超晶格密码的研究进展

童新海^{1,2}, 陈小明^{1,2*}, 徐述^{3*}

1. 中国科学技术大学信息科学技术学院, 合肥 230026;
2. 北京电子科技学院信息安全研究所, 北京 100070;
3. 北方信息技术研究所信息保障技术重点实验室, 北京 100072

* 联系人, E-mail: chenxmphd@besti.edu.cn; 18010005098@189.cn

现代密码学通过密码算法和密码协议将密码系统的安全性归结为密钥体系的安全性, 因此密钥管理是信息安全的基础工程, 其技术水平决定了整个密码系统的安全性和效益. 密钥的产生和分配一直是密钥管理中的瓶颈难题^[1](文献[1]中总结真实系统的十大安全威胁时说, 密钥无处可存, 现代计算装置不能安全地存储哪怕是微小的密钥). 采用基于物理实体的密码技术来产生和分发密钥以降低密钥管理风险、提升安全性, 是当前国际上信息安全技术发展的热点方向之一. 物理密码技术的典型代表有量子密钥分发技术和物理不可克隆函数(physical unclonable functions, PUF)技术. 其中, PUF具有使用方便、成本低、功耗省等特性. 美国和欧洲各国已经投入大量资金来研究和开发 PUF 及其在密码学和网络安全领域的应用技术(美国政府资助莱斯大学 3000 万美元开发 PUF 芯片, 作为认证锚应用于物联网).

超晶格是实现密钥产生和分发的一种新的类 PUF 技术, 其起源可以追溯到 1996 年 Zhang 等人^[2]在德国研究发现的半导体超晶格自发混沌现象. 他们发现液氮温区 GaAs/AlAs 超晶格在直流偏压作用下发生电流自发混沌振荡现象, 并预期这一现象能够作为一种理想的熵源来生产物理随机数. 2012 年 Huang 等人^[3,4]解决了室温下半导体超晶格量子共振隧穿难题, 实验观察到了超晶格室温自发混沌振荡以及超晶格器件间混沌同步等现象, 并以此为基础主导发明了基于超晶格的两大核心密钥管理新技术: 利用超晶格器件混沌振荡效应产生高质量物理随机数(密钥); 利用超晶格器件物理不可克隆孪生函数实现密钥的安全分发.

1 超晶格物理随机数技术

随机数是指 $\{0, 1\}$ 上的纯随机序列, 即 $\{0, 1\}$ 上独立同(均匀)分布的实验, 称为贝努利实验, 记为 i.i.d(independent identical distribution). 但随机数是一个数学定义, 从密码工程的角度来看, 随机数只是一种假设^[5](文献[5]指出: An ideal random number generator, however, is a fiction). 密码工程中通常使用数学采样方法和物理随机数装

陈小明 1996 年博士毕业于中国科学院软件研究所. 先后在中国科学院数学与系统科学研究院、北京电子技术研究所、北京信息科学技术研究院、北京电子科技学院从事密码理论和应用研究. 2015 年获国家技术发明奖, 2011 年获政府特殊津贴, 多次获密码科学技术进步奖. 主持过国家高技术研究发展计划、国家重点研发计划课题, 目前研究方向为密码学和计算理论.

徐述 北方信息技术研究所信息保障技术重点实验室研究员、中国科学院苏州纳米技术与纳米仿生研究所客座研究员、国家涉密信息系统密码应用与管理体系建设专家组成员、《密码与信息安全学报》编委、军事科学技术奖励评审委员会成员. 曾荣获总装备部与国防科工委联合颁发的高技术武器装备建设工程荣誉奖章, 国务院特殊津贴获得者, 第十三届全国政协委员.

置来产生随机数样本序列, 最常用的数学采样方法是伪随机数生成器, 但它的种子还是来源于物理随机数技术, 因此可以说密码工程中所使用的随机数都来源于物理随机数技术.

1.1 主要物理随机数技术

产生物理随机数的方法很多, 常用的有电路或电阻热噪声放大法(如 Intel 公司、Comscire 公司、瑞典 Protego 公司、中国科学院等研发的产品)、振荡器采样法(如复旦大学的产品)、混沌电路法(如清华大学、上海交通大学、浙江大学等的产品). 这些随机数技术受到物理熵源电子器件带宽的限制, 随机数产生速率均在 Mbit/s 量级(除非在

后处理阶段采用算法进行扩速,但这已经属于伪随机数技术了)。

为了研制更高速度的物理随机数发生装置,近年来日本 Takushoku University, 以色列 Bar-Ilan University 和中国太原理工大学、北京大学等研究基于混沌激光或者发光二极管的物理随机数技术,实现了 Gbit/s 甚至 Tbit/s 的物理随机数输出速度。但这些光电混合系统需要外部反馈,并进行电-光和光-电双重转换,系统复杂且对环境变化十分敏感,在实际应用中还存在诸多困难。

