



انجمن رمزایران

بسم الله الرحمن الرحيم



قطب علمی رمز

مروری بر محصولات موجود در زمینه برون سپاری امن داده

جواد قره چمنی

دانشکده کامپیوتر - دانشگاه صنعتی شریف

gharehchamani@ce.sharif.edu

پژوهشکده پارسا شریف

چشم انداز

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری



بیان مسئله

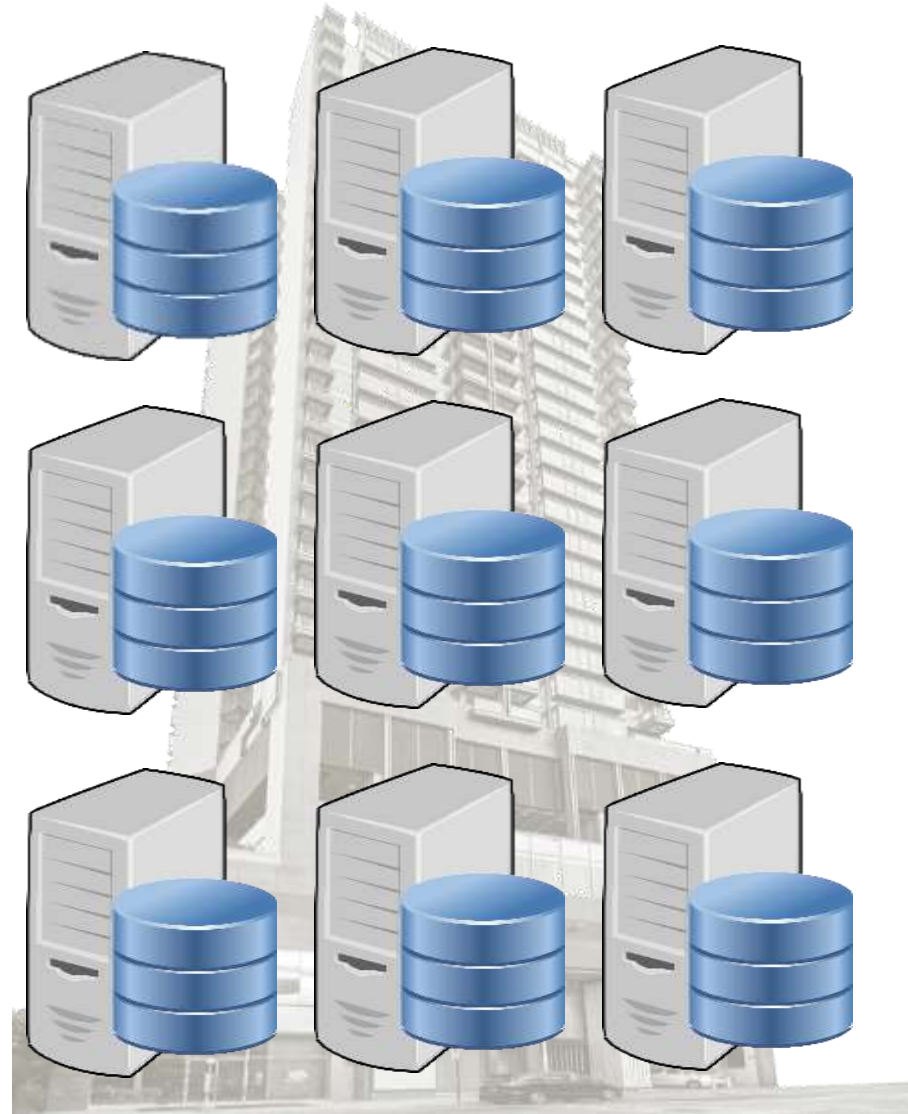


بررسی چند محصول تجاری



بررسی محصولات آزمایشگاهی موجود

بیان صورت مسئله



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

بیان صورت مسئله

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری



محصولات تجاری موجود در حوزه برون سپاری داده



Amazon Aurora ☐



Always Encrypted SQL Server ☐

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

امنیت در Amazon Aurora

□ ایزوله بودن شبکه با Amazon Virtual Private Cloud



□ مجوز دهی در سطح منابع با اتصال به مکانیزم احراز هویت آمازون



□ رمزنگاری AES256 برای انتقال



امنیت داده در رایانش ابری

رمزگذاری جستجوپذیر متقارن

رمزگذاری جستجوپذیر نامتقارن

رمزگذاری تمام همریخت

برون‌سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون‌سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون‌سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

