Exercise Sheet 5

Prof. Kenny Paterson, F. Günther
M. Backendal, M. Filić

Discussion Questions (Hash functions).

(a) Name a use-case where pre-image resistance of a hash function is important. Explain your answer.

(b) For blockchains (e.g., crypto currencies like Bitcoin), the hardness of finding partial pre-images of a certain form is used as a computational challenge ("proof-of-work"). (In the lecture, we called this "partial pre-image resistance 2": given a target string $t \in \{0,1\}^l$, it is infeasible to find m s.t. $H(m) = t \,\|\, z$ significantly faster than through 2^l hash computations.) Do you know how a proof-of-work scheme works? What do you think are real-world effects from setting such challenges based on cryptographic hardness?

Suggested focus. Attempt these problems
before class: Problem 1.
in class: Problem 2 (a) – (d).
in your own time: Problem 2 (e), Problem 3.

Suggested reading. Reading the following sections in the Boneh-Shoup book [1] might help with the problems on this exercise sheet: Sections 8.3 (birthday attacks), 8.4 (Merkle-Damgård) and 8.5 (building compression functions).

Problem 1 (Building hash functions).

(a) Let $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ be a hash function.

1) Let $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$ be defined as

$$h_2(x) := h_1\left(h_1(x_1)||h_1(x_2)\right),$$

where $x_1||x_2 = x$ with $x_1, x_2 \in \{0,1\}^{2m}$. Show that finding a collision in h_2 leads to finding a collision in h_1. For this, give an algorithm $\mathcal{A}$ that on input a collision in h_2 outputs a collision in h_1. (Informally speaking, this means that collision-resistance of h_1 implies collision-resistance of h_2.)

2) Generalizing 1), for any $i \geq 2$ let $h_i : \{0,1\}^{2^i m} \to \{0,1\}^m$ be defined recursively from h_{i-1} as follows:

$$h_i(x) = h_1\left(h_{i-1}(x_1)||h_{i-1}(x_2)\right),$$

where $x_1||x_2 = x$ with $x_1, x_2 \in \{0,1\}^{2^{i-1}m}$. Show that finding a collision in h_i leads to finding a collision in h_1.

(b) Recall the Davies-Meyer construction for a compression function $g\colon \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ from a block cipher $\mathsf{E}\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, working on a chaining value $t \in \{0,1\}^n$ and a message block $m \in \{0,1\}^k$:

$$g(t,m) := \mathsf{E}(m,t) \oplus t.$$

We will see that for variants of that design, collisions can be found efficiently.

Assume $k = n$. Provide collisions (i.e., colliding input pairs $(t_1, m_1) \neq (t_2, m_2)$) for the following functions.

1) Let g_1 be defined just like Davies-Meyer, but XOR-ing m instead of t:

$$g_1(t, m) := \mathsf{E}(m, t) \oplus m.$$

2) Let g_2 be defined as follows:

$$g_2(t, m) := \mathsf{E}(t, t \oplus m) \oplus t.$$

Your algorithms can use E and E^{-1} in an arbitrary way (since the description of a good block cipher can be assumed to be public), i.e., using a custom key with a custom message.

Problem 2 (Security notions for hash functions). Let $\mathsf{H}\colon \mathcal{D} \to \mathcal{R}$ be a hash function. In class we have discussed a formal definition of *collision resistance* (CR), which can be defined through a game as follows.

Game $\mathbf{CR}(\mathcal{A}, \mathsf{H})$
$(m_1, m_2) \leftarrow\!\!\$\ \mathcal{A}()$
Return $((m_1 \neq m_2) \wedge (\mathsf{H}(m_1) = \mathsf{H}(m_2)))$

We define the advantage of an adversary $\mathcal{A}$ in Game **CR** as $\mathbf{Adv}^{\mathrm{CR}}_{\mathsf{H}}(\mathcal{A}) := \Pr[\,\mathbf{CR}(\mathcal{A}, \mathsf{H})\,]$.

In this problem we will formalize the notions of *pre-image resistance* (Pre) and *second pre-image resistance* (Sec) for hash functions. We will show that CR implies Sec and that Sec implies pre-image resistance if the right definitions are in place.

(a) Let us define second pre-image resistance first.

Game $\mathbf{Sec}(\mathcal{A}, \mathsf{H})$
$m_1 \leftarrow\!\!\$\ \mathcal{D}$ // Sample u.a.r. from domain.
$h \leftarrow \mathsf{H}(m_1)$
$m_2 \leftarrow\!\!\$\ \mathcal{A}(m_1, h)$
Return $((m_1 \neq m_2) \wedge (h = \mathsf{H}(m_2)))$

Similar to above, let $\mathbf{Adv}^{\mathrm{Sec}}_{\mathsf{H}}(\mathcal{A}) := \Pr[\mathbf{Sec}(\mathcal{A}, \mathsf{H})]$.

