عنوان مقاله:
Computing Root Modulo a composite

محل انتشار:
سومین کنفرانس انجمن رمز ایران (سال: 1384)

تعداد صفحات اصل مقاله: 6

نویسندگان:
Koshiar Azimian - *Electronic Research Center, Sharif University of Technology, Department of Computer Engineering, Sharif University of Technology*

Ali Bagherzandi - *Department of Computer Engineering, Sharif University of Technology*

Javad Mohajeri - *Electronic Research Center, Sharif University of Technology*

Mahmoud Salmasizadeh - *Electronic Research Center, Sharif University of Technology*

خلاصه مقاله:
In this paper, we introduce a new computational problem and show that solving this problem is no easier than Factoring. As will be discussed, this new computational problem can be used to construct a new public key encryption scheme. The new public key encryption scheme will be provably secure, based on intractability of factoring problem.

کلمات کلیدی:
Public-key cryptography, computational complexity, computational number theory, factoring problem

لینک ثابت مقاله در پایگاه سیویلیکا: