无线无源远距离可重构安全传感终端设计

邓　洋[1]，张世杰[1]，刘成旺[1]，李　征[1]，冉　君[1]，钟永明[1]，王　坚[1]，施　昶[2]，李　钢[2]
（1. 成都普什信息自动化有限公司，四川　成都　611731；2. 电子科技大学，四川　成都　610054）

摘　要：为提高无源物联网安全性能，常在传感设备中加入加密算法。而传统无源传感终端的加密算法常采用伪随机数实现，其具有极大的安全隐患，且现有产生真随机数的方法需专用真随机数产生电路，其开销大，不适用于无源传感终端。同时，现有无源传感终端的加密算法不能重构，变换方式少，安全性很难进一步提升。为此，设计了一种无线无源可重构远距离安全传感终端，其采用 MCU 实现标准 RFID 通信协议，代替专用 RFID 芯片，能根据各种应用场景修改 MCU 代码，从而实现传感终端可重构功能；基于射频信号和 ADC 残差的兼容型真随机数发生器产生真随机数，无需专用电路；采用增强型可重构加密算法，结合真随机数极大地提升了传感终端安全性能，同时，采用多源能量收集电路架构，提升了终端接收灵敏度，从而实现传感终端的远距离通信功能。

关键词：真随机数；兼容性；可重构加密算法；多源能量收集；远距离
中图分类号：TN926；TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 06. 005
引用格式：邓洋，张世杰，刘成旺，等. 无线无源远距离可重构安全传感终端设计［J］. 网络安全与数据治理，2025，44(6)：36 - 41.

Design of wireless passive long-distance reconfigurable security sensing terminal

Deng Yang[1], Zhang Shijie[1], Liu Chengwang[1], Li Zheng[1], Ran Jun[1],
Zhong Yongming[1], Wang Jian[1], Shi Chang[2], Li Gang[2]
(1. Chengdu Pushi Information Automation Co., Ltd., Chengdu 611731, China;
2. University of Electronic Science and Technology of China, Chengdu 610054, China)

Abstract: To improve the security performance of passive Internet of Things, encryption algorithms are often added to sensor devices. The traditional encryption algorithm of passive sensor terminals often uses pseudorandom numbers to encrypt data, which has great security risks, and the existing methods of generating true random numbers require a special true random number generation circuit, which is expensive and not suitable for passive sensor terminals. At the same time, the encryption algorithm in the existing passive sensor terminal cannot be reconfigured, and the conversion mode is few, so it is difficult to further improve the security. Therefore, this paper designs a wireless passive reconfigurable remote security sensing terminal. It adopts the MCU to implement the standard RFID communication protocol instead of the dedicated RFID chip and can modify the MCU code arbitrarily according to various application scenarios, thereby achieving the reconfigurable function of the sensing terminal. And it uses a compatible true random number generator based on RF signal and ADC residuals to generate true random numbers without special circuit. The enhanced reconfigurable encryption algorithm combined with true random numbers greatly improves the encryption performance of sensing terminal. At the same time, the multi-source energy collection circuit architecture improves the receiving sensitivity of the terminal, so as to realize the long-distance communication function of the sensor terminal.

Key words: true random number; compatibility; reconfigurable encryption algorithm; multi-source energy harvesting; long distance

0　引言

随着物联网应用技术的高速发展，无源 RFID 感测系统受到了广泛研究，但现有无源 RFID 感测标签通信距离短，且因小型化和低成本特性，其安全性能常被忽视，同时，现有传感终端采用专用 RIFD 芯片，无法根据实际所需参量进行修改，重构性差，且固定的加密算法安全性不高。

1999 年，Steindl 等人提出了基于声表面波的无源传

感标签[1]，其采用声表面波反射信号的相位和幅度变化，实现信息感知，并据此实现了多类型传感功能。2015 年，Lee 等人提出了一种无源氢气浓度传感系统[2]，其将传感器集成在标签天线上，通过标签反射信号的频率和功率变化测量氢气浓度，由于传感器变化会导致标签天线和标签电路不匹配，限制了标签和读写器的工作距离，使得通信距离仅 25 cm。2016 年，Abdulhadi 等人研制了一种集成太阳能和射频能量收集的 RFID 传感标签[3]，采用太阳能和射频能供电的通信距离分别可达 27 m 和 7.48 m，但其没有实现 RFID 协议处理功能，无法实现可重构，灵活性差，并且由于其天线面积较大，具有一定的安装局限性。

