加密工程：

在硬件和嵌入式软件中植入高速和安全的加密系统

Cryptographic Engineering:

High-Speed and Secure Implementations of Cryptosystems

in Hardware and Embedded Software

概要
General overview

这是关于密码系统的高速，节能和安全实施的短期课程，适用于小型和大型计算和通信系统。 本课程专为有意理解，建模、设计、开发、测试和验证加密软件和硬件的工程师而设计。我们涵盖了算法、方法和技术，以便使用通用平台和技术创建最先进的加密嵌入式软件和硬件。

This short course on high-speed, energy-efficient and secure implementations of cryptosystems, suitable for small and large computing and communication systems. This course is designed for engineers interested in understanding, modeling, designing, developing, testing, and validating cryptographic software and hardware. We cover algorithms, methods, and techniques in order to create state-of-art cryptographic embedded software and hardware using common platforms and technologies.

主办单位

上海微技术国际合作中心(SIMTAC)

中国科学院上海微系统与信息技术研究所

课程安排

课程时间：2016 年 11 月 17 日—18 日（2 天）

报到注册时间：2016 年 11 月 17 号，上午 8:30-9:00

课程地点：上海集成电路技术与促进中心 （浦东新区张东路 1388 号 21 栋 1 楼多功能厅）

课程费用

个人报名：3,600 元/人（含授课费、场地租赁费、资料费、课程期间午餐），学员交通、食宿等费用自理。（如需了解附近酒店协议价格信息，请联系 Grace：18516128250 ）；

优惠折扣：在校学生注册费用 2,500 元/人；

团体报名：4 人以上团体报名优惠可协商。

请各单位收到通知后，积极选派人员参加。

报名方式

1. 下载报名表

电子报名表：

请打开微信，扫描以下二维码，或点击 https://www.wenjuan.com/s/fyMF7j/ 跳转至报名表！

如需纸质报名表：也可点击 http://www.simtac.org/?p=858&lang=zh 下载

2. 提交填妥的报名表

- 个人报名者及学生报名者，请直接提交报名表。
- 4 人以上团体报名者，请直接联系 Grace

收到您提交的报名表后，我们会发送邮件回执。如未收到回执，请通过以下方式联系：

请在报名截止日前将报名注册表发送至邮箱: training@simtac.org

手机：18516128250 搜索此号码加微信。**暗号：加密**

3. 付款

请于 11 月 15 日前将全款汇至以下账户。付款请备注：（**加密工程+单位/学校+姓名**）

银行信息：

户　名：	上海新微科技服务有限公司
开户行：	中国银行上海市嘉定支行
帐　号：	442969968121

支付宝信息：

公司名称：上海新微科技服务有限公司

支付宝账号：pay@simtac.org

课程梗概
Outline of the Course

第一天（6 小时）/First Day (6h)

公钥密码和计算要求（3 小时）

标准化的公钥密码算法：Diffie-Hellman，RSA，ElGamal 和数字签名算法。 椭圆曲线 DSA 和椭圆曲线集成加密方案。部分同态公钥函数。公钥密码术的组和计算要求。

Public-Key Cryptography and Computational Requirements (3h)

Standardized public-key cryptographic algorithms: Diffie-Hellman, RSA, ElGamal, and Digital Signature Algorithm. Elliptic Curve DSA, and Elliptic Curve Integrated Encryption Scheme. Partially homomorphic public-key functions. Groups and

computational requirements of public-key cryptography.

有限域和算术算法（3 小时）

大数的算术。指数算法和加法和减法链。非相邻形式。蒙哥马利乘法。 GCD 和反演算法。整数环和 p 元素的伽罗瓦域 GF（p）。 字段元素的表示。多项式和正规基。在 GF（2 ^ k）中的加法和乘法运算。正规基和最佳正规基的性质。字段元素的反转。

Finite Fields and Arithmetic Algorithms (3h)

Arithmetic with large numbers. Exponentiation algorithms and addition and subtraction chains. Non-adjacent forms. Montgomery multiplication. GCD and inversion algorithms. Integer rings and Galois fields of p elements, GF(p). Representation of field elements. Polynomial and normal bases. Addition and multiplication operations in GF(2^k). Properties of normal bases and optimal normal bases. Inversion of field elements.

第二天（6 小时）/Second Day (6h)

公钥密码术的硬件和软件实现（3 小时）

在嵌入式软件和硬件中实现组和字段操作，包括乘幂，标量乘法，场乘法和反转。高效硬件的统一算术。 PKC 的嵌入式软件实现原理。

Hardware and Software Implementations of Public-Key Cryptography (3h)

Implementing group and field operations in embedded software and hardware, including exponentiation, scalar multiplication, field multiplication and inversion. Unified arithmetic for efficient hardware. Principles of embedded software implementations of PKC.

侧信道攻击和对策（3 小时）

旁通道分析的基础。定时，电源和电磁攻击以及对策。高级旁通道分析技术。微架构攻击和对策。

Side-Channel Attacks and Countermeasures (3h)

Basics of side-channel analysis. Timing, power and electromagnetic attacks, and countermeasures. Advanced side-channel analysis techniques. Micro-architectural attacks and countermeasures.

