Creating Strong Total Commutative Associative One-Way Functions from Any One-Way Function

Lane A. Hemaspaandra [1]
Department of Computer Science
University of Rochester
Rochester, NY 14627, USA

Jörg Rothe [2]
Institut für Informatik
Friedrich-Schiller-Universität Jena
07740 Jena, Germany

Univ. of Roch., Dept. of Computer Science, Technical Report 98-688
May 8, 1998 (revised: May 26, 1998)

[1]Email: lane@cs.rochester.edu. Supported in part by grants NSF-CCR-9322513 and NSF-INT-9513368/DAAD-315-PRO-fo-ab.

[2]Email: rothe@informatik.uni-jena.de. Supported in part by grant NSF-INT-9513368/DAAD-315-PRO-fo-ab and a NATO Postdoctoral Science Fellowship from the Deutscher Akademischer Austauschdienst ("Gemeinsames Hochschulsonderprogramm III von Bund und Ländern"). Work done in part while visiting the University of Rochester.

Abstract

Rabi and Sherman [RS97] presented novel digital signature and unauthenticated secret-key agreement protocols, developed by themselves and by Rivest and Sherman. These protocols use "strong," total, commutative (in the case of multi-party secret-key agreement), associative one-way functions as their key building blocks. Though Rabi and Sherman did prove that associative one-way functions exist if P $\neq$ NP, they left as an open question whether any natural complexity-theoretic assumption is sufficient to ensure the existence of "strong," total, commutative, associative one-way functions. In this paper, we prove that if P $\neq$ NP then "strong," total, commutative, associative one-way functions exist.

Keywords: complexity-theoretic one-way functions, associativity.

1 Introduction and Preliminaries

Rabi and Sherman [RS97] study associative one-way functions (AOWFs) and show that AOWFs exist exactly if P $\neq$ NP. They also present the notion of strong AOWFs—AOWFs that are hard to invert even when one of their arguments is given. They give protocols due to Rivest and Sherman for two-party secret-key agreement and due to Rabi and Sherman for digital signatures, that depend on strong, total AOWFs. They also outline a protocol approach for multi-party secret-key agreement that depends on strong, total, commutative AOWFs.

There are two key worries regarding the Rabi-Sherman approach. The first is whether their protocols are secure even if strong, total, commutative AOWFs exist. This worry has two facets. The first facet is that, as they note, like Diffie-Hellman [DH76,DH79] the protocol they describe has no current proof of security (even if the existence of strong, total, commutative AOWFs is given), though Rabi and Sherman give intuitively attractive arguments suggesting the plausibility of security. In particular, they prove that certain direct attacks against their protocols are precluded by the fact that the protocols use strong, total AOWFs as building blocks. The second facet of the first worry is that their definition of strong, total, commutative AOWFs is a worst-case definition, as opposed to the average-case definition one desires for a satisfyingly strong approach to cryptography.

The second worry is that Rabi and Sherman provide no evidence at all that strong, total, commutative AOWFs exist, though they do prove that AOWFs exist if P $\neq$ NP. In this paper we completely remove that worry by proving that strong, total, commutative AOWFs exist if P $\neq$ NP. (In light of the above-mentioned first worry—and especially its second facet—we note, as did Rabi and Sherman, that the study of AOWFs should be viewed as

more of complexity-theoretic interest than of applied cryptographic interest, though it is hoped that AOWFs will in the long term prove, probably in average-case versions, to be of substantial applied cryptographic value.)

Phrasing our work in a slightly different but equivalent way, in this paper we prove that the existence of AOWFs (or, indeed, the existence of *any* one-way function) implies the existence of strong, total, commutative AOWFs. Furthermore, based on Kleene's [Kle52] distinction between *weak* and *complete equality* of partial functions, we give a definition of associativity that, for partial functions, is a more natural analog of the standard total-function definition than that of Rabi and Sherman, and we show that their and our results hold even under this more natural definition.

Fix the alphabet $\Sigma = \{0, 1\}$, and let Σ^* denote the set of all strings over Σ. The length of any string $x \in \Sigma^*$ will be denoted by $|x|$. Throughout this paper, when we use "binary function" we mean "two-argument function." Unless explicitly stated as being total, all functions may potentially be partial, i.e., "let σ be any binary function" does not imply that σ will necessarily be total. For any binary function σ, we will interchangeably use prefix and infix notation, i.e., $\sigma(x, y) = x\sigma y$. As is standard, pairs of strings will sometimes be encoded as a single string by some standard total, one-to-one, onto, polynomial-time computable pairing function, $\langle \cdot, \cdot \rangle : \Sigma^* \times \Sigma^* \to \Sigma^*$, that has polynomial-time computable inverses, and is non-decreasing in each argument when the other argument is fixed. Let FP denote the set of all polynomial-time computable (partial) functions. Regarding Part 3 of the following definition, we mention that we use the term "one-way function" in the same way Rabi and Sherman [RS97] do, i.e., in the complexity-theoretic (that is, worst-case) sense, and without requiring that the function necessarily be injective.

