بسم الله الرحمن الرحیم

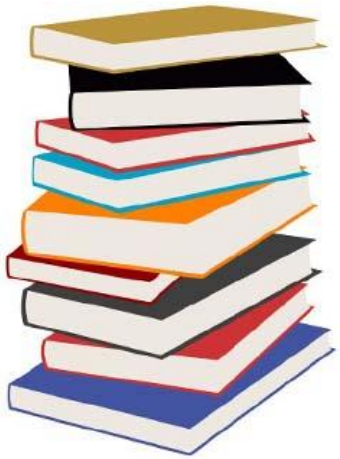
انتخابات‌های انتهابه‌انتها قابل راستی‌آزمایی

سید محمدمهدی احمدپناه
smahmadpanah@aut.ac.ir

ارائه درس پروتکل‌های امنیتی

دانشگاه صنعتی امیرکبیر
۲۸ تیر ۱۳۹۵

فهرست



- مقدمه
- خواسته‌های امنیتی
- مروری بر کارهای گذشته
- مدل‌سازی خواسته امنیتی
- ساختار کلی سیستم پیشنهادی
- معرفی اجزای سیستم
- بیان سیستم پیشنهادی
- جمع‌بندی
- مسائل باز و پروژه کارشناسی ارشد

مقدمه

- انتخابات الکترونیکی
  - ضرورت ایجاد سیستم انتخابات الکترونیکی
- اهمیت بررسی امنیت در انتخابات
  - ایجاد سیستم انتخابات امن
  - خواسته‌های امنیتی گوناگون

خواسته‌های امنیتی

- بررسی صلاحیت داشتن
- یکتایی رأی به ازای رأی‌دهنده
- عدم قابلیت بازاستفاده کردن
- **حریم خصوصی رأی‌دهنده**
- **قابلیت راستی‌آزمایی**
- جامع‌بودن
- مانع‌بودن
- ناظر به مسئولیت اجتماعی
- بی‌طرفی
- **تازگی رسید**

خواسته‌های امنیتی (ادامه)

- تعریف سیستم انتخابات انتهابه‌انتها قابل راستی‌آزمایی
  - خوش‌فرم‌بودن برگه‌های رأی ارائه‌شده
  - خوش‌فرم‌بودن برگه‌های رأی انداخته‌شده
  - ثبت‌شدن همانی که انداخته‌شده
  - شمارش همانی که ثبت‌شده
  - سازگاری
  - عدم وجود برگه رأی در شمارش که بررسی نشده
- تشخیص مرجع انتخابات بدخواه

خواسته‌های امنیتی (ادامه)

1. Cast as Intended
2. Recorded as Cast
3. Tallied as Recorded

- قابلیت راستی‌آزمایی انتخابات برای هر فرد ثالث خارجی
  - قابل تفویض‌بودن رسیدها به فرد ثالث
- عدم استفاده از رسید برای مشخص‌شدن محتوای رأی
  - جلوگیری از خرید و فروش رأی
- تعریف مدل استاندارد
  - بدون نیاز به فرضیات در گام راه‌اندازی یا دسترسی به یک اوراکل تصادفی

مروری بر کارهای گذشته

- مبتنی بر فرضیات مرحله راه‌اندازی
  - نیاز به حضور فرد ثالث مورد اعتماد
    - Remotegrity
    - طرح‌های مبتنی بر محاسبات چندطرفه قابل حسابرسی
- در مدل اوراکل تصادفی
  - نیاز به دسترسی به یک اوراکل تصادفی
    - Helios

مروری بر کارهای گذشته (ادامه)

- چاوم (سال ۱۹۸۱)
  - ارتباط بی‌نام
  - انتخابات با قابلیت راستی‌آزمایی انفرادی
- ساکو و کیلیان (سال ۱۹۹۵)
  - انتخابات با قابلیت راستی‌آزمایی همگانی
- چاوم (سال ۲۰۰۴) و نِف (سال ۲۰۰۴)
  - معرفی قابلیت راستی‌آزمایی انتهابه‌انتها
- کِرمِر و همکاران (سال ۲۰۱۰)
  - تعریف صوری و نمادین با استفاده از حساب Applied Pi

مدل‌سازی خواسته امنیتی

- نحوه مدل‌کردن صوری راستی‌آزمایی انتهابه‌انتها
  - رویکرد مبتنی بر بازی
    - تعریف یک بازی بین مهاجم و چالش‌گر
  - وجود مرجع انتخابات بدخواه و یا رأی‌دهندگان نادرستکار
    - شرط برنده‌شدن مهاجم: اختلاف از نتیجه واقعی انتخابات بیش از مقدار مشخصی باشد.
  - احتمال برنده‌شدن مهاجم بسیار کوچک باشد.

