Journal of Computer and System Sciences **58**, 648–659 (1999)
Article ID jcss.1998.1613, available online at http://www.idealibrary.com on IDEAL®

Creating Strong, Total, Commutative, Associative One-Way Functions from Any One-Way Function in Complexity Theory

Lane A. Hemaspaandra*

Department of Computer Science, University of Rochester, Rochester, New York 14627
E-mail: lane@cs.rochester.edu

and

Jörg Rothe†

Institut für Informatik, Friedrich-Schiller-Universität Jena, 07740 Jena, Germany
E-mail: rothe@informatik.uni-jena.de

Received June 30, 1998; revised November 13, 1998

Rabi and Sherman 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 multiparty secret-key agreement), associative one-way functions as their key building blocks. Although 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.

Key Words: associativity; computational complexity; cryptocomplexity; cryptography; one-way functions.

1. INTRODUCTION

Rabi and Sherman [RS97, RS93] 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

* Corresponding author. Supported in part by Grants NSF-CCR-9322513, NSF-INT-9513368/DAAD-315-PRO-fo-ab, and NSF-INT-9815095/DAAD-315-PPP-gü-ab. Work done in part while visiting Friedrich-Schiller-Universität Jena.

† Supported in part by Grants NSF-INT-9513368/DAAF-315-PRO-fo-ab and NSF-INT-9815095/DAAD-315-PPP-gü-ab, and a NATO Postdoctoral Science Fellowship from the Deutscher Akademischer Austauschdienst, sponsored by the "Gemeinsames Hochschulsonderprogramm III von Bund und Ländern" program. Work done in part while visiting the University of Rochester.

0022-0000/99 $30.00

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 and Hellman [DH76, DH79] the protocol they describe has no current proof of security (even if the existence of strong, total, commutative AOWFs is given), although 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, although they do prove that AOWFs exist if $P \neq NP$.[1] 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, although 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.

This paper is organized as follows. Section 2 provides definitions and other preliminaries, Section 3 establishes our main result. Section 4 discusses an issue related to injectivity. Section 5 proves that if $UP \neq NP$ then a construction of Rabi and Sherman is invalid. Section 6 presents conclusions and describes some open issues.

2. PRELIMINARIES

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 $|x|$.

[1] We mention that, after we sent this paper to them, they (Sherman, personal communication, June 1998) informed us that they had had discussions and proof sketches towards achieving the claim that strong AOWFs exist if $P \neq NP$.

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 nondecreasing 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 2.1. Let $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ be a binary function.

1. We say σ is *honest* if and only if there exists some po1ynomial p such that for every $z \in \text{image}(\sigma)$ there exists a pair $(x, y) \in \text{domain}(\sigma)$ such that $x\sigma y = z$ and $|x| + |y| \leqslant p(|z|)$.[2]

2. We say σ is FP-*invertible* if and only if there exists a total function $g \in \text{FP}$ such that for every $z \in \text{image}(\sigma)$, $g(z)$ 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.

DEFINITION 2.2. Let $\circ : \Sigma^* \times \Sigma^* \to \Sigma^*$ be any binary function. We say $\circ$ is *weakly associative*[3] 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 nontotal functions, since it does not evaluate as being false "equations" such as "undefined = 1010" (this situation 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

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

[3] Rabi and Sherman use the term "associative" for this notion, but for reasons we will immediately make clear, we use "weakly associative" to describe their notion.

functions, our definition of associativity—given in Definition 2.3 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. Kleene writes [Kle52, pp. 327–328]:

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

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 Rabi and Sherman's results [RS97] and our results hold even under this more restrictive definition. In a similar vein, we also define commutativity for (partial) binary functions.