国内传感标签起步较晚，2020 年，Inserra 等人研制了一种基于 RFID 的螺丝松动无源传感标签[4]，其通过螺钉松/紧改变标签天线和电路匹配状态，从而改变标签反射系数，据此可测量出螺钉松/紧状态，其通信距离仅 1.3 m。2021 年，Shao 等人提出了采用线圈结构的磁场传感器结合 RFID 技术实现无源射频电流感测标签[5]，其采用磁场传感器输出的电压幅值表征电流强度，但其电流动态测量范围仅为 5 A～17.5 A，且电压信号抗干扰能力差，同时，通信距离仅 5.2 m（EIRP 为 48 dBm）。

为增强传感终端安全性能，常采用基于伪随机数的加密算法，其安全性较弱；也常采用专用真随机数产生电路，但增加了系统成本和功耗。考虑到传感终端常采用 ADC 实现数模转换，因此，为实现资源共享，减少因实现真随机数产生器添加额外硬件资源而增加的成本和功耗，本文重点研究基于 ADC 的低复杂度高兼容真随机数产生器。

2000 年，Petrie 等人提出将电阻热噪声、振荡器采样和离散时间混沌系统结合实现真随机数发生器[6]，其性能优于采用单一熵源实现的真随机数发生器。之后，Callegari 等人和 Pareschi 等人分别提出采用多个 ADC 流水线架构实现真随机数发生器[7-8]，每一级 ADC 使用 1.5 bit 的分辨率，输出 1 位随机数，并且 ADC 的输入是前一级 ADC 输出的残差信号。2020 年，Jayaraj 等人在 SAR ADC 完成后，使用比较器对 ADC 输出的最低位（残差）继续比较一次，将比较结果作为随机数，可以同时完成模数转换和产生真随机数（True Random Numter，TRN）[9]。

以上文献提出的基于 ADC 实现真随机数发生器的方法难以真正实现，只适合专用芯片，增加了系统的设计复杂度和成本。2016 年，Liu 等人提出了基于传统 MCU 的 ADC 采样电阻分压电路电压的真随机数发生器[10]，但其过度依赖电阻和电路的热噪声，当 ADC 位宽小的时候，其输出数据变化很小或根本没有变化，致使很难产生高质量的真随机数。文献［11－12］给出了使用传统微处理器和流水线 ADC 相结合的结构来实现真随机数发生器的方法，这是在微处理器上基于 ADC 实现真随机数的典型例子，但其结构复杂，难以在无线无源低功耗设备上实现。

针对上述问题，本文在不增加无源传感终端复杂度的情况下，研究兼容型真随机数发生器和可重构加密算法，并进一步研究多源能量收集电路和高灵敏度 ASK 解调电路，增强无源终端接收灵敏度，提升无源终端通信距离，并设计出无线无源可重构远距离安全传感终端。

1 无线无源可重构远距离安全传感终端设计

为提升无线无源传感系统的通信距离，本文设计了一种无线无源可重构安全传感终端，其电路架构如图 1 所示，包括天线、匹配电路、功分器、整流电路、能量收集与管理电路、解调电路、调制电路、处理器（即 MCU）及真随机数产生和加密模块、传感电路、太阳能电池。其中，太阳能电池的输出端在串联一个二极管后，与整流电路的输出端并联连接至能量收集电路，从而实现多种能源的同时收集功能。这种设计不仅降低了终端的设计成本，而且在多种能量同时存在的情况下，其能量收集速率显著高于仅依赖单一能源的能量收集速率。MCU 可用于重构多种协议，适用于多种传感应用场景，且通过 MCU 内置的 ADC 采样外围熵源电路电压，并进行一系列变换，可实现兼容型真随机数发生器。