量子随机数发生器采用量子测量技术提取量子物理过程中的内禀熵输出随机数。典型的量子随机数发生器有如下几类。(1) 基于单光子探测技术的发生器。这类发生器的特点是需要使用单光子探测器来采样随机信号,从技术上可分为单光子路径区分方案、光子数路径纠缠方案、单光子时间分辨方案等。(2) 基于真空涨落的发生器。真空场涨落产生真空态散粒噪声,是性能优良的量子熵源,但真空态涨落信号很微弱,难以直接探测。(3) 基于自发辐射量子效应的发生器。当前量子随机数发生器的实用化面临的主要问题是发生器的体积仍然偏大,数据采集和后处理过程不能协同进行导致速度受限,量子随机数装置的量子特性的验证有困难(可以进行直接验证的方案速率不高)。

1.2 超晶格随机数技术

超晶格物理随机数技术是在我国学者原创性成果的基础上发展起来的纯电子学物理随机数技术,其发展历史漫长且曲折。为了研制固态高频微波振荡源,1970 年 IBM 公司的 Esaki 和 Tsu^[6]提出半导体超晶格的概念。超晶格由两种不同组元超薄层晶体以几到几十纳米厚度交替生长而成,两种超薄层晶体的结构需要严格匹配,使多层膜晶体仍然保持晶格完整性。超晶格在保持两种组成晶体性能的同时,形成了人工剪裁的周期性能带结构。超晶格的周期小于电子的德布罗意波长,具有一系列新的量子物理特性。1974 年 IBM 公司的科学家^[7]采用分子束外延(molecular beam epitaxy, MBE)方法成功制备出了半导体超晶格。超晶格结构具有其他半导体不具备的许多特征,是半个世纪以来半导体物理学和材料科学的重大突破。

根据 Esaki 和 Tsu^[6]理论预期的负微分电导效应和级联共振隧穿效应,1996 年 Zhang 等人^[2]发现在液氮和液氮温区,直流偏压下的 GaAs/AlAs 超晶格会发生电流自发混沌振荡。由于超晶格的混沌振荡只能在低温下实现,其应用研究长期停滞不前^[8]。为实现室温下超晶格的高频混沌振荡,人们进行了长达十多年的探索。Xia^[9]提出的 GaAs/AlAs 超晶格 Γ -X 谷间电子态混合理论否定了将 GaAs/AlAs 超晶格作为室温混沌振荡器件的构想。同时 Huang 等人^[3]据此理论分析认为,采用 $\text{Al}_{0.45}\text{Ga}_{0.55}\text{As}$ 作为超晶格势垒层既可消除漏电通道,又与 GaAs 的晶格常数严格匹配,可通过 MBE 设备生长出高质量的半导体超晶格 GaAs/

$\text{Al}_{0.45}\text{Ga}_{0.55}\text{As}$ 晶体材料,预期材料的非线性特性能够导致室温自发混沌振荡现象。2012 年他们采用这一技术路线生长出了 GaAs/ $\text{Al}_{0.45}\text{Ga}_{0.55}\text{As}$ 半导体超晶格(材料结构如图 1 所示),在随后的实验中观察到了预期的室温自发混沌振荡现象^[4],并以此为基础研制了物理随机数发生器芯片及板卡(图 2)。芯片工作温度范围大,最高可在 70°C 的环境温度下稳定工作,生产物理随机数的速度理论上可达 80 Gbits/s。这些成果发表在 *Physical Review Letter* 上^[10],在美国物理学会网站上有专题报道。自此,超晶格随机数技术得到国际同行的广泛关注。德国、西班牙、以色列、俄罗斯等国学者在超晶格随机振荡现象的物理机理分析和超晶格随机数在信息安全领域的应用两个方向进行了研究和探索^[11-14],这不仅为半导体超晶格与密码学的交叉融合发展开启了新篇章,也为超晶格密码的研究与发展奠定了良好的基础。

2 超晶格密钥分发技术

在研制出具有室温自发混沌振荡特性的半导体超晶格器件后, Li 等人^[4,15-19]又相继发现了超晶格的混沌控制与混沌同步特性、超晶格自发准周期振荡、相干共振和随机共振等物理现象,以及超晶格器件的物理单向函数特性。这些研究催生了一种新型的密钥管理技术——超晶格密钥分发技术。超晶格混沌同步现象保证了密钥分发功能的实现,超晶格的 PUF 特性保证了密钥分发的安全性。

