Summary: Cryptographic systems are derived using units in group rings. Combinations of types of units in group rings give units not of any particular type. This includes cases of taking powers of units and products of such powers and adds the complexity of the discrete logarithm problem to the system.

The method enables encryption and (error-correcting) coding to be combined within one system.

These group ring cryptographic systems may be combined in a neat way with existing cryptographic systems, such as RSA, and a combination has the combined strength of both systems.

Examples are given.

MSC:

94A60 Cryptography
20C05 Group rings of finite groups and their modules (group-theoretic aspects)

Keywords:
group ring; units in group rings; public key cryptography; coding

Full Text: Link arXiv