فرهنگ و اندیشهٔ ریاضی
سال ۳۸، شمارهٔ ۶۴ (بهار و تابستان ۱۳۹۸)، صص. ۱۴۳ تا ۱۵۷

کاربرد رمزنگاری در نظریهٔ بازی‌ها

مونا باباخانی و رضا ندیمی

چکیده

نظریهٔ بازی‌ها نقشی مهم در مدل‌سازی و حل مسائل دستگاه‌های چندعاملی مانند ارتباطات در شبکه‌های رایانه‌ای دارد و بررسی الگوریتم‌ها و پیچیدگیِ محاسباتیِ مسائل موجود در نظریهٔ بازی‌ها، به زمینهٔ پژوهشی پویایی در علوم رایانه تبدیل شده است. در نظریهٔ بازی‌ها از تعادل‌ها به‌مثابهٔ راه‌حلی برای دست‌یابی به پاسخ مسائل استفاده می‌شود. یکی از این تعادل‌ها که به تعادل همبسته معروف است، با استفاده از یک میانجی مورد اعتماد تعریف می‌شود. پژوهشگران حوزهٔ نظریهٔ بازی‌ها و رمزنگاری سعی در حذف میانجی با استفاده از پروتکل‌های رمزنگاری دارند. در این مقاله، به بررسی کاربرد جالب توجه رمزنگاری در حذف نقش میانجی از تعادل همبسته و مروری بر فعالیت‌های انجام شده در این باره می‌پردازیم.

۱. مقدمه

دانش نظریهٔ بازی‌ها[۱] و دانش طراحی پروتکل‌های رمزنگاری[۲] به مطالعهٔ تعامل بین عوامل بی‌اعتماد به یکدیگر می‌پردازند [۸]. در تعاملات چندعاملیِ رمزنگاری، مجموعه‌ای از عوامل با هدف ارزیابی یک تابع بر ورودی‌های خود و سرانجام، دریافت نتیجه‌ای از این محاسبات با یکدیگر در پیوند هستند و در نظریهٔ بازی‌ها، بازیکنان در بازی‌ای که برای همهٔ آنها عایدی‌هایی را برای مشارکت در بازی تضمین می‌کند، تعامل دارند و به فکر بیشینه کردن مقدار عایدی خود هستند. در سال‌های گذشته، پژوهش‌هایی در زمینهٔ فصل مشترک این دو دانشِ رو به گسترش انجام شده و پیوند این دو حوزه به امید یافتن راه‌حل‌ها و پروتکل‌های کارآمد، مورد مطالعه قرار گرفته است. این فصل مشترک دارای دو بخش کلی کاربرد

عبارات و کلمات کلیدی. نظریهٔ بازی‌ها؛ رمزنگاری؛ تعادل همبسته؛ میانجی.

[۱] game theory [۲] cryptography

پروتکل‌های رمزنگاری در حل مسائل موجود در نظریهٔ بازی‌ها، و کاربرد مدل‌ها و مفاهیم نظریهٔ بازی‌ها در طراحی پروتکل‌های رمزنگاری است. استفاده از پروتکل‌های رمزنگاری برای دست‌یابی به تعادل همبسته در بازی، نمونه‌ای از کاربرد رمزنگاری در نظریهٔ بازی‌ها است که مطالعات بر روی آن آغاز شده و رو به گسترش است. در ادامه به شیوهٔ استفاده از پروتکل‌های رمزنگاری برای دست‌یابی به تعادل همبستهٔ دلخواه در بازی‌ها می‌پردازیم و راه‌هایی برای دست‌یابی به تعادل‌های بهتر را نیز بیان می‌کنیم.

۲. نظریهٔ بازی‌ها و تعادل نش

نظریهٔ بازی‌ها به مطالعهٔ مدل‌های ریاضیِ تعارض و همکاری بین تصمیم‌گیرندگان عاقل می‌پردازد. ویژگی اصلیِ تصمیم‌گیری در شرایط بازی این است که هر بازیکن قبل از تصمیم‌گیری و انتخاب، باید واکنش دیگران را نسبت به انتخاب و تصمیم خود مورد تجزیه و تحلیل قرار دهد و آن‌گاه تصمیمی را اتخاذ کند که برای او بهترین است [۲]. اگر چند عامل در تعامل با یکدیگر باشند و سود و زیان هر عامل، به تصمیمات دیگر عامل‌ها وابسته باشد، جمعِ مورد نظر، یک بازی را شکل داده‌اند. هر بازی شامل چهار مؤلفهٔ مهم است: بازیکنان بازی، اطلاعات[۱]، حرکت[۲]های ممکن برای هر بازیکن در هر نقطه از بازی و عایدیِ حاصل از عملکرد. هر بازی، دو یا بیش از دو بازیکن دارد. در نظریهٔ بازی‌ها بازیکنان، عاقل[۳] و خودمحور[۴] هستند [۱۱]. عاقل به این معنی که تصمیمات آنها عقلانی است و در راستای بیشینه کردن عایدی است. عقلانیت، جزئی از دانش عمومی بازی است؛ به این معنی که هر بازیکن نه‌تنها عاقل است، بلکه می‌داند که بازیکنان دیگر نیز عاقل هستند و با استفاده از این آگاهی، تصمیم‌گیری می‌کند. خودمحور بودنِ بازیکن به این معنی است که او فقط به فکر بیشینه کردن عایدی خویش است.

الگوریتمی که هر بازیکن بر اساس آن حرکت خود را انتخاب می‌کند، *راهبرد*[۵] نامیده می‌شود [۲]. به عبارت دیگر، راهبرد، مهارتِ خوب بازی کردنِ هر بازیکن است. به هر nتایی از راهبردها، *نمایهٔ راهبرد*[۶] می‌گوییم. در نظریهٔ بازی‌ها دو نوع راهبرد وجود دارد. یکی *راهبرد محض*[۷] که همهٔ حرکات شما را در طول بازی تعیین می‌کند و دیگری، *راهبرد آمیخته*[۸] که تخصیص احتمال برای راهبردهای محض است و انتخاب تصادفیِ یکی از راهبردهای محض را ممکن می‌کند. نمایهٔ راهبرد s را در نظر بگیرید. s_i راهبرد بازیکن i و s_{-i} راهبردهای $n-1$ بازیکن دیگر بدون در نظر گرفتن راهبرد بازیکن i است و مجموعهٔ S_i همهٔ راهبردهای ممکن بازیکن i و مجموعهٔ S شامل همهٔ نمایه‌های راهبردهای ممکن بازی است.

