ZK Proofs III

Thursday, September 14, 2017 12:25 PM

Pedersen Commitment:

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

$Com_r(x) := g^x h^r$

g^x

$ZKPoK\{(x,r): C = Com_r(x) \;\&\; X = g^x\} =$

$ZKPoK\{(x,r): C = Com_r(x)\}$

$ZKPoK\{(x,r): C = g^x h^r \;\&\; X = g^x\}$

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

$k_1 \xleftarrow{\$} \mathbb{Z}_p$

$k_2 \xleftarrow{\$} \mathbb{Z}_p$

$K := g^{k_1} h^{k_2}$ $\xrightarrow{K}$ $c \xleftarrow{\$} \mathbb{Z}_p$

$\xleftarrow{c}$

$s_1 := k_1 + cx$

$s_2 := k_2 + cr$ $\xrightarrow{s_1, s_2}$ Verify $g^{s_1} h^{s_2} = K C^c$

- Correctness ("completeness")
- Extractability
- Simulatability.

$g^{s_1} h^{s_2} = g^{k_1 + cx} h^{k_2 + cr}$

$= (g^{k_1} h^{k_2})(g^{cx} h^{cr})$

$= K (g^x h^r)^c = K C^c$

$ZKPoK\{(x): g^x = X \;\&\; X_2 = h^x\}$

$P(x)$:

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

$K_1 = g^k, \; K_2 = h^k$ $\xrightarrow{K}$

...

ZK for arithmetic relations

$$ZKPoK\{(a,b,c,r): \underline{A=g^a},\ \underline{B=g^b},\ \underline{C=g^c h^r} \ \underline{\&\ (c=a+b)}\}$$

rewrite:

$$ZKPoK\{(a,b,r): \underline{A=g^a,\ B=g^b,\ C=(g^{(a+b)})h^r}\}$$

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

$L_1 = L_2$

$x \in L_1$ means $L_1((A,B,C),(a,b,c,r)) = A=g^a,\ B=g^b\ C=g^{(a+b)}h^r$ (L_2 accordingly)

$\exists w$ s.t. $L_1(x,w)=1$

$f(\underline{x,w}) = ((A,B,C),\underline{(a,b,c,r)}) \mapsto ((A,B,C),\underline{(a,b,r)})$

$x \in L_1, \quad f(x) \in L_2$

Multiplication:

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

$$\{(a,b): A=g^a,\ B=g^b,\ C=(\underbrace{A}_{(g^a)})^b\}$$

Diffie-Hellman tuple

(g^a, g^b, g^{ab})

$(g^a)\cdot(g^b) = g^{(a+b)}$

OR proofs:

$$ZKPoK\{(w): \underline{L_1(x,w)} \text{ or } \underline{L_2(x,w)}\}$$

predicate predicate

Ex. $ZKPoK\{(x): A = g^x \text{ or } B = g^x\}$

Idea: Use the simulator for the "false" branch

$P(x)$: $V(A,B)$

Assume $g^x = A$.

simulator for $ZKPoK\{(x): B = g^x\}$

$(K_B, (C_B), S_B) \leftarrow Sim(B)$

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

$K_A := g^{k_A}$ $\xrightarrow{K_A, K_B}$

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

Find c_A s.t.

$c = c_A + c_B$

$S_A := k_A + c_A x$ $\xrightarrow{S_A, S_B, c_A, c_B}$ Verify $c_A + c_B = c$

$K_A A^{c_A} = g^{S_A}$, $K_B B^{c_B} = g^{S_B}$

Proof:

- Simulatable
- Completeness
- extractability

Suppose $\mathcal{A}$

$Pr[Out[\mathcal{A}(A,B,1^\lambda) \leftrightarrow V(A,B,1^\lambda)] = 1] = p_{non\text{-}negl}$

Define $\mathcal{E}_{\mathcal{A}}$:

run $\mathcal{A}$ until it output K_A, K_B.

make a snapshot.

