Bezpečnost sítí 5G kódováním fyzické vrstvy (PLS)

Tomáš Knot, Karel Vlček
Ústav počítačových a komunikačních systémů
FAI UTB ve Zlíně, Nad stráněmi 4511
760 05 Zlín, Czech Republic
vlcek@fai.utb.cz

Dokonalá bezpečnost (Shannon)

- Komunikace s dokonalou bezpečností (**perfect security**) v teoretickém smyslu [1] definoval Shannon ve své studii z roku 1949
- Předpokládejme, že k-bitová zpráva M má být bezpečně odeslána od Alice k Bobovi **veřejně přístupným přenosovým kanálem**
- **Dokonalého zajištění** je dosaženo zakódováním zprávy M do přenášeného tvaru, do tvaru X, tak, aby platil relační vztah vyjadřující, že **vzájemná informace**: $I(M, X) = 0$

Realizace dokonalé bezpečnosti

- Podmínka $I(M,X)=0$ je splněna tím, že **Alice a Bob musejí nezbytně sdílet *k* bitů klíče**, pro dosažení dokonalé bezpečnosti při přenosu – tedy toho, **aby zpráva byla pro neoprávněného příjemce nedostupná**
- Tato podmínka je v sítích 5G splnitelná jen sporadicky, vzhledem k heterogenní struktuře sítí, u kterých se předpokládá, že budou uživateli poskytovat **mobilní připojení**; **přenosovým kanálem je zde volný prostor**

Šifrovací klíč pro 5G? – problém

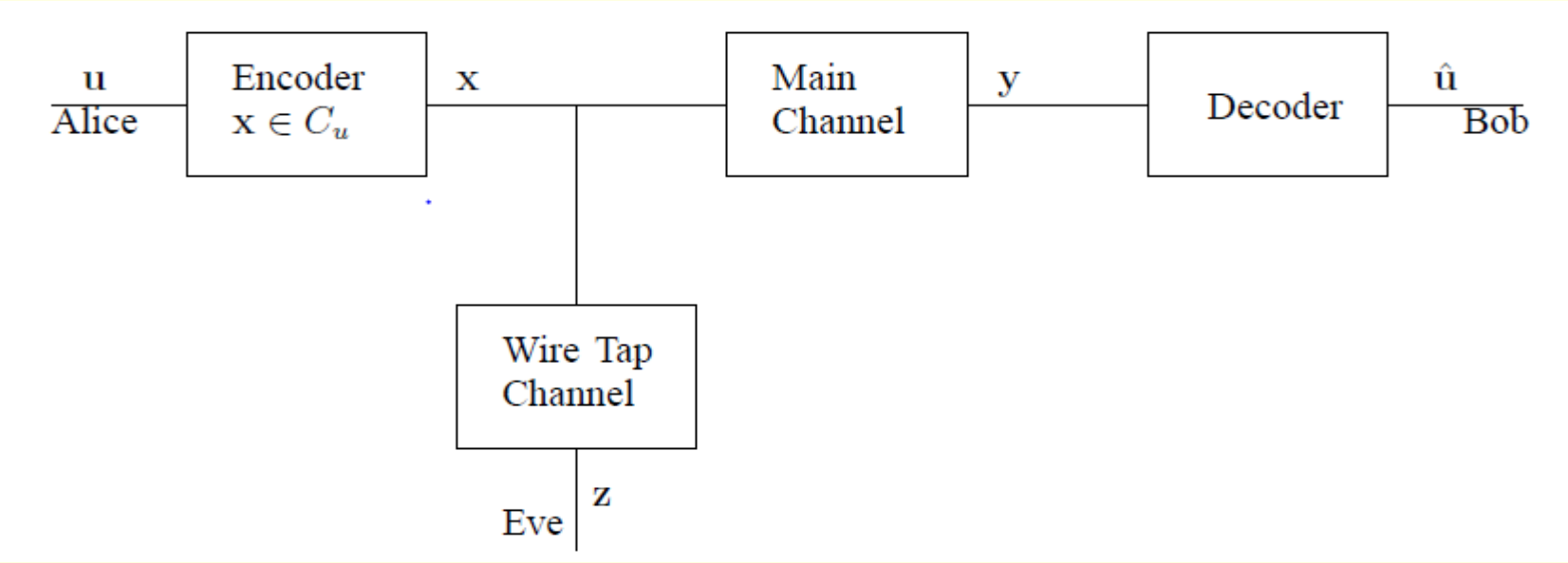
- Z předcházející definice Shannon došel k závěru, že **Alice a Bob by měli nezbytně sdílet k bitů klíče**, aby bylo dosaženo dokonalé bezpečnosti při přenosu zprávy
- **Alternativní představu** o bezpečnosti přenosu zprávy s utajením definuje Wyner [2], který zavádí pojem **odposlechový kanál C2**; pak v původním spojení Alice a Boba je **kanál C1 nazván hlavním kanálem**;
- Důležité je, že C1 a C2 jsou dva různé kanály

