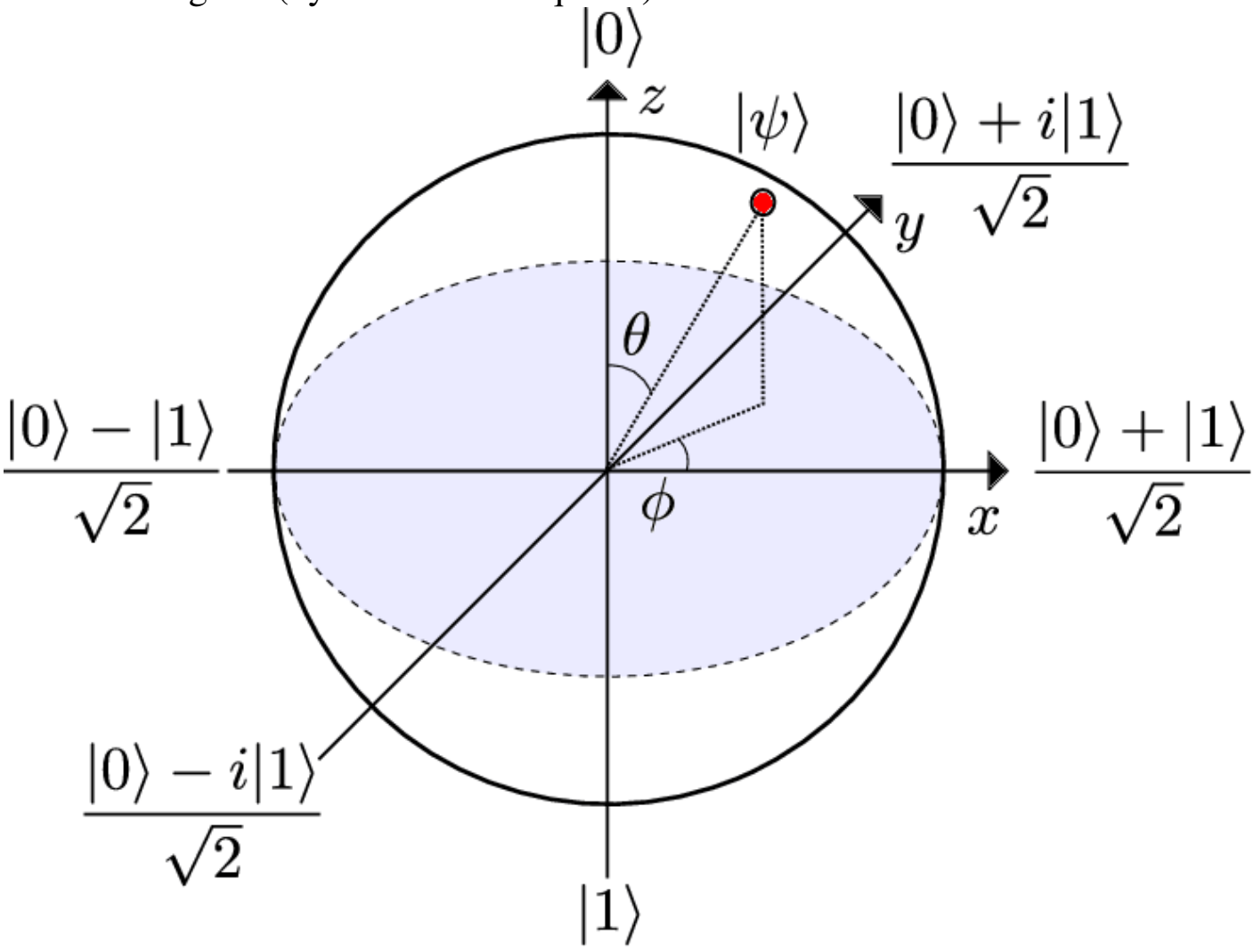
Stručně o kvantové kryptografii

současné znalosti kvantové mechaniky nabízejí aplikace v oblasti kryptografie
JEDNÁ se o výpočty založené na zcela jiných principech, než jsou Turingovy stroje či „klasické“

Blochův diagram (vysvětlení stavu qubitu):



Kvantová signalizace

jedná se o realizovatelnou technologii v podstatě ve fázi pilotních projektů
probíhají práce na zlepšování parametrů a praktičnosti

