Language Dependent Secure Bit Commitment

Toshiya Itoh[1] Yuji Ohta[1] Hiroki Shizuya[2]

[1] Department of Information Processing,
Interdisciplinary Graduate School of Science and Engineering,
Tokyo Institute of Technology,
4259 Nagatsuta, Midori-ku, Yokohama 227, Japan.

[2] Education Center for Information Processing, Tohoku University,
Kawauchi, Aoba-ku, Sendai 980, Japan.

Abstract. In this paper, we define two classes of languages, one induces opaque/transparent bit commitments and the other induces transparent/opaque bit commitments. As an application of opaque/transparent and transparent/opaque properties, we first show that if a language L induces an opaque/transparent bit commitment, then there exists a prover-practical perfect zero-knowledge proof for L, and we then show that if a language L induces a transparent/opaque bit commitment, then there exists a bounded round perfect zero-knowledge proof for L.

1 Introduction

A bit commitment is a two party (interactive) protocol between a sender S and a receiver R in which after the sender S commits to a bit $b \in \{0, 1\}$ at hand, (1) the sender S cannot change his mind in a computational or an information-theoretic sense; and (2) the receiver R learns nothing about the bit $b \in \{0, 1\}$ in a computational or an information-theoretic sense. Bit commitments have diverse applications to cryptographic protocols, especially to zero-knowledge proofs (see, e.g., [6], [1], [11], [9], [4], etc). For simplicity, we assume that a bit commitment f is noninteractive, i.e., the sender S sends to the receiver R only a single message C. According to computational power of senders and receivers, bit commitments can be classified into the following four possible types (see, e.g., [12]).

	Power of Sender S	Power of Receiver R
Type A	poly-time bounded	poly-time bounded
Type B	poly-time bounded	unbounded
Type C	unbounded	poly-time bounded
Type D	unbounded	unbounded

Feige and Shamir [6] used a bit commitment of Type A to show that any language $L \in \mathcal{NP}$ has a two round perfect zero-knowledge proof of knowledge. Brassard, Chaum, and Crépeau [1] and Naor et al [11] showed that any language $L \in \mathcal{NP}$ has a perfect zero-knowledge argument assuming the existence of a bit commitment of Type B and Bellare, Micali, and Ostrovsky [4] showed that

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 188-201, 1994.

any honest verifier statistical zero-knowledge proof for a language L can be transformed to a statistical zero-knowledge proof for the language L assuming the existence of a bit commitment of Type B. In addition, Goldreich, Micali, and Wigderson [9] used a bit commitment of Type C to show that any language $L \in \mathcal{NP}$ has a computational zero-knowledge proof. Now we look at the properties required to bit commitments for each possible type above.

Assume that the sender S is computationally unbounded. If there exist $r, s \in \{0,1\}^k$ such that $f(0,r) = f(1,s)$, then a cheating sender S^* chooses $r \in \{0,1\}^k$ to compute $C = f(0,r)$ and reveals 1 and $s \in \{0,1\}^k$ to change his mind. Thus any $r, s \in \{0,1\}^k$ must satisfy that $f(0,r) \neq f(1,s)$. Here we refer to such a bit commitment f as *transparent*. Assume that the receiver R is computationally unbounded. If the distribution of $f(0,r)$ is apart from that of $f(1,r)$, then a cheating receiver R^* might learn something about the value of the bit $b \in \{0,1\}$ only looking at $C = f(b,r)$. Thus the distributions of $f(0,r)$ and $f(1,s)$ must be almost identical. Here we refer to such a bit commitment f as *opaque*.

If both the sender S and the receiver R are computationally unbounded, then any bit commitment f must be transparent and opaque, however it is impossible to algorithmically implement such a bit commitment. This implies that there exists inherently no way of designing bit commitments of Type D. Thus only possible way of doing this is to physically implement such a bit commitment. This is referred to as an *envelope*. Assuming the existence of the envelope, Goldreich, Micali, and Wigderson [9] showed that any language $L \in \mathcal{NP}$ has a perfect zero-knowledge proof and then Ben-Or et al [2] showed that any language $L \in \mathcal{IP}$ has a perfect zero-knowledge proof. The goal of this paper is to algorithmically construct a bit commitment of Type D in a somewhat different setting.

In this paper, we consider the following framework: Our bit commitment f is allowed to have an additional input $x \in \{0,1\}^*$ and its property heavily depends on the additional input $x \in \{0,1\}^*$. In this setting, we define two classes of languages, one induces opaque/transparent bit commitments and the other induces transparent/opaque bit commitments. Informally, a language L induces an opaque/transparent bit commitment f_L if (1) for every $x \in L$, the distribution of $f_L(x,0,r)$ is *identical* to that of $f_L(x,1,r)$; and (2) for every $x \notin L$, the distribution of $f_L(x,0,r)$ is *completely different* from that of $f_L(x,1,r)$, and L induces a transparent/opaque bit commitment f_L if $\overline{L}$ induces an opaque/transparent bit commitment $f_{\overline{L}}$. Then we can show the following theorems:

Theorem 18: If a language L induces an opaque/transparent bit commitment, then there exists a prover-practical perfect zero-knowledge proof for L.

Theorem 21: If a language L induces a transparent/opaque bit commitment, then there exists a bounded round perfect zero-knowledge proof for L.

2 Preliminaries

Here we present several definitions necessary to the subsequent discussions.

Definition 1 [8]. Let $L \subseteq \{0,1\}^*$. A probability ensemble $\{U(x)\}_{x \in L}$ is said to be identical to a probability ensemble $\{V(x)\}_{x \in L}$ on L if for every $x \in L$,

$$\sum_{\alpha \in \{0,1\}^*} |\text{Prob}\{U(x) = \alpha\} - \text{Prob}\{V(x) = \alpha\}| = 0.$$

Let k be a security parameter. Let $g(b,r)$ be a polynomial (in k) time computable function. A function g is a noninteractive bit commitment if after the sender S sends $C = g(b,r)$ to the receiver R, (1) any cheating sender S^* cannot change his mind, i.e., S^* cannot reveal $r, s \in \{0,1\}^k$ such that $C = g(0,r) = g(1,s)$; and (2) any cheating receiver R^* learns nothing about the bit $b \in \{0,1\}$ only looking at $C = g(b,r)$. As a modification, let us consider bit commitments in the following setting: Let L be a language and let k be a polynomial. Assume that $f_L(x,b,r)$ is a polynomial (in $|x|$) time computable function for any $b \in \{0,1\}$ and any $r \in \{0,1\}^{k(|x|)}$.

Definition 2. A language L is said to induce an opaque/transparent (O/T for short) bit commitment f_L if

- opaque: for every $x \in L$, the distribution of $f_L(x,0,r)$ is identical to that of $f_L(x,1,r)$;
- transparent: for every $x \notin L$, there do not exist $r \in \{0,1\}^{k(|x|)}$ and $s \in \{0,1\}^{k(|x|)}$ such that $f_L(x,0,r) = f_L(x,1,s)$,

where k is a polynomial that guarantees the security of f_L.

