一直对意大利的学术很少接触，通信与密码学同行加拿大滑铁卢大学的龚光教授，也是 eSTREAM 算法 WG 的设计者之一，在意大利进行过学术研究。整理 09 年下载在个人电脑里的资料时，发现了意大利 08 年的未来互联网的在线资料。按照我的耐心和细致程度，这个方向应该对美国的一些技术结论进行关注，因为在中国做研究，有用的报告是可以按图索骥式的购买指南，即使有创新的技术也没有实现的环境。但是，出于对龚光教授的尊敬，进行了阅读并且注记。不可否认，欧洲的基础研究确实非常先进，在技术融合、涉及到网络与计算机应用的层面，美国走在前沿。本文结论部分有关于 T2T 中 RFID 的安全技术建议。对特定部分有研究兴趣可以到互联网上开放获取。

清华大学自动化学院[1]，网络与分组密码智能应用实验室[2] 罗岚 博士后[1]，教授[2]

秋天、2010

这几天成都的雨下得很大，雨水大得可以洗车。旁边的一条小河比平时的水流大了很多，水面离河堤还有大约还有两米。如果雨下到与河堤持平，成都可能就被水灾了。

如需讨论，请联系 lanneverlose@gmail.com

互联世界、人工智能和 RFID 的交叉应用研究

——2008 年意大利罗马大学 RFIDays Internal Report RR-08- 69 注记

这部 IEEE ITALY 系列出版物“RFID 的融合技术”研究报告 RR-08-69 在互联网上可以开放获取，由意大利罗马大学信息科学与技术系 G. Marrocco 编辑。一百多页的报告在交叉应用研究上有独到的见解，包括在未来互联网之真实世界网络的背景下对 RFID 传统的读、写技术、面向传感应用的整合以及有关电磁的硬件创新设计与分析技术；分布系统部分，对 RFID、智能应用技术、从静态到适时的互联世界、移动通信和安全方面的交叉研究。报告的赞助商：IBM、Microsoft、RadioLabs、Reply、CAENRFID、ELSAG DATAMAT。

一、RFID 阅读器和标签技术

在这份 IEEE ITALY 研究报告里，Siena 大学的 Alberto Toccafondi, Cristian Della Giovampaola, 和 Paolo Bra 在文章“面向 RFID 应用的 UHF-HF 整合传送”里把 UHF 迂回偶极天线和 ISO 15693 商业标签整合在一张 ISO 7810 ID-1 卡上两个独立的不同方向上；UHF 迂回偶极天线在设计时考虑了目前的 HF 天线的旋转设计。为了允许更好的控制电阻输入，特别使用了三个 EM 连接载荷条形码。可以看到天线的几何参数，例如载荷条形码空间、宽度和迂回步数在天线和 UHF 标签芯片之间获得一个非常好的结合匹配。他们的仿真测试结果是获得了一个非常优秀的整合传送 UHF 阅读器。罗马大学 Acustica O.M.Corbino 研究所的 M. Benetti, D. Cannatà, F. Di Pietrantonio, E. Verona 文章是“基于表面声波设备的 RFID 和无线传感器评价”，主要介绍了 SAW ID-标签的多种用途。罗马大学 Gaetano Marrocco 的“面向传感的 UHF-RFID 标签”，介绍了专门传感应用的 UHF 标签设计，通过计算机仿真实验和模型的构造测量证明了主传感和附加电子设备之间的被动传感目标特征。Florence 大学 Guido Biffi Gentili, Claudio Salvador 写的“一种新的多样完全活动 RFID 系统”。INTEL 公司的 Issy Kipnis, Scott Chiu, Marc Loyer 写的“一个 900MHz 的 UHF RFID 阅读 IC 接收器”。 Antennas 和 EMC 实验室 Mario Orefice, Gianluca Dassano 写的“一个 UHF 可控定向阅读天线”。 Carmine Piersanti†, Franco Fuschini*, Francesco Paolazzi‡, Vittorio Degli-Esposti†, Gabriele Falciasecca†写的“RFID 链接的电磁分析”，讨论了真实环境影响下，例如电磁连接、多路传播，在差错率和接收动力的系统实现下，给出一些阅读器和接收者之间的相关效果。

