Adaptively Secure Broadcast

Martin Hirt & Vassilis Zikas

ETH Zurich

Eurocrypt 2010

Outline

Talk Outline

- Motivation
- Known Broadcast Protocols
- Our Broadcast Protocols
- Conclusions

Outline

Talk Outline

- Motivation
- Known Broadcast Protocols
- Our Broadcast Protocols
- Conclusions

What is Broadcast

Intuition

- Sender holds some value x
- Every P_i shall learn x

What is Broadcast

Intuition

- Sender holds some value x
- Every P_i shall learn x

Standard Definition (property based)

- **Consistency**: Every player receives the same value x'.
- **Validity**: Sender correct $\Rightarrow x' = x$.
- **Termination**: Every player eventually receives value.

What is Broadcast

Intuition

- Sender holds some value x
- Every P_i shall learn x

Standard Definition (property based)

- **Consistency**: Every player receives the same value x'.
- **Validity**: Sender correct $\Rightarrow x' = x$.
- **Termination**: Every player eventually receives value.

Motivation

What is Broadcast

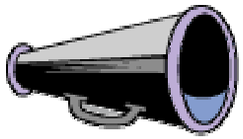
Intuition

- Sender holds some value x
- Every P_i shall learn x

Standard Definition (property based)

- **Consistency**: Every player receives the same value x'.
- **Validity**: Sender correct $\Rightarrow x' = x$.
- **Termination**: Every player eventually receives value.

Motivation



What is Broadcast

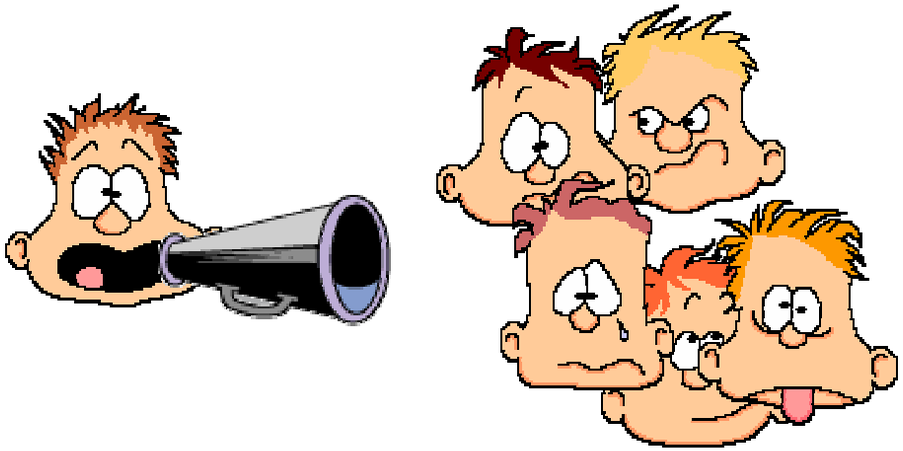
Intuition

- Sender holds some value x
- Every P_i shall learn x

Standard Definition (property based)

- **Consistency**: Every player receives the same value x'.
- **Validity**: Sender correct $\Rightarrow x' = x$.
- **Termination**: Every player eventually receives value.

Motivation



What is Broadcast

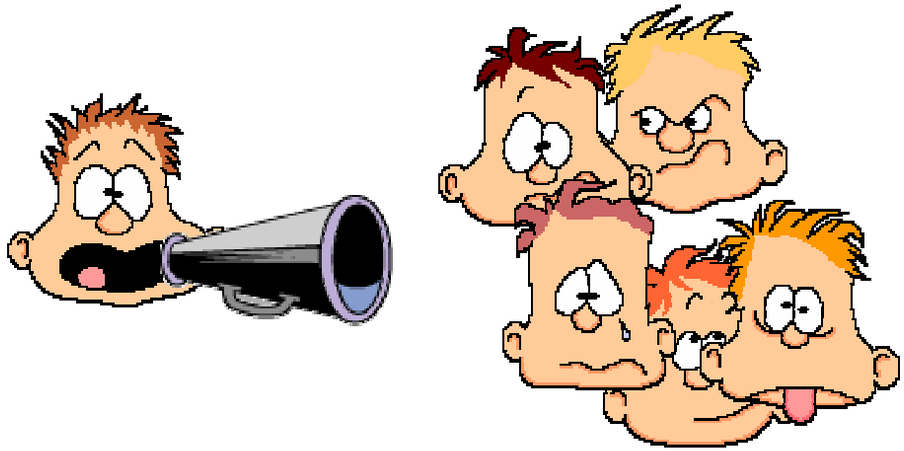
Intuition

- Property-Based Definition $\overset{?}{\approx}$ Megaphone

Standard Definition (property based)

- **Consistency**: Every player receives the same value x'.
- **Validity**: Sender correct $\Rightarrow x' = x$.
- **Termination**: Every player eventually receives value.

Motivation

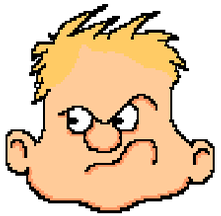
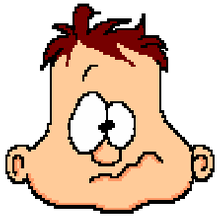
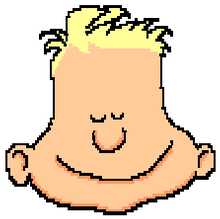


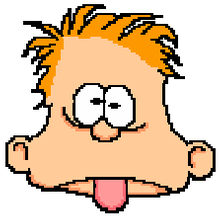
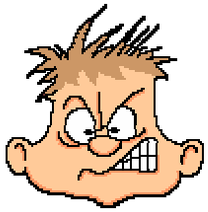
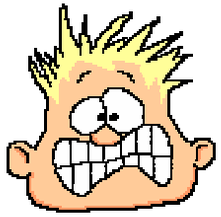
This Work

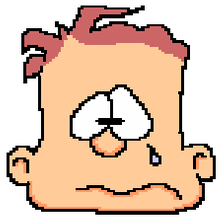
Contributions

1. Property-based definition of broadcast $\not\approx$ megaphone
2. Known broadcast protocols $\not\approx$ megaphone
3. Construct megaphone protocol (perfect / stat. / crypto.)