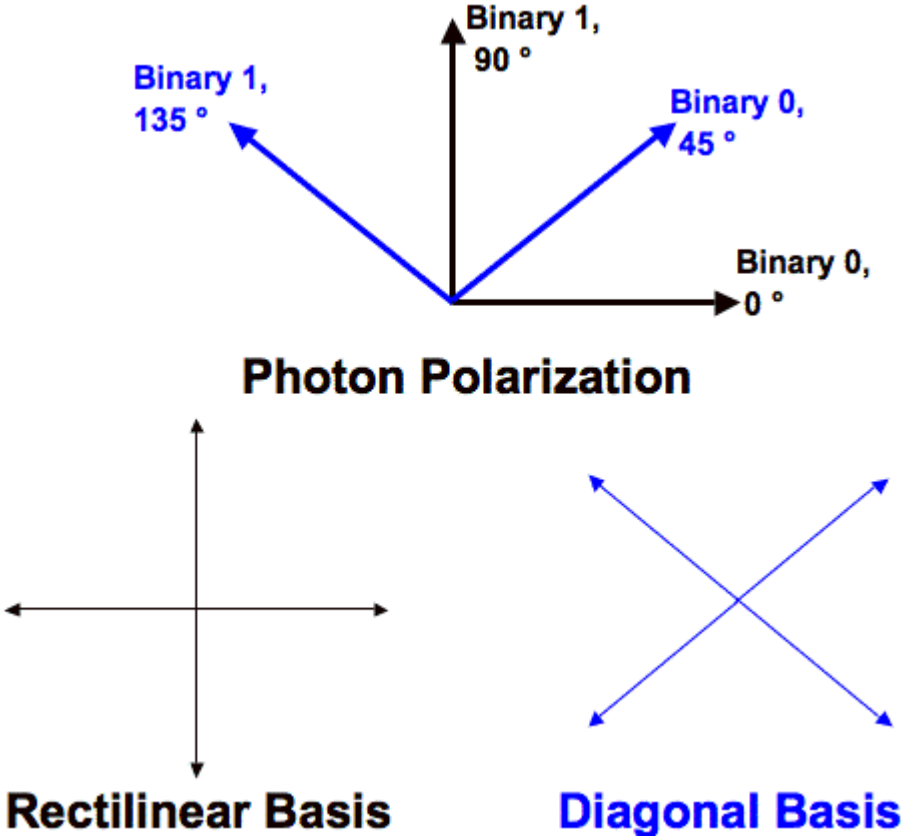
BB84

postulován 1984 Bennetem a Brassardem
využívá principů kvantové mechaniky:

- Teorém o klonování stavů - nemožnosti provést identickou kopii neznámého stavu

- Heisenbergův princip neurčitosti – nemožnost určení/změření obou polovin páru konjugovaných veličin: zde polarizace v různých bázích

komunikující si dohodnou báze pro měření polarizace fotonů:



pokud přicházející polarizovaný elektron měříme se správnou bází, zjistíme s určitostí, ve které ose je polarizován
pokud ale použijeme pro měření nesprávné báze, dojde k „přepolarizaci“ elektronu do jedné z os měřící báze s pravděpodobností přesně 50% … ergo nezjistíme nic

- vysílající vygeneruje náhodnou posloupnost bitů
- pro každý bit náhodně zvolí jednu z bází a ní foton správně polarizuje
- přijímající náhodně zvolí bázi a změři polarizaci
- po skončení přenosu vysílající veřejným kanálem oznámí pořadí bází a přijímající sdělí, kdy měřil ve správné bázi
- detekce odposlechu – vysílající náhodně vybere část úspěšně přenesených bitů a zveřejní je
- pokud příjemce naměřil stejná data, je kanál prohlášen za bezpečný a zbilé bity použity jako klíčový materiál

Bezpečnost:

v ideálním případě je protokol bezpečný bez ohledu prostředky, kterými případný útočník zasahující do komunikace disponuje
prakticky nejsme schopni spolehlivě generovat individuální fotony – pokud je bit nesen více jak jedním fotonem, může útočník část předmětných fotonů z přenosu zachytit, na nich provést potřebná měření a zbylé nechat bez zásahu dotéci protistraně

Eckertův protokol

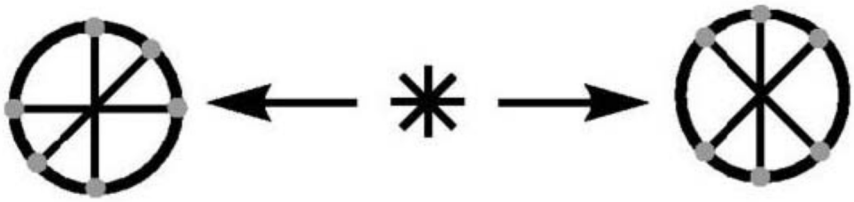
Ještě přidáme další „vymoženost“ kvantové mechaniky:

- Chování entanglovaných párů – pokud je na jedné částici entanglovaného páru změřena hodnota nějaké veličiny, entanglovaná částice okamžitě přejde do duálního stavu

získáme protokol podobný předchozímu s významným zlepšením:

1. centrální arbitr generuje entanglované páry elektron-pozitron a posílá je komunikujícím

2. komunikující náhodně volí jednu ze tří bází pro měření spinu:



3. pokud zvolí stejnou bázi a je jisté, že přijímající a odesílající naměří antikorelované hodnoty spinu
4. pokud zvolí rozdílné báze, oba naměří nezávislou náhodnou hodnotu
5. po zpracování dostatečného množství částic obě strany zveřejní pořadí použitých bází a ponechají si ta měření, kde byla použita stejná báze
6. dále zveřejní výsledky ostatních měření a spočítají míru korelace – dle kvantové mechaniky by měla být rovna $2\sqrt{2}$ … pokud není, je kanál odposloucháván a meření nebyla prováděna na entanglovaných částicích.

