基于延时控制的 Glitch PUF 电路设计

董永兴 徐金甫* 李军伟
(解放军信息工程大学 河南 郑州 450001)

摘 要 Glitch PUF 具有良好的非线性特性,可以很好地抵御建模攻击的威胁,保证信息安全。提出一种延时控制的 Glitch PUF 电路架构。利用延时调节模块控制不同路径的延时大小,T 触发器利用产生毛刺数量的奇偶性判决响应比特,使用 Monte Carlo 仿真验证所设计电路的性能。实验结果表明,所设计的 Glitch PUF 具有良好的唯一性和稳定性,且节约了资源。

关键词 Glitch PUF 延时控制 Monte Carlo 仿真 信息安全

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.11.050

DESIGN OF GLITCH PUF BASED ON DELAY CONTROL

Dong Yongxing Xu Jinfu* Li Junwei
(*The PLA Information Engineering University, Zhengzhou 450001, Henan, China*)

Abstract Glitch PUF has good nonlinear characteristics, and it can resist the threat of modeling attack and ensure information security. This paper proposes a delay control Glitch PUF architecture. The delay adjustment module was used to control the delay of different paths, and the T flip-flop used the parity of glitch number to determine the response bits. The performance of the designed circuit was verified by Monte Carlo simulation. The experimental results show that the designed Glitch PUF not only has good uniqueness and stability, but also saves resources.

Keywords Glitch PUF Delay control Monte Carlo simulation Information security

0 引 言

当今社会,传统密码安全手段受到新兴攻击技术的威胁越来越大。物理不可克隆函数(Physical Unclonable Function,PUF)因其不可克隆性和不可预测性等优良特性,在信息安全领域具有十分巨大的应用潜力[1-2]。目前大部分的物理不可克隆函数是基于现场可编程门阵列(FPGA)实现的。FPGA 作为一种半定制电路,可根据用户需求进行编程与配置,具有灵活性高、可重复配置等优点。但其应用于 PUF 时,缺点也很明显。尤其是对于延时类的 PUF 而言,电路的布局布线严重影响输出结果,这导致电路的输出结果出现一定的偏差。

为了解决这一问题,许多研究者采用专用集成电路(Application Specific Integrated Circuit,ASIC)设计 PUF 电路。针对 ASIC 电路设计成本高、周期长等特点,文献[3-5]使用 Monte Carlo 仿真方法,模拟工艺和环境的变化,验证所设计 PUF 的电路性能。

随着对 PUF 研究的不断深入,国内外学者提出了多种针对 PUF 电路的攻击技术[6-8]。文献[6]采用机器学习的逻辑回归(Logistic Regression, LR)和演化策略(Evolution Strategies, ES)对多种 PUF 电路成功攻击并实现预测。文献[7-8]从理论上描述了 PUF 激励响应行为,配合相应的算法攻击 PUF。机器学习对 PUF 电路实现攻击的主要原因是 PUF 电路的结构相对固定,产生的大量激励响应对具有一定的线性特性,使得机器学习能够预测延迟信息和生成信息之间的关系,从而实现对电路的攻击。因此,增强电路的非线性特性成为研究重点关注的问题。

文献[9]提出了一种利用门电路之间的延迟变量生成非线性毛刺波形的 Glitch PUF 架构。通过对电路

收稿日期:2019-06-17。董永兴,硕士生,主研领域:专用集成电路设计。徐金甫,教授。李军伟,讲师。

生成的毛刺信息进行获取、抖动校正、采样等操作,实现毛刺信息与输出信息的转化。文献[10]提出一种基于信号传输理论的 Glitch PUF 方案。该方案利用毛刺信号的非线性特性抵抗建模攻击,采用多级延迟采样电路实现输出响应,并用 Monte Carlo 仿真验证电路的性能。但为了保证性能,上述电路增加了辅助电路,增大了资源消耗。

