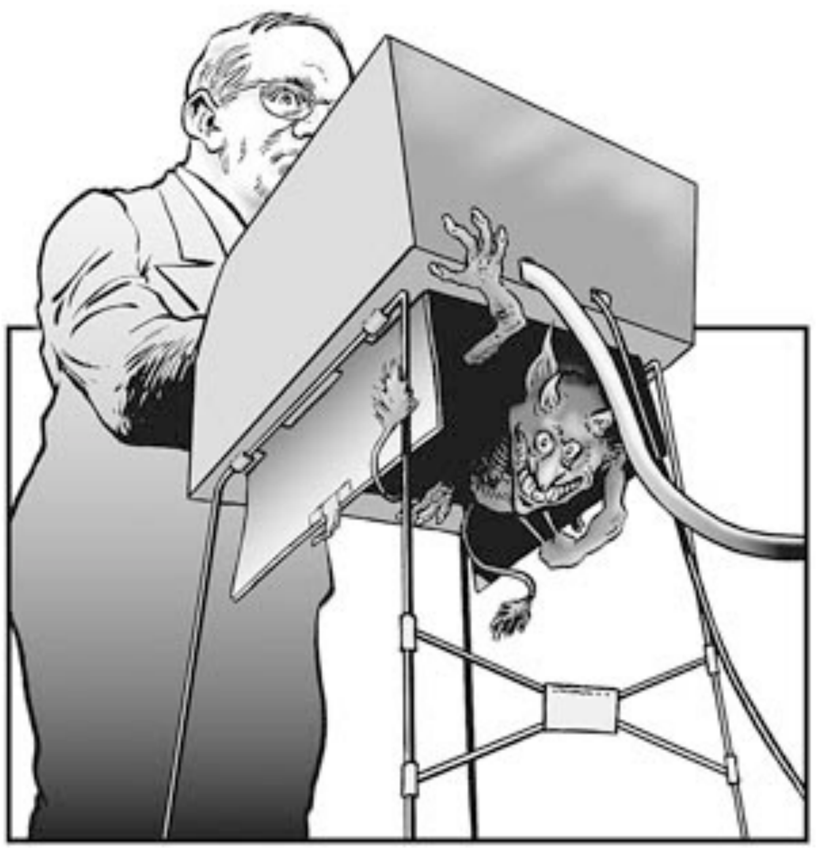
Analysis of an Electronic Boardroom Voting System

Mathilde Arnaud Véronique Cortier Cyrille Wiedling

VoteID'13

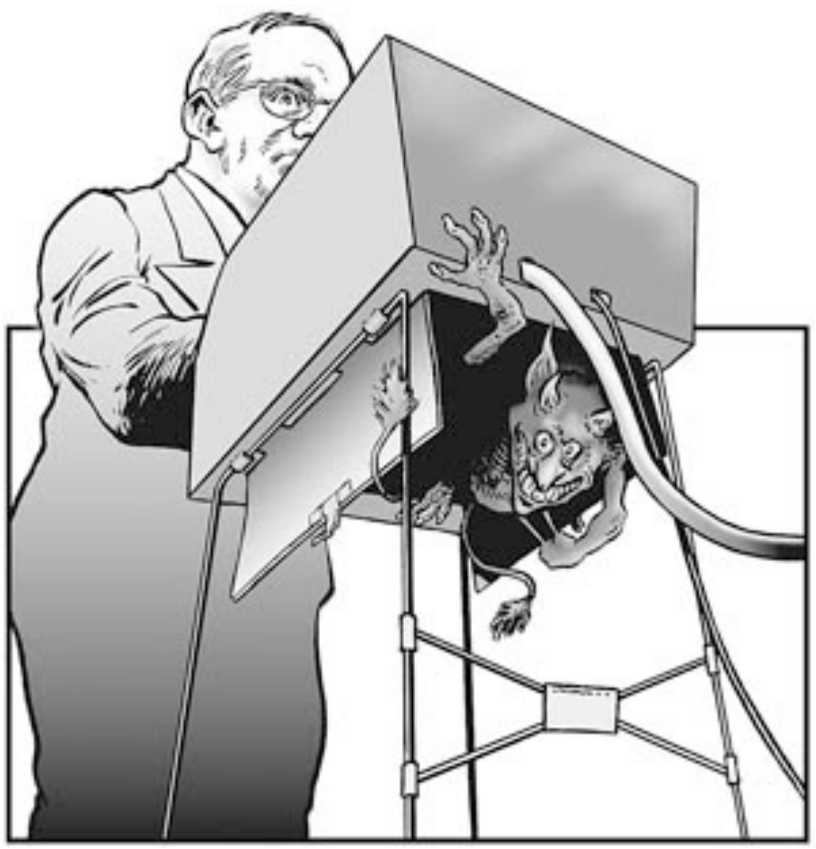
July 18th 2013

The Family of Electronic Voting



The Family of Electronic Voting

Voting Machines



- Authentication at the polling place.
- **Speed up** the process (voting, tally).
- **Better accessibility** for people.
- Proprietary systems **often subject to attacks**:

> Diebold Machines,
[Halderman et al., EVT'07]

> Indian Voting Machines,
[Gonggrijp et al., CCS'10]

The Family of Electronic Voting

- **Authentication from anywhere**.
- Systems often **difficult to understand** for non-cryptographers.
- Numerous solutions (proprietary and academic):
  - > Helios [Adida, SS'08]
  - > Civitas [Clarkson et al., S&P'08]
  - > FOO, Belenios, etc.
- Assume to **trust the voter's computer**.

Internet Voting

Different Interesting Properties

Anonymity

Verifiability

and more...

Easy-to-Understand

Usability

And Boardroom Voting ?

- Everyone in the same room (authentication by others).
- Efficiency of the voting process is necessary.
- Confidence in the result.

Boardroom Voting

- There are solutions, but...

  > Often in **black box**,

  > With **no verifiability**, ...

A **new proposal** from a subgroup of members of a CNRS commitee to achieve:

> **Simplicity**,

> **Privacy**,

> **Full Verifiability**.

Setting

A **boardroom**
(including all the voters)

Setting

A **boardroom**
(including all the voters)

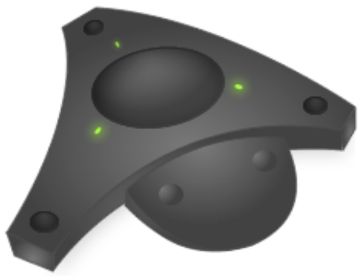
E-Voting Devices

Setting

A **boardroom**
(including all the voters)

E-Voting Devices

Link to



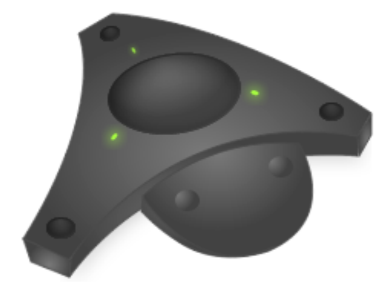
Central Device

Setting

A **boardroom**
(including all the voters)

E-Voting Devices

Link to



Central Device

Links to

Screen
(Visible by all)

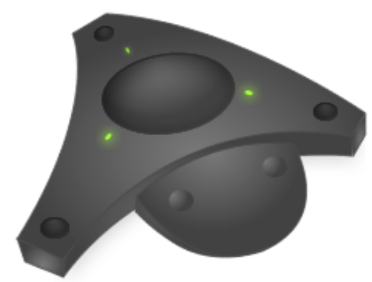
Setting

A **boardroom**
(including all the voters)

An **assessor**
(One voter, can be anyone)

