Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2024
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Homework 9, 110 pts. (ECE 4156) 135 pts. (ECE 6156)
Due Friday April 12 prior to 11:55pm

1) (40 pts.) Consider an instance of the HELP PUF with 2^{23} hazard-free paths. Assume that these hazard-free paths consist of 2^{22} rising (zero to one transition) paths and 2^{22} falling (one to zero transition) paths.

   a. (5 pts.) Describe the physical sources of entropy (randomness) in the HELP PUF.

Solution

The Physical sources of entropy (randomness) in HELP PUF are the manufacturing variations in the metal wires or transistors (die manufacturing variations).

   b. (10 pts.) Consider two specific paths whose delays are compared to produce a response bit. Discuss the entropy (i) on each path and (ii) in the comparison bit result. In particular, consider two PUF instances HELP_1 and HELP_2. Consider the same two specific paths in each HELP instance. Discuss the entropy in these paths for both HELP_1 and HELP_2.

Solution

(i) The entropy on each path is based on a fixed number of transistor delays. The entropy is produced by the delay needed to power on (or power off) each transistor. Once a transistor turns on, current flows and the next transistor in the path has its gate voltage changed. The channel length is the most impactful physical characteristic responsible for transistor delay. The random variations in transistor channel length thus are the most critical impact on each path's delay.

(ii) The variations in each path are random based on transistor delays. The comparison bit result will be unique and have randomness (entropy).

Considering the same two specific paths in each HELP instance, i.e., the paths for both HELP_1 and HELP_2, as the paths will be different, both instances of HELP will be random and different by a good margin and indistinguishable.

c. (10 pts.) Continuing the previous question, discuss how the entropy on each path can change the comparison bit result. In particular, consider how the path lengths in $HELP_1$ and $HELP_2$ may be related (correlated) to each other due to the use of Hardware Description Language (HDL) synthesis tools.

Solution

The HDL synthesis tools use heuristics which are not guaranteed to map logic designs to layout in the same manner each time. Therefore, unless some effort is made to use exactly the same synthesis result for each PUF, e.g., using the same physical-block (p-block) for $HELP_1$ as for $HELP_2$, then the path delays might be different due to different logic gate and layout mappings.

d. (15 pts.) Is it possible to build a model of the HELP PUF? In particular, assuming **you** are the adversary and **you** have access to the HELP PUF for a month, how would you propose to model build the HELP PUF? Make sure to discuss in your answer the fact that the HELP PUF you are trying to clone uses 2^{22} rising (zero to one transition) paths and 2^{22} falling (one to zero transition) paths.

Solution

An open question with respect to HELP is whether or not there is an overlap of logic gates used within the set of rising (or falling) paths. Clearly there are not 2^{22} (i.e., approximately 4 million) gates used in AES; in fact, efficient AES implementations have been reported with approximately 50,000 gates. Therefore, if the overlap of usage of logic gates can be somehow exploited, then it may be possible to model build the HELP PUF. This relationship has yet to be explored in the published literature.

2) (15 pts.) Consider a PUF which is enrolled and then tested a week later at all possible combinations of 0ºC, 25ºC, 85ºC and supply voltage (nominal), supply voltage (5% more than nominal) and supply voltage (5% less than nominal). Consider the case of a specific challenge-response pair. One approach to measure HD_{intra} is to compare the value of the response from enrollment versus the response from each of the combinations (nine comparisons total). A second approach is to compare each response with each other (45 comparisons in total). In your opinion, which approach is more appropriate for the authentication use case for the PUF (explain why)? Which approach to measure HD_{intra} is more appropriate for encryption (please explain why)?

Solution

The answer depends not so much on authentication versus encryption but rather depends on whether or not communication is only with a home base (e.g., a server) or is between each of the devices in the field with each other (in addition to the server at the home base). If authentication and encryption using PUF responses is only between a server and the PUF device in the field, the first approach (i.e., comparing the enrolled value with each of the nine temperature and voltage combinations) is preferable since this more closely matches the use case scenario. If authentication and encryption using PUF responses is between any of the PUF devices and/or with the server, then the second approach (i.e., 10 choose 2) is preferable since any pair in the group may want to authenticate or encrypt with each other.

Another comment is that if a PUF receives acceptable results with the second approach (10 choose 2), then, statistically speaking, it must also receive acceptable results with the first approach (enrollment bitstring compared to each of the nine temperature and voltage combinations). However, since so many of the relevant comparisons are left undone, acceptable PUF results from the first approach do not tell us that the results will also be equally acceptable for the second approach.

