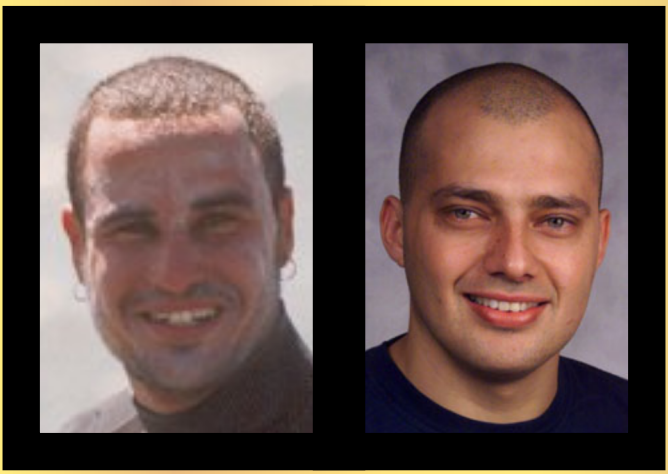


Statistically-Hiding Commitment from Any One-Way Function

Iftach Haitner Omer Reingold

2.3 Universal one-way hash functions (UOWHF)

Definition 2.3. *(universal one-way hash functions (UOWHF)) Let $\mathcal{F}$ be a family of functions mapping strings of length $\ell(n)$ to strings of length $m(n)$. We say that $\mathcal{F}$ is a family of* universal one-way hash functions *(following [NY89]) if the following hold:*

Samplable *$\mathcal{F}$ is polynomially samplable (in n).*

Efficient *There exists a polynomial-time algorithm that given $x \in \{0,1\}^{\ell(n)}$ and a description of $f \in \mathcal{F}$ outputs $f(x)$.*

Compression $m(n) < \ell(n)$.

Hardness *For all* PPT *A and $x \in \{0,1\}^{\ell(n)}$ the following is negligible in n:*

$$\Pr[(x, \mathsf{state}) \leftarrow A(1^n), f \leftarrow \mathcal{F}, x' \leftarrow A(x, \mathsf{state}, f) : x' \neq x \bigwedge f(x') = f(x)].$$

By [Rom90] (full proof is given in [KK05]), it follows that assuming the existence of a one-way function, there exists a family of universal one-way hash functions for some polynomial $\ell(n) \geq n$. Following [NY89, Lemma 2.1], we have that the latter construction implies a construction with $m(n) \leq \frac{1}{2}\ell(n)$.

2.5 Two-phase commitments

Definition 2.10. *(two-phase commitments) A* two-phase commitment scheme (S, R)*, with security parameter n and message lengths $(k_1, k_2) = (k_1(n), k_2(n))$, consists of four probabilistic polynomial-time interactive protocols: (S_c^1, R_c^1) the first commit stage, (S_r^1, R_r^1) the first reveal stage, (S_c^2, R_c^2) the second commit stage, and (S_r^2, R_r^2) the second reveal stage. Throughout, both parties receive the security parameter 1^n as input.*

1. *In the first commit stage, S_c^1 receives a private input $\sigma^{(1)} \in \{0,1\}^{k_1}$. At the end, S_c^1* locally *outputs some private information* prvt^1 *and R_c^1 outputs some public string* pub^1*.*

2. *In the first reveal stage, S_r^1 and R_r^1 receive as common input* pub^1 *and a string $\sigma^{(1)} \in \{0,1\}^{k_1}$ and S_r^1 receives as private input* prvt^1*. Let* trans *be the transcript of the first commit stage and the first reveal stage and includes R_r^1's decision to accept or reject.*

3. *In the second commit stage, S_c^2 and R_c^2 both receive the common input* trans*, and S_c^2 receives a private input $\sigma^{(2)} \in \{0,1\}^{k_2}$. At the end, S_c^2* locally *outputs some private information* prvt^2 *and R_c^2 outputs some public string* pub^2*.*

4. *In the second reveal stage, S_r^2 and R_r^2 receive as common input* pub^2 *and a string $\sigma^{(2)} \in \{0,1\}^{k_2}$, and S_r^2 receives as private input* prvt^2*. At the end, R_r^2 accepts or rejects.*

Definition 2.11. *(hiding) A two-phase commitment scheme (S, R), with security parameter n and message lengths $(k_1, k_2) = (k_1(n), k_2(n))$, is* statistically hiding *if the following hold: Given an ITM $\mathcal{R}^*$ and $\sigma^{(1)} \in \{0,1\}^{k_1}$, let $\mathsf{view}_{\langle \mathcal{S}_c^1(\sigma^{(1)}), \mathcal{R}^* \rangle}(n)$ denote the distribution on the view of $\mathcal{R}^*(1^n)$ when interacting with $\mathcal{S}_c^1(1^n, \sigma^{(1)})$. Similarly, for $\sigma^{(2)} \in \{0,1\}^{k_2}$ and $\Lambda \in \{0,1\}^*$ let $\mathsf{view}_{\langle \mathcal{S}_c^2(\sigma^{(2)}), \mathcal{R}^* \rangle}(\Lambda)$ denote the distribution on the view of $\mathcal{R}^*(\Lambda)$ when interacting with $\mathcal{S}_c^2(\sigma^{(2)}, \Lambda)$. We require that for any (even all-powerful) $\mathcal{R}^*$,*

1. *The views of R^* when interacting with the sender in the first phase on any two messages are statistically indistinguishable. That is, for all $\sigma^{(1)}, \widetilde{\sigma}^{(1)} \in \{0,1\}^{k_1}$, $\mathsf{view}_{\langle \mathcal{S}_c^1(\sigma^{(1)}), \mathcal{R}^* \rangle}(n)$ is statistically indistinguishable to $\mathsf{view}_{\langle \mathcal{S}_c^1(\widetilde{\sigma}^{(1)}), \mathcal{R}^* \rangle}(n)$.*

2. *The views of R^* when interacting with the sender in the second phase are statistically indistinguishable no matter what the sender committed to in the first phase. That is, for all $\sigma^{(1)} \in \{0,1\}^{k_1}$ and $\sigma^{(2)}, \widetilde{\sigma}^{(2)} \in \{0,1\}^{k_2}$, $\mathsf{view}_{\langle \mathcal{S}_c^2(\sigma^{(2)}), \mathcal{R}^* \rangle}(\Lambda)$ is statistically indistinguishable to $\mathsf{view}_{\langle \mathcal{S}_c^2(\widetilde{\sigma}^{(2)}), \mathcal{R}^* \rangle}(\Lambda)$,*

   where $\Lambda = \mathsf{transcript}\langle S^1(1^n, \sigma^{(1)}), R^*(1^n) \rangle$.