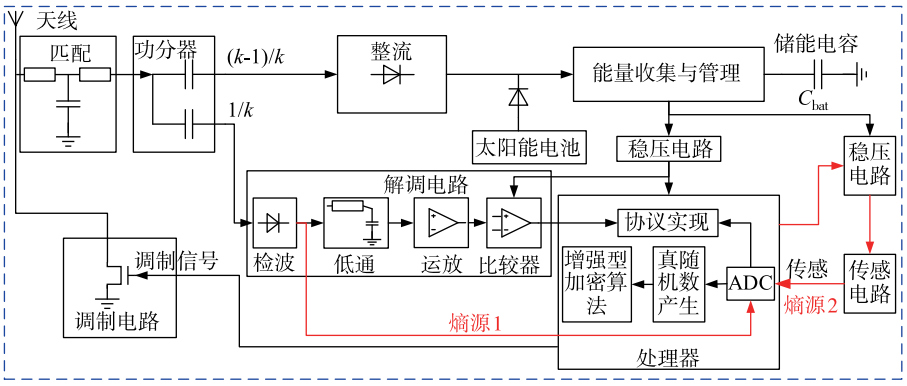


图 1　无线无源可重构安全传感终端

1.1 兼容型真随机数产生器

本文提出的兼容型真随机数产生器架构如图 1 中右下部分所示，包括熵源和处理器，熵源包括传感熵源和射频熵源，传感熵源由传感电路构成，射频熵源来自于射频收发电路的检波输出；处理器内置有 ADC，其主要用于无源传感终端进行模数转换，实现传感数据采集功能，通过 MCU 内置 ADC 采样传感熵源和射频熵源，进行适当处理产生真随机数，并将真随机数存储在存储器中。存储器中的真随机数可用于进一步循环迭代提升后处理过程中循环移位位数的随机性，从而迭代提升系统的真随机性。兼容型真随机数产生器工作流程如图 2 所示。

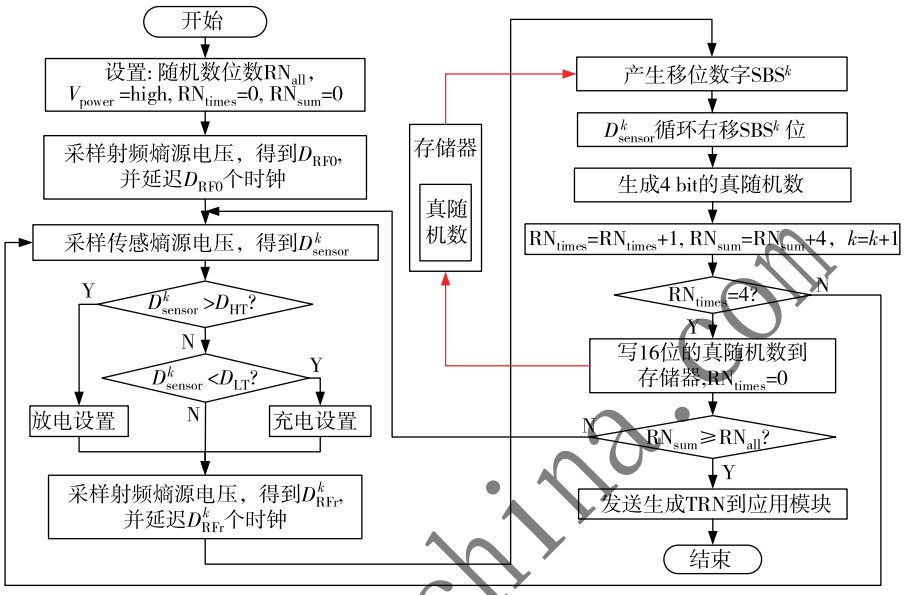


图 2 兼容型真随机数产生器工作流程

1.2 基于真随机数的增强型加密算法

鉴于 ISO/IEC 18000 标准的安全问题，我国提出的 GB/T 29768 协议增加了双向鉴别机制，结合任意加密算法，可极大地提高无源终端无线通信的安全性能。采用某一加密算法为例，其需要实现 K 次 F 函数，且需要进行 N 次子变换，如图 3 所示。通过在 F 的 N 次子变换之前将输入数据和一个 $4\times N$ bit 的真随机数进行简单的逻辑运算，可以提高 F 函数输出数据的随机性，从而提高加密算法的安全性能。由图 3 可知，增强型加密算法比原始加密算法更加安全，并且可完全兼容原始加密算法（采样逻辑或运算时，真随机数全 0 可兼容原始加密算法）。此外，用户可以根据不同的应用场景选择异或（Xor）或同或（Xnor）运算，类似重构加密算法，从而在相同数据、密钥和真随机数的情况下，也能产生完全不同的加密数据。因此增强型加密算法利用产生的真随机数改进加密算法中的函数逻辑，进而明显提升加密算法的安全性能。

