Cloning Games, Black Holes, and Cryptography

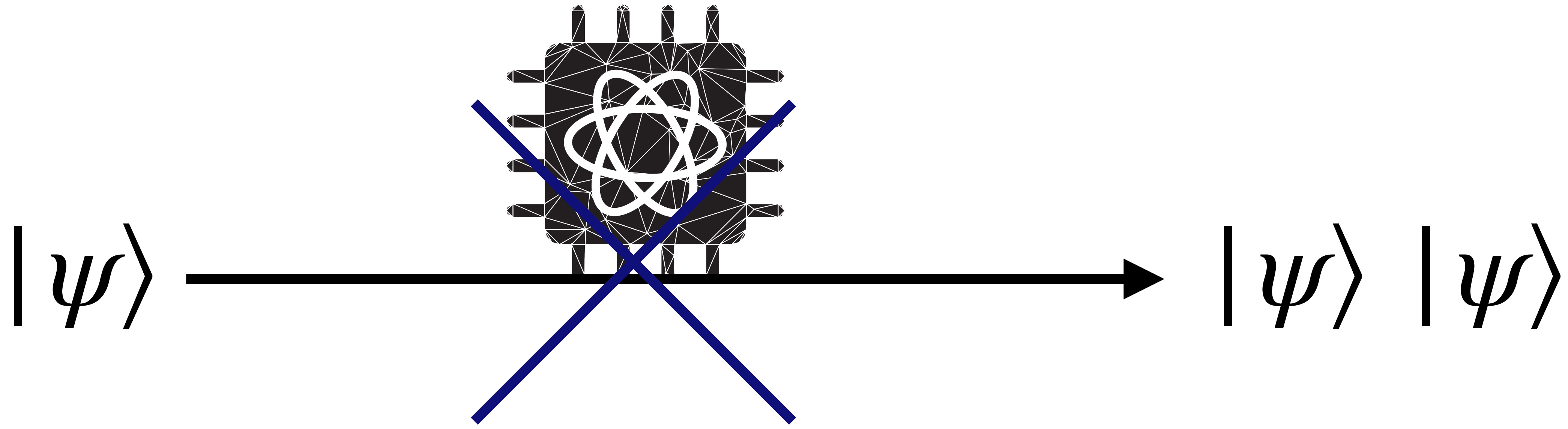
Alexander Poremba, Seyoon Ragavan, Vinod Vaikuntanathan
MIT and Boston University



The No-Cloning Theorem

Wootters-Zurek '82

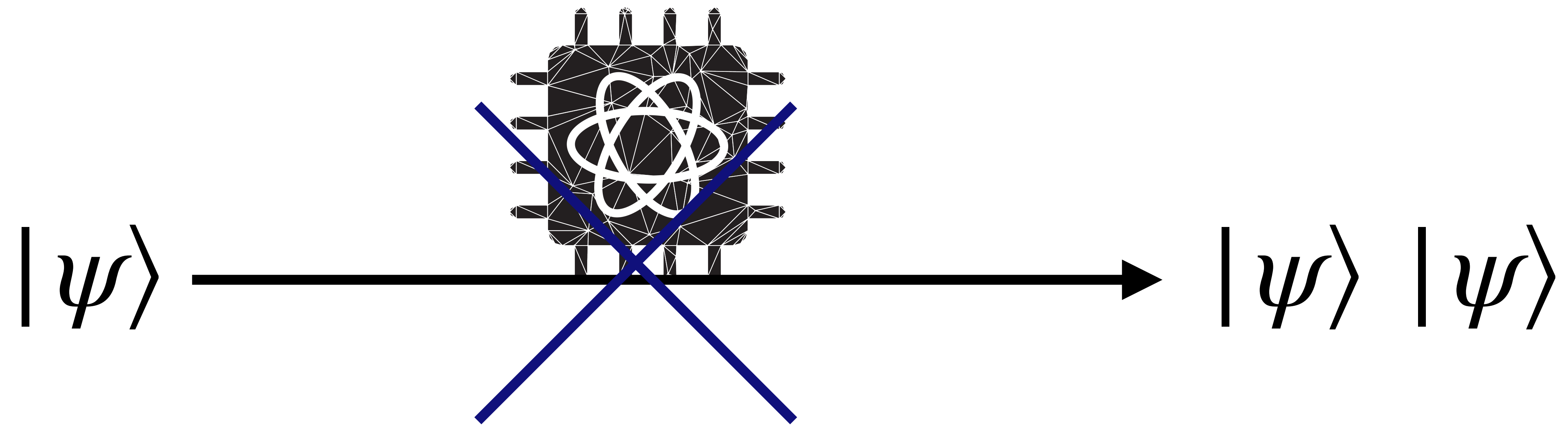
- Informally: quantum information cannot be copied and pasted



The No-Cloning Theorem

Wootters-Zurek '82

- Informally: quantum information cannot be copied and pasted

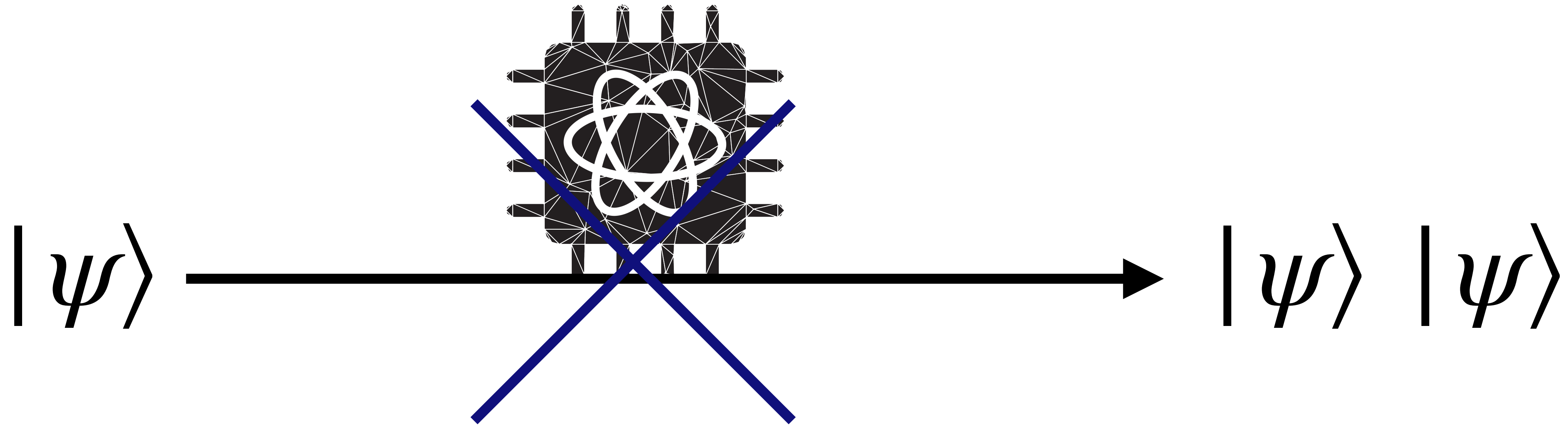


- Robust variant (Werner '98): it is not even possible to generate something close to $|\psi\rangle|\psi\rangle$ (in trace distance)

The No-Cloning Theorem

Wootters-Zurek '82

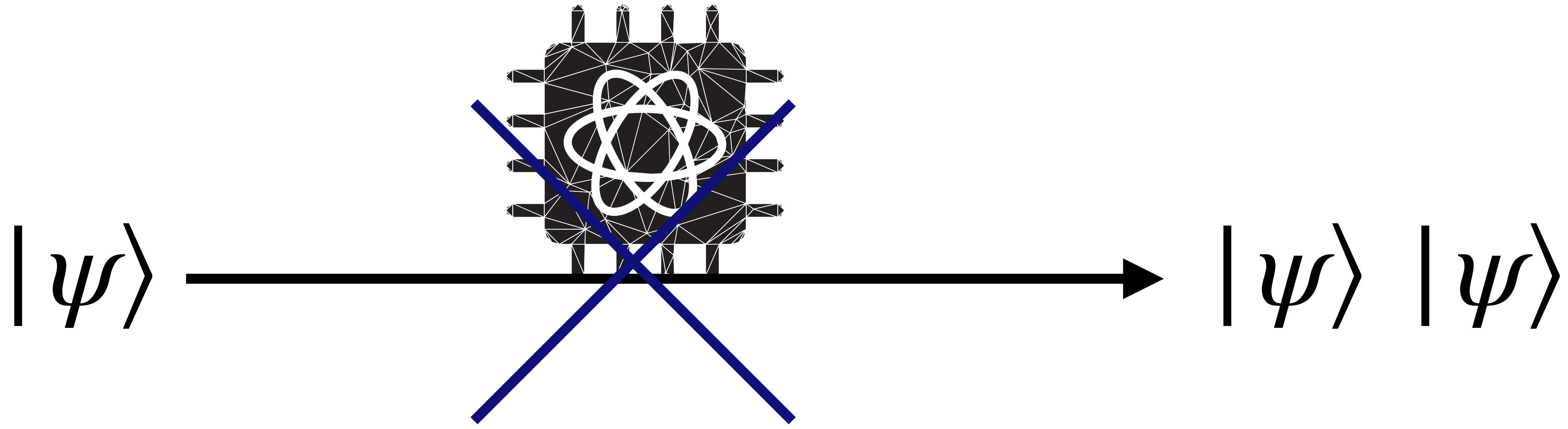
- Informally: quantum information cannot be copied and pasted



- Robust variant (Werner '98): it is not even possible to generate something close to $|\psi\rangle|\psi\rangle$ (in trace distance)
- Provides hope for **unclonable cryptography:** applications where we want to safeguard against duplication of information
    - However, it is rarely sufficient…

Goal: "Useful" No-Cloning Theorems

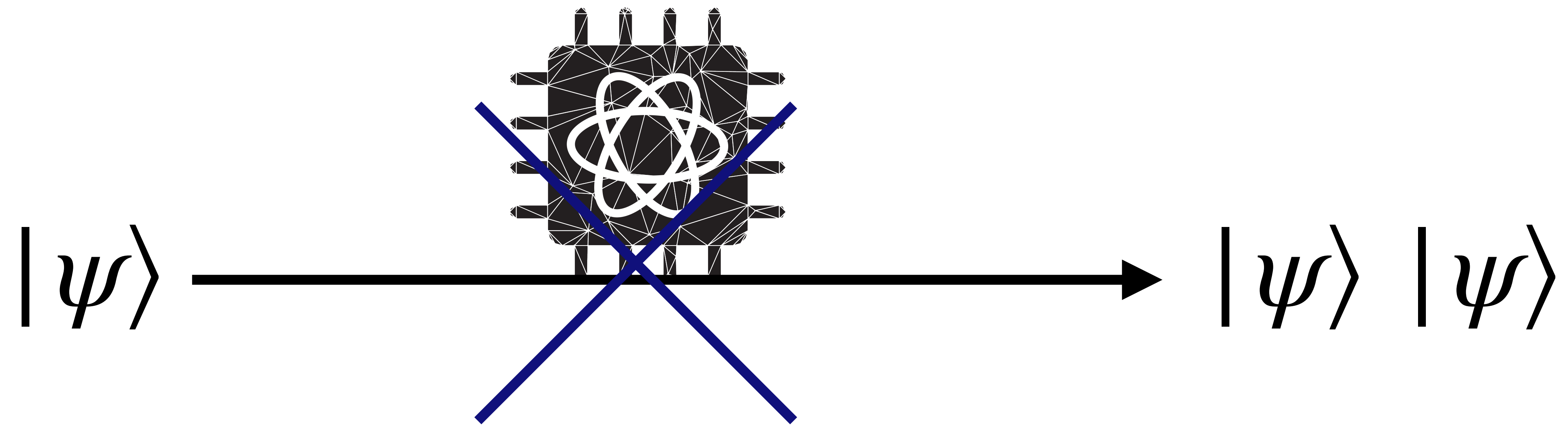
- Informally: quantum information cannot be copied and pasted



- Robust variant (Werner '98): it is not even possible to generate something close to $|\psi\rangle|\psi\rangle$ (in trace distance)
- **"Useful" variant (even stronger than robust):** it is not even possible for both states to have "some property" in common with $|\psi\rangle$

Goal: "Useful" No-Cloning Theorems

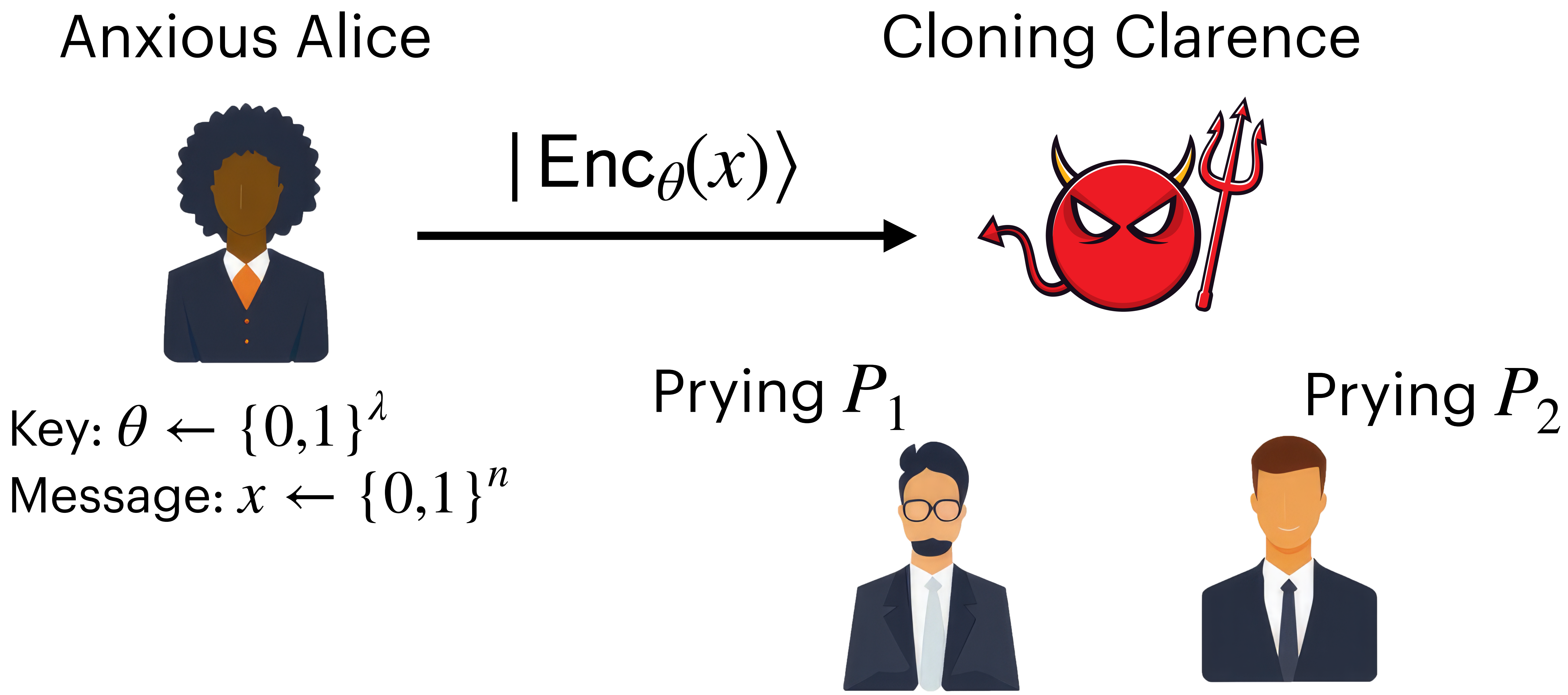
- Informally: quantum information cannot be copied and pasted



- Robust variant (Werner '98): it is not even possible to generate something close to $|\psi\rangle|\psi\rangle$ (in trace distance)
- **"Useful" variant (even stronger than robust):** it is not even possible for both states to have "some property" in common with $|\psi\rangle$
  - "Some property" depends on the particular application

(Search-Secure) Unclonable Encryption

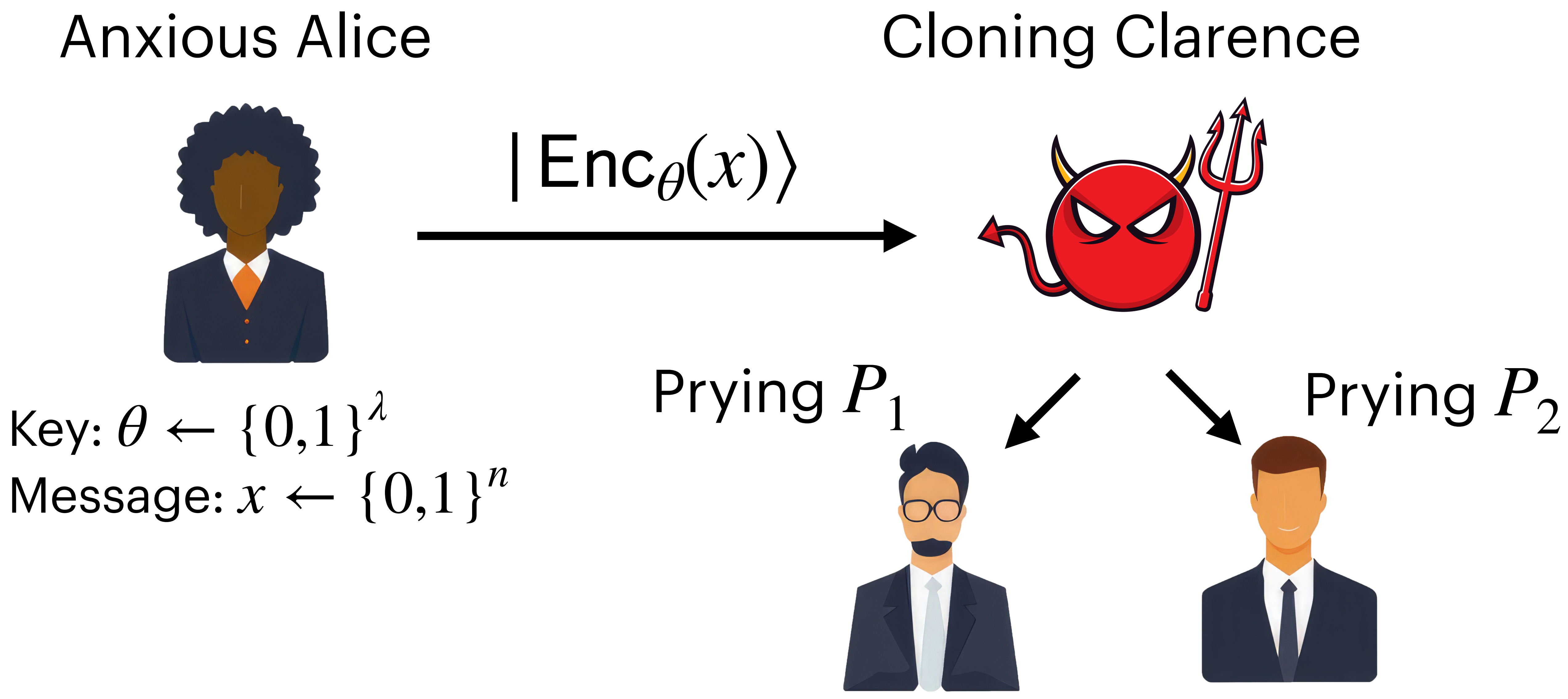
Broadbent and Lord ‘20



1. Alice samples a key θ and sends $|\text{Enc}_\theta(x)\rangle$ to Clarence

(Search-Secure) Unclonable Encryption

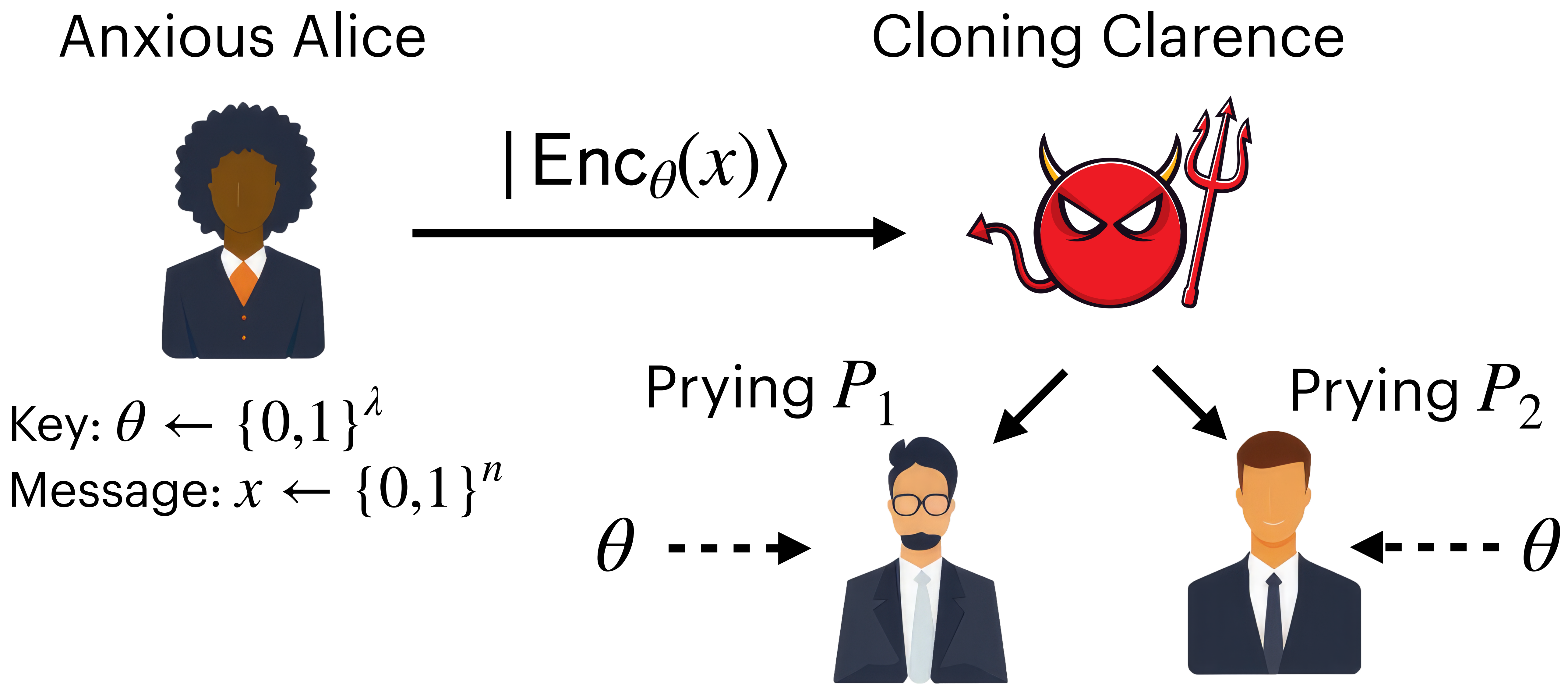
Broadbent and Lord '20



1. Alice samples a key θ and sends $|\mathsf{Enc}_\theta(x)\rangle$ to Clarence
2. Clarence sends some bipartite state to P_1, P_2

(Search-Secure) Unclonable Encryption

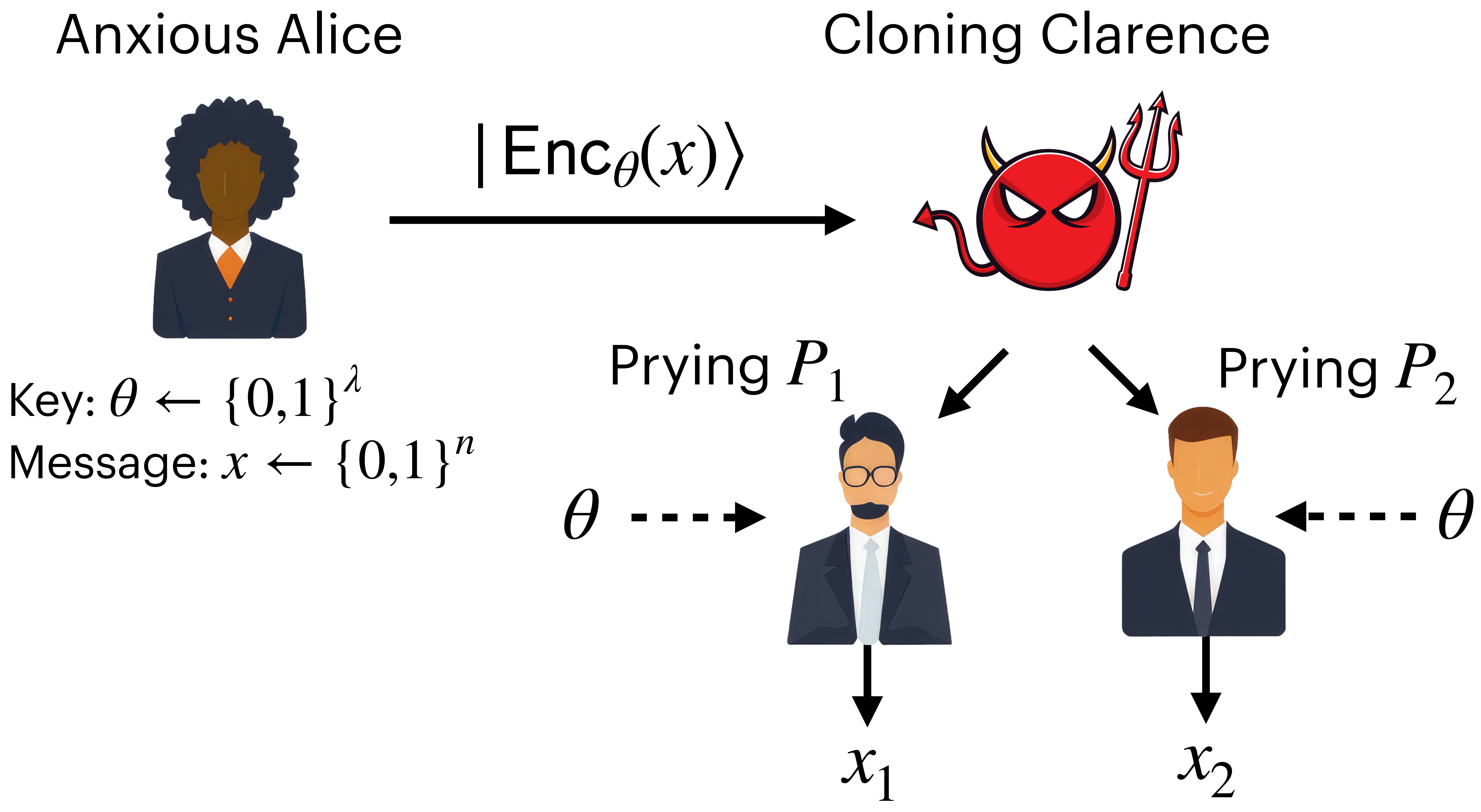
Broadbent and Lord '20



1. Alice samples a key θ and sends $|\mathsf{Enc}_\theta(x)\rangle$ to Clarence
2. Clarence sends some bipartite state to P_1, P_2
3. P_1, P_2 get access to θ