E-Voting Devices

Link to



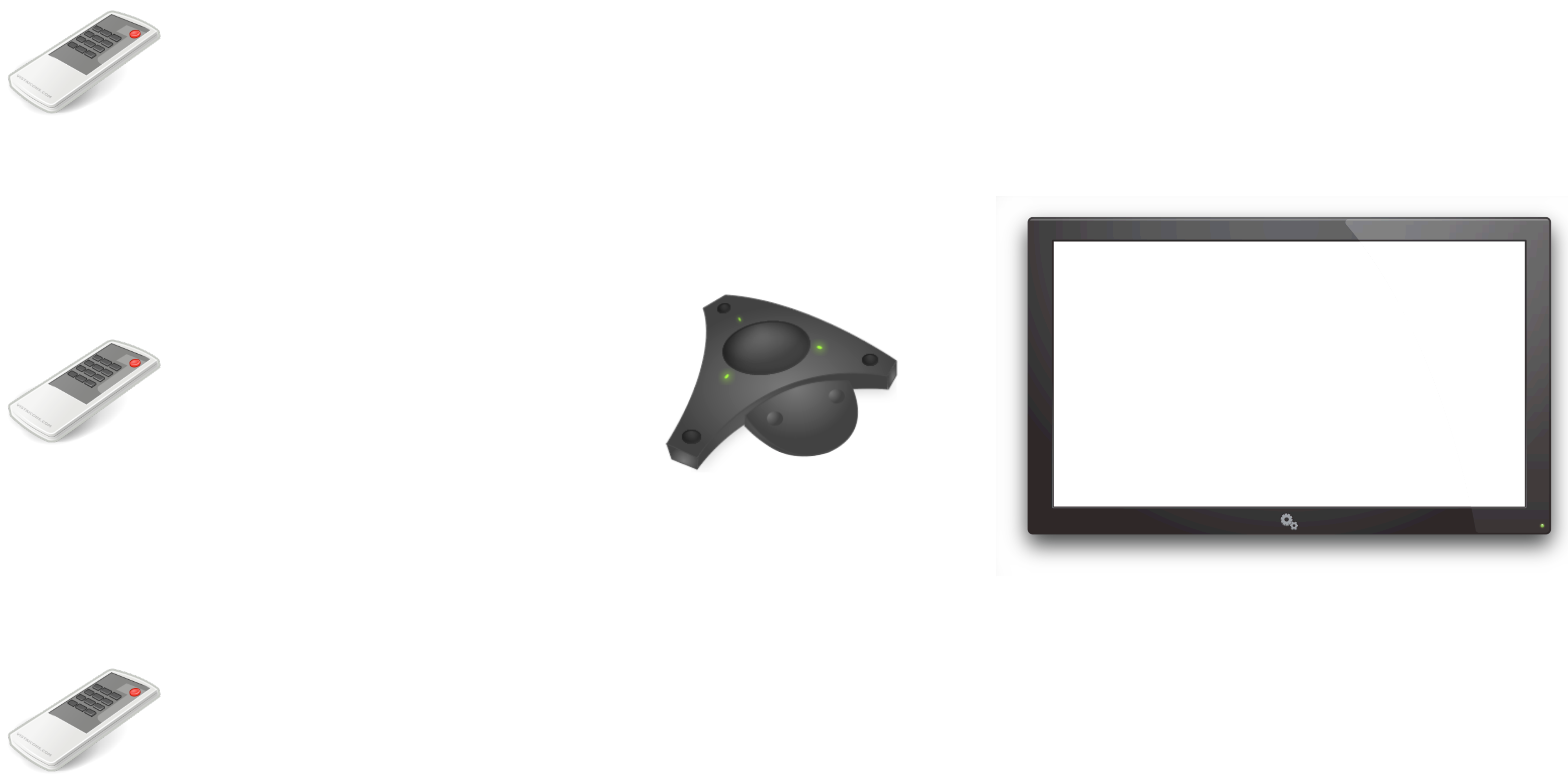
Central Device

Links to

Screen
(Visible by all)

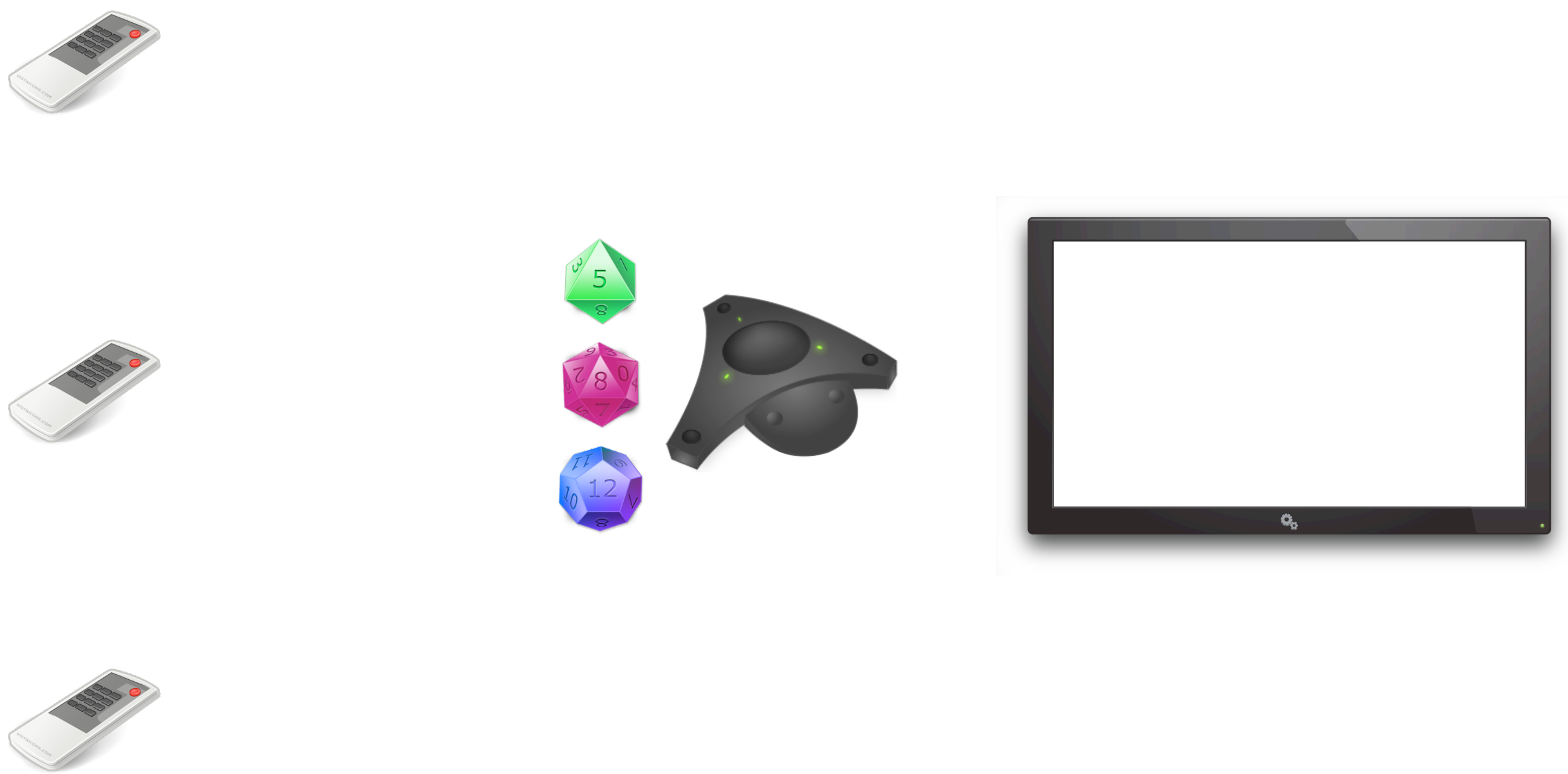
A First Approach

How it works ?



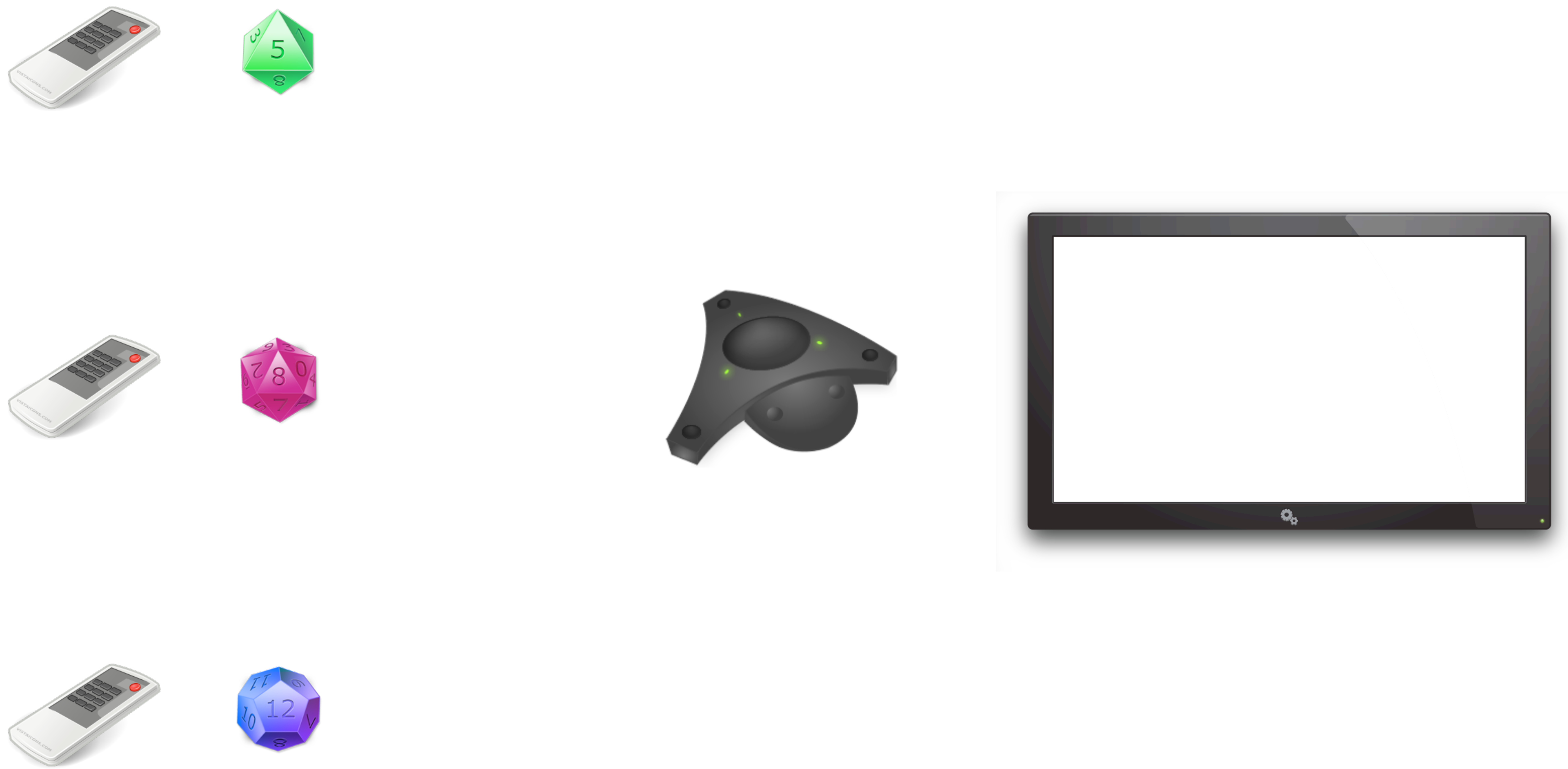
A First Approach

How it works ?



