University of Fribourg

Bern University of Applied Sciences

A Measure of Coercion-Resistance and its Application on JCJ Derivatives

Oliver Spycher

Biel, November 17th, 2011

Outline

δ-Coercion-Resistance by Küster et al.

Coercion Resistance of JCJ

Coercion Resistance of JCJ Derivatives

Outline

δ-Coercion-Resistance by Küster et al.

Coercion Resistance of JCJ

Coercion Resistance of JCJ Derivatives

Our Understading of Coercion-Resistance

A voting protocol is coercion-resistant, if the adversary cannot tell whether a subject complied or applied a counter-strategy.

Possible Coercive Attacks

- Receipt-based
- Simulation
- Randomization
- Forced Abstention

An attack

- two candidates c_1, c_2, three voters v_1, v_2, v_3
- v_1 wants to vote for c_1
- coercer wants v_1 to vote for c_2
- v_1 wins, if $r_2 = 3$; result denoted $R = (r_1, r_2)$

An attack

- two candidates c_1, c_2, three voters v_1, v_2, v_3
- v_1 wants to vote for c_1
- coercer wants v_1 to vote for c_2
- v_1 wins, if $r_2 = 3$; result denoted $R = (r_1, r_2)$

v_1 thinks

- *Given that v_2 and v_3 vote for c_2 with 50% probability each,* **the chance of winning is 25% when complying with the coercer and 0% otherwise**. *Is this worth it?*

The coercer is smart, so he chooses a better strategy.

A smarter attack

- two candidates c_1, c_2, three voters v_1, v_2, v_3
- v_1 wants to vote for c_1
- coercer wants v_1 to vote for c_2
- v_1 wins, **if the probability of his compliance is greater than the probability of his non-compliance**

R	$P(R\|c_1)$	$P(R\|c_2)$
$(0,3)$	0	0.25
$(1,2)$	0.25	0.5
$(2,1)$	0.5	0.25
$(3,0)$	0.25	0

A smarter attack

- two candidates c_1, c_2, three voters v_1, v_2, v_3
- v_1 wants to vote for c_1
- coercer wants v_1 to vote for c_2
- v_1 wins, **if the probability of his compliance is greater than the probability of his non-compliance**

R	$P(R\|c_1)$	$P(R\|c_2)$
$(0,3)$	0	0.25
$(1,2)$	0.25	0.5
$(2,1)$	0.5	0.25
$(3,0)$	0.25	0

$$P(money|c_1) = 0.25$$
$$P(money|c_2) = 0.75$$

Probability of winning dramatically increases for v_1 in case of complying with the coercer

A smarter attack

- two candidates c_1, c_2, three voters v_1, v_2, v_3
- v_1 wants to vote for c_1
- coercer wants v_1 to vote for c_2
- v_1 wins, **if the probability of his compliance is greater than the probability of his non-compliance**

R	$P(R \mid c_1)$	$P(R \mid c_2)$
$(0,3)$	0	0.25
$(1,2)$	0.25	0.5
$(2,1)$	0.5	0.25
$(3,0)$	0.25	0

$$P(money \mid c_1) = 0.25$$
$$P(money \mid c_2) = 0.75$$

Probability of winning dramatically increases for v_1 in case of complying with the coercer (by $\delta = 0.75 - 025$)

Coercion-resistance δ_{min} in the ideal protocol

Definitions

- k candidates, n honest participating voters
- $R = (r_0, .., r_k) result \in RES$, r_0 abstentions
- $P = (p_0, .., p_k)$ probability distribution of R

$r_0 + .. + r_k = n + 1$ (dishonest voters controlled by coercer)

Finding δ_{min}

- Coercer wants candidate j, voter wants candidate i
- $A_R^q = P(R|q)$*, given coerced voter voted for candidate q*
- Coercer accepts run, iff $A_R^i \leq A_R^j$
- $\delta_{min} = \max_j \sum_{R \in RES: A_R^i \leq A_R^j} (A_R^j - A_R^i)$

note: $A_R^i \leq A_R^j$, iff $\frac{r_j}{r_i} \geq \frac{p_j}{p_i}$

The meaning of δ_{min}

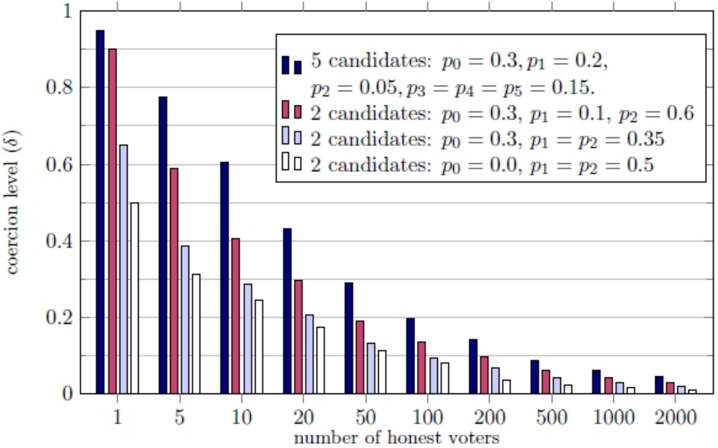
The maximum fraction of the desired reward expected to be lost, when not complying with the coercer, in opposition to complying.