2.1 物理不可克隆函数及其应用

借鉴人体生物特征(指纹和虹膜等)认证的思想, Papap^[20]于 2001 年提出利用硬件内在构造差异作为硬件标识的思想,并借此提出了物理不可克隆函数的概念。PUF 通过芯片制造过程中必然的工艺参数偏差或刻意引入的随

图1 半导体超晶格 GaAs/ $\text{Al}_{0.45}\text{Ga}_{0.55}\text{As}$ 材料结构示意图
Figure 1 Schematic diagram of the semiconductor superlattices GaAs/ $\text{Al}_{0.45}\text{Ga}_{0.55}\text{As}$

图2 超晶格物理随机数板卡

Figure 2 Random number generator based on superlattice devices

机因素实现挑战信号(输入)与响应信号(输出)之间的独特函数功能。从函数功能上看,同一设计方案和制造工艺下生产的每个 PUF 个体都是独特且不可克隆的,就像每个人的指纹或虹膜独特且不可克隆一样。此处的不可克隆包含物理不可克隆和数学不可克隆^[21],物理不可克隆指在材料的设计和生产工艺全部公开后,甚至连原制造者也无法复制以前生产的某个特定器件;数学不可克隆指不能通过器件的白盒和黑盒测试建模拟合器件的函数功能。关于数学和物理不可克隆方面的最新研究成果参考文献[22~24]。

PUF 器件具有 3 个关键特性^[21,25,26]: (1) 稳定性。同一 PUF 器件不同时刻接受同一挑战信号(输入)所产生的响应信号(输出)相同(少量差异可通过模糊提取技术来调同)。(2) 唯一性。同一设计和工艺下产生的两个具体 PUF 器件从函数功能的角度来看相关性很小甚至是统计独立的。(3) 不可预测性。对于一个具体的 PUF 器件,即使知道很多的输入输出对,也不能根据这些来预测一个不同于已知输入的新输入对应的输出。

PUF 概念的提出及其应用对密码学有革命性意义。PUF 理论将密码安全锚定在物理硬件的内禀安全因子上,这与现代密码学寓安全于密钥的思想有异曲同工之妙。PUF 将物理器件描述为由内禀安全因子决定的物理函数,与由密钥决定的具有特殊密码性质的数学函数在功能上相对应:理想的 PUF 类对应随机函数(类),一个具体的 PUF 器件对应随机函数的一个样本函数。PUF 思想的根本意图是将密码学中难以实现的随机函数(理想密码函数)用物理实体进行功能实现,打破了硬件仅仅是密码算法(数学)逻

辑的实现载体和密钥存储介质的旧观念,重新定义了硬件在密码学中的角色、地位和作用。因此,PUF 概念首次在 *Science* 上^[28]被提出后便得到了大量关注。*Journal of Cryptology* 也常出现 PUF 方面的论文^[29,30],在 *IEEE* 系列刊物中有关 PUF 研究的文献从每年几篇增长到 200 多篇^[25,31~35]。

PUF 比较成熟的应用主要有以下几个方向^[21,25,26]: (1) 充当伪随机函数或者 Hash 函数用于数据和实体认证。这是由 PUF 具有不可预测性导致的,理论上不可预测性蕴含伪随机性和单向性^[36]。(2) 作为随机数产生器用于密钥生产。由于 PUF 具有随机性,它可以用来产生随机数然后封装出各种密钥。(3) 作为密钥管理装置用于密钥分配。由于每个 PUF 器件唯一且不可克隆,在功能上相当于一个带“密钥”的密码算法(黑盒)。尽管合法使用方和攻击方都无法探测这个“密钥”,但拥有器件的一方可以排他性地使用黑盒功能从而实现密钥部署。(4) 作为防伪标识。PUF 器件的唯一性和不可克隆性使它天然具备防伪标识功能。上述应用目前都已有具体的芯片产品对应,例如 2013 年恩智浦的 SmartMX 安全微控制器就集成了名为 Intrinsic-ID 的 PUF 模块。

目前 PUF 的应用研究正在向纵深发展^[25,26],相应国际标准草案正在制订过程中^[37],基于 PUF 的密码算法和安全协议等正在成为新的研究方向^[26]。可以预见 PUF 对密码领域的影响将是全方位、多角度、可持续的。

2.2 超晶格物理不可克隆函数

Zhang 等人^[2]研究发明的混沌振荡超晶格芯片在特定

直流偏置下具有物理函数的特性: 输入信号会唯一且稳定地导出对应输出信号(其中微小波动可通过数据处理技术消除). 这一过程的电路结构如图 3 所示.