The opaque/transparent property guarantees that for every $x \in L$, any all powerful cheating receiver R^* cannot guess better at random the value of the bit $b \in \{0,1\}$ after receiving $f_L(x,b,r)$ from the sender S and for every $x \notin L$, any all powerful cheating sender S^* cannot change his mind after sending $f_L(x,b,r)$ to the receiver R. Let $\mathcal{OT}$ be the class of languages that induce O/T bit commitments. From Definition 2, it is clear that $\mathcal{OT} \subseteq \mathcal{NP}$.

Definition 3. A language L is said to induce a transparent/opaque (T/O for short) bit commitment f_L if $\overline{L}$ induces an O/T bit commitment $f_{\overline{L}}$.

Contrary to the opaque/transparent property, the transparent/opaque property guarantees that for every $x \in L$, any all powerful cheating sender S^* cannot change his mind after sending $f_L(x,b,r)$ to the receiver R and for every $x \notin L$, any all powerful cheating receiver R^* cannot guess better at random the value of the bit $b \in \{0,1\}$ after receiving $f_L(x,b,r)$ from the sender S. Let $\mathcal{TO}$ be the class of languages that induce T/O bit commitments. From Definitions 2 and 3, it is obvious that co-$\mathcal{TO} = \mathcal{OT} \subseteq \mathcal{NP}$.

Definition 4 [8]. An interactive protocol $\langle P,V \rangle$ is an interactive proof system for a language L if there exists an honest verifier V that satisfies the following:

- completeness: there exists an honest prover P such that for every $k > 0$ and for sufficiently large $x \in L$, $\langle P,V \rangle$ halts and accepts $x \in L$ with probability at least $1 - |x|^{-k}$, where the probabilities are taken over the coin tosses of P and V.

- **soundness**: for every $k > 0$, for sufficiently large $x \notin L$, and for any cheating prover P^*, $\langle P^*, V \rangle$ halts and accepts $x \notin L$ with probability at most $|x|^{-k}$, where the probabilities are taken over the coin tosses of P^* and V.

It should be noted that the resource of P is computationally unbounded while the resource of V is bounded by probabilistic polynomial (in $|x|$) time.

In the remainder of this paper, we assume that a term "zero-knowledge" implies "blackbox simulation" zero-knowledge.

Definition 5 [10]. An interactive proof system $\langle P, V \rangle$ for a language L is said to be (blackbox simulation) perfect zero-knowledge if there exists a probabilistic polynomial time Turing machine M_U such that for any (cheating) verifier V^* and for sufficiently large $x \in L$, the probability ensemble $\{M_U(x; V^*)\}_{x \in L}$ is identical to the probability ensemble $\{\langle P, V^* \rangle(x)\}_{x \in L}$ on L, where $M(\cdot; A)$ denotes a Turing machine with blackbox access to a Turing machine A.

From a practical purpose, Boyar, Friedl, and Lund [3] defined a notion of *prover-practical* (zero-knowledge) interactive proof systems.

Definition 6 [3]. An interactive proof system $\langle P, V \rangle$ for a language $L \in \mathcal{NP}$ is said to be prover-practical if the honest prover P runs in probabilistic polynomial time and some trapdoor information on input $x \in L$ is initially written on the private auxiliary tape of P.

Let $A, B \in \mathcal{NP}$ and let g be a reduction from A to B, i.e., g is a polynomial time computable function and for any $x \in \{0,1\}^*$, $x \in A$ iff $g(x) \in B$.

Definition 7 [6]. Let $A, B \in \mathcal{NP}$. A reduction g from A to B is said to be witness-preserving if there exists a polynomial time computable function h that given a witness w for any $x \in A$, $h(x, w)$ is a witness for $g(x) \in B$.

Definition 8 [6]. Let $A, B \in \mathcal{NP}$. A reduction g from A to B is said to be polynomial time invertible if there exists a polynomial time computable function γ that given a witness w' for $g(x) \in B$, $\gamma(g(x), w')$ is a witness for $x \in A$.

3 Examples

It is obvious from the Definitions 2 and 3 that $L \in \mathcal{OT}$ iff $\overline{L} \in \mathcal{TO}$. Thus we only exemplify several languages that induce O/T bit commitments.

For graphs G and H, we use $G \simeq H$ to imply that G is isomorphic to H and use $G \not\simeq H$ to imply that G is not isomorphic to H.

Definition 9. For an integer $h > 0$, Universal Graph Isomorphism Tuple UGIT is defined to be $\mathrm{UGIT} = \{\langle h, \langle G_1^0, G_1^1 \rangle, \langle G_2^0, G_2^1 \rangle, \ldots, \langle G_h^0, G_h^1 \rangle \rangle \mid G_i^0 \simeq G_i^1$ for each i $(1 \le i \le h)\}$.

Definition 10. For an integer $h > 0$, Existential Graph Isomorphism Tuple EGIT is defined to be $\mathrm{EGIT} = \{\langle h, \langle G_1^0, G_1^1 \rangle, \langle G_2^0, G_2^1 \rangle, \ldots, \langle G_h^0, G_h^1 \rangle \rangle \mid G_i^0 \simeq G_i^1$ for some i $(1 \le i \le h)\}$.

Definition 11. Let $N = p_1^{e_1} p_2^{e_2} \cdots p_h^{e_h}$ be the prime factorization of N. Define cMODd to be $N \in$ cMODd if and only if $p_i \equiv c \pmod{d}$ for each i $(1 \le i \le h)$.

In the following, we show that the languages UGIT, EGIT, and 1MOD4 induce O/T bit commitments f_{UGIT}, f_{EGIT}, and f_{1MOD4}, respectively.

Lemma 12. *The language* UGIT *induces an* O/T *bit commitment* f_{UGIT}.

Proof: For $x = \langle h, \langle G_1^0, G_1^1\rangle, \langle G_2^0, G_2^1\rangle, \ldots, \langle G_h^0, G_h^1\rangle\rangle$, let V_i $(1 \le i \le h)$ be a set of vertices for G_i^0 and G_i^1, and let $b \in \{0,1\}$ be a bit that a sender S wishes to send to a receiver R. Here we define a bit commitment f_{UGIT} for UGIT as follows: For each i $(1 \le i \le h)$, S chooses $\pi_i \in_{\mathrm{R}} \mathrm{Sym}(V_i)$. Then S computes a graph $H_i = \pi_i(G_i^b)$ and sends $\langle H_1, H_2, \ldots, H_h\rangle$ to R.