DEFINITION 2.3. Let $\sigma: \Sigma^* \times \Sigma^* \to \Sigma^*$ be any binary function. Define $\Gamma = \Sigma^* \cup \{\perp\}$ and define an extension $\hat{\sigma}: \Gamma \times \Gamma \to \Gamma$ of σ by

$$\hat{\sigma}(a, b) = \begin{cases} \sigma(a, b) & \text{if } a \neq 1 \text{ and } b \neq \perp \text{ and } (a, b) \in \text{domain}(\sigma) \\ \perp & \text{otherwise.} \end{cases} \tag{1'}$$

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

Every associative function is weakly associative; the converse, however, is not always true, so these are indeed different notions.

PROPOSITION 2.4. *The following statements are true.*

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. Regarding (3), note that the following binary function $\sigma: \Sigma^* \times \Sigma^* \to \Sigma^*$ is weakly associative but not associative:

$$\sigma(a, b) = \begin{cases} 111 & \text{if } a = 1 \text{ and } b = 11 \\ 0 & \text{if } a = 111 \text{ and } b = 1111 \\ \text{undefined} & \text{otherwise,} \end{cases} \tag{2'}$$

where 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 $(a, b) \notin \text{domain}(\sigma)$. ∎

DEFINITION 2.5. 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$^{\text{w}}$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 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 henceforth, when using equality signs with partial functions, will make it explicit that by equality we mean $=_{\text{c}}$.

DEFINITION 2.6. 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 $g_1 \in \text{FP}$ such that for every $z \in \text{image}(\sigma)$ and for each $x \in \Sigma^*$, if $\sigma(x, y) =_{\text{c}} z$ for some $y \in \Sigma^*$, then $\sigma(x, g_1(\langle x, z \rangle)) =_{\text{c}} z$.

(b) There exists a total function $g_2 \in \text{FP}$ such that for every $z \in \text{image}(\sigma)$ and for each $y \in \Sigma^*$, if $\sigma(x, y) =_{\text{c}} z$ for some $x \in \Sigma^*$, then $\sigma(g_2(\langle y, z \rangle), y) =_{\text{c}} z$.

3. STRONG, TOTAL, COMMUTATIVE, ASSOCIATIVE ONE-WAY FUNCTIONS

This section proves that $\text{P} \neq \text{NP}$ if and only if strong, total, commutative, associative one-way functions exist. Recall that Rabi and Sherman [RS97] show that A$^{\text{w}}$OWFs exist if and only if $\text{P} \neq \text{NP}$. However, they present no evidence that *strong* A$^{\text{w}}$OWFs exist, and they establish no structural conditions sufficient to imply that any exist. Solving these open questions, we show in Theorem 3.1 below that there exist strong, total, commutative A$^{\text{w}}$OWFs (equivalently, strong, total, commutative AOWFs) if and only if $\text{P} \neq \text{NP}$.

THEOREM 3.1. *The following five statements 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 part 2 of Proposition 2.4, (4) and (5) are equivalent. By part 1 of Proposition 2.4, (3) implies (2). 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. (5) (and, equivalently, (4)) implies (2) and (3). So to establish the theorem it suffices to show that (1) implies (5).

We will soon define a key function, σ. We at that point describe the intuition behind it, and we describe the two-phase strategy our proof will follow.

Assume $P \neq NP$, and let A be a set in $NP - P$. 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 only on M. For each string x, define the set of witnesses for "$x \in A$" (with respect to M) by

$$W_M(x) = \{ w \mid w \text{ is a witness for "} x \in \mathrm{A}\text{"} \}. \tag{3'}$$

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

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

$$\sigma(a, b) = \begin{cases} \langle x, \min(w_1, w_2) \rangle & \text{if } (\exists x \in \Sigma^*)\,(\exists w_1, w_2 \in W_M(x)) \\ & \quad [a = \langle x, w_1 \rangle \wedge b = \langle x, w_2 \rangle] \\ \langle x, x \rangle & \text{if } (\exists x \in \Sigma^*)\,(\exists w \in W_M(x))[(a = \langle x, x \rangle \wedge \\ & \quad b = \langle x, w \rangle) \vee (a = \langle x, w \rangle \wedge b = \langle x, x \rangle)] \\ \text{undefined} & \text{otherwise.} \end{cases} \tag{4'}$$

Very informally put, the intuition behind σ is that it reduces the number of witnesses by one, in a particular, careful way. "Case 3" below describes this more specifically. Also very informally put, the intuition behind why σ will prove to be hard to invert is that inversion requires obtaining witness information.

