工程成果	蓝牙加密算法的实时攻击
申请人	张斌
团队成员	
申请人自述	（请简述工程成果的目的和意义，解决了什么问题，有何贡献或影响，在何处应用，应用效果等。总字数不超过 1000 字，可附页） IEEE 802.15.1 规定的蓝牙标准采纳二级流密码 E0 来保护无线网络短距离通信的机密性。目前最好的攻击结果是 2005 年美密会上公布的条件相关攻击，给定 2^23.8 帧密钥流的头 24 个比特，可以在 2^38 离线复杂度、2^38 在线复杂度和 2^33 存储 （实际大约相当于 19 小时， 37 小时和 64GB） 内恢复密钥。本文对该算法进行了深入分析，发现了大量新的相关性，基于一种新的密码分析技术—条件掩码，给出了更致命且实时的攻击。我们的分析表明，给定 2^22.7 帧密钥流的头 24 个比特，可以在 2^22.1 离线复杂度、2^27 在线复杂度和 4MB 存储的条件下恢复密钥。我们的攻击进行了完整的计算机实验，只需几秒钟就可以恢复出密钥。这是目前为止对实际蓝牙加密体制的最好已知明文攻击。