On black-box separations of quantum digital signatures from pseudorandom states.

Saachi Mutreja
Columbia

Joint work with
Andrea Coladangelo (University of Washington).

Impagliazzo's Five Worlds

Algorithmica	P=NP
Heuristica	P≠NP, but problems in NP are easy on average.
Pessiland	hard on average problems in NP, OWFs don't exist.
Minicrypt	OWFs exist, PKE does not exist.
Cryptomania	PKE exists

What happens in the quantum world?

- Are OWFs necessary in the quantum world?

What happens in the quantum world?

- Are OWFs necessary in the quantum world?

- What are the ***minimal assumptions*** needed to build quantum cryptography?

Microcrypt

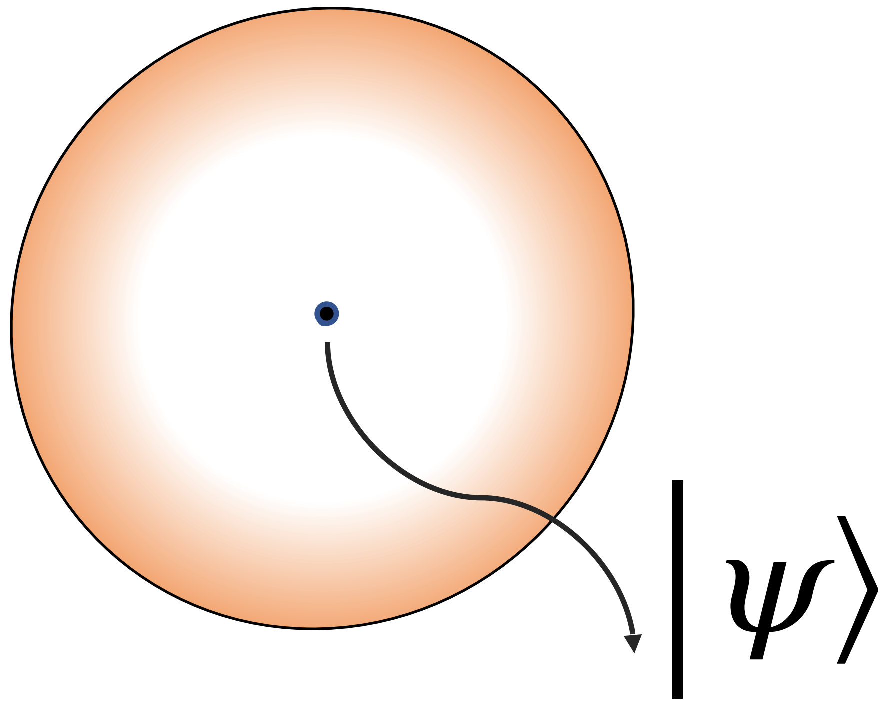
- Set of primitives that are potentially weaker than OWFs.
- Security is formulated in terms of the hardness of an inherently quantum problem.

Microcrypt

- Set of primitives that are potentially weaker than OWFs.
- Security is formulated in terms of the hardness of an inherently quantum problem.
- Although weaker than OWFs, microcrypt contains primitives like pseudo-random states (PRS), one way state generators (OWSGs), etc.

Pseudorandom States (PRSs)

- Computational Approximations to the Haar Measure.
- Intuitively, Haar distribution is the uniform distribution over quantum states.



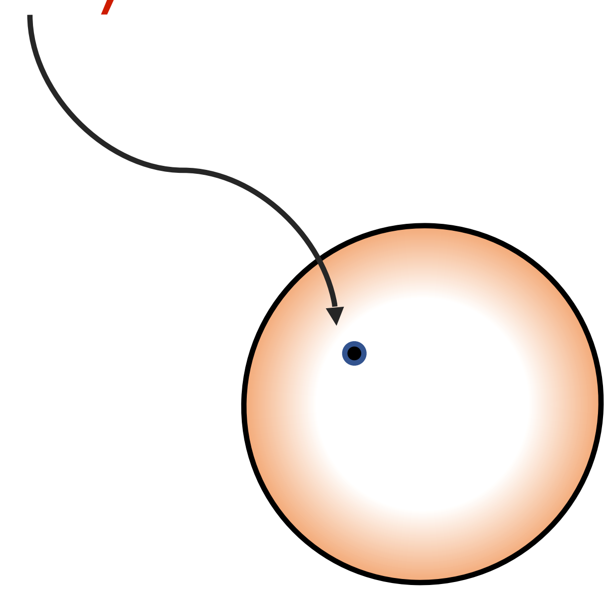
Pseudorandom states

A pair of efficient quantum poly-time (QPT) algorithms (GenKey, GenState) is a **pseudorandom state (PRS)** if

- Given security parameter λ, GenKey(1^λ) outputs a key $k \in \{0,1\}^\lambda$.
- given key $k \in \{0,1\}^\lambda$, GenState(k) outputs n-qubit state $|\psi\rangle = |\text{PRS}(k)\rangle$.
- for all t, for all poly-time algorithms D (called a **distinguisher**),

$$D\Big(\underbrace{|\psi\rangle, \ldots, |\psi\rangle}_{t}\Big) \approx D\Big(\underbrace{|\vartheta\rangle, \ldots, |\vartheta\rangle}_{t}\Big)$$

$|\vartheta\rangle$ is Haar-random



Pseudorandom States (PRSs)

- Where do PRSs fit in the complexity landscape?

2018: Zhengfeng Ji, Yi-Kai Liu, Fang Song defined PRS as quantum analogue of PRGs.

