Proving a Polynomial $f(x)$ with Degree $t-1$ exactly in Statistical Zero-Knowledge

*

Chunming Tang † Zhuojun Liu ‡ Mingsheng Wang§

Abstract

In this paper, we first propose two basic protocols, 1) in one protocol, the prover proves to the verifier that two committed integers are equal. 2) in another protocol, the prover convinces the verifier that a committed integer $a \neq 0$ holds. With the above protocols, we present our main protocol in which the prover can prove a polynomial $f(x)$ with degree $t-1$ exactly, in particular, our three protocols are statistical zero-knowledge proofs.

Keywords: cryptography, secret sharing, statistical zero-knowledge, commitment.

1 Introduction

In a (t, n)-secret sharing scheme, it is an interesting and practical problem how the dealer proves a polynomial $f(x)$ with degree $t-1$ exactly without revealing any further information about this polynomial to all players, where this polynomial is selected by the dealer in a field Z_p and p is a prime. There exist two reasons for the prover choosing a polynomial with degree $t-1$ exactly, one reason is in order to obtain (t, n)-scheme, the other is in order to obtain a perfect secret sharing scheme[1].

Using cut-and-choose protocol(it is not zero-knowledge), Benaloh proposed a protocol in which the dealer can convince all players a polynomial

*This work was supported in part by 973 project G1998030600.

†ctang@mmrc.iss.ac.cn, Key Laboratory of Mathematics Mechanization, Institute of Systems Science, Chinese Academy of Sciences, P.R.China

‡zliu@zgc.gov.cn, Key Laboratory of Mathematics Mechanization, Institute of Systems Science, Chinese Academy of Sciences, P.R.China

§mswang@is.iscas.ac.cn, State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, P.R.China

$f(x)$ with degree at most $t-1$, but, the protocol does not satisfy the following properties: 1) the dealer convinces all players the polynomial $f(x)$ with degree $t-1$ exactly; 2) the protocol is a zero-knowledge proof. In [2, 3], it has already been proposed as an open problem how to construct a protocol satisfying 1) and 2).

In [4], Camenisch and Michels proved in statistical zero-knowledge that $a+b = d(mod\ n)$, $ab = d(mod\ n)$, and $a^b = d(mod\ n)$ hold for commitments to a, b, d, n based on discrete logarithm. In [5], Boudot proposed a statistical zero-knowledge protocol for proving $x \in [a, b]$, where a and b are integers, and $a < b$.

In this paper, we mainly construct a protocol satisfying the 1) and 2).

The structure of this paper is following, we review camenisch and Michel's results and some other zero-knowledge proofs of knowledge based on discrete logarithm in section 2. In section 3, we prove that two committed integers are equal. In section 4, we propose a statistical zero-knowledge proofs for proving an integer $a \neq 0$. In section 5, we present a statistical zero-knowledge proof for proving a polynomial with degree $t-1$ exactly.

2 Preliminary

2.1 Commitment schemes

Pederson[6] proposed a computationally binding and unconditionally hiding scheme based on the discrete logarithm problem. Given a group G of prime order q and two random generators g and h such that $\log_g h$ is unknown and computing discrete logarithms is infeasible. A value $\alpha \in Z_q$ is committed to as $C_\alpha := g^\alpha h^r$, where r is randomly chosen from Z_q. We will use this commitment scheme for our construction and hence they will be statistical zero-knowledge proof of knowledge.

2.2 Zero-knowledge proofs of knowledge about some modular relations

In this section, we mainly review some results from in [4, 5, 14, 15]. Other zero-knowledge proofs of knowledge based on discrete logarithm are referred in [7]-[13],

2.2.1 proving that a discrete logarithm lies in a given range

A statistical zero-knowledge protocol proving that a discrete logarithm lies in a given range in [14, 15] was proposed. The protocol is denoted by

$$PK\{(\alpha) : y = g^{\alpha} \wedge -2^{\ddot{l}} < x < 2^{\ddot{l}}\}.$$

In [5], a statistical zero-knowledge protocol for proving $x \in [a, b]$ was proposed, which is denoted $PK\{(\alpha, \beta) : c_x = g^{\alpha}h^{\beta} \wedge \alpha \in [a, b])\}$.