We stress that the second condition of the above hiding definition (Definition 2.11) requires that the view of receiver in the second phase be indistinguishable for any two messages even given the transcript of the first phase, $\Lambda = \mathsf{transcript}\langle S^1(1^n, \sigma^{(1)}), R^*(1^n) \rangle$.

Definition 2.12. *($\binom{2}{1}$-binding) A two-phase commitment scheme (S, R), with security parameter n and message lengths $(k_1, k_2) = (k_1(n), k_2(n))$, is* computationally $\binom{2}{1}$-binding *if there exists a set $\mathcal{B}$ of first-phase transcripts and a negligible function ε such that:*

1. *For every (even unbounded) sender S^*, the first-phase transcripts in $\mathcal{B}$ make the second phase statistically binding, i.e. $\forall S^*, \forall \mathsf{trans} \in \mathcal{B}$, with probability at least $1 - \varepsilon(n)$ over pub^2, the output of R_c^2 in $\langle S^*(\mathsf{trans}), R_c^2(\mathsf{trans})\rangle$, there is at most one value $\sigma^{(2)} \in \{0,1\}^{k_2}$ such that $\langle S^*(\mathsf{pub}^2, \sigma^{(2)}), R_r^2(\mathsf{pub}^2, \sigma^{(2)})\rangle = \mathtt{Accept}$.*

2. *$\forall$ nonuniform PPT S^*, S^* succeeds in the following game with probability at most $\varepsilon(n)$ for all sufficiently large n:*

   (a) *S^* and R_c^1 interact and R_c^1 outputs pub^1. Let trans^1 be the transcript of the interaction.*

   (b) *S^* outputs two full transcripts trans and $\widetilde{\mathsf{trans}}$ of* both *phases with the following three properties:*

   - *Transcripts trans and $\widetilde{\mathsf{trans}}$ both start with prefix trans^1.*
   - *The transcript trans contains a successful opening of pub^1 to the value $\sigma^{(1)} \in \{0,1\}^{k_1}$ using a first-phase transcript not in $\mathcal{B}$, and R_r^1 and R_r^2 both accept in trans.*
   - *The transcript $\widetilde{\mathsf{trans}}$ contains a successful opening of pub^1 to the value $\widetilde{\sigma}^{(1)} \in \{0,1\}^{k_1}$ using a first-phase transcript not in $\mathcal{B}$, and R_r^1 and R_r^2 both accept in $\widetilde{\mathsf{trans}}$.*

   (c) *S^* succeeds if all of the above conditions hold and $\sigma^{(1)} \neq \widetilde{\sigma}^{(1)}$.*

Theorem 2.13. *([NOV06, Theorem 7.10]) If one way functions exist, then on security parameter n, we can construct in time $\mathsf{poly}(n)$ a collection of public-coin two-phase commitment schemes $Com_1, \ldots, Com_m$ for $m = \mathsf{poly}(n)$ such that:*

- *There exists an index i such that the scheme Com_i is hiding. (This property holds, regardless of whether the one-way function for which the scheme is based on is one-way or not.)*
- *For every index j, scheme Com_j is $\binom{2}{1}$-binding.*

2.6 Extending the message length

While Theorem 2.13 implies a set of two-phase commitment schemes with some given message lengths, for our purposes we need the message length of the first-phase commitment to be sufficiently (though still polynomially) long. The following lemma allows us to expand the message length of the first-phase commitment.

Lemma 2.14. *There exists an efficient procedure that given a two-phase commitment scheme with message lengths $(k_1(n), k_2(n))$ and a positive polynomial p, outputs a two-phase commitment scheme with message lengths $(p(n), 1)$, which is hiding whenever the given scheme is hiding and it is $\binom{2}{1}$-binding whenever the given scheme is $\binom{2}{1}$-binding.*

Proof. (of Lemma 2.14) Let $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ be a two-phase commitment with message lengths $(k_1(n), k_2(n))$. We assume w.l.o.g. that $k_1(n) = k_2(n) = 1$, since we can always decide to use only the first bit of the commitments. We define the two-phase commitment $(\mathcal{S}, \mathcal{R})$ with message lengths $(p(n), 1)$ as follows:

First-phase commit:

Common input: 1^n.
Sender's private input: $x_1 \in \{0,1\}^{p(n)}$.

1. For $i = 1 \ldots, p(n)$,

   $(\mathcal{S}_c^1, \mathcal{R}_c^1)$ run $\langle \widetilde{\mathcal{S}}_c^1(x_1[i]), \widetilde{\mathcal{R}}_c^1(1^{\ell(n)}) \rangle$, with $\mathcal{S}_c^1$ and $\mathcal{R}_c^1$ acting as $\widetilde{\mathcal{S}}_c^1$ and $\widetilde{\mathcal{R}}_c^1$ respectively.

   Let pub_i^1 be the public output and let prvt_i^1 be the private output of $\widetilde{\mathcal{S}}_c^1$ in the above execution.
2. $\mathcal{S}_c^1$ locally outputs $\mathsf{prvt}^1 = (\mathsf{prvt}_1^1, \ldots, \mathsf{prvt}_{p(n)}^1)$ and $\mathcal{R}_c^1$ outputs $\mathsf{pub}^1 = (\mathsf{pub}_1^1, \ldots, \mathsf{pub}_{p(n)}^1)$.

