



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



Kryptologie

*Netradiční moderní kryptologie:
Kvantová kryptografie a Teorie chaosu*

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

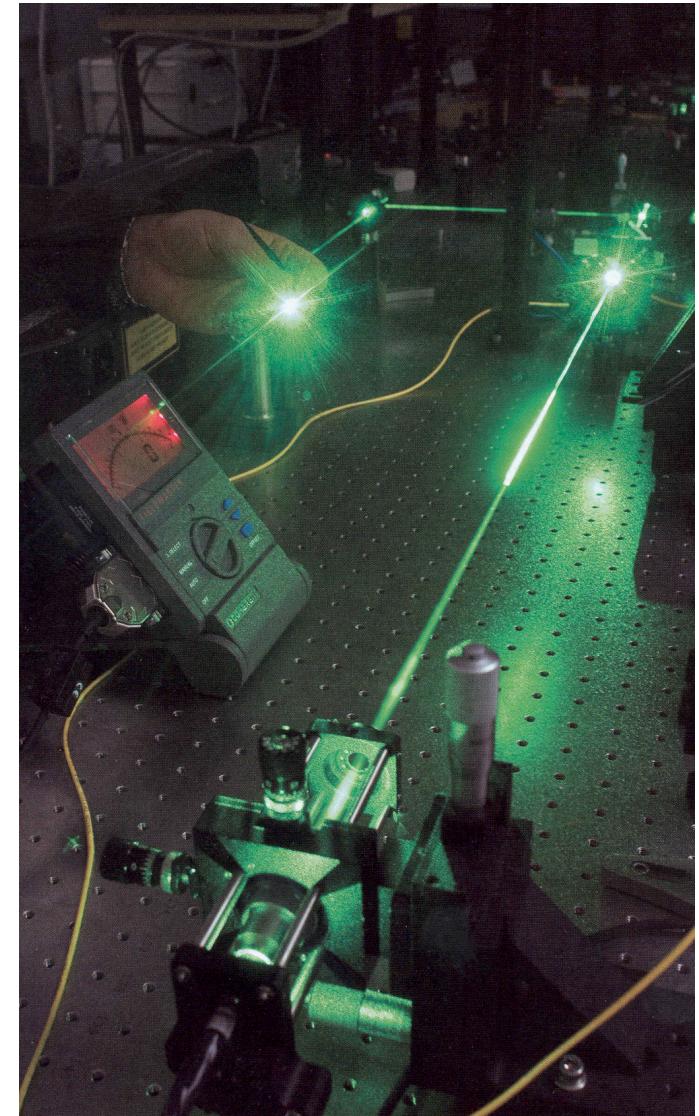
Obsah prezentace

- **Kvantová kryptografie**
- **Kryptografie založená na teorii chaosu**
- **Další netradiční přístupy**
 - **Fraktální geometrie**
 - **Kognitivní kryptografie**

1. Kvantová kryptografie

Kvantová kryptografie: Úvod

- Využití základního principu kvantové fyziky - Heisenbergův princip neurčitosti - proces měření vlastnosti v kvantovém stavu, ovlivňuje systém (jinou vlastnost).
- QKD - Quantum key distribution (systém kvantové distribuce klíče), hlavní komunikační kanál používá standardní šifry jako 3DES, AES



Zdroj obrázku: [1]

Kvantová kryptografie: Úvod

- Vytváří Shared Random bit string (Sdílený náhodný bitový řetězec), jež je využit jako klíč.
- Schopnost detekce přítomnosti “narušitele”
- Klasická veřejná kryptografie spoléhá na výpočetní složitost a neobsahuje detekci útoku či zabezpečení klíče.

Kvantová Kryptografie - Protokoly

- Prepare and measure protocols (BB84 protocol)
 - Využívá základní principy kvantové fyziky
 - Používá polarizaci fotonů
 - Přítomnost “narušitele” může způsobit s 50% pravděpodobností obdržení špatných hodnot.

Kvantová Kryptografie - Protokoly

- Entanglement based protocols (E91 protocol)
 - Založen na “propletení” páru fotonů
 - Používá korelaci spinů fotonů (nahoru / dolů)
 - Přítomnost “narušitele” způsobuje narušení korelace mezi párem fotonů

Kvantová Kryptografie - summarizace

- Jedná se o symetrickou šifru
- Náhodný klíč je vytvořen pomocí kvantového principu, samotná data jsou dále šifrovány volitelnou symetrickou šifrou - AES256, IDEA, CAST, atd...
- Pouze omezený distanční dosah - není možné využít repeaterů, zesilovačů pro generování náhodného klíče pomocí kvantového principu na větší vzdálenost.

Kvantová Kryptografie - summarizace

- Předpokládaný nástupce asymetrické kryptografie - s vynálezem velmi rychlého např. kvantového počítače tato oblast kryptografie zanikne (faktorizece součinu, eliptické křivky budou řešeny v řádech milisekund).
- Síla kvantové kryptografie nicméně leží na síle hlavní symetrické šifry. Kvantová kryptografie pouze řeší zabezpečený přenos symetrického klíče s detekcí narušitele.

Jak funguje Kvantová kryptografie

1. Nejdříve “Alice” odesílá fotony s různou orientací a pořizuje o tom záznam.
2. Pro každý příchozí bit “Bob” náhodně vybere typ filtru, jenž je použit k detekci, a zaznamená si jak použitý filtr, tak získanou bitovou hodnotu.
3. V případě, že by se narušitel “Eva” pokusil(a) sledovat tok fotonů, narazil(a) by na principy kvantové mechaniky. Pokud si vybere nesprávný filtr, dojde k vytvoření chyb změnou polarizace fotonů.

