A World Leading SFI Research Centre

CONNECT Centre for Future Networks

Science Foundation Ireland sfi For what's next

Quantum authentication tickets

Hazel Murray*, Jerry Horgan† and David Malone§

* Munster Technological University, Cork. hazel.murray@mtu.ie

† Walton Institute, Waterford Institute of Technology, Waterford. jerry.horgan@waltoninstitute.ie

§ Maynooth University, Co. Kildare. david.malone@mu.ie

Ticket-based authentication systems are used across the internet. They allow an entity or device to be issued a ticket which can be used to repeatedly authenticate to a service. We propose a quantum ticket algorithm (based on Gavinsky's coin scheme) which offers protection against phishing, replay and man-in-the-middle attacks, and authentication with the service does not require either quantum or encrypted communication channels. It also provides in-built ticket expiration and graded step-up authentication depending on levels of trust and risk.

What is ticket-based authentication?

Ticket-based authentication is based on time-limited tickets that enable users to connect to a service. Kerberos is an example of a ticket-based scheme which allows a client A to claim a ticket for a service B through the central trusted server S. Kerberos limits the lifetime of a ticket using timestamps, which requires synchronised clocks. Kerberos has no method for limiting the number of times a user can use a ticket within this lifetime and there is no mechanism within the ticket for responding to reductions in trust. In this scheme, we achieve both of these functionalities without requiring B to store information about A.

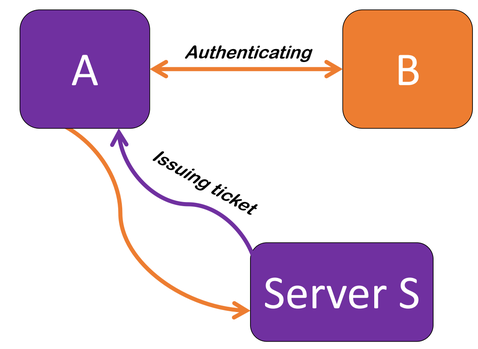
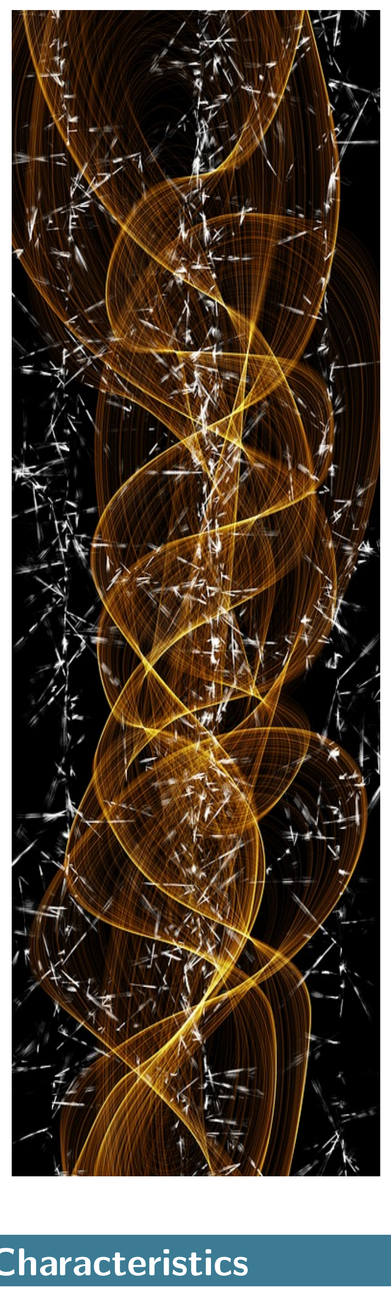


