Risk Balance in Exchange Protocols

Yanjing Wang

Joint work with Mohammad Torabi Dashti
Center voor Wiskunde en Informatica, Amsterdam

ASIAN'07, Dec 09 2007

Contents

Introduction to Exchange protocols

Exchange Protocols

Aim at establishing successful exchanges of electronic goods between two or more parties.

Introduction to Exchange protocols

Exchange Protocols

Aim at establishing successful exchanges of electronic goods between two or more parties.

- Fairness is a crucial requirement.

Introduction to Exchange protocols

Exchange Protocols

Aim at establishing successful exchanges of electronic goods between two or more parties.

- Fairness is a crucial requirement.
- No fair deterministic asynchronous exchange protocols without TTP [Even,Yacobi 1980].

Introduction to Exchange protocols

Exchange Protocols

Aim at establishing successful exchanges of electronic goods between two or more parties.

- Fairness is a crucial requirement.
- No fair deterministic asynchronous exchange protocols without TTP [Even,Yacobi 1980].
- Other methods are based on gradual release of information or gradual increase of privilege may approximate fairness.

Introduction to Exchange protocols

Example of 2-party Exchange Protocols with TTP

1.	$A \to TTP : h(s)$	where h is a hash function and $s \in S_A$
2.	$B \to TTP : SET$	where $SET = \{h(x) \mid x \in S_B\}$
3.	$TTP \to A, B : h(s)$	if $h(s) \in SET$
	$TTP \to A, B : \bot$	if $h(s) \notin SET$

Introduction to Exchange protocols

Example of 2-party Exchange Protocols with TTP

1. $A \rightarrow TTP : h(s)$ — where h is a hash function and $s \in S_A$
2. $B \rightarrow TTP : SET$ — where $SET = \{h(x) | x \in S_B\}$
3. $TTP \rightarrow A, B : h(s)$ — if $h(s) \in SET$

   $TTP \rightarrow A, B : \perp$ — if $h(s) \notin SET$

- We assume the third party can be compromised by paying some cost.

Introduction to Exchange protocols

Example of 2-party Exchange Protocols with TTP

1.	$A \to TTP : h(s)$	where h is a hash function and $s \in S_A$
2.	$B \to TTP : SET$	where $SET = \{h(x) \mid x \in S_B\}$
3.	$TTP \to A, B : h(s)$	if $h(s) \in SET$
	$TTP \to A, B : \bot$	if $h(s) \notin SET$

- We assume the third party can be compromised by paying some cost.
- The players have risks when the other party compromises the third party. One party may cause more damage to the other by compromising the TTP.

Introduction to Exchange protocols

Example of 2-party Exchange Protocols with TTP

1.	$A \to TTP : h(s)$	where h is a hash function and $s \in S_A$
2.	$B \to TTP : SET$	where $SET = \{h(x) \mid x \in S_B\}$
3.	$TTP \to A, B : h(s)$	if $h(s) \in SET$
	$TTP \to A, B : \bot$	if $h(s) \notin SET$

- We assume the third party can be compromised by paying some cost.
- The players have risks when the other party compromises the third party. One party may cause more damage to the other by compromising the TTP.
- We want to know the expected behaviors of rational agents if they can compromise the TTP by paying a cost.

Basic Game Theory

In a game we have Players, Strategies and Utilities.

Prisoner's dilemma

$A \backslash B$	Stay silent	Betray
Stay silent	1,1	-2,3
Betray	3,-2	-1,-1

Basic Game Theory

In a game we have Players, Strategies and Utilities.

Prisoner's dilemma

$A \backslash B$	Stay silent	Betray
Stay silent	1,1	-2,3
Betray	3,-2	-1,-1

The solutions of the game are the expected behavior of rational agents.

Nash equilibrium

Strategy pair (S_A, S_B) is a Nash equilibrium if A is making the best decision A can, given B's decision, and B is making the best decision B can, taking into account A's decision.

Basic Game Theory

In a game we have Players, Strategies and Utilities.

Prisoner's dilemma

$A \backslash B$	Stay silent	Betray
Stay silent	1,1	-2,3
Betray	3,-2	-1,-1

The solutions of the game are the expected behavior of rational agents.

