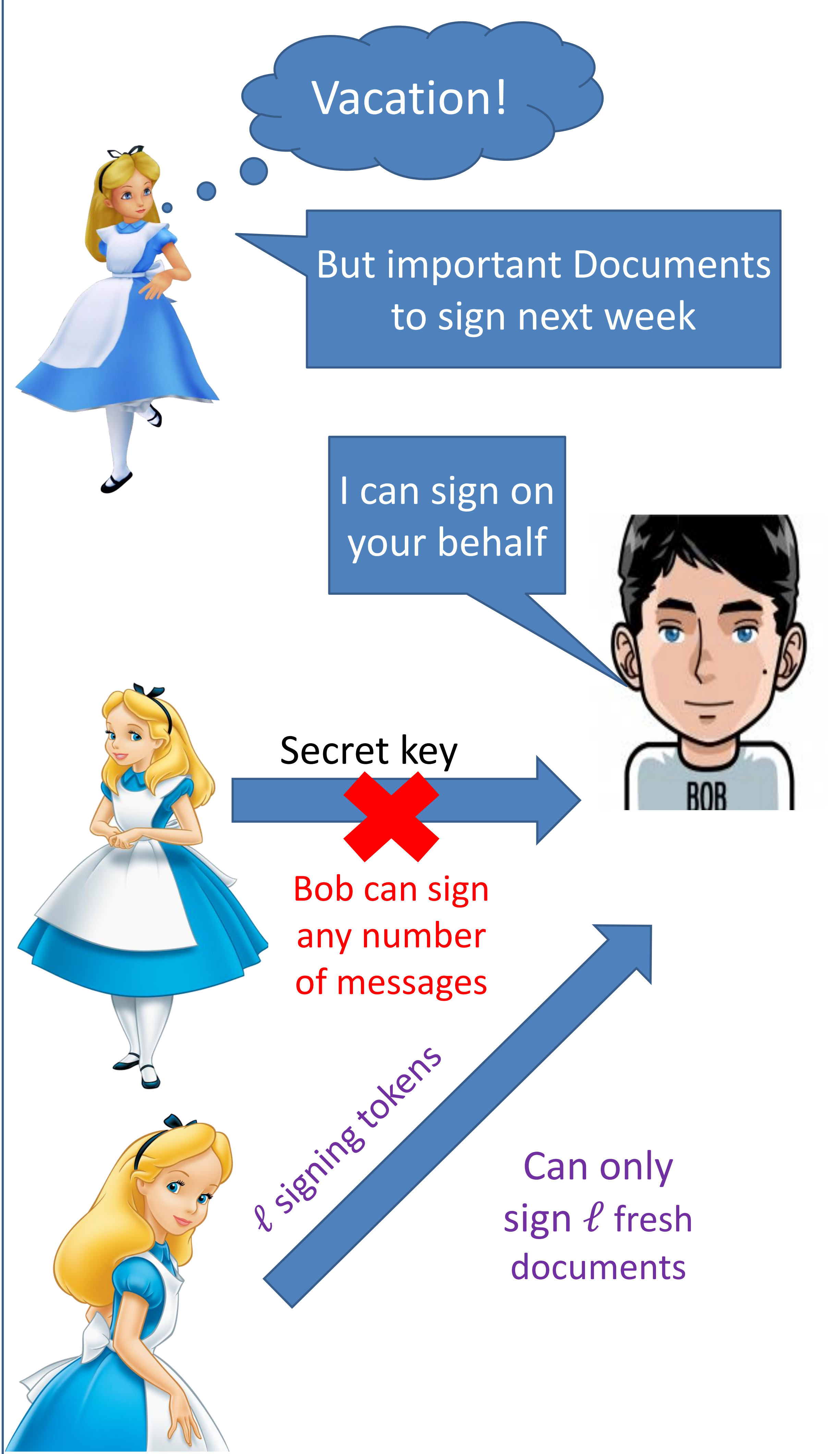
Noise-Tolerant Quantum Tokens For Mac

Amit Behera, Or Sattath, Uriel Shinar
Ben-Gurion University, Israel

Motivation


Vacation!
But important Documents to sign next week
I can sign on your behalf
BOB
Secret key
Bob can sign any number of messages
ℓ signing tokens
Can only sign ℓ fresh documents