در نظریهٔ بازی‌ها تعادل‌ها، راهی برای دست‌یابی به پاسخ هستند. در ادامه تعریفی از دو تعادل مهم در نظریهٔ بازی‌ها بیان شده است.

---

[۱] information [۲] action [۳] rational [۴] selfish [۵] strategy [۶] strategy profile [۷] pure strategy [۸] mixed strategy

تعریف ۱.۲ (تعادل نش[۱]). نمایهٔ راهبرد $s^* = (s_1^*, \ldots, s_n^*) \in S$ را یک تعادل نش (محض یا آمیخته) گوییم اگر

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*) \qquad \forall s_i \in S_i, \forall i \in \mathbb{N}. \tag{۱.۲}$$

این نمایهٔ راهبرد را بازیکنانِ مستقل از هم انتخاب می‌کنند. با فرض اینکه بازیکنانِ دیگر از نمایهٔ راهبرد s^* پیروی می‌کنند، بازیکن i با تغییر راهبرد خود نمی‌تواند عایدی خود را بهبود دهد. روشن است که هر وضعیت غالب، یک تعادل نش است. تعادل نش ممکن است منحصر به‌فرد نباشد. در بازی‌هایی با چندین تعادل نش، هر تعادل می‌تواند دارای عایدی متفاوت برای هر بازیکن باشد.

بازی ترسوها[۲] را در نظر بگیرید. در این بازی دو راننده طی یک درگیریِ خیابانی، تصمیم می‌گیرند تا از دو جهت مخالف با سرعت زیاد به سمت یکدیگر حرکت کنند. این بازی، دو نفره و متقارن است. در جدول ۱ ماتریس اطلاعات بازی نمایش داده شده است [۸]. همان‌طور که در ماتریس ملاحظه می‌کنید،

جدول ۱. ماتریس اطلاعات بازی ترسوها

بازیکن۲/بازیکن۱	توقف	حرکت
توقف	(۴٬۴)	(۱٬۵)
حرکت	(۵٬۱)	(۰٬۰)

هر دو بازیکن دارای دو وضعیت توقف و حرکت هستند. حرکت، انتخاب رانندهٔ شجاع خواهد بود که به مسیر خود ادامه می‌دهد و توقف، انتخاب رانندهٔ ترسو خواهد بود که از ادامهٔ حرکت در مسیر مستقیم منصرف می‌شود. به این دلیل، این بازی را *بازی ترسوها* می‌نامند. اگر هر دو بازیکن حرکت را انتخاب کنند، سرانجام یک تصادف ناگوار خواهند داشت! پس تصادف با عایدی‌های صفر برای هر دو بازیکن، بدترین وضعیت در بازی است. از سوی دیگر، اگر هر دو توقف را انتخاب کنند، عایدیِ هر دو چهار خواهد بود؛ وضعیتی با عایدی عادلانه اما ناپایدار چون هر بازیکن با فرض اینکه دیگری از این راهبرد پیروی می‌کند، با تغییر راهبرد خود می‌تواند عایدی پنج را داشته باشد. ولی دو نمایهٔ راهبرد که در آنها دو راننده انتخاب‌های متفاوت دارند، پایدار هستند؛ به این معنی که اگر بازیکنی فرض کند که بازیکن مقابل از این راهبرد پیروی می‌کند، او نیز پیروی از این راهبرد را ترجیح می‌دهد ولی این دو وضعیت دارای عایدی ناعادلانه هستند. پس این بازی دارای دو تعادل نش محض (توقف, حرکت) $= S_1$ و (حرکت, توقف) $= S_2$ است. این دو تعادل، دارای عایدیِ ناعادلانه برای دو بازیکن هستند به‌گونه‌ای که هر بازیکن، یکی از این دو تعادل را به‌منظورِ عایدی بیشتر ترجیح می‌دهد. این بازی دارای تعادل نش آمیخته‌ای با عایدی مورد انتظار $u(S_3) = (\frac{5}{4}, \frac{5}{4})$ است که در آن، بازیکنان هریک با احتمال $\frac{1}{4}$ توقف

[۱] Nash equilibrium [۲] chicken game

و با احتمال $\frac{۱}{۴}$ حرکت را انتخاب می‌کند. عایدی مورد انتظار این تعادل برابر است با:

$$u_i(S_۳) = \frac{۱}{۲} \times \frac{۱}{۲} \times ۴ + \frac{۱}{۲} \times \frac{۱}{۲} \times ۱ + \frac{۱}{۲} \times \frac{۱}{۲} \times ۵ + \frac{۱}{۲} \times \frac{۱}{۲} \times ۰ = \frac{۵}{۲}, \qquad i = ۱, ۲.$$

قضیه ۲.۲ ([۶]، ۱۹۵۰). *هر بازی راهبردیِ nنفرهٔ محدود دارای یک تعادل نش آمیخته است.*

تاکنون هیچ الگوریتم چندجمله‌ای برای پیدا کردن تعادل نش در بازی‌های عمومی ارائه نشده است.

۳. تعادل همبسته

رابرت اومان[۱] در سال ۱۹۵۹ با معرفی بازی ترسوها، مفهوم *تعادل همبسته*[۲] را ارائه و بیان کرد که بازیکنان با انتخابِ همبستهٔ راهبردهای خود، می‌توانند به نتایج بهتر دست یابند [۳]. تعادل همبسته، بیان توزیع احتمال مناسب بر روی همهٔ نمایه‌های راهبرد است؛ مانند احتمال‌های آمده در جدول ۲ برای بازی ترسوها. به بازی متقارن ترسوها در جدول ۱ دقت کنید. با توجه به ماتریس اطلاعات بازی، تعادل‌های

جدول ۲. نمایش احتمال‌ها در بازی ترسوها

بازیکن۲/بازیکن۱	توقف	حرکت
توقف	$P_{۱۱}$	$P_{۱۲}$
حرکت	$P_{۲۱}$	$P_{۲۲}$

نش بازی دارای توزیع احتمال‌های جدول ۳ بر روی نمایه‌های راهبرد هستند. در دو تعادل نش محض

جدول ۳. نمایش توزیع احتمال‌های سه تعادل نش بازی ترسوها

بازیکن۲/بازیکن۱	توقف	حرکت			
توقف	۰	۱	۰	۰	$\frac{۱}{۴}$
حرکت	۰	۰	۱	۰	$\frac{۱}{۴}$
	$S_۱$		$S_۲$		$S_۳$