目前的实验和分析表明, 当输入信号小于某个阈值 a (或者为零) 时, 超晶格在直流偏压下发生电流自发混沌振荡, 这可以看成是物理函数的特殊形式; 当输入信号处于一定范围 $[a, b]$ 时, 输出是输入的随机函数(这里的随机是针对不同的器件而言的); 而当信号大于阈值 b 时, 器件被击穿, 其特质因素在输出输入关系中已经没有什么表现了. 超晶格的这些性质可以概括如下:

$$y(t) = \begin{cases} \text{随机数发生器} & x(t) < a; \\ \text{物理随机函数} & a \leq x(t) \leq b; \\ \text{线性函数} & b \leq x(t). \end{cases} \quad (1)$$

根据这些实验结果, 可将超晶格器件中发现的函数特性纳入密码学中 PUF 理论框架下进行研究, 由此可借用 PUF 的术语、概念、方法和理论来系统研究超晶格器件的密码特性. 超晶格 PUF 特性的主要来源如下: (1) 不可克隆性. 超晶格是采用 MBE 原子级层状生长而成, 超晶格中量子阱之间电子的隧穿几率与势垒厚度成指数关系. 分子束外延生长时, 总会有无法避免的单原子层级的涨落, 这种涨落经过 50 个周期的积累会更加明显, 导致超晶格器件物理实体和电学特性的不可克隆性. (2) 单向性和不可预测性. 对于特定的超晶格器件, 输入(挑战)与输出(响应)之间的相关性很小(图 4). 实验分析表明, 输出是输入的复杂高

次非线性函数, 具有物理单向函数功能. 由此可以推测, 超晶格输入信号与对应输出信号之间具有不可预测性: 即使已知足够长的输入及对应的输出, 也无法预测新的输入所对应的输出.

目前对超晶格物理函数特性的研究还处于实验观察

图 3 (网络版彩色)超晶格物理函数示意图

Figure 3 (Color online) Sketch of the physical function for superlattice

图 4 (网络版彩色)超晶格物理函数输入输出之间的相关性. (a) 输入波形; (b) 超输出波形

Figure 4 (Color online) Correlation between input and output of superlattice physical function. (a) Input signal; (b) output signal

和分析阶段,超晶格 PUF 特性的物理机理还需要进一步研究,功能表现还需要系统评估。

2.3 超晶格 PUF 孪生现象

与集成电路制备的 PUF 芯片不同,超晶格 PUF 还具有物理不可克隆孪生现象。实验表明,同一晶圆上相邻位置产生的同规格(同尺寸同形状)的两个超晶格器件在同一挑战信号下输出几乎一样的响应信号,其相关系数在 95% 以上,如图 5 所示。

从器件功能上看,这是孪生现象,如果推广到多个超晶格器件就是多生现象。超晶格器件间具备孪生现象的必要条件是其来自同一晶圆。同样的制造设备和工艺条件下,来自不同晶圆的超晶格器件则没有孪生现象,原因是 MBE 材料生长过程会导致超晶格中的量子阱层和势垒层单原子级涨落,而共振隧穿电流对量子阱层和势垒层的单原子级涨落都极为敏感,使得不同晶圆制备的器件具有完全不同的电学特性。需要特别指出的是孪生现象与不可克隆性的关系。孪生现象具有非常严格的条件,尤其是它们必须使用同套设备在同一工艺条件下同时生长制备出来(后期器件封装可以不同时)。尽管同一晶圆上可能存在多个多生器件具有相似的电学特性(在同尺寸、同形状的条件下),但是这些器件中的任何一个都不可能在所设计的工艺条件下在另一个晶圆上被重复(克隆)出来。

2.4 基于超晶格 PUF 的密钥达成协议

超晶格孪生器件在密码学上相当于一个可以在两地各自运行的自带同一密钥的函数,而且不掌握器件物理实体的人无法探测函数的运行过程及结果,因此利用超晶格物理不可克隆孪生现象可以安全地异地达成密钥。密钥达成过程如图 6 所示。

密钥达成过程的安全性基于以下两点:(1)超晶格物理函数不可克隆,即器件物理实体及其电学特性一旦制备便不可克隆。第三方即使从公共信道上得到驱动信号,也不可能通过伪造、仿制器件或拟合其函数功能来得到输出信号(密钥);(2)超晶格器件的输出具有不可预测性。无器件方在得到驱动信号后不能通过数学方法推断出输出信号(密钥)。因此采用超晶格孪生现象实现了随机数在两地的排他性共享,由此建立密钥分发机制^[19]。由于采用孪生现象达成的共享随机数有大约 5% 的差异,可以采用密码学中的信息调同(information reconciliation)技术^[38]来消除此差异;信息调同过程会产生微弱的信息损失,可以采用密码学中的保密增强(privacy amplification)技术来弥补,最后达成无条件安全的密钥。