2.2.2 Proving in statistical zero-knowledge that $a+b \equiv d(mod\ n)$, $ab \equiv d(mod\ n)$ and $a^b \equiv d(mod\ n)$ hold

Let l be an integer such that $-2^l < a, b, d, n < 2^l$ holds and $\varepsilon > 1$ be security parameters. Furthermore, we assume that a group G of order $q > 2^{2\varepsilon l+5} (= 2^{2\ddot{l}+1})$ and two generators g and h are available such that $log_g h$ is not known. This group could for instance be chosen by the prover in which case she would have to prove that she has chosen it correctly. Finally, let the prover's commitments to a, b, d and n be $c_a := g^a h^{r_1}, c_b := g^b h^{r_2}, c_d := g^d h^{r_3}$, and $c_n := g^n h^{r_4}$, where r_1, r_2, r_3, and r_4 are randomly chosen elements of Z_q.

Camenisch and Michels([4]) assume that the verifier has already obtained the commitments c_a, c_b, c_d, and c_n. Then the prover can convince the verifier that $a + b \equiv d(mod\ n)$ holds by running the protocol denoted:

$$\begin{aligned} S_+ := PK\{&(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \vartheta, \varrho, \lambda) : \\ &c_a = g^{\alpha}h^{\beta} \wedge -2^{\ddot{l}} < \alpha < 2^{\ddot{l}} \wedge c_b = g^{\gamma}h^{\delta} \wedge -2^{\ddot{l}} < \gamma < 2^{\ddot{l}} \wedge \\ &c_d = g^{\varepsilon}h^{\zeta} \wedge -2^{\ddot{l}} < \varepsilon < 2^{\ddot{l}} \wedge c_n = g^{\eta}h^{\vartheta} \wedge -2^{\ddot{l}} < \eta < 2^{\ddot{l}} \wedge \\ &\frac{c_d}{c_a c_b} = c_n^{\varrho}h^{\lambda} \wedge -2^{\ddot{l}} < \varrho < 2^{\ddot{l}}\} \end{aligned}$$

Alternatively, she can convince the verifier that $ab \equiv d(mod\ n)$ holds by running the protocol:

$$\begin{aligned} S_* := PK\{&(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \vartheta, \xi, \rho, \sigma) : \\ &c_a = g^{\alpha}h^{\beta} \wedge -2^{\ddot{l}} < \alpha < 2^{\ddot{l}} \wedge c_b = g^{\gamma}h^{\delta} \wedge -2^{\ddot{l}} < \gamma < 2^{\ddot{l}} \wedge \\ &c_d = g^{\varepsilon}h^{\zeta} \wedge -2^{\ddot{l}} < \varepsilon < 2^{\ddot{l}} \wedge c_n = g^{\eta}h^{\vartheta} \wedge -2^{\ddot{l}} < \eta < 2^{\ddot{l}} \wedge \\ &c_d = c_b^{\alpha}c_n^{\rho}h^{\sigma} \wedge -2^{\ddot{l}} < \rho < 2^{\ddot{l}}\}. \end{aligned}$$

At the same time, they presented a protocol in which the prover can convince the verifier that $a^b \equiv d(mod\ n)$ holds for the committed integers without revealing any further information. The protocol is denoted by S_{exp} and its detail content is referred in [4].In the following, when denoting a protocol, we will abbreviate the protocol S_{exp} by a clause like to the statement that is proven and assume that the prover send the verifier all necessary

commitments; e.g.,

$$PK\{(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta,\theta,\kappa) : c_a = g^\alpha h^\beta \wedge c_b = g^\gamma h^\delta \wedge c_d = g^\varepsilon h^\zeta \wedge$$

$$c_n = g^\theta h^\kappa \wedge (\alpha^\gamma \equiv \varepsilon (mod\ \theta))\}$$