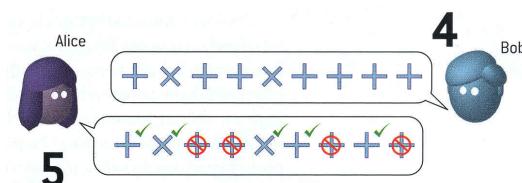
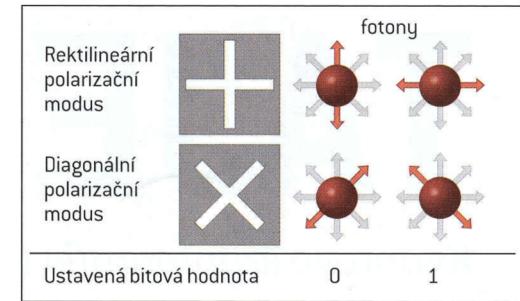
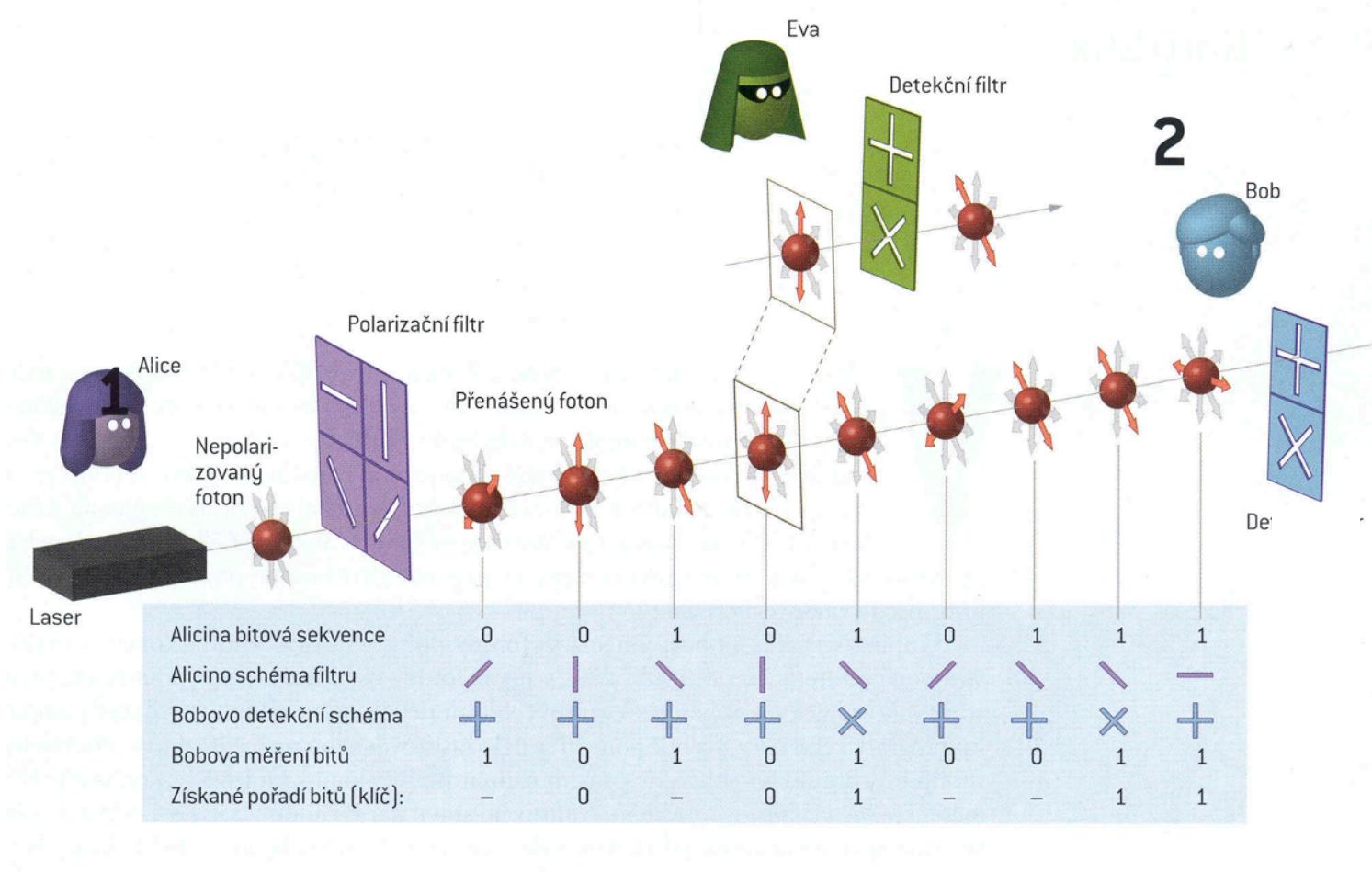
Příklad funkce dle: [1]

Jak funguje Kvantová kryptografie

4. Poté, co všechny fotony dorazily do “cíle”, sdělí Bob Alici jakýmkoliv veřejným kanálem (telefon, sms, email, nezabezpečený přenos po síti) pořadí filtrů (opačné - odzadu) jaké zvolil pro přicházející fotony. Nikoliv ale bitovou hodnotu!!!!
5. Alice sdělí Bobovi, které filtry zvolí správně - správné bitové hodnoty oba znají, dojde tak k vytvoření náhodného symetrického klíče.

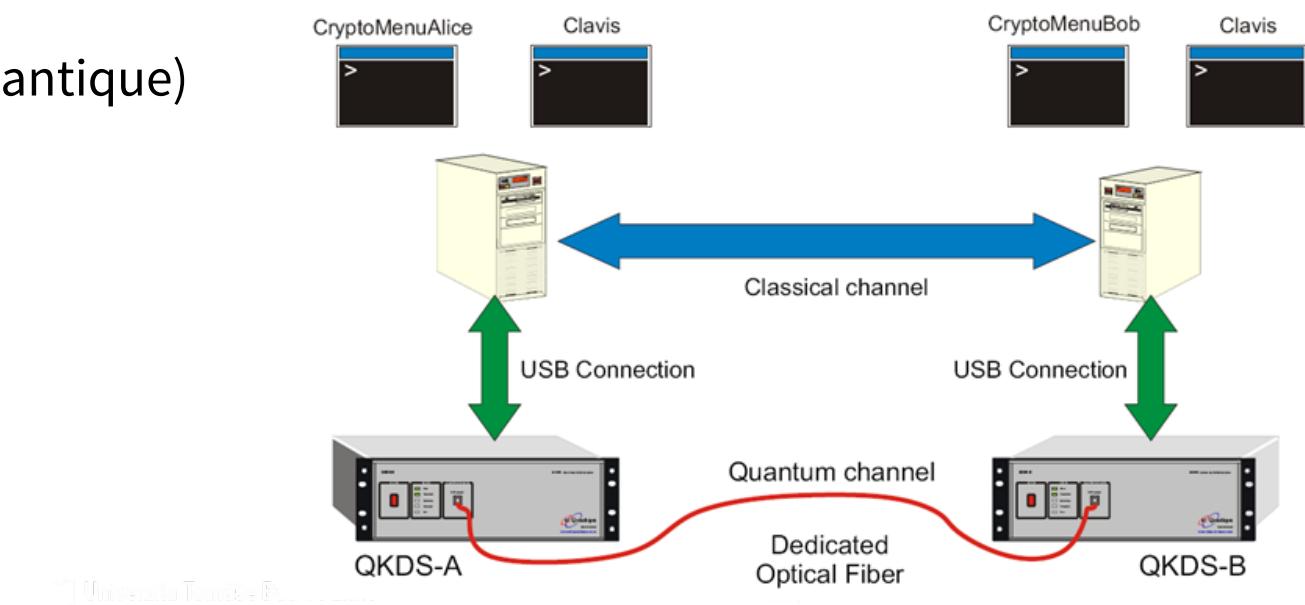
Příklad funkce dle: [1]

Jak funguje Kvantová kryptografie



Praktické aplikace Kvantové kryptografie

- Existuje řada reálných aplikací a systémů (od kvantových generátorů náhodných sekvencí do PCI-e slotů, přes komunikační systémy a serverové systémy:
 - CERBERIS (později firma IDQuantique)
 - CLAVIS2
 - MagiQ
 - ...

