Chaotic-based Security for Near Field Communication in Internet of Things devices

COLIN SOKOL KUKA

JAMES CHANDLER

MOHAMMED ALKAHTANI

PRESENTER :

Colin Sokol Kuka, PhD

UNIVERSITY OF YORK

sk1759@york.ac.uk

THE CITY OF LIVERPOOL COLLEGE

colin.kuka@liv-coll.ac.uk

Colin Sokol Kuka

15.69 · University of York · Edit

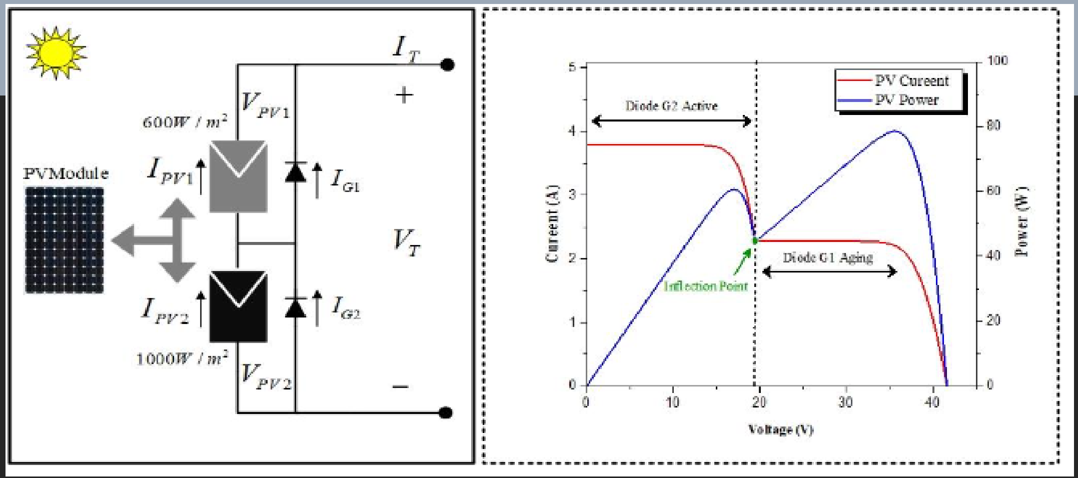
Researcher at the University of York

Lecturer and Programme Leader Electrical and Electronic Engineering at The City of Liverpool College

Research interests:

Control and Security Wireless Power Transfer, Memristor, Artificial Intelligence, [1-2]

Algorithms in Photovoltaic Management Systems [3-5]



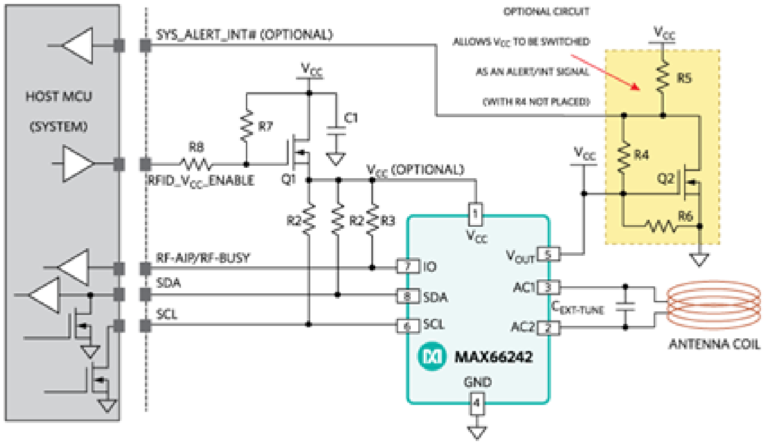
Near Field Communication NFC

Near Field Communication

- ❑Easy to use
- ❑Portable
- ❑Key , Ticket, ...

Security?

