Working Paper

Secure Implementation: An Alternative Characterization

Hideki Mizukami and Takuma Wakayama

Working Paper No. 238

October 22, 2008

FACULTY OF ECONOMICS
UNIVERSITY OF TOYAMA

3190 Gofuku, Toyama
930-8555 JAPAN

Secure Implementation: An Alternative Characterization*

HIDEKI MIZUKAMI†
Faculty of Economics, University of Toyama
mizukami@eco.u-toyama.ac.jp

and

TAKUMA WAKAYAMA
Institute of Social and Economic Research, Osaka University
wakayama@iser.osaka-u.ac.jp

October 22, 2008

*An earlier version of this paper was entitled "Full-Truthful Implementation in Nash Equilibria." We are especially grateful to an associate editor for invaluable suggestions. We are also grateful to Makoto Hanazono, Atsushi Kajii, Toyotaka Sakai, Tadashi Sekiguchi, and Yoshikatsu Tatamitani for their invaluable comments and suggestions. Finally, we would like to thank seminar participants at the 2005 Autumn Meeting of the Japanese Economic Association, Kyoto University, and the YNU Conference on Economic Theory for their comments. This research is partially supported by Grant-in-Aid for Young Scientists (B), #20730129 and #20730135.

†Corresponding author. Faculty of Economics, University of Toyama, 3190 Gofuku, Toyama 930-8555, Japan.

Abstract

We show that *restricted monotonicity*, with an auxiliary condition called *individual maximality*, is necessary and sufficient for secure implementation. This result gives us an alternative characterization of securely implementable social choice functions in terms of restricted monotonicity. We then discuss the importance of secure implementation in complete information environments in terms of Schelling (1960)'s *focal point*.

Keywords: Secure Implementation, Restricted Monotonicity, Individual Maximality, A Focal Point.

JEL Classification Numbers: C72, D71.

1 Introduction

Secure implementation, a concept that was developed by Saijo et al. (2007), is double implementation in Nash equilibria and dominant strategy equilibria. Saijo et al. (2007) showed that necessary and sufficient conditions for secure implementation are strategy-proofness and the rectangular property. In this paper, we provide alternative characterizations of securely implementable social choice functions.[1] In Theorem 1, we show that *restricted monotonicity*, a stronger version of monotonicity, and *individual maximality* form necessary and sufficient conditions for secure implementation. Moreover, in Corollary 2, we show that in some environments, restricted monotonicity alone, without individual maximality, is necessary and sufficient for secure implementation.

In the presence of restricted monotonicity, individual maximality is equivalent to strategy-proofness (although, in general, it is weaker than strategy-proofness). This fact, taken together with Theorem 1, leads to Corollary 1: Restricted monotonicity and strategy-proofness are necessary and sufficient conditions for secure implementation. This alternative characterization clarifies the fact that secure implementation is double implementation in Nash equilibria and dominant strategy equilibria. With regard to this description, we see that characterizations based on restricted monotonicity capture quite well the structure of secure implementation.

We also show in Corollary 3 a constancy result of secure implementation, which follows immediately from Corollary 2 and the result of Saijo (1987): In some environments, a social choice function satisfying dual dominance (Saijo (1987)) is securely implementable if and only if it is a constant function. In the literature, some other constancy results regarding secure implementation have been obtained. Bochet and Sakai (2007) reported the constancy result, which says that only the equal division function is symmetric and securely implementable in allotment economies with single-peaked preferences. Fujinaka and Wakayama (2008a) established that in economies with indivisible objects and money, only constant social choice functions are securely implementable under a domain-richness condition. Moreover, Fujinaka and Wakayama (2008b) showed the constancy result that the no-trade solution is the unique securely implementable social choice function that satisfies individual rationality in Shapley-Scarf housing markets.

Indeed, these results have negative implications for the existence of a non-trivial, securely implementable social choice function. If a non-trivial, securely implementable social choice function is found, however, then the secure mechanism, which securely implements the social choice function, is more likely to perform well in practice. In fact, in the experimental results of Cason et al. (2006), who compared the performances of a secure and a non-secure mecha-

[1] Mizukami and Wakayama (2005) also alternatively characterized securely implementable social choice functions in pure exchange economies in terms of a stronger version of non-bossiness.

nism, the secure mechanism performed better than the non-secure mechanism. Moreover, in complete information environments, the secure mechanism would have the advantage of preventing the miscoordination of agents in the light of Schelling (1960)'s *focal point*, which we discuss in greater detail in Section 4.

