G00002

ZERO-KNOWLEDGE PROVING SYSTEM AND METHOD

ABSTRACT

A zero-knowledge proving system includes a proving mechanism (100) for proving equality or inequality of two discrete logarithms and a verifying mechanism (150) for verifying said equality or inequality. The proving mechanism stores public information including a designated operation scheme, two input numbers α and β, and two predetermined bases g and h, private information x which is a discrete logarithm of α to the base g. After converting α, β and h to produce α', β' and γ' as follows: $\alpha' = \alpha^r$; $\beta' = \beta^r$; and $\gamma' = h^{xr}$, the equality of a $\log_\alpha\alpha'$ and $\log_\beta\beta'$ and the equality of $\log_g\alpha'$ and $\log_h\gamma'$ are proved. The verifying mechanism (150) verifies the equality of a $\log_\alpha\alpha'$ and $\log_\beta\beta'$ and the equality of $\log_g\alpha'$ and $\log_h\gamma'$. Then, the received β' and γ' are checked to determine the equality or inequality thereof, and it is determined whether the proof is acceptable, depending on the verification and the check results.

Fig. 1