Nash equilibrium

Strategy pair (S_A, S_B) is a Nash equilibrium if A is making the best decision A can, given B's decision, and B is making the best decision B can, taking into account A's decision.

Protocol as Strategic Game

- Players : A, B
- Strategies:
  - *Honest* (to do everything according to the protocol)
  - *Dishonest* (to compromise TTP by paying a cost)
- Utilities are as follows:

Protocol as Strategic Game

- Players : A, B
- Strategies:
  - *Honest* (to do everything according to the protocol)
  - *Dishonest* (to compromise TTP by paying a cost)
- Utilities are as follows:

Protocol Game

Given a two-party exchange protocol Prot with a TTP, the strategic game $G(\text{Prot})$ is defined as follows:

$A \backslash B$	$\mathcal{H}_B$	$\mathfrak{D}\mathcal{H}_B$
$\mathcal{H}_A$	$g_B^A - g_A^A, g_A^B - g_B^B$	$-r_A^A, r_A^B - c_B$
$\mathfrak{D}\mathcal{H}_A$	$r_B^A - c_A, -r_B^B$	$r_B^A - r_A^A - c_A, r_A^B - r_B^B - c_B$

Protocol as Strategic Game

- g_x^y is y's evaluation of the goods that x wants to exchange;
- r_x^y is y's evaluation of the risk that x has, if the TTP is compromised by the opponent of x;
- c_x is the cost x pays to compromise the TTP.

Protocol Game

Given a two-party exchange protocol Prot with a TTP, the strategic game $G(\text{Prot})$ is defined as follows:

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$g_B^A - g_A^A, g_A^B - g_B^B$	$-r_A^A, r_A^B - c_B$
$\mathcal{DH}_A$	$r_B^A - c_A, -r_B^B$	$r_B^A - r_A^A - c_A, r_A^B - r_B^B - c_B$

Simplified Protocol game $SG(\text{Prot})$

Simplified Protocol Game

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho - 1)g, (\rho - 1)g$	$-a, \rho a - c$
$\mathcal{DH}_A$	$\rho b - c, -b$	$\rho b - a - c, \rho a - b - c$

Simplified Protocol game $SG(\text{Prot})$

- $\rho > 1$ is a fixed exchange rate.

Simplified Protocol Game

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho - 1)g, (\rho - 1)g$	$-a, \rho a - c$
$\mathcal{DH}_A$	$\rho b - c, -b$	$\rho b - a - c, \rho a - b - c$

Simplified Protocol game $SG(\text{Prot})$

- $\rho > 1$ is a fixed exchange rate.
- g is the objective value of the goods to be exchanged.

Simplified Protocol Game

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho-1)g, (\rho-1)g$	$-a, \rho a - c$
$\mathcal{DH}_A$	$\rho b - c, -b$	$\rho b - a - c, \rho a - b - c$

Simplified Protocol game $SG(\text{Prot})$

- $\rho > 1$ is a fixed exchange rate.
- g is the objective value of the goods to be exchanged.
- a (b) is the risk of A (B) if the opponent compromises the TTP.

Simplified Protocol Game

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho-1)g, (\rho-1)g$	$-a, \rho a - c$
$\mathcal{DH}_A$	$\rho b - c, -b$	$\rho b - a - c, \rho a - b - c$

Simplified Protocol game $SG(\text{Prot})$

- $\rho > 1$ is a fixed exchange rate.
- g is the objective value of the goods to be exchanged.
- a (b) is the risk of A (B) if the opponent compromises the TTP.
- c is the cost of compromising the TTP.

Simplified Protocol Game

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho-1)g, (\rho-1)g$	$-a, \rho a - c$
$\mathcal{DH}_A$	$\rho b - c, -b$	$\rho b - a - c, \rho a - b - c$

Expected behavior of the protocol

Nash equilibria of simplified protocol games as the expected behaviors of the rational agents when executing the protocols.

