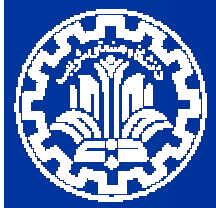
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف

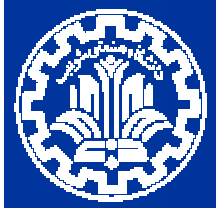
تحلیل صوری ویژگی وارسی‌پذیری میکس‌نت با استفاده از حساب پی کاربردی

بنیامین تختائی
حمیدرضا محروقی
رسول جلیلی

شهریورماه ۹۰



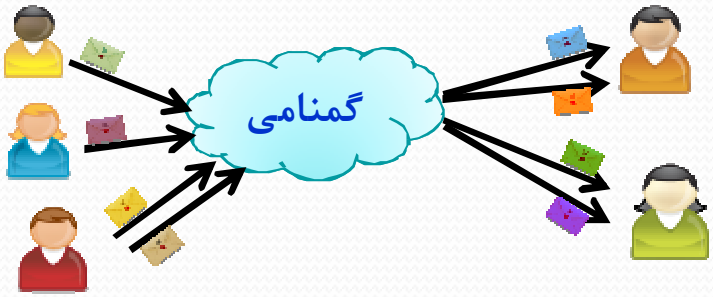
فهرست مطالب

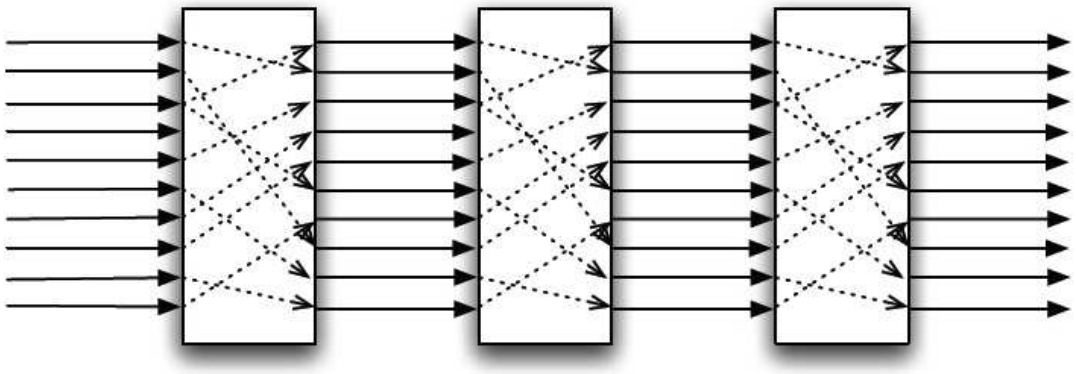


مقدمه

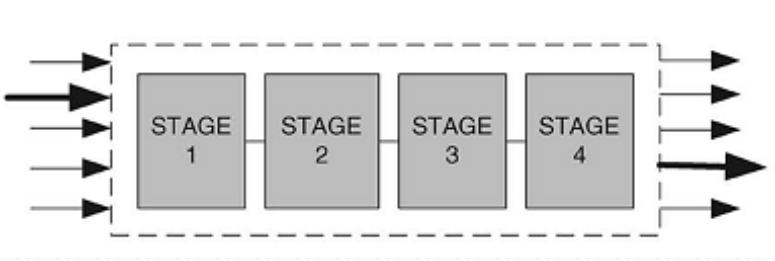
معرفی میکس‌نت - عملکرد

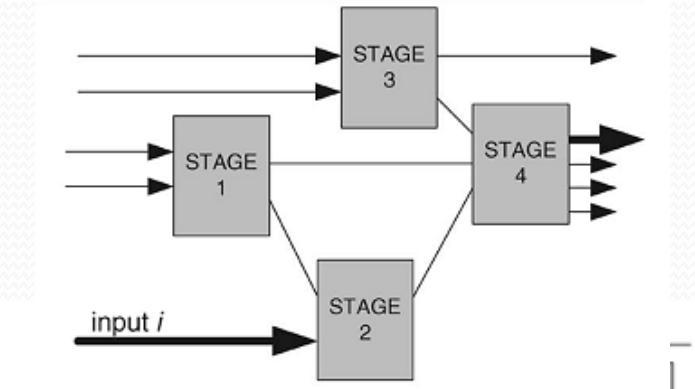
- ایجاد گمنامی به کمک رمزنگاری و جایگشت داده‌ها
  - شبکه‌ای از میکس‌ها
- سایر رویکردها
  - دی‌سی‌نت
  - مسیریابی پیازی
  - ...