Our proof takes a two-step approach. In particular, on our way towards a proof that (1) implies (5), we will first prove that:

Claim A. The function σ defined above is a strong, commutative AOWF.

Then we will:

Task B. Show how to extend σ to a strong, total, commutative AOWF.

Proof of Claim A. Note that σ is honest. Also, $\sigma \in \mathrm{FP}$. That is, given (a, b) as the input, it is easy to decide in polynomial time whether $(a, b) \in \mathrm{domain}(\sigma)$ 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 $\sigma(a, b)$. (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 $\langle x, \mathrm{PotentialWitness}\rangle$, and checking items of the form $\langle x, \mathrm{PotentialWitness}\rangle$ is easy because $\bigcup_{x \in \Sigma^*} W_M(x)$ is in P.)

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 $g_2 \in \mathrm{FP}$ such that given any z in the image 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 2.6 holds, so σ is a strong one-way function.

We now prove that σ is associative. Let $\hat{\sigma}$ be the extension of σ from Definition 2.3. 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

$$(a\hat{\sigma}b)\hat{\sigma}c = a\hat{\sigma}(b\hat{\sigma}c) \tag{5'}$$

holds, we distinguish three 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

$$(a\hat{\sigma}b)\hat{\sigma}c = \perp = a\hat{\sigma}(b\hat{\sigma}c). \tag{6'}$$

Case 2. $[a_1 = b_1 = c_1 \wedge \{a_2, b_2, c_2\} \not\subseteq \{a_1\} \cup W_M(a_1)]$. Equation (6′) holds, 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 $\hat{\sigma}$ decreases by one the number of witnesses. In particular, $\hat{\sigma}$ preserves the lexicographic minimum if both arguments contain witnesses for "$a_1 \in A$," outputs $\langle a_1, a_1\rangle$ if exactly one of its arguments contains a witness for "$a_1 \in A$," and outputs $\perp$ if neither contains a witness for "$a_1 \in A$." So we see that (in the current case) if $k \in \{0, 1\}$ then Eq. (6′) holds, if $k = 2$ then

$$(a\hat{\sigma}b)\hat{\sigma}c = \langle a_1, a_1\rangle = a\hat{\sigma}(b\hat{\sigma}c) \tag{7'}$$

holds, and if $k = 3$ then

$$(a\hat{\sigma}b)\hat{\sigma}c = \langle a_1, \min(a_2, b_2, c_2)\rangle = a\hat{\sigma}(b\hat{\sigma}c) \tag{8'}$$

holds.

Note that in each case Eq. (5′) 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. So Claim A is established. ▮

To complete the proof of Theorem 3.1, we now show how to extend σ to a strong, *total*, commutative AOWF.[4] That is, we now turn to Task B. Informally put, we will use an appropriately chosen string to plug the holes in σ. The fact that σ is an AOWF (rather than merely an A^{w}OWF) helps us avoid the key problem (see Section 5) in Rabi and Sherman's extension attempt.