Notation

$\Delta = |a - b|$ and $\Delta_U(S_A, S_B) = |\text{Utility}_A(S_A, S_B) - \text{Utility}_B(S_A, S_B)|$

Δ–condition

An exchange protocol Prot satisfies Δ-condition iff $\Delta < (1 - \frac{1}{\rho})g$ in $SG(\text{Prot})$. Such a protocol Prot is called *risk-balanced*.

Main result

Theorem

For any risk-balanced protocol Prot*, there are Nash equilibria in* $SG(\text{Prot})$*, and for each such Nash equilibrium* (S_A, S_B) *the following holds:*

$$\Delta_U(S_A, S_B) < (\rho - \frac{1}{\rho})g.$$

Sketch of the proof

Main result

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho - 1)g, (\rho - 1)g$	$-a, \rho a - c$
$\mathcal{DH}_A$	$\rho b - c, -b$	$\rho b - a - c, \rho a - b - c$

Sketch of the proof

1. Under the Δ−condition, $\Delta_U(\mathcal{H}_A, \mathcal{H}_B) = 0 < (\rho - \frac{1}{\rho})g$; $\Delta_U(\mathcal{DH}_A, \mathcal{DH}_B) < (\rho - \frac{1}{\rho})g$.

Main result

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho-1)g, (\rho-1)g$	$-a, \rho a - c$
$\mathcal{DH}_A$	$\rho b - c, -b$	$\rho b - a - c, \rho a - b - c$

Sketch of the proof

1. Under the Δ−condition, $\Delta_U(\mathcal{H}_A, \mathcal{H}_B) = 0 < (\rho - \frac{1}{\rho})g$; $\Delta_U(\mathcal{DH}_A, \mathcal{DH}_B) < (\rho - \frac{1}{\rho})g$.
2. Under the Δ−condition, $(\mathcal{H}_A, \mathcal{DH}_B)$ and $(\mathcal{DH}_A, \mathcal{H}_B)$ are not the Nash equilibria of $SG(\text{Prot})$.

Main result

$A\backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho-1)g,(\rho-1)g$	$-a,\rho a-c$
$\mathcal{DH}_A$	$\rho b-c,-b$	$\rho b-a-c,\rho a-b-c$

Sketch of the proof

1. Under the Δ–condition, $\Delta_U(\mathcal{H}_A,\mathcal{H}_B)=0<(\rho-\frac{1}{\rho})g$; $\Delta_U(\mathcal{DH}_A,\mathcal{DH}_B)<(\rho-\frac{1}{\rho})g$.
2. Under the Δ–condition, $(\mathcal{H}_A,\mathcal{DH}_B)$ and $(\mathcal{DH}_A,\mathcal{H}_B)$ are not the Nash equilibria of $SG(\text{Prot})$.
3. Either $(\mathcal{H}_A,\mathcal{H}_B)$ or $(\mathcal{DH}_A,\mathcal{DH}_B)$ is a N.E. of $SG(\text{Prot})$.

Main result

Theorem

For any risk-balanced protocol Prot*, there are Nash equilibria in* $SG(\text{Prot})$*, and for each such Nash equilibrium* (S_A, S_B) *the following holds:*

$$\Delta_U(S_A, S_B) < (\rho - \frac{1}{\rho})g.$$

Sketch of the proof

1. Under the Δ–condition, $\Delta_U(\mathcal{H}_A, \mathcal{H}_B) = 0 < (\rho - \frac{1}{\rho})g$; $\Delta_U(\mathcal{DH}_A, \mathcal{DH}_B) < (\rho - \frac{1}{\rho})g$.
2. Under the Δ–condition, $(\mathcal{H}_A, \mathcal{DH}_B)$ and $(\mathcal{DH}_A, \mathcal{H}_B)$ are not the Nash equilibria of $SG(\text{Prot})$.
3. Either $(\mathcal{H}_A, \mathcal{H}_B)$ or $(\mathcal{DH}_A, \mathcal{DH}_B)$ is a N.E. of $SG(\text{Prot})$.