$S_۱$ و $S_۲$، چنان‌که از واژهٔ محض مشخص است، هر دو بازیکن به‌طور قطعی حرکت را انتخاب می‌کنند و در نتیجه در هر دو، یک نمایهٔ راهبرد با احتمال یک انتخاب می‌شود و احتمال وقوع دیگر نمایه‌های راهبرد، صفر خواهد بود. این دو تعادل دارای عایدی ناعادلانه برای دو بازیکن هستند. دربارهٔ تعادل نش آمیختهٔ $S_۳$ وضعیت متفاوت است. بازیکنان هر یک با احتمال $\frac{۱}{۴}$ توقف و با احتمال $\frac{۱}{۴}$ حرکت را

[۱] Robert Aumann [۲] correlated equilibrium (CE)

انتخاب می‌کنند. در این تعادل، حتی بدترین نمایه نیز با احتمال ناصفر $\frac{۱}{۴}$ امکان وقوع دارد که وضعیت مناسبی نیست. حال فرض کنیم شخص سوم مورد اعتمادی وجود داشته باشد که به هر بازیکن به‌طور خصوصی پیروی از توزیع مذکور در جدول ۴ را پیشنهاد کند. تصادفی بودنِ دو انتخاب (حرکت ,توقف)

جدول ۴. نمایش احتمال‌های تعادل همبسته در بازی ترسوها

بازیکن۲/بازیکن۱	توقف	حرکت
توقف	۰	$\frac{۱}{۲}$
حرکت	$\frac{۱}{۲}$	۰

و (توقف,حرکت) معادل با یک چراغ راهنمایی است. چیزی که دربارهٔ این توزیع جالب است، قدرت خودتحمیلیِ این توزیع است: اگر هر یک از دو بازیکن فرض کند که دیگری از راهبرد پیشنهادی پیروی می‌کند، برای او پیروی از پیشنهاد، بهتر خواهد بود.

یک تعادل همبسته، توزیع احتمال $\{p_s\}$ بر روی نمایه‌های راهبرد تحت قیدهای زیر است: برای هر بازیکن i و هر دو راهبرد متفاوت j و j' متعلق به بازیکن i، مشروط بر اینکه نمایهٔ راهبردِ شامل j، راهبردی با توزیع مورد نظر باشد، عایدی مورد انتظار بازی j کمتر از بازی j' نیست:

$$\Sigma_{s\in S_{-i}}(u_{s-j}-u_{s_{j'}})p_{s_j}\geq ۰ \qquad (۱.۳)$$

همراه با شرط‌های $p_s\geq ۰$ و $\Sigma_s p_s = ۱$. نامساوی تعادل همبسته می‌گوید اگر نمایهٔ راهبرد بر اساس $\{p_s\}$ انتخاب شود و مؤلفهٔ هر بازیکن به‌طور خصوصی به او اطلاع داده شود و اگر همهٔ بازیکنان تصوّر کنند که دیگران از پیشنهاد پیروی می‌کنند، آن‌گاه پیشنهاد خود را به بازیکنان تحمیل می‌کند؛ به این معنی که هیچ بازیکنی راهبرد پیشنهادی خود را تغییر نمی‌دهد [۱۱]. این تعادل معمولاً دارای عایدی مورد انتظار عادلانه است. به عبارت دیگر، تعادل همبسته حالتی عمومی‌تر از تعادل نش است که توزیع همبستهٔ دلخواه بر روی نمایه‌های راهبرد را مجاز می‌داند. نامعادلهٔ تعادل همبسته، رابطه‌ای خطی نسبت به متغیرهای $\{p_s\}$ است و همیشه با برنامه‌ریزی خطی قابل حل است. بنابر قضیهٔ نش، این نامعادله دست‌کم یک پاسخ دارد. برای هر بازی می‌توان در زمان چندجمله‌ای یک تعادل همبسته پیدا کرد. در واقع می‌توان تعادل همبستهٔ دلخواهی را پیدا کرد که جواب بهینه نسبت به تابع خطی دلخواه از p_sها باشد. برای مثال، در بازی ترسوها، می‌توان مجموع عایدی‌های مورد انتظار بازیکنان را با بیشینه کردن تابع هدف $۸P_{۱۱}+۶P_{۱۲}+۶P_{۲۱}$ و تحت قیدهای مبتنی بر نامعادلهٔ تعادل همبسته، بهینه کرد. عایدی مورد انتظار از تعادل همبسته در بازی فوق برابر است با $u(CE)=(۳\frac{۱}{۴},۳\frac{۱}{۴})$ که این عایدیِ مورد انتظار، عادلانه و نسبت به عایدی هر سه تعادل نش بازی، بهتر است.

در بسیاری از بازی‌ها با استفاده از تعادل همبسته می‌توان به عایدی بیشتر و معمولاً عادلانه برای بازیکنان دست یافت و برخلاف تعادل نش، تعادل همبسته را می‌توان در زمان کارای چندجمله‌ای محاسبه کرد. برای ایجاد این همبستگی، به حضور شخص مورد اعتمادی که او را *میانجی*[۱] می‌نامند، نیاز است. او شخصی غیر از بازیکنان است که به ایشان در انتخاب راهبردشان به این شیوه کمک می‌کند: او یک نمایهٔ راهبرد را بر اساس یک توزیع مناسب (همان توزیع تعادل همبسته) که جزء دانش عمومی بازی است، انتخاب می‌کند و به‌طور خصوصی به هر بازیکن راهبرد مربوط به او را اطلاع می‌دهد. روشن است که با وجود توزیع احتمال مربوط به تعادل همبسته، راهبرد پیشنهادی اطلاعاتی را درباره راهبردهای پیشنهاد شده به بازیکنان دیگر در اختیار هر بازیکن قرار می‌دهد. در تعادل همبسته، بازیکنان با وجود داشتنِ اطلاعات شرطی از راهبرد پیشنهادی به بازیکنان دیگر، تمایلی به انحراف از تعادل ندارند. از طرفی، با وجود میانجی، تعداد افراد شرکت‌کننده در بازی، بیش از تعداد بازیکنان خواهد بود و در یک بازی nنفره برای داشتن راهبرد همبسته، $n+1$ نفر شرکت خواهند داشت. برای نظریه‌پردازان بازی‌ها این پرسش وجود دارد که آیا بدون وجود میانجی نیز می‌توان به همان عایدی مورد انتظار تعادل همبسته دست یافت؟ بارانی[۲] [۴] در کار خود برای حذف میانجی در بازی‌هایی با بیش از دو بازیکن، راه‌حلی ارائه کرد ولی حذف میانجی را در بازی‌هایی با دو بازیکن غیرممکن دانست.

