Q: Co je to IoT?
A: Na Wikipedii je pěkně vysvětlené, co je to IoT. Zároveň je zde motivace naznačena v záložce "Bezpečnost": https://cs.wikipedia.org/wiki/Internet_v%C4%9Bc%C3%AD#Bezpe%C4%8Dnost . Můžeš si to představit tak, že když máš chytrou domácnost, tak nechceš, aby ti nějaký hacker z druhé strany planety, zapínal a vypínal rychlovarnou konvici dle libosti. Může se zdát, že je to trivialita, ale určitě existují i jiné systémy, kde by se takové věci daly zneužít.
Proč do každého přístroje nedáme nějaké nabušené šifrovací zařízení? Je to drahé. Tak tam dámé levnější! Ve stejnou chvíli také nechceš čekat 5 minut, až se ti otevřou chytrá garážová vrata, protože šifrují pomalu, protože mají slabý hardware. Proto volíme kompromis mezi bezpečností a cenou -> lightweight cryptography.

Q: Co jsou operace XOR?
A: XOR je logická operace, kterou lze interpretovat jako sčítání v tělesech charakteristiky 2. Více info najdeš zde: https://cs.wikipedia.org/wiki/Exkluzivn%C3%AD_disjunkce.

Q: Chtěl bych se zeptat co to znamená že je oněch matic málo (sl.8).
A: Málo v tomto případě znamená, že regulárních matic, kde d-XOR-count je ostře menší než s-XOR-count, je méně než regulárních matic, kde d-XOR-count je větší nebo roven s-XOR-countu.

Q: Chybí mi trochu intuitivní vysvětlení, co znamená, že d-XOR-count je menší než s-XOR-count, nebo proč bychom to vlastně chtěli.
A: Zamýšlel jsem se nad tím už dříve, ale nepřšel jsem s žádným pěkným vysvětlením. Zapátrám a dám to do další prezentace.

Q: Proč je zajímavý případ, kdy d-XOR-count < s-XOR-count?
A: Asi hodně záleží na motivaci, na kterou jsem však dosud nenarazil. Mně osobně to zaujalo, protože je to nevyřešený problém a chtěl jsem se na to podívat:)

Q: Dá se Hammingova váha použít i nad jiným tělesem než je F_2, víme o nějakých uplatněních (mimo těleso F_2)?
A: Ano, určitě! Hammingova váha se dá použít i nad jinými tělesy (zatím jsem se setkal jen nad konečnými). Tenhle rok ji hojně používáme na samoopravných kódech, což je v zásadě jen chytře vybraná množina vektorů s nějakými dobrými vlastnostmi. Hodně těchto vlastností se dá odvodit s pomocí počítání nenulových pozic vektorů (Hammingovy váhy).

Q: Jak souvisí měření náročnosti implementace s XOR-metrikami?
A: Super otázka, to jsem měl popsat lépe. Libovolné násobení v konečných tělesech se dá reprezentovat násobením matice a vektoru (z lineární algebry), kde prvky matice i vektoru budou prvky z F_2^n. Tyto prvky se zase dají reprezentovat jako vektory nad F_2 dimenze n. To znamená, že násobení v konečném tělese dokážeme napsat jako násobení matice a vektoru větších dimenzí s hodnotami z F_2. No a když si zkusíš vynásobit dva vektory nad F_2, tak vlastně děláš hodně sčítaní nad Z_2. A to je ten XOR. Je zajímavé zkoumat, kolik XORů uděláš, protože to nějak odpovídá tomu, jak chytře dokážeš násobení naimplementovat. Přiznám se však, že v tomto vysvětlení hodně mávám rukama, a proto do bakalářky určitě dám nějaké přesnější vysvělení. Děkuju za připomínku!