在保证电路在具有良好非线性特性的同时令资源消耗较小是本文关注的重点。本文提出一种基于延时控制的 Glitch PUF 电路结构(Delay Controlled Glitch PUF, DC-Glitch PUF)。通过提取组合逻辑电路门的传输延时,控制路径延时差,采用 T 触发器采样电路输出波形。利用延时模块控制不同路径的波形到达 T 触发器的时间,使其达到良好的性能。在 TSMC 65 nm CMOS 工艺下,使用 Monte Carlo 仿真验证电路的性能。

1 Glitch PUF

Glitch PUF 首先由 Anderson 等[11]提出,该 PUF 基于 FPGA 实现,电路利用传输路径延时的不同产生毛刺,毛刺决定单元电路的输出结果,输入不同的激励信号选择不同单元电路“异或”输出响应。此结构的问题在于单元电路是静态输出,不能完全保证信息的安全。因此,非线性毛刺的动态输出是关键所在。Suzuki 等[9]提出了一种新的 Glitch PUF 架构,通过随机放置各种组合逻辑门,利用门延时和逻辑转换延时的不同,产生不同宽度的毛刺,保证了毛刺产生与输入数据的非线性。但为了有效采集信号,增加了抖动校正和资源消耗较大的采样电路。针对 Glitch PUF 的性能和应用场景而言,电路毛刺的产生和电路的轻量级属性是非常重要的。

2 毛刺产生

毛刺与 Glitch PUF 的性能密切相关。由于 Glitch PUF 依靠产生的毛刺信号决定电路的输出结果,因此,毛刺信号的峰值、宽度与非线性特性是 Glitch PUF 电路架构关注的重点。

组合逻辑电路的毛刺主要是由竞争冒险现象产生的。电路信号在传输过程中,通过门电路和电路连线时会有一定的延时,逻辑翻转也需要一定的转换时间。这使得电路信号在实际电路中传输时,到达逻辑门输入端的时间不同,逻辑的变化也有先后,从而导致电路出现意想不到的尖峰信号,这就是毛刺信号,其产生往往具有非线性特性。

毛刺产生受诸多因素的影响,如温度、电压和噪声等。在不考虑外界因素的影响下,电路本身的特性也会导致毛刺产生。

当电路的逻辑函数在一定条件下可以简化为 $Y = A \cdot \overline{A}$ 或者 $Y = A + \overline{A}$ 时,如图 1 所示,则可判定电路存在竞争冒险现象,有可能会产生毛刺信号。由此可知,电路逻辑对毛刺的产生有很大影响。

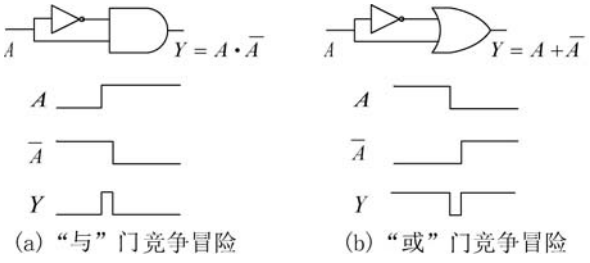

图 1 简单电路竞争冒险现象

对于逻辑组合电路而言,电路信号输入的顺序和传输延时也会影响到电路的输出。如图 2 所示,信号 C 到达“与”门的时间不同会使得电路输出结果不同。若 C 先于 A、B 到达“与”门,则电路出现狭窄的尖峰脉冲;反之,则电路输出不会产生毛刺信号。因此,实际电路中延时对于毛刺的产生有非常重要的作用。