This paper is organized as follows. Section 2 gives notation and definitions. We characterize securely implementable social choice functions in terms of restricted monotonicity in Section 3. In Section 4, we discuss the significance of secure implementation in complete information environments in terms of Schelling (1960)'s *focal point*. Section 5 presents our conclusions.

2 Notation and Definitions

Let $N := \{1, 2, \ldots, n\}$ be the set of *agents*, where $2 \leq n < +\infty$. Let A be the set of feasible *outcomes*.

Each agent $i \in N$ has *preferences* over A, which are represented by a complete and transitive binary relation R_i. The strict preference and indifference relations associated with R_i are denoted by P_i and I_i, respectively. Let $\mathscr{R}_i$ denote the set of possible preferences for agent $i \in N$. The *domain* is denoted by $\mathscr{R} := \mathscr{R}_1 \times \mathscr{R}_2 \times \cdots \times \mathscr{R}_n$. A *preference profile* is a list $R = (R_1, R_2, \ldots, R_n) \in \mathscr{R}$. It is assumed that each agent can observe not only her own preferences but also those of all other agents.

An *environment* is a collection $(N, A, \mathscr{R})$.

Let $LC_i(a; R_i) := \{b \in A \mid a\ R_i\ b\}$ be agent i's *lower contour set* of $a \in A$ at $R_i \in \mathscr{R}_i$. For each $i \in N$, let $ME_i(\bar{A}; R_i) := \left\{a \in \bar{A} \,\middle|\, a\ R_i\ b \text{ for all } b \in \bar{A}\right\}$ be the set of *maximal elements* in $\bar{A} \subseteq A$ at $R_i \in \mathscr{R}_i$.[2]

A *social choice function* is a single-valued function $f\colon \mathscr{R} \to A$ that assigns a feasible outcome $a \in A$ to each preference profile $R \in \mathscr{R}$. Given a social choice function f, let $O_i(R) := \left\{a \in A \,\middle|\, a = f(R'_i, R_{-i}) \text{ for some } R'_i \in \mathscr{R}_i\right\}$ be agent i's *option set* at $R \in \mathscr{R}$. Note that $O_i(R) = O_i(R'_i, R_{-i})$ for all $R \in \mathscr{R}$, all $i \in N$, and all $R'_i \in \mathscr{R}_i$.

Let M_i denote *agent i's message space*. A *message* of agent $i \in N$ is $m_i \in M_i$. Let $M := M_1 \times M_2 \times \cdots \times M_n$ be the *message space*. A *mechanism* is a pair $\Gamma = (M, g)$, where $g\colon M \to A$ is an *outcome function*. A mechanism (M, g) is called a *direct revelation mechanism* if $M_i = \mathscr{R}_i$ for all $i \in N$.[3] Given a social choice function f, a mechanism (M, g) is called the *associated direct revelation mechanism* if $M_i = \mathscr{R}_i$ for all $i \in N$ and $g = f$. A *message profile* is denoted by $m = (m_1, m_2, \ldots, m_n) \in M$.

[2] Note that $ME_i(\bar{A}; R_i)$ may be empty.

[3] In standard fashion, a direct revelation mechanism is a mechanism where each agent reveals all that she knows. Hence, in complete information environments, the direct revelation mechanism corresponds to a mechanism in which each agent announces the preference profile. Following the terminology of Saijo et al. (2007), however, we call a direct revelation mechanism a mechanism where each agent reports only her own preferences.

A message profile $m^* = (m_1^*, m_2^*, \ldots, m_n^*) \in M$ is a *Nash equilibrium* of a mechanism (M, g) at $R \in \mathscr{R}$ if, for all $i \in N$, $g(m_i^*, m_{-i}^*)\ R_i\ g(m_i', m_{-i}^*)$ for all $m_i' \in M_i$. Let $NE^\Gamma(R) \subseteq M$ denote the set of Nash equilibria of a mechanism $\Gamma = (M, g)$ at $R \in \mathscr{R}$. A message profile $m^* = (m_1^*, m_2^*, \ldots, m_n^*) \in M$ is a *dominant strategy equilibrium* of a mechanism (M, g) at $R \in \mathscr{R}$ if, for all $i \in N$, $g(m_i^*, m_{-i}')\ R_i\ g(m_i', m_{-i}')$ for all $m_i' \in M_i$ and all $m_{-i}' \in M_{-i}$. Let $DSE^\Gamma(R) \subseteq M$ be the set of dominant strategy equilibria of a mechanism $\Gamma = (M, g)$ at $R \in \mathscr{R}$.