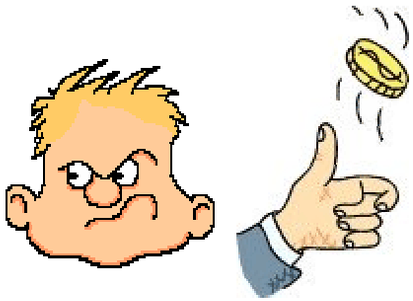
An Example

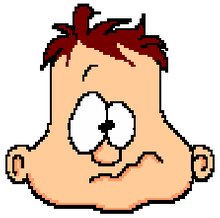




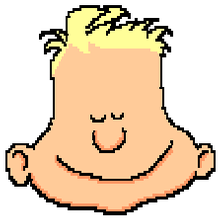




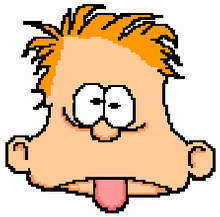


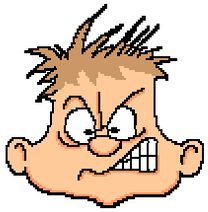

An Example

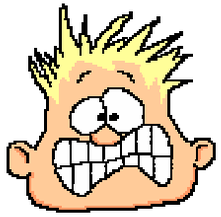


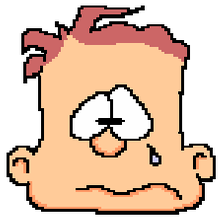




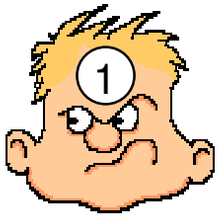


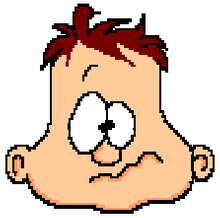


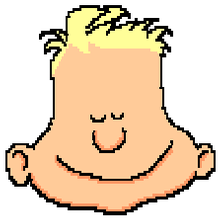


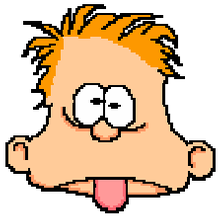


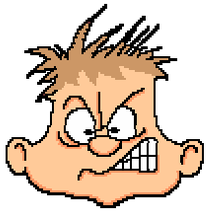
An Example

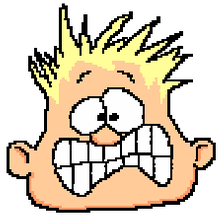


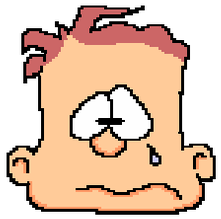




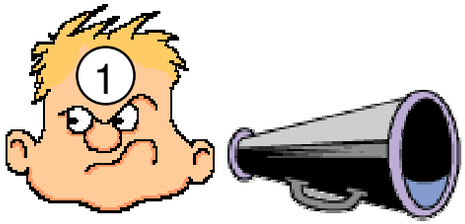




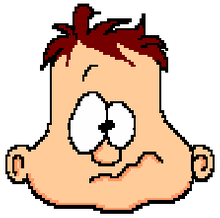


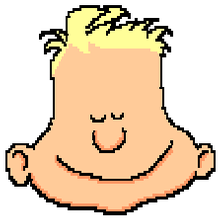


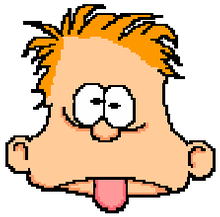
An Example

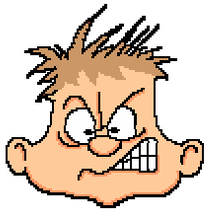


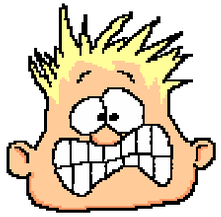
1

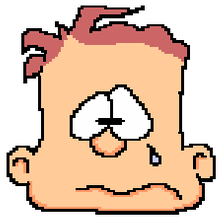




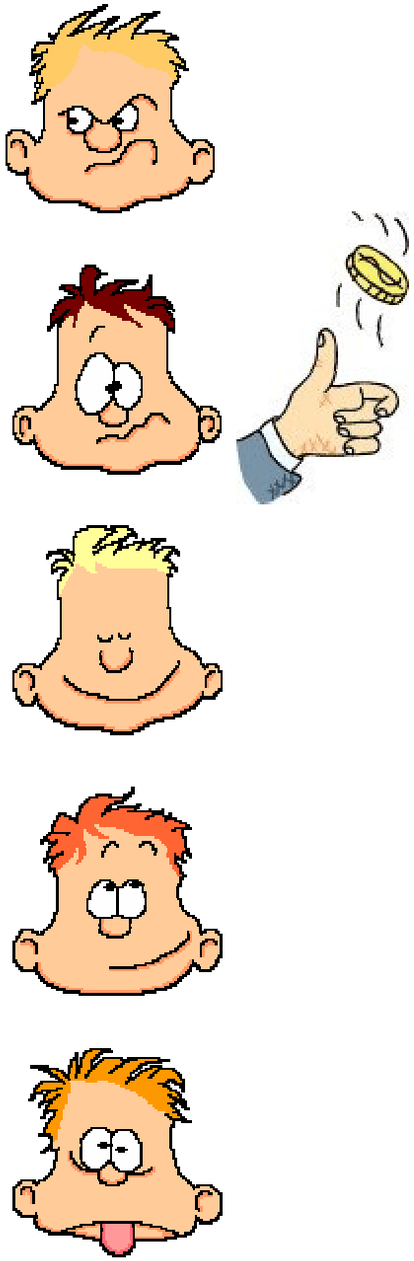






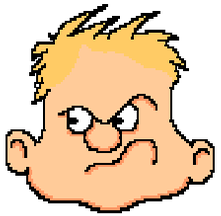


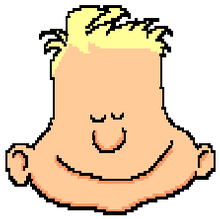
An Example

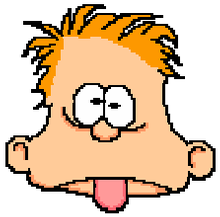


1

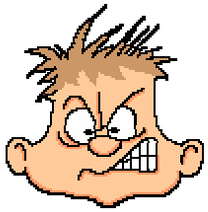
An Example

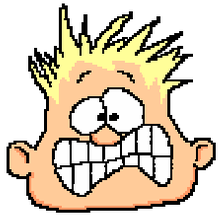


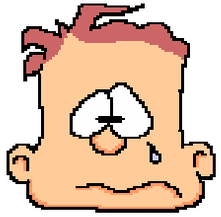




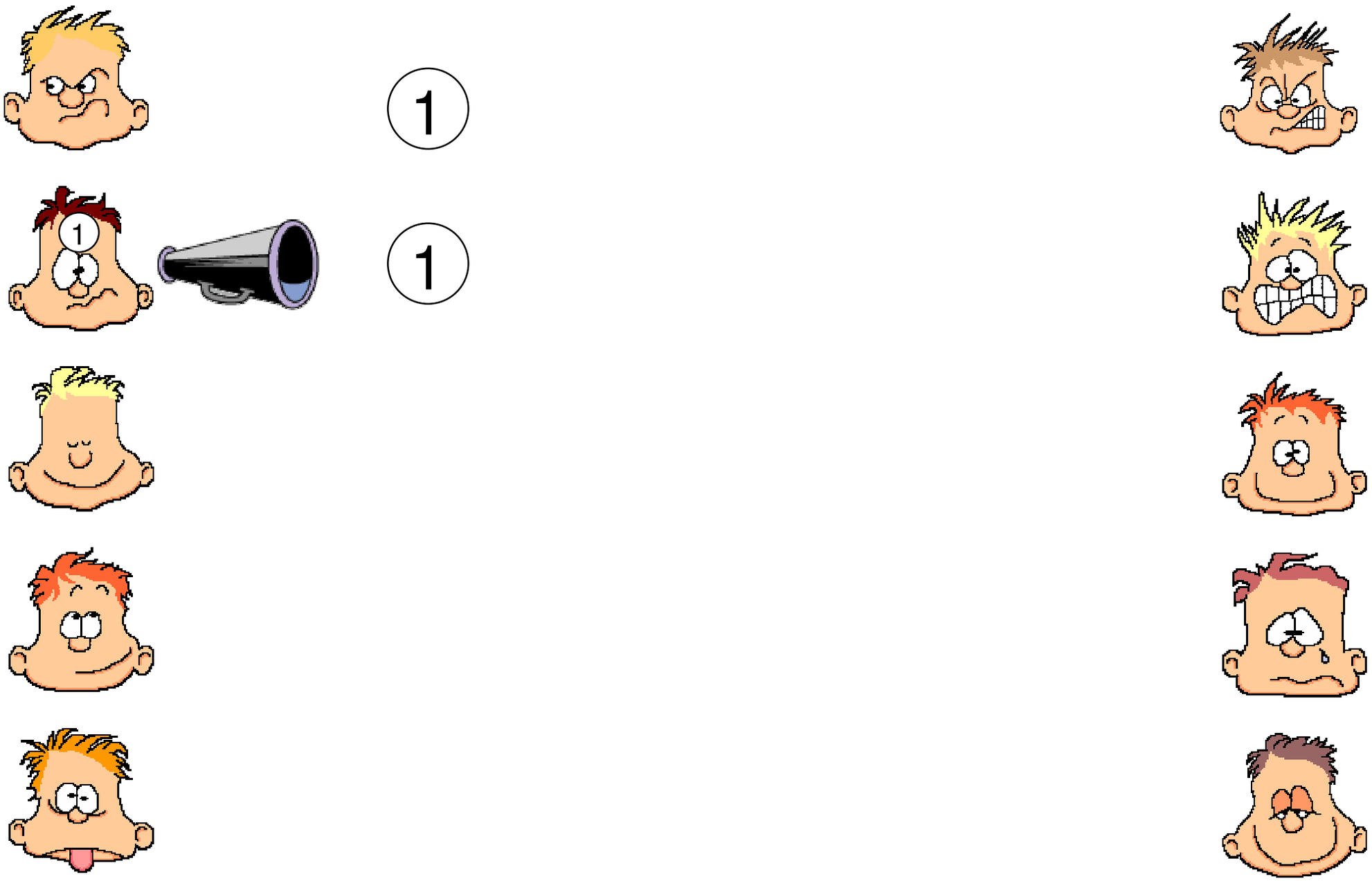
1



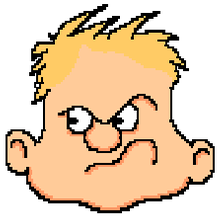




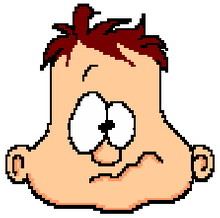
An Example



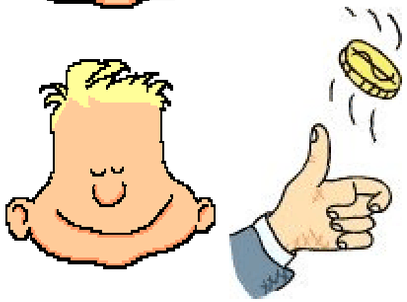
An Example

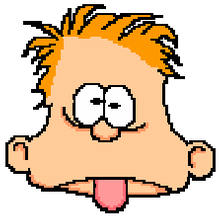


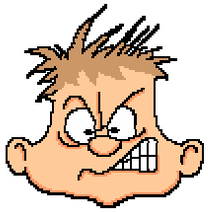
1

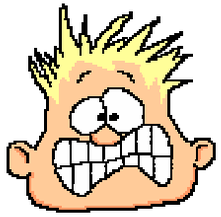


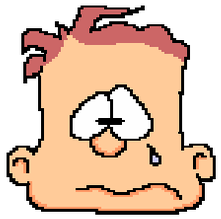
1



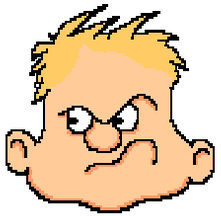




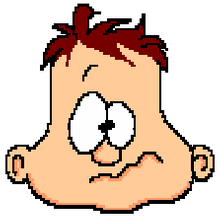




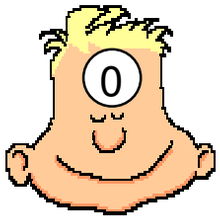
An Example



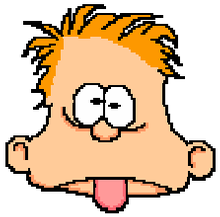
1

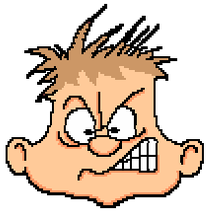


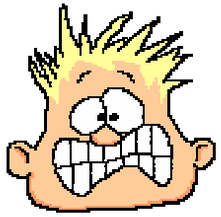
1

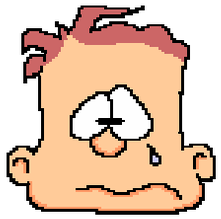


0

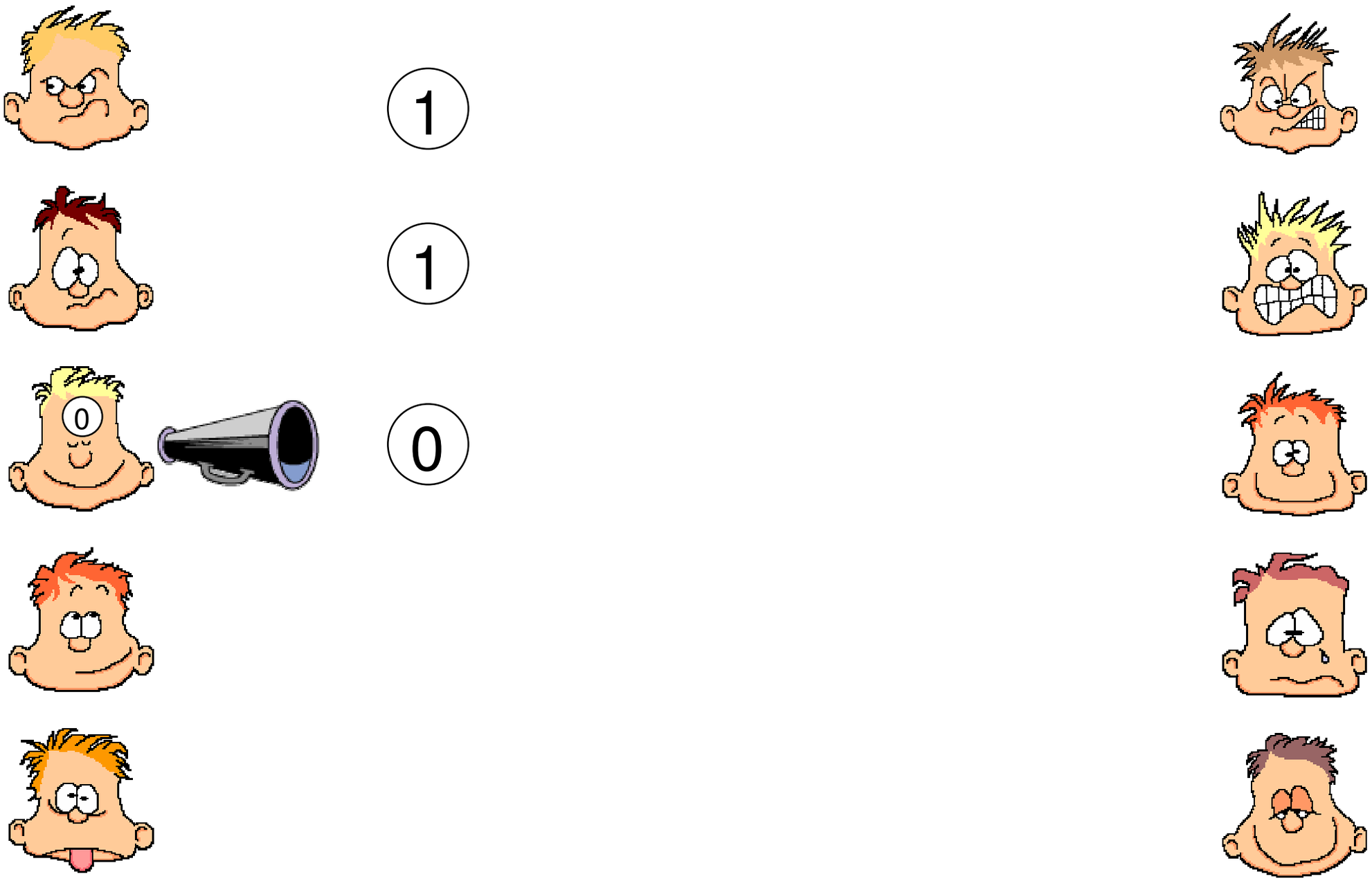




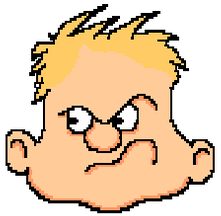




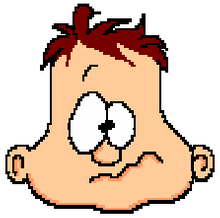
An Example



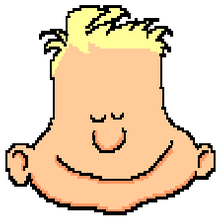
An Example



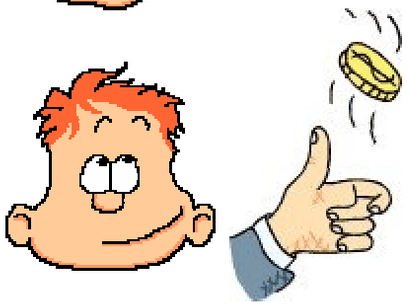