Assume that $x \in$ UGIT. It follows from Definition 9 that $G_i^0 \simeq G_i^1$ for each i $(1 \le i \le h)$. Then the distribution of $\langle H_1, H_2, \ldots, H_h\rangle$ for $b=0$ is *identical* to that of $\langle H_1, H_2, \ldots, H_h\rangle$ for $b=1$. Assume that $x \notin$ UGIT. It follows from Definition 9 that there exists at least an i_0 $(1 \le i_0 \le h)$ such that $G_{i_0}^0 \not\simeq G_{i_0}^1$. This implies that $\pi_{i_0}(G_{i_0}^0) \ne \varphi_{i_0}(G_{i_0}^1)$ for any $\pi_{i_0}, \varphi_{i_0} \in \mathrm{Sym}(V_{i_0})$. Then for any $\pi_i, \varphi_i \in \mathrm{Sym}(V_i)$ $(1 \le i \le h)$,

$$f_{\mathrm{UGIT}}(x, 0, \langle \pi_1, \pi_2, \ldots, \pi_h\rangle) \ne f_{\mathrm{UGIT}}(x, 1, \langle \varphi_1, \varphi_2, \ldots, \varphi_h\rangle).$$

Thus the language UGIT induces an O/T bit commitment f_{UGIT}. ∎

For an integer $h > 0$, define Universal Quadratic Residuosity Tuple UQRT to be UQRT $= \{\langle h, \langle x_1, N_1\rangle, \ldots, \langle x_h, N_h\rangle\rangle \mid x_i$ is a square modulo N_i for each i $(1 \le i \le h)\}$. Then in a way similar to Lemma 12, we can show the following:

Lemma 13. *The language* UQRT *induces an* O/T *bit commitment* f_{UQRT}.

Let us proceed to show the other examples.

Lemma 14. *The language* EGIT *induces an* O/T *bit commitment* f_{EGIT}.

Proof: Let $x = \langle h, \langle G_1^0, G_1^1\rangle, \langle G_2^0, G_2^1\rangle, \ldots, \langle G_h^0, G_h^1\rangle\rangle$ and let V_i $(1 \le i \le h)$ be a set of vertices for G_i^0 and G_i^1. Let $b \in \{0,1\}$ be a bit that a sender S wishes to send to a receiver R. Here we define a bit commitment f_{EGIT} for EGIT as follows: For each i $(1 \le i \le h)$, S first chooses $e_i \in_{\mathrm{R}} \{0,1\}$ and $\pi_i \in_{\mathrm{R}} \mathrm{Sym}(V_i)$. Then S computes $c \equiv e_1 + e_2 + \cdots + e_h + b \pmod{2}$ and a graph $H_i = \pi_i(G_i^{e_i})$ $(1 \le i \le h)$ and sends $\langle c, H_1, H_2, \ldots, H_h\rangle$ to R.

Assume that $x \in$ EGIT. It follows from Definition 10 that there exists at least an i_0 $(1 \le i_0 \le h)$ such that $G_{i_0}^0 \simeq G_{i_0}^1$. Then on that position i_0 $(1 \le i_0 \le h)$, the distribution of $\pi_{i_0}(G_{i_0}^0)$ is *identical* to that of $\pi_{i_0}(G_{i_0}^1)$. This implies that the distribution of $\langle c, H_1, H_2, \ldots, H_h\rangle$ for $b=0$ is *identical* to that of $\langle c, H_1, H_2, \ldots, H_h\rangle$ for $b=1$. Assume that $x \notin$ EGIT. It follows from Definition 10 that for every i $(1 \le i \le h)$, $G_i^0 \not\simeq G_i^1$. Then for any $e_i, d_i \in \{0,1\}$ and $\pi_i, \varphi_i \in \mathrm{Sym}(V_i)$ $(1 \le i \le h)$,

$$f_{\mathrm{EGIT}}(x, 0, \langle e_1, \ldots, e_h\rangle, \langle \pi_1, \ldots, \pi_h\rangle) \ne f_{\mathrm{EGIT}}(x, 1, \langle d_1, \ldots, d_h\rangle, \langle \varphi_1, \ldots, \varphi_h\rangle).$$

Thus the language EGIT induces an O/T bit commitment f_{EGIT}. ■

For an integer $h > 0$, define Existential Quadratic Residuosity Tuple EQRT to be EQRT $= \{\langle h, \langle x_1, N_1\rangle, \ldots, \langle x_h, N_h\rangle\rangle \mid x_i$ is a square modulo N_i for some i $(1 \le i \le h)\}$. Then in a way similar to Lemma 14, we can show the following:

Lemma 15. *The language* EQRT *induces an* O/T *bit commitment* f_{EQRT}.

The final example has different flavor from those of the examples above.

Lemma 16. *The language* 1MOD4 *induces an* O/T *bit commitment* f_{1MOD4}.

Proof: Let $x = p_1^{e_1} p_2^{e_2} \cdots p_h^{e_h}$ be the prime factorization of x. Let $b \in \{0,1\}$ be a bit that a sender S wishes to send to a receiver R. Define a bit commitment f_{1MOD4} for 1MOD4 as follows: First S chooses $r \in_{\mathrm{R}} Z_x^*$. Then S computes $c \equiv (-1)^b r^2 \pmod{x}$ and sends $c \in Z_x^*$ to R. It should be noted that -1 is a square modulo x if and only if $x \in$ 1MOD4.

Assume that $x \in$ 1MOD4. From Definition 11 and the fact that -1 is a square modulo x, it follows that $c \in Z_x^*$ is always a square modulo x regardless of the value of $b \in \{0,1\}$. This implies that the distribution of $c \in Z_x^*$ for $b = 0$ is *identical* to that of $c \in Z_x^*$ for $b = 1$. Assume that $x \notin$ 1MOD4. From Definition 11 and the fact that -1 is not a square modulo x, it follows that for any $r \in Z_x^*$, $c \equiv (-1)^b r^2 \pmod{x}$ is a square modulo x if and only if $b = 0$. Then for any $r, s \in Z_x^*$, $f_{\mathrm{1MOD4}}(x, 0, r) \neq f_{\mathrm{1MOD4}}(x, 1, s)$. Thus the language 1MOD4 induces an O/T bit commitment f_{1MOD4}. ■

It is easy to show that (1) $2 \in Z_N^*$ is a square modulo N if and only if $N \in \pm$1MOD8; (2) $3 \in Z_N^*$ is a square modulo N if and only if $N \in \pm$1MOD12; and (3) $5 \in Z_N^*$ is a square modulo N if and only if $N \in \pm$1MOD5. Then in a way similar to Lemma 16, we can show the following:

Lemma 17. *The languages* $\pm$1MOD8, $\pm$1MOD12, *and* $\pm$1MOD5 *induce* O/T *bit commitments* $f_{\pm\mathrm{1MOD8}}$, $f_{\pm\mathrm{1MOD12}}$, *and* $f_{\pm\mathrm{1MOD5}}$, *respectively.*

4 Opaque/Transparent Bit Commitments

Assume that a language L induces an O/T bit commitment f_L. Now let us consider the interactive protocol $\langle A, B\rangle$ on input $x \in \{0,1\}^*$: (A1) A chooses $b \in_{\mathrm{R}} \{0,1\}$ and $r \in_{\mathrm{R}} \{0,1\}^{k(|x|)}$ and sends $a = f_L(x, b, r)$ to B; (B1) B chooses $e \in_{\mathrm{R}} \{0,1\}$ and sends $e \in \{0,1\}$ to A; (A2) A sends to B $\sigma \in \{0,1\}^{k(|x|)}$ such that $a = f_L(x, e, \sigma)$; and (B2) B checks that $a = f_L(x, e, \sigma)$. After $n = |x|$ independent invocations from step A1 to step B2, V accepts $x \in \{0,1\}^*$ if and only if every check in step B2 is successful.

