Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 11/2007 **15. listopad 2007**

11/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1230 registrovaných odběratelů)

Obsah : str.

Příloha:
Příběh Štěpána Schmidta (všechny 4 části ve formátu doc) pribeh.doc

A. Soutěž v luštění 2007 skončila

Pavel Vondruška

Soutěž v luštění 2007 (http://soutez2007.crypto-world.info/), která byla doprovázena fiktivním příběhem Štěpána Schmidta skončila. Možnost vkládat správné výsledky řešení jednotlivých úloh byla uzavřena 15.11.2007 ve 13.00 hod.

Ceny (http://soutez2007.crypto-world.info/index.php?crypto=ceny) získali první tři řešitelé a dále tři řešitelé, kteří byli vylosování z 36 soutěžících, kteří dosáhli více než 15 bodů (limit pro zařazení do losování).

Stručná statistika letošní soutěže:
Celkem soutěžících: 109
Počet soutěžících, kteří vyřešili aspoň 1 úlohu: 103
Počet soutěžících zařazených do slosování: 36

Úlohy
Celkem publikovaných úloh: 21
Maximální počet bodů za publikované úlohy: 70

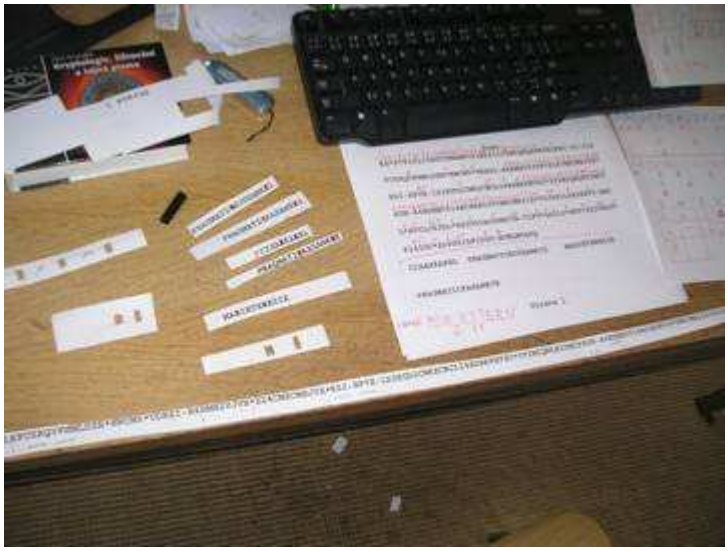
Všechny úlohy letos vyřešilo celkem 16 soutěžících (!):
room132 ,jmkollar , MD5Mir, gimli2, Bigbaz , Jahoda , ony , peta007 , m , Mirop , koc , sm4sh , Hujer , Benjamin , davidh , hodiny

Pořadí na prvních třech místech:

1	Room132	70	01.11 (19:58)
2	jmkollar	70	01.11 (19:59)
3	MD5Mir	70	01.11 (20:08)

Vylosovaní soutežící:

7	ony	70	01.11 (21:34
13	Hujer	70	02.11 (15:51)
24	Winetou	29	22.10 (14:32)



Řešení všech úloh, včetně postupů a návodů na jejich luštění, budou uvedeny v prosincovém čísle 15/2007, které vyjde 15.12.2007.

Všem úspěšným řešitelům blahopřeji !

Děkuji sponzorům soutěže:
- TNS (Trusted Network Solutions), http://www.tns.cz
- Zoner Press, http://www.zonerpress.cz/
- Královská huť, s.r.o., http://www.qobchod.cz
- Soom.cz, http://www.soom.cz

B. Z dějin československé kryptografie, část IV. Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 1 .

Mgr. Karel Šklíba (karel.skliba@crypto-world.info)

Šifrovací stroj ŠD – 1 byl prvním poválečným šifrátorem, který byl v Československu bez cizí pomoci vyvinut a poté prakticky několik let používán v československé šifrové službě, zejména v armádě. To bylo způsobeno několika faktory, za kterých šifrátor vznikal. První podmínkou bylo to, že v Československu po roce 1955 byla akutní potřeba strojového šifrového zabezpečení dálnopisných spojů a obecně vůbec dostupnosti šifrovacích strojů pro utajení spojení v armádě a v některých vládních úřadech. Po neúspěchu šifrátoru MAGDA bylo proto nutno urychleně vyvinout snadno prakticky použitelný stroj.

Druhým faktorem byla skutečnost, že šifrovací stroj ŠD – 1 neměl vlastní tvorbu hesla a tím byla jeho konstrukce výrazně jednodušší. Neobsahoval žádné mechanické ani elektrické bloky tvorby šifrovacího hesla a jednalo se vlastně pouze o sčítací zařízení otevřeného textu produkovaného dálnopisným strojem s heslem vkládaném na pětistopé děrné pásce. Proto se tomuto šifrovacímu stroji někdy také říkalo „sčítačka“ nebo „mixér“. Bezpečnost používání šifrovacího stroje ŠD – 1 proto závisela zejména na kvalitě vkládaného hesla a na správném používání, manipulaci a ukládání heslových materiálů. Sám šifrovací stroj ŠD – 1 by vlastně nemusel mít tajný charakter, neboť děrná páska s heslem, která byla pro úkon šifrování nebo dešifrování používána, byla ve svém pouzdru zapečetěna a ze stroje se vyjímala. Vzhledem k jednoduchosti konstrukce měl šifrovací stroj ŠD – 1 v porovnání s jinými šifrovacími stroji velmi malou náročnost na údržbu a i manipulace se strojem byla velmi jednoduchá a nevyžadovala ani žádné zvláštní odborné znalosti obsluhy.

Další podmínkou vývoje šifrátoru ŠD – 1 bylo vytvoření Zvláštní správy Ministerstva vnitra ČSR v květnu 1955. Zvláštní správa byla pověřena centralizovaným řízením šifrové služby v Československu, výzkumem a vývojem šifrovacích prostředků a výrobou šifrových materiálů. Po vzniku této správy bylo přikročeno k prověrce jednotlivých prostředků používaných v československé šifrové službě. Po provedení kryptologického rozboru všech typů používaných šifrovacích strojů v letech 1955 a 1956 byly zjištěny značné nedostatky v jejich kryptologické bezpečnosti, což mělo za následek zákaz jejich používání. V důsledku toho zůstala československá šifrová služba od roku 1957 naprosto bez šifrovacích strojů a byla odkázána pouze na ruční způsob šifrování. Tím byla ovšem značně snížena operativnost šifrové služby, což se projevilo zvláště nepříznivě ve složkách Ministerstva národní obrany a Ministerstva vnitra. Zvláštní správa, která měla jeden ze zásadních úkolů výzkum a vývoj šifrovacích strojů a zajištění jejich výroby pro všechny směry spojení v Československu, byla v důsledku toho vystavena značnému tlaku ze strany odpovědných funkcionářů zejména resortu obrany, aby urychleně vybavila jejich spojovací součásti výkonnými šifrovacími stroji. Tehdejším podmínkám a potřebám již ruční způsob šifrování ve většině případů nevyhovoval. Na základě rozhodnutí vedení Ministerstva vnitra ČSR byl v letech 1955 – 1957 vyvinut a zkonstruován v prototypech šifrovací stroj ŠD – 1 a byly zahájeny práce na vývoji šifrovacího stroje s vlastní tvorbou hesla pod označením ŠD – 2. Na základě rozborů potřeb šifrové služby v Československu a na základě nedostatku technických pracovníků na Zvláštní správě, kteří by byli schopni vyvinout kryptologicky bezpečný šifrátor s vlastní tvorbou hesla, byla v roce 1957 prostřednictvím vedení státu vyžádána odborná pomoc v SSSR. Této žádosti bylo vyhověno a na začátku listopadu 1957 byly na Zvláštní správu předány dva diskové šifrovací

stroje s označením ŠD – 2 s veškerou potřebnou dokumentací pro jejich výrobu. Souběžně s tím byl vyvinutý vlastní šifrovací stroj ŠD – 1 konzultován a schválen kryptology ze šifrové služby SSSR.

Šifrovací stroj ŠD – 1 byl elektromechanický reléový přídavek k dálnopisu používaný pro šifrování on-line (přímé šifrování) s výstupem do spojovací linky. Provozní napětí stroje bylo 220 V AC (tj.střídavých). Přijímací bloky pracovaly s proudem 40 mA. Rychlost šifrování byla 427,5 znaků za minutu (v technických popisech byl údaj 428 zn./min). Stroj obsahoval 5 relé, která byla označena R01 R02 R03 R04 R05, a měl odstředivý regulátor otáček motoru a stroboskop na jejich kontrolu. Rychlost vysílače připojeného dálnopisu musela být stejná (nebo případně menší) jako rychlost ŠD – 1 a oba stroje musely mít stejnou délku impulsů. Šifrovací stroj ŠD – 1 byl řešen jako samostatné přídavné zařízení ke každému dálnopisnému stroji, avšak v praxi byl potom používán zejména s dálnopisy firmy LORENZ. Bylo možné jej použít na všech druzích linkových i radiových pojítek jako normální dálnopis. Šifrovací stroj ŠD – 1 měl rozměry 620mm x 400mm x 350mm a jeho samostatná váha byla cca 35 kg.

Strojem bylo možné provádět tyto druhy práce:

1. šifrování
2. dešifrování
3. psaní otevřeným textem

Stroj měl v prototypu dvoupolohový přepínač, který byl při šifrování a dešifraci v poloze **Š** a při předávání otevřených textů v poloze **C** . Tento přepínač byl pravděpodobně později nahrazen třípolohovým.

Stroj měl akustické a optické kontrolní zařízení, které prakticky znemožňovalo vyslání otevřeného textu utajované zprávy a zabraňovalo jakémukoliv porušení provozních pravidel, při nichž by mohlo dojít ke kompromitaci šifry. Zejména bylo dbáno, aby nedošlo k vícenásobnému použití stejného úseku hesla a aby se hodnota hesla nedostala do spolupracujících dálnopisů nebo do použitých pojítek.

Šifrovací stroje ŠD – 1 umožňovaly uskutečnit tyto druhy šifrového spojení:

1. osobní
2. oběžníkové
3. vzájemné

Pro provádění těchto typů spojení bylo třeba vyrábět 3 druhy heslových materiálů na pětistopé papírové děrné pásce mod 32. Pokud byly tyto heslové materiály kvalitní (zcela náhodné se stejnou pravděpodobností výskytu každé hodnoty hesla), pak jak známo použití šifrátoru ŠD – 1 garantovalo absolutní kryptologickou bezpečnost utajení předávaných zpráv o neomezené délce. Z výše uvedeného plyne, že šifrovací stroj ŠD – 1 není z hlediska vlastní kompromitace zranitelný. Z hlediska kryptologického bylo nutno chránit pouze heslový materiál na děrné pásce v kazetě.

K šifrátoru ŠD – 1 byly heslové materiály dodávány na perforovaných papírových pětistopých děrných páskách o šířce 17,5 mm (plus mínus 0,3 mm) a tloušťce 0,1 mm. Páska byla smotána na papírový kroužek o vnitřním průměru 55,4 mm a byla vložena a zapečetěna v papírové kazetě (pouzdře). Délka pásky byla 60 až 90 metrů, což představovalo 24000 až 36000 znaků. Pásky byly číslovány pětimístnými sériemi na začátku a na konci a dále byla

páska číslována vzestupnou řadou po dvaceti znacích (1. číslo bylo modré a 2. číslo bylo červené). Páska mohla mít maximálně dvě slepení. Na začátku pásky bylo půl metru pouze s vodícími otvory. Snímač pásky krokoval o 2,50 mm (plus mínus 0,03 mm). Průměr vodících otvorů pásky byl 1,2 mm (plus mínus 0,03 mm) a průměr signálních otvorů pásky byl 1,8 mm (plus mínus 0,03 mm). Na šifrátoru byl namontován důmyslný řezač děrné pásky, jehož nůž bylo podle pravidel o používání zakázáno sejmout a který použitou heslovou pásku po každém kroku rozřezával. Toto zařízení bylo z mechanického hlediska velmi krásné a propracované, ale podle vyjádření odborných pracovníků ze SSSR nepředstavovalo prakticky žádný podstatný bezpečnostní prvek. Proto i takto rozřezané kousky heslové děrné pásky musely být skartovány podle přísných bezpečnostních předpisů (jako by nebyly rozřezány!). Výroba děrných pásek s heslem měla být zajišťována na Zvláštní správě MV, což se zpočátku dělo ručním způsobem a tudíž nebyla zajištěna potřebná kvalita hesla. Proto se podstatná část těchto šifrových materiálů nakupovala v SSSR a od roku 1958 probíhal na Zvláštní správě výzkum a laboratorní zkoušky stroje na výrobu heslových materiálů na papírovou děrnou pásku s krycím označením HPS – 2. První stroj, na kterém se vyráběla pětistopá heslová děrná páska, měl označení HS – 1. Při dovozu činily náklady na jeden pár děrné pásky bez dopravy 18,72 rublů a při plánované objednávce 6000 párů byly náklady na dopravu 60000 rublů tj. celkem 172320 rublů, tedy při kursu 1,16 celkem 199891,20 Kč.

