Temat 17

Orzeł czy reszka? — Protokoły kryptograficzne

Streszczenie

Zajęcia pozwolą zrozumieć jak zrealizować proste, lecz pozornie niemożliwe do wykonania zadanie polegające na uczciwym dokonaniu wyboru poprzez rzut monetą, przez ludzi, którzy sobie nie ufają, a mają kontakt jedynie telefoniczny.

Wskazane jest, by zajęcia poprzedzone były zajęciami nr 1 (nt. cyfr dwójkowych), nr 4 (nt. parzystości) oraz nr 14 (nt. funkcji jednokierunkowych).

Wiek

- ✓ 9 lat i więcej

Materiały

Każda grupa dzieci otrzyma:

- ✓ kartę pracy: Symulacja rzutu kostką
- ✓ ok. 25 żetonów w dwóch kolorach

Orzeł czy reszka?

Wprowadzenie

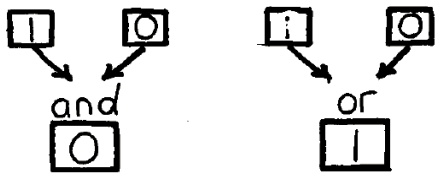
Pierwsza wersja scenariusza powstawała w czasie, gdy jeden z autorów (Mike Fellows) pracował w szkole w Peru. Stąd taka a nie inne fabuła towarzyszącej zajęciom opowieści.

Żeńskie drużyny piłkarskie z miast Lima i Cuzco mają zdecydować, w którym z nich rozegrany będzie finał rozgrywek pucharowych. Najprostszym rozwiązaniem wydaje się rzut monetą. Jednak miasta są od siebie znacznie oddalone i ze względów finansowych jak i czasowych nie jest możliwe, by przedstawiciele drużyn spotkały się przed meczem w celu wykonania rzutu monetą. Czy mogą to zrobić przez telefon? Wydaje się, że tak – Alicja, przedstawicielka pierwszego klubu, mogłaby rzucać monetą, a Bob, przedstawiciel drugiego klubu, mógłby obstawić „orzeł" lub „reszka". Niestety nikt nie może zagwarantować, że Alicja zachowa się uczciwie. Co więcej, znaczenie i waga turnieju może sprawić, że trudno będzie nie ulec pokusie kłamstwa (po jednej stronie) czy podejrzeń o nieuczciwość (po drugiej stronie).

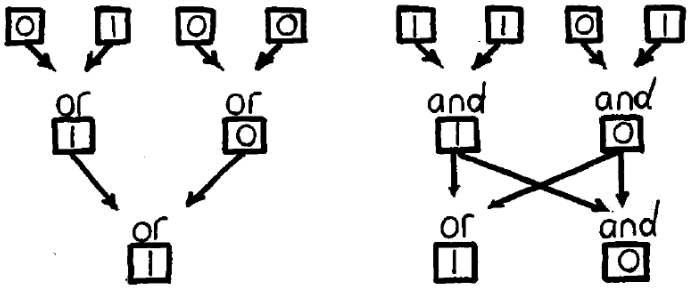
Drużyny – jak przekonamy się o tym w czasie zajęć -- znajdują jednak sposób na rozwiązanie problemu braku wzajemnego zaufania. Wspólnie projektują układ elektroniczny, złożony z bramek logicznych typu AND i bramek OR. Projekt mógłby powstać przez telefon, ale ze względów praktycznych lepiej posłużyć się urządzeniem typu fax. W czasie projektowania każda ze stron musi zadbać o to, by układ był wystarczająco złożony, aby niemożliwe było oszukiwanie. Obie drużyny powinny mieć pełną wiedzę na temat konstrukcji układu.