Wynerův zdokonalený model

- Wyner zavádí v práci datované již r. 1975 [2] alternativní představu o bezpečnosti přenosu zprávy s utajením tím, že zavádí definici pojmu **odposlechový kanál**
- V původním spojení Alice a Boba je kanál **C1** nazván **hlavním kanálem**
- Důležitou změnou, ve srovnání s modelem zavedeným Shannonem, je to, že zpráva určená Alici je odposlouchávána kanálem **C2**, který je nazvaný **odposlechový kanál**

Wynerův model odposlechu

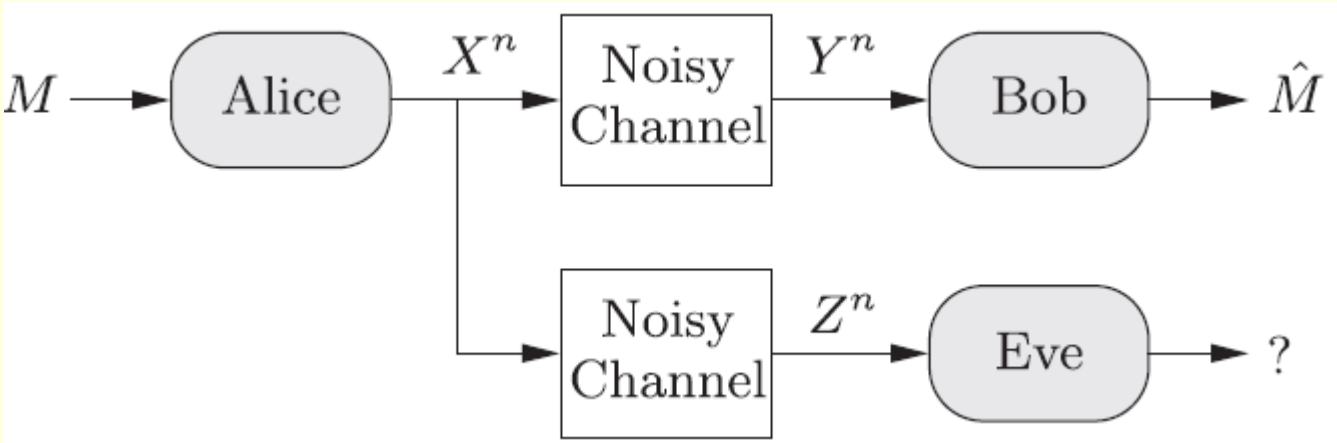
- Je-li odposlech popisován modelem kanálu je podle schématu **Wynerova modelu**, viz obr.



- V [5] je schéma analyzováno následovně:

Wynerův kanál pro odposlech

- **Wynerův model kanálu pro odposlech** popisuje hlavní kanál (main) a odposlechový kanál (wiretap) rozdílnými vztahy



- Popis umožňuje použít vhodný postup při řešení tak, aby byl splněn požadavek utajení