$$\Pr[G^{\mathcal{A},\mathcal{E},d,\theta}_{\mathrm{E2E-Ver}}(1^{\lambda}, m, n) = 1] \leq \epsilon$$

ساختار کلی سیستم پیشنهادی

- نمادگذاری

Π: سیستم انتخابات

λ: پارامتر امنیتی

n: تعداد رأی‌دهنده‌ها

m: تعداد کاندیداها

$\mathcal{V} = \{V_1, \ldots, V_n\}$: مجموعه رأی‌دهنده‌ها

$\mathcal{P} = \{P_1, \ldots, P_m\}$: مجموعه کاندیدا

$\mathcal{U} \subseteq 2^{\mathcal{P}}$: مجموعه زیرمجموعه‌های کاندیداهای مجاز

$\mathcal{U}_\ell$: کاندیداهای انتخاب‌شده توسط رأی‌دهنده V_ℓ

ساختار کلی سیستم پیشنهادی (ادامه)

- نمادگذاری

E2E: End-to-End

EA: Election Authority

BB: Bulletin Board

Election Evaluation Function (f)

$f: \mathcal{P}^* \rightarrow \mathbb{Z}_+^m$ s.t.

$$f(\mathcal{U}_1, \ldots, \mathcal{U}_n) = \langle t_1, \ldots, t_m \rangle$$

ساختار کلی سیستم پیشنهادی (ادامه)

- یک سیستم انتخابات Π، یک پنج‌تایی از الگوریتم‌ها و پروتکل‌های زیر است:

- Setup (Algorithm)
- Cast (Protocol)
- Tally (Protocol)
- Result (Algorithm)
- Verify (Algorithm)

ساختار کلی سیستم پیشنهادی (ادامه)

- Setup $(1^{\lambda}, \mathcal{P}, \mathcal{V}, \mathcal{U})$
  - اجرا توسط EA
  - تولید یک کلید محرمانه اصلی msk و پارامترهای عمومی سیستم Pub (حاوی $\mathcal{P}, \mathcal{V}, \mathcal{U}$) و مقادیر محرمانه رأی‌دهندگان $s_1, \ldots, s_n$
  - EA یک حالت st دارد که در ابتدا msk است.
  - EA در ابتدا گزارش عمومی T = Pub را به BB ارسال می‌کند.

ساختار کلی سیستم پیشنهادی (ادامه)

- Cast
  - پروتکل بین V_ℓ، BB و EA
  - V_ℓ با ورودی $(Pub, s_\ell, \mathcal{U}_\ell)$، EA با ورودی msk و BB با ورودی T
  - EA حالت خود و BB نیز T را به‌روز می‌کنند.
  - در صورت موفقیت‌آمیزبودن، V_ℓ رسید α_ℓ را دریافت می‌کند.

ساختار کلی سیستم پیشنهادی (ادامه)

- Tally
  - پروتکل بین BB و EA
  - ورودی مشترک Pub و EA با ورودی msk و BB با ورودی T
  - در صورت موفقیت‌آمیزبودن، BB گزارش عمومی T را به‌روز می‌کند.

ساختار کلی سیستم پیشنهادی (ادامه)

- Result(T)
  - خروجی R_T برای نتیجه انتخابات
    - در صورت تعریف‌نشده‌بودن نتیجه، خروجی $\perp$ برگردانده می‌شود.
  - خروجی این الگوریتم، همان نتیجه شمارش آرا و نتیجه انتخابات است.

ساختار کلی سیستم پیشنهادی (ادامه)

- Verify(T, α)
  - α رسید رأی‌دهنده از خروجی پروتکل Cast
  - خروجی مقدار صفر یا یک

ساختار کلی سیستم پیشنهادی (ادامه)

- تعریف صحت انتخابات
  - سیستم انتخابات Π صحت دارد اگر برای هر اجرای درستکارانه از آن:

$$\text{Result}(T) = f(\mathcal{U}_1,\ldots,\mathcal{U}_n) \text{ and } \wedge_{\ell=1}^{n} (\text{Verify}(T,\alpha_\ell) = 1).$$

معرفی اجزای سیستم

- Perfectly Binding Commitment
  - Additively Homomorphic
    - استفاده از طرح الجمال روی منحنی‌های بیضوی
- Param := (p, a, b, g, q)
- Elliptic Curve E: $y^2 = x^2 + ax + b \pmod p$
  - G گروه دوری تولیدشده توسط g
    - با فرض برقراری DDH روی G
  - $g^a , g^b \rightarrow g^{ab}$ random-like in G

معرفی اجزاء سیستم (ادامه)