Let $\mathscr{E}$*-equilibrium* be a game theoretic equilibrium concept. Let $g(\mathscr{E}^\Gamma(R)) := \{a \in A \mid a = g(m) \text{ for some } m \in \mathscr{E}^\Gamma(R)\}$ denote the set of $\mathscr{E}$*-equilibrium outcomes* of a mechanism $\Gamma = (M, g)$ at $R \in \mathscr{R}$, where $\mathscr{E}^\Gamma(R) \subseteq M$ denotes the set of $\mathscr{E}$-equilibria of the mechanism at R. A direct revelation mechanism $\Gamma = (\mathscr{R}, g)$ *truthfully implements* a social choice function f *in* $\mathscr{E}$*-equilibria* if $R \in \mathscr{E}^\Gamma(R)$ and $g(R) = f(R)$ for any $R \in \mathscr{R}$.[4] A mechanism $\Gamma = (M, g)$ *securely implements* a social choice function f if $g(NE^\Gamma(R)) = g(DSE^\Gamma(R)) = f(R)$ for any $R \in \mathscr{R}$.[5] A social choice function is *securely implementable* if there exists a mechanism that securely implements it.

Next, we introduce some properties of social choice functions. *Restricted monotonicity* is a version of *monotonicity*[6] (Maskin (1999)) that requires the following. Suppose there is a change from $R \in \mathscr{R}$ to $R' \in \mathscr{R}$. Then, for each agent $i \in N$, if any outcome that was weakly worse for her than $f(R)$ *in her option set* at R when her preferences were R_i remains weakly worse for her than $f(R)$ when her preferences are R_i', then $f(R)$ must still be f-optimal at R'.

Definition 1 (Restricted Monotonicity). A social choice function f satisfies *restricted monotonicity* if, for all $R, R' \in \mathscr{R}$, if $LC_i(f(R); R_i) \cap O_i(R) \subseteq LC_i(f(R); R_i')$ for all $i \in N$, then $f(R') = f(R)$.

Remark 1. Restricted monotonicity is stronger than monotonicity, by definition.

Definition 2 (Individual Maximality). A social choice function f satisfies *individual maximality* if, for all $R \in \mathscr{R}$, $ME_i(O_i(R); R_i) \neq \emptyset$ for all $i \in N$.

Remark 2. Individual maximality is weaker than strategy-proofness, by definition.

Definition 3 (Strategy-Proofness). A social choice function f satisfies *strategy-proofness* if $f(R) \in ME_i(O_i(R); R_i)$ for all $R \in \mathscr{R}$ and all $i \in N$.

Remark 3. Consider the associated direct revelation mechanism $\Gamma = (\mathscr{R}, f)$ for a given social choice function f. Then, f satisfies strategy-proofness if and only if $R \in DSE^\Gamma(R)$ for all $R \in \mathscr{R}$.

[4] Since we are focusing on social choice functions, truthful $\mathscr{E}$-implementation can be defined as $R \in \mathscr{E}^\Gamma(R)$ and $g(R) = f(R)$ for any $R \in \mathscr{R}$, instead of as $R \in \mathscr{E}^\Gamma(R)$ and $g(R) \in f(R)$ for any $R \in \mathscr{R}$.

[5] To simplify the notation, we write $f(R)$ instead of $\{f(R)\}$.

[6] A social choice function f satisfies *monotonicity* if, for all $R, R' \in \mathscr{R}$, if $LC_i(f(R); R_i) \subseteq LC_i(f(R); R_i')$ for all $i \in N$, then $f(R') = f(R)$.

3 Characterizations

This section provides alternative characterizations of securely implementable social choice functions in terms of restricted monotonicity. Theorem 1 below establishes that restricted monotonicity and an auxiliary condition, individual maximality, together form necessary and sufficient conditions for secure implementation. It should be noted that Theorem 1 holds even when $n = 2$.