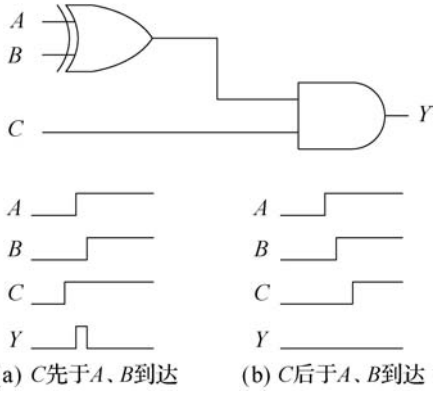

图 2 多输入组合逻辑电路产生毛刺的情况

3 PUF 电路设计

3.1 延时调节模块设计

经过前文分析,毛刺的产生与电路延时息息相关。由于传输路径的脉冲过滤限制和逻辑门存在惯性延迟,导致产生的毛刺不一定能全部传递到输出端。只有脉冲宽度大于惯性延迟的毛刺,才可以经由逻辑门输出。因此,为保证良好的电路性能,控制电路毛刺信号的产生是十分重要的。

以“异或”门为例,如图 3 所示,w 为输入信号 x_1 和 x_2 的延时差宽度。当 w 大于惯性延迟 d 时,产生的毛刺可以输出;反之,输出端不会输出逻辑 1。当 $w = d$

时,毛刺波形有 50% 的概率输出。

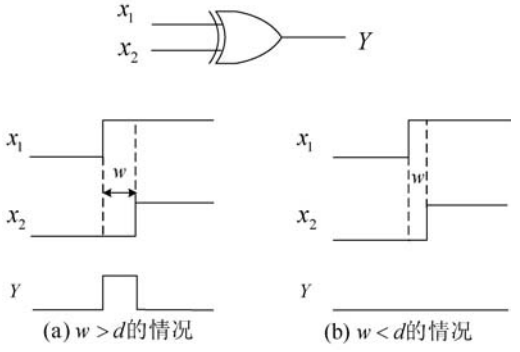

图 3　“异或”门的惯性延迟影响毛刺输出

本文在毛刺产生模块的路径上增加延时调节模块,用以改变毛刺的宽度,以期提高电路性能。如图 4 所示,多路不同数量的缓冲器链连接到多路数据选择器,选择信号 S 通过数据选择器选择不同的延时路径输出波形。延时调节模块不同路径延时的大小不仅与缓冲器数量有关,而且与器件参数有关。沟道长度和宽度的不同、阈值电压的差别、金属连线等都会使延时大小不同。因此,即使是相同的选择信号,延时也存在差异,使得电路随机性增加。

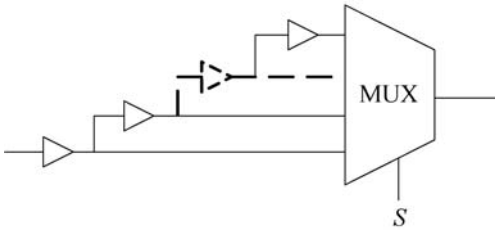

图 4　延时调节模块

3.2　毛刺产生模块

电路的逻辑会影响电路毛刺的产生。本文借鉴竞争冒险电路,采用“与非”门和“非或”门相结合,使用“异或”门输出波形。如图 5 所示,Delay 单元为延时调节模块。本文采用四级延迟,选择信号 $S[1:0]$ 用于控制路径的延时。x_1、x_2、x_3、x_4 为输入信号,Y 为输出。通过控制延迟调节模块的选择信号,使得不同路径的延时不同,以此调节信号到达逻辑门的先后顺序,控制毛刺信号的宽度。

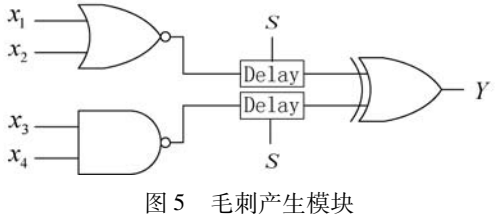

图 5　毛刺产生模块

为使得电路产生的毛刺宽度对延迟调节模块更敏感,本文采用“异或”门树网络,如图 6 所示。电路增加了输入信号的数量,增强了产生毛刺的非线性特性,增加其抗建模攻击属性。延迟调节模块选择不同的延迟大小,使得信号到达“异或”门的时间不同,对毛刺的产生和能否传递到输出端有重要影响。