- Perfectly Binding Commitment
  - Gen(Param; 1^{λ}):
    - picks $x \leftarrow Zq$, sets $h := g^x$, and outputs $ck := (Param; h)$
  - $Com_{ck}(m; r)$:
    - outputs $c := (g^r; g^m h^r)$
  - $Ver_{ck}(c; m; r)$:
    - outputs accept if $c = (g^r; g^m h^r)$; otherwise, outputs reject
  - $Com_{ck}(m_1; r_1) \cdot Com_{ck}(m_2; r_2) = Com_{ck}(m_1+m_2; r_1+r_2)$

معرفی اجزاء سیستم (ادامه)

- A Σ Protocol for Candidate Encoding Correctness
  - N = n+1
  - هر برگه رأی شامل دو قسمت مشابه حاوی لیستی از m کد- رأی مربوط به لیست کاندیداها
  - $E_{l,j}^{(a)}$: دو مجموعه تعهدها
    - $a \in \{0,1\}$, $\ell = 1,\ldots,n$, $j = 1,\ldots,m$
    - هر مجموعه به جایگشتی از کدهای کاندیداها متعهد می‌شود.
    - کدکردن کاندیدای P_j با مقدار N^{j-1}

معرفی اجزاء سیستم (ادامه)

$P(i, r)$:

Define b_j such that $i = \sum_{j=0}^{\log m - 1} b_j 2^j$. Pick

- $t_j, z_j, y_j, r_j, w_j, f_j \leftarrow \mathbb{Z}_q$ for $j \in [0, \log m - 1]$.

Compute the following commitments:

- For $j \in [0, \log m - 1]$,
  - $B_j = \mathsf{Com}_{\mathsf{ck}}(b_j; r_j)$; $T_j = \mathsf{Com}_{\mathsf{ck}}(t_j; z_j)$;
  - $Y_j = \mathsf{Com}_{\mathsf{ck}}((1 - b_j)t_j; y_j)$;
  - $W_j = \mathsf{Com}_{\mathsf{ck}}(w_j; f_j)$.

Define A_j, a_j, r'_j such that $A_j = B_j^{N^{2^j}-1} \cdot \mathsf{Com}_{\mathsf{ck}}(1; 0) = \mathsf{Com}_{\mathsf{ck}}(a_j; r'_j)$, for $j \in [0, \log m - 1]$. Define $\{\beta_j, \gamma_j\}_{j=0}^{\log m}$ such that $\prod_{j=0}^{\log m - 1}(a_j X + w_j) = \sum_{j=0}^{\log m} \beta_j X^j$ and $\prod_{j=0}^{\log m - 1}(r'_j X + f_j) = \sum_{j=0}^{\log m} \gamma_j X^j$. (Note that for efficiency reasons, the prover needs to choose the $\{r_j\}_{j=0}^{\log m - 1}$ such that $\gamma_{\log m} = r$ in previous step.)

- For $j \in [0, \log m - 1]$, $D_j = \mathsf{Com}_{\mathsf{ck}}(\beta_j; \gamma_j)$.

Return $\phi_1 = \{B_j, T_j, Y_j, W_j, D_j\}_{j=0}^{\log m - 1}$ and

$\text{state}_\phi = \{t_j, z_j, y_j, r_j, b_j, w_j, f_j\}_{j=0}^{\log m - 1}$.

معرفی اجزاء سیستم (ادامه)

$P \to V$: Send ϕ_1.

$V \to P$: Send $\rho \leftarrow \mathbb{Z}_q$.

$P(\text{state}_\phi)$: Compute the following answers:

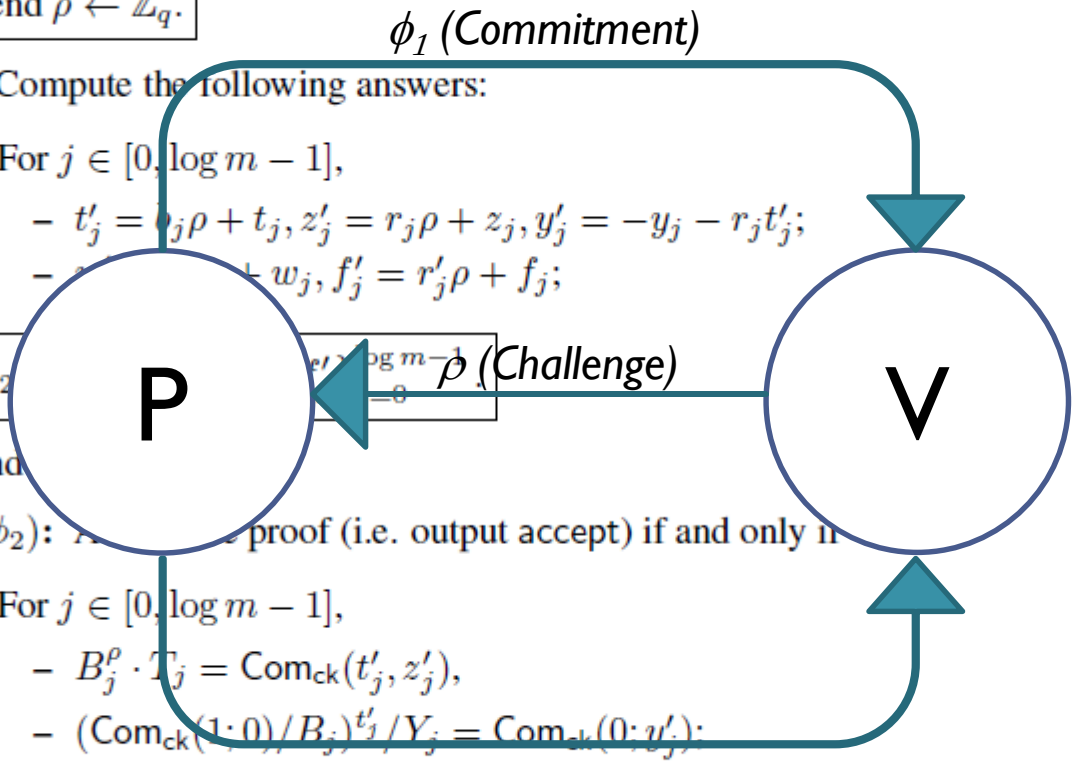
- For $j \in [0, \log m - 1]$,
  - $t'_j = \ldots \rho + t_j, z'_j = r_j \rho + z_j, y'_j = -y_j - r_j t'_j$;
  - $\ldots + w_j, f'_j = r'_j \rho + f_j$;