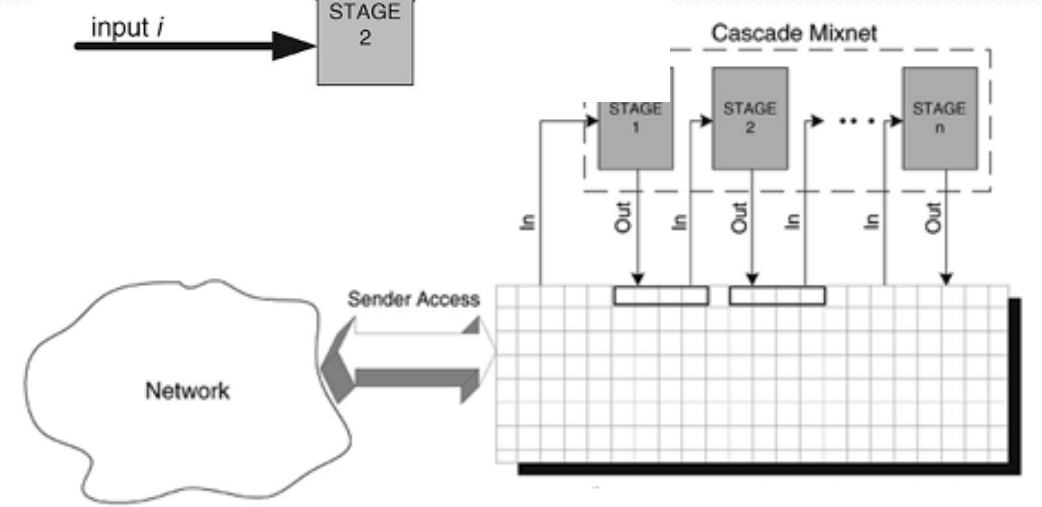




معرفی میکس‌نت (ادامه) – انواع



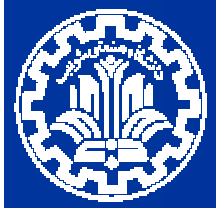




- تبدیل رمزنگاری
  - رمزگشا
  - رمزگذار مجدد
- توپولوژی
  - متوالی
  - جریان آزاد
- وارسی‌پذیر
- مبتنی بر تابلوی اعلانات

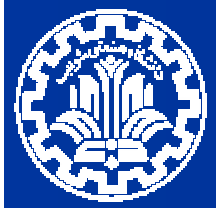
معرفی میکس‌نت (ادامه) - وارسی‌پذیری

- وارسی‌پذیری: امکان وارسی عملکرد میکس‌نت
  - فردی
  - عمومی
- رویکردهای اثبات
  - احتمالاتی: RPC
  - قطعی: میلی‌میکس
- آیا میکس‌نت واقعاً وارسی‌پذیر است؟
  - بررسی صحت ادعای وارسی‌پذیر بودن یک میکس‌نت
  - نیاز به تحلیل دقیق
    - یکی از رویکردها استفاده از روش‌های صوری است.



