
&= \frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle\right).
\end{aligned}$$

Następnie Pi nakłada bramkę Hadamarda na pierwszy qubit, zmieniając stan na:

$$\begin{aligned}|\psi_{t=2}\rangle &= (\mathbf{H}\otimes\mathbf{I}\otimes\mathbf{I})\frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle+\alpha\,|011\rangle+\beta\,|110\rangle+\beta\,|101\rangle\right)=\\ &=\frac{1}{\sqrt{2}}\Big(\alpha\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes(|00\rangle+|11\rangle)+\\ &+\beta\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\otimes(|10\rangle+|01\rangle)\Big)=\\ &=\frac{1}{2}(\alpha\,|000\rangle+\alpha\,|100\rangle+\alpha\,|011\rangle+\alpha\,|111\rangle+\\ &+\beta\,|010\rangle+\beta\,|001\rangle-\beta\,|110\rangle-\beta\,|101\rangle).\end{aligned}$$

Następnie Pi mierzy pierwsze dwa qubity przy użyciu pomiaru częściowego $\mathcal{P}$ składającego się z macierzy

$$\begin{aligned}\mathcal{P}=\{&\mathbf{P}_{00?}=|0\rangle\langle 0|\otimes|0\rangle\langle 0|\otimes\mathbf{I},\mathbf{P}_{01?}=|0\rangle\langle 0|\otimes|1\rangle\langle 1|\otimes\mathbf{I},\\ &\mathbf{P}_{10?}=|1\rangle\langle 1|\otimes|0\rangle\langle 0|\otimes\mathbf{I},\mathbf{P}_{11?}=|1\rangle\langle 1|\otimes|1\rangle\langle 1|\otimes\mathbf{I}\}\end{aligned}$$

i otrzymuje – w zależności od wyniku pomiaru – z jednakowym prawdopodobieństwem stany:

- dla wyniku 00?: $\frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle+\beta\,|001\rangle\right)=\frac{1}{\sqrt{2}}\left(|00\rangle\otimes|\psi\rangle\right)$,
- dla wyniku 01?: $\frac{1}{\sqrt{2}}\left(\alpha\,|011\rangle+\beta\,|010\rangle\right)=\frac{1}{\sqrt{2}}\left(|01\rangle\otimes\mathbf{Z}\,|\psi\rangle\right)$,
- dla wyniku 10?: $\frac{1}{\sqrt{2}}\left(\alpha\,|100\rangle-\beta\,|101\rangle\right)=\frac{1}{\sqrt{2}}\left(|10\rangle\otimes\mathbf{X}\,|\psi\rangle\right)$,
- dla wyniku 11?: $\frac{1}{\sqrt{2}}\left(\alpha\,|111\rangle-\beta\,|110\rangle\right)=\frac{1}{\sqrt{2}}\left(|11\rangle\otimes\mathbf{XZ}\,|\psi\rangle\right)$.

Zauważmy, że stan qubitu Sigmy, w zależności od wyniku pomiaru Pi, jest jednym z czterech stanów: $|\psi\rangle$, $\mathbf{Z}\,|\psi\rangle$, $\mathbf{X}\,|\psi\rangle$ lub $\mathbf{XZ}\,|\psi\rangle$. Widać zatem, że jeżeli Sigma wie, jaki wynik uzyskuje Pi, może tak zmienić swój stan, używając kombinacji bramek $\mathbf{X}$ i $\mathbf{Z}$, by odzyskać oryginalny stan Pi. W przypadku wyniku pomiaru 00 nie musi nic robić, w przypadku 01 nakłada na swój qubit bramkę odwrotną do $\mathbf{X}$, czyli $\mathbf{X}^\dagger$; w przypadku 10 nakłada bramkę $\mathbf{Z}^\dagger$, a w przypadku wyniku pomiaru 11 – bramki $\mathbf{Z}^\dagger\mathbf{X}^\dagger$.

Wykorzystując splątanie kwantowe oraz informację klasyczną, można przenieść stan qubitu Pi na qubit Sigmy, co może pozwolić np. na kradzież kluczy do zamków kwantowych, które opisywaliśmy wcześniej.

Dodatek A

Podstawy matematyczne

A.1 Liczby zespolone

Czy widział ktoś kiedyś liczbę? Na przykład takie czterdzieści dwa[1]? Czy można ją zobaczyć? Możemy zobaczyć reprezentację liczby czterdzieści dwa w postaci zapisu dziesiętnego

$$42,$$

lub binarnego

$$101010,$$

możemy też zobaczyć czterdzieści dwa obiekty — na przykład ręczniki. Jednak samej liczby zobaczyć nie możemy, bo jest ona pojęciem abstrakcyjnym, które istnieje niezależnie od reprezentacji czy interpretacji. Liczba czterdzieści dwa jest liczbą naturalną. Tak samo jest z liczbami wymiernymi i rzeczywistymi — nie możemy ich zobaczyć, dotknąć czy powąchać; jednakże możemy na nich działać.

Powyższe wprowadzenie ma przekonać Czytelnika, że liczby zespolone, o których zaraz będzie mowa, nie są straszniejsze, dziwaczniejsze czy bardziej abstrakcyjne niż liczby naturalne, całkowite, wymierne czy rzeczywiste. Dla matematyka liczby są pewnymi obiektami, między którymi istnieją relacje, na których można wykonywać pewne operacje i które mają pewną (mniej lub bardziej elegancką) strukturę matematyczną. Dla fizyka czy inżyniera natomiast liczby służą do opisu rzeczywistości: naturalne – do zliczania obiektów, wymierne – do opisu stosunków między licznościami, rzeczywiste – do mierzenia czasu, odległości, siły, a zespolone – do opisywania prądu zmiennego, fal lub mechaniki kwantowej. Liczby zespolone stosowane są często tam, gdzie mamy do czynienia z obrotami lub cyklicznie zmieniającymi się wartościami.

Przejdźmy zatem do rzeczy: zdefiniujmy liczby zespolone i działania, jakie można na nich wykonywać. Na początek wprowadźmy jednostkę urojoną: „i”,

[1] Zobacz: Douglas Adams, „Autostopem przez Galaktykę”.

czyli taką liczbę, której kwadrat równy jest $\mathrm{i}^2 = -1$. Teraz możemy powiedzieć, że *liczbą zespoloną* możemy nazwać dowolną liczbę z taką, że

$$z = a + b\mathrm{i},$$

gdzie a i b są liczbami rzeczywistymi. Samą liczbę a nazywamy *częścią rzeczywistą* z i oznaczamy ją przez $\mathrm{Re}\, z$, a b nazywamy *częścią urojoną* liczby z i oznaczamy przez $\mathrm{Im}\, z$. Zbiór liczb zespolonych oznacza się przez $\mathbb{C}$. Oznaczamy, że z należy do zbioru $\mathbb{C}$ – albo inaczej: że jest liczbą zespoloną – pisząc $z \in \mathbb{C}$.