An example protocol

A secret comparison protocol based on [Teepe 06]

1. $A \rightarrow \Gamma : (f_{\text{prov}}, A, B, \omega)$, where $\omega = h(\mathcal{I}, \aleph, A, B)$
2. $B \rightarrow \Gamma : (f_{\text{verif}}, A, B, \Omega_B)$, where $\Omega_B = \{h(i, \aleph, A, B) \mid i \in \mathcal{E}_B\}$
3. Γ checks if $\omega \in \Omega_B$. If yes, then $\Gamma \downarrow \textsc{ftp} : \omega$, else $\Gamma \downarrow \textsc{ftp} : \bot$.
4. A, B fetch the result from FTP.

Requirements

- G1 Only if both A and B know $\mathcal{I}$, then A learns that B knows $\mathcal{I}$, and likewise for B.
- G2 By means of the protocol, only A and B, and no one else, may learn that A or B know $\mathcal{I}$.
- G3 By means of the protocol, no one learns $\mathcal{I}$.
- G4 B learns that A knows $\mathcal{I}$, iff A learns that B knows $\mathcal{I}$ (which is *"fairness"*).

An example protocol

A secret comparison protocol based on [Teepe 06]

1. $A \to \Gamma : (f_{\text{prov}}, A, B, \omega)$, where $\omega = h(\mathcal{I}, \aleph, A, B)$
2. $B \to \Gamma : (f_{\text{verif}}, A, B, \Omega_B)$, where $\Omega_B = \{h(i, \aleph, A, B) \mid i \in \mathcal{E}_B\}$
3. Γ checks if $\omega \in \Omega_B$. If yes, then $\Gamma \downarrow$ FTP : ω, else $\Gamma \downarrow$ FTP : $\perp$.
4. A, B fetch the result from FTP.

Uneven risk

A severe defect of the protocol is the uneven risk distribution that it induces. If A compromises Γ, the amount of harm to B is not proportional to the harm caused to A when Γ is compromised by B.

An example protocol

A secret comparison protocol based on [Teepe 06]

1. $A \to \Gamma : (f_{prov}, A, B, \omega)$, where $\omega = h(\mathcal{I}, \aleph, A, B)$
2. $B \to \Gamma : (f_{verif}, A, B, \Omega_B)$, where $\Omega_B = \{h(i, \aleph, A, B) \mid i \in \mathcal{E}_B\}$
3. Γ checks if $\omega \in \Omega_B$. If yes, then $\Gamma \downarrow$ FTP : ω, else $\Gamma \downarrow$ FTP : $\perp$.
4. A, B fetch the result from FTP.

Uneven risk

$A \backslash B$	$\mathcal{H}_B$	$\mathcal{DH}_B$
$\mathcal{H}_A$	$(\rho-1)g, (\rho-1)g$	$-a, \rho a - c$
$\mathcal{DH}_A$	$\rho b - c, -b$	$\rho b - a - c, \rho a - b - c$

where $b = |\Omega_B| \cdot g >> g = a$ when $|\Omega_B| >> 1$. If $\rho b - c > (\rho - 1)g$ then $\mathcal{DH}_A$ is the dominating strategy of A then the difference between expected utilities is not bounded by a reasonable small number.

A Risk-balanced Protocol

Intuitive idea behind the protocol

1. $A \to B:$ $\mathtt{blind}_A(\mathcal{I})$
2. $B \to A:$ $\mathtt{sign}_B(\mathtt{blind}_A(\mathcal{I}))$
3. $A:$ $\mathtt{unblind}_A(\mathtt{sign}_B(\mathtt{blind}_A(\mathcal{I}))) = \mathtt{sign}_B(\mathcal{I})$
4. $A \to \Gamma:$ $x = \mathtt{sign}_B(\mathcal{I})$
5. $B \to \Gamma:$ $y = \{\mathtt{sign}_B(i) | i \in \mathcal{E}_B\}$
6. $\Gamma:$ Comapare x and members of y