(Search-Secure) Unclonable Encryption

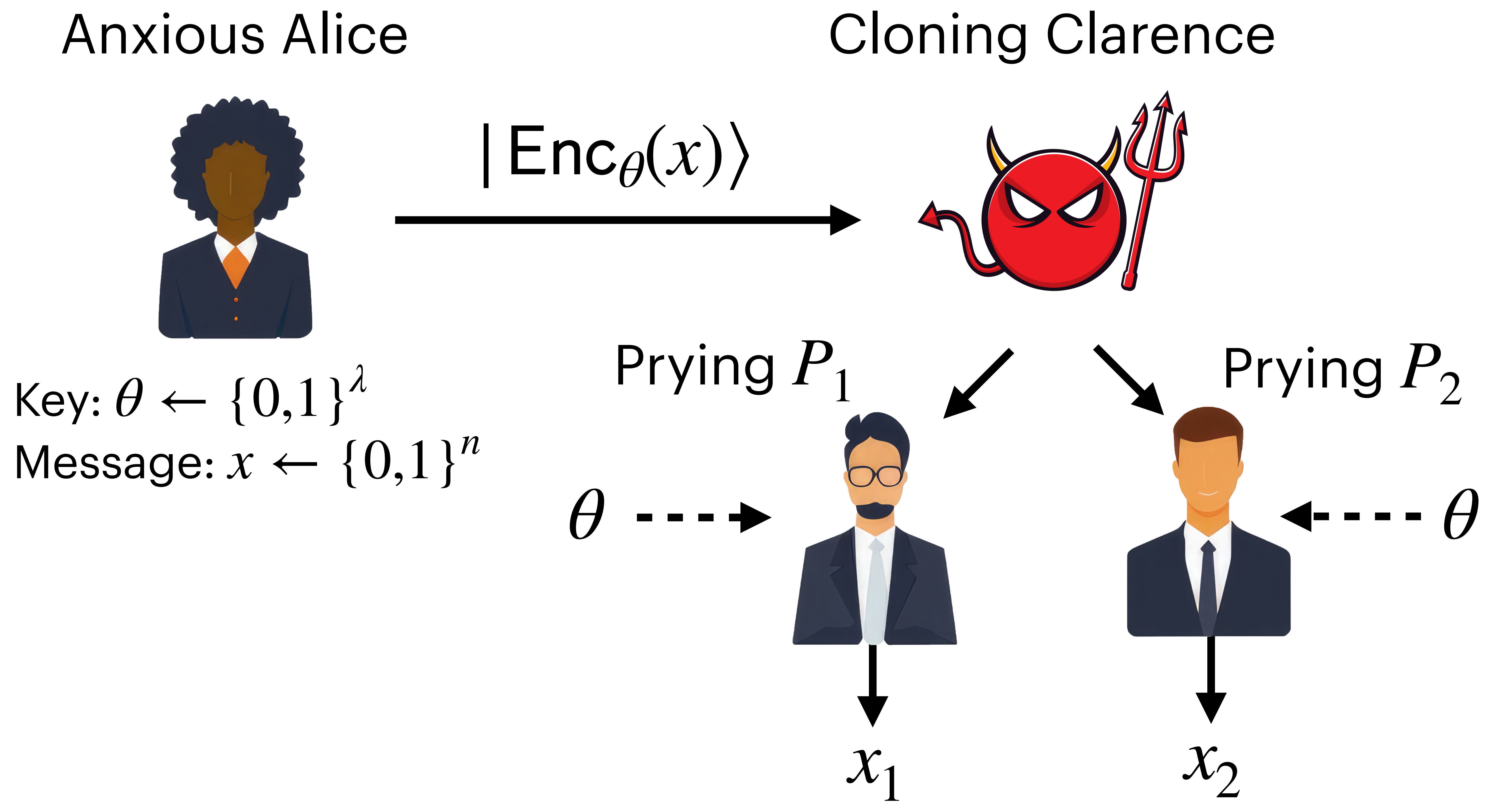
Broadbent and Lord '20



1. Alice samples a key θ and sends $|\mathsf{Enc}_\theta(x)\rangle$ to Clarence
2. Clarence sends some bipartite state to P_1, P_2
3. P_1, P_2 get access to θ
4. They guess x_1, x_2 and win if both guesses are correct ($x_1 = x_2 = x$)

(Search-Secure) Unclonable Encryption

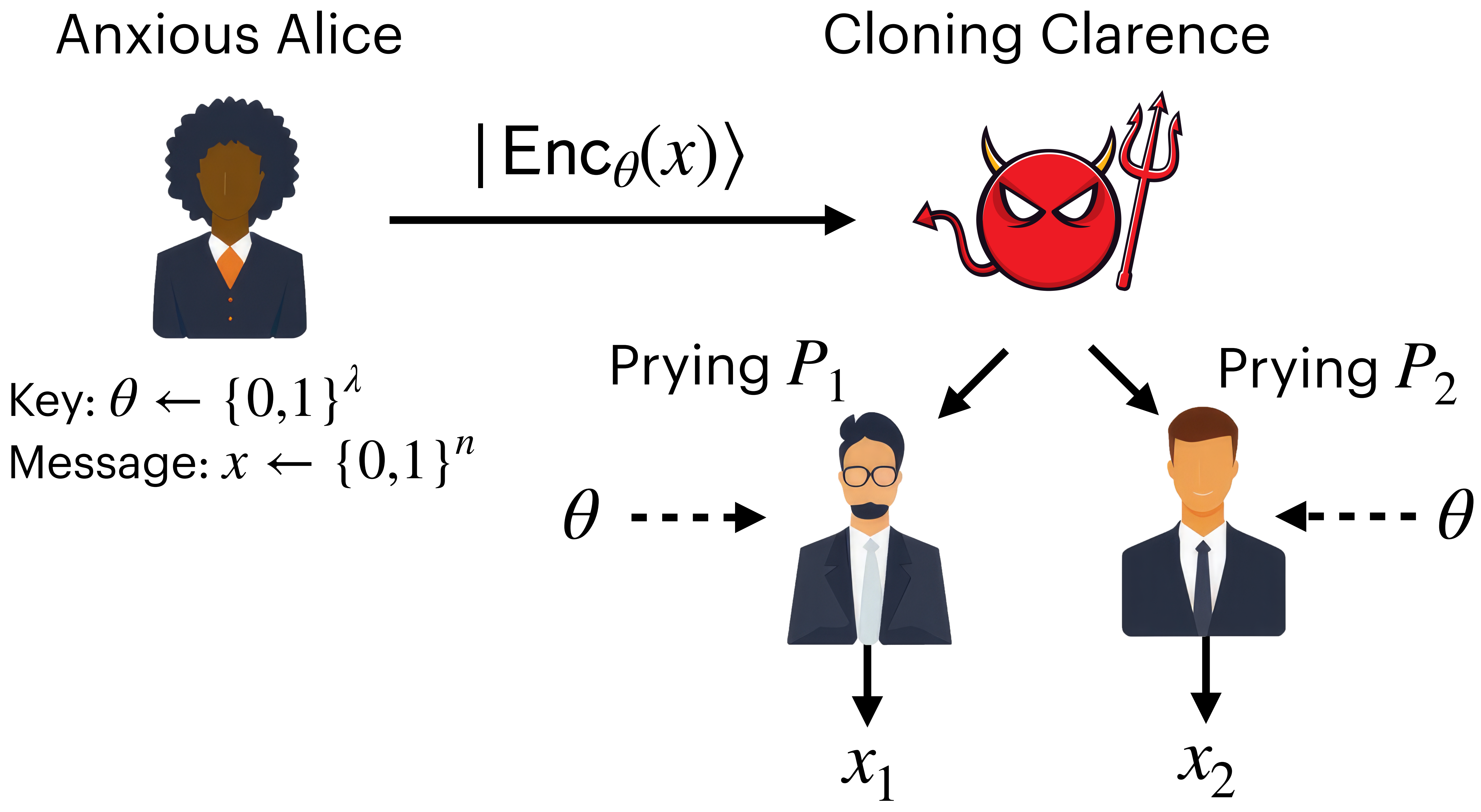
The Need for <u>Useful</u> No-Cloning



- If $|\text{Enc}_\theta(x)\rangle$ is classical (or clonable): Clarence can just clone it and send copies to P_1, P_2!

(Search-Secure) Unclonable Encryption

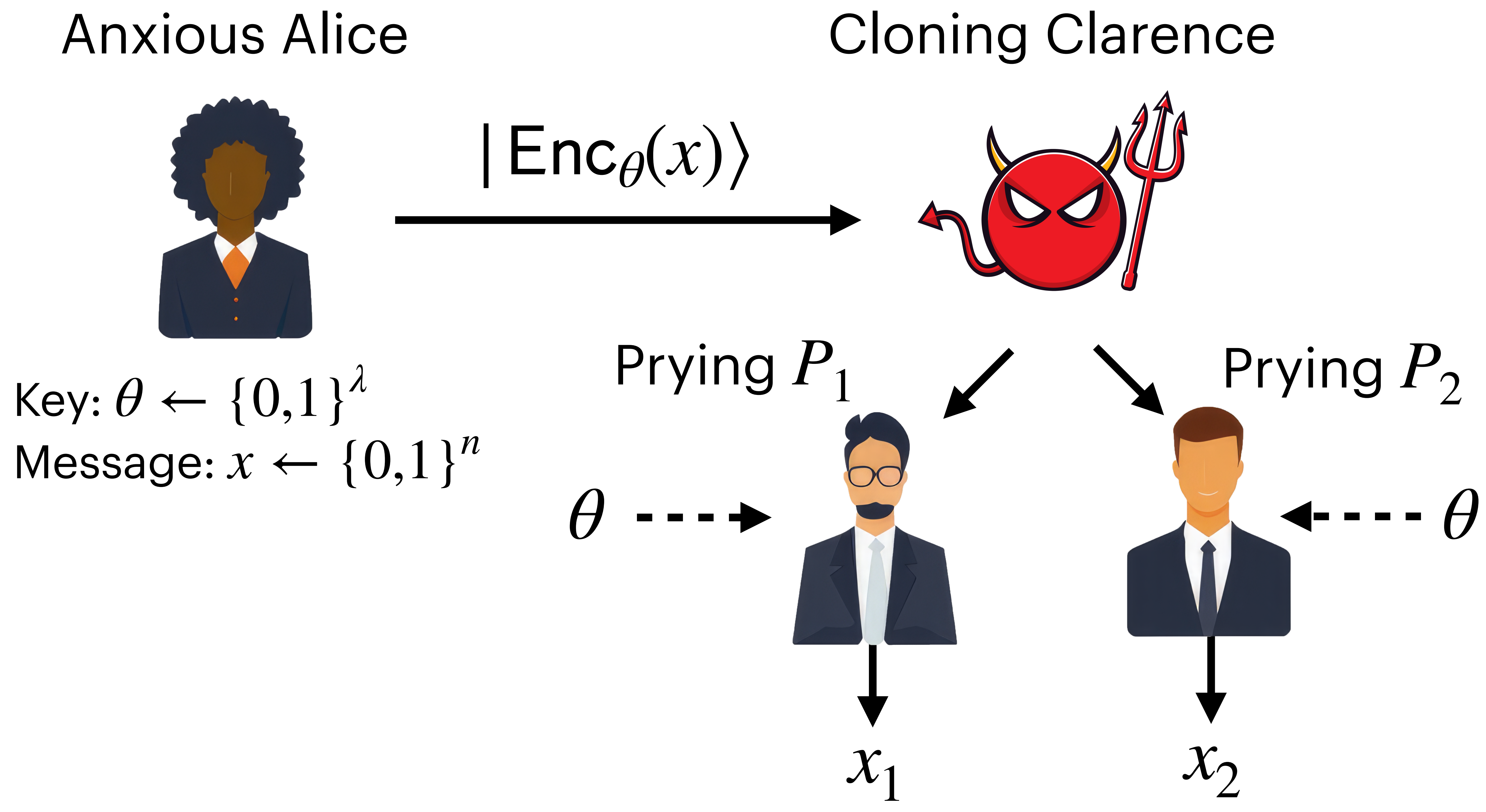
The Need for Useful No-Cloning



- If $|\mathsf{Enc}_\theta(x)\rangle$ is classical (or clonable): Clarence can just clone it and send copies to P_1, P_2!
- Useful no-cloning: Clarence should not be able to produce *any* two states that reveal x (given θ)

Definitions and Our Results

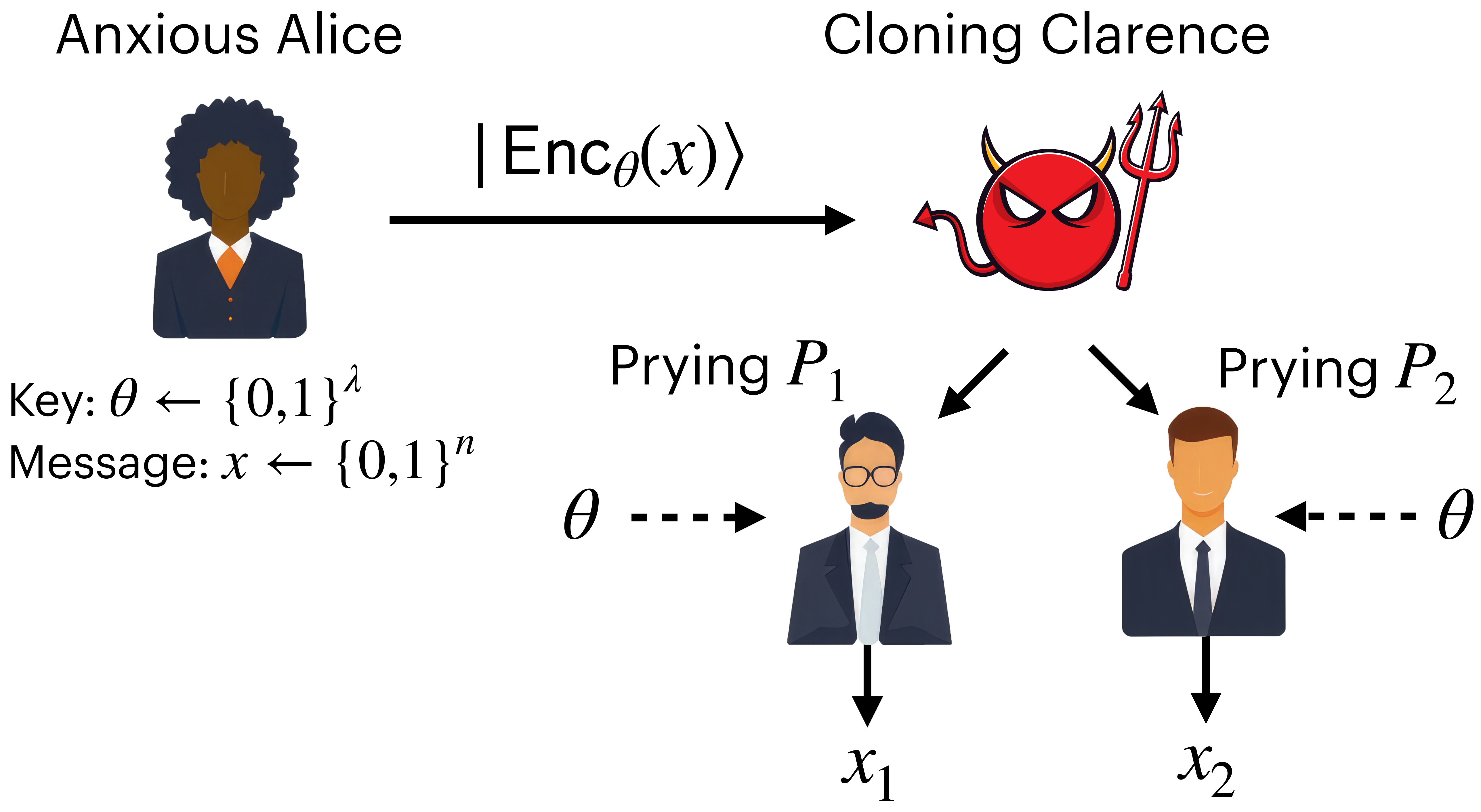
Previous Slides: Search Security



- Value of this game:

$$\omega(G) = \Pr_{\theta \leftarrow \{0,1\}^\lambda, x \leftarrow \{0,1\}^n} \left[x_1 = x_2 = x\right]$$

Previous Slides: Search Security

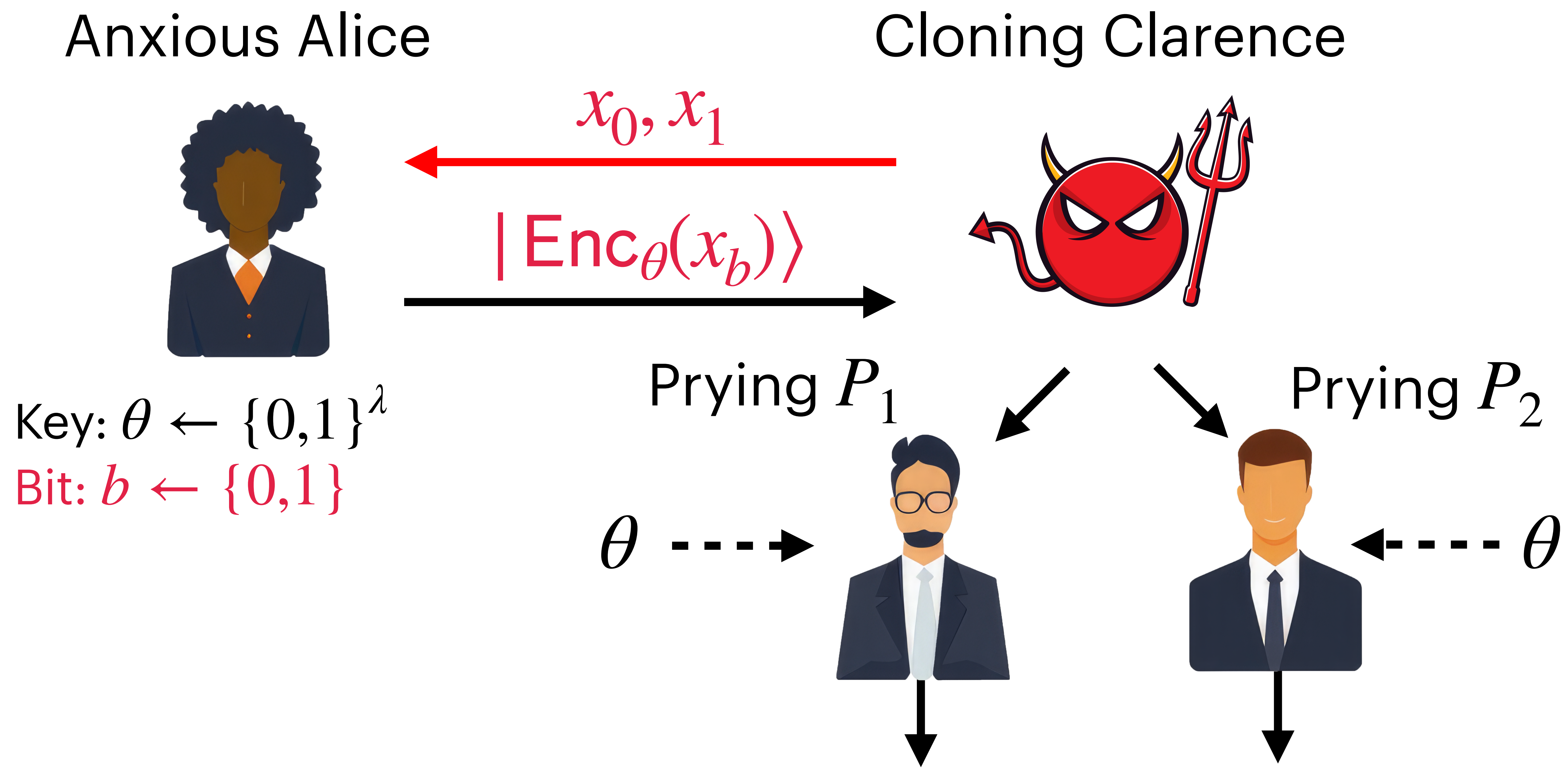


- Value of this game:

$$\omega(G) = \Pr_{\theta \leftarrow \{0,1\}^\lambda, x \leftarrow \{0,1\}^n} \left[x_1 = x_2 = x\right]$$

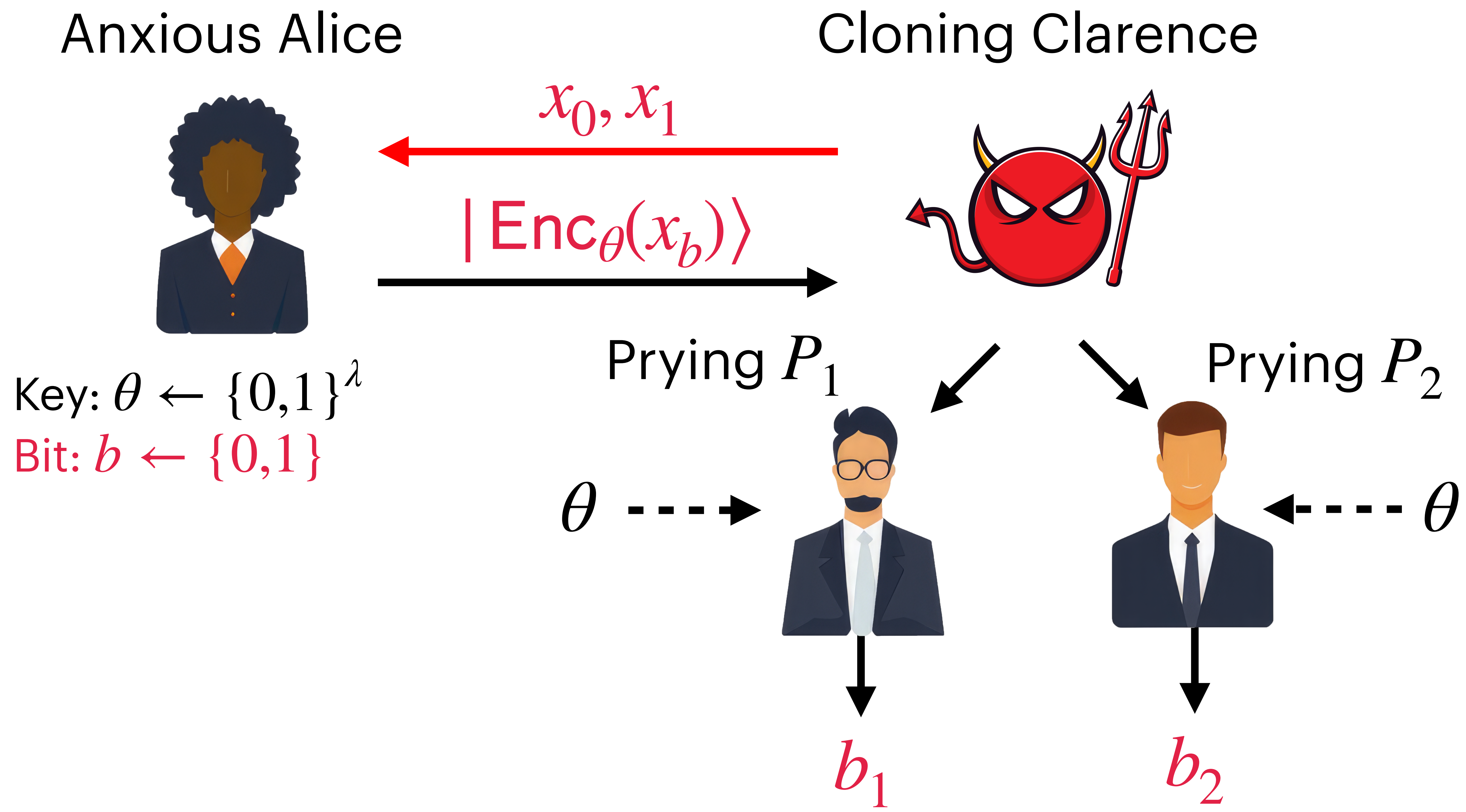
- Search security: want $\omega(G) \leq \mathsf{negl}(\lambda)$

The Ideal Notion: IND-CPA Security



1. Clarence sends two challenge messages $x_0, x_1 \in \{0,1\}^n$ to Alice
2. Alice encrypts one of them at random and sends it to Clarence

The Ideal Notion: IND-CPA Security

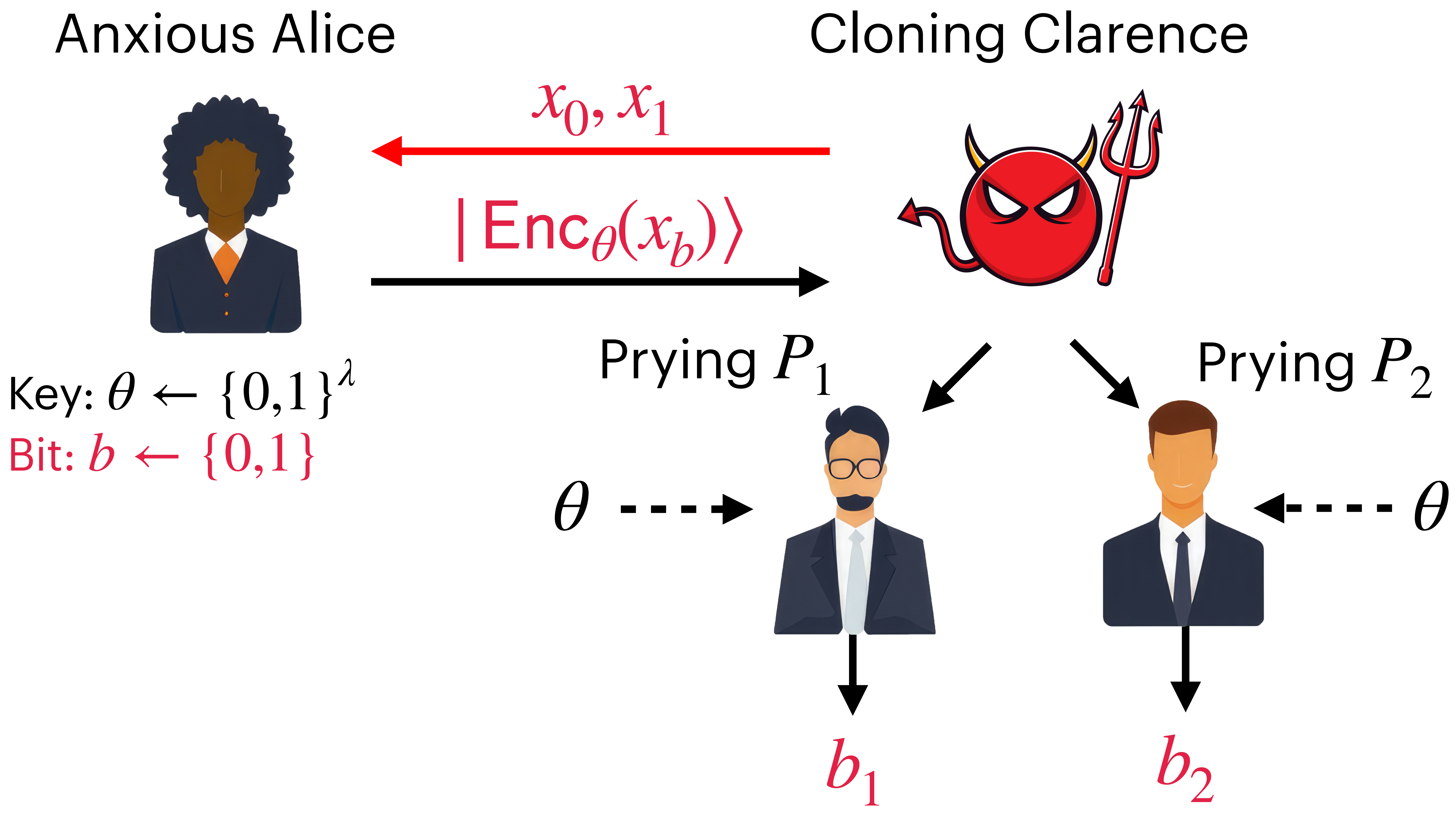


1. Clarence sends two challenge messages $x_0, x_1 \in \{0,1\}^n$ to Alice
2. Alice encrypts one of them at random and sends it to Clarence
3. At the end, P_1, P_2 guess which of the two messages was encrypted
4. IND-CPA security: want

$$\Pr_{\theta \leftarrow \{0,1\}^\lambda, b \leftarrow \{0,1\}} \left[b_1 = b_2 = b \right] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