1

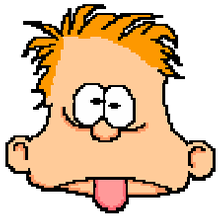


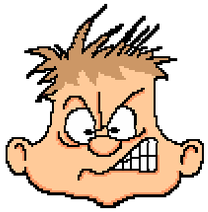
1

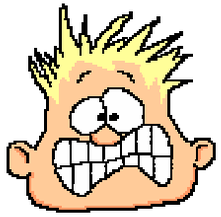


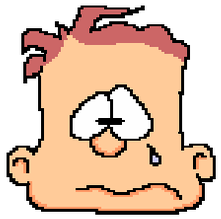
0



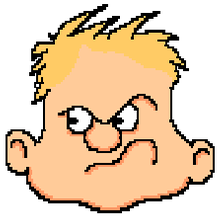




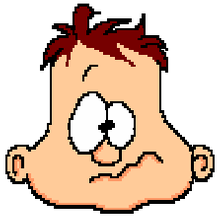




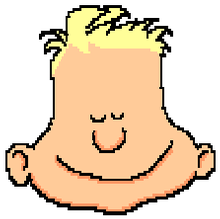
An Example



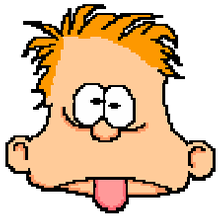
1

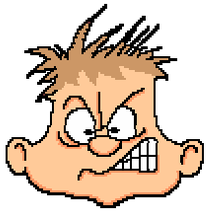


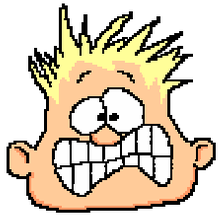
1

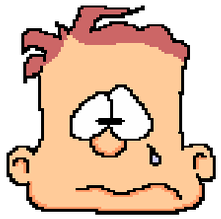


0

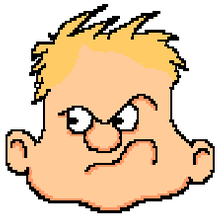




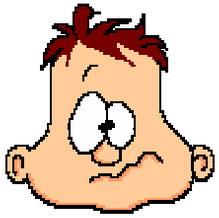




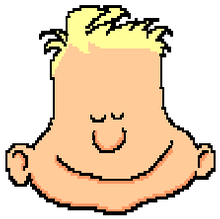
An Example



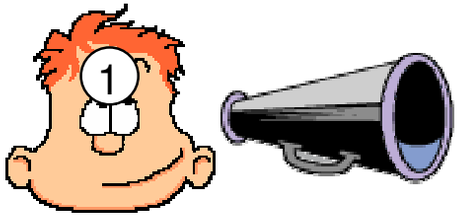
1



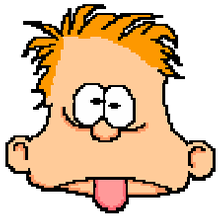
1

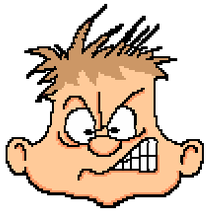


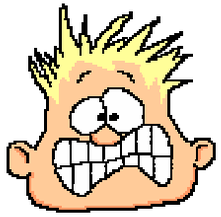
0

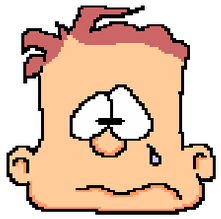


1

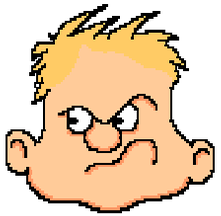




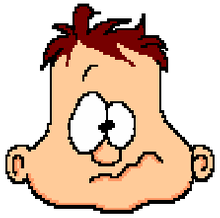




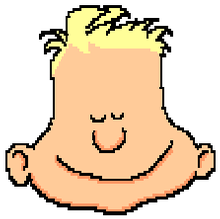
An Example



1

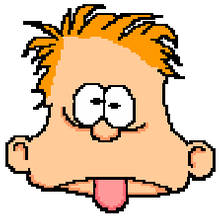


1



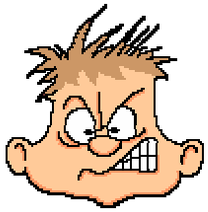
0

1

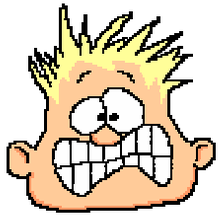


1

1

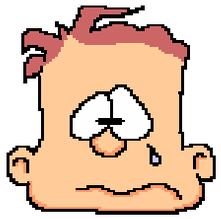


0



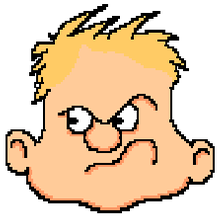
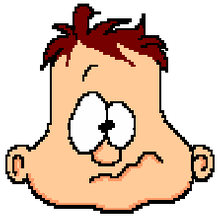
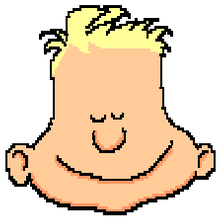
1

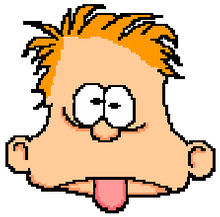
1



0

An Example



1 1

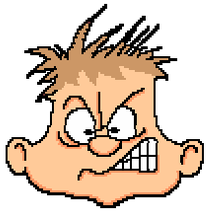
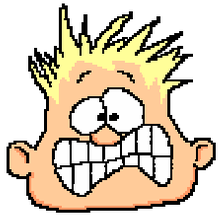
1 0

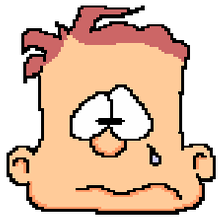
0 1

1 1

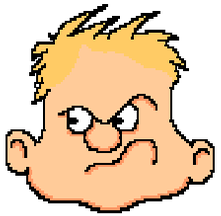
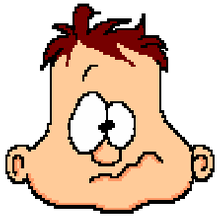
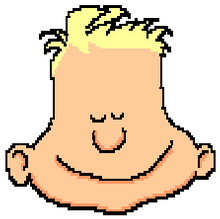
1 0

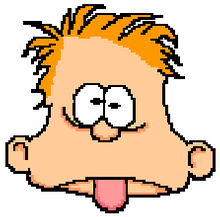
Pr(all coins are 1) = ??




An Example



1 1

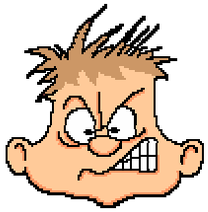
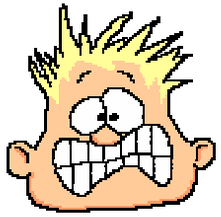
1 0

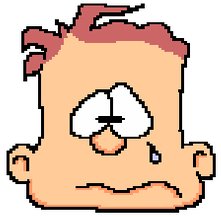
0 1

1 1

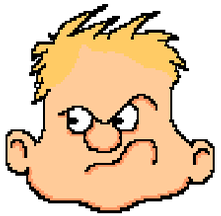
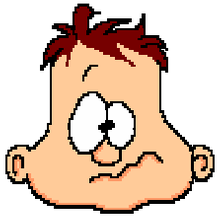
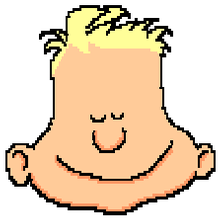
1 0

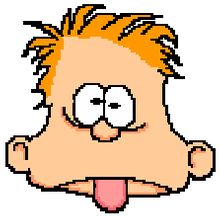
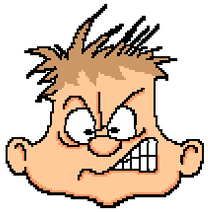
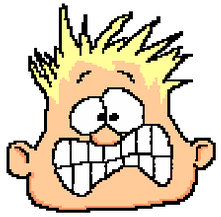
$$\Pr(\text{all coins are } 1) = 2^{-10}$$

