Jan JAŠEK, Antonín ČERNOCH, Karel LEMR
RCPTM, Společná laboratoř optiky Univerzity Palackého a Fyzikálního ústavu Akademie věd České republiky, Olomouc

Generování náhodných čísel prostřednictvím temných detekcí lavinových fotodiod

Náhodná čísla jsou důležitá pro celou řadu aplikací a metody jejich generace jsou v současné době často diskutovaným tématem, zejména z pohledu kryptografie a počítačového zabezpečení. Tento článek si klade za cíl popsat a otestovat možnosti využití temných detekcí lavinových fotodiod operujících v Geigerově režimu pro vytvoření kvantového generátoru pravých náhodných čísel. Hlavní předností našeho generátoru je časově úsporná generace a efektivita zpracování dat, přičemž takto generovaná data splňovala i vysoké nároky moderních kryptografických aplikací.

Klíčová slova: generátory náhodných čísel, temné detekce, jednofotonové lavinové fotodiody, Peresův algoritmus

1. ÚVOD

Náhodná čísla jsou důležitá pro mnoho aplikací, jako jsou statistické výzkumy, numerické výpočty, modelování a simulace (např. Monte Carlo), mnohé hry a loterie [2]. Od vzniku výpočetní techniky se pak náhodná čísla začala hojně využívat pro potřeby kryptografických aplikací, jako je generace bezpečnostních klíčů, šifrování aj. [2–6].

Poptávka po vhodných generátorech náhodných čísel je zejména v oblasti moderní kryptografie velmi vysoká. V dnešní době není problém opatřit si sadu náhodných čísel vygenerovaných například programem v počítači, ale jsou tato čísla doopravdy náhodná? Koneckonců, počítač je jen nástroj, co plní určitou sadu příkazů, a je tedy naprosto předvídatelný. Pokud chceme generovat doopravdy náhodná a nepředvídatelná čísla, je třeba využít fyzikální jevy, ať už klasické nebo kvantové [2, 3].

Ačkoliv metody klasické fyziky nabízejí poměrně široké možnosti k pozorování a měření náhodných jevů (např. šum elektrického obvodu [7]), ukazuje se, že tyto jevy jen spadají do kategorie chaotických systému, které jsou ve skutečnosti zcela deterministické [2]. Matematický popis těchto jevů je natolik složitý, že i velmi malá odchylka ve vstupních parametrech způsobí naprosto odlišný vývoj [3, 8]. Jevy klasické fyziky se tedy jeví náhodné pouze do té doby, než přesně určíme jejich vstupní parametry [2]. V tu chvíli jsme jev schopni přesně zopakovat, což je například v šifrování samozřejmě nežádoucí.

Přístup klasické fyziky v těchto případech selhává. Nabízí se otázka, jaká je situace z pohledu fyziky kvantové. Kvantové jevy obvykle existují v tzv. superpozici (sloučení více stavů) a až akt měření je donutí „zvolit" jednu konkrétní hodnotu příslušející určitému stavu. Tyto výsledky nejsou (s výjimkou systémů připravených ve vlastním stavu měřidla) deterministické a nemůžeme je tedy jednoznačně předpovědět ani zopakovat. Můžeme jen spočítat pravděpodobnost, že takový výsledek nastane [9]. Výsledky měření kvantových jevů tedy interpretujeme statisticky a může nám tak posloužit jako ideální zdroj nahodilosti.

Cílem tohoto článku je popsat a otestovat možnosti využití temných detekcí lavinových fotodiod operujících v Geigerově režimu k vytvoření kvantového generátoru pravých náhodných čísel. Hlavní předností našeho generátoru je časově úsporná generace a efektivita zpracování dat, přičemž díky principům kvantové mechaniky by takto generovaná náhodná čísla měla splňovat i vysoké nároky moderních kryptografických aplikací. Článek pojednává o základních principech náhodnosti i jejím testování a rozebírá principy a metody potřebné pro jejich generaci. Dále pak popisuje experimentální uspořádání pro generaci náhodných čísel s využitím temných detekcí lavinových fotodiod, následné zpracování dat a výsledky statistického testování.

2. NÁHODNÁ ČÍSLA

Generování náhodných čísel

Existují dvě možnosti, jak generovat náhodná čísla. První a nejčastěji využívaná možnost zahrnuje použití deterministického matematického algoritmu [10]. Takovýto generátor pak nazveme pseudonáhodný generátor náhodných čísel (PRNG – pseudorandom number generator) [4]. Druhou možností je použít generátor pravých náhodných čísel (TRNG – true random number generator), který využívá fyzikálního jevu – ať už chaotického procesu nebo jevu kvantového (v takovém případě označujeme generátor jako QRNG, kvantový generátor náhodných čísel) [10]. Pro naše potřeby generátory produkují bitový řetězec (sekvenci) náhodných 0 a 1, které mohou být dle potřeby dále rozděleny na menší podřetězce [4].

Pseudonáhodná čísla nejsou klasickými náhodnými čísly, jak už ostatně napovídá jejich jméno. V podstatě jde jen o výstup počítačových algoritmů, které pro generaci náhodných čísel využívají (obvykle) náhodný vstupní parametr nazývaný seed [4]. Algoritmy samotné jsou zcela deterministické a často i veřejné. Proto, pokud je odhalen seed, je známá i celá výsledná sekvence, což je poněkud nevhodné například právě pro kryptografické aplikace. Na druhou stranu je pak pomocí PRNG možno generovat náhodná čísla velmi rychle, což může být dostačující předností například při simulacích Monte Carlo [3]. Tyto algoritmy také mají sice velmi dlouhou, ale přesto konečnou periodu, kdy se po určité době začíná generovaná sekvence přesně opakovat.