1.3 远距离传感终端设计

在图 1 中，功分器用于将输入功率按 1∶K 分配至解调和整流电路。在仅有射频能量的应用中，可增加 K 值，以便将更多的能量用于能量收集。而在仅有太阳能的应用中，可减小 K 值，以确保更多能量用于解调，从而提高解调灵敏度。在多源能量收集电路架构中，为了同时实现能量收集和长距离通信，可设置 $K=2$，以实现能量均匀分配。

（1）高灵敏度解调电路设计

商用无源终端灵敏度约 -22 dBm，这需实现射频能量收集的最小输入功率，一般解调灵敏度会更高。本文讨论的 ASK 解调电路结构如图 1 所示，可通过式（1）计算出本文设计的终端解调灵敏度：

$$P_{\mathrm{tag}}^{\mathrm{sensitivity}}=P_{\mathrm{ASK}}-G_{\mathrm{tag}}+10\log\left(\frac{1}{K}\right) \tag{1}$$

其中，P_{ASK} 表示仅解调电路的灵敏度，K 是功分器的比例因子。

为实现远距离通信，采用倍压整流原理实现信号检波，提升检波输出电压，进一步采用运放放大检波信号，可极大地提升 ASK 解调灵敏度。经测试，设计的终端信号接收灵敏度可达 -45.5 dBm，依据 Friis 公式（式（2）），传感终端通信距离可达 217 m。这明显改善了传感终端的通信距离，实现了传感终端远距离通信。

$$P_{\mathrm{tag}}=P_{\mathrm{EIRP}}+G_{\mathrm{tag}}+L_{\mathrm{pol}}+10\log\left(\frac{\lambda}{4\pi R}\right)^2 \tag{2}$$