Liczby zespolone przedstawia się na tzw. płaszczyźnie zespolonej, na której na osi poziomej odkłada się wartość części rzeczywistej, a na osi pionowej wartość części urojonej.

Moduł i argument liczby zespolonej

W przypadku liczby zespolonej możemy mówić o dwóch jej własnościach: module i argumencie. *Moduł liczby zespolonej* zadany jest jak w twierdzeniu Pitagorasa – jako

$$|z| = |a + b\mathrm{i}| = \sqrt{a^2 + b^2}.$$

Należy zauważyć, że moduł liczby zespolonej jest rzeczywisty i zawsze większy lub równy zero. Moduł rozumiemy jako odległość liczby z od liczby $0 = 0 + 0\mathrm{i}$.

Argumentem liczby zespolonej $z = a + bi \neq 0 + 0\mathrm{i}$ nazywamy liczbę rzeczywistą ϕ z przedziału $[0, 2\pi)$ spełniającą układ równań

$$\cos\phi = \frac{a}{|z|} \text{ oraz } \sin\phi = \frac{b}{|z|}.$$

Inaczej można powiedzieć, że argument liczby z to wyrażona w radianach wartość kąta skierowanego ϕ pomiędzy osią rzeczywistą a półprostą poprowadzoną od środka układu współrzędnych i przechodzącą przez punkt będący graficzną reprezentacją liczby z. Ilustracją do powyższych definicji jest Rysunek A.1.

Wzór Eulera

Dla liczby rzeczywistej ϕ możemy zapisać następującą relację, nazywaną wzorem Eulera:

$$e^{\mathrm{i}\phi} = \cos\phi + \mathrm{i}\sin\phi.$$

Zauważmy, że dla każdego $\phi \in \mathbb{R}$ moduł liczby $|e^{\mathrm{i}\phi}| = 1$.

Postać trygonometryczna liczby zespolonej

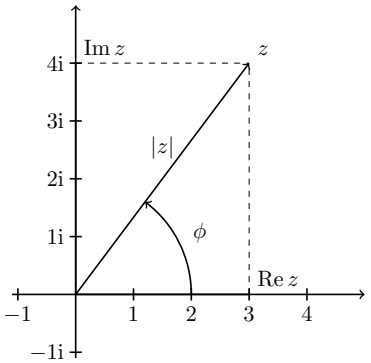
Liczbę zespoloną $z = a + b\mathrm{i} \neq 0 + 0\mathrm{i}$ można zapisać w postaci trygonometrycznej

$$z = |z|(\cos\phi + \mathrm{i}\sin\phi),$$

gdzie ϕ jest argumentem liczby zespolonej. Korzystając ze wzoru Eulera, możemy zapisać liczbę z jako

$$z = |z|e^{\mathrm{i}\phi}.$$

Warto dodać, że w fizyce moduł liczby nazywany jest często *amplitudą*, a argument – *fazą*.



Rysunek A.1: Płaszczyzna zespolona. Liczba zespolona $z = 3 + 4\mathrm{i}$ znajduje się na końcu strzałki. Moduł liczby z, oznaczony jako $|z|$, to długość strzałki. Wynosi on $\sqrt{3^2 + 4^2} = 5$; natomiast argument jest oznaczony jako ϕ i wynosi $\arccos \frac{3}{5} \approx 0{,}92$ rad.

Sprzężenie liczby zespolonej

Sprzężeniem liczby zespolonej $z = a + b\mathrm{i}$ jest liczba

$$z^* = a - b\mathrm{i}.$$

Sprzężenie geometrycznie może być rozumiane jako odbicie symetryczne liczby wokół osi rzeczywistej.

Operacje arytmetyczne na liczbach zespolonych

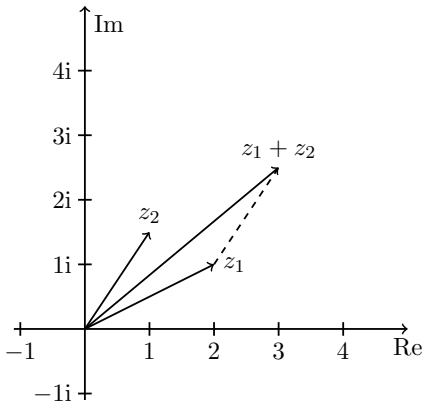
Dodawanie i odejmowanie liczb zespolonych przeprowadza się w sposób naturalny, tzn. jeśli dodajemy dwie liczby zespolone $z_1 = a_1 + b_1\mathrm{i}$ oraz $z_2 = a_2 + b_2\mathrm{i}$, to ich suma wynosi $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)\mathrm{i}$, a ich różnica $z_1 - z_2 = (a_1 - a_2) + (b_1 - b_2)\mathrm{i}$. Geometryczna interpretacja dodawania liczb zespolonych jest podana na Rysunku A.2(a).

Mnożenie i dzielenie liczb zespolonych jest nieco mniej intuicyjne. Jeśli dane są z_1 i z_2 takie jak powyżej, ich iloczyn wynosi:

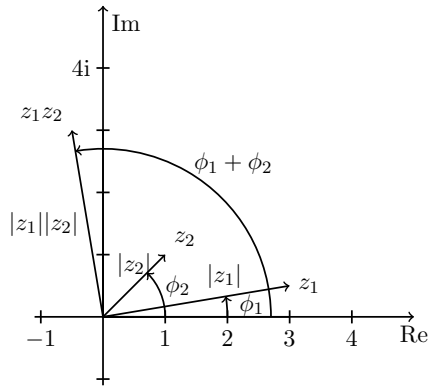
$$\begin{aligned} z_1 z_2 =& (a_1 + b_1\mathrm{i})(a_2 + b_2\mathrm{i}) = \\ =& a_1 a_2 + a_1 b_2\mathrm{i} + b_1 a_2 i - b_1 b_2 = (a_1 a_2 - b_1 b_2) + (a_1 a_2 + b_1 b_2)\mathrm{i}, \end{aligned}$$

a ich iloraz wynosi:

$$\frac{z_1}{z_2} = \frac{a_1 + b_1\mathrm{i}}{a_2 + b_2\mathrm{i}} = \frac{(a_1 + b_1\mathrm{i}) \cdot (a_2 - b_2\mathrm{i})}{(a_2 + b_2\mathrm{i}) \cdot (a_2 - b_2\mathrm{i})} = \left(\frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2}\right)\left(\frac{b_1 a_2 - a_1 b_2}{a_2^2 + b_2^2}\right)\mathrm{i}.$$



(a) Dodawanie liczb zespolonych $z_1 = 2 + 1\mathrm{i}$ oraz $z_2 = 1 + \frac{3}{2}\mathrm{i}$.



