Chips cloning technique

Integrated circuits can be compromised using Undetectable hardware Trojans

From <https://thehackernews.com/2013/09/Undetectable-hardware-Trojans.html>

M 1:120

A team of researchers from the U.S. and Europe has developed a Hardware Trojan, which is an undetectable to many techniques, raising the question on need of proper hardware qualification.
They released a paper on stealthy Dopant-Level Hardware Trojans, showing how integrated circuits used in computers, military equipment and other critical systems can be maliciously compromised during the manufacturing process.
"*In this paper we propose an extremely stealthy approach for implementing hardware Trojans below the gate level, and we evaluate their impact on the security of the target device. Instead of adding additional circuitry to the target design, we insert our hardware Trojans by changing the dopant polarity of existing transistors.*" states the paper abstract.

Personal Identification Chip that is about the size of a grain of rice and implanted under the skin.

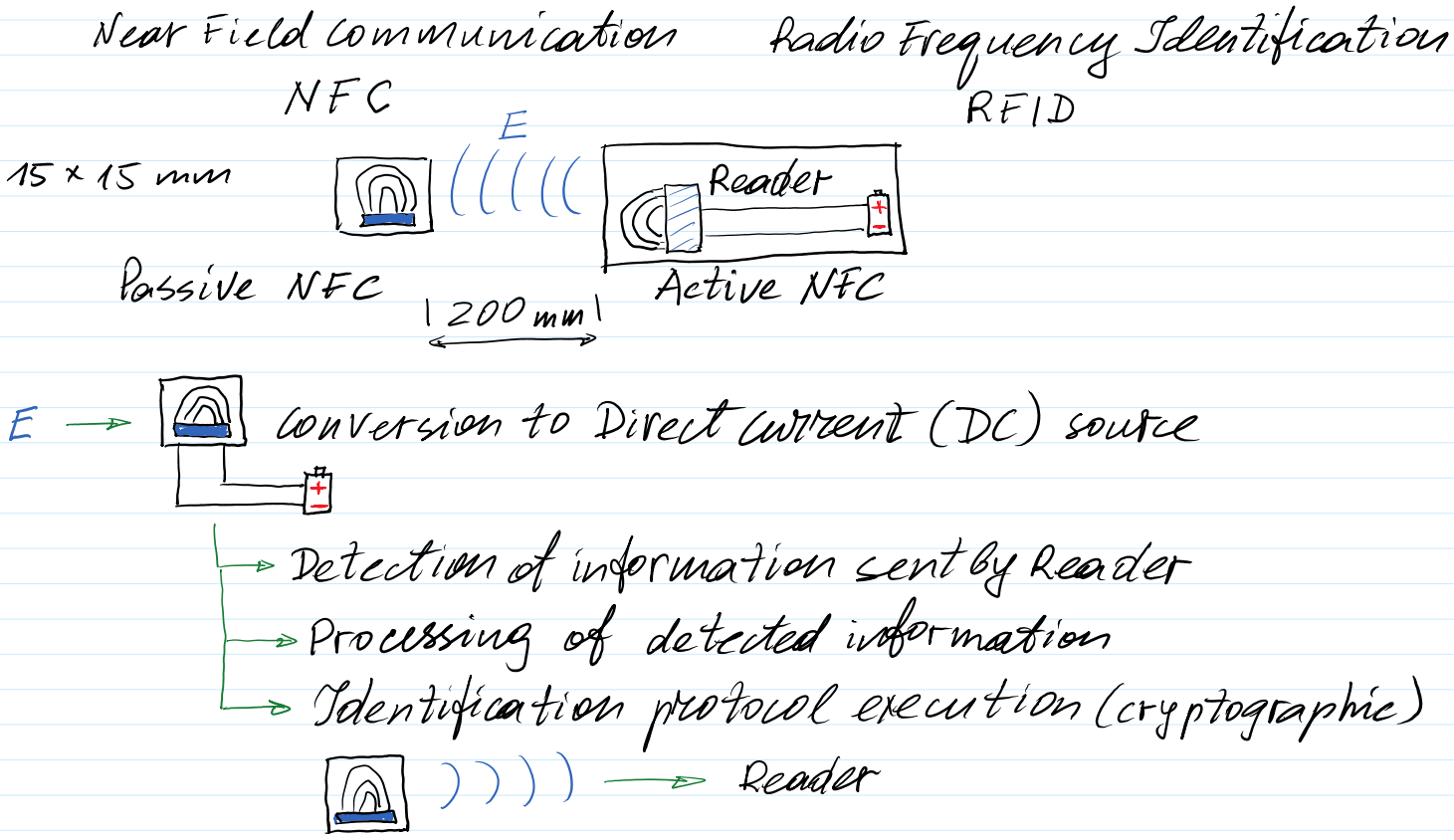
Would YOU let your boss implant you with a microchip? Belgian firm offers to turn staff into cyborgs to replace ID cards.