Čísla generovaná matematickými algoritmy tedy nejsou skutečně náhodná, a tudíž jsou jen pseudonáhodná. Pro dosažení nepředvídatelnosti se pak jako seed často používá výstup z nějakého fyzikálního generátoru náhodných čísel, který tyto nedostatky částečně vyvažuje [4]. Některé PRNG pak ke generaci seedu mohou využívat i lidskou činnost (například doba mezi údery kláves klávesnice [3], pohyb myši na obrazovce [4]). Je také třeba být na pozoru, který algoritmus používáme a kdo jej ve skutečnosti implementoval.

Generátory pravých náhodných čísel vždy využívají za svůj základ fyzikální jevy [11], speciální důraz je pak kladen na jevy kvantové povahy. Zájem o tyto generátory náhodných čísel stoupl zejména v posledních letech, kdy se začala stále více projevovat nedostatečná kryptografická bezpečnost spojená s používáním pseudonáhodných čísel. Ta vyústila v prolomení bezpečnosti několika různých systémů, jako například zabezpečení operačního systému Windows [12] aj. [13].

Odpovědí těmto problémům byla celá řada návrhů generátorů pravých náhodných čísel, včetně těch kvantových. Takovéto generátory jsou postaveny na měření různých fyzikálních jevů,

například radioaktivního rozpadu [14], měření intenzity dopadajícího osvětlení na fotodetektoru mobilního telefonu [13], měření časového intervalu mezi fotony jednofotonového zdroje [10] a další. Tyto generátory se liší zejména rychlostí generace dat, která se pohybuje řádově mezi 10 kbit – 1 Mbit za sekundu, dále pak dobou a účinnosti zpracování nasbíraných dat.

Zamysleme se nyní nad tím, jaké vlastnosti by měl vykazovat ideální generátor pravých náhodných čísel. Ilustrovat takovýto generátor můžeme například pomocí hodů mince, která má strany označené čísly „0“ a „1“. Mince samotná bude samozřejmě dokonale vyvážená (tedy ideální). Co vlastně od takového TRNG požadujeme?

V prvé řadě by výsledná data měla být uniformně rozdělená, tedy každý výsledek je zastoupen se stejnou četností. Pro naši minci to znamená, že po určitém počtu hodů by mělo padnout stejné množství 0 i 1. To by naše mince splnit měla, přece jen je dokonale vyvážená. Druhým požadavkem je nezávislost jednotlivých výsledků. To naše mince splňuje, výsledek předchozího hodu neovlivní další hod ani po libovolném množství hodů. Třetí obecnou podmínkou je, aby ošetřením vstupních parametrů nebyla ovlivněna nepředvídatelnost generátoru. Pro hod naší mince by toto ošetření představovalo přesné změření její polohy, orientace, hybnosti a momentu hybnosti v počátku hodu.

Takováto mince tedy představuje velmi dobrý generátor náhodných čísel. Samozřejmě, i kdybychom takovou „férovou“ minci dokázali vytvořit, házení mincí pro vytvoření řetězců tvořených miliony bitů by bylo poněkud nepraktické – rychlost generace bitů by byla příliš nízká. TRNG proto obvykle využívají fyzikální jevy, které jsou dostatečně nepředvídatelné (například atmosférický šum nebo šum elektrického obvodu [3, 4]), v případě QRNG pak jevy kvantové (radioaktivní rozpad, foton na děliči svazku aj. [15]), které jsou nepředvídatelné již ze své podstaty [9]. Zásadní nevýhodou TRNG (případně QRNG) oproti PRNG je nižší rychlost generace [4], v závislosti na použitém fyzikálním jevu pak může být problematický i způsob měření výsledků, případně cena použité experimentální aparatury.

Náhodnost a nepředvídatelnost

Požadovanou vlastností každého generátoru náhodných čísel je nepředvídatelnost výsledků [4]. V případě PRNG to znamená, že pokud je neznámý seed, tak ze znalosti libovolného počtu předchozích hodnot by nemělo být možno dopředu předpovědět další výsledek generátoru. Stejně tak by ve výsledné sekvenci nemělo být možné najít jakýkoliv vzor či vztah mezi jednotlivými bity, který by umožnil seed odhalit [4]. Jak je to ale v případě TRNG a proč je požadovanou vlastností právě nepředvídatelnost?

Jak náhodnost, tak i nepředvídatelnost vyjadřují naši neschopnost najít v určité sekvenci vzor, který by nám umožnil předpovědět příští výsledek [4]. Zatímco ale nepředvídatelné jevy vykazují vzory jen těžko rozlišitelné, opravdu náhodné jevy nevykazují vzory vůbec žádné. Vztah náhodnosti a nepředvídatelnosti tedy můžeme popsat takto: skutečně náhodný jev je nepředvídatelný. Neschopnost předvídat jev však ještě nezaručuje jeho náhodnost.

Již v úvodu bylo naznačeno, že jevy klasické fyziky jsou deterministické, a tudíž nenáhodné. To je velmi silné tvrzení, na které mezi vědeckou komunitou dodnes nebyl vyvozen jednoznačný názor [3]. V dnešní době je možné jakožto generátor pravých náhodných čísel využít dva možné zdroje – měření kvantových jevů a chaotické systémy [3]. Teoretický rozdíl je značný – výsledky měření kvantových jevů jsou (vyjma systémů připravených ve vlastním stavu měřidla) samy o sobě definovány statistikou interpretací a jejich náhodnost (a tedy i nepředvídatelnost) plyne ze samotných definic kvantové mechaniky [9]. Chaotické systémy pak představují jevy, jejichž matematický model je natolik složitý, že jakákoliv nepřesnost ve vstupních parametrech způsobí dramatickou změnu ve vývoji celého systému [3, 8]. Jako příklad můžeme uvést dvojkyvadlo nebo vývoj počasí. Přesné ošetření všech vstupních parametrů zanechá přesně definovaný dynamický systém, který v žádném případě nepředvídatelný není [3, 8].