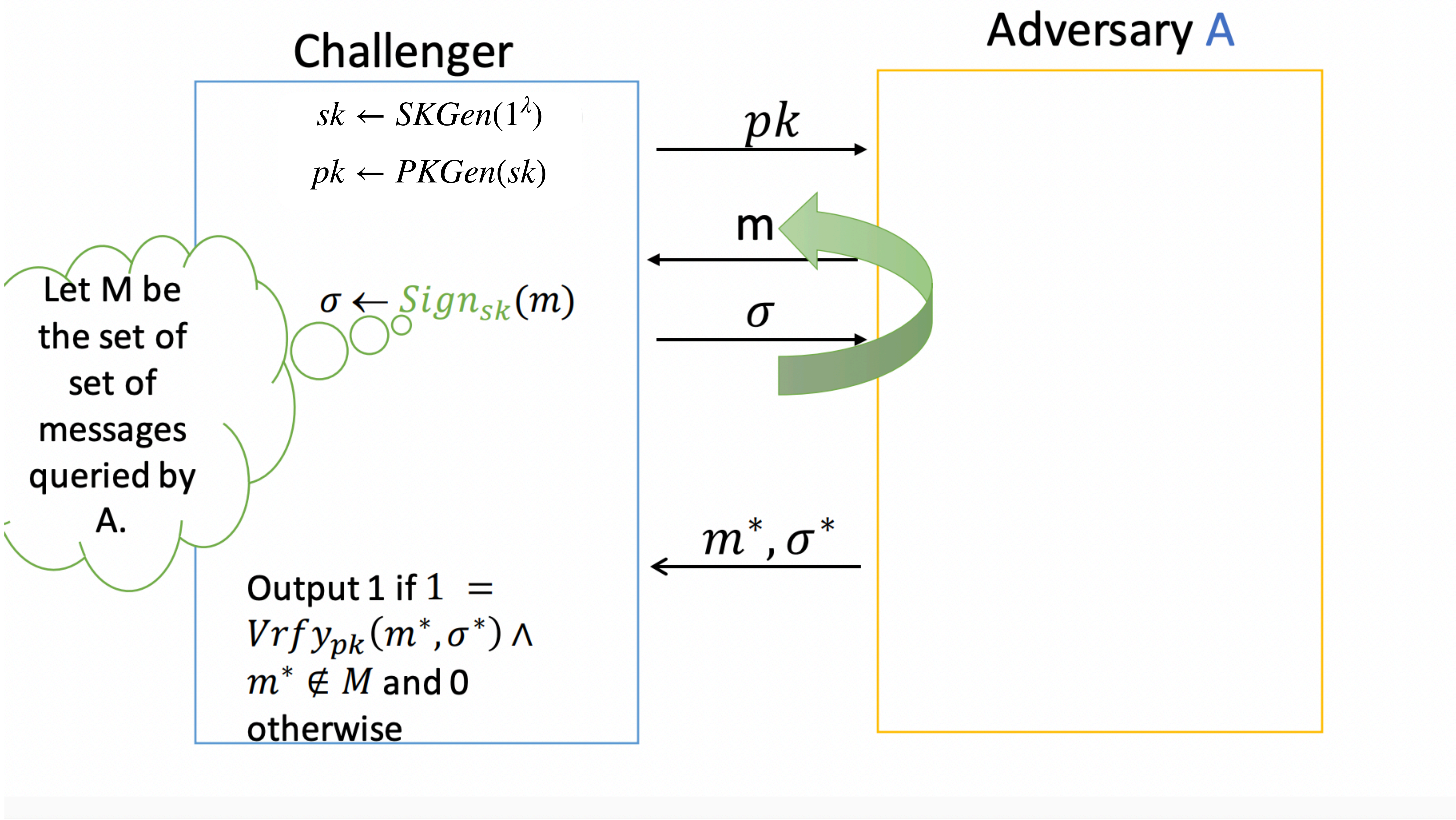
Construction: PRS can be constructed from quantum secure one-way functions (OWFs).

2021: William Kretschmer showed OWFs ***cannot*** be constructed from PRS
in a black-box way.

PRS $\rightarrow$???

Classical Digital Signatures (DS)

Unforgeability security game between adversary A and challenger C.