(b) Mnożenie liczb zespolonych $z_1 = 3 + \frac{1}{2}\mathrm{i}$ oraz $z_2 = 1 + 1\mathrm{i}$. Aby uzyskać ich iloczyn, musimy pomnożyć amplitudy i dodać fazy.

Rysunek A.2: Graficzna reprezentacja dodawania i mnożenia liczb zespolonych.

Mnożenie i dzielenie liczb zespolonych łatwiej objaśnić, wykorzystując postać trygonometryczną. Jeżeli $z_1 = |z_1|e^{\mathrm{i}\phi_1}$, a $z_2 = |z_2|e^{\mathrm{i}\phi_2}$, to:

$$z_1 z_2 = |z_1||z_2|e^{\mathrm{i}(\phi_1+\phi_2)} \text{ oraz } \frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}e^{\mathrm{i}(\phi_1-\phi_2)}.$$

Geometryczna interpretacja mnożenia liczb zespolonych jest podana na Rysunku A.2(b).

Korzystając z powyższych faktów, policzmy wartość wyrażenia $z^* z$ dla liczby zespolonej $z = a + b\mathrm{i}$:

$$z^* z = (a + b\mathrm{i})^*(a + b\mathrm{i}) = (a - b\mathrm{i})(a + b\mathrm{i}) = a^2 - b^2\mathrm{i}^2 = a^2 + b^2 = |z|^2.$$

Wyrażenie to będzie nam później potrzebne.

A.2 Wektory

Niech dany będzie pewien zbiór, którego elementy możemy do siebie dodawać i mnożyć je przez liczby rzeczywiste lub zespolone. Dodatkowo załóżmy, że operacje te zachowują się zgodnie z regułami wymienionymi poniżej. Taki zbiór nazywamy *przestrzenią wektorową*, a elementy tego zbioru – *wektorami*. Będziemy je tutaj oznaczać przez $|v\rangle$, zamiast, jak to często bywa w zwyczaju, przez $\vec{v}$. Oznaczenie $|v\rangle$ czytamy jako „*ket* v". Stosuje się je w mechanice kwantowej, a pochodzi ono z tzw. notacji Diraca[2], którą posługujemy się w tej książce.

[2]Od nazwiska fizyka Paula Diraca.

Dla nas wektory są kolekcją liczb. Gdy te liczby są rzeczywiste, mówimy o *rzeczywistej przestrzeni wektorowej*; gdy zespolone – o *zespolonej przestrzeni wektorowej.*

Gdy mówi się o wektorach, wiele osób odruchowo wyobraża je sobie jako strzałki na płaszczyźnie. My jednak posługujemy się abstrakcyjnymi wektorami w przestrzeniach, które mają wiele wymiarów. Zatem dla nas to wyobrażenie nie będzie przydatne. Jednakże trzeba zaznaczyć, że wszystkie własności wektorów, które tutaj będziemy wprowadzać, mają również odniesienie do zwykłych wektorów na płaszczyźnie.

Wymagamy, aby wektory posiadały własności wymienione poniżej. Na początek zaznaczmy, iż spośród wektorów wyróżniamy jeden wektor 0, który nazywamy wektorem zerowym. Niech $|u\rangle, |v\rangle, |z\rangle$ oznaczają wektory, a α, β oznaczają liczby (skalary). Korzystając z tych założeń, prezentujemy listę wymaganych własności wektorów:

- Przemienność dodawania $|u\rangle + |v\rangle = |v\rangle + |u\rangle$;
- Łączność dodawania wektorów $(|u\rangle + |v\rangle) + |z\rangle = |u\rangle + (|v\rangle + |z\rangle)$;
- Dla każdego wektora $|u\rangle$ zachodzi $0 + |u\rangle = |u\rangle + 0 = |u\rangle$;
- Dla każdego wektora $|u\rangle$ istnieje wektor przeciwny -$|u\rangle$ taki, że

$$|u\rangle + (-|u\rangle) = 0;$$

- Łączność mnożenia przez skalar $\alpha(\beta|u\rangle) = (\alpha\beta)|u\rangle$;
- Rozdzielność dodawania skalarów względem mnożenia przez wektor

$$(\alpha + \beta)|u\rangle = \alpha|u\rangle + \beta|u\rangle;$$

- Rozdzielność dodawania wektorów względem mnożenia przez skalar

$$\alpha(|u\rangle + |v\rangle) = \alpha|u\rangle + \alpha|v\rangle;$$

- 1 razy wektor daje ten sam wektor: $1|u\rangle = |u\rangle$.

Wektory kolumnowe

Zapiszmy pionową jednokolumnową tablicę n liczb:

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Możemy wprowadzić działanie mnożenia takiej tablicy przez skalar α w następujący sposób:

$$\alpha \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \alpha x_1 \\ \alpha x_2 \\ \vdots \\ \alpha x_n \end{bmatrix}.$$

Możemy też wprowadzić dodawanie takich tablic:

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

Zauważmy zatem, że w ten sposób możemy wprowadzić konkretną reprezentację wektorów. Jeżeli liczby $x_1, x_2, \ldots, x_n$ oraz liczby $y_1, y_2, \ldots, y_n$, a także liczba α są rzeczywiste, to zbiór takich wektorów kolumnowych oznaczamy przez $\mathbb{R}^n$. Jeżeli te liczby są zespolone, to oznaczamy taki zbiór jako $\mathbb{C}^n$.

Wektory wierszowe

Podobnie do wektorów kolumnowych możemy zapisać wektory wierszowe, np. taki jak poniżej:

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \end{bmatrix}.$$

Możemy łatwo zauważyć, że takie wektory można dodawać ze sobą i mnożyć przez skalar. Wektory takie oznaczamy symbolem $\langle u|$, który czytamy „*bra* u".