和其他密钥分发技术^[39,40,41]相比,超晶格密钥分发技术具有安全性高和不消耗预分配密钥等优点,且仅需借助公开信道便可实现安全密钥分发。超晶格器件在制备中会带来一定管理负担,这是由于同一晶圆上多生器件存在

图 5 孪生超晶格器件输出之间的相关性。(a) A 为孪生超晶格器件共同输入波形;(b) 波形 B₁ 和波形 B₂ 分别为两个孪生器件的输出波形
Figure 5 Correlation between output signals of superlattice PUF pairs. (a) A corresponds to the identical input signal of superlattice PUF pairs; (b) B₁ and B₂ are the output signals of a superlattice PUF pair, respectively

图6 超晶格密钥达成原理架构图

Figure 6 Schematic diagram of superlattice key agreement

的可能性,需要对器件的生成制备过程进行严格监管,生长出来后未加工成器件的晶圆需要被销毁。

采用超晶格 PUF 研制的密钥分发原理样机如图 7 所示。

3 超晶格密码学的理论意义与应用价值

超晶格密码在 PUF 理论、自认证无条件安全密钥分发技术以及密码形态和应用模式等方面有重要创新。2000 年之前,硬件在密码学中主要充当密码算法数学逻辑的实现载体和密钥存储的介质,PUF 理论创建和应用推广改变了硬件在信息安全领域的角色和地位。超晶格密码将具有密码特性的超晶格器件纳入 PUF 的理论框架下进行研究,是典型的新兴交叉学科研究方向。其中的超晶格物理不可克隆孪生子是新的密码学和 PUF 概念,丰富和发展了 PUF 理论。超晶格密码充分体现了基于硬件的密码技术的价值,它面向密钥管理关键瓶颈问题,创新性地发展出优质高效的物理随机数(密钥)产生技术和自认证无条件安全密钥分发技术,推动了密钥管理技术的进步。2018 年 9 月在以“超晶格密码学”为主题的第 636 次香山科学会议上,密码学者、微电子器件专家、信息安全工程师等共同研讨了超晶格密码的研究和发展现状,会议形成共识:超晶格密码有助于解决困扰保密通信领域的难题,能够推动信息安全领域的技术进步。

超晶格密码是信息安全领域的基础性技术,应用前景广阔。超晶格物理随机数技术和超晶格密钥分发技术的应用研究已经取得了不少突破。超晶格物理随机数技术达到了技术成熟度 7 级标准,已经具备进入实际应用的条件,所开发的超晶格高速随机数发生器已通过有关资质单位的检测评估。超晶格密钥分发技术已现雏形,依据超晶格密钥分发技术制备的超晶格密钥分发原理样机实物如图 7 所示。在实验环境下该系统已达到 10 MBit/s 的密钥分发速率,根据超晶格本征的性能极限估算,理论预期的密钥分发速度可以达到 1 GBit/s。因此该系统不仅能作为密钥

图7 超晶格密钥分发系统原型机

Figure 7 Prototype of superlattice key distribution system

分配装置,而且完全能够实现高清视频数据实时在线一次一密加解密(直接使用超晶格系统输出的密钥流按位异或加解密文件,不需要采用其他的密码算法)。2019 年 5 月该系统已经在苏州和北京之间进行了密码通信实验和演示,各项技术指标均符合预期。

原理上所有抽象意义下的单向函数和(伪)随机函数能发挥作用的密码功能都可以用超晶格 PUF 来实现,超晶格 PUF 预期的应用如下:(1) 随机数或密钥产生。依照现有密码技术标准,基于硬件的随机数发生器是密码系统不可或缺的基础构件,目前国内密码领域主要使用的随机数发生器芯片在速度和稳定性等方面都有不足。采用超晶格随机数芯片能够克服这些问题,有效解决密码系统对大量实时高效优质随机数的需要。(2) 密钥的部署和更新。密码系统的初始密钥大都采用分散递送或加密递送的方式部署,分散递送会造成递送成本成倍增加,加密递送会带来新的密钥管理问题。采用超晶格密钥分发技术可以解决这些问题。与其他密钥分发技术相比,其突出优点是:超晶格密钥分发技术使用器件预分配而不是数据预分配,器件不可克隆而数据可以拷贝,因此超晶格密钥分发技术具有本质的安全优势;还可以进一步设计出具有前向安全性的密钥达成协议(只需再临时增加一个一次性参数来配合使用);与基于算法的密钥分发协议相比,其具备天然抗侧信道攻击能力。因此在密码系统中使用超晶格器件来部署和更新密钥,既能化解安全风险,又能降低成本。(3) 实体认证。目前大量的物联网设备在接入互联网后,由于不具有数据标识的唯一性,设备被篡改、假冒等安全问题大量暴露,成为物联网发展的掣肘。超晶格 PUF 的天然属性能够有效满足设备认证过程中所需的随机设备 ID、认证协议中的随机数等需求,达到较高的安全性。(4) 无条件安全的认证及加密应用。在高安全需求的网络建设中,需要配备无条件安全的加密服务,因此需配置大量密钥,典型的场景如量子密钥分发系统。由于 PUF 理论上可以达到无条件安全,因此超

