**Homework for section 1 (due on Feb. 1st)**

Search recent announcements from *Samsung*, *INTEL*, and *TSMC* on their nanowire technology MBCFET:

* + How do you compare the various approaches?
	+ What are the implications for users such as Apple, AMD, and others?

**Homework for section#2**

Use online resource, and find examples for DES and for AES

* + Pick your plain text
	+ Pick a key
	+ Find the cipher text
	+ Decrypt back

[**http://extranet.cryptomathic.com/descalc/index**](http://extranet.cryptomathic.com/descalc/index)[**https://8gwifi.org/CipherFunctions.jsp**](https://8gwifi.org/CipherFunctions.jsp)

[**https://cryptii.com/pipes/aes-encryption**](https://cryptii.com/pipes/aes-encryption)

[**http://testprotect.com/appendix/AEScalc**](http://testprotect.com/appendix/AEScalc)

[**http://extranet.cryptomathic.com/aescalc/index**](http://extranet.cryptomathic.com/aescalc/index)

[**https://asecuritysite.com/**](https://asecuritysite.com/)

**Homework 3A for section#3**

Use online RSA calculator tool:

* + P=11 and q=7
	+ Calculate n=pxq
	+ Calculate 𝜙(n)
	+ Pick e < 𝜙(n) verify gcd (e, 𝜙(n))=1
	+ Calculate d the inverse of e mod 𝜙(n)
	+ Pick plain text P > 500 and find C the cipher of P
	+ Decrypt C

[**https://www.cryptool.org/en/cto-highlights/rsa-step-by-step**](https://www.cryptool.org/en/cto-highlights/rsa-step-by-step)

[**http://umaranis.com/rsa\_calculator\_demo.html**](http://umaranis.com/rsa_calculator_demo.html)

[**http://www.math.com/students/calculators/source/prime-number.htm**](http://www.math.com/students/calculators/source/prime-number.htm)

[**https://planetcalc.com/3311/**](https://planetcalc.com/3311/)

[**https://dsri.github.io/modinverse/**](https://dsri.github.io/modinverse/)

**Homework 3B for section#3**

Find an example with online tool for ECC

* + α=2 *,* β=2,  *23* ( $y^{2}$*≡* $x^{3}$*+* α *.* $x$ *+* β *mod n* )
	+ Find a primitive
	+ Pick secret keys *a* and *b*
	+ Calculate public keys A and B
	+ Calculate *a*B and *b*A
	+ Extract the common key

[**http://www.christelbach.com/ECCalculator.aspx**](http://www.christelbach.com/ECCalculator.aspx)

[**https://asecuritysite.com/encryption**](https://asecuritysite.com/encryption)

[**http://www.graui.de/code/elliptic2/**](http://www.graui.de/code/elliptic2/)

**Homework for section #6**

1. Develop the truth tables for

* + (A⊕B) + C
	+ (A . B) ⊕ C

2. Develop the truth table for the following device (Latch):



**A**

**NOR**

**NOR**

**B**

**C**

**D**

3. For the device above, find C and D when:

3.1 Initial setting: A=0 and B=1 ; then B become 0 ?

3.2 Initial setting: A=1 and B=0 ; then A become 0 ?

3.3 Initial setting: A=0 and B=1 ; then A become 1 ?

3.4 Initial setting: A=1 and B=1 ; then a) step1: A become 0 ?

 b) step2: B become 0 ?

3.5 Initial setting: A=1 and B=1 ; then a) step1: B become 0 ?

 b) step2: A become 0 ?

**Homework for section #8 part-1**

A PUF technology has:

* An intra-PUF error rate of 5% ( average error when the same cell is subject to repetitive queries to generate responses)
* An inter-PUF error rate of 40% (average error when the cells of one device are compared with the cells of different devices)
* The cryptographic protocol uses keys generated from the PUFs at various length: 32-bit, 64-bit, 128-bit, and 256-bit

For each key length, use Poisson calculator to respond:

* What is the FRR if the threshold T1 is more than10 errors?
* What is the FAR if the threshold T2 is less than 15 errors?
* Find T1 for FRR<1ppm (part per million)
* Find T2 for FAR<1ppm

Example of resource: https://keisan.casio.com/exec/system/1180573179

**Homework for section#8: part 2 A**

A ring oscillator PUF technology has:

* + 16 rings
	+ 10ns per clock cycle
	+ Needs 50 clock cycles to evaluate one pair

1- The cryptographic protocol use 64-bit streams of pairs

 What is the latency to match these 64 pairs?