Kódování pro spolehlivost i pro bezpečnost je identické, ale …

- Kódování pro spolehlivost i pro bezpečnost je identické, **liší se** ale **v tom, jak je využíváno**
- **Redundance** ve zprávě je využitelná pro **spolehlivost přenosu (reliability)** při splnění

$$\Pr\{U \neq \hat{U}\} \to 0$$

- Tatáž **redundance** ve zprávě využitelná **pro utajení (secrecy)**, tento účel využití je stanoven podmínkou pro vzájemnou informaci ve vztahu pro odposlechový kanál:

$$I(U;Z)/n \to 0$$

Využití zakódování pro utajení

- Ve Wynerově modelu se předpokládá, že C1 a C2 jsou diskrétní kanály (kanály s konečnou abecedou symbolů) bez paměti DMCs (Discrete Memoryless Channels)
- Předpokládejme, že Alice a Bob posílají zprávu s k-bity **pomocí hlavního kanálu C1**
- Alice zakóduje zprávu M do n-bitového slova (posloupnosti) X, Bob, který je legitimním příjemcem zprávy i slídilka Eve tedy přijmou zprávu, ale **dvěma různými kanály C1 a C2**

Technika kódování fyzické vrstvy

- **Kódování fyzické vrstvy** je změna formátu, kterým lze měnit tvar zprávy, tím je vytvářena, a chráněna přenášená informace ve zprávě
- Zdroj zprávy je charakterizován „**informační vydatností**“, tedy veličinou zvanou **entropie**
- Množství přenášené informace je možné dosáhnout zvýšením rychlosti přenosu
- Tím se ale blížíme ke hranici nazývané **kapacita kanálu**, překročení kapacity kanálu se projeví vyšší chybovostí zprávy po přenosu

Utajení zajišťuje fyzická vrstva

- Základy bezpečnosti fyzické vrstvy jsou dány i **způsobem použité modulace signálů**
- **Základní vlastnosti** jsou dány i způsobem modulace (např. **CDMA**, **OFDM**, **MIMO**)
- Tyto různorodé vlastnosti je možné porovnávat veličinou s názvem **entropie zdroje zpráv**
- Kvalita komunikačního systému je hodnocena podle **spolehlivosti přenosu zpráv**, **ale i jeho odolnosti vůči odposlechu – kapacitou pro utajení** C_s (Secrecy Capacity)

Zabezpečení i spolehlivost

- **Zakódování**, zprávy od Alice má nyní dva cíle: prvním cílem může být **zabezpečení,** to se dá formulovat podmínkou o vzájemné informaci vztahem $(1/n)\,I(M;Z) \to 0$ při $n \to \infty$, ale také má zakódování i druhý cíl, tím je **spolehlivost**
- Obě úlohy **redundance** informace ve zprávě – malá pravděpodobnost **výskytu chyby** označovaným **FEC** (**F**orward **E**rror **C**orrection)
- **Zabezpečení bez použití šifrovacího klíče**, ale vyžaduje, aby pro **C1** a **C2** platily podmínky:

Podmínky pro kapacity C1 a C2

- **Kapacita pro utajení** C_s je funkcí kapacity kanálů, **hlavního C1** a **odposlechového C2**
- Wyner [2] ukázal, že jestliže **C2** je menší, než **C1**, (**C2** je kapacita **C1** zřetězená s dalším DMC) pak **kapacita pro utajení** C_s je kladná
- Csiszár a Körner [3] prokázali, že **kapacita pro utajení je kladná i v případech, kdy C1 je méně „zašuměná“ než C2**, ale **výpočet kapacity pro utajení** C_s pro **obecný případ je neřešitelný**, máme-li C_s vyčíslit **z C1 a C2**