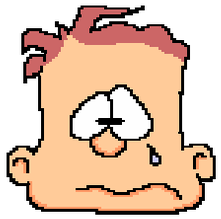





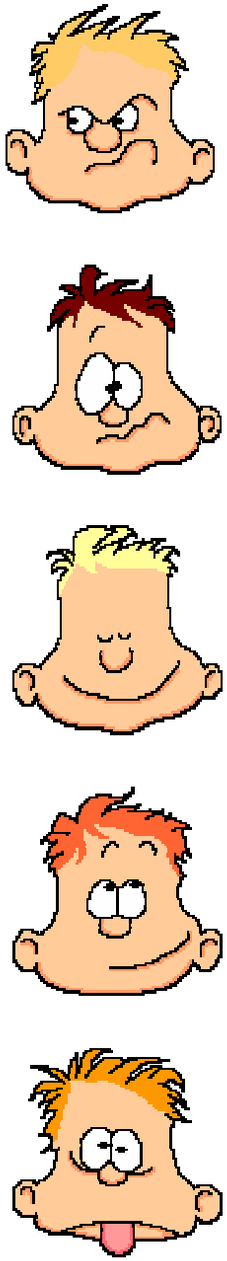

An Example

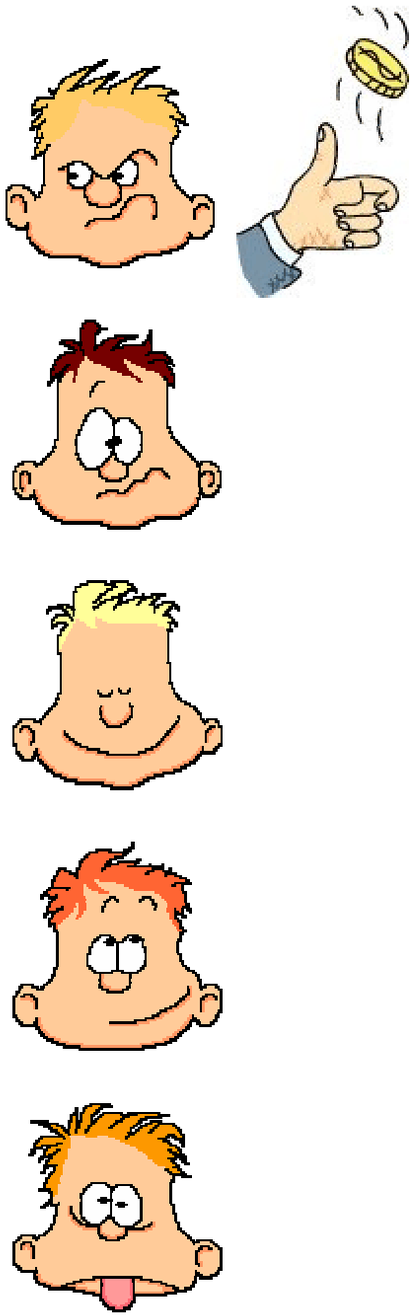



An Example

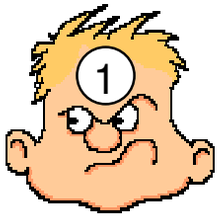


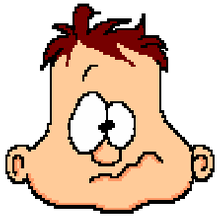
Goal: all coins are 1

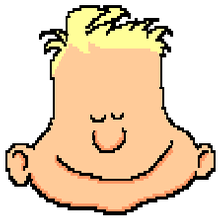
An Example

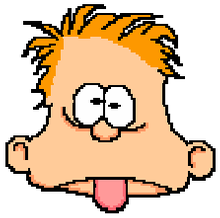


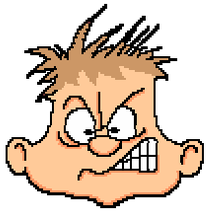
An Example

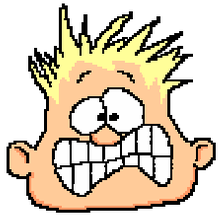


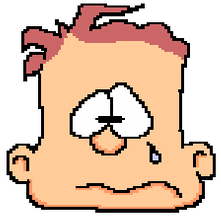




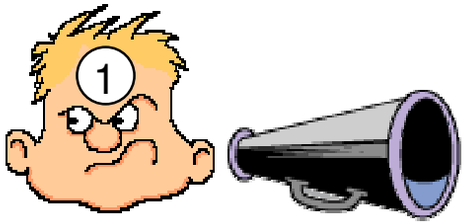




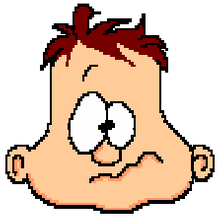


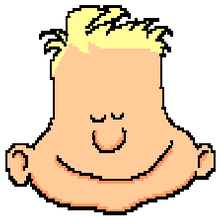


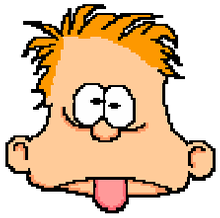
An Example

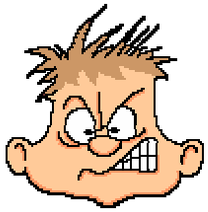


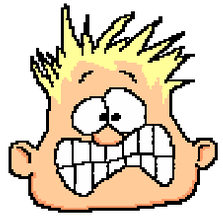
1

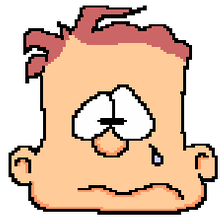




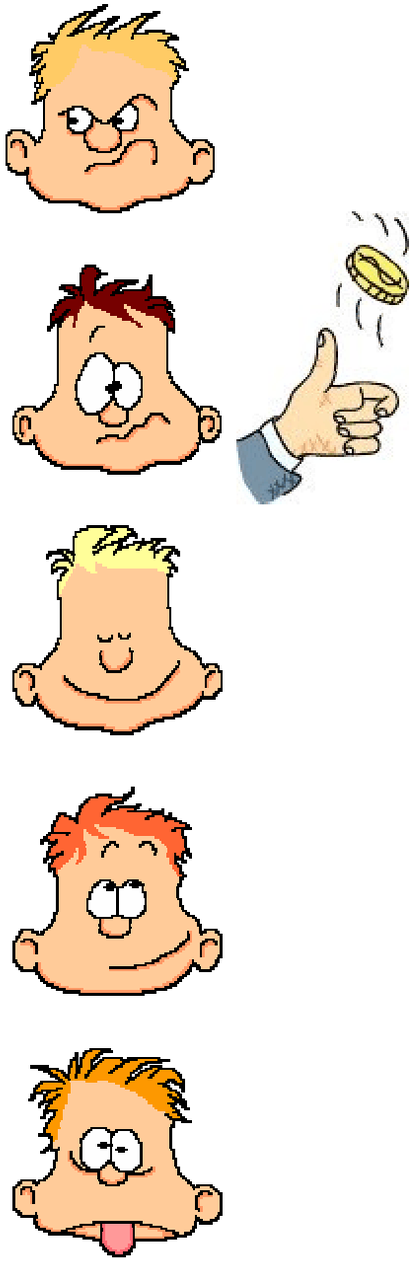






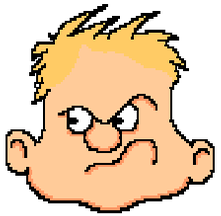


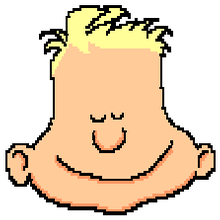
An Example

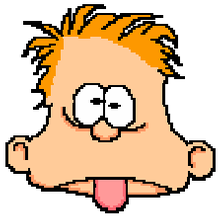


1

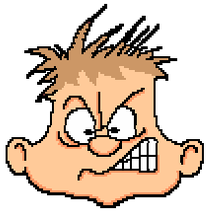
An Example

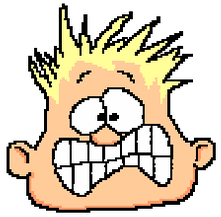