Solution: Tokenized MAC

- $Keygen \to sk$ (secret),
- $Tokengen(sk) \to |tok\rangle$ (Signing tokens)
- $Sign_{|tok\rangle}(m) \to \sigma$ (Signature)
- $Verify_{sk}(m, \sigma) \to$ Yes/No.

- Correctness: **Signing** a **document using a valid token passes verification.**
- Security: Given **oracle access to verification,** one **cannot sign $\ell + 1$ distinct documents using ℓ tokens.**
- Previous Constructions: [1]

Impracticality of previous work[1]

- Used highly entangled states as the tokens that are hard to prepare.
- Required perfect quantum devices.

Our Goal: To construct an alternate scheme which is practically feasible.

Our Contributions

- The first Tokenized MAC scheme that uses **Conjugate Coding states for the signing token.**
- The first tokenized MAC scheme to be **noise tolerant upto 14% error**.

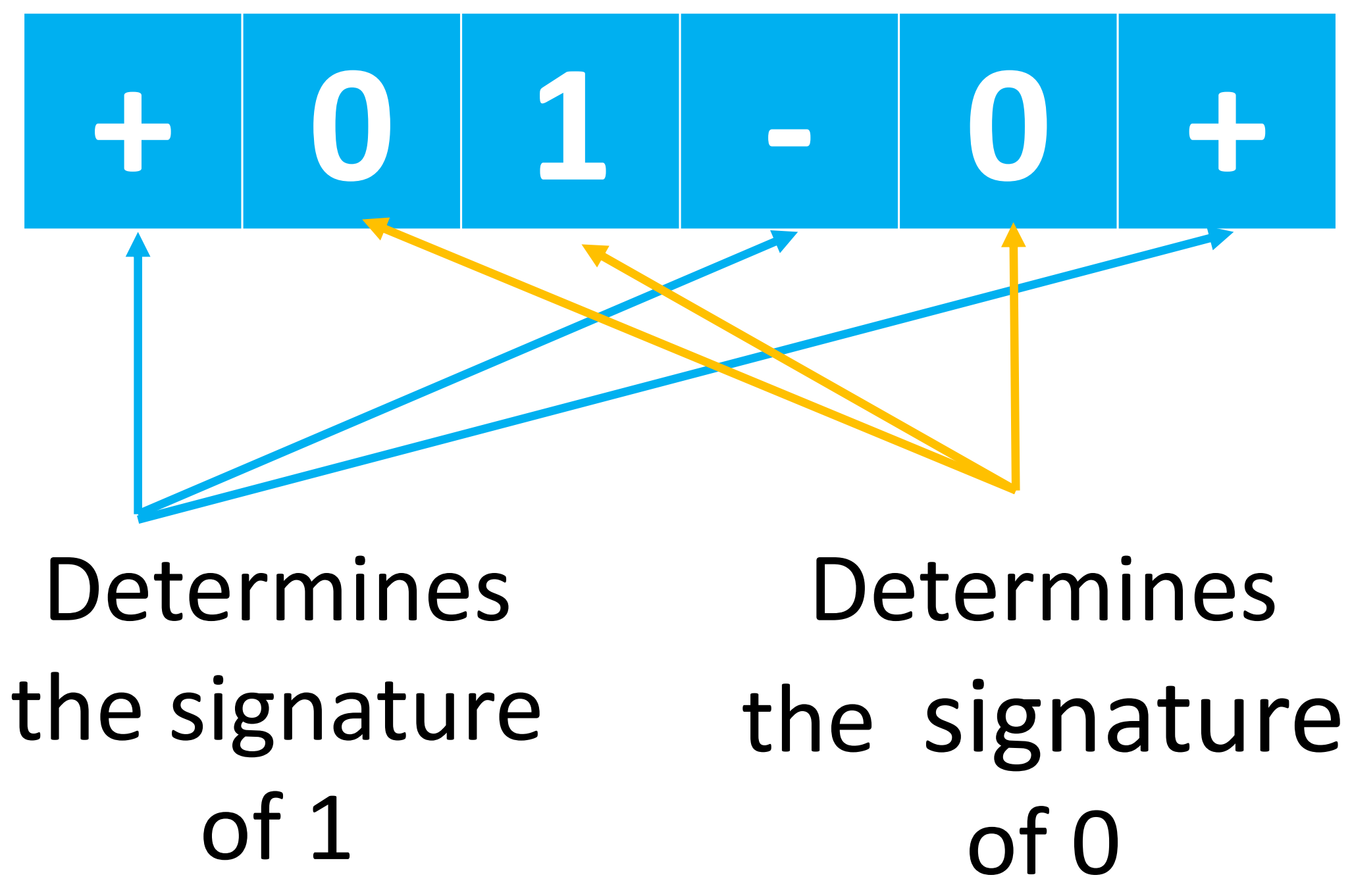
Assumptions: **Post-quantum collision-resistant hash functions** exist.