Z praktického hlediska se díváme na poněkud odlišnou situaci. Přesné vymezení vstupních parametrů by vskutku zanechalo chaotické systémy deterministické, nicméně tohoto vymezení není ve většině reálných situací možno docílit [8]. Jako příklad můžeme využít atmosférický šum, který je dnes jako zdroj náhodných čísel hojně používán [3]. Pro ošetření vstupních parametrů tohoto jevu by pravděpodobně bylo třeba znát rychlost a směr pohybu každé molekuly v atmosféře planety [3]. Tento požadavek je v dnešní době naprosto nereálný a atmosférický šum tedy můžeme považovat za dostatečný (ne-li naprostý) zdroj náhodnosti. Nepředvídatelnost TRNG tedy můžeme ošetřit použitím vhodného fyzikálního jevu.

Jak již bylo řečeno, nepředvídatelnost vyjadřuje jen naši neschopnost najít v náhodné sekvenci vzor, který by nám umožnil předpovědět příští výsledek, ne skutečnou náhodnost. Je třeba si proto uvědomit, že například několik století zpátky by pravděpodobně čísla pseudonáhodná byla interpretována jako pravá náhodná čísla, jelikož by bez pomocí výpočetní techniky nebylo možné objevit jejich konečnou opakovací periodu. Z podobného důvodu v dnešní době můžeme jako náhodné jevy interpretovat chaotické systémy – zabraňuje nám v tom jen technologický pokrok. Můžeme tedy říct, že nepředvídatelnost vyjadřuje pouze to, jak náhodně na nás jev působí, a právě to jsme schopni testovat.

Maximální možná přesnost měření se ovšem neustále zvyšuje, a proto jednoho dne i dnes reálně neměřitelné parametry mohou být měřitelné. Oproti tomu jevy kvantové zůstanou (alespoň podle současných teoriích) navždy ve světě statistiky [9], a tedy i ideálním zdrojem skutečné náhodnosti. Jelikož tato práce popisuje generování náhodných čísel pomocí měření jevů kvantové optiky, budeme nepředvídatelnost a náhodnost považovat za ekvivalentní.

Statistická testovací sada společnosti NIST

Pro testování náhodnosti výsledků generátorů náhodných čísel je třeba použít vhodný testovací software. V této práci jsme zvolili testovací sadu společnosti NIST (National Institute of Standards and Technology) je jednou z nejstarších amerických vědeckých organizací. Její součástí je také divize pro počítačové zabezpečení, která pro potřeby testování generátorů náhodných čísel vhodných pro šifrování vydala statistický testovací balík NIST nazvaný Statistical Test Suite (STS). Tento testovací balík nám poslouží jako výchozí posuzovací kritérium, zda náš generátor náhodných čísel splňuje nároky náhodnosti pro kryptografické účely. NIST STS se skládá z celkem patnácti výchozích testů. Jejich detailní popis, doporučené vstupní sekvence a příklady použití můžeme najít v [4].

Interpretace testů

NIST STS jako vstup vždy přijme binární datový řetězec, který reprezentuje naměřená data. Tento řetězec rozdělí na uživatelem zvolený počet binárních sekvencí a ty následně testuje jednotlivě. Toto dělení je nutné pro výslednou interpretaci testů. Koneckonců, výsledkem statistického testu pro každou sekvenci je pouze empirická P-hodnota. Na základě těchto P-hodnot je pro každou sekvenci přijata nebo odmítnuta nulová hypotéza.

NIST STS volí pro interpretaci výsledků dva přístupy. Nejprve je pro každou sekvenci vypočítaná tzv. P-hodnota, tedy pravděpodobnost, že obdržíme právě takovou sekvenci za předpokladu, že data byla náhodná. Je-li P-hodnota vyšší než hladina významnosti 1 %, sekvence je přijata jako náhodná. Následně je provedeno porovnání výsledného počtu přijatých sekvencí a odmítnutých sekvencí, čímž můžeme ošetřit, zda se v řetězci nevyskytují lokální nenáhodné anomálie, tedy zda zastoupení nepravděpodobných výsledků odpovídá pravděpodobnosti jejich rozložení. Druhým kritériem je pak posouzení distribuce výsledných P-hodnot a určení tak jejich uniformnosti. Pokud by sekvence vykazovaly stále stejnou P-hodnotu, pravděpodobně by generátor vytvářel periodicky stejná data, což je v našem případě nežádoucí. Program spočítá globální P-hodnotu jako pravděpodobnost, že skutečně náhodná data poskytnou námi pozorované rozložení individuálních P-hodnot spočtených pro každou sekvenci.

Poměry přijatých ku odmítnutým sekvencí i P-hodnoty vypočítané uniformnosti distribuce P-hodnot jednotlivých sekvencí můžeme pro každý test nalézt v *tab. 3* v experimentální části. Nutná kritéria pro splnění testu se liší dle počtu přijatých sekvencí, pro 100 sekvencí je nejnižší přijatelný poměr 96/100 a nejnižší přijatelná globální P-hodnota 0,0001. Testy, které nesplní tato kritéria, jsou označeny hvězdičkou. Detailní popis interpretace testů můžeme najít v [4].

3. EXTRAHOVÁNÍ BITŮ Z NEUNIFORMNÍ NÁHODNÉ SEKVENCE

V experimentální praxi je měření náhodných jevů velmi ovlivněno vybraným způsobem a parametry měření. Často pak dochází k tomu, že měření, byť i principiálně náhodného jevu, vygeneruje silně neuniformní (tedy předvídatelnou) sekvenci. Tato odchylka od nepředvídatelnosti přitom není způsobena nenáhodností jevu, jen nevhodným způsobem sběru dat, ve kterém nejsou všechny události stejně pravděpodobné. Jednoduchým příkladem může být měření, zda temná detekce nastala nebo nenastala v konkrétním časovém úseku (sekce 4). Pokud bude toto časové okno příliš velké, budou temné detekce zaznamenány takřka při každé iteraci. Pokud je příliš malé, nebudou v daném časovém intervalu zaznamenány téměř žádné temné detekce. Tuto neuniformnost je obvykle možno odstranit kalibrací měřicí aparatury, v našem případě zvolením vhodného časového intervalu, ovšem tento interval je pro každou fotodiodu jiný a navíc nemusí být v čase konstantní.

