Yang, Leixin; Du, Weizhang

Niederreiter public-key cryptosystem based on QC-LDPC. (Chinese. English summary)

Zbl 1219.94084  

Summary: A Niederreiter public-key cryptosystem based on QC-LDPC codes was proposed. As the check matrix of QC-LDPC codes is sparse, and has the structure of circulative blocks and high error correction capability, compared with other public-key cryptosystem, the key sizes of the new cryptosystem is reduced and transmission rate is improved. A new parity-check matrix was mapped by invertible transformation matrix $Q$ with diagonal form. The sparse characteristic of $H'$ is countraveled. Through analyzing existing attacking methods, the security of the cryptosystem is confirmed to be improved.

MSC:

94A62 Authentication, digital signatures and secret sharing  
68P25 Data encryption (aspects in computer science)

Keywords:

low-density parity-check (LDPC) codes; QC-LDPC codes; quasi-cyclic low-density parity-check (QC-LDPC); cyclic matrices; Niederreiter public-key cryptosystem; security analysis

Full Text: DOI