2- The intra-PUF error rate is 5% ( average error when the same

 pair is subject to repetitive queries to generate responses)

 What is the FRR if the maximum threshold

 of acceptance is 10 bad CRP errors?

**Homework for section#8: part 2 B**

An Arbiter PUF technology has:

* + - 32 stages of MUX
		- 100ns per clock cycle

1-The cryptographic protocol use 64-bit challenges

What is the latency to generate 64-bit responses?

2-The intra-PUF error rate of 5%

What is the FRR if the threshold is 10 bad CRP errors?

**Homework #8 D**

This circuit is available for the design of a PUF with 64-bit long CRP:

* SRAM-based memory PUF with 2KByte array
* The PUF has 5% error rates without ternary states, and 0.1% error rates with ternary states

1- How many possible CRPs are available to authenticate the PUF?

2- Without ternary states, what is the maximum threshold of defects that

 is acceptable to get FRR<1%

3- With ternary states, what is the maximum threshold of defects that

 is acceptable to get FRR<1%

**Homework #8 E**

1- Read the documentation prepared by NIST on random number:

**NIST SP 800-22:**

2- Pick two out of the 15 tests and explain the method in more detail

**Homework #9A**: **Password manager with SH-1**

* Use your NAU email address & pick a fake password.
* Calculate the MD of the fake password PW with SHA-1.
* Calculate the MD of email address ⊕ PW.

The first two digits of the MD to generate an address.

* Plot the result in a table.
* Repeat with two other fake passwords.

**Homework #9B**: **Password manager with PUF**

**(a) The addressable PUF managers used in the circuit have 7% error rates and follow Poisson distribution.**

**(b) 128-bit long responses/challenges are generated from PUF-1 from the hashing of “A” and stored.**

**(c) 20-bit long addresses are generated from PUF-2 to store the challenges from the hashing of “B”.**

**Question 1:** The threshold for positive authentication is a match of 100 bits for the responses. What is the FRR?

**Question 2:** to reduce FRR, all addresses at Hamming distance of 1 from the addresses extracted in (c) are also tested. What is the new FRR?

**Question 3:** What if all addresses at Hamming distance of 2 are tested as well?

**Homework Section #11-A**

The ReRAM has 16X32 cells

1. A ring oscillator-based PUF uses two cells from different rows to generate a response (0 or 1), both cells share the same column.
	* + Each of the 32 columns has different pairs generating different responses.
		+ 1000 clock cycles are used to count the number of oscillations of one ring.
	1. How many different pairs are available in this PUF?
	2. How many cells are read to generate 128-bit long keys?
	3. How many read cycles are needed for the 128-bit long keys?
2. An arbiter based PUF uses 8-bit long stream to generate a response of 8 bits.
	* + Two adjacent rows are controlled by the same MUX.
		+ Two adjacent columns feed the same RS latch.
		+ Two adjacent latches feed the same XOR to generate a response.
	1. How “strong” is this PUF?
	2. How many cells are read to generate 8-bit long keys?
	3. How many read cycles are needed for the 128-bit long keys?
3. Compare the PUF of question 1 with the PUF of question 2.

**Homework #12-A**

 The Key exchange protocol is as follow:

* A SRAM PUF has 32x32 cells – Each cell has a 10-bit long address
* The message digest (hashing of random number and password) is 512-bit long
* From the message digest 32 addresses are generated in the 32x32 array
* 8 bits are generated at each address by using a congruent random number generator

Questions:

1- How many possible ways 256-bit long keys can be generated in this protocol?

2- Assuming that the average error rate is 0.1%, what is the proportion of keys with

 (a) zero bad bit?

 (b) one bad bit?

 (c) two bad bits?

**Optional Homework #12-B**

 A TAPKI protocol with RBC generates 256-bit keys from SRAM PUFs:

* Array of 32x32 cells
* Follows Poisson distribution; λ=4
* The latency of the encryption of the **User ID** with AES cycle is 1µs at the server level
* The RBC uses AES in the search engine

**Questions:**

1- Without fragmentation, what is the average latency of the RBC (with Poisson)?

2- With fragmentation by 4, what is the latency of the RBC (with Poisson)?

3- If the error rate of the PUF is cut to 0.001% with ternary states, the noise injection is 9.374%, and the protocol uses an HPC 10,000 faster, what is the latency with fragmentation by 4?