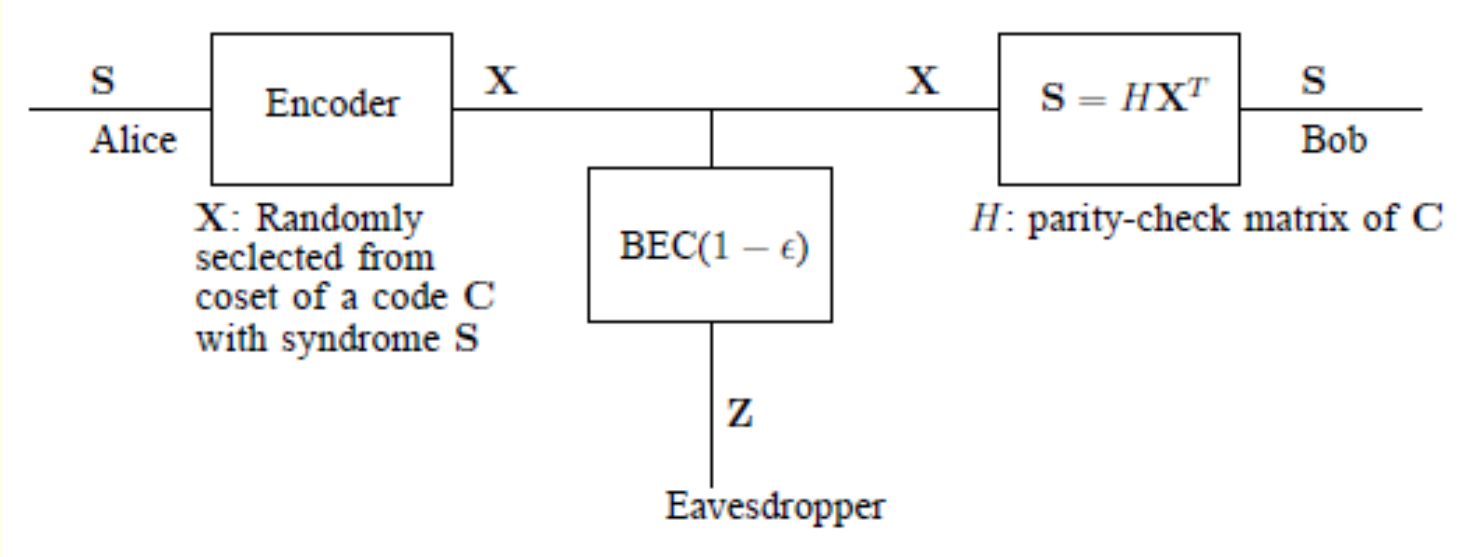
Podmínka vzájemné informace

- Pro utajení zprávy posílané ze zdroje A (Alice) do místa příjmu B (Bob), **je použito náhodně zvolených slov**, pro tuto techniku je nutné mít k dispozici (nejlépe lineární) kód – **LDPC kód**
- Za těchto podmínek a při splnění požadavku limitní hodnoty vzájemné informace bude poslán do místa příjmu **vektor syndromu**, který reprezentuje daný symbol zprávy, tím je dosaženo **splnění požadované podmínky**:

$$I(U;Z)/n \to 0$$

Utajení náhodným výběrem slov

- **Syndrom symbolu** zprávy **je** tedy skutečným náhodným slovem, které může být použito při přenosu a přitom je splněna podmínka utajení
- **Metoda je** znázorněna **na obrázku (**viz [5])



Zjednodušující podmínky pro C_s

- Největšího pokroku dosáhl M. van Dijk [4], když navrhl zjednodušující předpoklad pro výpočet tím, že definoval a použil konvexní funkci $I(X,Y)-I(X,Z)$ na stejném rozdělení
- Navíc, jak uvádí [4], je tato funkce definována na stejném rozdělení $P_X(x)$, bude **kapacita pro utajení** vyčíslitelná jako hodnota kapacity hlavního kanálu zmenšená o kapacitu kanálu odposlechového, pomocí relačního zápisu:

$$C_s = 1 - Capacity\left(BEC\left(1-\varepsilon\right)\right) = 1-\left(1-\left(1-\varepsilon\right)\right) = 1-\varepsilon$$

Ochrana před odposlechem kódováním fyzické vrstvy (PLS)

- Metody kódování odposlechového kanálu pro uspořádání dle předcházející relace je založeno na popisu náhodných symbolů
- Přenáší-li *k*-bitovou zprávu, představuje praktickou cestu, k vyčíslení podle vztahu pomocí symbolického zápisu $C_s = 1 - \varepsilon$
- Tento zjednodušený vztah přináší nejčastěji citovaná výzkumná zpráva [5].
- Zajímavý přístup pro přímé zjištění, kapacity pro utajení, použili autoři [6].