Definition 1.1 *Let $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ be any binary function.*

1. *We say σ is* honest *if and only if there exists some polynomial p such that for every $z \in \text{range}(\sigma)$ there exists a pair $(x, y) \in \text{domain}(\sigma)$ such that $x\sigma y = z$ and $|x| + |y| \leq p(|z|)$.*[1]
2. *We say σ is* FP-invertible *if and only if there exists a total function $g \in \text{FP}$ such that for every $z \in \text{range}(\sigma)$, $g(z)$ is some element of $\sigma^{-1}(z) = \{(x, y) \in \text{domain}(\sigma) \mid x\sigma y = z\}$.*
3. *We say σ is a* one-way function *if and only if σ is honest, polynomial-time computable, and not* FP*-invertible.*

Rabi and Sherman [RS97] define a notion of associativity for binary functions as follows:

[1] This definition of honesty for binary functions is that of Rabi and Sherman [RS97], and is equivalent to requiring $|\langle x, y \rangle| \leq p(|z|)$, since there exists some polynomial q (that depends on the pairing function chosen) such that for every $x, y \in \Sigma^*$, $|\langle x, y \rangle| \leq q(|x| + |y|)$ and $|x| + |y| \leq q(|\langle x, y \rangle|)$.

Definition 1.2 *Let* $\circ : \Sigma^* \times \Sigma^* \to \Sigma^*$ *be any binary function. We say* $\circ$ *is* weakly associative[2] *if and only if* $x \circ (y \circ z) = (x \circ y) \circ z$ *holds for all* $x, y, z \in \Sigma^*$ *such that each of* (x, y), (y, z), $(x, y \circ z)$, *and* $(x \circ y, z)$ *is an element of* domain($\circ$).

This type of associativity, however, is not natural for non-total functions, since it does not evaluate as being false "equations" such as "undefined = 1010" (this can occur in $x \circ (y \circ z) = (x \circ y) \circ z$ in various ways, e.g., if (x, y), $(x \circ y, z)$, and (y, z) are in the domain of $\circ$ but $(x, y \circ z)$ is not). It would seem more natural for a definition of associativity for binary functions to require that both sides of the above equation stand or fall together. That is, for each triple of strings $x, y, z \in \Sigma^*$, either both sides should be defined and equal, or each side should be undefined. Drawing on Kleene's careful discussion of how to define equality between partial functions, our definition of associativity—given in Definition 1.3 below—achieves this natural behavior.

Associativity expresses equality between two functions each of which can be viewed as a 3-ary function that results from a given binary function. The distinction in the two definitions of associativity can be said to come from two distinct interpretations of "equality" between functions, known in recursive function theory as *weak equality* and *complete equality* (see Kleene [Kle52]). Kleene suggests the use of two different equality symbols—we will use "$=_w$" and "$=_c$" and we have modified the following quotation to use these also—and he writes:

> We now introduce "$\psi(x_1, \ldots, x_n) =_c \chi(x_1, \ldots, x_n)$" to express, for particular $x_1, \ldots, x_n$, that if either of $\psi(x_1, \ldots, x_n)$ and $\chi(x_1, \ldots, x_n)$ is defined, so is the other and the values are the same (and hence if either of $\psi(x_1, \ldots, x_n)$ and $\chi(x_1, \ldots, x_n)$ is undefined, so is the other). The difference in the meaning of (i) "$\psi(x_1, \ldots, x_n) =_w \chi(x_1, \ldots, x_n)$" and (ii) "$\psi(x_1, \ldots, x_n) =_c \chi(x_1, \ldots, x_n)$" comes when one of $\psi(x_1, \ldots, x_n)$ and $\chi(x_1, \ldots, x_n)$ is undefined. Then (i) is undefined, while (ii) is true or false according as the other is or is not undefined.— [Kle52, pp. 327–328]

We feel that complete equality is the more natural of the two notions. Thus, following the notion of *complete equality* between functions, we propose the following definition of associativity for binary functions. Nonetheless, we will show that the results of Rabi and Sherman [RS97] and of the present paper hold even under this more restrictive definition. In a similar vein, we also define commutativity for (partial) binary functions.

[2] They call this "associative," but for reasons we will immediately make clear, we use "weakly associative" to describe their notion.

Definition 1.3 *Let $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ be any binary function. Define $\Gamma = \Sigma^* \cup \{\perp\}$ and define an extension $\widehat{\sigma} : \Gamma \times \Gamma \to \Gamma$ of σ as follows:*

$$\widehat{\sigma}(a,b) = \begin{cases} \sigma(a,b) & \text{if } a \neq \perp \text{ and } b \neq \perp \text{ and } (a,b) \in \text{domain}(\sigma) \\ \perp & \text{otherwise.} \end{cases}$$

We say σ is associative *if and only if, for every $x, y, z \in \Sigma^*$, $(x\widehat{\sigma}y)\widehat{\sigma}z = x\widehat{\sigma}(y\widehat{\sigma}z)$ (i.e., $(x\sigma y)\sigma z =_c x\sigma(y\sigma z)$). We say σ is* commutative *if and only if, for every $x, y \in \Sigma^*$, $x\widehat{\sigma}y = y\widehat{\sigma}x$ (i.e., $x\sigma y =_c y\sigma x$).*

Clearly, every associative function is weakly associative, since our notion of associativity is more restrictive than weak associativity. The converse, however, is not always true, so these are indeed different notions.

Proposition 1.4 *1. Every associative binary function is weakly associative.*

2. Every total binary function is associative if and only if it is weakly associative.

3. There exists a binary function that is weakly associative, but not associative.

Proof. (1) and (2) are immediate from the definitions. To prove (3), we define the following binary function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$:

$$\sigma(a,b) = \begin{cases} 111 & \text{if } a = 1 \text{ and } b = 11 \\ 0 & \text{if } a = 111 \text{ and } b = 1111 \\ \text{undefined} & \text{otherwise.} \end{cases}$$

By "undefined" above we do not mean some new token "undefined," but rather we simply mean that for cases handled by that line of the definition $(a,b) \notin \text{domain}(\sigma)$.

Let $\widehat{\sigma}$ be the extension of σ defined in Definition 1.3. Note that $(1\widehat{\sigma}11)\widehat{\sigma}1111 = 0$, but $1\widehat{\sigma}(11\widehat{\sigma}1111) = \perp$. Thus, σ is not associative. However, σ *is* weakly associative, since no three strings in Σ^* satisfy the four domain conditions required in Definition 1.2. ∎

Definition 1.5 *1. A binary function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ is an* AOWF *if and only if σ is both associative and a one-way function.*

2. [RS97] *A binary function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ is an* A^{w}OWF *if and only if σ is both weakly associative and a one-way function.*

Rabi and Sherman [RS97] also introduce the notion of *strong* one-way functions—binary one-way functions that are hard to invert even if one of their arguments is given. Strongness clearly implies one-way-ness. (We note that "strongness" here should not be confused with the property of strong-FP-invertibility of functions introduced by Allender [All86,All85].)

To avoid any possibility of ambiguity we henceforward, when using equality signs with partial functions, will make it explicit that by equality we mean $=_c$.

Definition 1.6 *A binary function σ is said to be* strong *if and only if σ is not* FP*-invertible even if one of its arguments is given. More formally, binary function σ is* strong *if and only if neither (a) nor (b) holds:*

(a) *There exists a total function $g_1 \in$ FP such that for every $z \in$ range(σ) and for each $x \in \Sigma^*$, if $\sigma(x, y) =_c z$ for some $y \in \Sigma^*$, then $\sigma(x, g_1(\langle x, z\rangle)) =_c z$.*

(b) *There exists a total function $g_2 \in$ FP such that for every $z \in$ range(σ) and for each $y \in \Sigma^*$, if $\sigma(x, y) =_c z$ for some $x \in \Sigma^*$, then $\sigma(g_2(\langle y, z\rangle), y) =_c z$.*

2 Main Result

Rabi and Sherman [RS97] show that A^{w}OWFs exist if and only if P $\neq$ NP. They present no evidence that *strong* A^{w}OWFs exist, and they establish no structural conditions sufficient to imply that any exist. Solving these open questions, we show in Theorem 2.1 below that there exist strong, total, commutative A^{w}OWFs (equivalently, strong, total, commutative AOWFs) if and only if P $\neq$ NP.

Theorem 2.1 *The following are equivalent.*

1. P $\neq$ NP.
2. *There exist A^wOWFs.*
3. *There exist AOWFs.*
4. *There exist strong, total, commutative A^wOWFs.*
5. *There exist strong, total, commutative AOWFs.*

Proof. By Proposition 1.4.2, (4) and (5) are equivalent. Rabi and Sherman [RS97] have shown the equivalence of (1) and (2), by exploiting the associativity of the closest common ancestor relation for configurations in the computation tree of nondeterministic Turing machines. Since (5) (and, equivalently, (4)) implies (2) and (3), and since each of (2) and (3) implies (1) (by Proposition 1.4.1 and by the equivalence of (1) and (2)), it suffices to show that (1) implies (5) to establish the theorem.

Assume P $\neq$ NP, and let A be a set in NP $\perp$ P. Let M be a nondeterministic polynomial-time Turing machine accepting A. By a *witness* for "$x \in A$" we mean a string $w \in \Sigma^*$ that encodes some accepting computation path of M on input x. Assume, without loss of generality, that for each $x \in A$, every witness w certifying that $x \in A$ satisfies $|w| =$

$p(|x|) > |x|$ for some strictly increasing polynomial p depending on M. For each string x, define the set of witnesses for "$x \in A$" (with respect to M) by

$$W_M(x) = \{w \mid w \text{ is a witness for "} x \in A\text{"}\}.$$

Note that if $x \notin A$ then $W_M(x) = \emptyset$.

For any strings $u, v, w \in \Sigma^*$, $\min(u, v)$ will denote the lexicographically smaller of u and v, and $\min(u, v, w)$ will denote the lexicographically smallest of u, v, and w. Define the binary function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ by

$$\sigma(a,b) = \begin{cases} \langle x, \min(w,y)\rangle & \text{if } (\exists x \in \Sigma^*)\,(\exists w, y \in W_M(x))\,[a = \langle x, w\rangle \ \wedge\ b = \langle x, y\rangle] \\ \langle x, x\rangle & \text{if } (\exists x \in \Sigma^*)\,(\exists w \in W_M(x))\,[(a = \langle x, x\rangle \ \wedge\ b = \langle x, w\rangle) \\ & \qquad\qquad \vee\ (a = \langle x, w\rangle \ \wedge\ b = \langle x, x\rangle)] \\ \text{undefined} & \text{otherwise.} \end{cases}$$

On our way towards a proof that (1) implies (5), we will first prove that the function σ defined above is a strong, commutative AOWF. Then we will show how to extend σ to a strong, total, commutative AOWF, thus establishing (5).

σ is clearly honest. Also, $\sigma \in$ FP. That is, given (a, b) as the input, it is easy to decide in polynomial time whether $(a, b) \in \text{domain}(\sigma)$, and if so, which of $\langle x, x\rangle$ or $\langle x, w\rangle$ for suitable $x \in \Sigma^*$ and $w \in W_M(x)$ should be output as the value of $\sigma(a, b)$.[3]

Now, we show that σ cannot be inverted in polynomial time, even if one of its arguments is given. Assume, for instance, that there exists a total function $g_2 \in$ FP such that given any z in the range of σ and any second argument b for which there is some $a \in \Sigma^*$ with $\sigma(a, b) =_c z$, it holds that $\sigma(g_2(\langle b, z\rangle), b) =_c z$. Then, contradicting our assumption that $A \notin$ P, A could be decided in polynomial time as follows. On input x, to decide whether or not $x \in A$, compute $g_2(\langle\langle x, x\rangle, \langle x, x\rangle\rangle)$, interpret it as a pair $\langle d, e\rangle$, and accept if and only if $d = x$ and $e \in W_M(x)$. An analogous proof works for the case of a fixed first argument. Thus, neither (a) nor (b) of Definition 1.6 holds, so σ is a strong one-way function.

We now prove that σ is associative. Let $\widehat{\sigma}$ be the extension of σ from Definition 1.3. Fix any strings $a = \langle a_1, a_2\rangle$, $b = \langle b_1, b_2\rangle$, and $c = \langle c_1, c_2\rangle$ in Σ^*. Let k equal how many of a_2, b_2, and c_2 are in $W_M(a_1)$. For example, if $a_2 = b_2 = c_2 \in W_M(a_1)$, then $k = 3$. To show that

$$(a\widehat{\sigma}b)\widehat{\sigma}c = a\widehat{\sigma}(b\widehat{\sigma}c) \tag{2.a}$$

[3]Recall our assumption that for each $x \in A$, every witness w for "$x \in A$" satisfies $|w| = p(|x|) > |x|$. This assumption ensures that there is no ambiguity in determining whether a and b are of the form $\langle x, x\rangle$ or of the form $\langle x, \text{PotentialWitness}\rangle$, and checking items of the form $\langle x, \text{PotentialWitness}\rangle$ is easy as $\bigcup_{x\in\Sigma^*} W_M(x)$ is in P.

holds, we distinguish the following cases.

Case 1: $[a_1 \neq b_1 \ \vee \ a_1 \neq c_1 \ \vee \ b_1 \neq c_1]$. In light of the definition of σ, we have

$$(a\widehat{\sigma}b)\widehat{\sigma}c = \bot = a\widehat{\sigma}(b\widehat{\sigma}c). \tag{2.b}$$

Case 2: $[a_1 = b_1 = c_1 \ \wedge \ \{a_2, b_2, c_2\} \not\subseteq \{a_1\} \cup W_M(a_1)]$. (2.b) holds here too, in light of the definition of σ.

