姓　名：黄华伟

职　称：副教授

邮　箱：hwhuang7809@163.com

基本情况

黄华伟，男，江西樟树人，1978 年 9 月生，工学博士，现为贵州师范大学数学科学学院副教授，硕士生导师。

研究方向

代数学、密码学与信息安全、学科教学（数学）

开设课程

基础代数、密码学基础、有限域及其应用

教育经历

1. 2004-09 至 2008-06，西安电子科技大学，密码学专业，博士
2. 2001-09 至 2004-06，江西师范大学，基础数学专业，硕士
3. 1997-09 至 2001-06，江西师范大学，数学教育专业，学士

工作经历

1. 2014-01 至现在，　贵州师范大学，数学科学学院，副教授
2. 2013-07 至 2013-12，贵州师范大学，数学与计算机科学学院，讲师
3. 2009-01 至 2013-06，华南农业大学，信息学院，讲师
4. 2008-07 至 2008-12，华南农业大学，信息学院，助教

科研成果

(1) **Huawei Huang** , Lunzhi Deng, Yunyun Qu, Chunhua Li. Zero-knowledge identification scheme with companion matrices of primitive polynomials. International Journal of Embedded Systems 12(2): 216-225, 2020.

(2) **Huang Huawei**, Deng Lunzhi, Li Chunhua, Pan Chunhua. Cryptanalysis of an Encryption Scheme Using Matrices over Finite Fields. Chinese Journal of Electronics. Vol. 27, No. 2: 292-296, 2018.

(3) **Huawei Huang**, Yunyun Qu, Lunzhi Deng. Zero-Knowledge Identification Scheme Based on Symmetry Ergodic Matrices Exponentiation Problem. ICCSP '17: Proceedings of the 2017 International Conference on Cryptography, Security and Privacy，2017, 71-75.

(4) **Huawei Huang**, Lunzhi Deng, Yunyun Qu, Chunhua Li. The structure of certain F-abundant semigroups. Journal of Discrete Mathematical Sciences and Cryptography. Vol. 19(5&6): 1041-1051，2016.

(5) **Huawei Huang**, Chunhua Li. The structure of certain F-inverse semigroups. Journal of Discrete Mathematical Sciences and Cryptography. Vol. 18(4): 433-438，2015.

(6) **黄华伟**,彭长文,瞿云云,李春华.遍历矩阵密码体制的安全性. 通信学报, 2015,Vol. 36(8):61-67

(7) **Huawei Huang**, Changwen Peng. Companion matrix and recognition of primitive polynomial. Journal of Discrete Mathematical Sciences & Cryptography. Vol. 17(1): 39-48，2014.

(8) **黄华伟**，祝胜林，周敏. 基于 TEME 问题的公钥密码体制的密码分析, 通信学报， Vol 32 No.11A, p 174-177, 2011.

(9) **Huang Huawei**, Yang Bo, Zhu Shenling, Xiao Guozhen. Generalized ElGamal public key cryptosystem based on a new Diffie-Hellman problem. The second conference provable security- ProvSec 2008, Berlin: Springer-verlag, LNCS 5324, 2008, p. 1–21.

科研项目

1. 国家自然科学基金,地区项目，11661022,基于矩阵半群的公钥密码体制研究，项目批准号：61462016 ，2015/01-2018/12，40 万元，已结题，主持；

2. 贵州省科学技术基金项目，黔科合基础［2021]313，基于非交换环与半环的抗量子分析密码体制研究，2021/04-2024/04，10 万元，在研，主持；

2. 贵州省科学技术基金项目，黔科合基础［2014]2125，矩阵半群及其公钥密码体制研究，2014/08-2017/08，5.8 万元，已结题，主持；

获奖情况

荣获贵州师范大学自然科学类“2014 年度科研先进个人”。