۴. محاسبات چندعاملی رمزنگاری

بخش بزرگی از رمزنگاری به *محاسبات چندعاملی*[۳] می‌پردازد. در این محاسبات، بیش از یک عامل حضور دارد. هر عامل P_i ورودی t_i را در اختیار دارد و همه قصد محاسبهٔ تابع $s = f(t_1, \ldots, t_n)$ را بر روی همهٔ ورودی‌ها دارند. هدف این است که هر عامل از خروجی صحیح s آگاه شود (صحّت محاسبات) بدون اینکه هیچ اطلاعی از ورودی‌های عوامل دیگر پیدا کند (محرمانگی). MPC دو هدفِ صحّت محاسبات و محرمانگیِ ورودی‌ها را در یک زمان دنبال می‌کند. از *تسهیم راز*[۴] می‌توان به‌عنوان یکی از مشهورترین نمونهٔ محاسبات چندعاملی یاد کرد که البته معمولاً در طراحی پروتکل‌های MPC مورد استفاده قرار می‌گیرد [۱۱]. مقدار تابع f علاوه بر ورودی‌های عوامل، ممکن است به مقداری تصادفی مانند r نیز بستگی داشته باشد، یعنی $f(t_1, \ldots, t_n; r)$. در این صورت، مقدار r نباید تحت کنترل هیچ‌یک از عوامل باشد و باید در طی محاسبات با توجه به توزیعی مشخص تولید شود. علاوه بر این، f به‌جای خروجی واحد، می‌تواند برای هر عامل یک خروجی به‌صورت $(s_1, \ldots, s_n)$ داشته باشد و در این حالت، لازمهٔ محرمانگی این است که p_i فقط از مقدار s_i آگاه شود.

[۱] mediator [۲] Imre Barany [۳] multi-party computation (MPC) [۴] secret sharing

۵. حذف میانجی

محاسبات چندعاملیِ رمزنگاری و نظریهٔ بازی‌ها علاوه بر تفاوت‌ها، شباهت‌هایی نیز با یکدیگر دارند. این شباهت‌ها دلیلی بر علاقهٔ پژوهشگران به مطالعهٔ فصل مشترک این دو دانش است. برای استفاده از رمزنگاری در نظریهٔ بازی‌ها، لازم است که بازی‌ها را در حیطهٔ رمزنگاری وارد کنیم. در اینجا بازی را به‌صورت بازی تعمیم‌یافته‌ای فرض می‌کنیم که بازیکنانش از نظر محاسباتی محدود هستند و این محدودیت توسط پارامتر امنیتی تعریف می‌شود. بازی‌های (راهبردی) تعمیم‌یافته با گفتگوی کم‌ارزش[۱] یا به‌اختصار، *بازی‌های تعمیم‌یافته*[۲]، نوعی خاص از بازی‌ها هستند. پایهٔ بازی تعمیم‌یافتهٔ G^* بازی راهبردی G است. در فاز گفتگوی کم‌ارزش[۳] یا مقدمه[۴]، بازیکنان براساس پروتکل ارتباطی به تبادل پیام می‌پردازند. نوع مدل ارتباطی مورد استفاده به فرض‌های مسئله بستگی دارد و یک بار با همهٔ جزئیات مورد توافق طرفین قرار می‌گیرد. بعد از مقدمه در فاز بازی، بازی اصلی مطابق معمول اجرا می‌شود. عایدی‌های بازی تعمیم‌یافته دقیقاً همان عایدی‌های بازی اصلی است. چون فاز مقدمه در میزان عایدی بازیکنان تأثیری ندارد، به آن *گفتگوی کم‌ارزش* گفته می‌شود. راهبرد بازیکن P_i در این بازی، شامل راهبرد آن در فاز مقدمه و انتخاب حرکت در بازی اصلی است. نمایهٔ راهبرد معتبر در بازی تعمیم‌یافته باید شامل دستورالعمل رفتار بازیکنان در زمان امتناع برخی از آنها از اجرای فاز مقدمه نیز باشد. حتی همهٔ بازیکنان نیز می‌توانند از این فاز صرف‌نظر کنند و به‌سراغ بازی اصلی بروند. در اینجا فرض بر این است که هر بازیکن فقط از فاز مقدمه می‌تواند امتناع کند و فاز بازی همیشه اجرا می‌شود. البته در صورت لزوم، می‌توان امتناع از فاز بازی را نیز مدل‌سازی کرد. برای شروع، لازم است فرض شود که بازیکنان

(۱) از نظر محاسباتی محدود هستند (مانند عوامل شرکت‌کننده در برخی پروتکل‌های رمزنگاری) و
(۲) پیش از شروع بازی اصلی، با یکدیگر در ارتباط هستند (بازی تعمیم‌یافته).

برای تعریف قدرت محاسباتیِ بازیکنان، لازم است راهبردهای هر دو بازیکن در زمان چندجمله‌ای احتمالی[۵] از پارامتر امنیتی قابل محاسبه باشند.

تعریف ۱.۵ (تعادل نش محاسباتی). تعادل نش محاسباتی بازی دو نفرهٔ تعمیم‌یافته G، یک نمایهٔ راهبرد (s_1^*, s_2^*) مستقل است چنان‌که

(۱) s_1^* و s_2^* هر دو در زمان چندجمله‌ای احتمالی قابل محاسبه باشند؛

---

[۱] (strategic) games extended by cheap-talk [۲] extended games [۳] cheap-talk [۴] preamble [۵] probabilistic polynomial time (PPT)

(۲) برای هر راهبرد دیگر s_1' و s_2' که در زمان چندجمله‌ای قابل محاسبه باشد، یک تابع جزئی μ از پارامتر امنیتی k وجود دارد به‌طوری که

$$u_1(s_1', s_2^*) \leq u_1(s_1^*, s_2^*) + \mu(k)$$

و

$$u_2(s_1^*, s_2') \leq u_2(s_1^*, s_2^*) + \mu(k).$$

به این معنی که اگر بازیکنی به‌تنهایی از این تعادل تغییرِ راهبرد دهد، عایدی او حداکثر به میزان ناچیزی افزایش خواهد یافت و لذا از چنین تغییری صرف‌نظر می‌کند.