Case 3: $[a_1 = b_1 = c_1 \ \wedge \ \{a_2, b_2, c_2\} \subseteq \{a_1\} \cup W_M(a_1)]$. In this case, note that $\widehat{\sigma}$ decreases by one the number of witnesses, in particular preserving the lexicographic minimum if both arguments contain witnesses for "$a_1 \in A$," outputting $\langle a_1, a_1 \rangle$ if exactly one of its arguments contains a witness for "$a_1 \in A$," and outputting $\bot$ if neither contains a witness for "$a_1 \in A$." So it is not hard to see that (in the current case) if $k \in \{0, 1\}$ then (2.b) holds, if $k = 2$ then

$$(a\widehat{\sigma}b)\widehat{\sigma}c = \langle a_1, a_1 \rangle = a\widehat{\sigma}(b\widehat{\sigma}c)$$

holds, and if $k = 3$ then

$$(a\widehat{\sigma}b)\widehat{\sigma}c = \langle a_1, \min(a_2, b_2, c_2) \rangle = a\widehat{\sigma}(b\widehat{\sigma}c)$$

holds.

Note that in each case (2.a) is satisfied. Furthermore, it is easy to see from the definition of σ that σ is commutative. Thus, σ is a strong, commutative AOWF, as claimed earlier.

Finally, to complete the proof, we now show how to extend σ to a strong, *total*, commutative AOWF.[4] The fact that σ is an AOWF (rather than merely an A$^{\text{w}}$OWF) helps us avoid the key problem in Rabi and Sherman's extension attempt (see Footnote 4).

Fix any string $x_0 \notin A$ (one must exist, since $A \notin \text{P}$). Let a_0 be the pair $\langle x_0, 1x_0 \rangle$. Note that a_0 is neither of the form $\langle x, x \rangle$ for any $x \in \Sigma^*$, nor of the form $\langle x, w \rangle$ for any $x \in \Sigma^*$

[4] Rabi and Sherman [RS97] give a construction that they claim lifts any A$^{\text{w}}$OWF whose domain is in P to a total A$^{\text{w}}$OWF. However, it is far from clear that their construction achieves this. In fact, we show that any proof that their construction is valid would immediately prove that UP = NP. (Note: Valiant's class UP consists of those languages accepted by nondeterministic polynomial-time Turing machines having the property that on all inputs they have no more than one accepting path [Val76].) In particular, we provide the following counterexample to Rabi and Sherman's assertion, the proof of which shows that if UP $\neq$ NP then their construction does not always preserve weak associativity.

Proposition 2.2 *If* UP $\neq$ NP, *then there exists an* A$^{\text{w}}$OWF $\tilde{\sigma}$ *satisfying* $(\exists \tilde{a})[(\tilde{a}, \tilde{a}) \notin \text{domain}(\tilde{\sigma})]$ *such that the construction that Rabi and Sherman claim converts* A$^{\text{w}}$OWFs *into total* A$^{\text{w}}$OWFs *in fact fails on* $\tilde{\sigma}$.

We prove the proposition as follows. Fix a set $A' \in \text{NP} - \text{UP}$ and an NP machine M' accepting A'. Let the polynomial p' and, for each x, let the witness sets $W_{M'}(x)$ be defined analogous to the definitions of p and

and any witness $w \in W_M(x)$ (because $x_0 \notin A$ and thus does not have any witnesses). Note that, by the definition of σ, for each y, $(a_0, y) \notin \text{domain}(\sigma)$ and $(y, a_0) \notin \text{domain}(\sigma)$. Define the total function $\tau : \Sigma^* \times \Sigma^* \to \Sigma^*$ as follows: Whenever $(a, b) \in \text{domain}(\sigma)$, define $\tau(a, b) = \sigma(a, b)$; otherwise, define $\tau(a, b) = a_0$.

τ is a strong, total, commutative AOWF. In particular, τ is honest, since for a_0, which is the only string in the range of τ that is not in the range of σ, it holds that $\tau(a_0, a_0) = a_0$ and $|a_0| + |a_0| \leq 2|a_0|$. Also, $\tau \in \text{FP}$, since $\sigma \in \text{FP}$ and $\text{domain}(\sigma) \in \text{P}$. That τ is strong follows from the facts that $\text{range}(\sigma) \subseteq \text{range}(\tau)$ and σ is strong. Finally, to see that τ is associative, note that if $a\widehat{\sigma}(b\widehat{\sigma}c) = \perp$ then $a\tau(b\tau c) = a_0$ and otherwise $a\tau(b\tau c) = a\widehat{\sigma}(b\widehat{\sigma}c)$. Similarly, if $(a\widehat{\sigma}b)\widehat{\sigma}c = \perp$ then $(a\tau b)\tau c = a_0$ and otherwise $(a\tau b)\tau c = (a\widehat{\sigma}b)\widehat{\sigma}c$. The associativity of τ now follows easily, given that σ is associative. The commutativity of τ is immediate from the definition of τ and the commutativity of σ (recall our definition of commutativity is based on (complete) equality, and thus $(a, b) \in \text{domain}(\sigma)$ if and only if $(b, a) \in \text{domain}(\sigma)$). Hence, τ is a strong, total, commutative AOWF. ∎