امنیت Always Encrypted SQL Server

□ مشخصات کلی

- پشتیبانی در MS SQL Server 2016
- پشتیبانی در Azure SQL Server
- قابل ترکیب با Transparent Data Encryption



□ احراز هویت و مجاز شماری

- ایجاد Master Key
- ایجاد Column Encryption Key

KVbSAO1byRtuMhbKMKfM8GX0SMZYUBCr7YDPvCCMKjYERXyJlidsMOB4VQCFF+RezdBWeostZ
 IDFnVbhstU4FyQlJTMwEjtUmigdSRNcicm2F36gcR0ieksekuCB6zVcBCP46BUZbjXlvSjRcSN/gy
 r4rhDcmmZzj1LriaXrTw1+FRHL8COp4+/fJ27DEx6q8FHU6mTyZbwde+BS0oDf8ckaCp2WFSEI
 bprXHhWQ56gy4KJRBpnqynCc6PYvP9PIL2BB0+...RPVd9v5yTuDDON1areGX
 mZR05cPLtCsYwVvKVaSy6gy6GVs0VZa3RyYL...nlt/fD2lqXlJcZi4dxEk
 woTo+o+pf9WKWc3ybnYRldceu4jtHY40B...bUQOU20/DkDn7mU
 8DaGtVyzlvXG70Ql/0JlQh9xgCd281SNhQL...NjpfyUgXowKLS3rg
 OmIjJkOV8WZMEvdSl/RE9zmJD3hz9ANJ2...gyJjn5xESMEwtPCv
 OHVdQzqQBTPLqCd84ec9uBKK2p6DXW+...zk/7ubJlPofa4GI4IQ
 qKCR1R1a0kdDRJV+ADt729JxvPzm7WBRW...gnfU794GYNQx1M11TR
 gwUmHxLTSRVKZDnXCuTl/peh+v3e+WJV...G4SbkDRUOKrwGxWcJozp
 07pM5zEjImBjg+QfDEarHkbs7pV5095A...4H/AB4fAhZd2mBaoGyx1hSL5uSp4cs7vn3
 6iMIDC8Rhg9NemD56Tr2xjJ8j5359Z8...r0g1+JNRck57FSHE1SbteXniBMC/xqVttE00/I
 DocWCT0fo39fMpkNM0eZc5h5DBS...neg/4wr957cOpNFNRRUeJTxxk2loI0/ThxwPjNR
 Fq0Xx/TVkqnlJzXhTfbnVwoSlls...+1v1E3wreAupq6aGS3u6ExSsd0Nk+qKBrkzBAjD
 J1f/W7Q8+Tya2ml...um+XN3gFUSF59rbQeBF2gAPzAx17kmDIX