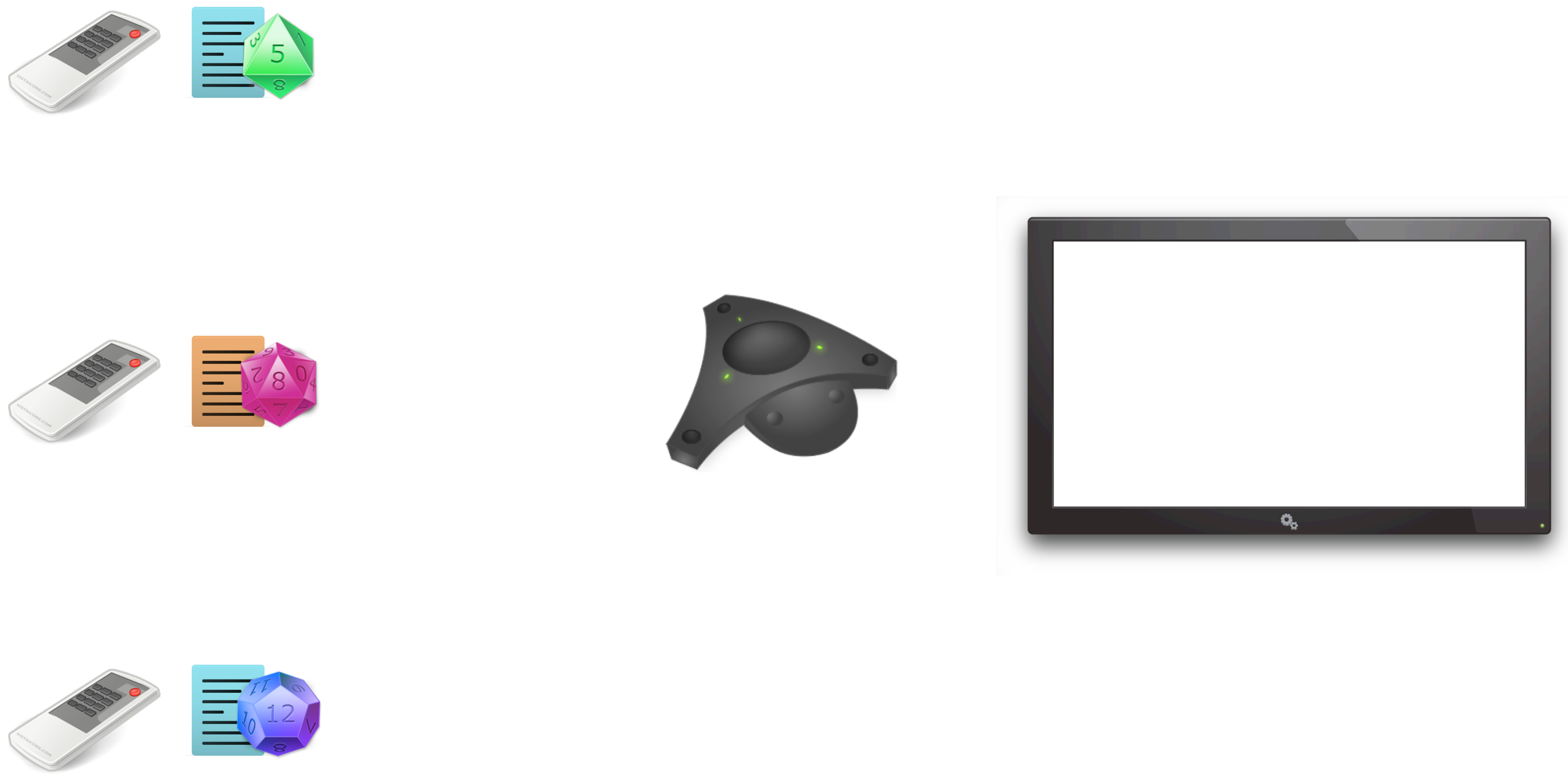
A First Approach

How it works ?



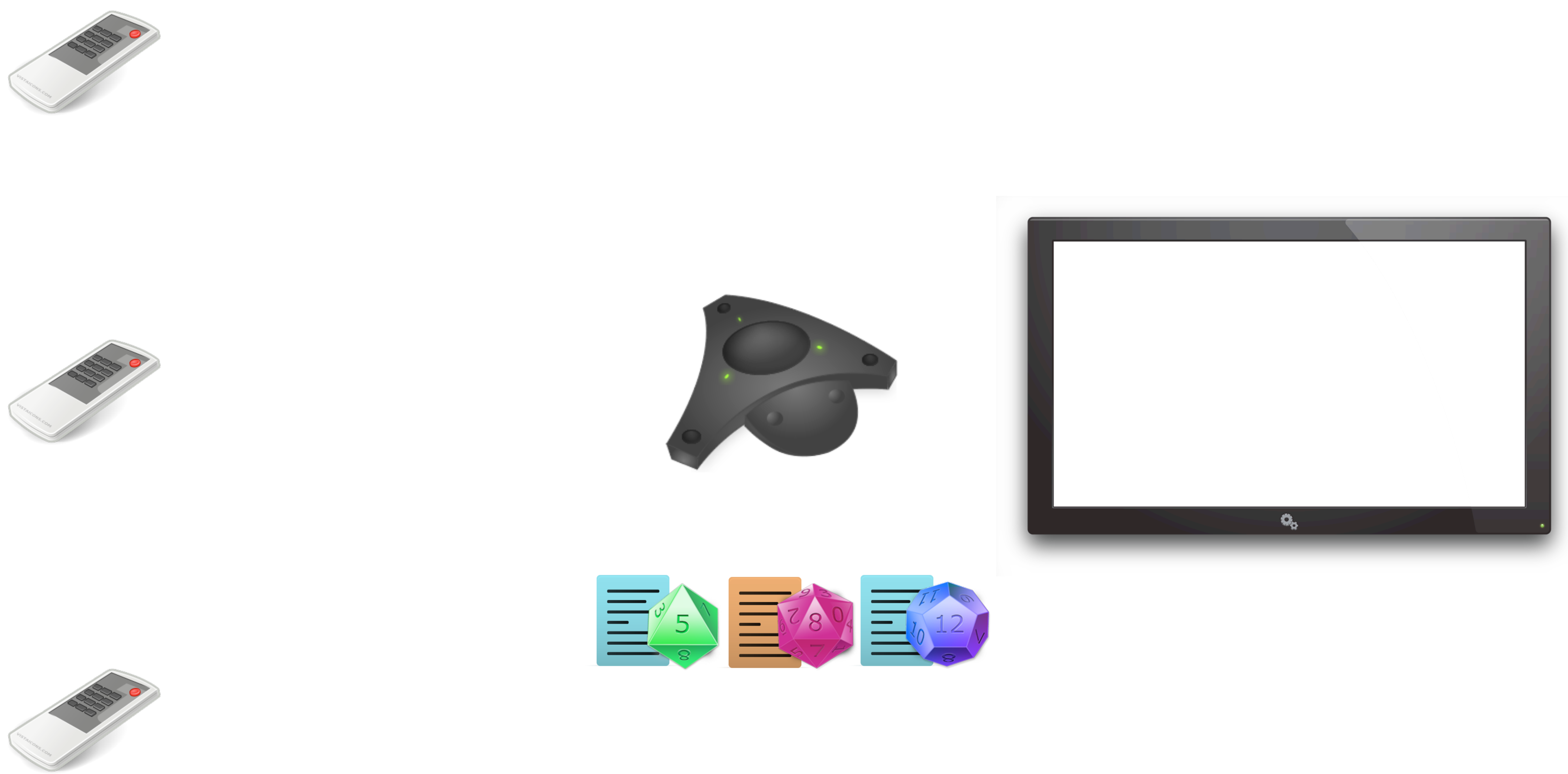
A First Approach

How it works ?



A First Approach

How it works ?