Omówienie

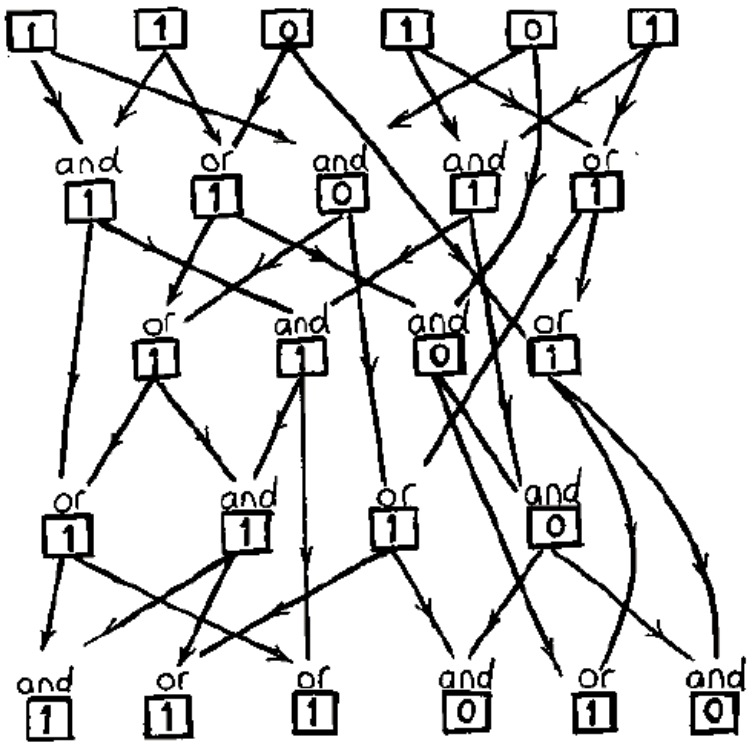
Zasady działania bramek logicznych są proste. Każda z nich ma dwa wejścia i jedno wyjście. Na każdym wejściu może się pojawić jedna z dwóch wartości: 0 (fałsz) lub 1 (prawda). Na wyjściu bramki AND wartość 1 (prawda) pojawi się wówczas, gdy obie z wartości na wejściu są równe 1 (prawda) lub 0 (fałsz). Dla przykładu: jeśli bramka AND ma na wejściach 0 i 1, to na wyjściu pojawi się 0. Bramka OR ma na wyjściu wartość 1 jeśli przynajmniej jedno z wejść ma wartość 1 a wartość 0 – tylko jeśli obie wartości wejścia to 0.



Wyjście jednej bramki może stać się wejściem innej (czy nawet kilku innych). Dzięki temu istnieje możliwość stworzenia bardziej skomplikowanego układu logicznego. Poniżej znajduje się ilustracja dwóch przykładowych układów. Pierwszy (pokazany na rysunku po lewej stronie) powstaje, gdy wyjścia dwóch bramek OR połączymy z wejściami trzeciej tego rodzaju bramki, to w efekcie uzyskamy układ, który na wyjściu będzie mieć wartość 1, jeśli tylko którykolwiek z czterech wejść będzie równe 1. Drugi jest jeszcze bardziej złożony: wyjście każdej z dwóch bramek AND jest podłączone do wejścia dwóch bramek różnego rodzaju, więc na wyjściu całego układu pojawiają się dwie wartości



Układ, który można by użyć do symulacji rzutu kostką w problemie drużyn piłkarskich musi być bardziej złożony. Będzie miał sześć wartości na wejściu i sześć na wyjściu. Zilustrowano na nim przebieg jednej z symulacji.



W jaki sposób taki układ może być używany to wykonania rzutu monetą przez telefon? Alicja wybiera w sposób losowy dane wejściowe w postaci sześciu cyfr 0 lub 1. Informację tę zachowuje w tajemnicy. Do Boba przesyła natomiast cyfry, które pojawiają się na wyjściu układu. Boba, jeśli chce wygrać, musi odgadnąć, czy wśród cyfr na wejściu była parzysta czy nieparzysta liczba cyfr 1 – mówiąc inaczej musi odgadnąć parzystość wejścia układu. Jeśli układ bramek logicznych jest odpowiednio złożony, to Bob nie jest w stanie odkryć, jaka jest właściwa odpowiedź i zmuszony jest do wybierania w sposób losowy (może w tym celu rzucić nawet monetą!). Bob wygra – i mecz play-off odbędzie się w Cuzo – jeśli jego przypuszczenia okażą się słuszne. Alicja wygra – i mecz odbędzie się w Limie – jeśli Bob pomyli się. Niezwłocznie po przekazaniu przez Boba sugestii, Alicja ujawnia utrzymywane w tajemnicy cyfry wejściowe. Dzięki temu-Bob będzie mógł sprawdzić sam, czy na wyjściu pojawi się wcześniej podany wynik.

