SPP 2253 Nano Security funded by DFG

On the design of genetic analogue keys for biologically logic-locked circuits for Nano-security applications

Animesh Pratap Singh[1], Elmira Moussavi[2], Daniyar Kizatov[1,2], Dominik Sisejkovic[2], Xuan Thang Vu[1], Sven Ingebrandt[1], Rainer Leupers[2], Farhad Merchant[2], Vivek Pachauri[1]

1. Institute of Materials in Electrical Engineering 1, RWTH Aachen University, Sommerfeldstrasse 24, 52074 Aachen, Germany.
2. Institute for Communication Technologies and Embedded Systems, RWTH Aachen University, Kopernikusstraße 16, 52074 Aachen

Introduction

Logic-locking has emerged as one of the frontline techniques in securing the integrated circuits from hardware attacks – which usually find their origins in the vulnerabilities related to the manufacturing and supply line. Despite being efficient, logic locking is not entirely secure from hardware attacks because of inherent limitations in digital key gates. An alternative to this is the idea of 'BioKeyGates (BioKGs)' that uses 'genetic analogue keys' for the logic locking. BioKGs not only provide a more secure platform, but also re-configurability post manufacturing [1]. Here, we have discussed about designing the genetic analogue keys and challenges & opportunities in the state of the art.

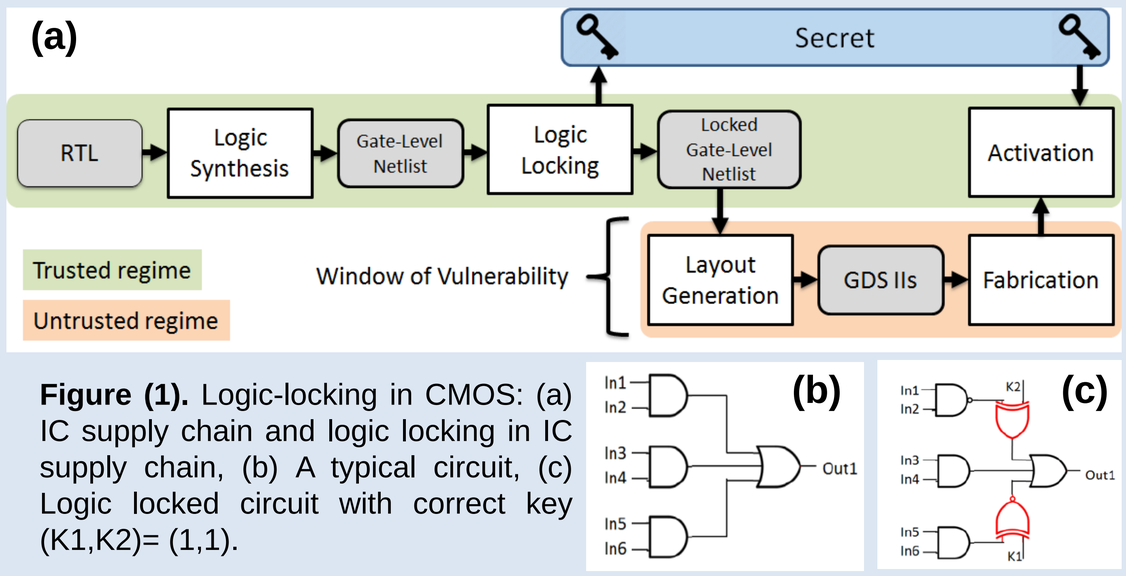


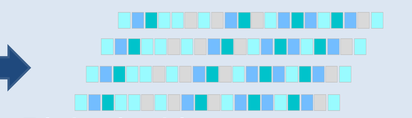
Figure (1). Logic-locking in CMOS: (a) IC supply chain and logic locking in IC supply chain, (b) A typical circuit, (c) Logic locked circuit with correct key (K1,K2)= (1,1).