Plausible Bootstrapping from Search to IND Security

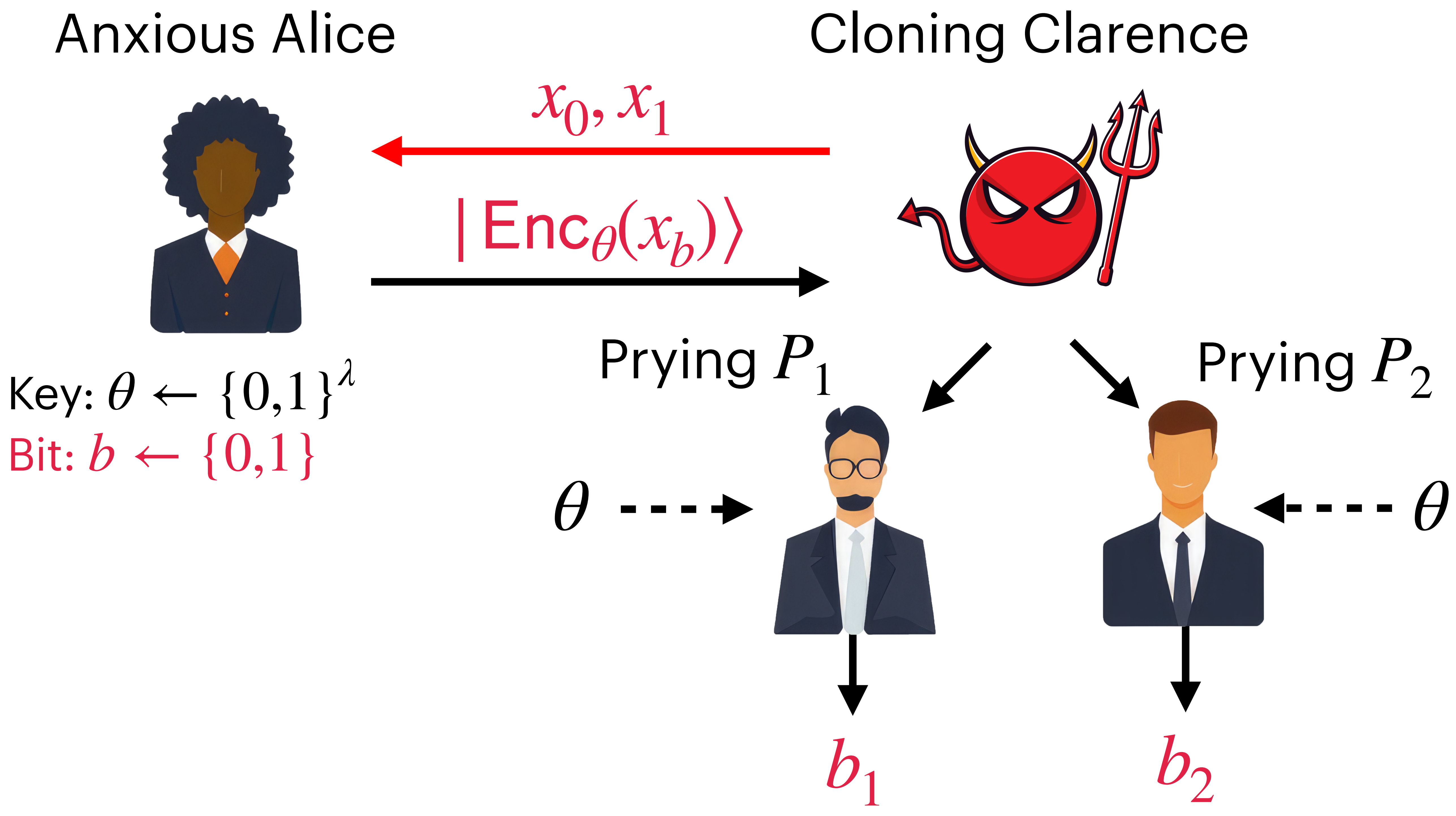
Broadbent and Lord '20



- Assume we have a scheme SearchEnc satisfying search security

Plausible Bootstrapping from Search to IND Security

Broadbent and Lord '20

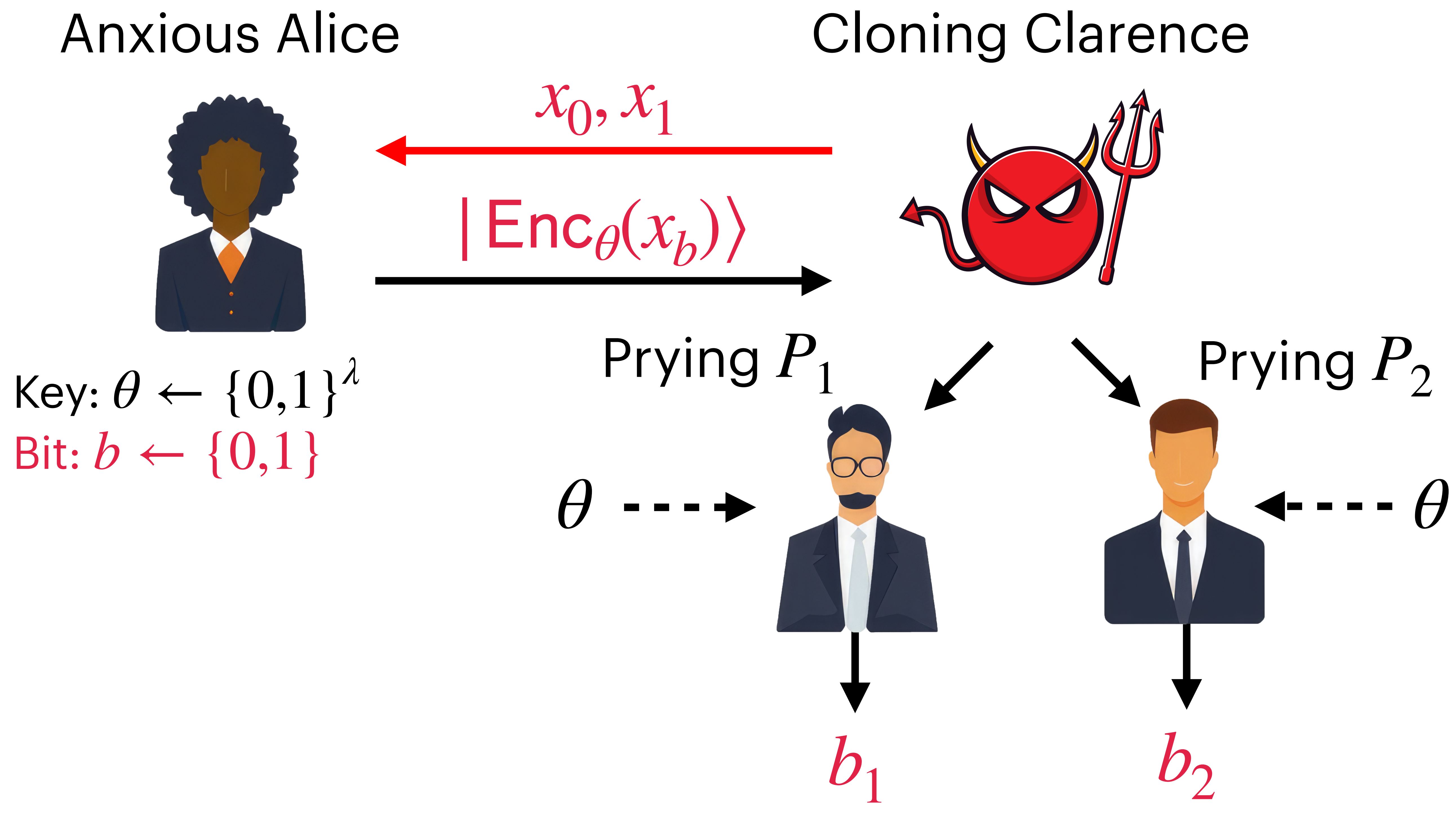


- Assume we have a scheme SearchEnc satisfying search security
- Then let INDEnc_θ sample $r \leftarrow \{0,1\}^n$ and output

$$|\mathsf{INDEnc}_\theta(x)\rangle = (x \oplus \mathsf{PRF}(r), |\mathsf{SearchEnc}_\theta(r)\rangle)$$

Plausible Bootstrapping from Search to IND Security

Broadbent and Lord '20



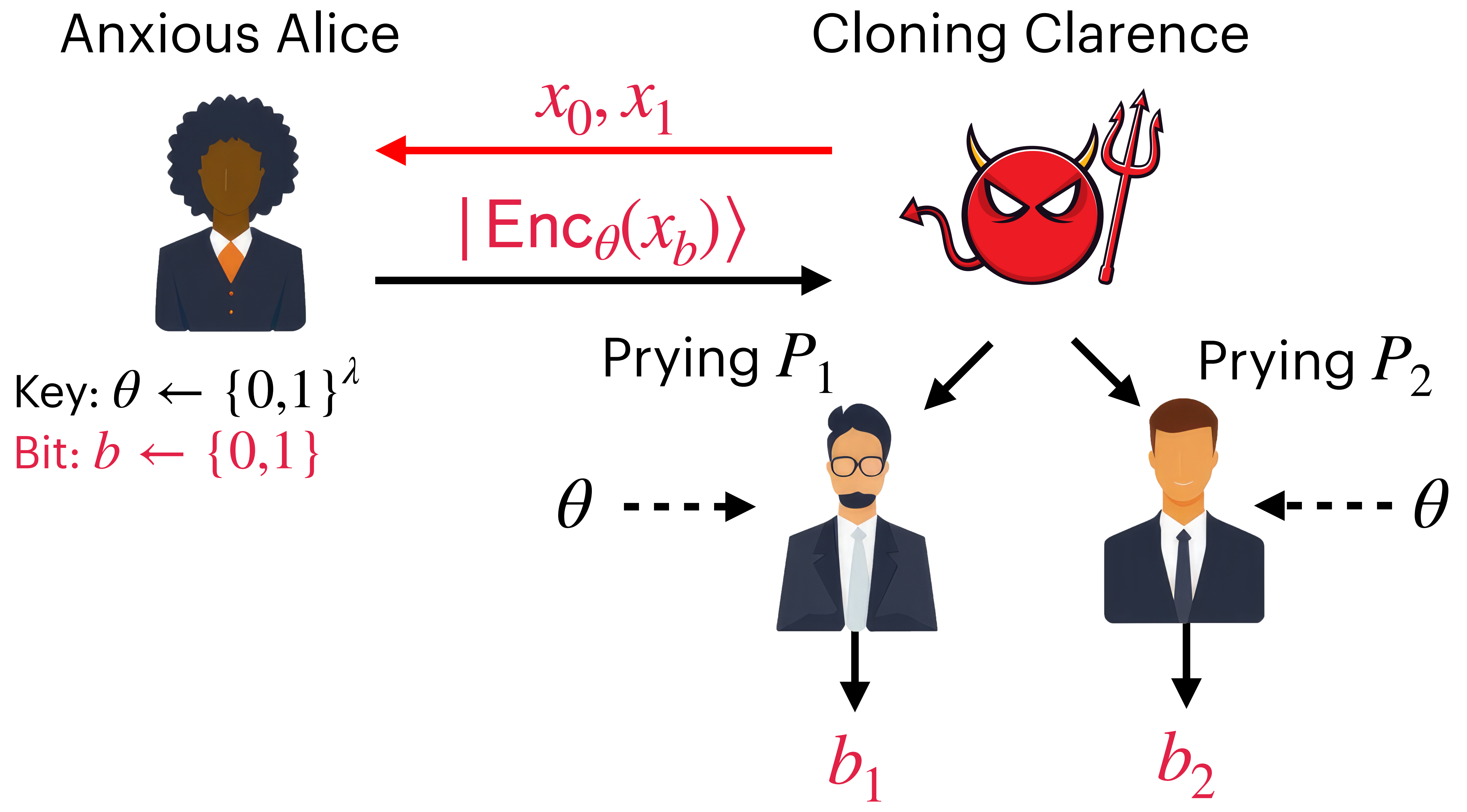
- Assume we have a scheme SearchEnc satisfying search security
- Then let INDEnc_θ sample $r \leftarrow \{0,1\}^n$ and output

$$|\mathsf{INDEnc}_\theta(x)\rangle = (x \oplus \mathsf{PRF}(r), |\mathsf{SearchEnc}_\theta(r)\rangle)$$

- Broadbent-Lord: evidence that this may be IND-secure when PRF is instantiated with a random oracle

Plausible Bootstrapping from Search to IND Security

Broadbent and Lord '20



- Assume we have a scheme SearchEnc satisfying search security
- Then let INDEnc_θ sample $r \leftarrow \{0,1\}^n$ and output

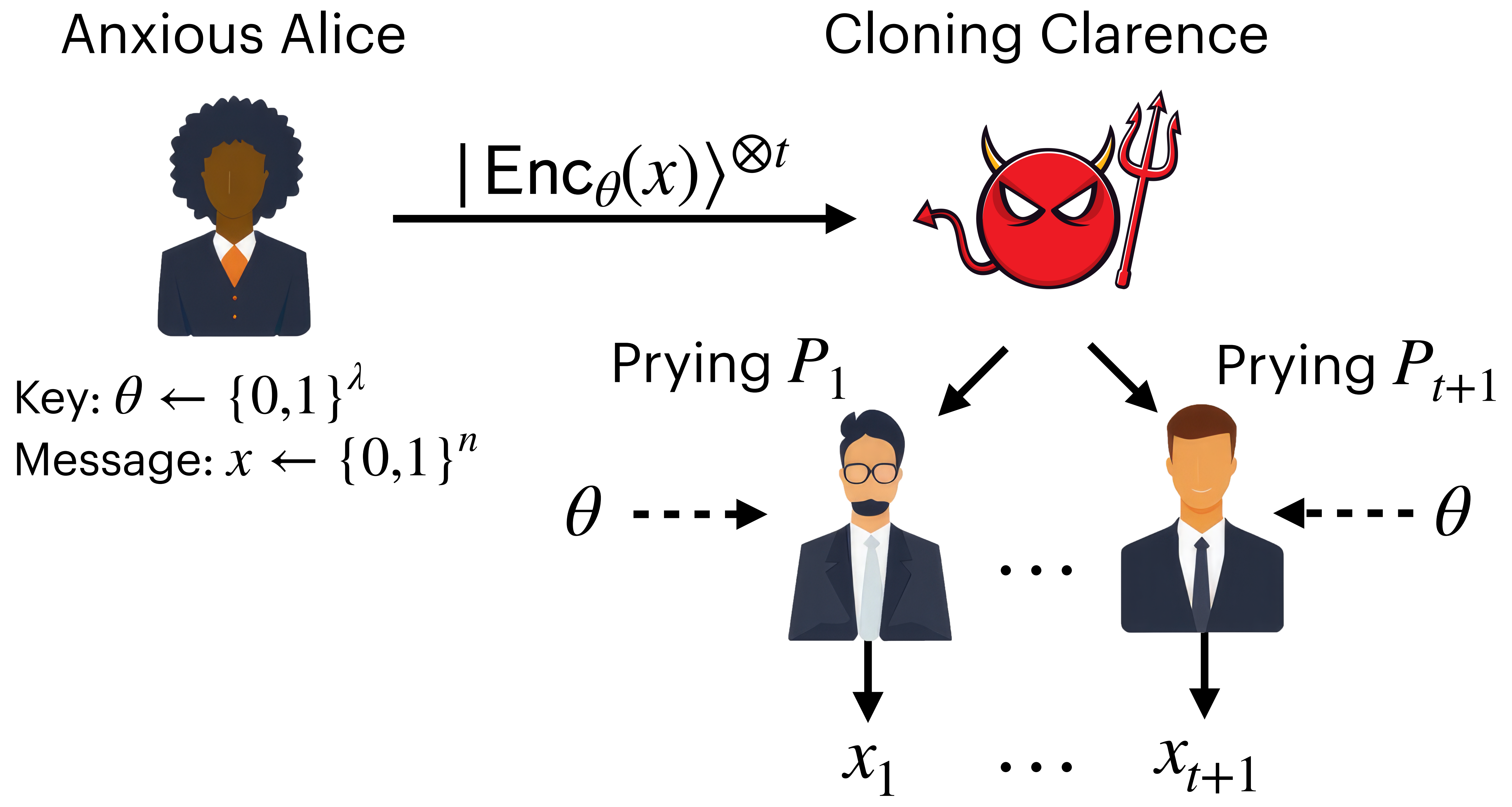
$$|\mathsf{INDEnc}_\theta(x)\rangle = (x \oplus \mathsf{PRF}(r), |\mathsf{SearchEnc}_\theta(r)\rangle)$$

- Broadbent-Lord: evidence that this may be IND-secure when PRF is instantiated with a random oracle

Actually proving IND-security is a notoriously difficult open problem!

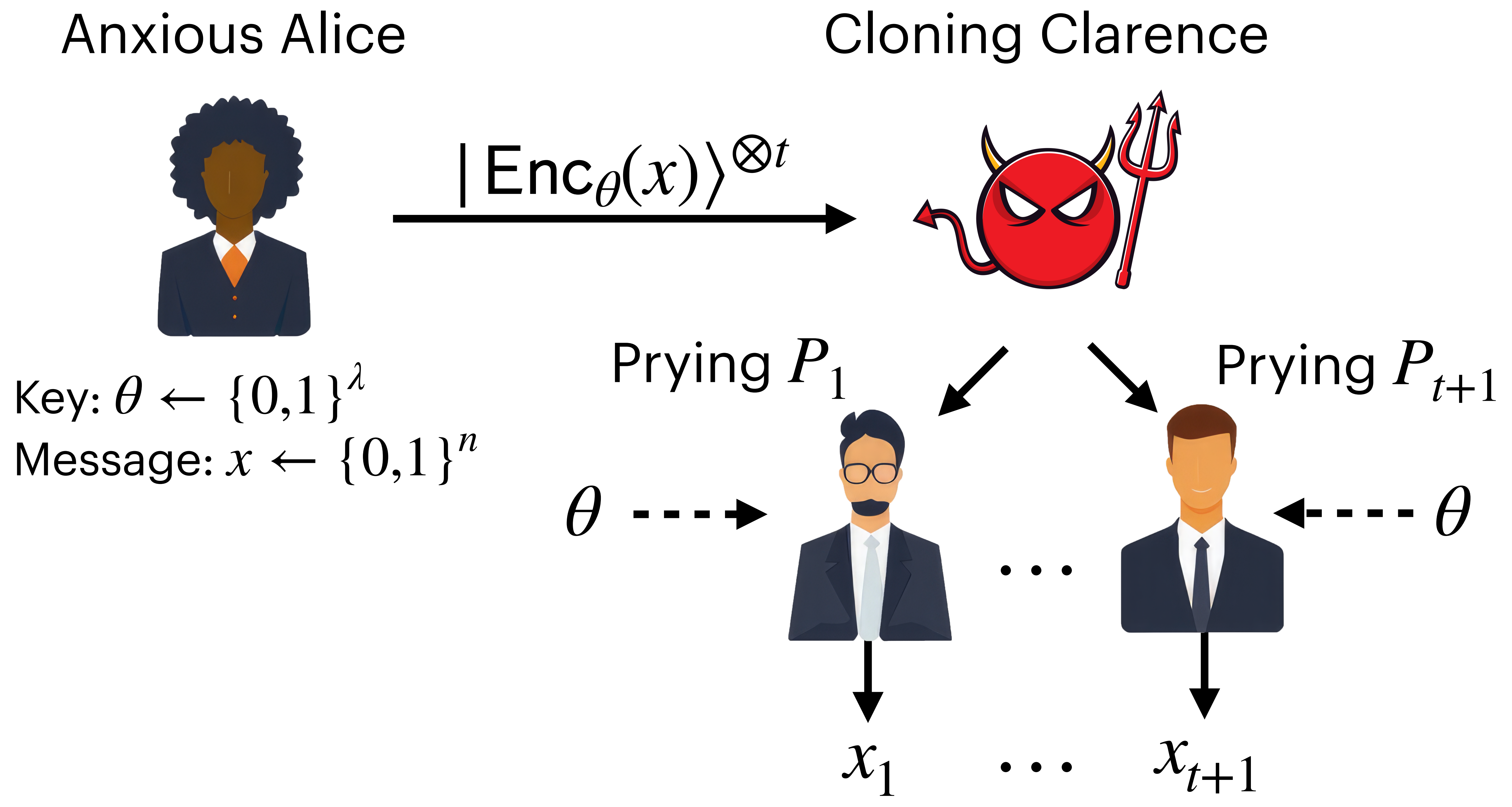
(Need Goldreich-Levin-style argument where P_1, P_2 both get the <u>same</u> challenge r)

This Talk: Multi-Copy Search Security



- Clarence receives $t = \mathsf{poly}(\lambda)$ identical pure ciphertext states, and forwards some states to $t+1$ isolated players

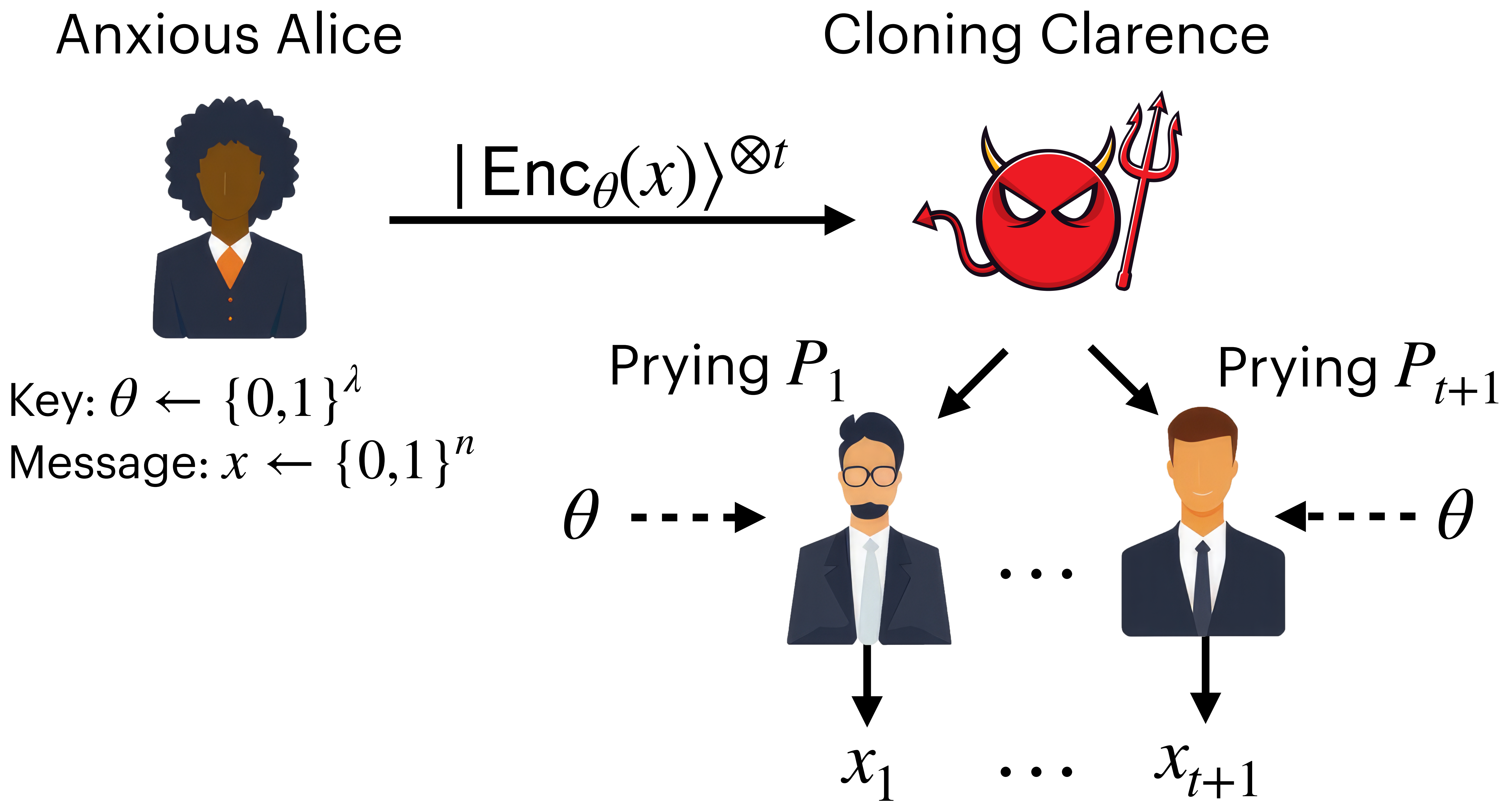
This Talk: Multi-Copy Search Security



- Clarence receives $t = \mathsf{poly}(\lambda)$ identical pure ciphertext states, and forwards some states to $t+1$ isolated players
- Value of this game:

$$\omega(G) = \Pr_{\theta \leftarrow \{0,1\}^\lambda, x \leftarrow \{0,1\}^n} \left[x_1 = \ldots = x_{t+1} = x \right]$$

This Talk: Multi-Copy Search Security

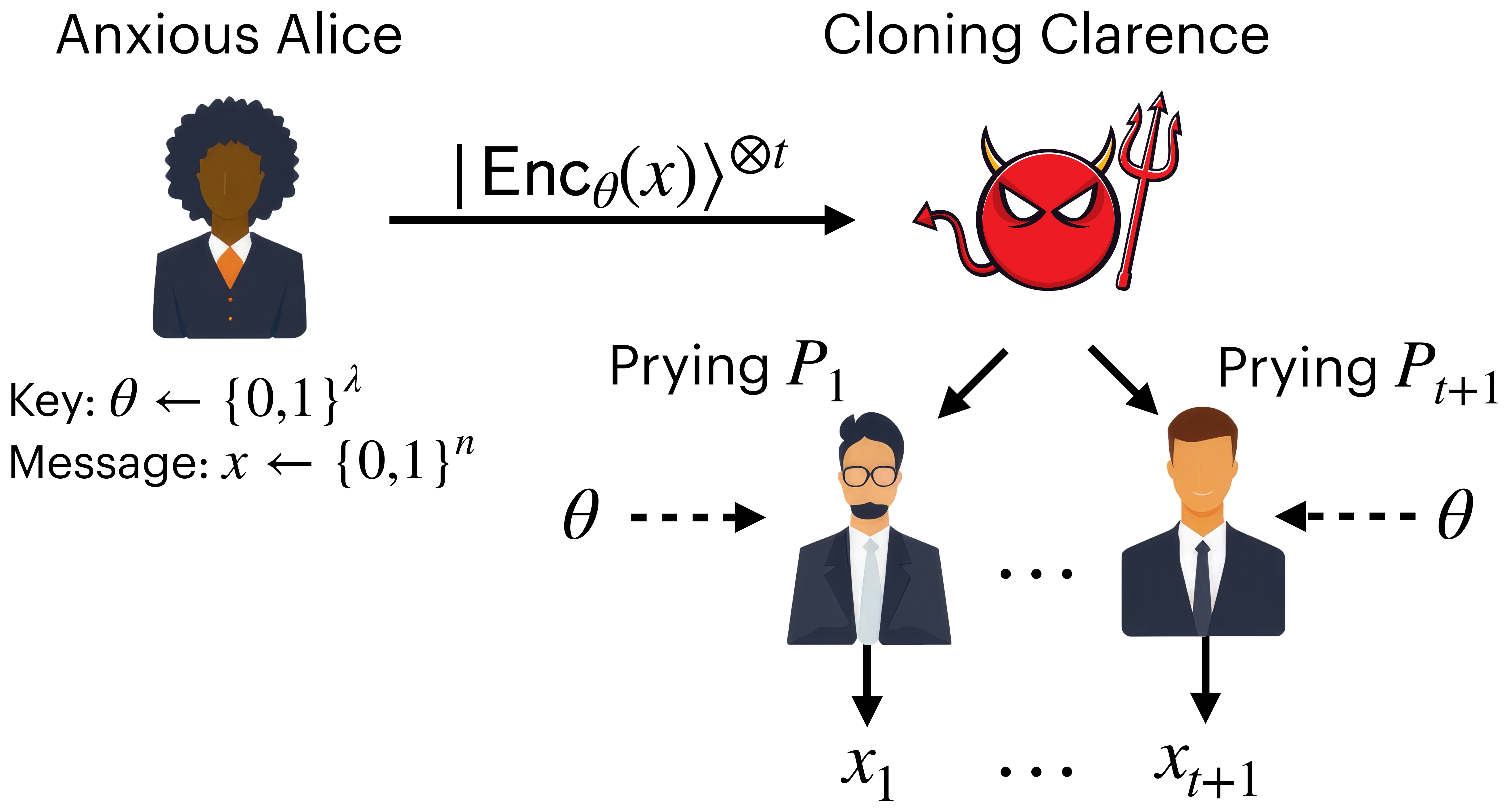


- Clarence receives $t = \mathsf{poly}(\lambda)$ identical pure ciphertext states, and forwards some states to $t+1$ isolated players
- Value of this game:

$$\omega(G) = \Pr_{\theta \leftarrow \{0,1\}^\lambda, x \leftarrow \{0,1\}^n}\left[x_1 = \ldots = x_{t+1} = x\right]$$

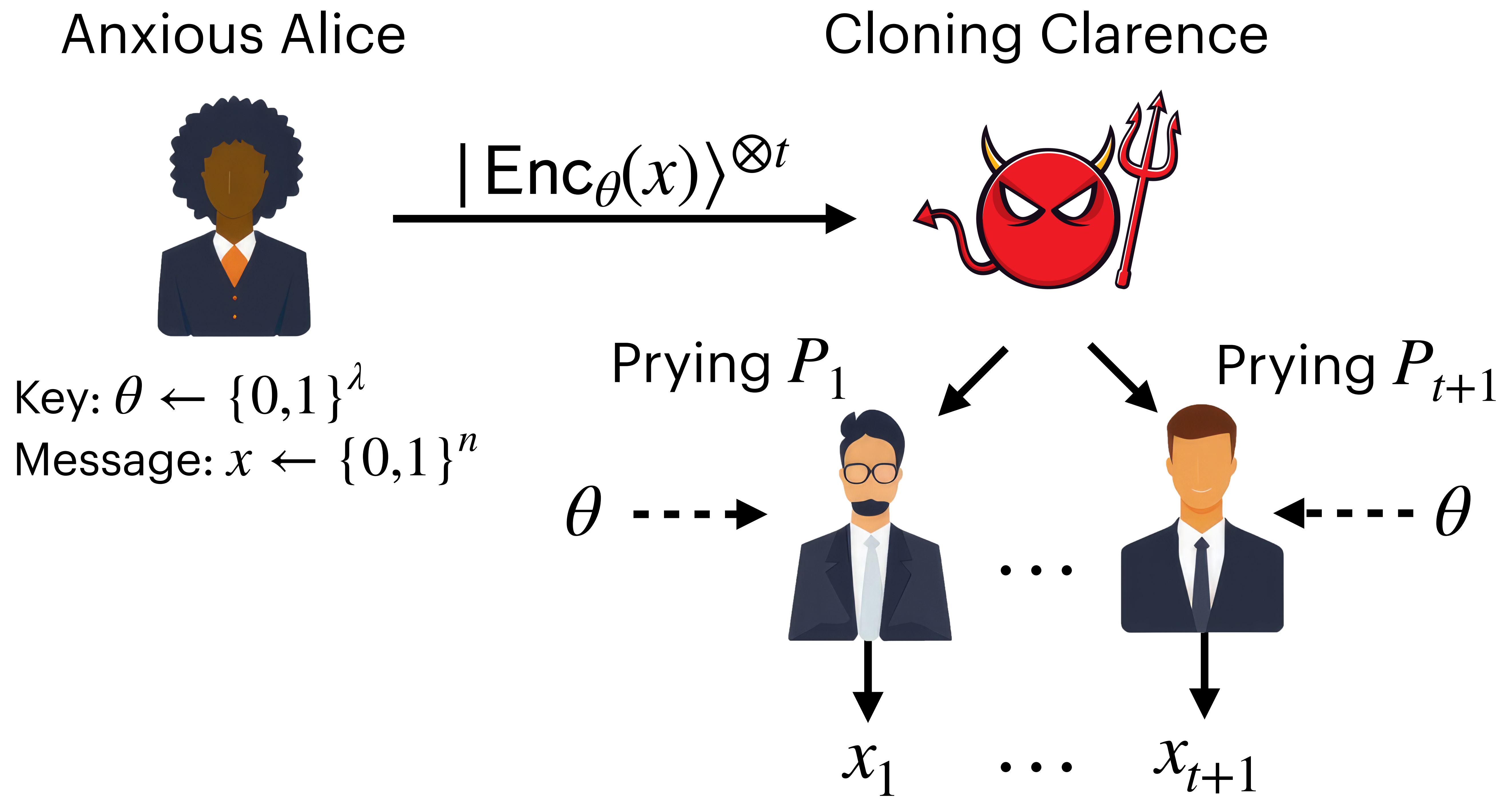
- Search security: want $\omega(G) \leq \mathsf{negl}(\lambda)$

A Trivial Strategy Attaining $\omega(G) = 2^{-n}$



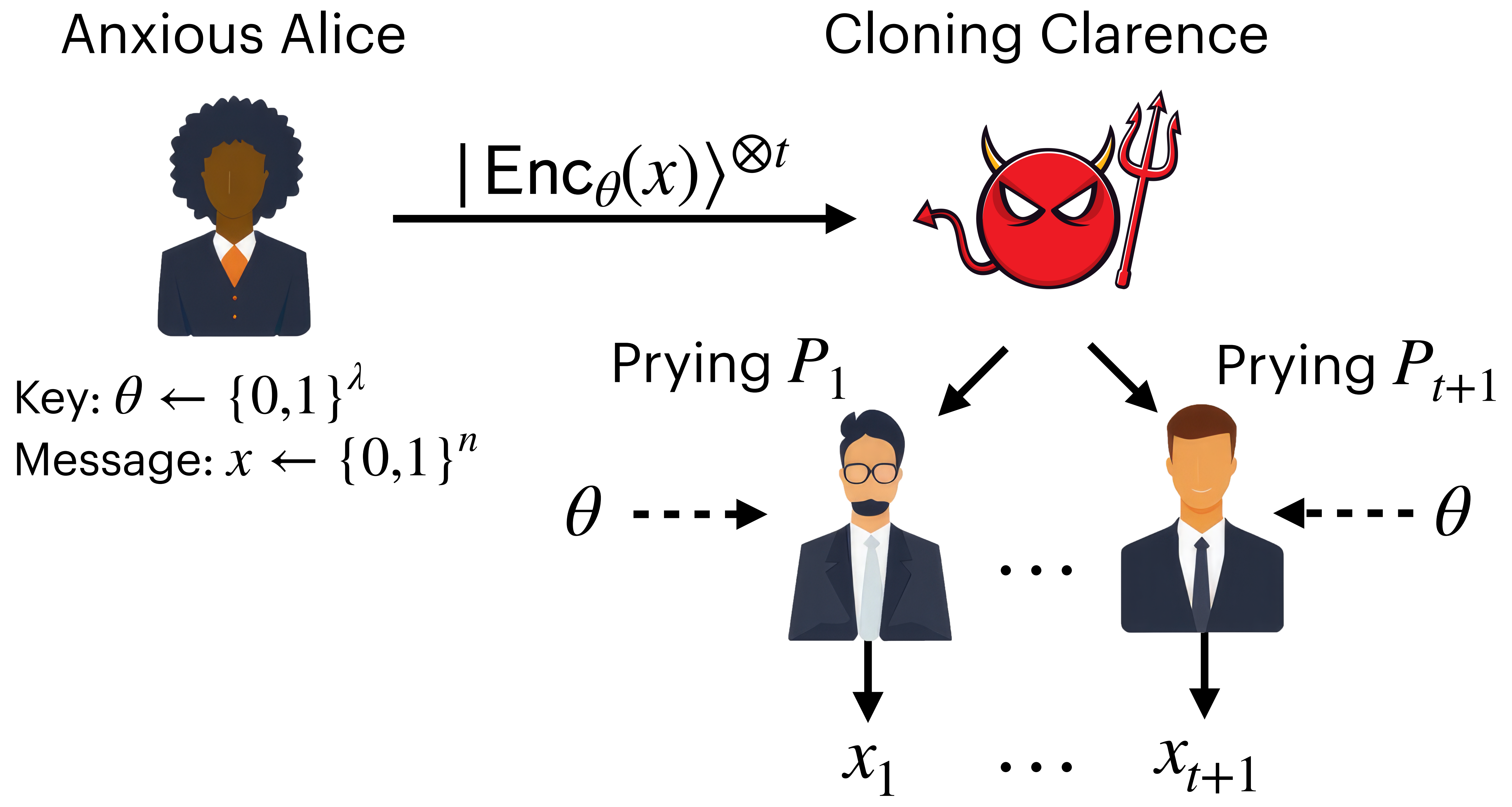
- Clarence forwards one copy of $|\mathsf{Enc}_\theta(x)\rangle$ to each of $P_1, \ldots, P_t$

A Trivial Strategy Attaining $\omega(G) = 2^{-n}$



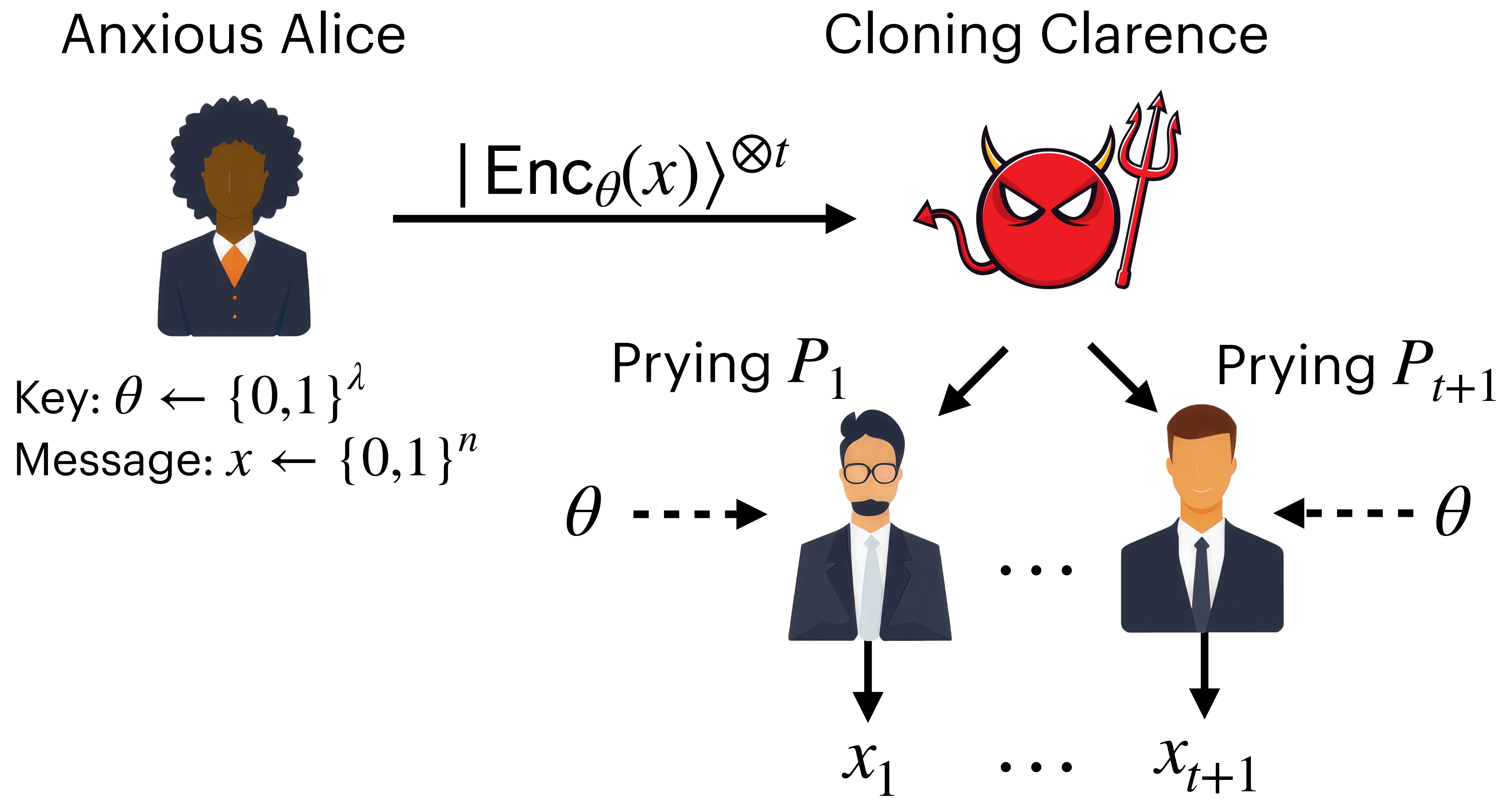
- Clarence forwards one copy of $|\text{Enc}_\theta(x)\rangle$ to each of $P_1, \ldots, P_t$
- $P_1, \ldots, P_t$ will be able to decrypt and recover x...

A Trivial Strategy Attaining $\omega(G) = 2^{-n}$



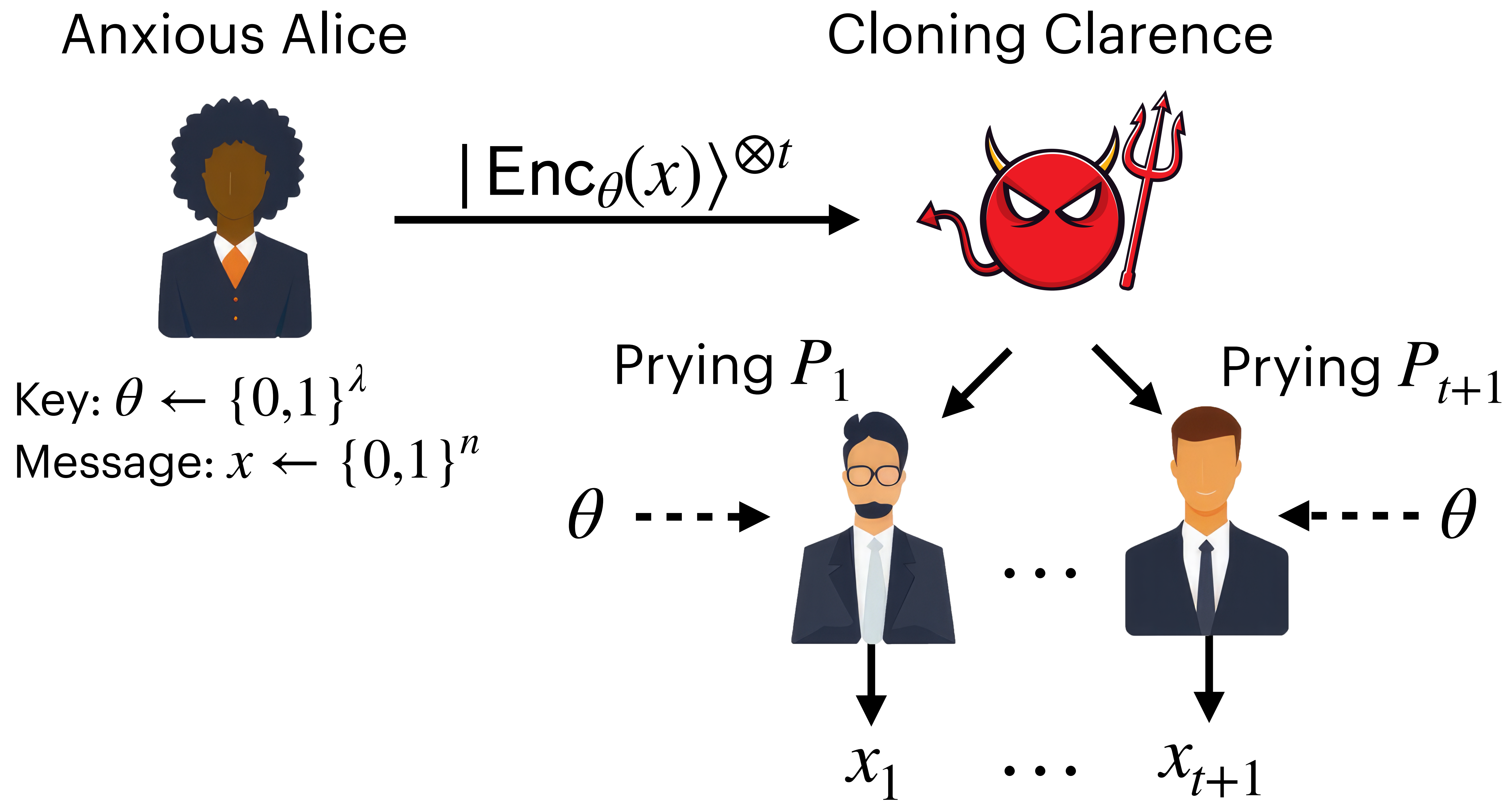
- Clarence forwards one copy of $|\mathsf{Enc}_\theta(x)\rangle$ to each of $P_1, \ldots, P_t$
- $P_1, \ldots, P_t$ will be able to decrypt and recover x...
- ...but P_{t+1} will have to guess a random string $x_{t+1} \leftarrow \{0,1\}^n$

A Trivial Strategy Attaining $\omega(G) = 2^{-n}$



- Clarence forwards one copy of $|\text{Enc}_\theta(x)\rangle$ to each of $P_1, \ldots, P_t$
- $P_1, \ldots, P_t$ will be able to decrypt and recover x...
- ...but P_{t+1} will have to guess a random string $x_{t+1} \leftarrow \{0,1\}^n$
- Success probability: 2^{-n}

A Trivial Strategy Attaining $\omega(G) = 2^{-n}$

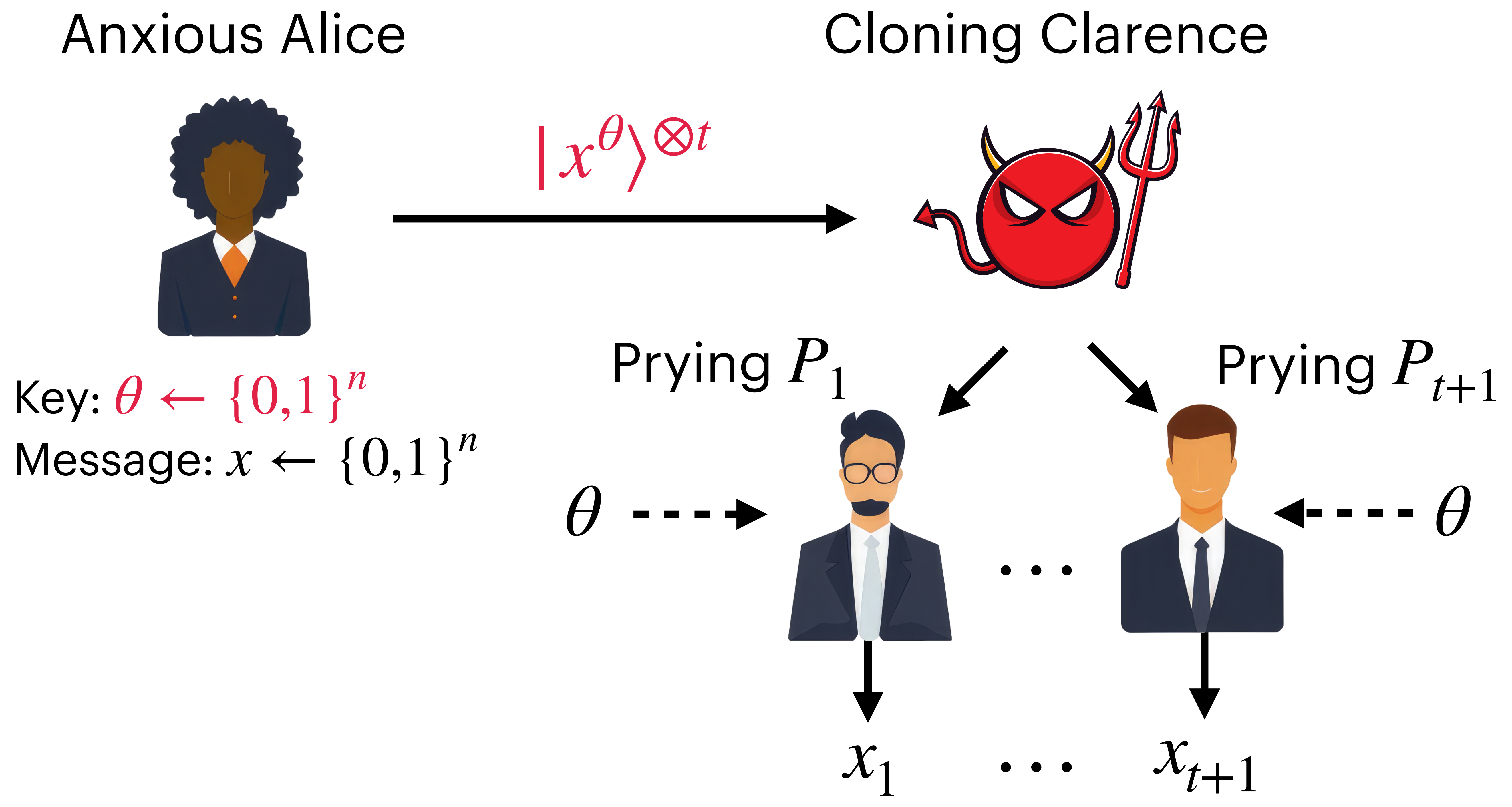


- Clarence forwards one copy of $|\mathsf{Enc}_\theta(x)\rangle$ to each of $P_1, \ldots, P_t$
- $P_1, \ldots, P_t$ will be able to decrypt and recover x...
- ...but P_{t+1} will have to guess a random string $x_{t+1} \leftarrow \{0,1\}^n$
- Success probability: 2^{-n}

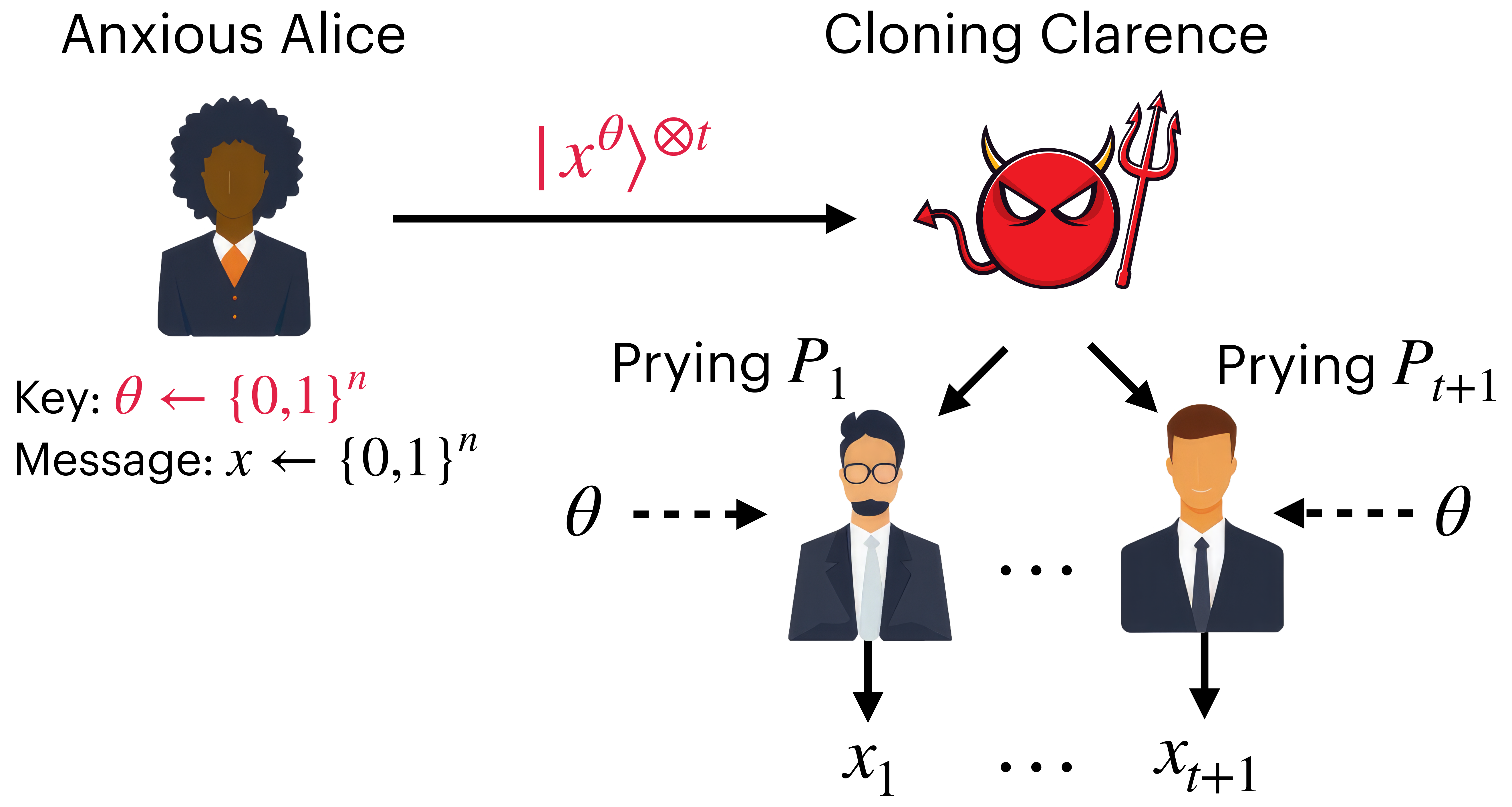
Ideal goal: a construction which doesn't admit any strategies achieving better than 2^{-n}