1. Podziel dzieci na małe grupy, przekaż kartkę z ilustracją układu i żetony, a następnie przedstaw odpowiednią narrację. Być może dzieci powinny wyobrazić sobie, że jedno z nich jest kapitanem, który bierze udział w losowaniu dotyczącym meczu z lokalnym rywalem szkoły. Należy ustalić konwencję dotyczącą kolorów żetonów – np. czerwone to 0, niebieskie – 1. Dzieci powinny to ustalenie zaznaczyć w legendzie karty pracy.

2. Pokaż dzieciom, w jaki sposób umieszczać powinny żetony na wejściu. Wyjaśnij zasady działania bramek AND i OR – ich krótki opis znajduje się u dołu karty (rozważ, czy dzieci nie powinny pokolorować opisu).

3. Pokaż, w jaki sposób dzieci mają posługiwać się schematem układu tak, aby na wyjściu pojawiły się odpowiednie wartości. To wymaga od nich dokładności i ostrożności. Poniższa tabela (która nie powinna być pokazywana dzieciom) przedstawia kompletny zbiór możliwych par: wejście – wyjście.

Input	000000	000001	000010	000011	000100	000101	000110	000111
Ouput	000000	010010	000000	010010	010010	010010	010010	010010
Input	001000	001001	001010	001011	001100	001101	001110	001111
Ouput	001010	011010	001010	011010	011010	011010	011010	011111
Input	010000	010001	010010	010011	010100	010101	010110	010111
Ouput	001000	011010	001010	011010	011010	011010	011010	011111
Input	011000	011001	011010	011011	011100	011101	011110	011111
Ouput	001010	011010	001010	011010	011010	011010	011010	011111
Input	100000	100001	100010	100011	100100	100101	100110	100111
Ouput	000000	010010	011000	011010	010010	010010	011010	011010
Input	101000	101001	101010	101011	101100	101101	101110	101111
Ouput	001010	011010	011010	011010	011010	011010	011010	011111
Input	110000	110001	110010	110011	110100	110101	110110	110111
Ouput	001000	011010	011010	011010	011010	111010	011010	111111
Input	111000	111001	111010	111011	111100	111101	111110	111111
Ouput	001010	011010	011010	011010	011010	111010	011010	111111

4. Teraz w każdej grupie powinien zostać dokonany podział na dwa zespoły. Następnie należy wybrać przedstawicieli zespołów: Alę i Boba. Alicja w sposób losowy ustala dane wejściowe, następnie oblicza ciąg wartości na wyjściu, którą przekazuje Benkowi. On w tym momencie próbuje odgadnąć parzystość danych wejściowych (tj. czy liczba cyfr „1” na wejściu jest parzysta czy nieparzysta). Wszyscy mogą się naocznie przekonać, że Bob po prostu zgaduje. Następnie Alicja ujawnia wszystkim dane wejściowe układu i można sprawdzić, kto wygrał (w razie wątpliwości można sprawdzić – jeśli ktoś podejrzewa, że w międzyczasie Alicja zmieniła wybór – wartość na wyjściu układu dla ujawnionych danych wejściowych). W tym momencie symulację rzutu kostką można uznać za zakończoną.

Bob mógłby oszukiwać, jeśli byłby w stanie, znając ciąg wartości na wyjściu układu, odkryć odpowiadające my dane wejściowe. W interesie Alicji jest więc zadbać o to, by układ logiczny przedstawiał funkcję jednokierunkową (w sensie określonym w czasie zajęć nr 14), co uniemożliwia Bobowi oszukiwanie. Funkcja jednokierunkowa to taka, w przypadku której łatwo wyznaczyć wartość dla konkretnych danych wejściowych, a niezmiernie trudno określić dane wejściowe odpowiadające konkretnym wartościom.