Read more: http://www.dailymail.co.uk/sciencetech/article-4203148/Company-offers-RFID-microchip-implants-replace-ID-cards.html#ixzz57Z0aeYgj
Follow us: @MailOnline on Twitter | DailyMail on Facebook

From <http://www.dailymail.co.uk/sciencetech/article-4203148/Company-offers-RFID-microchip-implants-replace-ID-cards.html>

Near Field communication NFC

Radio Frequency Identification



INTRINSIC ID

***Intrinsic* ID SRAM PUF Technology & Solutions: Physically Unclonable Function**

Intrinsic ID delivers strong, device-unique data security and authentication solutions for the connected world. These authentication solutions are based on Intrinsic ID's patented SRAM Physical Unclonable Function or SRAM PUF technology.

Using this technology, security keys and unique identifiers can be extracted from the innate characteristics of each semiconductor. Similar to biometrics measures, these identifiers cannot be cloned, guessed, stolen or shared. Keys are generated only when required and don't remain stored on the system, hence providing the highest level of protection.

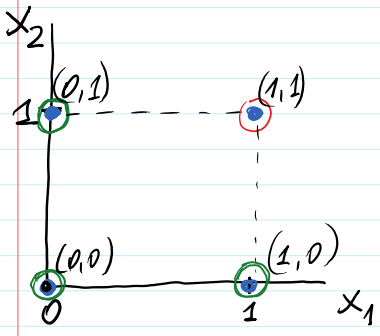
Our SRAM PUF-based security solutions are very suitable for applications such as secure key generation and storage, device authentication, flexible key provisioning and chip asset management. They can be used to secure payments, to protect highly sensitive data, for anti-counterfeiting and anti-cloning, to prevent identity theft, piracy of media content and software apps, software reverse engineering, and more.

Intrinsic ID's security solutions are available as hard and soft Intellectual Property (IP) and are used by companies who want a proven, easy and cost-efficient way to provide a solid trust base within their devices and applications.

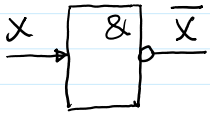
From <https://www.intrinsic-id.com/sram-puf-technology-solutions/>

Principle of work with logical gates

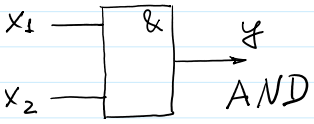
Logical Inversion, AND, NAND : $x \in \{0,1\}$; $x_1, x_2 \in \{0,1\}^2$

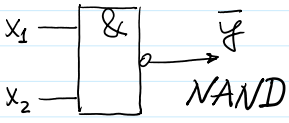


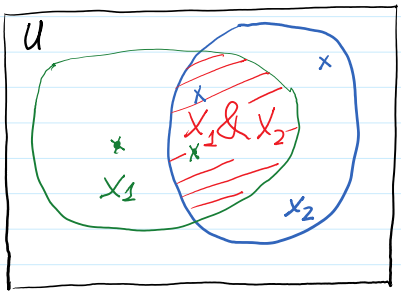
x	$\bar{x}$
0	1
1	0

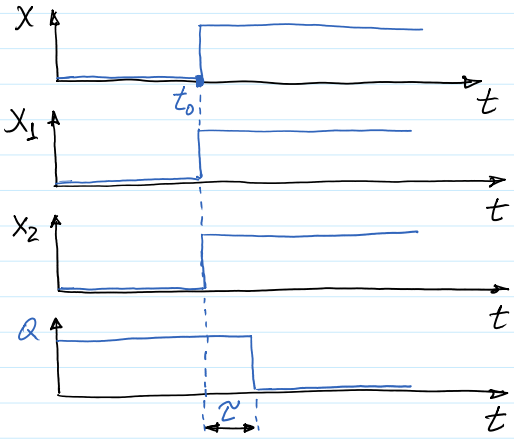


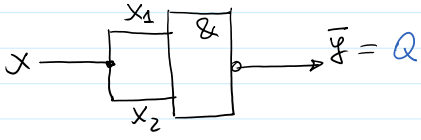
x_1	x_2	$y = x_1 \& x_2$	$\bar{y} = \overline{x_1 \& x_2}$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	0