Set ϕ_2 ... $\log m - 1$ ... $= 0$

$P \to V$: send ...

$V(E, \phi_1, \rho, \phi_2)$: ... proof (i.e. output accept) if and only if

- For $j \in [0, \log m - 1]$,
  - $B_j^\rho \cdot T_j = \text{Com}_{\text{ck}}(t'_j, z'_j)$,
  - $(\text{Com}_{\text{ck}}(1; 0)/B_j)^{t'_j}/Y_j = \text{Com}_{\text{ck}}(0; y'_j)$;
  - $A_j^\rho \cdot W_j = \text{Com}_{\text{ck}}(w'_j, f'_j)$;
- $E^{\rho^{\log m}} \prod_{j=0}^{\log m - 1} D_j^{\rho^j} = \text{Com}_{\text{ck}}(\prod_{j=0}^{\log m - 1} w'_j; \prod_{j=0}^{\log m - 1} f'_j)$;



معرفی اجزاء سیستم (ادامه)

- Producing the Verifier's Challenge
  - $\{0,1\}^{\ell_\Sigma}$ فضای چالش‌ها ؛ $\ell_\Sigma = |q|$
  - افراز سکه‌های رأی‌دهندگان a به k بلوک؛ یعنی $a_1,\ldots,a_k$
  - برای هر a_i، اثبات صحت برگه رأی EA با استفاده از یک پروتکل سیگما جداگانه که در آن a_i چالش باشد.
    - پذیرش صحت اثبات EA توسط Verfier در صورتی‌که همه پروتکل‌های سیگما معتبر باشند.
  - قضیه بعدی مشخص می‌کند که خطای درستی با kبار اجرای پروتکل سیگما به شرح بالا، به صورت نمایی افت می‌کند.

معرفی اجزاء سیستم (ادامه)

- Producing the Verifier's Challenge
  - $a = (a_1,\ldots,a_k)$
  - $H_\infty(a) = \theta$
  - all adversarial prover *A*

$$\epsilon(m,n,k,\theta) = \Pr\left[\begin{array}{l} \mathsf{ck} \leftarrow \mathsf{Gen}(\mathsf{Param}, 1^\lambda); (E, x, r, \{\phi_{1,i}\}_{i=1}^k) \leftarrow \mathcal{A}(\mathsf{Param}, \mathsf{ck}); \\ \{\phi_{2,i}\}_{i=1}^k \leftarrow \mathcal{A}(\mathbf{a}_1, \ldots, \mathbf{a}_k) : \mathsf{Ver}_{\mathsf{ck}}(E; x; r) = \text{accept} \quad \wedge \\ x \notin \{N^0, \ldots, N^{m-1}\} \ \wedge \ \forall i \in [k], V(E, \phi_{1,i}, \mathbf{a}_i, \phi_{2,i}) = \text{accept} \end{array}\right]$$
$$\leq 2^{k \log\log m - \theta + k}.$$

