Security and Privacy, Blatt 5

Franziska Hutter (3295896)
Felix Truger (3331705)
Felix Bühler (2973410)

9. Juli 2018

Problem 1: Schnorr's protocol - special honest verifier zero-knowledge

It is easy to see, that (P, V) as given for Schnorr's protocol has the form of a Σ-protocol with commitment a, challenge e and response z. The "special honest verifier ZK" property requires: $\exists$ ppt simulator M such that $\forall x \in L_R$ and $e \in \{0,1\}^t : M(x,e) = Trans^P_{V^e}(x)$ where $Trans^P_{V^e}(x)$ is the Transcript of an interaction between P and V using challenge e on input x.

to be continued

Problem 2: Homomorphic properties of algorithms

$p = (\mathcal{G}, q, g, h)$ fixed, $r_0, r_1, v_0, v_1 \in \mathbb{Z}_q$, we show:

$$com^{r_0+r_1}(p, v_0 + v_1) \stackrel{!}{=} com^{r_0}(p, v_0) \cdot com^{r_1}(p, v_1)$$

By just applying the definition of com in the Pedersen commitment scheme, we know:

$$com^{r_0+r_1}(p, v_0 + v_1) = g^{v_0+v_1} \cdot h^{r_0+r_1}$$
$$com^{r_0}(p, v_0) = g^{v_0} \cdot h^{r_0}$$
$$com^{r_1}(p, v_1) = g^{v_1} \cdot h^{r_1}$$

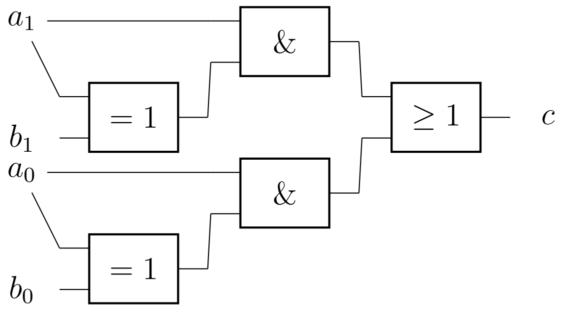
Thus:

$$\begin{aligned} com^{r_0}(p, v_0) \cdot com^{r_1}(p, v_1) &= g^{v_0} \cdot h^{r_0} \cdot g^{v_1} \cdot h^{r_1} \\ &= g^{v_0} \cdot g^{v_1} \cdot h^{r_0} \cdot h^{r_1} \\ &= g^{v_0+v_1} \cdot h^{r_0+r_1} \\ &= com^{r_0+r_1}(p, v_0 + v_1) \end{aligned}$$

Problem 3: Building circuits for functions

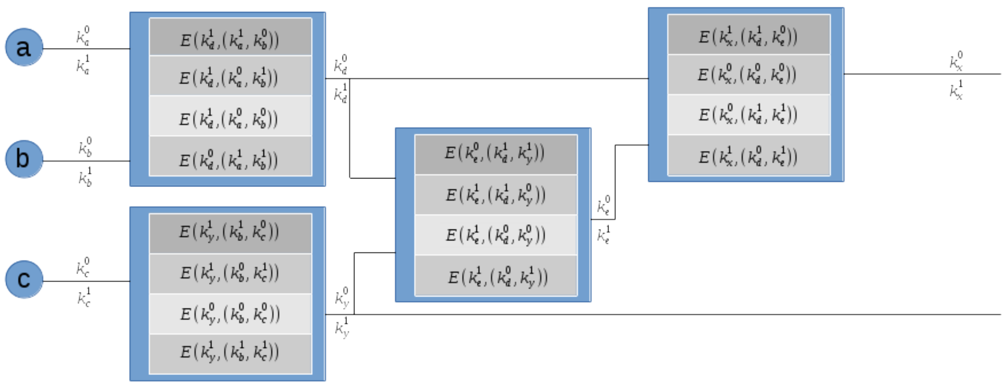
Note: We used the slightly different IEC notation where " $= 1$" denotes an XOR gate and " ≥ 1" denotes an OR gate.

Find the drawing of our circuit for f below.



Problem 4: Garbled circuits

Find a garbled circuit for the given circuit below.



Problem 5: 51%-Attack on Bitcoin