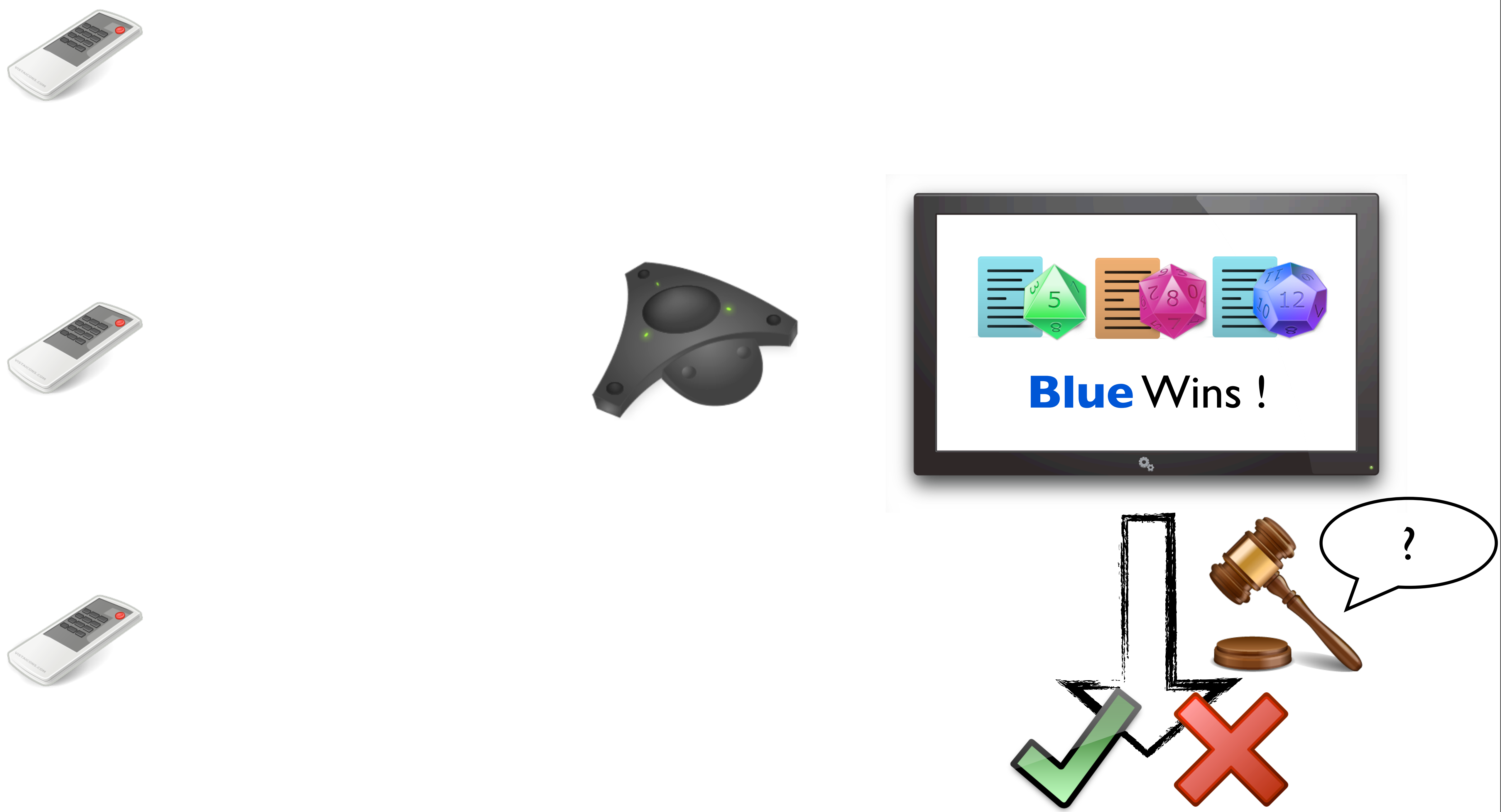


A First Approach

How it works ?

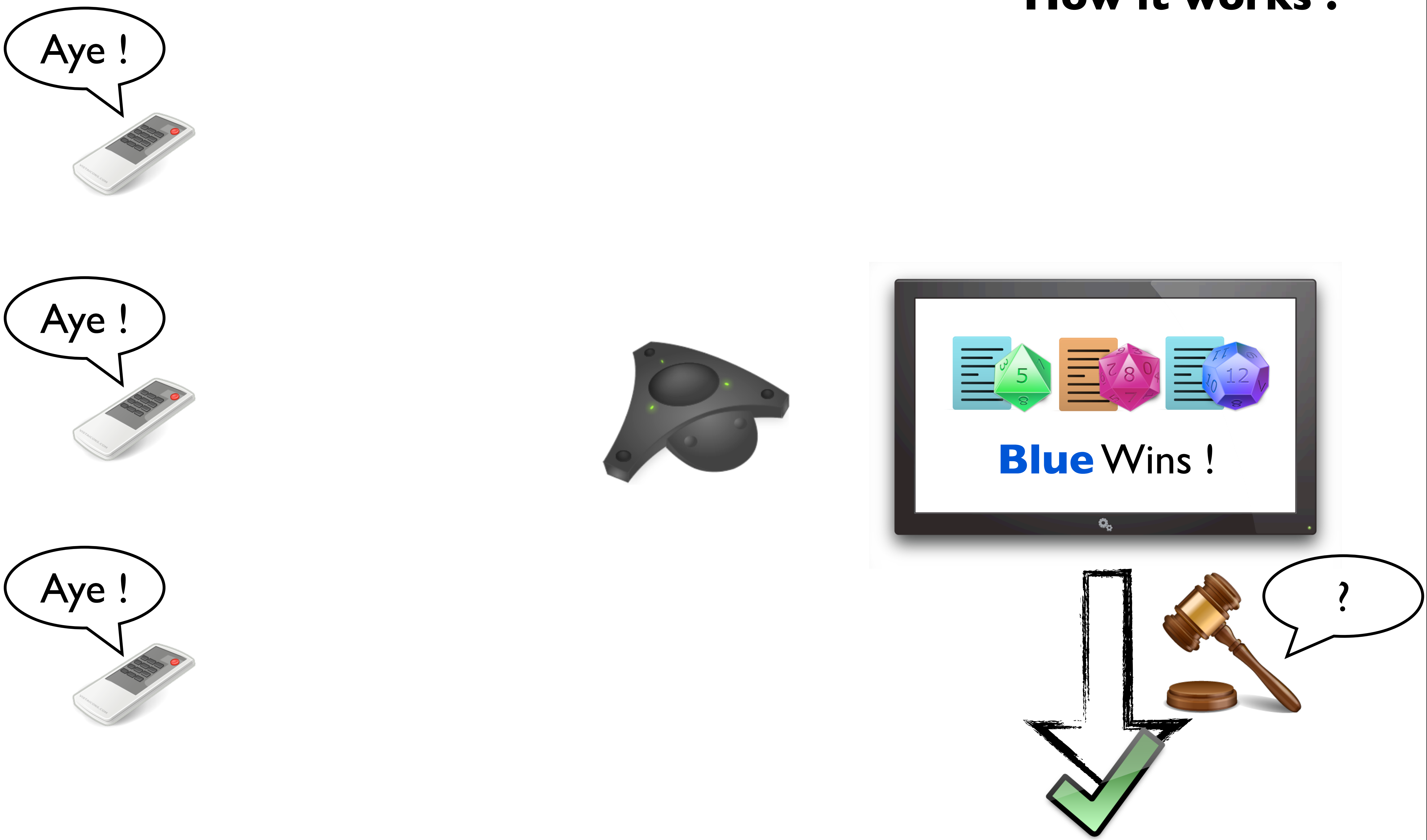
A First Approach

How it works ?



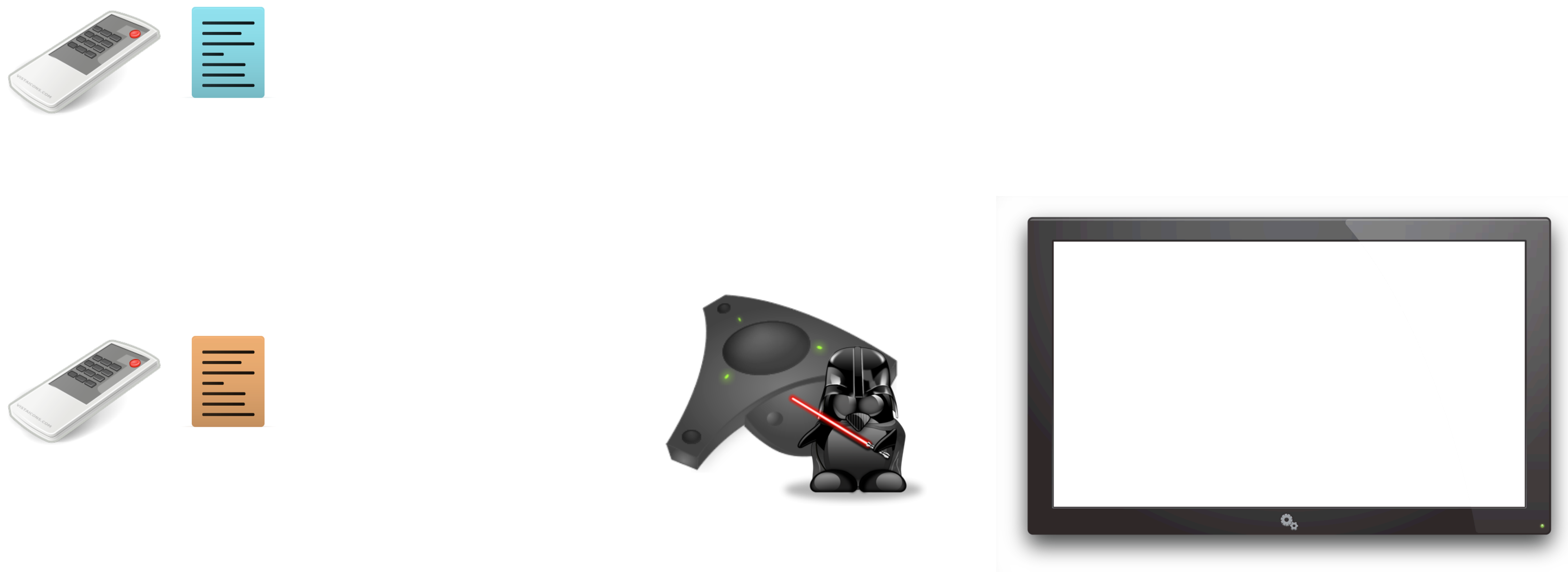
A First Approach

How it works ?



But...