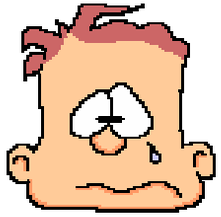




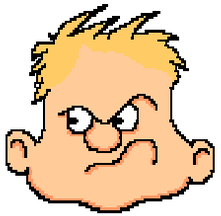
1

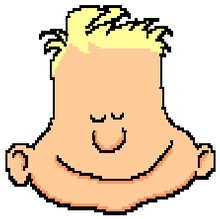


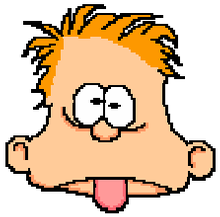




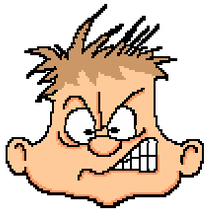
An Example

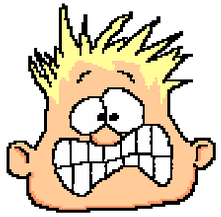


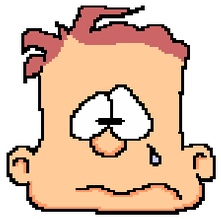




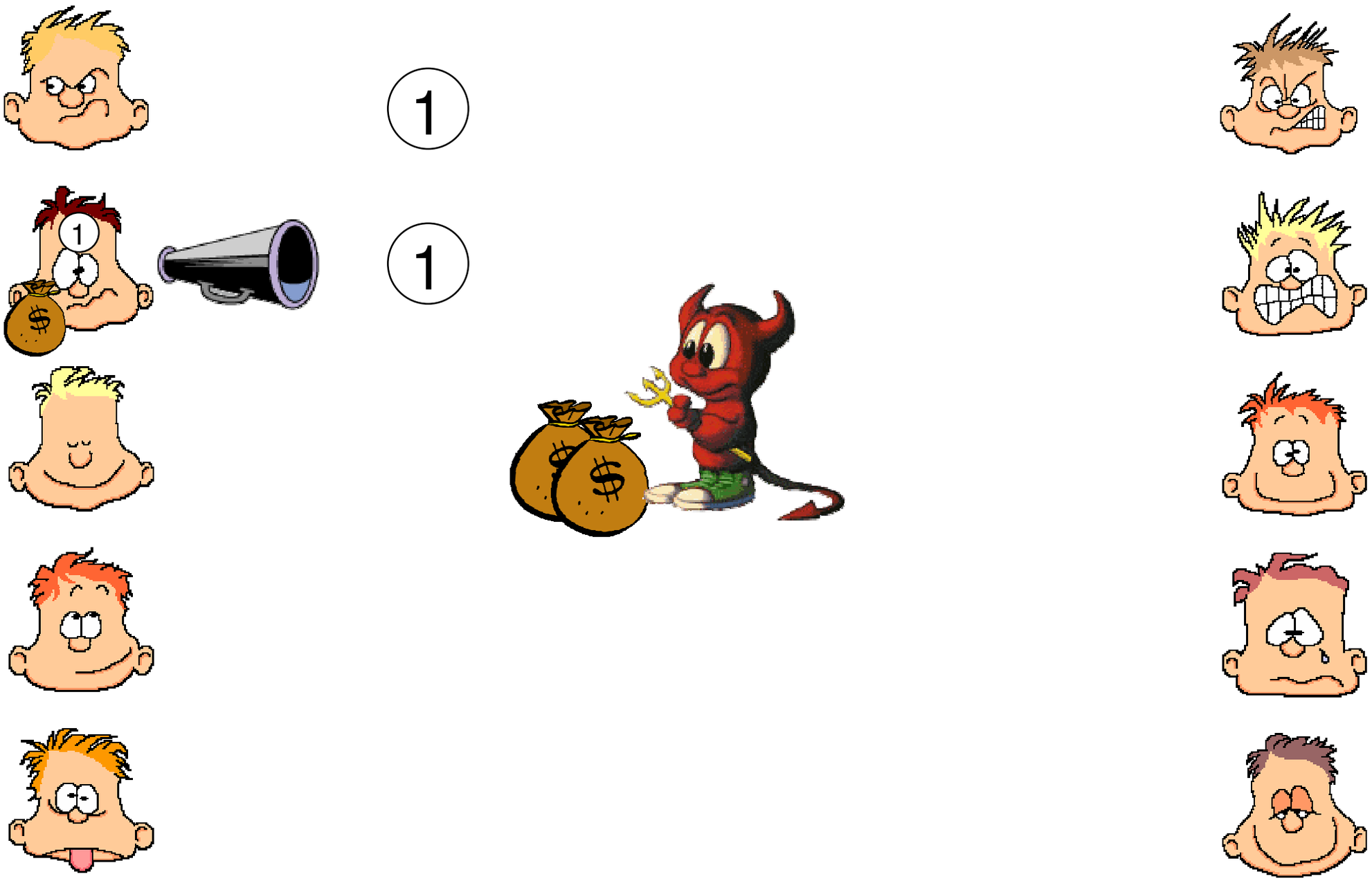
1



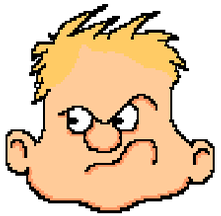


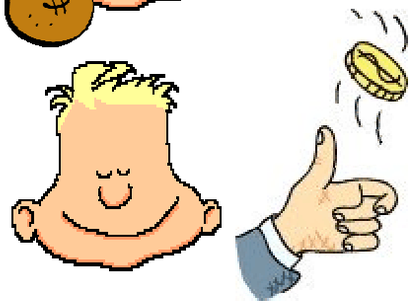


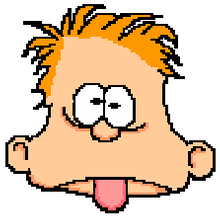
An Example



An Example

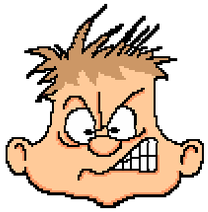


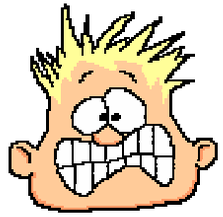


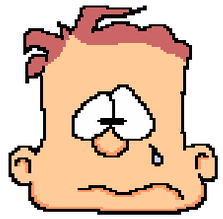


1

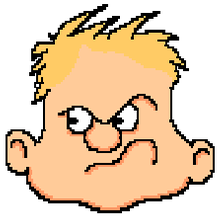
1

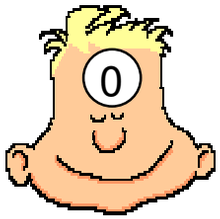


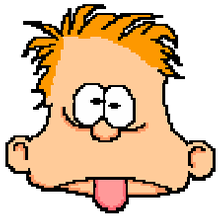




An Example

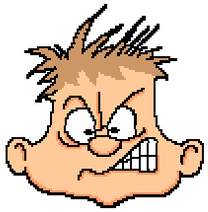


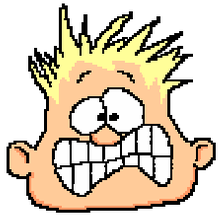


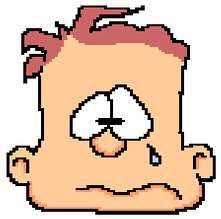


1

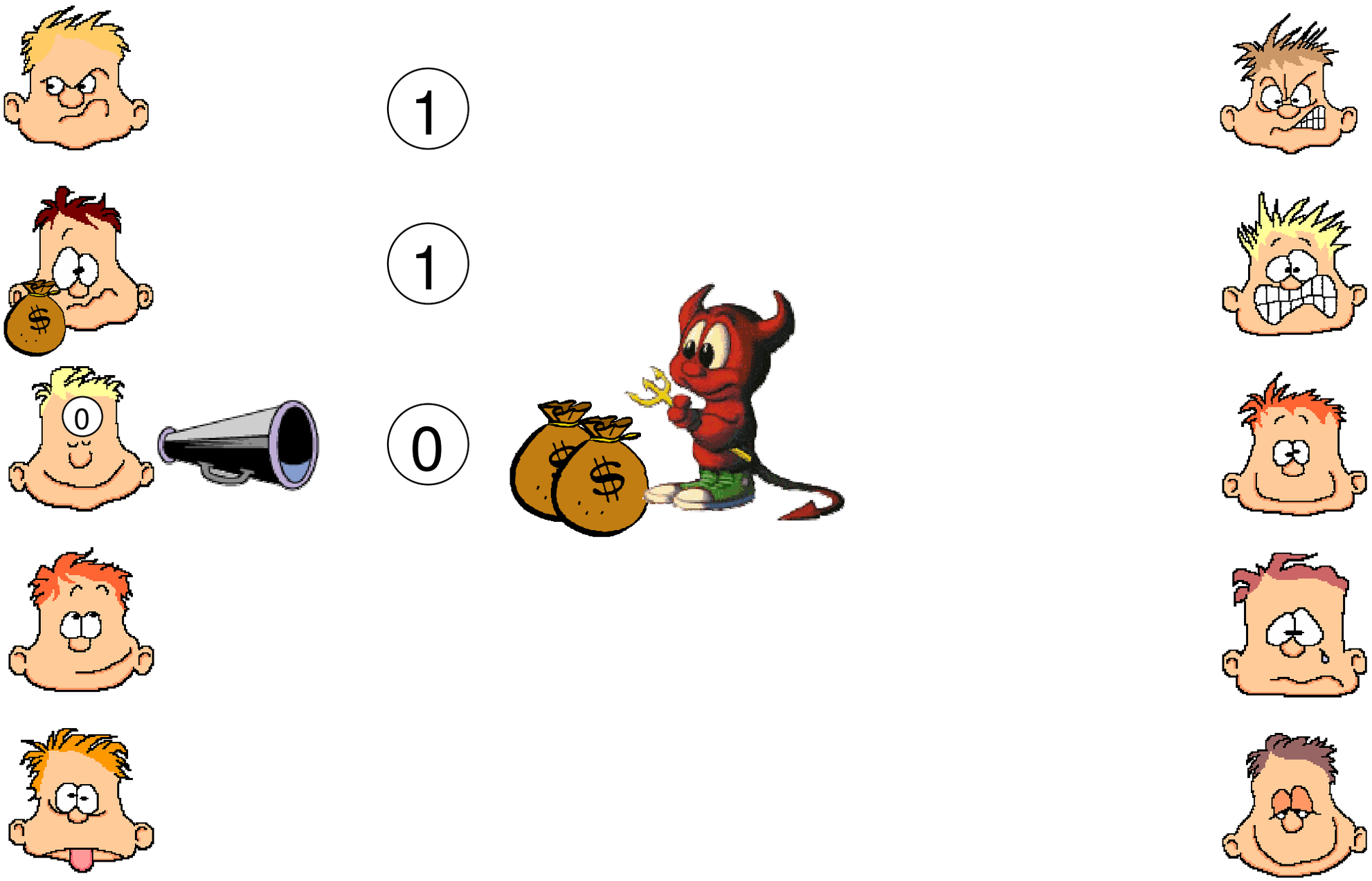
1



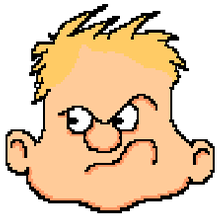


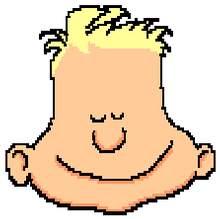


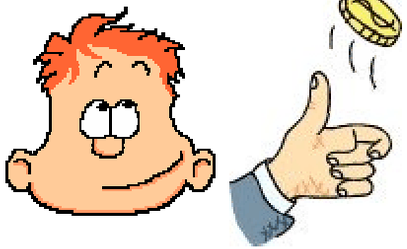