Theorem 1. *A social choice function f is securely implementable if and only if it satisfies restricted monotonicity and individual maximality.*

Proposition 1 (Dasgupta et al. (1979)) is used in the proof of Theorem 1.

Proposition 1 (Dasgupta et al. (1979)). *A social choice function is truthfully implemented in Nash equilibria by a direct revelation mechanism if and only if it is truthfully implemented in dominant strategy equilibria by the same direct revelation mechanism.*

Proof of Theorem 1. Let $\Gamma = (\mathscr{R}, f)$ denote the associated direct revelation mechanism.

The if part. Step 1: f satisfies strategy-proofness.

Suppose to the contrary that $f(R) \notin ME_i(O_i(R); R_i)$ for some $R \in \mathscr{R}$ and some $i \in N$. Let $b \in A$ be such that $b \in ME_i(O_i(R); R_i)$.[7] Then, $b \neq f(R)$. Since $b \in O_i(R)$, $b = f(\bar{R}_i, R_{-i})$ for some $\bar{R}_i \in \mathscr{R}_i$.

Since $f(\bar{R}_i, R_{-i}) = b \in ME_i(O_i(R); R_i)$, we have $LC_i(f(\bar{R}_i, R_{-i}); R_i) \cap O_i(R) = O_i(R)$. Since $LC_i(f(\bar{R}_i, R_{-i}); \bar{R}_i) \cap O_i(R) \subseteq O_i(R)$ and $LC_i(f(\bar{R}_i, R_{-i}); R_i) \cap O_i(R) = O_i(R)$, we obtain $LC_i(f(\bar{R}_i, R_{-i}); \bar{R}_i) \cap O_i(R) \subseteq O_i(R) = LC_i(f(\bar{R}_i, R_{-i}); R_i) \cap O_i(R)$. Hence, it follows from $O_i(R) = O_i(\bar{R}_i, R_{-i})$ that $LC_i(f(\bar{R}_i, R_{-i}); \bar{R}_i) \cap O_i(\bar{R}_i, R_{-i}) \subseteq LC_i(f(\bar{R}_i, R_{-i}); R_i) \cap O_i(\bar{R}_i, R_{-i})$. Thus, we have $LC_i(f(\bar{R}_i, R_{-i}); \bar{R}_i) \cap O_i(\bar{R}_i, R_{-i}) \subseteq LC_i(f(\bar{R}_i, R_{-i}); R_i) \cap O_i(\bar{R}_i, R_{-i}) \subseteq LC_i(f(\bar{R}_i, R_{-i}); R_i)$. So, since $LC_j(f(\bar{R}_i, R_{-i}); R_j) \cap O_j(\bar{R}_i, R_{-i}) \subseteq LC_j(f(\bar{R}_i, R_{-i}); R_j)$ for all $j \neq i$, restricted monotonicity implies $f(R) = f(\bar{R}_i, R_{-i})$, which contradicts $f(R) \neq b = f(\bar{R}_i, R_{-i})$.

Step 2: $R \in NE^{\Gamma}(R)$ and $f(NE^{\Gamma}(R)) = f(R)$ for all $R \in \mathscr{R}$.

Pick any $R \in \mathscr{R}$. Since f satisfies strategy-proofness by Step 1, it follows from Remark 3 that $R \in DSE^{\Gamma}(R)$. So, $R \in NE^{\Gamma}(R)$.

Suppose $\bar{R} \in NE^{\Gamma}(R)$. Then, for any $i \in N$, $f(\bar{R})\ R_i\ f(R'_i, \bar{R}_{-i})$ for any $R'_i \in \mathscr{R}_i$. This implies $f(\bar{R}) \in ME_i(O_i(\bar{R}); R_i)$ for all $i \in N$, implying $LC_i(f(\bar{R}); R_i) \cap O_i(\bar{R}) = O_i(\bar{R})$ for all $i \in N$. Since $LC_i(f(\bar{R}); \bar{R}_i) \cap O_i(\bar{R}) \subseteq O_i(\bar{R})$ and $LC_i(f(\bar{R}); R_i) \cap O_i(\bar{R}) = O_i(\bar{R})$ for all $i \in N$, we have $LC_i(f(\bar{R}); \bar{R}_i) \cap O_i(\bar{R}) \subseteq O_i(\bar{R}) = LC_i(f(\bar{R}); R_i) \cap O_i(\bar{R})$ for all $i \in N$. This implies $LC_i(f(\bar{R}); \bar{R}_i) \cap O_i(\bar{R}) \subseteq LC_i(f(\bar{R}); R_i) \cap O_i(\bar{R}) \subseteq LC_i(f(\bar{R}); R_i)$ for all $i \in N$. Therefore, restricted monotonicity implies $f(R) = f(\bar{R})$. So, $f(R) = f(\bar{R})$ for any $\bar{R} \in NE^{\Gamma}(R)$. This implies $f(NE^{\Gamma}(R)) = f(R)$. Thus, $f(NE^{\Gamma}(R)) = f(R)$ for all $R \in \mathscr{R}$.