A possible attack



Similar to Clash Attacks [Küsters et al., S&P'12].

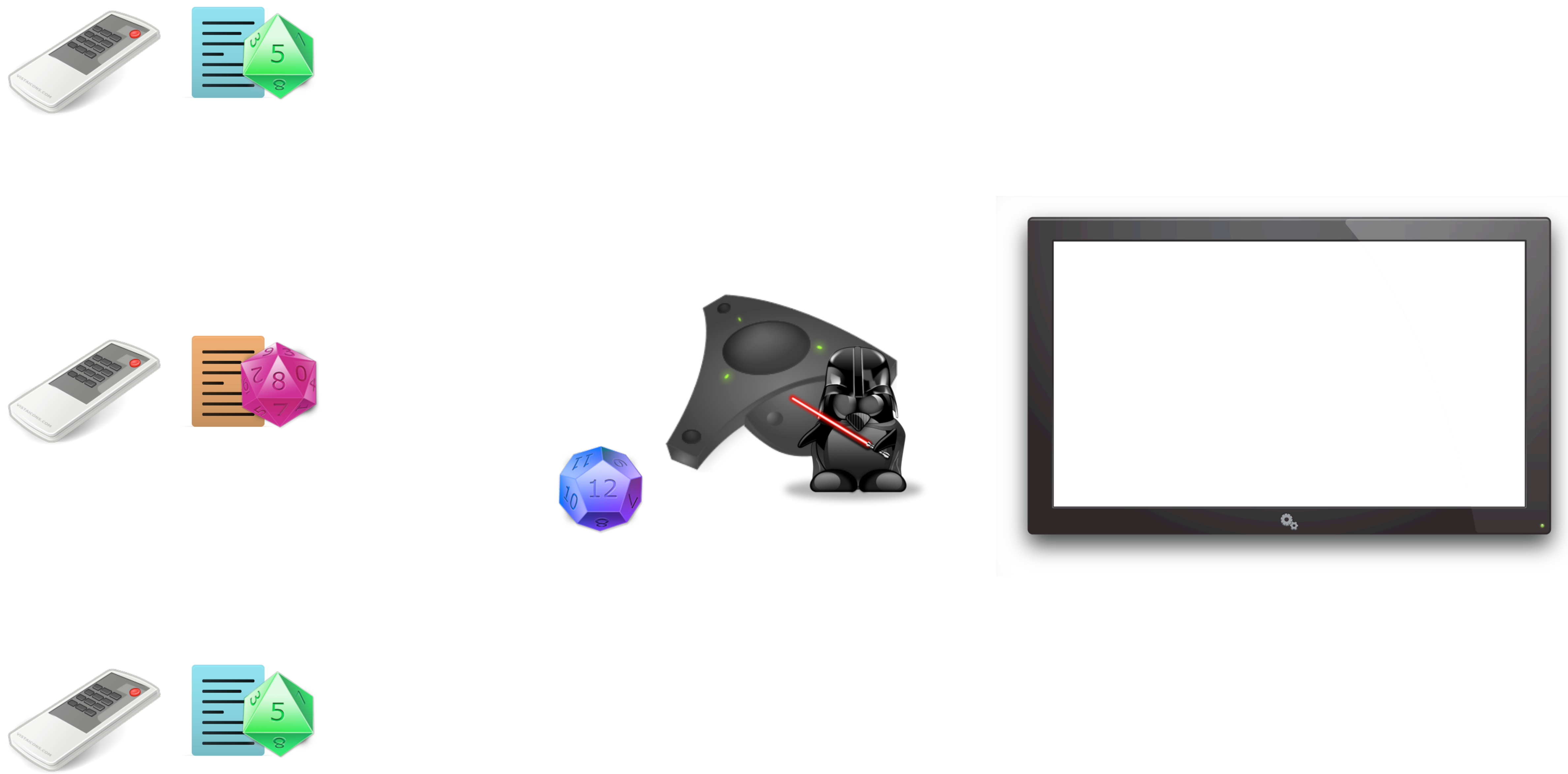
But...

A possible attack

Similar to Clash Attacks [Küsters et al., S&P'12].

But...

A possible attack



Similar to Clash Attacks [Küsters et al., S&P'12].

But...

A possible attack

Similar to Clash Attacks [Küsters et al., S&P'12].

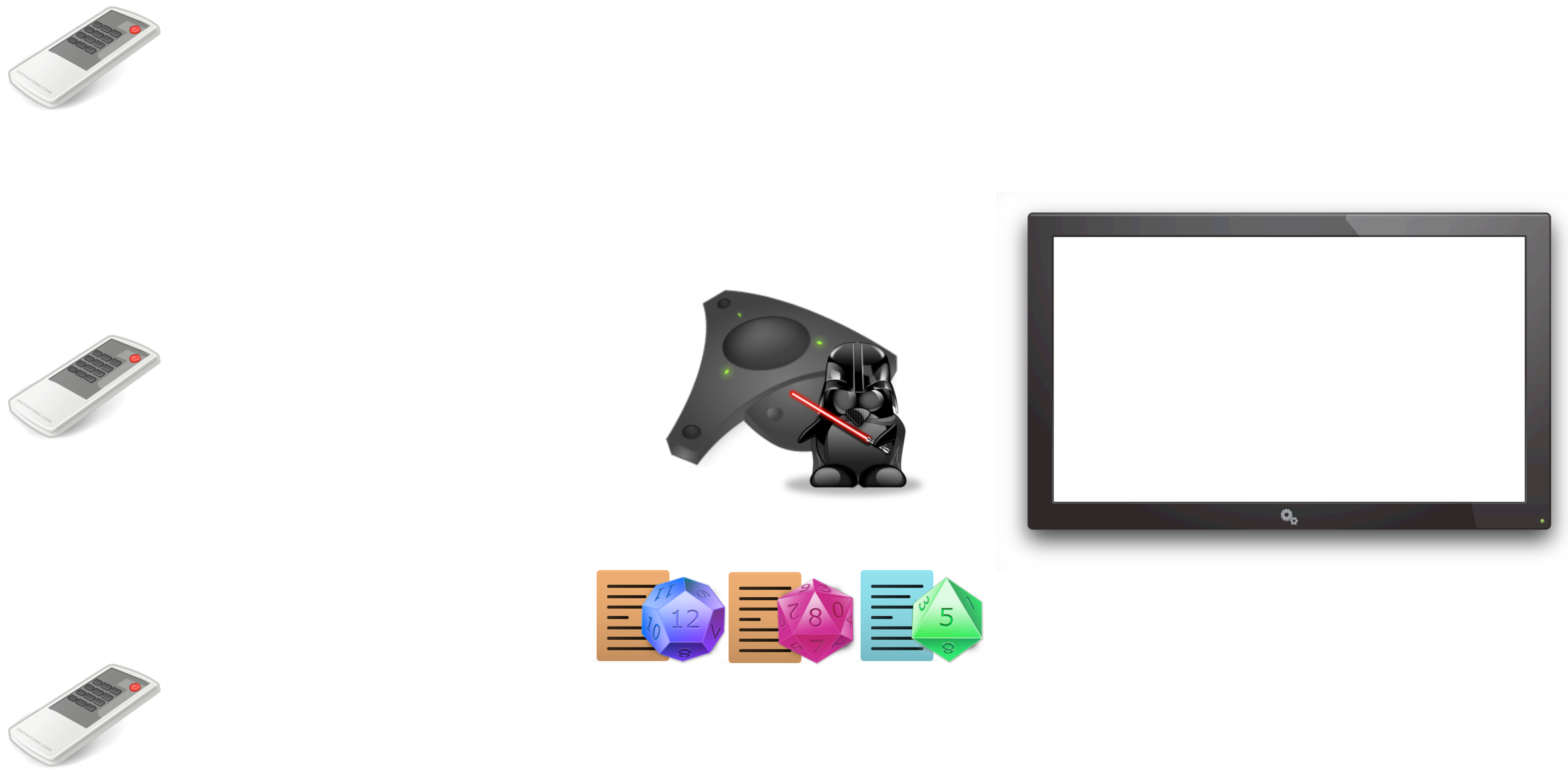
But...

A possible attack

Similar to Clash Attacks [Küsters et al., S&P'12].

But...

