Composing ZK Proofs

Tuesday, September 17, 2019 10:59 AM

Goals for today: construct proofs for specifications like:

ex1: $ZK\,PoK\{(a,b,c): A=g^a \; B=g^b \; C=g^c \text{ and } c=ab+5\}$

ex2: $ZK\,PoK\{(x): A=g^x \text{ OR } B=g^x\}$

But first: Commitments!

Strawman 1: Why not g^{x+r}?

$X = g^{x+\text{blinding factor}}$

Recall Rock-paper-scissors from Day 2:

Alice: m_1 = "rock" → $h(m_1)$ → piazza

Bob: m_2 = "paper"

commitment $h(m_1 \,\|\, \text{long random string})$

Alice: $X = g^{x+r}$ ← random 256-bit number; $0,1,2 \rightarrow$

↳ publish piazza

Bob: Y ←

reveal x, r

$x' = x+1$

$r' = r-1$

y, r'

So, g^{x+r} is not "binding"

Solution: Pedersen Commitment

$g^x \cdot h^r$ must be $h = g^\gamma$ for some γ

two different random generators

Defn: a commit scheme is a tuple (setup, com, open)

Syntax:

- public parameters $pp \leftarrow Setup(1^\lambda)$
- $C \leftarrow com_r(X)$ (message X; random blinding factor r; pp implicit)
- $\{0,1\} \leftarrow open(C, r, X)$

Security properties:

- Correctness: $\forall X, P_r\left[\begin{matrix} pp \leftarrow Setup(1^\lambda),\ r \xleftarrow{\$} \mathbb{Z}_p \\ C \leftarrow com_r(X), \end{matrix} : open(C,r,X)\right] = 1$
- Hiding: $\forall X, Y, pp, \quad \{r \xleftarrow{\$} \mathbb{Z}_p : C \leftarrow com_r(X)\} = \{r' \xleftarrow{\$} \mathbb{Z}_p : C' \leftarrow com_r(Y)\}$

- binding $\forall A, \Pr\left[\begin{array}{l} pp \leftarrow setup(1^\lambda) \\ (C, x, y, r, r') \leftarrow A(1^\lambda, pp) : \\ x \neq y, \ open(C, r, x) = 1 \\ \text{and } open(C, r', y) = 1 \end{array}\right] \leq negl(\lambda)$

Pedersen commitment: (instantiates commitment def'n above)

$setup(1^\lambda)$: $\{G_\lambda\}$ ← family of DLog, prime order

$pp = (g, h)$ where $g \xleftarrow{\$} G_\lambda$, $h \xleftarrow{\$} G_\lambda$

$Com_r(pp, X)$:
parse pp as (g, h)
$C = g^X h^r$

$Open(C, r, X)$
return 1 if $C \stackrel{?}{=} g^X h^r$

- Correctness ✓
- Hiding $\forall x, y, \{g^x h^r\} = \{g^y h^{r'}\}$ ✓ ($r \xleftarrow{\$} \mathbb{Z}_p$, $r' \xleftarrow{\$} \mathbb{Z}_p$)

↑ Uniform over G.

$|\mathbb{Z}_p| = |G|$,
and $Com_{(\cdot)}(x)$ is surjective

Given x and C, there is some value r such that $C = g^x h^r$

$C / g^x = h^r$

↑ generator

- Binding:

Proof by reduction

Assume we have an A that violates "binding".

Then we can construct A' that breaks discrete log.

- Suppose we have A, such that

binding game → $\Pr\left[\begin{array}{l} (C, r_1, r_2, x_1, x_2) \leftarrow A(g, h) \\ C = g^{x_1} h^{r_1} = g^{x_2} h^{r_2}, \ x_1 \neq x_2 \end{array}\right] > negl(\lambda)$

Use A to ...

We must construct $\mathcal{A}'$.

$$\Pr\left[b \leftarrow \mathcal{A}'(g, B) : g^b = B\right] > \text{negl}(\lambda)$$

$\mathcal{A}'(g, B)$:

$(C, r_1, r_2, x_1, x_2) \leftarrow \mathcal{A}(g, h = B)$

s.t. $C = g^{x_1} B^{r_1} = g^{x_2} B^{r_2}$ $> \text{negl}(\lambda)$

return $g^{r_1} \neq B$

$x_1 + b r_1 = x_2 + b r_2$

$(x_1 - x_2) = b(r_2 - r_1)$ ✓

$\left(\frac{x_1 - x_2}{r_2 - r_1}\right)$

ZK PoK $\{(x, r) : C = g^x h^r\}$

prove "I know the opening of C"