Previous Candidate 1: BB84 States

- Ciphertext state is $|x^\theta\rangle = \mathsf{H}^\theta|x\rangle$



Previous Candidate 1: BB84 States

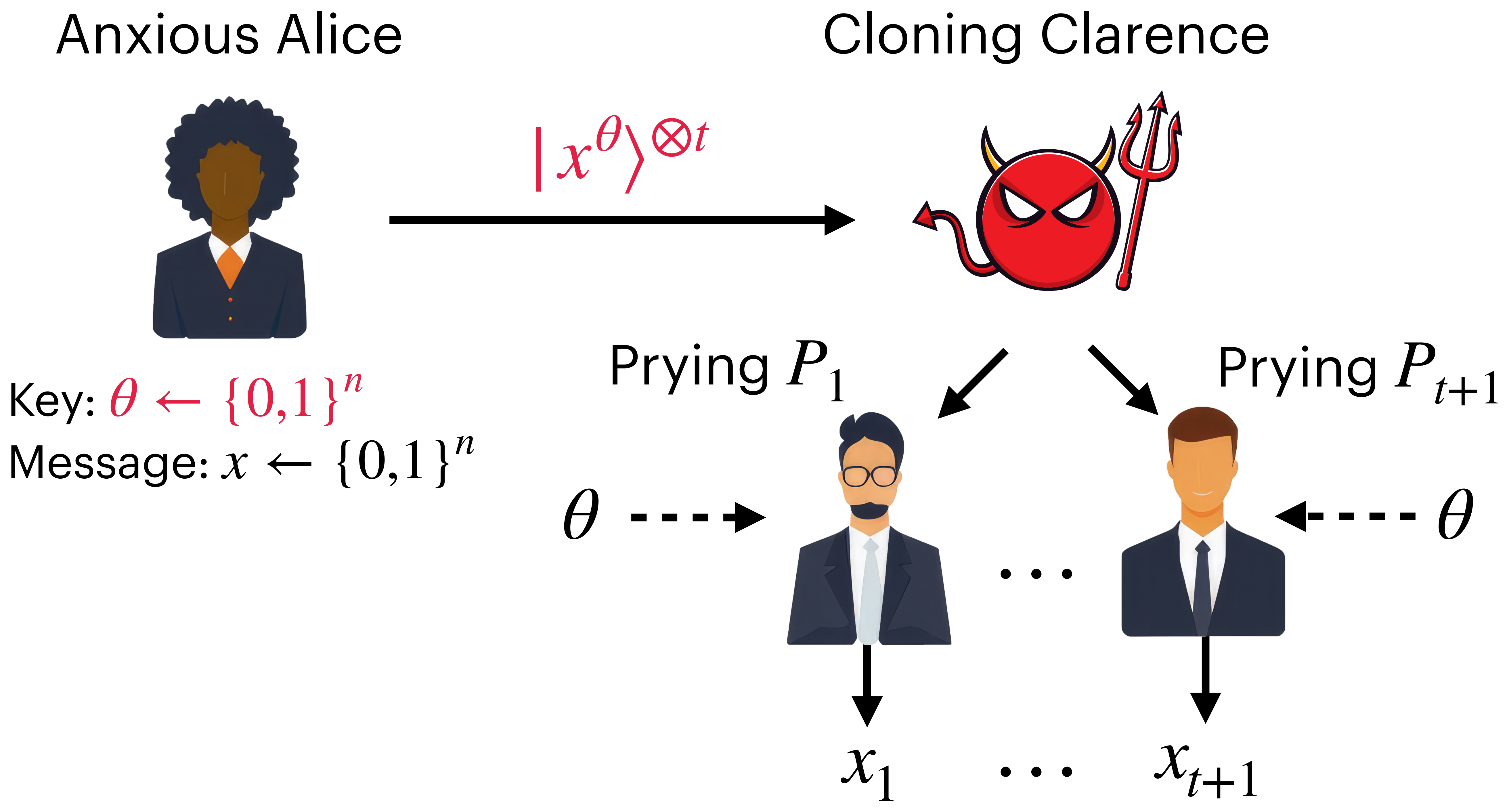


- Ciphertext state is $|x^\theta\rangle = \mathsf{H}^\theta|x\rangle$
- Previous work* (TFKW13, BL20) when $t = 1$:

$$\omega(G) = \left(\cos^2(\pi/8)\right)^n \approx 2^{-0.228n}$$

*same constant as in the CHSH game

Previous Candidate 1: BB84 States



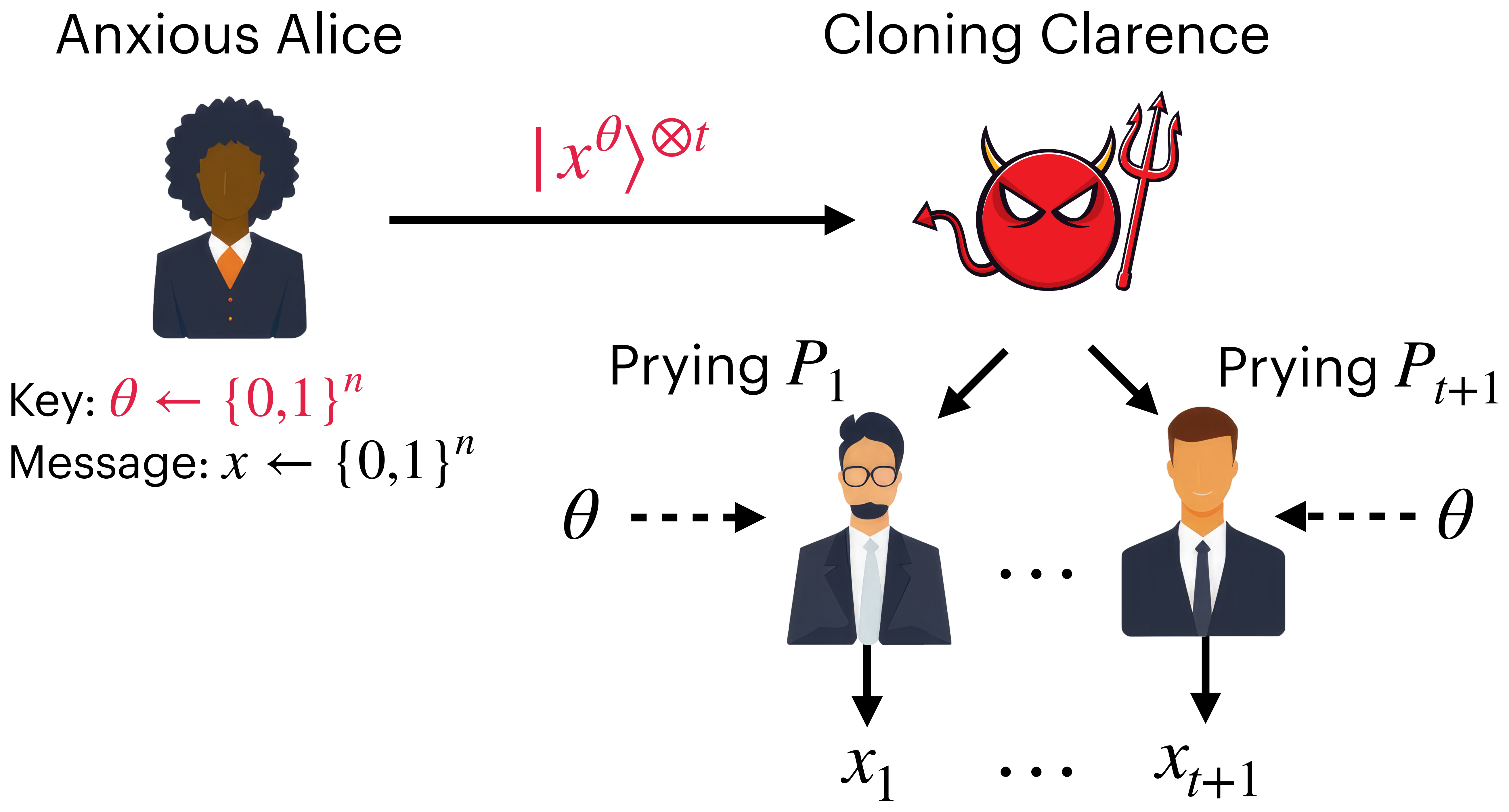
- Ciphertext state is $|x^\theta\rangle = \mathsf{H}^\theta|x\rangle$
- Previous work* (TFKW13, BL20) when $t = 1$:

$$\omega(G) = \left(\cos^2(\pi/8)\right)^n \approx 2^{-0.228n}$$

- For $t \geq 2$: **completely broken** ($\omega(G) = 1$)**!**

*same constant as in the CHSH game

Previous Candidate 1: BB84 States



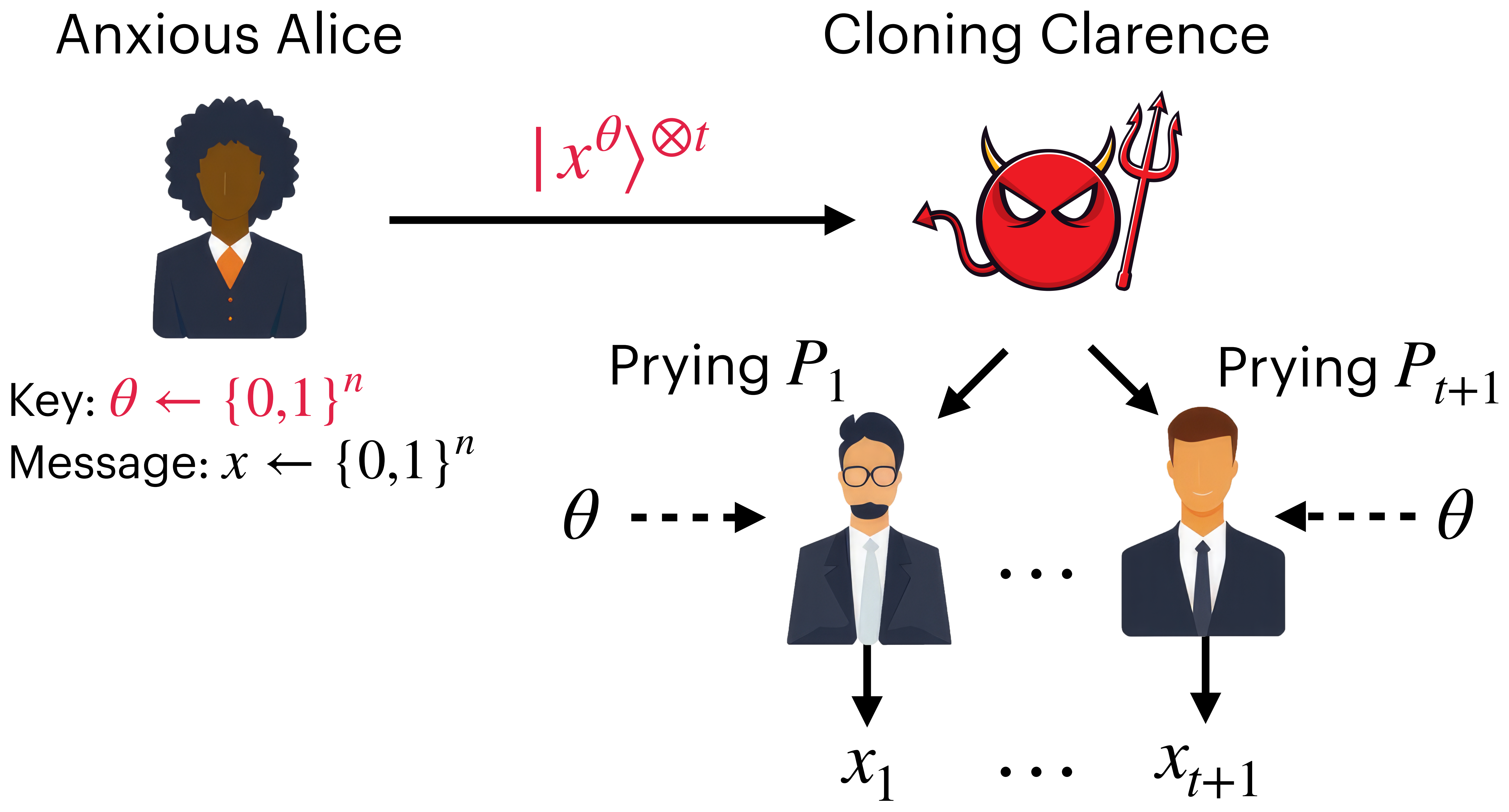
- Ciphertext state is $|x^\theta\rangle = \mathsf{H}^\theta|x\rangle$
- Previous work* (TFKW13, BL20) when $t = 1$:

$$\omega(G) = \left(\cos^2(\pi/8)\right)^n \approx 2^{-0.228n}$$

- For $t \geq 2$: **completely broken ($\omega(G) = 1$)!**
  - Clarence:
    - Measure one copy in the standard basis (as if $\theta = 0^n$) and the other in the Hadamard basis (as if $\theta = 1^n$)

*same constant as in the CHSH game

Previous Candidate 1: BB84 States



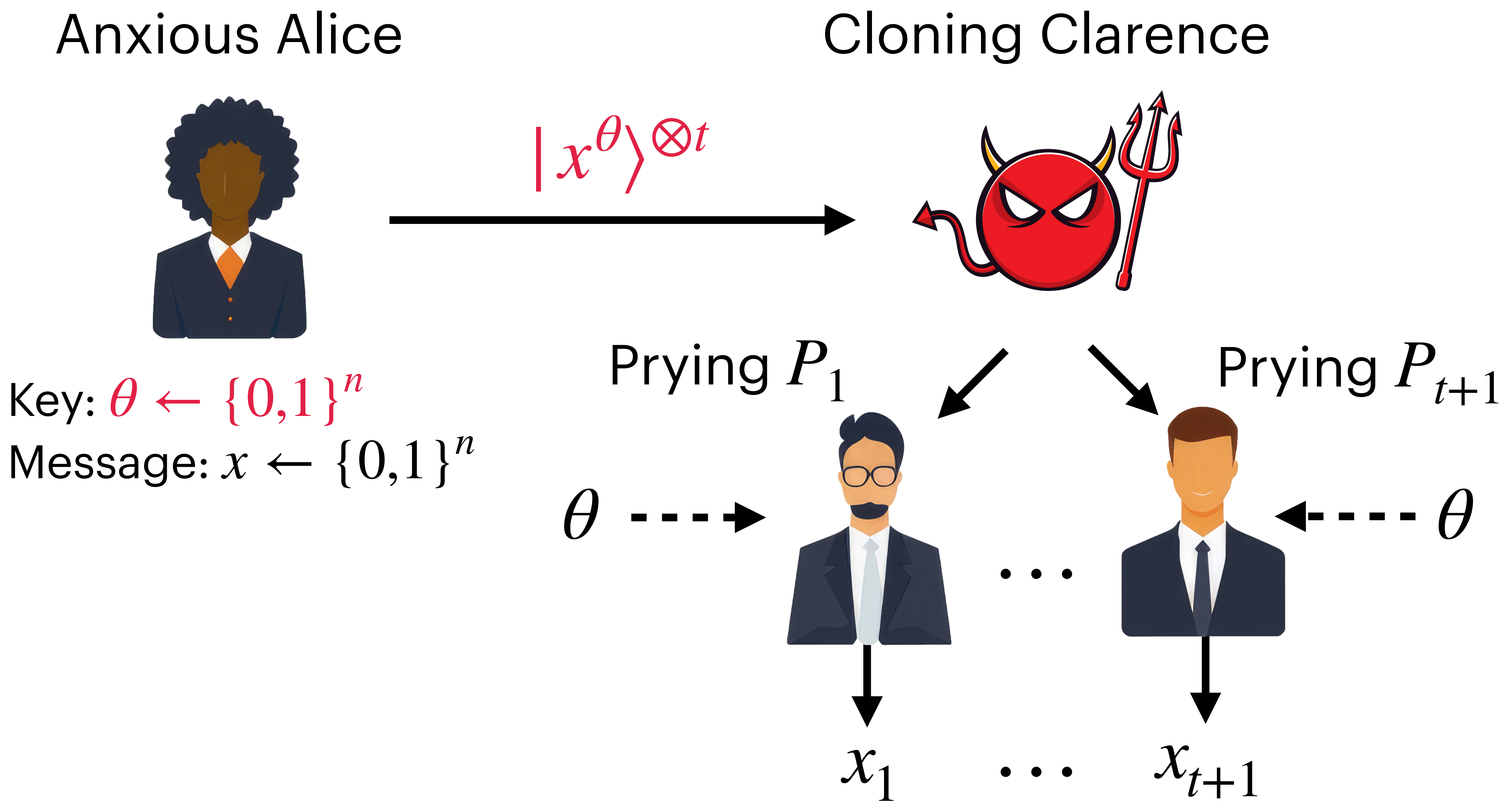
- Ciphertext state is $|x^\theta\rangle = \mathsf{H}^\theta|x\rangle$
- Previous work* (TFKW13, BL20) when $t = 1$:

$$\omega(G) = \left(\cos^2(\pi/8)\right)^n \approx 2^{-0.228n}$$

- For $t \geq 2$: **completely broken ($\omega(G) = 1$)!**
  - Clarence:
    - Measure one copy in the standard basis (as if $\theta = 0^n$) and the other in the Hadamard basis (as if $\theta = 1^n$)
    - Forward these results to all players.

*same constant as in the CHSH game

Previous Candidate 1: BB84 States



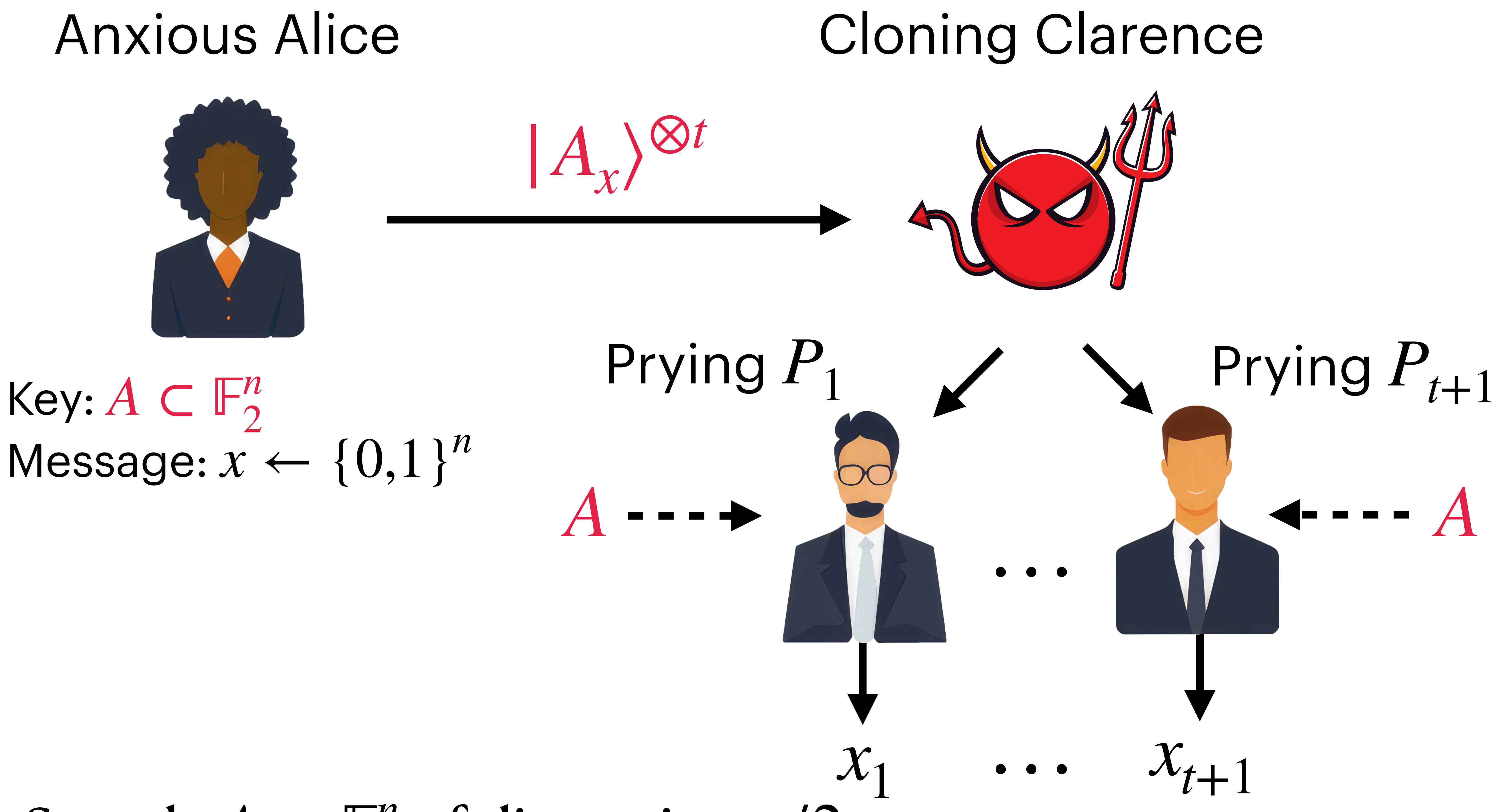
- Ciphertext state is $|x^\theta\rangle = \mathsf{H}^\theta |x\rangle$
- Previous work* (TFKW13, BL20) when $t = 1$:

$$\omega(G) = \left(\cos^2(\pi/8)\right)^n \approx 2^{-0.228n}$$

- For $t \geq 2$: **completely broken ($\omega(G) = 1$)!**
  - Clarence:
    - Measure one copy in the standard basis (as if $\theta = 0^n$) and the other in the Hadamard basis (as if $\theta = 1^n$)
    - Forward these results to all players.
  - All players can mix-and-match these results to recover x after receiving θ

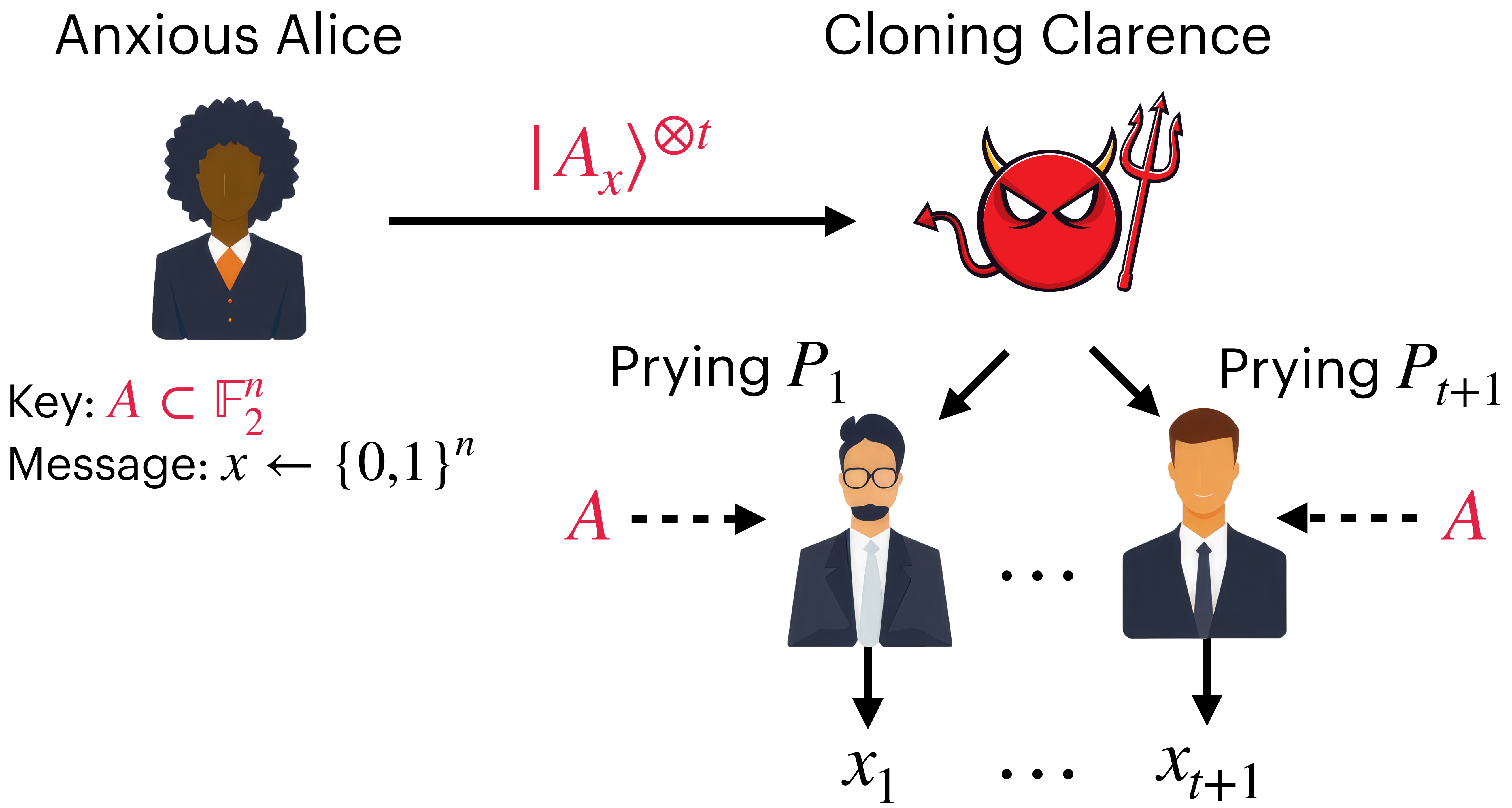
*same constant as in the CHSH game

Previous Candidate 2: Subspace Coset States



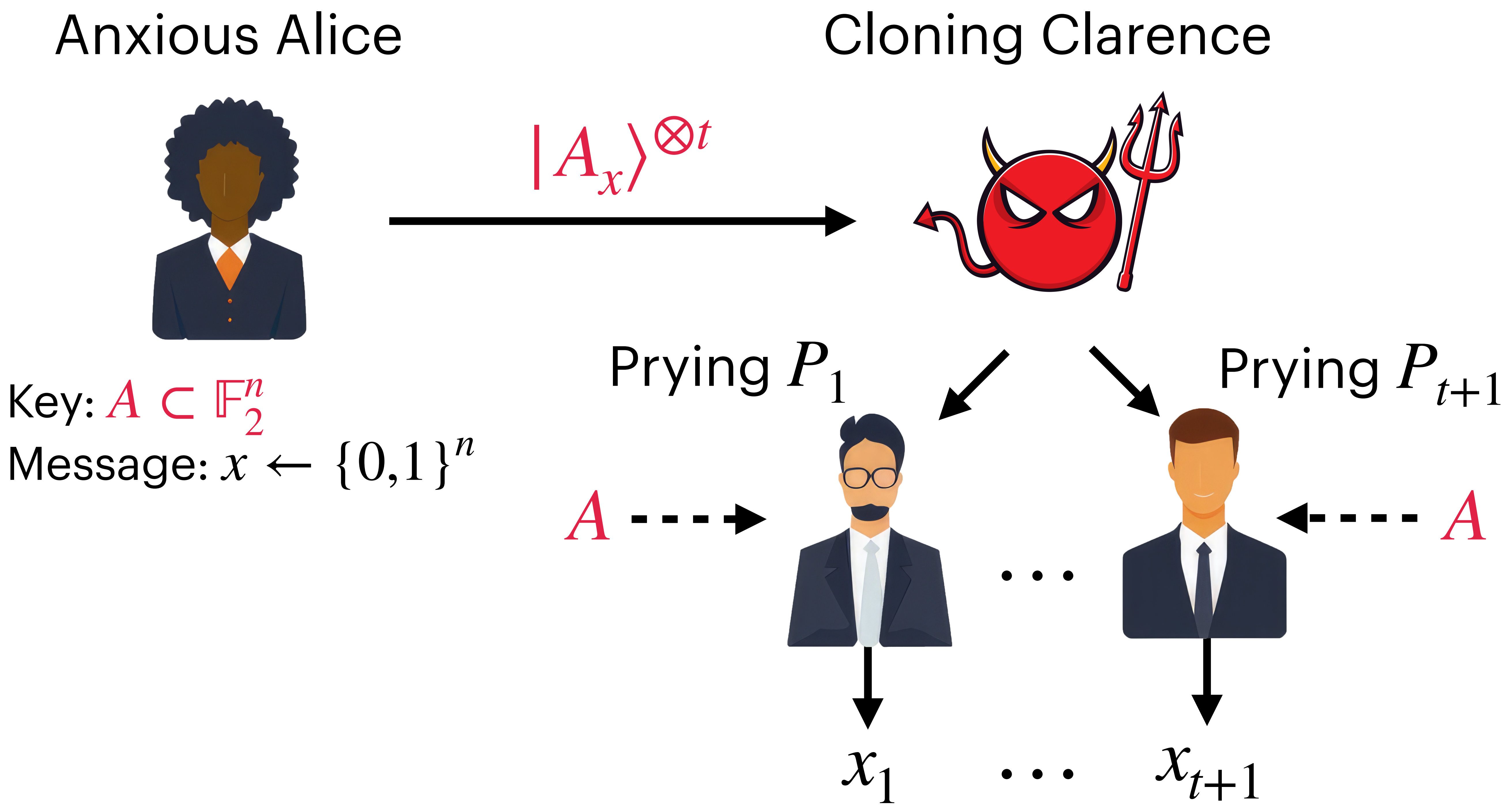
- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$