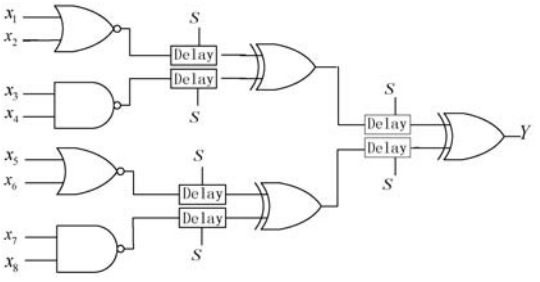

图 6　延时敏感型毛刺产生模块

3.3　采样模块

当毛刺产生模块输出波形后,需要采样电路将波形转化为响应比特位。如何在极短时间内准确采样产生的脉冲信号并输出响应是 Glitch PUF 电路设计的关键。最普遍的思想就是提高时钟采样精度,使用多相位时钟采集波形,但这样做会使得电路资源消耗增大。

文献[9]与文献[10]采用了相同的采样电路,如图 7 所示。信号波形输入后,通过缓冲器对波形延时传递,使用 D 触发器采样不同时刻的波形并输出逻辑值。电路存在毛刺波形与无毛刺波形相比,输出位 b_i 会有所不同,如图 8 所示。虽然这样的采集方案减少了时钟线的资源消耗,但为了保证有效的采样精度,增加了缓冲器和 D 触发器的数量,使电路资源消耗也增多。

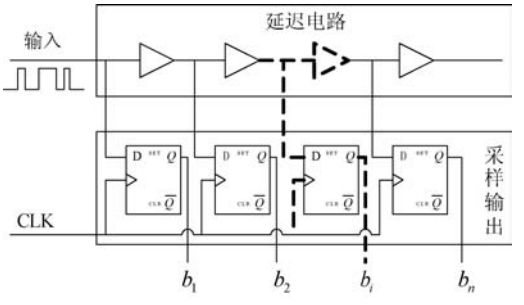

图 7　延迟采样电路

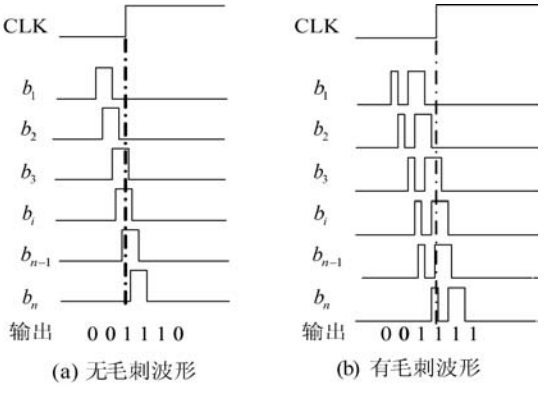

图 8　不同波形下的采样结果

不同于文献[9 – 10]提出的通过使用延时电路采样信号波形的思想,本文提出利用波形产生毛刺数量的奇偶性来判决生成响应值,使用 T 触发器采样毛刺产生模块电路的输出。

T 触发器输入端置“1”,输出波形连接至 T 触发器时钟端,Q 端输出,如图 9 所示。当波形有偶数个上升沿时,Q 端输出为“1”,反之,输出为“0”。当毛刺产生模块输出的毛刺信号过窄或峰值过低,不足以使得触发器输出翻转时,电路输出不变。在实际电路运行过程中,难免会出现错误翻转的情况,T 触发器采样使得电路错误翻转次数为偶数次时,并不会改变电路的输出,这增加了电路的鲁棒性。

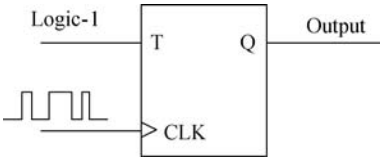

图 9 T 触发器采样电路

3.4 电路架构

Glitch PUF 电路的架构如图 10 所示。通过控制单元发出的 $S[1:0]$ 控制毛刺产生模块中延迟调节模块的延迟大小,C 通过数据选择器选择不同的毛刺波形输入到采样电路,采样电路输出单比特响应。