Bezpečnost:
podobně jako v předchozím případě nejsou kladeny podmínky na prostředky, kterými disponuje útočník
protokol netrpí problémem rozdělování přenosových shluků

Kvantová kryptoanalýza

využívá něčeho – čeho se nám nedostává v klasických počítačích: masivního paralelismu
pomocí superpozice stavů mohou qubity kvantového počítače držet kombinaci exponenciálně mnoha stavů a „paralelně“ na nich provádět výpočet
pokud umíme na konci „vyselektovat“ správné řešení dojde k asymptotickému zrychlení výpočtu

Shorrův algoritmus

významným způsobem urychluje faktorizaci – až na úroveň P – tedy polynomiální omezení času
jedná se o kombinaci klasického a kvantového výpočtu
pravděpodobnostní algoritmus – převádí problém faktorizace na problém hledání periody funkce:

nechť *n* je složené číslo, hledáme funkci

$$f_{y,n}(a) = y^a \bmod(n),$$

kde *y* je náhodné celé číslo nesoudělné s *n*.
buď *r* perioda funkce *f*, potom $f_{y,n}(a) = f_{y,n}(a + r)$ a odtud

$$y^r \equiv 1 \bmod(n)$$

tedy

$$\left(y^{\frac{r}{2}} - 1\right)\left(y^{\frac{r}{2}} + 1\right) \equiv 1 \bmod(n)$$

(pokud je *r* liché, zvolíme jiné *y*).
Nutně je *n* soudělné s jedním z činitelů nalevo -> hledáme *nsd* (viz. rozšířený euklidův algoritmus)
nalezení *r* nelze na klasickém počítači zvládnout polynomiálně, ale na kvantovém ano:

1. zvolíme náhodně *y* nesoudělné s *n* a *q* t.ž. $2n^2 \leq q \leq 3n^2$
2. mějme kvantový registr rozdělený na části R1 a R2, do R1 zapíšeme superpozici čísel 0 … *r*-1, do R2 zapíšeme 0
3. Z hodnot R1 paralelně vypočteme hodnoty $f_{y,n}(a)$ a jejich superpozici zapíšeme do R2
4. Změříme část R2 jako hodnotu *k* – registr přejde do stavu, kdy v části R2 je hodnota *k* a v části R1 je superpozice čísel, které dávají funkční hodnotu *k*

5. Provedeme kvantovou Fourrierovu transformaci na R1 a výsledek vrátíme opět do R1 – tím dojde ke zvýšení amplitud stavů, které odpovídají $1/r$ a tyto tedy můžeme měřit s větší pravděpodobností. Navíc odstraní ofsety periody.
6. Změříme registr s výsledkem s. Opakováním kroků 2-6 získáme dostatečné množství vzorků z okolí násobků periody pro určení r.
7. Na klasickém počítači rozšířeným euklidovým algoritmem zjistíme nsd $\left(y^{\frac{r}{2}}-1\right), n$ a $\left(y^{\frac{r}{2}}+1\right), n$.

Poznámky
na rozdíl od kvantové signalizace Shorrův algoritmus stále v teoretické rovině asymptotická složitost $O\left((\log n)^2(\log(\log n))(\log(\log(\log n)))\right)$ … tedy polynomiálně omezená vůči délce n.

Útoky proti metodám kryptografické ochrany

Co je cílem útoku:

- utajení
- autenticita
- integrita
- vzájemnost
- koordinace
- práh spolupráce
- nepopiratelnost
- náhodnost
- anonymita
- dostupnost
- podpis

Kdo je potenciální útočník:

- laik venkovní
- laik domácí
- hacker
- vnější profesionál
- vnitřní profesionál
- organizace
- zákonná moc

