作业讲解 III

2024.12.19

作业讲解 III - 1

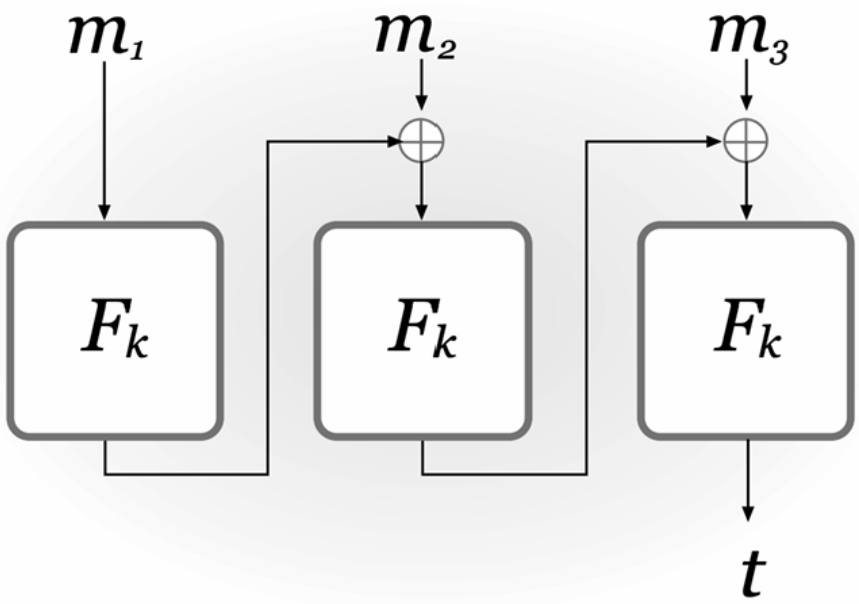
Exercises 4.13

4.13 We explore what happens when the basic CBC-MAC construction is used with messages of different lengths.

(a) Say the sender and receiver do not agree on the message length in advance (and so $\mathsf{Vrfy}_k(m,t) = 1$ iff $t \stackrel{?}{=} \mathsf{Mac}_k(m)$, regardless of the length of m), but the sender is careful to only authenticate messages of length $2n$. Show that an adversary can forge a valid tag on a message of length $4n$.

(b) Say the receiver only accepts 3-block messages (so $\mathsf{Vrfy}_k(m,t) = 1$ only if m has length $3n$ and $t \stackrel{?}{=} \mathsf{Mac}_k(m)$), but the sender authenticates messages of any length a multiple of n. Show that an adversary can forge a valid tag on a new message.

作业讲解 III - 1



作业讲解 III - 1

Solution: There are multiple solutions; we provide one in each case.
(a) Let $m_1, m_2 \in \{0,1\}^n$ be arbitrary. The attacker requests a tag on the message m_1, m_2, and obtains in return a tag t. One can check that t is also a valid tag on the message $m_1, m_2, m_1 \oplus t, m_2$.

