

Cryptographic Protocols

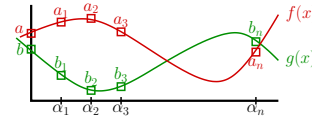
Spring 2018

Part 7

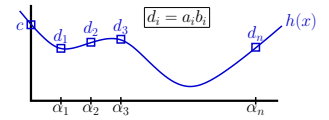
Generic Commitment Multiplication Protocol

0. **Starting point:** D is committed to a, b, c by \boxed{a} , \boxed{b} , and \boxed{c} .

1. **CSP of a, b with degree t**
 $\Rightarrow f(x), g(x)$



2. **CSP of c with degree $2t$**
 use $h(x) = f(x)g(x)$



3. **Checks**

$\forall P_i: d_i \stackrel{?}{=} a_i b_i$, broadcast accusation bit.

On accusation: Open $\boxed{a_i}$, $\boxed{b_i}$, $\boxed{d_i}$, check $a_i b_i \stackrel{?}{=} d_i$.

Commit State

Open Protocol

1. **Open**

D broadcasts $g(x)$.

2. **Check consistency**

P_i accuses dealer if $g(\alpha_i) \neq s_i$.

3. **Compute secret**

If $\leq t$ accusations: $s = g(0)$.

If $> t$ accusations: disqualify dealer.

Proof:

Facts about two-dimensional polynomials (1/3)

Given: $f(x, y) = f_{00} + f_{10}x + f_{01}y + f_{11}xy + \dots + f_{tt}x^t y^t \in \mathbb{F}[x, y]$

Fact 1: $f_{y_0}(x) := f(x, y_0)$ is a one-dimensional polynomial of degree t .

Proof: $f(x, y_0) = (f_{00} + f_{01}y_0 + \dots + f_{0t}y_0^t)$
 $+ (f_{10} + f_{11}y_0 + \dots + f_{1t}y_0^t)x$
 $+ \dots$
 $+ (f_{t0} + f_{t1}y_0 + \dots + f_{tt}y_0^t)x^t$

Facts about two-dimensional polynomials (2/3)

Given: $f(x, y) = f_{00} + f_{10}x + f_{01}y + f_{11}xy + \dots + f_{tt}x^t y^t \in \mathbb{F}[x, y]$

Fact 2: Let $X = \{x_1, \dots, x_{t+1}\}$ and $Y = \{y_1, \dots, y_{t+1}\}$. Then $f(x, y)$ is uniquely defined by $W := \{(x_i, y_j, z_{ij}) \mid (x_i, y_j) \in X \times Y\}$.

Proof (existence): $\exists \geq 1$ such $f(x, y)$: **Lagrange-Interpolation**

Find $L_{ij}(x, y)$ with $\begin{cases} L_{ij}(x_i, y_j) = 1 \\ L_{ij}(x_{i'}, y_{j'}) = 0 \text{ for } (i', j') \neq (i, j) \end{cases}$

$$\Rightarrow L_{ij}(x, y) := \prod_{\substack{i'=1 \\ i' \neq i}}^{t+1} \frac{x - x_{i'}}{x_i - x_{i'}} \prod_{\substack{j'=1 \\ j' \neq j}}^{t+1} \frac{y - y_{j'}}{y_j - y_{j'}}$$

and define

$$f(x, y) := \sum_{i,j=1}^{t+1} L_{ij}(x, y) z_{ij}.$$

Facts about two-dimensional polynomials (3/3)

Given: $f(x, y) = f_{00} + f_{10}x + f_{01}y + f_{11}xy + \dots + f_{tt}x^t y^t \in \mathbb{F}[x, y]$

Fact 2: Let $X = \{x_1, \dots, x_{t+1}\}$ and $Y = \{y_1, \dots, y_{t+1}\}$. Then $f(x, y)$ is uniquely defined by $W := \{(x_i, y_j, z_{ij}) \mid (x_i, y_j) \in X \times Y\}$.

Proof (uniqueness): $\exists \leq 1$ such $f(x, y)$

1. Let $f_1(x, y)$ and $f_2(x, y)$ degree- t -polynomials through W .
2. $f_\Delta(x, y) := f_1(x, y) - f_2(x, y)$ is a degree- t -polynomial.
3. $\forall (x_i, y_j) \in X \times Y : f_\Delta(x_i, y_j) = 0$.
4. $\forall y_j \in Y : f_{y_j}(x) := f_\Delta(x, y_j)$ is a polynomial of degree t (Fact 1).
5. $\forall y_j \in Y : f_{y_j}(x_1) = f_{y_j}(x_2) = \dots = f_{y_j}(x_{t+1}) = 0$; thus $f_{y_j} \equiv 0$.
6. Thus: $\forall (x, y_j) \in \mathbb{F} \times Y : f_\Delta(x, y_j) = 0$.
7. $\forall x \in \mathbb{F} : f_x(y) := f_\Delta(x, y)$ is a polynomial of degree t (Fact 1).
8. $\forall x \in \mathbb{F} : f_x(y_1) = f_x(y_2) = \dots = f_x(y_{t+1}) = 0$; thus $f_x \equiv 0$.
9. Thus: $\forall (x, y) \in \mathbb{F} \times \mathbb{F} : f_\Delta(x, y) = 0$; thus $f_\Delta \equiv 0$.

Commit Protocol

1. Distribution

D selects random polynomial

$$f(x, y) = \sum_{i=0}^t \sum_{j=0}^t f_{ij} x^i y^j, \text{ with } f_{0,0} = s,$$

and sends $h_i(x) = f(x, \alpha_i)$, $k_i(y) = f(\alpha_i, y)$ to P_i .

2. Consistency checks

$\forall P_i, P_j$: P_i sends $k_i(\alpha_j)$ to P_j , P_j complains if $k_i(\alpha_j) \neq h_j(\alpha_i)$.
 D broadcasts $f(\alpha_i, \alpha_j)$.

3. Accusation

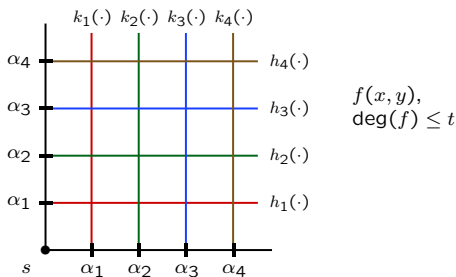
$\forall P_i$: if P_i has received contradicting values from D : **accuse** D .
 D broadcasts $h_i(x)$ and $k_i(y)$.

Repeat until no further accusation.

4. Compute share

If $> t$ accusing players: disqualify dealer.
If $\leq t$ accusing players: $s_i = k_i(0)$.

Commit Protocol



MPC Operations: Overview

	Passive	Active (commitment scheme)	Crypt. (normal commitments)	Inf.-Theo. (distributed commitments)
Input	Shamir sharing	+commit/CTP		
Add	linearity	+homomorph		
Mult.	mult.prot. $[n/2]$	+CMP/CTP	$B^a \sim C$	generic $[n/3]$
Output	interpolate	+CTP		$[n/3]$