3) Are transistor delays a good source of randomness? Please explain (i) at least one reason why you think this is true and (ii) at least one reason why you think that this is not true.

Solution

(i) Transistor delays are a reliable source of randomness because the variations are due to tiny manufacturing variations which have no feasible model (otherwise the design of the manufacturing process would have used the model to reduce the occurrence of the variations). Furthermore, by calculating delay differences between two paths (as opposed to using the absolute delay values), statistical correlations between the two paths tend to cancel each other out.

(ii) Transistors delays are a poor source of variations because they tend to exhibit correlations. For example, if one transistor has a lower threshold voltage due to a smaller gate oxide thickness, then the neighboring transistor is, statistically speaking, also more likely to have a similarly thin gate oxide thickness.

4) (10 pts.) What is the purpose of a fuzzy extractor?

Solution

The major purpose of fuzzy extraction is to encode or "sketch" the challenges in a way that with helper data calculated the original response can be recovered or extracted even in the presence of one or a few bit errors. In other words, even with "fuzziness" or errors in the responses, the encoding techniques including helper data calculations enable the reliable extraction of the correct response with a high probability (depending on how many bit errors there are – above a certain threshold the fuzzy extraction no longer works).

5) (10 pts.) What is the primary benefit of using a controlled PUF in a PUF-based authentication protocol?

Solution

The usage of a controlled PUF prevents a *chosen-challenge* attack. The protocol utilizes a OWF to hash the input challenge before applying the input to the PUF, making it computationally infeasible to control the bits applied to the PUF.

6) (20 pts.) Consider the reverse fuzzy extractor.

a. (10 pts.) What is the purpose of a reverse fuzzy extractor? Be sure to distinguish your answer from the answer you gave for the purpose of a fuzzy extractor (see question 4 above); in other words, if you give the same answer here you will receive zero points.

Solution

A fuzzy extractor has two procedures as follows. First, there is the Generate or Gen process which produces helper data. Second, there is a Reproduce or Rep process which error-corrects a response with potential bit errors given the potentially erroneous response and the helper data.

The original published approaches to fuzzy extraction carried out the Gen process on the server during enrollment (i.e., where the server is the main computational entity interacting with the resource constrained chip with the PUF) while the Rep process is carried out on the same chip as the PUF. However, the observation that the Gen process is much simpler and more constrained than the Rep process led to the proposal of reverse fuzzy extraction.

A reverse fuzzy extractor implements the expensive Rep process on the server with the Gen process implemented on the same chip as the PUF. The purpose of this is to reduce the energy and computational overheads incurred on the resource constrained PUF chip.

b. (10 pts.) What must the server do to the stored response bitstring it has in its secure database in a reverse fuzzy extractor scheme?

Solution

In the reverse fuzzy extractor scheme, the server must **"error-correct"** the stored response bitstring r_i using the helper data hd_i to produce r''_i which hopefully is equal to r'_i (where r'_i is the uncorrected PUF response to the challenge).

7) [ECE 6156 only!] (15 pts.) How does TVcomp in HELP greatly reduce the variations in PND for the same challenges over a wide range of temperature and voltage conditions?

Solution

TVcomp applies known statistical methods to map PND values to a Gaussian distribution by using the mean and standard deviation of the PND values. When the statistical TVcomp methods are provided with a large range of enrollment values, the result can compensate for most temperature and voltage variations.

8) [ECE 6156 only!] (10 pts.) Why is it a concern in a reverse fuzzy extractor that the helper data changes from one run of the protocol to the next?

Solution

Helper data leaks some information about the response r_i in fuzzy extractors. But, with variations in helper data string additional information may be revealed that the adversary can use in attack models.

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES, INCLUDING OTHER/PREVIOUS SECTIONS OF ECE COURSES TAUGHT BY PROFESSOR MOONEY SUCH AS THOSE WITH NAMES INCLUDING HARDWARE ORIENTED SECURITY AND TRUST AS WELL AS CRYPTOGRAPHIC HARDWARE FOR EMBEDDED SYSTEMS. ALL HOMEWORK SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SUBMISSIONS MUST BE DONE ONLINE. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE WITH THICK INK AND MAY NOT BE ABLE TO USE LOW RESOLUTION PHOTOS OF HANDWRITTEN DIAGRAMS). FAILURE TO PROVIDE CLEAR AND LEGIBLE ANSWERS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).