VRF Construction:

$Gen(1^{\lambda})$:

$sk: \bar{u}; u_0; u_1; \dots; u_n$

$pk: g^{\bar{u}}, g^{u_0}, g^{u_1}, \dots, g^{u_n}, h$

Eval(sk, x):

$x = x_1 x_2 \dots x_n$

$y = e(g^{\bar{u} u_0 u_1^{x_1} u_2^{x_2} \dots u_n^{x_n}}, h)$

$\pi_i = g^{\bar{u} u_1^{x_1} u_2^{x_2} \dots u_i^{x_i}}; i = 1, 2, \dots, n$

$\pi_0 = g^{\bar{u} u_0 u_1^{x_1} u_2^{x_2} \dots u_n^{x_n}}$

Verify(pk, x, y, π)

Check $\begin{cases} e(\pi_1, g) = e(g^{\bar{u}}, g^{u_1^{x_1}}) \\ e(\pi_i, g) = e(\pi_{i-1}, g^{u_i^{x_i}}) \ \forall i \end{cases}$

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

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

Given $g, g^{x}, g^{x^2}, g^{x^3}, \dots, g^{x^{l-1}}, g^{x^{l+1}}, g^{x^{l+2}}, \dots, g^{x^{\lambda}}$

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

Reduction: Q = # Queries

$l = 4Q(n+1)$, $m = 4Q$

Choose: $r_1, r_2, \ldots, r_n, r' \xleftarrow{R} \mathbb{Z}_m$

$s_1, s_2, \ldots, s_n, s' \xleftarrow{R} \mathbb{Z}_p$

$k \xleftarrow{R} \{0; 1; 2; \ldots; n\}$

$sk: u_0 = x^{km+r'} s'$, $\bar{u} = x^m$, $u_i = x^{r_i} s_i$

calculate: PK: $g^{x^{r_i} s_i}$, g^{x^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 $i = 1; 2; \ldots; Q$:

If $k(\overline{X^i}) = 0$ then abort

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

$\pi_j = g^{x^{C(\overline{X^i}, j)} J(\overline{X^i}, j)}$

, h

Challenge: If $C(X^*) \neq l$ then abort

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

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

Begin sampling phrase:

Sampling phrase:

$$T((\overline{X}), (r_i), K) = \begin{cases} 1 \text{ if } C(X') \neq 1 \quad \forall_{i=1}^{Q} K(\overline{X^q}) = \\ 0 \text{ otherwise} \end{cases}$$

$$a_{min} = \frac{1}{8Q(n+1)}$$

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

$$k_1, k_2, \dots, k_T \xleftarrow{R} \{0, 1, \dots, n\}$$

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

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

If $a'_{\overline{X}} \geq a_{min}$, not abort with $Pr = \frac{a_{min}}{a'_{\overline{X}}}$.

Else calculate $Y^{J(X')}$

Security analysis:

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

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

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

$$Pr[A(\overline{X}) \text{ guess right}$$

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

Được quét bằng CamScanner

sampling phrase motivation:

Because $\Pr[A^{(\overline{X})}$ guess right$] - \frac{1}{2}$ can be negative for some $(\overline{X})$, we can't estimate $\Pr[\overline{\text{abort}(\overline{X})}]$

$\Rightarrow$ We wish to make $\Pr[\overline{\text{abort}(\overline{X})}]$ close to a certain value

Let $a_{\overline{X}}$ denote the probability we will NOT abort before the sampling phrase ($\Pr[\tau((\overline{X}), (r), k] = 0$)

In the paper, we have: $a_{\overline{X}} \geq a_{min}$

$\Rightarrow$ We wish $\Pr[\overline{\text{abort}(\overline{X})}] = a_{min}$ $\Rightarrow$ when $\tau((\overline{X}), (r), k) = 0$, abort with $\Pr = \frac{a_{min}}{a_X}$ $\Rightarrow$

Impossible, since we don't know a_X

$\Rightarrow$ Calculate $a'_{\overline{X}}$, and see that $a'_{\overline{X}}$ is close to a_X with overwhelming probability

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

right]

$\overline{(\overline{X})}]$

$])$ $\Pr[A$ chooses $\overline{X}]$

guess right$] - \frac{1}{2})$

VIKA

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

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

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

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

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

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

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

VIKA

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

We have: $E[a'_{\overline{X}}] = a_{\overline{X}}$

$$\Pr[Ta'_{\overline{X}} \leq Ta_X(1-\frac{\epsilon}{8})] < e^{-Ta_X\cdot(\frac{\epsilon}{8})^2/2} = a_{min}\frac{\epsilon}{8}$$

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

$$= 1 - a_X\left(\sum_i \Pr[a'_{\overline{X}} = i].\Pr[\text{abort sample} \mid a'_{\overline{X}} = i]\right)$$

$$\geq 1 - a_X\left(\Pr[a'_{\overline{X}} \leq a_X(1-\frac{\epsilon}{8})] + \sum_{i \geq a_X(1-\frac{\epsilon}{8})} \Pr[a'_{\overline{X}} = i].\frac{a_{min}}{a'_{\overline{X}}}\right)$$

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

nal

$$\cancel{\geq 1 - a_X a} \quad 1 - a_{min} - a_{min}\cdot\frac{3\epsilon}{8}$$

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

VIKA

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

$$\geq \frac{1}{2} + \frac{3\epsilon}{64Q(n+1)}$$ (lazy, Just see the pap

Thus, if A can win with Probability $\frac{1}{2} + \epsilon$, then A' can win with probability $\frac{1}{2} + \frac{3\epsilon}{64Q(n+1)}$

This is much better than Dodis-Yampovsky's VRF.

VIKA