Mini Scheme for 1-bit

- $\boldsymbol{Keygen(1^{\lambda})}$ −creates a key $(a, b) \in \{0,1\}$^2λ.
- $\boldsymbol{Tokengen_{sk}}$- creates the token $|t\rangle = H^{b}|a\rangle$.
- $\boldsymbol{Sign_{|t\rangle}(m)}$- Measures the qubits of $(\mathrm{H}^{\mathrm{m}})^{\otimes\lambda}\,|t\rangle$ in the computational basis, to get a signature σ.
- $\boldsymbol{Verify_{sk}\,(m, \sigma)}$ − checks if the signature σ is consistent with $(\mathrm{H}^{\mathrm{m}})^{\otimes\lambda}\,|t\rangle$ on the computational basis.

Achieves Unconditional mini scheme Security

A typical Signing token



Noise Tolerant Variant

- Noise Model: **IID Errors**
- Achieved by making the verification lenient: accept a signature **even if consistency check fails at most η fraction of the qubits**.
- We show that for $\eta < 0.07$, the scheme is secure, and is tolerant to IID errors occurring with probability 2η on each qubit.

A Noise Preserving Lift

- Standard techniques used in quantum money schemes can lift the mini-scheme to a full blown tokenized MAC scheme.
- The lift preserves noise tolerance.
- The lift assumes only post quantum collision resistant hash functions

Security Proof Idea

- Obstacle: Dealing the verification oracle- **repeated successful queries on the same message**.
- Solution: Strengthen the adversary by providing extra data on a successful query. Now she **does not need to repeatedly query on a document previously accepted.**
- Reduce such an adversary to an adversary in one of two games both of which has negligible winning probability (proven by semidefinite programming).

Application

- TMACs imply **Quantum One-time memory in the presence of stateless Hardware oracle.**
- Implies **Private Quantum Money.**
- Our scheme **may be practically implementable** in the recent future since it is **noise-tolerant** and requires only **Conjugate coding states that are easy to prepare and transfer over long distances.**

Open Question

- Classical MACs imply one-way functions. Do TMACs imply **Quantum-secure One-way functions?**

- What are its relations between related cryptographic primitives such as **Quantum Encryption with Certified Deletion, Copy-protection** etc? Do they imply each other?

Reference:
[1]Ben-David and O. Sattath. Quantum Tokens for Digital Sig-natures, 2016, arXiv:1609.09047.

Read the Full Paper at: https://arxiv.org/pdf/2105.05016.pdf