روش‌های صوری

- مبتنی بر ارائه‌ی یک توصیف و اثبات ریاضی
- مراحل
  - توصیف صوری پروتکل با دید انتزاعی
    - زبان‌های توصیف مبتنی بر منطق، جبر و ...
  - بیان ویژگی امنیتی
  - اثبات برقراری ویژگی در توصیف صوری
    - روش‌های اثباتی مبتنی بر وارسی مدل، اثبات قضیه
- حساب پی کاربردی
  - زبانی برای توصیف صوری پروتکل
  - از خانواده‌ی جبر فرآیند: CCS، Pi، و Applied Pi
  - توصیف شرکت‌کنندگان در پروتکل در قالب فرآیند
  - قابلیت تعریف توابع رمزنگاری دلخواه



حساب پی کاربردی

- نحو
  - ترم‌ها
    - نام‌ها، متغیرها، توابع
  - نظریه‌های هم‌ارزی
    - تعریف صوری توابع رمزنگاری و روابط آن‌ها
  - فرآیندها
    - توصیف رفتار شرکت‌کنندگان در پروتکل
- معناشناسی
  - تساوی ساختاری
  - کاهش داخلی
  - کاهش برچسب‌دار

$L, M, N, T, U, V ::=$

$a, b, c, k, m, n, s, t, r, \ldots$	name
x, y, z	variable
$g(M_1, \ldots, M_l)$	function

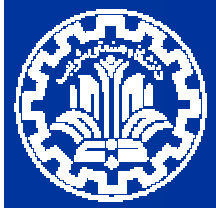
```
sdec(x, senc( x ,y) )   =   y
dec(x, enc(pk(x),y) )   =   y
checksign( pk(x), y, sign(x,y) )   =   ok
```

$P, Q, R ::=$ processes

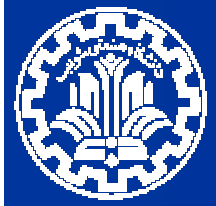
0	null process
$P \mid Q$	parallel comp.
$!P$	replication
$\nu\, n.P$	name restriction
$u(x).P$	message input
$\overline{u}\langle M\rangle.P$	message output
if $M = N$ then P else Q	cond'nl

$A, B, C ::=$ extended processes

P	plain process
$A \mid B$	parallel comp.
$\nu\, n.A$	name restriction
$\nu\, x.A$	variable restriction
$\{^M/_x\}$	active substitution



توصیف صوری وارسی‌پذیری میکس‌نت



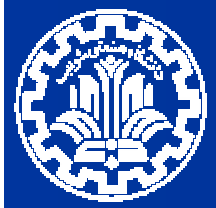
کارهای مرتبط

- تحلیل ویژگی‌های متنوع امنیتی
  - حریم خصوصی، گمنامی، وارسی‌پذیری
- میکس‌نت
  - بررسی گمنامی میکس‌نت با زبان CSP
    - عدم توجه به وارسی‌پذیری

B. Wolff et. al, "**Towards a Formal Analysis of a Mix Network**," Technical Report 171, Albert-Ludwigs-Universität Freiburg, 2002

  - ویژگی وارسی‌پذیری
    - عدم توجه به ساختار داخلی میکس‌نت

S. Kremer, M. Ryan, and B. Smyth , "**Election verifiability in electronic voting protocols**," *Computer Security–ESORICS 2010*



توصیف صوری میکس‌نت

- ویژگی‌های میکس‌نت مورد بررسی
  - وارسی‌پذیر، متوالی، مبتنی بر تابلوی اعلانات
- تعریف چارچوبی برای فرآیند مخلوط‌سازی
  - کاربران، میکس‌نت، مرجع مورد اعتماد، و گیرنده
- فرآیند مخلوط‌سازی: سه‌تایی $\langle Mixnet, U, T \rangle$
  - میکس‌نت Mixnet
  - کاربر U
  - مرجع T

