**Probabilistic Contract Signing**

Vitaly Shmatikov

---

**Rabin’s Beacon**

- A "beacon" is a trusted party that publicly broadcasts a randomly chosen number between 1 and N every day.

---

**Rabin’s Contract Signing Protocol**

\[
\begin{align*}
\text{sig}_A & \text{"I am committed if } i \text{ is broadcast on day } D \text{"} \\
\text{sig}_B & \text{"I am committed if } i \text{ is broadcast on day } D \text{"} \\
\end{align*}
\]

\[
\text{CONTRACT}(A, B, \text{future date } D, \text{contract terms})
\]

\[
\begin{align*}
\text{sig}_A & \text{"I am committed if } 1 \text{ is broadcast on day } D \text{"} \\
\text{sig}_B & \text{"I am committed if } i \text{ is broadcast on day } D \text{"} \\
\end{align*}
\]

\[
\text{sig}_A \text{"I am committed if } N \text{ is broadcast on day } D \text{"}
\]

\[
\text{sig}_B \text{"I am committed if } N \text{ is broadcast on day } D \text{"}
\]

2N messages are exchanged if both parties are honest.

---

**Probabilistic Fairness**

- Suppose B stops after receiving A’s ith message
  - B has sigA"committed if } i \text{ is broadcast}"
  - sigA"committed if } i+1 \text{ is broadcast}"
  - sigA"committed if } i+2 \text{ is broadcast}"
  - …
  - sigA"committed if } i+k \text{ is broadcast}"
- A has sigB"committed if } i \text{ is broadcast}"
- …
- sigB"committed if } i+k+1 \text{ is broadcast}"
- … and beacon broadcasts number b on day D
  - If b < i, then both A and B are committed
  - If b > i, then neither A, nor B is committed
  - If b = i, then only A is committed

This happens only with probability 1/N.

---

**Properties of Rabin’s Protocol**

- **Fair**
  - The difference between A’s probability to obtain B’s commitment and B’s probability to obtain A’s commitment is at most 1/N
    - But communication overhead is 2N messages
- **Not optimistic**
  - Need input from third party in every transaction
    - Same input for all transactions on a given day sent out as a one-way broadcast. Maybe this is not so bad!
- **Not timely**
  - If one of the parties stops communicating, the other does not learn the outcome until day D

---

**BGMR Probabilistic Contract Signing**

[Ben-Or, Goldreich, Micali, Rivest '85-90]

- Doesn’t need beacon input in every transaction
- Uses sigA"I am committed with probability p_A" instead of sigA"I am committed if } i \text{ is broadcast on day } D \text{"}
- Each party decides how much to increase the probability at each step
  - A receives sig_B"I am committed with probability p_B" from B
  - Sets p_A = \min(1, p_B \cdot \alpha)
  - Sends sig_A"I am committed with probability p_A" to B
  - … the algorithm for B is symmetric
**BGMR Message Flow**

- \( \text{sig}_B \) \( \text{I am committed with probability} \ 0.10 \)
- \( \text{sig}_A \) \( \text{I am committed with probability} \ 0.10 \)
- \( \text{CONTRACT}(A, B, \text{future date} D, \text{contract terms}) \)
- \( \text{sig}_B \) \( \text{I am committed with probability} \ 0.20 \)
- \( \text{sig}_A \) \( \text{I am committed with probability} \ 0.20 \)
- ... 
- \( \text{sig}_B \) \( \text{I am committed with probability} \ 1.00 \)
- \( \text{sig}_A \) \( \text{I am committed with probability} \ 1.00 \)

**Conflict Resolution**

- \( \text{sig}_A \) \( \text{I am committed with probability} \ pA1 \)
- \( \text{sig}_B \) \( \text{I am committed with probability} \ pA2 \)
- \( \text{sig}_B \) \( \text{I am committed with probability} \ pB1 \)

- Waits until date D
- If \( p < p_{B1} \), contract is binding, else contract is canceled

**Judge**

- Waits until date D to decide
- Announces verdict to both parties
- Tosses coin once for each contract
- Remembers previous coin tosses
  - Constant memory: use pseudo-random functions with a secret input to produce repeatable coin tosses for each contract
- Does not remember previous verdicts
  - Same coin toss combined with different evidence (signed message with a different probability value) may result in a different verdict

**Privilege and Fairness**

- Privilege
  - A party is privileged if it has the evidence to cause the judge to declare contract binding
  - Intuition: at each step the parties should have comparable probabilities of causing the judge to declare contract binding (privilege must be symmetric)

- Fairness
  - At any step where \( \text{Prob}(B \text{ is privileged}) > v, \) \( \text{Prob}(A \text{ is not privileged} | B \text{ is privileged}) < \frac{1}{1+\alpha} \)
  - Intuition: at each step, the parties should have comparable probabilities of causing the judge to declare contract binding

**Properties of BGMR Protocol**

- Fair
  - Privilege is almost symmetric at each step:
    - if \( \text{Prob}(B \text{ is privileged}) > p_{A0} \) then
    - \( \text{Prob}(A \text{ is not privileged} | B \text{ is privileged}) < 1-1/\alpha \)
- Optimistic
  - Two honest parties don’t need to invoke a judge
- Not timely
  - Judge waits until day D to toss the coin
  - What if the judge tosses the coin and announces the verdict as soon as he is invoked?

**Formal Model**

- Protocol should ensure fairness given any possible behavior by a dishonest participant
  - Contact judge although communication hasn’t stopped
  - Contact judge more than once
  - Delay messages from judge to honest participant

- Need nondeterminism
  - To model dishonest participant’s choice of actions
- Need probability
  - To model judge’s coin tosses
- The model is a Markov decision process
Constructing the Model

- Discretize probability space of coin tosses
  - The coin takes any of N values with equal probability
- Fix each party’s "probability step"
  - Rate of increases in the probability value contained in the party’s messages determines how many messages are exchanged
- A state is unfair if privilege is asymmetric
  - Difference in evidence, not difference in commitments
- Compute probability of reaching an unfair state for different values of the parties’ probability steps

Attack Strategy

- Dishonest B's probability of driving the protocol to an unfair state is maximized by this strategy:
  1. Contact judge as soon as first message from A arrives
  2. Judge tries to send verdict to A (the verdict is probably negative, since A's message contains a low probability value)
  3. B delays judge's verdicts sent to A
  4. B contacts judge again with each new message from A until a positive verdict is obtained
- This strategy only works in the timely protocol
  - In the original protocol, coin is not tossed and verdict is not announced until day D
- Conflict between optimism and timeliness

Analysis Results

For a higher probability of winning, dishonest B must exchange more messages with honest A

Attacker’s Tradeoff

- Linear tradeoff for dishonest B between probability of winning and ability to delay judge's messages to A
- Without complete control of the communication network, B may settle for a lower probability of winning

Summary

- Probabilistic contract signing is a good testbed for probabilistic model checking techniques
  - Standard formal analysis techniques not applicable
  - Combination of nondeterminism and probability
  - Good for quantifying tradeoffs
- Probabilistic contract signing is subtle
  - Unfairness as asymmetric privilege
  - Optimism cannot be combined with timeliness, at least not in the obvious way