رمزنگاران و نظریه‌پردازان بازی‌ها سعی دارند که با شبیه‌سازی میانجی در بازی‌ها با استفاده از پروتکل‌های رمزنگاری، به تعادل‌های قوی‌تر و پایدارتر دست یابند. حذف میانجی در بازی بر مبنای قضیه‌ای مهم انجام می‌گیرد:

قضیه ۲.۵. *([۸، ۱۱]) هر تعادل نش محاسباتی متعلق به بازی تعمیم‌یافتهٔ G^*، همان عایدی مورد انتظار برای بازیکنان در تعادل همبستهٔ معادل در بازی اصلی G را نتیجه می‌دهد.*

روند بازی تعمیم‌یافتهٔ جدید به این صورت است: در آغاز با توجه به پارامتر امنیتی، بازیکنان با اجرای هر پروتکل دو نفره‌ای به تبادل پیام می‌پردازند و با یکدیگر در ارتباط هستند. سپس هر بازیکن حرکت خود را انتخاب می‌کند و در پایان، هر دو در بازی اصلی، به‌طور همزمان حرکت خود را انجام می‌دهند. تعادل همبستهٔ $\{p_s\}$ از بازی اصلی را در نظر بگیرید. میانجی، انتخابی را بر اساس توزیع تعادل همبستهٔ $\{p_s\}$ در زمان چندجمله‌ای انجام و حرکت هر بازیکن را به او اطلاع می‌دهد. بنابراین برای حذف میانجی، هر دو بازیکن باید پروتکل رمزنگاری π را که به‌طور امن انتخابی را بر اساس توزیع $\{p_s\}$ انجام می‌دهد، اجرا کنند. راهبرد هر بازیکن باید پیروی از پروتکل و سپس دریافت حرکت a از اجرای π و انجام آن حرکت باشد. تعریف دقیق راهبرد باید شامل کاری که هر بازیکن در زمان انحراف (در اینجا پیروی نکردن از پروتکل) دیگری باید انجام دهد نیز بشود.

با توجه به مفاهیم نظریهٔ بازی‌ها، متقلب را می‌توان با استفاده از سطح مینیماکس خودش مورد تنبیه قرار داد. این کمترین عایدی است که بازیکنی می‌تواند به بازیکن دیگر تحمیل کند. مقدار مینیماکس بازیکن یک و دو به‌ترتیب، به‌صورت زیر تعریف می‌شوند:

$$v_1 = \min_{s_2} \max_{s_1} u_1(s_1, s_2),$$

و

$$v_۲ = \min_{s_۱} \max_{s_۲} u_۲(s_۱, s_۲).$$

پس اگر بازیکنی از پروتکل منحرف شود و بازیکن مقابل متوجه این انحراف گردد، بازیکن مقابل، خاطی را با مقدار مینیماکس او تنبیه می‌کند. به عبارت دیگر، مقداری را که بازیکن دو در حال بیشینه کردن آن است، بازیکن یک با انتخاب راهبرد مناسب کمینه می‌کند. عایدی‌های حاصل از تعادل همبستهٔ $[u_۱, u_۲]$ برای هر دو بازیکن، بزرگتر یا مساوی با مقدار مینیماکس هر دو بازیکن است: $u_i \geq v_i$. اگر بازی مورد بحث، یک بازی مجموع-صفرِ دو نفره باشد، مینیماکس، خود یک تعادل نش است. این نوع تنبیه معمولاً به بازیکنی که در حال اعمال تنبیه است نیز صدمه می‌زند. در [۵] از الگوی رمزنگاری با *توانایی رمزگذاری‌کور*[۱] به‌عنوان ابزاری برای طراحی پروتکل استفاده شده است. این الگوی رمزنگاری، نمونه‌ای از رمزنگاری‌های کلید عمومی است و مانند دیگر الگوهای رمزنگاریِ کلید عمومی دارای الگوریتم‌هایی برای تولید کلید Gen، رمزگذاری Enc و رمزگشایی Dec به‌اضافهٔ الگوریتم‌های رمزگذاری کور و ترکیب است.

تعریف ۳.۵ (الگوی رمزنگاری با توانایی رمزگذاری کور). الگوی رمزنگاری کلید عمومی ε را با توانایی رمزگذاری کور گویند اگر الگوریتم‌های PPT، Blind و Combine وجود داشته باشند که برای هر پیام m و هر متن رمز شده از این پیام $c \in \mathrm{Enc}_{pk}(m)$:

- برای هر پیام دیگر m' (این پیام را *فاکتور رمزگذاری‌کور* می‌نامند)، $\mathrm{Blind}_{pk}(c, m')$ یک رمزگذاری تصادفی از $m + m'$ را تولید کند، یعنی توزیع $\mathrm{Blind}_{pk}(c, m')$ معادل با توزیع $\mathrm{Enc}_{pk}(m + m')$ باشد:

$$\mathrm{Enc}_{pk}(m + m') \equiv \mathrm{Blind}_{pk}(c, m');$$

- اگر $r_۱$ و $r_۲$ دو عدد تصادفی مورد استفاده در دو رمزگذاری کور متوالی باشند، آن‌گاه برای هر دو فاکتور رمزگذاری کور $m_۱$ و $m_۲$:

$$\mathrm{Blind}_{pk}(\mathrm{Blind}_{pk}(c, m_۱; r_۱), m_۲; r_۲) = \mathrm{Blind}_{pk}(c, m_۱ + m_۲; \mathrm{Combine}_{pk}(r_۱, r_۲)).$$

در الگوهای رمزنگاری با توانایی رمزگذاری کور، هر شخصی می‌تواند متن رمزشدهٔ c از m را بدون آگاهی از m و کلید خصوصی، به‌طور تصادفی به یک رمزگذاری از $m + m'$ ترجمه کند که راهی مناسب برای ترکیب چندین رمزگذاری کور در یک عملیات است. در واقع می‌توان به‌سادگی از هر شخصی خواست تا اطلاعات رمزشده را مجدداً بدون اطلاع از متن اصلی و کلید خصوصی، رمز کند. در بازی‌های معمولی دو نفره، راهبردهای ممکن بازیکنان در بازی به‌صورت فهرستی از دوتایی‌ها است و نمایهٔ راهبرد نهایی، انتخاب

[۱] blindable encryption

تصادفی یکی از این دوتایی‌ها است به‌گونه‌ای که هر بازیکن فقط باید از مؤلفهٔ مربوط به خود آگاهی یابد. مؤلفهٔ اول، متعلق به بازیکن اول و مؤلفهٔ دوم، متعلق به بازیکن دوم است. بازیکن یک به‌عنوان آماده‌ساز[۱] P و بازیکن دو به‌عنوان انتخاب‌کننده[۲] C فهرستی از دوتایی‌ها (نمایهٔ راهبردها) $\{(a_i, b_i)\}_{i=1}^{n}$ را به اشتراک گذاشته‌اند. آنها باید اندیس i را به‌طور تصادفی انتخاب کنند طوری که P فقط a_i و C فقط b_i را بیاموزد. پروتکل جایگزین میانجی ارائه شده در [۵] به این صورت است:

ورودی‌های عمومی: فهرستی از دوتایی‌ها مانند $\{(a_i, b_i)\}_{i=1}^{n}$ و کلید عمومی pk.