Vývojovou skupinu šifrovacího stroje ŠD – 1 vedl na Zvláštní správě Ing. Lubomír Odvárko. Ve skupině pracovali i dipl. tech. Zdeněk Křesina a další technik Zich. V listopadu 1957 byla výroba tohoto stroje plánována na roky 1958 a 1959 v předpokládané sérii 500 kusů v Závodech Jana Švermy v Brně se subdodavateli součástek Teslou Praha a MEZ Náchod. Předpokládaná cena jednoho kusu byla 15 až 20 tisíc Kčs. Technická dokumentace pro sériovou výrobu byla hotova v prvním čtvrtletí 1958 a první kusy měly být vyrobeny asi v druhém pololetí roku 1959. Nakonec ale probíhala výroba v 1. spojovací základně ČSLA (Československé lidové armády) v Hradci Králové. Bylo vyrobeno asi 50 kusů při ceně cca 10.000 Kčs za kus. Tyto šifrátory byly používány v československé šifrové službě zejména v letech 1960 až 1963. Potom byly postupně nahrazovány šifrovacími stroji ŠD – 3 rovněž čistě československé výroby a taktéž fungujících na principu vloženého hesla.

C. Testy obrazové kvality snímačů otisků prstů Suprema

Martin Drahanský (**drahan@fit.vutbr.cz, FIT VUT v Brně, www.fit.vutbr.cz/~drahan**)
Ondřej Nezhyba (**nezhyba@digitus.cz, Digitus s.r.o., www.digitus.cz**)

Biometrické systémy se stávají součástí našeho každodenního života. Pronikají rovněž do cestovních dokladů, kde se etabloval otisk prstu, obličej a duhovka. V tomto článku se zaměříme pouze na systém pro rozpoznávání otisků prstů od společnosti Suprema.

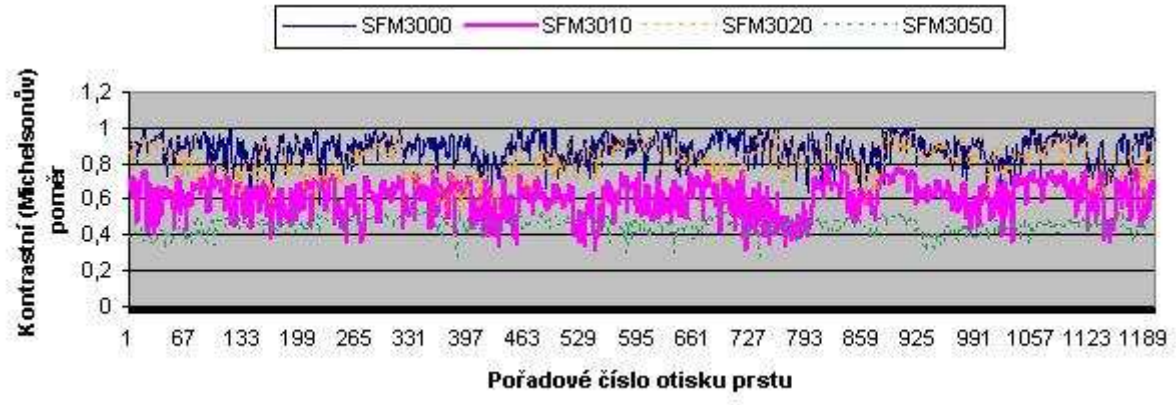
Každý biometrický systém se obecně skládá ze vstupní jednotky (obvykle senzor), jednotky zpracování a porovnání. Každá z těchto částí se dá testovat a pro některé aplikace je dokonce nutné provedení kompletního testování. K testování algoritmů na zpracování a porovnání otisků prstů existuje relativně velké množství metrik [5,1]. Podmínkou pro provedení některých testů je ovšem znalost struktury šablony, v níž je otisk prstu uložen (struktura neobsahuje obrázek, ale extrahované markanty s příslušnými informacemi, příp. jiné údaje dle typu algoritmu). U senzorů firmy Suprema nám bohužel nebyly poskytnuty informace ke struktuře šablon, tzn. že jsme nebyli schopni takové testování provést. Zaměřili jsme se proto (dle požadavku zadavatele) na testování kvality obrázků otisků prstů, které jsou získatelné z níže uvedených senzorů společnosti Suprema.

Všechny senzory byly připojeny k základní jednotce **Suprema SFM3000 EVK**, což je destička vývojového kitu, jež umí spolupracovat s následujícími senzorovými jednotkami [3]: **SFM3000**, **SFM3010**, **SFM3020**, **SFM3050**.

Vývojové prostředí, stejně jako všechny uvedené senzory, bylo zapůjčeno firmou Digitus s.r.o. (www.digitus.cz) a nachází se v biometrické laboratoři na Ústavu inteligentních systémů, Fakultě informačních technologií, VUT v Brně (www.fit.vutbr.cz).

Určení kontrastních poměrů

Pro definici kontrastu obrazu v této metrice jsme použili Michelsonův kontrast [1,4,6]. Dle definice jsme vypočítali hodnotu lokálních rozdílů intenzit. Jejich zprůměrňováním jsme potom došli k celkovému kontrastu obrazu.



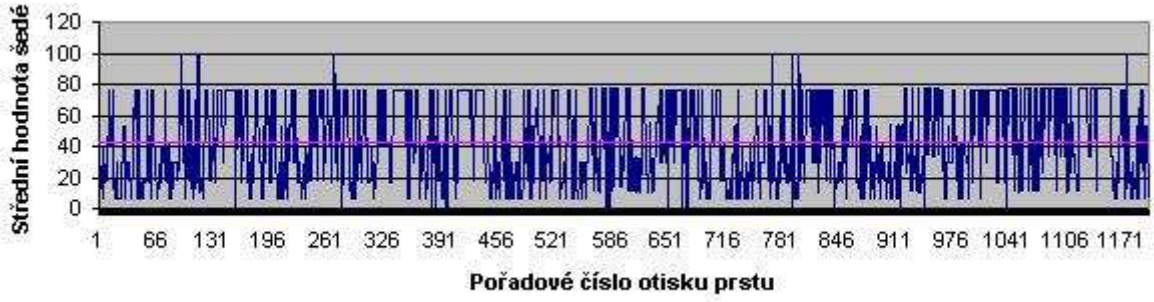
Obrázek 1: Michelsonův kontrastní poměr pro všechny senzory

Lokální rozdíly intenzit jsme určovali na dílčích částech (regionech) obrazu předem specifikovaného rozsahu. Kvůli různým velikostem výstupů jsme se rozhodli určovat lokální rozdíly na poměrných velikostech dílčích částí, jejich velikost jsme zvolili jako přímo úměrnou velikosti celého obrazu.

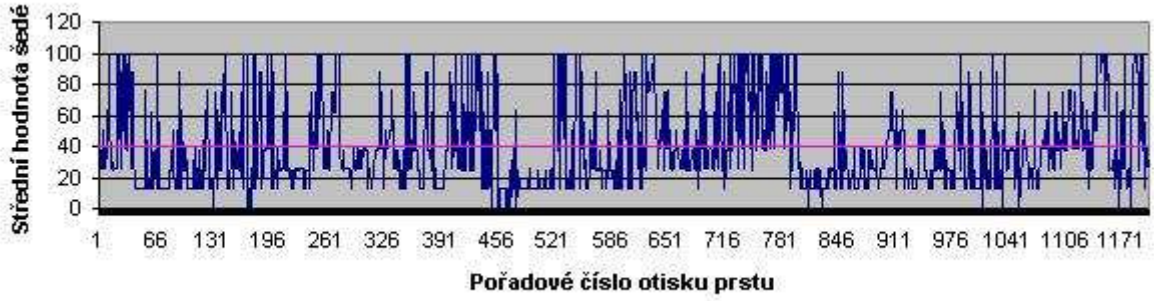
Obecně lze těžko určit přesné hodnoty kontrastu, kterého by měly obrázky dosahovat. Velmi záleží na kvalitě rozpoznávacího algoritmu, jenž může správně rozpoznat i obrázky s nízkými kontrastními poměry. Přesto platí, že čím větší kontrast senzor poskytuje, tím lepší je odlišení papilárních linií od pozadí, a tím kvalitnější je vstup pro rozpoznávací algoritmus. Maximální hodnota kontrastu je 1. Čím více se jí senzory blíží, tím lepší poskytují obrazový výstup. Do této metriky se též promítá kvalita otisku prstu. Čím větší plocha prstu je zachycena, tím vyšší je i kontrast, a tedy i kvalita snímku. Celkové rozložení kontrastních poměrů všech senzorů je uvedeno v obrázku 1.

Střední hodnota šedé

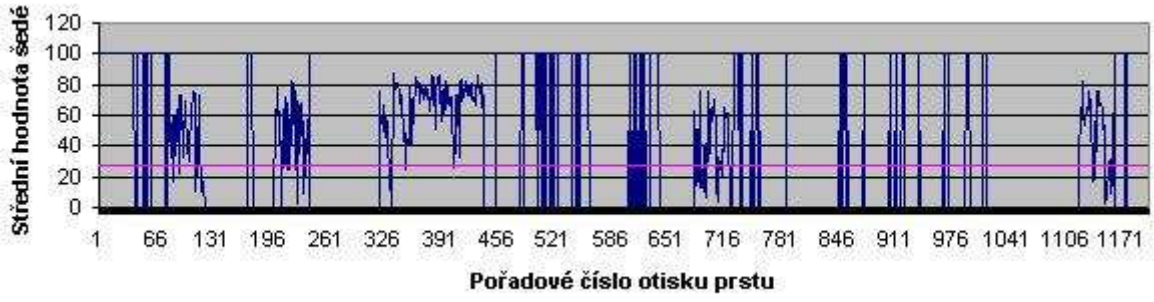
Tato metoda vyjadřuje schopnost senzoru odlišit od sebe pozadí a papilární linie [1,6]. V histogramu obrázku jsou obvykle jasně zřetelné dva vrcholy, které reprezentují právě pozadí a papilární linie.
Níže uvedené grafy vyjadřující kompletní hodnoty odchylek ve všech naměřených vzorcích jsou uvedeny v obrázcích 2 až 5 (modrou barvou jsou znázorněny střední hodnoty šedé pro každý obrázek daného senzoru; fialovou barvou je znázorněna průměrná hodnota).



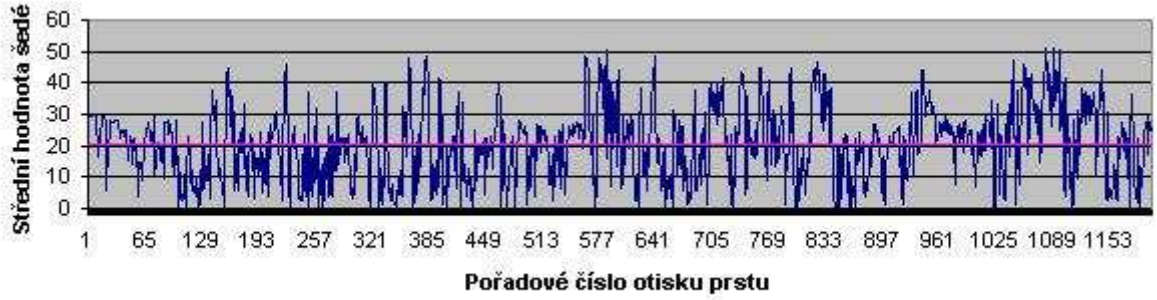
Obrázek 2: Střední hodnoty šedé pro senzor Suprema SFM3000 (průměr ≅ 43)



Obrázek 3: Střední hodnoty šedé pro senzor Suprema SFM3010 (průměr ≅ 40)

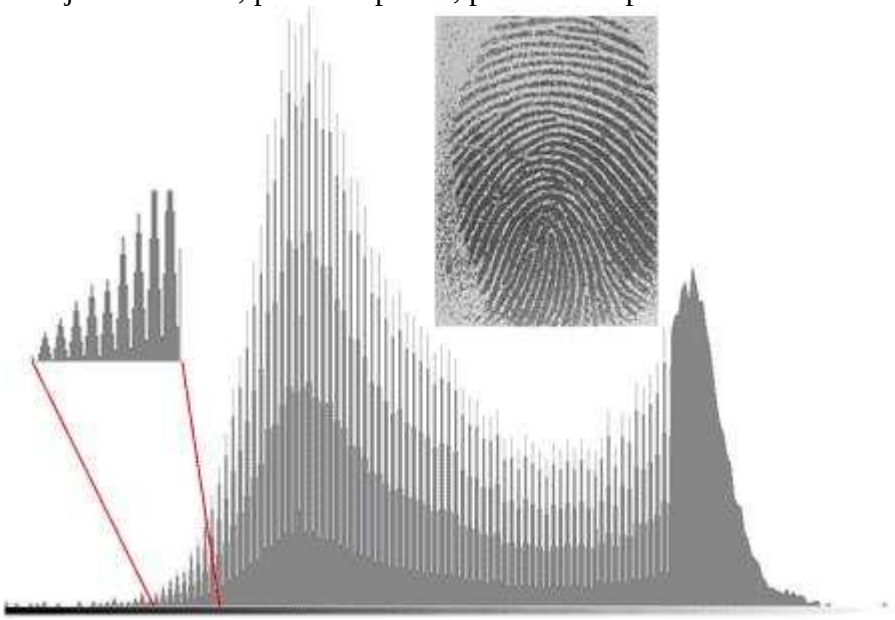


Obrázek 4: Střední hodnoty šedé pro senzor Suprema SFM3020 (průměr ≅ 28)



Obrázek 5: Střední hodnoty šedé pro senzor Suprema SFM3050 (průměr ≅ 21)

Z výše uvedených výsledků nemusí být zřejmé reálné hodnocení senzorů. Přestože některé senzory dosahovaly velkých odchylek a neprošly by tedy toleranční hranicí 20% [6], jejich histogramy vykazovaly dostatečné rozlišení. Výsledky vycházejí z přesného rozboru histogramu, metoda však neposkytuje dostatečné rozlišení v řídkých histogramech. Tyto histogramy mají velmi nerovnoměrné rozložení, ale přesto jsou viditelné dva vrcholy jasně určující papilární linie a pozadí, přičemž ostatní vrcholy jsou téměř zanedbatelné. Proto je nutné umět histogramy správně interpretovat. Plně relevantního výsledku bez nutnosti další interpretace jsme proto dosáhli pouze u senzoru 3050, který poskytuje výstupy s plnohodnotným histogramem.
Zajímavostí vhodné za povšimnutí na testovacích datech ze senzoru SFM3050 je neúplnost histogramu získaných obrázků – viz obrázek 6. Základní linie kopíruje očekávanou křivku, ale při detailním pohledu je vidět, že každá druhá hodnota je nulová. Efektivnost senzoru tím evidentně není nijak ovlivněna, přesto se ptáme, proč senzor provádí toto filtrování.