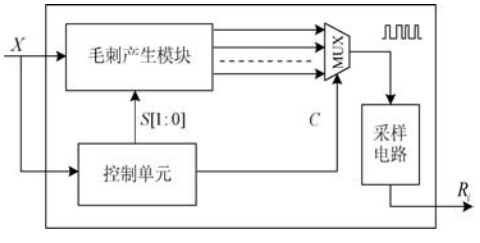

图 10 电路架构

为节约资源且增加电路的随机性,本文在单比特响应电路的基础上,设计多比特 Glitch PUF 输出电路结构,如图 11 所示。每增加一个单比特响应电路可增加一位输出。采用循环输入方式,将单比特电路不同的输出结果经由“异或”门输出。可在每个输出后接一个采样 T 触发器,有 N 个毛刺产生模块,则可产生 N 比特不同的输出。

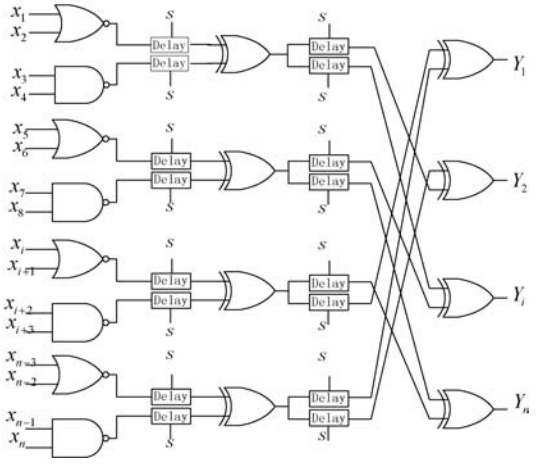

图 11 多比特响应电路结构

不同于 Anderson PUF 的单元电路静态输出,本文提出的电路架构可实现动态输出。随着输入信号和控制信号的变化,输出随之改变,可增强电路的随机性和安全性。

4 实验结果

4.1 电路输入与毛刺波形

本文采用 TSMC 65 nm CMOS 工艺库,使用 Monte Carlo 仿真验证所设计的 Glitch PUF 电路性能。毛刺产生模块的输入采用伪随机数发生器随机生成 x_i,如图 12 所示。通过设置不同的选择信号 $S[1:0]$,使得路径延迟不同。图 13 为一个毛刺产生模块的输出波形与采样电路输出波形。由实验可知,在输入 x_i 不同时,电路会产生意想不到的尖峰脉冲,而这些尖峰脉冲的出现,使得输出结果出现变化。但并不是所有的尖峰脉冲都会引起输出结果的改变,有些尖峰脉冲的宽度很小或者峰值很低,并不会引起结果的改变。

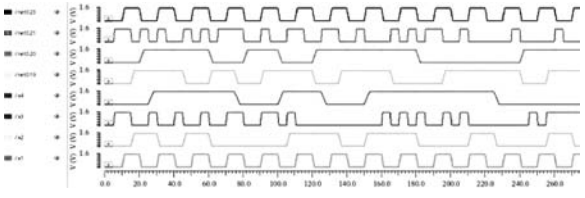

图 12 毛刺产生模块的输入

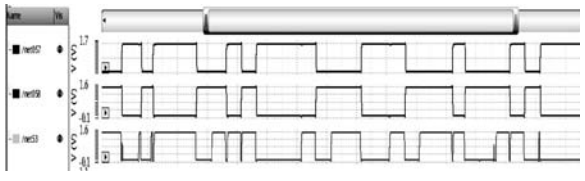

图 13 毛刺波形与采样结果波形

4.2 Monte Carlo 仿真

本文在环境温度为 27 ℃时,对电路 Monte Carlo 仿真 200 次,毛刺波形如图 14 所示。可以看出,毛刺的宽度和峰值不完全一致。在仿真过程中,电路的采样结果会随着毛刺波形的改变而改变。