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

The function τ is a strong, total, commutative AOWF. In particular, τ is honest, since for a_0, which is the only string in the image of τ that is not in the image of σ, it holds that $\tau(a_0, a_0) = a_0$ and $|a_0| + |a_0| \leqslant 2\,|a_0|$. Also, $\tau \in \mathrm{FP}$, since $\sigma \in \mathrm{FP}$ and $\mathrm{domain}(\sigma) \in \mathrm{P}$. That τ is strong follows from the facts that $\mathrm{image}(\sigma) \subseteq \mathrm{image}(\tau)$ and σ is strong. Finally, to see that τ is associative, note that if $a\hat{\sigma}(b\hat{\sigma}c) = \perp$ then $a\tau(b\tau c) = a_0$, and otherwise $a\tau(b\tau c) = a\hat{\sigma}(b\hat{\sigma}c)$. Similarly, if $(a\hat{\sigma}b)\hat{\sigma}c = \perp$ then $(a\tau b)\tau c = a_0$, and otherwise $(a\tau b)\tau c = (a\hat{\sigma}b)\hat{\sigma}c$. 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 $(a, b) \in \mathrm{domain}(\sigma)$ if and only if $(b, a) \in \mathrm{domain}(\sigma)$). Hence, τ is a strong, total, commutative AOWF. ▮

Rabi and Sherman emphasize the importance of explicitly exhibiting strong, total A^{w}OWFs [RS97], since the cryptographic protocols given in [RS97] rely on their existence. Rabi and Sherman also pose as an open issue the problem of whether a strong, total A^{w}OWF can be constructed from any given one-way function [RS93]. The proof of Theorem 3.1 solves both 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 A^{w}OWF) based on any clocked NP machine accepting a language in $\mathrm{NP} - \mathrm{P}$. Similarly, the proof of Theorem 3.1 shows how, given (as a program) any one-way function, along with its polynomial runtime and honesty bounds, one can obtain a clocked NP machine accepting a language in $\mathrm{NP} - \mathrm{P}$. Thus, as the title of this paper claims, from any given one-way

[4] Rabi and Sherman [RS97] give a construction that they claim lifts any A^{w}OWF whose domain is in P to a total A^{w}OWF. However, it is far from clear that their construction achieves this claim. In fact, Section 5 shows that any proof that their construction is valid would immediately prove that UP = NP.

function one can create a strong, total, commutative AOWF (equivalently, a strong, total, commutative A^{w}OWF).

We pass on the comment of a referee that the previous paragraph should not be read as suggesting that actually implementing such a transformation, for example in the computer language C, would be the work of just a few minutes, or would result in a very short, simple C program.

4. INJECTIVE, ASSOCIATIVE ONE-WAY FUNCTIONS

We mention briefly the issue of injective (i.e., one-to-one) AOWFs and A^{w}OWFs. Valiant [Val76] introduced the complexity class UP, unambiguous polynomial time, which 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 computation path. UP has long played a central role in complexity-theoretic cryptography. Rabi and Sherman give no evidence that injective A^{w}OWFs might exist. In fact, they prove that no total A^{w}OWF can be injective. Thus, in light of part 2 of Proposition 2.4, no total AOWF can be injective. However, as Theorem 4.1 we show that $P \neq UP$ if and only if injective A^{w}OWFs (and indeed injective AOWFs) exist.

The lack of injectivity for total, commutative AOWFs and A^{w}OWFs comes close to following already just from commutativity. 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 image 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., it is possible that $\sigma(a, b) =_{c} x$ yet for some string $y \neq x$ it holds that $\sigma(b, a) =_{c} y$).

THEOREM 4.1. *The following statements are equivalent.*

1. $P \neq UP$.
2. *There exist injective A^{w}OWFs.*
3. *There exist injective AOWFs.*
4. *There exist strong, commutative, unordered-injective A^{w}OWFs.*
5. *There exist strong, commutative, unordered-injective AOWFs.*

Proof. That (2) implies (1) follows immediately by standard techniques (those of [GS88], but for functions with two arguments). By part 1 of Proposition 2.4, (3) implies (2). That (1), (4), and (5) are pairwise equivalent follows as a corollary from the proof of Theorem 3.1; note, crucially, that if the definition of σ given in that proof is based on some set $A \in UP - P$, 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 $A \in \mathrm{UP} - \mathrm{P}$, define the language $A' = \{1x \mid x \in A\}$. Note that $A' \in \mathrm{UP} - \mathrm{P}$. 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 3.1 (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

$$\sigma(a, b) = \begin{cases} 0a & \text{if } a \in A' \text{ and } W_M(a) = \{b\} \\ \text{undefined} & \text{otherwise.} \end{cases} \tag{9'}$$