An Example

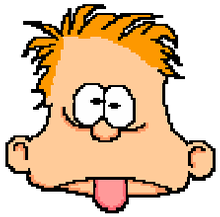


An Example





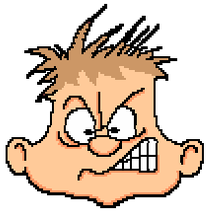


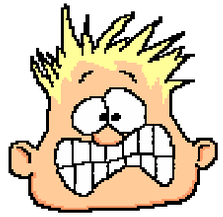


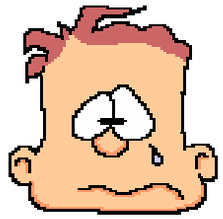
1

1

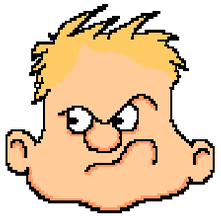
0

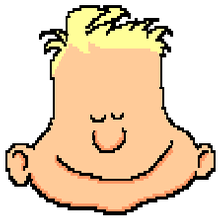


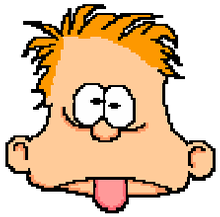




An Example



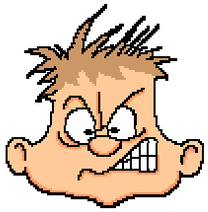


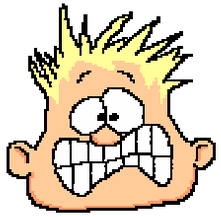


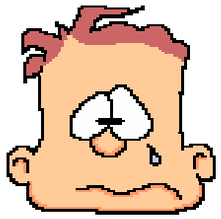
1

1

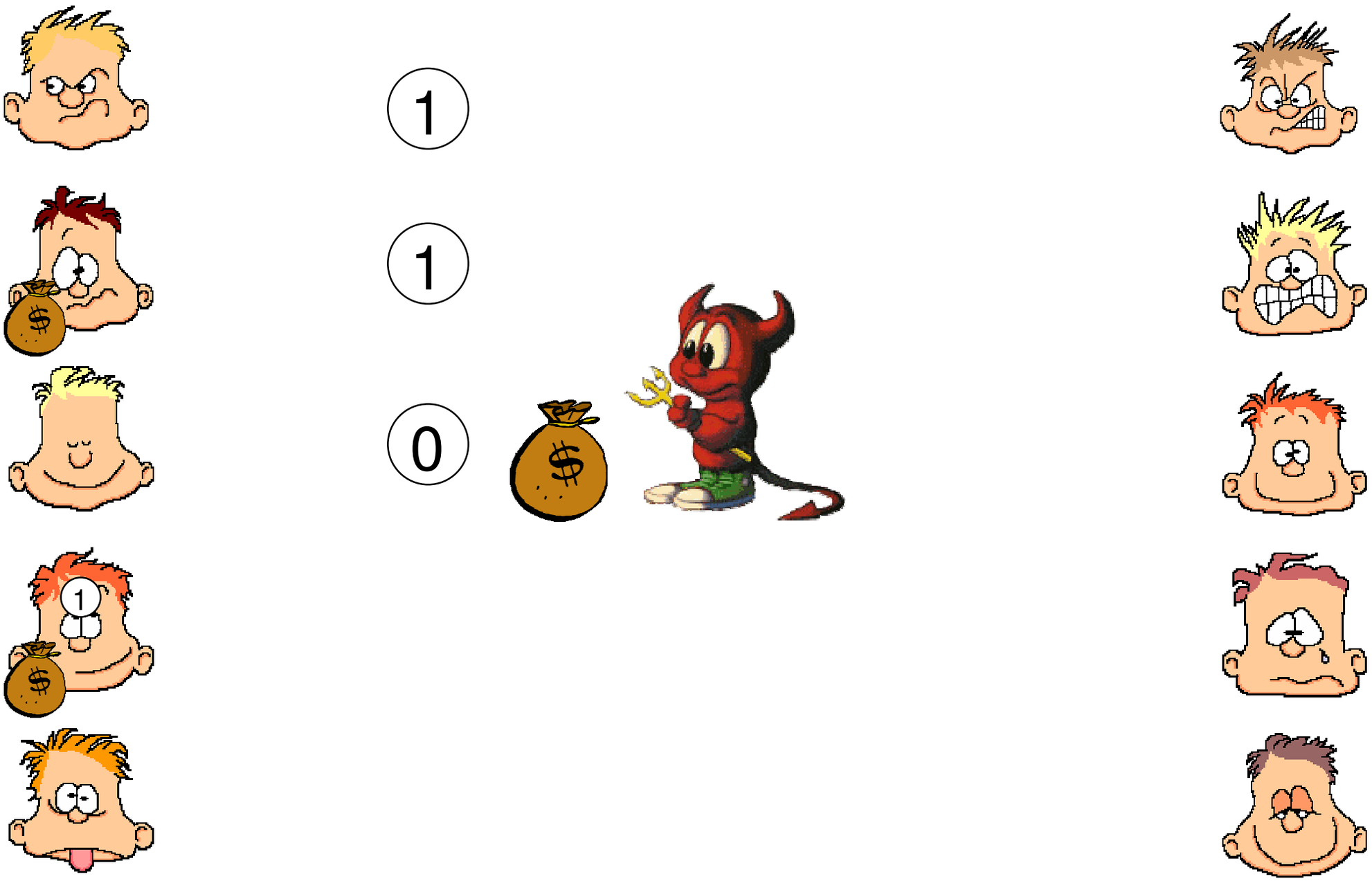
0



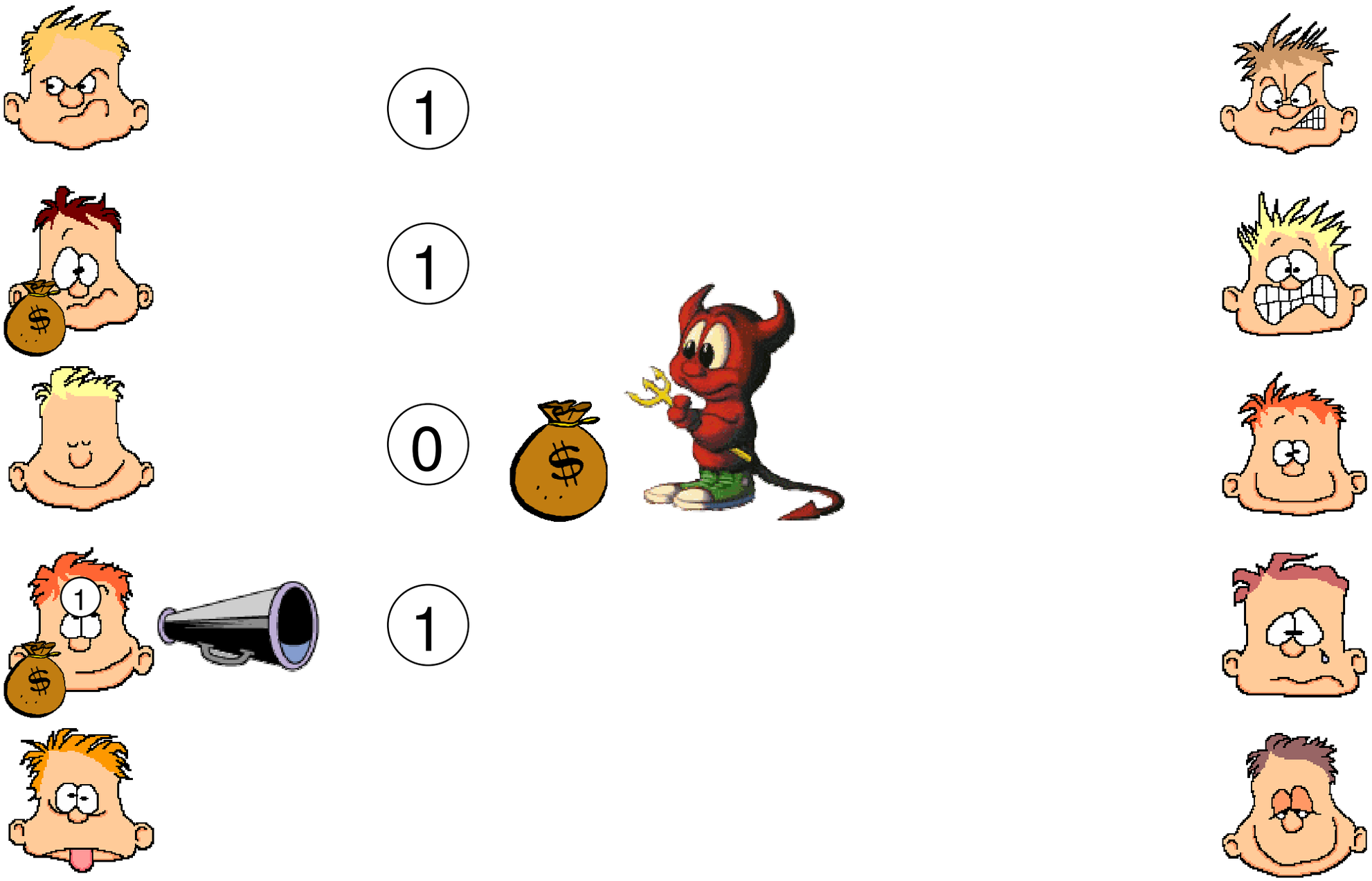




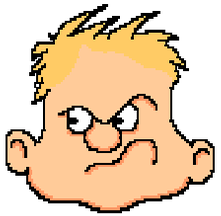
An Example

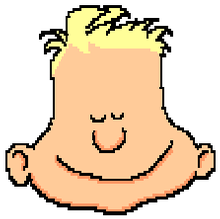


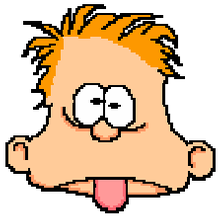
An Example



An Example

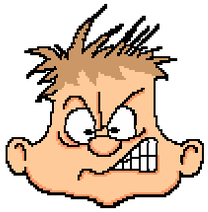
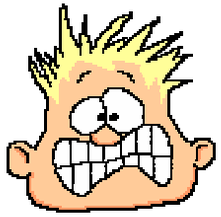


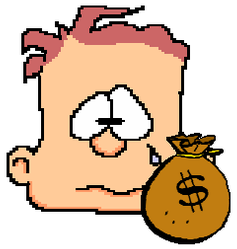




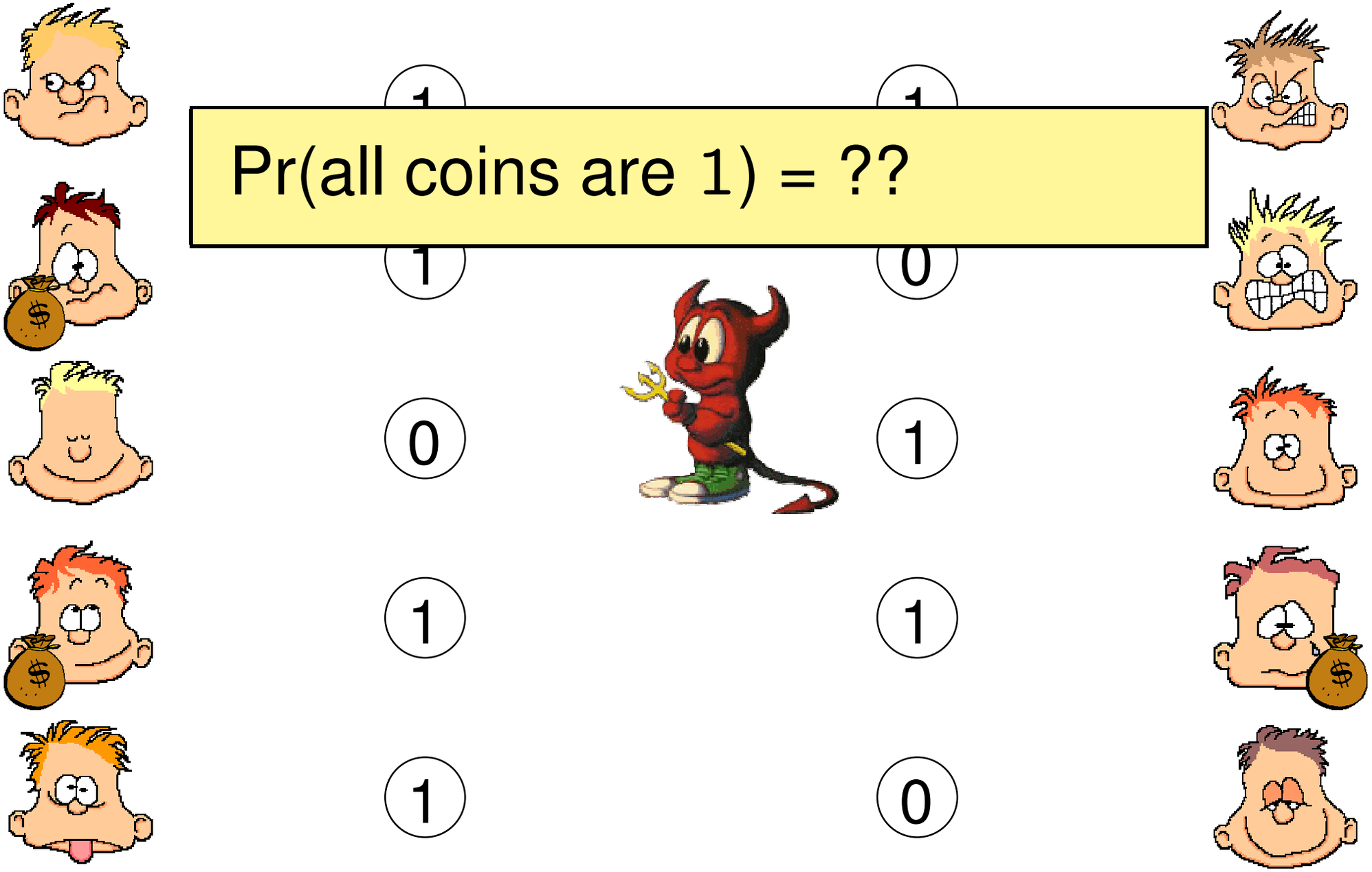
1
1
0
1
1

1
0
1
1
0

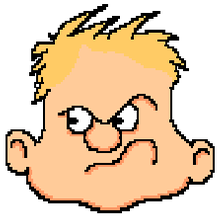


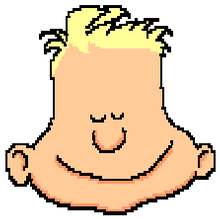

An Example

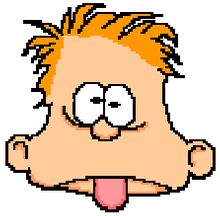


Pr(all coins are 1) = ??