Pro nastolení uniformnosti v sekvenci je proto vhodnější využít počítačových algoritmů, které dokáží náhodné bity z neuniformní binární náhodné sekvence vyextrahovat [16]. Těchto algoritmů je hned několik a liší se zejména svou účinností extrakce a dobou zpracování. Podmínkou fungování těchto algoritmů je, aby sekvence byla náhodná, jednotlivé bity byly na sobě nezávislé a aby pravděpodobnost obou bitů byla v čase konstantní [17].

Nejjednodušší algoritmus extrahující bity z binárních sekvencí byl navržen von Neumannem [16]. Jeho myšlenka tkví v rozdělení sekvence na dvojice po sobě následujících bitů. Následně, pokud máme náhodnou binární sekvenci s pravděpodobností bitu 0 označenou jako p a pravděpodobnost bitu 1 jako q, je výskyt dvou po sobě jdoucích událostí pq stejně pravděpodobný jako dvojice událostí qp (tedy 01 a 10 má v sekvenci stejnou pravděpodobnost výskytu). Tyto dvojice událostí tedy můžeme nahradit bity 0 a 1 a vytvořit tak námi hledanou uniformní sekvenci. Stejně ovšem nemůžeme postupovat u po sobě jdoucích událostí pp a qq, jejichž pravděpodobnosti obecně neznáme. Tyto bity tedy musíme zahodit.

Jednoduchost tohoto algoritmu umožňuje velice rychlé zpracování dat, jeho nevýhodou je ovšem účinnost extrakce. Pro $p = q = 0{,}5$ (tedy pro dokonale uniformní sekvenci) je šance na dvojici událostí $pq = 0{,}25$, tedy 25 %. Celková šance k uskutečnění námi použitelných událostí je tedy v naprosto dokonalém případě $pq + qp = 0{,}5 = 50$ %. Jejich nahrazením bity 0 a 1 ale ztratíme další polovinu dat. Maximální účinnost extrakce von Neumannova algoritmu je tedy pouhých 25 % délky původní sekvence [16]. Účinnosti pro neuniformní sekvence jsou pak ještě podstatně nižší.

Uveďme si ilustrační příklad. Naše výchozí neuniformní sekvence byla vygenerována událostmi „*qqpqqqppqp*“, jde tedy o binární sekvenci „1101110010“. Aplikací von Neumannova algoritmu dostaneme sekvenci „×0××1“ přičemž × reprezentuje dvojice bitů, které musíme zahodit. Výsledná sekvence je tedy „01“, jež je skutečně uniformní, ovšem za cenu ztráty 4/5 dat. Znázornění můžeme vidět v *tab. 1*.

Tab. 1 Příklad použití von Neumannova algoritmu

von Neumann

11	01	11	00	10	… výchozí sekvence
×		×	×		… odhozené bity
	0			1	… extrahovaná sekvence

Peresův algoritmus

Existují ovšem i další algoritmy extrahující bity z neuniformní náhodné sekvence, které dosahují daleko vyšší účinnosti extrakce. Právě z tohoto důvodů jsme se v naší práci rozhodli použít algoritmus Peresův [17]. Tento algoritmus je jakousi iterací von Neumannova algoritmu a umožňuje extrahovat ze sekvence maximální míru Shannonovy entropie H, kterou můžeme vypočítat podle vztahu (1) [18]

$$H(X) = -\sum_{i=1}^{N} p_i \log_2(p_i), \tag{1}$$

kde X je náhodná veličina nabývající N možných hodnot s pravděpodobnostmi p_i, kde i nabývá hodnot v intervalu <0;N>. Fungování Peresova algoritmu (jednu jeho iteraci) si ukážeme v *tab. 2* na stejném příkladě jako výše.

Tab. 2 Příklad použití Peresova algoritmu

iterace Perese

11	01	11	00	10	… výchozí sekvence
	0			1	… přímo extrahovaná sekvence
0	1	0	0	1	… sekvence x (XOR výchozí sekvence)
1		1	0		… sekvence y (transformace 00→0, 11→1)

Sekvence x představuje XORování a sekvence y jakýsi „doplňkový von Neumannův algoritmus“. Tato část algoritmu tedy hledá v sekvenci dvojice stejných po sobě jdoucích bitů, přičemž dvojici 00 nahradí bitem 0 a dvojici 11 nahradí bitem 1. Sekvence x i sekvence y jsou pak dále každá zvlášť iterovány Peresovým algoritmem jako nové vstupní sekvence. Iterace jsou ukončeny ve chvíli, kdy ze zbývajících sekvencí již není možné extrahovat další náhodná data. Tímto opakovaným postupem bude konečná extrahovaná sekvence našeho příkladu „0101“. Velikost výsledné uniformní sekvence je tedy oproti použití von Neumannova algoritmu (v tomto případě) dvojnásobná.