Transpozycja

Możemy teraz wprowadzić operację *transpozycji* wektorów. Oznaczamy ją przez $\square^T$. Zamienia ona wektory wierszowe na kolumnowe i kolumnowe na wierszowe, tzn.:

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}^T = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \end{bmatrix}$$

oraz

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \end{bmatrix}^T = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Sprzężenie hermitowskie

Dla wektorów wierszowych i kolumnowych zespolonych możemy wprowadzić specyficzną operację *sprzężenia hermitowskiego*, oznaczaną znakiem sztyletu $\square^\dagger$.

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}^\dagger = \begin{bmatrix} {x_1}^* & {x_2}^* & \cdots & {x_n}^* \end{bmatrix}$$

oraz

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \end{bmatrix}^\dagger = \begin{bmatrix} {x_1}^* \\ {x_2}^* \\ \vdots \\ {x_n}^* \end{bmatrix}.$$

Dla naszych potrzeb w mechanice kwantowej utożsamiamy sprzężenie hermitowskie „keta" z odpowiednim wektorem „bra" oraz sprzężenie hermitowskie „bra" z „ketem":

$$|u\rangle^\dagger = \langle u| \text{ oraz } \langle u|^\dagger = |u\rangle .$$

Iloczyn skalarny

Iloczynem skalarnym wektorów nazywamy funkcję, która dla dwóch wektorów, $|u\rangle$ i $|v\rangle$, zwraca liczbę rzeczywistą lub zespoloną, która spełnia poniższe własności:

- $\langle u|v\rangle = \langle v|u\rangle^*$,
- $(\alpha \langle u|)\,|v\rangle = \alpha \langle u|v\rangle$, $(\langle u| + \langle v|)\,|z\rangle = \langle u|z\rangle + \langle v|z\rangle$,
- $\langle u|u\rangle \geqslant 0$,
- $\langle u|u\rangle = 0$ wtedy i tylko wtedy, gdy $|u\rangle = 0$.

Przeprowadźmy teraz na wektorach następującą operację: niech będą dane dwa wektory – $|u\rangle, |v\rangle \in \mathbb{C}^n$:

$$|u\rangle = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad |v\rangle = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix};$$

wówczas

$$\langle u|v\rangle = x_1^* y_1 + x_2^* y_2 + \ldots + x_n^* y_n$$

nazywamy iloczynem skalarnym wektorów $|u\rangle$ oraz $|v\rangle$[3]. Skalarnie można mnożyć tylko wektory o tej samej liczbie elementów. Wynikiem iloczynu skalarnego jest liczba.

Kombinacja liniowa wektorów

Gdy mamy dane dwie liczby, α i β, oraz dwa wektory, $|u\rangle$ i $|v\rangle$, możemy uzyskać taki wektor

$$|z\rangle = \alpha\,|u\rangle + \beta\,|v\rangle\,,$$

który nazywamy *kombinacją liniową wektorów* $|u\rangle$ i $|v\rangle$ o współczynnikach α i β. A ogólniej: wektor

$$|z\rangle = \alpha_1\,|u_1\rangle + \alpha_2\,|u_2\rangle + \ldots + \alpha_n\,|u_n\rangle$$

nazywamy kombinacją liniową wektorów $|u_1\rangle\,, |u_2\rangle\,, \ldots, |u_n\rangle$ o współczynnikach $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Liniowa zależność wektorów

Mając dany zbiór wektorów $\{|u_1\rangle\,, |u_2\rangle\,, \ldots, |u_n\rangle\}$, mówimy, że jest on *liniowo zależny*, jeżeli istnieje jeden taki wektor $|u_i\rangle$ oraz niezerowe współczynniki $\alpha_1, \alpha_2, \ldots, \alpha_n$ takie, że:

$$\alpha_i\,|u_i\rangle = \alpha_1\,|u_1\rangle + \alpha_2\,|u_2\rangle + \ldots + \alpha_{i-1}\,|u_{i-1}\rangle + \alpha_{i+1}\,|u_{i+1}\rangle + \ldots + \alpha_n\,|u_n\rangle\,.$$

Oznacza to, że jeden z wektorów można zapisać jako kombinację liniową o niezerowych współczynnikach pozostałych wektorów.

Baza i wymiar przestrzeni wektorowej

Jeżeli zbiór n wektorów $\{|u_1\rangle\,, |u_2\rangle\,, \ldots, |u_n\rangle\}$ należących do danej przestrzeni wektorowej nie jest liniowo zależny i dodanie dowolnego wektora niezerowego z tej przestrzeni do zbioru spowoduje, że stanie się on liniowo zależny, to taki zbiór nazywamy *bazą przestrzeni wektorowej*. Wówczas mówimy, że przestrzeń wektorowa ma *wymiar* n. Każda przestrzeń wektorowa ma bazę.

Dowolny wektor możemy zapisać jako kombinację wektorów bazowych. Nas natomiast interesują tylko bazy, które jednocześnie tworzą zbiór ortonormalny, tzn. taki, że dla wektorów z bazy $\{|e_1\rangle\,, |e_2\rangle\,, \ldots |e_n\rangle\}$ zachodzi $\langle e_i|e_j\rangle = 0$ dla $i \neq j$ dla $i = 1, 2, \ldots, n$ i $j = 1, 2, \ldots, n$ oraz $\langle e_i|e_i\rangle = 0$ dla $i = 1, 2, \ldots, n$. Wtedy wektor $|u\rangle$ zapisujemy w następujący sposób:

$$|u\rangle = \langle e_1|u\rangle\,|e_1\rangle + \langle e_2|u\rangle\,|e_2\rangle + \ldots + \langle e_n|u\rangle\,|e_n\rangle\,.$$

[3]Matematycznie można zdefiniować inne iloczyny skalarne, ale nam nie będą one tu potrzebne.

W przypadku wektorów kolumnowych jedną bazę wyróżnia się szczególnie i nazywa się ją *bazą obliczeniową*. Składa się ona z wektorów:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, |n-1\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

Zapamiętajmy: nie należy mylić wektora zerowego 0 z wektorem $|0\rangle$; ten pierwszy składa się z samych zer, a drugi ma na pierwszej pozycji 1.

Norma euklidesowa

Jeżeli mamy zdefiniowany iloczyn skalarny wektorów, to możemy wprowadzić pojęcie długości wektora – lub inaczej: *normy wektora*. Normy wektorów powinny posiadać następujące własności:

- Dla każdego wektora $|u\rangle$ i liczby α: $\|\alpha\,|u\rangle\| = |a|\||u\rangle\|$.
- Dla każdych dwóch wektorów $|u\rangle$ oraz $|v\rangle$: $\||u\rangle + |v\rangle\| \leqslant \||u\rangle\| + \||v\rangle\|$.
- Tylko i wyłącznie dla wektora zerowego 0: $\|0\| = 0$.