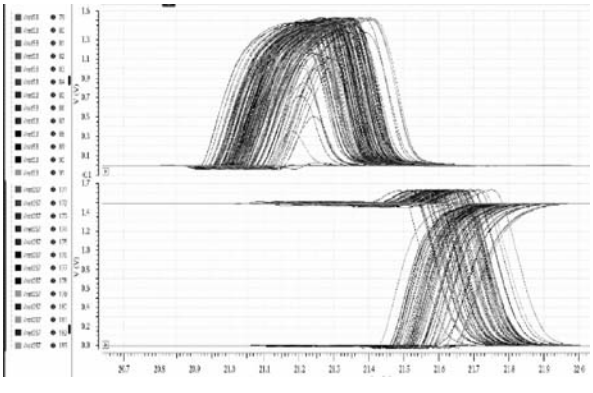

图 14 Monte Carlo 仿真结果

电路不采用延迟模块的结果显示,有 125 次仿真结果使得采样电路的输出为逻辑 0,这表示在实际电路制作过程中,所设计的毛刺产生模块的唯一性为 62.5%。多次实验显示,将两条路径的延迟差增大时,产生逻辑 0 数量减小,最小数目为 103 次,电路唯一性达到 48.5%。

PUF 电路在运行过程中会受到温度变化的影响。为验证电路的稳定性,通过 Parametric Analysis 将仿真温度区间设置为 -40 ~ 85 ℃,每隔 1 ℃仿真一次,共仿真 126 次。结果显示,有 18 次仿真波形出现错误翻转,其中有 7 次波形翻转了偶数次,导致输出结果未发生变化。因此电路在温度区间[-40,85]的稳定性为 91.3%。在温度区间[-10,70]有 3 次波形发生翻转,电路的稳定性为 96.3%。

基于延时控制的 Glitch PUF 与其他相关论文结果对比如表 1 所示。可以看出,基于延时控制的 Glitch PUF 的唯一性仅次于 FRO PUF,但 FRO PUF 的唯一性仅是在 27℃时测量,且采用了精细的延迟配置线来提升性能。在稳定性方面,本文 PUF 与其他 PUF 基本持平,但其采样的温度范围更大,更贴近电路的实际使用环境。因此,本文所设计的 DC-Glitch PUF 具有良好的唯一性和稳定性,有较高的应用价值。

表 1　不同 PUF 性能对比

PUF	唯一性/%	稳定性/%	工作环境/℃
RPUF[12]	48.4	94.8	-20 ~ 50
FRO PUF[13]	49.9	94.9	27
SRAM PUF[14]	44.0	99.5	不详
X-Point PUF[15]	48.4	95.8	不详
XRBRPUF[16]	40.7	98.2	0 ~ 70
本文电路	48.5	96.3	-10 ~ 70

5　结　语

本文设计了一种基于延时控制的 Glitch PUF 电路。通过毛刺产生模块、延时调节模块、T 触发器采样电路等,控制电路路径延时,调节毛刺生成宽度,实现数据的比特输出。在 TSMC 65 nm CMOS 工艺下,使用 Cadence 验证设计的电路逻辑功能正确,Monte Carlo 仿真结果显示电路具有良好的唯一性和稳定性。基于延时控制的 Glitch PUF 电路利用生成毛刺的非线性特性,可以抵御建模攻击的威胁,可应用于信息安全领域。

参　考　文　献

[1] 庞子涵,周强,高文超,等. FPGA 物理不可克隆函数及其实现技术[J]. 计算机辅助设计与图形学学报,2017,29(9):1590 - 1603.

[2] 尹魏昕,贾咏哲,高艳松,等. 物理不可克隆函数(PUF)研究综述[J]. 网络安全技术与应用,2018(6):41 - 42,54.

