رمزگذاری جست‌وجوپذیر نامتقارن

محمدحسن عامری اختیار آبادی

دانشکده مهندسی برق– دانشگاه صنعتی شریف

Ameri_mohammadhasan@ee.sharif.edu

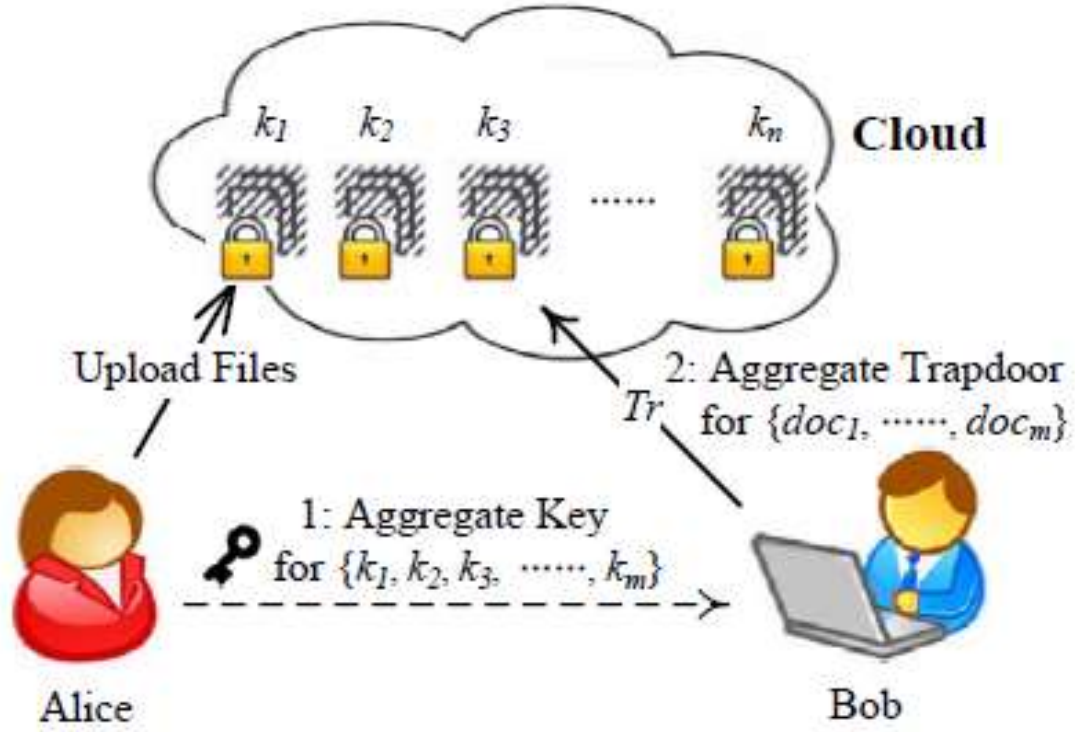
چشم‌انداز

- مقدمه
  - اهداف استفاده از الگوریتم‌های رمزگذاری جست‌وجوپذیر نامتقارن
  - تاریخچه‌ی مختصری از رمزنگاری جست‌وجوپذیر نامتقارن
  - انواع الگوریتم‌های رمزگذاری جست‌جوپذیر نامتقارن
- رمزگذاری جست‌وجوپذیر کلید عمومی
  - مبتنی بر زیرساخت کلید عمومی
  - شناسه بنیاد
- رمزگذاری ویژگی‌بنیاد
- رمزگذاری جست‌وجوپذیر ویژگی‌بنیاد
- نتیجه‌گیری

رمزگذاری جست‌وجوپذیر نامتقارن

چرا الگوریتم‌های رمزگذاری جست‌وجوپذیر نامتقارن

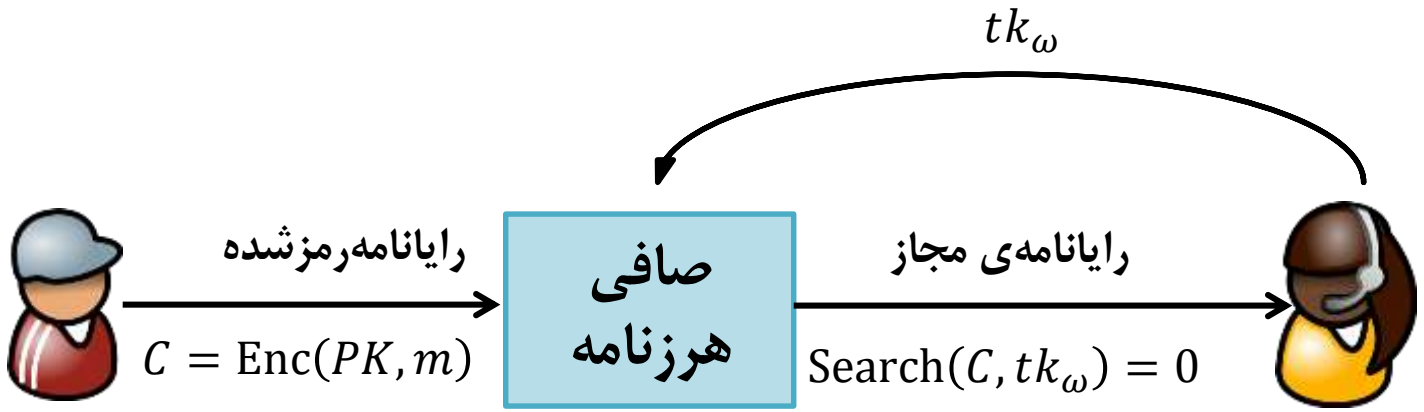
- اشتراک گذاری اطلاعات به صورت جست‌وجوپذیر
  - مبتنی بر رمزگذاری متقارن: نیاز به الگوریتم‌های مدیریت کلید