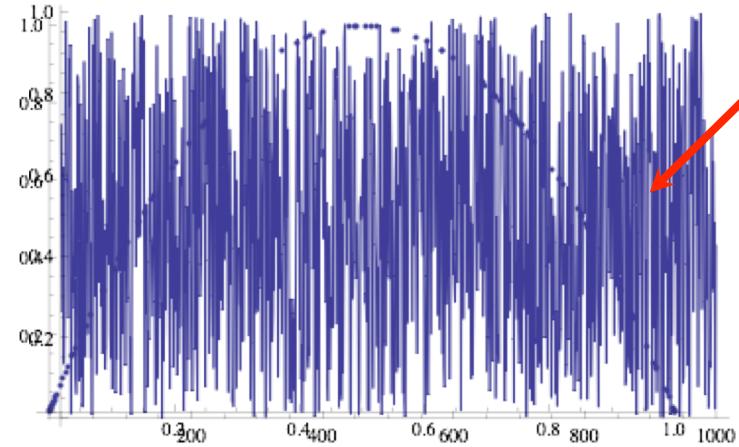


Zdroj obrázku: [2]

13

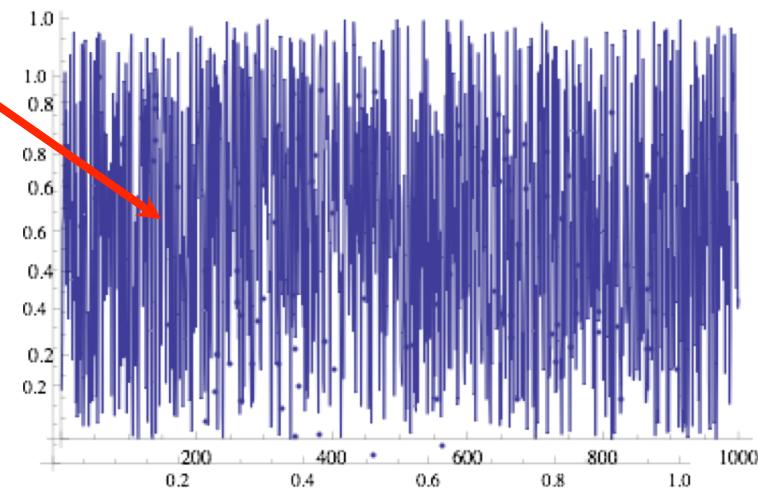
2. Kryptografie založená na teorii chaosu

Chaos vs. Náhoda

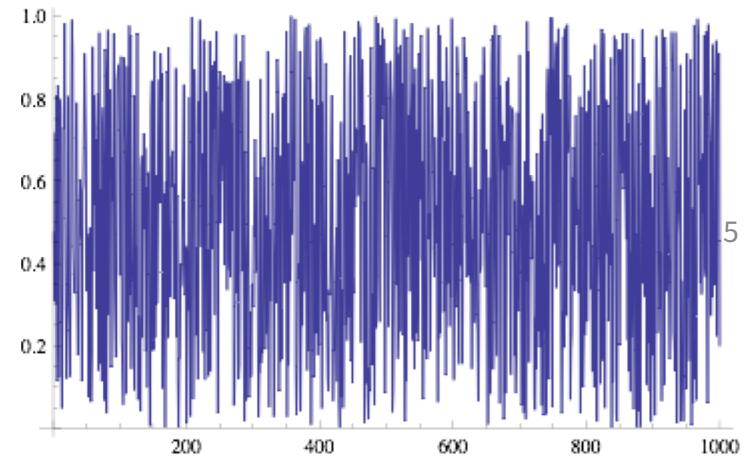
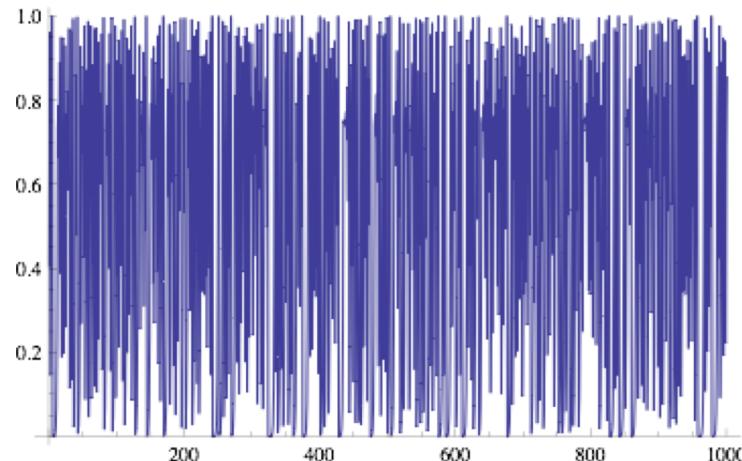


Chaos

$\{x_k, x_{k+1}\}$



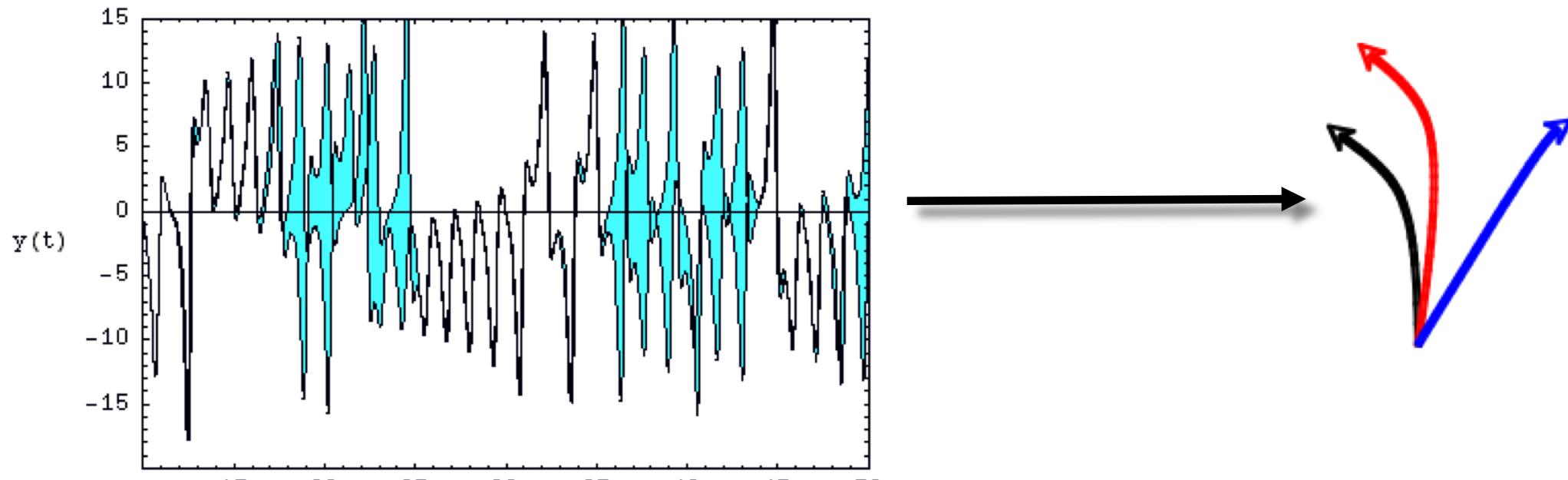
Randomness



Teorie Chaosu - Nový fenomén

- Chaos leží na pomezí mezi stochastismem a determinismem - projevuje se stochasticky, ale je tam přítomna "dynamika na pozadí")
- Základní vlastnosti deterministického chaosu je extrémní citlivost na počáteční podmínky - divergence (rozbíhavost) velmi blízkých trajektorií.
- Tohoto jevu se pak využívá v Kryptologii - precizní nastavení systémů je klíčem k zachování komunikace - tedy že systém "neujede" někam mimo oblast řešení