Rabi and Sherman emphasize the importance of explicitly exhibiting strong, total AᵂOWFs [RS97], since the cryptographic protocols given in [RS97] rely on their existence, and they also pose as an open issue the problem of whether a strong, total AᵂOWF can be constructed from any given one-way function [RS93]. The proof of Theorem 2.1 solves these open issues. Indeed, the function τ defined in the above proof shows how to construct a strong, total, commutative AOWF (equivalently, a strong, total, commutative AᵂOWF)

$W_M(x)$ earlier in the proof of Theorem 2.1. Define the binary function $\tilde{\sigma} : \Sigma^* \times \Sigma^* \to \Sigma^*$ by

$$\tilde{\sigma}(a,b) = \begin{cases} \langle x, w\rangle & \text{if } (\exists x \in \Sigma^*)\,(\exists w \in W_{M'}(x))\,[a = \langle x, w\rangle = b] \\ \langle x, x\rangle & \text{if } (\exists x \in \Sigma^*)\,(\exists w \in W_{M'}(x))\,[(a = \langle x, x\rangle \ \wedge\ b = \langle x, w\rangle) \\ & \qquad\qquad \vee\ (a = \langle x, w\rangle \ \wedge\ b = \langle x, x\rangle)] \\ \text{undefined} & \text{otherwise.} \end{cases}$$

It is not hard to verify that $\tilde{\sigma}$ is indeed an AᵂOWF. Let $\tilde{a}$ be a fixed string such that $(\tilde{a}, \tilde{a}) \notin \text{domain}(\tilde{\sigma})$. For the particular function $\tilde{\sigma}$ defined above, such a string $\tilde{a}$ indeed exists (e.g., let $\tilde{a} = \langle x_0, 1x_0\rangle$ for any particular fixed $x_0 \notin A'$, see the discussion of a_0 in the proof of Theorem 2.1 as to why this is right)—in contrast, the "c" of [RS97, p. 242, l. 10] may not in general exist. Now, using the Rabi-Sherman technique, extend $\tilde{\sigma}$ to a total function, $\tilde{\tau}$, the same way we will obtain the total extension τ of σ later in the proof of Theorem 2.1. Fix some string $\tilde{x} \in A'$ that has two distinct witnesses w and y in $W_{M'}(\tilde{x})$ (such $\tilde{x}$, w, and y exist, as $A' \notin \text{UP}$), and let $a = \langle \tilde{x}, w\rangle$, $b = \langle \tilde{x}, y\rangle$, and $c = \langle \tilde{x}, \tilde{x}\rangle$. Then, we have $(a\tilde{\tau}b)\tilde{\tau}c = \tilde{a} \neq \langle \tilde{x}, \tilde{x}\rangle = a\tilde{\tau}(b\tilde{\tau}c)$, and thus $\tilde{\tau}$ is not associative (and thus is not weakly associative). (The reason that $(a\tilde{\tau}b)\tilde{\tau}c = \tilde{a}$ may not be clear to the reader; to see why this holds, one must look at the Rabi-Sherman technique of extending $\tilde{\sigma}$ to $\tilde{\tau}$, which, very informally, is to use $\tilde{a}$ as a dumping ground.) We mention that, for essentially the same reason, $\tilde{\sigma}$ is not associative (and thus is not an AOWF), since $(a\widehat{\tilde{\sigma}}b)\widehat{\tilde{\sigma}}c = - \neq \langle \tilde{x}, \tilde{x}\rangle = a\widehat{\tilde{\sigma}}(b\widehat{\tilde{\sigma}}c)$, where $\widehat{\tilde{\sigma}}$ is the extension of $\tilde{\sigma}$ from Definition 1.3.

Even if Rabi and Sherman's proof were valid, their claim would not be particularly useful to them, as the AᵂOWFs they construct [RS97, proof of Theorem 5] do not in general have domains that are in P. In contrast, our σ *does* have a domain that is in P, and their method (corrected to remove the "c" problem) does preserve associativity, and so is useful to us.

based on any clocked NP machine accepting a language in NP $\perp$ P. Similarly, the proof of Theorem 2.1 shows how, given any one-way function (along with its polynomial runtime and honesty bounds), one can obtain a clocked NP machine accepting a language in NP $\perp$P. Thus, as the title of this paper claims, from any given one-way function one can create a strong, total, commutative AOWF (equivalently, a strong, total, commutative A$^{\text{w}}$OWF).

Finally, we mention briefly the issue of injective (i.e., one-to-one) AOWFs and A$^{\text{w}}$OWFs. Valiant's class UP (unambiguous polynomial time [Val76], see Footnote 4) has long played a central role in complexity-theoretic cryptography. Rabi and Sherman give no evidence that injective A$^{\text{w}}$OWFs might exist. In fact, they prove that no total A$^{\text{w}}$OWF can be injective. Thus, in light of Proposition 1.4.2, no total AOWF can be injective. However, as Theorem 2.3 we show that P $\neq$ UP if and only if injective A$^{\text{w}}$OWFs (and indeed injective AOWFs) exist.