Obrázek 6: Histogram senzoru SFM3050 (využití pouze poloviny rozsahu osy x)

Počet papilárních linií (RIP Count)

Tuto metriku jsme poupravili pro otisky prstů z přístupových systémů (zde většinou chybí delta). Pro RIP Count [1,2,6] použijeme definici pro výpočet množství papilárních linií v horizontálním a vertikálním směru [2,6]. Obecně lze tvrdit, že čím je hustota papilárních linií v obrázku vyšší, tím přesnější je poté proces rozpoznávání [2,6]. Hustota je též přímo závislá na snímací ploše senzoru.

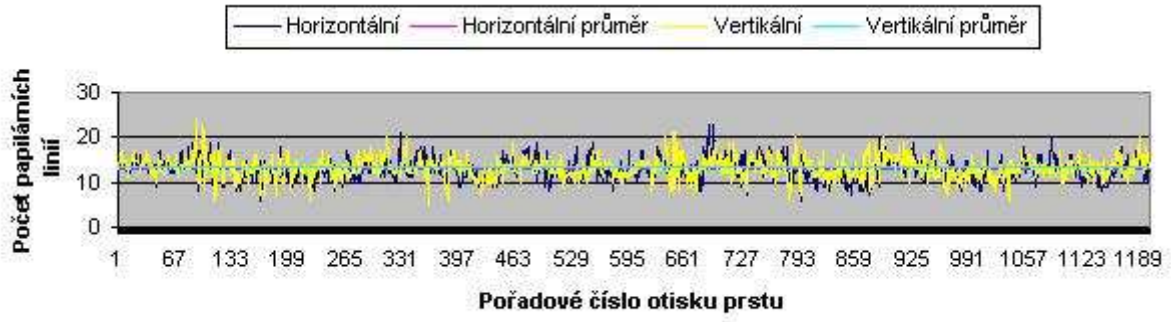
Některé krajní hodnoty nemusejí odpovídat reálnému stavu. Vzhledem k nižší kvalitě některých obrázků nebyla občas možná automatická detekce papilárních linií [6]. Teprve případná aplikace filtru může tyto hodnoty zpřesnit, což již přesahuje rámec těchto testů. Navíc by aplikace filtru zkreslila informace o reálné kvalitě obrázků dodávaných daným senzorem.

Naměřené hodnoty počtu papilárních linií v horizontálním a vertikálním směru jsou sumarizovány v tabulce 1.

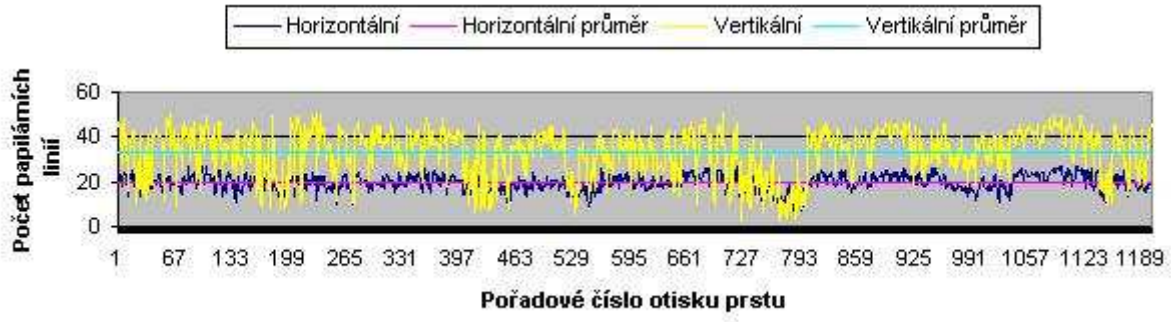
Tabulka 1: Průměrné, maximální a minimální počty papilárních linií

Senzor	SFM3000	SFM3010	SFM3020	SFM3050
Horizontální minimum	6,00	6,00	9,00	10,00
Horizontální průměr	12,86	19,30	19,93	21,25
Horizontální maximum	23,00	27,00	30,00	31,00
Vertikální minimum	5,00	3,00	11,00	11,00
Vertikální průměr	13,26	33,18	22,79	25,67
Vertikální maximum	24,00	51,00	31,00	37,00

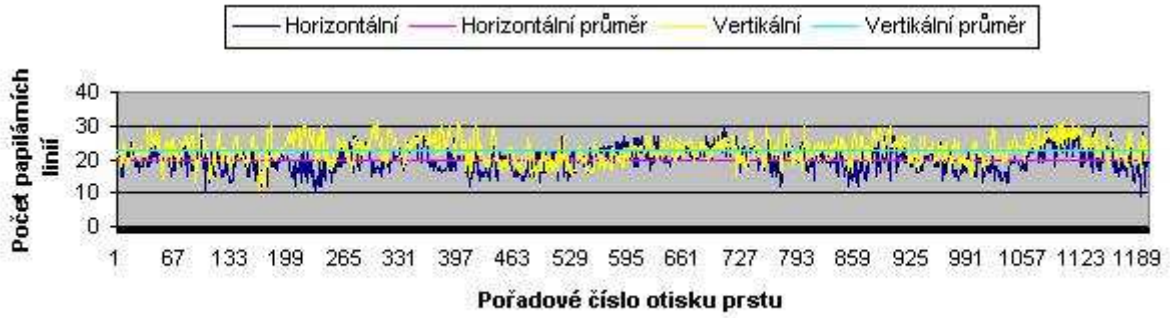
Určení konkrétní hodnoty počtu papilárních linií v daném směru je velmi specifické a tuto hodnotu nelze tedy obecně určit. Pro daný senzor lze ale spočítat dlouhodobý průměr. Když se potom bude některá hodnota aktuálního otisku prstu lišit, může to znamenat, že daný otisk prstu má nevyhovující kvalitu, a mělo by tudíž dojít k načtení nového otisku prstu.



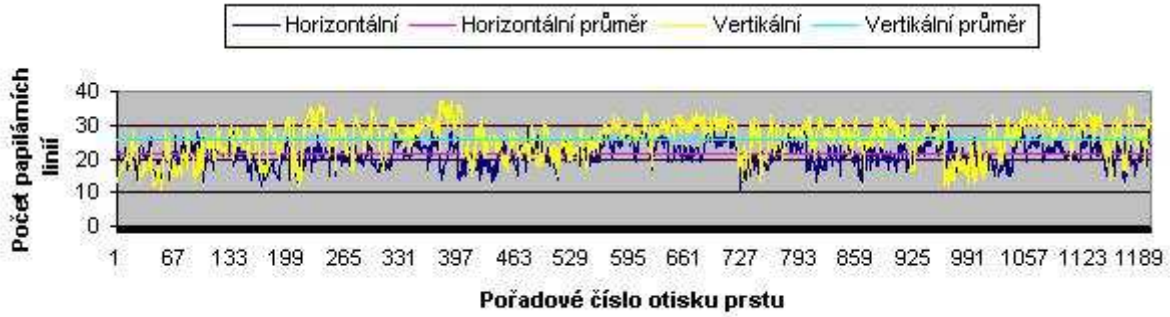
Obrázek 7: Počty papilárních linií senzoru SFM3000



Obrázek 8: Počty papilárních linií senzoru SFM3010



Obrázek 9: Počty papilárních linií senzoru SFM3020



Obrázek 10: Počty papilárních linií senzoru SFM3050

Míra FTA a spokojenost uživatelů

Spokojenost uživatelů je úzce spjata s mírou FTA (*Failure to Acquire*) [1,5,6], ale závisí pochopitelně i na algoritmech zpracování otisku prstu, které následují za fází nasnímání.

Jednotliví uživatelé, kteří se podíleli na tvorbě databáze otisků prstů, zaznamenávali okamžiky, kdy senzor nereagoval na snímání a nebo nenasnímal žádný obrázek, příp. obrázek neobsahoval otisk prstu, ačkoliv uživatelův prst se fyzicky nacházel na ploše senzoru. Dále tito uživatelé zaznamenávali silně zkreslené a nebo poškozené otisky prstů, u nichž nebylo prokazatelné, zda toto zkreslení způsobil uživatel. Všechny tyto výsledky jsou shrnuty v tabulce 2.

Tabulka 2: Míra FTA a procentuální počet nekvalitních otisků prstů jednotlivých senzorů

Senzor / Míra	Míra FTA [%]	Nekvalitní otisk prstu [%]
SFM3000	0,595	7,500
SFM3010	2,140	15,120
SFM3020	0,000	5,710
SFM3050	0,120	5,600

Z tabulky 2 jasně vyplývá, že nejlepších výsledků dosáhl senzor SFM3020, dále SFM3050, SFM3000 a nejhůře dopadl SFM3010.

Uživatelům se nejlépe pracovalo se senzorem SFM3050, čemuž odpovídá i druhé místo ve kvantitativním vyjádření z tabulky 2. Zde se občas projevil problém latentních otisků prstů.

Dalším dobře hodnoceným senzorem byl SFM3010, který zpočátku dělal většině uživatelů problémy, tzn. museli se s ním naučit pracovat. Jakmile ale prošli procesem zaučení a práci se senzorem zvládli, dosahovali velmi kvalitních výsledků. I ze subjektivního pohledu jim připadala práce příjemná, byť tomu neodpovídají hodnoty z tabulky 2. Hodnoty v této tabulce

ovšem obsahují i otisky prstů, které neprošly právě ve fázi zaučování. V tomto případě by bylo lepší vytvořit dlouhodobější statistiku, která by pro tento senzor dopadla asi lépe.

Na třetím místě se umístil senzor SFM3020, jenž sice vykazoval občasné problémy s latentními otisky prstů, ale jinak s ním víceméně nebyly žádné problémy. Nejhůře byl hodnocen senzor SFM3000, který často nereagoval a byl velmi citlivý na vlhké prsty, přičemž latentní otisky prstů mu již činily docela velké potíže.

Kompatibilita senzorů

V rámci provedeného testu jsme se zaměřili i na kompatibilitu jednotlivých snímačů, tzn. co se stane, když se uživatel zaregistruje jedním senzorem a poté se chce verifikovat jiným. Souhrn kompatibility je uveden v tabulce 3.

Tabulka 3.6: Hodnocení přenositelnosti jednotlivých senzorů

		Verifikace (autentizace)			
	Snímač	SFM3000	SFM3010	SFM3020	SFM3050
Registrace	SFM3000	A	---	---	---
	SFM3010	---	A	---	---
	SFM3020	---	---	B	---
	SFM3050	---	---	C	D

Legenda:
A ⇒ Rychlá a příjemná registrace a verifikace, 100% úspěšnost
B ⇒ Uživatelsky náročnější registrace; zvládá rotace ±90°; verifikace prakticky bezproblémová
C ⇒ Prsty musejí být položeny ve stejné poloze a ve stejném směru
D ⇒ Je-li prst v ideální pozici a kvalitní, funguje; zvládá rotace ±50°

Závěr

Závěrem lze tedy říci, že celkově nejlépe se umístil senzor SFM3050 (obdržel celkem 38,1 % bodového hodnocení), který používá kapacitní technologii. Dále se umístil optický senzor SFM3020 (obdržel celkem 31,0 % bodového hodnocení), za ním termický průtahový SFM3010 (obdržel celkem 19,0 % bodového hodnocení) a na konci stupnice se umístil SFM3000 (obdržel celkem 11,9 % bodového hodnocení) s technologií E-Field. Veškeré hodnoty v závorkách byly spočteny dle předchozích výsledků jednotlivých testů (kromě kompatibility).