Teorie Chaosu - Nový fenomén



- Simulace dvou stejných systémů - jeden "nastartován s počátečními podmínkami "0" a druhý s 0.000000000000001

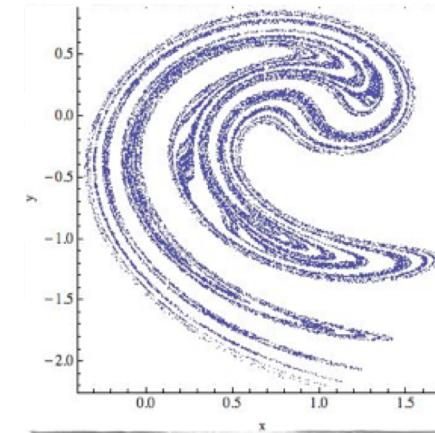
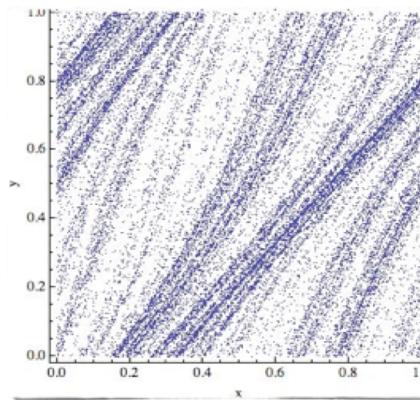
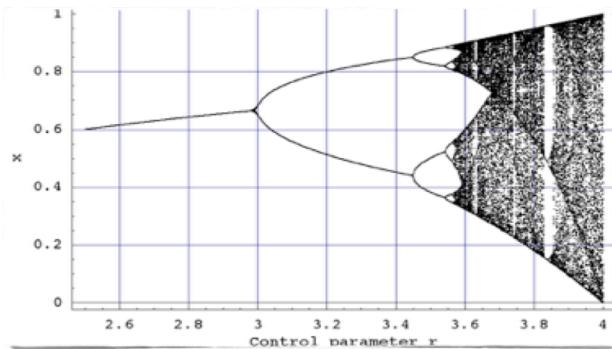
Chaos vs. Náhoda

- Využívá základní principy kvantové fyziky
- Používá polarizaci fotonů
- Přítomnost “narušitele” může způsobit s 50% pravděpodobností obdržení špatných hodnot.

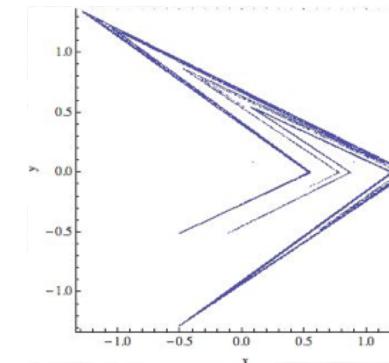
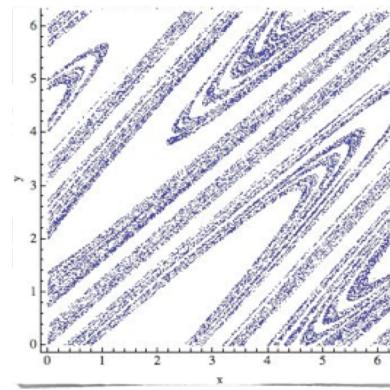
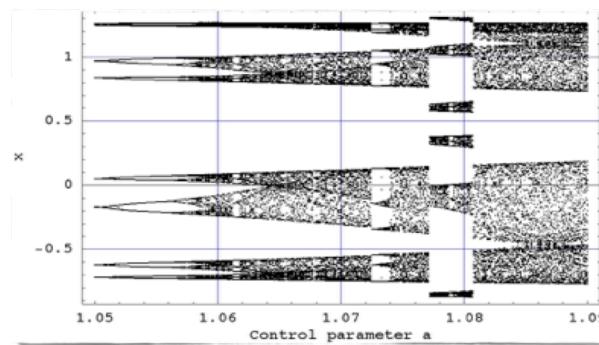
Rozdělení chaotických systémů

- Diskrétní systémy - chaotické mapy (iterace jednoduchých rekurentních vztahů)
- Time-continuos systémy - Podivné Atractory (řešení soustavy diferenciálních rovnic spojitych v čase)
- Časoprostorový Chaos (paralelní spřažení desítek chaotických systémů přes "chaotické vazby) - tedy chaos nejen v čase jak u chaotických map, ale i v prostoru) [3].

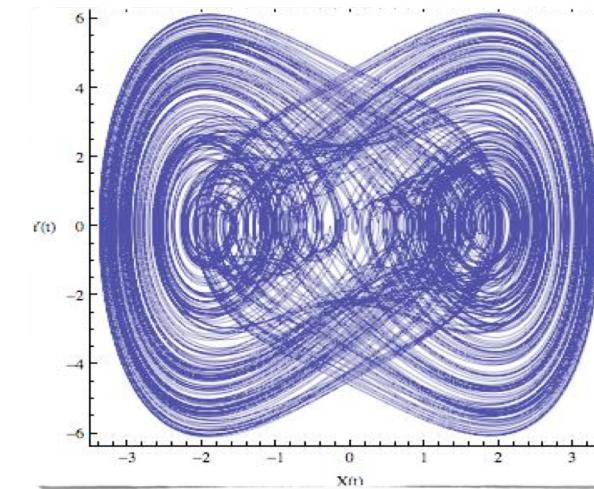
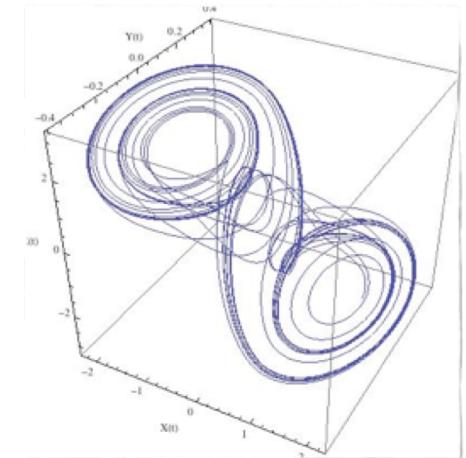
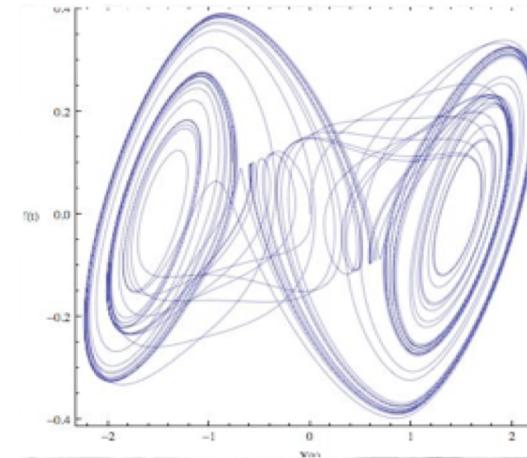
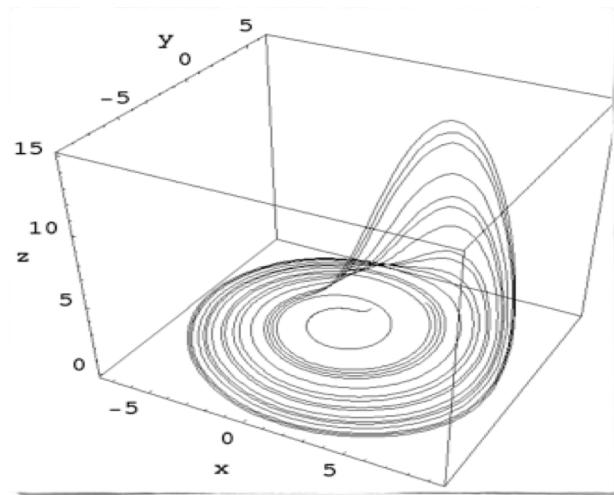
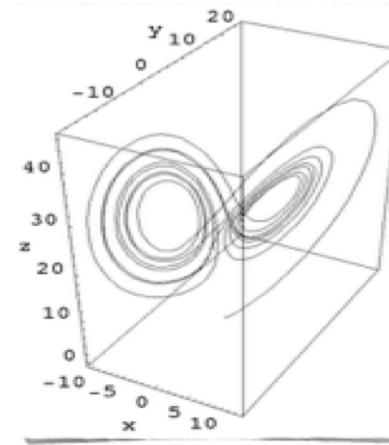
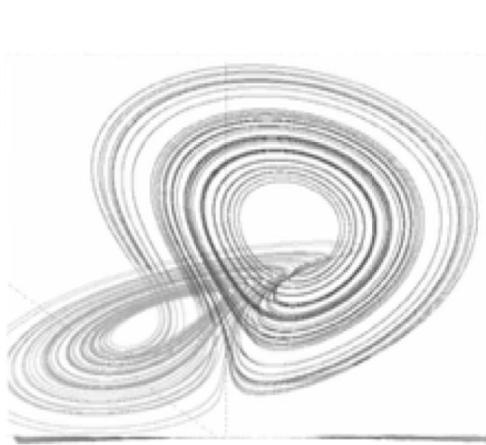
Chaotické Mapy