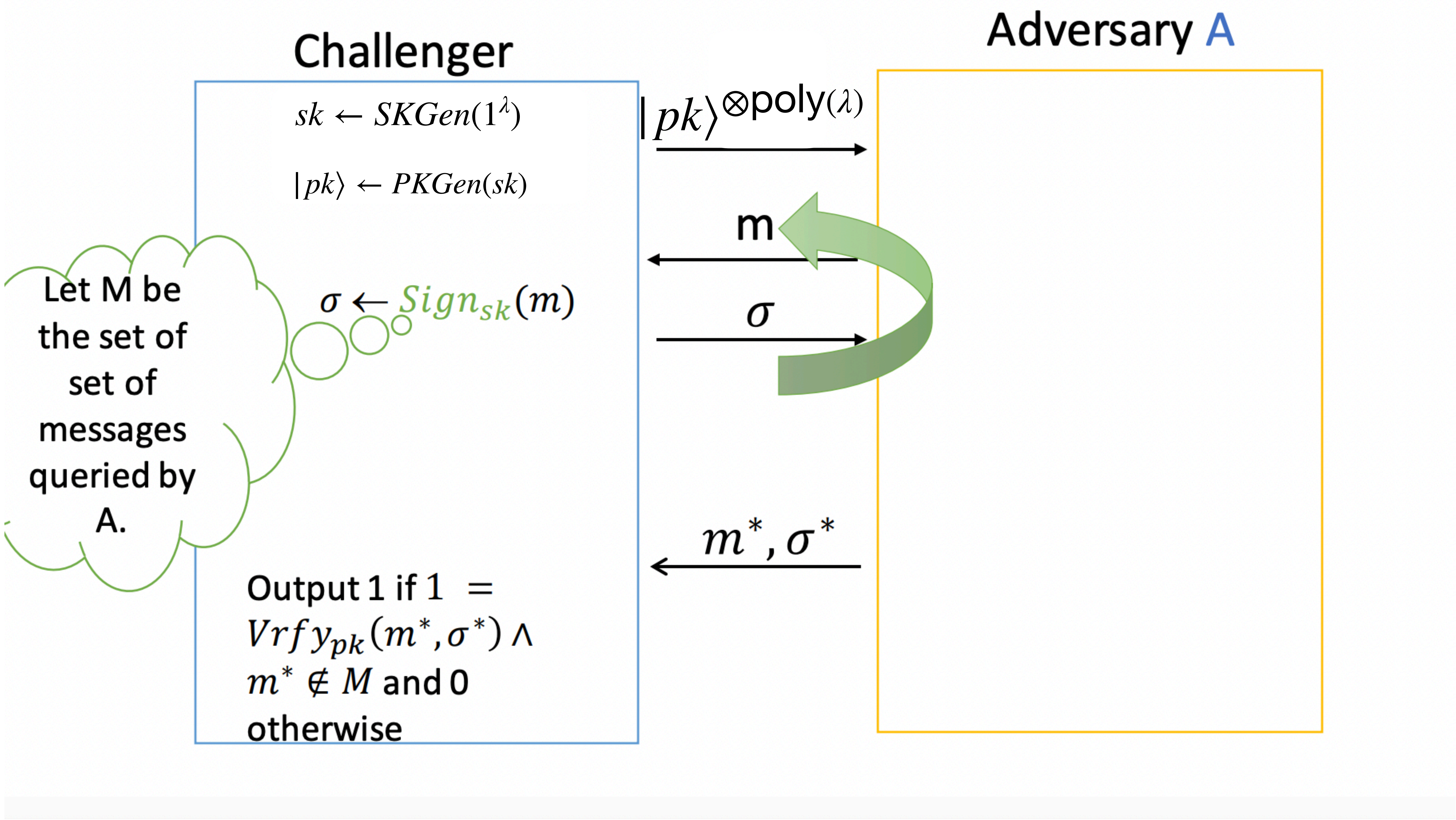
Quantum Public Key Digital Signatures

Tuple of algorithms (Skgen, Pkgen, Sign, Verify):

- SKgen$(1^\lambda) \rightarrow$ sk: QPT algorithm for generating the secret key.
- PKgen$(sk) \rightarrow |pk\rangle$: deterministic QPT algorithm for generating the quantum public key.
- Sign$(m, sk) \rightarrow \sigma$: QPT algorithm for signing a classical message, to produce a classical signature.
- Verify $(m, \sigma, |pk\rangle) \rightarrow 0/1$: QPT algorithm that takes as input a message, a candidate signature, $|pk\rangle$, and outputs accept/reject.

Prior Work

PRS→ One time secure QDS scheme with quantum public keys. (MY22a)



Main Result

There exists a quantum oracle $\mathcal{O}$ such that:

- **PRSs exist relative to $\mathcal{O}$.**
- **No multi-time secure QDS scheme exists relative to $\mathcal{O}$.**

Main Result

There exists a quantum oracle $\mathcal{O}$ such that:

- **PRSs exist relative to $\mathcal{O}$.**
- **No multi-time secure QDS scheme exists relative to $\mathcal{O}$.**

There does not exist a fully black box construction of multi-time secure quantum digital signature (QDS) schemes from pseudo-random states (PRS).

Oracle $\mathcal{O}$

$$\mathcal{O} = (\mathcal{U}, Q)$$

- $\mathcal{U}$: Collection of haar random unitaries $\{\mathcal{U}_\ell\}_{\ell \in \mathbb{N}}$, where each $\mathcal{U}_\ell$ is an indexed list of 2^ℓ haar random unitaries acting on ℓ qubits.
- Q: classical oracle for a fixed EXP complete problem.

QDS schemes do not exist relative to $(\mathscr{U}, \mathscr{Q})$

An Adversary A breaking any QDS scheme relative to $\mathscr{O}$.

- How can A use $\mathscr{Q}$?

QDS schemes do not exist relative to $(\mathscr{U}, \mathscr{Q})$

An Adversary A breaking any QDS scheme relative to $\mathscr{O}$.

- How can A use $\mathscr{Q}$?

A uses $\mathscr{Q}$ to perform a *brute-force* search for a secret key sk such that, signatures generated using sk pass the verification procedure with the public key $|pk\rangle_{sk^*}$.

Simulating queries to $\mathscr{U}$

Informal statement:

Let C be a quantum circuit making poly(λ) queries to a haar random unitary U on λ qubits.

Then, w.h.p. over sampling two such Haar random unitaries U and U', for a given input $|x\rangle$,

$$|\Pr[C^U(|x\rangle) = 1] - \Pr[C^{U'}(|x\rangle) = 1]| \leq \text{negl}(\lambda)$$

Simulating queries to $\mathscr{U}$

Informal statement:

Let C be a quantum circuit making poly(λ) queries to a haar random unitary U on λ qubits.

