

CLAIMS

1. A method for generation and/or authentication of time-based one-time passwords (TOTPs), comprising, at a client device:
 - 5 performing an initialisation operation comprising:
 - determining a time period;
 - generating one or more one-way function (OWF) chains for each of one or more sub-periods of the time period, wherein an OWF chain for a sub-period is generated by:
 - 10 dividing the sub-period into N segments of equal duration; and
 - recursively applying a one-way function N times to a random initial secret that is a head node of the OWF chain, to generate a tail node of the OWF chain; and
 - 15 transmitting, to one or more verifier devices, an initialisation message comprising a client identifier and the tail nodes of respective OWF chains, such that a TOTP generated by the client device is verifiable by the one or more verifier devices using one of the tail nodes as a verify point.
2. A method according to claim 1, further comprising performing a proof generation operation comprising:
 - 20 determining a number M of segments remaining from a current time until the end of a current sub-period of the one or more sub-periods;
 - generating a TOTP by M recursive evaluations of the OWF, starting with a head node of the OWF chain for the current sub-period; and
 - 25 transmitting an authentication message comprising the client identifier and the TOTP to one of the verifier devices.
3. A method according to claim 1 or claim 2, wherein a head node of an OWF chain for each sub-period is generated by a pseudo-random number generator using a head node of an OWF chain for the immediately preceding sub-period.
 - 30
4. A method according to claim 3, further comprising an auto-replenishment operation prior to all nodes of the OWF chain or OWF chains being consumed.
5. A method according to claim 4, wherein the auto-replenishment operation comprises
 - 35 distributing one or more additional verify points to the one or more verifier devices using a one-time signature scheme.

6. A method according to any one of claims 1 to 5, comprising, at a verifier device of the verifier devices, performing an authentication operation comprising:
- receiving the client identifier and the TOTP;
 - determining, based on a time of receipt of the authentication message, a number Z of time segments that have elapsed since a time of last authentication of the client device;
 - generating verification data by Z recursive evaluations of the OWF, starting with the TOTP; and
 - if the verification data matches the verify point for a current sub-period, updating the verify point to be the TOTP; and updating the time of last authentication to the time of receipt of the authentication message.
7. A method according to any one of claims 1 to 6, wherein the proof generation operation is performed at regular intervals as a proof of aliveness of the client device.
8. A method according to claim 7, wherein the authentication operation further comprises determining whether a difference between the time of receipt of the authentication message and the time of last authentication of the client device exceeds an aliveness time threshold.
9. An apparatus for generation of time-based one-time passwords (TOTPs), comprising at least one processor in communication with computer-readable storage, the computer-readable storage having instructions stored thereon for causing the at least one processor to:
- perform an initialisation operation comprising:
 - determining a time period;
 - generating one or more one-way function (OWF) chains for each of one or more sub-periods of the time period, wherein an OWF chain for a sub-period is generated by:
 - dividing the sub-period into N segments of equal duration; and
 - recursively applying a one-way function N times to a random initial secret that is a head node of the OWF chain, to generate a tail node of the OWF chain;
 - and
 - transmitting, to one or more verifier devices, an initialisation message comprising a client identifier and the tail nodes of respective OWF chains, such that a TOTP generated by the client device is verifiable by the one or more verifier devices using one of the tail nodes as a verify point.

10. An apparatus according to claim 9, wherein the instructions further cause the at least one processor to perform a proof generation operation comprising:
determining a number M of segments remaining from a current time until the end of a current sub-period of the one or more sub-periods;
5 generating a TOTP by M recursive evaluations of the OWF, starting with a head node of the OWF chain for the current sub-period; and
transmitting an authentication message comprising the client identifier and the TOTP to one of the verifier devices.
11. An apparatus according to claim 9 or claim 10, wherein the instructions further cause
10 a head node of an OWF chain to be generated for each sub-period by a pseudo-random number generator using a head node of an OWF chain for the immediately preceding sub-period.
12. An apparatus according to claim 11, wherein the instructions further cause the at
15 least one processor to perform an auto-replenishment operation prior to all nodes of the OWF chain or OWF chains being consumed.
13. An apparatus according to claim 12, wherein the auto-replenishment operation
20 comprises distributing one or more additional verify points to the one or more verifier devices using a one-time signature scheme.
14. An apparatus according to any one of claims 10 to 13, wherein the proof generation operation is performed at regular intervals as a proof of aliveness of the apparatus.
15. A verification server comprising at least one processor in communication with
25 computer-readable storage, the computer-readable storage having stored thereon instructions for causing the at least one processor to perform an authentication operation comprising:
receiving a client identifier and a TOTP from a client device;
retrieving a stored verify point and a time of last authentication for the client
30 device based on the client identifier and a current time;
retrieving a one-way function (OWF);
determining, based on a time of receipt of the authentication message, a number Z of time segments that have elapsed since the time of last authentication;
35 generating verification data by Z recursive evaluations of the OWF, starting with the TOTP; and

if the verification data matches the verify point for the current time, updating the verify point to be the TOTP; and updating the time of last authentication to the time of receipt of the authentication message.

16. A verification server according to claim 15, wherein the authentication operation
- 5 further comprises determining whether a difference between the time of receipt of the authentication message and the time of last authentication of the client device exceeds an aliveness time threshold.