Near Field Communication NFC

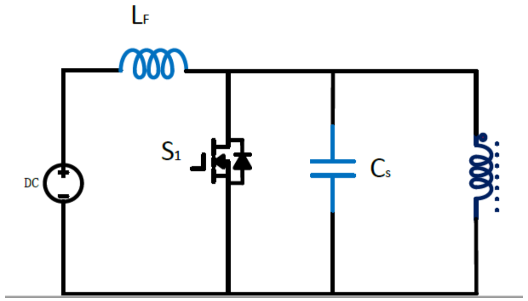


NFC is based on Secure Hash Algorithms (SHA-256)

Based on the “Hash function”

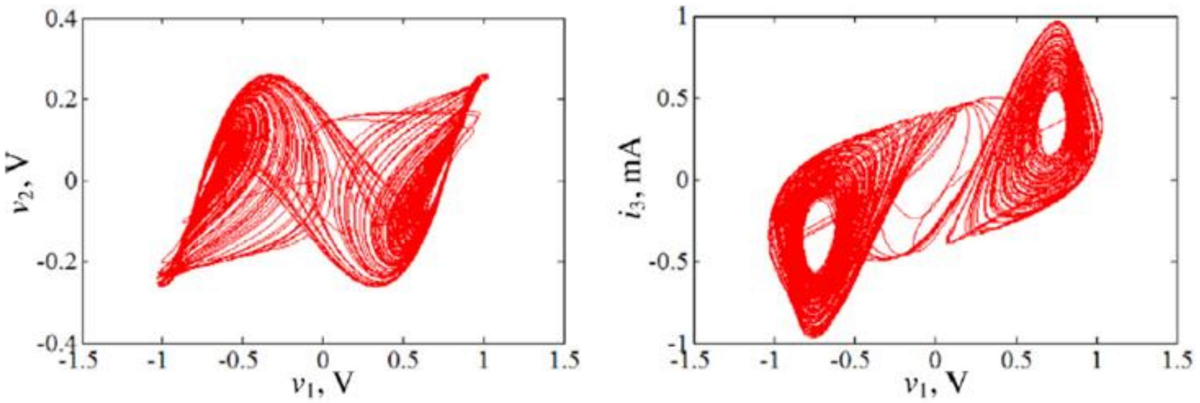
https://www.xorbin.com/tools/sha256-hash-calculator

New Topology of NFC



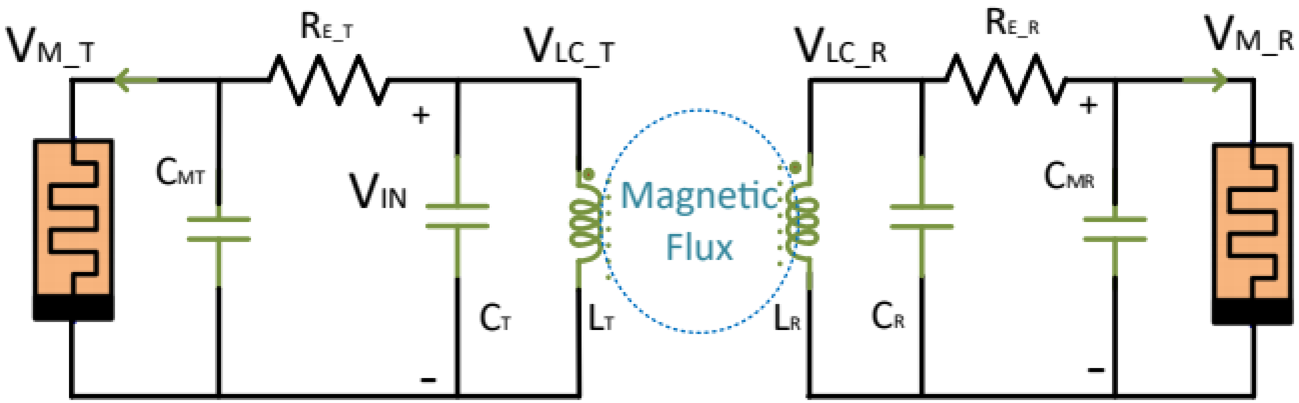
- Switch Power dissipation
- Additional circuit to control the switching time
- Security issues – based on algorithms