[7] It should be noted that $ME_i(O_i(R); R_i) \neq \emptyset$ by individual maximality.

Step 3: f is securely implementable.

By Step 2, $R \in NE^{\Gamma}(R)$ and $f(NE^{\Gamma}(R)) = f(R)$ for all $R \in \mathscr{R}$. This implies that f is truthfully Nash implemented by Γ. So, by Proposition 1, f is truthfully dominant strategy implemented by Γ: $R \in DSE^{\Gamma}(R)$ for all $R \in \mathscr{R}$. This implies $R \in DSE^{\Gamma}(R) \subseteq NE^{\Gamma}(R)$ for all $R \in \mathscr{R}$. Hence, $f(R) \in f(DSE^{\Gamma}(R)) \subseteq f(NE^{\Gamma}(R))$ for all $R \in \mathscr{R}$. Thus, $f(DSE^{\Gamma}(R)) = f(NE^{\Gamma}(R)) = f(R)$ for all $R \in \mathscr{R}$, because $f(NE^{\Gamma}(R)) = f(R)$ for all $R \in \mathscr{R}$.

The only if part. Since f is securely implementable, it is also dominant strategy implementable. So, f satisfies strategy-proofness by the revelation principle for dominant strategy implementation. Hence, it follows from Remark 2 that f satisfies individual maximality. In the remainder of the proof of the only if part, we show that f satisfies restricted monotonicity.

Step 1: $R \in NE^{\Gamma}(R)$ and $f(NE^{\Gamma}(R)) = f(R)$ for all $R \in \mathscr{R}$.

Since f is securely implementable, the revelation principle for secure implementation (Saijo et al. (2007)) implies that it is securely implemented by Γ. So, $f(NE^{\Gamma}(R)) = f(DSE^{\Gamma}(R)) = f(R)$ for all $R \in \mathscr{R}$. Moreover, the revelation principle for dominant strategy implementation implies that f satisfies strategy-proofness. So, it follows from Remark 3 that $R \in DSE^{\Gamma}(R)$ for all $R \in \mathscr{R}$, which implies $R \in DSE^{\Gamma}(R) \subseteq NE^{\Gamma}(R)$ for all $R \in \mathscr{R}$.

Step 2: f satisfies restricted monotonicity.

Pick any $R, \bar{R} \in \mathscr{R}$ such that $LC_i(f(R); R_i) \cap O_i(R) \subseteq LC_i(f(R); \bar{R}_i)$ for all $i \in N$. Then, $R \in NE^{\Gamma}(R)$ by Step 1. Since $R \in NE^{\Gamma}(R)$, it follows that for all $i \in N$, $f(R)\ R_i\ f(R'_i, R_{-i})$ for all $R'_i \in \mathscr{R}_i$. This implies $f(R) \in ME_i(O_i(R); R_i)$ for all $i \in N$. So, $LC_i(f(R); R_i) \cap O_i(R) = O_i(R)$ for all $i \in N$.

