Call for Papers
Mikulášská kryptobesídka

2. – 3. 9. 2021, Praha
https://mkb.tns.cz

Základní informace

S ohledem na COVID-19 proběhne jubilejní 20. ročník workshopu Mikulášská kryptobesídka jako spojená akce pro roky 2020 a 2021. Akce je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *2. září* a (b) půldne prezentací příspěvků a diskusí v pátek *3. září 2021*. Pro workshop jsou domluveny zvané příspěvky od:

- Bernhard Esslinger, Univ. Siegen, Německo – o projektu CrypTool.
- Gregor Leander, Ruhr Univ. Bochum, Německo – k aktuálnímu vývoji symetrické kryptografie.
- Miloslav Dušek, Univ. Palackého Olomouc, ČR – k aktuálnímu vývoji kvantové kryptologie.
- Otokar Grošek, STU v Bratislave, Slovensko – na téma (ne)náhodnosti.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: https://mkb.tns.cz.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž se zajímavými finančními odměnami pro finalisty) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: https://mkb.tns.cz. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a tak, aby přišly nejpozději do *31. května 2021*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2020/21 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny programovým výborem workshopu a autoři budou informováni o přijetí/odmítnutí do *29. června*. Příspěvek pro sborník workshopu pak musí být dodán do *19. července*.

Důležité termíny

Návrhy příspěvků:	31. května 2021
Oznámení o přijetí/odmítnutí:	29. června 2021
Příspěvky pro sborník:	19. července 2021
Konání MKB 2021:	2. – 3. 9. 2021

Programový výbor

Peter Gaži, IOHK Research, SR
Jan Hajný, FEKT VUT v Brně, CZ
Vašek Matyáš, FI MU, Brno, CZ – předseda
Bohuslav Rudolf, NÚKIB & MFF UK, Praha, CZ
Martin Stanek, UK, Bratislava, SR
Petr Švenda, FI MU, Brno, CZ