Previous Candidate 2: Subspace Coset States



- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$
- Parse a message x as two cosets $A + s$ and $A^\perp + s'$

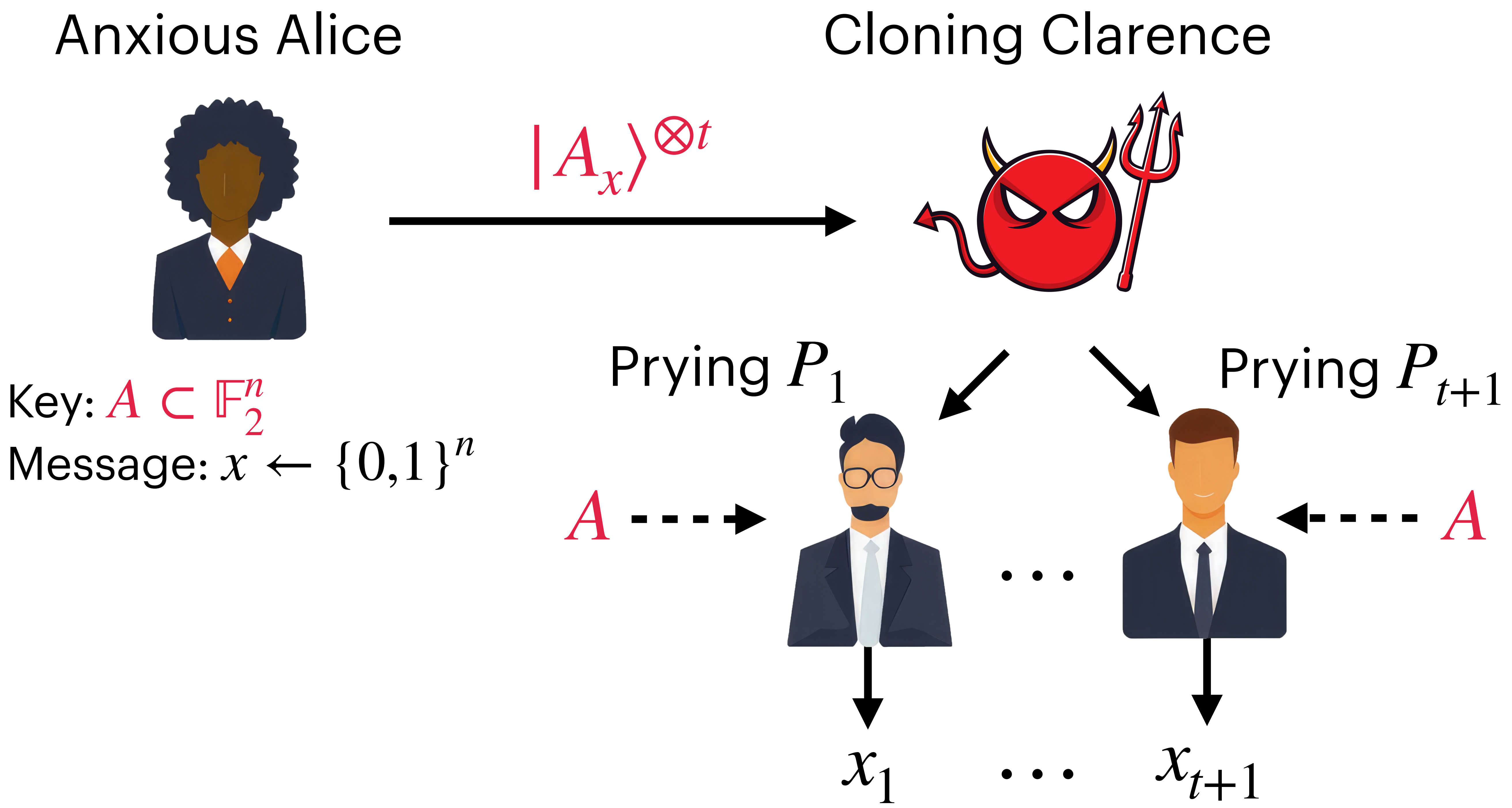
Previous Candidate 2: Subspace Coset States



- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$
- Parse a message x as two cosets $A + s$ and $A^{\perp} + s'$
- Define

$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle s', a\rangle} |a + s\rangle$$

Previous Candidate 2: Subspace Coset States

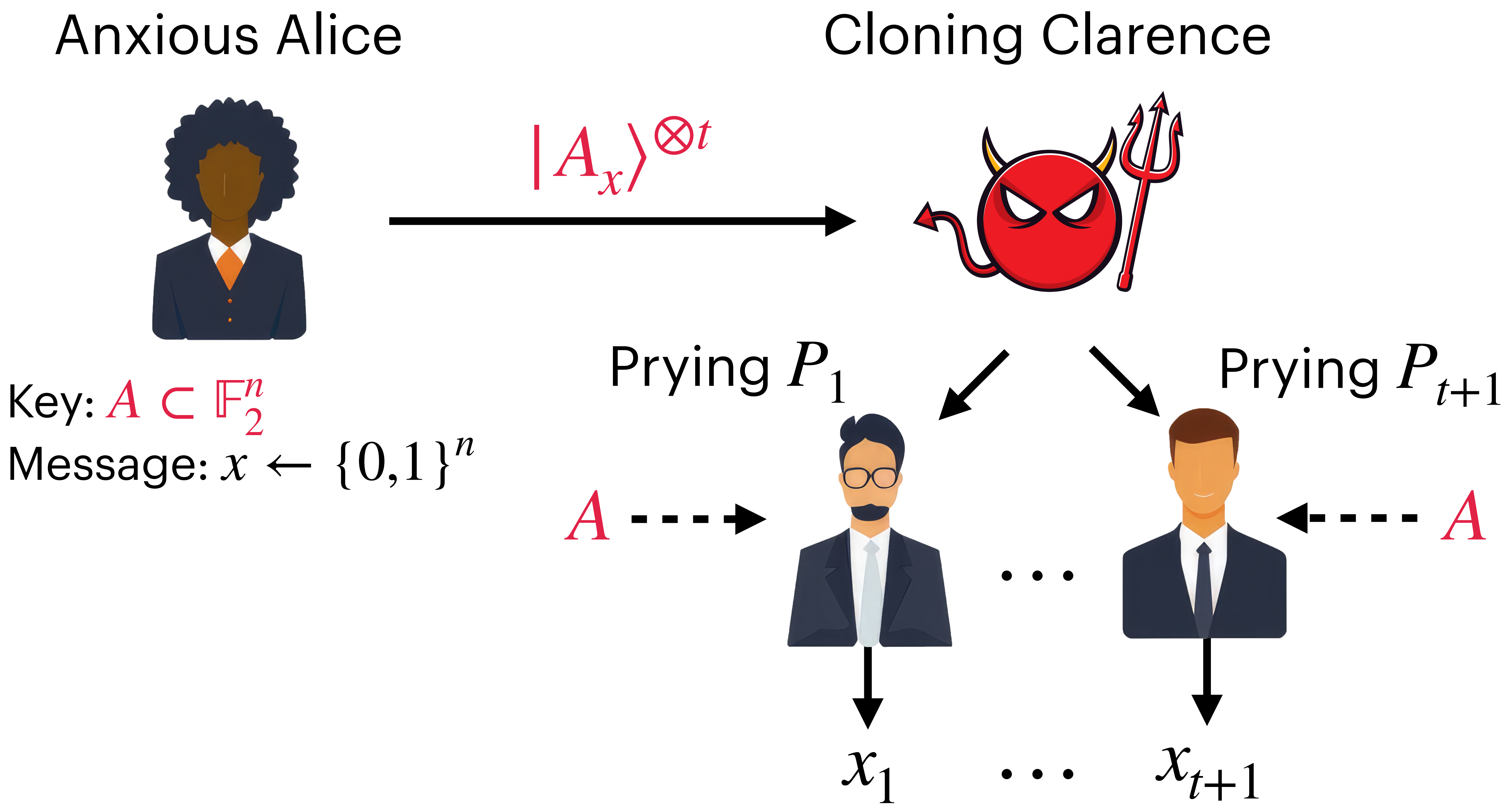


- Ciphertext state is $|A_x\rangle = |A_{s,s'}\rangle$

- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$
- Parse a message x as two cosets $A + s$ and $A^{\perp} + s'$
- Define

$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle s', a\rangle} |a + s\rangle$$

Previous Candidate 2: Subspace Coset States



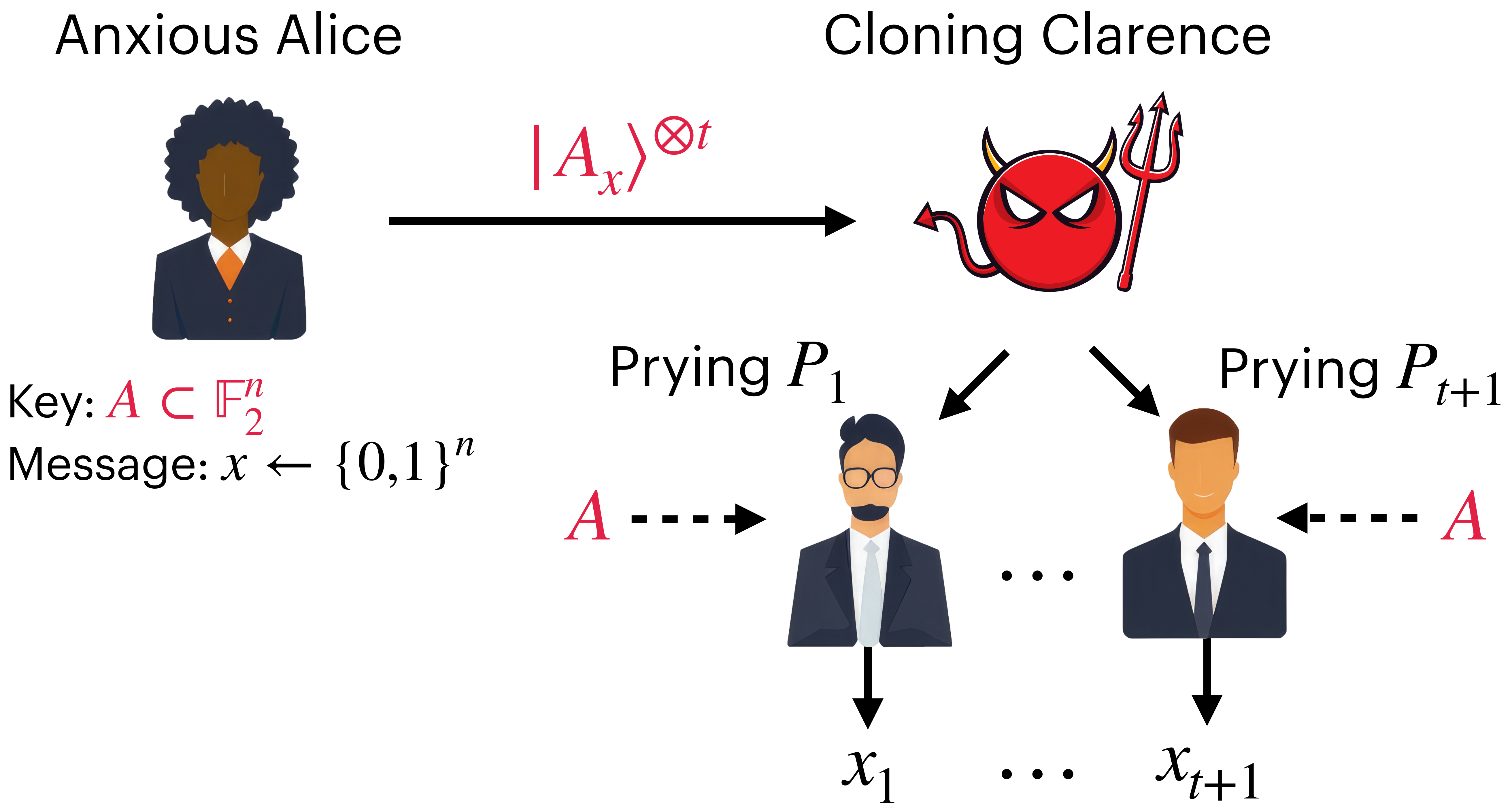
- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$
- Parse a message x as two cosets $A + s$ and $A^\perp + s'$
- Define

$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle s',a\rangle} |a + s\rangle$$

- Ciphertext state is $|A_x\rangle = |A_{s,s'}\rangle$
- Previous work (CLLZ21, CV22) when $t = 1$:

$$\omega(G) \leq \left(\cos(\pi/8)\right)^{n+o(n)} \approx 2^{(-0.114+o(1))n}$$

Previous Candidate 2: Subspace Coset States



- Ciphertext state is $|A_x\rangle = |A_{s,s'}\rangle$
- Previous work (CLLZ21, CV22) when $t = 1$:

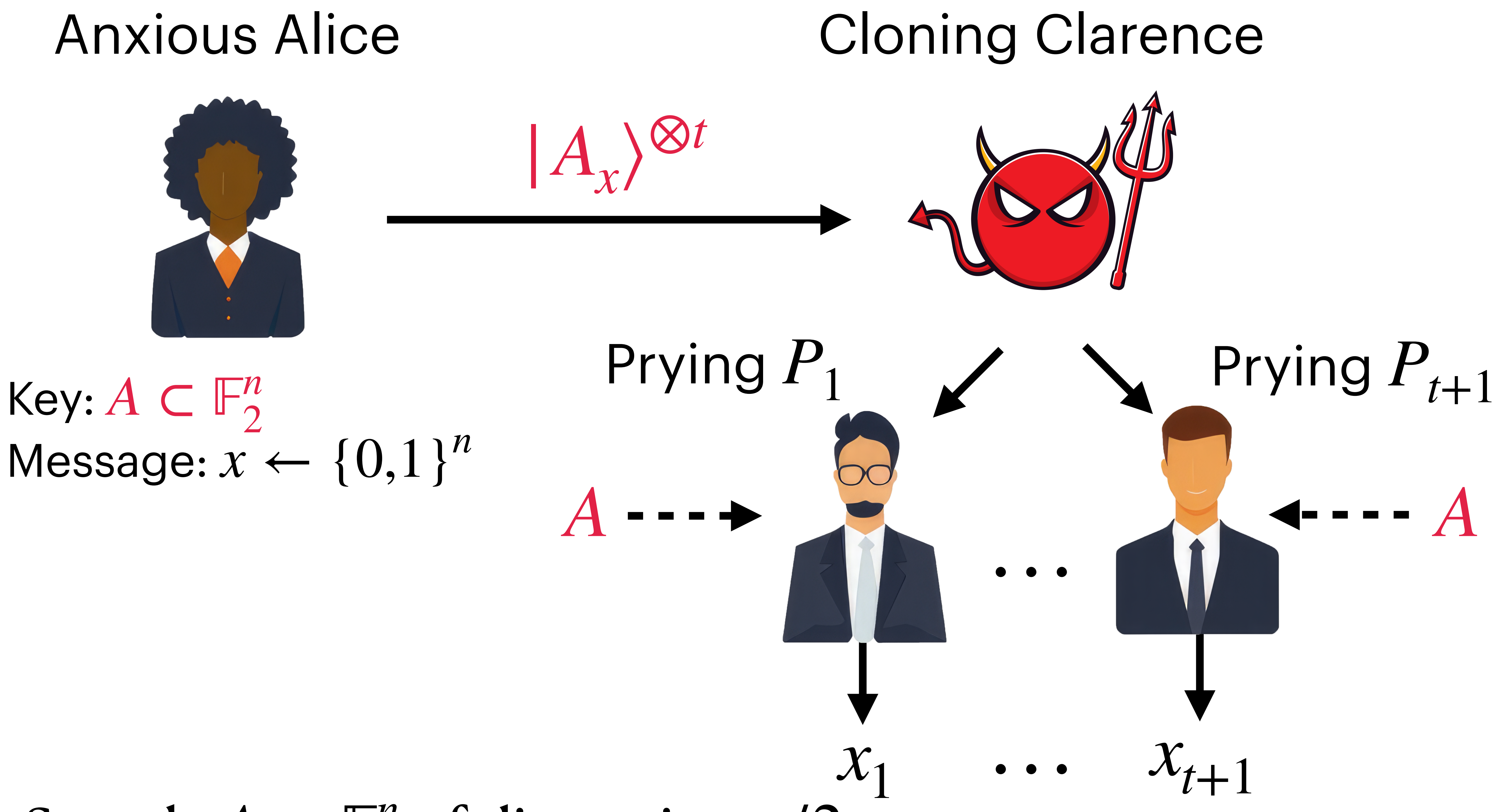
$$\omega(G) \leq \left(\cos(\pi/8)\right)^{n+o(n)} \approx 2^{(-0.114+o(1))n}$$

- For $t \gg n$: **completely broken!**

- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$
- Parse a message x as two cosets $A + s$ and $A^\perp + s'$
- Define

$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle s',a\rangle} |a + s\rangle$$

Previous Candidate 2: Subspace Coset States



- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$
- Parse a message x as two cosets $A + s$ and $A^\perp + s'$
- Define

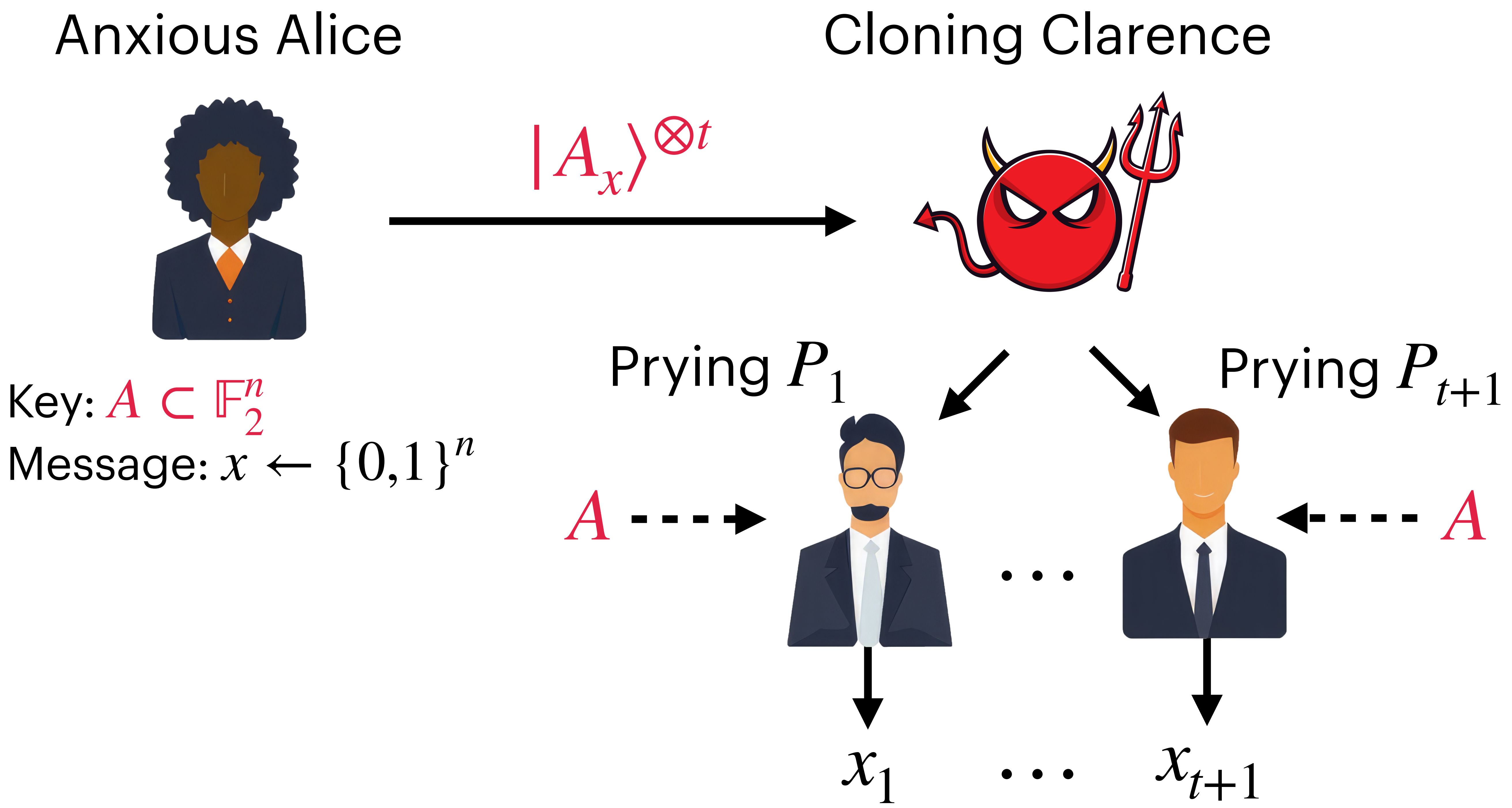
$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle s', a\rangle} |a + s\rangle$$

- Ciphertext state is $|A_x\rangle = |A_{s,s'}\rangle$
- Previous work (CLLZ21, CV22) when $t = 1$:

$$\omega(G) \leq \left(\cos(\pi/8)\right)^{n+o(n)} \approx 2^{(-0.114+o(1))n}$$

- For $t \gg n$: **completely broken!**
  - Clarence:
    - Measure $\gg n/2$ copies in the standard basis and $\gg n/2$ copies in the Hadamard basis
    - Measurement results suffice to recover A, s, s'

Previous Candidate 2: Subspace Coset States



- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$
- Parse a message x as two cosets $A + s$ and $A^\perp + s'$
- Define

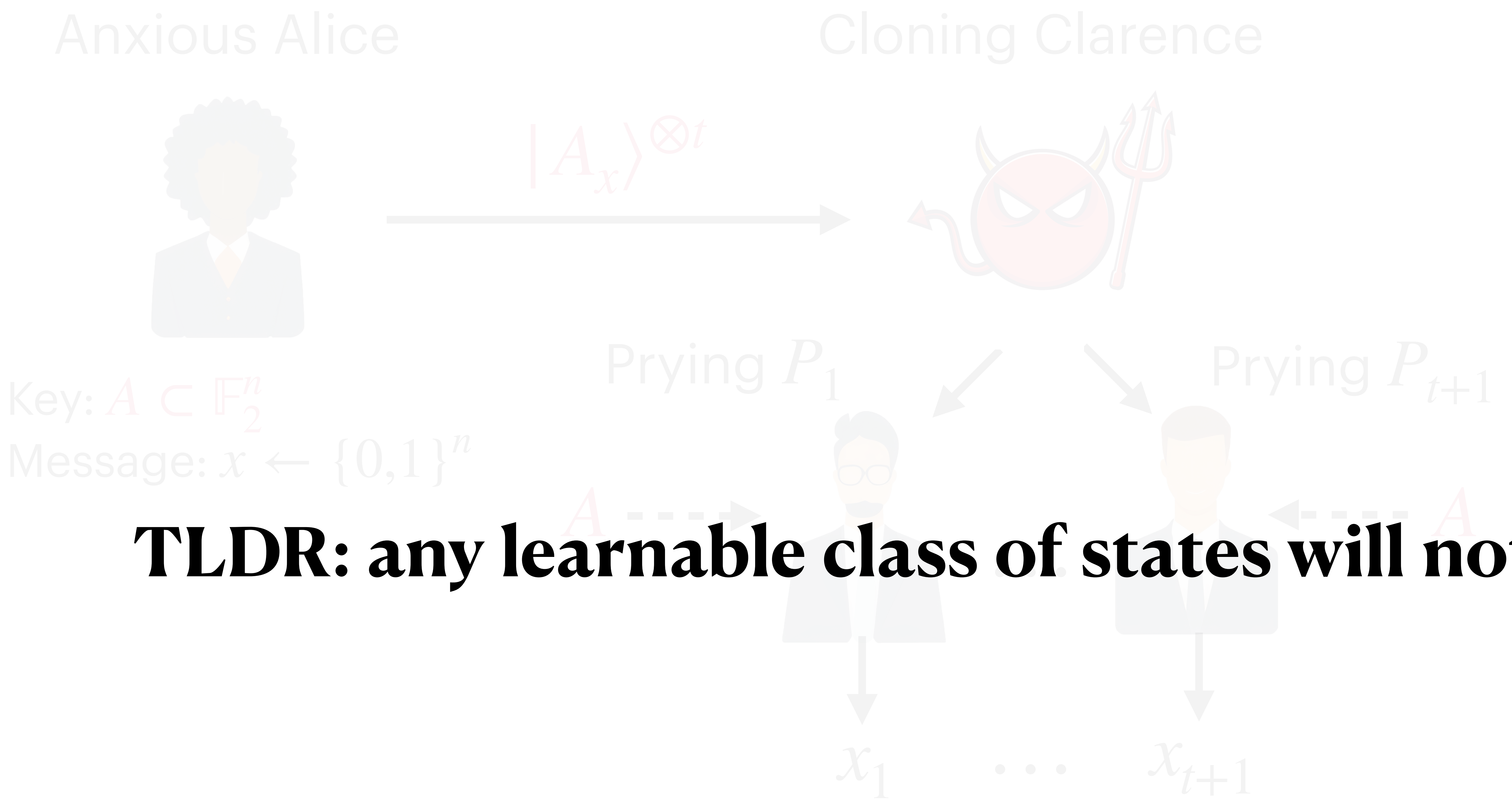
$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle s', a\rangle} |a + s\rangle$$

- Ciphertext state is $|A_x\rangle = |A_{s,s'}\rangle$
- Previous work (CLLZ21, CV22) when $t = 1$:

$$\omega(G) \leq \left(\cos(\pi/8)\right)^{n+o(n)} \approx 2^{(-0.114+o(1))n}$$

- For $t \gg n$: **completely broken!**
  - Clarence:
    - Measure $\gg n/2$ copies in the standard basis and $\gg n/2$ copies in the Hadamard basis
    - Measurement results suffice to recover A, s, s'
  - $P_1, \ldots, P_{t+1}$ don't need to be told A

Previous Candidate 2: Subspace Coset States



TLDR: any learnable class of states will not suffice for multi-copy security!