Then, w.h.p. over sampling two such Haar random unitaries U and U', for a given input $|x\rangle$,

$$|\Pr[C^U(|x\rangle) = 1] - \Pr[C^{U'}(|x\rangle) = 1]| \leq \text{negl}(\lambda)$$

This concentration bound is strong enough to support a union bound over *all standard basis inputs* $|x\rangle$.

Simulating queries to $\mathscr{U}$

In our setting $C = \text{Verify}^{\mathscr{Q}}(\text{PKGen}^{\mathscr{Q}}(\,.\,), m, .\,)$, for some message m, which makes T queries to $\mathscr{U}$.

$\mathscr{Q}$ can perform brute force search over secret keys sk, by replacing oracle calls to $\mathscr{U}$ with unitary T designs.

Using A's queries to C

- A makes polynomially many queries to the signing oracle, obtaining message-signature pairs (m_i, σ_i).

Using A's queries to C

- A makes polynomially many queries to the signing oracle, obtaining message-signature pairs (m_i, σ_i).
- $\mathcal{Q}$ runs an iterative brute force attack which depends on (m_i, σ_i), identifying a shrinking the set of "candidate" secret keys.

Using A's queries to C

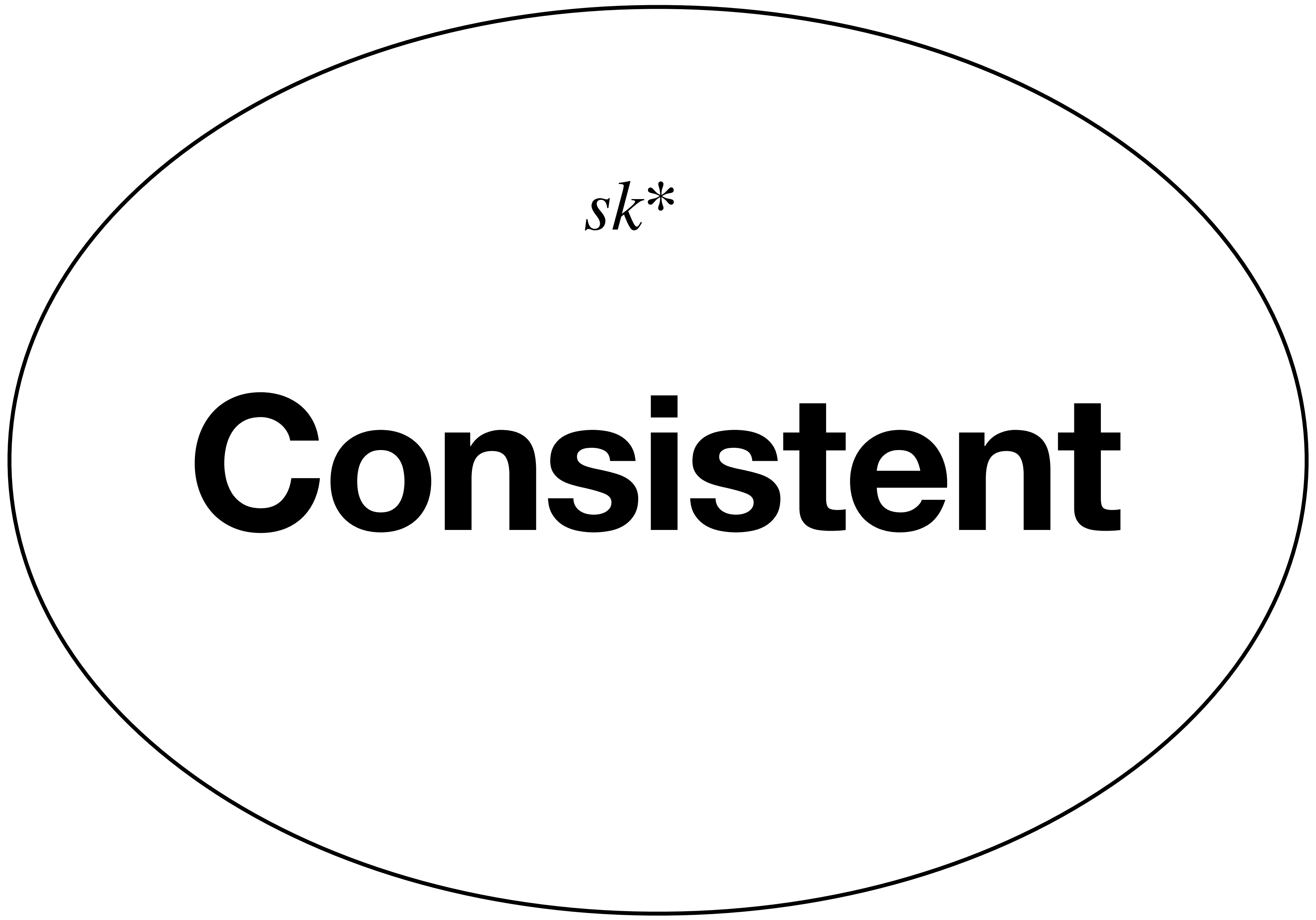
- A makes polynomially many queries to the signing oracle, obtaining message-signature pairs (m_i, σ_i).
- $\mathcal{Q}$ runs an iterative brute force attack which depends on (m_i, σ_i), identifying a shrinking the set of "candidate" secret keys.
- $\mathcal{Q}$ samples a secret key from the set of candidate secret keys.

Iterative brute force attack

- $\mathcal{Q}$ generates the set Consistent.

- $sk \in$ Consistent if

  $\forall i, \Pr[Verify^{\mathcal{U}',\mathcal{Q}}(PKGen^{\mathcal{U}',\mathcal{Q}}(sk), m_i, \sigma_i) = 1] \geq \frac{9}{10}$ where $\sigma_i =$ $\mathrm{Sign}^{\mathcal{U},\mathcal{Q}}(sk^*, m_i)$.