Theorem 1 *Let a, b, d, and n be integers that are committed to by the prover as described above, Then All three Potocols S_+, S_*, and S_{exp} are statistical zero-knowledge proofs that $a + b \equiv d (mod\ n)$, $ab \equiv d (mod\ n)$ and $a^b \equiv d (mod\ n)$ hold, respectively.*

2.2.3 proving the pseudo-primality of a committed number

In [4], J.Camenish and M.Michels show how the prover and the verifier can do Lehmann's primality test[1] for a number committed by prover such that the verifier is convinced that the test was correctly done but does not learn any other information. The general idea is that the prover commits to s random bases a_i and then prove that for these bases $a_i^{(m-1)/2} \equiv \pm 1 (mod\ m)$ holds. Furthermore, the prover must commit to a base, say $\tilde{a}$, such that $\tilde{a}^{(m-1)/2} \equiv -1 (mod\ m)$ holds to satisfy the second condition in Lehmann's primality test. We call this protocol S_{prime} which is described in [4]. In the following section, $PK\{(\alpha,\beta) : c_a = g^\alpha h^\beta \wedge \alpha \in \{prime\}\}$ denotes proving that an integer a is a prime by S_{prime}.

Theorem 2 *Given a commitment c_m to an integer, the protocol S_{prime} is a statistical zero-knowledge proof that the committed integer is a prime with error-probability at most 2^{-s} for the primality-test.*

All described protocols can be combined in natural ways. First of all, one can use multiple bases instead of a single one in any of the above proofs. Then, executing any number of instances of these protocols in parallel and choosing the same challenges for all of them in each round corresponding to the $\wedge$-composition of the statements the single protocols prove.

[1] An odd integer $m > 1$ is *prime* if and only if

$$\forall a \in Z_m^* : \ a^{(m-1)/2} \equiv \pm 1\ (mod\ m)\ and\ \exists a \in Z_m^* : \ a^{(m-1)/2} \equiv -1\ (mod\ m).$$

3 The statistical zero-knowledge proof for $a+b=d$, $ab=d$, and $d=a^b$

In [4], Camenisch and Michels obtained the statistical zero-knowledge proofs for $a+b \equiv d(mod\ n)$, $ab \equiv d(mod\ n)$, and $a^b \equiv d(mod\ n)$, however, the verifier gets only commitments to some integers without obtaining any further information in these protocols. Now, we will generalize their results and construct the statistical zero-knowledge proof for $a+b=d$, $ab=d$, and $d=a^b$, furthermore, the verifier also obtains nothing information except commitments to some integers.

Assume l, q and commitment scheme be uniform in 2.2.2, and the verifier gets commitments c_a, c_b, c_d to a, b, d, respectively. Then, in the following two protocols S'_+ and S'_* the prover can convince the verifier that $a+b=d$ and $ab=d$ hold.

$$
\begin{aligned}
S'_+ := PK\{(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta,\lambda) :\ & \\
& c_a = g^\alpha h^\beta \wedge -2^{\ddot{l}} < \alpha < 2^{\ddot{l}} \wedge \\
& c_b = g^\gamma h^\delta \wedge -2^{\ddot{l}} < \gamma < 2^{\ddot{l}} \wedge \\
& c_d = g^\varepsilon h^\zeta \wedge -2^{\ddot{l}} < \varepsilon < 2^{\ddot{l}} \wedge \\
& \tfrac{c_d}{c_a c_b} = h^\lambda\}
\end{aligned}
$$

$$
\begin{aligned}
S'_* := PK\{(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta,\sigma) :\ & \\
& c_a = g^\alpha h^\beta \wedge -2^{\ddot{l}} < \alpha < 2^{\ddot{l}} \wedge \\
& c_b = g^\gamma h^\delta \wedge -2^{\ddot{l}} < \gamma < 2^{\ddot{l}} \wedge \\
& c_d = g^\varepsilon h^\zeta \wedge -2^{\ddot{l}} < \varepsilon < 2^{\ddot{l}} \wedge \\
& c_d = c_b^\alpha h^\sigma\}
\end{aligned}
$$