Note that the lack of injectivity for total AOWFs and A$^{\text{w}}$OWFs noted above can be said to be an artifact of commutativity in the following sense. Consider any commutative function σ such that there exist elements a and b with $a \neq b$ and $(a,b) \in \text{domain}(\sigma)$. Then $\sigma(a,b) =_c \sigma(b,a)$, and so σ is not injective. Now let us generalize the notion of injectivity so as to keep the general intuition of its behavior, yet so as to not to clash so strongly with commutativity. Given any binary function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$, we say σ is *unordered-injective* if and only if for all $a,b,c,d \in \Sigma^*$, if $(a,b),(c,d) \in \text{domain}(\sigma)$ and $\sigma(a,b) =_c \sigma(c,d)$, then $\{a,b\} = \{c,d\}$. That is, each element $x =_c \sigma(a,b)$ in the range of σ has at most one unordered pair $\{a,b\}$ (possibly degenerate, i.e., $\{a,a\} = \{a\}$) as its preimage. If σ is commutative, then both orderings of this unordered pair, (a,b) and (b,a), will map to x; if not, one cannot know (i.e., $\sigma(a,b) =_c x$ but $\sigma(b,a) =_c y \neq x$ is possible).

Theorem 2.3 *The following are equivalent.*[5]

1. P $\neq$ UP.

[5]**Proof of Theorem 2.3.** That (2) implies (1) follows immediately by standard techniques, and by Proposition 1.4.1, (3) implies (2). That (1), (4), and (5) are pairwise equivalent follows as a corollary from the proof of Theorem 2.1 (note, crucially, that if the definition of σ given in that proof is based on some set $A \in \text{UP} - \text{P}$, then σ is unordered-injective, since no string x in A can have more than one witness). So it suffices to prove that (1) implies (3). Assuming $A \in \text{UP} - \text{P}$, define the language $A' = \{1x \mid x \in A\}$. Clearly, $A' \in \text{UP} - \text{P}$. Let M be some UP machine accepting A'. Let the polynomial p and, for each x, let the witness sets $W_M(x)$ be defined as in the proof of Theorem 2.1 (note that, for each $x \in A'$, $W_M(x)$ now is a singleton). Without loss of generality, assume that for each $x \in A'$, the unique witness w certifying that $x \in A'$ starts with a 1 as its first bit, i.e., $w \in 1\Sigma^*$. Define the binary function $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ as follows:

$$\sigma(a,b) = \begin{cases} 0a & \text{if } a \in A' \text{ and } W_M(a) = \{b\} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Let $\widehat{\sigma}$ be the extension of σ as in Definition 1.3. Note that for all $a,b,c \in \Sigma^*$, it holds that $(a\widehat{\sigma}b)\widehat{\sigma}c = -- = a\widehat{\sigma}(b\widehat{\sigma}c)$ by definition of σ. Thus, σ is associative according to Definition 1.3. Also, σ clearly is injective, and the standard proof approach (see, e.g., the proof of Theorem 2.1) shows that σ is a one-way function. ∎

2. *There exist injective A^wOWFs.*

3. *There exist injective $AOWFs$.*

4. *There exist strong, commutative, unordered-injective A^wOWFs.*

5. *There exist strong, commutative, unordered-injective $AOWFs$.*

3 Conclusions

So, in this paper, we have shown that P $\neq$ NP is a sufficient condition for strong, total, commutative AOWFs (equivalently, for strong, total, commutative A^wOWFs) to exist. Since by standard techniques (namely, the natural binary-function injectivity-not-required analog of a result of Grollmann and Selman [GS88,Sel92], see also [Ko85]), P $\neq$ NP is also a necessary condition for the existence of such functions, we obtain a complete characterization. This characterization solves the conjecture of Rabi and Sherman that strong A^wOWFs exist [RS97], inasfar as one can solve it without solving the P $\stackrel{?}{=}$ NP question. Moreover, our proofs have shown how to construct a strong, total, commutative AOWF (equivalently, a strong, total, commutative A^wOWF) from any given one-way function, which resolves an open problem of Rabi and Sherman [RS93].

We mention that most cryptographic applications are in general concerned with average-case complexity and randomized algorithms instead of worst-case complexity and deterministic algorithms. However, as Rabi and Sherman stress, the intriguing concept of (weakly) associative one-way functions, particularly when they are total and strong and ideally in an average-case version, may be expected to be useful in many cryptographic applications such as in the key-agreement protocol proposed by Rivest and Sherman in 1984 (see [RS97]), and may eventually offer elegant solutions to a variety of practical cryptographic problems.

Acknowledgments. We thank Alan Selman for sharing with us his knowledge of the history and literature of partial functions, and of Kleene's work.

References

[All85] E. Allender. Invertible functions, 1985. PhD thesis, Georgia Institute of Technology.