An Example







$$\Pr(\text{all coins are } 1) = 2^{-7} \approx 1\%$$

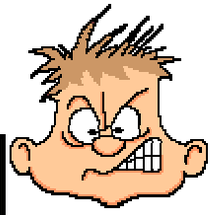
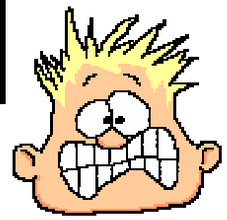
0 1

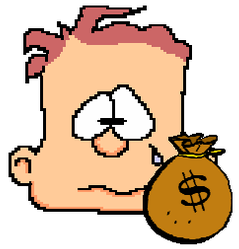
1 1

1 0

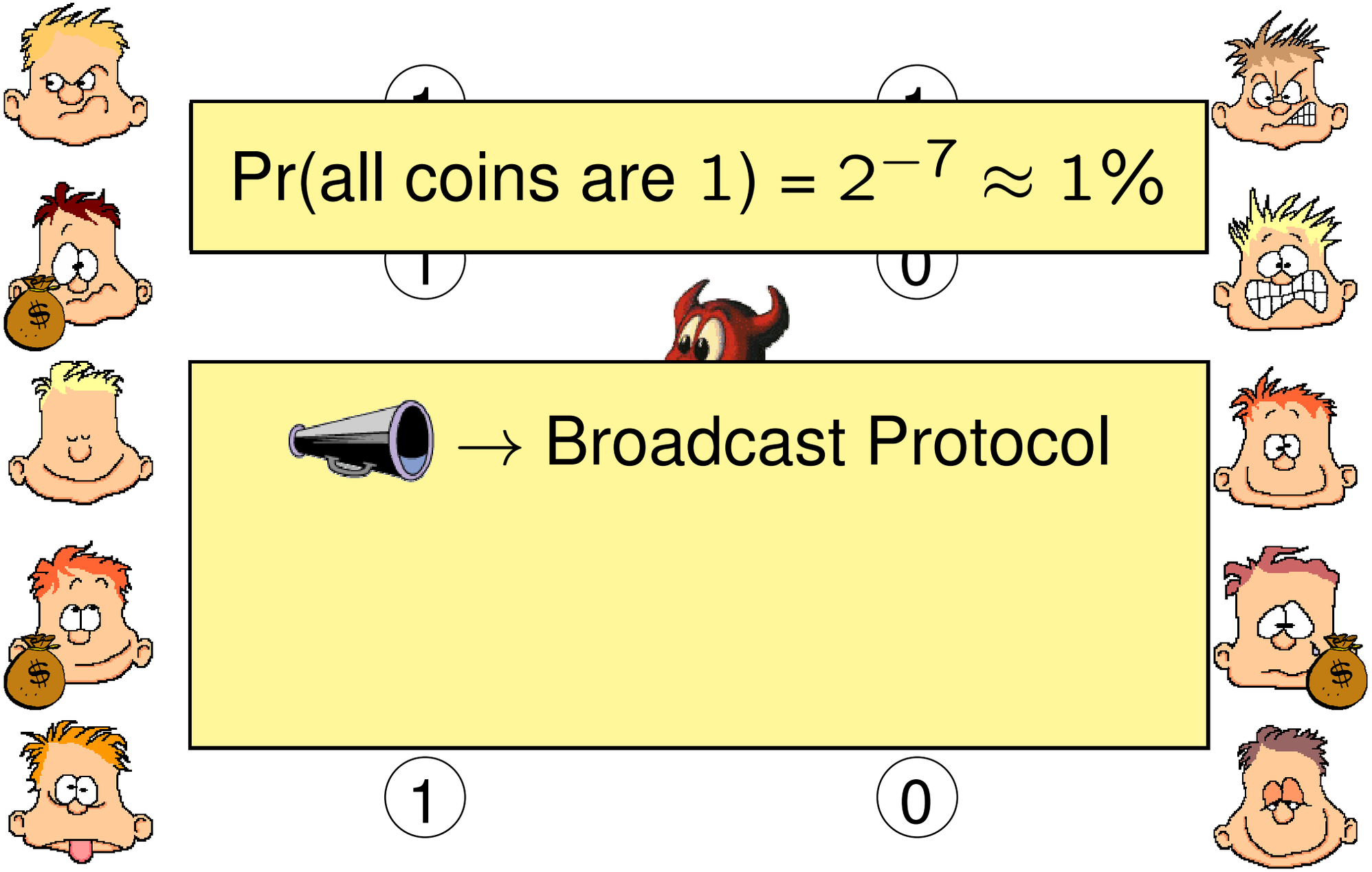
0 1

1 0



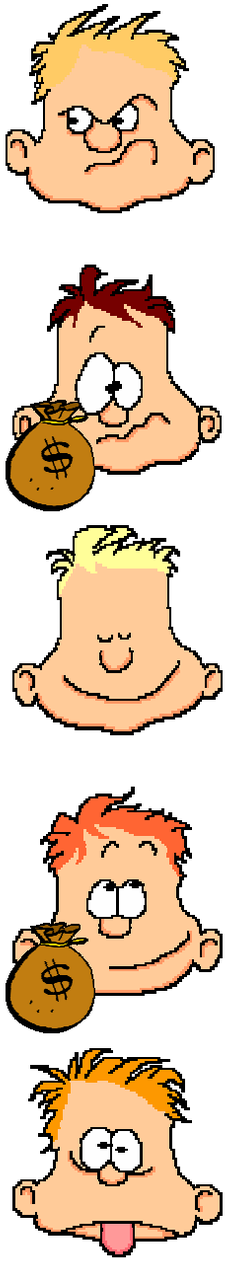

An Example

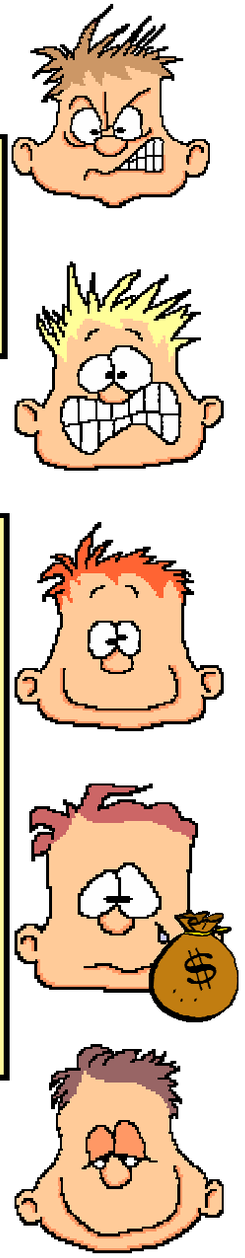


$$\Pr(\text{all coins are } 1) = 2^{-7} \approx 1\%$$

$\rightarrow$ Broadcast Protocol

An Example

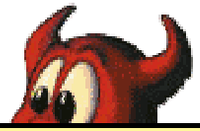


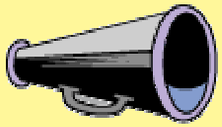


1 1

$$\Pr(\text{all coins are } 1) = 2^{-7} \approx 1\%$$

1 0





$\rightarrow$ Broadcast Protocol

[LSP,DS,BGP,CW,LLR,. . .]

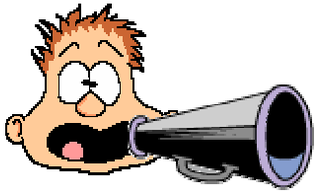
$$\Pr(\text{all coins are } 1) \approx 9\%$$

1 0

The Problem

The Expectation

Broadcast Protocol $\equiv$



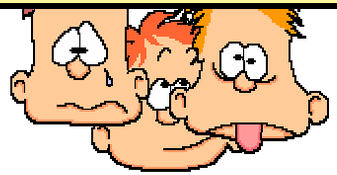
The Problem

The Expectation

Functionality (informal)

1. Sender $\xrightarrow{x} \mathcal{F}$
2. $\mathcal{F} \xrightarrow{x}$ all recipients

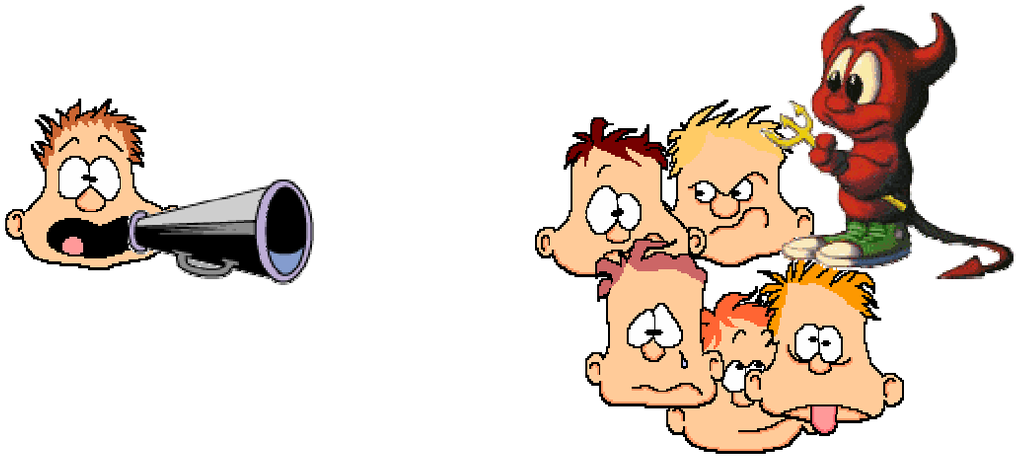
Bro



The Problem

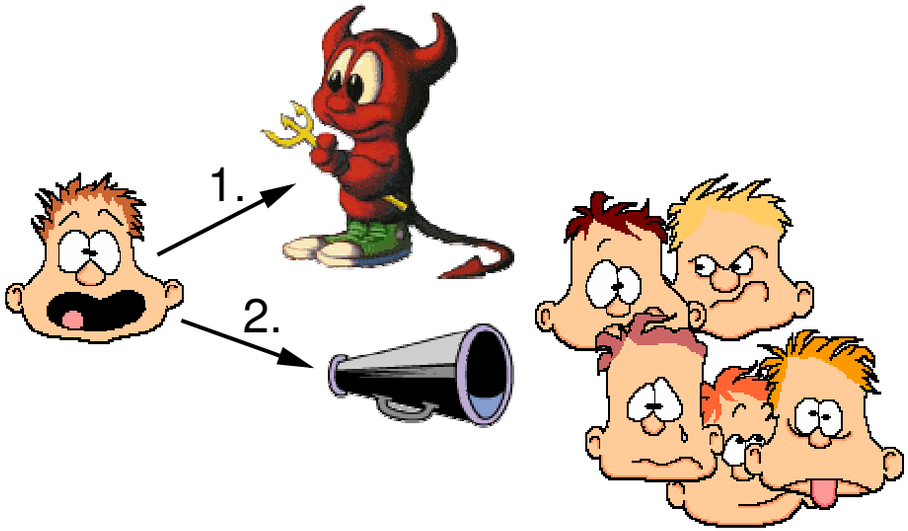
The Expectation

Broadcast Protocol $\equiv$



The Reality

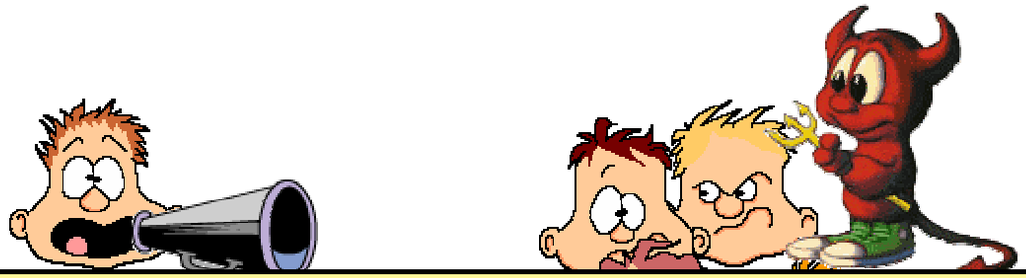
Broadcast Protocol $\equiv$



The Problem

The Expectation

Broadcast Protocol $\equiv$



Functionality (informal)

1. Sender $\xrightarrow{x} \mathcal{F}$
2. $\mathcal{F} \xrightarrow{x}$ Adv
3. Adversary can corrupt sender
4. If Sender is corrupted: Adv $\xrightarrow{x'} \mathcal{F}$