晶格密码可用于量子密钥分发系统,解决经典信道的无条件安全认证和密钥池的无条件安全加密等问题。

4 超晶格密码的研究问题

超晶格室温自发混沌振荡现象、超晶格随机数同步现象等被中国学者发现后,在国际上引起了相关行业研究人员的广泛关注,出现了不少理论研究成果及其在密码学中的应用尝试,如超晶格随机数技术已达到7级以上的技术成熟度,并被用来开发相关的型号产品。但超晶格密码前期的研究和应用也存在比较明显的缺陷:一是研究方法缺乏普适性,二是研究结果不成体系,三是技术路线没有完全融入密码和信息安全领域。支持超晶格密码器件大范围应用的理论基础还不完善,现有的部分应用实例也有待进一步的系统性安全评估,完整的超晶格密码应用技术体系和应用生态尚未建立。超晶格密码面临的这些问题和其他新型密码技术在初创阶段面临的问题是相似的。综上所述,当前亟待开展的研究课题如下:

第一,超晶格 PUF 特性的物理机理分析。超晶格器件是一个多自由度的非线性动力学系统,这是超晶格密码安全性最根本的保证。在启发式分析和实验现象观测的基础上,还需要从超晶格密码器件的物理本质出发,对超晶格物理不可克隆的机理和超晶格动力学系统的过程展开深入研究,系统论证超晶格密码器件安全性。(1)超晶格器件

的物理不可克隆特性是由制备超晶格材料的 MBE 生长技术决定的,MBE 的岛状生长会引起单原子层级涨落,导致材料间的结构参数存在差异。需要定量刻画材料的微观结构参数与器件宏观性能之间的关系,在基本的物理和技术假设下,从逻辑上导出克隆器件的困难性。(2)超晶格 PUF 单向函数特性来源于超晶格器件的非线性动力学行为,因此需要对超晶格器件的物理模型进行定性构建、调整拟合和定量优化,解析超晶格器件的电子输运特性和动力学行为。

第二,超晶格密码器件的安全性检测评估技术研究。除了对超晶格 PUF 进行物理机理分析外,按照密码学的思想采用黑盒模型评估超晶格器件的密码安全性也很重要,主要包括超晶格器件的 PUF 特性和孪生子功能的统计检测和超晶格器件输出数据的熵估算等。(1)超晶格器件的密码学特性包括稳定性、独立性、不可预测性和孪生子功能等几个指标,这些指标的检测一般采用假设统计检验方法。(2)在超晶格器件的密码应用过程中需要估计超晶格器件的平均香农熵、样本熵、极小熵或其他 Rényi 熵。

第三,超晶格密码应用协议设计和安全性形式化证明。(1)研制自认证无条件安全超晶格密钥达成协议并对协议的安全性和其他性能进行系统评估。(2)发展超晶格密钥分发协议各个环节所需的支撑技术,主要是后处理技术,包括信息调同和保密增强技术等。

致谢 感谢“十三五”国家密码发展基金(MMJ20180112)资助。感谢中国科学院苏州纳米技术与纳米仿生研究所张耀辉、刘佩华、殷志珍、宋贺伦、吴涵、彭振云、吴德明、丁朋、莫海峰、刘伟、黄寓洋、李文和北京电子科技学院阎亚龙、夏超、解建国、徐莉伟在论文完成过程中的讨论和帮助。

推荐阅读文献

- Schneier B. Applied Cryptography. Hoboken: Wiley, 1996
- Zhang Y H, Kastrup J, Klann R, et al. Synchronization and chaos induced by resonant tunneling in GaAs/AlAs superlattices. Phys Rev Lett, 1996, 77: 3001
- Huang Y Y, Wen L, Ma W Q. Experimental observation of spontaneous chaotic current oscillations in GaAs/Al_{0.45}Ga_{0.55}As superlattices at room temperature. Chin Sci Bull, 2012, 579: 2070–2072
- Li W, Aviad Y, Reidler I, et al. Chaos synchronization in networks of semiconductor superlattice. Europhys Lett, 2015, 112: 30007
- Schindler W, Killmann W. Evaluation criteria for true (physical) random number generator used in cryptographic applications. In: 4th International Workshop on Cryptographic Hardware and Embedded Systems, 2003. 431–449
- Esaki L, Tsu R. Superlattice and negative differential conductivity in semiconductors. IBM J Res Dev, 1970, 40: 61–65
- Esaki L, Chang L L. New transport phenomenon in a semiconductor superlattice. Phys Rev Lett, 1974, 33: 495
- Kapitaniak T. Controlling Chaos. Pittsburgh: Academic Press, 1996. 142–145
- Xia J B. I - X mixing effect in GaAs/AlAs superlattice and heterojunctions. Phys Rev B, 1990, 41: 3117
- Li W, Reidler I, Aviad Y, et al. Fast physical random-number generation based on room-temperature chaotic oscillations in weakly coupled superlattices. Phys Rev Lett, 2013, 111: 044102
- Alvaro M, Carretero M, Bonilla L L, et al. Noise-enhanced spontaneous chaos in semiconductor superlattices at room temperature. Europhys Lett, 2014, 107: 37002
- Poyser C L, Akimov A V, Balanov A G, et al. A weakly coupled semiconductor superlattice as a harmonic hypersonic-electrical transducer. New J Phys, 2015, 17: 083064