A Risk-balanced Protocol

Intuitive idea behind the protocol

1. $A \to B$: $\mathtt{blind}_A(\mathcal{I})$
2. $B \to A$: $\mathtt{sign}_B(\mathtt{blind}_A(\mathcal{I}))$
3. A : $\mathtt{unblind}_A(\mathtt{sign}_B(\mathtt{blind}_A(\mathcal{I}))) = \mathtt{sign}_B(\mathcal{I})$
4. $A \to \Gamma$: $x = \mathtt{sign}_B(\mathcal{I})$
5. $B \to \Gamma$: $y = \{\mathtt{sign}_B(i) | i \in \mathcal{E}_B\}$
6. Γ : Comapare x and members of y

Risk-balanced

If Γ is not compromised, then the protocol satisfies G4. The amount of expected harm to a cheated B would be limited and proportional to the damage that B could cause to A if Γ was compromised by B, and vice versa. Rational A and B will end up with similar utilities.

Summary

- We study the behavior of rational agents in exchange protocols which rely on trustees.
- We allow malicious parties to compromise the trustee by paying a cost and, thereby, present a game analysis that advocates exchange protocols which induce balanced risks on the participants. If risk-balanced condition holds then, the difference between participants' utilities is limited to a factor independent of the TTP's trustworthiness.
- We also present a risk-balanced protocol for fair confidential secret comparison.

Future works

- Continue the exploration of the conceptual meaning of balancing risk.
- Study more concrete examples.
- TTP would always learn whether the exchange was successful or not. Hiding this information from TTP remains to be studied.
- A drawback of the protocol is its communication costs and the computation burden. Equivalent protocols with less, and evenly distributed, computation and communication costs are thus desirable.

Other game theoretical approaches to protocol Analysis

1. L. Buttyan and J. Hubaux. Toward a formal model of fair exchange: a game theoretic approach. Technical Report SSC/1999/39, EPFL, Lausanne, 1999.
2. L. Buttyan, J. Hubaux, and S. Capkun. A formal model of rational exchange and its application to the analysis of syverson protocol. J. Computer Security, 12(3-4):551 87, 2004.
3. J. Halpern and V. Teague. Rational secret sharing and multiparty computation: extended abstract. In Proceedings of the thirty-sixth annual ACM symposium on Theory of computing, pages 623-632. ACM Press, 2004.
4. K. Imamoto, J. Zhou, and K. Sakurai. An evenhanded certified email system for contract signing. In ICICS 05, volume 3783 of LNCS, pages 13. Springer, 2005.

Thank you for your attention!

A Risk-balanced Protocol

1. B generates n and $(\alpha, \bar{\alpha})$ and then computes $\pi = h(\omega_1, \cdots, \omega_\ell)$,
   where $\omega_j = h(i_j^{\bar{\alpha}} \bmod n)$, when $\mathcal{E}_B = \{i_1, \cdots, i_\ell\}$.
2. $B \rightarrow A : \alpha, n$
3. A generates a random number $\lambda < n$ such that $gcd(\lambda, n) = 1$.
4. $A \rightarrow B : (\mathcal{I} \cdot \lambda^{\alpha}) \bmod n$
5. $B \rightarrow A : (\mathcal{I} \cdot \lambda^{\alpha})^{\bar{\alpha}} \bmod n,\ \pi$
6. A computes $((\mathcal{I} \cdot \lambda^{\alpha})^{\bar{\alpha}} \lambda^{-1}) \bmod n = \mathcal{I}^{\bar{\alpha}} \bmod n$. Then A lets
   $\omega = h(\mathcal{I}^{\bar{\alpha}} \bmod n)$.
7. $A \rightarrow \Gamma : [f_{\text{prov}}, A, B, \omega, \pi]_{\mathcal{K}(A\Gamma)}$
8. $B \rightarrow \Gamma : [f_{\text{verif}}, A, B, \Omega_B]_{\mathcal{K}(B\Gamma)}$, where $\Omega_B = \{\omega_1, \cdots, \omega_\ell\}$
9. Γ checks whether π corresponds to Ω_B. If yes then
   Γ checks whether $\omega \in \Omega_B$. If yes, then
   $\Gamma \downarrow \text{FTP} : \omega$, and A, B fetch the result from FTP.
   else
   $\Gamma \downarrow \text{FTP} : \perp$, and A, B fetch the result from FTP.