بیان سیستم پیشنهادی

- انتخابات یک از m (مشابه ریاست جمهوری ایران)
  - البته طرح کلی می‌تواند چند از m باشد.
  - $\mathcal{U} = \{\{P_1\}, \ldots, \{P_m\}\}$
- $\text{Setup}(1^\lambda, \mathcal{P}, \mathcal{V}, \mathcal{U})$
  - اجرای $\text{Gen}(\text{Param}, 1^\lambda)$ توسط EA برای محاسبه کلید تعهد ck
  - برای هر $\ell \in [n]$، EA مراحل زیر را انجام می‌دهد:
    - انتخاب شماره منحصربه‌فرد برای برگه رأیِ دوتایی ℓام (tag_ℓ)
    - انتخاب جایگشت‌های تصادفی $\pi_\ell^{(0)}$ و $\pi_\ell^{(1)}$ روی [m] برای بهم‌ریختن ترتیب زوج‌های (کد-رأی، کاندیدا) در بخش $s_\ell^{(i)}$ از برگه رأی

بیان سیستم پیشنهادی (ادامه)

- انتخاب جایگشت‌های تصادفی $\pi_\ell^{(0)}$ و $\pi_\ell^{(1)}$ روی [m] برای بهم‌ریختن ترتیب زوج‌های (کد-رأی، کاندیدا) در بخش $s_\ell^{(i)}$ از برگه رأی دوتایی s_ℓ
- برای حفظ حریم خصوصی، جایگشت‌های برگه‌های رأی را به صورت متعهدشده به BB ارسال می‌کند.
- برای $j \in [m]$، کد-رأی‌های منحصربه‌فرد $C_{\ell,j}^{(0)}, C_{\ell,j}^{(1)} \leftarrow Zq$
  - $C_{\ell,j}^{(i)}$ قسمتی از بخش $s_\ell^{(i)}$ از s_ℓ است که کاندیدای Pj را مشخص می‌کند.
- برای $a \in \{0,1\}$، بخش $s_\ell^{(a)} = \{(P_j, C_{\ell,j}^{(a)})\}_{j \in [m]}$ و در نهایت، برگه رأی $s_\ell = (tag_l, s_\ell^{(0)}, s_\ell^{(1)})$ را تولید می‌کند.

بیان سیستم پیشنهادی (ادامه)

- برای $j \in [m]$، محاسبه $j' = \pi_{\ell}^{(0)}(j)$ و
- برای $a \in \{0,1\}$، انتخاب مقدار تصادفی $t_{\ell,j'}^{(a)} \leftarrow Z_q$ و محاسبه تعهد کد-رأی برای $C_{\ell,j'}^{(a)}$:

$$U_{\ell,j'}^{(a)} = Com_{ck}(C_{\ell,j'}^{(a)}; t_{\ell,j'}^{(a)})$$

- برای $a \in \{0,1\}$، انتخاب مقدار تصادفی $r_{\ell,j'}^{(a)} \leftarrow Z_q$ و محاسبه تعهد کدشده کاندیدا برای $P_{j'}$:

$$E_{\ell,j'}^{(a)} = Com_{ck}((n+1)^{j'-1}; r_{\ell,j'}^{(a)})$$

که در آن $(n+1)^{j'-1}$ کدشده کاندیدای $P_{j'}$ است.

بیان سیستم پیشنهادی (ادامه)

- برای a∈{0,1}، داده پیش‌حسابرسی $\phi_{1,\ell,j'}^{(a)}$ برای راستی‌آزمایی $E_{\ell,j'}^{(a)}$ تولید می‌شود. حالت اثبات‌کننده $state_{1,\ell,j'}^{(a)}$ را نیز نگه‌داری می‌کند. نحوه تولید این دو در گام اول پروتکل سیگما

- اطلاعات عمومی مربوط به s_ℓ ، یعنی Pub_ℓ به شکل زیر است:

$$Pub_\ell = (tag_l, \{(U_{\ell,j'}^{(a)}, E_{\ell,j'}^{(a)}, \phi_{1,\ell,j'}^{(a)})\}_{j\in[m]}^{a\in\{0,1\}}$$

  - مرتب‌شده بر اساس tag

- اطلاعات عمومی که توسط EA تولید می‌شود:

$$Pub = (\mathrm{ck}, \mathcal{P}, \mathcal{U}, \{Pub_\ell\}_{l\in[n]}$$

و کلید محرمانه EA:

$$msk = \{Pub_\ell, s_l, msk_l, state_{\phi,l}\}_{l\in[n]}$$

$$msk_\ell = \left\{(C_{\ell,j}^{(a)}, t_{\ell,j}^{(a)}, \pi_\ell^{(a)}(j) = j', r_{\ell,j}^{(a)})\right\}_{j\in[m]}^{a\in\{0,1\}} \text{ and } \mathrm{state}_{\phi,\ell} = \left\{\mathrm{state}_{\phi,\ell,j'}^{(a)}\right\}_{j\in[m]}^{a\in\{0,1\}}$$

بیان سیستم پیشنهادی (ادامه)

- Cast
  - ورودی $(Pub_\ell, s_l, \mathcal{U}_l)$
  - V_l با سکه‌اندازی $a_l \leftarrow \{0,1\}$ و انتخاب بخش برای $s_\ell^{(a)}$ رأی‌دادن
  - کاندیدای مورد نظر $\mathcal{U}_l = \{P_{j_l}\}$
  - V_l باید $C_{\ell,j_l}^{(a_l)}$ که کد-رأی متناظر با P_{j_l} در بخش $s_\ell^{(a)}$ است، ارائه کند.
  - در نهایت، V_l رأی $\Psi_\ell = (tag_l, a_l, C_{\ell,j_l}^{(a_l)})$ را بیندازد.