[Cui et al. 14]

چرا الگوریتم‌های رمزگذاری جست‌وجوپذیر نامتقارن (ادامه)

- طراحی صافی هرزنامه



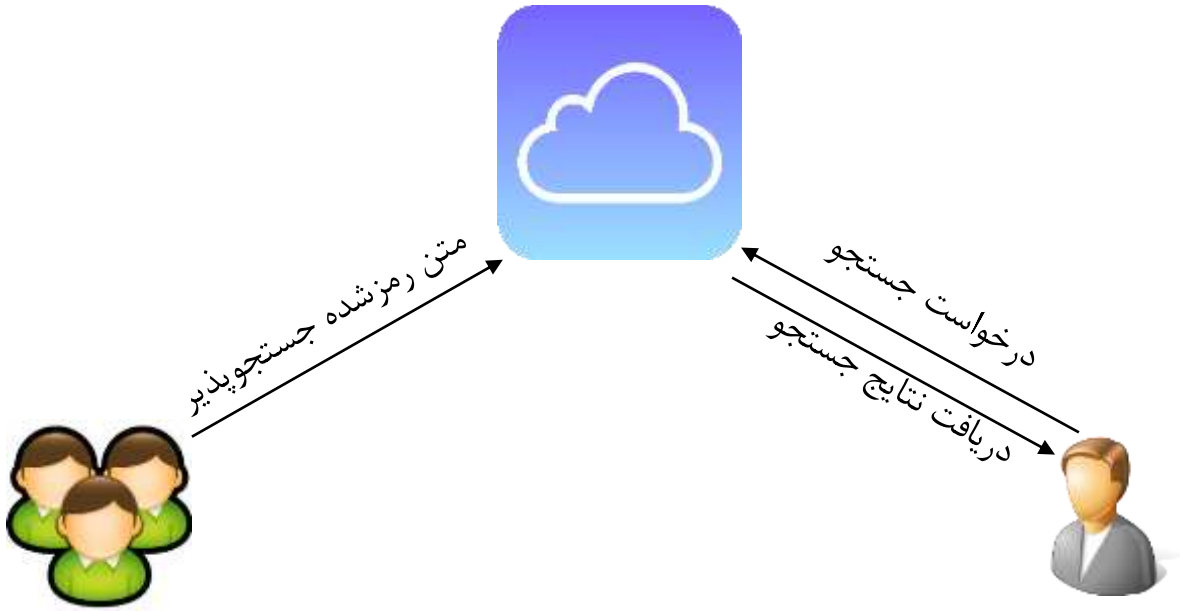
[Boneh, Sahai, Waters 12]

تاریخچه

- اولین طرح رمزگذاری جست‌وجو پذیر مبتنی بر کلید عمومی [Boneh et al.04]
- معرفی رمزگذاری جستجوپذیر شناسه بنیاد [Abdalla et al.05]
- حمله‌ی حدس کلمات کلیدی [Byun et al.06]
- ارائه‌ی طرح‌های مقاوم در مقابل حمله‌ی حدس کلمات کلیدی [Xu et al.13]
- رمزگذاری جست‌وجوپذیر ویژگی بنیاد [Zheng et al.14]
- طرح‌هایی در جهت رفع انتظارات ما از رمزگذاری جست‌وجوپذیر
- جست‌وجوی چندواژه‌ای [Miao et al.16]
- جست‌وجوی رتبه بندی شده [Hu et al.15]
- قابلیت به روز رسانی [Sun et al.16]

انواع الگوریتم‌های جستجوپذیر نا متقارن

- رمزگذاری جست‌وجوپذیر مبتنی بر زیرساخت کلید عمومی
- رمزگذاری جست‌وجوپذیر شناسه‌بنیاد
- رمزگذاری جست‌وجوپذیر ویژگی‌بنیاد



ساختار رمزگذاری جست‌وجوپذیر کلید عمومی

رمزگذاری جست‌وجوپذیر مبتنی بر زیرساخت کلید عمومی [Boneh et al.04]