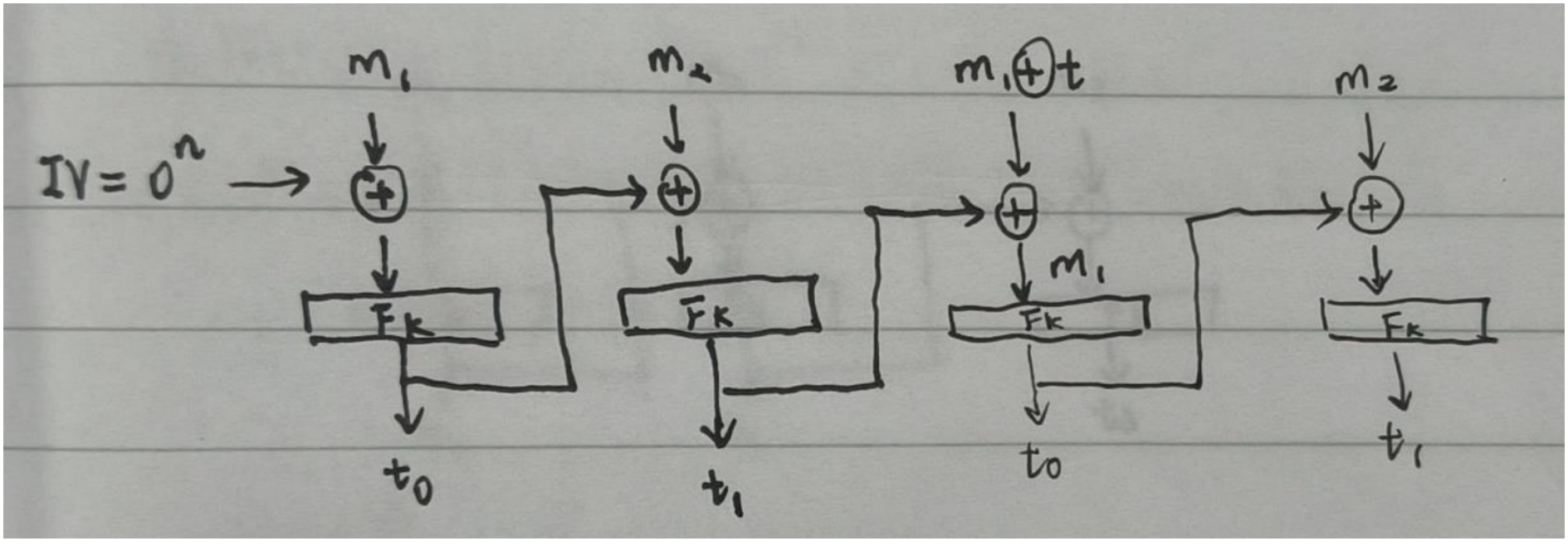


图: @221900459

作业讲解 III - 1

(b) Let $m_1, m_2, m_3 \in \{0,1\}^n$ be arbitrary. Obtain tag t_1 on the message m_1, tag t_2 on the message $t_1 \oplus m_2$, and tag t_3 on the message $t_2 \oplus m_3$. Then t_3 is a valid tag for the 3-block message m_1, m_2, m_3.

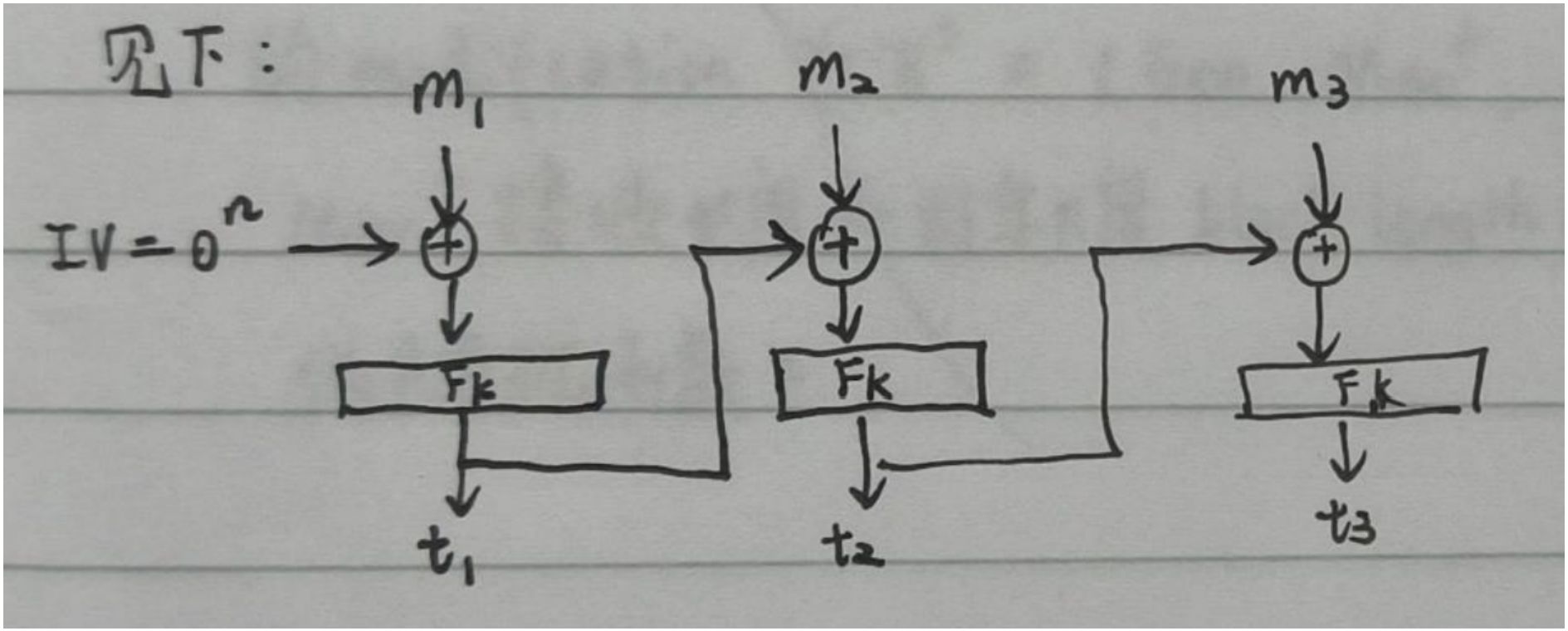


图: @221900459

作业讲解 III - 2

Exercises 4.19

4.19 Prove that the following modification of basic CBC-MAC gives a secure MAC for arbitrary-length messages if F is a pseudorandom function. (Assume all messages have length a multiple of the block length.) $\mathsf{Mac}_k(m)$ first computes $k_\ell := F_k(\ell)$, where ℓ is the length of m. The tag is then computed using basic CBC-MAC with key k_ℓ.