Example

- $k = 2$ candidates, $n = 2000$ honest participating voters
- $P = (p_0 = 0.3, p_1 = 0.35, p_2 = 0.35)$ probability distribution of R
- Coercer offers 50.–

- $\delta_{min} = 0.021$, assuming voter wants candidate 1
- $E(money|complying) - E(money|notcomplying) = \delta_{min} \times 50.-$
- **In average the voter will loose 1.05** Should he comply?

Get a feeling



Outline

δ-Coercion-Resistance by Küster et al.

Coercion Resistance of JCJ

Coercion Resistance of JCJ Derivatives

Making JCJ an ideal protocol

If JCJ were ideal regarding coercion-resistance, then $\delta = \delta_{min}$, but is it?

Assumptions

- trustworthy registrars during setup
- trustworthy talliers (as a group)
- anonymous channel
- trusted platform
- adversarial uncertainty

$\rightarrow$ JCJ relies on **adversarial uncertainty regarding R and Γ**

Given the distribution of R, JCJ can be shown to be ideal. But how handle Γ? How big will it be?

Coercion based on Γ

Coercer wants to find out if voter applied counter-strategy by observing how many fake votes have been cast.

Assume Γ a random Variable with distribution $F_\Gamma(x)$

Assume $F_\Gamma(x)$ has only 1 local maximum

Coercion based on Γ

Coercer wants to find out if voter applied counter-strategy by observing how many fake votes have been cast.

Assume Γ a random Variable with distribution $F_\Gamma(x)$

Assume $F_\Gamma(x)$ has only 1 local maximum

Voter wins, if $\Gamma <= x_0; F_\Gamma(x_0) = \max F_\Gamma(x)$

Easy to see that $\delta_\Gamma = \frac{1}{\max F_\Gamma(x)}$

Coercion based on Γ

Coercer wants to find out if voter applied counter-strategy by observing how many fake votes have been cast.

Assume Γ a random Variable with distribution $F_\Gamma(x)$

Assume $F_\Gamma(x)$ has only 1 local maximum

Voter wins, if $\Gamma <= x_0; F_\Gamma(x_0) = \max F_\Gamma(x)$

Easy to see that $\delta_\Gamma = \frac{1}{\max F_\Gamma(x)}$

What do we conclude from our experiment?

Coercion based on Γ

Coercer wants to find out if voter applied counter-strategy by observing how many fake votes have been cast.

Assume Γ a random Variable with distribution $F_\Gamma(x)$

Assume $F_\Gamma(x)$ has only 1 local maximum

Voter wins, if $\Gamma <= x_0; F_\Gamma(x_0) = \max F_\Gamma(x)$

Easy to see that $\delta_\Gamma = \frac{1}{\max F_\Gamma(x)}$

What do we conclude from our experiment?

How do δ_Γ and δ_{min} relate to eachother?

Outline

δ-Coercion-Resistance by Küster et al.

Coercion Resistance of JCJ

Coercion Resistance of JCJ Derivatives

The Schemes

To improve the efficiency of time-critical operations

- KH11 (Luzern)
- SKHS11b (VoteID)
- Clarke
- SKHS11a (FCJCJ)
- FCJCJ++
- Araujo

Except Araujo: Trade-off between coercion-resistance and efficiency (parameter)

Araujo: No verifiability in the sense of the other schemes

SKHS11b, Clarke, SKHS11a (FCJCJ), FCJCJ++

Associate votes with voter roll entries to improve efficiency in tallying.

Trade-off between coercion-resistance and efficiency controlled by parameter β.

Coercer strategy: Count number of votes associated with voter roll entry. Compute δ_β similar as δ_Γ.

Comparison

10000 voters

	SKHS11b	Clarke	SKHS11a	FCJCJ++
δ	0.1	0.1	0.1	0.1
β	16	16	10	10
Setup	o	o	o	x
Casting	o	x	o	o
Tallying	x	o	x	o

Comparison

10000 voters

	SKHS11b	Clarke	SKHS11a	FCJCJ++
δ	0.04	0.04	0.04	0.04
β	100	100	25	25
Setup	o	o	o	x
Casting	o	x	o	o
Tallying	x	o	x	o

Comparison

10000 voters

	SKHS11b	Clarke	SKHS11a	FCJCJ++
δ	0.01	0.01	0.01	0.01
β	2000	2000	100	100
Setup	o	o	o	x
Casting	o	x	o	o
Tallying	x	o	x	o

Thank You!

Questions / Remarks

e-voting.bfh.ch and **www.secuso.cased.de**

contacts, papers, reports