مرجع صدور گواهی برای کلید عمومی

تولید متن رمزشده‌ی
جست‌وجو پذیر و انبارش آن

بابک

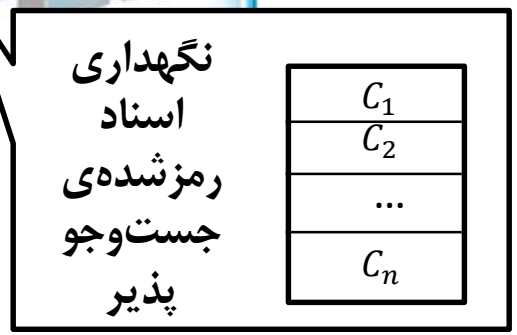
بهروز

کلید عمومی آذر

آذر

تولید و ارسال نشان جست‌وجو

ارسال نتیجه‌ی جست‌وجو



ویژگی‌های الگوریتم رمزگذاری جست‌وجوپذیر مبتنی بر زیرساخت کلید عمومی

۱. ارائه دهنده‌ی یک ساختار چند مالک داده‌ای

۲. عدم نیاز به استفاده از الگوریتم‌ها و پروتکل‌های توافق کلید

۳. نیاز برخط جهت وارسی گواهی صادر شده برای کلید عمومی

۴. هدف: حذف نیاز به وارسی گواهی مربوط به کلید عمومی

رمزگذاری شناسه بنیاد

- معرفی مفهوم رمزگذاری شناسه بنیاد [Shamir 84]
- ساخت و طراحی اولین نمونه‌ی عملی با استفاده از نگاشت دوخطی [Boneh-Franklin 01]
- حذف نیاز برخط برای وارسی گواهی کلید عمومی

رمزگذاری جست‌وجوپذیر شناسه بنیاد [Abdalla et al.05]