First-phase reveal:

Common input: 1^n, $\mathsf{pub}^1 = (\mathsf{pub}_1^1, \ldots, \mathsf{pub}_{p(n)}^1)$ and $x_1 \in \{0,1\}^{p(n)}$.
Sender's private input: $\mathsf{prvt}^1 = (\mathsf{prvt}_1^1, \ldots, \mathsf{prvt}_{p(n)}^1)$.

1. For $i = 1 \ldots, p(n)$,

   $(\mathcal{S}_c^1, \mathcal{R}_c^1)$ run $\langle \widetilde{\mathcal{S}}_r^1(\mathsf{prvt}_i^1, \mathsf{pub}_i^1, x_1[i]), \widetilde{\mathcal{R}}_r^1(\mathsf{pub}_i^1), x_1[i] \rangle$, with $\mathcal{S}_c^1$ and $\mathcal{R}_c^1$ acting as $\widetilde{\mathcal{S}}_c^1$ and $\widetilde{\mathcal{R}}_c^1$ respectively. Let trans_i be the transcript of the execution.
2. $\mathcal{S}_c^1$ accepts if $\widetilde{\mathcal{S}}_r^1$ accepts in all of the above executions.

Second-phase commit:

Common input: $\mathsf{trans} = (\mathsf{trans}_1, \ldots, \mathsf{trans}_{p(n)})$.
Sender's private input: $b \in \{0,1\}$.

1. For $i = 1 \ldots, p(n)$,

   $(\mathcal{S}_c^2, \mathcal{R}_c^2)$ run $\langle \widetilde{\mathcal{S}}_c^2(b, \mathsf{trans}_i), \widetilde{\mathcal{R}}_2^1(\mathsf{trans}_i)\rangle$, with $\mathcal{S}_c^2$ and $\mathcal{R}_c^2$ acting as $\widetilde{\mathcal{S}}_c^2$ and $\widetilde{\mathcal{R}}_c^2$ respectively.

   Let pub_i^2 be the public output and let prvt_i^2 be the private output of $\widetilde{\mathcal{S}}_c^2$ in the above execution.
2. $\mathcal{S}_c^2$ locally outputs $\mathsf{prvt}^2 = (\mathsf{prvt}_1^2, \ldots, \mathsf{prvt}_{p(n)}^2)$ and $\mathcal{R}_c^2$ outputs $\mathsf{pub}^2 = (\mathsf{pub}_1^2, \ldots, \mathsf{pub}_{p(n)}^2)$.

Second-phase reveal:

Common input: $\mathsf{pub}^2 = (\mathsf{pub}_1^2, \ldots, \mathsf{pub}_{p(n)}^2)$ and $b \in \{0,1\}$.
Sender's private input: $\mathsf{prvt}^2 = (\mathsf{prvt}_1^2, \ldots, \mathsf{prvt}_{p(n)}^2)$.

1. For $i = 1 \ldots, p(n)$,

   $(\mathcal{S}_c^2, \mathcal{R}_c^2)$ run $\langle \widetilde{\mathcal{S}}_r^2(\mathsf{prvt}_i^2, \mathsf{pub}_i^2, b), \widetilde{\mathcal{R}}_r^1(\mathsf{pub}_i^2), b\rangle$, with $\mathcal{S}_c^2$ and $\mathcal{R}_c^2$ acting as $\widetilde{\mathcal{S}}_c^2$ and $\widetilde{\mathcal{R}}_c^2$ respectively.
2. $\mathcal{S}_c^2$ accepts if $\widetilde{\mathcal{S}}_r^1$ accepts in all of the above executions.

The correctness of $(\mathcal{S},\mathcal{R})$ is evident, and it is also clear that $(\mathcal{S},\mathcal{R})$ is hiding given that $(\widetilde{\mathcal{S}},\widetilde{\mathcal{R}})$ is. Assuming that $(\widetilde{\mathcal{S}},\widetilde{\mathcal{R}})$ is $\binom{2}{1}$-binding, we show that $(\mathcal{S},\mathcal{R})$ is $\binom{2}{1}$-binding as follows: We define $\mathcal{B}$, a set of first-phase transcripts of $(\mathcal{S},\mathcal{R})$ as $B \stackrel{\text{def}}{=} \left\{\mathsf{outs}^2 = (\mathsf{outs}_1^2,\ldots,\mathsf{outs}_{p(n)}^2) : \exists i \in p(n) \text{ s.t. } \mathsf{outs}_i^2 \in \widetilde{B}\right\}$, where $\widetilde{B}$ is the set of first-phase transcripts of $(\widetilde{\mathcal{S}},\widetilde{\mathcal{R}})$ that make that second-phase commitment statistically binding. It is easy to see that indeed any transcript in $\mathcal{B}$, makes the second-phase commitment of $(\mathcal{S},\mathcal{R})$ statistically binding (as in Definition 2.12). Finally, let A be an adversary that breaks the $\binom{2}{1}$-binding of $(\mathcal{S},\mathcal{R})$ by outputting two transcripts $\mathsf{trans} = (\mathsf{trans}_1\ldots,\mathsf{trans}_{p(n)})$ and $\widetilde{\mathsf{trans}} = (\widetilde{\mathsf{trans}}_1\ldots,\widetilde{\mathsf{trans}}_{p(n)})$. By our definition of $\mathcal{B}$, there must exists an index $i \in p(n)$ such that both trans_i and $\widetilde{\mathsf{trans}}_i$ are not in $\widetilde{B}$, trans_i and $\widetilde{\mathsf{trans}}_i$ contain different first-phase openings $\sigma^{(1)} \neq \widetilde{\sigma}^{(1)}$, and $\widetilde{\mathcal{R}}_r^1$ and $\widetilde{\mathcal{R}}_r^2$ accept in both transcripts.