بیان سیستم پیشنهادی (ادامه)

- EA رأی را می‌گیرد و حالت **st** خود را با اضافه‌کردن ψ_ℓ به‌روز می‌کند. رسید α_ℓ حاوی رأی ψ_ℓ و بخش $s_\ell^{(1-a_l)}$ برای حسابرسی به V_l داده می‌شود.

بیان سیستم پیشنهادی (ادامه)

- Tally
  - $\tilde{V}$: مجموعه رأی‌دهندگانی که با موفقیت رأی دادند.
  - برای هر $V_l \in \tilde{V}$، EA از (tag_l, a_l) از ψ_ℓ ، برای بازیابی اطلاعات حسابرسی $s_\ell^{(1-a_l)}$ از s_ℓ استفاده می‌کند.
  - ارسال لیست $\{(\psi_\ell, s_\ell^{(1-a_l)})\}_{V_l \in \tilde{V}}$ به BB
  - بازکردن همه تعهدهای کد-رأی‌ها $(\{U_{\ell,\mathrm{j}}^{(a)}\}_{l\in[n],j\in[m]}^{a\in\{0,1\}})$ با ارسال لیست زوج‌های $\{C_{\ell,\mathrm{j}}^{(a)}, t_{\ell,\mathrm{j}}^{(a)}\}_{l\in[n],j\in[m]}^{a\in\{0,1\}}$ به BB

بیان سیستم پیشنهادی (ادامه)

- EA برای هر ψ_ℓ متناظر با $V_l \in \tilde{V}$ مراحل زیر را انجام می‌دهد:
  - محل کد-رأی بازشده C_ℓ که با کد-رأی انداخته‌شده $C_{\ell,j_l}^{(a_l)}$ مطابقت می‌کند، را پیدا می‌کند.
  - کد-رأی C_ℓ را با نشان 'voted' مشخص می‌کند.
  - تعهد $E_{\ell,j'_l}^{(a_l)}$ مربوطه را به مجموعه $\mathsf{E}_{\text{tally}}$ اضافه می‌کند.
    - یادآوری: $j_\ell' = \pi_\ell^{(a_l)}(j_l)$

بیان سیستم پیشنهادی (ادامه)

- همه تعهدهای $\{E_{\ell,j}^{(1-a_l)}\}_{j\in[m]}$ مرتبط با کد-رأی‌های موجود در $s_\ell^{(1-a_l)}$را به مجموعه E_{open} اضافه می‌کند.
  - در نهایت، E_{tally} حاوی مجموعه آرا برای شمارش و E_{open} حاوی اطلاعات برای راستی‌آزمایی صحت برگه رأی است.
  - ارسال لیست کد-رأی‌های نشان‌دار به همراه E_{tally} و E_{open} به BB
  - تولید همه چالش‌های $\{\rho_E\}_{E\in E_{tally}}$ پروتکل‌های سیگما برای اعتبارسنجی تعهدهای موجود در E_{tally} و ارسال آن‌ها به BB (گام دوم پروتکل سیگما)
- استخراج چالش‌ها از تصادفی‌بودن مربوط به سکه‌اندازی رأی‌دهندگان

بیان سیستم پیشنهادی (ادامه)

- تهیه همه داده‌های پس‌حسابرسی $\{\phi_{2,E}\}_{E\in E_{tally}}$ پروتکل‌های سیگما برای اعتبارسنجی تعهدهای موجود در E_{tally}. (گام سوم پروتکل سیگما)
  - سه‌تایی داده پیش‌حسابرسی، چالش و پس‌حسابرسی برای تشکیل یک اثبات سیگمای کامل برای یک تعهد معتبر، به ازای هر تعهد در E_{tally}
- محاسبه شمارش آرا با استفاده از homomorphism
  - $E_{sum} = \prod_{E\in E_{tally}} E$
  - محاسبه (T, R)
    - T نتیجه انتخابات کدشده در مبنای N؛ تعهدشده با مقدارتصادفی R
    - R مجموعه همه مقادیر تصادفی استفاده‌شده در تعهدهای E_{tally} است.