Kapacita pro utajení C_s (Secrecy Capacity) v reálném prostředí

- Reálnému prostředí lépe odpovídá distribuční funkce, **Rayleighovy pravděpodobnostní distribuční funkce** pro **hlavní** (s indexy M) a **odposlechový** kanál (s indexy W):

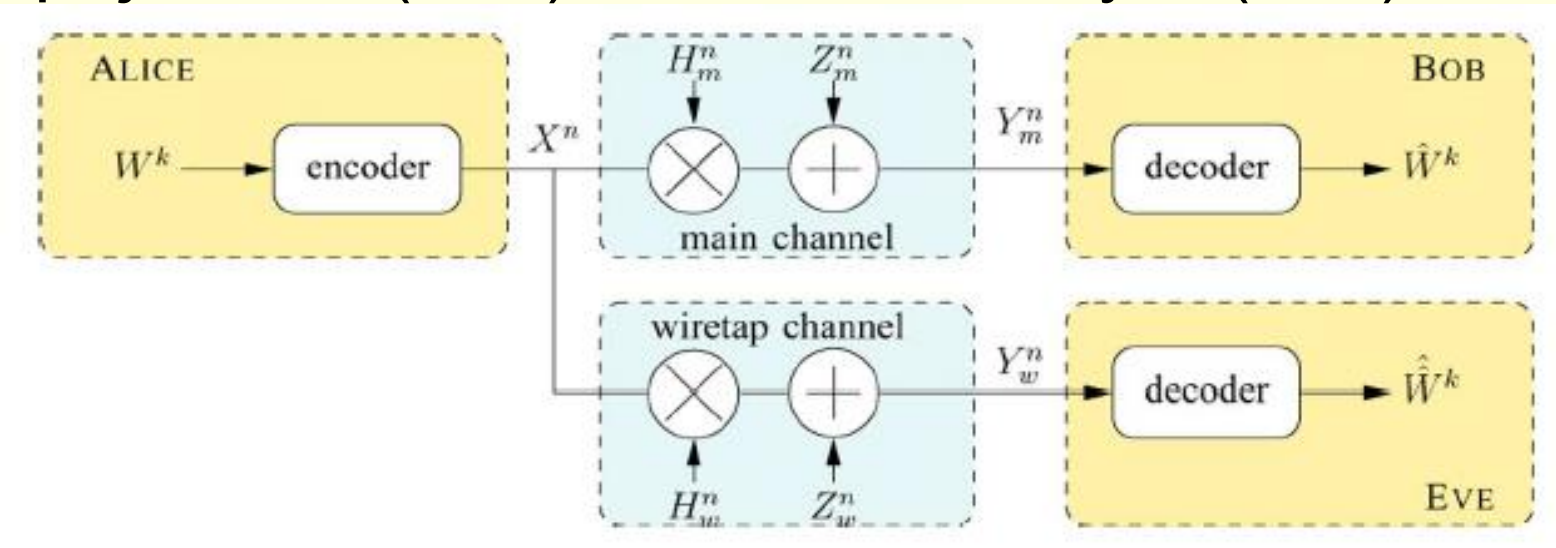
$$C_M = \frac{1}{2}\log\left(1+\frac{P}{N_M}\right) \qquad C_W = \frac{1}{2}\log\left(1+\frac{P}{N_W}\right)$$

- Dosazením do výchozího vztahu je kapacita pro utajení: $C_s = C_M - C_W$, kde

$$C_s = \begin{cases} \log\left(1+\gamma_M\right) - \log\left(1+\gamma_W\right) & pro \quad \gamma_M > \gamma_W \\ 0 & pro \quad \gamma_M \le \gamma_W \end{cases}$$

Reálné technické řešení PLS [13]

- **Prostředky utajení** legitimní uživatelky A (Alice), která posílá zprávu legitimnímu příjemci B (Bob) a situace slídilky E (Eve)



- v reálném prostředí dle **Rayleighovy funkce**

Vlastnosti zakódování pro PLS

- **Požadavky na vlastnosti kódů** vhodných pro zakódování zprávy pro utajení (secrecy) je charakterizovaná požadavkem na **dosažení maximální hodnoty kapacity kanálu** (kódy, označované ***Capacity-Achieving Codes***)
- Tuto podmínku jsou schopny splnit **iterativně dekódovatelné kódy** (nejčastěji **LDPC kódy**, **Lattice kódy** nebo **Polární kódy**, ale i další)
- Popis vlastností těchto kódů je, s ohledem na proveditelnost dekodérů, analyzován v [8] a [9]

PLS použitím dalších vhodných redundantních kódů

- Kromě ochrany fyzické vrstvy použitím LDPC kódů se náš příspěvek nutně musí zmínit i o řešení **pomocí** jiných **redundantních kódů blízkých kódům náhodným**, které mají předpoklad, že budou vyhovovat podmínce:

$$\frac{E_b}{N_0} > \frac{2^{\frac{R}{B}} - 1}{\frac{R}{B}} = \frac{2^{\eta} - 1}{\eta}$$

- Příkladem je použití “Lattice Codes”, které přinášejí povzbudivé výsledky.