Since the latter holds for any breaking of the $\binom{2}{1}$-binding of $(\mathcal{S},\mathcal{R})$, there must exist $i' \in p(n)$ (which can be efficiently found) such that A breaks the $\binom{2}{1}$-binding of $(\mathcal{S},\mathcal{R})$ conditioned that the above holds w.r.t. $\mathsf{trans}_{i'}$ and $\widetilde{\mathsf{trans}}_{i'}$. Thus, the existence of A implies an adversary the breaks the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}},\widetilde{\mathcal{R}})$. □

3.1 Main reduction

In this section we construct a bit-commitment scheme such that the following hold: The scheme is statistically hiding whenever the two-phase commitment is hiding, and the scheme is *weekly* binding whenever the two-phase commitment is $\binom{2}{1}$-binding.

Construction 3.1. *(The basic scheme) Let $\mathcal{F}$ be a family of universal one-way hash functions mapping strings of length $\ell(n)$ to strings of length $m(n) \leq \frac{1}{2}\ell(n)$, let $\mathcal{H}$ be a family of Boolean pairwise independent hash functions defined over strings of length $\ell(n)$ and finally let $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ be a two-phase commitment scheme with message lengths $(\ell(n), 1)$.*

Commit stage:

Common input: 1^n.
Sender's private input: $b \in \{0,1\}$.

// **First-phase commit:**

1. *$\mathcal{S}_c$ chooses uniformly at random $x_1 \in \{0,1\}^{\ell(n)}$.*
2. *$(\mathcal{S}_c, \mathcal{R}_c)$ run $\langle \widetilde{\mathcal{S}}_c^1(x_1), \widetilde{\mathcal{R}}_c^1(1^n) \rangle$, with $\mathcal{S}_c$ and $\mathcal{R}_c$ acting as $\widetilde{\mathcal{S}}_c^1$ and $\widetilde{\mathcal{R}}_c^1$ respectively.*

   Let pub^1 be the public output and let prvt^1 be the private output of $\widetilde{\mathcal{S}}_c^1$ in the above execution.
3. *$\mathcal{R}_c$ chooses uniformly at random $f \in \mathcal{F}$ and sends it to $\mathcal{S}$.*
4. *$\mathcal{S}_c$ sends $y = f(x_1)$ back to $\mathcal{R}$.*
5. *$\mathcal{R}_c$ flips a random coin $\mathsf{dec} \in \{0,1\}$.*

   If $\mathsf{dec} = 0$, // **Relying on the first-phase commitment.** **(binding if y=f(x̃))**

   (a) *$\mathcal{S}_c$ chooses uniformly at random $h \in \mathcal{H}$ and sends h and $c = b \oplus h(x)$ to $\mathcal{R}_c$.*

   (b) *$\mathcal{R}_c$ outputs $\mathsf{pub} = (\mathsf{dec}, \mathsf{pub}^1, f, y, h, c)$.*

   (c) *$\mathcal{S}_c$ locally outputs $\mathsf{prvt} = (\mathsf{prvt}^1, x_1)$.*

   Otherwise (i.e., $\mathsf{dec} = 1$), // **Verifying the first-phase commitment and moving to second-phase commitment.** **(binding if y≠f(x̃))**

   $\mathcal{S}_c$ sends x_1 to $\mathcal{R}_c$ and $(\mathcal{S}_c, \mathcal{R}_c)$ run $\langle \widetilde{\mathcal{S}}_r^1(\mathsf{prvt}^1, \mathsf{pub}^1, x_1), \widetilde{\mathcal{R}}_r^1(\mathsf{pub}^1), x_1) \rangle$, with $\mathcal{S}_c$ and $\mathcal{R}_c$ acting as $\widetilde{\mathcal{S}}_c^1$ and $\widetilde{\mathcal{R}}_c^1$ respectively. Let trans be the transcript of the execution.

   If $\widetilde{\mathcal{R}}_c^r$ rejects, then $\mathcal{R}_c$ outputs $\perp$ (i.e., it will be impossible to decommit this execution).

   Otherwise,

   (a) *$(\mathcal{S}_c, \mathcal{R}_c)$ run $\langle \widetilde{\mathcal{S}}_c^2(b, \mathsf{trans}), \widetilde{\mathcal{R}}_c^2(\mathsf{trans}) \rangle$, with $\mathcal{S}_c$ and $\mathcal{R}_c$ acting as $\widetilde{\mathcal{S}}_c^2$ and $\widetilde{\mathcal{R}}_c^2$ respectively. Let pub^2 be the public output and let prvt^2 be the private input of $\widetilde{\mathcal{S}}_c^2$ in the above execution.* *output*

   (b) *$\mathcal{S}_c$ locally outputs $\mathsf{prvt} = \mathsf{prvt}^2$ and $\mathcal{R}_c$ outputs $\mathsf{pub} = (\mathsf{dec}, \mathsf{pub}^2)$.*

Iftach Haitner Omer Reingold

Reveal stage:

In case $\mathsf{dec} = 0$, **(binding if y=f(x̃))**
Common input: 1^n, $b \in \{0,1\}$ *and* $\mathsf{pub} = (0, \mathsf{pub}^1, f, y, h, c)$.
Sender's private input: $\mathsf{prvt} = (\mathsf{prvt}^1, x_1)$.

$\mathcal{S}_r$ *sends* x_1 *to* $\mathcal{R}_r$ *and* $(\mathcal{S}_r, \mathcal{R}_r)$ *run* $\langle \widetilde{\mathcal{S}}_r^1(\mathsf{prvt}^1, \mathsf{pub}^1, x_1), \widetilde{\mathcal{R}}_r^1(\mathsf{pub}^1, x_1)\rangle$, *with* $\mathcal{S}_r$ *and* $\mathcal{R}_r$ *acting as* $\widetilde{\mathcal{S}}_r^1$ *and* $\widetilde{\mathcal{R}}_r^1$ *respectively.*

If $\widetilde{\mathcal{R}}_r^1$ *rejects, or* $f(x_1) \neq y$ *or* $c \oplus h(x_1) \neq b$, *then* $\mathcal{R}_r$ *outputs* `Reject`.