$$MixProcess_n(d_1, \ldots d_n) = Mixnet[U_1 \mid \ldots \mid U_n \mid T]$$

$$Mixnet = \nu c, a, b.(\_ \mid M)$$

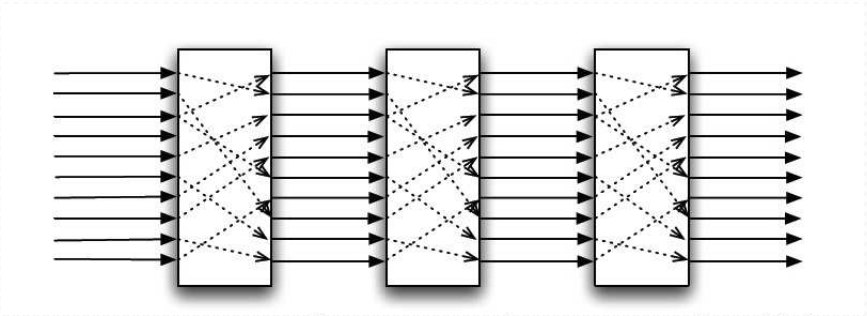
$$U \triangleq c(pk_{server}).\ a(id)\ .\ \nu\ r\ .\ \overline{b}\left\langle id, \mathrm{penc}(pk_{server}, r, m)\right\rangle$$

$$T \triangleq\ \nu\ sk_{server}\ .\ \overline{c}\left\langle \mathrm{pk}(sk_{server})\right\rangle .\ (!(\nu\ id_u\ .\ \overline{a}\left\langle id_u\right\rangle .\ \overline{c}\left\langle id_u\right\rangle) \mid BB)$$

بیان صوری ویژگی وارسی‌پذیری

- وارسی‌پذیری به معنای ارائه‌ی آزمون (اثباتی) درستی عملکرد است.
- وارسی‌پذیری در میکس‌نت‌های رمزگذار مجدد
  - یک میکس‌نت رمزگذار مجدد وارسی‌پذیر است هرگاه نشان دهد

برای تمام مراحل mix_i جایگشت π وجود دارد که $\forall j \leq n : C_{j,i} = \mathrm{renc}(C_{\pi(j),i-1})$



- تعریف هم‌مقداری دو دسته داده $\tilde{T} \leftrightarrows \tilde{T}'$
  - جایگشتی از یک‌دیگر
  - رمزشده‌ی داده‌های یکسان

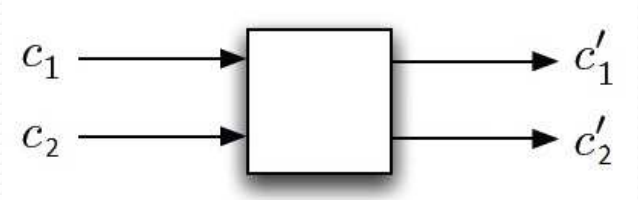
- بیان صوری وارسی‌پذیری
  - برای فرآیند مخلوط‌سازی با داده‌های خروجی $\tilde{u}$ ، آزمون یا اثبات Φ با شرایط زیر قابل طراحی باشد:
    ۱. آزمون Φ در گزاره‌ی زیر صدق نماید:

$$\Phi\sigma \wedge \Phi\{\tilde{u}'/\tilde{u}\}\sigma \Rightarrow \tilde{u}\sigma \overset{\leftrightarrow}{\simeq} \tilde{u}'\sigma$$

    ۲. برای حداقل یک اجرای فرآیند مخلوط‌سازی، آزمون Φ برقرار باشد.

- منطبق بر تعریف شهودی وارسی‌پذیری
  - شرط دوم: اثبات میکس‌نت برای داده‌های خروجی صحیح (عملکرد صحیح) برقرار است.
  - شرط اول: اثبات میکس‌نت فقط برای «هم‌مقدارهای خروجی صحیح» برقرار است.