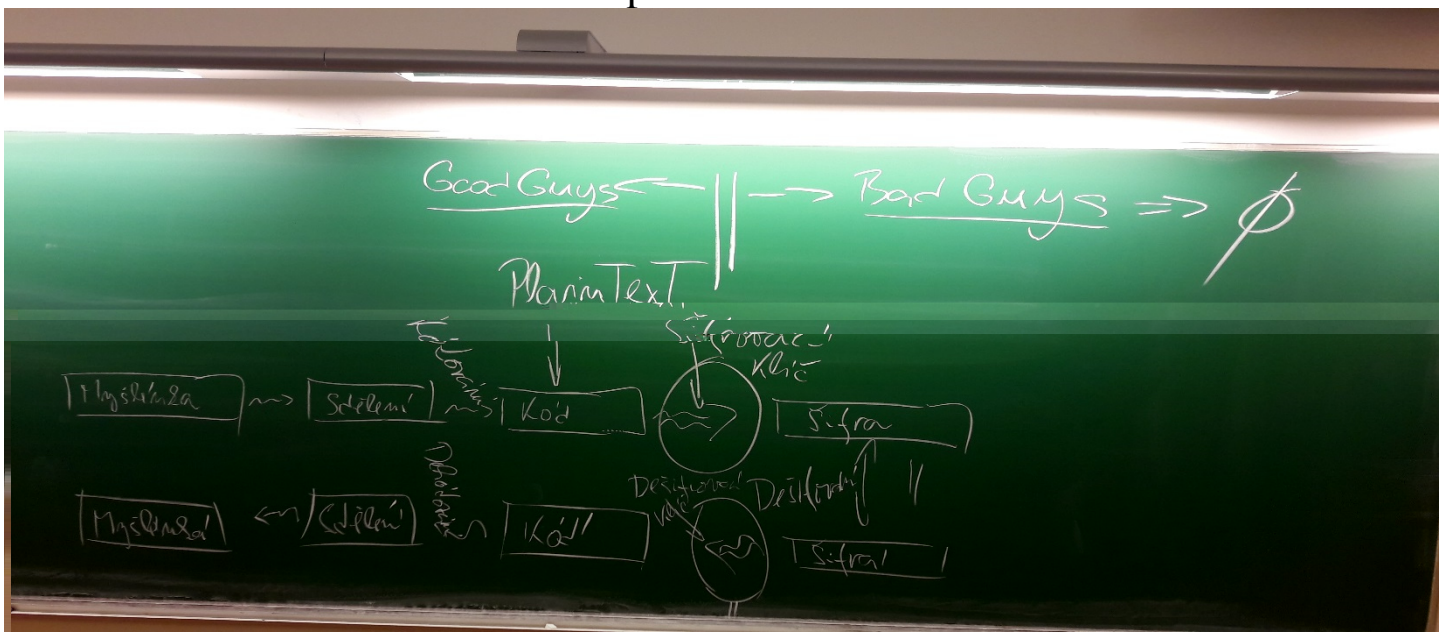
Jak se útočník chová:

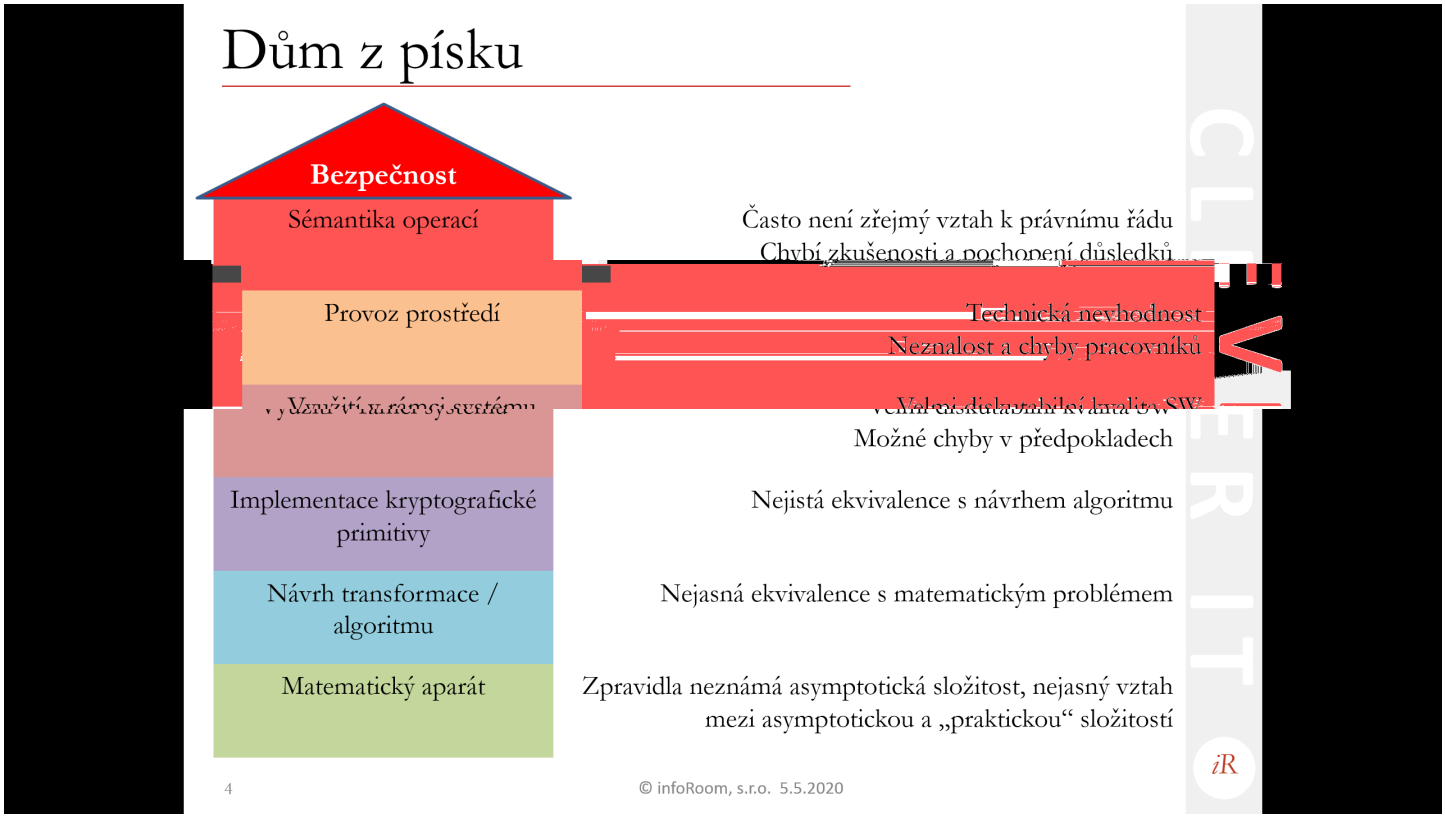
- zachycuje
- pozměňuje
- opakuje
- podsouvá
- mění pořadí
- působí mizení