- برپاسازی
- تولید کلید خصوصی
- رمزگذاری
- تولید نشان جست‌وجو
- جست‌وجو

نهادهای شرکت کننده

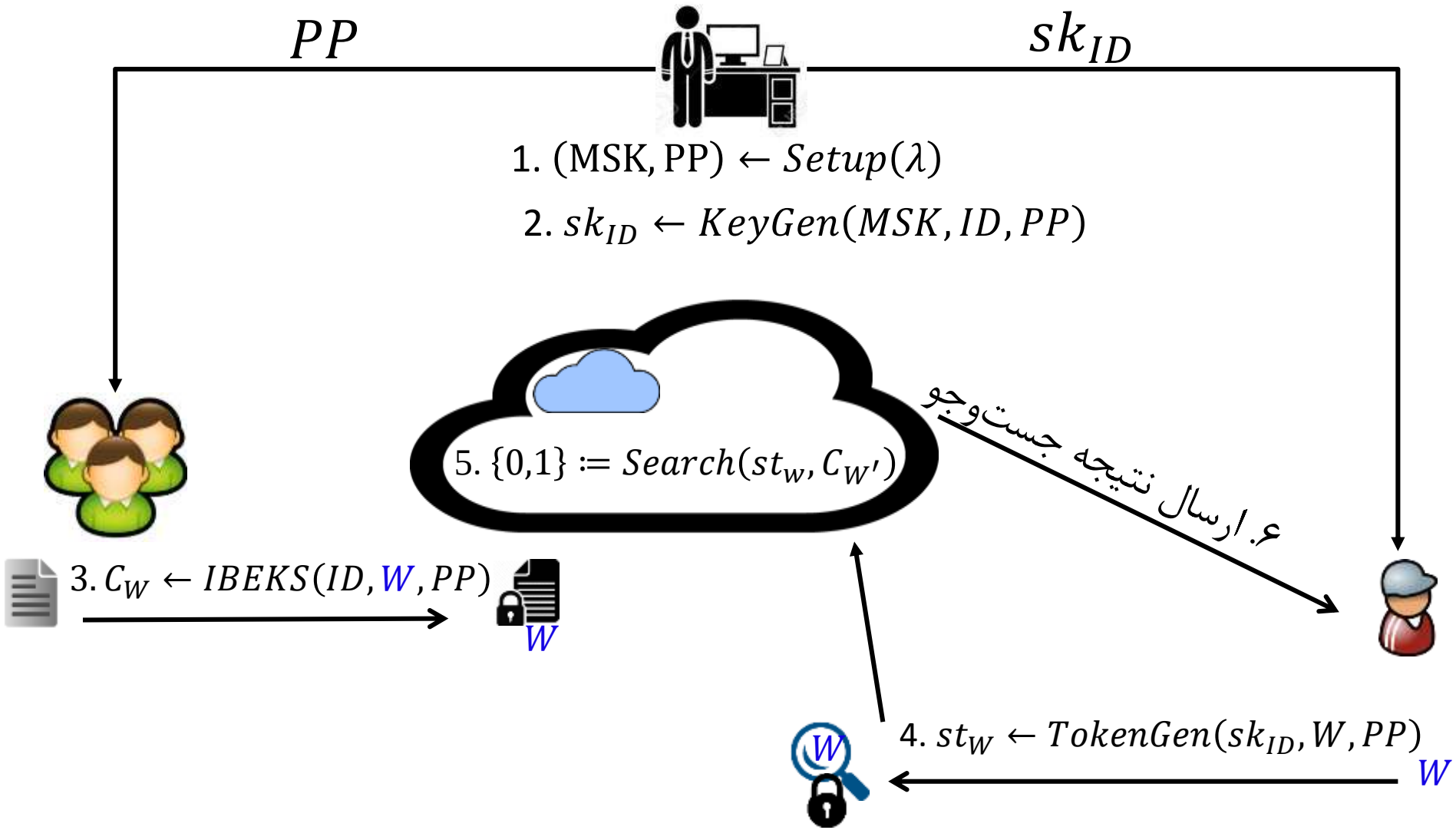

مرکز تولید کلید


کاربر داده


مالک داده

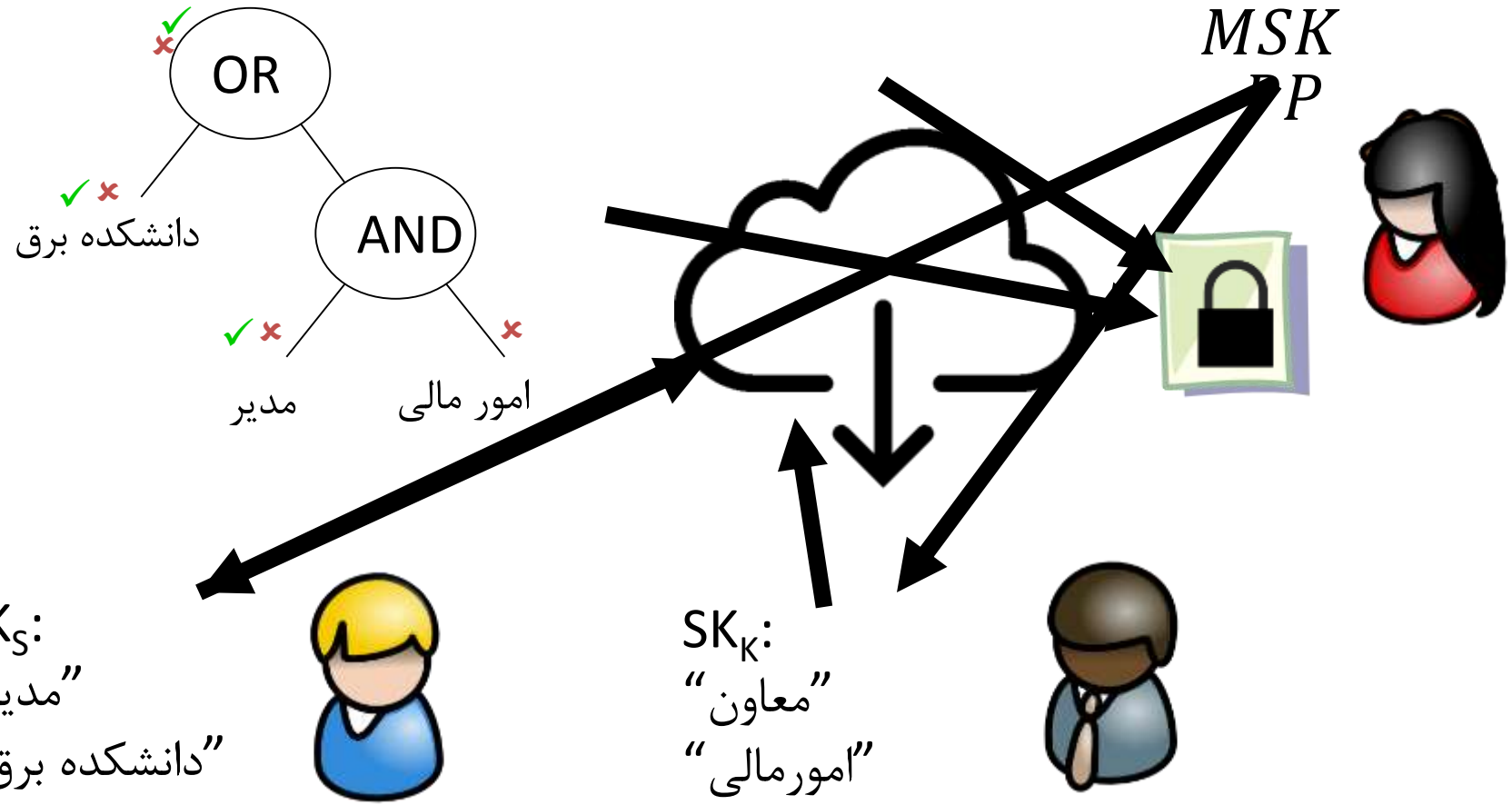

مجموعه‌ی ابری

رمزگذاری جست‌وجوپذیر شناسه بنیاد



ساختار رمزگذاری ویژگی‌بنیاد

رمزگذاری ویژگی‌بنیاد [Goyal, Pandey, Sahai, Waters 06]



رمزگذاری جست‌وجوپذیر ویژگی‌بنیاد وارسی پذیر

رمزگذاری جست‌وجوپذیر ویژگی بنیاد وارسی پذیر (VABKS*)[Zheng et al.14]

۱. تولید شاه کلید خصوصی و پارامترهای عمومی
۲. انتشار پارامترهای عمومی سامانه

$$(msk, pp) \leftarrow Setup(\lambda)$$

برپاسازی

تولید کلید
رمزگذاری
تولید نشان
جست‌وجو
وارسی

* Verifiable Attribute-based Keyword Search (VABKS)

رمزگذاری جست‌وجوپذیر ویژگی بنیاد وارسی پذیر(ادامه)