The following protocol S'_{exp} will guarantee that the prover convinces the verifier that $a^b = d$ holds.

$$
\begin{aligned}
S'_{exp} := PK\{(\alpha,\beta,\xi,\chi,\gamma,\delta,\eta,(\lambda_i,\mu_i,\xi_i,\sigma_i,\tau_i,\vartheta_i,\psi_i)_{i=1}^{l_b-1},(\omega_i,\rho_i)_{i=1}^{l_b-2},) :\ & \\
c_a = g^\alpha h^\beta \wedge -2^{\ddot{l}} < \alpha < 2^{\ddot{l}} \wedge & \\
c_d = g^\gamma h^\delta \wedge -2^{\ddot{l}} < \gamma < 2^{\ddot{l}} \wedge & \\
(\textstyle\prod_{i=0}^{l_b-1} c_{b_i}^{2^i})/c_b = h^\eta \wedge & \\
c_{v_1} = g^{\lambda_1} h^{\mu_1} \wedge \ldots \wedge c_{v_{l_b-1}} = g^{\lambda_{l_b-1}} h^{\mu_{l_b-1}} \wedge & \\
c_{v_1} = c_a^\alpha h^{\xi_1} \wedge c_{v_2} = c_{v_1}^{\lambda_1} h^{\xi_2} \wedge \ldots \wedge c_{v_{l_b-1}} = c_{\nu_{l_b-2}}^{\lambda_{l_b-2}} h^{\xi_{l_b-1}} \wedge & \\
-2^{\ddot{l}} < \lambda_1 < 2^{\ddot{l}} \wedge \ldots \wedge -2^{\ddot{l}} < \lambda_{l_b-1} < 2^{\ddot{l}} \wedge & \\
c_{\mu_1} = g^{\omega_1} h^{\rho_1} \wedge \ldots \wedge c_{\mu_{l_b-2}} = g^{\omega_{l_b-2}} h^{\rho_{l_b-2}} \wedge & \\
-2^{\ddot{l}} < \omega_1 < 2^{\ddot{l}} \wedge \ldots \wedge -2^{\ddot{l}} < \omega_{l_b-2} < 2^{\ddot{l}} \wedge & \\
((c_{b_0} = h^{\sigma_0} \wedge c_{\mu_0}/g = h^{\tau_0}) \vee (c_{b_0}/g = h^{\vartheta_0} \wedge c_{\mu_0}/c_a = h^{\psi_0})) \wedge & \\
((c_{b_1} = h^{\sigma_1} \wedge c_{\mu_1}/c_{\mu_0} = h^{\tau_1}) \vee & \\
(c_{b_1}/g = h^{\vartheta_1} \wedge c_{\mu_1} = c_{\mu_0}^{\lambda_1} h^{\psi_1})) \wedge \ldots \wedge &
\end{aligned}
$$

$$((c_{b_{l_b-2}} = h^{\sigma_{l_b-2}} \wedge c_{\mu_{l_b-2}}/c_{\mu_{l_b-3}} = h^{\tau_{l_b-2}}) \vee$$
$$(c_{b_{l_b-2}}/g = h^{\vartheta_{l_b-2}} \wedge c_{\mu_{l_b-2}} = c_{\mu_{l_b-3}}^{\lambda_{l_b-2}} h^{\psi_{l_b-2}})) \wedge$$
$$((c_{b_{l_b-1}} = h^{\sigma_{l_b-1}} \wedge c_d/c_{\mu_{l_b-2}} = h^{\tau_{l_b-1}}) \vee$$
$$(c_{b_{l_b-1}}/g = h^{\vartheta_{l_b-1}} \wedge c_d = c_{\mu_{l_b-2}}^{\lambda_{l_b-1}} h^{\psi_{l_b-1}}))\}$$

Theorem 3 *Let a, b, and d be integers that are committed to by the prover as described above, Then All three Protocols S'_+, S'_*, and S'_{exp} are statistical zero-knowledge proofs that $a+b=d$, $ab=d=$ and $a^b=d$ hold, respectively.*

Proof: We explain mainly this reason that $a+b=d$ holds, however, the proofs of $ab=d$ and $a^b=d$ are omitted.

