太田（和）·崎山研究室

太田 和夫
Kazuo OHTA

崎山 一男
Kazuo SAKIYAMA

研究课题 采用基于数学理论的自顶向下法、来自实装的自底向上法来综合研究密码系统

关键词 密码理论，密码系统，公钥密码，密钥密码，安全性证明，边频攻击，嵌入式密码 LSI，散列函数，安全系统

所属专业	研究生院信息理工学研究科　综合信息学专业
研究成员	太田 和夫 教授，崎山 一男 教授，岩本 贡 特任助教
所属学会	电子信息通信学会，信息处理学会，IACR、IEEE Information Theory Society Membership
研究设备	用于密码程序开发·实验的「FPGA 板」，各种测试设备「示波器、逻辑分析仪」，开放性实验室 1 间（73m²），密码理论的基本文献 300 册（其中多数有历史价值），FPGA 板

研究概要

数据交换的安全性及散列函数的评价

互联网上数据交换频繁活跃的今天，为了避免数据被别人偷看，就要确保其安全性，并且还必须验证这些数据是否由本人所写，因此密码就成为很重要的东西。我们的世界本来就存在很多密码，而且还在不断地产生新密码，其中就会有一些未显示安全性的密码或者令人担忧的会泄漏信息的安装方法。

如果大家都普遍使用没有经过安全验证的密码，就会产生非常严重的问题，因此该研究室在发生该问题之前，从「理论」和「安装」两个角度来评价其安全性。

用于显示密码技术安全性的基本工具是计算复杂性理论。事实证明，破解某个密码或散列函数，其难度相当于解一个很难的数学题（比如素数分解），如果素数分解不能被解开，那么就能保证其密码技术的安全性（安全性证明技法）。

边频攻击的对策研究

最近该研究室通过收集装置泄漏的电磁波及耗电量等信息，表明能够推断在密码处理中使用的秘密信息（边频攻击）。迄今为止，比起研究人员在考虑安全性理论时所设想的情况，现实中的攻击者更能利用大量的信息进行攻击。

针对边频攻击确立安全的密码系统安装法，是该研究室追究的重要课题。

为了在出现更强大的攻击者时也能保证密码的安全性，他们还在努力钻研如何扩展、充实已确立的安全性证明技法，使其能够抵抗边频攻击。

特别是以 IC 卡这种嵌入式用途为主要研究对象，除了以前在开发嵌入式系统时所重视的高效化的性价比之外，他们还针对边频攻击等一系列尝试获取秘密信息的各种攻击，着手研究如何增强它的抗攻击能力。

人材培养、咨询

该研究室对人材培养也非常积极，根据企业需求，接受企业员工进行培训等。比如企业能够制造电子结算系统，但却没有人才来确保数据实际交换时的安全性，他们就可以为企业培养这样的人才。

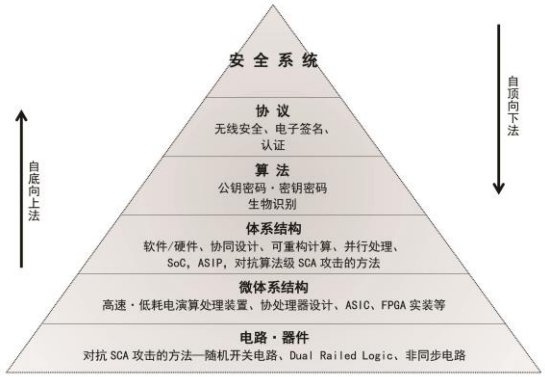
到目前为止，该研究室既接受来自大型电子厂商、通信企业的员工作为博士课程的学生，又派送毕业生到企业进行实践，通过这样的方式确立了教育程序，同时也接受企业的咨询业务。

太田教授在 NTT 研究所、美国密码研究中心的马萨诸塞州工科大学（MIT），一方面推进可证明安全性的理论研究，另一方面在电子货币、电子投标等项目开发上具有丰富的经验。

崎山副教授在日立半导体事业部 3G（第 3 代）手机系统的 LSI 开发、欧洲密码研究中心-比利时王立鲁汶大学（KUL）中，在研究抗边频攻击的密码安装法上有很丰富的经验。

安全系统的研究开发

该研究室采用自顶向下法（太田教授）、自底向上法（崎山副教授）来推进安全系统的研究开发，以这些经验为基础，他们能够为企业提出有效的建议。再进一步提供确保安全性的详细技术，比如密码长度是多少，抗边频攻击较强的密码产品是哪一个等这类信息也是他们咨询业务的内容。



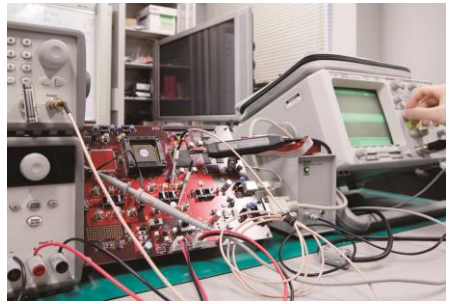
安全系统的层结构和研究方法

优　势

培养通晓从密码安全性概念·理论到安全系统安装法的人才

没有研究室在教授密码时会追溯到安全性的概念、理论上来。该研究室通过基于数学理论的分析，希望培养出人才，能够证明为什么这是安全的。

此外他们还试图培养能够运用硬件、软件来构建和安装具有抗攻击性的安全系统的人才。他们的优势就是不断培养出能够证明系统安全性，且能向让任何人解说清楚的人才。


使用 SASEBO 板的安全性评价环境

未来展望

和企业共同研究安全有效的散列函数

到目前为止，该研究室将重点放在安全性理论上进行了研究。因为主干部分非常扎实，所以今后会考虑在枝干部分，也就是在理论应用领域展开研究。比如安全有效的散列函数的设计。导入日益高级化的信息化社会的安全系统也是因为能耐用的新散列函数的需求非常大。

再举一例，就是研究在不久的将来，有望作为识别标签来替换条形码的电子标签「RFID」安装法。如果不能低成本制作电子标签，电子标签就不可能普及，因此使用高价公钥就比较困难。但是仅用廉价的技术，理论上从安装层面又不能确保其高度的安全性。该研究室权衡成本和安全性之间的平衡点，意欲挑战在何处取舍等与电子标签相关的模型制作。

在任何场合都并不是仅用安全性理论来解决的问题。必须要将企业对于成本和安全性的立场考虑进去，摸索和企业进行共同研究的方法。

如今除了用互联网来交换庞大的重要数据和个人信息外，也可以用 IC 卡、手机来付费及交易，因此安全问题就被进一步放大。如今的社会，如果有人存有恶意，就有可能用有线龙头去盗取别人的信息。遇到这样的社会形势，寄予该研究室的期望与所担当的任务应该会越来越大。