二、基于分布系统的交叉应用研究

罗马大学 Franco Mazzenga 和 RadioLabs 的 Marco Vari 写的“基于主动和被动设备的室内定位技术”是一个关于室内定位无线技术的简单综述，基于网络的被动 RFID 使用一些系统参数，例如 RFID 的稠密度，在定位准确度和成本方面给出了合适的实现。Modena e Reggio Emilia 大学的 Marco Mamei, Franco Zambonelli 文章是“RFID 标签的游动智能”，分部代理/机器人在物理环境下的定位探测相关活动的系统开发数量被极度限制，这篇文章基于真实世界、低成本和普通目的，通过实际使用 RFID 标签技术进行信息界面实现。人/机器人在我们通常的环境下可以通过适当的 RFID 标签读写扩散/感知。通过允许目标扩散信息踪迹而且允许随后的追踪，人/机器人对遗忘在某处的目标进行追踪的应用进行测试和评估。文章列出了几种评估经验、限制和更进一步的应用。Superiore Mario Boella 研究所 Fabio Forno,

Antonio Sciarappa 写的“互联世界里的 RFID：从静态到适时”，从使用静态索引的被动标签 RFID 应用到支持新技术的无处不在通信、普适计算机和智能环境的动态应用。这个概念面向网络设备、大数量智能目标具体连接到互联世界。这篇文章指出了处理异构和动态技术的目前中间件的限制，然后介绍了一种建立在顶层适时通信协议覆盖网，整合和联合目标网络的新颖方法。罗马大学 RFID Lab 的 U. Biader Ceipidor, C. M. Medaglia, A. Moroni, G. Orlandi, S. Sposato 的文章“NFC：在 RFID 和移动之间的整合，现状和未来”。这篇文章描述了近距通信（Near Field Communication，NFC）一个小范围，基于标准无线连接的 RFID 技术，产生一个在欧洲称为 StoLPaN 研究的项目，基于标准环境的 NFC 生态系统的重要。degli Studi di Roma “Tor Vergata”大学的 Gianluigi Me, Giuseppe F 写的“RFID 安全”，针对 RFID 密码 KEELOQ 的攻击，这项工作在开放获取的“**密码学 2008 国际会议综述**”介绍了。Politechico di Torino，自动化与信息系的 C.Demartini, F.Gandino, B.Montrucchio,M.Rebaudengo, E.R.Sanchez 的文章“农业食品策略的 RFID：认证、完整和私密的方法”，安全算法使用 RSA 类型的密码系统提高安全，同时适合在 PDA 上使用。欧洲专利办公室的 Maurizio Ricciardi 在附录里有一篇文章，“RFID 的专利评价”。

三、结论

以前在研究中间件、RFID、传感网络的分组密码算法智能应用时，没有站在未来互联网的高度。下一代互联网关注度主要放在了 INTERNET 的扩容、结构和相关服务的应用研究上，未来互联网为了互联一切，融合了真实世界网络和网络结构，同时，进行了网络和服务的研究和整合。从有线到无线，从 INTERNET 到互联一切，未来互联网络更远的目标也许是想涵盖所有通信手段和世界。博士论文“分组密码算法设计与评估应用研究”（同样可以在线获取）在 4.5.2 节对 T2T 通信里使用的 RFID 相关安全技术做了研究，这篇博士论文建议未来互联网从 E2E 升级到 T2T 时，模仿全球银行的做法----“分组密码无处不在”，在所有需要使用安全技术的环节，使用分组密码算法的不同模式。时间同样验证了：在不同级别使用分组密码即使是金融环境都可以足够安全。这种方式应该可以推广到 RFID 在互联一切的安全技术里，灵活、智能的应用为不同环境预留了不同的接口。

参考文献：

Gaetano Marrocco Editor, Jointly organized by University of Roma “Tor Vergata” CNIPA IEEE – Italy Section Workshop on Emerging Technologies for Radio-frequency Identification，Book of Proceedings, June, 2008