برپاسازی

تولید کلید

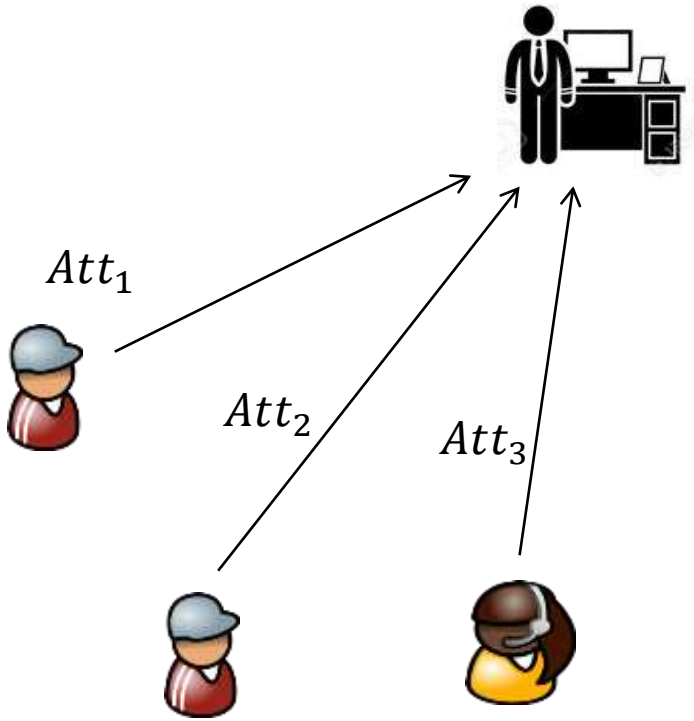
رمزگذاری

تولید نشان

جست‌وجو

وارسی

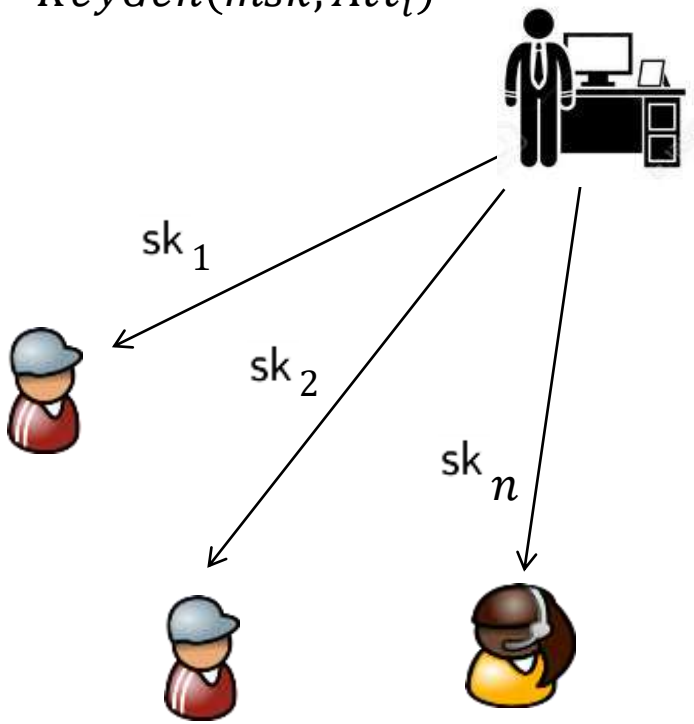
احراز اصالت جهت دریافت کلید خصوصی



رمزگذاری جست‌وجوپذیر ویژگی بنیاد وارسی پذیر(ادامه)