- Sample $A \subset \mathbb{F}_2^n$ of dimension $n/2$
- Parse a message x as two cosets $A + s$ and $A^\perp + s'$
- Define

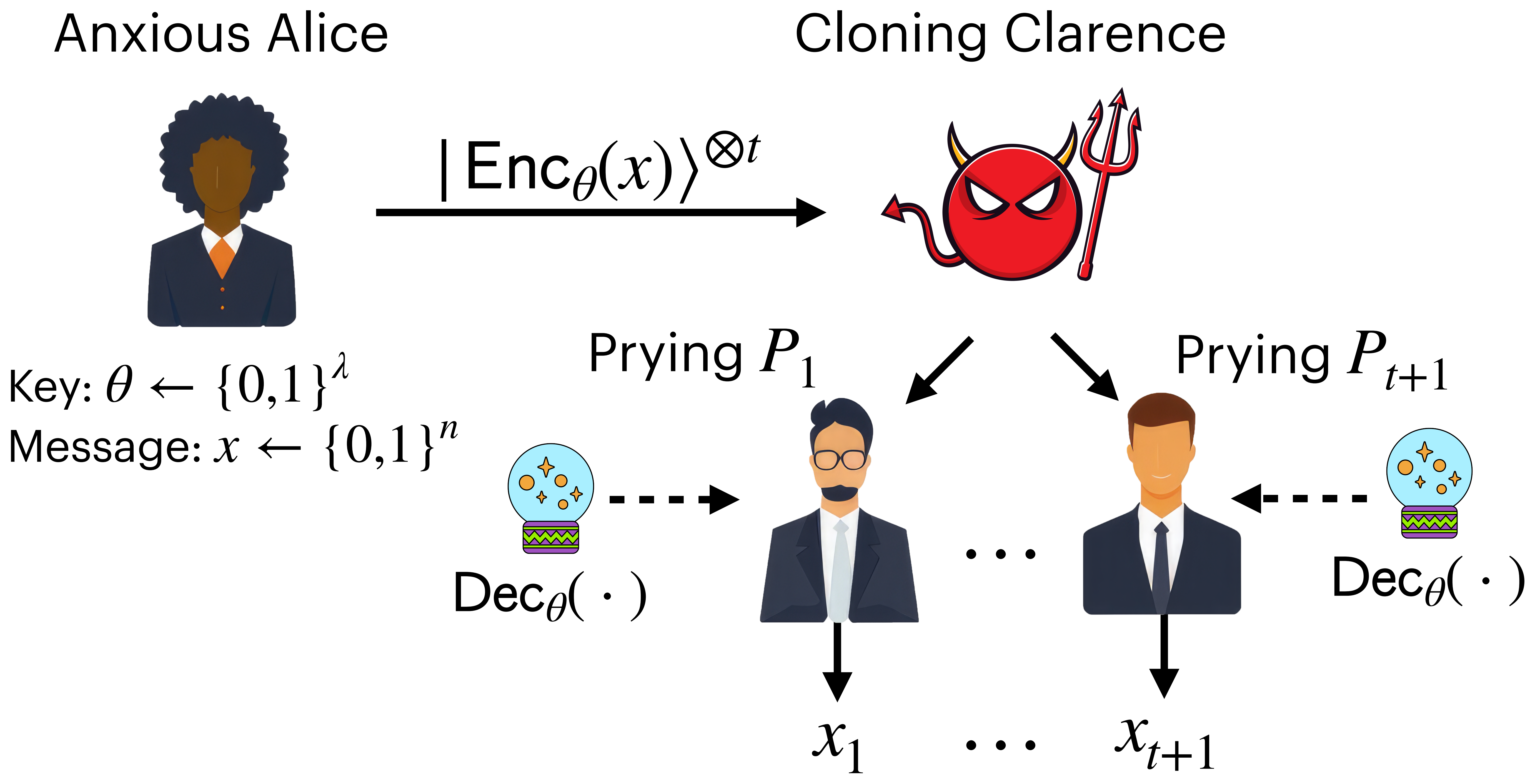
$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle s',a\rangle} |a + s\rangle$$

- Ciphertext state is $|A_x\rangle = |A_{s,s'}\rangle$
- Previous work (CLLZ21, CV22) when $t = 1$:

$$\omega(G) \leq \left(\cos(\pi/8)\right)^{n+o(n)} \approx 2^{(-0.114+o(1))n}$$

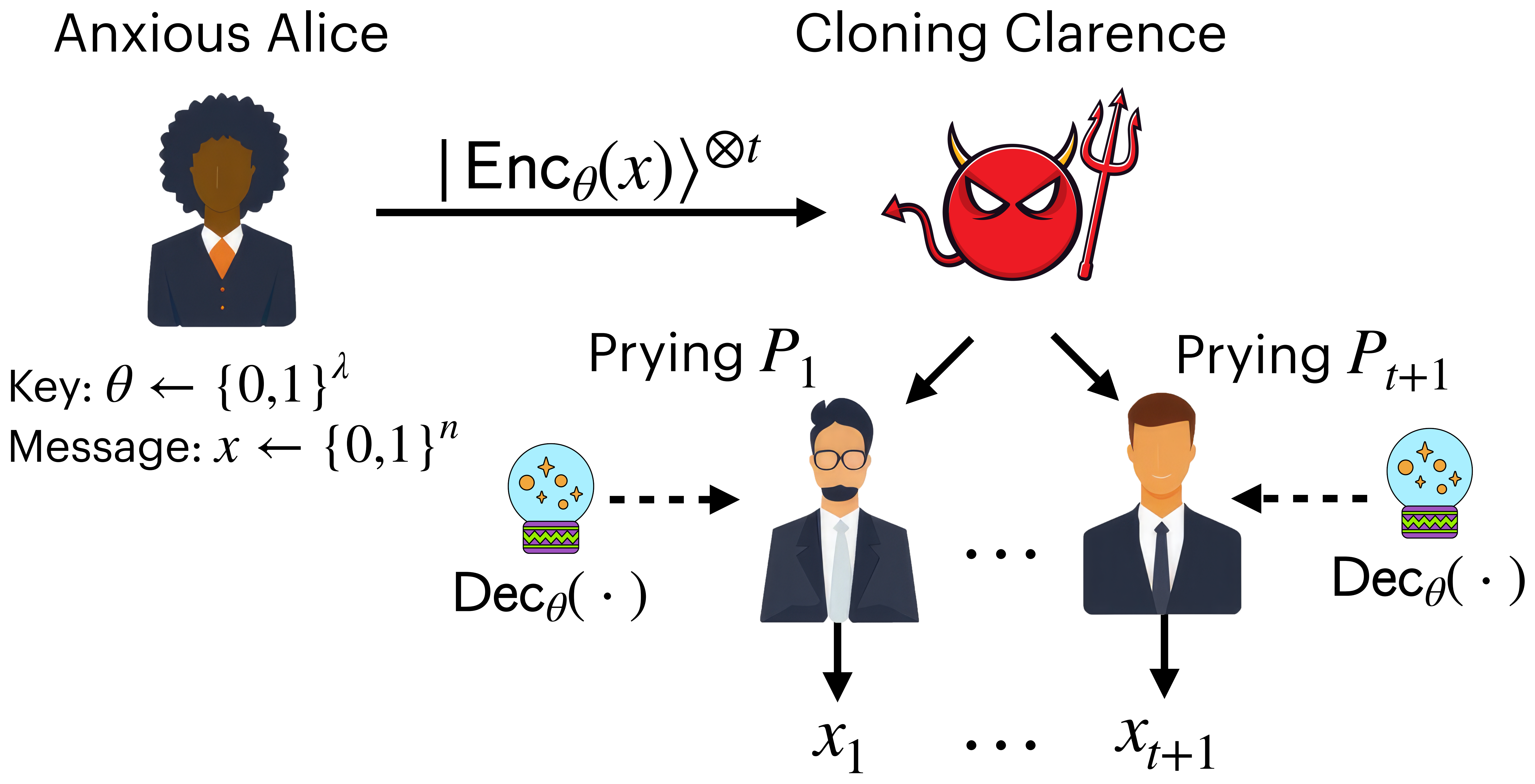
- For $t \gg n$: **completely broken!**
  - Measure $\gg n/2$ copies in the standard basis and $\gg n/2$ copies in the Hadamard basis
  - Measurement results suffice to recover A, s, s'
- $P_1, \ldots, P_{t+1}$ don't need to be told A

Our Model: One Oracle Query



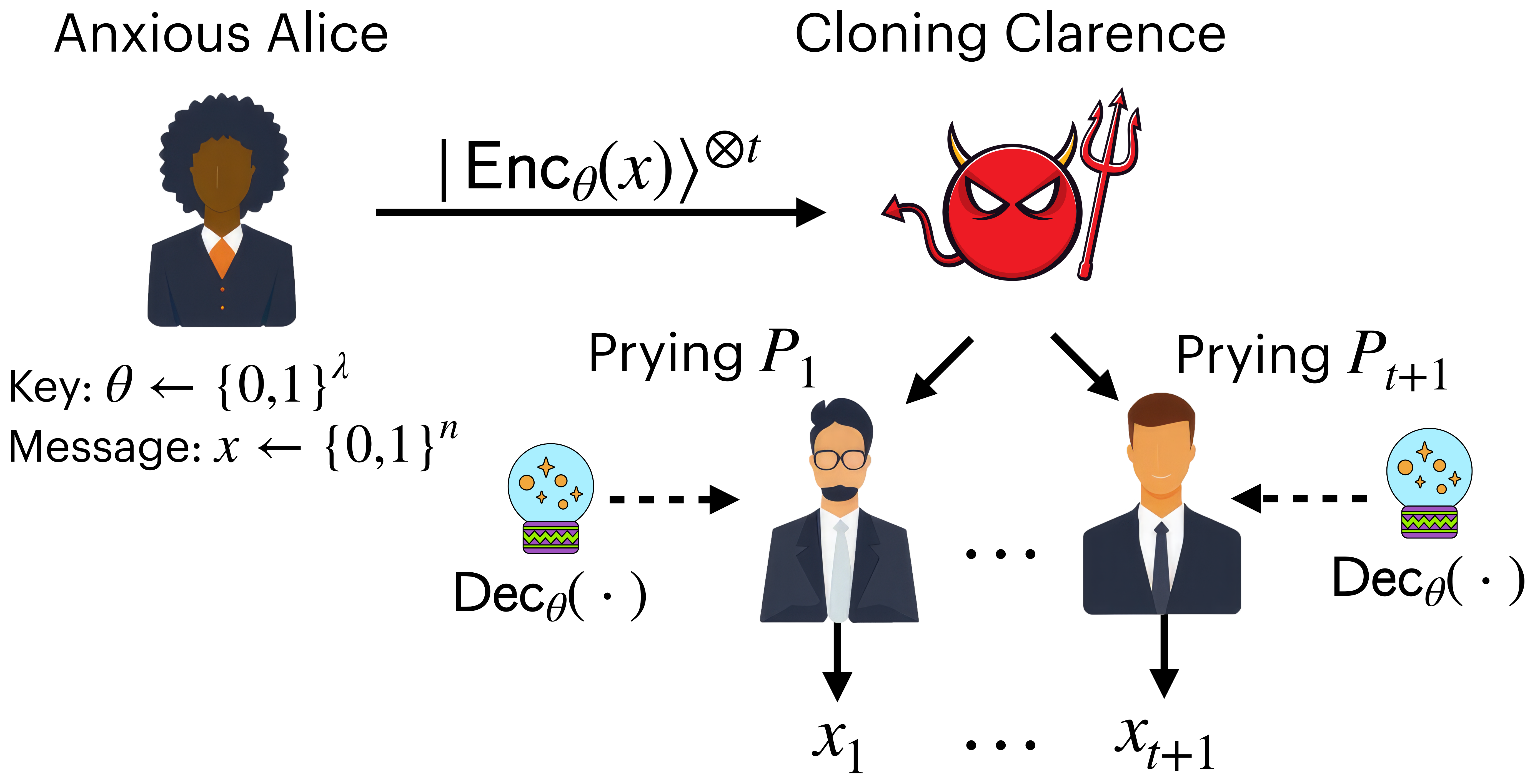
- Each of $P_1, \ldots, P_{t+1}$ is given one oracle query to the decryption functionality

Our Model: One Oracle Query



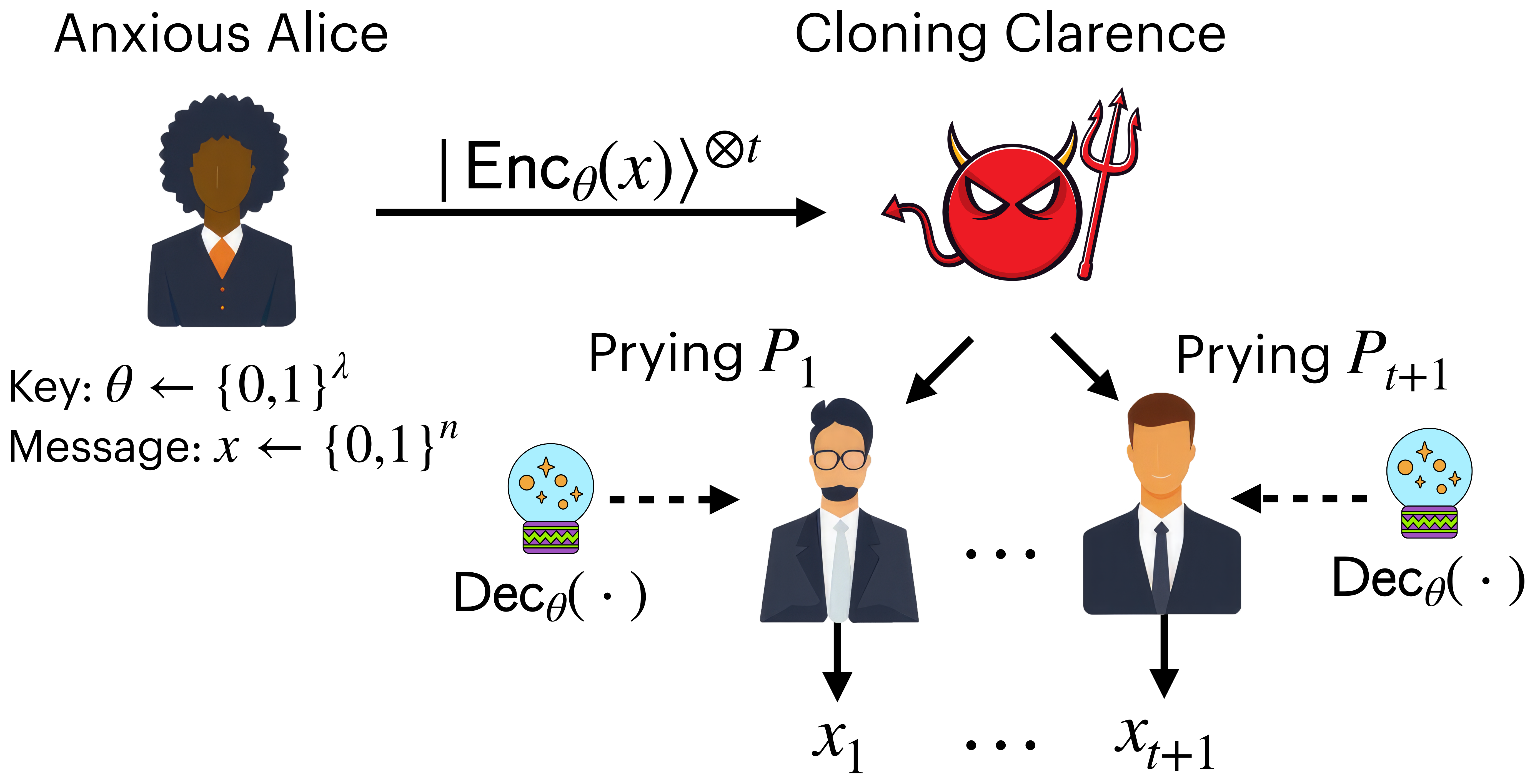
- Each of $P_1, \ldots, P_{t+1}$ is given one oracle query to the decryption functionality
- Not ideal, but oracle models have been used in other works on unclonable encryption

Our Model: One Oracle Query



- Each of $P_1, \ldots, P_{t+1}$ is given one oracle query to the decryption functionality
- Not ideal, but oracle models have been used in other works on unclonable encryption
- Still enables the trivial 2^{-n} strategy

Our Model: One Oracle Query



- Each of $P_1, \ldots, P_{t+1}$ is given one oracle query to the decryption functionality
- Not ideal, but oracle models have been used in other works on unclonable encryption
- Still enables the trivial 2^{-n} strategy
- Still enables attacks on learnable classes of states

Our Results

- First candidate unclonable encryption scheme which is plausibly multi-copy search secure for any $t = \mathsf{poly}(n)$

Our Results

- First candidate unclonable encryption scheme which is plausibly multi-copy search secure for any $t = \mathsf{poly}(n)$
  - Based on *binary phase states,* which are pseudorandom → unlearnable

Our Results

- First candidate unclonable encryption scheme which is plausibly multi-copy search secure for any $t = \mathsf{poly}(n)$
  - Based on *binary phase states,* which are pseudorandom $\rightarrow$ unlearnable
  - Evidence towards this scheme's security: a proof when $t \ll n/\log n$ in the single-oracle-query model

Our Results

- First candidate unclonable encryption scheme which is plausibly multi-copy search secure for any $t = \mathsf{poly}(n)$
  - Based on *binary phase states,* which are pseudorandom → unlearnable
  - Evidence towards this scheme's security: a proof when $t \ll n/\log n$ in the single-oracle-query model
  - In fact: for any constant *t*, the success probability in the single-oracle-query model is $O(2^{-n})$ → essentially tight!

Our Results

- First candidate unclonable encryption scheme which is plausibly multi-copy search secure for any $t = \mathsf{poly}(n)$
    - Based on *binary phase states,* which are pseudorandom → unlearnable
    - Evidence towards this scheme's security: a proof when $t \ll n/\log n$ in the single-oracle-query model
    - In fact: for any constant t, the success probability in the single-oracle-query model is $O(2^{-n})$ → essentially tight!
        - Previous work (BL20) showed how to do this for $t = 1$ with large ciphertext states ($> n$ qubits), but our ciphertext states only comprise n qubits

Our Results

- First candidate unclonable encryption scheme which is plausibly multi-copy search secure for any $t = \text{poly}(n)$
  - Based on *binary phase states,* which are pseudorandom → unlearnable
  - Evidence towards this scheme's security: a proof when $t \ll n/\log n$ in the single-oracle-query model
  - In fact: for any constant t, the success probability in the single-oracle-query model is $O(2^{-n})$ → essentially tight!
    - Previous work (BL20) showed how to do this for $t = 1$ with large ciphertext states ($> n$ qubits), but our ciphertext states only comprise n qubits
- Application of our $t = 1$ result to black hole physics (Hawking radiation decoding)
  - Relies on the above properties

Unclonable Encryption, Through the Years

Authors	Security	Copies	Assumptions	Other caveats
Broadbent-Lord ‘20	Search	1		

Unclonable Encryption, Through the Years

Authors	Security	Copies	Assumptions	Other caveats
Broadbent-Lord ‘20	Search	1		
Ananth-Kaleoglu-Li-Liu-Zhandry ‘22	IND	1	Random oracle	
Ananth-Kaleoglu-Yuen ‘24	IND	1		Quantum decryption keys

Unclonable Encryption, Through the Years

Authors	Security	Copies	Assumptions	Other caveats
Broadbent-Lord '20	Search	1		
Ananth-Kaleoglu-Li-Liu-Zhandry '22	IND	1	Random oracle	
Ananth-Kaleoglu-Yuen '24	IND	1		Quantum decryption keys
Our work	**Search**	$o(n/\log n)$	**Adversaries only get one oracle query to Dec**	

Unclonable Encryption, Through the Years

Authors	Security	Copies	Assumptions	Other caveats
Broadbent-Lord ‘20	Search	1		
Ananth-Kaleoglu-Li-Liu-Zhandry ‘22	IND	1	Random oracle	
Ananth-Kaleoglu-Yuen ‘24	IND	1		Quantum decryption keys
Our work	**Search**	$o(n/\log n)$	**Adversaries only get one oracle query to Dec**	
Bhattacharya-Culf ‘25	IND	1		Distinguishing advantage $1/\text{poly}(\lambda)$

Unclonable Encryption, Through the Years

Authors	Security	Copies	Assumptions	Other caveats
Broadbent-Lord '20	Search	1		
Ananth-Kaleoglu-Li-Liu-Zhandry '22	IND	1	Random oracle	
Ananth-Kaleoglu-Yuen '24	IND	1		Quantum decryption keys
Our work	**Search**	$o(n/\log n)$	**Adversaries only get one oracle query to Dec**	
Bhattacharya-Culf '25	IND	1		Distinguishing advantage $1/\text{poly}(\lambda)$
Çakan-Goyal-Kitagawa-Nishimaki-Yamakawa '25	Search	Unbounded poly!	IO, OWFs	

Our Construction and Analysis

Pseudorandom States

- Function Gen which maps λ-bit strings to n-qubit states

Pseudorandom States

- Function Gen which maps λ-bit strings to n-qubit states
- Goal: the following two distributions are computationally indistinguishable for any $t = \mathsf{poly}(\lambda, n)$:
  - Ideal: $|\psi\rangle^{\otimes t}$ for $|\psi\rangle \leftarrow \text{Haar}(n)$
  - Pseudorandom: $|\mathsf{Gen}(k)\rangle^{\otimes t}$ for $k \leftarrow \{0,1\}^{\lambda}$

Pseudorandom States

- Function Gen which maps λ-bit strings to n-qubit states
- Goal: the following two distributions are computationally indistinguishable for any $t = \mathsf{poly}(\lambda, n)$:
  - Ideal: $|\psi\rangle^{\otimes t}$ for $|\psi\rangle \leftarrow \mathrm{Haar}(n)$
  - Pseudorandom: $|\mathsf{Gen}(k)\rangle^{\otimes t}$ for $k \leftarrow \{0,1\}^\lambda$
- Unclonability properties:
  - Werner '98: Haar random states are multi-copy unclonable

Pseudorandom States

- Function Gen which maps λ-bit strings to n-qubit states
- Goal: the following two distributions are computationally indistinguishable for any $t = \mathsf{poly}(\lambda, n)$:
  - Ideal: $|\psi\rangle^{\otimes t}$ for $|\psi\rangle \leftarrow \text{Haar}(n)$
  - Pseudorandom: $|\mathsf{Gen}(k)\rangle^{\otimes t}$ for $k \leftarrow \{0,1\}^{\lambda}$
- Unclonability properties:
  - Werner '98: Haar random states are multi-copy unclonable
  - Implies pseudorandom states are multi-copy unclonable → a natural candidate for unclonable encryption!

Pseudorandom States: Construction

Ji-Liu-Song '18, Brakerski-Shmueli '19

- Theorem: if $\left\{f_k : \{0,1\}^n \rightarrow \{0,1\} : k \in \{0,1\}^\lambda\right\}$ is a PRF, then

$$|\mathsf{Gen}(k)\rangle = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{f_k(z)} |z\rangle$$

is a pseudorandom state

Pseudorandom States: Construction

Ji-Liu-Song '18, Brakerski-Shmueli '19

- Theorem: if $\left\{f_k : \{0,1\}^n \to \{0,1\} : k \in \{0,1\}^\lambda\right\}$ is a PRF, then

$$|\mathsf{Gen}(k)\rangle = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{f_k(z)} |z\rangle$$

is a pseudorandom state

- Alternate way of writing this: $\frac{1}{2^{n/2}} \mathsf{U}_{f_k} \sum_{z=0}^{2^n-1} |z\rangle = \mathsf{U}_{f_k} \mathsf{H}^{\otimes n} |0^n\rangle$, where

$$\mathsf{U}_f := \sum_{z=0}^{2^n-1} (-1)^{f(z)} |z\rangle\langle z| \text{ is a phase oracle for } f$$

Unclonable Encryption from Pseudorandom States

- Secret-key encryption using a PRG: $\mathsf{Enc}_k(m) = m \oplus \mathsf{PRG}(k)$

Unclonable Encryption from Pseudorandom States

- Secret-key encryption using a PRG: $\mathsf{Enc}_k(m) = m \oplus \mathsf{PRG}(k)$
- Our unclonable secret-key encryption using a PRS: very similar!

$$|\mathsf{Enc}_k(x)\rangle = \mathsf{Z}^x|\mathsf{Gen}(k)\rangle = \frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1}(-1)^{\langle x,z\rangle + f_k(z)}|z\rangle = \mathsf{U}_{f_k}\mathsf{H}^{\otimes n}|x\rangle$$

Unclonable Encryption from Pseudorandom States

- Secret-key encryption using a PRG: $\mathsf{Enc}_k(m) = m \oplus \mathsf{PRG}(k)$
- Our unclonable secret-key encryption using a PRS: very similar!

$$|\mathsf{Enc}_k(x)\rangle = \mathsf{Z}^x|\mathsf{Gen}(k)\rangle = \frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1}(-1)^{\langle x,z\rangle + f_k(z)}|z\rangle = \mathsf{U}_{f_k}\mathsf{H}^{\otimes n}|x\rangle$$

- Decryption simply applies $\mathsf{H}^{\otimes n}\mathsf{U}_{f_k}$ and measures in the standard basis

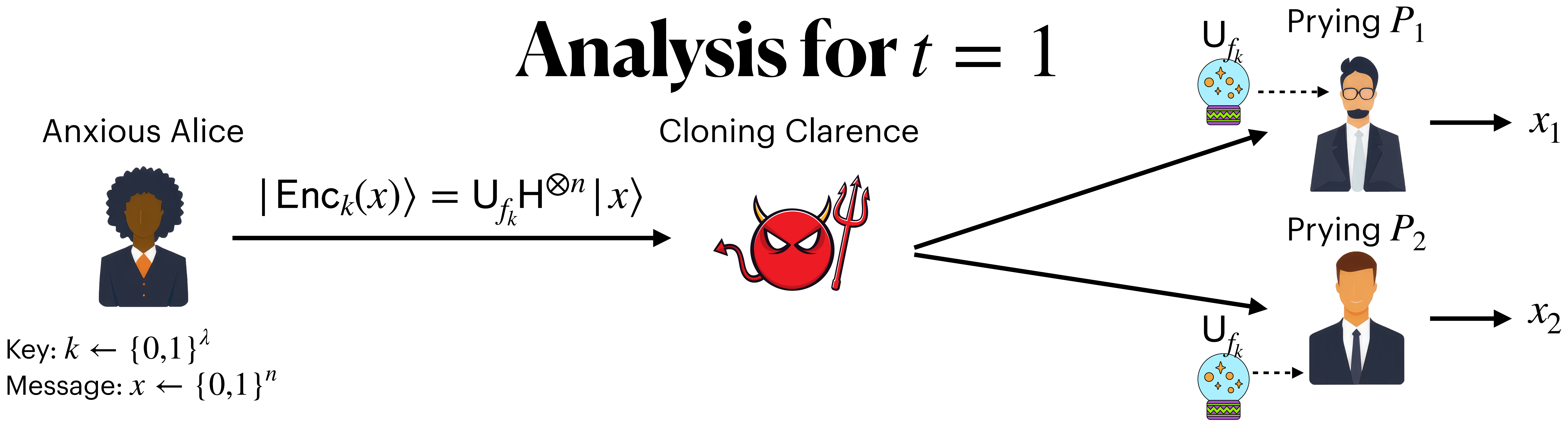
Unclonable Encryption from Pseudorandom States

- Secret-key encryption using a PRG: $\mathsf{Enc}_k(m) = m \oplus \mathsf{PRG}(k)$
- Our unclonable secret-key encryption using a PRS: very similar!

$$|\mathsf{Enc}_k(x)\rangle = \mathsf{Z}^x |\mathsf{Gen}(k)\rangle = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{\langle x,z\rangle + f_k(z)} |z\rangle = \mathsf{U}_{f_k} \mathsf{H}^{\otimes n} |x\rangle$$