By the opaque/transparent property of f_L, we can show in almost the same way as the case of random self-reducible languages [13] that L has a perfect zero-knowledge proof. In the protocol $\langle A, B\rangle$, however, A needs to evaluate $\sigma \in \{0,1\}^{k(|x|)}$ such that $a = f_L(x, e, \sigma)$ for each iteration. Thus in general, $\langle A, B\rangle$ could not be prover-practical. In this section, we show a stronger result, i.e., L has a prover-practical perfect zero-knowledge proof.

Theorem 18. *If a language L induces an* O/T *bit commitment, then there exists a* prover-practical *perfect zero-knowledge proof for the language L.*

Proof: Let f_L be an O/T bit commitment induced by a language L. From Definition 2, we have an $\mathcal{NP}$-statement below:

$$x \in L \Longleftrightarrow \exists r, s \in \{0,1\}^{k(|x|)} \text{ s.t. } f_L(x,0,r) = f_L(x,1,s). \tag{1}$$

Let us consider the following interactive protocol $\langle P, V\rangle$ for L.

Interactive Protocol $\langle P, V\rangle$ for L

common input: $x \in \{0,1\}^*$.

P0-1: P reduces an $\mathcal{NP}$-statement of Eq.(1) to a directed Hamiltonian graph $G=(V,E)$, where $|V| = n = |x|^c$ for some constant $c > 0$.
P0-2: P defines an adjacency matrix $A_G = (a_{ij})$ of $G=(V,E)$.
V0-1: V reduces an $\mathcal{NP}$-statement of Eq.(1) to a directed Hamiltonian graph $G=(V,E)$, where $|V| = n = |x|^c$ for some constant $c > 0$.
V0-2: V defines an adjacency matrix $A_G = (a_{ij})$ of $G=(V,E)$.
P1-1: P chooses $\pi \in_R \mathrm{Sym}(V)$ and $s_{ij} \in_R \{0,1\}^{k(|x|)}$ $(1 \le i, j \le n)$.
P1-2: P computes $c_{ij} = f_L(x, a_{\pi(i)\pi(j)}, s_{ij})$.
$P \to V$: $C = (c_{ij})$ $(1 \le i, j \le n)$.
V1: V chooses $e \in_R \{0,1\}$.
$V \to P$: $e \in \{0,1\}$.
P2-1: For $e=0$, P assigns $\langle \pi, s_{11}, \ldots, s_{nn}\rangle$ to w.
P2-2: For $e=1$, P assigns $\langle\langle i_1, j_1\rangle, \ldots, \langle i_n, j_n\rangle, s_{i_1 j_1}, \ldots, s_{i_n j_n}\rangle$ to w such that $\langle i_1, j_1\rangle, \ldots, \langle i_n, j_n\rangle$ is a single cycle.
$P \to V$: w.
V2-1: For $e=0$, V checks that $c_{ij} = f_L(x, a_{\pi(i)\pi(j)}, s_{ij})$ for each i, j $(1 \le i, j \le n)$.
V2-2: For $e=1$, V checks that $\langle i_1, j_1\rangle, \ldots, \langle i_n, j_n\rangle$ is indeed a single cycle and that $c_{i_m j_m} = f_L(x, 1, s_{i_m j_m})$ for each m $(1 \le m \le n)$.

After $n = |V|$ independent invocations from step P1-1 to step V2-2, V accepts $x \in \{0,1\}^*$ if and only if every check in step V2-1 and step V2-2 is successful.

We show that the protocol $\langle P, V\rangle$ is a prover-practical perfect zero-knowledge proof for the language L if L induces an O/T bit commitment f_L.

Completeness: If L induces an O/T bit commitment f_L, then $L \in \mathcal{NP}$, i.e.,

$$x \in L \Longleftrightarrow \exists r, s \in \{0,1\}^{k(|x|)} \text{ s.t. } f_L(x,0,r) = f_L(x,1,s).$$

Assume that for the common input $x \in L$ to $\langle P, V\rangle$, the honest prover P has $r, s \in \{0,1\}^{k(|x|)}$ such that $f_L(x,0,r) = f_L(x,1,s)$. Since the reduction from any $L \in \mathcal{NP}$ to a directed Hamiltonian graph (DHAM) is known to be witness-preserving, P can compute in polynomial (in $|x|$) time a Hamiltonian cycle H of $G=(V,E)$ in step P0-1. Then P can execute in polynomial (in $|x|$) time every process of $\langle P, V\rangle$. It is obvious that P always causes V to accept $x \in L$.

Soundness: From Eq.(1), it follows that for any $x \notin L$, there does not exist $r, s \in \{0,1\}^{k(|x|)}$ such that $f_L(x,0,r) = f_L(x,1,s)$. This implies that $G = (V,E)$ generated in step V0-1 is not a Hamiltonian graph. We show the soundness condition of $\langle P, V\rangle$ by contradiction. Assume that for some $k_0 > 0$ and infinitely many $x \notin L$, there exists a cheating prover P^* that causes V to accept $x \notin L$ with probability at least $|x|^{-k_0}$. Let $L' \subseteq \overline{L}$ be an infinite set of such $x \notin L$. Then from a standard analysis (see, e.g., [5]), it follows that there must exist $C = (c_{ij})$ that passes both tests in steps V2-1 and V2-2. We note that for any $x \in L'$, there do not exist $r, s \in \{0,1\}^{k(|x|)}$ such that $f_L(x,0,r) = f_L(x,1,s)$. This implies that P^* cannot change his mind after step P1-2 even if P^* is infinitely powerful. To pass the test in step V2-1, $C = (c_{ij})$ must be an encoding of a non-Hamiltonian graph $G = (V,E)$ generated in step V0-1, while to pass the test in step V2-2, $C = (c_{ij})$ must be an encoding of a Hamiltonian graph $\tilde{G} = (\tilde{V}, \tilde{E})$. This contradicts the assumption that $G = (V,E)$ generated in step V0-1 is not a Hamiltonian graph. Then for each $k > 0$ and sufficiently large $x \notin L$, any cheating prover P^* causes V to accept $x \notin L$ with probability at most $|x|^{-k}$.

Perfect Zero-Knowledgeness: This can be shown in a way similar to the case of random self-reducible languages [13]. The construction of M_U for any cheating verifier V^* is as follows:

Construction of M_U

common input: $x \in L$.