演讲者简历/Speaker Biography

Çetin Kaya Koç

美国加利福尼亚大学圣塔芭芭拉分校博士学位、研究教授；
俄勒冈州立大学终身教授；
加密硬件和嵌入式系统(CHES)研讨会联合创始人；
密码工程杂志创始主编；
IEEE Fellow

Koç博士于1988年在美国加州大学圣巴巴拉分校获得电子与计算工程博士学位。他的研究兴趣是在电子投票、网络物理安全、加密硬件和嵌入式系统、椭圆曲线密码和有限域、以及确定性、混合和真随机数发生器。 Koç是加密硬件和嵌入式系统（CHES）研讨会的共同创始人。 CHES研讨会是最大的密码会议和首要论坛，致力于展示嵌入式系统的密码硬件和安全性的各个方面的科学进步。 Koç是“密码工程杂志”的创始主编，该杂志是CHES社区的官方杂志，涵盖CHES研讨会的研究领域。 Koç还是另外两个会议的共同创始人：国际有限域算术研讨会（WAIFI）和嵌入式系统的安全证明（PROOFS）。 WAIFI是一个工程师和数学家的论坛，他们感兴趣于有限域的高效软件和硬件实现。另一方面，PROOFS研讨会的目标是促进发展提高嵌入式系统安全性的方法，特别是那些包含加密机制的方法。

Koç曾在IEEE Transactions on Computers（2003-2008和2015-现在）和IEEE Transactions on Mobile Computing（2003-2007）的编辑委员会中工作。他是2003年4月和2008年11月的IEEE计算机交易的密码和密码分析硬件和嵌入式系统的客户联合编辑。此外，Koç自2016年3月起担任著名的国际计算机科学基础杂志的副主编。2007年，Koç因其对密码工程的贡献被选为IEEE Fellow。 Koç是三本书的合著者，分别是2007年，2009年和2014年由Springer出版的关于可重构硬件，密码学工程和数学和计算科学中的开放问题的密码算法。除了作为共同编辑贡献6次会议论文外，他还撰写或合作撰写了130多篇期刊和会议论文，11项美国专利和2项专利申请。 Koç成功指导了15博士学生和37硕士学生毕业，并指导了5名本科生的研究论文。他的博士学生中有10位目前是教授（2名在美国，1名在墨西哥， 7名在其他国家），剩下的学生则在全球高科技公司中工作。Koç历任休斯顿大学助理教授（1988-1992），俄勒冈州立大学助理教授、副教授和终身教授（1992-2007）。他在俄勒冈州立大学建立了信息安全实验室，并于2001年9月获得杰出和持续研究领导奖。目前，Koç是加州大学圣巴巴拉分校计算机科学系和创意研究学院的研究教授。

Dr. Koç* received his Ph.D. in Electrical & Computer Engineering from University of California Santa Barbara in 1988. His research interests are in electronic voting, cyber-physical security, cryptographic hardware and embedded systems, elliptic curve cryptography and finite fields, and deterministic, hybrid and true random number generators. Koç is the co-founder of the Workshop on Cryptographic Hardware and Embedded Systems (CHES). The CHES Workshop is the largest cryptography conference and the premier forum for presenting scientific advances in all aspects of cryptographic hardware and security of embedded systems. Koç is the founding

Editor-in-Chief of the Journal of Cryptographic Engineering, which is the official journal of the CHES community, covering research areas of the CHES Workshop. Koç is also co-founder of two other conferences: International Workshop on the Arithmetic of Finite Fields (WAIFI) and Security Proofs for Embedded Systems (PROOFS). WAIFI is a a forum of engineers and mathematicians interested in efficient software and hardware realizations of finite fields. On the other hand, the goal of the PROOFS workshop is to promote methodologies that increase the confidence level in the security of embedded systems, especially those that contain cryptographic mechanisms.

Koç has been in the editorial boards of IEEE Transactions on Computers (2003-2008 and 2015-now) and IEEE Transactions on Mobile Computing (2003-2007). He was a guest co-editor of April 2003 & November 2008 issues of the IEEE Transactions on Computers on cryptographic and cryptanalytic hardware and embedded systems. Furthermore, Koç is an Associate Editor of the prestigious International Journal of Foundations of Computer Science since March 2016. In 2007, Koç was elected as IEEE Fellow for his contributions to cryptographic engineering. Koç is the co-author of the three books Cryptographic Algorithms on Reconfigurable Hardware, Cryptographic Engineering, and Open Problems in Mathematics and Computational Science, published by Springer in 2007, 2009, and 2014, respectively. In addition to contributing to 6 conference proceedings as co-editor, he has also authored or co-authored more than 130 journal and conference papers, and 11 US patents and 2 applications. Koç has graduated 15 Ph.D. students and 37 M.S. students, and also directed research theses of 5 undergraduate students. 10 of his Ph.D. students are currently professors (2 in the US, 1 in Mexico, and 7 in other countries), the remaining work for global high-tech companies. Koç was an Assistant Professor at University of Houston (1988-1992), Assistant, Associate and Full Professor at Oregon State University (1992-2007). He established Information Security Laboratory at Oregon State University, and received Award for Outstanding and Sustained Research Leadership in September 2001. Currently, Koç is a research professor in the Department of Computer Science and the College of Creative Studies at University of California Santa Barbara.

上海新微科技服务有限公司

2016 年 10 月 18 日