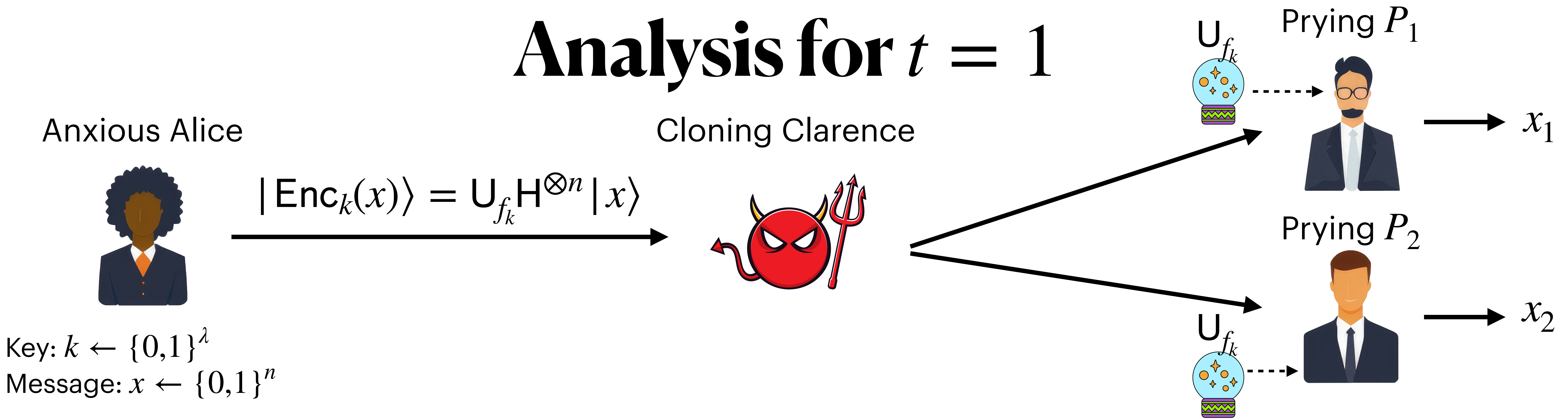
- Decryption simply applies $\mathsf{H}^{\otimes n}\mathsf{U}_{f_k}$ and measures in the standard basis
- Werner '98: these states are not multi-copy clonable by a computationally bounded adversary
- Our goal is to prove a stronger theorem ("useful no-cloning"): Cloning Clarence cannot construct *any* $t+1$ states that reveal x given k
  - This is why we go to an oracle model

Analysis for $t = 1$



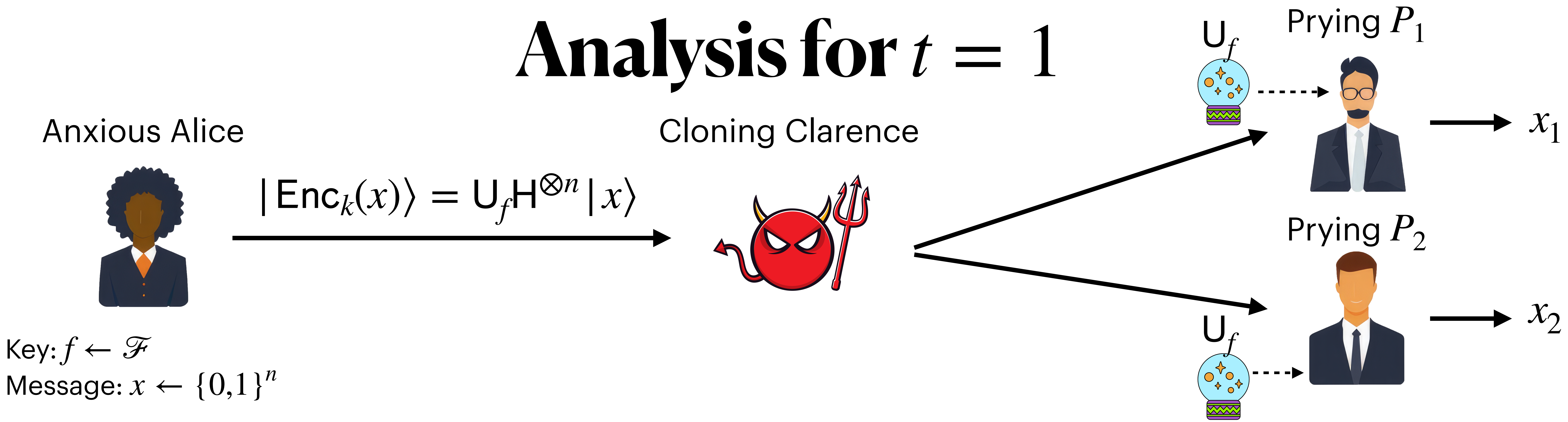
- Step 1: pass from a PRF f_k to a truly random function $f \in \mathcal{F}$ from $\{0,1\}^n \rightarrow \{0,1\}$

Analysis for $t = 1$



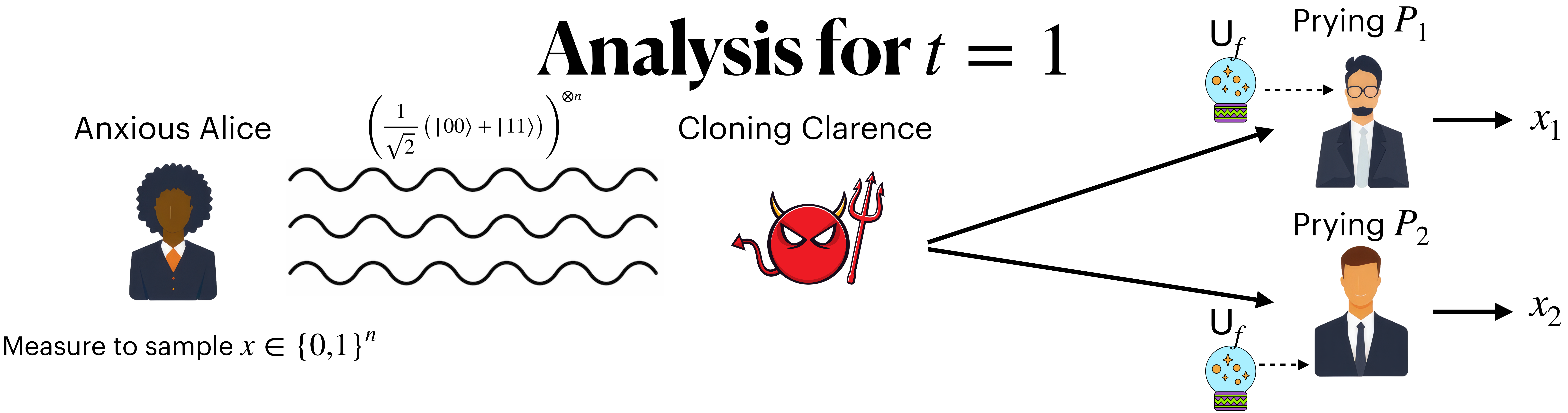
- Step 1: pass from a PRF f_k to a truly random function $f \in \mathscr{F}$ from $\{0,1\}^n \to \{0,1\}$
- This is the only step where we will use the fact that the adversaries are computationally bounded

Analysis for $t = 1$



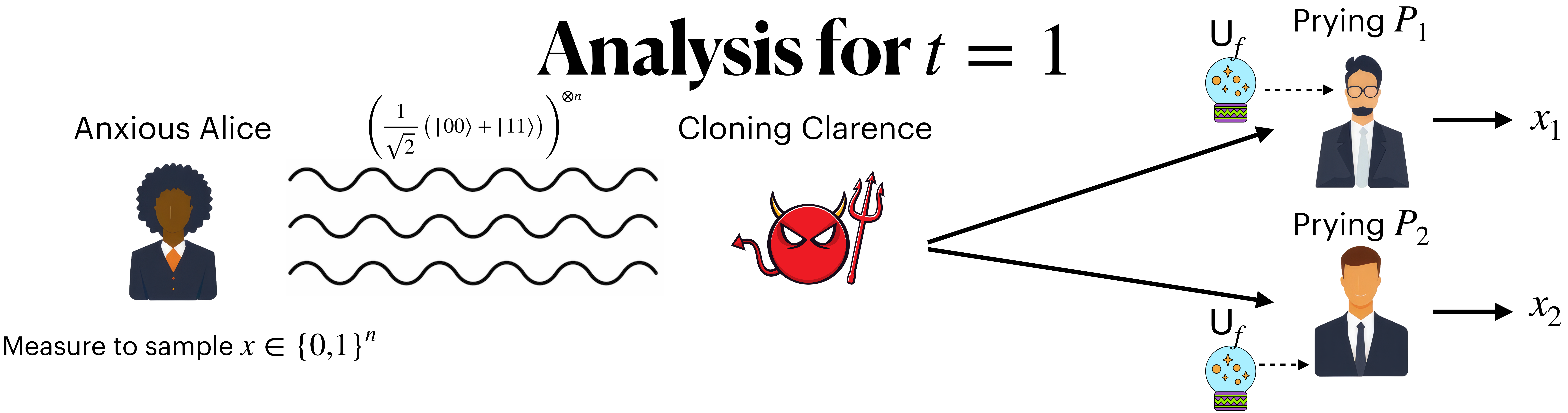
- Step 2: switch to an entanglement-based formulation where Alice and Clarence begin the game sharing entangled qubits

Analysis for $t = 1$



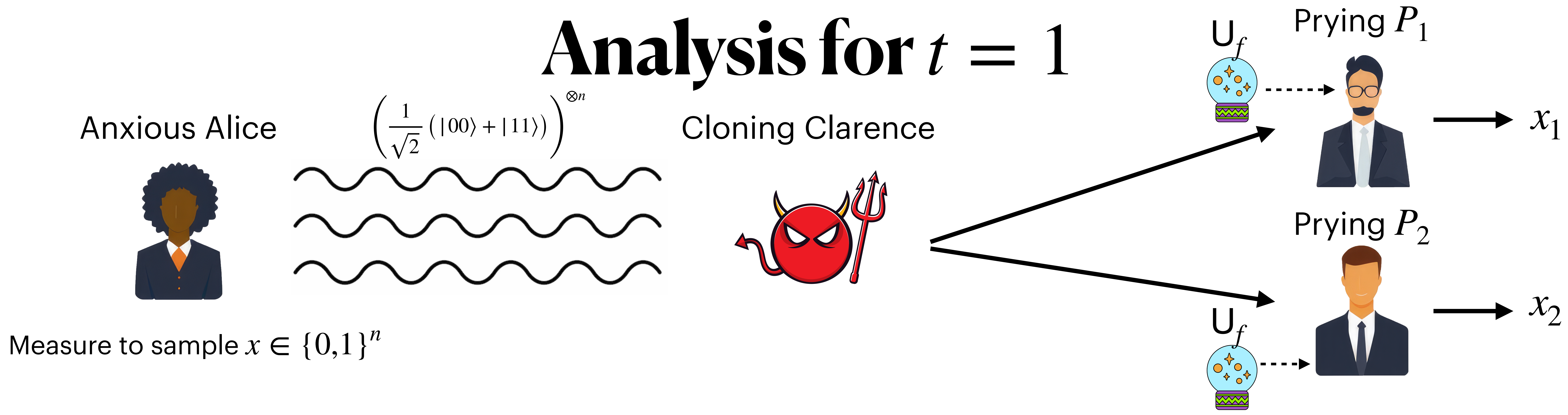
1. Clarence can act arbitrarily on his half of the EPR pair and forward some states to P_1, P_2

Analysis for $t = 1$



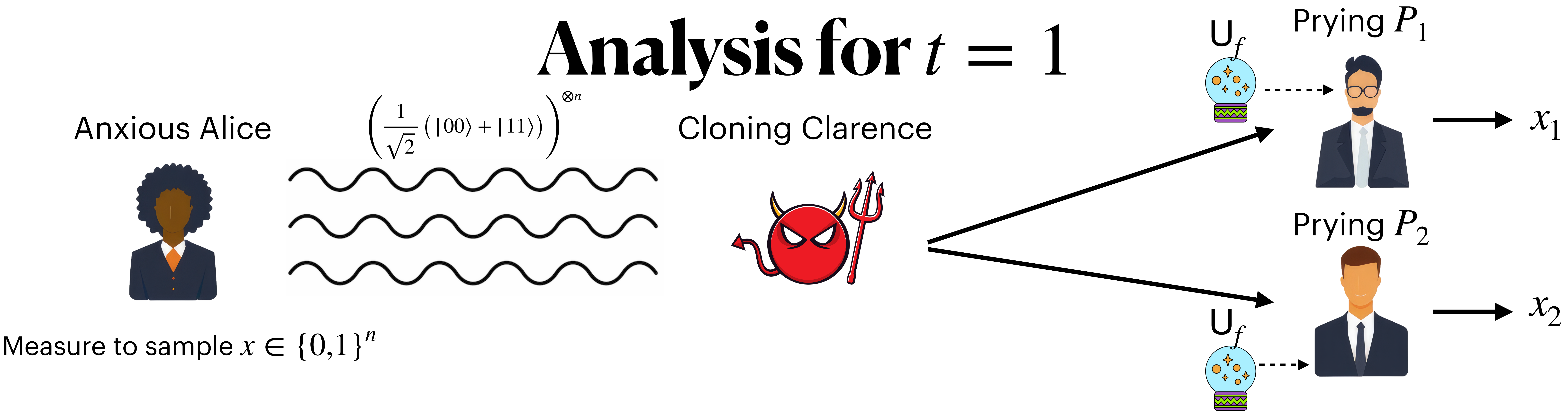
1. Clarence can act arbitrarily on his half of the EPR pair and forward some states to P_1, P_2
2. Alice samples $f \leftarrow \mathscr{F}$, applies $\mathsf{H}^{\otimes n}\mathsf{U}_f$ to her half, and measures it (in the standard basis)

Analysis for $t = 1$



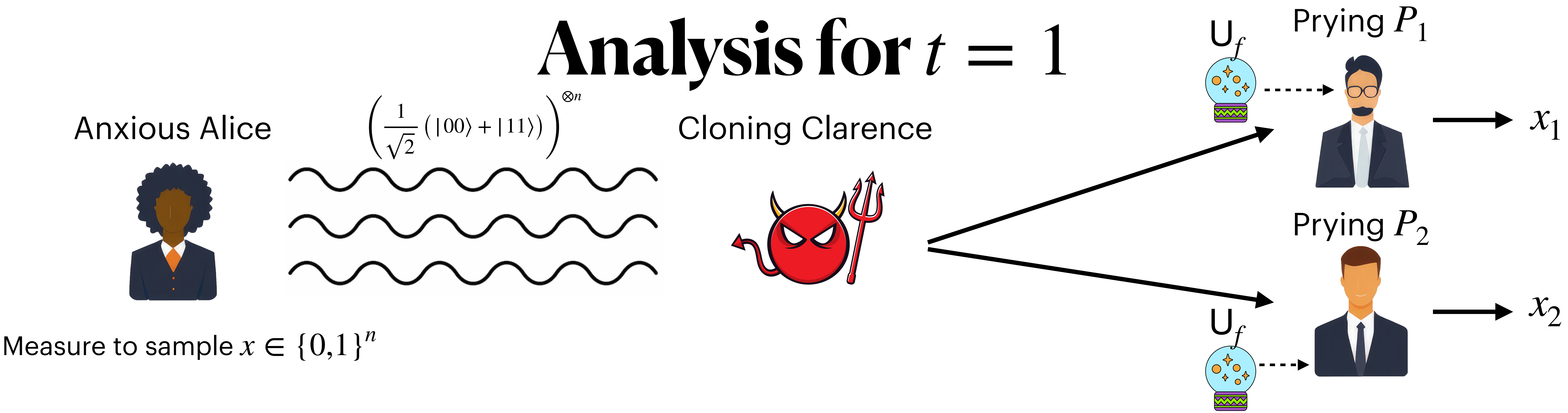
1. Clarence can act arbitrarily on his half of the EPR pair and forward some states to P_1, P_2
2. Alice samples $f \leftarrow \mathscr{F}$, applies $\mathsf{H}^{\otimes n}\mathsf{U}_f$ to her half, and measures it (in the standard basis)
3. P_1, P_2 make one query to U_f and output their guesses. Win if $x_1 = x_2 = x$.

Analysis for $t = 1$



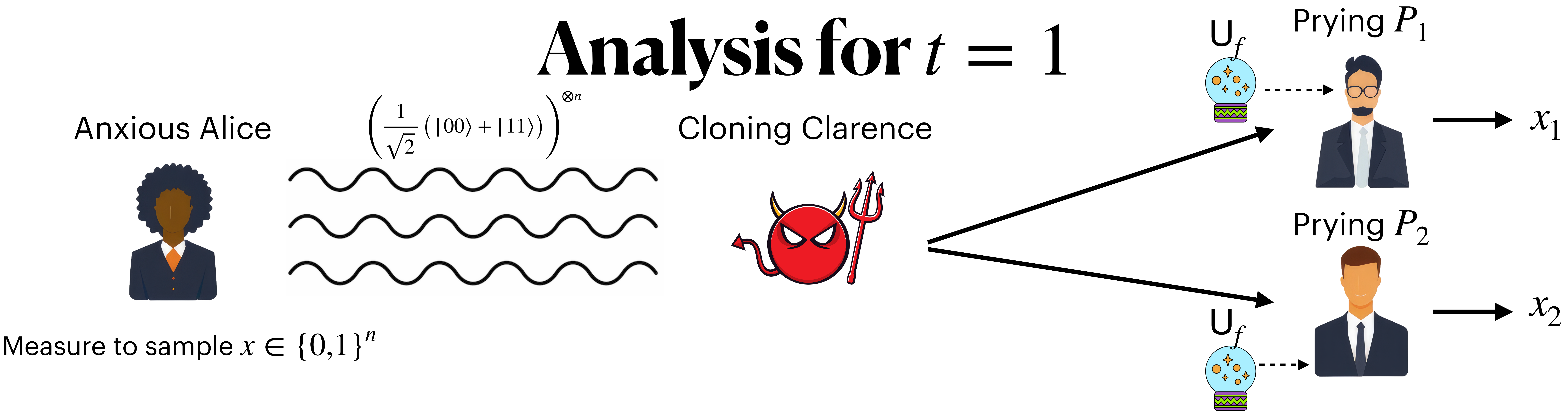
- This is a monogamy-of-entanglement (MOE) game

Analysis for $t = 1$



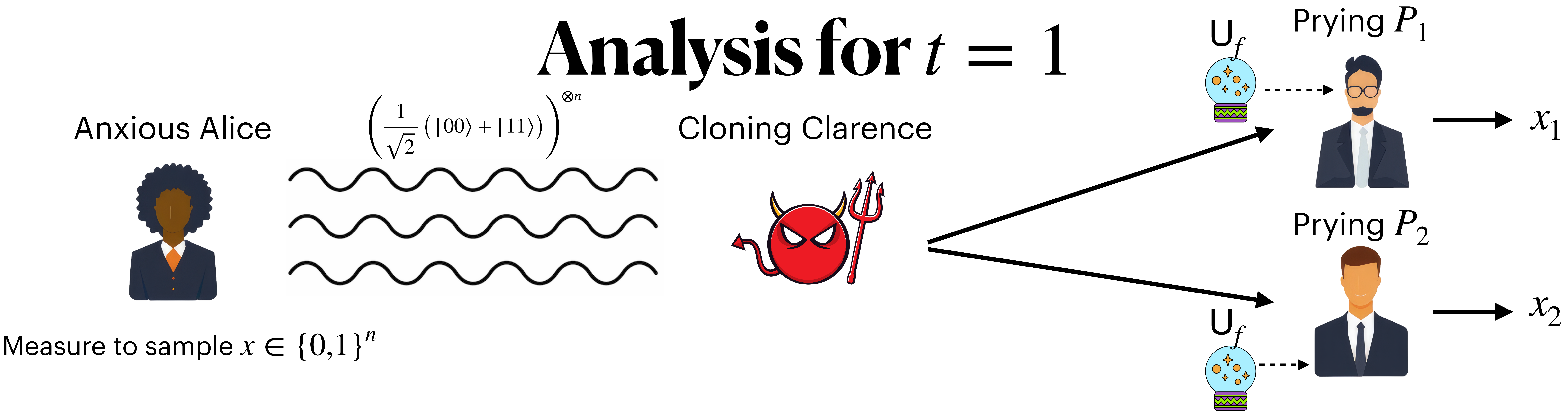
- This is a <u>monogamy-of-entanglement (MOE) game</u>
- Existing techniques for analysing MOE games (TFKW'13) face two problems:

Analysis for $t = 1$



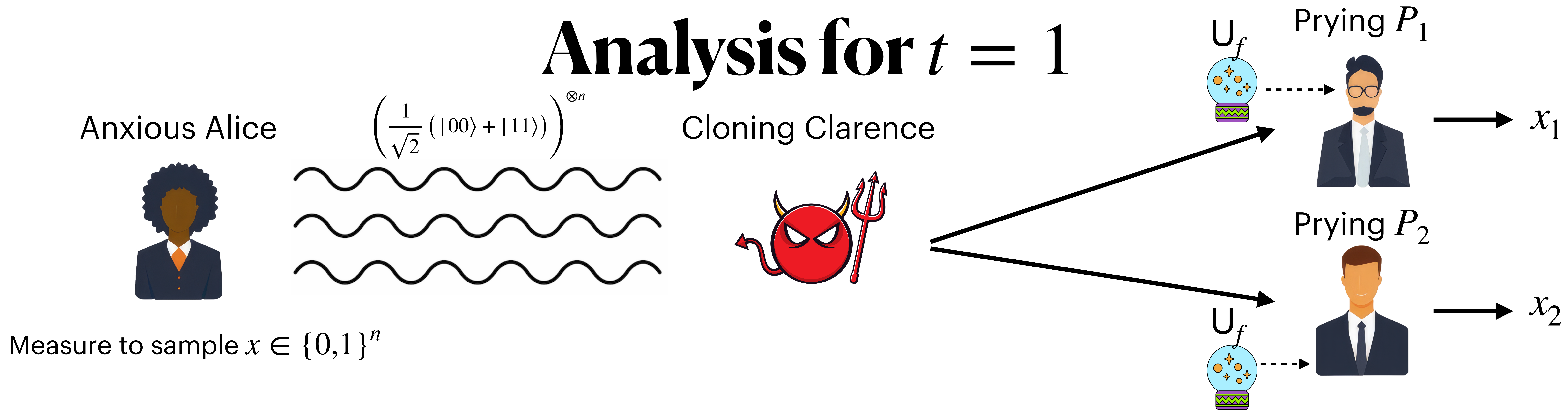
- This is a monogamy-of-entanglement (MOE) game
- Existing techniques for analysing MOE games (TFKW'13) face two problems:
  - Can only ever hope to prove an upper bound of $O(2^{-n/2})$ on winning probability

Analysis for $t = 1$



- This is a <u>monogamy-of-entanglement (MOE) game</u>
- Existing techniques for analysing MOE games (TFKW'13) face two problems:
  - Can only ever hope to prove an upper bound of $O(2^{-n/2})$ on winning probability
  - Cannot prove *any* meaningful bound in the multi-copy case

Analysis for $t = 1$



- This is a monogamy-of-entanglement (MOE) game
- Existing techniques for analysing MOE games (TFKW'13) face two problems:
  - Can only ever hope to prove an upper bound of $O(2^{-n/2})$ on winning probability
  - Cannot prove *any* meaningful bound in the multi-copy case
- Our approach: analyse using binary types (AGQY22) and a novel generalisation called subtypes

New Linear Algebraic Tools

- Analysis boils down to bounding the operator norm of rescaled blockwise tensor product of matrices

New Linear Algebraic Tools

- Analysis boils down to bounding the operator norm of rescaled blockwise tensor product of matrices
- Theorem (this work): let $\left\{\gamma_{i,j} \in \mathbb{C} : 1 \leq i, j \leq R\right\}$ be of magnitude at most 1, and let

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,R} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{R,1} & \cdots & \mathbf{A}_{R,R} \end{bmatrix}, \mathbf{B} = \begin{bmatrix} \mathbf{B}_{1,1} & \cdots & \mathbf{B}_{1,R} \\ \vdots & \ddots & \vdots \\ \mathbf{B}_{R,1} & \cdots & \mathbf{B}_{R,R} \end{bmatrix}$$

be matrices with spectral norm ≤ 1.

New Linear Algebraic Tools

- Analysis boils down to bounding the operator norm of rescaled blockwise tensor product of matrices
- <u>Theorem (this work):</u> let $\left\{\gamma_{i,j} \in \mathbb{C} : 1 \leq i, j \leq R\right\}$ be of magnitude at most 1, and let

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{1,1} & \dots & \mathbf{A}_{1,R} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{R,1} & \dots & \mathbf{A}_{R,R} \end{bmatrix}, \mathbf{B} = \begin{bmatrix} \mathbf{B}_{1,1} & \dots & \mathbf{B}_{1,R} \\ \vdots & \ddots & \vdots \\ \mathbf{B}_{R,1} & \dots & \mathbf{B}_{R,R} \end{bmatrix}$$ be matrices with spectral norm ≤ 1.

- Then

$$\begin{bmatrix} \gamma_{1,1}\mathbf{A}_{1,1} \otimes \mathbf{B}_{1,1} & \dots & \gamma_{1,R}\mathbf{A}_{1,R} \otimes \mathbf{B}_{1,R} \\ \vdots & \ddots & \vdots \\ \gamma_{R,1}\mathbf{A}_{R,1} \otimes \mathbf{B}_{R,1} & \dots & \gamma_{R,R}\mathbf{A}_{R,R} \otimes \mathbf{B}_{R,R} \end{bmatrix}$$ also has spectral norm ≤ 1.

Summary of Our Construction

- Our unclonable encryption scheme: $|\mathsf{Enc}_k(x)\rangle = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{\langle x,z\rangle + f_k(z)} |z\rangle$

Summary of Our Construction

- Our unclonable encryption scheme: $|\mathsf{Enc}_k(x)\rangle = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{\langle x,z\rangle + f_k(z)} |z\rangle$
  - Plausibly multi-copy search secure for any $t = \mathsf{poly}(n)$

Summary of Our Construction

- Our unclonable encryption scheme: $|\mathsf{Enc}_k(x)\rangle = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{\langle x,z\rangle + f_k(z)} |z\rangle$
    - Plausibly multi-copy search secure for any $t = \mathsf{poly}(n)$
    - Evidence towards this scheme's security: in the single-oracle-query model, $\omega(G) \leq 2^{O(t \log t) - n}$

Summary of Our Construction

- Our unclonable encryption scheme: $|\mathsf{Enc}_k(x)\rangle = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{\langle x,z\rangle + f_k(z)} |z\rangle$
  - Plausibly multi-copy search secure for any $t = \mathsf{poly}(n)$
  - Evidence towards this scheme's security: in the single-oracle-query model, $\omega(G) \leq 2^{O(t \log t) - n}$
    - For any constant t: $O(2^{-n}) \rightarrow$ essentially tight
    - For $t \ll n/\log n$: $\mathsf{negl}(n)$

Open Questions

- Proving stronger security for our construction?

Open Questions

- Proving stronger security for our construction?
- Multi-copy security from milder assumptions than IO?

Open Questions

- Proving stronger security for our construction?
- Multi-copy security from milder assumptions than IO?
- IND security in the plain model with classical decryption keys and distinguishing advantage $\mathsf{negl}(\lambda)$?
  - Open even for the single-copy case!