Základní pravidlo: zpravidla jde o peníze

1. cena provedení útoku
2. zisk útočníka
3. vaše ztráta

Z teoretického hlediska důležitá síla útočníka, obvykle předpokládáme polynomiální čas vzhledem k velikosti vstupu





Útočníkova síla

do roku 2004 se odhadovalo nejméně 2.10^9, většina z nich dostupná via Internet
je vyzkoušeno, že během 1 roku lze získat přibližně 0,1% celkového výkonu

Moorovo pravidlo: výkon počítačů roste cca 2x za 18 měsíců

existují organizace vlastnící značný výpočetní výkon – větší firmy, univerzity, … přitom tyto počítače může nepozorovaně využívat malá skupina lidí – administrátoři, vedení

odhady síly:

rok	*nenápadně*	*veřejný projekt*
2004	10^8 MY	2.10^9 MY
2014	$10^{10\text{-}11}$ MY	$10^{11\text{-}13}$ MY

MY = mips year, t.j. 1 rok práce počítače o výkonu 1mips

pro srovnání – krabička zápalek (faktorizace)

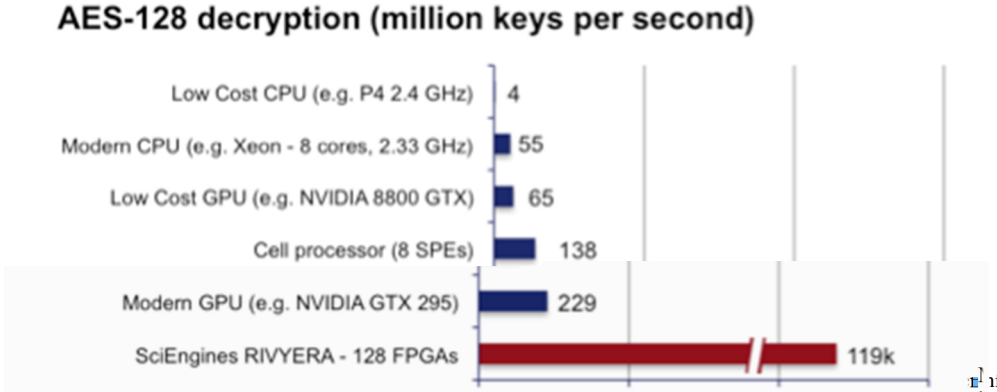
bitů n	*potřeba MY*
512	3.10^4
768	2.10^8
1024	3.10^{11}
1280	1.10^{14}
1536	3.10^{16}
2048	3.10^{20}

odhady jsou spočteny pro v současnosti asymptoticky nejlepší algoritmus na faktorizaci velkých čísel – *general number field sieve*

zvláštní čísla jako třeba Fermatova čísla lze rozkládat ještě cca 1000 až milionkrát rychleji

Nebo ještě jinak – srovnání RSA a symetrické šifry:

Sym. klíč	*modul RSA*
80	1024
112	2048
128	3072
192	7680
256	15360



Pro AES ukazuje dosažitelné výkony tabulka

Úspěšný útok

– obecně porušení (trvalé či dočasné) některé z vlastností systému, lze chápat různě formálněji:
kryptosystém je (1-ε) bezpečné, pokud žádná P-time procedura nedokáže výslednou šifru rozlišit od náhodné posloupnosti s pravděpodobností větší než (1-ε)/2

Šifrovací algoritmy

nejvíce nejasností okolo šifrovacích algoritmů:

- kryptosystém nemusí být bezpečný pro jistá rozložení pravděpodobnosti v prostoru plaintextů (pouze $\mathbf{o}(n^c)$ možných plaintextů)
- může být získána parciální informace o plaintextu
- nabyty znalosti o vztazích mezi zprávami, bez znalosti obsahu

Skládání šifrovacích operací

následným použitím dvou kryptosystémů které lze zlomit v čase $\mathbf{o}(2^n)$ a prostoru $\mathbf{o}(2^n)$ získáme kryptosystém stejné odolnosti, nikoliv $\mathbf{o}(2^{2n})$
skládání šifrovacích schémat nesnižuje odolnost, t. zn. výsledné schéma má sílu silnějšího subschématu, pokud jsou oba klíče voleny nezávisle

existuje celá řada útoků lišících se navzájem výchozími podmínkami, kterých útočník využívá, různé útoky nemusí být obecně účinné
obecně cílem analýzy je získat použitý šifrovací klíč

útočník se často snaží používat *apriorní informace*:

- v jakém jazyce je zpráva psána
- předpoklad výskytu jistých slov
- použitý kryptosystém
- vnitřní struktura zprávy
- …

Útoky lze rozdělit dle celé řady kriterií. Časté je dělení

Znalost zašifrovaného textu (ciphertext only att.)