بیان سیستم پیشنهادی (ادامه)

- بازکردن همه تعهدهای E_{open}
  - Open: مجموعه همه openningها
- ارسال Open، E_{sum} و (T, R) به BB
- در پایان، BB حاوی اطلاعات کد-رأی‌های نشان‌دار و اطلاعات زیر خواهد بود:

$$\text{Pub}, \left\{(C_{\ell,j}^{(a)}, t_{\ell,j}^{(a)})\right\}_{\ell\in[n],j\in[m]}^{a\in\{0,1\}}, (\mathbf{E}_{\text{tally}}, E_{\text{sum}}, (T,R)),$$

$$(\text{Open}, \mathbf{E}_{\text{open}}), \{\rho_E\}_{E\in\mathbf{E}_{\text{tally}}}, \{\phi_{2,E}\}_{E\in\mathbf{E}_{\text{tally}}}.$$

بیان سیستم پیشنهاد (ادامه)

- Result

- با استفاده از الگوریتم زیر، نتیجه کدشده انتخابات در T را می‌توان مشخص کرد.

Set $X \leftarrow T$;
For $j = 1, \ldots, m$:
- $x_j \leftarrow X \bmod (n+1)$;
- $X \leftarrow (X - x_j)/(n+1)$;

Return $\langle x_1, \ldots, x_m \rangle$;

بیان سیستم پیشنهادی (ادامه)

- Verify
  - رسید α به شکل $(tag, a, C, s^{(1-a)})$ تجزیه می‌شود.
  - نتیجه این الگوریتم برابر با یک خواهد بود اگر همه بررسی‌های زیر معتبر باشند:

۱) همه اطلاعات متعهدشده در گزارش عمومی T مربوط به n برگه رأی هستند، طبق tagهای جداگانه مرتب شده باشند و هیچ دو کد-رأی‌ای با tag مشابه، نشان 'voted' نداشته باشند.

بیان سیستم پیشنهادی (ادامه)

۲) اگر $\hat{C}$ یک کد-رأی موجود در بخش $\hat{s}^{(\hat{a})}$ از یک برگه رأی باشد و نشان 'voted' داشته باشد، فقط اطلاعات متعهدشده در بخش دیگر $\hat{s}^{(1-\hat{a})}$ از آن برگه رأی باز شده باشد.

۳) همه اثبات‌های سیگما مرتبط با تعهدهای موجود در E_{tally} معتبر باشند.

۴) $E_{sum} = \prod_{E \in E_{tally}} E$

بیان سیستم پیشنهادی (ادامه)

۵) همه openningهای تعهدها معتبر باشند.

۶) tag مربوط به رسید، برابر یکی از tag_lها ($l \in [n]$) باشد و $a = a_l$

۷) کد-رأی نشان‌دار و مربوط به tag_l (که در مرحله قبل مشخص شد)، همان C موجود در رسید باشد.

۸) تناظر بین کدشده کاندیدا و کد-رأی افشاشده در بازکردن تعهدهای $\{ U_{l,j}^{(1-a_l)}, E_{l,j}^{(1-a_l)} \}_{j \in [m]}$ (که l همان مقدار مشخص‌شده در مرحله ۶ است) برابر با همان قسمت در بخش $s^{(1-a)}$ باشد.

مثالی از سیستم پیشنهادی

- Referendum
  - P_1 = YES, P_2 = NO : candidates
  - $V_1;V_2;V_3$: voters

$$(C_{1,1}^{(0)} = 27935, C_{1,2}^{(0)} = 75218, C_{1,1}^{(1)} = 84439, C_{1,2}^{(1)} = 77396),$$
$$(C_{2,1}^{(0)} = 58729, C_{2,2}^{(0)} = 45343, C_{2,1}^{(1)} = 14582, C_{2,2}^{(1)} = 93484),$$
$$(C_{3,1}^{(0)} = 52658, C_{3,2}^{(0)} = 65864, C_{3,1}^{(1)} = 84373, C_{3,2}^{(1)} = 49251)$$

101	
27935	YES
75218	NO
84439	YES
77396	NO

102	
58729	YES
45343	NO
14582	YES
93484	NO

103	
52658	YES
65864	NO
84373	YES
49251	NO

مثالی از سیستم پیشنهادی (ادامه)

101	
$\mathsf{Com}_{\mathsf{ck}}(27935; t_{1,1}^{(0)})$ $\mathsf{Com}_{\mathsf{ck}}(75218; t_{1,2}^{(0)})$	$\mathsf{Com}_{\mathsf{ck}}(1; r_{1,1}^{(0)})$ $\mathsf{Com}_{\mathsf{ck}}(4; r_{1,2}^{(0)})$
$\mathsf{Com}_{\mathsf{ck}}(77396; t_{1,2}^{(1)})$ $\mathsf{Com}_{\mathsf{ck}}(84439; t_{1,1}^{(1)})$	$\mathsf{Com}_{\mathsf{ck}}(4; r_{1,2}^{(1)})$ $\mathsf{Com}_{\mathsf{ck}}(1; r_{1,1}^{(1)})$