Genetic Keys in the Logic-Locking Framework

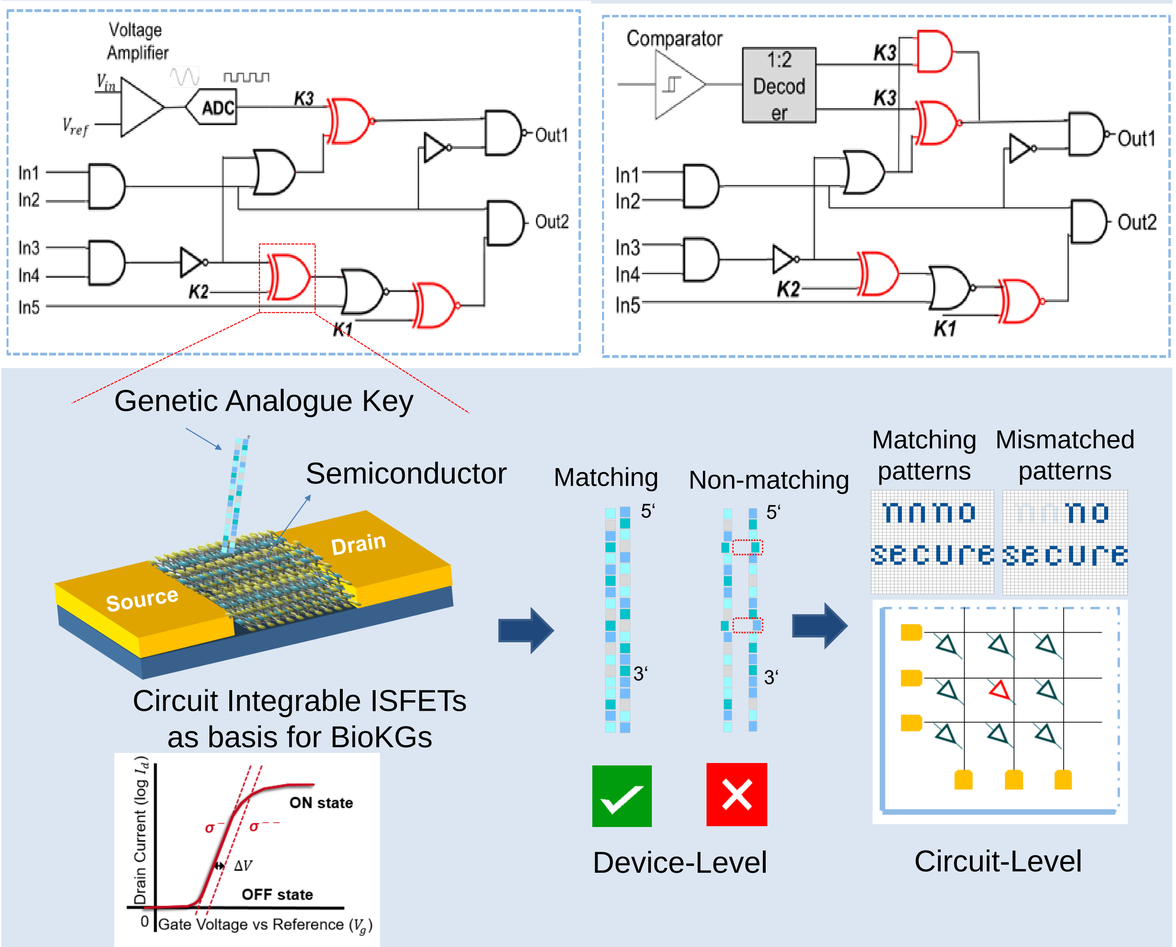
…1001001110001…. Binary code

…200100211001…. Triplet code

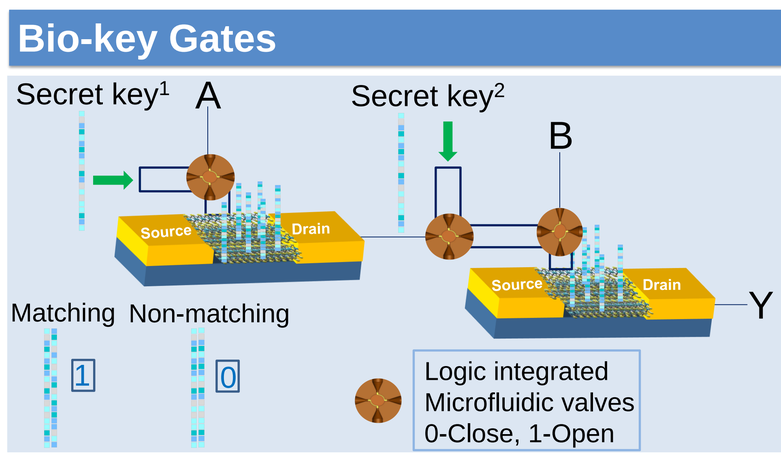
…TACAACGCGA…. DNA code



Biological key sequences



Bio-key Gates



A	B	Y
0	0	0
0	1	0
1	0	0
1	1	1

Information Encoding into Analogue (genetic) Keys

Encoding

Challenges & Opportunities

1. Encoding technology:
   - Prone to high error in encoding larger sequences (>300 nts) limiting the amount of encoded information for BioKGs [2].
   - Development of new, dedicated error correction code schemes.
2. Analogue-key recognition technology:
   - High specificity ISFET-based detection optimal only for sequence length (10-25 nts).
   - Development of alternative approaches to overcome sequence lengths and specificity issues with circuit integratable ISFETs.

Conclusion

DNA as an analogue key for Bio-KGs in logic-locking offers a promising nano-security paradigm. There are certain limitations in converting secret information into genetic analogue-key (Error free encoding) and reading with ISFETs (sensitivity and specificity) mainly due to the length of the analogue-key sequence. As part of BioNanoLock project, we aim first at overcoming the specific challenges as discussed above towards carrying out logic-integration of BioKGs as an alternative logic locking scheme.

References

[1] I. Polian et al., "Nano Security: From Nano-Electronics to Secure Systems," 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2021, pp. 1334-1339, doi: 10.23919/DATE51398.2021.9474187.

[2] Meiser, L.C., Antkowiak, P.L., Koch, J. *et al.* Reading and writing digital data in DNA. *Nat Protoc* 15, 86–101 (2020).

[3] Hwang, M. T., et al. (2016). "Highly specific SNP detection using 2D graphene electronics and DNA strand displacement." Proc Natl Acad Sci U S A 113(26): 7088-7093.

Acknowledgements

The authors thank the DFG for funding the research project "Bio-Nanoelectronic based Logic Locking for Secure Systems (BioNanoLock)" Nr. 440055779 and Project Nr. 445865083.

Animesh Pratap Singh, M. Sc.
Institute of Materials in Electrical Engineering 1
RWTH Aachen University
Sommerfeldstr. 24, 52074 Aachen, Germany
singh@iwe1.rwth-aachen.de

NESSY
Fall School on
Nano-Electronics for Secure Systems