[3] Lao Y,Parhi K K. Statistical analysis of MUX-based physical unclonable functions[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,2014,33(5):649 - 662.

[4] 钱浩宇,汪鹏君,张跃军,等. 基于单稳态定时偏差的高识别性 PUF 电路设计[J]. 浙江大学学报(理学版),2017,44(1):64 - 69.

[5] 李刚,汪鹏君,张跃军,等. 基于 65nm 工艺的多端口可配置 PUF 电路设计[J]. 电子与信息学报,2016,38(6):1541 - 1546.

[6] Ulrich R,Sehnke F,Solter J,et al. Modeling attacks on physical unclonable functions[C]//ACM Conference on Computer and Communications Security. ACM,2010:237 - 249.

[7] Gao Y S,Al-Sarawi S F,Abbott D,et al. Modeling attack resilient reconfigurable latent obfuscation technique for PUF based lightweight authentication[EB]. [2019 - 06 - 17]. arXiv:1706.06232,2017.

[8] Ganji F,Tajik S,Seifert J P,et al. Let me prove it to you:RO PUFs are provably learnable[C]//Proceedings of the 2015 18th International Conference on Information Security and Cryptology. Springer,2016:345 - 358.

[9] Suzuki D,Shimizu K. The glitch PUF:A new delay-PUF architecture exploiting glitch shapes[C]//The 12th International Workshop on Cryptographic Hardware and Embedded Systems(CHES). Springer,2010.

[10] 张跃军,汪鹏君,李刚,等. 基于信号传输理论的 Glitch 物理不可克隆函数电路设计[J]. 电子与信息学报,2016,38(9):2391 - 2396.

[11] Anderson J H. A PUF design for secure FPGA-based embedded systems[C]//Proceedings of the 2010 15thAsia and South Pacific Design Automation Conference. IEEE,2010:1 - 6.

[12] Ye J,Hu Y,Li X W. RPUF:Physical unclonable function with randomized challenge to resist modeling attack[C]//2016 IEEE Asian Hardware-Oriented Security and Trust. IEEE,2016:1 - 6.

[13] 李昌婷,章庆隆,刘宗斌,等. FROPUF:从基于 FPGA 的震荡环 PUF 中提取更多的熵[J]. 信息安全学报,2018,3(1):16 - 30.

[14] Gong M L,Liu H L,Mim R,et al. Pitfall of the strongest cells in static random access memory physical unclonable functions[J]. Sensors,2018,18(6):1776.

(下转第 333 页)

-85.
[8] 蔡晶晶,宗汝,蔡辉. 基于空域平滑稀疏重构的 DOA 估计算法[J]. 电子与信息学报,2016,38(1):168-173.
[9] Mohimani H, Babaie-Zadeh M, Jutten C. A fast approach for overcomplete sparse decomposition based on smoothed L0 norm[J]. IEEE Transactions on Signal Processing,2009,57(1): 289-301.
[10] 赵瑞珍,林婉娟,李浩,等. 基于光滑 l_0 范数和修正牛顿法的压缩感知重建算法[J]. 计算机辅助设计与图形学学报, 2012,24(4):478-484.
[11] 孙娜,刘继文,肖东亮. 基于 BFGS 拟牛顿法的压缩感知 SL0 重构算法[J]. 电子与信息学报,2018,40(10):2408-2414.
[12] 伍飞云,周跃海,童峰. 基于似零范数和混合优化的压缩感知信号快速重构算法[J]. 自动化学报,2014,40(10): 2145-2150.
[13] 陈金立,李伟,朱筱嵘,等. 基于修正近似双曲正切函数的平滑 l_0 范数算法[J]. 计算机工程与设计,2018,39(12): 3717-3721,3754.
[14] Ma W K, Hsieh T H, Chi C Y. DOA estimation of quasi-Stationary signals with less sensors than sources and unknown spatial noise covariance: a Khatri-Rao subspace approach [J]. IEEE Transactions on Signal Processing,2010,58(4): 2168-2180.