The statistical zero-knowledge claims follows from the statistical zero-knowledgeness of the building blocks.

Running the prover with this protocol and using standard techniques, the knowledge extractor can compute integers $\hat{a}, \hat{b}, \hat{d}, \hat{r_1}, \hat{r_2}, \hat{r_3}$ such that $c_a = g^{\hat{a}} h^{\hat{r_1}}$, $c_b = g^{\hat{b}} h^{\hat{r_2}}$, and $c_d = g^{\hat{d}} h^{\hat{r_3}}$ hold. Moreover, $-2^{\ddot{l}} < \hat{a} < 2^{\ddot{l}}$, $-2^{\ddot{l}} < \hat{b} < 2^{\ddot{l}}$, and $-2^{\ddot{l}} < \hat{d} < 2^{\ddot{l}}$, hold for these integers.

When running the prover with S'_+, the knowledge extractor can further compute integers $\hat{r_4} \in Z_q$ such that $c_d/(c_a c_b) = h^{\hat{r_4}}$ holds.

Therefore we have $g^{\hat{d}-\hat{a}-\hat{b}} h^{\hat{r_3}-\hat{r_1}-\hat{r_2}} = h^{\hat{r_5}}$ and hence, provided that the discrete log of h to the base g is not known, we must have

$$\hat{d} \equiv \hat{a} + \hat{b} (mod\ q).$$

Thus we have $\hat{d} = \hat{a} + \hat{b} + \bar{w}q$ for some integer $\bar{w}$. Since $2^{2\ddot{l}+1} < q$ and due to the constraints on $\hat{a}, \hat{b}, \hat{d}$ we can conclude that the integer $\bar{w}$ must be 0 and hence

$$\hat{d} = \hat{a} + \hat{b}$$

must hold. ∎

In the following, when denoting a protocol, we will abbreviate the protocol S'_{exp} by a clause like to the statement that is proven and assume that the prover send the verifier all necessary commitments; e.g.,

$$PK\{(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta) : c_a = g^{\alpha} h^{\beta} \wedge c_b = g^{\gamma} h^{\delta} \wedge c_d = g^{\varepsilon} h^{\zeta} \wedge (\alpha^{\gamma} = \varepsilon)\}$$

Remarks: By using protocol S'_+, S'_*, we can construct a statistical zero-knowledge proof proving that a committed integer a is either odd or even.

4 Proving that two committed integers are equal

Assume c_a and c_b are commitments to integers a and b, and the verifier has obtained these commitments before the protocol beginning. A protocol, in which the prover convinces the verifier that $a = b$ holds, will be proposed in this section, and it is denoted by $S_=$.

$$S_= : PK\{(\alpha, \beta, \gamma, \delta, \lambda) :$$
$$c_a = g^\alpha h^\beta \wedge -2^{\ddot{l}} < \alpha < 2^{\ddot{l}} \wedge \quad (1)$$
$$c_b = g^\gamma h^\delta \wedge -2^{\ddot{l}} < \gamma < 2^{\ddot{l}} \wedge \quad (2)$$
$$\frac{c_a}{c_b} = h^\lambda\} \quad (3)$$

Theorem 4 *If c_a and c_b are commitments to integers a and b as described above, the protocol $S_=$ is a statistical zero-knowledge proof that $a = b$ holds.*

Proof: The statistical zero-knowledge claims follows from the statistical zero-knowledgeness of commitment scheme.

Running the prover with this protocol and using standard techniques, the knowledge extractor can compute integers $\hat{a}, \hat{b}, \hat{r_1}, \hat{r_2}$ such that $c_a = g^{\hat{a}} h^{\hat{r_1}}$ and $c_b = g^{\hat{b}} h^{\hat{r_2}}$, hold. Moreover, $-2^{\ddot{l}} < \hat{a} < 2^{\ddot{l}}$, and $-2^{\ddot{l}} < \hat{b} < 2^{\ddot{l}}$ hold for these integers.