$\$ \mathbb{Z}_p$

Sample $c_1 \xleftarrow{\$} \mathbb{Z}_p$

$c_2 \xleftarrow{\$} \mathbb{Z}_p$

$s_{A,1}, s_{B,1}, c_{A,1}, c_{B,1} \leftarrow A'(c_1)$

$(s_{A,2}), (s_{B,2}), (c_{A,2}), (c_{B,2}) \leftarrow A'(c_2)$

Prob $\approx p^2$ $\quad c_{A,1} + c_{B,1} = c_1$

$c_{A,2} + c_{B,2} = c_2$

$A^{c_{A,1}} K_A = g^{s_{A,1}} \qquad B^{c_{B,1}} K_B = g^{s_{B,1}}$

$A^{c_{A,2}} K_A = g^{s_{A,2}} \qquad B^{c_{B,2}} K_B = g^{s_{B,2}}$

$c_{A,1} \neq c_{A,2}$ or $c_{B,1} \neq c_{B,2}$

Solve $x_A = (s_{A,1} - s_{A,2}) / (c_{A,1} - c_{A,2})$

$x_B = \ldots$

Range Proof:

$$ZK\,PoK\{(X, r) : C = g^X h^r \;\&\; X \in [0, 2^8)\}$$

Idea: Commit binary expansion of X

$$X = X_0 + 2X_1 + 4X_2 \ldots 128X_7$$

$ZK\{($ ~~$X_0 = g^{X_0}, X_1 = g^{X_1}, X_2 = g^{X_2} \ldots$~~

$X = (X_0)(X_1)^2(X_2)^4 \ldots$

↳ $C_0 = g^{X_0} h^{r_0}$ for $r_0 \xleftarrow{\$} \mathbb{Z}_p$

ephemeral commitments $C_1 = g^{X_1} h^{r_1}$ $\quad r_1 \xleftarrow{\$} \mathbb{Z}_p$

$\ldots$

$\ldots X_7 r_7$

$C_7 = g^{\cdots} h^{r}$

Prove: $\exists (X, r, X_0, X_1, \ldots X_7, r_0, r_1, \ldots r_7)$:

~~$C_0 = g^{X_0} h^{r_0}$~~ $C_0 = h^{r_0}$ OR $C_0 = g h^{r_0}$

$\cdots$

$C_7 = g^{X_7} h^{r_7}$ & $X_i \in [0,1]$

$$C = \left(C_0 \cdot C_1^2 \cdot C_2^4 \cdots C_7^{(128)}\right) h^{r - (r_0 + 2r_1 + 4r_2 \ldots 128 r_7)}$$

$$\left(g^{(X_0 + 2X_1 + \ldots 128 X_7)}\right)\left(h^{r_0 + 2r_1 + 4r_2 \ldots 128 r_7}\right)\left(h^{r - (r_0 + \ldots)}\right)$$

$$= g^{(X_0, \ldots)} h^{r}$$

$\{(X, r', \ldots)$: $C / (C_0 C_1^2 C_2^4 \cdots) = h^{r'}\}$

and $C_0 = g h^{r_0}$ or $C_0 = h^{r_0}$

$\cdots$

Variation: Floating representation.

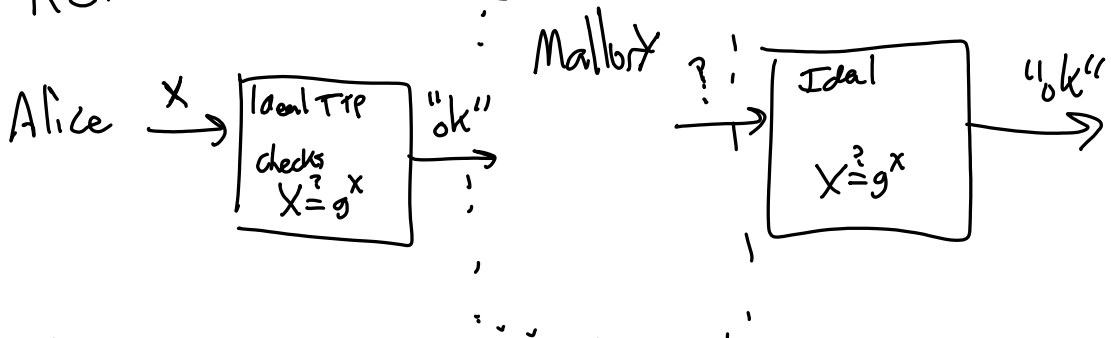
$ZK\{(X, r, a, b) : C = g^X h^r$ & $X = a \cdot 10^b$ eg 1120000