□ رمزنگاری

- تنها دو روش قطعی و تصادفی

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

محصولات آزمایشگاهی موجود



Raluca Popa



Stephen Tu



Zhian He

(MIT 2012) CryptDB •

(MIT 2013) MONOMI •

(Hong Kong 2015) SDB •

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

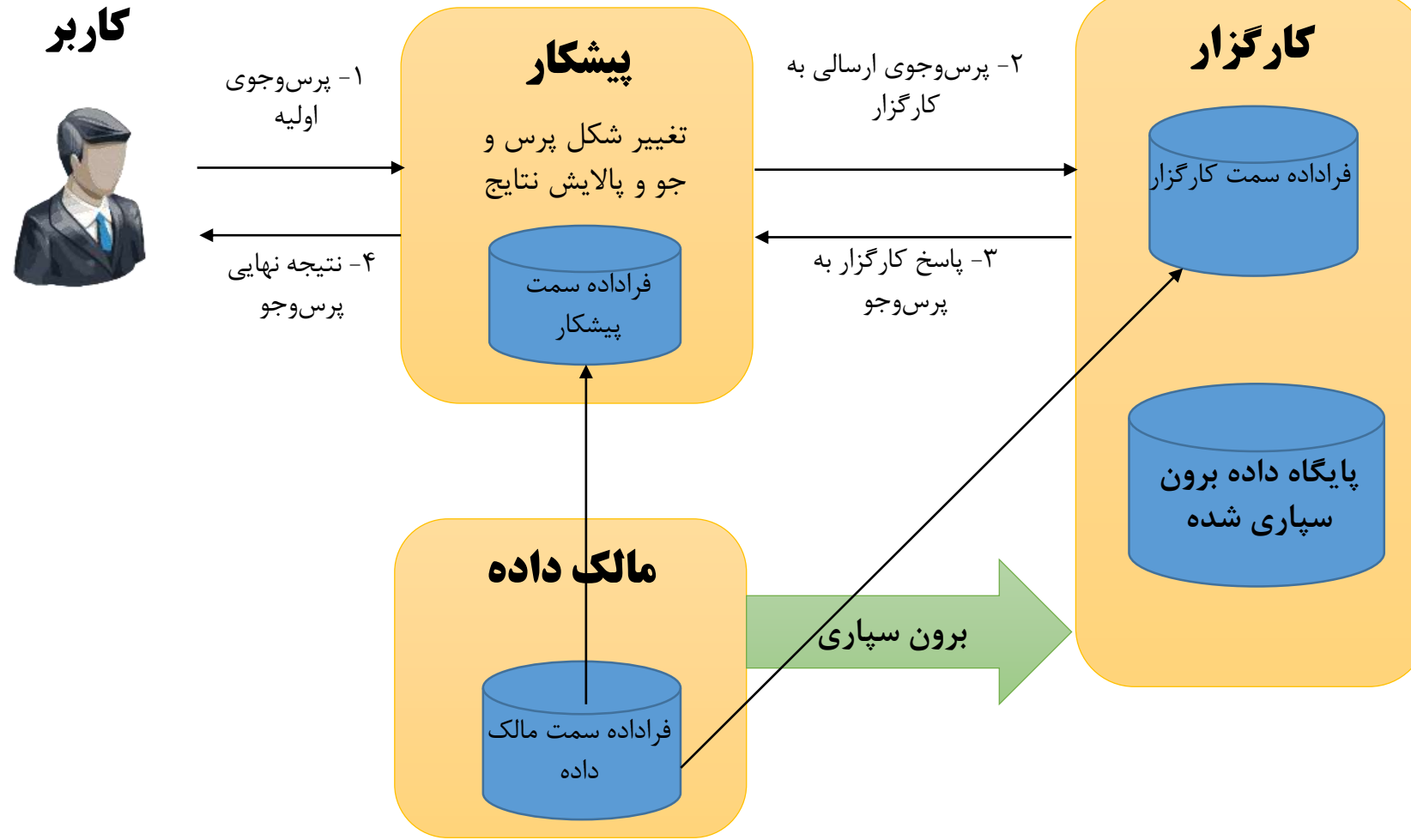
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

معماری مشترک سیستم های برون سپاری



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

اهداف در سامانه های برون سپاری

□ افزایش حداکثری توان پردازشی
○ پردازش در کارگزار

□ افزایش حداکثری توان ذخیره سازی
○ عدم ذخیره سازی در پیشکار

□ کاهش هزینه نگهداری

□ عدم کاهش امنیت داده ها
○ عدم نمایش داده در کارگزار



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

مسئله اصلی!



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

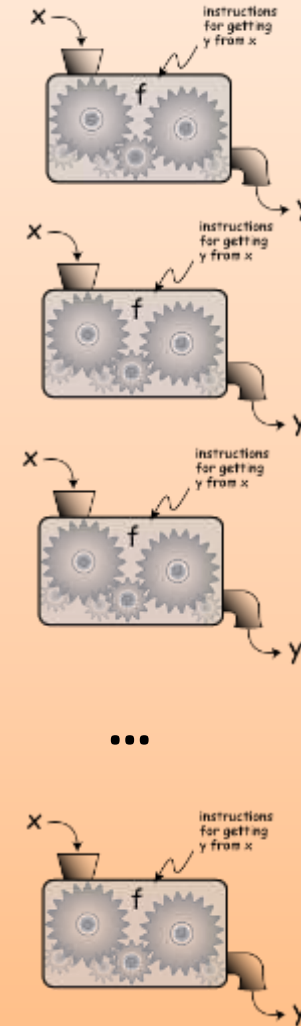
در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

CryptDB – اجزای اصلی

پایگاه داده سمت کارگزار



پروکسی کارگزار (مغز اصلی)