اطلاعات آماده‌ساز: کلید خصوصی sk.

(۱) آماده‌ساز: تغییر جایگشت و رمزگذاری.

(الف) برگزیدن جایگشت تصادفی π بر روی $[n]$؛

(ب) به‌ازای هر $i \in [n]$، دوتایی‌ها به این صورت تغییر جایگشت می‌دهند و رمزگذاری می‌شوند: $(c_i, d_i) = (\mathrm{Enc}_{pk}(a_{\pi(i)}), \mathrm{Enc}_{pk}(b_{\pi(i)}))$؛

(پ) ارسال فهرست جدید $\{(c_i, d_i)\}_{i=1}^{n}$ به انتخاب‌کننده.

(۲) انتخاب‌کننده: انتخاب و انجام رمزگذاری کور.

(الف) برگزیدن اندیس تصادفی $l \in [n]$ و مقدار تصادفی فاکتور رمزگذاری کور β؛

(ب) انجام رمزگذاری کور بر روی دوتایی انتخاب‌شده از فهرستِ

$$(e, f) = (\mathrm{Blind}_{pk}(c_l, \circ), \mathrm{Blind}_{pk}(d_l, \beta));$$

(پ) دوتایی (e, f) را به آماده‌ساز ارسال می‌کند.

(۳) آماده‌ساز: رمزگشایی و دست‌یابی به خروجی.

(الف) آماده‌ساز دوتایی دریافتی را رمزگشایی می‌کند: $a = \mathrm{Dec}_{sk}(e)$ و $b' = \mathrm{Dec}_{sk}(f)$. خروجی متعلق به آماده‌ساز، مقدار a است؛

(ب) مقدار b' را به انتخاب‌کننده ارسال می‌کند.

(۴) انتخاب‌کننده: استخراج و دست‌یابی به خروجی.

- انتخاب‌کننده مؤلفهٔ خود را از b' استخراج می‌کند: $b = b' - \beta$ خروجیِ متعلق به انتخاب‌کننده است.

پروتکل ارائه شده به‌طور امن، تابع مسئلهٔ انتخاب همبسته با توزیع یکنواخت نمایهٔ راهبردها را با عوامل صادق اما کنجکاو محاسبه می‌کند. برای امن کردنِ پروتکل برای عوامل غیرصادق، کافی است که بعد از هر مرحله، عامل مربوطه با روش اثباتِ *دانش-صفر*[۳] ثابت کند که از اطلاعاتی که ارسال می‌کند، آگاهی

[۱] preparer [۲] chooser [۳] zero-knowledge proof

کامل دارد. در این اثبات، عاملی متقاعد می‌شود که طرف مقابل او صاحب اطلاعات است اما به هیچ طریقی نمی‌تواند این اطلاعات را استخراج کند. در صورت نیاز به افزودن مرحلهٔ تولید کلید به پروتکل، لازم است که این مرحله به P واگذار شود. این کار پیش از آغاز پروتکل انجام می‌شود و باید اطمینان پیدا کرد که کلیدهای انتخابی توسط P، کلیدهای بدی نباشند. راه‌حل مناسب این است که P با استفاده از روش اثباتِ دانش-صفر ثابت کند که به‌طور کامل از الگوریتم تولید کلید پیروی کرده است. در طراحی این پروتکل، فرض بر یکنواخت بودنِ توزیع تعادل همبسته است اما اگر توزیع تعادل همبسته یکنواخت نباشد، چه باید کرد؟

در برخی از بازی‌ها، تعادل همبسته با بیشینهٔ عایدی مورد انتظار برای بازیکنان، دارای توزیع غیریکنواخت است. راه‌حل ارائه شده در [۵] برای توزیع غیریکنواخت، تکرار زوج راهبردهای معادل در فهرست زوج راهبردها است. در ادامهٔ مقاله پروتکل پیشنهادی در [۱۲] بیان شده است. این پروتکل پیشنهادی، مشابه با پروتکل قبلی است ولی به‌عکس گذشته مؤلفهٔ اول، متعلق به عامل انتخاب‌کنندهٔ C و مؤلفهٔ دوم، متعلق به عامل آماده‌ساز P است:

ورودی‌های عمومی عبارت‌اند از فهرستی از جفت حرکت‌ها به‌همراه احتمال وقوع آنها در توزیع تعادل همبستهٔ $\{(a_i, b_i, p_i)\}_{i=1}^{n}$ و کلید عمومی pk.

اطلاعات آماده‌ساز: کلید خصوصی sk.

(۱) آماده‌ساز: شیفت و رمزگذاری.

(الف) انتخاب مقدار تصادفی $r_0 \in [0, 1)$؛

(ب) کمترین مقدار l را با توجه به قید $\frac{1}{l} \leq \min_i\{p_i\}$ انتخاب کرده و بازه $[0, 1)$ را به l بلوک مساوی تقسیم می‌کند؛

(پ) به‌ازای $\lambda = 1, \ldots, l$، بلوک λ را به‌صورت زیر می‌سازد:

اگر به‌ازای iای، $frac(\widehat{p}_i + r_0) \in [\frac{\lambda-1}{l}, \frac{\lambda}{l})$، آن‌گاه بلوک λ عبارت است از

$$((\mathrm{Enc}_{pk}(a_i), \mathrm{Enc}_{pk}(b_i)), \mathrm{Enc}_{pk}(\frac{frac(l(\widehat{p}_i + r_0))}{l}),$$

$$(\mathrm{Enc}_{pk}(a_{i+1}, \mathrm{Enc}_{pk}(b_{i+1}))))$$

وگرنه با انتخاب مقدار تصادفی $q_\lambda \in [0, \frac{1}{l})$ بلوک λ عبارت است از

$$((\mathrm{Enc}_{pk}(a_j), \mathrm{Enc}_{pk}(b_j)), \mathrm{Enc}_{pk}(q_\lambda), (\mathrm{Enc}_{pk}(a_j), \mathrm{Enc}_{pk}(b_j)))$$

به‌طوری که $j = \min\{j' | frac(\widehat{p}_{j'} + r_0) > \frac{\lambda-1}{l}\}$؛

(ت) فهرست بلوک‌ها را به انتخاب‌کننده ارسال می‌کند.