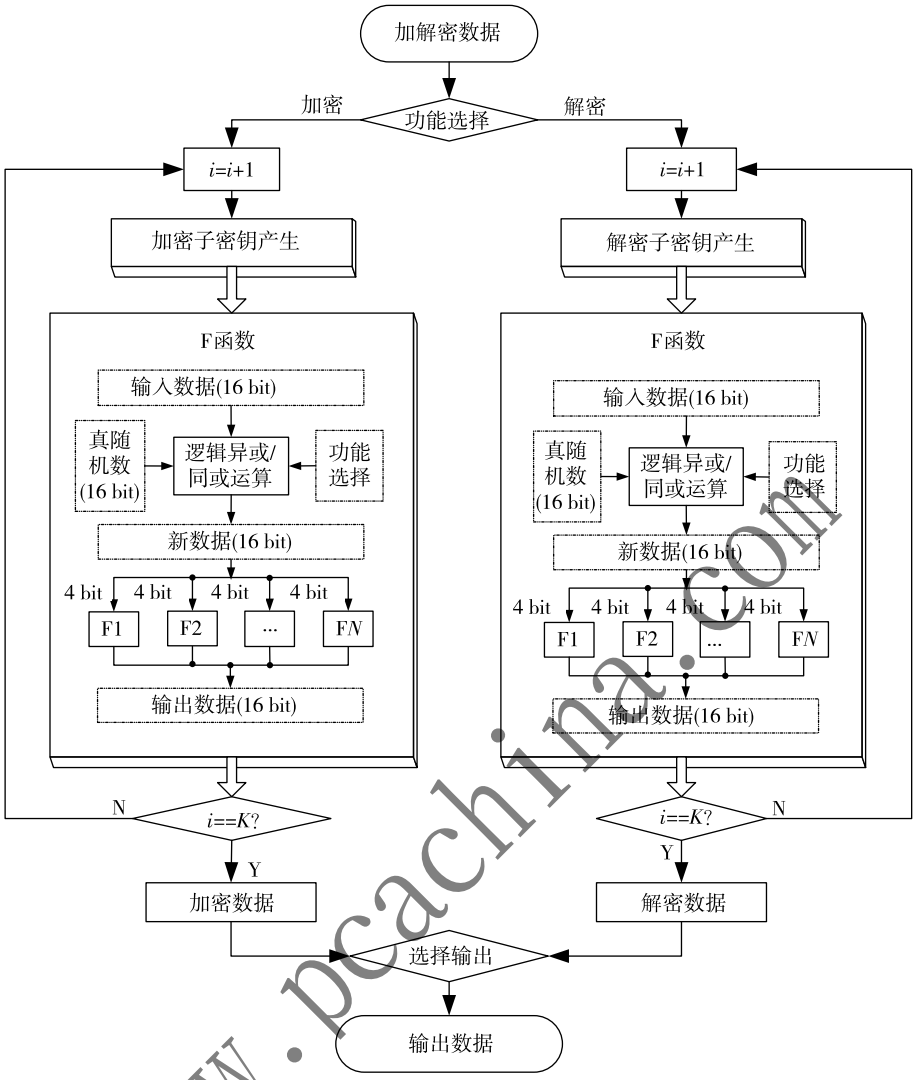


图 3　基于真随机数的增强型加密算法实现方法

（2）多源能量收集电路设计

BQ25570 是一款高度集成的能量收集纳米电源管理芯片，非常适合超低功率应用场景，其专门用于收集和管理来自光伏（太阳能）、热电发电机和射频微波产生的微瓦（μW）到毫瓦（mW）的功率。BQ25570 能够实现 DC-DC 的升压功能，其输入 VIN 低至 600 mV，并且，当 BQ25570 正常启动后，其输入 VIN 电压可以低至 100 mV。

本文提出基于 BQ25570 实现太阳能和射频能量收集与管理，其结构如图 4 所示，太阳能电池经二极管的输出和 RF-DC 输出并联连接到 BQ25570 的输入引脚，享用一个能量收集电路，减少了系统的面积，节约了成本，并能够实现能量的同时收集，降低单种能源的充电时间。同时，在 BQ25570 的输入引脚处并联一个稳压二极管，防止电压过高而损耗器件。

BQ25570 的工作过程主要包括两部分：充电过程和

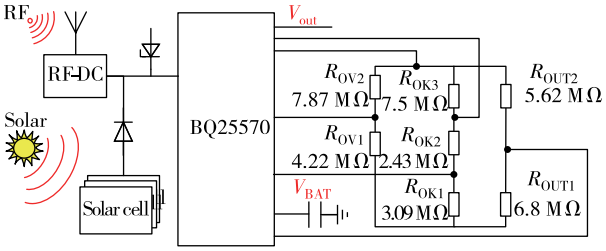


图 4　多源能量收集电路设计

放电过程。在首次充电过程中，$V_{BAT}=0$，BQ25570 开始处于冷启动（cold start）状态，随着 V_{BAT} 的增加，当 V_{BAT} 大于 V_{STOR_CHGEN}（约 1.6 V）时，BQ25570 处于正常工作状态，也叫做热启动（hot start）状态。可以通过三个可配置的参数来控制 BQ25570 的工作过程，这三个参数分别为：V_{BAT_OV}（V_{BAT} 上升的阈值电压）、$V_{BAT\_OK\_PROG}$（V_{BAT} 下降的阈值电压）和 $V_{BAT\_OK\_HYST}$（V_{BAT} 开始放电的

阈值电压）。这三个参数的具体值可通过 7 个电阻来设置，如图 4 所示。

V_{BAT_OV}的计算公式如下：

$$V_{BAT\_OV} = \frac{3}{2} V_{BIAS}\left(1 + \frac{R_{OV2}}{R_{OV1}}\right) \tag{3}$$

其中，V_{BIAS}是固定值，约为 1.21 V，根据图 4 中的电阻值，可以计算出 V_{BAT_OV} 约为 5.2 V，因此，当 V_{BAT} > 5.2 V时，关闭主充电泵，并且 V_{BAT}最高为 5.5 V。