دریافت کلید خصوصی از طریق کانال احراز اصالت شده

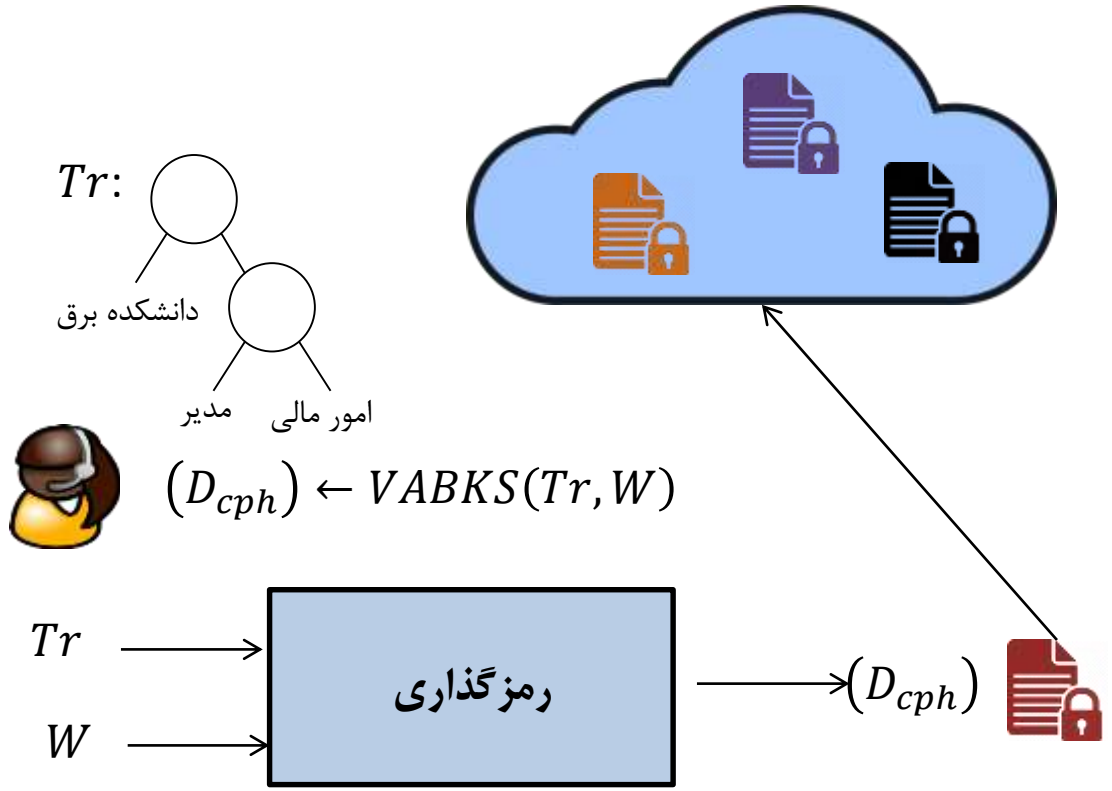
$$sk_i \leftarrow KeyGen(msk, Att_i)$$



- برپاسازی
- تولید کلید
- رمزگذاری
- تولید نشان
- جست‌وجو
- وارسی

رمزگذاری جست‌وجوپذیر ویژگی بنیاد وارسی پذیر(ادامه)

تولید متن رمزشده‌ی جست‌وجو پذیر و انبارش آن در ابر



- برپاسازی
- تولید کلید
- رمزگذاری
- تولید نشان
- جست‌وجو
- وارسی

رمزگذاری جست‌وجوپذیر ویژگی بنیاد وارسی پذیر(ادامه)

برپاسازی

تولید کلید

رمزگذاری

تولید نشان

جست‌وجو

وارسی

تولید نشان جست‌وجو و ارسال آن برای مجموعه‌ی ابری

$st_\omega \leftarrow TokenGen(sk, W)$

sk

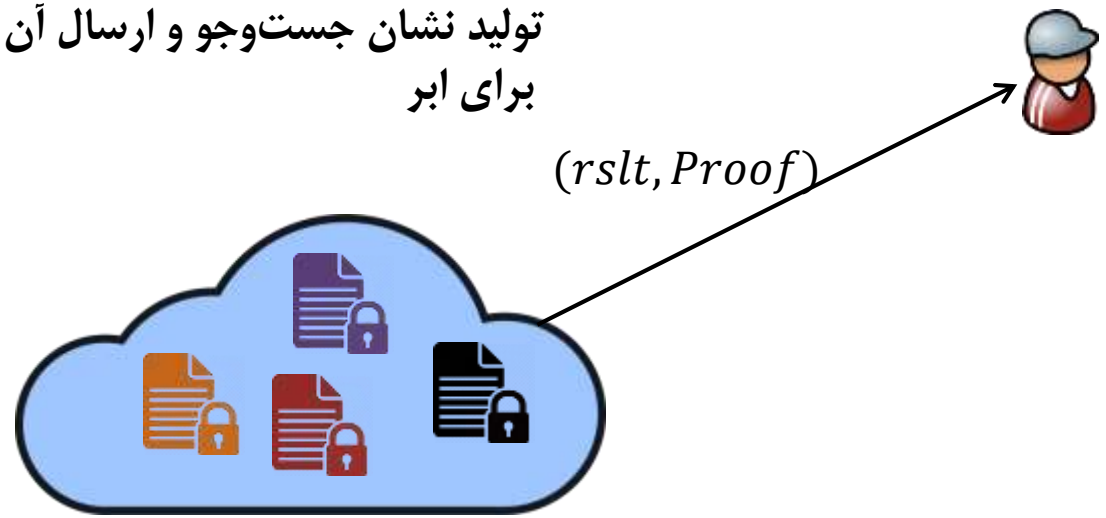
W

تولید دریچه‌ی جستجو

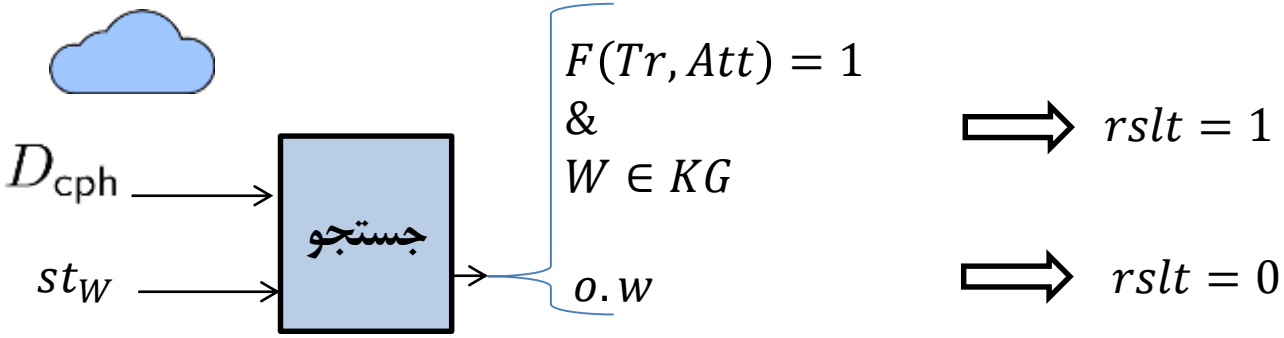
st_ω

رمزگذاری جست‌وجوپذیر ویژگی بنیاد وارسی پذیر(ادامه)