(۲) انتخاب‌کننده: انتخاب و انجام رمزگذاری کور.

(الف) انتخاب تصادفی بلوک $((c_{a_1}, c_{b_1}), c_p, (c_{a_2}, c_{b_2}))$ از فهرست بلوک‌ها؛

(ب) انتخاب مقدار تصادفی فاکتور رمزگذاری کور $\beta - 1$؛

(پ) ارسال مقدار $c'_p = \mathrm{Blind}_{pk}(c_p, \beta_1)$ به آماده‌ساز؛

(۳) آماده‌ساز: رمزگشایی از احتمال.

- ارسال مقدار $p' = \mathrm{Dec}_{sk}(c'_p)$ به انتخاب‌کننده.

(۴) انتخاب کننده: انتخاب حرکت‌ها.

(الف) $p = p' - \beta_1$؛

(ب) تولید یک عدد تصادفی جدید β_2؛

(پ) با احتمال l_p، $(e, f) = (\mathrm{Blind}_{pk}(c_{a_1}, \beta_2), \mathrm{Blind}_{pk}(c_{b_1}, 0))$ انتخاب می‌شود وگرنه $(e, f) = (\mathrm{Blind}_{pk}(c_{a_2}, \beta_2), \mathrm{Blind}_{pk}(c_{b_2}, 0))$؛

(ت) ارسال (e, f) به آماده‌ساز.

(۵) آماده‌ساز: رمزگشایی و دست‌یابی به خروجی.

(الف) خروجی آماده‌ساز برابر با مقدار $\mathrm{Dec}_{sk}(f)$ است؛

(ب) ارسال مقدار $b' = \mathrm{Dec}_{sk}(e)$ به انتخاب‌کننده.

(۶) انتخاب کننده: استخراج و دست‌یابی به خروجی.

- خروجی انتخاب‌کننده برابر با مقدار $b = b' - \beta_2$ است.

توجه کنید که $\widehat{p_i} = \sum_i p_j$ و $frac(x)$ تابع قسمت اعشاری x است.

تفاوت دیگر دو پروتکل در طول پیام آنها است. در هر دو پروتکل، طولانی‌ترین پیام در مرحلهٔ اول ارسال می‌شود. در پروتکل مذکور در [۵] طول پیام در صورت استفاده از توزیع غیریکنواخت برابر است با کوچکترین مضرب مشترک بین مخرج احتمال‌ها ولی در پروتکل مذکور در [۱۲] این مقدار برابر است با معکوس کوچکترین احتمال ناصفر که بجز حالت توزیع یکنواخت که این دو برابرند، کوچکتر از کوچکترین مضرب مشترک مخرج احتمال‌ها است.

دو پروتکل با ساختاری مشابه را برای شبیه‌سازی میانجی در بازی مشاهده کردید. پیروی از هر دو پروتکل تعادل نش، محاسباتی هستند که بازیکنان به‌تنهایی تمایلی برای انحراف از آنها ندارند. هر دو پروتکل نمونه‌هایی کارا برای بازی راهبردی دو نفره با اطلاعات کامل هستند. از رمزنگاری برای حذف میانجی در بازی‌هایی با بیش از دو بازیکن و بسیاری از بازی‌ها می‌توان استفاده کرد؛ حتی در بازی‌های با اطلاعات ناقص. در حالت کلی حذف میانجی در بازی‌ها در دو مرحله انجام می‌شود: در مرحلهٔ مقدمه،

بازیکنان پروتکل محاسباتی چندعاملی مناسبی را برای محاسبهٔ نمایهٔ $(s_1, \ldots, s_n)$ اجرا می‌کنند؛ سپس عامل p_i حرکت پیشنهادی s_i را برای استفاده در بازی اصلی در اختیار دارد.

با استفاده از پروتکل‌ها و الگوهای گوناگون رمزنگاری می‌توان به تعادل‌ها و اهداف متنوعی دست یافت. با استفاده از ترکیب نظریهٔ بازی‌ها و پروتکل‌های MPC می‌توان تعریفی قوی‌تر از تعریف‌های گذشته برای تعادل‌های تعاونی ارائه داد. این تعادل که تعادل (نش یا همبستهٔ) *انعطاف‌پذیر*[1] نام دارد، ممکن است در خیلی از بازی‌ها وجود نداشته باشد ولی خودش نمونه‌ای از کاربرد رمزنگاری در نظریهٔ بازی‌ها است. تعادل انعطاف‌پذیر در مقابل همهٔ تبانی‌های دشمن که حتی برای برخی از اعضا سودمند است، باید امن باشد. بنابراین این تعادل بسیار پایدار است.

نمایهٔ راهبرد مستقل $(x_1^*, \ldots, x_n^*)$ را یک تعادل نش kانعطاف‌پذیر می‌نامیم اگر برای همهٔ گروه‌های تبانی‌کنندهٔ C با حداکثر تعداد k عضو، همهٔ راهبردهای همبستهٔ انحرافی x_c متعلق به اعضای C و برای همهٔ اعضا $P_i \in C$ داشته باشیم

$$u_i(x_c^*, x_{-c}^*) \geq u_i(x_c, x_{-c}^*).$$

بنابراین هیچ‌یک از اعضای ائتلاف دشمن به‌وسیله انحراف از این تعادل، سودی نخواهند برد. اگر x یک تعادل همبستهٔ kانعطاف‌پذیر برای بازی G با تابع f باشد و π پروتکل محاسباتی چندعاملی باشد که تابع f را به‌طور امن در مقابل تبانی حداکثر k عامل محدود (نامحدود) از نظر توان محاسباتی، محاسبه می‌کند، آن‌گاه اجرای π در مرحلهٔ مقدمه (و استفاده از هر راهبرد برای برخورد با افراد خاطی)، یک تعادل نش محاسباتی (عادی) kانعطاف‌پذیر برای بازی تعمیم‌یافتهٔ G^* را نتیجه می‌دهد که به همان عایدی x دست می‌یابد [۱۱]. بنابراین با استفاده از پروتکل‌هایی که در برابر تبانی حداکثر k عامل امن هستند، در فرآیند حذف میانجی می‌توان به تعادل‌های kانعطاف‌پذیر دست یافت.