$V_{BAT_OK_PROG}$的计算公式如下：

$$V_{BAT\_OK\_PROG} = V_{BIAS}\left(1 + \frac{R_{OK2}}{R_{OK1}}\right) \tag{4}$$

根据图 4 中的电阻值可以计算出 $V_{BAT\_OK\_PROG}$ 约为 2.2 V，因此，当 V_{BAT} <2.2 V 时，V_{out} =0。

$V_{BAT_OK_HYST}$的计算公式如下：

$$V_{BAT\_OK\_HYST} = V_{BIAS}\left(1 + \frac{R_{OK2} + R_{OK3}}{R_{OK1}}\right) \tag{5}$$

根据图 4 中的电阻值可以计算出 $V_{BAT\_OK\_HYST}$ 约为 5.1 V，因此，在 V_{BAT}的充电过程中，当 V_{BAT} >5.1 V 时，开始放电，也就是 V_{out}开始输出，其输出电压通过如下公式计算：

$$V_{out} = V_{BIAS}\left(\frac{R_{OUT2} + R_{OUT1}}{R_{OUT1}}\right) \tag{6}$$

根据图 4 中的电阻值，可以计算出 V_{out} 约为 2.4 V，其为标签的有源电路供电。

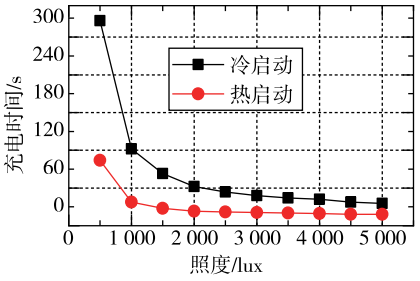
2　传感标签性能测试验证

本文测试不同光照强度下能量收集充电时间（电容充满），并测试光照强度为 500 lux 和射频输入能量为 −8 dBm时，能量收集充电过程，测试数据如图 5 所示。

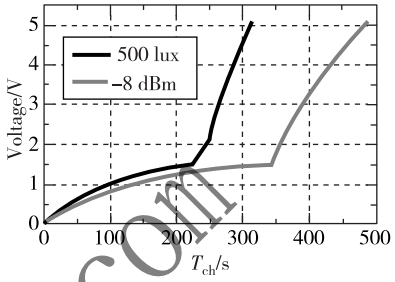
图 5（a）显示了在不同光照强度下，无线能量收集系统的冷热启动时间，可以看出，在光照强度为 500 lux 时，冷启动充电时间约 330 s（可将电容充满），说明无线能量收集系统在光照强度为 500 lux 时能够收集到足够的能量。在图 5（b）中分别给出了光照强度为 500 lux 和射频输入功率为 −8 dBm 时的冷启动充电过程，其分别在约 330 s 和 490 s 可将电容充满，说明设计的无源传感终端可分别收集光能和射频能量实现自供电功能。进一步地，若在室外工作，直接采用光能收集技术，结合设计的高灵敏度解调电路，无源传感终端通信距离可以达到 217 m。

3　结束语

本文设计了一款无线无源可重构安全传感终端，其采用 MCU 实现 RFID 协议，代替专用 RFID 标签，可实现多种协议重构功能，采用基于射频信号和 ADC 残差的兼容型真随机数产生方法，并基于产生的真随机数设计了增强型可重构加密算法，在不增加无线无源传感终端资



(a)不同光照强度下的充电时间



(b)多源能量同时收集充电过程

图 5　多源能量收集测试数据

源情况下提升了其安全性能。进一步采用多源能量收集技术提升了终端无线能量收集性能，且提升了标签接收灵敏度，测试结果显示，标签接收灵敏度达到 −45.5 dBm，理论通信距离达到 217 m，远超传统 RFID 系统 20 m 的通信距离。本文的无线无源可重构安全传感终端设计方法和测试结果可为无源物联提供参考。

参考文献

[1] STEINDL R, POHL A, SEIFERT F. Impedance loaded SAW sensors offer a wide range of measurement opportunities [J]. IEEE Transactions on Microwave Theory and Techniques, 1999, 47 (12): 2625 – 2629.