4. POPIS EXPERIMENTU A DOSAŽENÉ VÝSLEDKY

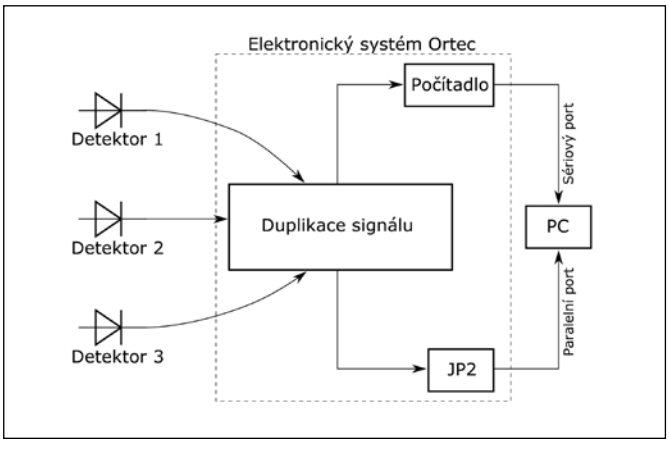
Jak již bylo zmíněno v úvodu, cílem našeho experimentu bylo popsat a otestovat použití temných (falešných) detekcí ke generování náhodných čísel. Výsledná data musela být vždy upravena na binární řetězec, aby mohla být otestována pomocí NIST STS. Veškeré algoritmy na úpravu dat byly implementované v jazyce Python. Pro tvorbu grafů a histogramů byl použit program Graphics Layout Engine.

Pro měření událostí jsme použili lavinové fotodiody značky Perkin Elmer operující v Geigerově režimu zapojené podle schéma na *obr. 1*. Tyto fotodiody jsou natolik citlivé, že jsou schopné zaregistrovat dopad i jednotlivých fotonů, nicméně v tomto případě byly fotodiody zacloněné a my jsme detekovali pouze jejich temné detekce. Dosažená opakovací perioda byla 0,1 milisekund. Pokud v tomto časovém intervalu dioda zaznamená temnou detekci, vyšle TTL puls do klopného obvodu JP2 (SLO) a do počítadla sčítajícího počet impulzů. Klopný obvod komunikuje s počítačem prostřednictvím paralelního portu. Pro řízení této komunikace jsme použili vlastní program implementované v jazyce C.

Klopný obvod je elektronický obvod, který nabývá právě dva stabilní napěťové stavy – polohu 0 a polohu 1. Přepínám těchto stavů je možné uchovávat informaci. Pokud klopný obvod zaregistruje TTL puls, přepne se do polohy 1 a v té setrvává, dokud není uživatelem resetován. Skrze paralelní port je pak pomocí počítače možné zjistit, v jaké poloze se klopný obvod nachází a případně ho resetovat. Klopný obvod JP2 má čtyři vstupy, čímž umožňuje vést signály až pro čtyři detektory najednou, my jsme současně využili tři.

Řídicí program v nekonečném cyklu četl hodnoty napětí na paralelním portu, přičemž při každé iteraci resetoval klopný obvod do polohy 0 s opakovací periodou 0,1 milisekund. Dosáhli jsme tak rychlosti sběru neuniformních náhodných dat přibližně 4,5 kbit za sekundu. Kopie TTL pulsů byla posílaná na počítadlo (Dual Counter Timer, Ortec), pomocí kterého jsme zároveň zapisovali počet temných detekcí za jednotku času (v tomto případě 0,1 sekundy). Tato data jsme využili pro vykreslení histogramu.

Tento způsob generace dat se ukázal být poměrně rychlý. Čekací doba je zde omezena vlastně jen mrtvou dobou detektoru a rychlostí resetování klopného obvodu, který se po každém zaznamenaném napětí musí resetovat do výchozí hodnoty 0. Problémem se ale ukázala být silná neuniformita sekvence, jelikož každý detektor vykazuje jiný počet temných detekcí za jednotku času. Pro vyvážení počtu 0 a 1 jsme proto použili Peresův algoritmus [17]. Ten značně prodloužil dobu zpracování dat, obzvláště pro detektory s vysokým počtem temných detekcí (a tedy vyrovnanějším počtem 0 a 1), což mohlo být zapříčiněno využitím programovacího jazyka Python.



Obr. 1 Schéma experimentální sestavy pro měření sledu temných detekcí dle kapitoly 4.4

Je třeba zmínit, že pro Peresův algoritmus jsme při XORování nemohli řetězec rozdělit v půli a XORovat vždy dva znaky – výsledný počet 0 a 1 nebyl dostatečně v rovnováze (lišil se téměř o jedno procento). Tento problém byl pravděpodobně způsoben fluktuacemi 0 a 1 napříč celým souborem dat. Problém jsme vyřešili odlišnou generací podřetězců – jeden podřetězec obsahoval všechny členy se sudým indexem a druhý podřetězec všechny členy s lichým indexem z původního řetězce stejně, jak to ve svém článku navrhl sám Peres [17].

Naměřená data prošla statistickým testováním bez chyby, jak můžeme vidět z výsledků v tab. 3, a potvrdila tak myšlenku náhodnosti temných detekcí pro všechny tři detektory.

Tab. 3 Výsledky statistického testu NIST STS po aplikaci Peresova algoritmu na data získaná měřením sledu temných detekcí. Velikost každé sekvence pro detektor 1 je 1,02 Mbit, pro detektor 2 je to 1,7 Mbit a pro detektor 3 je to 6 Mbit. Minimální počet úspěšně vyhodnocených sekvencí pro splnění testu je 96, pro testy náhodné procházky a variace náhodné procházky je to: 65 pro detektor 1, 60 pro detektor 2 a 80 pro detektor 3. Minimální P-hodnota úspěšně vyhodnoceného testu je 0,0001. V těchto případech splnily kritéria NIST STS všechny testy