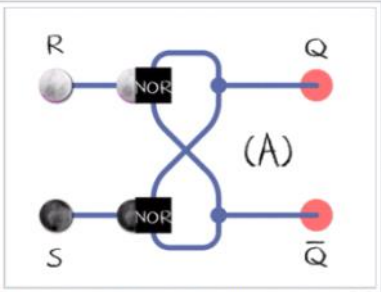




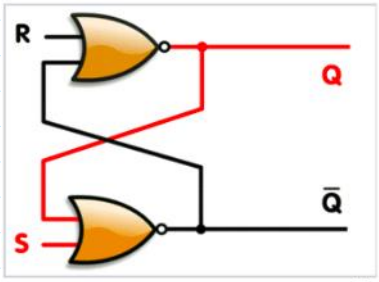
x_1	x_2	x	$\bar{y} = Q$
0	0	0	1
1	1	1	0

Flip-flop (electronics)

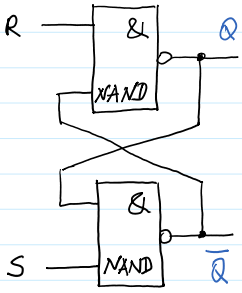
From <https://en.wikipedia.org/wiki/Flip-flop_(electronics)>



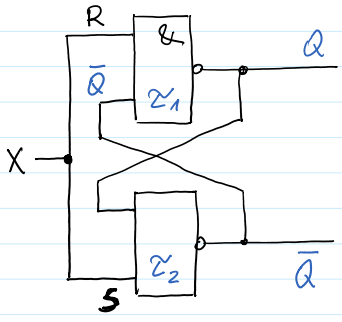
An animated SR latch. Black and white mean logical '1' and '0', respectively.
(A) S = 1, R = 0: set
(B) S = 0, R = 0: hold
(C) S = 0, R = 1: reset
(D) S = 1, R = 1: not allowed
The restricted combination (D) leads to an unstable state.



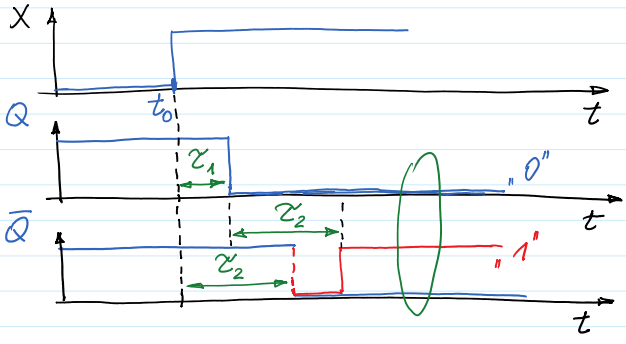
An animation of a SR latch, constructed from a pair of cross-coupled NOR gates. Red and black mean logical '1' and '0', respectively.

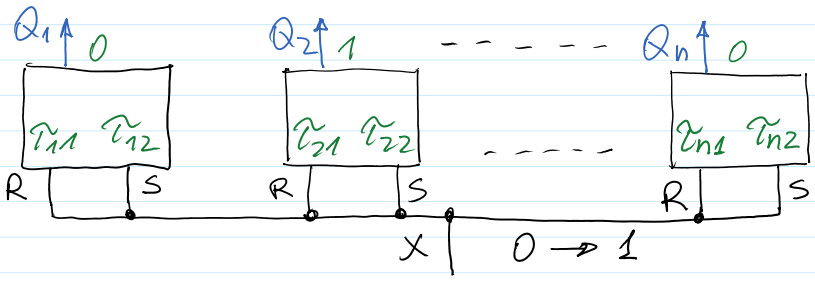


R	S	Q	$\bar{Q}$
1	0	0	1
1	1	0	1
0	1	1	0
1	1	1	0
0	0	1	1
1	1	?	?



$\tau_1 < \tau_2$





(0100 .... 11 0)

1 čipas su n RS-trig.

Išvada: kiekvienas čipas iš n RS-trig. išduos skirtingą

informacija, kai x pereis iš 0 → 1

NFC – Near Field Commun. chip.

Intrinsic LTD: 1) kodo paklaida yra 15% → naud. kodav., kuris ištaiso klaidas. Kodai gali ištaisyti 25% klaidų.

2) rekomenduojama, kad RS čipai tvarėtų 40 – 50 baitų kodą ~ 320 – 400 bitų kodas

3) 25% klaidų → informatyvūs bitai bus 300 bitų iš 400. → čipus skaičius $2^{300} \sim 10^{100}$

Atvejį $\tau_1 > \tau_2$ nubrėžti per atsishaitymą.