مطالعه‌ی موردی: میلی‌میکس

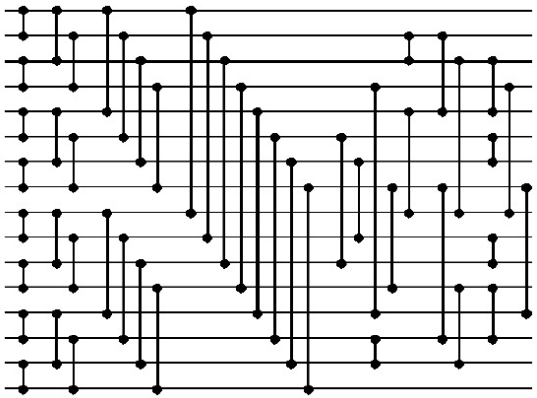


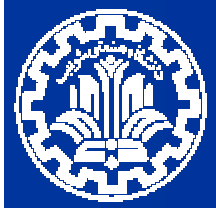
- مبتنی بر ساختار شبکه‌ی مقایسه‌گر
- وارسی‌پذیری مقایسه‌گر با اثبات قطعی
  - اثبات هیچ‌آگاهی PEP
    - Plaintext Equivalence Proof
  - اثبات هیچ‌آگاهی DISPEP
    - Disjunctive PEP
- ایجاد یک شبکه‌ی مخلوط‌ساز بر مبنای مقایسه‌گر

$$(m_1, m_2) = (m'_1, m'_2) \vee (m_1, m_2) = (m'_2, m'_1)$$

$$\text{DISPEP}\quad m_1 = m'_1 \vee m_1 = m'_2$$

$$\text{PEP}\quad m_1 m_2 = m'_1 m'_2$$





میلی‌میکس: توصیف صوری

- توابع و نظریه‌های هم‌ارزی
  - رمزنگاری متقارن، رمزگذاری مجدد، ترکیب هم‌ریخت
  - اثبات هیچ‌آگاهی PEP
  - اثبات هیچ‌آگاهی DISPEP

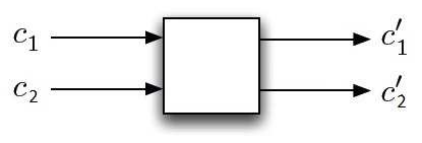
$$\Sigma = \{\mathrm{ok}, \mathrm{fst}, \mathrm{snd}, \mathrm{pair}, \oplus, \otimes, \odot, \mathrm{pk}, \mathrm{penc}, \mathrm{renc},$$
$$\mathrm{pepPf}, \mathrm{checkPepPf}, \mathrm{dispepPf}, \mathrm{checkDispepPf}\}$$

$$\mathrm{checkPepPf}(c, \mathrm{renc}(r, c), \mathrm{pepPf}(c, \mathrm{renc}(r, c), r)) = \mathrm{ok}$$

$$\mathrm{checkDispepPf}(c_1, c_2, \mathrm{renc}(r_1, c_1), \mathrm{dispepPf}(c_1, c_2, \mathrm{renc}(r_1, c_1), r_1)) = \mathrm{ok}$$
$$\mathrm{checkDispepPf}(c_1, c_2, \mathrm{renc}(r_2, c_2), \mathrm{dispepPf}(c_1, c_2, \mathrm{renc}(r_2, c_2), r_2)) = \mathrm{ok}$$

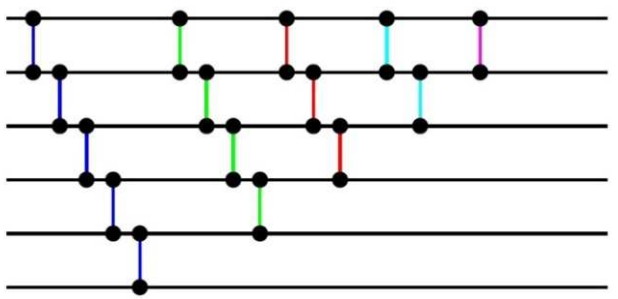
میلی‌میکس: توصیف صوری (ادامه)

