VRF

Gen (1^B)

sk: $\bar{u}, u_0, u_1, \ldots, u_n$

PK: $g^{\bar{u}}, g^{u_0}, g^{u_1}, \ldots, g^{u_n}, h$

Eval (SK, X):

$X = X_1 X_2 \ldots X_n$

$Y = e(g^{\bar{u} u_0 u_1^{X_1} u_2^{X_2} \ldots u_n^{X_n}}, h)$

$\pi_i = g^{\bar{u} u_1^{X_1} u_2^{X_2} \ldots u_i^{X_i}}; \quad i = 1, 2, \ldots, n$

$\pi_0 = g^{\bar{u} u_0 u_1^{X_1} u_2^{X_2} \ldots u_n^{X_n}}$

Verify (PK, X, Y, π)

Check $\begin{cases} e(\pi_1, g) = e(g^{\bar{u}}, g^{u_1^{X_1}}) \\ e(\pi_i, g) = e(\pi_{i-1}, g^{u_i^{X_i}}) \quad \forall i \end{cases}$

Check $e(\pi_0, g) = e(\pi_n, g^{u_0}), \quad e(\pi_0, h) = Y$

Assumption: $x \xleftarrow{B} \mathbb{Z}_p$

Given $g, g^x, g^{x^2}, g^{x^3}, \ldots, g^{x^{i-1}}, g^{x^{i+1}}, g^{x^{i+2}}, \ldots, g^x$

$e(g, h)^{x^i}$ vs random

Reduction: $Q = \#$ Queries

$L = 4Q(n+L)$, $m = 4Q$

Choose: $r_1, r_2, \ldots, r_n, r' \xleftarrow{R} Z_m$

$\qquad s_1, s_2, \ldots, s_n, s' \xleftarrow{R} Z_p$

$\qquad k \xleftarrow{R} \{0, L, 2, \ldots, n\}$

$sk: u_i = x^{km+r's'}$, $\bar{u} = x^m$, $u_i = x^{r_i s_i}$

calculate: $PK: gx^{r_i s_i}, gx^m, g^{x^{km+r's'}}$

Oracle: A output $\overline{X^1}, \overline{X^2}, \ldots, \overline{X^Q}$

$C(X) = km + r' + m + r_1 X_1 + r_2 X_2 + \ldots + r_n X_n$

$J(X) = s_1^{X_1} s_2^{X_2} \ldots s_n^{X_n} s'$

$C(X, i) = m + r_1 X_1 + r_2 X_2 + \ldots + r_i X_i$

$J(X, i) = s_1^{X_1} s_2^{X_2} \ldots s_i^{X_i}$

For $i = 1, 2, \ldots, Q$:

$\quad$ $\underline{1)\ k(\overline{X^i}) = 0 \text{ then abort}}$

$\quad$ Else calculate $Y = e(gx^{C(\overline{X^i})}, h)^{J(\overline{X^i})}$

$\qquad\qquad\qquad \Pi_j = gx^{C(\overline{X^i}, j)} J(\overline{X^i}, j)$

Challenge: $\underline{1)\ C(X) \neq L \text{ then abort}}$

Else:
$\qquad$ Denote $(\overline{X}) = (\overline{X^1}, \overline{X^2}, \ldots, \overline{X^Q}, X')$

$\qquad\qquad\qquad (r) = (r_1, r_2, \ldots, r_n, r')$

Begin sampling phase:

Sampling phrase:

$$T((X'), (r), k) = \begin{cases} 1 & \text{if } C(X') \neq 1 \; \bigvee_{i=1}^{Q} K(\overline{X^i}) = 0 \\ 0 & \text{otherwise} \end{cases}$$

$$q_{min} = \frac{1}{8Q(n-1)}$$

$$T = 128 \, \epsilon^{-2} \ln\left(\left(\frac{\epsilon}{8}\right)^{-1} q_{min}^{-1}\right) q_{min}^{-1}$$

$$K_1, K_2, \ldots, K_T \xleftarrow{R} \{0, 1, \ldots, n\}$$

$$(r_1), (r_2), \ldots, (r_T) \xleftarrow{R} \mathbb{Z}_p^{n+1}$$

Calculate $a'_{\overline{X}} = \frac{1}{T} \sum_{i=1}^{T} T(\overline{X}, (r_i), K_i)$.

If $a'_{\overline{X}} \geq q_{min}$, abort with $pr = \frac{q_{min}}{a'_{\overline{X}}}$.

Else calculate $y^{T(X')}$

Security analysis:

$$Pr[A \text{ win}] = \sum_{(\overline{X})} Pr[A \text{ chooses } \overline{X}] \cdot Pr[A(\overline{X}) \text{ guess right}]$$

Let $\text{abort}(\overline{X})$ denote the event A' aborts when A chooses $(\overline{X})$

$$Pr[A' \text{ win}] = \sum_{(\overline{X})} \left(Pr[\text{abort}(\overline{X})] \cdot \frac{1}{2} + Pr[\overline{\text{abort}(\overline{X})}] \cdot Pr[A(\overline{X}) \text{ guess right}] \right) Pr[A \text{ chooses } \overline{X}]$$

$$= \sum_{(\overline{X})} Pr[\overline{\text{abort}(\overline{X})}] \, Pr[A \text{ choose } \overline{X}] \left(Pr_A[A(\overline{X}) \text{ guess right}] - \frac{1}{2} \right)$$