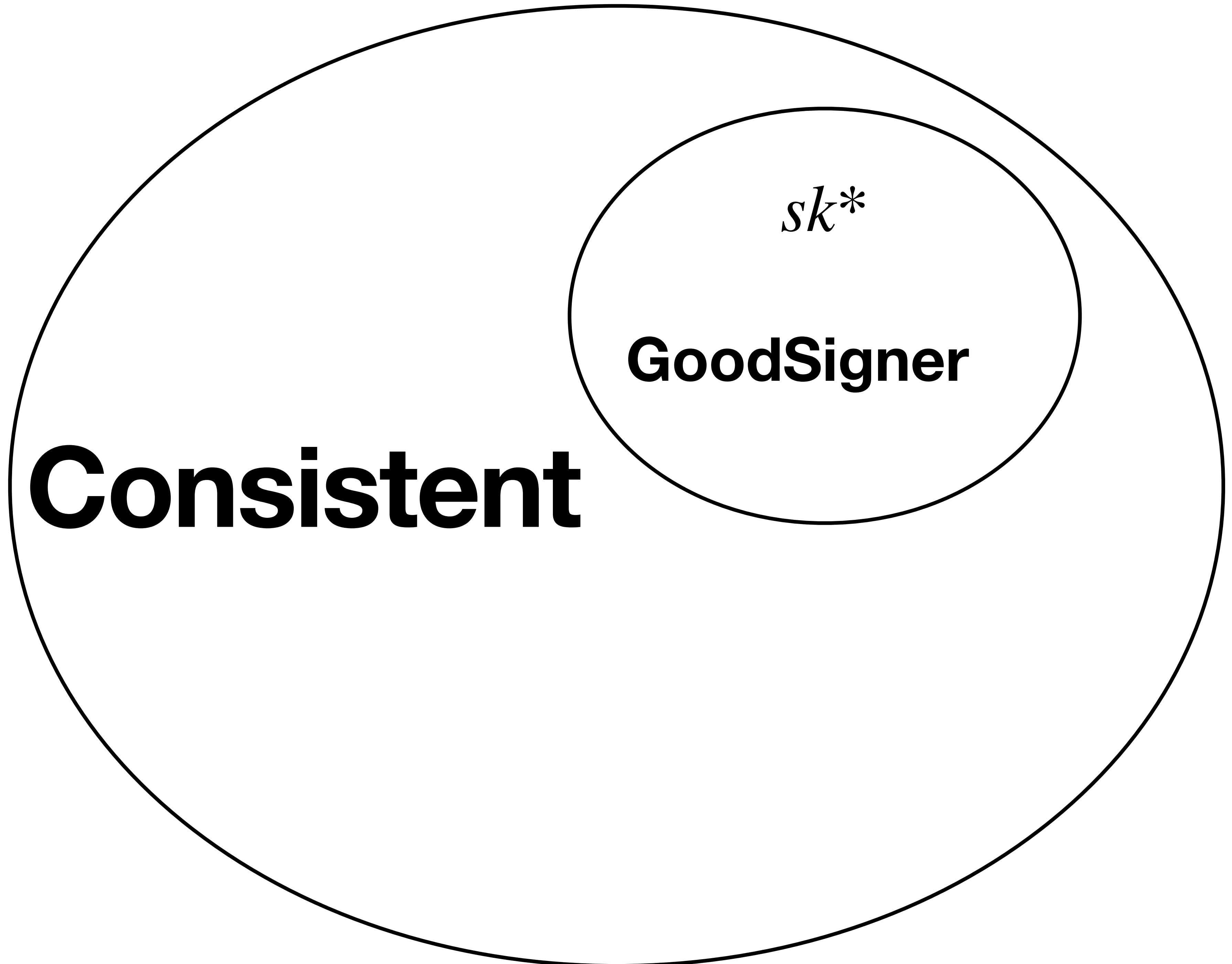


Iterative procedure to find a good signer sk

Q generates the set Goodsigner.

- $sk \in$ Goodsigner if most $sk' \in$ Consistent accept most signatures generated by sk.

  $|accept_{sk}| \geq \frac{9}{10}|Consistent|$, where $accept_{sk} = \{sk' : |m : Verify(PKgen(sk'), m, Sign(sk, m))| \geq \frac{1}{8}\}$