تولید نشان جست‌وجو و ارسال آن برای ابر



$$(rslt, proof) \leftarrow Search(D_{\text{cph}}, st_W)$$



- برپاسازی
- تولید کلید
- رمزگذاری
- تولید نشان

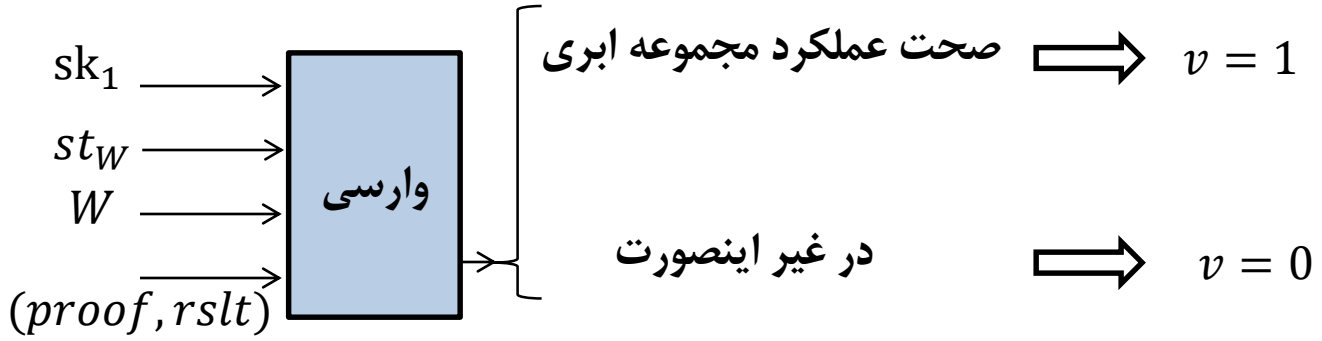
جست‌وجو

- وارسی

رمزگذاری جست‌وجوپذیر ویژگی بنیاد وارسی پذیر(ادامه)

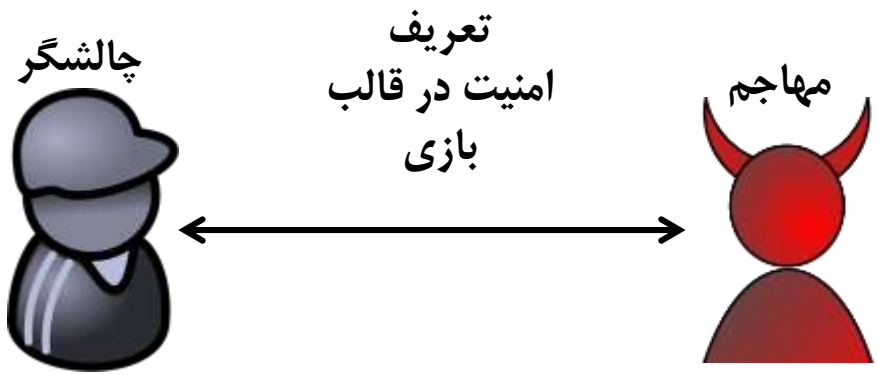
وارسی صحت عملکرد ابر
در هنگام جست‌وجو

$$\{0,1\} = Verify(sk_1, st_W, W, (proof, rslt))$$



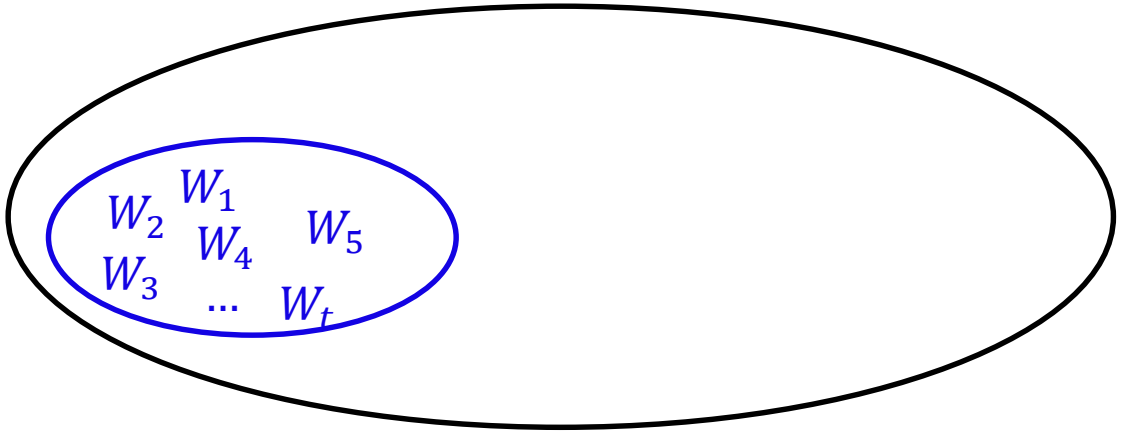
رمزگذاری جست‌وجوپذیر ویژگی بنیاد وارسی پذیر(ادامه)