& $a \in [0, 2^8]$

& $b \in [0, 2^8]$

Problem with Composition:

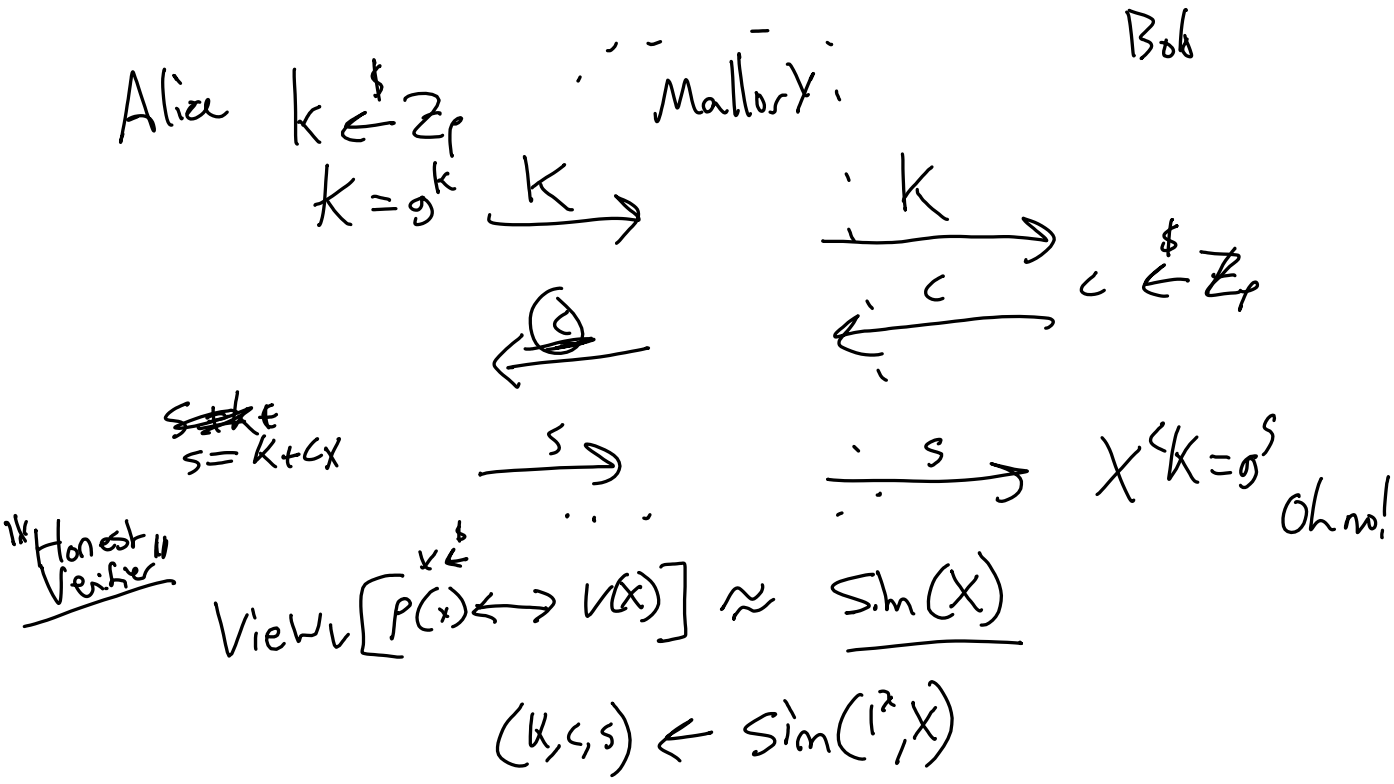
Return ideal functionality:



Can M replay?

In ideal world: No!

In Schnorr protocol!



"Honest Verifier"

$$View_V\left[P(x) \xleftrightarrow{k} V(x)\right] \approx Sim(X)$$

$$(K, c, s) \leftarrow Sim(1^\lambda, X)$$