M0-1: $\mathbf{count} := 0$; and $\mathbf{conv} := \varepsilon$, where ε is a null string.
M0-2: M_U provides V^* with r_{V^*} as random coin tosses for V^*.
M0-3: M_U simulates steps P0-1 and P0-2.
M1-1: M_U chooses $\alpha \in_R \{0,1\}$.
M1-2: M_U chooses an n vertex random cycle of which adjacency matrix is $H = (h_{ij})$.
M2-1: If $\alpha = 0$, then M_U simulates steps P1-1 and P1-2.
M2-2: If $\alpha = 1$, then M_U chooses $s_{ij} \in_R \{0,1\}^{k(|x|)}$ and computes $c_{ij} = f(x, h_{ij}, s_{ij})$.
M3: M_U runs V^* on input $\langle x, r_{V^*}, \mathbf{conv}, C\rangle$ to generate e.
M4-1: If $e \notin \{0,1\}$, then M_U halts and outputs $\langle x, r_{V^*}, \mathbf{conv}\|\langle C, e\rangle\rangle$, where $x\|y$ denotes the concatenation of strings $x, y \in \{0,1\}^*$.
M4-2: If $e \neq \alpha$, then go to step M1-1.
M4-3: If $e = \alpha$, then M_U simulates steps P2-1 and P2-2 depending on $\alpha \in \{0,1\}$.
M5-1: M_U sets $\mathbf{conv} := \mathbf{conv}\|\langle C, e, w\rangle$ and $\mathbf{count} := \mathbf{count} + 1$.
M5-2: If $\mathbf{count} < n$, then go to step M1-1; otherwise M_U halts and outputs $\langle x, r_{V^*}, \mathbf{conv}\rangle$.

Note that for any $x \in L$, the distribution of $f_L(x,0,r)$ is identical to that of $f_L(x,1,r)$. This implies that the distribution of $f_L(x, a_{\pi(i)\pi(j)}, s_{ij})$ is identical to that of $f_L(x, h_{ij}, s_{ij})$ for every $x \in L$. Then the probability that $e = \alpha$ in step M4-3 is *exactly* 1/2. Since M_U iterates $n = |x|^c$ times the procedure from step M1-1 to step M5-2, M_U runs in expected polynomial (in $|x|$) time. Note again that for every $x \in L$, the distribution of $f_L(x, 0, r)$ is identical to that of $f_L(x, 1, r)$. Then the probability ensemble $\{\langle P, V^*\rangle(x)\}_{x\in L}$ is identical to the probability ensemble $\{M_U(x; V^*)\}_{x\in L}$ on L.

Thus the protocol $\langle P, V\rangle$ is a prover-practical perfect zero-knowledge proof for L if L induces an O/T bit commitment f_L. ∎

For a language $L \in \mathcal{NP}$, define a polynomial time computable relation R_L to be $\langle x, y\rangle \in R_L$ if and only if $\rho(x, y) = \mathtt{true}$, where ρ is a polynomial (in $|x|$) time computable predicate that witnesses the language $L \in \mathcal{NP}$. As immediate corollaries to Theorem 18, we can show the following:

Corollary 19 (to Theorem 18). *Let L be $\mathcal{NP}$-complete. If the language L induces an* O/T *bit commitment, then the polynomial time hierarchy collapses.*

Corollary 20 (to Theorem 18). *If a language L induces an* O/T *bit commitment, then there exists a perfect zero-knowledge proof of knowledge for R_L.*

5 Transparent/Opaque Bit Commitments

Here we consider the case that L induces a T/O bit commitment (see Definition 3), and show that if a language L induces a T/O bit commitment, then there exists a bounded round perfect zero-knowledge proof for L.

Theorem 21. *If a language L induces a* T/O *bit commitment, then there exists a two round prefect zero-knowledge proof for the language L.*

Proof: Let L be a language that induces a T/O bit commitment f_L. Here we overview the outline of the protocol $\langle P, V\rangle$ for L. Let $x \in \{0,1\}^*$ be a common input to $\langle P, V\rangle$. For each i $(1 \le i \le |x|)$, V chooses $e_i \in_R \{0,1\}$, $r_i \in_R \{0,1\}^{k(|x|)}$ and computes $\alpha_i = f_L(x, e_i, r_i)$. Then V reduces the following $\mathcal{NP}$-statement,

$$\exists e_1, e_2, \ldots, e_{|x|} \exists r_1, r_2, \ldots, r_{|x|} \text{ s.t. } \bigwedge_{i=1}^{|x|} \alpha_i = f_L(x, e_i, r_i), \tag{2}$$

to a directed Hamiltonian graph $G = (V, E)$, where $|V| = |x|^d$ for some constant $d > 0$. Let H be a Hamiltonian cycle of G. From the witness-preserving property of the reduction from any $L \in \mathcal{NP}$ to DHAM, there exist polynomial time computable functions g and h that satisfy

$$G = g(\alpha_1, \alpha_2, \ldots, \alpha_{|x|});$$
$$H = h(\langle \alpha_1, \alpha_2, \ldots, \alpha_{|x|}\rangle, \langle e_1, e_2, \ldots, e_{|x|}; r_1, r_2, \ldots, r_{|x|}\rangle).$$

Here V generates many random copies of G and commits to them with the T/O bit commitment f_L. After these preliminary steps, V shows to P that V knows the Hamiltonian cycle H of G. If V succeeds to convince P, then P shows to V that P knows $e_1, e_2, \ldots, e_{|x|}$.

Interactive Protocol $\langle P, V\rangle$ for L

common input: $x \in \{0,1\}^*$.

V1-1: V chooses $e_i \in_R \{0,1\}$ and $r_i \in_R \{0,1\}^{k(|x|)}$ for each i $(1 \le i \le |x|)$.
V1-2: V computes $\alpha_i = f_L(x, e_i, r_i)$.
V1-3: V computes $G = g(\alpha_1, \ldots, \alpha_{|x|})$, i.e., V reduces the $\mathcal{NP}$-statement of Eq.(2) to a directed Hamiltonian graph $G = (V, E)$, where $|V| = n = |x|^d$ for some $d > 0$.
V1-4: V defines an adjacency matrix $A_G = (a_{ij})$ of $G = (V, E)$.
V1-5: V computes $H = h(\langle \alpha_1, \ldots, \alpha_{|x|}\rangle, \langle e_1, \ldots, e_{|x|}; r_1, \ldots, r_{|x|}\rangle)$, where H is one of Hamiltonian cycles of $G = (V, E)$.
V1-6: V chooses $\pi_\ell \in_R \mathrm{Sym}(V)$ $(1 \le \ell \le n^2)$ and $s_{ij}^\ell \in_R \{0,1\}^{k(|x|)}$ $(1 \le i, j \le n)$.
V1-7: V computes $c_{ij}^\ell = f_L(x, a_{\pi_\ell(i)\pi_\ell(j)}, s_{ij}^\ell)$.
$V \to P$: $\langle \alpha_1, \alpha_2, \ldots, \alpha_{|x|}\rangle$, $\langle (c_{ij}^1), (c_{ij}^2), \ldots (c_{ij}^{n^2})\rangle$ $(1 \le i, j \le n)$.
P1: P chooses $b_\ell \in_R \{0,1\}$ for each ℓ $(1 \le \ell \le n^2)$.
$P \to V$: $\langle b_1, b_2, \ldots, b_{n^2}\rangle \in \{0,1\}^{n^2}$.
V2-1: If $b_\ell = 0$ $(1 \le \ell \le n^2)$, V assigns $\langle \pi_\ell, s_{11}^\ell, s_{12}^\ell, \ldots, s_{nn}^\ell\rangle$ to w_ℓ.
V2-2: If $b_\ell = 1$ $(1 \le \ell \le n^2)$, V assigns

