Introduction to Cryptography: Assignment 10

Group number 57

Elwin Tamminga s1013846

Lucas van der Laan s1047485

1

(a) In Schnorr's protocol, the last message r is computed using $v - ca$ and the check is done using $V \stackrel{?}{=} g^r A^c$ while in the variation in Table 1, r is computed using $cv - a$ and the check is done using $V^c \stackrel{?}{=} g^r A$. The main difference can be seen by rewriting the verification check:

Schnorr:

$$\begin{aligned} V &= g^r \cdot A^c \\ g^v &= g^{v-ca} \cdot g^{ac} \\ g^v &= g^v \end{aligned}$$

Σ:

$$\begin{aligned} V^c &= g^r \cdot A \\ g^{vc} &= g^{cv-a} \cdot g^a \\ g^{vc} &= g^{cv} \end{aligned}$$

(b) Alice has all the information she would need to create a valid r such that the protocol will always succeed. This because r is created using 2 of Alice's own variables and the challenge c that she receives from Bob.

We can proof this is the case by rewriting the formula from the Σ protocol like we did in question (a).

(c) The formulas for r and r':

$$\begin{aligned} r &= cv - a \\ r' &= c'v - a \end{aligned}$$

We can then rewrite this so we can calculate a:

$$\begin{aligned} a &= cv - r \\ a &= c'v - r' \end{aligned}$$

We can then equate the formulas to each other:

$$\begin{aligned} cv - r &= c'v - r' \\ cv - c'v &= r - r' \\ v(c - c') &= r - r' \\ v &= \frac{r - r'}{c - c'} \\ a &= c \cdot \frac{r - r'}{c - c'} - r \end{aligned}$$

(d) There are q possibilities for the challenge c. So there is a $1/q$ probability that the simulator uses the same c as the protocol. If $r \xleftarrow{\$} \mathbb{Z}/q\mathbb{Z}$ and $V = (g^r A)^{\frac{1}{c}}$, then if we use these values in the verification check in the protcol with the same challange, we get:

$$\begin{aligned} V^c &= g^r \cdot A \\ ((g^r \cdot A)^{\frac{1}{c}})^c &= g^r \cdot A \\ (g^r \cdot A)^{\frac{c}{c}} &= g^r \cdot A \\ g^r \cdot A &= g^r \cdot A \end{aligned}$$

So then both the protocol and the simulator generate a specific transcript (V; c; r).

(e) The cheating verifier Bob can choose a c to their liking in $\mathbb{Z}/q\mathbb{Z}$, this results in Bob choosing $c = 0$ because $r \longleftarrow cv - a = 0 \cdot v - a = -a \mod q$. This means $a = -r \mod q$.

2

(a) $v = 0$, because $g^0 = 1 = V$
$c = h(p; g; A; V; m)$
$V = g^r \cdot g^{ac}$
$g^v = g^{r+ac}$
$v = r + ac$
$ac = v - r$
$a = \frac{v-r}{c}$
$a = \frac{-r}{h(p;g;A;1;m)}$

(b) $V = g$, so $v = 1$ because $g^1 = 1$
We can now apply this knowledge in the same way as we did in question (a), which leads to:
$a = \frac{1-r}{h(p;g;A;g;m)}$

(c) V has been reused, which means that the randomly chosen variable v has also been reused.

We know from question (a) that $a = \frac{v-r}{c}$. So we have $a = \frac{v-r}{c} = \frac{v-r'}{c'}$.

$c = h(p; g; A; V; m)$
$c' = h(p; g; A; V; m')$

$$\begin{aligned}
\frac{v-r}{c} &= \frac{v-r'}{c'} \\
c(v-r') &= c'(v-r) \\
cv - cr' &= c'v - rc' \\
cv - c'v &= cr' - rc' \\
v(c-c') &= cr' - rc' \\
v &= \frac{cr' - rc'}{c-c'}
\end{aligned}$$

$$\begin{aligned}
a &= \frac{\frac{cr'-rc'}{c-c'} - r}{c} \\
a &= \frac{\frac{cr'-rc'}{c-c'}}{c} - \frac{r}{c} \\
a &= \frac{cr' - rc'}{c(c-c')} - \frac{r}{c}
\end{aligned}$$

(d) She reused v, which leads to reusing V, which is meant to be uniquely generated for every new signature.

(e) Because then she would generate a new v and V for every single iteration. By following the protocol, you do not leak the private key. This is because the private key is used in the calculation for variables that she sends to the other party. If the other party retrieves more than 1 signature pair with the same V, they can derive the private key from that, like we did in question (c).