- توصیف مقایسه‌گر
  - تولید اثبات PEP
  - تولید اثبات DISPEP
    - به کارگیری عملگر انتخاب غیرقطعی
- توصیف میکس‌نت میلی‌میکس
  - توصیف بازگشتی



$$
\begin{aligned}
&comparator \triangleq \\
&\quad \nu\, r_1 . \nu\, r_2 . comp(c_1) . comp(c_2) . \\
&\quad \text{let } c_1' = \text{renc}(r_1, c_1) \text{ in} \\
&\quad \text{let } c_2' = \text{renc}(r_2, c_2) \text{ in} \\
&\quad \text{let } pep = \text{pepPf}(c_1 \odot c_2, c_1' \odot c_2', r_1 \oplus r_2) \text{ in} \\
&\quad (\ \text{let } dispep = \text{dispepPf}(r_1, c_1, c_2, c_1') \text{ in} \\
&\qquad \overline{cm}\langle\!\langle c_1, c_2, c_1', c_2', pep, dispep \rangle\!\rangle + \\
&\quad\ \text{let } dispep = \text{dispepPf}(r_2, c_1, c_2, c_2') \text{ in} \\
&\qquad \overline{cm}\langle\!\langle c_1, c_2, c_2', c_1', pep, dispep \rangle\!\rangle\ )
\end{aligned}
$$

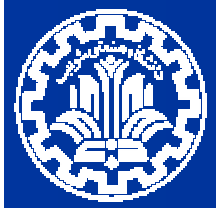
$$
\begin{aligned}
&millimix_n \triangleq \\
&\quad mixIn(c) . \\
&\quad \overline{cm}\langle \pi_1(c) \rangle . \overline{cm}\langle \pi_2(c) \rangle . cm(o_1) . \\
&\quad \overline{cm}\langle \pi_4(o_1) \rangle . \overline{cm}\langle \pi_3(c) \rangle . cm(o_2) . \\
&\quad \vdots \\
&\quad \overline{cm}\langle \pi_4(o_{n-2}) \rangle . \overline{cm}\langle \pi_n(c) \rangle . cm(o_{n-1}) . \\
&\quad \bar{b}\langle\!\langle o_1, o_2, \cdots, o_n \rangle\!\rangle . \\
&\quad (mixIn(\ \langle\!\langle \pi_3(o_1), \ldots, \pi_3(o_{n-1}) \rangle\!\rangle\ ) \mid millimix_{n-1}\ ) . \\
&\quad \bar{b}\langle \pi_4(o_{n-1}) \rangle .
\end{aligned}
$$



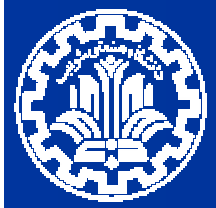
- ارائه‌ی آزمون وارسی‌پذیری برای میلی‌میکس

$$\Phi \triangleq \bigwedge_{i=1}^{n-1}(c_{i+1} = \pi_2(P_{i,n-1})) \wedge c_1 = \pi_1(P_{1,n-1})$$
$$\bigwedge_{i=1}^{n-1}(\pi_4(P_{i,i}) = u_{i+1}) \wedge \pi_3(P_{1,1}) = u_1$$
$$\bigwedge_{j=1}^{n-1}\bigwedge_{i=1}^{j}(\text{checkPepPf}(\pi_5(P_{i,j})) = \text{checkDispepPf}(\pi_6(P_{i,j})) = ok)$$
$$\bigwedge_{j=1}^{n-2}\bigwedge_{i=2}^{j}(\pi_1(P_{i,j}) = \pi_4(P_{i-1,j}) \wedge \pi_2(P_{i,j}) = \pi_3(P_{i+1,j+1}))$$
$$\bigwedge_{i=1}^{n-2}(\pi_1(P_{1,i}) = \pi_4(P_{1,i+1}) \wedge \pi_2(P_{1,i}) = \pi_3(P_{i+1,j+1}))$$

- اثبات برقراری شرایط مورد نیاز این آزمون برای $n = 2$
  - شرط اول: استنتاج حکم $\tilde{u} \overset{\leftrightarrow}{\simeq} \tilde{u}'$ از نظریه‌های هم‌ارزی
  - شرط دوم: صورت عملکرد صحیح میلی‌میکس بدیهی است.