作业讲解 III - 2

Solution: Roughly speaking, this construction reduces to fixed-length CBC-MAC where an independent key k_ℓ is used for messages of length ℓ. Since fixed-length CBC-MAC is secure, the overall construction is secure. A full solution would require a formal proof.

Theorem 4.11

$$\mathsf{CBC}_k(x_1, \ldots, x_\ell) \stackrel{\text{def}}{=} F_k\left(F_k\left(\cdots F_k(F_k(x_1) \oplus x_2) \oplus \cdots\right) \oplus x_\ell\right),$$

where $|x_1| = \cdots = |x_\ell| = n$. (We leave CBC_k undefined on the empty string.) Note that CBC is computed in the same way as basic CBC-MAC, although here we explicitly allow inputs of different lengths.

A set of strings $P \subset (\{0,1\}^n)^*$ is *prefix-free* if it does not contain the empty string, and no string $X \in P$ is a prefix of any other string $X' \in P$. We show:

THEOREM 4.11 *If F is a pseudorandom function, then* CBC *is a pseudorandom function as long as the set of inputs on which it is queried is prefix-free. Formally, for any* PPT *distinguisher D that queries its oracle on a prefix-free set of inputs, there is a negligible function* negl *such that*

$$\left|\Pr[D^{\mathsf{CBC}_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1]\right| \leq \mathsf{negl}(n),$$

where k is chosen uniformly from $\{0,1\}^n$ and f is chosen uniformly from the set of functions mapping $(\{0,1\}^n)^*$ to $\{0,1\}^n$ (i.e., the value of f at each input is uniform and independent of the values of f at all other inputs).

作业讲解 III - 2

For an adversary $\mathcal{A}$, suppose he queries the sets of messages $M_1, M_2, \ldots, M_\alpha$ with lengths $l_1, l_2, \ldots, l_\alpha$, respectively, and the MACs applied are $\mathrm{CBC}_{F_k(l_1)}, \mathrm{CBC}_{F_k(l_2)}, \ldots, \mathrm{CBC}_{F_k(l_\alpha)}$. Since $F()$ is a pseudorandom function, $\mathrm{CBC}_{F_k(l_i)}$ is indistinguishable from CBC_{r_i}, where r_i is random.

Furthermore, since $M_1, M_2, \ldots, M_\alpha$ are all prefix-free (as the messages in M_i all have the same length and thus cannot have a prefix relationship), by Theorem 4.11, $\mathrm{CBC}_{r_1}, \mathrm{CBC}_{r_2}, \ldots, \mathrm{CBC}_{r_\alpha}$ are all indistinguishable from random functions. Consequently, $\mathrm{CBC}_{F_k(l_1)}, \mathrm{CBC}_{F_k(l_2)}, \ldots, \mathrm{CBC}_{F_k(l_\alpha)}$ are also indistinguishable from random functions.

作业讲解 III - 2

Therefore, the queries made by $\mathcal{A}$ can be considered as queries on $M_1, M_2, \ldots, M_\alpha$ with respect to the random functions $f_1, f_2, \ldots, f_\alpha$. Suppose he attempts to forge a message with length l_i and its corresponding tag. Since queries on messages of other lengths can be considered as queries on different random functions, they provide no assistance in the forgery. The difficulty of forging is "equivalent" to querying only the messages in M_i, which brings us back to the scenario of fixed-length CBC-MAC. We already know that fixed-length CBC-MAC is secure.

作业讲解 III - 3

Exercises 5.5

5.5 Prove that Construction 5.6 is unforgeable when instantiated with any encryption scheme (even if not CPA-secure) and any secure MAC (even if not strongly secure).