[All86] E. Allender. The complexity of sparse sets in P. In *Proceedings of the 1st Structure in Complexity Theory Conference*, pages 1–11. Springer-Verlag *Lecture Notes in Computer Science #223*, June 1986.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[DH79] W. Diffie and M. Hellman. Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, 67(3):397–427, 1979.

[GS88] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.

[HRW97] L. Hemaspaandra, J. Rothe, and G. Wechsung. On sets with easy certificates and the existence of one-way permutations. In *Proceedings of the 3rd Italian Conference on Algorithms and Complexity*, pages 264–275. Springer-Verlag *Lecture Notes in Computer Science #1203*, 1997.

[Kle52] S. Kleene. *Introduction to Metamathematics*. D. van Nostrand Company, Inc., New York and Toronto, 1952.

[Ko85] K. Ko. On some natural complete operators. *Theoretical Computer Science*, 37(1):1–30, 1985.

[RH96] J. Rothe and L. Hemaspaandra. Characterizations of the existence of partial and total one-way permutations. Technical Report Math/Inf/96/7, Institut für Informatik, Friedrich-Schiller-Universität, Jena, Germany, April 1996.

[RS93] M. Rabi and A. Sherman. Associative one-way functions: A new paradigm for secret-key agreement and digital signatures. Technical Report CS-TR-3183/UMIACS-TR-93-124, Department of Computer Science, University of Maryland Baltimore County, Baltimore, MD, 1993.

[RS97] M. Rabi and A. Sherman. An observation on associative one-way functions in complexity theory. *Information Processing Letters*, 64(2):239–244, 1997.

[Sel92] A. Selman. A survey of one-way functions in complexity theory. *Mathematical Systems Theory*, 25(3):203–221, 1992.

[Val76] L. Valiant. The relative complexity of checking and evaluating. *Information Processing Letters*, 5(1):20–23, 1976.

A Open Problems

We mention the following open issues. First, note that the strong, total, commutative AOWF τ defined in the proof of Theorem 2.1 has the property that an unbounded number of elements from its domain may be mapped to a single element in its range. Can any total AOWF (or even any strong total AOWF) be two-to-one[6] or polynomial-to-oneΓ If so, what structural conditions characterize their existenceΓ

Secondly, we note that Hemaspaandra, Rothe, and Wechsung [HRW97,RH96] define a different notion of honesty (here called "complete honesty") more restrictive than the common one—the latter one being used in most papers, e.g., in [GS88,Ko85,Sel92,RS97], and also in the present paper. According to their definition, a function f is said to be *completely honest* if there exists some polynomial p such that for all elements z in the range of f and for *all* elements y in the domain of f, if $z = f(y)$ then $|y| \leq p(|z|)$. We say any AOWF (respectively, any A^{w}OWF) that is completely honest is a *complete AOWF* (respectively, a *complete* $A^{w}OWF$); and we note that all non-total AOWFs and A^{w}OWFs constructed in this paper indeed are completely honest. But what about *total* AOWFsΓ

Recall the technique that we used to lift the AOWF σ defined in the proof of Theorem 2.1 to the total AOWF τ. Clearly, this trick violates *complete* honesty, since strings of unbounded length may be mapped to a single string of fixed length. Thus, for this lifting-partial-to-total technique to work, it is crucial that the common definition of honesty (given in Definition 1.1) is used. We pose as an open problem whether complete AOWFs (respectively, strong complete AOWFs) can be turned into total complete AOWFs (respectively, total strong complete AOWFs) even under this more demanding definition of complete honesty. To solve this problem, some clever scheme of how to handle "garbage" elements (pairs on which the partial function is not defined) seems to be required to ensure that for the resulting total function no other property—such as associativity, complete honesty, etc.—is violated.

On the other hand, the fact that no total AOWF is injective (see Footnote 6) can be extended to the more flexible notion of unordered-injectivity only if complete honesty is used: Honesty as defined in Definition 1.1 seems to be too weak to make the proof of Proposition A.1 work.

Proposition A.1 *No total complete AOWF is unordered-injective.*

Proof. Suppose that there exists some total, unordered-injective, complete AOWF σ. Since

[6]Such a function cannot be one-to-one, since the result that no total A^{w}OWF is injective [RS97] is, by Proposition 1.4.2, equivalent to the assertion that no total AOWF is injective.

σ is total, unordered-injective, and associative, we have

$$(\forall a, b, c \in \Sigma^*)[(a = c \ \wedge \ \sigma(b, c) = \sigma(a, b)) \ \vee \ (a = \sigma(a, b) \ \wedge \ \sigma(b, c) = c)].$$

Fix an arbitrary string $c \in \Sigma^*$. Then, by the above statement, for all strings $a, b \in \Sigma^*$ with $a \neq c$, it holds that $a = \sigma(a, b)$. But this means that σ cannot be completely honest, since we may fix strings $a \neq c$ and b such that b is exponentially longer than a, yet $|\sigma(a, b)| = |a|$. It follows that σ is not a complete AOWF, contradicting our supposition and completing the proof. ∎