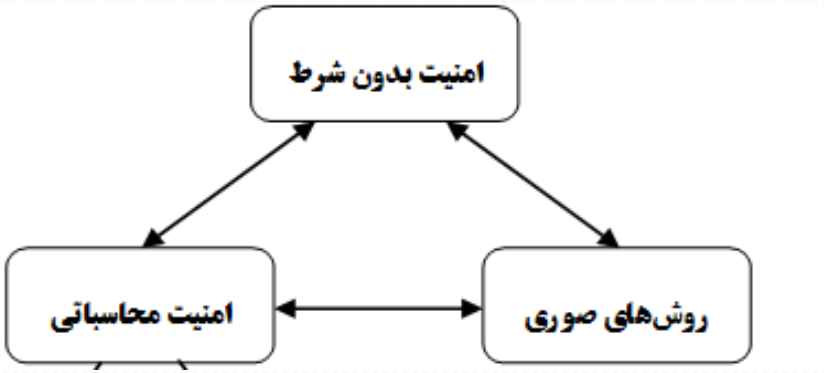
جمع‌بندی و سوی کارهای آتی



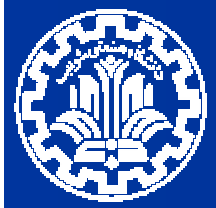
جمع‌بندی

- تعریف صوری فرآیند مخلوط‌سازی
- بیان صوری ویژگی وارسی‌پذیری
- بررسی میلی‌میکس به عنوان مطالعه‌ی موردی
  - توصیف صوری پروتکل میلی‌میکس
  - اثبات صوری ویژگی وارسی‌پذیری

کارهای آتی



- اثبات وارسی‌پذیری در فضای محاسباتی
  - کامل نبودن رویکرد صوری
    - امنیت قابل اثبات
      - تئوری اطلاعاتی (بدون شرط)
      - امنیت محاسباتی
      - روش‌های صوری
  - امکان ارائه‌ی حمله در فضای محاسباتی علیه میلی‌میکس
  - تلاش برای پرکردن شکاف میان امنیت محاسباتی و روش‌های صوری
- تحلیل گمنامی میکس‌نت‌های وارسی‌پذیر
  - در نظر گرفتن تاثیرات جانبی ویژگی وارسی‌پذیری
- تحلیل میکس‌نت‌های وارسی‌پذیر با اثبات احتمالاتی
  - استفاده از حساب پی کاربردی احتمالاتی



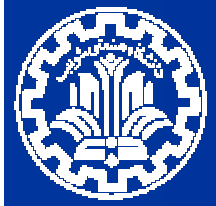
مراجع

[1] K. Sampigethaya and R. Poovendran, "**A survey on mix networks and their secure applications**," *Proceedings of the IEEE*, vol. 94, 2006, p. 2142–2181.

[2] M. Abadi and C. Fournet, "**Mobile values, new names, and secure communication,**" *ACM SIGPLAN Notices*, vol. 36, 2001, pp. 104-115.

[3] S. Kremer, M. Ryan, and B. Smyth, "**Election verifiability in electronic voting protocols**," *Computer Security–ESORICS 2010*, 2011, p. 389–404

[4] M. Jakobsson and A. Juels, "**Millimix: Mixing in small batches**," *DIMACS Techical report*, 1999, p. 99–33



با تشکر از توجه شما ...

سوال؟!