Warto tu zauważyć, że dla każdego wektora $|u\rangle$ jego norma jest nieujemna $\||u\rangle\| \geqslant 0$. Nas będzie interesować tylko i wyłącznie *norma euklidesowa* wektora $\||u\rangle\| = \sqrt{\langle u|u\rangle}$.

W przypadku wektora kolumnowego

$$|u\rangle = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

mamy następujący wzór na normę euklidesową:

$$\begin{aligned} \||u\rangle\| = \sqrt{\langle u|u\rangle} &= \sqrt{{x_1}^* x_1 + {x_2}^* x_2 + \ldots + {x_n}^* x_n} \\ &= \sqrt{|x_1|^2 + |x_2|^2 + \ldots + |x_n|^2}. \end{aligned}$$

Wektor unormowany

Wektor $|u\rangle$, którego norma jest równa jeden $\||u\rangle\| = 1$, nazywamy *unormowanym*.

Ortogonalność

Dwa wektory $|u\rangle$ i $|v\rangle$ nazywamy *ortogonalnymi* (lub inaczej – prostopadłymi), gdy ich iloczyn skalarny wynosi zero $\langle u|v\rangle = 0$. Jeżeli wektory $|u\rangle$ i $|v\rangle$ są unormowane i ortogonalne, to nazywamy je *ortonormalnymi*.

A.3 Macierze

Macierzą nazywamy prostokątną tablicę liczb. Dla nas będą to liczby rzeczywiste lub zespolone. Przykładowo poniżej dana jest macierz o wymiarach m na n:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

Liczby a_{ij} nazywamy *elementami macierzowymi* albo po prostu elementami macierzy. Jeżeli liczby a_{ij} są rzeczywiste, to opisujemy macierz jako $\mathbf{A} \in \mathbb{R}^{mn}$, natomiast jeżeli są zespolone – $\mathbf{A} \in \mathbb{C}^{mn}$. Dlatego też zamiast pisać za każdym razem, że mówimy o macierzach lub wektorach rzeczywistych lub zespolonych, będziemy stosować znak $\mathbb{F}$[4] jako zamiennik dla $\mathbb{R}$ oraz $\mathbb{C}$.

Dodawanie

Jeżeli mamy dwie macierze $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{mn}$ o identycznych rozmiarach, to możemy je dodawać do siebie, otrzymując macierz $\mathbf{A} + \mathbf{B} \in \mathbb{F}^{mn}$. Zatem, mając dane dwie poniższe macierze:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{bmatrix},$$

dodajmy je do siebie w następujący sposób – element po elemencie:

$$\mathbf{A} + \mathbf{B} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{bmatrix}.$$

Mnożenie przez skalar

Mnożenie macierzy $\mathbf{A} \in \mathbb{F}^{mn}$ przez skalar α polega na pomnożeniu każdego elementu tej macierzy przez dany skalar. W wyniku tego działania otrzymujemy macierz $\alpha\mathbf{A} \in \mathbb{F}^{mn}$

$$\alpha\mathbf{A} = \begin{bmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \cdots & \alpha a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \cdots & \alpha a_{mn} \end{bmatrix}.$$

[4] Z angielskiego *field*, czyli ciało liczbowe.

Transpozycja

Transpozycja macierzy $\mathbf{A} \in \mathbb{F}^{mn}$ polega na zamianie wierszy tej macierzy z jej kolumnami. Otrzymujemy wówczas macierz $\mathbf{A}^T \in \mathbb{F}^{nm}$:

$$\mathbf{A}^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}.$$

Sprzężenie hermitowskie

Sprzężenie hermitowskie macierzy $\mathbf{A} \in \mathbb{F}^{mn}$ to połączenie transpozycji macierzy ze sprzężeniem zespolonym każdego jej elementu; zatem $\mathbf{A}^\dagger \in \mathbb{F}^{nm}$ ma postać:

$$\mathbf{A}^\dagger = \begin{bmatrix} {a_{11}}^* & {a_{21}}^* & \cdots & {a_{m1}}^* \\ {a_{12}}^* & {a_{22}}^* & \cdots & {a_{m2}}^* \\ \vdots & \vdots & \ddots & \vdots \\ {a_{1n}}^* & {a_{2n}}^* & \cdots & {a_{mn}}^* \end{bmatrix}.$$

Zauważmy, że dla macierzy rzeczywistych sprzężenie hermitowskie i transpozycja zachowują się tak samo.

Mnożenie macierzy przez wektor kolumnowy

Mnożenie macierzy $\mathbf{A} \in \mathbb{F}^{mn}$ z prawej strony przez wektor kolumnowy $|x\rangle \in \mathbb{F}^n$ polega na policzeniu sumy iloczynów elementów macierzy z odpowiednimi elementami wektora. Otrzymujemy wtedy $\mathbf{A}\,|x\rangle \in \mathbb{F}^m$:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \quad |x\rangle = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},$$

$$\mathbf{A}\,|x\rangle = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix}.$$

Zauważmy, że liczba elementów wektora „wejściowego” odpowiada liczbie wierszy macierzy, a liczba elementów wektora „wyjściowego” odpowiada liczbie kolumn.

Mnożenie macierzy przez macierz

Operacje dodawania i mnożenia macierzy przez skalar są intuicyjne. *Mnożenie macierzy* przez siebie jest nieco bardziej złożone. Jeżeli mamy dane macierze $\mathbf{A} \in \mathbb{F}^{mk}$ oraz $\mathbf{B} \in \mathbb{F}^{kn}$

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k1} & b_{k2} & \cdots & b_{kn} \end{bmatrix},$$

to wynikiem ich wymnożenia jest macierz $\mathbf{C} \in \mathbb{F}^{mn}$

$$\mathbf{C} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$$

taka, że jej elementy macierzowe c_{ij} mają następująca postać:

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj}, \text{ dla } i = 1, 2, \ldots, m \text{ oraz } j = 1, 2, \ldots, n.$$