$$\langle \langle i_1^\ell, j_1^\ell\rangle, \langle i_2^\ell, j_2^\ell\rangle, \ldots, \langle i_n^\ell, j_n^\ell\rangle, s_{i_1^\ell j_1^\ell}^\ell, s_{i_2^\ell j_2^\ell}^\ell, \ldots, s_{i_n^\ell j_n^\ell}^\ell\rangle$$

to w_ℓ such that $\langle i_1^\ell, j_1^\ell\rangle, \langle i_2^\ell, j_2^\ell\rangle, \ldots, \langle i_n^\ell, j_n^\ell\rangle$ is a single cycle.
$V \to P$: $\langle w_1, w_2, \ldots, w_{n^2}\rangle$.
P2-1: P computes $G = g(\alpha_1, \alpha_2, \ldots, \alpha_{|x|})$ and an adjacency matrix $A_G = (a_{ij})$ of G.
P2-2: For each $b_\ell = 0$ $(1 \le \ell \le n^2)$, if $c_{ij}^\ell = f_L(x, a_{\pi_\ell(i)\pi_\ell(j)}, s_{ij}^\ell)$ for each i, j $(1 \le i, j \le n)$, then P continues; otherwise P halts and rejects $x \in \{0,1\}^*$.
P2-3: For each $b_\ell = 1$ $(1 \le \ell \le n^2)$, if $\langle i_1^\ell, j_1^\ell\rangle, \langle i_2^\ell, j_2^\ell\rangle, \ldots, \langle i_n^\ell, j_n^\ell\rangle$ is indeed a single cycle and $c_{i_m^\ell j_m^\ell}^\ell = f_L(x, 1, s_{i_m^\ell j_m^\ell}^\ell)$ for each m $(1 \le m \le n)$, then P continues; otherwise P halts and rejects $x \in \{0,1\}^*$.
P2-4: If there exist $\beta_i \in \{0,1\}, t_i \in \{0,1\}^{k(|x|)}$ such that $\alpha_i = f_L(x, \beta_i, t_i)$ for every i $(1 \le i \le |x|)$, then P continues; otherwise P halts and rejects $x \in \{0,1\}^*$.
$P \to V$: $\langle \beta_1, \beta_2, \ldots, \beta_{|x|}\rangle$.
V3: If $\beta_i = e_i$ for every i $(1 \le i \le |x|)$, then V halts and accepts $x \in \{0,1\}^*$; otherwise V halts and rejects $x \in \{0,1\}^*$.

Now we turn to show that if L induces a T/O bit commitment f_L, then the protocol $\langle P, V\rangle$ for L is a two round perfect zero-knowledge proof for L.

Completeness: Assume here that $x \in L$. If V follows the protocol above, then $G = (V, E)$ is always a Hamiltonian graph. From the T/O property of f_L, it follows that for every $x \in L$, there does not exist $r, s \in \{0,1\}^{k(|x|)}$ such that $f_L(x, 0, r) = f_L(x, 1, s)$. Thus for each i $(1 \le i \le |x|)$, P can find in step P2-4 a *unique* $\beta_i \in \{0,1\}$ such that $\alpha_i = f_L(x, e_i, t_i)$ for some $t_i \in \{0,1\}^{k(|x|)}$. Then V always halts and accepts $x \in L$ in step V3.

Soundness: Assume that $x \notin L$. Define an interactive protocol $\langle A, B\rangle$ for $\overline{L} \in \mathcal{OT}$ to be on input $x \in \{0,1\}^*$ (1) A (resp. B) plays the role of V (resp. P); and (2) $\langle A, B\rangle$ simulate $\langle P, V\rangle$ except that the process from step V1-6 to step P2-3 in $\langle P, V\rangle$ is executed in serial.

From the T/O property of f_L, it follows that for every $x \notin L$, the distribution of $f_L(x, 0, r)$ is identical to that of $f_L(x, 1, s)$. Then the protocol $\langle A, B\rangle$ can be simulated in a perfect zero-knowledge manner for every $x \notin L$ by using the resettable simulation technique [9]. It turns out that the subprotocol of $\langle P, V\rangle$, from step V1-6 to step P2-3, is *perfectly witness indistinguishable* [6], because it can be regarded as the parallel composition of the protocol $\langle A, B\rangle$ by exchanging the roles of A and B. Then in the protocol $\langle P, V\rangle$, any cheating P^* cannot guess better at random the value of $e_i \in \{0,1\}$ for each i $(1 \le i \le |x|)$. Thus for each $k > 0$ and sufficiently large $x \notin L$, any cheating prover P^* causes V to accept $x \notin L$ with probability at most $|x|^{-k}$.

Perfect Zero-Knowledgeness: This can be shown in almost the same way as the case of graph nonisomorphism [9]. From the polynomial time invertible property of the reduction from any $L \in \mathcal{NP}$ to DHAM, there exist polynomial time computable functions g and γ that satisfy

$$g(\alpha_1, \ldots, \alpha_{|x|}) = G; \quad \gamma(G, H) = \langle \beta_1, \ldots, \beta_{|x|}; t_1, \ldots, t_{|x|}\rangle,$$

where H is one of Hamiltonian cycles of G and $\alpha_i = f_L(x, \beta_i, t_i)$ for each i $(1 \le i \le |x|)$. Here we use H_t to denote the *t-th* (n-vertex) single cycle for each t $(1 \le t \le n!)$ in the lexicographic order. Then the construction of M_U for any cheating verifier V^* is as follows:

Construction of M_U

common input: $x \in L$.

- M0-1: $\mathbf{count} := 1$; and $\mathbf{conv} := \varepsilon$, where ε is a null string.
- M0-2: M_U provides V^* with r_{V^*} as random coin tosses for V^*.
- M1-1: M_U runs V^* on input x, r_{V^*} to generate $\langle \alpha_1, \ldots, \alpha_{|x|}\rangle$, $\langle (c_{ij}^1), \ldots (c_{ij}^{n^2})\rangle$.
- M1-2: $\mathbf{conv} := \mathbf{conv} \| \langle \langle \alpha_1, \ldots, \alpha_{|x|}\rangle, \langle (c_{ij}^1), \ldots (c_{ij}^{n^2})\rangle\rangle$.
- M2: M_U chooses $b_\ell \in_{\mathrm{R}} \{0,1\}$ for each ℓ $(1 \le \ell \le n^2)$.
- M3-1: M_U runs V^* on input $x, r_{V^*}, \langle b_1, b_2, \ldots, b_{n^2}\rangle$ to generate $\langle w_1, \ldots, w_{n^2}\rangle$.
- M3-2: $\mathbf{conv} := \mathbf{conv} \| \langle \langle b_1, \ldots, b_{n^2}\rangle, \langle w_1, \ldots, w_{n^2}\rangle\rangle$.
- M4-1: M_U computes $G = g(\alpha_1, \ldots, \alpha_{|x|})$ and an adjacency matrix $A_G = (a_{ij})$ of G.
- M4-2: For each $b_\ell = 0$ $(1 \le \ell \le n^2)$, if $c_{ij}^\ell = f_L(x, a_{\pi_\ell(i)\pi_\ell(j)}, s_{ij}^\ell)$ for each i, j $(1 \le i, j \le n)$, then M_U continues; otherwise M_U halts and outputs $\langle x, r_{V^*}, \mathbf{conv}\rangle$.
- M4-3: For each $b_\ell = 1$ $(1 \le \ell \le n^2)$, if $\langle i_1^\ell, j_1^\ell\rangle, \langle i_2^\ell, j_2^\ell\rangle, \ldots, \langle i_n^\ell, j_n^\ell\rangle$ is indeed a single cycle and $c_{i_m^\ell j_m^\ell}^\ell = f_L(x, 1, s_{i_m^\ell j_m^\ell}^\ell)$ for each m $(1 \le m \le n)$, then M_U continues; otherwise M_U halts and outputs $\langle x, r_{V^*}, \mathbf{conv}\rangle$.