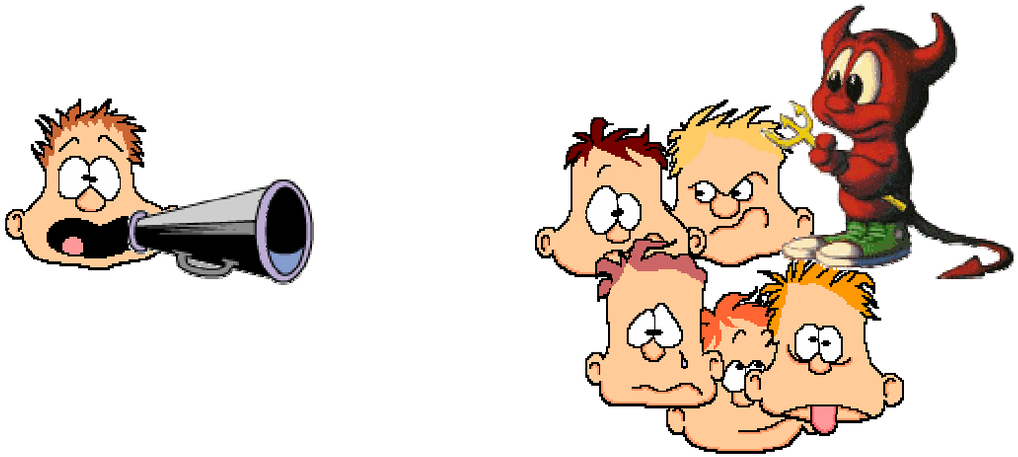
   Otherwise: $\mathcal{F}$ sets $x' = x$
5. $\mathcal{F} \xrightarrow{x'}$ all recipients

The Problem

The Expectation

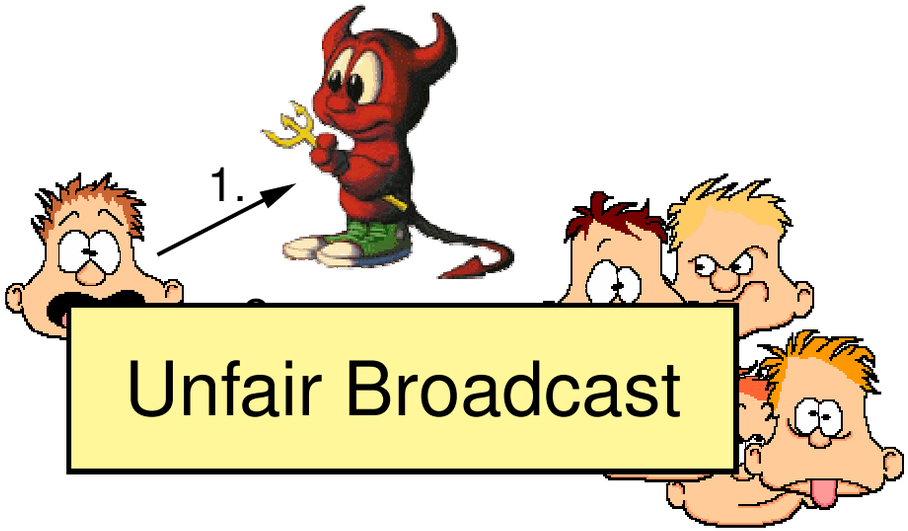
Fair Broadcast

Broadcast Protocol $\equiv$



The Reality

Broadcast Protocol $\equiv$



Unfair Broadcast

Outline

Talk Outline

- Motivation
- Known Broadcast Protocols
- Our Broadcast Protocols
- Conclusions

Known Broadcast Protocols

Sample Broadcast Protocol [LSP,DS,BGP,CW,LLR,. . .]

1. Sender sends x to all players
2. Players . . .
3. . . .

Known Broadcast Protocols

Sample Broadcast Protocol [LSP,DS,BGP,CW,LLR,. . .]

1. Sender sends x to all players
2. Players . . .
3. . . .

The Attack

- Adversary gets x in Step 1 *before honest players*.
- If Adversary does not like x, she *corrupts Sender*, and *sends* x' to honest players.

Known Broadcast Protocols

Sample Broadcast Protocol [LSP,DS,BGP,CW,LLR,. . .]

1. Sender sends x to all players
2. Players . . .
3. . . .

The Attack

- Adversary gets x in Step 1 *before honest players*.
- If Adversary does not like x, she *corrupts Sender*, and *sends* x' to honest players.

$\Rightarrow$ **Unfair Broadcast**

Known Broadcast Protocols

S

1

2

3

Property-Based Definition of Broadcast

- **Consistency**: All players receives the same value.
- **Validity**: Sender correct $\Rightarrow$ this is his value.
- **Termination**: Every player eventually receives value.

The Attack

- Adversary gets x in Step 1 *before honest players*.
- If Adversary does not like x, she *corrupts Sender*, and *sends* x' to honest players.

$\Rightarrow$ **Unfair Broadcast**

Known Broadcast Protocols

Property-Based Definition of Broadcast

- **Consistency**: All players receives the same value.
- **Validity**: Sender correct $\Rightarrow$ this is his value.
- **Termination**: Every player eventually receives value.

Simultaneous Broadcast

- different senders, ensure independence of messages
- [CGMA85,CR87,Gen95,Gen00,HM05,Hev06,...]
- use broadcast as sub-protocol (property based :-S)

$\Rightarrow$ **Unfair Broadcast**

Known Broadcast Protocols

Sample Broadcast Protocol [LSP,DS,BGP,CW,LLR,. . .]

1. Sender sends x to all players
2. Players . . .
3. . . .

The Attack

- Adversary gets x in Step 1 *before honest players*.
- If Adversary does not like x, she *corrupts Sender*, and *sends* x' to honest players.

$\Rightarrow$ **Unfair Broadcast**

Known Broadcast Protocols

Secure Channels Model — Synchronous

- maximum network delay, common clock
- no minimum network delays!
- no simultaneous multi-send
- small clock skews allowed

The Attack

- Adversary gets x in Step 1 *before honest players*.
- If Adversary does not like x, she *corrupts Sender*, and *sends* x' to honest players.

$\Rightarrow$ **Unfair Broadcast**

Known Broadcast Protocols

Secure Channels Model — Synchronous

- maximum network delay, common clock
- no minimum network delays!
- no simultaneous multi-send
- small clock skews allowed

Dolev-Strong Broadcast [DS82]

- unfair even with simultaneous multi-send

sends x' to honest players.

$\Rightarrow$ **Unfair Broadcast**

Known Broadcast Protocols

Secure Channels Model — Synchronous

- maximum network delay, common clock
- no minimum network delays!
- no simultaneous multi-send
- small clock skews allowed

Dolev-Strong Broadcast [DS82]

Dual-Failure Model [GP92]

- active and fail corruptions
- fail during send $\rightarrow$ unfair

Outline

Talk Outline

- Motivation
- Known Broadcast Protocols
- Our Broadcast Protocols
- Conclusions

Adaptively Secure Broadcast

Considered Model

- secure channels model, synchronous
- same problem apparently also in other models

Adaptively Secure Broadcast

Considered Model

- secure channels model, synchronous
- same problem apparently also in other models

Without Setup

- known: unfair broadcast: $t < n/3$
- fair broadcast (megaphone): $t < n/3$

Adaptively Secure Broadcast

Considered Model

- secure channels model, synchronous
- same problem apparently also in other models

Without Setup

- known: unfair broadcast: $t < n/3$
- fair broadcast (megaphone): $t < n/3$

With Setup (i.t. or crypto.)

- known: unfair Broadcast: $t < n$
- fair broadcast (megaphone): $t \leq n/2$
- assumes signature functionality

Fair Broadcast w/o Setup — $t < n/3$

Approach

- 1. VSS [BGW88], 2. Reconstruct
- VSS uses broadcast, deploy with unfair broadcast
- Analysis (white box) $\rightarrow$ still secure

Fair Broadcast w/o Setup — $t < n/3$

Approach

- 1. VSS [BGW88], 2. Reconstruct
- VSS uses broadcast, deploy with unfair broadcast
- Analysis (white box) $\rightarrow$ still secure

VSS [BGW88]

1. Dealer distributes some polynomials to each player
2. Players pairwisely check consistency
3. Inconsistency $\rightarrow$ complain by broadcast
4. Dealer broadcasts correct value, goto 3

Fair Broadcast w/o Setup — $t < n/3$

Analysis

- Broadcasted values are known to adv. *at beforehand*
- $\rightarrow$ fair broadcast $\approx$ unfair broadcast

- Analysis (white box) $\rightarrow$ still secure

VSS [BGW88]

1. Dealer distributes some polynomials to each player
2. Players pairwisely check consistency
3. Inconsistency $\rightarrow$ complain by broadcast
4. Dealer broadcasts correct value, goto 3

Fair Broadcast w/o Setup — $t < n/3$

Approach

- 1. VSS [BGW88], 2. Reconstruct
- VSS uses broadcast, deploy with unfair broadcast
- Analysis (white box) $\rightarrow$ still secure

Fair Broadcast w/o Setup — $t < n/3$

Approach

- 1. VSS [BGW88], 2. Reconstruct
- VSS uses broadcast, deploy with unfair broadcast
- Analysis (white box) $\rightarrow$ still secure

Optimality ($t < n/3$)

- follows directly from necessity for unfair broadcast

Fair Broadcast w/ Setup — $t \leq n/2$

Approach 1

- 1. VSS [CDDHR99], 2. Reconstruct
- VSS uses broadcast $\rightarrow$ deploy with unfair broadcast
- Analysis (white box) $\rightarrow$????

Fair Broadcast w/ Setup — $t \leq n/2$

Approach 1

- 1. VSS [CDDHR99], 2. Reconstruct
- VSS uses broadcast $\rightarrow$ deploy with unfair broadcast
- Analysis (white box) $\rightarrow$????

Approach 2

- 1. VSS, 2. Reconstruct
- pimp VSS from [CDDHR99], use signatures,

  adjust complaints and accusations (see paper)
- $t \leq n/2$: correctness only guaranteed for honest dealers

Fair Broadcast w/ Setup — $t \leq n/2$

Optimality ($t \leq n/2$)

- Assume π for $t > n/2$.
- Sender p_S, $n-1$ recipients R, $t-1 \geq |R|/2$.
- No simultaneous multi-send $\rightarrow$ proceed msg by msg.
- After each msg, some $A \subseteq R$ obtain information on x.
- Consider first $A \subseteq R$ with $|A| \geq t-1$.
- Observe: $B = R \setminus A$ has no information on x.
- Adversary can corrupt A, and, *depending on* x, can corrupt p_s (in total t players).

Conclusions

Known Broadcast Protocols

- do not realize natural functionality (megaphone)
- **use with care!**

Conclusions

Known Broadcast Protocols

- do not realize natural functionality (megaphone)
- **use with care!**

better: don’t use it ;-)

Conclusions

Known Broadcast Protocols

- do not realize natural functionality (megaphone)
- **use with care!**

better: don't use it :-)

care = prove your protocol secure

Conclusions

Known Broadcast Protocols

- do not realize natural functionality (megaphone)
- **use with care!**

New Broadcast Protocol

- (slightly) less efficient
- requires $t \leq n/2$ (this is optimal)
- **plug-and-play usage**

Conclusions

Known Broadcast Protocols

-
-

Thank You

Ne

-
- requires $t \leq n/2$ (this is optimal)
- **plug-and-play usage**

TOC