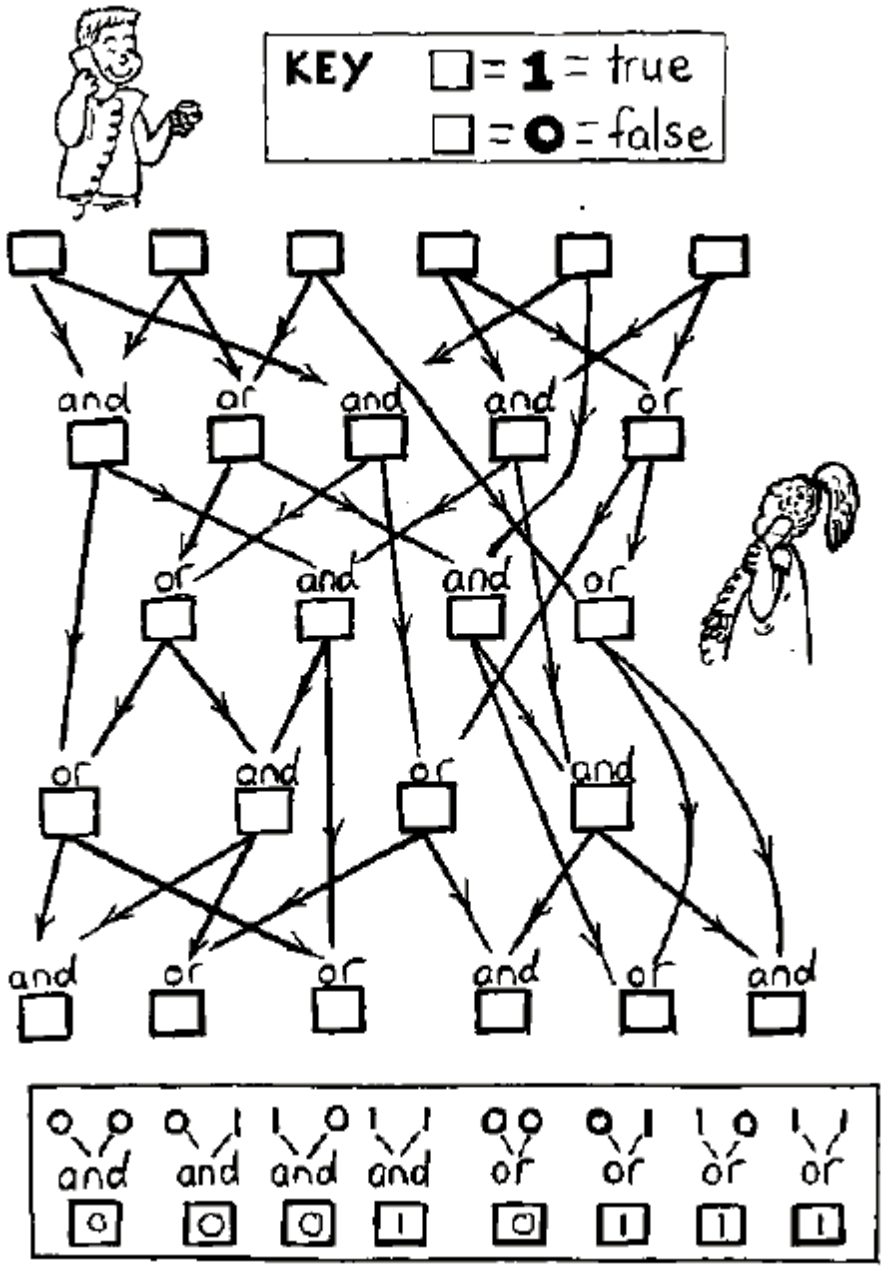
Alicja mogłaby oszukiwać, jeśli potrafiłaby znaleźć dane wejściowe o różnej parzystości, które dają ten sam ciąg wartości na wyjściu. Zadaniem Boba jest więc zapewnienie tego, by możliwie mało różnych danych dawało takie same ciągi wartości na wyjściu układu.