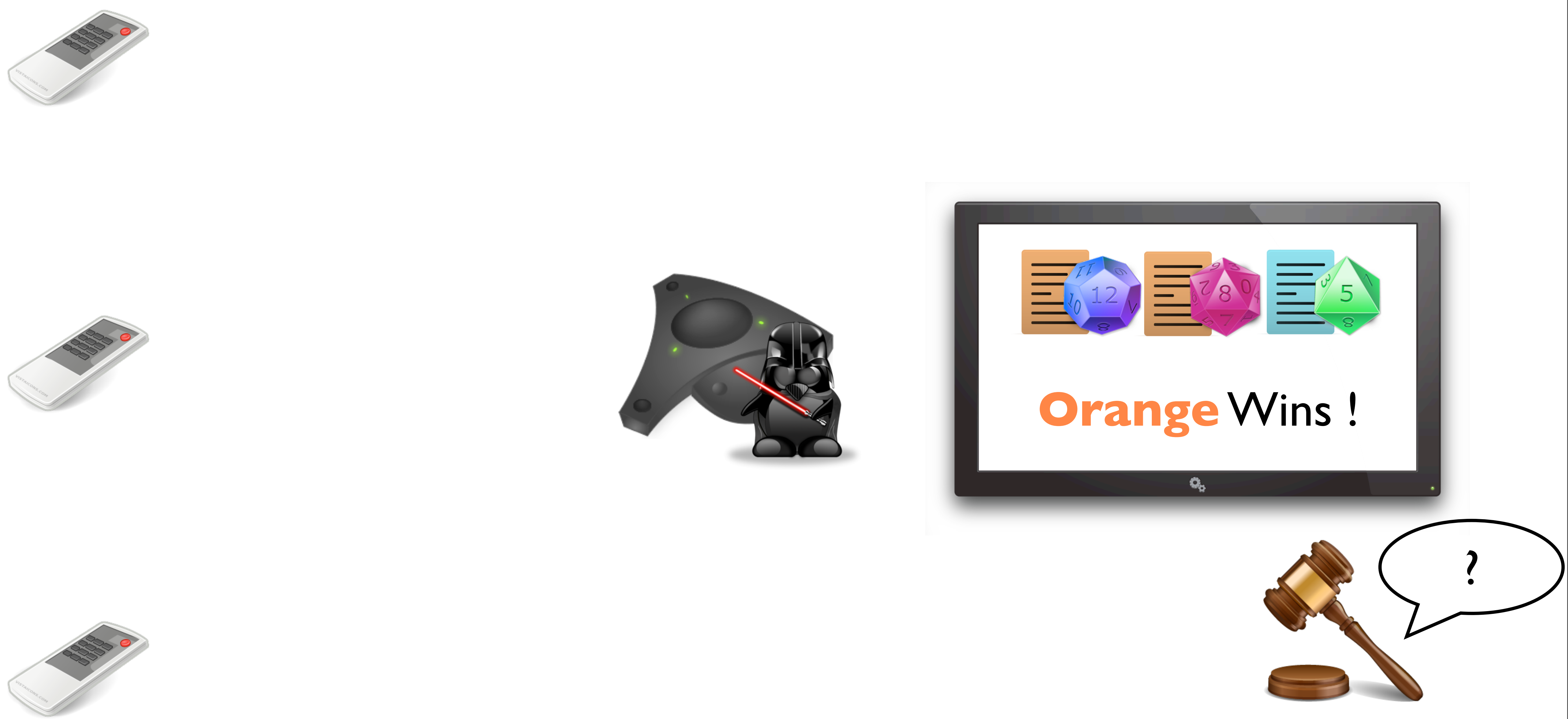
A possible attack



Similar to Clash Attacks [Küsters et al., S&P'12].

But...

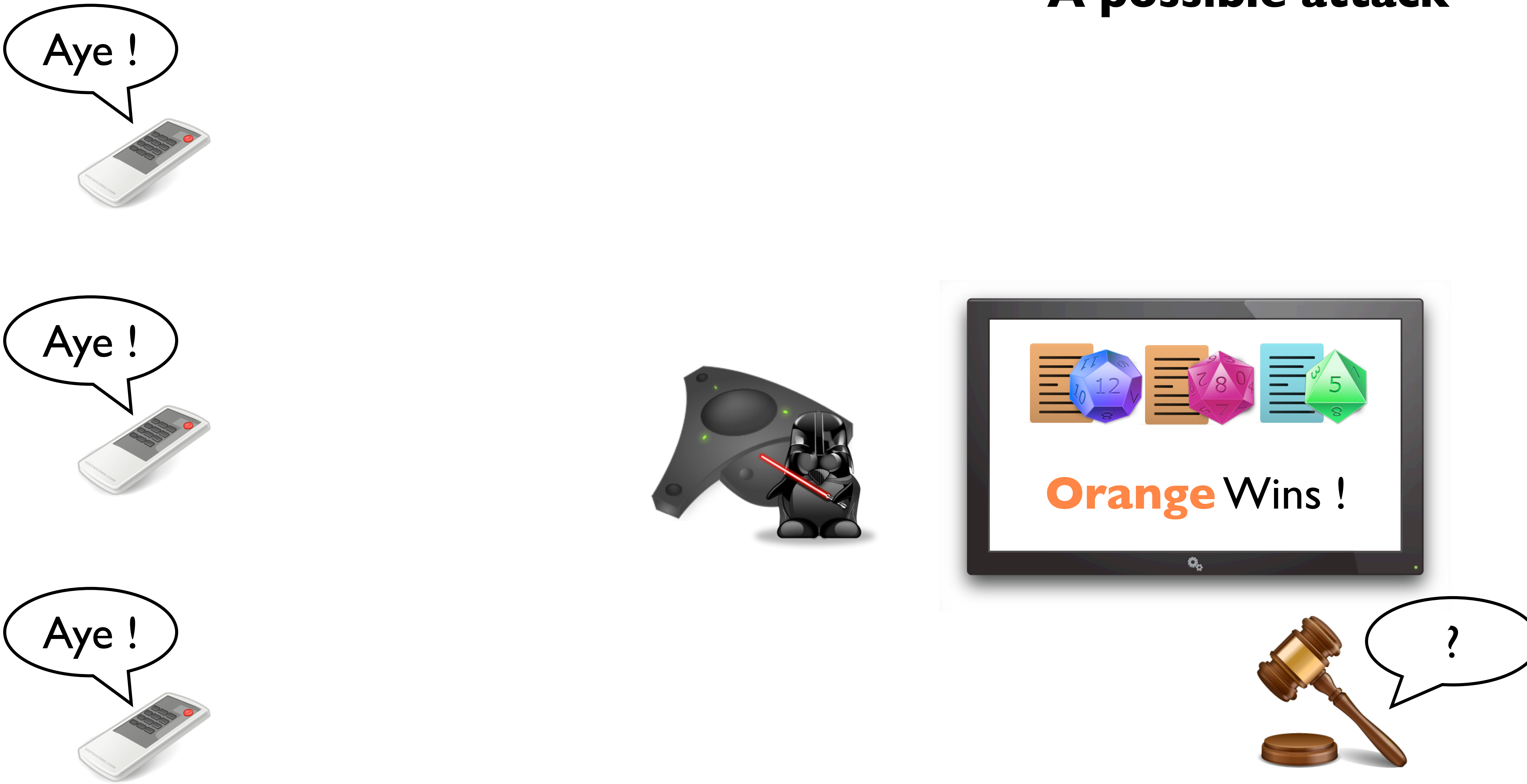
A possible attack



Similar to Clash Attacks [Küsters et al., S&P'12].

But...

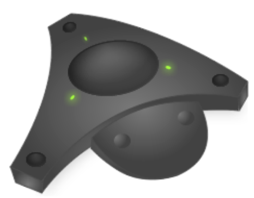
A possible attack



Similar to Clash Attacks [Küsters et al., S&P'12].

Two New Versions

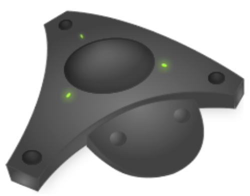
F2FV 1 :



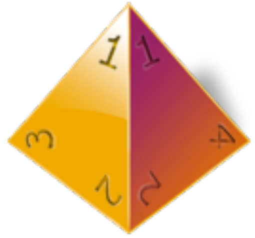

Randomness genererated
by the central device

Two New Versions

F2FV2:





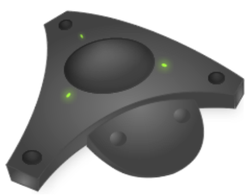


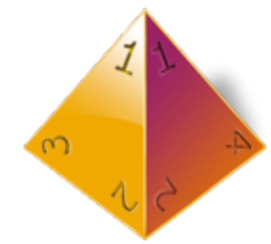
One more randomness
generated by the voter.

The system **still has privacy issues** when central device is corrupted.

Two New Versions

F2FV3:





Randomness only
generated by the voter.

We need that **voters generate actual random numbers**.

Contributions

We have **three** (slightly) **different protocols** for boardroom voting.

> **None of them** ensures privacy when BB is corrupted.

> **All of them** are easy to understand.

In this paper, we provide:

> **Proofs of privacy** of F2FV2 and F2FV3 assuming that infrastructure players are honest.

> **Proofs of correctness** in the case of a dishonest ballot box (central device).

Did you say « proofs » ?

Proof in a **symbolic model**.

We model the protocols using **applied pi-calculus**.

In the presence of an **attacker** who :

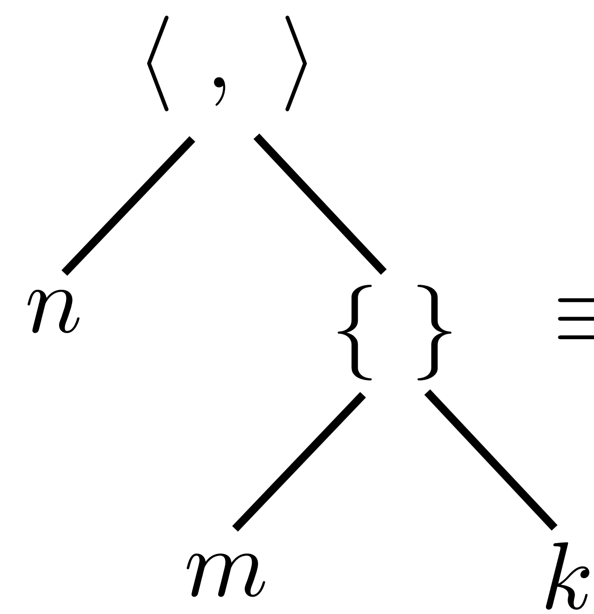
- can **read** every message sent on the network,
- can **intercept** messages,
- can **create** and **send** new messages.
- can **vote** himself.

