UNIVERZITET U SARAJEVU -
ELEKTROTEHNIČKI FAKULTET
S a r a j e v o
Zmaja od Bosne bb

Na osnovu čl. 5. i 6. Odluke Vijeća Univerziteta u Sarajevu - Elektrotehničkog fakulteta o definiranju procedure realizacije naučnoistraživačkih seminara na trećem ciklusu studija – doktorskom studiju (broj: 01-503/21 od 01.02.2021. godine) i Odluke Vijeća Univerziteta u Sarajevu - Elektrotehničkog fakulteta (broj: 01-53/24 od 08.01.2024. godine), Univerzitet u Sarajevu - Elektrotehnički fakultet, daje

O B A V I J E S T
o odbrani seminara

Student trećeg ciklusa studija - doktorskog studija, Emir Dervišević, magistar elektrotehnike - diplomirani inženjer elektrotehnike, branit će Naučnoistraživački seminar 2.1, pod naslovom "Izbor baza sa pseudo-slučajnim funkcijama u BB84 protokolu" (naziv na engleskom jeziku: "Bases Selection with Pseudo-Random Functions in BB84 Scheme)".

Seminar je izrađen u saradnji sa akademskim savjetnikom, dr. Miralemom Mehićem, vanrednim profesorom Univerziteta u Sarajevu - Elektrotehničkog fakulteta.

Odbrana seminara, održat će se 1. februara 2024. godine (četvrtak), s početkom u 9:00 sati, u prostorijama Univerziteta u Sarajevu - Elektrotehničkog fakulteta (sala 3-46 - BitLab, treći sprat).

Odbrana seminara je javna.

Obavijest o odbrani i sažetak seminara, oglašavaju se na oglasnim pločama i internet stranici Univerziteta u Sarajevu - Elektrotehničkog fakulteta.

Oglašeno:
Sarajevo, 19.01.2024. godine

UNIVERZITET U SARAJEVU ELEKTROTEHNIČKI FAKULTET

Naučnoistraživački seminar 2.1

Student:
Emir Dervišević, magistar elektrotehnike – diplomirani inženjer elektrotehnike

Akademski savjetnik:
Prof. dr. Miralem Mehić

" Izbor baza sa pesudo-slučanim funkcijama u BB84 protokolu" (eng. "Bases Selection with Pseudo-Random Functions in BB84 Scheme")

SAŽETAK/ABSTRACT

Bosanski jezik:
Budući da se spektar usluga dostupnih u modernim telekomunikacijskim mrežama neprestano širi, sigurnost postaje sve važnija. Istovremeno, u eri konstantnog napretka matematike i računarstva, sigurnost postojećih kriptografskih rješenja postaje upitna. Kvantna distribucija kriptografskih ključeva (engl. *Quantum Key Distribution*, QKD) je obećavajuća tehnologija razmjene tajnih kriptografskih ključeva koja omogućuje dugo očekivanu praktičnu Informacijsko-Teorijsko Sigurnu (ITS) komunikaciju. Stopa generisanja ključeva, međutim, jedno je od ograničenja njene raširene primjene za osiguranje protoka podataka visoke propusnosti. Ovaj rad adresira gore pomenuto ograničenje primjenom savršeno korelisanog odabira baza koji je definisan izlazom pseudo-slučajnih funkcija temeljenih na primjeni autentifikacijskih kodova uz funkciju za izračun sažetka s ključem (engl. *keyed-Hash Message Authentication Code*, HMAC). U teoriji, predložena varijanta BB84 protokola je odlikovana ITS sigurnošću, smanjuje zahtjev za memorijom i smanjuje intenzitet komunikacije tokom faze naknadne obrade. Može se primijeniti u QKD mrežama s ciljem povećanja kapaciteta i prilagođavanjem korisnicima različitih sigurnosnih potreba.

Engleski jezik:
Because the spectrum of services available in modern telecommunication networks is constantly expanding, security has become increasingly important. Simultaneously, in an era of constant progress in mathematics and computing, the security of existing cryptographic solutions becomes questionable. Quantum Key Distribution (QKD) is a promising secret key agreement primitive that enables long-awaited practical Information-Theoretical Secure (ITS) communications. The key generation rate, however, is one of the limitations of its widespread application to secure high throughput data flows. This paper addresses the aforementioned limitation by employing perfectly correlated bases selection defined by the output of Pseudo-Random Functions based on the keyed-Hash Message Authentication Code construction. In theory, the proposed variant of the BB84 scheme is ITS, reduces memory requirements, and reduces communication overhead during the post-processing stage. It can benefit QKD networks as a service by increasing capacity and accommodating users with varying security needs.