- 13 Hramov A E, Makarov V V, Maximenko V A, et al. Intermittency route to chaos and broadband high-frequency generation in semiconductor superlattice coupled to external resonator. *Phys Rev E*, 2015, 92: 022911
- 14 Ruiz-Garcia M, Essen J, Carretero M, et al. Enhancing chaotic behavior at room temperature in GaAs/(Al,Ga)As superlattices. *Phys Rev E*, 2017, 95: 085204
- 15 Yin Z Z, Song H L, Zhan Y H, et al. Noise-enhanced chaos in a weakly coupled GaAs/(Al,Ga)As superlattice. *Phys Rev E*, 2017, 95: 012218
- 16 Huang Y Y, Li W, Ma W Q, et al. Spontaneous quasi-periodic current self-oscillations in a weakly coupled GaAs/(Al,Ga)As superlattice at room temperature. *Appl Phys Lett*, 2013, 102: 242107
- 17 Huang Y Y, Qin H, Li W, et al. Experimental evidence for coherence resonance in a noise-driven GaAs/AlAs superlattice. *Europhys Lett*, 2014, 105: 47005
- 18 Mompo E, Ruiz-Garcia M, Carretero M, et al. Coherence resonance and stochastic resonance in an excitable semiconductor superlattice. *Phys Rev Lett*, 2018, 121: 086806
- 19 Liu W, Yin Z Z, Chen X M, et al. A secret key distribution technique based on semiconductor superlattice chaos devices. *Sci Bull*, 2018, 63: 1034
- 20 Pappu R S. Physical one-way functions. Doctor Dissertaion. Cambridge: Massachusetts Institute of Technology, 2001
- 21 Maes R. Physically Unclonable Functions: Constructions, Properties and Applications. Berlin, Heidelberg: Springer-Verlag, 2013
- 22 Ganji F. On the Learnability of Physically Unclonable Functions. Berlin, Heidelberg: Springer, 2018
- 23 Tajik S. On the Physical Security of Physically Unclonable Functions. Berlin, Heidelberg: Springer, 2019
- 24 You W Q, Chen X M. Research and application of physical unclonable functions. In: IEEE 3rd Information Technology and Mechatronics Engineering Conference, 2018
- 25 Böhm C, Hofer M. Physical Unclonable Functions in Theory and Practice. New York: Springer Science+Business Media, 2013
- 26 Halak B. Physically Unclonable Functions: From Basic Design Principles to Advanced Hardware Security Applications. Berlin, Heidelberg: Springer, 2018
- 27 Tuyls P. Towards Hardware-Intrinsic Security: Foundations and Practice. Berlin, Heidelberg: Springer-Verlag, 2010
- 28 Pappu R, Recht B, Taylor J, et al. Physical one-way functions. *Science*, 2002, 297: 2026–2030
- 29 Maiti A, Schaumont P. Improved ring oscillator PUF: An FPGA-friendly secure primitive. *J Cryptol*, 2011, 24: 375
- 30 Tajik S, Dietz E, Frohmann S, et al. Photonic side-channel analysis of arbiter PUFs. *J Cryptol*, 2017, 30: 550
- 31 Maiti A, Casarona J, Maiti A, et al. A large scale characterization of RO-PUF. In: IEEE Symposium on Hardware-Oriented Security and Trust, 2010. 94–99
- 32 Rose G S, McDonald N, Yan L K, et al. A write-time based memristive PUF for hardware security applications. In: IEEE/ACM International Conference on Computer-Aided Design, 2013. 830–833
- 33 Herder C, Yu M D, Koushanfar F, et al. Physical unclonable functions and applications: A tutorial. *Proc IEEE*, 2014, 102: 1126–1141
- 34 Liu R, Wu H, Pang Y, et al. Experimental characterization of physical unclonable function based on 1 kb resistive random access memory arrays. *IEEE Electr Device Lett*, 2015, 36: 1380
- 35 Gope P, Lee J, Quek T Q S. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. *IEEE T Inf Foren Sec*, 2018, 99: 1
- 36 Goldreich O. Foundations of Cryptography: Basic Tools. Cambridge: Cambridge University Press, 2003
- 37 Shangguan X L, Zhang L W, Shi H S. An overview of hot topics on research of international standards for information security (in Chinese). *Inf Technol Stand*, 2015, 11: 76 [上官晓丽, 张立武, 石竑松. 国际信息安全标准研究项目热点概述. 信息技术与标准, 2015, 11: 76]
- 38 Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: International Conference on the Theory and Applications of Cryptographic Techniques, 2004
- 39 Chen X, You W. A new cryptosystem based on positive braids. In: Conference Proceedings IEEE UIC/IWC, 2018
- 40 Christian K, Mario P. Applied Quantum Cryptography. Berlin, Heidelberg: Springer, 2012
- 41 Scarani V, Bechmann-Pasquinucci H, Cerf N, et al. The security of practical quantum key distribution. *Rev Mod Phys*, 2008, 81: 1301–1350