Otherwise, $\mathcal{R}_r$ *outputs* `Accept`.

In case $\mathsf{dec} = 1$, **(binding if y≠f(x̃))**
Common input: 1^n, $b \in \{0,1\}$ *and* $\mathsf{pub} = (1, \mathsf{pub}^2)$.
Sender's private input: $\mathsf{prvt} = \mathsf{prvt}^2$.

$(\mathcal{S}_r, \mathcal{R}_r)$ *run* $\langle \widetilde{\mathcal{S}}_r^2(\mathsf{prvt}^2, \mathsf{pub}^2, b), \widetilde{\mathcal{R}}_r^2(\mathsf{pub}^2, b)\rangle$, *with* $\mathcal{S}_r$ *and* $\mathcal{R}_r$ *acting as* $\widetilde{\mathcal{S}}_r^2$ *and* $\widetilde{\mathcal{R}}_r^2$ *respectively.* $\mathcal{R}_r$ *outputs the same output as* $\widetilde{\mathcal{R}}_r^2$ *does in the above execution.*

3.1.1 The scheme is hiding

Lemma 3.3. *If $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ is hiding, then $(\mathcal{S}, \mathcal{R})$ is statistically hiding.*

Proof. Assuming that $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ is hiding, then the hiding in the case that $\mathsf{dec} = 1$ is evident. That is, by the hiding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$, no information about x_2 (and thus about b) has leaked to the receiver. Note that the receiver also gets the values of f and $f(x_1)$, but this information could be generated from x_1 and thus it reveals no additional information about x_2.

In the complementary case ($\mathsf{dec} = 0$) the situation is a bit more involved. Essentially, the only information that the receiver obtains about b is $y = f(x_1)$ and $c = b \oplus h(x_1)$. Since f is condensing and by the pairwise independence of $\mathcal{H}$, it is easy to see that with overwhelming probability (y, c) contains only negligible information about b and thus the protocol is hiding.

3.1.2 The scheme is weakly binding

Lemma 3.5. *If $\mathcal{F}$ is a family of universal one-way hash functions and $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ is $\binom{2}{1}$-binding, then $(\mathcal{S}, \mathcal{R})$ is $\frac{17}{18}$-binding.*

Proof. Let $S^* = (S_c^*, S_r^*)$ be an algorithm trying to break the binding of $(\mathcal{S}, \mathcal{R})$ and recall $\mathsf{BndBreak}$ from Definition 2.6. Let $i \in \{0,1\}$ and let p be a positive polynomial, we define $\gamma_i^{S^*,p}(n) \stackrel{\text{def}}{=} \Pr_{\mathsf{outs} \leftarrow <S_c^*(1^n), \mathcal{R}_c(1^n)>}[\mathsf{BndBreak}^{S_r^*, \mathcal{R}_r}(\mathsf{outs}) > \frac{1}{p(n)} | \mathsf{dec} = i]$. Namely, $\gamma_i^{S^*,p}(n)$ is the probability that the output of the commit stage enables S^* to cheat in the reveal stage with noticeable probability. The proof of the Lemma 3.5 follows by the next claim.

Claim 3.6. *For any* PPT *S^* and any positive polynomial p, for large enough n there exists $i \in \{0,1\}$ such that $\gamma_i^{S^*,p}(n) < \frac{8}{9}$.*

Therefore, for any positive polynomial p and large enough n, $\Pr_{\mathsf{outs} \leftarrow <S^*(1^n), \mathcal{R}_c(1^n)>}[\mathsf{BndBreak}^{S^*, \mathcal{R}_r}(\mathsf{outs}) > \frac{1}{p(n)}] = \Pr[\mathsf{dec} = 0] \cdot \gamma_0^{S^*,p}(n) + \Pr[\mathsf{dec} = 1] \cdot \gamma_1^{S^*,p}(n) \leq 1 - \frac{1}{2} \cdot \frac{1}{9}$, and the proof of Lemma 3.5 follows.

Claim 3.6. *For any* PPT S^* *and any positive polynomial* p*, for large enough* n *there exists* $i \in \{0,1\}$ *such that* $\gamma_i^{S^*,p}(n) < \frac{8}{9}$.

Proof. (of Claim 3.6) We assume toward a contradiction that the claim does not hold and prove that either the hardness of the universal one-way hash functions or the $\binom{2}{1}$-binding of the underlying two-phase commitment scheme are violated. More formally, let S^* be algorithm and p be a positive polynomial such that for infinitely many n's and for both values of $i \in \{0,1\}$, it holds that $\gamma_i^{S^*,p}(n) \geq \frac{9}{10}$. Assuming that the $\binom{2}{1}$-binding of the underlying bit-commitment scheme holds, we use S^* to construct an algorithm M^{S^*}, described next, that breaks with noticeable probability the hardness of the universal one-way hash functions. Recall that in order to break the hash function, M^{S^*} should first select a value x and then given a random hash function f, it needs to output another element $x' \neq x$ such that $f(x) = f(x')$.

Before presenting the algorithm, we would like first to make the dependency of S_c^* and $\mathcal{R}_c$ on the their random-coins explicit. That is, we assume that S_c^* and $\mathcal{R}_c$ are deterministic efficient algorithms that get as additional inputs random strings $rand_{S_c^*} \in \{0,1\}^{\ell_{S_c^*}(n)}$ and $(\mathsf{dec}, f, rand_{\mathcal{R}_c}) \in \{0,1\} \times \mathcal{F} \times \{0,1\}^{\ell_{\mathcal{R}_c}(n)}$ respectively. We assume w.l.o.g. that both $\ell_{S_c^*}$ and $\ell_{\mathcal{R}_c}$ are some known polynomials.