Abstraction

Messages are represented by **terms**.

Nonces, keys :

$$n, m, \ldots, k_1, k_2, \ldots$$



$$\equiv \langle n, \{m\}_k \rangle$$

Primitives :

$$\{m\}_k, \langle m_1, m_2 \rangle$$

Modeling deduction rules :

$$\frac{x \quad y}{\langle x, y \rangle} \qquad \frac{\langle x, y \rangle}{x} \qquad \frac{\langle x, y \rangle}{y} \qquad \frac{x \quad y}{\{x\}_y} \qquad \frac{\{x\}_y \quad y}{x}$$

Applied Pi-Calculus

$\phi, \psi ::=$	formulae	
$M = N \mid M \neq N \mid \phi \wedge \psi \mid \phi \vee \psi$		
$P, Q, R ::=$	(plain) processes	
0		null process
$P \mid Q$		parallel composition
$!P$		replication
$\nu n.P$		name restriction
if ϕ then P else Q		conditional
$u(x).P$		message input
$\overline{u}\langle M \rangle.P$		message output
$\mathsf{event}(M).P$		event
$A, B, C ::=$	extended processes	
P		plain process
$A \mid B$		parallel composition
$\nu n.A$		name restriction
$\nu x.A$		variable restriction
$\{^{M}/_{x}\}$		active substitution

Introduced by Abadi and Fournet

Modeling the Protocol

A **simple equationnal theory**:

$$\mathsf{fst}(\mathsf{pair}(x_1, x_2)) = x_1$$

$$\mathsf{snd}(\mathsf{pair}(x_1, x_2)) = x_2$$

Modeling the Protocol

A **simple equationnal theory**:

$$\mathsf{fst}(\mathsf{pair}(x_1, x_2)) = x_1$$

$$\mathsf{snd}(\mathsf{pair}(x_1, x_2)) = x_2$$

A **sample**, the voter:

$$\begin{aligned} V_n(c, c_e, c_a, c_p, v) = \\ & \nu k \ . \ c(x) \ . \\ & \overline{c}\langle\langle x, k, v\rangle\rangle \ . \\ & c_e(y) \ . \\ & \text{if } \langle x, k, v\rangle \in_n y \\ & \text{then } \overline{\overline{c_a}}\langle \mathsf{ok}\rangle \text{ else } \overline{\overline{c_a}}\langle \mathsf{fail}\rangle \end{aligned}$$

Modeling the Protocol

A **simple equational theory**:

$$\mathsf{fst}(\mathsf{pair}(x_1, x_2)) = x_1$$

$$\mathsf{snd}(\mathsf{pair}(x_1, x_2)) = x_2$$

A **sample**, the voter:

$$\begin{aligned} V_n(c, c_e, c_a, c_p, v) = \ & \\ & \nu k \ . \ c(x) \ . \\ & \overline{c}\langle\langle x, k, v\rangle\rangle \ . \\ & c_e(y) \ . \\ & \text{if } \langle x, k, v\rangle \in_n y \\ & \text{then } \overline{\overline{c_a}}\langle \mathsf{ok}\rangle \text{ else } \overline{\overline{c_a}}\langle \mathsf{fail}\rangle \end{aligned}$$

$$\begin{aligned} B_n(c_v^1, \ldots, c_v^n, c_b) = \ & \\ & \nu r_1, \ldots, r_n \ . \\ & \overline{c_v^1}\langle r_1\rangle \ . \ \ldots \ . \ \overline{c_v^n}\langle r_n\rangle \ . \\ & c_v^1(y_1) \ . \ \ldots \ . \ c_v^n(y_n) \ . \\ & (\overline{c_b}\langle y_1\rangle \mid \cdots \mid \overline{c_b}\langle y_n\rangle) \end{aligned}$$

$$\begin{aligned} E_n(c_b, c_e, c_p) = \ & \\ & c_b(t_1) \ . \ \ldots \ . \ c_b(t_n) \ . \\ & \text{let } r = \langle t_1, \ldots, t_n\rangle \text{ in} \\ & \overline{c_p}\langle r\rangle \ . \ (! \ \overline{c_e}\langle r\rangle) \end{aligned}$$

$$\begin{aligned} A_n(c_e, c_a^1, \ldots, c_a^n, c_p) = \ & \\ & c_e(z') \ . \\ & c_a^1(z_1) \ . \ \ldots \ . \ c_a^n(z_n) \ . \\ & \text{if } \Psi_n(z', z_1, \ldots, z_n) \\ & \text{then } \overline{c_p}\langle \mathsf{ok}\rangle \text{ else } \overline{c_p}\langle \mathsf{fail}\rangle \end{aligned}$$

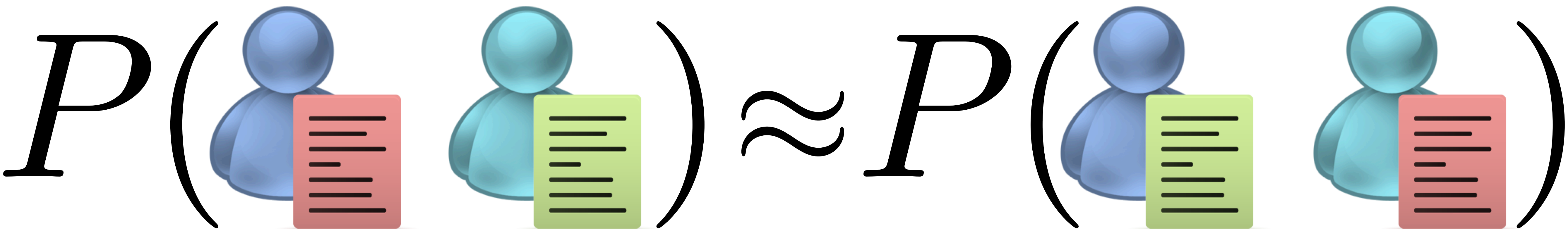
Property 1: Privacy

Privacy: (Delaune, Kremer, Ryan, 2009)

$P($   $) \approx P($   $)$

Property 1: Privacy

Privacy: (Delaune, Kremer, Ryan, 2009)



A bit more formally...

A process specification P satisfies **ballot secrecy** iff:

$$P\left[V_A\left\{^{v_1}/_v\right\} \mid V_B\left\{^{v_2}/_v\right\}\right] \approx_l P\left[V_A\left\{^{v_2}/_v\right\} \mid V_B\left\{^{v_1}/_v\right\}\right]$$

with $\approx_l$ the **observational equivalence**.

Privacy Results

Theorem 1

Assuming that the **infrastructure players** (Ballot Box, Screen, Assessor) **are honest** and, at least, **two voters are honest**:

F2FV2 and F2FV3 preserve ballot privacy.

Privacy Results

Theorem 1

Assuming that the **infrastructure players** (Ballot Box, Screen, Assessor) **are honest** and, at least, **two voters are honest**:

F2FV2 and F2FV3 preserve ballot privacy.

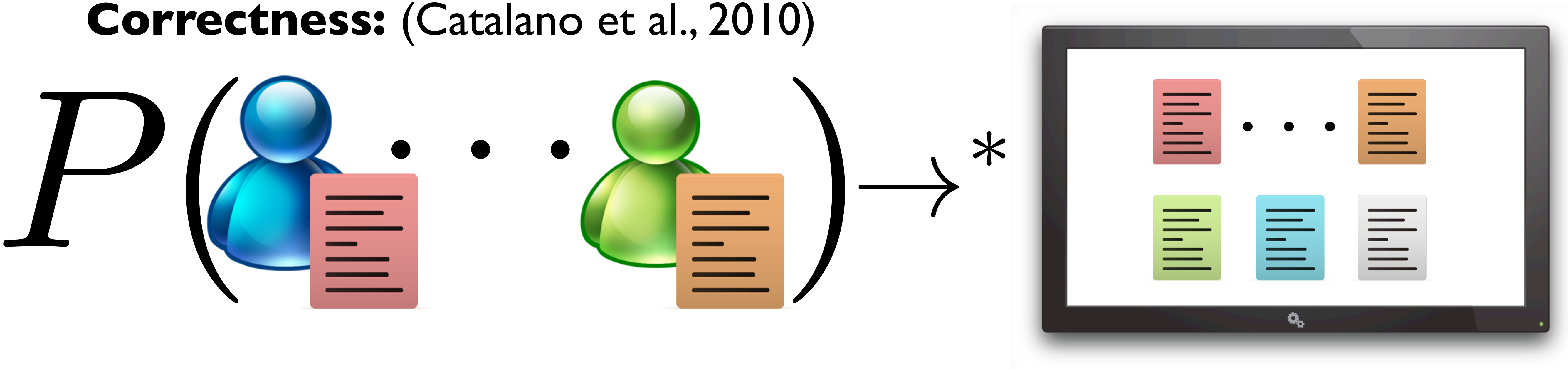
Theorem 2

Even if the **Assessor is also dishonest**:

F2FV2 and F2FV3 still preserve ballot privacy.