Show that CR implies Sec, i.e., for every adversary $\mathcal{A}$ against the **Sec** game, there exists an adversary $\mathcal{B}$ against the **CR** game such that

$$\mathbf{Adv}^{\mathrm{CR}}_{\mathsf{H}}(\mathcal{B}) \geq \mathbf{Adv}^{\mathrm{Sec}}_{\mathsf{H}}(\mathcal{A}).$$

(b) Let us now define *pre-image resistance*. In the lecture, you have seen an informal definition roughly defining it as: "given $h \in \mathcal{R}$, it is infeasible to find $m \in \mathcal{D}$ such that $\mathsf{H}(m) = h$." This informal definition is ambiguous in the following sense: it does not specify who chooses h and how it is chosen. Two possible interpretations are: (i) h is sampled uniformly at random from $\mathcal{R}$ and given to $\mathcal{A}$, or (ii) h is computed as $h \leftarrow \mathsf{H}(m)$ for some m that is sampled uniformly at random from $\mathcal{D}$. This leads to the following two security games, respectively.

Game $\mathbf{rPre}(\mathcal{A}, \mathsf{H})$	Game $\mathbf{Pre}(\mathcal{A}, \mathsf{H})$
$h \leftarrow\!\!\$\ \mathcal{R}$	$m \leftarrow\!\!\$\ \mathcal{D}$
$m' \leftarrow\!\!\$\ \mathcal{A}(h)$	$h \leftarrow \mathsf{H}(m)$
Return $(h = \mathsf{H}(m'))$	$m' \leftarrow\!\!\$\ \mathcal{A}(h)$
	Return $(h = \mathsf{H}(m'))$

For any adversary $\mathcal{A}$ playing against these games we define its advantage as

$$\mathbf{Adv}^{\mathrm{rPre}}_{\mathsf{H}}(\mathcal{A}) := \Pr[\mathbf{rPre}(\mathcal{A}, \mathsf{H})] \qquad \text{and} \qquad \mathbf{Adv}^{\mathrm{Pre}}_{\mathsf{H}}(\mathcal{A}) := \Pr[\mathbf{Pre}(\mathcal{A}, \mathsf{H})].$$

So which of the two definitions is the correct one? The answer is: either choice can be appropriate, but **Pre** is more common. The main goal of doing cryptography is to be able to deploy secure protocols (for example: TLS, SSH, and so on). If formally analysing and proving the security of any system requires to use either of the above definitions (or, likewise, yet another definition that is slightly different from the above), then doing so is appropriate. As the result of this philosophy, we often end up with a zoo of different definitions that all capture the same high-level intuition, but are not formally equivalent or even comparable (i.e., when neither of two definitions can be shown to imply the other). It is important to understand how these definitions relate to each other, and how they relate to entirely different security notions.

On slide 14 of Lecture 10-11-12-13 we saw that collision resistance does not imply pre-image resistance when $\mathcal{D} = \{0,1\}^*$ and $\mathcal{R} = \{0,1\}^n$ for any $n \in \mathbb{N}$, via the following construction. (The slides implicitly assume $\mathcal{D} = \{0,1\}^*$. In practice we have finite $\mathcal{D} = \{0,1\}^{\leq N}$ for a very large N; for example, SHA-256 has a message size limit of $N = 2^{64} - 1$ bits ≈ 2 exabytes.)

Let $\mathsf{G}\colon \mathcal{D} \to \mathcal{R}'$ be a collision-resistant hash function for $\mathcal{R}' = \{0,1\}^n$, and for any appropriate $\mathcal{D} \supseteq \{0,1\}^n$. Define a new hash function $\mathsf{H}\colon \mathcal{D} \to \mathcal{R}$ for $\mathcal{R} = \{0,1\}^{n+1}$ as follows:

Algorithm $\mathsf{H}(m)$
If $|m| = n$ then return $1 \,\|\, m$
Else return $0 \,\|\, \mathsf{G}(m)$

Explain why H

1) is still collision-resistant,
2) succeeds to show that CR does not imply rPre, but
3) does not show whether CR implies Pre.

(c) Show that CR does not imply Pre when $\mathcal{D} = \mathcal{R}$. The main goal of this part is to demonstrate that *some* condition on the relative sizes of $\mathcal{D}$ and $\mathcal{R}$ is necessary if we want to prove some implication from CR to Pre.

(d) In part (a) we saw that CR implies second pre-image resistance (Sec). We now want to show that, for a general hash function H, Sec implies Pre if the domain $\mathcal{D}$ of H is much larger than its range $\mathcal{R}$. Together, these two claims imply that CR implies Pre when $|\mathcal{D}| \gg |\mathcal{R}|$.