When running the prover with $S_=$, the knowledge extractor can further compute integers $\hat{r_3} \in Z_q$ such that $c_a/c_b = h^{\hat{r_3}}$ holds.

Therefore we have $g^{\hat{a}-\hat{b}} h^{\hat{r_1}-\hat{r_2}} = h^{\hat{r_3}}$ and hence, provided that the discrete log of h to the base g is not known, we must have

$$\hat{a} \equiv \hat{b} (mod\ q).$$

Thus we have $\hat{a} = \hat{b} + \bar{w}q$ for some integer $\bar{w}$. Since $2^{2\ddot{l}+1} < q$ and due to the constraints on $\hat{a}, \hat{b}$ we can conclude that the integer $\bar{w}$ must be 0 and hence

$$\hat{a} = \hat{b}$$

must hold. ∎

Assume an integer a is known, the following protocol $S'_=$ is a statistical zero-knowledge proof that the committed integer b is equal to a.

$$S'_= := PK\{(\alpha, \beta, \lambda) :$$
$$c_b = g^\alpha h^\beta \wedge -2^{\ddot{l}} < \alpha < 2^{\ddot{l}} \wedge \quad (4)$$
$$\frac{c_b}{g^a} = h^\lambda\} \quad (5)$$

5 Proving that a committed integer is not equal to 0

In this section, we will present a protocol by which the prover can convince the verifier that an integer a is not 0, furthermore, it is statistical zero-knowledge.

For an arbitrary integer a, it can be written $\prod_{i=1}^{i=t} p_i^{k_i}$, where $p_1, ..., p_r$ are primes and $k_1, ..., k_r$ are integers. Now, if the prover can prove that a has form $\prod_{i=1}^{r} p_i^{k_i}$ and all $p_1, ..., p_r$ are primes, then $a \neq 0$ holds.

Assume l, q and commitment scheme be set in 2.2.2, and let prover's commitments to $a, s_1 = p_1^{k_1}, ..., s_r = p_r^{k_r}, p_1, ..., p_r, k_1, ..., k_r$, and suppose the verifier has already obtained all commitments before the protocol begins. The following protocol will prove that the integer a is not 0.

$S_{a\neq 0} := PK\{(\alpha, \beta, \rho, (\delta_i, \varepsilon_i, \zeta_i, \eta_i, \theta_i, \mu_i)_{i=1}^{i=r}) :$

$$c_a = g^{\alpha} h^{\beta} \wedge -2^{\ddot{l}} < \alpha < 2^{\ddot{l}} \wedge \tag{6}$$

$$c_{s_1} = g^{\delta_1} h^{\varepsilon_1} \wedge ... \wedge c_{s_r} = g^{\delta_r} h^{\varepsilon_r} \wedge \tag{7}$$

$$(-2^{\ddot{l}} < \delta_1 < 2^{\ddot{l}}) \wedge ... \wedge (-2^{\ddot{l}} < \delta_r < 2^{\ddot{l}}) \wedge \tag{8}$$

$$c_a / c_{s_1} ... c_{s_r} = h^{\rho} \wedge \tag{9}$$

$$c_{p_1} = g^{\zeta_1} h^{\eta_1} \wedge ... \wedge c_{p_r} = g^{\zeta_r} h^{\eta_r} \wedge \tag{10}$$

$$(-2^{\ddot{l}} < \zeta_1 < 2^{\ddot{l}}) \wedge ... \wedge (-2^{\ddot{l}} < \zeta_r < 2^{\ddot{l}}) \wedge \tag{11}$$

$$c_{k_1} = g^{\theta_1} h^{\mu_1} \wedge ... \wedge c_{k_r} = g^{\theta_r} h^{\mu_r} \wedge \tag{12}$$

$$(-2^{\ddot{l}} < \theta_1 < 2^{\ddot{l}}) \wedge ... \wedge (-2^{\ddot{l}} < \theta_r < 2^{\ddot{l}}) \wedge \tag{13}$$

$$(\delta_1 = \zeta_1^{\theta_1}) \wedge ... \wedge (\delta_r = \zeta_r^{\theta_r}) \wedge \tag{14}$$

$$\zeta_1 \in \{prime\} \wedge ... \wedge \zeta_r \in \{prime\}\} \tag{15}$$

Theorem 5 *Let a be an integer that is committed by c_a. Then $S_{a\neq 0}$ is a statistical zero-knowledge proof that $a \neq 0$ holds.*