(101,1,77396)	
27935	YES
75218	NO

(102, 1, 14582)	
58729	YES
45343	NO

(103, 0, 52568)	
84373	YES
49251	NO

$$E_{\text{sum}} = \mathsf{Com}_{\mathsf{ck}}(4; r_{1,2}^{(1)}) \cdot \mathsf{Com}_{\mathsf{ck}}(1; r_{2,1}^{(1)}) \cdot \mathsf{Com}_{\mathsf{ck}}(1; r_{3,1}^{(0)}) = \mathsf{Com}_{\mathsf{ck}}(6; r_{1,2}^{(1)} + r_{2,1}^{(1)} + r_{3,1}^{(0)})$$

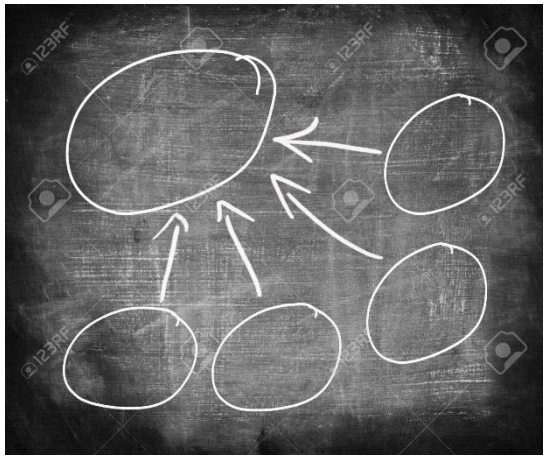
مثالی از سیستم پیشنهادی (ادامه)

101			
27935	YES	$(1, r_{1,1}^{(0)})$	$\mathsf{Com}_{\mathsf{ck}}(1; r_{1,1}^{(0)})$
75218	NO	$(4, r_{1,2}^{(0)})$	$\mathsf{Com}_{\mathsf{ck}}(4; r_{1,2}^{(0)})$
77396	VOTED		$\mathsf{Com}_{\mathsf{ck}}(4; r_{1,2}^{(1)})$
84439			$\mathsf{Com}_{\mathsf{ck}}(1; r_{1,1}^{(1)})$

Encodings	
YES	1
NO	4

جمع‌بندی

- بیان خواسته‌های امنیتی و تعریف انتخابات انتهابه‌انتها قابل راستی‌آزمایی
- بیان مزیت سیستم پیشنهادی نسبت به کارهای گذشته
- بیان جزئیات سیستم پیشنهادی



مسائل باز

- برآورده‌کردن خواسته‌های امنیتی دیگر
  - تغییر در طرح برای اضافه‌شدن خواسته‌های دیگر
- حذف تابلوی اعلانات
  - اهمیت حفظ امنیت تابلوی اعلانات
- بیان صوری قابلیت راستی‌آزمایی انتهابه‌انتها با رویکرد جدید
- کاهش پیچیدگی و افزایش کارایی طرح

پروژه کارشناسی ارشد

- اضافه‌کردن خواسته امنیتی جدید به سیستم موجود
  - مطالعه خواسته‌های امنیتی و تعیین محدودیت‌های اعمال هر یک
  - مطالعه کارهای موجود در برآورده‌سازی خواسته‌های امنیتی
  - امکان‌سنجی خواسته‌های امنیتی ممکن برای افزودن و انتخاب خواسته مورد نظر، طبق فرضیات و مشخصات سیستم پیشنهادی
  - طرح سیستم جدید برای خواسته‌های امنیتی جدید
  - اثبات درستی سیستم ارائه‌شده

منابع و مراجع

[۱] Kiayias, Aggelos, Thomas Zacharias, and Bingsheng Zhang. "End-to-end verifiable elections in the standard model." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 468-498. Springer Berlin Heidelberg, 2015.

[۲] Popoveniuc, Stefan, John Kelsey, Andrew Regenscheid, and Poorvi Vora. "Performance requirements for end-to-end verifiable elections." In Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections, pp. 1-16. USENIX Association, 2010.

[۳] Adida, Ben. "Helios: Web-based Open-Audit Voting." In USENIX Security Symposium, vol. 17, pp. 335-348. 2008.

[۴] Zagórski, Filip, Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, and Poorvi L. Vora. "Remotegrity: Design and use of an end-to-end verifiable remote voting system." In International Conference on Applied Cryptography and Network Security, pp. 441-457. Springer Berlin Heidelberg, 2013.

[۵] Kremer, Steve, Mark Ryan, and Ben Smyth. "Election verifiability in electronic voting protocols." In European Symposium on Research in Computer Security, pp. 389-404. Springer Berlin Heidelberg, 2010.

با سپاس از توجه شما! ☺