útočník má k dispozici pouze zachycený zašifrovaný text, dále může využívat apriorních informací - pracuje tedy jen se statistickými rozbory, distribucí, pravděpodobností.
Systém, který není odolný vůči tomuto útoku nelze označit za bezpečný.

Znalost otevřeného textu (known plaintext att.)

předpokládá se, že útočník má k dispozici pár otevřený text + odpovídající šifra

Pravděpodobný text (probably plaintext att.)

útočník na základě okolností odeslání zprávy může učinit částečný odhad obsahu zprávy

Zvolený otevřený text (choosen plaintext att.)

útočník může získat k libovolnému otevřenému textu odpovídající šifru, velmi používaný útok, vhodný i proti statistickým databázím

Zvolená šifra (choosen ciphertext att.)

používá se v případě, že útočník může šifrovacím algoritmem zašifrovat velké množství zpráv, aby našel plaintext odpovídající zvolené šifře.

Digitální podpisy

- key-only attack – zná pouze veřejný klíč oběti
- known signature attack – dtto + má k dispozici pár (zpráva-podpis)
- chosen signature attack – útočník si může vybrat zprávy, které si nechá podepsat

úspěšné útoky

- existenciální podvržení – útočník úspěšně podvrhl podpis, ne nutně jím zvolené zprávy
- selektivní podvržení – podvržen podpis některých zpráv dle volby útočníka
- universální podvržení – útočník nezná klíč ale může podvrhnout podpis libovolné zprávy
- totální průlom – zjištěn podpisovací klíč

Brute force attack, exhaustive search

jediná možnost proti skutečně dobře navrženým šifrám, útočník se snaží vyzkoušet celý prostor klíčů, zpráv, …
Současná hranice zvládnutelnosti je 2^{56}, vzrůst výkonu počítačů odpovídá čtyřnásobku za 3 roky, tedy do 10 let se hranice posune k 2^{64} a během 20 let dosáhne 2^{80}. ... a toto bylo napsáno v roce 2007

Speciální druhy útoků proti určitým kryptografickým metodám

Diferenční analýza (Differential att.)

provádí rozbor změn které nastávají ve výsledné šifře a jejich závislosti na (malých) změnách –diferencích - šifrovaného otevřeného textu
hledá se statistická závislost mezi diferencemi na vstupu a na výstupu … to omezuje možné klíče

metoda účinná proti DES, FEAL, …

Lineární kryptoanalýza

hledá se způsob, jak část transformace šifry nahradit lineárními rovnicemi alespoň nad některými bity plaintextu/klíče/výsledné šifry
tzn. hledají se výrazy typu $X_{i_1} \otimes X_{i_2} \otimes X_{i_3 \ldots} \otimes X_{i_m} \otimes Y_{i_1} \otimes Y_{i_2} \otimes \ldots Y_{i_n} = 0$ které mají vysokou, nebo naopak nízkou pravděpodobnost, že platí pro různé kombinace vstupních bitů X_i a výstupních bitů Y_i.
Tato pravděpodobnost se pro příslušný výraz nazývá *sklon k linearitě.*
Pravděpodobnost že výraz platí charakterizuje linearitu příslušné části algoritmu.
zejména se vyhodnocují nelineární části algoritmu jako s-boxy … pro každý S-box se vyhodnotí sklon k linearitě všech kombinací vstupů a výstupů
Následně se skládají sklony k linearitě všech S-boxů použitých v průběhu šifrování

na základě znalosti množství párů plaintext – šifra je potom možno odhadovat bity klíče

Integrální kryptoanalýza

podobně jako diferenční analýza hledá závislost mezi bity vstupu a výstupu šifry, pracuje však nad množinami plaintextů / šifer

analyzují se však rozdíly (např XOR celé skupiny) mezi kombinacemi plaintextů a kombinacemi výsledných šifer … a opět se z toho usuzuje na hodnotu vybraných bitů klíče

Kolize klíčů (Key collisions)

kolizí klíčů K_1 a K_2 rozumíme

$$\mathbf{E}(K_1, P) = \mathbf{E}(K_2, P)$$

J.Quisquater publikoval algoritmus hledající kolize v čase $\mathbf{O}\left(2^{n/2}\right)$. V případě DESu k danému P existuje 2^{48} kolizí.