We begin by constructing the reduction in this part and will treat the formal relation of advantages in part (e). Let $|\mathcal{D}| \gg |\mathcal{R}|$. Given any adversary $\mathcal{A}$ against Game **Pre** (attacking pre-image resistance) for H, construct a new adversary $\mathcal{B}$ against Game **Sec** (attacking second pre-image resistance) for H. Provide an intuitive argument, why $\mathcal{B}$ succeeds when $\mathcal{A}$ succeeds.

Adversary $\mathcal{B}(m_1, h)$
...
Return m_2

(e) Derive constants $0 < \alpha, \beta < 1$ (either can be parameterized with $|\mathcal{D}|$ and $|\mathcal{R}|$, or none) such that $\mathbf{Adv}^{\text{Sec}}_{\mathsf{H}}(\mathcal{B}) \geq \alpha \cdot \mathbf{Adv}^{\text{Pre}}_{\mathsf{H}}(\mathcal{A}) - \beta$ for $\mathcal{A}$ and $\mathcal{B}$ from part (d). To do this, try to answer the following questions:

- Let m_1 be a message sampled in Game **Sec** for $\mathcal{B}$ and let $h \leftarrow \mathsf{H}(m_1)$. Let s be the event that h has a unique (i.e., only a *s*ingle) pre-image. What is an upper bound (that can be parameterized with $|\mathcal{D}|$ and $|\mathcal{R}|$) on the probability $\Pr[s]$?
- Separate the probability that adversary $\mathcal{A}$ recovers a pre-image of $h = \mathsf{H}(m_1)$ into the cases that h has a single, resp. has more than a single pre-image. That is, condition on s and $\neg s$. Use the upper bound above to give a bound for the former case.
- What is a lower bound on the *second* pre-image advantage of $\mathcal{B}$, in terms of the pre-image advantage of $\mathcal{A}$? Hint: Give a lower bound on the probability that adversary $\mathcal{A}$ (and hence $\mathcal{B}$) recovers a second pre-image of $h = \mathsf{H}(m_1)$ (i.e., a pre-image m_2 that is not equal to m_1), given that there is more than one pre-image (case $\neg s$). Give the bound in terms of $\Pr[\mathbf{Pre}(\mathcal{A}, \mathsf{H})|\neg s]$. Integrate this into the second case for $\mathcal{A}$'s advantage above.

Problem 3 (Joux's attack). Let H_1 and H_2 be Merkle-Damgård hash functions with output space $\{0,1\}^n$, based on some compression functions h_1 and h_2, respectively. We define a new function $H_{12}(M) = H_1(M)||H_2(M)$. One might expect that finding a collision for H_{12} takes $\Theta(2^n)$ evaluations of the function (according to the birthday bound, because the output space of H_{12} is $\{0,1\}^{2n}$). Let us see if this intuition is correct.

For simplicity, the complexity unit we use below is one evaluation of the function H_{12}. (This implies that one evaluation of each of h_1, h_2, H_1, H_2 has $O(1)$ complexity as well. Can you explain why?) In part (a) you might want to use one evaluation of the function h_1 as the complexity unit. Feel free to do so. It does not make a difference to the overall solution.

(a) We say that an s-collision for a hash function H is a set of messages $M_1, \ldots, M_s$ such that $\mathsf{H}(M_1) = \cdots = \mathsf{H}(M_s)$. The goal of this part of the question is to find an s-collision for H_1. Let each message M_i for $i \in \{1, \ldots, s\}$ consist of b blocks (each n-bits long) and let $s = 2^b$. Show how to use the birthday attack b times on the compression function h_1 (from the construction of the Merkle-Damgård hash function) to find an s-collision $M_1, \ldots, M_s$ for H_1 in $O(b \cdot 2^{\frac{n}{2}})$ steps.

(b) Let $b = \frac{n}{2}$. Using the result from part (a) explain how to find a collision for H_{12} (with high probability) in an additional $O(2^b)$ steps. (The total complexity of the attack is then $O\left(\frac{n}{2} \cdot 2^{\frac{n}{2}}\right) + O(2^{\frac{n}{2}}) = O\left(n \cdot 2^{\frac{n}{2}}\right)$.)

(c) What can you say about the intuition from the beginning of the question (the use of the birthday bound to estimate the complexity of finding collisions for H_{12}) after solving (a) and (b)? Is it correct or incorrect? Explain your answer.

Acknowledgements. This exercise sheet is in part inspired by (and adapted from) the books "A Graduate Course in Applied Cryptography" by Dan Boneh and Victor Shoup, and "Cryptography: Theory and Practice" by Douglas Stinson.

References

[1] D. Boneh and V. Shoup. *A Graduate Course in Applied Cryptography.* Online, version 0.6 edition, Jan. 2023.