Ukázka toho, kde všude se systém může chaoticky "vyskytnout" v libovolné iteraci a jaká dynamika jej "řídí"

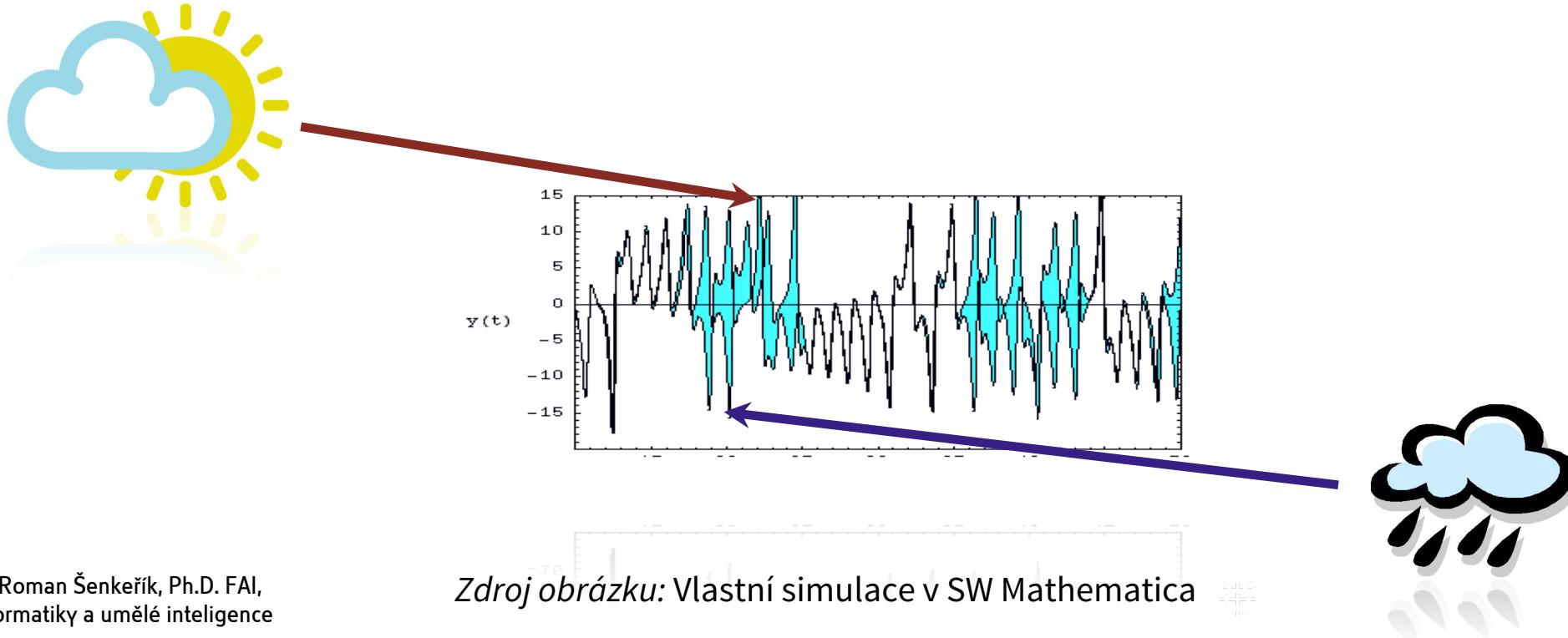


Podivné Atraktory



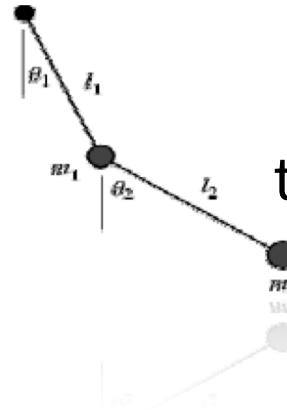
Butterfly Effect - Motýlí efekt

- Nic do činění s motýly
- Objeven Edwardem Lorenzem
 - Jakákoliv malá změna může způsobit extrémní změnu v budoucím chování systému.
Populární forma: Mávnutí motýlích křídel nad Tokiem může způsobit bouři nad New Yorkem.