$P(x, r)$ $\qquad$ $V(C)$

$k_x \xleftarrow{\$} \mathbb{Z}_p$

$k_r \xleftarrow{\$} \mathbb{Z}_p$

$K = g^{k_x} h^{k_r}$ $\xrightarrow{K}$ $\xleftarrow{\$}$ $c \leftarrow \mathbb{Z}_p$

$s_x = k_x + cx$

$s_r = k_r + cr$ $\xrightarrow{s_x, s_r}$ $g^{s_x} h^{s_r} = K C^c$

Sanity check: $g^{k_x + cx} h^{k_r + cr} = g^{k_x} h^{k_r} \cdot (g^x h^r)^c$ ✓

$\cdot\, g^{xc} h^{rc}$

Λ ... proofs Prod

Arithmetic [illegible]

$$ZKPK\{(a,b,c,r): A=g^a,\ B=g^b,\ C=g^c h^r\}$$

and $a+b=c$

Approach to do so:

find a equivalent predicate/witness

$C=g^c h^r$ $a+b=c$

$C=g^{a+b}h^r = A\cdot B\cdot h^r$

$Pred(a',b',r') = \{A=g^{a'},\ B=g^{b'},\ C=AB h^{r'}\}$ $\quad C/A/B=h^{r'}$

$\Downarrow$

find a,b,c,r s.t. $Pred(a,b,c,r)=1$

how? $c' := a'+b'$

$a := a'$

$b := b'$

$r := r'$

---

multiplication: $ZKPoK\{(a,b,c): A=g^a,\ B=g^b,\ C=g^c\}$

and $a\cdot b=c$

$C=g^{ab}$

~~$C=g^a+g^b$~~

$ZKPoM(a,b)$: $A=g^a$ $B=g^b$ $C=g^{ab}$

$A=g^a$ $B=g^1$ $C=A^b$

OR proofs: $ZKPoK\{(x): A=g^x \text{ OR } B=g^x\}$

$\Downarrow$

$(w): P_1(w)$ OR $P_2(w)$ generalized

WLOG, s.t. $A=g^x$

sim for $ZK\{(x): B=g^x\}$ $V(A,B)$

$P(x)$

$(K_B, C_B, S_B) \leftarrow Sim_B$ — $C_B \xleftarrow{\$} \mathbb{Z}_q$, $S_B \xleftarrow{\$} \mathbb{Z}_p$, $K_B = g^{S_B} / B^{C_B}$

$k_A \xleftarrow{\$} \mathbb{Z}_p$

$K_A = g^{k_A}$

$K_A, K_B \rightarrow$

$\leftarrow c \xleftarrow{\$} \mathbb{Z}_p \setminus \{0\}$

Solve for C_A s.t. that $C = C_A + C_B$

$S_A = C_A x + k_A$

$S_A, S_B, C_A, C_B \rightarrow$

check $C_A + C_B = C$

$K_A A^{C_A} = g^{S_A}$

$K_B B^{C_B} = g^{S_B}$

- Simulation:
- Extraction: .... Same as for Schnorr

$C_{A_1}, C_{B_1}, S_{A_1}, S_{B_1} \leftarrow A'(c_1)$

$C'_{A_2}, C_{B_2}, S_{A_2}, S_{B_2} \leftarrow A'(c_2)$

Range proof:

$ZK\{(x, r) : C = g^x h^r \text{ and } x \in [0, 2^8)\}$

Idea: make pedersen commitments to binary expansion of x

$x = x_0 + 2x_1 + \dots 128 x_7$ $\quad x_i \in \{0, 1\}$

$C_0 = g^{x_0} h^{r_0}$ $\quad r_0 \xleftarrow{\$} \mathbb{Z}_q$

$\vdots$ $\quad \vdots$

$C_7 = g^{x_7} h^{r_7}$

ephemeral commitments

Prove: ① committed values are bits $C_i = g^0 h^{r_i}$ OR $C_i = g^1 h^{r_i}$

And ② $C = C_0 \cdot C_1^2 \cdot C_2^4 \cdots C_7^{128}$

$g^{x_0} \cdot g^{x_1 \cdot 2^1} \cdots g^{x_7 \cdot 2^7}$ $h^{r - (r_0 + r_1 \cdot 2 + \ldots r_7 \cdot 128)}$