- Memristors



Highest Level of Encryption

New Topology of NFC

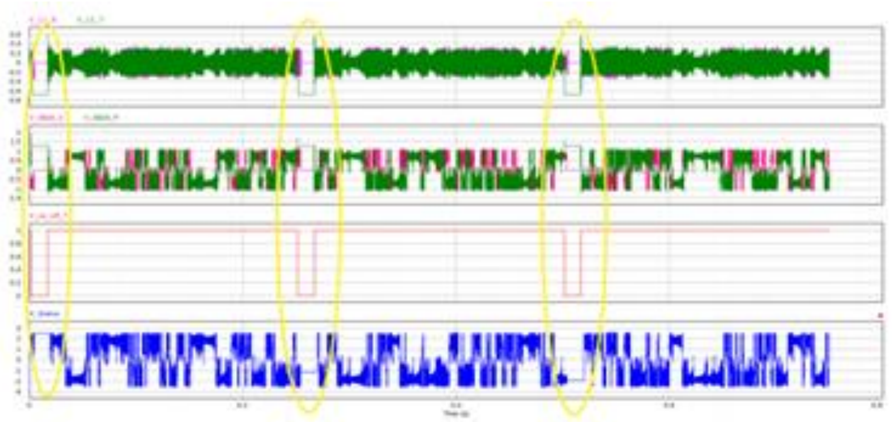


- No switches
- No Additional circuit
- Highest Level of Security – No Copy

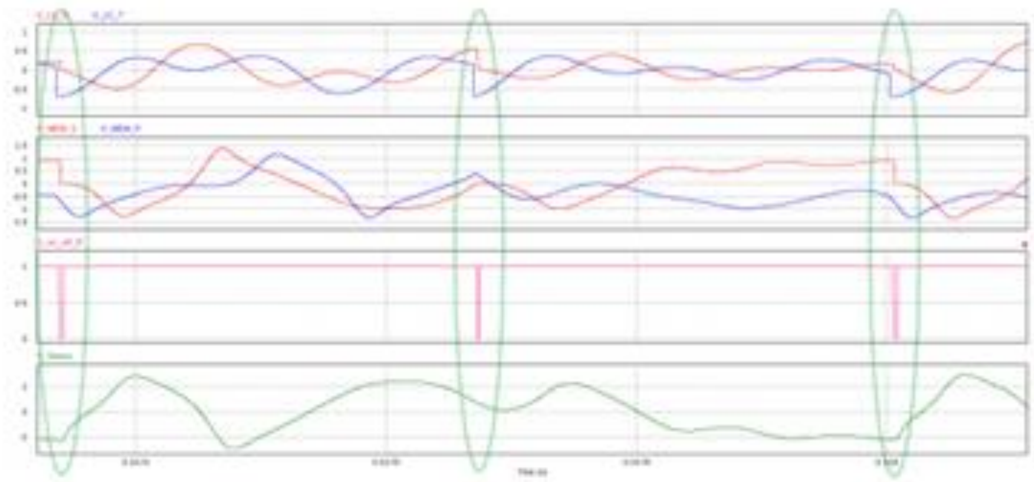
	WTP (NFC)	M-WPT
Power	Transmitted (Harvested)	Harvested
Data	Oscillation	Chaos
Distance	Over 30 cm (10 cm)	10 cm
Operating Frequency	Up to 13.5 MHz	Up to 7 KHz
Control	Timing, Switches and Data Algorithm	Data
Receivers	Many	Only one

[2]

Simulations



Time step of the chaotic behaviour when the receiver is disconnected (highlighted in yellow): the LC and memristor voltage V_{LC} and V_M in receiver and transmitter, in purple and green respectively. At the disconnection (in the 3^{rd} graph), the receiver memristor holds its last status as shown in the 4^{th} graph in blue.



Data transmission at 3Kbps, it is possible to notice the time of switching (highlighted in green) the chaotic behaviour in the LC, the memristor voltage and the internal status in the 4^{th} graph.