Summary for “超晶格密码的研究进展”

Advances in superlattice cryptography research

Xinhai Tong^{1,2}, Xiaoming Chen^{1,2*} & Shu Xu^{3*}¹ School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China;² Research Center for Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China;³ Key Laboratory of Information Security Technology, North Institute of Information Technology, Beijing 100072, China

* Corresponding authors, E-mail: chenxmphd@besti.edu.cn; 18010005098@189.cn

One of the widely-known opinions in modern cryptography is that the security of a cryptosystem depends on the security of key. Therefore, key management is the foundation engineering of information security field and its corresponding technical level plays a decisive role in the security and efficiency of entire cryptosystem. Key generation and key distribution are two bottleneck problems of key management which make practical cryptosystem complex and costly to make up for the defects of security. Cryptographic techniques based on physical methods are introduced to generate and distribute secure key which greatly reduce the risk of key management than the traditional techniques based on mathematical methods. Currently, it is a popular research direction to solve cryptographic problems with physical entities such as quantum cryptography, physical unclonable function (PUF), etc.

Superlattice cryptography is a brand-new cryptographic technology based on semiconductor superlattice device physics which was developed upon the innovative works of superlattice material electronic characteristics researches and is gaining increasing international influence. Superlattice device taps into the random variation during fabrication processes, therefore the secret is extremely difficult to predict or extract. Moreover, once matched superlattice device pairs are produced, anyone cannot obtain or duplicate, including the original producer with complete set of equipment. Superlattice devices can be used similar to traditional PUF hardware that extract secrets from physical characteristics. It takes full advantages of the internal security of hardware to establish new cryptographic mechanism and application pattern with superlattice PUF devices. On one hand, with the theoretical framework of PUF being introduced to superlattice research, superlattice cryptography becomes a cross-discipline that puts forward a new concept of hardware cryptography and develops PUF theory, and leads to a new research direction for cryptography. On the other hand, superlattice PUF pairs provide a feasible approach to the key management that has long obstructed the information security engineering.

This review briefly introduces the origin and development of superlattice cryptography along with current state-of-the-art advances of practical technologies including physical random number generation technology and superlattice key distribution technology. Based on the spontaneous chaotic oscillation of GaAs/Al_{0.45}Ga_{0.55}As semiconductor superlattice, high-quality, efficient and stable physical random number technology was developed, which has laid a good foundation for the subsequent research and development of superlattice cryptography. The superlattice devices were incorporated into the framework of PUF theory in cryptography, and soon afterwards chaos synchronization between unclonable matched superlattice pairs was discovered, based on which a long-haul public-channel secure key distribution was experimentally demonstrated with an unconditional security key distribution protocol with self-authentication capability created. The theoretical significance and application potential of superlattice cryptography have been recognized by cryptographers, microelectronic experts and information security engineers. Despite of academic progress made and innovative technologies exploited in several aspects of superlattice cryptography, our research method and relevant technical route are still quite simple and limited.

In the following research, the physical mechanism related to the security properties of superlattice cryptography is urgently needed to be further analyzed, methods to evaluate the security properties of superlattice cryptography devices are going to be systematically developed and a formal proof of the protocol design and security model of the superlattice cryptography will be built. The future works are expected to establish superlattice cryptography as a fundamental information security technology which is fully independently controllable from fundamental theory through device manufacturing technology all the way to application technology in our country.

superlattice cryptography, physical unclonable function, key distribution, key management

doi: 10.1360/TB-2019-0291