پرس و جوی خام

پرس و جوی
بازنویسی شده

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

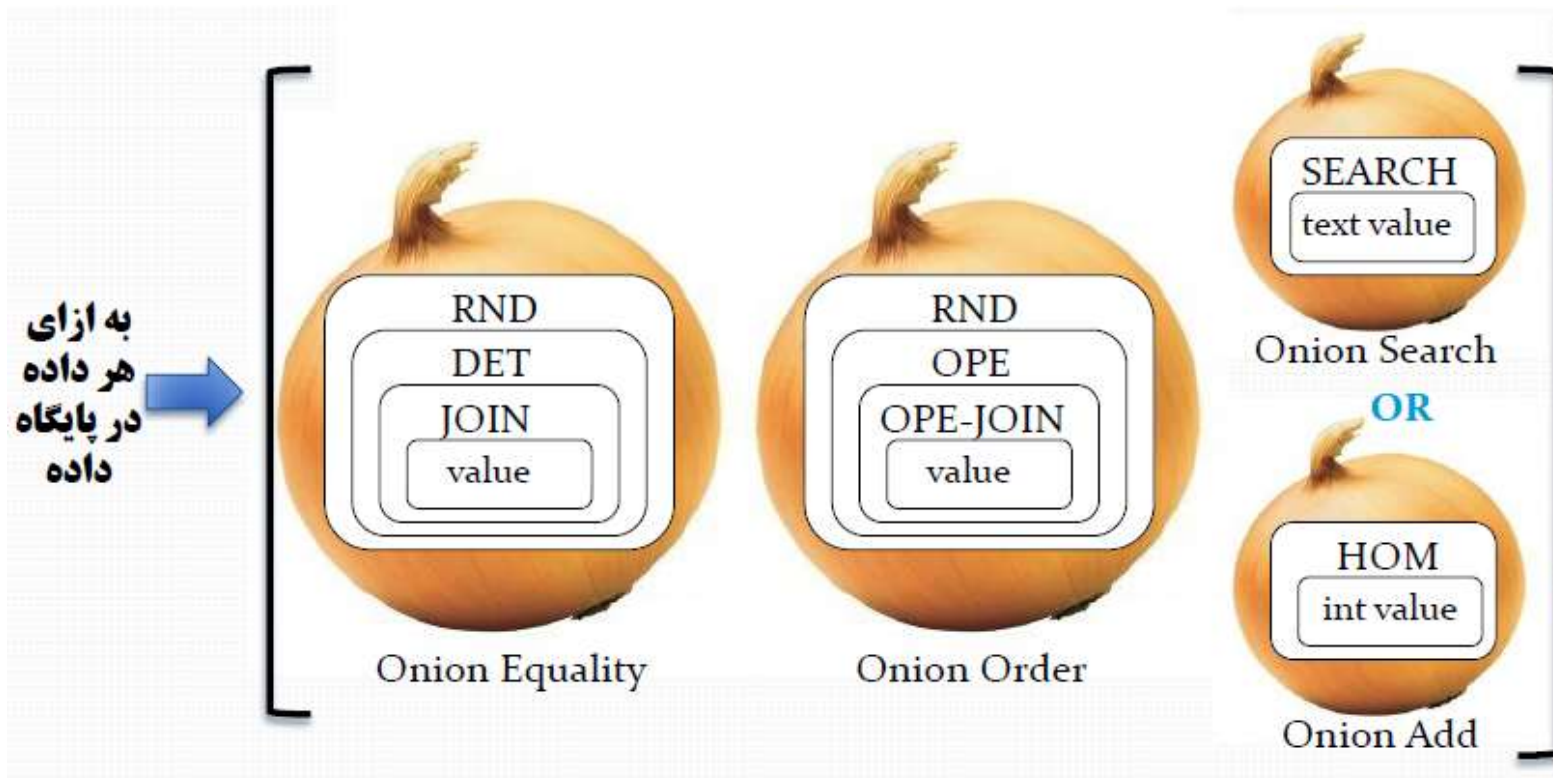
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

CryptDB – نحوه ذخیره سازی داده ها



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

CryptDB – نحوه اجرای پرس و جو

SELECT ID FROM Employees
WHERE Name = 'Alice'



پاسخ
رمزگشایی شده



UPDATE Table1 SET C2-Eq =
ENCRYPTTRND(Key, C1, C2, FC2MV)
Table1 WHERE C2-Eq = x7b3d



پاسخ رمز شده

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

مشکلات CryptDB

```
USE [AdventureWorks2014];
GO

SELECT [Name]
FROM [Production].[Product]
WHERE [ListPrice] = ( SELECT [ListPrice]
FROM [Production].[Product]
WHERE [Name] = 'Chain Stays'
);

GO
```