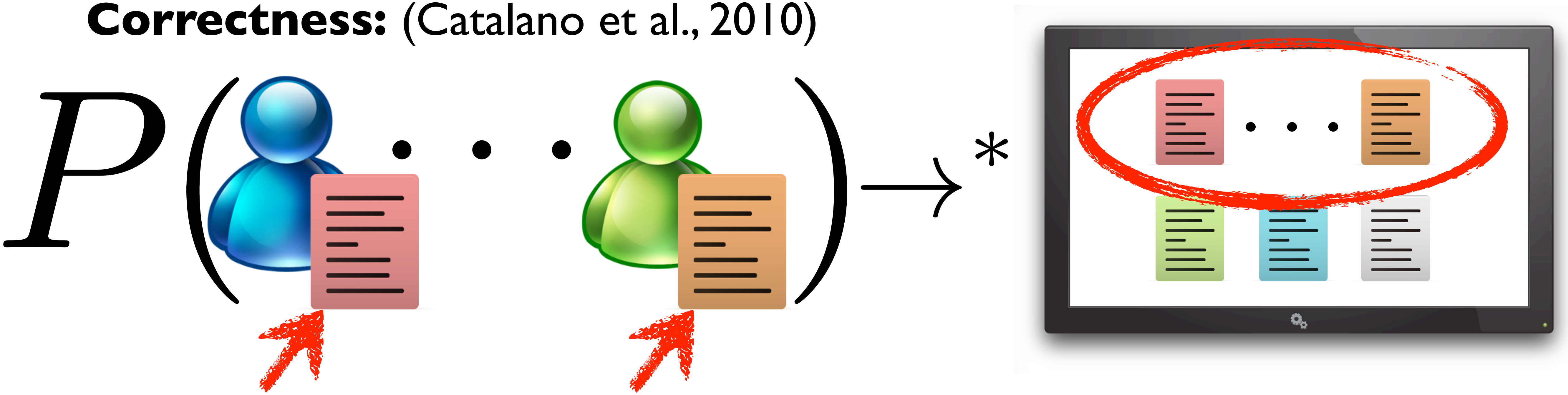
Property 2: Correctness

Correctness: (Catalano et al., 2010)



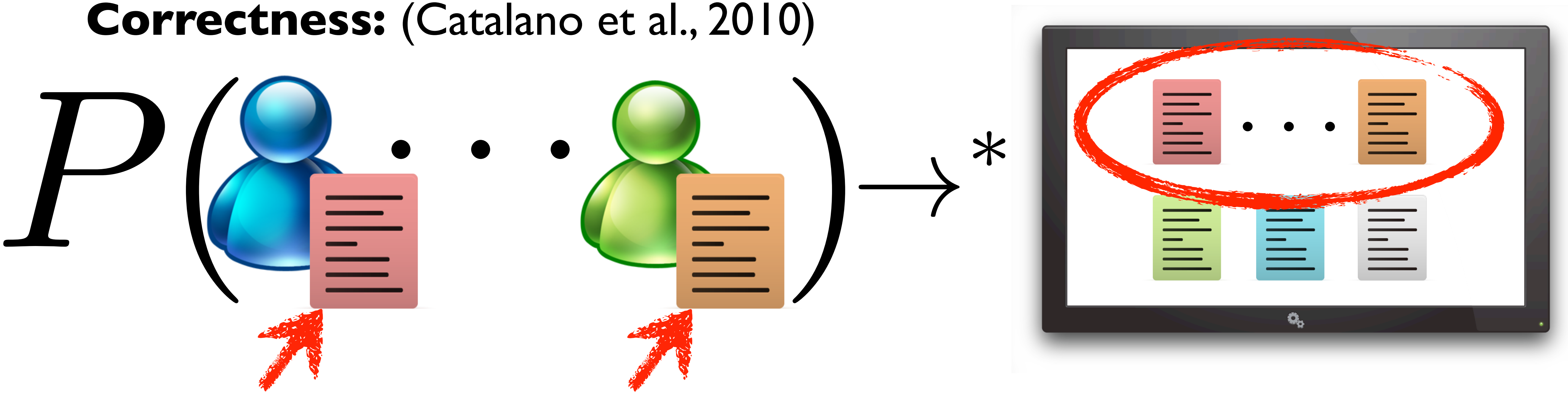
Property 2: Correctness

Correctness: (Catalano et al., 2010)



Property 2: Correctness

Correctness: (Catalano et al., 2010)



A bit more formally...

$\forall v_1, \ldots, v_m$
and every execution of the protocol leading to validation of result t_r:

$$P\,[V_1(v_1) \mid \cdots \mid V_m(v_m)] \rightarrow^* \nu\tilde{n}.\,(\text{event}(t_r)\ .\ Q \mid Q')$$

then $\exists\ v_{m+1}, \ldots, v_n$ and a permutation τ such that:

$$t_r = \langle v_{\tau(1)}, \ldots, v_{\tau(n)} \rangle$$

Correctness Results

Theorem 3

Even if the **Ballot Box is corrupted**, assuming that **the Screen and the Assessor are honest**:

F2FV2 and F2FV3 ensure vote correctness.

Results: Summary

Results	Privacy			Correctness		
\ Corr. Players System \	None	Ballot Box	Assessor	None	Ballot Box	Assessor
F2FV1	✓	✗	✓	✓	✗	✗
F2FV2	✓	✗	✓	✓	✓	✗
F2FV3	✓	✗	✓	✓	✓	✗

Conclusion

- Two versions of a boardroom voting system **ensuring privacy** and **vote correctness** in a very convenient way.

- To ensure vote correctness, we need that:

  > Voters **really use** (unpredictable) random numbers.

  > Voters **must cast a vote** (even blank) and **check it**.

Conclusion

- Two versions of a boardroom voting system **ensuring privacy** and **vote correctness** in a very convenient way.

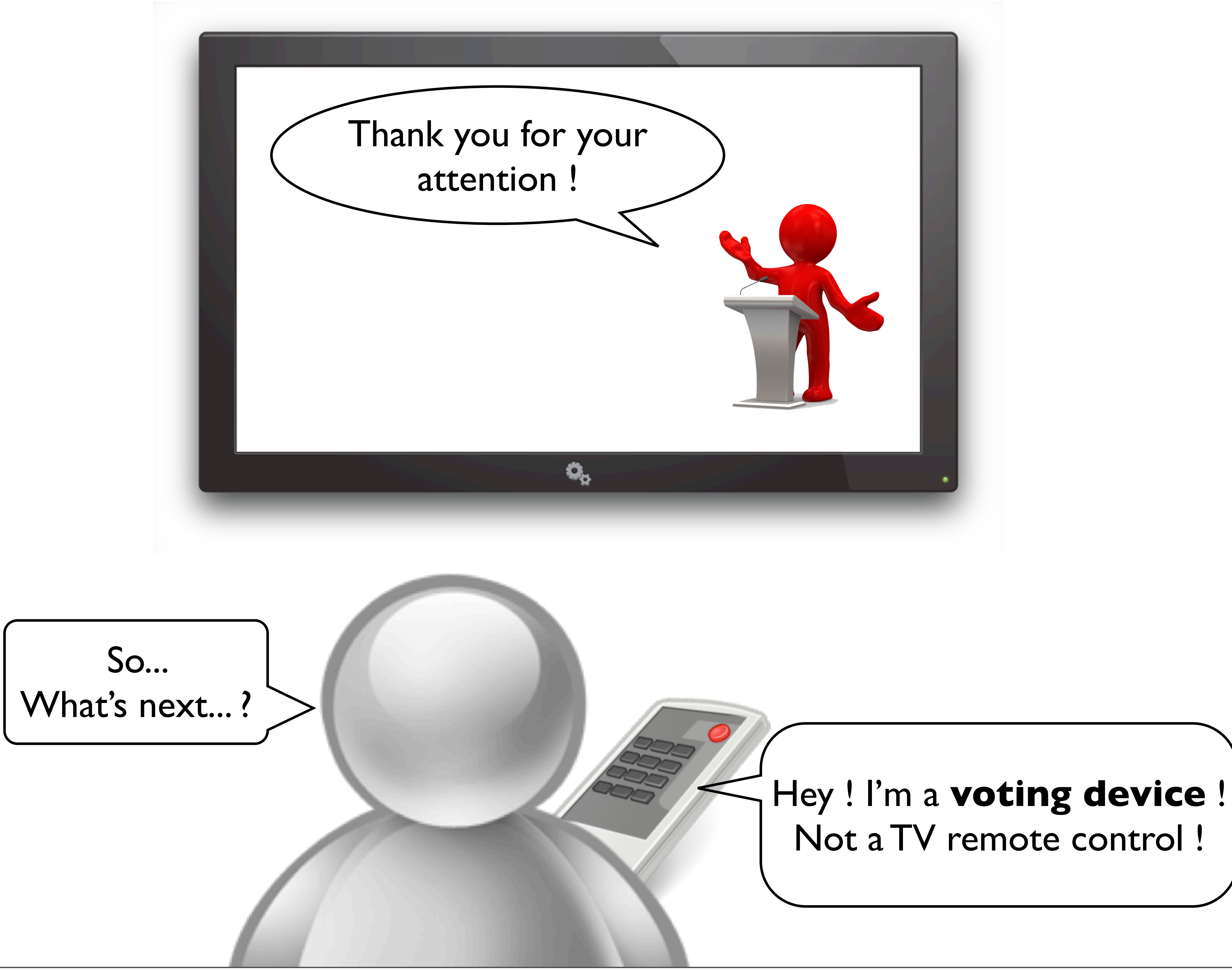
- To ensure vote correctness, we need that:

  > Voters **really use** (unpredictable) random numbers.

  > Voters **must cast a vote** (even blank) and **check it**.

Future Work

- Although the system is clearly **not coercion-resistant**, we may have a form of **receipt-freeness**.


Thank you for your attention !
So... What's next... ?
Hey ! I'm a **voting device** ! Not a TV remote control !