Výsledek testu: Uspěl

Test	Detektor 1		Detektor 2		Detektor 3	
	Poměr	P-hod	Poměr	P-hod	Poměr	P-hod
Frekvence	99/100	0,62	100/100	0,57	98/100	0,92
Bloková Frekvence	99/100	0,78	100/100	0,66	98/100	0,78
Kumulativní Suma	98/100	0,39	99/100	0,29	98/100	0,6
Běhy	100/100	0,97	99/100	0,86	100/100	0,55
Nejdelší Běh	100/100	0,19	99/100	0,46	97/100	0,05
Hodnost matice	100/100	0,64	99/100	0,96	99/100	0,9
FFT	98/100	0,55	98/100	0,80	100/100	0,02
Nepřekrývající se šablony	98/100	0,51	98/100	0,50	99/100	0,54
Překrývající se šablony	99/100	0,19	100/100	0,08	99/100	0,22
Univerzální	98/100	0,22	100/100	0,002	100/100	0,9
Entropie	100/100	0,28	100/100	0,85	100/100	0,06
Náhodná procházka	68/69	0,21	63/64	0,39	83/84	0,43
Var. náhodné procházky	68/69	0,29	63/64	0,37	82/84	0,44
Sériový	99/100	0,20	99/100	0,70	99/100	0,46
Lineární komplexity	98/100	0,55	98/100	0,21	98/100	0,15

Již jsme zmínili, že doba zpracování Peresovým algoritmem rostla spolu se zvyšující se uniformností dat. Stejně tak ale rostla i výtěžnost extrahování dat, jak můžeme vidět na hodnotách *tab. 4*, kde je nejvíce dat vyextrahováno právě pro detektor s největší střední hodnotou frekvence temných detekcí. Účinnost extrakce (myšleno jako účinnost extrahování „náhodnosti" sekvence, nikoliv množství dat) můžeme vypočítat podle vztahu

$$\eta_e = \frac{H_0}{H_I} \approx \frac{N_0}{H_I}, \qquad (2)$$

kde H_0 je hodnota vstupní Shannonovy informace, H_I je hodnota výstupní Shannonovy informace a N_0 je délka sekvence po aplikaci Peresova algoritmu.

Tabulka kromě množství vstupních a výstupních dat porovnává také účinnost extrakce η_e. Můžeme vidět, že η_e dosahuje nejméně 99,3 %, a tedy že Peresův algoritmus zachoval 99,3 % náhodnosti původní sekvence. Také můžeme vidět, že účinnost extrakce spolu s množstvím výsledných dat roste.

Tab. 4 Porovnání vstupního a výstupního množství dat v závislosti na střední hodnotě frekvence temných detekcí a odpovídající účinnosti extrakce Peresova algoritmu pro všechny tři detektory

Vstupní hodnoty

	Detektor 1	**Detektor 2**	**Detektor3**
Množství naměřených dat	1,43 Gbit	1,43 Gbit	1,43 Gbit
Frekvence temných detekcí	107,9 Hz	55,5 Hz	627,5 Hz
Pravděpodobnost bitu 1	1,68 %	0,87 %	9,44 %

Výstupní hodnoty

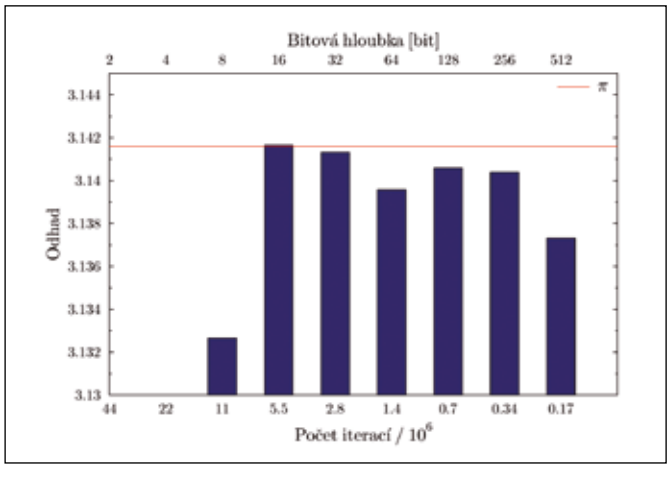
	Detektor 1	**Detektor 2**	**Detektor3**
Množství extrahovaných dat	175 Mbit	102 Mbit	641 Mbit
Účinnost extrakce	99,44 %	99,30 %	99,53 %

Dále můžeme vygenerovaná náhodná čísla otestovat také odhadnutím velikosti čísla π pomocí jednoduché simulace Monte Carlo, jejíž výsledky můžeme vidět v *tab. 5*. Tato simulace potřebuje ke správnému odhadování obecně velké množství dat. Přesnost odhadu čísla π závisí na dvou faktorech. Za prvé je pro přesný odhad třeba simulaci mnohokrát iterovat, tedy čím vyšší počet iterací, tím přesnější odhad. Za druhé je pak třeba mít vstupní čísla dostatečně jemně rozlišená. Jelikož je naše vygenerovaná sekvence binární a π potřebujeme vyjádřit v desítkové soustavě, musíme naše data převést.

Můžeme si ovšem zvolit bitovou hloubku každého převedeného čísla, tedy kolik bitů z binární sekvence bude tvořit jednotlivá převedená desítková čísla. Čím vyšší je tato bitová hloubka, tím větší je interval vygenerovaných desítkových čísel a tím přesnější by také měl být i výsledný odhad. Cenou za větší bitovou hloubku i za vyšší počet iterací je ovšem i větší spotřeba dat. Můžeme si položit otázku, jaký je optimální poměr těchto dvou faktorů, pokud

máme konstantní objem dat. Závislost přesnosti odhadnuté hodnoty π na zvyšující se bitové hloubce (a zároveň snižujícím se počtu iterací) od 2 bitů do 512 bitů při konstantní velikosti dat můžeme vidět na *obr. 2*.

Z obrázku můžeme vyčíst, že nejméně efektivní jsou vždy krajní hodnoty, tedy pokud zvolíme bitovou hloubku příliš nízkou nebo příliš vysokou. Výsledné odhady čísla π najdeme v tab. *5*. Můžeme vidět, že navzdory očekáváním nebyl nejpřesnější odhad pomocí dat vygenerovaných detektorem 3, u kterého byla využita největší bitová šířka i nejvyšší počet iterací. Odchylka od tabelované hodnoty π je nicméně velmi malá (řádově 10^{-4}), proto můžeme odhady považovat vzhledem k použité metodě za přesné.