□ عدم پشتیبانی از پرس و جو های تو در تو ۴/۲۲

□ تنها پشتیبانی از انواع داده عددی و رشته ای

5 8
9 1 2

Semantic Web
idea Web way
search
data books information
results articles

□ نیاز به هوش انسانی برای مدیریت پرس و جو های پیچیده



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

MONOMI

- انتقال داده های میانی به پیشکار موجب کندی سیستم
- محاسبات پیچیده روی داده های رمز شده هزینه بر
 - FHE ها 10^9 بار کند تر
 - روش های تک منظوره مناسب تر ولی سخت تر
- افزودن ستون اضافه موجب افزایش سرعت برخی و کاهش سایرین
- ارایه راهکاری بر مبنای CryptDB و پیاده سازی Designer و Planner
- پشتیبانی ۱۹/۲۲ مدل پرس و جوی TPC-H
- هدف پشتیبانی پرس و جوهای تحلیلی

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

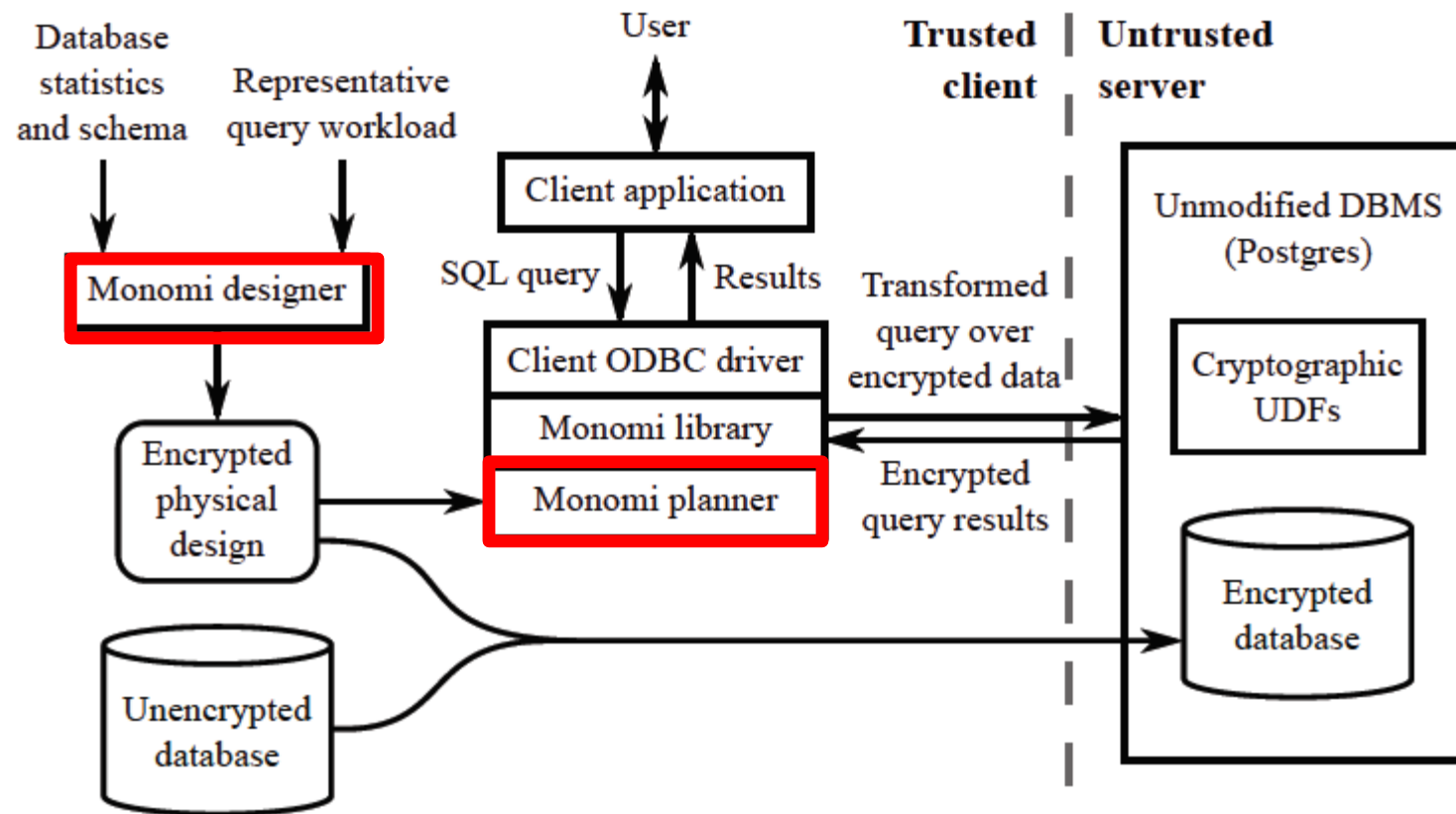
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