Let $\hat{\sigma}$ be the extension of σ as in Definition 2.3. Note that for all $a, b, c \in \Sigma^*$, it holds that $(a\hat{\sigma}b)\hat{\sigma}c = \perp = a\hat{\sigma}(b\hat{\sigma}c)$ by definition of σ. Thus, σ is associative, according to Definition 2.3. Also, note that σ is injective, and the standard proof approach (see, e.g., the proof of Theorem 3.1) shows that σ is a one-way function. ▌

5. ON A CONSTRUCTION OF RABI AND SHERMAN

As mentioned in footnote 4, Rabi and Sherman [RS97] give a construction that they claim lifts any A$^{\mathrm{w}}$OWF whose domain is in P to a total A$^{\mathrm{w}}$OWF. It is far from clear that their construction achieves this claim. In fact, we show that any proof that their construction is valid would immediately prove that UP = NP. In particular, we provide the following counterexample to Rabi and Sherman's assertion.

THEOREM 5.1. *If* $\mathrm{UP} \neq \mathrm{NP}$, *then there exists an* A^wOWF $\tilde{\sigma}$, *satisfying* $(\exists \tilde{a})[(\tilde{a}, \tilde{a}) \notin \mathrm{domain}(\tilde{\sigma})]$ *and having domain in* P, *such that the construction that Rabi and Sherman claim converts* A^wOWFs *into total* A^wOWFs *in fact fails on* $\tilde{\sigma}$.

Proof. The general idea behind this proof is that we will show that if $\mathrm{UP} \neq \mathrm{NP}$ then the Rabi–Sherman construction does not always preserve weak associativity.

Fix a set $A' \in \mathrm{NP} - \mathrm{UP}$ and an NP machine M' accepting A'. Let the polynomial p' and, for each x, let the witness sets $W_{M'}(x)$ be defined analogously to the definitions of p and $W_M(x)$ earlier in the proof of Theorem 3.1. Define the binary function $\tilde{\sigma}: \Sigma^* \times \Sigma^* \to \Sigma^*$ by

$$\tilde{\sigma}(a, b) = \begin{cases} \langle x, w \rangle & \text{if } (\exists x \in \Sigma^*)\,(\exists w \in W_{M'}(x))[a = \langle x, w \rangle = b] \\ \langle x, x \rangle & \text{if } (\exists x \in \Sigma^*)\,(\exists w \in W_{M'}(x))[(a = \langle x, x \rangle \wedge b = \langle x, w \rangle) \\ & \qquad \vee (a = \langle x, w \rangle \wedge b = \langle x, x \rangle)] \\ \text{undefined} & \text{otherwise.} \end{cases} \tag{10'}$$

It is not hard to verify that $\tilde{\sigma}$ is an A$^{\mathrm{w}}$OWF.

Let $\tilde{a}$ be a fixed string such that $(\tilde{a}, \tilde{a}) \notin \mathrm{domain}(\tilde{\sigma})$. 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 3.1 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 obtained the total extension "τ" of "σ" in the proof of Theorem 3.1. Fix some string $\tilde{x} \in A'$ that has two distinct witnesses w_1 and w_2 in $W_{M'}(\tilde{x})$ (such $\tilde{x}$, w_1, and w_2 exist, as $A' \notin \mathrm{UP}$), and let $a = \langle \tilde{x}, w_1 \rangle$, $b = \langle \tilde{x}, w_2 \rangle$, and $c = \langle \tilde{x}, \tilde{x} \rangle$. Then, we have $(a\tilde{\tau}b)\tilde{\tau}c = \tilde{a} \neq \langle \tilde{x}, \tilde{x} \rangle = a\tilde{\tau}(b\tilde{\tau}c)$. Thus $\tilde{\tau}$ is not associative (and thus, as it is total, 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 $(a\hat{\tilde{\sigma}}b)\hat{\tilde{\sigma}}c = \perp \neq \langle \tilde{x}, \tilde{x} \rangle = a\hat{\tilde{\sigma}}(b\hat{\tilde{\sigma}}c)$, where $\hat{\tilde{\sigma}}$ is the extension of $\tilde{\sigma}$ from Definition 2.3. ∎