Proof: *Completeness:* If $a \neq 0$, the prover can prove that $a = \prod_{i=1}^{r} p_i^{k_i}$ holds in (6)-(14); in (15), the prover proves that all of $p_1, ..., p_r$ are prime numbers. As a result, the verifier believes that $a \neq 0$ holds .

Soundness: If $a = 0$, the prover may prove that a is a composite integer in (6)-(14); however, she can not prove that each of $p_1, ..., p_r$ is prime; so, the verifier rejects.

Zero-knowledgeness: $S_{a\neq 0}$ is statistical zero-knowledge from Theorem 2, 3 and 4. ∎

6 Proving a polynomial $f(x)$ with degree $t-1$ exactly

Assume $c_b = (c_{b_0}, c_{b_1}, ..., c_{b_m})$ and $c_a = (c_{a_0}, c_{a_1}, ..., c_{a_m})$ are commitments to all exponents of x and all coefficients, respectively, in polynomial $f(x)$, furthermore, we assume that the i-th term is $a_i x^{b_i}$, that is, $f(x) = a_0 x^{b_0} + a_1 x^{b_1} + ... + a_m x^{b_m}$. If all above commitments satisfy the following: 1) there exists a committed integer b_j is equal to $t-1$; 2) other all committed integers $b_i \in [0, t-2]$, where $i \neq j$; 3) $a_j \neq 0$ holds, then the degree of the polynomial $f(x)$ is $t-1$ exactly. In total subsection, we assume arbitrary two committed integers b_i and b_k is not equal, where $i \neq k$ and $m \leq r$.

Protcol 1

1. the prover chooses randomly a permutation π, obtains two vectors $c_{a'} = \pi c_a = (c_{a'_0}, c_{a'_1}, ..., c_{a'_m})$ and $c_{b'} = \pi c_b = (c_{b'_0}, c_{b'_1}, ..., c_{b'_m})$, and sends $c_{a'}$ and $c_{b'}$ to the verifier.

2. The prover proves to the verifier that a committed integer $b'_j = t-1$ holds by $S'_{=}$.

3. The prover proves to the verifier that the committed integer $a'_j \neq 0$ holds by $S_{a \neq 0}$.

4. The prover proves to the verifier that all committed integer $b'_i \in [0, t-2]$, where $i \neq j$, i.e.,
   $PK : \{((\alpha_i, \beta_i)_{i=0, i\neq j}^{m}) : c_{b'_0} = g^{\alpha_0} h^{\beta_0} \wedge \alpha_0 \in [0, t-2] \wedge ... \wedge c_{b'_{j-1}} = g^{\alpha_{j-1}} h^{\beta_{j-1}} \wedge \alpha_{j-1} \in [0, t-2] \wedge c_{b'_{j+1}} = g^{\alpha_{j+1}} h^{\beta_{j+1}} \wedge \alpha_{j+1} \in [0, t-2] \wedge ... \wedge c_{b'_m} = g^{\alpha_m} h^{\beta_m} \wedge \alpha_m \in [0, t-2]\}$.

5. The prover obtains the primitive c_a and c_b by $c_a = c'_a \pi^-$ and $c_b = c'_b \pi^-$.

Theorem 6 *Let $c_b = \{c_{b_0}, c_{b_1}, ..., c_{b_m}\}$ and $c_a = \{c_{a_0}, c_{a_1}, ..., c_{a_m}\}$ are commitments to all exponents of x and all coefficients, respectively, in polynomial $f(x)$, then the Protocol 1 is a statistical zero-knowledge proof that the degree of the polynomial $f(x)$ is $t-1$ exactly.*

Proof: 1) *Completeness:* If $f(x) = \sum_{i=0}^{m} a_i x^{b_i}$ is a polynomial with degree $t-1$ exactly, then, in the above protocol the prover can convince the verifier the polynomial with degree $t-1$ exactly. In particular, the verifier does not know j, which satisfies $b_j = t-1$, because we rearrange the c_a and c_b by a random permutation π in the first step in *protocol* 1.