به‌کمک پروتکل‌هایی با سرویس‌ها و ویژگی‌های متنوع می‌توان به اهداف متنوع دیگری رسید. برای مثال، یکی از بدرفتاری‌های ممکن در حین اجرای فاز مقدمه این است که عوامل بداندیش مانع شوند که افراد صادق خروجی خود از پروتکل (که معادل است با راهبرد پیشنهادی میانجی به بازیکن) را دریافت کنند. برای مقابله با چنین بدرفتاری، کافی است از پروتکل‌های با ویژگی تحویل خروجی استفاده کرد که این ویژگی مانع از این رفتار می‌شود. این ویژگی، دریافت خروجی را توسط همهٔ عوامل شرکت‌کننده تضمین می‌کند.

یکی دیگر از بدرفتاری‌های ممکن در حین اجرای مقدمه این است که عاملی از اجرای پروتکل امتناع کند و پروتکل را بدون دریافت خروجی به پایان برساند. در رمزنگاری، پروتکل زمانی با موفقیت به پایان

[1] resilient (Nash or correlated) equilibrium

می‌رسد که دارای خروجی باشد. در پروتکل‌ها به عوامل اجازهٔ تشخیص خطا و عامل خاطی داده می‌شود. برای مثال، P_n را به‌عنوان عامل خطاکار در نظر بگیرید. یک پروتکل می‌تواند *منصفانه* باشد به این معنی که اگر عاملی خروجی صحیح را دریافت کرد، می‌تواند اطمینان داشته باشد که دیگران نیز خروجی صحیح خود را دریافت کردند. اگر پروتکل منصفانه باشد، امتناع از اجرا پیش از آنکه کسی اطلاعی از خروجی خود داشته باشد، اتفاق می‌افتد. در این صورت یک راه‌حل ساده در زمان امتناع عامل P_n، اجرای مجدد مرحلهٔ مقدمه است. اما این راه‌حل مناسب به نظر نمی‌رسد. در این صورت P_n با انکار رفتار خود و ادامهٔ آن در هر تکرار، می‌تواند سبب اجرای همیشگی این فاز شود. برای محدود کردن بازی و جلوگیری از چنین بدرفتاری‌هایی، می‌توان از راهبرد تنبیهی قوی‌تری استفاده کرد. در این راه‌حل نیز مرحلهٔ مقدمه مجدداً اجرا می‌شود اما این بار بدون عامل P_n. حال تابع بر روی ورودی‌های $n-1$ بازیکن دیگر و مقدار پیش‌فرض $\perp$ برای ورودی P_n محاسبه می‌شود: $f'(t_1,\ldots,t_{n-1};r) = f(t_1,\ldots,t_{n-1},\perp;r)$.
و در صورت امتناع دیگر بازیکنان نیز همین فرآیند تکرار می‌شود. در هر مرحله حداقل یک عامل خاطی از محاسبات حذف می‌شود و از آنجا که تعداد بازیکنان محدود است، بازی نیز محدود خواهد بود. از این راه‌حل برای زمانی که بازیکنان نوع خود را تغییر می‌دهند نیز می‌توان استفاده کرد. در این حالت، برای ورودی هر عامل دامنه‌ای تعریف می‌شود. در صورت دریافت مقداری خارج از دامنه مشخص شده، مقدار پیش فرض جایگزین نوع آن عامل شده و مقدمه با حذف عامل خاطی از محاسبات تکرار می‌شود. نکتهٔ مهم این است که پیش از همه باید مقدار پیش‌فرضِ $\perp$ را در دامنهٔ تابع تعریف کرد. فرآیند حذف عامل خاطی از اجرای پروتکل، در امنیت محاسبه تأثیری ندارد [۱۱].

مراجع

[۱] باباخانی، م.، *نظریهٔ بازی‌ها و رمزنگاری*، پایان‌نامهٔ کارشناسی‌ارشد، دانشگاه مازندران، ۱۳۹۳.

[۲] عبدلی، ق.، *نظریهٔ بازی‌ها و کاربردهای آن (بازی‌های ایستا و پویا با اطلاعات کامل)*، سازمان انتشارات جهاد دانشگاهی، ۱۳۸۶، تهران.

[3] Aumann, R., Subjectivity and correlation in randomized strategies, *Mathematical Economics Journal*, **1** (1974), 67–96.

[4] Barany, I., Fair distribution protocols or how the players replace fortune, *Mathematics of Operations Research*, **17** (1992), no. 2, 327–340.

[5] Dodis, y., Halevi, S., Rabin, T., *A cryptographic solution to a game theoretic problem*, Advances in Cryptology – Crypto, 2000, 112–130

[6] Fudenberg, D., Tirole, J., *Game Theory*, MIT Press, 1991.

[7] Goldwasser, S., Micali, S., Probabilistic encryption, *Journal of Computer and System Sciences*, **28** (1984), no. 2, 270–299.

[8] Katz, J., *Bridging game theory and cryptography: Recent results and future directions*, In: 5th Conference on the Theory of Cryptography, 2008.

[9] Kol, G., Naor, M., *Cryptography and game theory: Designing protocols for exchanging information*, In: 5th Conference on the Theory of Cryptography, 2008.

[10] Nash, J., Non-cooperative games, *Annals of Mathematics*, **54** (1951), no. 2, 286–295.

[11] Nisan, N., Roughgarden, T., Tardos, E., Vazirani, V., *Algorithmic Game Theory*, Cambridge University Press, Cambridge, 2007.

[12] Teague, V., Selecting correlated random actions, *Financial Cryptography*, 3110 (2004), 181–195.

تاریخ ارسال: ۹۵/۴/۲۰؛ تاریخ بازنگری: ۹۶/۶/۹؛ تاریخ پذیرش: ۹۶/۶/۱۳

مونا باباخانی: دانشگاه مازندران، دانشکدهٔ علوم ریاضی
رایانامه: babakhani@lavasan.tpnu.ac.ir

رضا ندیمی: دانشگاه مازندران، دانشکدهٔ علوم ریاضی
رایانامه: nadimi@umz.ac.ir