CONSTRUCTION 5.6

Let $\Pi_E = (\mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme and let $\Pi_M = (\mathsf{Mac}, \mathsf{Vrfy})$ be a message authentication code, where in each case key generation is done by simply choosing a uniform n-bit key. Define a private-key encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ as follows:

- Gen': on input 1^n, choose independent, uniform $k_E, k_M \in \{0,1\}^n$ and output the key (k_E, k_M).
- Enc': on input a key (k_E, k_M) and a plaintext message m, compute $c \leftarrow \mathsf{Enc}_{k_E}(m)$ and $t \leftarrow \mathsf{Mac}_{k_M}(c)$. Output the ciphertext $\langle c, t \rangle$.
- Dec': on input a key (k_E, k_M) and a ciphertext $\langle c, t \rangle$, first check if $\mathsf{Vrfy}_{k_M}(c, t) \stackrel{?}{=} 1$. If yes, output $\mathsf{Dec}_{k_E}(c)$; if no, output $\perp$.

作业讲解 III - 3

Solution: We denote the tuple $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ as Π'. Suppose that this construction is not unforgeable; then there exists an attacker $\mathcal{A}$ such that the probability $Pr[\mathit{Mac}\text{-forge}_{\mathcal{A},\Pi'}(n) = 1]$ is non-negligible.
Let's say $\mathcal{A}$ makes encryption-oracle queries for messages $m_1, \ldots, m_\ell$, and in return obtains ciphertexts $\langle c_1, t_1\rangle, \ldots, \langle c_\ell, t_\ell\rangle$. Let $\langle c, t\rangle$ be the ciphertext output by the attacker. Then, $\mathit{Mac}\text{-forge}_{\mathcal{A},\Pi'}(n) = 1$ is equivalent to $\mathsf{Vrfy}_{k_M}(c, t) = 1$ and $m \notin \{m_1, \ldots, m_\ell\}$.
Note that if $c \in \{c_1, \ldots, c_\ell\}$, there would exist some $m_i \neq m$ such that $\mathsf{Enc}_{k_E}(m_i) = c_i = c = \mathsf{Enc}_{k_E}(m)$, which would lead to a decryption failure. Therefore, $c \notin \{c_1, \ldots, c_\ell\}$. Hence, if $\mathit{Mac}\text{-forge}_{\mathcal{A},\Pi'}(n) = 1$, it must be the case that $c \notin \{c_1, \ldots, c_\ell\}$ and $\mathsf{Vrfy}_{k_M}(c, t) = 1$.

作业讲解 III - 3

We consider an attacker $\mathcal{A}'$ against Π_M who only needs to randomly generate a k'_E and provide $\mathcal{A}$ with access to $\mathrm{Enc}_{k'_E}()$ and $\mathrm{Mac}_{k_M}()$, and outputs the same ciphertext $\langle c, t \rangle$ as $\mathcal{A}$.
If $\mathit{Mac}\text{-forge}_{\mathcal{A},\Pi'}(n) = 1$, then $c \notin \{c_1, \ldots, c_\ell\}$ and $\mathrm{Vrfy}_{k_M}(c, t) = 1$, which implies $\mathit{Mac}\text{-forge}_{\mathcal{A}',\Pi}(n) = 1$. Therefore,
$Pr[\mathit{Mac}\text{-forge}_{\mathcal{A}',\Pi}(n) = 1] \geq Pr[\mathit{Mac}\text{-forge}_{\mathcal{A},\Pi'}(n) = 1]$, which is non-negligible, contradicting the security of Π_M.

作业讲解 III - 4

Exercises 5.4

5.4 Show that Construction 5.6 is not necessarily CCA-secure if it is instantiated with a secure MAC that is not *strongly* secure.

CONSTRUCTION 5.6

Let $\Pi_E = (\mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme and let $\Pi_M = (\mathsf{Mac}, \mathsf{Vrfy})$ be a message authentication code, where in each case key generation is done by simply choosing a uniform n-bit key. Define a private-key encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ as follows:

- Gen': on input 1^n, choose independent, uniform $k_E, k_M \in \{0,1\}^n$ and output the key (k_E, k_M).
- Enc': on input a key (k_E, k_M) and a plaintext message m, compute $c \leftarrow \mathsf{Enc}_{k_E}(m)$ and $t \leftarrow \mathsf{Mac}_{k_M}(c)$. Output the ciphertext $\langle c, t \rangle$.
- Dec': on input a key (k_E, k_M) and a ciphertext $\langle c, t \rangle$, first check if $\mathsf{Vrfy}_{k_M}(c, t) \stackrel{?}{=} 1$. If yes, output $\mathsf{Dec}_{k_E}(c)$; if no, output $\perp$.

