Definition: Linear hash function. Let $D$ be a $b \times m$ Boolean matrix.

Let $h_D : \{0,1\}^m \rightarrow \{0,1\}^b$ be a linear function defined by $h_D(x) = Dx$ (using mod 2 arithmetic).
For $C \subseteq \{0,1\}^m$, let $h(C) = \{h(x) : x \in C\}$

Random linear hash function is obtained by choosing the matrix $D$ randomly.

Lemma: Let $C \subseteq \{0,1\}^m$ and $c = \frac{|C|}{2^b} \leq 1$.
Let $h : \{0,1\}^m \to \{0,1\}^b$ be a random linear function and $z$ be a random element of $\{0,1\}^b$.
Then $Prob(z \in h(C)) \geq c - (c^2/2)$.

Proof: Note that, for $x \neq y$, $Prob(h(x) = h(y))$ is $2^{-b}$ (as each bit of $h(x)$ agrees with the corresponding bit of $h(y)$ with probability $1/2$).
Thus, for a random $z$, probability that $h(x) = h(y) = z$, for two distinct $x, y$ is at most $2^{-2b}$.
It follows that $Prob(z \in h(C))$
$\geq \Sigma_x Prob(z = h(x)) - \Sigma_{x \neq y} Prob(z = h(x) = h(y))$
$\geq \frac{|C|}{2^b} - \frac{\binom{|C|}{2}}{2^{2b}} \geq c - \frac{c^2}{2}$.

Theorem: NON-ISO is in AM.

Proof: Assume $G_1$ and $G_2$ do not have any nontrivial automorphism, and each has $n$ vertices.

The number of graphs which are isomorphic to atleast one of them is $n!$ or $2n!$ based on whether the graphs are isomorphic or not.

So if one chooses at random a graph among $2^{\binom{n}{2}}$ possible graphs, (where $n$ is the number of vertices in $G_1, G_2$), then the probablity of finding a graph which is isomorphic to one of $G_1$ and $G_2$ (call this set $C$), gives us a separation.

However, $n!$ is too small compared to $2^{\binom{n}{2}}$.

So one uses a random hash function from a binary string of length $\binom{n}{2}$ to a string of length $q = \lceil \log_2(n!) \rceil + 2$.
Now, for a random hash function $h$ and a random $z$, the probability that $z$ is in $h(C)$ is at most $n!/2^q$ if graphs are isomorphic and at least $2(n!/2^q) - (2(n!/2^q))^2/2 \geq \frac{3}{2}(n!/2^q)$, otherwise.

Thus, the verifier can send the prover a random hash function $h$ and a random $z$, and ask prover to provide a graph $G$ which is isomorphic to one of $G_1$ and $G_2$ (along with a proof) such that $h(G) = z$.
The probability that the prover passes this test is at least $\frac{3}{2} * \frac{n!}{2^q}$, if the graphs are non-isomorphic and at most $\frac{n!}{2^q}$ if the graphs are iso-morphic.
This probability can be modified to satisfy the requirements of AM protocol.
To get around automorphism problem, use $\langle G, p \rangle$, where $p$ is supposed to give an automorphism of $G$.

Corollary: If graph isomorphism problem is NP-complete then PH collapses!