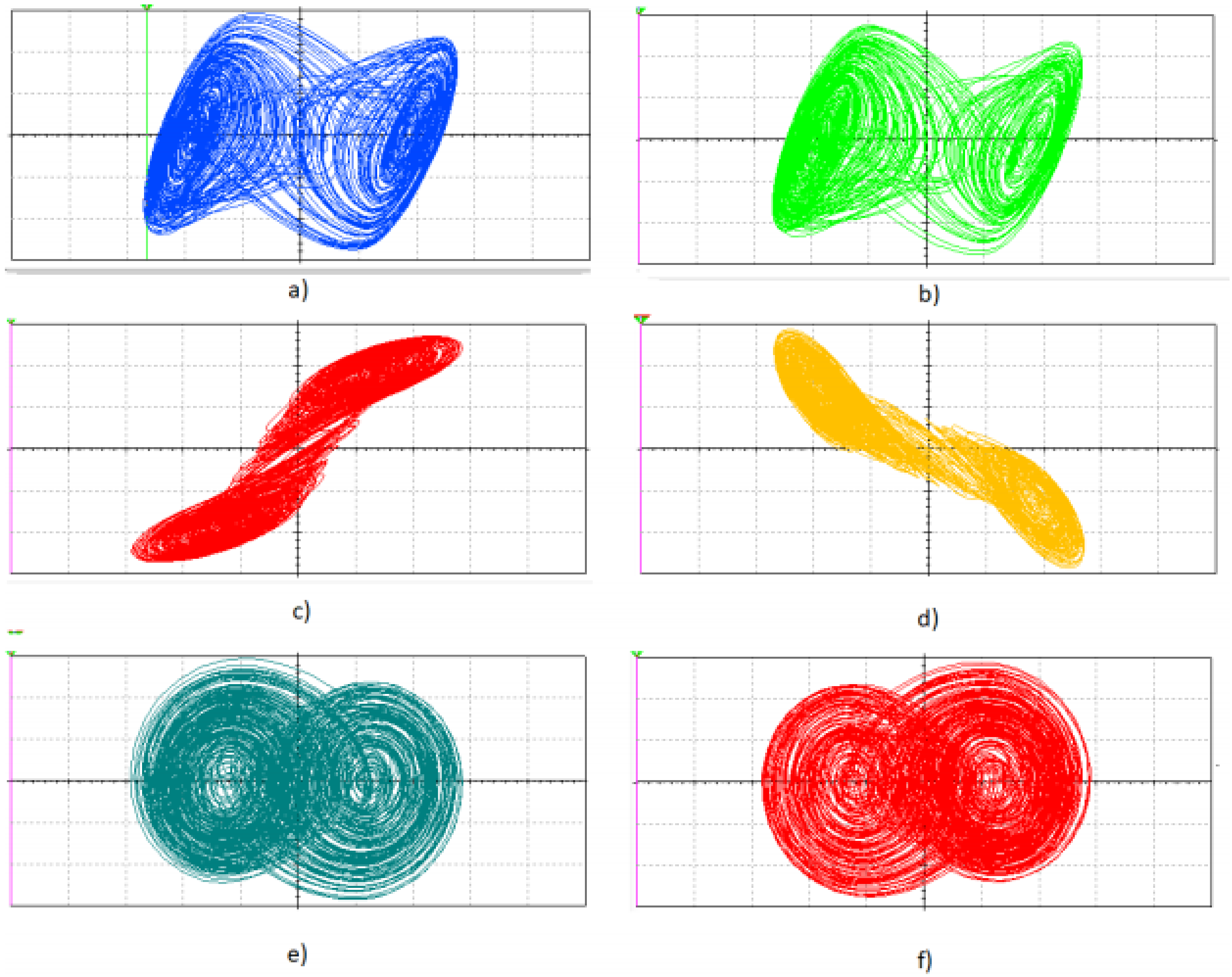
Chaotic waveform

Synchronisation of Chaotic waveforms:

$$\begin{cases} \frac{dv_1}{dt} = \frac{1}{C_1}[(v_2 - v_1)G - f(v_d)] \\ \frac{dv_2}{dt} = \frac{1}{C_2}[(v_2 - v_1)G - i_L] \\ \frac{di_3}{dt} = -\frac{1}{L_T}[v_2 - R_0 i_3] \end{cases}$$

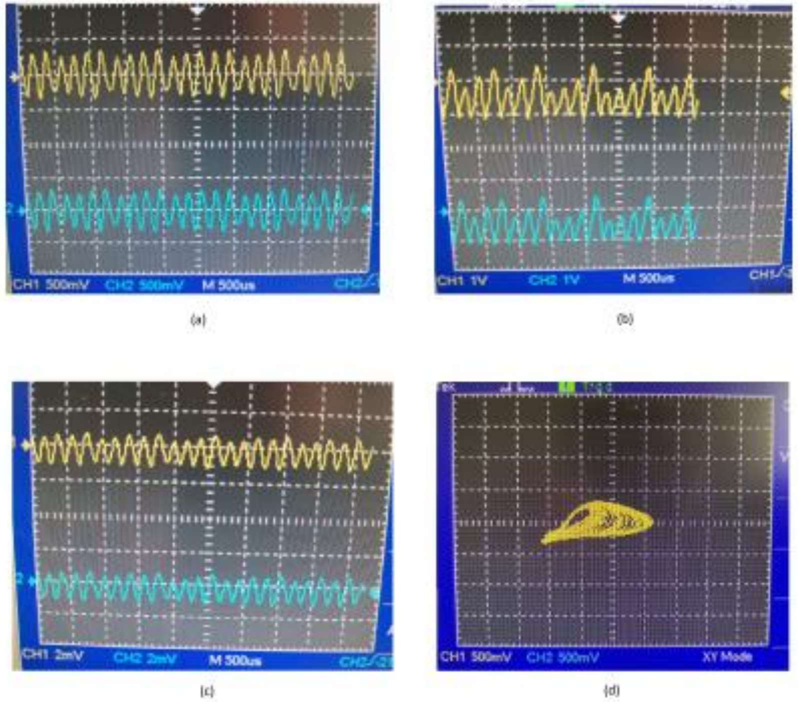
where the $f(v_d)$ is the diode function:

$$f(v_d) = G_b v_1 + 0.5(G_a - G_b)[|v_1 + B_p| - |v_1 - B_p|]$$

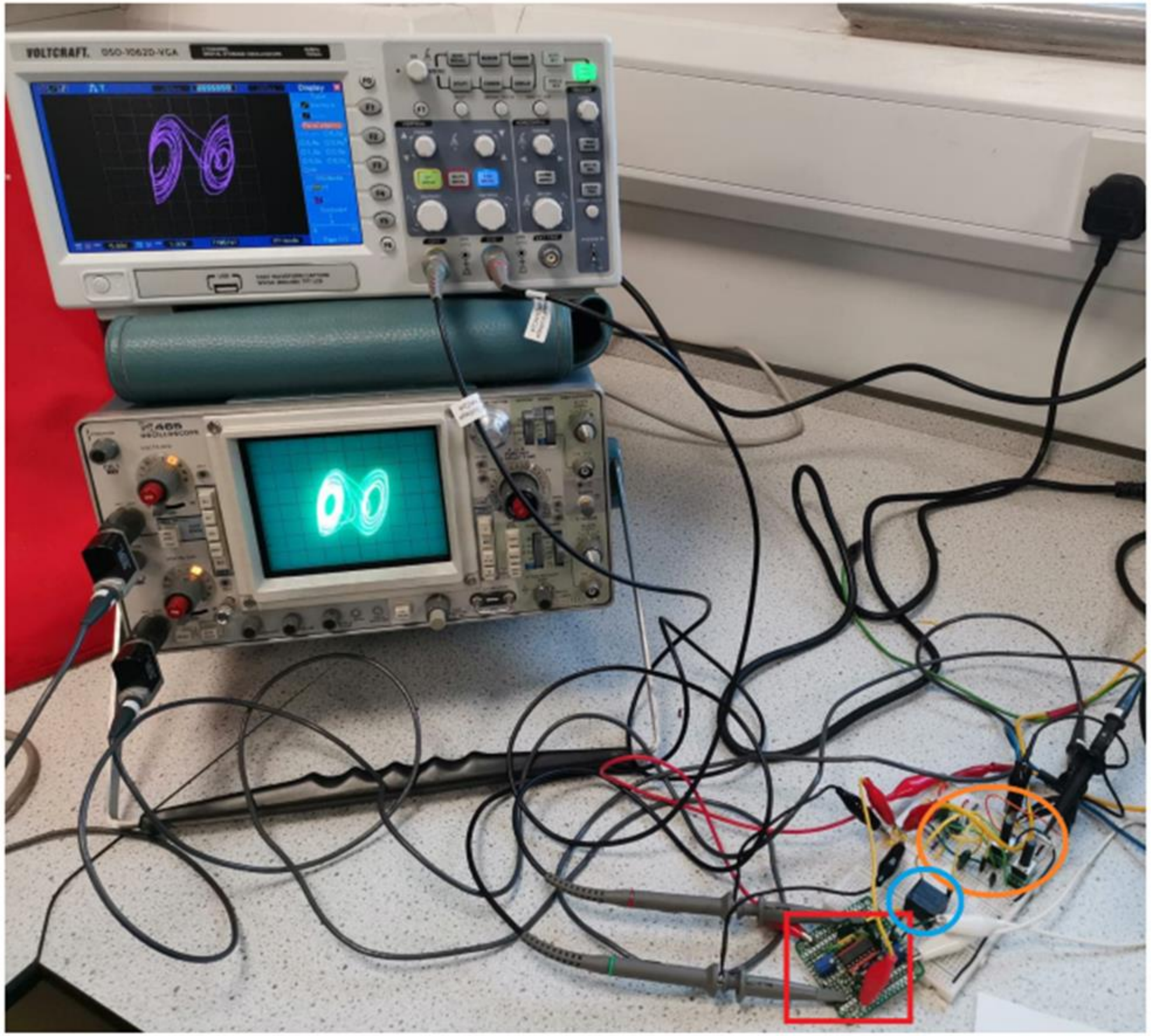


Synchronisation of the phase portraits of a chaotic attractor: voltage in the inductor V_{LC} referred to the memristor voltage V_M in the transmitter (a) and receiver(b) coil; current in the inductor i_L referred to the memristor voltage V_M in the transmitter (c) and receiver (d) coil; the memristor voltage V_M referred to its