Literatura

[1] *BioFinger*, Fraunhofer Gesellschaft – Institut für Graphische Datenverarbeitung, Darmstadt, 2004, s. 273

[2] Drahanský, M.: *Biometric Security Systems – Fingerprint Recognition Technology*, disertační práce, FIT-VUT, 2005, s. 140 (ISBN 80-214-2969-0)

[3] Drahanský, M., Nötzel, R., Bonfig, K.W.: *Senzoren zur Fingerabdruckerkennung*, SSS2004, Band 5, Kreuztal, bQuadrat, DE, s. 49-60, ISBN 3-933609-19-4

[4] Dannemiller, J.L., Stephens, B.R.: *Asymmetries in Contrast Polarity Processing in Young Human Infants*, Journal of Vision, 2001, s. 112 – 125, ISSN 1534-7362

[5] Mansfield, A.J., Wayman, J.L.: *Best Practices in Testing and Reporting Performance of Biometric Devices*, National Physical Laboratory & San Jose State University, 2002, ISSN 1471-0005

[6] Drahanský, M., Orság, F., Malinka, K.: *Závěrečná zpráva – Testování senzorů firmy Suprema*, verze 1.4, 2006-2007

D. Možnosti odposlechu optických vláken

Jan Dušátko (jan@dusatko.org)

1. Úvod

Tento materiál slouží pro základní přehled možných postupů pro odposlech optických vláken v ideálním prostředí (nekorozívní prostředí případně ochranná atmosféra). Obsahuje všeobecně dostupné údaje z fyziky, informace o materiálech, technologiích výroby, konstrukci a charakteristikách obvyklých optických tras, následně pak zhodnocení teoretických i praktických možností útoku na komunikační trasy.

2. Optická komunikace

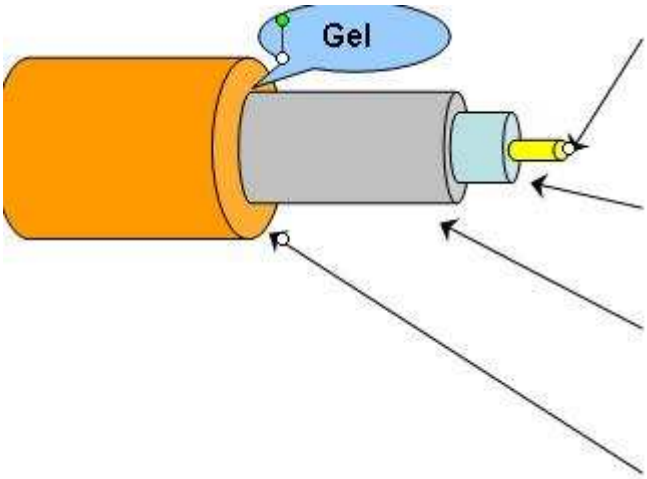
2.1 Základní vlastnosti optických vláken

Základní vlastností optického vlákna a podstatnou výhodou oproti klasickému metalickému vedení je jeho imunita oproti elektromagnetickému rušení. Další vcelku ne nepodstatnou výhodou je teoretická nemožnost toto vlákno odposlouchávat.

Pro pochopení způsobu optické komunikace je nutno znát architekturu optického vlákna. Základem vlákna jsou dvě vrstvy. Jádro s průměrem od 5.2 do 62.5 μm (pro srovnání, lidský vlas má tloušťku okolo 30-75 μm) s nízkým indexem lomu. Pak je to střední vrstva s průměrem 125 μm, která má index lomu vyšší. Jako materiály jsou používány akrylát, polyamid, křemičité sklo nebo křemičité sklo s příměsí fosfátů a neodymu. Ale to není vše. To, co vidíme z optického vedení, je hlavně ochranná vrstva, která pokrývá odrazovou vrstvu a zajišťuje stabilní mechanické připojení konektoru. Zároveň slouží jako ochrana před únikem signálu, neboť má značně vysoké albedo (odrazivost), především ve viditelné části spektra. Celá tato struktura je vložena do opláštění z fluoroplastu, polyamidu nebo kevlaru. Mezi opláštěním a ochrannou vrstvu lze často nalézt gel, který má zamezit vniknutí vody nebo jiných těkavých látek. Ty by mohly po nějakém čase reagovat s materiálem a zvýšit útlum signálu. (Praktická zkušenost: po povodních, kdy byly zatopeny optické trasy jednoho podniku, došlo k masovému jevu, kde z míst svárů vzlínala znečištěná voda a zhruba do roka se zvýšil útlum tak, že bylo nutné trasy vyměnit.)

Doporučená mez poloměru ohybu u optických vláken se pohybuje okolo 50mm, ale je to mez určená pro přenášení signálu. Výrobci udávají mechanické vlastnosti těchto výrobků mez ohybu od 7 do 15 mm. Teplotní rozsahy, při kterých je zaručen přenos, jsou zvláště pro křemičitá vlákna impozantních -190 °C až 390 °C. Pro přenos dat se používají spektra o vlnové délce od 1550 nm (infračervené) do 248 nm (ultrafialové), útlum na vlákně se pohybuje zhruba v rozmezí 2-30 dB, dle materiálu. Telekomunikace nepoužívají plnou spektrální šířku, ale hlavně vlnové délky 1550nm, 1200/1300nm a 750/850nm.

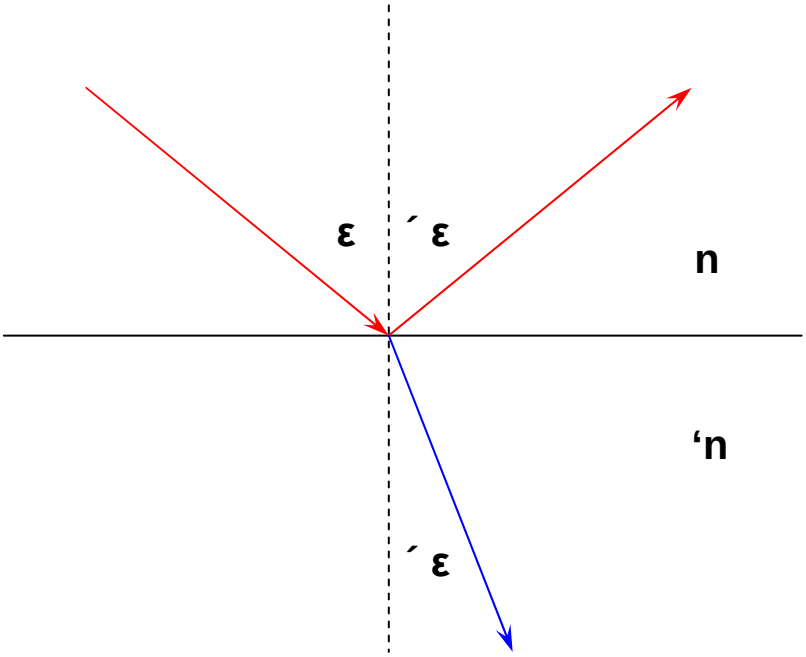
Meze odolnosti
Teplota: -190 °C až 385 °C
Poloměr ohybu: 7 mm při 20 °C
Doporučená mez ohybu r.: 50 mm



Core – jádro, umožňující přenos světelného paprsku, průměr od 5,2 do 62,5 μm, útlum 2-30 dB dle materiálu
(lidský vlas má průměr 30-75 μm),
Vlnová délka světla od 400 nm (fialové) do 1550 nm (infračervené)
Cladding – střední vrstva s vyšším indexem lomu, průměr 125 μm, akrylát / polyamid / křemičité sklo / křemičité sklo s příměsí fosfátů nebo neodymu.
Buffer of Coating – ochranná vrstva pokrývající jádro a odrazovou vrstvu, zajišťuje stabilní mechanické připojení konektorů.
Vysoké albedo ve viditelné části spektra.
Sheat – z fluoroplastu, polyamidu, nebo kevlaru, většinou je mezi touto vrstvou a ***Buffer of Coating*** – ochranný gel kvůli zamezení přístupu vody nebo jiných těkavých látek (difůze nečistot, změna indexu lomu a zvýšení útlumu).

2.2 Principy optického přenosu

Optický přenos je založen na několika základních jevech známých ze středoškolské fyziky. Jedná se o situaci, kdy na rozhraní dvou látek s různým indexem lomu dochází při určitém úhlu k téměř dokonalému odrazu. Při použití optického vlákna je úhel tak nízký, že za standardních podmínek nedochází k téměř žádnému jinému jevu. Pro možnost odposlechu je nutné změnit tyto standardní podmínky. Fyzikální charakteristiky jsou popsány na následujících dvou obrázcích.



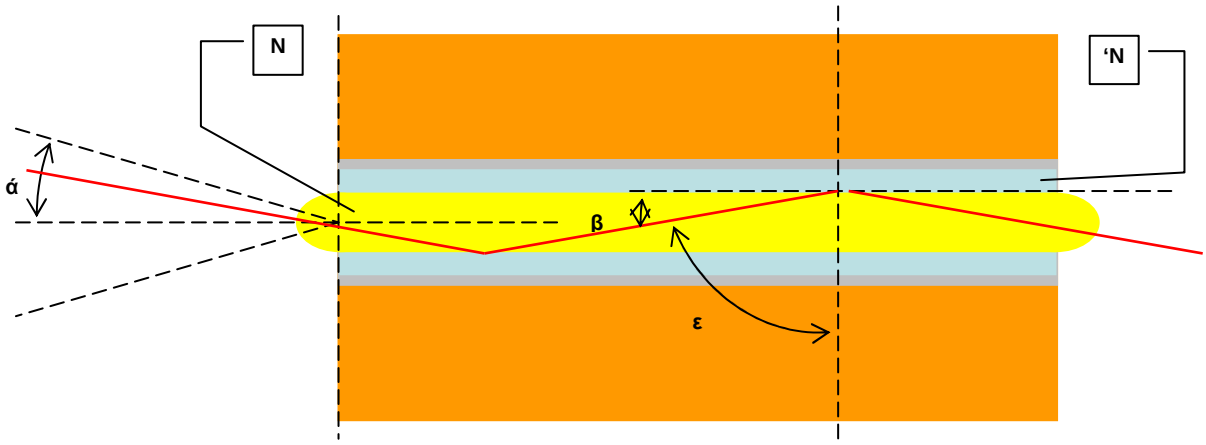
Zákon odrazu
$\varepsilon = \acute{\varepsilon}$

Zákon lomu (Schnelliův)
$\sin \varepsilon / \sin \acute{\varepsilon} = v / \acute{v} = \acute{n} / n$

Index lomu
$n = c/v$

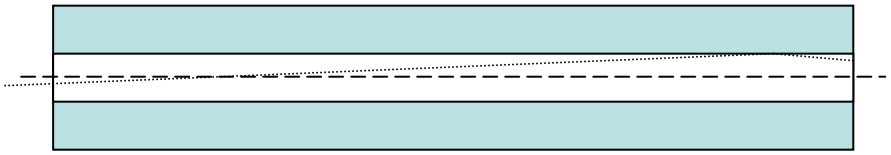
Mezní úhel odrazu
$\sin \varepsilon_m = v / \acute{v} = \acute{n} / n$

Vstupní úhel α signálu - signál, který vstupuje mimo tento úhel, se rozptýlí nebo neodráží, nemá dostatečný úhel.
Numerická Apertura - sinus (90° - úhel odrazu ε) = sin β
Čím větší je NA, tím je vyšší propustnost ale i slabší signál.
Index lomu – poměr rychlosti světla ve vakuu a v udaném materiálu
N – index lomu jádra
N‘ – index lomu střední vrstvy



2.3 Typy používaných vláken

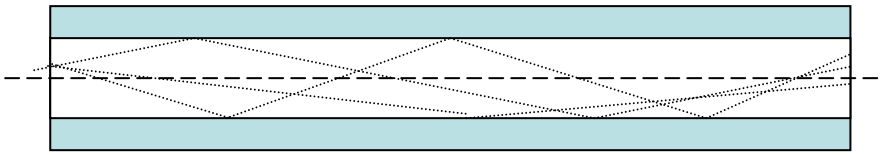
Při optických přenosech se používá podle vzdálenosti několik druhů vláken. Pro delší vzdálenost se používají, tzv. **Single-mode** (jednovidová) vlákna, kde je menší průměr jádra, nižší úhel a díky tomu je potřeba i nižší výkon laseru. Na druhou stranu jsou zde vyšší nároky na přesnost a citlivost zdroje a detektoru. Díky nižšímu počtu odrazů se snižuje i riziko problémů (viz přenosové problémy).



Pro kratší vzdálenost je možné použít multi-mode (vícevidová) vlákna. Jedná se o dvě mírně odlišné technologie.

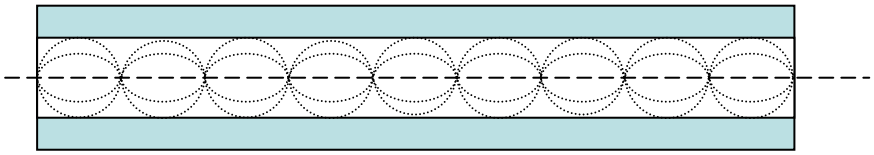
Multimode stepped index

Jedná se o starší technologii přenosu, kde vlákno má větší průměr (vyšší počet odrazů, následně i vyšší energie pro přenos), náklady na výrobu jsou nižší. Díky nižší přesnosti a velkému úhlu dochází ke vzniku barevné chyby (při odrazech dochází k částečné polarizaci a posunům fází). Často trpí přenosovými problémy.



Multimode graded index

Novější technologie přenosu, vlákno má sice větší průměr (vyšší počet odrazů, následně i vyšší energie pro přenos), náklady na výrobu jsou nižší než u single-mode, výroba je náročnější než u starší technologie. V průřezu celého vlákna je odstupňován index lomu, paprsek po delší cestě se šíří nepatrně rychleji a díky tomu se vyrovnává barevná chyba, kterou vícevidová vlákna trpí.