M^{S^*}:

First stage, selecting a value x.

Input: 1^n

a Select uniformly at random $rand_{S_c^*} \in \{0,1\}^{\ell_{S_c^*}(n)}$, $rand_{\mathcal{R}_c} \in \{0,1\}^{\ell_{\mathcal{R}_c}(n)}$ and $f \in \mathcal{F}$.

b Simulate $\langle S_c^*(rand_{S_c^*}), \mathcal{R}_c(1, f, rand_{\mathcal{R}_c})\rangle$.

Let $\mathsf{outs} = (\mathsf{prvt}, \mathsf{pub})$ be the private output of S_c^* and the public output in the above simulation and let $\mathsf{outs}[x_1]$ be the value of x_1 in pub (see the commit stage of Construction 3.1 for $\mathsf{dec} = 1$).

c Output $x = \mathsf{outs}[x_1]$ and $\mathsf{state} = (rand_{S_c^*}, rand_{\mathcal{R}_c})$.

Second stage, finding a collision.

Input: x, $\mathsf{state} = (rand_{S_c^*}, rand_{\mathcal{R}_c})$, $f' \in \mathcal{F}$

d Simulate $\langle S_c^*(rand_{S_c^*}), \mathcal{R}_c(0, f', rand_{\mathcal{R}_c})\rangle$.

Let $\mathsf{outs}' = (\mathsf{prvt}', \mathsf{pub}')$ be the private output of S_c^* and the public output in the above simulation.

e For both $i \in \{0,1\}$:

Simulate $\langle S_r^*(\mathsf{prvt}', \mathsf{pub}', b), \mathcal{R}_r(\mathsf{pub}', i)\rangle$.

Let z_i be the value of the variable x_1 that R_r gets from S_r^* in the simulation (see the reveal stage of Construction 3.1 for $\mathsf{dec} = 0$).

f If $\mathcal{R}_r$ accepts for both $i \in \{0,1\}$, output $x' = z_j$, where $j \in \{0,1\}$ is such that $z_j \neq x$. (Note that since $\mathcal{R}_r$ accepts in both cases, it follows that $i = c \oplus h(z_i)$ for both $i \in \{0,1\}$ and thus $z_0 \neq z_1$).

Some intuition: *By the* $\binom{2}{1}$*-binding of* $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$*, it follows that after the first-phase commit, there is only a* single *value,* $\widetilde{x}$*, such that if the first-phase commitment is "opened" to this value, it might be possible to cheat in the second-phase commitment. Since* S^* *manages to cheat (also) for* $\mathsf{dec} = 1$ *and therefore* S^* *is able to break the second-phase commitment of* $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$*, it holds w.h.p. that* x*, defined in the first-stage of* M^{S^*}*, is equal to* $\widetilde{x}$*.*

Let us now consider the second-stage of M^{S^*}*. Since* S_c^* *does not know the value of* dec *when sending* y *in the simulation of Line (d), it should send* y *such that* $y = f'(\widetilde{x})$ *where* y *is the value sent by* S_r^* *to* $\mathcal{R}_r$ *after the first-phase commit. The point is that since we are using the same random coins as in the first stage, this is the same* $\widetilde{x}$ *as before. Whenever* S^* *breaks the commitment for* $\mathsf{dec} = 0$*, it needs to open the first-phase commitment into two elements* $z_0 \neq z_1$ *such that* $f'(z_0) = f'(z_1) = y$*. Thus, w.h.p. it holds that* $f'(z_0) = f'(z_1) = f'(\widetilde{x})$ *and* M^{S^*} *violates the hardness of* $\mathcal{F}$*.*

We now return to the formal proof. For any value of the parties random coins $frand = (rand_{S_c^*}, \mathsf{dec}, f, rand_{\mathcal{R}_c}) \in \{0,1\}^{\ell_{S_c^*}(n)} \times \{0,1\} \times \mathcal{F} \times \{0,1\}^{\ell_{\mathcal{R}_c}(n)}$, let $\mathsf{outs}(frand) \stackrel{\text{def}}{=} (\mathsf{prvt}(frand), \mathsf{pub}(frand))$, where $\mathsf{prvt}(frand)$ and $\mathsf{pub}(frand)$ are the private output of S_c^* and the public output in $\langle S_c^*(rand_{S_c^*}), \mathcal{R}_c((\mathsf{dec}, f, rand_{\mathcal{R}_c})\rangle$ respectively. The following lemma is the heart of our proof.

Lemma 3.7. *Assuming that $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ is $\binom{2}{1}$-binding and that Claim 3.6 does not hold w.r.t. $\mathcal{S}^*$, then there exists a set $L \subseteq \{0,1\}^{\ell_{S_c^*}(n)} \times \{0,1\}^{\ell_{\mathcal{R}_c}(n)}$ of density $\frac{1}{6}$ for which the following hold:*

1. *For all $(rand_{S_c^*}, rand_{\mathcal{R}_c}) \in L$ and any value of $\mathsf{dec} \in \{0,1\}$,*

$$\Pr_{f \leftarrow \mathcal{F}}[\mathsf{BndBreak}^{S_r^*, \mathcal{R}_r}(\mathsf{outs}(rand_{S_c^*}, \mathsf{dec}, f, rand_{\mathcal{R}_c})) \geq \frac{1}{p(n)}] \geq \frac{2}{3},$$

2. *There exists a mapping $\sigma : \{0,1\}^{\ell_{S_c^*}(n)} \times \{0,1\}^{\ell_{\mathcal{R}_c}(n)} \to \{0,1\}^{\ell(n)}$ s.t. for all $(rand_{S_c^*}, rand_{\mathcal{R}_c}) \in L$,*

$$\Pr_{f \leftarrow \mathcal{F}}[\mathsf{outs}(rand_{S_c^*}, 1, f, rand_{\mathcal{R}_c})[x_1] = \sigma(rand_{S_c^*}, rand_{\mathcal{R}_c})] \geq \frac{1}{2}.$$

Claim 3.8. $\Pr_{rand \leftarrow G}[\nexists x \in \{0,1\}^{\ell(n)} \ s.t. \ w^{rand}(x) > \frac{1}{2}] = neg.$

Thus, we conclude the proof of Lemma 3.7, by letting $\sigma(rand) = \widetilde{x}$ if there exists $\widetilde{x}$ such that $w^{rand}(\widetilde{x}) > \frac{1}{2}$ and letting $\sigma(rand) = 0$ otherwise, and defining $L \stackrel{\text{def}}{=} G \cap \left\{rand : w^{rand}(\sigma(rand)) > \frac{1}{2}\right\}$.