5. Warto zapytać dzieci o to, czy rozumieją od czego zależy uczciwość Alicji i Boba. Układ przedstawiony na kartce pozwala czasem Alicji na oszukiwanie – jak pokazuje tabela np. ciąg wartości 010010 odpowiada kilku różnym danym wejściowym: 000001, 000011, 000101 itd. Dla porównania ciąg 011000 odpowiada już tylko wejściu 00010. Trzeba mieć świadomość, że w przypadku realizacji komputerowej układu liczba używanych bitów byłaby większa (każdy kolejny bit podwaja liczbę możliwych ciągów).

6. Poproś grupy dzieci, aby zaprojektowały swój własny układ logiczny na potrzeby symulacji rzutu monetą. Niech zastanowią się, czy można stworzyć projekt, który ułatwiałby oszukiwanie którejś ze stron. Nie ma powodu, by układ składał się koniecznie z sześciu wejść. Liczba wejść nie musi też być równa liczbie wyjść.

Karta pracy: Symulacja rzutu kostką

Wybierz dowolnie dane wejściowe układu i wyznacz ciąg wartości na wyjściu.

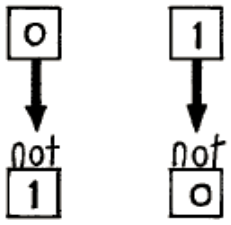


Modyfikacje i wersje rozszerzone

1. W praktyce problemem jest wymaganie współpracy przy tworzeniu układu (obwodu), który będzie do przyjęcia przez obie zainteresowane strony. Może wydawać się to wręcz niewykonalne – zwłaszcza przez telefon! Okazuje się jednak, że istnieje rozwiązanie – tworzone są niezależnie od siebie dwa układy, które udostępniane są przez obie strony sobie nawzajem: Alicja wyznacza wartości wyjściowe obu układów dla tych samych danych i ustala ostateczny układ bitów na zasadzie „1 – jeśli na obu wyjściach było 1, 0 – w przeciwnym wypadku". Dzięki zastosowaniu tego rozwiązania przedstawiciel żadnej ze stron nie może oszukiwać – jeśli jeden z układów jest funkcją jednokierunkową, to złożenie dwóch układów również jest funkcją jednokierunkową.

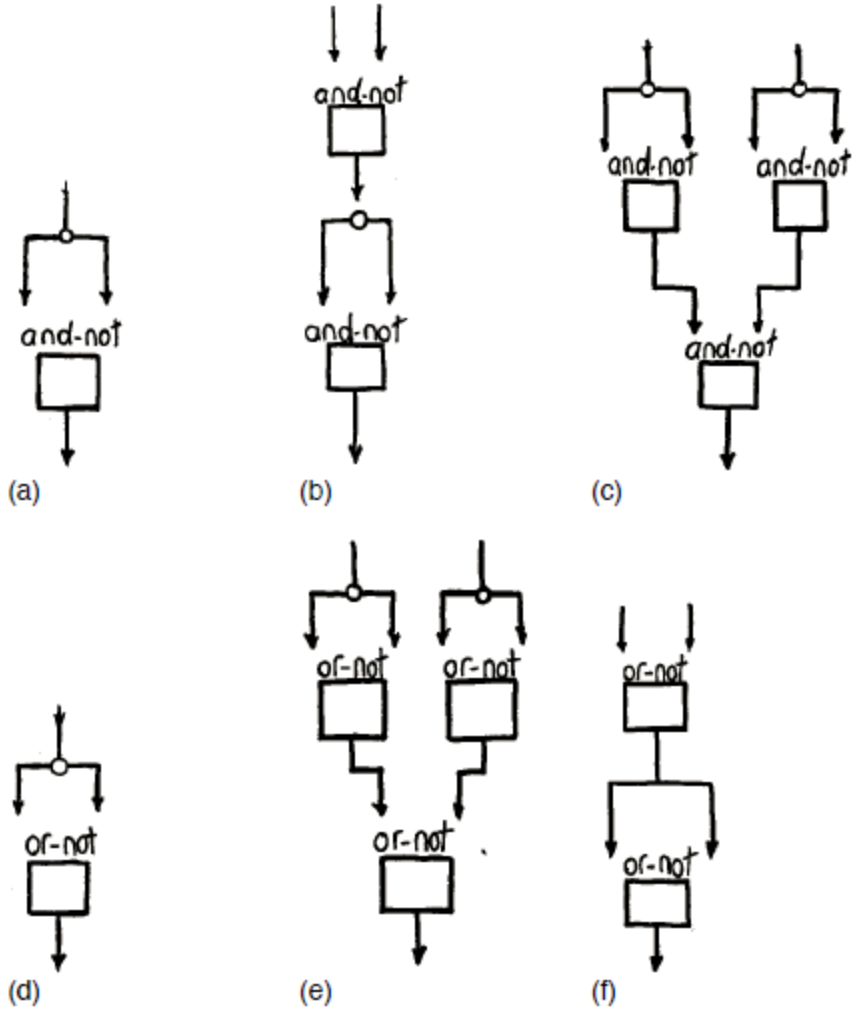
Dwie kolejne propozycje nie odnoszą się bezpośrednio do tematu protokołów kryptograficznych, ale raczej dotyczą koncepcji układów logicznych złożonych z bramek AND i OR. Pozwalają na badanie pewnych ważnych pojęć, które są fundamentalne nie tylko dla układów komputerowych, ale dla samej logiki jako takiej. Chodzi o pojęcie algebry Boole'a (matematyk George Boole żył w latach 1815-64).