Since $LC_i(f(R); R_i) \cap O_i(R) = O_i(R)$ and $LC_i(f(R); R_i) \cap O_i(R) \subseteq LC_i(f(R); \bar{R}_i)$ for all $i \in N$, we have $O_i(R) \subseteq LC_i(f(R); \bar{R}_i)$ for all $i \in N$. So, for all $i \in N$, $f(R)\ \bar{R}_i\ f(R'_i, R_{-i})$ for all $R'_i \in \mathscr{R}_i$, implying $R \in NE^{\Gamma}(\bar{R})$. Hence, $f(R) \in f(NE^{\Gamma}(\bar{R}))$, whereas $f(NE^{\Gamma}(\bar{R})) = f(\bar{R})$ by Step 1. Thus, $f(R) \in f(NE^{\Gamma}(\bar{R})) = f(\bar{R})$. This implies $f(\bar{R}) = f(R)$, because f is a single-valued function. □

Remark 4. The revelation principle for secure implementation tells us that secure implementation is equivalent to double implementation in Nash equilibria and dominant strategy equilibria by the associated direct revelation mechanism. Hence, secure implementability implicitly requires *Nash implementability by the associated direct revelation mechanism*. When considering implementation by the associated direct revelation mechanism, satisfying individual maximality is equivalent to the mechanism possessing the *best response property*[8] (Jackson et al. (1994)), which would be an appropriate restriction on mechanisms in order for the Nash equilibrium concept to make sense, as pointed out by Jackson et al. (1994). Theorem 1 indicates that secure implementation by the associated

[8]A mechanism (M, g) satisfies the *best response property* if, for all $R \in \mathscr{R}$, all $i \in N$, and all $m_{-i} \in M_{-i}$, there exists $m_i \in M_i$ such that $g(m_i, m_{-i})\ R_i\ g(m'_i, m_{-i})$ for all $m'_i \in M_i$.

direct revelation mechanism is impossible as long as the mechanism violates the best response property.

As shown in the proof of Theorem 1, individual maximality, together with restricted monotonicity, implies strategy-proofness. It then follows from Remark 2 that individual maximality and strategy-proofness are equivalent in the presence of restricted monotonicity. Thus, Theorem 1 leads to the following corollary.

Corollary 1. *A social choice function is securely implementable if and only if it satisfies restricted monotonicity and strategy-proofness.*

Theorem 1 and Corollary 1 provide alternative characterizations of securely implementable social choice functions. In contrast to the characterization by Saijo et al. (2007), our characterizations have the advantage of using a version of monotonicity, which is a well-known property in implementation theory. In fact, Corollary 1 makes evident the fact that secure implementation is double implementation in Nash equilibria and dominant strategy equilibria.

Furthermore, in certain environments, individual maximality is redundant in the characterization of securely implementable social choice functions. The following is due to Dasgupta et al. (1979).

Proposition 2 (Dasgupta et al. (1979)). *Suppose that $\mathscr{R}$ is rich.*[9] *Then, if a social choice function satisfies monotonicity, it also satisfies strategy-proofness.*

Proposition 2, together with Remark 1, implies that restricted monotonicity implies strategy-proofness if $\mathscr{R}$ is rich. Then, by Remark 2, restricted monotonicity implies individual maximality if $\mathscr{R}$ is rich. In addition, if A is finite, then individual maximality is automatically satisfied by the completeness and transitivity of preferences, regardless of whether or not $\mathscr{R}$ is rich. Thus, we have the following corollary.

Corollary 2. *Suppose that either (i) A is finite or (ii) $\mathscr{R}$ is rich. Then, a social choice function is securely implementable if and only if it satisfies restricted monotonicity.*

We end this section by providing a corollary which follows directly from Corollary 2 and Proposition 3 (Saijo (1987)) below.

Proposition 3 (Saijo (1987)). *A social choice function satisfying dual dominance*[10] *is monotonic if and only if it is constant.*

[9] Given $a, b \in A$, *b improves with respect to a for $i \in N$ as the preference profile changes from R to R'* if (i) $a\, P_i\, b$ and $b\, R'_i\, a$ or (ii) $a\, R_i\, b$ and $b\, P'_i\, a$. A domain $\mathscr{R}$ is *rich* (Maskin and Sjöström (2002)) if, for all $a, b \in A$ and all $R, R' \in \mathscr{R}$, if, for all $i \in N$, b does not improve with respect to a for when the preference profile changes from R to R', then there exists $R'' \in \mathscr{R}$ such that $LC_i(a; R_i) \subseteq LC_i(a; R''_i)$ and $LC_i(b; R'_i) \subseteq LC_i(b; R''_i)$ for all $i \in N$.