internal voltage status V_0 in the transmitter (e) and receiver (f).

Experiments

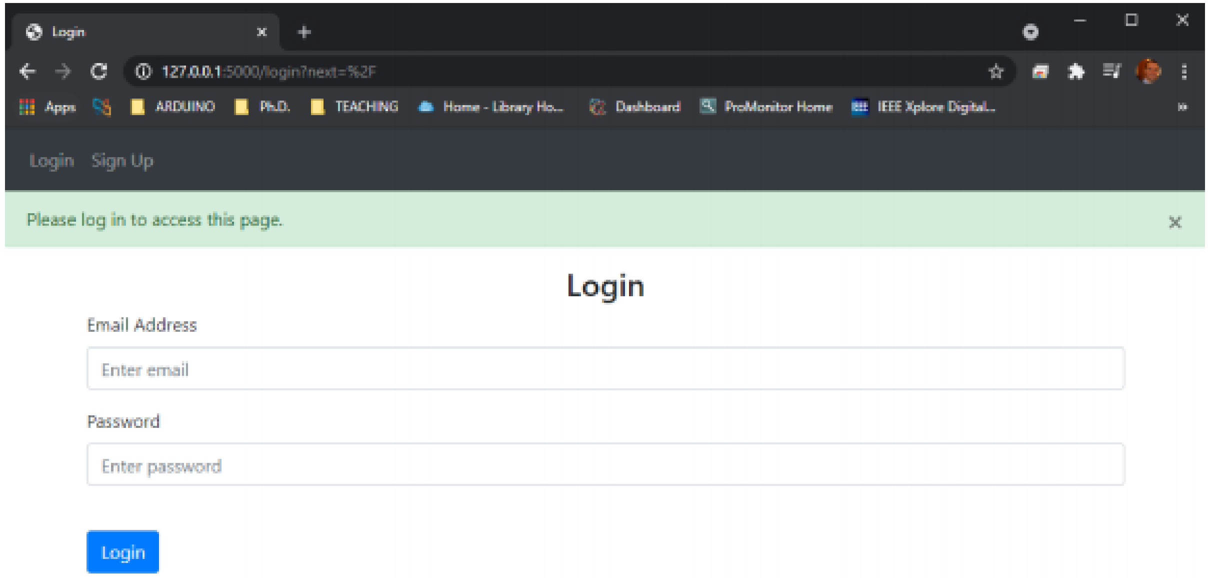


Experiment results: a) chaotic behaviour of the voltage in the primary (yellow) and secondary (blue) coil; voltage in the the primary (yellow) and secondary (blue) memristor; c) voltage in R = 1 Ω for current measure in the primary (yellow) and secondary (blue) coil; d) XY-plot of the single attractor phase portrait.