Proof. (of Claim 3.8) For any random coins $frand = (rand_{S_c^*}, 1, f, rand_{\mathcal{R}_c}) \in \{0,1\}^{\ell_{S_c^*}(n)} \times \{0,1\} \times \mathcal{F} \times \{0,1\}^{\ell_{\mathcal{R}_c}(n)}$, let $\mathsf{trans}(frand)$ be the first-phase transcript of the interaction with $\widetilde{\mathcal{R}}$ embedded in the transcript of $\langle S_c^*(rand_{S_c^*}), \mathcal{R}_c((1, f, rand_{\mathcal{R}_c})\rangle$ (i.e., the transcripts of the interactions with $\widetilde{\mathcal{R}}_c^1$ and $\widetilde{\mathcal{R}}_r^1$). Recall the set $\mathcal{B}$ from Definition 2.10 w.r.t. $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$, which has the property that if a first-phase transcript of an interaction with $\widetilde{\mathcal{R}}$ is in $\mathcal{B}$, then the second-phase commitment with $\widetilde{\mathcal{R}}$ is statistically binding. It follows that for almost all $(rand_{S_c^*}, rand_{\mathcal{R}_c}) \in G$ (save but a set of negligible probability) it holds that,

$$\Pr_{f \leftarrow \mathcal{F}}[\mathsf{BndBreak}^{S_r^*, \mathcal{R}_r}(\mathsf{outs}(rand_{S_c^*}, 1, f, rand_{\mathcal{R}_c})) \geq \frac{1}{p(n)} \bigwedge \mathsf{trans}(rand_{S_c^*}, 1, f, rand_{\mathcal{R}_c}) \notin \mathcal{B}] \geq \frac{2}{3} - neg(n).$$

Let's assume towards a contradiction that Claim 3.8 does not hold. Therefore, by the above observation there exists non-negligible set $G' \subseteq G$, such that the following holds for any $rand \in G'$:

1. $\nexists x \in \{0,1\}^{\ell(n)}$ s.t. $w^{rand}(x) > \frac{1}{2}$,
2. $\Pr_{f \leftarrow \mathcal{F}}[\mathsf{BndBreak}^{S_r^*, \mathcal{R}_r}(\mathsf{outs}(rand_{S_c^*}, 1, f, rand_{\mathcal{R}_c}) \geq \frac{1}{p(n)} \bigwedge \mathsf{trans}(rand_{S_c^*}, 1, f, rand_{\mathcal{R}_c}) \notin \mathcal{B}]) \geq \frac{3}{5}$.

We conclude the proof, by showing that the above set implies violation of the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$. Before doing that, we would like to make the dependence of $\mathcal{R}_c$ in its random coins even more explicit. Recall that we assume that $\mathcal{R}_c$ is a deterministic algorithm gets as additional input the random coins $(\mathsf{dec}, f, rand_{\mathcal{R}_c}) \in \{0,1\} \times \mathcal{F} \times \{0,1\}^{\ell_{\mathcal{R}_c}(n)}$. To make the discussion more precise, we write that $rand_{\mathcal{R}_c} = (rand_{\widetilde{\mathcal{R}}_c^1}, rand_{other})$ where $rand_{\widetilde{\mathcal{R}}_c^1} \in \{0,1\}^{\ell_{\widetilde{\mathcal{R}}_c^1}(n)}$ is the random-coins used in the execution of $\widetilde{\mathcal{R}}_c^1$ embedded in the execution of $\mathcal{R}_c$. The following algorithm breaks the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$.

T^{S^*}**:**

Input: 1^n

The interaction part.

a Select uniformly at random $rand_{S_c^*} \in \{0,1\}^{\ell_{S_c^*}(n)}$.

b Interact with $\widetilde{\mathcal{R}}_c^1(1^n)$ by invoking $S_c^*(rand_{S_c^*})$ and simulating its interaction with $\mathcal{R}_c$ by forwarding messages between S_c^* and $\widetilde{\mathcal{R}}_c^1$.

Let trans^1 be the transcript of the above interaction and let $rand_{\widetilde{\mathcal{R}}_c^1}$ be the random coins used by $\widetilde{\mathcal{R}}_c^1$ in the above interaction. (We do not need to actually know the value of $rand_{\widetilde{\mathcal{R}}_c^1}$ for the run of T^{S^*} and only use it in order to simplify notation.)

Producing two transcripts.

a Select uniformly at random $rand_{other} \in \{0,1\}^{\ell_{\mathcal{R}_c^1}(n)-\ell_{\widetilde{\mathcal{R}}_c^1}(n)}$.

b For $i \in \{0,1\}$:

1. Select uniformly at random $f_i \in \mathcal{F}$.
2. Simulate $\langle S_c^*(rand_{S_c^*}), \mathcal{R}_c(1, f_i, rand_{\widetilde{\mathcal{R}}_c}, rand_{other}\rangle$ starting from Line 3 of Construction 3.1 (note that given trans^1, we do not need to know $rand_{\widetilde{\mathcal{R}}_c}$ in order to simulate).
   Let $\mathsf{outs}_i^2 = (\mathsf{prvt}_i^2, \mathsf{pub}_i^2)$, where prvt_i^2 and prvt_i^2 are the private output of S_c^* and the public output in the above simulation respectively. Let trans_i^2 and trans_i^3 be the transcripts of the interactions with $\widetilde{\mathcal{R}}_r^1$ and $\widetilde{\mathcal{R}}_c^2$ in the above simulation.
3. Simulate $\langle S_r^*(\mathsf{prvt}_i^2, \mathsf{pub}_i^2, 0), \mathcal{R}_r(\mathsf{pub}_i^2, 0)\rangle$.
   Let trans_i^4 be the transcript of the interaction with $\widetilde{\mathcal{R}}_r^2$ in the above simulation.
4. Set $\mathsf{trans}_i = (\mathsf{trans}^1, \mathsf{trans}_i^2, \mathsf{trans}_i^3, \mathsf{trans}_i^4)$.

c Output $(\mathsf{trans}_0, \mathsf{trans}_1)$.