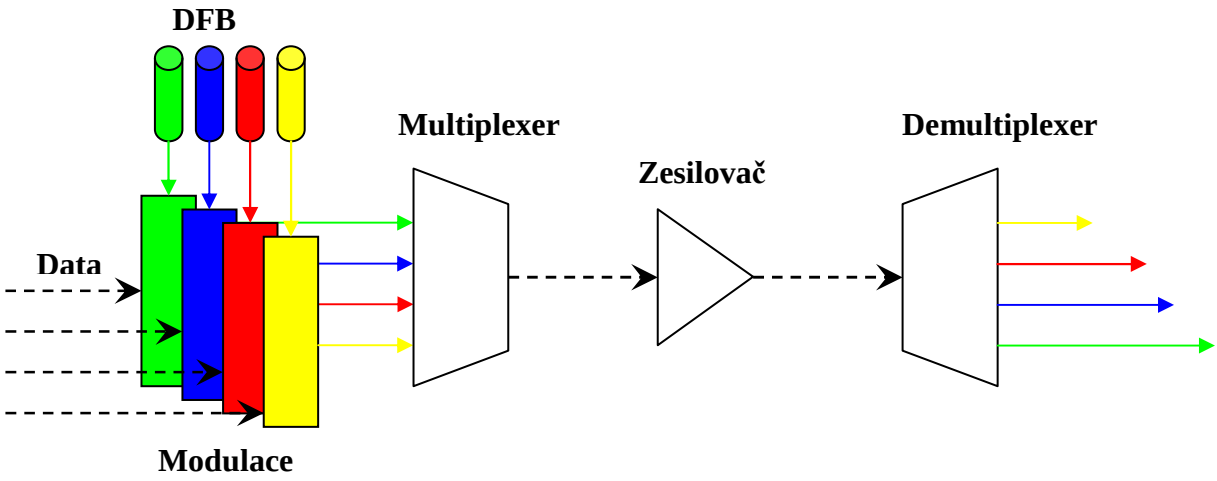
Fotonická vlákna (crystal fibre, hollow-core fibre)

Novinkou v laboratořích jsou nové typy vláken, kde při vytváření není vyplněno jádro ničím než inertním plynem, případně je zde vakuum. Tato vlákna dosahují nadstandardních přenosových charakteristik s téměř nulovým útlumem, na druhou stranu jejich nasazení není otázkou blízké budoucnosti. Zatím se jedná o ryze experimentální prvky, případně speciální aplikace pro odstranění chromatické disperze.

2.4 Možnosti přenosu

Uvedená vlákna se používají pro jednu frekvenci, nebo pro několik frekvencí současně, kdy mezi přenášenými vlnovými délkami je předem daný odstup pásem. Technologie přenosu několika vlnových délek se nazývá DWDM (Dence Wavelength Divisor Multiplexing). Pro tyto přenosy je nutné zajistit vlákna, která mají pro použité frekvence přibližně shodný útlum. Přenosová zařízení jsou podstatně dražší, protože musí zvládnout odfiltrovat a zpracovat několik frekvencí, zároveň i vyšší datové toky.

Princip činnosti jednotlivých DWDM technologií je obdobný. Několik laděných laserů, každý na jiné frekvenci (vlnové délce), zasílá signál do předzesilovače. Ten srovná výsledný výkon signálů na shodnou úroveň. V multiplexeru jsou všechny signály poskládány a odeslány skrz médium. Běžně se používá 32 lambd (vlnových délek), špičková zařízení zvládnou až 128 lambd. Odstup (spaning) mezi jednotlivými kanály (vlnovými délkami) je 50/100/200 GHz.



2.5 Přenosové problémy

2.5.1 Tlumení

Absorpce signálu na nečistotách

Mechanismus, kdy se útlum v materiálu mění na teplo. Signál je odražen, případně pohlcen nečistotami. V případě odrazu může dojít ke skládání opačných fází, což může také způsobit vyrušení signálu.

1) Vlastní (intrizická) absorpce
Je způsobená buď ultrafialovou nebo infračervenou absorpcí. První je způsobena elektronovými přechody ve skle, druhá interakcí fotonů s vibračním spektrem molekul optického skla.

2) Nevlastní (extrinzická) absorpce
Je způsobená kovovými nečistotami a hydroxylovými skupinami zbytkové vody z výroby.

Lineární rozptyl

Přechod části nebo celého optického výkonu z jednoho vidu (lambdy) do jiného vidu. Tyto rozptyly mohou být Mieho[1] nebo Rayleighův[2]. Příčiny Rayleighova rozptylu lze redukovat, ale nelze odstranit.

Nelineární rozptyl

Při vyšších hustotách optického výkonu může dojít zvláště u značně dlouhých vláken k rozptylům. Dochází při něm k přenosům optického výkonu mezi jednotlivými vidy (tedy Brillouinův[3] nebo Ramanův[4] rozptyl).

---

[1] Mieho rozptyl - rozptyl na lokálních nehomogenitách velikosti stejné nebo větší než vlnová délka používaného záření.
[2] Raileighův rozptyl – rozptyl na lokálních nehomogenitách, jejich rozměry jsou menší než vlnová délka použitého záření

Kritický ohyb

Při příliš velkém ohybu dochází k porušení standardních přenosových podmínek a signál se dostane na mezní úhel odrazu. Tento velký ohyb může být značně lokální (malý, namáhání střihem), nebo na vzdálenosti maximálně jednotek mm (velký, ohyb vlákna). V těchto případech dochází k výstupu signálu mimo jádro, ven z vlákna. Podle velikosti ohybu dojde k vyzáření směrem ven nebo směrem dovnitř kružnice, kterou vlákno opisuje. Vyzáření dovnitř vzniká častěji v místech, kde je vlákno namáháno střihem a má značně malý poloměr ohybu (tzv. microbending).

2.5.2 Disperze

Vnitrovidová - chromatická disperze - barevná chyba

Jedná se o shodný princip jako u barevné chyby čoček/rozptylek. Při vstupu nebo při lomu/odrazu na rozhraní, případně při několikanásobných odrazech dojde k posunům fází, po kterých se mohou skládat signály. Výsledkem může být posun spektra. Rozdíly fází mohou být způsobeny optickými vlastnostmi materiálu (**materiálová disperze**) nebo disperzními vlastnostmi struktury vlákna (**vlnová disperze**).

- **Materiálová disperze**
  Vzniká v důsledku různých rychlostí jednotlivých frekvenčních složek v materiálu.
- **Vlnová disperze**
  Vzniká díky rozdílným vlnovým délkám (nepřesný zdroj, vlastnosti optického média, následky chromatické disperze atd.) a rozdílným cestám signálu (následky odrazů).

Mezividová disperze

Vzniká v důsledku zpoždění jednotlivých vidů v mnohobodovém vlákně, výsledkem může být „rozšíření impulsu“ signálu. Tato chyba může být potlačena použitím mnohabodového vlákna.

2.5.3 Vidový šum

Jedná se o fluktuace v přenášeném signálu, jejichž charakteristický čas je delší jak rozlišovací doba optického detektoru. Jsou způsobeny mezividovou disperzí, fázovou korelací mezi jednotlivými přenášenými frekvencemi, nehomogenitami optického prostředí a zdroji s malou spektrální šířkou a velkou koherentní délkou.

---

[3] Brillouinův rozptyl – rozptyl způsobený tepelnými kmity molekul vlákna, foton vzniká v horním a dolním postranním pásmu.

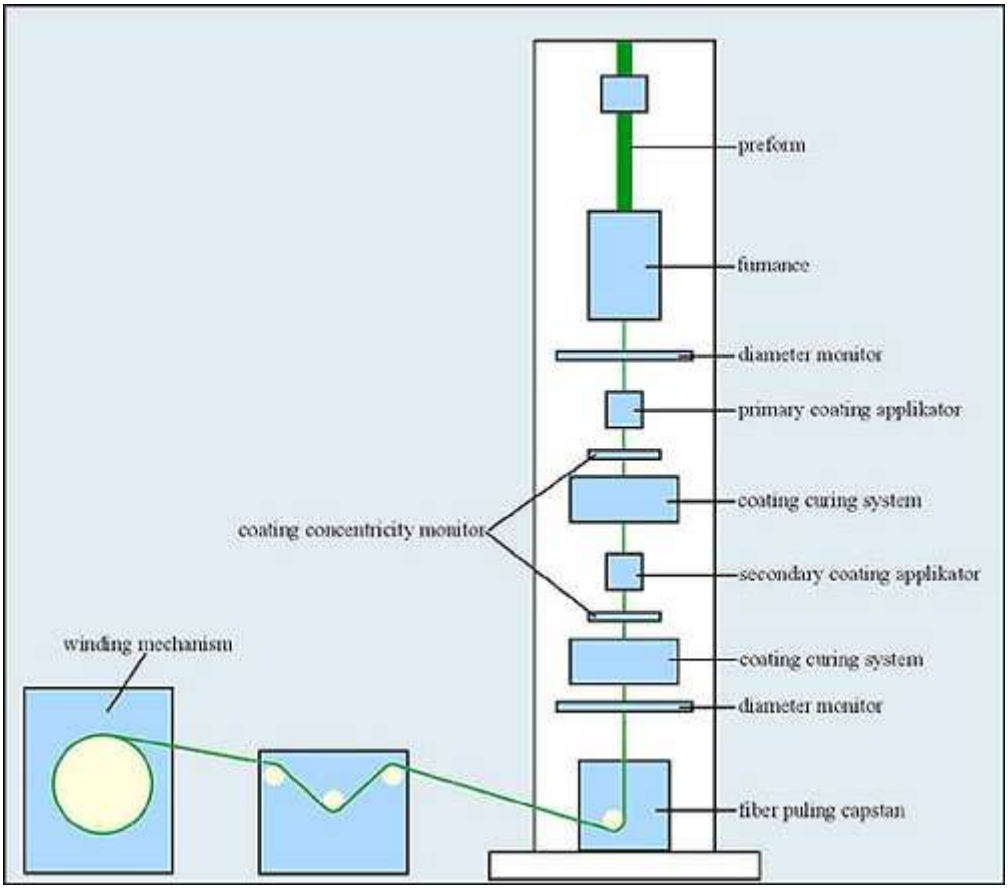
[4] Ramanův rozptyl – rozptyl způsobený tepelnými kmity molekul vlákna, foton vzniká v horním a dolním postranním pásmu, vyšší pravděpodobnost vzniku má foton v horním pásmu.

2.5.4 Polarizace

Všeobecně optická vlákna nezachovávají polarizaci, proto je nutné používat detektory, které nejsou citlivé na směr polarizace přicházejícího signálu. Za určitých podmínek může být zachování polarizace potřebné, v tomto případě je nutné použít materiál, který má požadované vlastnosti vzhledem k přenášené frekvenci.

2.6 Technologie výroby optických vláken

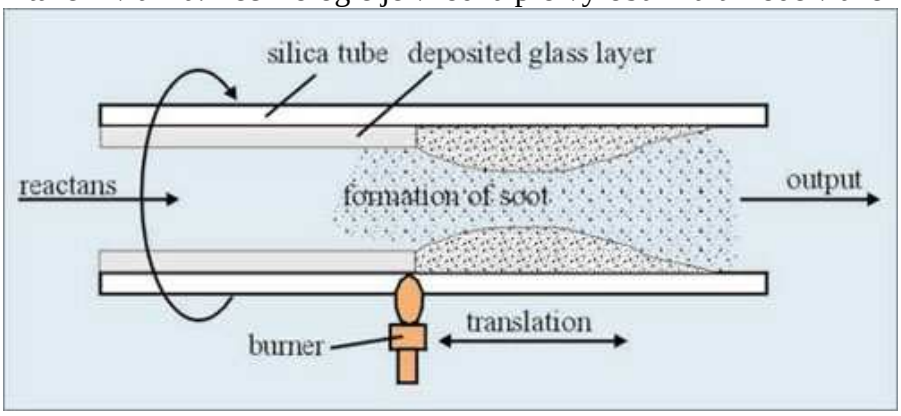
Optická vlákna se v současné době vyrábějí s použitím dvou základních technologií. Jednak je to tažením vlákna ze zdrojového kmene (nejčastěji čistý SiO_2), kde povrch je dopován dalšími prvky. Druhou možností je kmen z vícesložkových materiálů, kde je možné vhodně ovlivňovat index lomu postupem přípravy polotovaru. Obecný postup výroby je uveden v příkladu na následujícím obrázku:



Zdrojovým kmenem (preformou) je válcovitý útvar, z něhož se při zahřátí na teplotu tavení táhne vlastní vlákno. To může být při přípravě dále upravováno. Pro změnu indexu lomu se nejčastěji používají kysličníky boru, fluoru, fosforu a germania. Příprava kmenů je možná pomocí reakcí, které vytvářejí drobné částice těchto kysličníků (reakce těkavých složek kysličníku křemičitého a dopujících prvků v plynném skupenství) a jejich dalším zpracováním. Těkavé složky jsou většinou halogenidy s nízkým bodem varu - $SiCL_4$, $GeCL_4$, BBr_3, atd. Základními metodami využívajícími kondenzace z plynné fáze jsou následující technologie:

2.6.1 MCVD – modifikovaná chemická depozice z plynné fáze

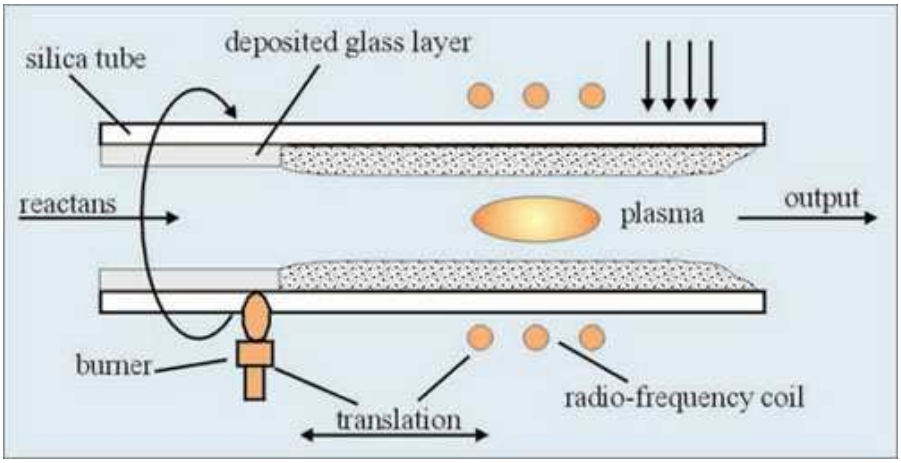
Jedná se o technologii, kde se do trubice z kysličníku křemičitého přivádí směs halogenidů a čistého kyslíku. Tato trubice je místně zahřívána elektrickou pecí nebo kyslíkovodíkovým hořákem, pohyb ohřevu je po celé délce trubice. V zóně se vytváří teplota okolo 1650 °C, kdy jednotlivé složky oxidují a částice se ukládají před horkou zónou. Zároveň s jejich ukládáním dochází k jejich slévání. Změny indexu lomu se dosáhne vhodnou modifikací složení plynné fáze. Po ukončení kondenzačního procesu se trubice po celé své délce zbortí a připraví tak k tažení vlákna. Technologie je vhodná pro výrobu Multimode vláken.



2.6.2 PMCVD – plazmatická modifikovaná chemická depozice z plynné fáze

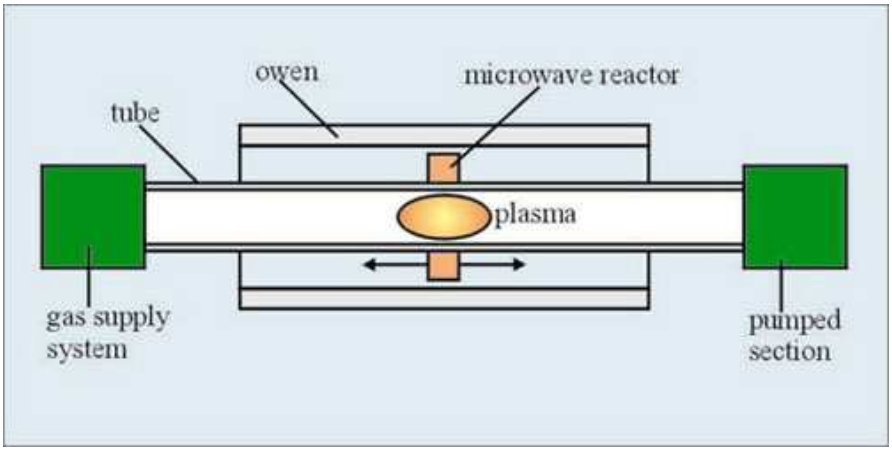
Tato technologie je podobná předchozí technologii, jen místo vstupu plynů vstupuje neizotermické nebo izotermické plazma udržované mikrovlnným generátorem. Tato technologie umožňuje podstatně přesnější řízení profilu indexu lomu a dosahuje se vyšší rychlosti ukládání

.



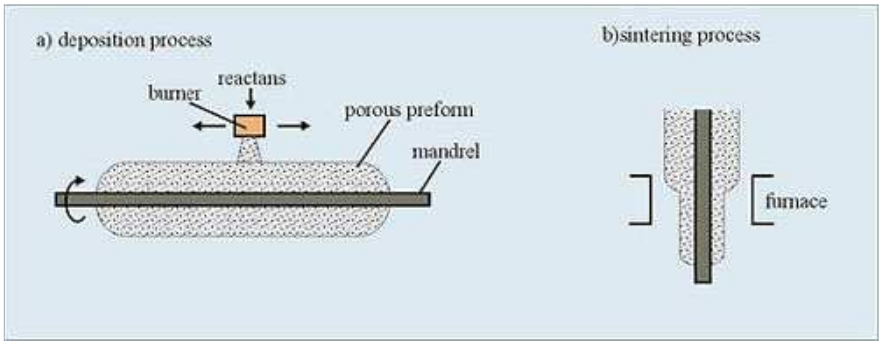
2.6.3 PCVD – plazmatická chemická depozice z plynné fáze

Při použití tohoto postupu je kyslíkovodíkový hořák nahrazen plazmatickým prstencem. To znamená urychlení postupu, protože odpadají fáze sušení a spékání. Touto metodou se vyrábějí vlákna PCV (Plastic Clad Silica), kde jádro je z SiO_2 a plášť ze silikonové pryskyřice, nebo vlákna s jádrem s kysličníku křemičitého a s pláštěm z dopovaného kysličníku křemičitého.



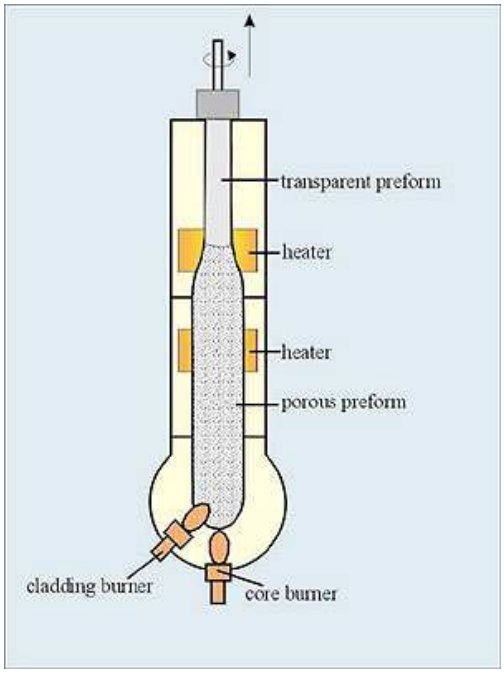
2.6.4 OVD – vnější depozice z plynné fáze

Metoda OVD, jinak také hydrolýza plamenem, OVPO nebo extrémní CVD byla první, při které byla vyrobena gradientní vlákna s nízkým útlumem. Halogenidy se při ní vstřikují přímo do plamene hořáku, po výsledné reakci se kysličníky usazují na povrchu trnu (jádra). Dochází tak k řízenému usazování částic s požadovaným chemickým složením.



2.6.5 VAD – axiální depozice z plynné fáze

Uvedená technologie je variantou předchozí OVD, kde jsou použity dva hořáky. Jeden v axiální ose a jeden v radiální ose. Díky tomuto postupu odpadá vysoušení a spékání, je možné vyrábět kontinuálně vlákna s požadovanou přesností.



2.7 Přehledy vlnových délek, typu laserů a dalších charakteristik

tabulka 1 - Nejčastěji používané vlnové délky, výkony laseru a typy vláken

Vlnová délka nm. min.	Vlnová délka nm. max.	Výkony v mW	Typ vlákna
650	660	50, 100	Multimode
780	800	50, 100	Singlemode
805	810	500	Multimode
820	840	50, 100	Singlemode
840	870	50, 100	Singlemode
920	950	50, 100	Singlemode
960	990	50, 100	Singlemode
975	980	500, 1000, 1500	Multimode

tabulka 2 - Nejčastěji používané typy laseru a průměrný útlum vhodných vláken

Vlnová délka nm	Typ laseru nebo zesi-lovače	Útlum signálu dB
1550	LED	0.050
1300	LED	0.030
1064	ND:YAG	0.012
850	LED	0.013
820	LED	0.006
647	Krypton Red	0.008
633	HeNe	0.008
532	KTP	0.013
515	Argon Green	0.014
488	Argon Blue	0.013
308	Excimer	0.27
248	Krypton Fluoride	1.1

tabulka 3 - Rychlost datových toků, délka bitu a řádové množství fotonů

Rychlost v Mbit/s	**Rychlost v MB/s**	**Délka bitu m/bit**	**Délka paketu (2 KB)/m**	**Řádové množství fotonů na jeden bit z laseru 1W při λ=1250 nm**
1	0,125	286,0906	4687308,79	10^{21}
10	1,25	28,6091	468730,88	10^{20}
100	12,5	2,8609	46873,09	10^{19}
1000 (1 Gb/s)	125	0,2861	4687,31	10^{18}
10000 (10 Gb/s)	1250	0,0286	468,73	10^{17}
100000 (100 Gb/s)	12500	0,0029	46,87	10^{16}

tabulka 4 - Vztah vlnové délky a energie fotonu

Vlnová délka λ	Energie fotonu
1550 nm	$1,28*10^{-28}$
1300 nm	$1,52*10^{-28}$
1064 nm	$1,86*10^{-28}$
850 nm	$2,33*10^{-28}$
820 nm	$2,42*10^{-28}$
647 nm	$3,07*10^{-28}$
633 nm	$3,14*10^{-28}$
532 nm	$3,73*10^{-28}$
515 nm	$3,85*10^{-28}$
488 nm	$4,07*10^{-28}$
308 nm	$6,45*10^{-28}$
248 nm	$8,01*10^{-28}$

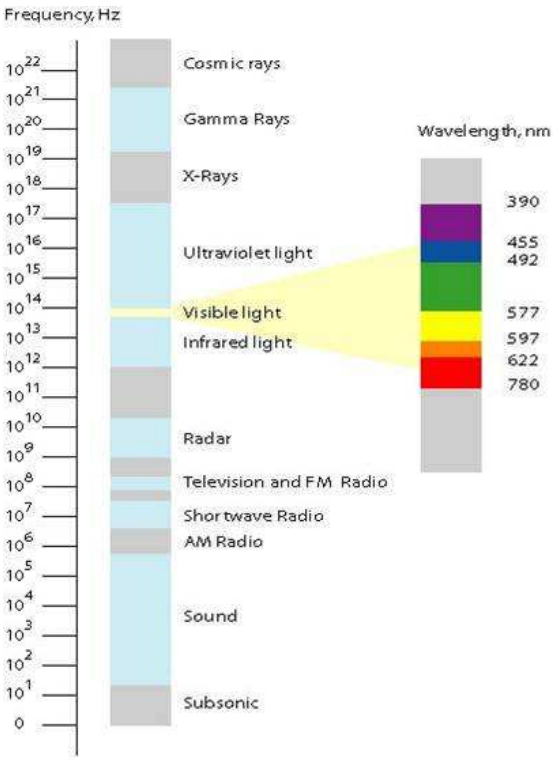
Vlnová délka světla nejčastěji používaná v IT λ=1250 nm

Rychlost světla c=299987762,254372 ms^{-1}

Planckova konstanta h=$6,626068*10^{-34}$ kgm^2s^{-1}

Energie fotonu E=hc/λ

2.8 Přehled frekvenčních rozsahů



Tento přehled ukazuje frekvenční rozsahy, které platí ve spodní části spektra hlavně pro snáze pochopitelný zvuk. Je zde hlavně pro ilustraci jednotlivých frekvenčních rozsahů a vlnových délek pro část elektromagnetického vlnění - světlo.

3 MOŽNOSTI ODPOSLECHU OPTICKÝCH TRAS – OBLASTI

Pro odposlech optických tras lze využít několik fyzikálních zákonitostí, většinou se jedná o různé využití odrazu a lomu, může to ale být i rozdělení paprsku nebo některé formy převodu signálů. Zde jsou zmíněny možnosti postavené na jednotlivých fyzikálních principech.

3.1 S přerušením vlákna

3.1.1 Optická výhybka

Optická výhybka je zařízení ve tvaru písmene „Y“, které se vloží do cesty signálu. Při správné konstrukci jde část paprsku jedním ramenem a část druhým ramenem. Při průchodu se signál rozdělí na dvě části, jedna pokračuje a může být svedena do monitorovacího zařízení, kde je dále zpracována, druhá prochází skrz původní trasu.

3.1.2 Optotronika

Optotronika je (bude) digitální výpočetní technika postavená na optických prvcích. V tuto chvíli existují spolehlivé optické zesilovače, první tranzistory a další zařízení, ze kterých lze

sestavit optický obvod schopný zpracovat vstupující signál, to znamená vytvořit z něho kopii schopnou dalšího zpracování.

3.1.3 Optoelektronický převodník

Optoelektronický převodník je libovolné zařízení, které převádí optický signál na elektronický a obráceně. Jako převodník může být brán i aktivní nebo pasivní prvek, podstatně výhodnější je ale specializované zařízení. Signál je na jedné straně převeden na elektrický signál, který se určitým způsobem zpracuje (vytvoření kopie a/nebo modifikace), je pak převeden na optický signál a dále odeslán.