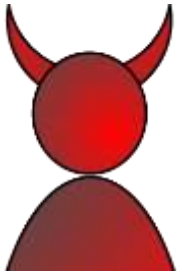
- محرمانگی کلمه‌ی کلیدی
  - یافتن کلمه‌ی کلیدی متناظر با یک متن رمزشده با دانستن یک نشان معتبر
- امنیت در مقابل حمله کلمات کلیدی منتخب
  - هدف: عدم تمایز بین رمزشده‌ی دوکلمه‌ی کلیدی
- محرمانگی نشان
  - عدم تشخیص اختصاص دو نشان به یک کلمه
- وارسی پذیری
  - هدف: عدم امکان تولید نتیجه‌ی جست‌وجوی اشتباه به همراه یک تضمین معتبر



حمله‌ی حدس کلمات کلیدی [Byun et al.06]

«در عمل تعداد کلمات کلیدی جستجو محدود هستند»





st_{W^*}

$$C_1 = IBEKS(ID, W_1, PP)$$

$$C_2 = IBEKS(ID, W_2, PP)$$

$$\vdots$$

$$C_i = IBEKS(ID, W_i, PP)$$

$$\vdots$$

$$C_{W^*} = IBEKS(ID, W^*, PP)$$

$$\vdots$$

$$C_t = IBEKS(ID, W_t, PP)$$

$$1 := Search(st_{W^*}, C_{W^*})$$

$$0 := Search(st_{W^*}, C_i)$$

نتیجه گیری

جمع‌بندی و نتیجه‌گیری

- معرفی رمزسامانه‌های رمزگذاری جست‌وجوپذیر نامتقارن
- آشنایی با کنترل دسترسی در سامانه‌های جست‌وجوپذیر و چالش‌های امنیتی آن
  - حفظ محرمانگی کلمات کلیدی رمزشده
  - حمله‌ی حدس کلمات کلید در سامانه‌های رمزنگاری جستجوپذیر نامتقارن
  - وارسی پذیری
  - خاصیت محرمانگی نشان جست‌وجو
- چالش‌ها
  - رتبه بندی امن در نتایج حاصل از جست‌وجو در الگوریتم‌های رمز جست‌وجوپذیر ویژگی بنیاد
  - بررسی جنبه‌های عملی طرح ارائه شده
  - ارائه‌ی طرح‌های رمزگذاری جست‌وجوپذیر با خاصیت جست‌جوی فازی
  - ارتقای امنیت طرح‌های رمزگذاری جستجت‌وجوپذیر در مقابل حمله‌ی حدس کلمات کلیدی

مراجع

[Cui et al. 14] Cui, B., Liu, Z., & Wang, L. (2014). Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud. *IEEE TRANSACTIONS ON COMPUTERS*, *6*(1), 1.

[Boneh, Sahai, Waters 12] Boneh, Dan, Amit Sahai, and Brent Waters. "Functional encryption: a new vision for public-key cryptography." *Communications of the ACM* 55.11 : 56-64, 2012.

[Xu et al.13] Xu, Peng, Hai Jin, Qianhong Wu, and Wei Wang. "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack." *IEEE Transactions on computers* 62, no. 11 (2013): 2266-2277.

[Zheng et al.14] Zheng, Qingji, Shouhuai Xu, and Giuseppe Ateniese. "VABKS: verifiable attribute-based keyword search over outsourced encrypted data." In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp. 522-530. IEEE, 2014.

[Miao et al.16] Miao, Yinbin, Jianfeng Ma, Ximeng Liu, Fushan Wei, Zhiquan Liu, and Xu An Wang. "m2-ABKS: Attribute-Based Multi-Keyword Search over Encrypted Personal Health Records in Multi-Owner Setting." *Journal of medical systems* 40, no. 11 (2016): 246.

[Hu et al.15] Hu, Chengyu, Bo Yang, and Pengtao Liu. "Multi-keyword ranked searchable public-key encryption." *International Journal of Grid and Utility Computing* 6, no. 3-4 (2015): 221-231.

[Sun et al.16] Sun, Wenhai, Shucheng Yu, Wenjing Lou, Y. Thomas Hou, and Hui Li. "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud." *IEEE Transactions on Parallel and Distributed Systems* 27, no. 4 (2016): 1187-1198.

مراجع

[Sharim 84] Shamir, Adi. "Identity-based cryptosystems and signature schemes." In *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47-53. Springer Berlin Heidelberg, 1984.

[Bone-Franklin01] Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." In *Annual International Cryptology Conference*, pp. 213-229. Springer Berlin Heidelberg, 2001.

[Goyal et al.06] Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89-98. Acm, 2006.

با تشکر از توجه شما