Even if Rabi and Sherman's proof were valid, their claim would not be particularly useful to them, as the A$^{\mathrm{w}}$OWFs they construct [RS97, Proof of Theorem 5] do not in general have domains that are in P. In contrast, the function σ of our proof of Theorem 3.1 *does* have a domain that is in P, and their method (corrected to remove the "c" problem) does preserve associativity (note: we did not say weak associativity), and so proved useful to us.

6. CONCLUSIONS AND OPEN PROBLEMS

We have shown that $\mathrm{P} \neq \mathrm{NP}$ is a sufficient condition for strong, total, commutative AOWFs (equivalently, for strong, total, commutative A$^{\mathrm{w}}$OWFs) 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]) $\mathrm{P} \neq \mathrm{NP}$ 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$^{\mathrm{w}}$OWFs exist [RS97], inasfar as one can solve it without solving the $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$ question. Moreover, our proofs show how to construct a strong, total, commutative AOWF (equivalently, a strong, total, commutative A$^{\mathrm{w}}$OWF) from any given one-way function, which resolves an open problem of Rabi and Sherman [RS93].

We mention that most cryptographic applications are 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.

We mention two open issues. What formal claims can one prove regarding the security of the protocols of Rabi, Rivest, and Sherman? Also, in those cases where injectivity (i.e., one-to-one-ness) is known to be precluded, is polynomial-to-one-ness—or even two-to-one-ness—also precluded?

ACKNOWLEDGMENTS

We thank Alan Selman for sharing with us his knowledge of the history and literature of partial functions, and Kleene's work. We are deeply indebted to an anonymous referee for a careful, detailed report that helped us to much improve this paper's clarity and presentation.

REFERENCES

[All85] E. Allender, "Invertible Functions," Ph.D. thesis, Georgia Institute of Technology, 1985.

[All86] E. Allender, The complexity of sparse sets in P, *in* "Proceedings of the 1st Structure in Complexity Theory Conference, June 1986," Lecture Notes in Computer Science, Vol. 223, pp. 1–11, Springer-Verlag, New York/Berlin, 1986.

[DH76] W. Diffie and M. Hellman, New Directions in cryptography, *IEEE Trans. Inform. Theory* **IT-22**, No. 6 (1976), 644–654.

[DH79] W. Diffie and M. Hellman, Privacy and authentication: An introduction to cryptygraphy, *Proc. IEEE* **67**, No. 3 (1979), 397–427.

[GS88] J. Grollmann and A. Selman, Complexity measures for public-key cryptosystems, *SIAM J. Comput.* **17**, No. 2 (1988), 309–335.

[Kle52] S. Kleene, "Introduction to Metamathematics," van Nostrand, New York/Toronto, 1952.

[Ko85] K. Ko, On some natural complete operators, *Theoret. Comput. Sci.* **37**, No. 1 (1985), 1–30.

[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, College Park, MD, 1993. [Available on-line at `http://www.cs.umbc.edu/pub/REPORTS/cs-93-18.ps`].

[RS97] M. Rabi and A. Sherman, An observation on associative one-way functions in complexity theory, *Information Processing Letters* **64**, No. 2 (1997), 239–244.

[Sel92] A. Selman, A survey of one-way functions in complexity theory, *Mathematical Systems Theory* **25**, No. 3 (1992), 203–221.

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