Figure: High level protocol. Purple: quantum, orange: classical



Our quantum ticket mechanism

Like Kerberos, we assume A and B have established trusted symmetric keys with S. Unlike Kerberos, we assume S has a quantum communication channel with A to issue the ticket. The validation of the ticket is based on the quantum complexity problem known as the Hidden Matching Problem (HMP). This problem allows an entity B, who holds classical strings $x_1, \ldots, x_k$ that correspond to quantum registers $|\alpha(x_1)\rangle, \ldots, |\alpha(x_k)\rangle$, to verify that A holds the quantum registers via a zero-knowledge protocol. A begins by requesting a ticket to access B from S:

1. $A \rightarrow S$: $A, B, \mathcal{N}_A$ where nonce, $\mathcal{N}_A$, is used as a session identifier and to randomize step 2's encrypted output.
2. $\mathbf{S} \rightarrow \mathbf{A}$: $\mathtt{ticket}_B, |\alpha(\mathbf{x_1})\rangle, \ldots, |\alpha(\mathbf{x_k})\rangle, \{\mathtt{ticketID}, \mathcal{N}_A, B\}_{k_{\langle A,S\rangle}}$ where $\mathtt{ticket}_B = \{\mathtt{ticketID}, x_1, \ldots, x_k, A\}_{k_{\langle B,S\rangle}}$.

A now has a ticket to present to B.

A now authenticates to B using only classical communication:

1. A presents her ticket to B:
   $A \rightarrow B$: $\mathtt{ticket}_B, \mathtt{ticketID}$
2. B will ask A to measure a selection of quantum registers. The size of t will depend on the trust/reputation of A.
   $B \rightarrow A$: SetB where $\mathtt{SetB} \subset [k], s.t. |\mathtt{SetB}| = t$
3. A will randomly select $2t/3$ of the values in SetB to measure and informs B of her selection.
   $A \rightarrow B$: SubsetA
4. B tells A which basis (indicated by 0 or 1) to measure each register w.r.t.
   $B \rightarrow A$: SetM where $\forall i \in \mathtt{SubsetA}, m_i \in \{0, 1\}$
5. Finally A measures the chosen registers with the relevant basis and reports a version of the results to B
   $A \rightarrow B$: $(\mathbf{a_i}, \mathbf{b_i})$ where $\mathtt{Measure}|\alpha(\mathbf{x_i})\rangle \Rightarrow (\mathbf{a_i}, \mathbf{b_i})$
6. B uses these results to verify whether A holds the relevant quantum registers using HMP.
   $B \rightarrow A$: *Outcome* where *Outcome* = True if $(x_i, m_i, a_i, b_i) \in HMP_4 \; \forall i \in \mathtt{SubsetA}$

The protocol above is based on Gavinsky's Quantum Coin Scheme [1].

Characteristics

Each time a particular register is measured, it collapses and cannot be reused. This quantum property allows it to be secure against phishing and replay attacks and ensures a limited number of uses for the ticket. The number of uses of the ticket is determined both by the number of quantum registers, k, included in the token, and the number of registers, t, that are requested at each verification. This size, t, can be adapted based on the current trust B has for the client and previous high-risk actions of the client. This protocol requires quantum memories for the storage of the quantum registers by A, A must also have quantum measurement capabilities and to issue the ticket there must exists a quantum communication channel between A and S.
In the traditional Kerberos protocol, a symmetric key is generated for A and B to use to encrypt their communication traffic once A has authenticated to B. This could easily be included inside $\mathtt{ticket}_B$ in this mechanism with the quantum protocols adding an additional layer of security. If limited lifetimes, in addition to limited usages are required, this can also be included by following the Kerberos mechanism.

[1] D. Gavinsky, "Quantum money with classical verification," in *2012 IEEE 27th Conference on Computational Complexity*. IEEE, 2012, pp. 42–52.

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

Waterford Institute of Technology INSTITIÚID TEICNEOLAÍOCHTA PHORT LÁIRGE

Maynooth University National University of Ireland Maynooth

Ireland's European Structural and Investment Funds Programmes 2014-2020 Co-Funded by the Irish Government and the European Union

European Union European Regional Development Fund

Science Foundation Ireland sfi For what's next