3.2 Bez přerušení vlákna

3.2.1 Ohyb vlákna

Ohyb vlákna je tou nejjednodušší metodou, jak odposlechnout komunikaci bez narušení trasy. Protože při ohybu vlákna dojde k narušení standardních podmínek odrazu (bude se měnit úhel, pod kterým je signál odrážen), může dojít až k částečnému odrazu signálu, tj. úhel pod kterým se signál odráží, se dostane na svoji mez. Část signálu pak pokračuje správnou cestou, dojde k odrazu, část je nasměrována do vrstvy s vyšším indexem lomu, tedy dojde k lomu. Požadavkem je zamezit rozptýlení tohoto signálu v ochranné vrstvě a tento signál patřičným způsobem zpracovat. Tato technologie nebude použitelná u fotonických vláken (crystal core, hollow-core fibre) z důvodu příliš velké numerické apertury, ohyb vlákna by musel být v řádech mikrometrů.

3.2.2 Využití kvantových jevů

Další metodou je využití kvantových jevů, které vznikají na rozhraní materiálů. Kvantového tunelování je schopná každá částice (otázku, zda je vhodné foton považovat za částici, nechávám stranou). Princip těchto zařízení spočívá v tzv. potlačeném úplném odrazu. Na těchto principech již existují optická zařízení známé jako děliče svazku. Jde například o dva hranoly, kde v jednom je úhel vstupu proudu fotonů / elektromagnetické vlny takový, aby docházelo na rozhraní k úplnému odrazu. Rozhraním je v tomto okamžiku míněn přechod z materiálu do okolního prostředí. Protože v místě odrazu vzniká určitá forma vlnové poruchy, přiblížení druhého hranolu na určitou dostatečně malou vzdálenost (tuto vzdálenost lze spočítat – jedná se o velikost potenciálové bariéry pro kvantový tunelový jev) umožní přenos tohoto signálu. Se vzrůstající vzdáleností mezi těmito hranoly exponenciálně klesá počet fotonů, které „přeskočí“ vrstvu, jenž je pro ně díky zákonům odrazu jinak zakázaná. Podobným způsobem je možné realizovat zařízení, kde místo hranolů je použit optický kabel.

3.2.3 Omezení dané kvantovými jevy a kvantová kryptografie

Stejně jako je možné využít některých kvantových jevů, jiné jevy omezují nebo zabraňují možnosti odposlechu. Nejčastěji zmiňovanou metodou odolnou proti odposlechu je kvantová kryptografie. Příčinou těchto neúspěchů je několik. Jednak signál není posílán velkým souborem fotonů (viz **tabulka 3**) jako u klasického signálu, dále je pak vlastní měření stavu fotonu omezeno některými fyzikálními zákony. Tyto zákony ve výsledku znemožňují odposlech zprávy bez její modifikace. Protože přenos je založen na směru polarizace fotonu a detekci jeho přítomnosti, současné fyzikální znalosti nás opravňují k předpokladu, že potencionální útočník má možnost získat pouze jednu hodnotu. Nevýhodou tohoto kanálu je možnost náhodné ztráty přenášeného signálu díky jevům spojeným s tímto přenosem (viz. **Chyba! Nenalezen zdroj odkazů.**). Tato nevýhoda se může stát pomocníkem v obraně proti odposlechu.

4 NÁVRHY KONKRÉTNÍCH REALIZACÍ

4.1 Návrh optické výhybky

Optickou výhybku je možné realizovat dvěmi způsoby. Buď tou nejjednodušší formou, tedy zařízením ve tvaru písmene Y, kde za dodržení určitých pravidel konstrukce dojde k rozdělení svazku, druhou možností je vytvoření děliče svazku na základě potlačení úplného odrazu nebo použitím polopropustného zrcadla. Druhé jmenované zařízení má výhodu v možnosti regulovat intenzitu procházejícího záření a intenzitu záření svedenou do monitorovacího kanálu.

4.2 Návrh optotronického zařízení

Optotronika je (bude) digitální technikou založenou na zpracování optického signálu. Tato technika je zatím v plenkách a zpracování signálu je určeno pro velice specifickou vlnovou délku. Vlnové délky mimo rozsah budou zařízením pohlceny nebo rozptýleny. Z těchto důvodů bude muset být před vstupem do zařízení barevný filtr, který jiné frekvence od odesilatele odkloní na zpracování do přístroje pro danou frekvenci. Optotronika by měla dokázat přímo v místě signál analyzovat, př. i modifikovat, kopii odesílat třetím kanálem a data odesílat na výstupu příjemci tak, aby měli stejnou intenzitu jako na vstupu. Zařízení se pro danou frekvenci a digitální signál může chovat jako zařízení, které nemá žádný útlum. Zvnějšku (pro měřicí přístroje) bude tedy nerozlišitelné od kabelu. To je jen jedna z možných variant, existuje určitý počet možných zapojení podobně jako u elektronických schémat. Toto zapojení bude určitě dané požadavky kladenými na přístroj.

4.3 Návrh optoelektronického zařízení

Optoelektronická zařízení se dnes v komunikační technice vyskytují všude, kde je nutný převod elektronické komunikace na optickou a zpět. V principu jde o zařízení, které se vloží do cesty optickému signálu. Na vstupu dojde k přeměně optického signálu od odesilatele na elektronický, ten je určitým způsobem zpracován/modifikován, následně přeměněn zpět na optický a odeslán příjemci. Na vstupu i výstupu by měla být možná modifikace, která umožní simulaci zbytku trasy. Požadovaná zařízení by neměla mít MAC adresu, případně by měla být schopna ji skrýt nebo podvrhnout. Další a to dost podstatnou nevýhodou je rychlost šíření signálu, která je pro elektroniku zhruba 0,6c. Právě s těmito problémy je nutné počítat a upravit chování zařízení takovým způsobem, aby nebyl detekován „nárůst vzdálenosti“ nebo jiné, odesílatelem či příjemcem neočekávané stavy, které by toto zařízení na trase představovalo.

4.4 Návrh zařízení pro odposlech při ohybu

Odposlech při ohybu vlákna je založen na principu měnícího se úhlu dopadu a odrazu. Jednak může dojít k jevu částečného odrazu, který zvýší útlum ale signál je mimo střední vrstvu, dále může dojít k úplnému odrazu a signál je směrován mimo vlákno. Pro meze ohybu se v normách udává rádius 50 mm, mez ohybu vlákna udávaná výrobci se pohybuje u poloměru 2-5 mm, dle vlákna a výrobce.
Pro odposlech je nutné se zbavit obalu z plastů, ochranného gelu a hlavně v maximální možné míře ochranné vrstvy, která má značně vysoké albedo. Tato vrstva je schopná často vystupující signál znehodnotit. Vzhledem k chemickým vlastnostem je nutné použít značně agresivní

chemikálie, povrch vlákna pak neutralizovat. Pro broušení a leptání je nutné zajistit podmínky, které neumožní vstup jakýchkoliv agresivních složek do jádra nebo střední vrstvy (mohlo by dojít k nežádoucím jevům). Takto upravené vlákno je nutné ohnout na předem spočítaném poloměru. Protože se vstupní údaje pro výpočet liší podle typu aplikace (druh optického kabelu[5] - jeho numerické apertury[6], vlnové délky[7] signalizace, vstupního úhlu[8] a druhu použitého média – SM, MM-GI, MM-SI), je vhodnější použít přípravek, který dovolí v určitém rozmezí zmenšovat a zvětšovat poloměr ohybu. Vhodné nastavení nechá část signálu uvnitř vedení a zajistí jenom částečný „odběr“. Pro hrubý výpočet velikosti ohybu stačí základní znalosti trigonometrie.

4.5 Návrh zařízení pro injektáž při ohybu

Návrh zařízení pro injektáž optického signálu zpět do vlákna a modifikaci datového toku při ohybu spočívá na podobných principech jako předchozí zařízení. Podmínkou je zde úplné vyzáření signálu a následně opačným způsobem injektáž signálu skrz obal zpět do jádra. Při znalosti vstupního výkonu signálu[9], indexu lomu vzduchu a materiálu jádra je možné spočítat intenzitu, místo a vstupní úhel signálu injektovaného zpět do jádra. Při vstupu dojde k určitému rozptýlení signálu, které se těžko odlišuje od chyb na trase. Lepší výsledek zajišťují optoelektronická zařízení.

4.6 Návrh pro odposlech pomocí potlačení úplného odrazu

Na rozdíl od aplikací jako je dělič svazku, odposlech pomocí principu potlačení úplného odrazu[10] vyžaduje malou bariéru. Ta musí mít vyšší index lomu, aby docházelo k odrazu zpět do jádra, na druhou stranu musí mít pouze omezenou šířku, aby se chovala jako potenciálová bariéra. Protože signál je velice slabý, musí být téměř okamžitě zesílen a zpracován dříve, než dojde k jeho utlumení.

5 MOŽNOSTI DETEKCE ÚTOKU

5.1 Detekce přerušení vlákna

Detekce, případně přesné určení přerušení je možné při použití přístroje na principu OTDR[11] (Optical Domain Time Reflectometry). Pomocí tohoto přístroje je možné zjistit celkovou délku trasy z bodu měření, případně další problémy.

---

[5] Index lomu je možné dopočítat při znalosti látek tvořících přenosové médium.
[6] Numerickou aperturu nebo indexy lomu je možné získat buď na stránkách výrobce vlákna, nebo hledáním vlastností specifikovaných materiálů.
[7] Vlnová délka signálu závisí na typu vlákna a oblasti aplikace
[8] Vstupní úhly (úhly akceptace signálu) je možné dopočítat z NA (numerické apertury).
[9] Celkový výkon je daný výkonem laseru na straně odesílatele a útlumem vlákna
[10] Princip potlačení úplného odrazu je popsán ve Fenymanových přednáškách z fyziky (druhý díl, strana 625-627)
[11] Tyto přístroje používají metodu zpětného rozptylu, tzv. optickou reflektometrii, která je založená na měření optického výkonu rozptýleného (Rayleighův rozptyl) v různých bodech optického vlákna

5.2 Detekce změny útlumu vlákna

Stejně jako v případě přerušení vlákna je možná detekce, případně přesné určení místa nebo míst útlumu při použití přístroje na principu OTDR. Tento přístroj dokáže vyhodnotit celkový útlum trasy, útlum jednotlivých prvků (sváry nebo jiné spoje) a měrný útlum jednotlivých vláken.
Jednou z dalších možností je měření přijímaného zářivého výkonu na straně aktivního prvku a jeho monitorování. Některé aktivní prvky pro telekomunikace již mají implementovány metody pro monitorování změny útlumu komunikační trasy.

5.3 Detekce změny indexu lomu prostředí

Přestože ODTR dokáže vyhodnotit nehomogenitu vláken, detekce změny indexu lomu prostředí (například difůzí specifických rozpouštědel nebo agresivních látek, jakými je např. voda) jsou nejednoznačné. Je možné zde zjistit změnu útlumu v daném místě, způsobenou například právě vodou, a detekovat změnu charakteristik média a přibližnou vzdálenost.

5.4 Detekce změny charakteristik barevné chyby

Protože každý optický kabel má určitou barevnou chybu (závisí na konstrukci vlákna), je možné vlastnosti barevné chyby použít i pro testování, zda nedošlo k narušení komunikačního kanálu. Hypoteticky je možné použít barevnou chybu kabelu nebo trasy pro tuto diagnostiku, měření by muselo být prováděno na úrovni přijímače. Takové zařízení by muselo v určitých časových intervalech tuto chybu měřit a společně s útlumem vyhodnocovat.

5.5 Detekce přítomnosti optického zesilovače

Optický zesilovač lze detekovat alespoň následujícími metodami. První vychází z principu provozu tohoto zesilovače, který je laděný pro určitou, předem danou frekvenci. Pro detekci tohoto zesilovače je možné zaslat signál na frekvenci s určitým odstupem a zjišťovat rozdíly charakteristik. Pokud se liší od předpokládaných (naměřených nebo modelovaných charakteristik), je značně pravděpodobné, že je zde takové zařízení umístěno. Druhá metoda je závislá na naměřených charakteristikách vlákna, uložených v databázi. Vlákno časem ztrácí svoje přenosové vlastnosti a zvyšuje útlum. Jakékoliv snížení útlumu nebo jeho skoková změna je známkou pravděpodobného nasazení uvedeného zařízení. Poslední metodou je detekce změn barevné chyby. Změny barevné chyby jsou minimální, hodně závisí na použité technologii, vzdálenosti a stavu vlákna. Jakýkoliv zesilovač tuto chybu odstraňuje, „čistí“ signál a tedy zároveň odstraňuje vedlejší efekt barevné chyby.

5.6 Detekce přítomnosti digitálního zařízení pro zpracování dat (optotroniky)

Přítomnost digitálního zařízení pro zpracování dat lze zjistit několika způsoby. Asi nejjednodušším je odeslání analogového signálu na vedlejší frekvenci takovým způsobem, který je obtížně digitálně zpracovatelný. Protože digitální příjem a vysílání je řešeno určitými stavovými signály, je možné zaslat záměrně zdeformovaný signál, který digitální zařízení nezaregistruje (mimo nosnou frekvenci) nebo jej není schopné zpracovat (deformace signalizace). Pokud je na cestě zařízení pro zpracování dat, je nuceno signalizací k opakování přenosu (principy komunikace). Podmínkou jsou dvě zařízení na opačných stranách komunikační lin-

ky s nastavenými metodami testování a vyhodnocení těchto deformací signálu. Jedná se o jednu možnost, jak lze tuto přítomnost (hypoteticky) testovat.