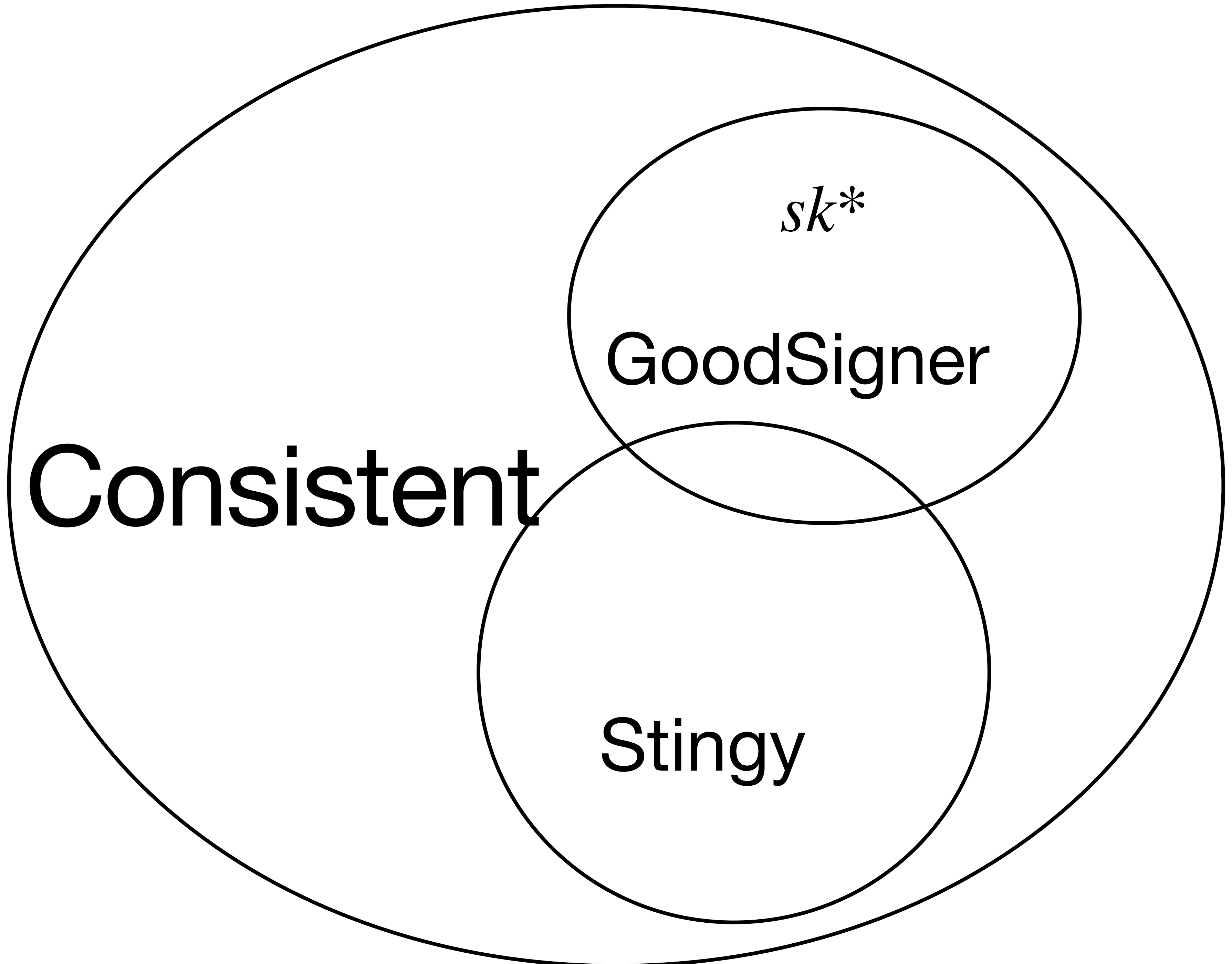


Iterative procedure to find a good signer sk

Q generates the set Stingy.

- $sk \in$ Stingy if it does not accept most signatures generated by most $sk' \in$ Consistent.

$$|friends_{sk}| \leq \frac{1}{2}|Consistent|, \text{ where } friends_{sk} = \{sk' : sk \in accept_{sk'}\}$$