(right page, partially cut off)

sampling

Because $Pr[A \ ^{(\overline{X})}$

for some $(\overline{X})$, we c

$\Rightarrow$ We wish to make

to a certain value

let $a_{\overline{X}}$ denote the

before the sampling

In the paper, we ha

$\Rightarrow$ We wish $Pr[\overline{\text{abo}}$

$T((\overline{X}), (r), k) = 0,$

Impossible, since

$\Rightarrow$ Calculate $a'_{\overline{X}}$

to $a_{\overline{X}}$ with ove

$\Rightarrow Pr[\overline{\text{abort}(}$

sampling phrase motivation:

Because $Pr[A \text{ guess right}] - \frac{1}{2}$ can be negative

for some $(\bar{X})$, we can't estimate $Pr[\overline{abort(\bar{X})}]$

$\Rightarrow$ We wish to make $Pr[\overline{abort(\bar{X})}]$ close

to a certain value

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad$ NOT

let $a_{\bar{X}}$ denote the probability we will abort

before the sampling phrase $(Pr[r((\bar{X}),(r),k)$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad = 0)$

In the paper, we have : $a_{\bar{X}} \geqslant a_{min}$

$\Rightarrow$ We wish $Pr[\overline{abort(\bar{X})}] = a_{min} \Rightarrow$ when

$r((\bar{X}),(r),k) = 0$, abort with $Pr = \frac{a_{min}}{a_X} \Rightarrow$

Impossible, since we don't know a_X

$\Rightarrow$ Calculate $a'_{\bar{X}}$, and see that $a'_{\bar{X}}$ is close

to a_X with overwhelming probability

$\Rightarrow Pr[\overline{abort(\bar{X})}]$ is very close to $a_{min} \forall (X)$

$(\bar{X})]$

$) Pr[A \text{ chooses } \bar{X}]$

Chernoff bound:

$X_1, X_2, \ldots, X_n$ are independent random variable

$X = X_1 + X_2 + \ldots + X_n$, $\mu = E[X]$

$\forall \epsilon > 0$

$$Pr[X \geq (1+\epsilon)\mu] \leq \left(\frac{e^{\epsilon}}{(1+\epsilon)^{1+\epsilon}}\right)^{\mu}$$

$$Pr[X \leq (1-\epsilon)\mu] \leq \left(\frac{e^{\epsilon}}{(1-\epsilon)^{1-\epsilon}}\right)^{\mu}$$

Proof: $Pr[X \geq (1+\epsilon)\mu] = Pr[e^{tX} \geq e^{t(1+\epsilon)\mu}] \leq \frac{E[e^{tX}]}{e^{t(1+\epsilon)}}$

$$= \frac{E[e^{tX_1}] E[e^{tX_2}] \ldots E[e^{tX_n}]}{e^{t(1+\epsilon)\mu}}$$

$E[e^{tX_i}] = (1-p) + pe^{t} \leq e^{p(e^{t}-1)}$

$\Rightarrow Pr[X \geq (1+\epsilon)\mu] \leq e^{\mu(e^{t}-1) - t(1+\epsilon)\mu}$

We choose t so that $\mu(e^{t}-1) - t(1+\epsilon)\mu$ is minim

$(t = \ln(1+\epsilon))$

Thus $Pr[X \geq (1+\epsilon)\mu] \leq \left(\frac{e^{\epsilon}}{(1+\epsilon)^{1+\epsilon}}\right)^{\mu}$

Similarly, $Pr[X \leq (1-\epsilon)\mu] = Pr[-X \geq (\epsilon-1)\mu]$

Thus $Pr[X \leq (1-\epsilon)\mu] \leq \left(\frac{e^{\epsilon}}{(1-\epsilon)^{1-\epsilon}}\right)^{\mu}$

We can have a less tight bound, but nicer look

$$Pr[X \geq (1+\epsilon)\mu] \leq e^{-\mu\epsilon^2/(2+\epsilon)}$$

$$Pr[X \leq (1-\epsilon)\mu] \leq e^{-\mu\epsilon^2/2}$$

Estimate $Pr[\overline{abort(\overline{X})}]$ and $Pr[abort(\overline{X})]$

We have: $E[\acute{a}_{\overline{x}}] = a_{\overline{x}}$

$$Pr[T\acute{a}_{\overline{x}} \leq T_{a_x}(1-\frac{\epsilon}{8})] < e^{-T_{a_x} \cdot (\frac{\epsilon}{8})^2/2} = a_{min}\frac{\epsilon}{8}$$

Thus $Pr[\overline{abort(\overline{X})}] = 1 - Pr[\overline{abort(\overline{X})}]$

$$= 1 - a_x \left(\sum_i Pr[\acute{a}_{\overline{x}} = i] \cdot Pr[abort\ sample\ |\ \acute{a}_{\overline{x}} = i] \right)$$

$$\geq 1 - a_x \left(Pr[\acute{a}_{\overline{x}} \leq a_x(1-\frac{\epsilon}{8})] + \sum_{i > a_x(1-\frac{\epsilon}{8})} Pr[\acute{a}_{\overline{x}} = i] \cdot \frac{a_{min}}{\acute{a}_{\overline{x}}} \right)$$

nal $\geq 1 - a_x \left(a_{min}\frac{\epsilon}{8} + \frac{a_{min}}{a_x(1-\frac{\epsilon}{8})} \right)$

$\cancel{} a_x \quad 1 - a_{min} - a_{min}\frac{3\epsilon}{8}$

Similarly, $Pr[abort(\overline{X})] \geq a_{min}(1-\frac{1}{4}\epsilon)$

ViKA

$$\Pr[A' \text{win}] \geqslant \left(1 - a_{min} - a_{min} \cdot \frac{3\varepsilon}{8}\right) \cdot \frac{1}{2} + \left(1 - \frac{1}{4}\varepsilon\right) a_{min}$$

$$\geqslant \frac{1}{2} + \frac{3\varepsilon}{64Q(n+1)}$$