2)*Soundness:* If $f(x)$ is not a polynomial with degree $t-1$ exactly, there exist three cases: 1) if there is not a committed $b_j = t-1$, the second step is wrong; 2) if there is a $b_j = t-1$, however, $a_j = 0$ holds, the third step is wrong; 3) if $b_j = t-1$ and $a_j \neq 0$ hold, but there exists a committed b_k not in $[0, t-2]$, then fourth step is wrong. So, if $f(x)$ is not a polynomial with degree $t-1$ exactly, the prover can convince the verifier the polynomial with degree $t-1$ exactly with negligible probability.

3) *Zero-knowledge:* By theorem 2, 3, and 4, we know that our protocol satisfies statistical zero-knowledge.

References

[1] D.R. Stinson, Cryptography: Theory and Practice. CRC Press, London. 1996

[2] J.C.Benaloh, Secret Sharing Homomorphisms: Keeping Shares of a Secret. *Proc of CRYPTO'86*, Berlin: Springer, 1986.

[3] L.Xishong, H.Liang, and Z.Zhencheng, Computer Cryptography and Its Applications, *Industry Publish of National Defence*, Beijing, 2001.

[4] J.Camenisch, M.Michels, Proving in Zero-knowledge that a Number is the Product of Two Safe Primes. *Advances in Cryptology-EUROCRYPT'99*, pp 106-121, Berlin: Springer, 1999.

[5] F.Boudot, Efficient Proofs that a Committed Number Lies in an Interval. *Advances in Cryptology-EUROCRYPT'00*, pp 431-444, Berlin: Springer, 2000.

[6] T.P.Pedersen, Non-interactive and information-theoretic secu5re verifiable secret sharing. *Advances in Cryptology-CRYPTO'91*, pp 129-140, Berlin: Springer, 1991.

[7] D.Chaum, J.H.Evertse, and J.van de Graaf, and R.Peralta, Demonstrating possession of a discrete logarithm without revealing it. *Advances in Cryptology-CRYPTO'86*, pp 200-212, Berlin: Springer, 1987.

[8] C.P.Schnorr, Efficient signature generation for smart cards. *J of Cryptology*, 4(3):239-252, Berlin: Springer, 1991.

[9] J.Camenisch, and M.Stadler, Efficient group signature schemes for large groups. *Advances in Cryptology-CRYPTO'97*, pp 410-424, Berlin: Springer, 1997.

[10] S.Brands, Electronic cash systems based on the representation problem in groups of prime order, *Advances in Cryptology-CRYPTO'93*, pp 1-15, Berlin: Springer, 1993.

[11] D.Chaum, J.E.Evertse, and J.van de Graaf, An improved protocol for demonstrating possession of discrete logarithms and some generalizations, *Advances in Cryptology-EUROCRYPT'87*, pp 127-141, Berlin: Springer, 1988.

[12] D.Chaum, and T.P.Pedersen, Wallet databases with observers, *Advances in Cryptology-CRYPTO'92*, pp 89-105, Berlin: Springer, 1993.

[13] R.Cramer, I.Damgard, and B.Schoenmakers, Proofs of partial knowledge and simplified design of witness hiding protocols, *Advances in Cryptology-CRYPTO'94*, pp 174-187, Berlin: Springer, 1994.

[14] E.Fujisaki, and T.Okamoto, Statistical zero-knowledge protocols to prove modular polynomial relations. *Advances in Cryptology-CRYPTO'97*, pp 16-30, Berlin: Springer, 1997.

[15] A.Chan, Y.Frankel, and Y.Tsiounis, Easy come-easy go divisible cash. *Advances in Cryptology-EUROCRYPT'98*, pp 561-575, Berlin: Springer, 1998.