作业讲解 III - 4

Solution: Let $\Pi = (\mathit{Gen}, \mathit{Mac}, \mathit{Vrfy})$ be a secure MAC. Construct $\Pi' = (\mathit{Gen}, \mathit{Mac}', \mathit{Vrfy}')$ such that $\mathrm{Mac}'_k(m)$ outputs $\mathrm{Mac}_k(m)\|0$ and such that $\mathrm{Vrfy}'_k(m, t\|b) = \mathrm{Vrfy}_k(m, t)$. (I.e., Mac' appends a 0-bit to the original tag, and Vrfy' ignores this extra bit.) It is immediate that the scheme is not strongly secure (since the attacker can simply flip the final bit of a tag on some message), but the scheme is still secure.
It is easy to give a chosen-ciphertext attack on Construction 5.6 when constructed using Π, by having the attacker just flip the final bit of the challenge ciphertext and request decryption of the resulting, modified ciphertext.

作业讲解 III - 5

Exercises 6.3

6.3 Let (Gen, H) be a collision-resistant hash function. Is $(\mathsf{Gen}, \hat{H})$ defined by $\hat{H}^s(x) \stackrel{\text{def}}{=} H^s(H^s(x))$ necessarily collision resistant?

作业讲解 III - 5

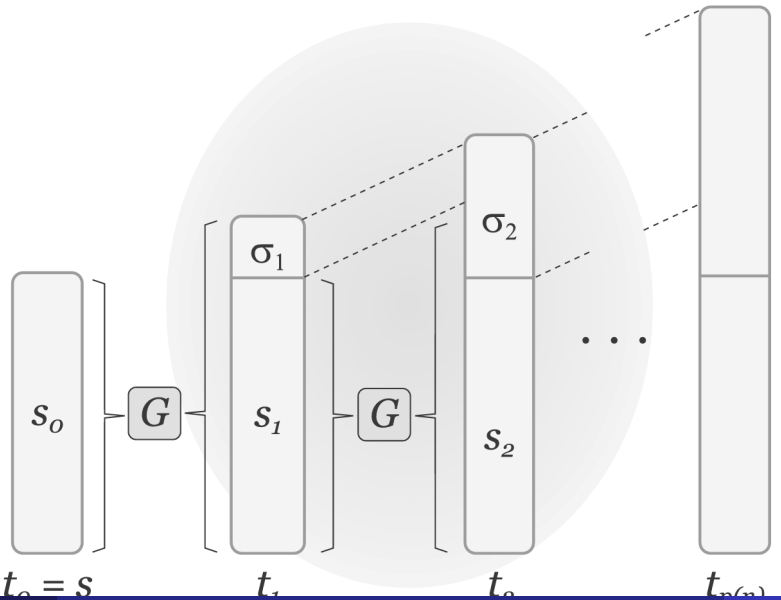
Solution: Yes. Let x, x' be a collision for $\hat{H}$; that is, $H^s(H^s(x)) = H^s(H^s(x'))$. There are two cases:
(a) $H^s(x) = H^s(x')$: in this case, x, x' is a collision for the original H. Therefore, such a pair can only be found with negligible probability.
(b) $H^s(x) \neq H^s(x')$: set $y = H^s(x)$ and $y' = H^s(x')$. By the assumption in this case, $y \neq y'$ and yet $H^s(y) = H^s(y')$. Thus, y, y' is a collision in H. Once again, this implies that such a pair x, x' can be found with only negligible probability (otherwise, by computing H^s once on each one obtains a collision y, y' in H^s).

作业讲解 III - 6

Theorem 8.19

THEOREM 8.19 *If there exists a pseudorandom generator G with expansion factor $n+1$, then for any polynomial* poly *there exists a pseudorandom generator $\hat{G}$ with expansion factor* poly(n).

See pages 279 and following in the textbook "Introduction to Modern Cryptography (3rd edition)".



作业讲解 III - 6

$\hat{G}(s) = G(G(s)[0, n-1])||G(s)[n]$ $H_0 : G(G(s)[0, n-1])||G(s)[n], s \leftarrow (0,1)^n$
$H_1 : G(r_1[0, n-1])||r_1[n], r_1 \leftarrow (0,1)^{n+1}$
$H_2 : r_2 = r_2[0, n]||r_2[n+1], r_2 \leftarrow (0,1)^{n+2}$

The distributions H_0 and H_1 both take the form of $G(s_1[0, n-1])||s_1[n]$, where $s_1[0, n-1]$ represents the first $n-1$ bits of s_1, and $s_1[n]$ is the n-th bit.
The distributions H_1 and H_2 both take the form of $s_2||$randombit, where s_2 is a string and randombit is a randomly chosen bit.