Obr. 2 Závislost přesnosti odhadnuté hodnoty π na rostoucí bitové hloubce a snižujícím se počtu iterací

Tab. 5 Výsledky odhadnutí čísla π pomocí simulace Monte Carlo
Odhad čísla π

	Detektor 1	**Detektor 2**	**Detektor 3**
Bitová hloubka	16 bit	16 bit	64 bit
Počet iterací	$5{,}5{\cdot}10^{6}$	$3{,}2.10^{6}$	$5{\cdot}10^{6}$
Odhad čísla π	3,14165	3,1407	3,1418
Chyba odhadu	$5{,}63{\cdot}10^{-5}$	$8{,}65{\cdot}10^{-4}$	$2{,}5{\cdot}10^{-4}$

5. ZÁVĚR

Navrhli jsme, sestavili a otestovali úsporný kvantový generátor náhodných čísel využívající měření temných detekcí lavinových fotodiod operujících v Geigerově režimu. Požadavkem generátoru bylo vygenerovat náhodnou binární sekvenci, kterou můžeme následně otestovat souborem statistických testů NIST STS.

Popsaný experiment využíval ke generaci náhodných čísel temné detekce lavinové fotodiody. Detekovali jsme sled temných detekcí a pro komunikaci s počítačem jsme využili klopný obvod a paralelní port, s dosaženou opakovací periodou 0,1 milisekund a rychlostí sběru dat 4,5 kbit/s pro každý detektor, přičemž jsme mohli aktivně využívat až čtyři detektory současně. Je třeba zmínit, že rychlost této experimentální sestavy je omezena pouze rychlostí přepínání klopného obvodu, maximální možná rychlost generace dat by pro lavinové fotodiody s vyšším počtem temných detekcí (například fotodiody bez přídavného chlazení) byla ještě mnohokrát vyšší.

Takto generovaná data byla přímo binární, nicméně nebyla uniformně rozložená. Implementovali jsme proto Peresův algoritmus, který slouží k extrahování náhodnosti z binární neuniformně rozložené náhodné sekvence. Výhodou tohoto algoritmu je jeho účinnost – algoritmus zachovává maximální možnou míru Shannonovy entropie *H*, a tedy i maximální možnou „míru náhodnosti" obsažené v sekvenci. Nevýhodou je dlouhá doba zpracování dat, která ale mohla být částečně způsobena použitím programovacího jazyku Python.

Experiment se ukázal být velmi úspěšný a všechny požadavky statistického balíku NIST STS použitého k testování byly splněny. Účinnost extrakce Shannonovy entropie *H* dosahovala více než 99,3 % a při použití námi vygenerovaných náhodných čísel pro odhad π pomocí simulace Monte Carlo jsme určili π s přesností na čtyři desetinná místa. Vzhledem k dosaženým výsledkům můžeme konstatovat, že námi navržený generátor náhodných čísel je plně funkční a splňuje požadavky na kryptografickou bezpečnost. Jeho další výhodou je také maximální úspora při zpracování generovaných dat.

I přes dosažené výsledky je nicméně otázkou, nakolik je metoda generace pomocí temných detekcí opravdu náhodná. Dá se považovat za kvantovou nebo stochastickou? Původem temných detekcí je termální fluktuace, která excituje elektron do vodivostního pásu. Elektron je mikroskopická částice, může být v kvantové superpozici neexcitovaný-excitovaný. V případě, že je excitovaný, může být urychlen závěrným napětím a excitovat další nosiče náboje a my změříme makroskopický proud. Otázka zde je, zda elektrony skutečně existují v kvantové superpozici neexcitovaný--excitovaný, nebo zda jsou v distinktivních stavech podléhajících určitému stochastickému rozdělení, jehož parametry my neznáme. Z takového pohledu by pak šlo o jevy nepředvídatelné, nicméně ne skutečně náhodné. Na tuto otázku jsme ale nenašli jasnou odpověď.

Autoři děkují projektu LO1305 poskytnutým Ministerstvem školství, mládeže a tělovýchovy ČR. Autoři také děkují společnosti CESNET za poskytování datových služeb.

Článek vychází z bakalářské práce Jana Jaška [1].

Literatura

[1] J. Jašek, „Generování náhodných čísel prostřednictvím lavinových fotodiod," bakalářská práce UP v Olomouci 2017.

[2] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Opt. Express*, vol. 18, no. 12, pp. 13029–13037, 2010.

[3] M. Haahr, "Randomness," 1998. Available at https://www.random.org/randomness/.

[4] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. V. Levenson, N. A. Heckert, and D. L. Banks, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, 2010.

[5] F. X. Wang, C. Wang, W. Chen, S. Wang, F. S. Lv, D. Y. He, Z. Q. Yin, H. W. Li, G. C. Guo, and Z. F. Han, "Robust quantum random number generator based on avalanche photodiodes," *Journal of Lightwave Technology*, vol. 33, no. 15, pp. 3319–3326, 2015.

[6] E. Carter, "The generation and application of random numbers," *Forth Dimensions*, vol. 16, 1994.

[7] S. K. Tawfeeq, "A random number generator based on single-photon avalanche photodiode dark counts," *Journal of Lightwave Technology*, vol. 27, no. 24, pp. 5665–5667, 2009.

[8] S. H. Kellert, *In the Wake of Chaos: Unpredictable Order in Dynamical Systems*. University of Chicago, 1994.

[9] D. J. Griffiths, *Introduction to Quantum Mechanics; 2nd ed.* Upper Saddle River, NJ: Pearson, 2005.

[10] H.-Q. Ma, Y. Xie, and L.-A. Wu, "Random number generation based on the time of arrival of single photons," *Appl. Opt.*, vol. 44, no. 36, pp. 7760–7763, 2005.

[11] C. H. Vincent, "The generation of truly random binary numbers," *Journal of Physics E Scientific Instruments*, vol. 3, pp. 594–598, 1970.