[10] A social choice function f satisfies *dual dominance* if, for all $a, a' \in f(\mathscr{R})$, there exist $R, R', R'' \in \mathscr{R}$ with $f(R) = a$ and $f(R') = a'$ such that $LC_i(a; R_i) \subseteq LC_i(a; R''_i)$ and $LC_i(a'; R'_i) \subseteq LC_i(a'; R''_i)$ for all $i \in N$, where $f(\mathscr{R}) := \{a \in A \mid a = f(R) \text{ for some } R \in \mathscr{R}\}$.

Corollary 3. *Suppose that either (i) A is finite or (ii) $\mathscr{R}$ is rich. Then, a social choice function satisfying dual dominance is securely implementable if and only if it is constant.*

4 Discussions

This section provides another interpretation of secure implementation and discusses the importance of secure implementation in complete information environments in terms of Schelling (1960)'s *focal point*.

The revelation principle for secure implementation says that secure implementation is equivalent to double implementation in Nash equilibria and dominant strategy equilibria by the associated direct revelation mechanism. The revelation principle for dominant strategy implementation tells us that truthful reporting by each agent is a dominant strategy equilibrium in the associated direct revelation mechanism. Moreover, by Proposition 1 (Dasgupta et al. (1979)), if truth-telling by each agent is a dominant strategy equilibrium of the associated direct revelation mechanism, then it is also a Nash equilibrium of the mechanism. Taken together, these lead to the following interpretation of secure implementation: Secure implementation is Nash implementation by the associated direct revelation mechanism, where truth-telling by each agent is required to be a Nash equilibrium of the mechanism.[11]

In complete information environments, the requirement that truthful revelation by each agent be a Nash equilibrium of the associated direct revelation mechanism would be appealing from a practical standpoint. Suppose that there is an associated direct revelation mechanism that implements a social choice function but violates the requirement, and suppose that it has multiple equilibria. In such a mechanism, it would be hard for agents to predict one another's actions, which could lead to miscoordination. Since, in complete information environments, each agent knows with certainty every other agent's true preferences, and since all Nash equilibrium outcomes are the same by full implementability, if truthful reporting by each agent is a Nash equilibrium of the mechanism, then the *truthful* Nash equilibrium would be salient and could

[11] Since the seminal paper by Maskin (1999), many papers have sought to fully characterize the class of Nash implementable social choice correspondences. However, the full characterizations rely on complicated mechanisms with *large* message spaces used in the constructive proofs. Aside from the papers, Saijo (1988) showed that Nash implementation can be achieved by a mechanism with a *smaller* message space, by paying attention to informational decentralization and efficiency of mechanisms (e.g., see Hurwicz (1960, 1972) and Williams (1986, 2001) for the significance of informational decentralization and efficiency in mechanism design and implementation theory). Tatamitani (2001) subsequently focused attention on informational decentralization and considered Nash implementation by a self-relevant mechanism. From the viewpoint of the literature on Nash implementation, Nash implementation by the associated direct revelation mechanism, which is the *simplest* informationally decentralized mechanism, with the additional restriction that truthful reporting by each agent must be a Nash equilibrium of the mechanism is thought of as secure implementation.

serve as a *focal point* (Schelling (1960)),[12] and agents would thereby be able to coordinate their actions.

While it is true that the requirement of the existence of the truthful Nash equilibrium in the associated direct revelation mechanism drastically narrows the class of implementable social choice functions, it can be justified by the salience property of such an equilibrium. In order to make practical use of a theoretically constructed mechanism, it is important to pay attention to the possibility that agents fail to coordinate their actions, which is very likely if the mechanism possesses multiple equilibria, as mentioned above and demonstrated in coordination game experiments (e.g., see Camerer (2003)). In a mechanism with a focal point equilibrium, on the other hand, agents would be able to coordinate their actions even if there exist multiple equilibria. Thus, in complete information environments, secure implementation can be conceived as implementation by a mechanism designed for the purpose of preventing miscoordination.

5 Conclusion

In this paper, we have shown that restricted monotonicity and individual maximality (or strategy-proofness) form both necessary and sufficient conditions for secure implementation. We have also shown that in certain environments, restricted monotonicity alone is necessary and sufficient for secure implementation. Our characterizations of secure implementation, which are based on a stronger version of monotonicity, seem to capture quite well the structure of secure implementation, i.e., double implementation in Nash equilibria and dominant strategy equilibria. Moreover, we have discussed the practical appeal of secure implementation in complete information environments in terms of Schelling (1960)'s focal point. Since the secure mechanism has important practical advantages over non-secure ones, an important direction for further research is to search for non-trivial, securely implementable social choice functions in various environments.