Chaos ve skutečném světě

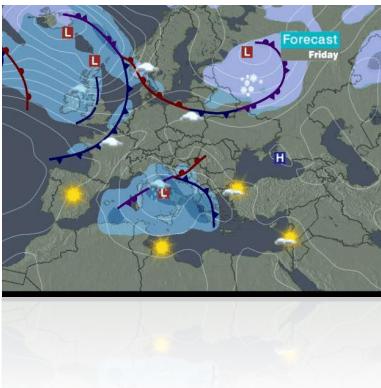
- Mechanické systémy - dvojité kyvadlo



turbulentní proudění



- Počasí



- Burzovní nebo devizový trh

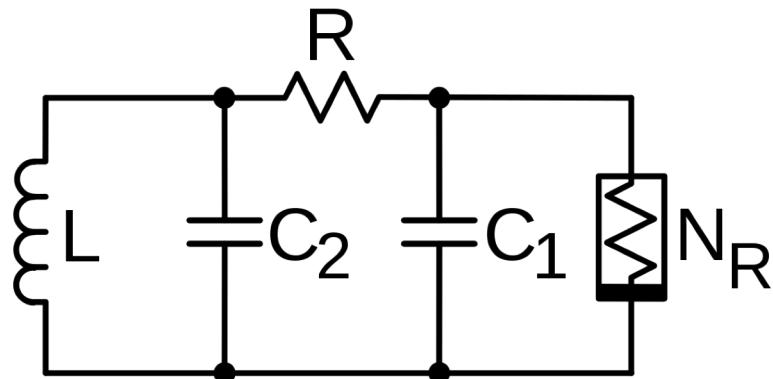
Chaos ve skutečném světě

- Lékařství – EKG



- Komunikace a Kryptografie

- Elektronické obvody (Chua circuit)



Zdroj obrázku: [4]

Použití teorie chaosu pro šifrování

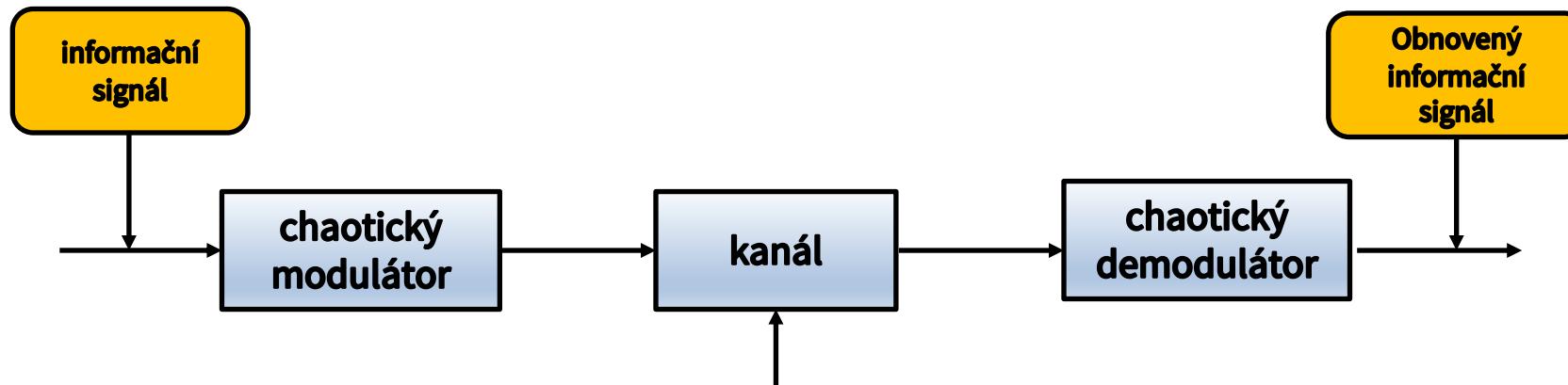
- V principu založeno na Synchronizaci více Chaotických systémů [5].
- Využívá známého jevu - Motýlího efektu, tedy citlivosti na počátečních podmínkách.
 - Na straně přijímače a vysílače musí být naprosto stejně nastavené a synchronizované systémy.
 - Právě nastavení, typ, parametry chaotického systému jsou v podstatě klíčem

Použití teorie chaosu pro šifrování

- Existuje celá řada technik - nejznámější je chaotická modulace (existují 2 přístupy), dále maskování, klíčování a využívání časoprostorového chaosu - CML systémů.
- Použití není limitováno jen na práci se signály (modulace, maskování, klíčování), ale i v digitální oblasti - např. transformací chaotického signálu do binární oblasti se šifrují nejčastěji obrázky...

Šifrování pomocí chaosu - Modulace

- Modulace chaotického systému

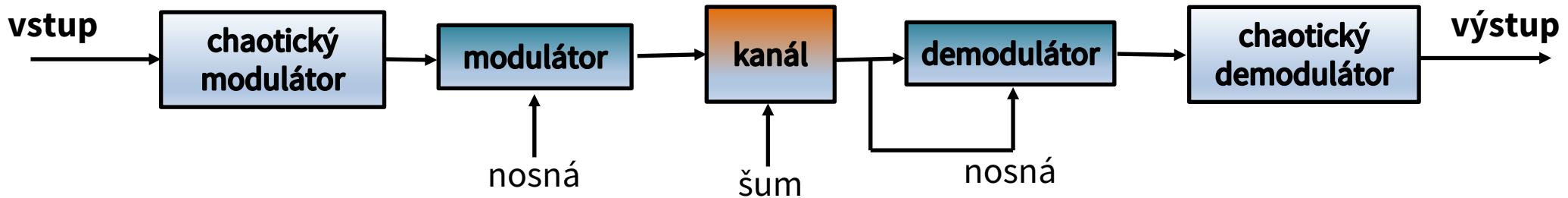


- Určeno především pro práci se signály - např. pro vysílačky a jiné typy např. frekvenčních modulací

Příklad funkce dle: [5]

Šifrování pomocí chaosu - Modulace

- Modulace chaotického systému



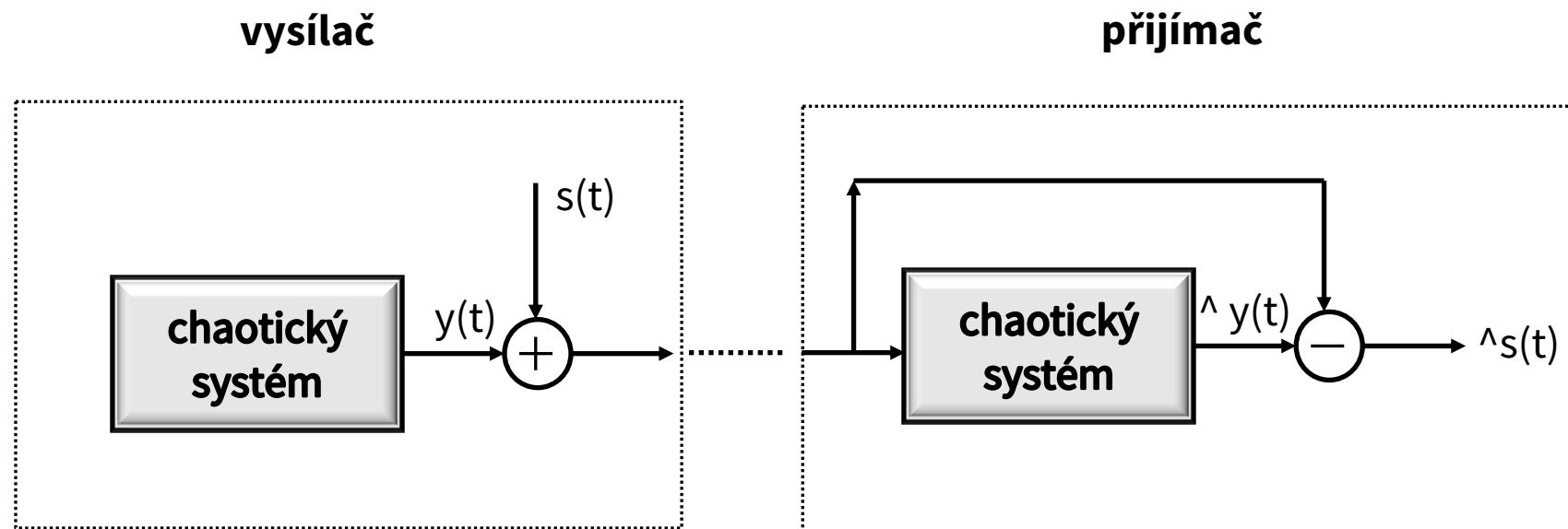
- Určeno především pro práci se signály - např. pro vysílačky a jiné typy např. frekvenčních modulací

Příklad funkce dle: [5]

Šifrování pomocí chaosu - Chaotické Maskování

- Stejně jako v případě modulace, založeno na synchronizaci chaotických systémů.
- Užitečný signál je na straně vysílače “přidán - přičten - sloučen” s chaotickým signálem. Na straně přijímače ja pak odečten a měli bychom získat “užitečnou informaci”.
- Nevýhoda - velmi náchylné na šum a poruchy!
- V binární formě se jedná o jednoduché “sečtení” nebo “XOR” informačních dat a chaotických dat (podobně jako proudová šifra).