Iloczyn macierzowy można rozumieć również w następujący sposób: jeżeli zapiszemy macierz $\mathbf{A}$ jako wektor kolumnowy wektorów wierszowych

$$\mathbf{A} = \begin{bmatrix} \langle a_1| \\ \langle a_2| \\ \vdots \\ \langle a_k| \end{bmatrix},$$

gdzie $\langle a_1| = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1k} \end{bmatrix}, \langle a_2| = \begin{bmatrix} a_{21} & a_{22} & \ldots & a_{2k} \end{bmatrix}, \ldots, \langle a_m| = \begin{bmatrix} a_{m1} & a_{m2} & \ldots & a_{mk} \end{bmatrix}$, natomiast macierz $\mathbf{B}$ jako wektor wierszowy wektorów kolumnowych

$$\mathbf{B} = \begin{bmatrix} |b_1\rangle & |b_2\rangle & \ldots & |b_n\rangle \end{bmatrix},$$

gdzie

$$|b_1\rangle = \begin{bmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{k1} \end{bmatrix}, \quad |b_1\rangle = \begin{bmatrix} b_{12} \\ b_{22} \\ \vdots \\ b_{k2} \end{bmatrix}, \quad \ldots, \quad |b_1\rangle = \begin{bmatrix} b_{1n} \\ b_{2n} \\ \vdots \\ b_{kn} \end{bmatrix},$$

to iloczyn macierzy $\mathbf{C} = \mathbf{AB}$ można zapisać jako macierz iloczynów skalarnych

$$\mathbf{C} = \begin{bmatrix} \langle a_1|b_1\rangle & \langle a_1|b_2\rangle & \cdots & \langle a_1|b_n\rangle \\ \langle a_2|b_1\rangle & \langle a_2|b_2\rangle & \cdots & \langle a_2|b_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle a_m|b_1\rangle & \langle a_m|b_2\rangle & \cdots & \langle a_m|b_n\rangle \end{bmatrix}.$$

Macierz zerowa

Macierz $\mathbf{0} \in \mathbb{F}^{mn}$, która składa się z samych zer

$$\mathbf{0} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix},$$

nazywamy *zerową*. Dla dowolnych macierzy $\mathbf{A} \in \mathbb{F}^{km}$ oraz $\mathbf{B} \in \mathbb{F}^{nl}$ mamy

$$\mathbf{A0} = \mathbf{0} \in \mathbb{F}^{kn},\ \mathbf{0B} = \mathbf{0} \in \mathbb{F}^{ml}.$$

Macierz diagonalna

Macierz kwadratowa $\mathbf{A}_m \in \mathbb{F}^{mm}$, która wygląda następująco:

$$\mathbf{A} = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{mm} \end{bmatrix},$$

nazywana jest *macierzą diagonalną*. Elementy $a_{11}, a_{22}, \ldots, a_{mm}$ nazywane są *przekątną macierzy*, bądź jej *diagonalą*.

Macierz jednostkowa

Macierz kwadratową $\mathbf{I}_m \in \mathbb{F}^{mm}$ diagonalną, która ma jedynki na przekątnej

$$\mathbf{I}_m = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

nazywamy *jednostkową*. Macierz taka zachowuje się w mnożeniu macierzowym jak 1 w mnożeniu skalarnym. Weźmy macierze $\mathbf{A} \in \mathbb{F}^{km}$ oraz $\mathbf{B} \in \mathbb{F}^{mn}$. Uzyskamy wtedy

$$\mathbf{AI}_m = \mathbf{A},\ \mathbf{I}_m\mathbf{B} = \mathbf{B}.$$

Macierz odwrotna

Dla macierzy kwadratowej $\mathbf{A} \in \mathbb{F}^{mm}$ może (ale nie musi) istnieć macierz $\mathbf{A}^{-1} \in \mathbb{F}^{mm}$, która daje

$$\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_m.$$

Macierz $\mathbf{A}^{-1}$ nazywamy *odwrotną* do macierzy $\mathbf{A}$. W zależności od tego, jaką jest macierz $\mathbf{A}$, macierz $\mathbf{A}^{-1}$ może istnieć lub nie. Nie będziemy się tu zajmować warunkami istnienia macierzy odwrotnej, gdyż – jak zobaczymy później – dla macierzy nas interesujących macierze odwrotne będą istnieć zawsze i w dodatku będą miały szczególną postać.

Iloczyn Kroneckera

Dla danych dwóch macierzy $\mathbf{A} \in \mathbb{F}^{mn}$ i $\mathbf{B} \in \mathbb{F}^{kl}$ wynikiem ich *iloczynu Kroneckera* jest taka macierz $\mathbf{C} \in \mathbb{F}^{m\times k, n\times l}$, która powstaje przez pomnożenie każdego elementu macierzowego macierzy $\mathbf{A}$ przez całą macierz $\mathbf{B}$, tak jak w poniższym wzorze:

$$\mathbf{C} = \mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \cdots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & a_{m2}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{bmatrix}.$$

Zauważmy, że wymiary macierzy wynikowej to $m \times k$ na $n \times l$. Poniżej wymienimy listę własności iloczynu Kroneckera, które są potrzebne do zrozumienia własności obwodów kwantowych:

- Iloczyn Kroneckera nie musi być przemienny: $\mathbf{A} \otimes \mathbf{B} \neq \mathbf{B} \otimes \mathbf{A}$.
- Rozdzielność iloczynu Kroneckera względem dodawania:

$$\mathbf{A} \otimes (\mathbf{B} + \mathbf{C}) = \mathbf{A} \otimes \mathbf{B} + \mathbf{A} \otimes \mathbf{C},$$

$$(\mathbf{A} + \mathbf{B}) \otimes \mathbf{C} = \mathbf{A} \otimes \mathbf{C} + \mathbf{B} \otimes \mathbf{C}.$$

- Łączność mnożenia przez skalar: $(c\mathbf{A}) \otimes \mathbf{B} = \mathbf{A} \otimes (c\mathbf{B}) = c(\mathbf{A} \otimes \mathbf{B})$.
- Łączność iloczynu Kroneckera: $(\mathbf{A} \otimes \mathbf{B}) \otimes \mathbf{C} = \mathbf{A} \otimes (\mathbf{B} \otimes \mathbf{C})$.
- Jeżeli możemy pomnożyć macierze $\mathbf{A}$ i $\mathbf{C}$ oraz $\mathbf{B}$ i $\mathbf{D}$, to:

$$(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = (\mathbf{AC}) \otimes (\mathbf{BD}).$$

- Odwrotność: $(\mathbf{A} \otimes \mathbf{B})^{-1} = \mathbf{A}^{-1} \otimes \mathbf{B}^{-1}$.
- Transpozycja oraz sprzężenie hermitowskie:

$$(\mathbf{A} \otimes \mathbf{B})^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}} \otimes \mathbf{B}^{\mathrm{T}}, \quad (\mathbf{A} \otimes \mathbf{B})^{\dagger} = \mathbf{A}^{\dagger} \otimes \mathbf{B}^{\dagger}.$$