[2] LEE J S, OH J, JUN J, et al. Wireless hydrogen smart sensor based on Pt/Graphene-immobilized radio-frequency identification tag [J]. ACS Nano, 2015, 9 (8): 7783 – 7790.

[3] ABDULHADI A E, ABHARI R. Multiport UHF RFID-tag antenna for enhanced energy harvesting of self-powered wireless sensors [J]. IEEE Transactions on Industrial Informatics, 2016, 12 (2): 801 – 808.

[4] INSERRA D, HU W, LI Z, et al. Screw relaxing detection with UHF RFID tag [J]. IEEE Access, 2020, 8: 78553 – 78564.

[5] SHAO Z, WEN Y, XU Z, et al. Cable current detection with passive RF sensing tags [J]. IEEE Transactions on Industrial Electronics, 2022, 69 (1): 930 – 939.

[6] PETRIE C S, CONNELLY J A. A noise-based IC random number generator for applications in cryptography [J]. IEEE Trans. Circuits Syst. I, 2000, 47 (5): 615 – 621.

[7] CALLEGARI S, ROVATTI R, SETTI G. Embeddable ADC-based

true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos [J]. IEEE Trans. Signal Process., 2005, 53 (2): 793 – 805.

[8] PARESCHI F, SETTI G, ROVATTI R. Implementation and testing of high-speed CMOS true random number generators based on chaotic systems [J]. IEEE Trans. Circuits Syst. I, 2010, 57 (12): 3124 – 3137.

[9] JAYARAJ A, GUJARATHI N N, VENKATESH I, et al. 0.6V-1.2 V, 0.22 pJ/bit true random number generator based on SAR ADC [J]. IEEE Trans. Circuits Syst. II, 2020, 67 (10): 1765 – 1769.

[10] LIU J, MAO J, LIU P. Design and implement of a MCU based random number generater [C]//2016 11th International Conference on Computer Science & Education (ICCSE), 2016: 945 – 948.

[11] FABBRI M, CALLEGARI S. Very low cost entropy source based on chaotic dynamics retrofittable on networked devices to prevent RNG attacks [C]// 2014 21st IEEE International Conference on Electronics, Circuits and Systems (ICECS), 2014: 175 – 178.

[12] CALLEGARI S, FABBRI M, BEIRAMI A. Very low cost chaos-based entropy source for the retrofit or design augmentation of networked devices [J]. Analog Integrated Circuits and Signal Processing, 2016, 87 (2): 155 – 167.

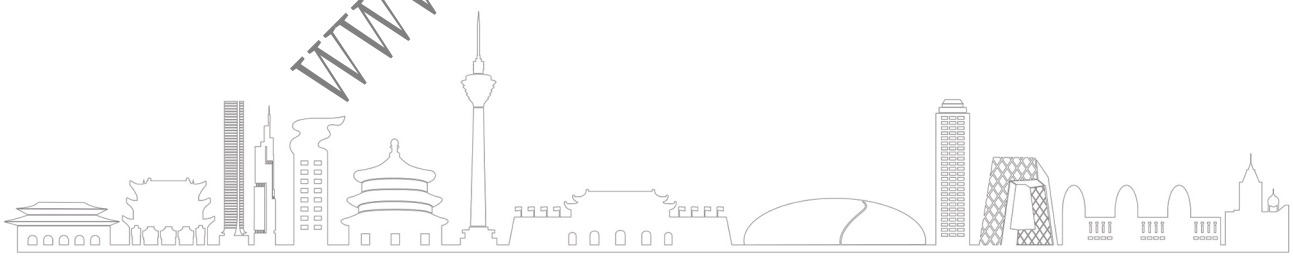
(收稿日期: 2025 – 03 – 31)

作者简介:

邓洋 (1981 –), 男, 硕士, 高级工程师, 主要研究方向: 物联网及工业互联网、智能终端、信息安全。

张世杰 (1973 –), 男, 硕士, 高级工程师, 主要研究方向: 物联网及工业互联网应用、智能终端、信息安全。

李钢 (1986 –), 通信作者, 男, 博士, 副研究员, 主要研究方向: 无源物联网、通信导航、嵌入式软件系统。E-mail: ligangpm@ uestc. edu. cn。



版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部