Random attack

útočník se tupě pokouší uspět s podvrženou zprávou, pokud systém nemá definovanou přiměřenou odezvu na chybné zprávy, může být tato metoda účinná

Birthday attack

pravděpodobnost, že mezi 23 lidmi jsou dva stejného data narození přesahuje 1/2
útočník připraví r_1 variant podvržené zprávy a r_2 variant původní zprávy. Pravděpodobnost, že takto získá pár podvržená zpráva / původní zpráva, které mají stejný hash kód je

$$1 - \mathbf{e}^{-\frac{r_1 \cdot r_2}{2^n}}$$

což pro $r_1 = r_2 = 2^{n/2}$ činí zhruba 63%.

Meet in the middle attack

obdoba přechozího útoku. Vytvoříme r_1 variant prvního bloku podvržené zprávy a r_2 variant posledního bloku. Poté počítáme "z obou stran" , t. j. od inicializačního vektoru a pozpátku od hash-kódu a snažíme se "potkat" ve stejné hodnotě zřetězující proměnné (chaining variable)
útok je rovněž možno použít proti DES a většině iteračních šifer

Man in the middle attack

Timing attack

účinný útok proti mnoha ***implementacím*** RSA. Spočívá v měření odezvy druhé strany. V závislosti na použitém klíči se totiž může měnit čas potřebný na zašifrování zprávy. Z doby odezvy tak lze odhadovat, jak klíč vypadá.

Fixed point attack

Hledáme H_{i-1} a X_i tak aby

$$\mathbf{f}\left(X_i, H_{i-1}\right) = H_{i-1}$$

pokud zřetězující proměnná nabyde hodnoty H_{i-1} , můžeme vložit libv. množství bloků X_i. Útok je reálně možný pouze pokud můžeme manipulovat s hodnotou inicializačního vektoru, nebo pokud **f** má velké množství pevných bodů.
Snadnou obranou je ke zprávě přidat její délku.
Hledání pevných bodů lze používat i při analýze šifrovacích algorimů. Šifrovací algoritmus lze brát jako náhodnou permutaci a tedy je pravděpodobné, že pevné body lze najít. V DES pro skupinu weak a semiweak klíčů existuje celkem 2^{33} pevných bodů.

Generátory

Choosen input atttack

Útočník ovládá nebo alespoň všechny, nebo některé zdroje entropie generátoru, pokud má přístup k výstupu, může provádět adaptivní útok

Kryptoanalytický útok

Hledání charakteristiky výstupní posloupnosti, predikovatelnosti způsobené nesprávným návrhem generátoru, odpovídá lámání proudových šifer

Iterative guessing

Pokud při překlíčování generátor nezahrne dostatečné množství nové entropie, je změna vnitřního stavu generátoru „příliš malá“
Pokud útočník znal stav generátoru před změnou, dokáže nalézt stav po změně a nadále predikovat výstup

Podaný přehled není zdaleka úplný, obsahuje pouze několik víceméně náhodně zvolených reprezentantů. Vůbec jsme se nezabývali triviálními útoky spočívajícími v opakovaném použití starých zpráv, slepování nových zpráv z útržků starých apod.

Kvantová kryptografie

využití kvantových jevů (Heissenbergův princip neurčitosti, entanglované páry, teorém o klonování kvantových stavů), tzn. **nikoliv** výpočty obdobné turingovým strojů,
v různém stadium teoretických úvah a laboratorních testů, praktická použitelnost v nejlepším případě nejistá
zajímavé je, že kvantová kryptografie nabízí dokazatelně bezpečné metody

Kvantová signalizace – BB84 algoritmus

Použitelný k distribuci klíčů
Mezi odesílatelem a příjemcem musí být konvenční komunikační kanál a kvantový kanál (dnes optické vlákno)

- Nejprve se pošle dostatečný objem dat:
  - Odesílatel generuje fotony polarizované náhodně s rovnoměrným rozložením mezi 4 možné roviny (tj báze X a +) a odesílá kvantovým kanálem
  - Příjemce náhodně zvolí bázi a provede měření polarizace.
- Odesílatel sdělí otevřenou komunikací pořadí bází, v nichž byly jednotlivé fotony polarizovány.
- Příjemce si ponechá hodnoty které měřil ve správné bázi. Tyto bity budou tvořit klíč.
- Příjemce otevřenou komunikací sdělí, které fotony si ponechal
- Odesílatel zná jejich polarizaci, tzn. oba mají stejnou posloupnost měření.
- Pro detekci odposlechu si příjemce a odesílatel sdělí hodnoty několika náhodně zvolených měření. Pokud najdou rozdíl, linka je odposlouchávána a klíč nelze použít.

Protokol založen na skutečnosti, že pokud zvolíme pro měření správnou bázi, získáme správný výsledek. Pokud ne, získáme náhodný výsledek, ale polarizace fotonu se změní na polarizaci dle použité báze.

Pro n náhodných kontrolních bitů má útočník šanci $1 – (¾)^n$, že bude odhalen, lze tedy docílit libovolné jistoty.

V praxi je to složitější, měření jsou zatížena významnou chybovostí, která narůstá s délkou přenosové cesty. V současné době se podařilo dosáhnout vzdálenosti cca 500km.