Lattice Codes (1)

- Kódy definované nad svazovými strukturami, (**Lattice kódy**), se vyznačují a jsou vytvářeny **pseudonáhodnými algoritmy redundance** kódových posloupností či kódových slov.
- Tato jejich vlastnost je zárukou **velké** hodnoty **entropie zdroje kódových slov**, kterou je **pseudonáhodná charakteristika** vytváření redundantních částí zpráv a tedy relativně obtížně dekódovatelná; struktura svazové definiční veličiny, naopak tuto vazbu zvyšuje.

Lattice Codes (2)

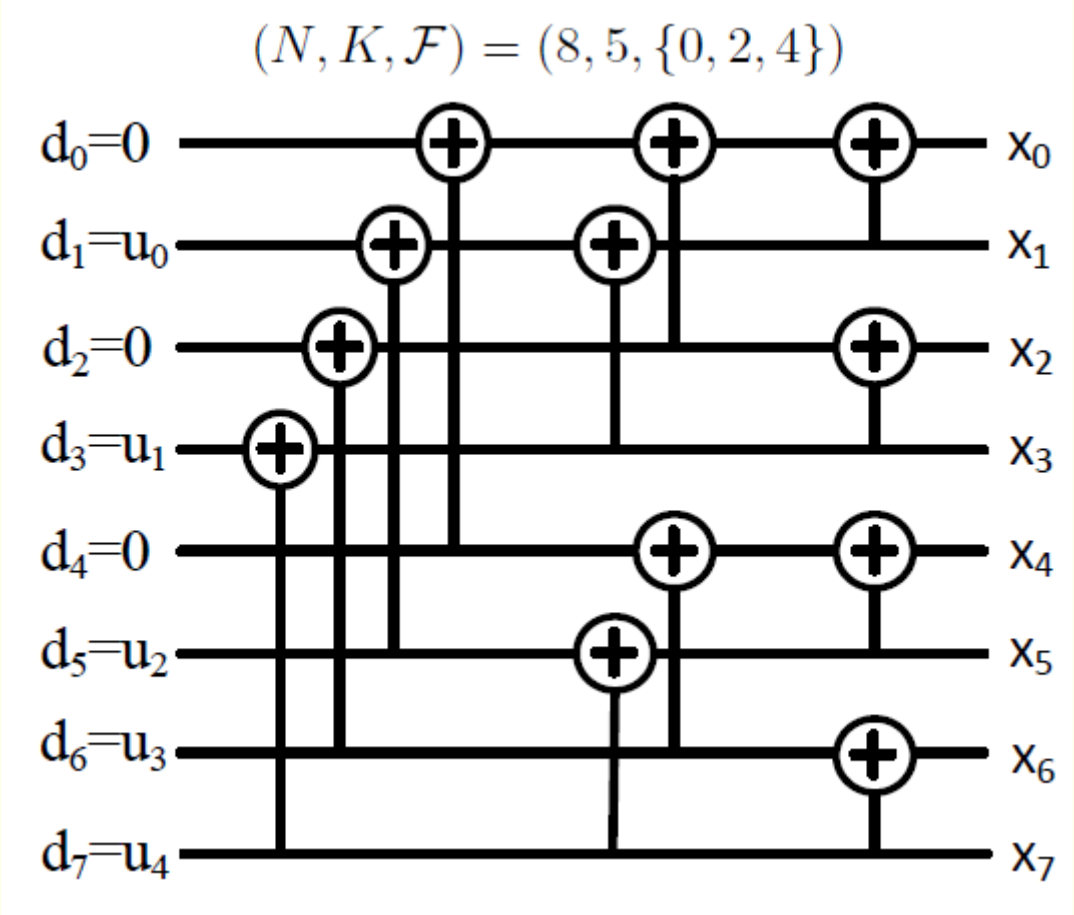
- Obecný popis **Lattice kódů** [7] zahrnuje značnou variabilitu závislostí, principiální vlastností je **svaz**, který je definovaný jako soubor bodů v uvažovaném *n*-rozměrném prostoru, ale který zahrnuje všechny **lineární kombinace s celočíselnými koeficienty** tvořícími bázi z *n* lineárně nezávislých vektorů
- Tato vlastnost dovoluje, aby byla definována generující matice G, tato **matice obsahuje bázové** tj. lineárně nezávislé vektory.