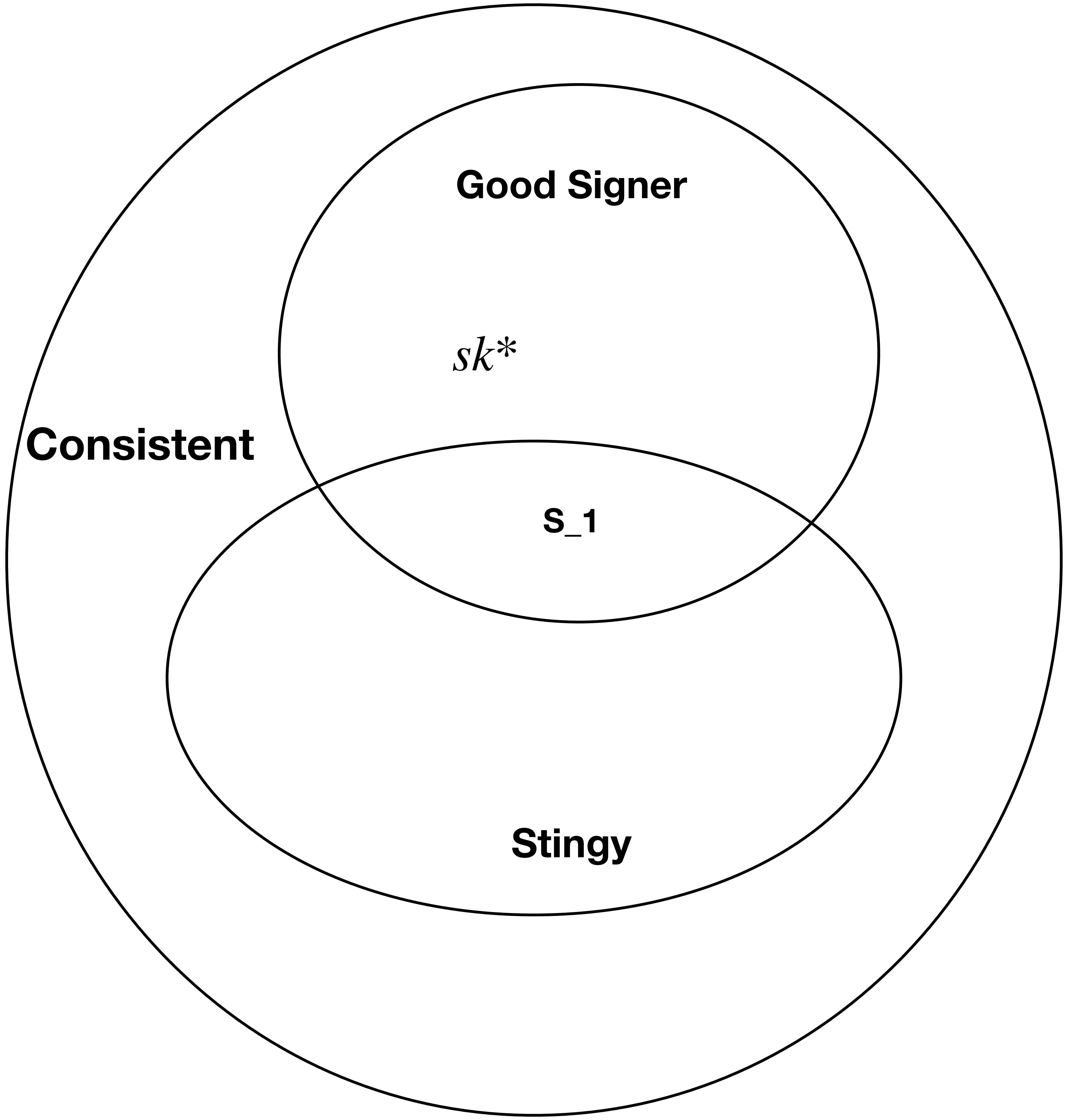


Iterative procedure to find a good signer sk

Q generates the set Stingy.

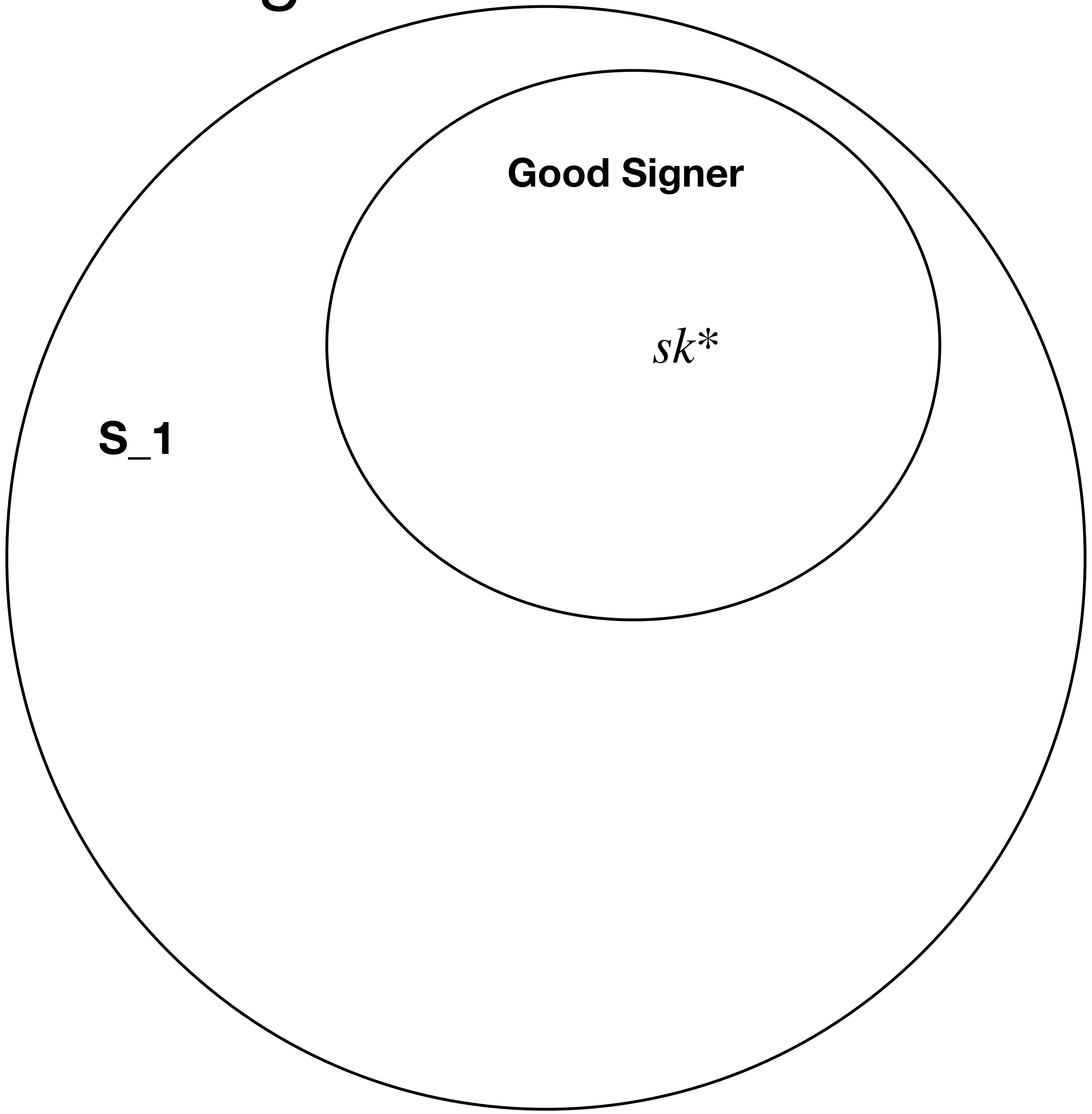
Q samples a key sk from S_1.

Candidates $= sk \cup$ Candidates



Iterative procedure to find a good signer sk

$\mathcal{Q}$ generates the set GoodSigner.