Protokol neřeší man-in-the-middle attack.

Přenesený klíč se použije v „konvenčním“ kryptografickém algoritmu.

Kvantová teleportace

Lze docílit toho, že jediný foton se při správném průchodu vhodným krystalem změní ve dvojici fotonů, které se nacházejí v neurčitém stavu, ale některé vlastnosti mají korelovány. Pokud dojde k změření některé vlastnosti na jedné částici, druhá částice okamžitě získá příslušnou korelovanou hodnotu vlastnosti … nezávisle na vzdálenosti.

- Odesílatel si tedy připraví entanglovaný pár A-B, jednu částici si ponechá, druhou pošle příjemci.
- Pokud chce odesílatel přenést neznámý stav částice C:
- Spojí stav částice C do stavu entanglovaného páru – výsledný stav má 3 Q-bity
- Provede měření na druhých dvou QUbitech sloučeného stavu – toto měření ovlivní stav jak částice A, tak i B, ale nic konkrétního neřinese o částici C tzn. její stav zůstává neznámý a nemění se
- Odesílatel sdělí klasickým kanálem příjemci výsledek měření

Kvantové generování náhody

v jednoduché podobě použito v „klasických „ generátorech – čtení šumu PN předchodu, sledování okamžiků rozpadu atomů radioaktivních izotopů

Shorův algoritmus

umožňuje s pomocí kvantového počítače provádět faktorizaci čísel v čase $O(n^2 \log(n) \log\log(n))$ … a to by byl problém

problém faktorizace lze převést na problém hledání periody funkce:
pro *n* které chceme faktorizovat a *y* nesoudělné s *n* nechť

$$f_{y,n}(a) = y^a \bmod(n)$$

funkce je zjevně periodická s nějakou periodou *r* a proto

$$y^a \equiv y^{a+r} \bmod(n)$$

odkud

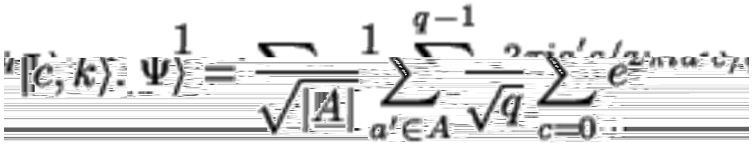
$$y^r \equiv 1 \bmod(n) \text{ a též } \left(y^{r}/_2 + 1\right)\left(y^{r}/_2 - 1\right) \equiv 0 \bmod(n)$$

pro sudou periodu. Tzn. některá ze závorek musí být dělitelná *n* a pouze hledáme NSD $\left(y^{r}/_2 + 1\right)$ a $\left(y^{r}/_2 - 1\right)$, což se dá v logaritmickém čase.
Zbývá najít periodu *r*, což deterministicky na klasickém počítači není P-time
Kvantový počítač ale umožňuje počítat s masivním paralelismem.
QUbit může obsahovat superpozici mnoha hodnot – popsanou vlnovou funkcí a vhodným čtením stavu můžeme dělat průměty části stavu (tzn. lze vlnovou funkci částečně zkolabovat)

- Zvolíme náhodně *y* nesoudělné s *n* a zvolíme $2n^2 <= q <= 3n^2$
- Do R1 části kvantového registru R1,R2 vložíme superpozici čísel 0 – (q-1) , do R2 dáme 0:
  - $$|\Psi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle.$$
- Paralelně spočítáme $f_{y,n}(a)$ a superpozici výsledků vložíme do části R2
  - $$|\Psi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, y^a \bmod n\rangle.$$
- Změříme část R2 kvantového registru jako hodnotu … vyjde *k*, ale registr přejde do stavu
  - $$|\Psi\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} |a', k\rangle,$$
    tj. obsahuje superpozici pouze čísel, pro které má funkce hodnotu *k*

… to už je téměř ono

- Abychom mohli měření opakovat (a nevadil měnící se úvodní offset) nahradíme část R1 Fourierovou transformací:



nyní již lze výpočet opakovat a měřením získáme dostatev vzorků pro odhad hodnoty *r*.

Registr R1,R2 musí mít velikost log(*q)* QUbitů
Tady končí legrace, pokud by někdo měl počítač s řádově tisíci-QUbitovými registry, dokázal by v polynomiálním čase faktorizovat a tím pádem i počítat diskrétní logaritmy.

Postkvantová kryptografie

Předpokládejme, že existuje kvantový počítač s tisíci-QUbitovými registry:

- víme, že přestanou být bezpečné algoritmy založené na diskrétním logaritmu a faktorizaci (RSA, El-Gamal, DSA) a to včetně všech odvozenin (EC)
- přestanou být použitelé všechny konstrukty odvozené od těchto algoritmů
- většina symetrických šifer není dotčena – zrychlí se kryptoanalýza, ale to lze pokrývají dostatečne dlouhé klíče
- zkoumají se asymetrické algoritmy, které nepostihne výpadek bezpečnosti – McElliceův algoritmus, Merkelovo schéma, RLCE, aplikace supersingulárních elyptických křivek