Claim 3.9. *T^{S^*} breaks the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ with non-negligible probability.*

Proof. Conditioned on $rand = (rand_{S_c^*}, rand_{\widetilde{\mathcal{R}}_c^1}, rand_{other}) \in G'$, we have by the second property of G'

$$\Pr_{f_0 \leftarrow \mathcal{F}}[\mathsf{BndBreak}^{S_r^*, \mathcal{R}_r}(\mathsf{outs}_0) \geq \tfrac{1}{p(n)} \bigwedge(\mathsf{trans}^1, \mathsf{trans}_0^2) \notin \mathcal{B}] \geq \tfrac{3}{5}. \tag{3}$$

Clearly, the above also holds w.r.t. f_1, outs_1 and trans_1^2. Moreover, by the first property of G', we have the following w.r.t. any $z \in \{0,1\}^{\ell(n)}$,

$$\Pr_{f_1 \leftarrow \mathcal{F}}[\mathsf{outs}_1[x_1] \neq z \bigwedge \mathsf{BndBreak}^{S_r^*, \mathcal{R}_r}(\mathsf{outs}_1) \geq \tfrac{1}{p(n)} \bigwedge(\mathsf{trans}^1, \mathsf{trans}_1^2) \notin \mathcal{B}] \geq \tfrac{3}{5} - \tfrac{1}{2} = \tfrac{1}{10}. \tag{4}$$

Setting $z = \mathsf{outs}_0[x_1]$, since f_1 is independent of f_0, it follows that

$$\begin{aligned} & \Pr_{f_0 \leftarrow \mathcal{F}, f_1 \leftarrow \mathcal{F}}[\mathsf{outs}_0[x_1] \neq \mathsf{outs}_1[x_1] \bigwedge \forall i \in \{0,1\}\ \mathsf{BndBreak}^{S_r^*, \mathcal{R}_r}(\mathsf{outs}_i) \geq \frac{1}{p(n)} \bigwedge(\mathsf{trans}^1, \mathsf{trans}_i^2) \notin \mathcal{B}] \\ \geq & \quad \frac{3}{5} \cdot \frac{1}{10} = \frac{3}{25}. \end{aligned}$$

Therefore, we conclude that condition that $rand \in G'$, the following happens with probability at list $\frac{3}{25} \cdot \frac{1}{p(n)^2}$:

1. both trans_0 and trans_1 starts with trans^1,
2. the first-phase transcripts (i.e., $(\mathsf{trans}^1, \mathsf{trans}_i^2)$) in both trans_0 and trans_1 are not in $\mathcal{B}$,
3. the value of x_1 in trans_0 and in trans_1 is different,
4. $\widetilde{\mathcal{R}}_r^1$ and $\widetilde{\mathcal{R}}_r^2$ accept in both trans_0 and trans_1.

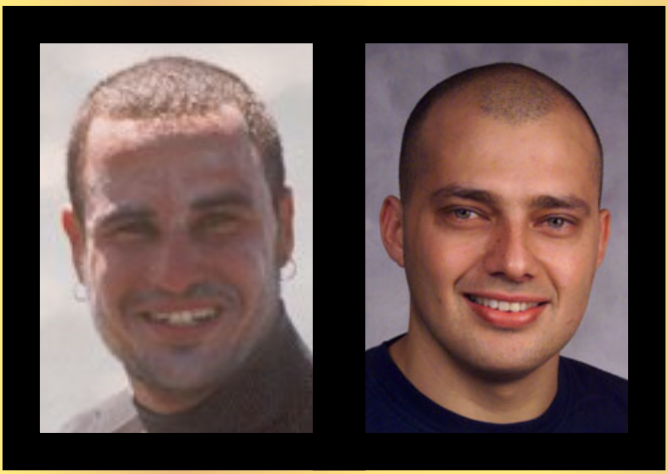
Since we assume that G' is non-negligible, T^{S^*} breaks the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$. □

3.2 Completing the construction

The following corollary follows by the lemmata about Construction 3.1 (Lemma 3.1 and Lemma 3.5) and the standard bit-commitment binding amplification (Proposition 2.9).

Corollary 3.10. *There exists an efficient procedure that given a family of universal one-way hash functions and a two-phase commitment scheme, outputs a bit-commitment scheme which is statistically hiding whenever the underlying protocol is hiding and it is computationally binding whenever the underlying protocol is* $\binom{2}{1}$*-binding.*

By the above Corollary, the existence of universal one-way hash functions ([Rom90, KK05]), the existence of a collections of two-phase commitment schemes that are all $\binom{2}{1}$-binding and at least one of them is hiding (Theorem 2.13) and the standard bit-commitment hiding amplification (Proposition 2.8). It follows that statistical bit-commitment can be constructed using any one-way function. Finally, the proof of Theorem 1.1 follows by the above conclusion and the standard transformation of a bit-commitment scheme into a commitment scheme of any polynomial length.



Statistically-Hiding Commitment from Any One-Way Function

Iftach Haitner Omer Reingold

Iftach Haitner Omer Reingold

Iftach Haitner Omer Reingold