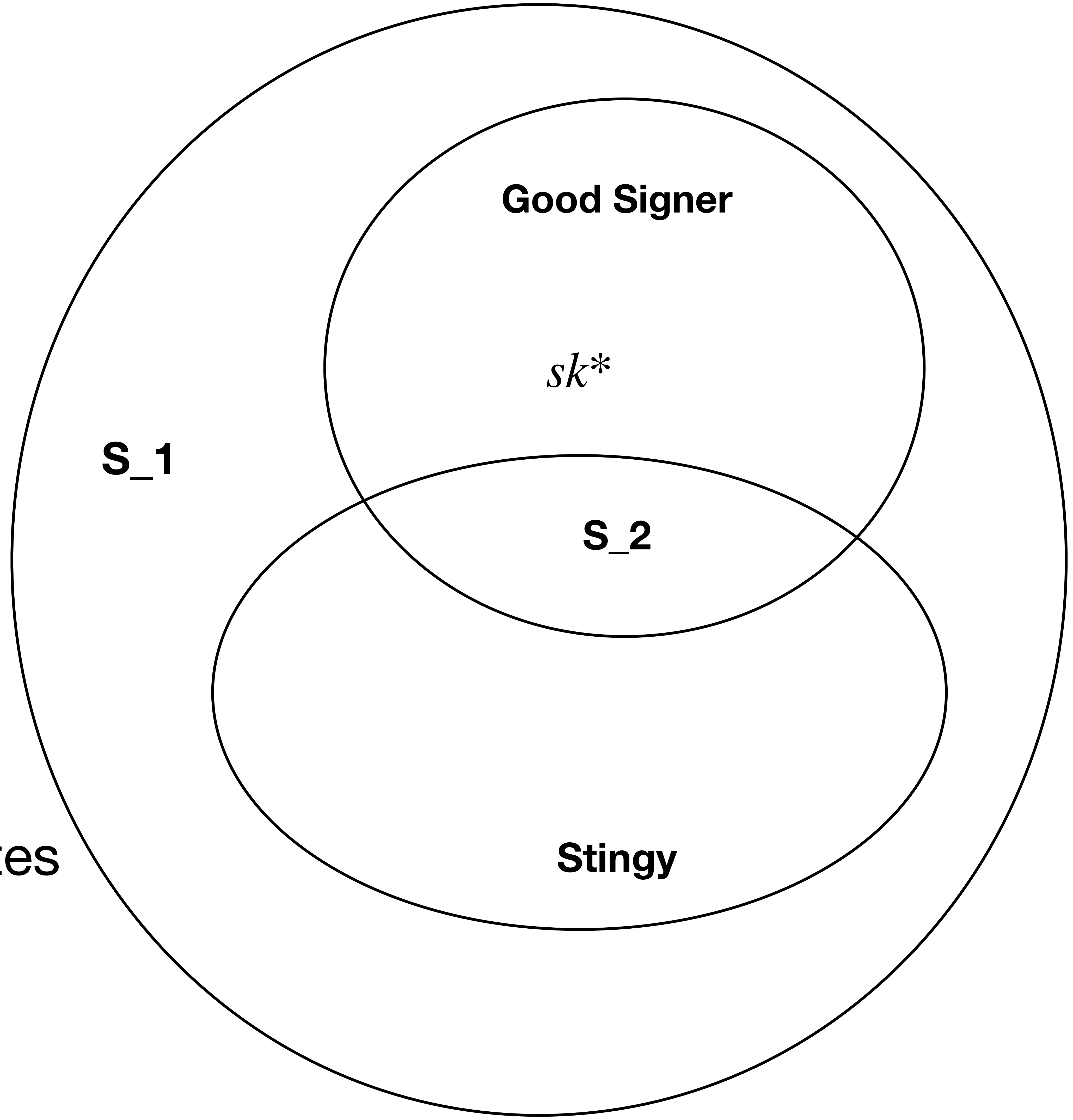


Iterative procedure to find a good signer sk

Q generates the set Stingy.

Q samples a key sk from S_2.

Candidates $= sk \cup$ candidates



PRSs exist relative to $\mathscr{O}$

On input key k, sample a unitary from $\mathscr{U}_{|k|}$, and apply it to $|0\rangle^{\otimes |k|}$.

PRSs exist relative to $\mathcal{O}$

On input key k, sample a unitary from $\mathcal{U}_{|k|}$, and apply it to $|0\rangle^{\otimes |k|}$.

Security proof sketch:

Want to show that, for all QPT $A^{(.),\mathcal{U}}$, $\exists$negl such that,

$$\left| \Pr_{k \leftarrow [2^\lambda]} [A^{\mathcal{U}_k, \mathcal{U}_1, \ldots \mathcal{U}_{2^\lambda}}(1^\lambda) = 1] - \Pr_{W \leftarrow \mu_{2n(\lambda)}} [[A^{W, \mathcal{U}_1, \ldots \mathcal{U}_{2^\lambda}}(1^\lambda) = 1]\right| \leq \text{negl}(\lambda)$$

PRSs exist relative to $\mathcal{O}$

Main Idea:

Reduce PRS distinguishing task to a black box Grover search problem.

Construct an algorithm B such that,

$$|\mathbb{E}_{k \leftarrow [2^\lambda]}[\Pr[B^{e_k} = 1]] - \Pr[B^{0^{2^\lambda}} = 1]| = \mathrm{adv}(A)$$

Open Questions

- Result only applies to digital signatures with a quantum public key, but with classical secret key and signatures. If we allow the latter to be quantum as well, then is there a construction?