

第 3 弾

ICT リテラシー強化講習会

An Introduction to Public Key Cryptography

(暗号理論入門)

The lecture will include elliptic curves (Elliptic Curve Diffie-Hellman key agreement and Elliptic Curve Digital Signature Algorithm) and some implementation issues (bases in the characteristic 2 finite fields), cryptographic protocols and finally some specific applications.

講 師 Aleksandar Jurisic 教授 (University of Ljubljana, Slovenia)

日 程 11 月 16 日 (木) 15:30 - 17:00

11 月 30 日 (木) 15:30 - 17:00

場 所 東北大学大学院情報科学研究科大講義室

対 象 情報科学研究科の教員

情報科学研究科・工学研究科・理学研究科の大学院生

問合せ先

情報科学研究科情報基礎科学専攻

宗政 昭弘 munemasa@math.is.tohoku.ac.jp

先進的 ICT リテラシー強化教育プログラム実行委員会