

## Call for Papers Mikulášská kryptobesídka

4. – 5. prosince 2025, Praha  
<https://mkb.tns.cz>

### Základní informace

Letos se uskuteční 24. ročník workshopu Mikulášská kryptobesídka. 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 4. 12. a (b) půldne prezentací příspěvků a diskusí v pátek 5. 12. 2025. Pro workshop jsou domluveny zvané příspěvky od:

- Peeter Laud, Cybernetica, Estonsko: Efficient Two-Party ML-DSA Protocol.
- Lenka Mareková & Kenny Paterson, ETH Zurich, CH: Four Attacks and a Proof for Telegram.
- Vadim Lyubashevsky, IBM Research, CH: On lattice cryptography or zero-knowledge.
- Tomáš Sušánka, Trezor, ČR: On practical deployment of cryptographic systems.
- Tomas Rosa, Raiffeisenbank & MFF UK, ČR: Elektronické útoky v terénu rozhraní PC - modely a zneužití.
- Marek Sýs, FI MU, Brno, ČR: Lattice-based attacks and cryptography.

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 přes www stránky workshopu: <https://mkb.tns.cz>. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu PDF a tak, aby přišly nejpozději do 27. června 2025. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2025 – 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 27. srpna. Příspěvek pro sborník workshopu pak musí být dodán do 30. září.

### Důležité termíny

|                               |                     |
|-------------------------------|---------------------|
| Návrhy příspěvků:             | 27. června 2025     |
| Oznámení o přijetí/odmítnutí: | 27. srpna 2025      |
| Příspěvky pro sborník:        | 30. září 2025       |
| Konání MKB 2025:              | 4.-5. prosince 2025 |

### Programový výbor

Peter Gaži, IOG Research, SR  
Jan Hajný, FEKT VUT v Brně, ČR  
Vašek Matyáš, FI MU, ČR – předseda  
Tomáš Rabas, NÚKIB, ČR

Martin Stanek, UK, Bratislava, SR  
Adolf Středa, MFF UK, ČR  
Petr Švenda, FI MU, Brno, ČR