M5-1: M_U resets V^* to the state of step M1-2.
M5-2: If $\texttt{count} > n!$, then M_U halts and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$.
M5-3: If $H_{\texttt{count}}$ is a Hamiltonian cycle of G, then $H := H_{\texttt{count}}$ and go to step M7-2.
M5-4: M_U chooses $\tilde{b}_\ell \in_{\mathrm{R}} \{0,1\}$ for each ℓ $(1 \le \ell \le n^2)$.
M6-1: M_U runs V^* on input $x, r_{V^*}, \langle \tilde{b}_1, \ldots, \tilde{b}_{n^2}\rangle$ to generate $\langle \tilde{w}_1, \ldots, \tilde{w}_{n^2}\rangle$.
M6-2: For each $\tilde{b}_\ell = 0$ $(1 \le \ell \le n^2)$, if $c^\ell_{ij} = f_L(x, a_{\tilde{\pi}_\ell(i)\tilde{\pi}_\ell(j)}, \tilde{s}^\ell_{ij})$ for each i, j $(1 \le i, j \le n)$, then M_U continues; otherwise $\texttt{count} := \texttt{count} + 1$ and go to step M5-1.
M6-3: For each $\tilde{b}_\ell = 1$ $(1 \le \ell \le n^2)$, if $\langle \tilde{i}^\ell_1, \tilde{j}^\ell_1\rangle, \langle \tilde{i}^\ell_2, \tilde{j}^\ell_2\rangle, \ldots, \langle \tilde{i}^\ell_n, \tilde{j}^\ell_n\rangle$ is a single cycle and $c^\ell_{\tilde{i}^\ell_m \tilde{j}^\ell_m} = f_L(x, 1, \tilde{s}^\ell_{\tilde{i}^\ell_m \tilde{j}^\ell_m})$ for each m $(1 \le m \le n)$, then M_U continues; otherwise $\texttt{count} := \texttt{count} + 1$ and go to step M5-1.
M7-1: If $b_\ell \ne \tilde{b}_\ell$ for some ℓ $(1 \le \ell \le n^2)$, then M_U computes a Hamiltonian cycle H of $G = (V, E)$ from w_ℓ and $\tilde{w}_\ell$; otherwise $\texttt{count} := \texttt{count} + 1$ and go to step M5-1.
M7-2: M_U computes $\langle \beta_1, \beta_2, \ldots, \beta_{|x|}; t_1, t_2, \ldots, t_{|x|}\rangle = \gamma(G, H)$.
M7-3: If $\alpha_i = f_L(x, \beta_i, t_i)$ for every i $(1 \le i \le |x|)$, then set $\texttt{conv} := \texttt{conv} \| \langle \beta_1, \beta_2, \ldots, \beta_{|x|}\rangle$; otherwise M_U halts and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$.
M7-4: M_U halts and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$.

We first show that M_U terminates in expected polynomial (in $|x|$) time for any cheating verifier V^*. Define $K \subseteq \{0,1\}^{n^2}$ to be a subset of $\langle b_1, b_2, \ldots, b_{n^2}\rangle \in \{0,1\}^{n^2}$ for which V^* passes the tests in steps M4-2 and M4-3. Then the following three cases are possible: (C1) $\|K\| \ge 2$; (C2) $\|K\| = 1$; and (C3) $\|K\| = 0$, where $\|A\|$ denotes the cardinality of a finite set A.

In the case of (C1), the expected number I_{C1} of invocations of V^* satisfies

$$I_{\mathrm{C1}} \le 1 + \frac{\|K\|}{2^{n^2}} \cdot \left(\frac{\|K\| - 1}{2^{n^2}}\right)^{-1} = 1 + \frac{\|K\|}{\|K\| - 1} \le 3.$$

In the case of (C2), the probability that V^* passes the tests in steps M4-2 and M4-3 is exactly 2^{-n^2}. Then M_U halts and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$ in step M4-2 or M4-3 with probability $1 - 2^{-n^2}$. If V^* passes the tests in steps M4-2 and M4-3, then M_U must exhaustively searches a Hamiltonian cycle H of G at most in $n!$ steps. Thus it turns out that the expected number I_{C2} of invocations is bounded by $I_{C2} = 1 + 2^{-n^2} \cdot n! < 2$. In the case of (C3), M_U always halts and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$ with a single invocation of V^*. Thus M_U terminates in expected polynomial (in $|x|$) time for any cheating verifier V^*.

We then show that for any verifier V^*, M_U on any input $x \in L$ simulates the real interactions between P and V^* in a perfect zero-knowledge manner.

In the case of (C3), M_U always halts in step M4-2 or step M4-3 and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$ with the distribution identical to one in $\langle P^*, V\rangle$.

In the case of (C1), the following three cases are possible: (C1-1) M_U halts in step M4-2 or step M4-3 and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$; (C1-2) M_U halts in step M5-2 or step M7-3 and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$; and (C1-3) M_U halts in step M7-4 and outputs $\langle x, r_{V^*}, \texttt{conv}\rangle$. In the case of (C1-1), it is obvious that the distribution of

$\langle x, r_{V^*}, \mathbf{conv}\rangle$ is identical to one in $\langle P, V^*\rangle$. Note that P returns $\langle \beta_1, \beta_2, \ldots, \beta_{|x|}\rangle$ iff every α_i $(1 \le i \le |x|)$ is properly generated. From the polynomial time invertible property of the reduction from any $L \in \mathcal{NP}$ to DHAM, it follows that every α_i $(1 \le i \le |x|)$ is properly generated iff $G = g(\alpha_1, \alpha_2, \ldots, \alpha_{|x|})$ is a Hamiltonian graph. Then in the case of (C1-2), the distribution of $\langle x, r_{V^*}, \mathbf{conv}\rangle$ is identical to one in $\langle P, V^*\rangle$. Let us consider the case that M_U in step M7-1 finds $b_\ell \ne \tilde{b}_\ell$ for some ℓ $(1 \le \ell \le n^2)$. We assume without loss of generality that $b_\ell = 0$ and $\tilde{b}_\ell = 1$. Then

$$w_\ell = \langle \pi_\ell, s_{11}^\ell, s_{12}^\ell, \ldots, s_{nn}^\ell\rangle;$$
$$\tilde{w}_\ell = \langle \langle \tilde{i}_1^\ell, \tilde{j}_1^\ell\rangle, \langle \tilde{i}_2^\ell, \tilde{j}_2^\ell\rangle, \ldots, \langle \tilde{i}_n^\ell, \tilde{j}_n^\ell\rangle, \tilde{s}_{\tilde{i}_1\tilde{j}_1}^\ell, \tilde{s}_{\tilde{i}_2\tilde{j}_2}^\ell, \ldots, \tilde{s}_{\tilde{i}_n\tilde{j}_n}^\ell\rangle.$$