2. Dzieci mogą zauważyć, że ciąg 000000 na wejściu zawsze determinuje taki sam ciąg na wyjściu, a ciąg 111111 wiąże się z otrzymaniem identycznego ciągu na wyjściu. (Mogą przy tym istnieć inne różnocyfrowe dane wyjściowe, którym na wyjściu odpowiadać będzie 000000 czy 111111.) To prosta konsekwencja tego, że układ składa się z bramek AND i OR. Przez dodanie bramek NOT, których działanie polega na zmianie wartości bitu 0 → 1 lub 1 → 0), dzieci mogą stworzyć układ, pozbawiony ww. własności.



3. Istnieją dwa inne ważne rodzaje bramek: AND-NOT oraz OR-NOT. Odpowiadają one prostym układom bramek AND i NOT oraz OR i NOT. Inaczej mówiąc np. „a AND--NOT b" odpowiada układowi „NOT (a AND b). Ich znaczenie wynika z tego, że posiadają interesująca własność: wszystkie inne rodzaje bramek można uzyskać przez złożenie odpowiedniej liczby bramek AND-NOT, jak i OR-NOT.

Po przedstawieniu tych dwóch rodzajów bramek, zachęć dzieci to zbadania, czy różne rodzaje bramek mogą powstać przez złożenie innych bramek logicznych (różnego lub nawet tego samego rodzaju). Poniższy rysunek pokazuje, jak za pomocą bramek AND-NOT (na górze) i OR-NOT (na dole) stworzyć trzy podstawowe rodzaje bramek.



O co w tym wszystkim chodzi?

W ciągu ostatnich lat dostrzegamy ogromny rozwój handlu internetowego. Sprawą niezwykle istotną jest zapewnienie bezpieczeństwa elektronicznych transakcji finansowych i wymiany prawnie wiążących dokumentów podpisanych cyfrowo. Bezpieczeństwo i poufność (tajność) komunikacji w sieciach komputerowych jest możliwa do zrealizowania dzięki zastosowaniu odpowiednich technik kryptograficznych. Już ponad 30 lat temu informatycy-naukowcy stworzyli podstawy kryptografii klucza publicznego (jest o tym mowa w czasie zajęć nr 18).

Kryptografia nie zajmuje się tylko problemem utajniania informacji, ale również ograniczonego (kontrolowanego) wykorzystania informacji poufnych oraz budowania zaufania pomiędzy osobami odległymi od siebie geograficznie. Wynalezione zostały metody (protokoły) kryptograficzne, które pozwalają na rzeczy z pozoru niemożliwe do realizacji, np. na tworzenie podpisów cyfrowych, które są praktycznie nie do podrobienia czy przedstawianie tzw. dowodów z wiedzą zerową (np. gwarancji posiadania hasła bez jego ujawniania). Symulacja rzutu monetą przez telefon jest prostszym ale analogicznym problemem z gatunku tych, które mogą wydawać się niemożliwe do realizacji.