Iloczyn zewnętrzny

Nazwą *iloczyn zewnętrzny* wektora kolumnowego

$$|u\rangle = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

i wektora wierszowego

$$\langle v| = \begin{bmatrix} y_1 & y_2 & \cdots & y_m \end{bmatrix}$$

określamy macierz powstałą z iloczynu macierzowego tych wektorów:

$$|u\rangle\langle v| = \begin{bmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_m \\ x_2y_1 & x_2y_2 & \cdots & x_2y_m \\ \vdots & \vdots & \ddots & \cdots \\ x_ny_1 & x_ny_2 & \cdots & x_ny_m \end{bmatrix}.$$

Notacja Diraca

W tym miejscu mamy dość wiedzy, by docenić notację Diraca. Iloczyn skalarny $\langle u|v\rangle$ wektorów $|u\rangle$ i $|v\rangle$ czytamy jako „*braket* u v”[5]. Natomiast iloczyn $|u\rangle\langle v|$ czytamy jako „*ketbra* u v”. Interesujące jest zatem wyrażenie $|u\rangle\langle v|x\rangle$, w którym nawiasy możemy rozłożyć w taki sposób: $|u\rangle\left(\langle v|x\rangle\right)$ lub tak: $\left(|u\rangle\langle v|\right)|x\rangle$. Wzory te mają różne znaczenie, ale ponieważ sprowadzają się one do mnożenia macierzy, mają tę samą wartość. Co ciekawe, od razu można zauważyć, że wyrażenie $|u\rangle\langle v|x\rangle$ jest równe wyrażeniu $\langle v|x\rangle\,|u\rangle$, ponieważ mnożenie skalara przez wektor jest przemienne.

Macierze unitarne

Macierze kwadratowe, które przy mnożeniu z prawej strony przez wektor nie zmieniają jego normy, nazywamy macierzami *unitarnymi*. Znaczy to, że dla każdego $|u\rangle \in \mathbb{F}^n$ i dla każdej macierzy unitarnej $\mathbf{U} \in \mathbb{F}^{nn}$ mamy

$$\|\mathbf{U}\,|u\rangle\| = \||u\rangle\|.$$

Dla każdej macierzy unitarnej $\mathbf{U}$ istnieje macierz odwrotna $\mathbf{U}^{-1}$, tzn.:

$$\mathbf{U}\mathbf{U}^{-1} = \mathbf{U}^{-1}\mathbf{U} = \mathbf{I}_m.$$

Dlatego macierze unitarne często utożsamiane są z obrotami. Macierze unitarne mają pewną ciekawą własność – ich odwrotność jest ich sprzężeniem hermitowskim, tzn. $\mathbf{U}^{-1} = \mathbf{U}^\dagger$.

Zauważmy, że jeżeli macierz $\mathbf{U}$ przekształca $|u\rangle$ na $|v\rangle$, to macierz $\mathbf{U}^\dagger$ przekształca $|v\rangle$ na $|u\rangle$, tzn. jeżeli $|v\rangle = \mathbf{U}\,|u\rangle$, to $|u\rangle = \mathbf{U}^\dagger\,|v\rangle$.

[5] Ang. „bracket” – nawias.

A.4 Podsumowanie

Przedstawiony powyżej formalizm matematyczny pozwala zrozumieć podstawy informatyki kwantowej. Zauważcie, że zaczęliśmy ten dodatek od liczb zespolonych – czyli pewnego opisu obrotów na płaszczyźnie – a skończyliśmy na macierzach unitarnych, które opisują obroty w przestrzeniach wektorowych. Jak widać, mechanika kwantowa jest zbudowana na obrotach, które możemy nazwać – z łaciny – rewolucjami.

O autorach

Piotr Gawron

Informatyk kwantowy pracujący w Instytucie Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk w Gliwicach. Jego zainteresowania naukowe obejmują kwantowe języki programowania, gry kwantowe, ograniczone obrazy i cienie numeryczne macierzy, sieci tensorowe oraz statystyczną analizę wyników wyborów powszechnych. Od wielu lat aktywny członek polskiego fandomu fantastyki naukowej. Kiedyś organizator i współorganizator konwentów fantastyki. Ostatnio zaangażowany w popularyzację nauki na konwentach. Miłośnik rocka francuskiego.

Michał Cholewa

Matematyk z wykształcenia, fantasta z zamiłowania, informatyk z zawodu. Nałogiem czytania zarażono go podstępnie za młodu; zainteresowanie matematyką przyszło wkrótce potem, kiedy okazała się zdecydowanie bardziej przejrzysta niż nauki miękkie. Obronił doktorat w Instytucie Informatyki Teoretycznej i Stosowanej PAN, gdzie do dzisiaj pracuje w Zespole Systemów Multimedialnych. Fan twórczości Stanisława Lema, Joe'ego Haldemana, Teda Chianga i Petera Wattsa. Oraz słodyczy. Laureat Nagrody im. Janusza Zajdla w roku 2015 za „Fortę" oraz Srebrnego Wyróżnienia Nagrody Literackiej im. Jerzego Żuławskiego za tę samą powieść.

Katarzyna Kara

Z wykształcenia – graficzka; na co dzień zajmuje się rysunkiem koncepcyjnym, tworzy komiksy (acz głównie do szuflady), robi ilustracje i maluje murale. Absolwentka ASP w Katowicach. Ukończyła kierunek grafika warsztatowa, jej dyplom dotyczył litografii bawnej, a praca teoretyczna nosiła tytuł: „Graficzna struktura porządkowa w komiksie: jej zastosowanie oraz psychofizjologiczne źródła". Aneksem do dyplomu był natomiast komiks „Alice". Lubi fantastykę, a w wolnych chwilach gra w LARP-y i planszówki. „Rewolucja stanu" to jej książkowy debiut.

Skorowidz

Bibliografia

[1] Michel Le Bellac. *Wstęp do informatyki kwantowej.* Wydawnictwo Naukowe PWN, Warszawa, 2012.

[2] Marian Chudy. *Wprowadzenie do Informatyki Kwantowej.* Akademicka Oficyna Wydawnicza Exit, Warszawa, 2011.

[3] Richard Feynman. *Wykłady o obliczeniach.* Prószyński i S-ka, Warszawa, 2007.