Šifrování pomocí chaosu - Chaotické Maskování

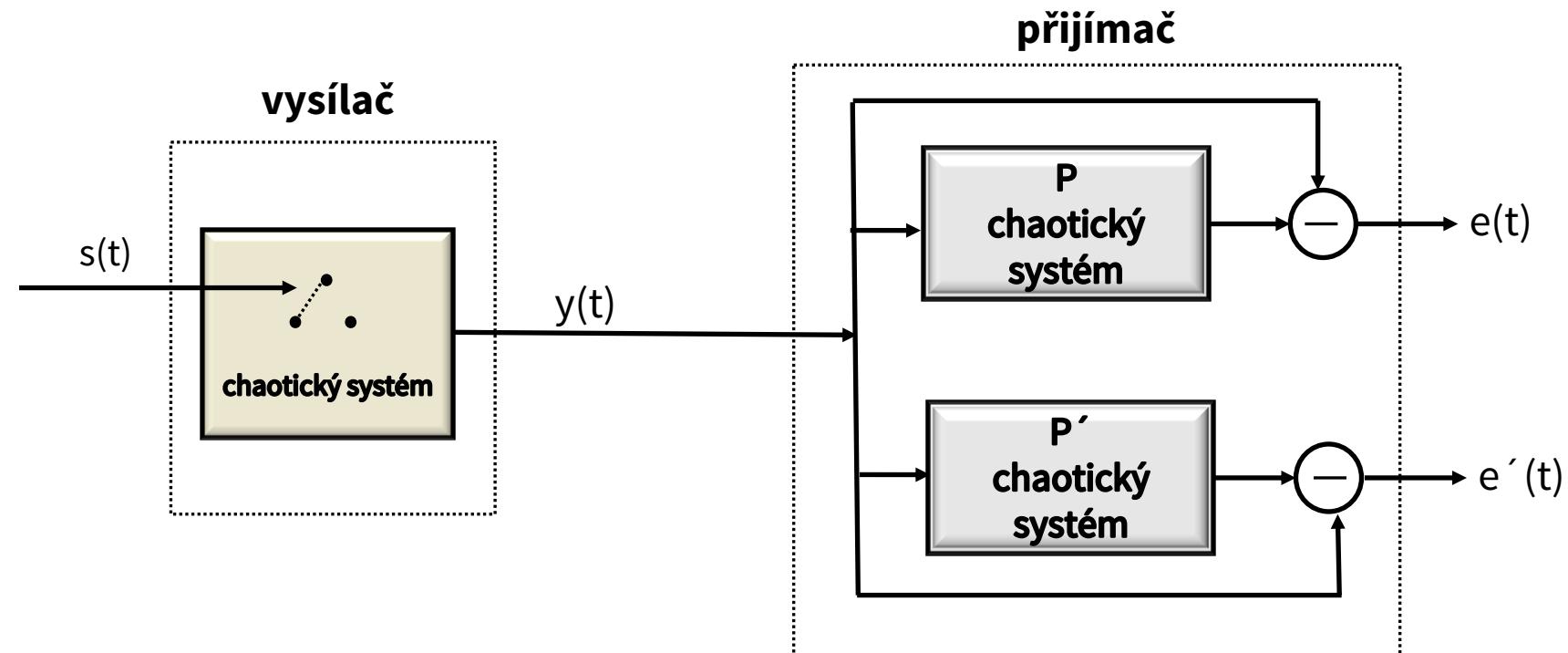


Příklad funkce dle: [5]

Šifrování pomocí chaosu - Chaotické klíčování

- Založeno na synchronizaci dvou různých chaotických systémů.
- Vhodné pro digitální přenosy (např. binární) - na straně přijímače zjišťujeme, s kterým systémem se nám přijatý signál synchronizoval, tomu odpovídá např. vyslaný bit.
- Dále existuje např Diferenciální chaotické klíčování a jiné...

Šifrování pomocí chaosu - Chaotické klíčování



Příklad funkce dle: [5]

Šifrování pomocí chaosu - CML Systémy

- Časoprostorový chaotický systém je prostorově rozšířený systém, který může vykazovat chaos jak v prostoru, tak v čase [1].
- CML (coupled map lattices) je považován za základní model časoprostorového chaotického systému. CML je dynamický systém, který je diskrétní v čase a prostoru [1].

Šifrování pomocí chaosu - CML Systémy

- CML je složen z nelineárních map umístěných na mřížkách, kterým se říká lokální mapy. Každá lokální mapa je spojena s další lokální mapou, za určitých podmínek.
- Vzhledem k vnitřní nelineární dynamice jednotlivých lokálních map a šíření prostorových spojů mezi jednotlivými mapami, může CML vykazovat časoprostorový chaos.
- Jedná se o paralelní spřažené chaotické systémy. Je možno si jej představit jako řadu "houpaček" na hřišti, které propojím nelineární vazbou (gumovým lanem) a jednu rozhoupou - chaos se pak šíří v čase i následně v prostoru mezi houpačkami.

Šifrování pomocí chaosu - CML Systémy

- Jedna z nejpopulárnějších CML je definována podle rovnice [1]:

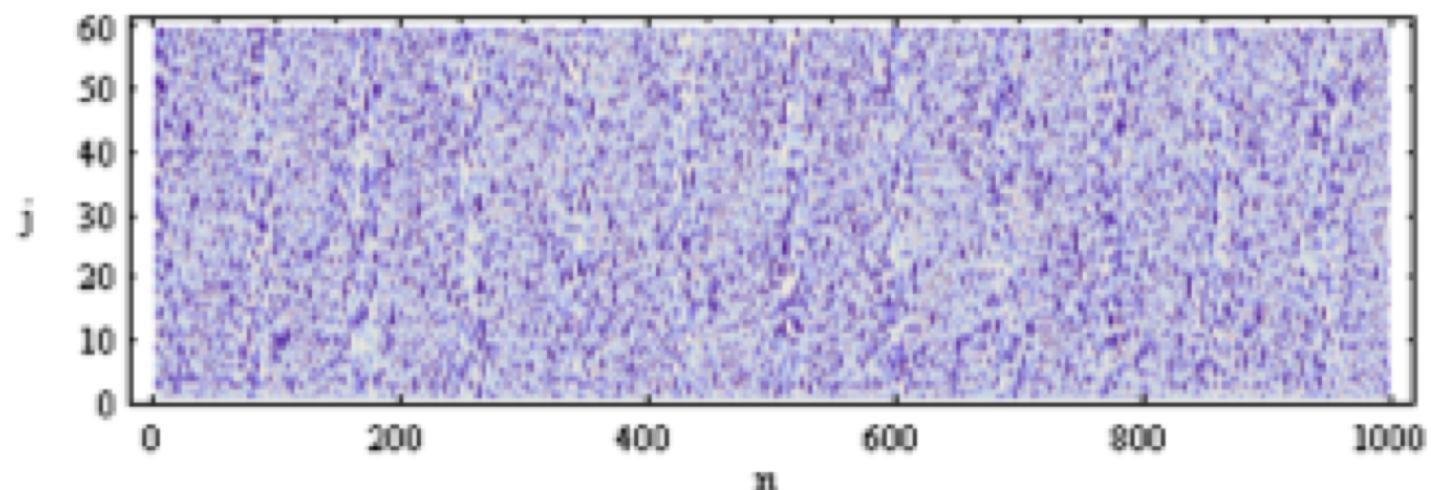
$$x_{n+1}^j = (1 - \varepsilon)f(x_n^i) + \frac{\varepsilon}{2}[f(x_n^{j+1}) + f(x_n^{j-1})]$$

- Kde funkce f reprezentuje rovnici s chaotickým chováním, například logistickou rovnici [1]:

$$x_{n+1} = rx_n(1 - x_n)$$

Šifrování pomocí chaosu - CML Systémy

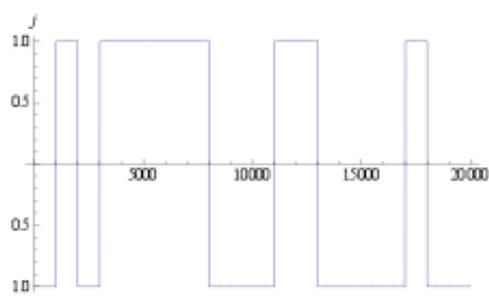
- Struktura CML: příklad - v jeden čas získáme např. 60 chaotických signálů - vhodné pro velká data



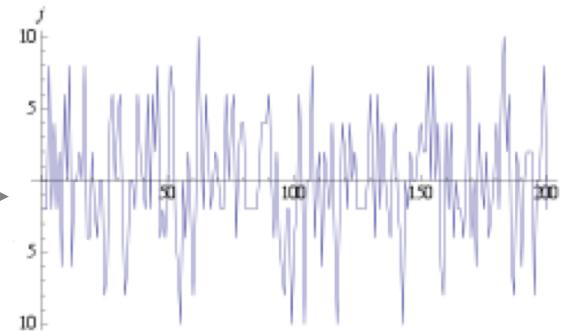
Zdroj obrázku: [6]

Šifrování pomocí chaosu - CML Systémy

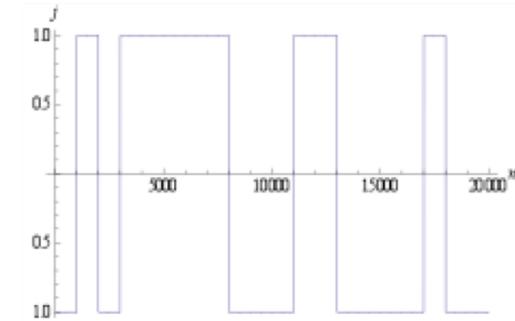
Zdrojová informace



Zašifrovaná informace

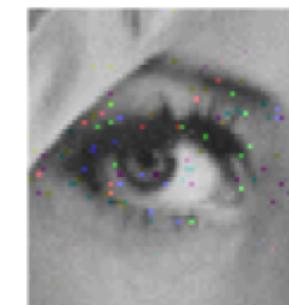
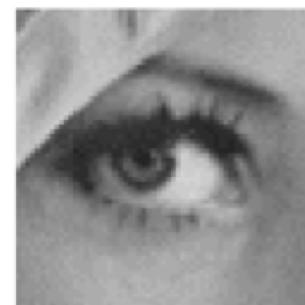


Dešifrovaná informace



Šifrování pomocí chaosu - CML Systémy

- Ukázka šifrování barevných obrázků, pomocí jednoduchého CML systému



Šifrování pomocí chaosu - CML Systémy

- CML obsahuje “ještě více extrémní citlivost” na výpočty a nastavení.
- Díky omezení bitové hloubky čísel a “zaokrouhlování” se projevují nepatrné odchylky, které se šířením v čase a prostoru zvětšují - mohou vznikat nepřesně dešifrované bity atd...

3. Další netradiční přístupy

Fraktální kryptografie

Netradiční kombinace teorie fraktálů (fraktální geometrie) a základních principů substitučních šifer [7].

- Využití jednoduchých affinních transformací pro tvorbu grafických fraktálů (algoritmus IFS – Iterated Function System).
- Pomocí jednoduché sady affinních transformací je vytvořen obrazec – který graficky substituuje znak.
- Sada affinních transformací = klíč.
- Další nástavbou je pak neuro-fraktální šifrování (s využitím podružné substituce jako koeficienty (váhy) neuronové sítě).

Kognitivní kryptografie

Kognitivní vědy představují interdisciplinární vědecké zkoumání mysli, simulaci mozkové činnosti a napodobení (modelování) lidského pojetí chápání světa. Základní ideou jsou možnosti identifikace uživatele (vlastníka/příjemce) nebo specifické (personalizované klíče) [8].

- Kognitivní (personalizovaná) kryptografie, tedy představuje systém, kdy chceme generovat šifrovací klíče, které nejsou zcela náhodné sekvence, ale ve kterých jsou některé osobní údaje embedovány (vloženy).
- Tyto klíče (algoritmy) umožňují nejen bezpečně zašifrovat data, ale ve zvláštních případech by rovněž mohly umožnit identifikaci majitele určitého klíče, který byl použit k provedení konkrétního kryptografického úkolu.

Seznam odkazů

- [1] Nejlépe střežená tajemství. Scientific American (české vydání), 77. SCIAM, 2005.
- [2] Quantum Cryptography. [online]. Dostupné z:
http://cryptowiki.net/index.php?title=Quantum_cryptography
- [3] SPROTT, Julien C. Chaos and time-series analysis. New York: Oxford University Press, 2003. ISBN 0198508409.
- [4] Chua's circuit. [online]. Dostupné z: https://en.wikipedia.org/wiki/Chua%27s_circuit
- [5] HLADÍK, Michal. Deterministický chaos: Princip a aplikace. Zlín, 2006. bakalářská práce (Bc.). Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky.
- [6] KLIMKOVÁ, Eva. Využití deterministického chaosu pro utajenou komunikaci - šifrování pomocí chaosu. Zlín, 2010. diplomová práce (Ing.). Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky
- [7] ZELINKA, Ivan, František VČELAŘ a Marek ČANDÍK. Fraktální geometrie: principy a aplikace. Praha: BEN - technická literatura, 2006. ISBN 80-7300-191-8.
- [8] OGIELA, L., & Takizawa, M. (2017). Personalized cryptography in cognitive management. Soft Computing, 21(9), 2451-2464.



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204