Lattice Codes (3)

- Svaz je tedy popsán následující definiční relací: $\Lambda = \{\lambda = Gx; x \in Z^n\}$, která zaručuje **potřebný relační vztah „navíc“**, ten je potom využitý pro **iterativní** algoritmus **dekódování**.
- Při výzkumu tzv. “**Weak Secrecy**” (WS), se při “Lattice Codes”, s odposlechovým kanálem s AGWN charakteristikou přenosu a jsou proto v současné době intenzívně zkoumány i v souvislosti s **PUFs** (**P**hysical **U**nclonable **F**unctions) [11].

Polární kódy (1)

- Principiální transformace pro vytvoření **polarizace kanálu**, který je postupem pro vytvoření polárních kódů



Polární kódy (2)

- Polární kódy prokazatelně dosahují rychlosti přenosu informace až do hodnoty kapacity kanálu pro **binární symetrický kanál bez paměti s polynomiální závislostí a mají střední složitost algoritmů pro zakódování a dekódování** popsanou výrazem $O\left(n \log n\right)$.
- Roku 2016 vyhlásila firma Huawei, že dosáhla hranice 27 Gbitů/s pro přenos dat ze serveru k zákazníkovi a tím vyhovuje požadavkům **5G mobilních sítí** s použitím Polárních kódů [6].

Kódování fyzické vrstvy – souhrn

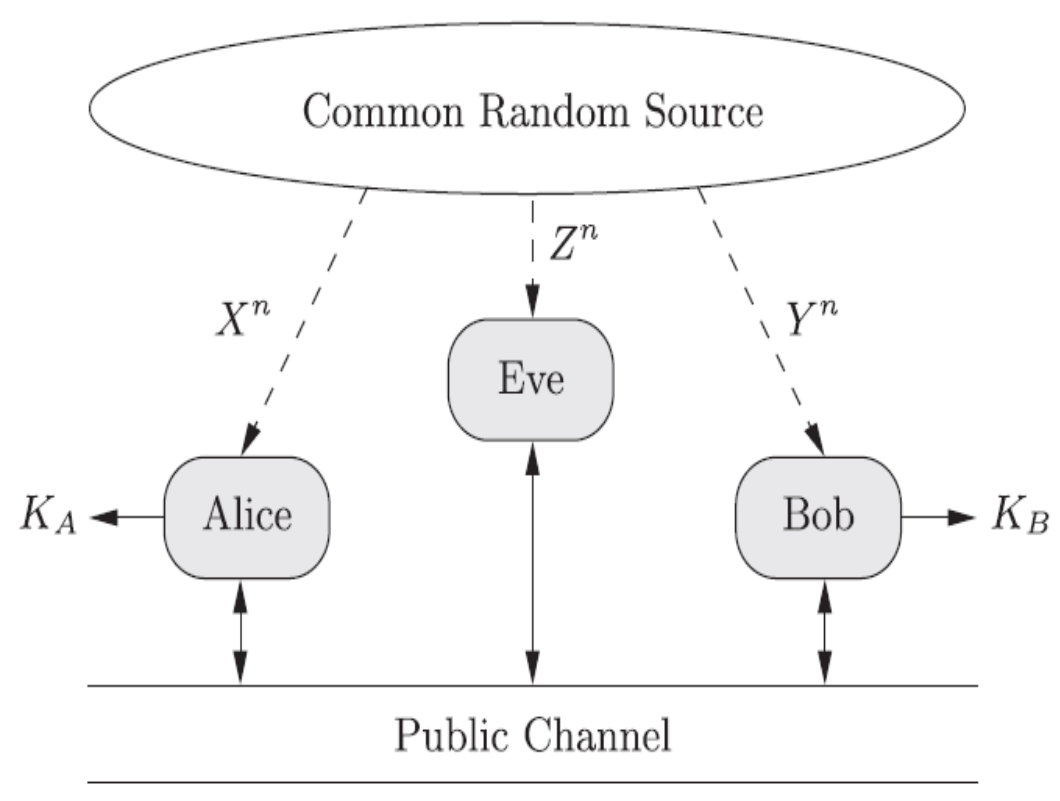
- Aaron D. Wyner ve studii [12] z roku 1975 modeloval šumový odposlechový kanál, který je složen z legitimního vysílače zprávy (Alice), legitimního příjemce zprávy (Bob) a příjemce zprávy neoprávněného – slídila (Eve)