W sytuacji rzeczywistej, Alicja i Bob nie projektowaliby układu logicznego na papierze, ale użyliby odpowiedniego oprogramowania. Prawdopodobnie nie byliby nawet zainteresowani poznaniem szczegółów jego działania. Ale chcieliby mieć pewność, że żaden z nich nie ma możliwości wpływu na wynik niezależnie od mocy komputera.

W zasadzie, każdy spór może być rozwiązany przez odwołanie się do neutralnego osądu. W tym przypadku sędzia ma w posiadaniu: układ złożony z bramek logicznych, dane wejściowe Ali, ciąg wartości przekazany do Boba i jego odpowiedź (próba odgadywania) dotycząca parzystości. Informacje te stają się informacjami publicznymi, więc żadna z zainteresowanych stron nie może im zaprzeczyć. Sędzia jest w stanie potwierdzić uczciwość przeprowadzonej symulacji. Sam fakt istnienia jasnej procedury sprawdzania uczciwości czyni nieprawdopodobnym, by spór nie miał zostać rozstrzygnięty. Sytuacja jest bez porównania lepsza od tej, gdzie Alicja rzucałaby prawdziwą monetą a Bob odgadywał – żaden sędzia nie podjąłby się tej sprawy!

Układ logiczny przedstawiony w czasie zajęć jest w praktyce nieużyteczny -- z racji swych małych rozmiarów nie pozwala na zapewnienie odpowiedniego bezpieczeństwa. Lepszą ochronę zapewnia zastosowanie 32 bitów. I taka liczba może okazać się niewystarczająca – wszystko zależy od samego układu logicznego. Można sobie wyobrazić wykorzystanie innego rodzaju funkcji jednokierunkowej (np. podobnej do tej z zajęć nr 14). W praktyce często korzysta się z metod opartych o niebanalny problem rozkładu dużych liczb na czynniki pierwsze (nie jest to jednak problem NP-zupełny – będzie o nich mowa w następnym rozdziale). Łatwo można sprawdzić, czy jakaś liczba dzieli inną, ale szukanie dzielników dużej liczby jest problemem złożonym obliczeniowo. Trudno byłoby zilustrować użycie tej metody w przypadku

Alicji i Boba, jeśli chcemy używać tylko kartki i długopisu – w praktyce wykorzystuje się odpowiednie oprogramowanie.

Koncepcja podpisu elektronicznego opiera się na podobnych pomysłach. Dzięki upublicznieniu ciągu wartości wyjściowych układu funkcji jednokierunkowej, Alicja jest w stanie wykazać, że to właśnie ona wygenerowała taki wynik – nikt inny nie może wymyślić danych wejściowych, którym odpowiadać będzie wynik. Nikt nie podszyje się pod Alicję! W przypadku prawdziwego podpisu elektronicznego, potrzeba bardziej złożonego protokołu, który pozwoli na potwierdzenie autorstwa nawet gdyby Alicja zaprzeczała temu. Zasadniczy pomysł jest jednak ten sam.

Możemy wyobrazić sobie inne praktyczne zastosowanie ww. metody – partia pokera przez telefon (albo negocjacje na temat jakiegoś kontraktu), kiedy nie ma sędziego, który mógłby nadzorować przebieg gry. Oczywiście gracze nie mogą ujawniać kart w czasie gry. Ale wymagamy, by postępowali uczciwie – nie powinni twierdzić, że są w posiadaniu asa, jeśli tak nie jest! Po zakończeniu gry musi być możliwość sprawdzenia poszczególnych ruchów przeciwnika. Istnieje jednak problem zasadniczy dotyczący rozdawania kart w czasie gry. Okazuje się, że można go rozwiązać z użyciem protokołu, który nie różni się wiele od symulacji rzutu kostką.

Protokoły kryptograficzne są niezmiernie ważne w czasie transakcji elektronicznych. Pozwalają zidentyfikować właściciela karty (np. płatniczej), a także uwierzytelnić (potwierdzić autentyczność) nadawcę wiadomości. Zapewnienie niezawodności takich metod jest decydującym czynnikiem rozwoju handlu elektronicznego.