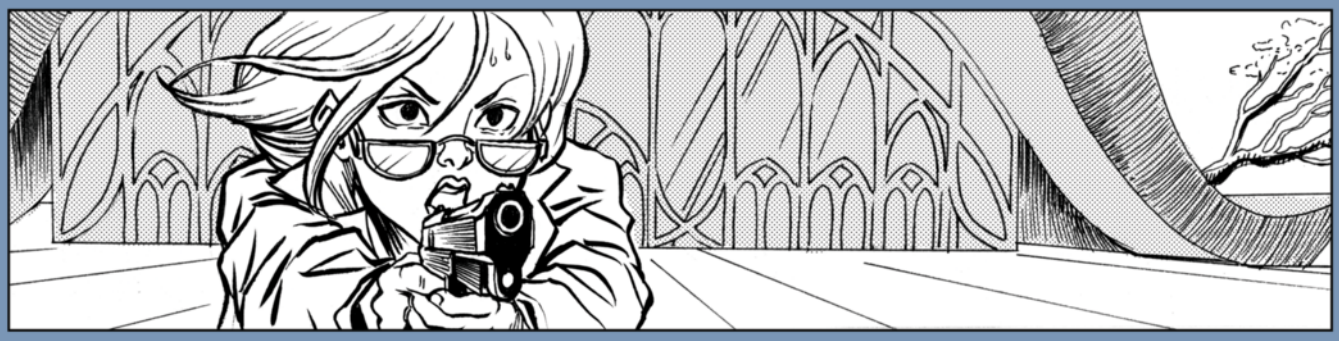
[4] Krzysztof Giaro, Marcin Kamiński. *Wprowadzenie do algorytmów kwantowych.* Akademicka Oficyna Wydawnicza EXIT, Warszawa, 2003.

[5] Mika Hirvensalo. *Algorytmy kwantowe.* Wydawnictwa Szkolne i Pedagogiczne, Warszawa, 2004.

[6] Gerard J. Milburn. *Procesor Feynmana: wprowadzenie do obliczeń kwantowych.* Wydawnictwo CiS, Warszawa, 2000.

[7] Joanna Wiśniewska, Marek Sawerwain. *Informatyka kwantowa.* Wydawnictwo Naukowe PWN, Warszawa, 2015.

[8] Stefan Węgrzyn, Jerzy Klamka, Sławomir Bugajski, Mirosław Gibas, Ryszard Winiarczyk, Lech Znamirowski, Jarosław A. Miszczak, Sławomir Nowak. *Nano i Kwantowe Systemy Informatyki.* Wydawnictwo Politechniki Śląskiej, Gliwice, 2003.



ŚWIAT, JAKI ZNAMY – ŚWIAT WOLNYCH SIECI INFORMACYJNYCH, ŚWIAT SWOBODNEJ WYMIANY WIEDZY I DOŚWIADCZEŃ – SKOŃCZYŁ SIĘ NIEODWOŁALNIE. WOLNY DOSTĘP DO WIEDZY OKAZAŁ SIĘ SZKODLIWĄ IDEĄ, A NAJBARDZIEJ SKORZYSTALI NA NIM ZBRODNIARZE, TWÓRCY BRONI BIOLOGICZNEJ, KTÓRA NIEOMAL ZMIOTŁA CYWILIZACJĘ Z POWIERZCHNI ZIEMI. ZDZIESIĄTKOWANA PRZEZ TERROR, WOJNY I EPIDEMIĘ LUDZKOŚĆ POWOLI ODRADZA SIĘ POD CZUJNYM OKIEM CERBERA. JEGO AGENCI MAJĄ JEDEN CEL: NIE DOPUŚCIĆ, ABY WIEDZA STAŁA SIĘ ZNÓW POWSZECHNIE DOSTĘPNA.

JEDNAK WSZECHOBECNA CENZURA RODZI BUNT. NIEKTÓRZY SĄ NAWET GOTOWI GINĄĆ – I ZABIJAĆ – ZA WOLNY DOSTĘP DO INFORMACJI. I NAJWYRAŹNIEJ CZUJĄ SIĘ DOŚĆ PEWNIE, BY RZUCIĆ CERBEROWI WYZWANIE – BO CZYM INNYM MOŻE BYĆ ZAMACH NA WYSOKIEGO DYGNITARZA ORGANIZACJI W JEJ GŁÓWNEJ KWATERZE? TERAZ CERBER MUSI UŻYĆ WSZYSTKICH DOSTĘPNYCH ŚRODKÓW, BY ZNALEŹĆ ZLECENIODAWCÓW NAPASTNIKA. NIESTETY, JEGO AS ATUTOWY, KWANTOWA HAKERKA EVE, WŁAŚNIE ZASIADA NA ŁAWIE OSKARŻONYCH POD ZARZUTEM ZDRADY NA RZECZ GRUPY TERRORYSTYCZNEJ ALICE...

ISBN 9788392605416

9 788392 605416

IITiS
INSTYTUT INFORMATYKI TEORETYCZNEJ i STOSOWANEJ PAN

Oddajemy w ręce Czytelnika nietypowe wydawnictwo składające się z dwóch części: pierwsza to komiks akcji, którego tematyka nawiązuje do pewnych zagadnień informatyki kwantowej, druga – to podręcznik z wyłożonymi podstawami tej dziedziny.

Autor części podręcznikowej, Piotr Gawron – pracownik naukowy Instytutu Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk – wyjaśnia: *„Chciałem stworzyć publikację na temat informatyki kwantowej, która byłaby zrozumiała dla mnie samego z czasów, kiedy miałem osiemnaście lat. Szukałem wtedy informacji o mechanice kwantowej, ale publikacje popularnonaukowe były – z mojej perspektywy – napisane zbyt niejasnym językiem. Dlatego postanowiłem, że w tym podręczniku będę używać języka zrozumiałego dla umysłów ścisłych – języka matematyki. Uznałem jednak, że sam wykład to trochę za mało, żeby przyciągnąć takiego czytelnika, jakim byłem w czasach nauki w liceum. Stąd pomysł, aby podstawy informatyki kwantowej pokazać w formie futurystycznego, sensacyjnego komiksu”.*

Książka została przygotowana dzięki programowi eNgage, będącemu częścią projektu SKILLS, realizowanego przez Fundację na rzecz Nauki Polskiej.

Promuje on nowatorskie przedsięwzięcia popularnonaukowe, których celem jest nie tylko w przystępny sposób mówić o nauce, ale też być dla ich twórców okazją do nabycia nowych umiejętności. Macie zatem przed sobą książkę-eksperyment; jednak, jako jej autorzy, liczymy, że będziecie się przy niej dobrze bawić – niezależnie od tego, czy przeczytacie jedną, czy obie jej części.