[12]When considering truthful Nash implementation as opposed to secure implementation, the truthful Nash equilibrium of the associated direct revelation mechanism could not be salient; hence, it could not be a focal point. The reason for this is that, when secure implementation is impossible, the mechanism often has an *untruthful* Nash equilibrium whose outcome is not the same as that of the truthful Nash equilibrium. Recall that the truthful Nash equilibrium becomes salient only because all Nash equilibrium outcomes are the same by full implementability. In fact, the truthful Nash equilibrium would not be highlighted if the associated direct revelation mechanism has an untruthful Nash equilibrium outcome that Pareto dominates the truthful Nash equilibrium outcome. See also Moore and Repullo (1988) for a similar discussion.

References

BOCHET, O. AND T. SAKAI (2007): "Secure Implementation in Allotment Economies," mimeo., Maastricht University and Yokohama National University.

CAMERER, C. F. (2003): *Behavioral Game Theory: Experiments in Strategic Interaction*, Princeton University Press.

CASON, T. N., T. SAIJO, T. SJÖSTRÖM, AND T. YAMATO (2006): "Secure Implementation Experiments: Do Strategy-Proof Mechanisms Really Work?" *Games and Economic Behavior*, 57, 206–235.

DASGUPTA, P., P. J. HAMMOND, AND E. MASKIN (1979): "The Implementation of Social Choice Rules: Some General Results on Incentive Compatibility," *Review of Economic Studies*, 46, 185–216.

FUJINAKA, Y. AND T. WAKAYAMA (2008a): "Secure Implementation in Economies with Indivisible Objects and Money," *Economics Letters*, 100, 91–95.

——— (2008b): "Secure Implementation in Shapley–Scarf Housing Markets," mimeo., Osaka University.

HURWICZ, L. (1960): "Optimality and Informational Efficiency in Resource Allocation Processes," in *Mathematical Methods in the Social Sciences*, ed. by K. J. Arrow, S. Karlin, and P. Suppes, Stanford University Press, 27–46.

——— (1972): "On Informationally Decentralized Systems," in *Decision and Organization*, ed. by R. Radner and C. B. McGuire, North-Holland, 297–336.

JACKSON, M. O., T. R. PALFREY, AND S. SRIVASTAVA (1994): "Undominated Nash Implementation in Bounded Mechanisms," *Games and Economic Behavior*, 6, 474–501.

MASKIN, E. (1999): "Nash Equilibrium and Welfare Optimality," *Review of Economic Studies*, 66, 23–38.

MASKIN, E. AND T. SJÖSTRÖM (2002): "Implementation Theory," in *Handbook of Social Choice and Welfare*, ed. by K. J. Arrow, A. K. Sen, and K. Suzumura, North-Holland, vol. 1, 237–288.

MIZUKAMI, H. AND T. WAKAYAMA (2005): "Bossiness and Implementability in Pure Exchange Economies," in *RIMS Kokyuroku*, vol. 1461 of *Mathematics of Optimization: Methods and Practical Solutions*, 126–140.

MOORE, J. AND R. REPULLO (1988): "Subgame Perfect Implementation," *Econometrica*, 56, 1191–1220.

SAIJO, T. (1987): “On Constant Maskin Monotonic Social Choice Functions,” *Journal of Economic Theory*, 42, 382–386.

——— (1988): “Strategy Space Reduction in Maskin’s Theorem: Sufficient Conditions for Nash Implementation,” *Econometrica*, 56, 693–700.

SAIJO, T., T. SJÖSTRÖM, AND T. YAMATO (2007): “Secure Implementation,” *Theoretical Economics*, 2, 203–229.

SCHELLING, T. C. (1960): *The Strategy of Conflict*, Harvard University Press.

TATAMITANI, Y. (2001): “Implementation by Self-Relevant Mechanisms,” *Journal of Mathematical Economics*, 35, 427–444.

WILLIAMS, S. R. (1986): “Realization and Nash Implementation: Two Aspects of Mechanism Design,” *Econometrica*, 54, 139–151.

——— (2001): “Sufficient Conditions for Nash Implementation,” *Review of Economic Design*, 6, 325–342.