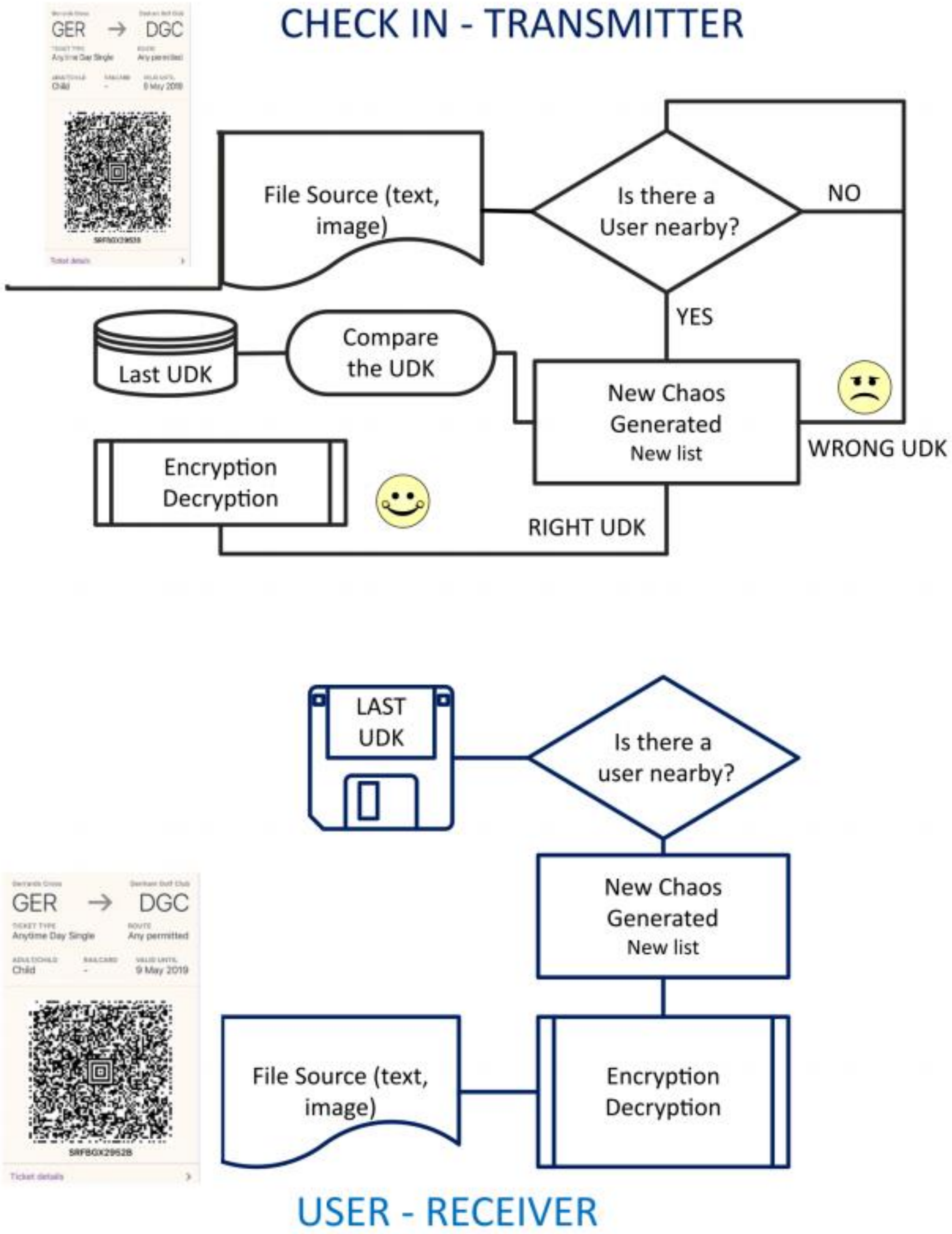


The prototype transmitter highlighted in orange, the receiver in red and the coupling transformer in blue.

IoT web application



Use of Python and use chaotic encryption for web resources.



Flowchart of the entry system described in steps.

References

[1] Kuka, S., Ni, K. and Alkahtani, M., 2020. A review of methods and challenges for improvement in efficiency and distance for wireless power transfer applications. *Power Electronics and Drives*, *5*.

[2] Kuka, C.S., Hu, Y., Xu, Q. and Alkahtani, M., 2020. An Innovative Near-Field Communication Security Based on the Chaos Generated by Memristive Circuits Adopted as Symmetrical Key. *IEEE Access*, *8*, pp.167975-167984.

[3] Alkahtani, M., Hu, Y., Alghaseb, M.A., Elkhayat, K., Kuka, C.S., Abdelhafez, M.H. and Mesloub, A., 2021. Investigating Fourteen Countries to Maximum the Economy Benefit by Using Offline Reconfiguration for Medium Scale PV Array Arrangements. Energies, 14(1), p.59.

[4] Alkahtani, M., Wu, Z., Kuka, C.S., Alahammad, M.S. and Ni, K., 2020. A Novel PV array reconfiguration algorithm approach to optimising power generation across non-uniformly aged PV arrays by merely repositioning. J—Multidisciplinary Scientific Journal, 3(1), pp.32-53.

[5] Wu, Z., Li, W., Kuka, S. and Alkahtani, M., 2019, October. Analysis of dust deposition on PV arrays by CFD simulation. In *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society* (Vol. 1, pp. 5439-5443). IEEE.