From the assumption that $b_\ell = 0$ and $\tilde{b}_\ell = 1$, it follows that w_ℓ passes the test in step M4-2 and $\tilde{w}_\ell$ passes the test in step M6-3. Thus the Hamiltonian cycle H of G is given by

$$H = \langle \langle \pi_\ell^{-1}(\tilde{i}_1^\ell), \pi_\ell^{-1}(\tilde{j}_1^\ell)\rangle, \langle \pi_\ell^{-1}(\tilde{i}_2^\ell), \pi_\ell^{-1}(\tilde{j}_2^\ell)\rangle, \ldots, \langle \pi_\ell^{-1}(\tilde{i}_n^\ell), \pi_\ell^{-1}(\tilde{j}_n^\ell)\rangle\rangle.$$

From the polynomial time invertible property of the reduction from any $L \in \mathcal{NP}$ to DHAM, it follows that $\gamma(G, H) = \langle \beta_1, \beta_2, \ldots, \beta_{|x|}; t_1, t_2, \ldots, t_{|x|}\rangle$ and $\alpha_i = f_L(x, \beta_i, t_i)$ $(1 \le i \le |x|)$. The T/O property of f_L guarantees that for every $x \in L$, there does not exist $r, s \in \{0,1\}^{k(|x|)}$ such that $f_L(x, 0, r) = f_L(x, 1, s)$. Then $\beta_i = e_i$ for each i $(1 \le i \le |x|)$ and thus in the case of (C1-3), the distribution of $\langle x, r_{V^*}, \mathbf{conv}\rangle$ is identical to one in $\langle P, V^*\rangle$.

In the case of (C2), the following three cases are possible: (C2-1) M_U halts in step M4-2 or step M4-3 and outputs $\langle x, r_{V^*}, \mathbf{conv}\rangle$; (C2-2) M_U halts in step M5-2 or step M7-3 and outputs $\langle x, r_{V^*}, \mathbf{conv}\rangle$; and (C2-3) M_U halts in step M7-4 and outputs $\langle x, r_{V^*}, \mathbf{conv}\rangle$. In a way similar to the case of (C1), we can show that in the cases of (C2-1), (C2-2), and (C2-3), the distribution of $\langle x, r_{V^*}, \mathbf{conv}\rangle$ is identical to one in $\langle P, V^*\rangle$. Then for any cheating verifier V^*, M_U on input $x \in L$ simulates $\langle P, V^*\rangle$ in a perfect zero-knowledge manner.

Thus the interactive protocol $\langle P, V\rangle$ is a two round perfect zero-knowledge proof for L if L induces a T/O bit commitment f_L. ∎

6 Concluding Remarks

From Theorem 18, it follows that any language $L \in \mathcal{OT}$ has an unbounded round perfect zero-knowledge Arthur-Merlin proof. This however could be improved, because any language $L \in \mathcal{OT}$ has an $\mathcal{NP}$-proof [8]. Then

1. If a language L induces an O/T bit commitment, then does there exist a bounded round perfect zero-knowledge proof for the language L?

To affirmatively solve this, a verifier will have to flip private coins, because Goldreich and Krawczyk [7] showed that there exists a bounded round (blackbox simulation) zero-knowledge Arthur-Merlin proof for L, then $L \in \mathcal{BPP}$.

Languages that induce O/T or T/O bit commitments might have diverse applications to many cryptographic protocols. Then

2. What is the other application of languages that induce O/T or T/O bit commitments?

Every known random self-reducible language [13], e.g., graph isomorphism, quadratic residuosity, etc., induces an O/T bit commitment. Then finally

3. For any language L, if L is random self-reducible, then does L induce an O/T bit commitment?

References

1. Brassard, G., Chaum, D., and Crépeau, C., "Minimum Disclosure Proofs of Knowledge," *J. Comput. System Sci.*, Vol.37, No.2, pp.156-189 (1988).
2. Ben-Or, M., Goldreich, O., Goldwasser, S., Håstad, J., Kilian, J., Micali, S., and Rogaway, P., "Everything Provable is Provable in Zero-Knowledge," *Proceedings of Crypto'88*, Lecture Notes in Computer Science 403, pp.37-56 (1990).
3. Boyar, J., Friedl, K., and Lund, C., "Practical Zero-Knowledge Proof: Giving Hints and Using Deficiencies," *J. Cryptology*, Vol.4, No.3, pp.185-206 (1991).
4. Bellare, M., Micali, S., and Ostrovsky, R., "The (True) Complexity of Statistical Zero-Knowledge," *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pp.494-502 (1990).
5. Feige, U., Fiat, A., and Shamir, A., "Zero-Knowledge Proofs of Identity," *J. Cryptology*, Vol.1, No.2, pp.77-94 (1988).
6. Feige, U. and Shamir, A., "Zero-Knowledge Proofs of Knowledge in Two Rounds," *Proceedings of Crypto'89*, Lecture Notes in Computer Science 435, pp.526-544 (1990).
7. Goldreich, O. and Krawczyk, H., "On the Composition of Zero-Knowledge Proof Systems," *Proceedings of ICALP'90*, Lecture Notes in Computer Science 443, pp.268-282 (1990).
8. Goldwasser, S., Micali, S., and Rackoff, C., "The Knowledge Complexity of Interactive Proof Systems," *SIAM J. Comput.*, Vol.18, No.1, pp.186-208 (1989).
9. Goldreich, O., Micali, S., and Wigderson, A., "Proofs That Yield Nothing But Their Validity or All Languages in $\mathcal{NP}$ Have Zero-Knowledge Proof Systems," *J. Assoc. Comput. Mach.*, Vol.38, No.1, pp.691-729 (1991).
10. Goldreich, O. and Oren, Y., "Definitions and Properties of Zero-Knowledge Proof Systems," *J. Cryptology*, Vol.7, No.1, pp.1-32 ((1994).
11. Naor, M., Ostrovsky, R., Venkatesan, R., and Yung, M., "Perfect Zero-Knowledge Arguments for $\mathcal{NP}$ Can Be Based on General Complexity Assumptions," *Proceedings of Crypto'92*, Lecture Notes in Computer Science 740, pp.196-214 (1993).
12. Ostrovsky, R., "Comparison of Bit-Commitment and Oblivious Transfer Protocols when Players have Different Computing Power," *DIMACS Technical Report* #90-41, pp.27-29 (1990).
13. Tompa, M. and Woll, H., "Random Self-Reducibility and Zero-Knowledge Interactive Proofs of Possession of Information," *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science*, pp.472-482 (1987).