

## Call for Papers Mikulášská kryptobesídka

30. 11. – 1. 12. 2017, Praha  
<http://mkb.tns.cz>

### Základní informace

Letos proběhne už 17. 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 30. listopadu a (b) půldne prezentací příspěvků a diskusí v pátek 1. prosince 2017. Pro workshop jsou domluveny zvané příspěvky od:

- Mike Just, Heriot-Watt University, Skotsko.
- Timo Kasper, Německo.
- Juraj Somorovsky, Ruhr-Universität Bochum, Německo.
- Pavel Vondruška, CETIN & MFF UK, ČR.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: <http://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: <http://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 28. září 2017. Pro podávání příspěvků prosím použijte adresu matyas.ZAVINAC@fi.muni.cz a do předmětu zprávy uveďte „MKB 2017 – návrh příspěvku“. Přijem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do 30. října. Příspěvek pro sborník workshopu pak musí být dodán do 13. listopadu.

### Důležité termíny

Návrhy příspěvků:	28. září 2017
Oznámení o přijetí/odmítnutí:	30. října 2017
Příspěvky pro sborník:	13. listopadu 2017
Konání MKB 2017:	30. 11. – 1. 12. 2017



### Programový výbor

Peter Gaži, IOHK Research, Čína  
Michal Hojsík, Honeywell & MFF UK, Praha, CZ  
Vašek Matyáš, FI MU, Brno, CZ – předseda

Tomáš Rosa, Raiffeisenbank a MFF UK, CZ  
Bohuslav Rudolf, NBÚ & MFF UK, Praha, CZ  
Petr Švenda, FI MU, Brno, CZ