

## Call for Papers Mikulášská kryptobesídka

7. – 8. prosince nebo září (rozhodne se 1. 5.) 2023, Praha  
<https://mkb.tns.cz>

### Základní informace

S ohledem na COVID-19 se až 1. 5. rozhodne, zda proběhne i 22. ročník workshopu Mikulášská kryptobesídka na konci léta 2023 nebo v prosinci. 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 7.?. a (b) půldne prezentací příspěvků a diskusí v pátek 8.?. 2023. Pro workshop jsou domluveny zvané příspěvky od:

- Stephan Krenn, Austrian Institute of Technology, Rakousko,
- Florian Fröwis, ID Quantique, Rakousko,
- Lejla Batina, Radboud University Nijmegen, Nizozemí,
- Ján Jančár & Adam Janovský, FI MU, ČR,
- Bohuslav Rudolf, NÚKIB & MFF UK, ČR.

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 22. května 2023. Pro podávání příspěvků prosím použijte adresu matyas.ZAVINAC@fi.muni.cz a do předmětu zprávy uveďte „MKB 2023 – návrh příspěvku“. 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 19. června. Příspěvek pro sborník workshopu pak musí být dodán do 19. července.

### Důležité termíny

Návrhy příspěvků: 22. května 2023  
Oznámení o přijetí/odmítnutí: 19. června 2023  
Příspěvky pro sborník: 19. července 2023  
Konání MKB 2023: 7.-8. prosince nebo září 2023



### Programový výbor

Peter Gaži, IOG Research, SR  
Jan Hajný, FEKT VUT v Brně, CZ  
Ivan Homoliak, FIT VUT v Brně, CZ  
Vašek Matyáš, FI MU, CZ – předseda  
Bohuslav Rudolf, NÚKIB & MFF UK, CZ

Martin Stanek, UK, Bratislava, SR  
Adolf Středa, MFF UK, CZ  
Marek Sýs, FI MU, Brno, CZ  
Petr Švenda, FI MU, Brno, CZ