5.7 Detekce změny při kvantovém přenosu

Při kvantování optického signálu je nositelem informace polarizace signálu. Díky neurčitosti není možné najednou změřit (detekovat) foton a jeho polarizaci. V okamžiku odposlechu dochází k modifikaci jednoho z parametrů (foton stočí rovinu polarizace a informace se ztratí nebo dojde k jeho pohlcení a informace se také ztratí). Zatím není známa metoda, jak tento kanál odposlechnout bez modifikace přenášených dat. Na druhou stranu, tento kanál musí mít implementován korekční mechanismy z důvodu možnosti náhodné ztráty signálu. Proto potenciální útok na kvantovou kryptografii bude založen nejspíše na metodách, které by teoreticky mohly využívat vlastnosti vyšší vrstvy (chyby návrhu korekčních mechanismů).

6 ZHODNOCENÍ RIZIK A MOŽNÉ OCHRANY

Pro zhodnocení jednotlivých rizik je u datových přenosů na optické trase nutné znát nejenom metody použitelné pro odposlech, ale i pro zpracování dat. Dále do hry vstupuje potenciální zájem o subjekt např. z ekonomického hlediska a další možnosti.

6.1 Riziko přerušení spojeni

Je ekvivalentem DoS útoku, jedná se o znemožnění komunikace. Díky jednoduchosti realizace a výsledným dopadům je tato hrozba nejsilnější a je tak vhodné ji ohodnotit nejvyšším rizikem. Tuto hrozbu je možné realizovat za cenu v řádu stovek až tisíců korun, může se jednat jak o vandalství, tak o znemožnění komunikace v určitých klíčových okamžicích předem připraveným útokem.

Detekce tohoto útoku je poněkud problematická. Diagnostikou trasy lze poznat za určitých podmínek přibližnou vzdálenost (tedy oblast, proto není vhodné šetřit na managementu prvků), pomocí měřicích přístrojů i konkrétní umístění.

Obranou proti této hrozbě je využití redundantních sítí, nebo komunikační struktury poskytovatele jako je MPLS. Protože výstavba vlastních tras je vysoce nákladná, je vhodnější použití dodané komunikační služby a zajistit je vhodnými kryptografickými technikami.

Cíle útočníka:

- důvod přerušení spojení
- zjištění přenosové trasy
- fyzický přístup k médiu
- fyzické prostředky (krumpáč)

Cíle napadeného:

- snížení významu přerušení trasy (nákup komunikačních tras od třetí strany, redundance tras)
- transakční režim přenosů
- včasné upozornění a náprava

6.2 Riziko odposlechu přenášených informací

Hrozba odposlechu přenášených dat je podstatně nižší, při množství subjektů používajících optické trasy a „zajímavosti“ těchto subjektů se jedná o přibližně 3 - 5 % firem (banky, výzkum, vývoj). Pro realizaci hrozby přerušení spojení stačí „nůžky“, pro odposlech je již nutné značně sofistikované zařízení a nějaká ta výpočetní technika. Vzhledem k finanční náročnosti tohoto útoku je nutné počítat s investicí v řádu tisíců až miliónů korun. Tato metoda útoku musí přinést útočníkovi zisk, který je srovnatelný nebo vyšší než investovaná částka. Zde mohou hrát roli ekonomické nebo politické zájmy.

Detekce tohoto útoku záleží na schopnostech aktivních prvků a četnostech jejich měření. Je zde možné detekovat útlum, změnu barevné chyby nebo indexu lomu prostředí. Nevýhodou je, že současná zařízení nedokáží plně pokrýt detekčními schopnostmi jednotlivé možnosti útoku.

Obranou proti této hrozbě je při dostatečné citlivosti dat (citlivá nebo cenná = zpeněžitelná data) použít šifrovací zařízeni s dostatečně silným klíčem. Cena těchto zařízení je sice vysoká, ale eliminují tak význam odposlechu.

Cíle útočníka:

- důvod odposlechu
- zjištění přenosové trasy
- fyzický přístup k médiu
- technologické a odborné znalosti
- dostatečné materiálové zázemí
- dostatečná výpočetní kapacita
- dostatečný čas

Cíle napadeného:

- snížení významu odposlechu
  - šifrované přenosy
  - pravidelné změny algoritmu
  - pravidelné změny klíčů
  - transakční režim přenosu s možností volby trasy (vícecestné spojení)
- detekce pokusu o odposlech
  - zařízení s možností detekce přerušení
  - zařízení s možností detekce jevů, které vznikají při odposlechu
  - včasné upozornění a náprava

6.3 Riziko modifikace přenášených informací

Hrozba modifikace přenášených dat má nejnižší úroveň. Na rozdíl od předchozích útoků je zde nutný nejenom přístup k sofistikovanému zařízení a výpočetní technice, ale i podrobná znalost prostředí a dostatek času. Pro finanční náročnosti tohoto útoku je nutné počítat s investicí v řádu miliónů až stovek miliónů korun. Také tato metoda útoku musí přinést útočníkovi zisk, který je srovnatelný nebo vyšší než investovaná částka. Zde hrají roli pouze ekonomické nebo politické zájmy.

Detekce tohoto útoku leží na úrovni aplikační vrstvy, konkrétně je nutné zajistit nezávislou kontrolu provedených transakcí, jejich verifikaci a další kontroly včetně častých změn kódů. Šance detekovat tento útok je i na nižší úrovni, porovnáváním přenosových charakteristik s historií a kontrola tras.

Obranou proti této hrozbě je při dostatečné citlivosti dat (citlivá nebo cenná = zpeněžitelná data) použít šifrovací zařízení, pravidelná výměna klíčů, náhodné změny komunikačních

tras, případně nasazení kvantové kryptografie. Cena postupů a zařízení je sice značně vysoká, ale tak je možné (podle dostupných informací) alespoň částečně eliminovat uvedenou hrozbu.

Cíle útočníka:
- důvod modifikace
- zjištění přenosové trasy
- fyzický přístup k médiu
- technologické a odborné znalosti
- dostatečné materiálové zázemí
- dostatečná výpočetní kapacita
- dostatečný čas

Cíle napadeného:
- snížení významu odposlechu a modifikace
  - pravidelné změny algoritmu
  - pravidelné změny klíčů
  - transakční režim přenosu s možností volby trasy (vícecestné spojení)
  - verifikace transakcí
- detekce pokusu o odposlech a modifikaci
  - zařízení s možností detekce přerušení
  - zařízení s možností detekce jevů, které vznikají při odposlechu
  - porovnávání přenesených transakcí
  - včasné upozornění a náprava

7 ZDROJE

Pro tento materiál byly použity informace z následujících zdrojů:

1) Richard Feynman: Feynmanovy přednášky z fyziky s řešenými příklady
   a. ISBN 80-7200-405-0
   b. ISBN 80-7200-420-4
   c. ISBN 80-7200-421-2
   d. ISBN 978-80-253-0391-7

2) Tréninkové materiály: Fibre Channel Technology

3) http://eprint.iacr.org/

4) http://www.google.com

5) http://www.wikipedia.org

6) http://xxx.arxiv.org/

E. Mikulášská kryptobesídka 2007 - Program

Vašek Matyáš, FI MU Brno
http://mkb.buslab.org/

6. prosince 2007 (čtvrtek)

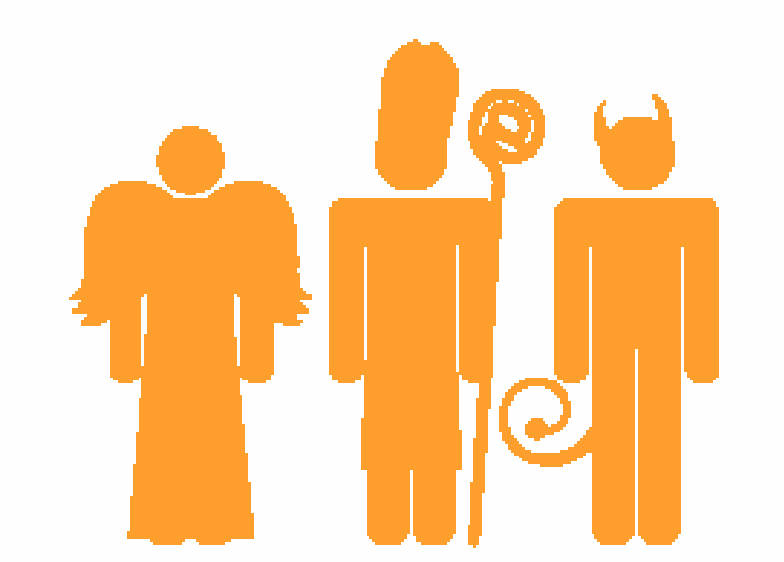
8:45 –	*Registrace*
9:30 – 9:40	*Zahájení workshopu*
9:40 – 10:40	*Zvaný příspěvek* Willi Meier – Design and Analysis of eSTREAM candidates
10:40 – 11:40	*Zvaný příspěvek* Claudia Diaz – Observable Steganographic File Systems
11:40 – 12:30	KEYMAKER, vyhlášení výsledků – sponzor Grisoft
12:30 – 13:30	*Oběd*
13:30 – 14:30	*Zvaný příspěvek* Zdeněk Říha – Cryptography and electronic passports
14:30 – 15:00	Markus Dunte – On the Way to Secure Delivery of Scaleable Coded Media
15:00 – 15:30	*Přestávka na kávu*
15:30 – 16:30	*Zvaný příspěvek* Vlastimil Klíma – Speciální blokové šifry a speciální hašovací funkce
16:30 – 16:50	*Krátká prezentace* Petr Švenda – Authenticated Key Exchange with Group Support for Wireless Sensor Networks
16:50 – 17:20	Peter Kosinar, Richard Ostertág – Dávkové overovanie podpisov v schéme postavenej na RSA
17:20 – 17:50	*Rump session*
18:00 –	*Večeře*

Následuje série neformálních diskusí v prostorách centra vyhrazených pouze pro účastníky kryptobesídky.

7. prosince 2007 (pátek)

9:09 – 9:15	*Zahájení druhého dne workshopu*
9:15 – 10:15	*Zvaný příspěvek* Pavel Vondruška – Doba nomenklátorů
10:15 – 10:45	*Přestávka na kávu*
10:45 – 11:15	Pavol Zajac – How to solve XTDR-DL using NFS
11:15 – 11:35	*Krátká prezentace* Jan Krhovják – The Sources of Randomness in Mobile Devices
11:44 –	*Mikuláš – přichází od RSA*

Závěr workshopu



Mikulášská kryptobesídka 2007 - http://mkb.buslab.org/

Partnery akce jsou: Microsoft & Trusted Network Solutions
Partner tomboly: RSA - The Security Division of EMC
Partner KEYMAKER: GRISOFT
Mediální partneři: Data Security Management a Crypto-World

F. Konference EOIF GigaCon

Anna Uścińska anna.uscinska@swmedia.cz

Konference EOIF Elektronický oběh informací ve firmě
Kdy: dne 12.prosince 2007
Kde: hotel Diplomat, Praha

Podrobnosti na stránce www.eoif.swmedia.cz

Konference **Elektronický oběh informací ve firmě** se věnuje nejnovějším technologiím pro elektronické zpracování, ukladání a sdílení informací ve firmě.
Součástí konference bude mimo odborných přednášek, diskuzí a konzultací i prezentace produktů a řešení.

Inaugurační přednášku bude mít **Edvard Kožušník,** který je jedním ze zakladatelů think-tanku eStat.cz - Efektivní stát, občanské sdružení Michala Tošovského.

Z dalších zajímavých témat si dovolím upozornit na přednášku s aktuálním (dosud trochu opomíjeným) tématem **Elektronická archivace dat se zachováním původu** (Z. Loebl a P. Vondruška).

Témata přednášek:

- OCR/OMR systémy
- faxové systémy
- inter/intra/extranet
- mobilní řešení
- správa oběhu dokumentů
- systémy archivace dokumentů
- hromadný výtisk
- PKI – elektronický dokument
- workflow
- CRM
- systémy týmové spolupráce

Mediální partneři: Ben – technická literatura, Ccmag, CryptoWorld, E-mag – technologický, Hakin9, It Point, Lex – a Wolters Klower business, Linux+, Press Forum

Mezi účastníky budou **vylosovány atraktivní dárky** od Ben – technická literatura, DS Software, Hakin9 a Linux+!

Neváhejte, přihlášte se už dnes! Počet účastníků je omezen!

Kontakt:
Weronika Buszko weronika.buszko@swmedia.cz
tel.+420 246 019 138
fax.+420 227 203 610
Anna Uścińska anna.uscinska@swmedia.cz

G. O čem jsme psali v listopadu 2000 – 2006

Crypto-World 11/1999

Crypto-World 11/2000

Crypto-World 11/2001

Crypto-World 11/2002

Crypto-World 11/2003

Crypto-World 11/2004

Příloha : Crypto-World 11/2004 – speciál (24 stran)
(V.Klíma : Nedůvěřujte kryptologům, ke stažení na adrese :
http://crypto-world.info/index2.php?vyber=casop6)

Crypto-World 11/2005

Crypto-World 11/2006

H. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/