(上接第 285 页)

[21] 陈湘川. 信息缺乏网络中的通信算法研究[D]. 合肥:中国科学技术大学,2000.
[22] 肖琳琳,陈杰,马冬妍,等. 中国工业企业两化融合现状实证研究[J]. 中国科技论坛,2016(9):71-77.
[23] 曾文献,张淑青,孟庆林,等. 基于改进 BP 神经网络的网络入侵检测研究[J]. 石家庄学院学报,2019,21(3): 23-30.
[24] 逯玉婧. 基于深度信念网络的入侵检测算法研究[D]. 石家庄:河北师范大学,2016.
[25] 王明. 基于卷积神经网络的网络入侵检测系统[D]. 北京:北京邮电大学,2018.
[26] 陈万志,李东哲. 结合白名单过滤和神经网络的工业控制网络入侵检测方法[J]. 计算机应用,2018,38(2):363-369.

(上接第 303 页)

[9] 秦靖辉. 安全电子商务 SET 协议的研究与改进[D]. 广州: 广东工业大学,2016.
[10] 韩炼冰. 椭圆曲线密码算法的 FPGA 设计与实现[D]. 成都: 电子科技大学,2018.
[11] Kavitha S, Alphonse P J A, Reddy Y V. An improved authentication and security on efficient generalized group key agreement using hyper elliptic curve based public key cryptography for IoT health care system[J]. Journal of medical systems,2019,43(8):260.
[12] 卢闻捷. 改进椭圆曲线密码体制在 SET 协议中的应用[J]. 计算机系统应用,2018,27(4):34-38.
[13] 李尚泽. 椭圆曲线标量乘算法改进及应用[D]. 北京: 北京化工大学,2017.
[14] Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS[J]. Telematics and Informatics, 2019, 38: 100-117.
[15] 吴旦. 椭圆曲线加密算法在卫星通信中的应用[J]. 数字通信世界,2018,165(9):160.
[16] Toughi S, Fathi M H, Sekhavat Y A. An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System[J]. Signal Processing,2017,141(12): 217-227.
[17] Beelen P, Datta M. Generalized hamming weights of affine cartesian codes[J]. Finite Fields and Their Applications, 2018,51(5):130-145.
[18] 王子青. 移动支付系统加密认证算法及安全协议的研究与实现[D]. 南京: 南京邮电大学,2016.
[19] 魏娟. SET 加密技术在 B2C 电子商务中的应用研究[J]. 赤峰学院学报(自然科学版),2017,33(5):109-110.
[20] Mehta E, Solanki A. Minimization of mean square error for improved euler elliptic curve secure hash cryptography for textual data[J]. Journal of Information and Optimization Sciences,2017,38(6):813-826.
[21] 魏南强. 基于 SET 协议的电子商务安全问题[J]. 山东工业技术,2017(4):137.

(上接第 315 页)

[15] Liu R, Chen P Y, Peng X, et al. X-Point PUF: Exploiting sneak paths for a strong physical unclonable function design [J]. IEEE Transactions on Circuits and Systems I: Regular Papers,2018,65(10):3459-3468.
[16] Liu W Q, Zhang L, Zhang Z R, et al. XOR-based low-cost reconfigurable PUFs for IoT security[J]. ACM Transactions on Embedded Computing Systems,2019,18(3):25.

(上接第 327 页)

[6] 李校南,王雪瑞,戴紫彬,等. 可重构分簇式分组密码处理架构[J]. 计算机应用与软件,2014,31(1):315-318,326.
[7] 陈侨川. 一种基于 DES 和 RSA 算法的混合加密算法[D]. 昆明:云南大学,2015.
[8] 陈运启,张翼. 煤矿瓦斯监控系统关键数据加密算法的研究与实现[J]. 工矿自动化,2012(7):7-10.
[9] 马汝超,赵亮. 煤矿安全监控系统数据加密技术[J]. 工矿自动化,2017,43(2):15-18.