[12] L. Dorrendorf, Z. Gutterman, and B. Pinkas, "Cryptoanalysis of the random number generator of the windows operating system," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 1, pp. 10:1–10:32, 2009.
[13] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," *Phys. Rev. X*, vol. 4, p. 031056, 2014.
[14] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector," *Phys. Rev. A*, vol. 83, p. 023820, 2011.
[15] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information*, vol. 2, p. 16021, 2016.
[16] J. von Neumann, "Various Techniques Used in Connection with Random Digits," *J. Res. Nat. Bur. Stand.*, vol. 12, pp. 36–38, 1951.
[17] Y. Peres, "Iterating von Neumann's procedure for extracting random bits," *Ann. Statist.*, vol. 20, no. 1, pp. 590–597, 1992.
[18] C. E. Shannon, "A mathematical theory of communication," vol. 27, pp. 379–423, 623–656, 1948.

Bc. Jan Jašek, RCPTM, Společná laboratoř optiky Univerzity Palackého a Fyzikálního ústavu Akademie věd ČR, 17. listopadu 12, 772 07 Olomouc, jan.jasek01@upol.cz
Mgr. Antonín Černoch, Ph.D., RCPTM, Společná laboratoř optiky Univerzity Palackého a Fyzikálního ústavu Akademie věd ČR, 17. listopadu 12, 772 07 Olomouc, antonin.cernoch@upol.cz, tel.: 585 631 549
doc. Mgr. Karel Lemr, Ph.D., RCPTM, Společná laboratoř optiky Univerzity Palackého a Fyzikálního ústavu Akademie věd ČR, 17. listopadu 12, 772 07 Olomouc, k.lemr@upol.cz, tel.: 585 631 547

Jedná se o vědecký článek.

Odešel profesor Emil Wolf

Emil Wolf se narodil 30. července 1922 v Praze a zemřel 5. června 1918, dožil se tedy téměř 96 let. Z Československa odešel v roce 1939 a po zastávkách v Bristolu, Manchesteru, Cambridge a Edinburghu, kde působil jako asistent Maxe Borna, zbytek své dlouhé vědecké kariéry strávil v Rochesteru v USA, když před tím ještě působil v Berkeley, Torontu a New Yorku. Protože na prof. Wolfa bude napsáno mnoho vzpomínek, zaměřím se jen na okolnosti, které souvisejí s jeho kontakty s pracovníky v České republice a zvláště v Olomouci.

První kontakty s ním navázal profesor Bedřich Havelka během mezinárodního kongresu ICO v Paříži v roce 1963. Od té doby pracovníci Laboratoře optiky, později Společné laboratoře optiky, a katedry optiky Přírodovědecké fakulty UP s ním udržovali písemné kontakty, méně časté před rokem 1990, ale hodně intenzivní i s osobními setkáními po roce 1990. Mé první osobní setkání s ním se odehrálo na optické konferenci v Jeně v roce 1979, kam přijel jako president Americké optické společnosti OSA, a od té doby jsem se mohl podílet na spolupráci při přípravě jednotlivých svazků monografické řady Progress in Optics (North Holland, Amsterdam), jichž vyšlo 60 svazků od roku 1961 pod edicí prof. Wolfa, čeští autoři dodali 13 kapitol. Před rokem 1990 nedocenitelná pomoc prof. Wolfa spočívala v pomoci s nedostupnou literaturou i s možností zúčastnit se významných zahraničních konferencí v optice, zejména pravidelných konferencí o koherenci a kvantové optice konaných v Rochesteru.

Prof. Wolf je zakladatelem moderní teorie částečné koherence a vždy dával přednost klasické teorii druhého řádu, protože se domníval, že je tam stále hodně problémů k řešení. V poslední době zejména propojil teorii koherence a polarizace, což shrnul v knize *Introduction to the Theory of Coherence and Polarization* (Cambridge University Press, 2007). Když dopisoval se zpožděním dnes již klasické dílo Principles of Optics (Pergamon Press, Oxford 1959, 7 vydání), nabádal ho spoluautor Max Born, aby vydání knihy nezdržoval dopisováním kapitoly o částečné koherenci, která stejně nebude nikoho zajímat. Brzy se vlastnost koherence stala ústředním problémem fyziky. Jako spoluautor této knihy je prof. Wolf pravděpodobně nejcitovanějším fyzikem. Ale se svými studenty publikoval také fundamentální práce z kvantové optiky, např. o kvazidistribucích ve fázovém prostoru. Ještě je třeba zmínit knihu *Optical Coherence and Quantum Optics* (Cambridge University Press, 1995) napsanou spolu s Leonardem Mandelem, která podává nejrozsáhlejší a velmi detailní přehled problematiky.

Profesor Emil Wolf obdržel velkou řadu mezinárodních cen a zahraničních vyznamenání. Zlaté medaile obdržel také v roce 1991 od Palackého univerzity, ČSAV a JČMF a v roce 1992 se stal čestných doktorem Palackého univerzity. Jako člen Klubu přátel UP podporoval studenty optiky na UP. Byl také zahraničním členem Učené společnosti ČR.

Ve sborníku symposia *Tribute to Emil Wolf*, které organizoval v San Diego v roce 2003 jeho žák Tomasz Jannson, je jedna kapitola s názvem *Emil Wolf and Optics in the Czech Republic* (SPIE Press 2005, editor T. Jannson), která připomíná vliv prof. Wolfa na naši práci.

Takže závěrem lze konstatovat, že založení a rozvoj optických pracovišť v Olomouci je svázán se jmény profesora Bedřicha Havelky a profesora Emila Wolfa a aktivní pracovníci v optice v Olomouci jim vyjadřují hlubokou vděčnost.

prof. RNDr. Jan Peřina, DrSc.,
katedra optiky a Společná laboratoř optiky PŘF UP