$$C_s = \left[\log\left(1 + SNR_B\right) - \log\left(1 + SNR_E\right) \right]^+$$

- A.D.Wyner formuloval podmínky bezpečného přenosu, tj. přenosu se zdrojem s teoretickou bezpečností, kdy **pravděpodobnost chyby** v legitimním přijímači **bude libovolně malá**.

Bezpečnost (Secrecy) sítí 5G kódováním fyzické vrstvy (PLS)

- **Presentace** je zpracována pro studii [14], **uvádí** přehled a praktické **poznatky o** implementaci **šifrování bez použití klíče**.



Literatura (1)

[1] Shannon, C., E.: Communication theory of secrecy systems, Bell Syst. Tech J., vol. 28, pp. 656-715, Oct. 1949.

[2] Wyner, A.: The Wire-Tap Channel, Bell Syst. Tech J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] Csiszár, I., Körner, J.: Broadcast channels with confidential messages, IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 339 – 348, May 1978.

[4] M. van Dijk: On a special class of broadcast channels with confidential messages, IEEE Trans. Inf. Theory, vol. 43, no 2, pp. 712 – 714, Mar. 1997.

[5] Thangaraj, A., Dihidar, S., Calderbank, McLaughin, S., W., Merolla, J.-M.: Applications of LDPC codes to the wiretap channel, IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933 – 2945, Aug. 2007.

[6] “Huawei achieves 27Gbps 5G speeds www.telecomasia.net/with Polar Code” (http://www.telecomasia.net/content/huawei-achieves-27gbps-5g-speeds-polar-code?)

[7] Burr, A.: Lattice Coding and its Applications in Communications, University of York, http://malb.io/discrete-subgroup/slides/2016-05-04-burr.pdf.

[8] Johnson, S., J.: Iterative Error Correction, Cambridge University Press, ISBN 978-0-521-87148-8.

Literatura (2)

[9] Vlček, K.: Rozšíření souboru instrukcí ARM procesoru pro multimediální digitální komunikace, XXVI. konference Radiokomunikace (18. – 20. 10. 2016), ISBN 978-80-905345-9-9, pp. 197 – 210.

[10] Vlček, K.: Optimalizace parametrů algoritmu dekódování LDPC kódu pro empirické modely přístupových sítí 5G, XXVIII. Radiokomunikace ´18, ISBN 978-80-87942-45-1, pp. 235 – 243.

[11] Kai Sun, and al.: Application of … Codes on PUFs …, 978-1-5090-6625-4/17, pp. 867-70, (2017).

[12] Poor, V., Schaefer, R. F.: Wireless Physical Layer Security, (2019), pp. 1-8, www.pnas.org/doi/10..1073/pnas.1618130114.

[13] Bloch, M., Barros, J., Rodrigues, M.R.D., McLauhlin, S.W.: Wireless Information – Theoretic Security, IEEE Transactions on Information Theory, vol. 54, no. 6, June 2008, pp. 2515 – 2534.

[14] Vlček, K., Žalud, V.: Řešení některých bezpečnostních rizik v sítích 5G, (Zabezpečení fyzické vrstvy mobilních sítí 5G pomocí náhodného charakteru redundantních kanálových kódů) XXIX. Radiokomunikace ´19), Pardubice, Česká republika, (15. – 17. 2019).