MONOMI – معماری کلی



S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich, "Processing analytical queries over encrypted data," in *Proceedings of the VLDB Endowment*, 2013, vol. 6, no. 5, pp. 289–300.

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر

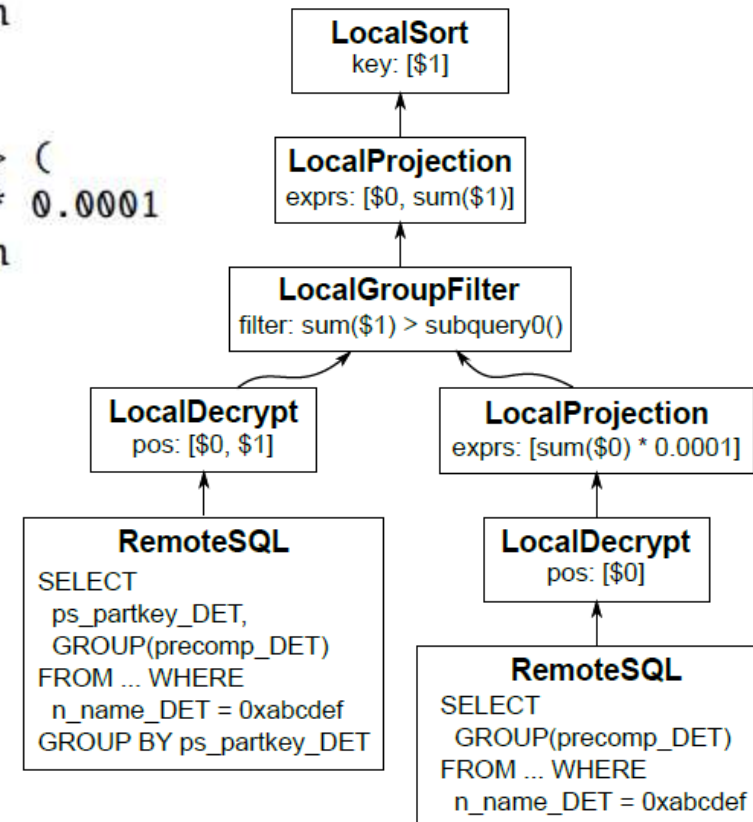
مروری بر محصولات موجود در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در رایانش ابری

Planner & Designer – MONOMI

□ عدم امکان کل پرس و جو در کارگزار

```
SELECT  ps_partkey,
        SUM(ps_supplycost * ps_availqty) AS value
FROM    partsupp JOIN supplier JOIN nation
WHERE   n_name = :1
GROUP BY ps_partkey
HAVING  SUM(ps_supplycost * ps_availqty) > (
        SELECT SUM(ps_supplycost * ps_availqty) * 0.0001
        FROM  partsupp JOIN supplier JOIN nation
        WHERE n_name = :1 )
ORDER BY value DESC;
```



S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich, "Processing analytical queries over encrypted data," in *Proceedings of the VLDB Endowment*, 2013, vol. 6, no. 5, pp. 289–300.

امنیت داده در رایانش ابری

رمزگذاری جستجوپذیر متقارن

رمزگذاری جستجوپذیر نامتقارن

رمزگذاری تمام همریخت

برون‌سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون‌سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون‌سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

MONOMI – راه کارهایی جهت بهبود کارایی

- محاسبه و ذخیره از پیش انجام شده به ازای هر سطر
 - $ps_supplycost * ps_availqty$
- رمزنگاری با سر بار کم حافظه
 - استفاده از مد هایی از AES که حجم داده رمز شده خیلی تغییر نکند
 - ذخیره سال از تاریخ در یک ستون دیگر
- ذخیره مقادیر رمز هم ریخت جمعی Pailliar برخی ستون ها برای انجام عملیات ریاضی
- استفاده از designer جهت یافتن بهترین ساختار

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

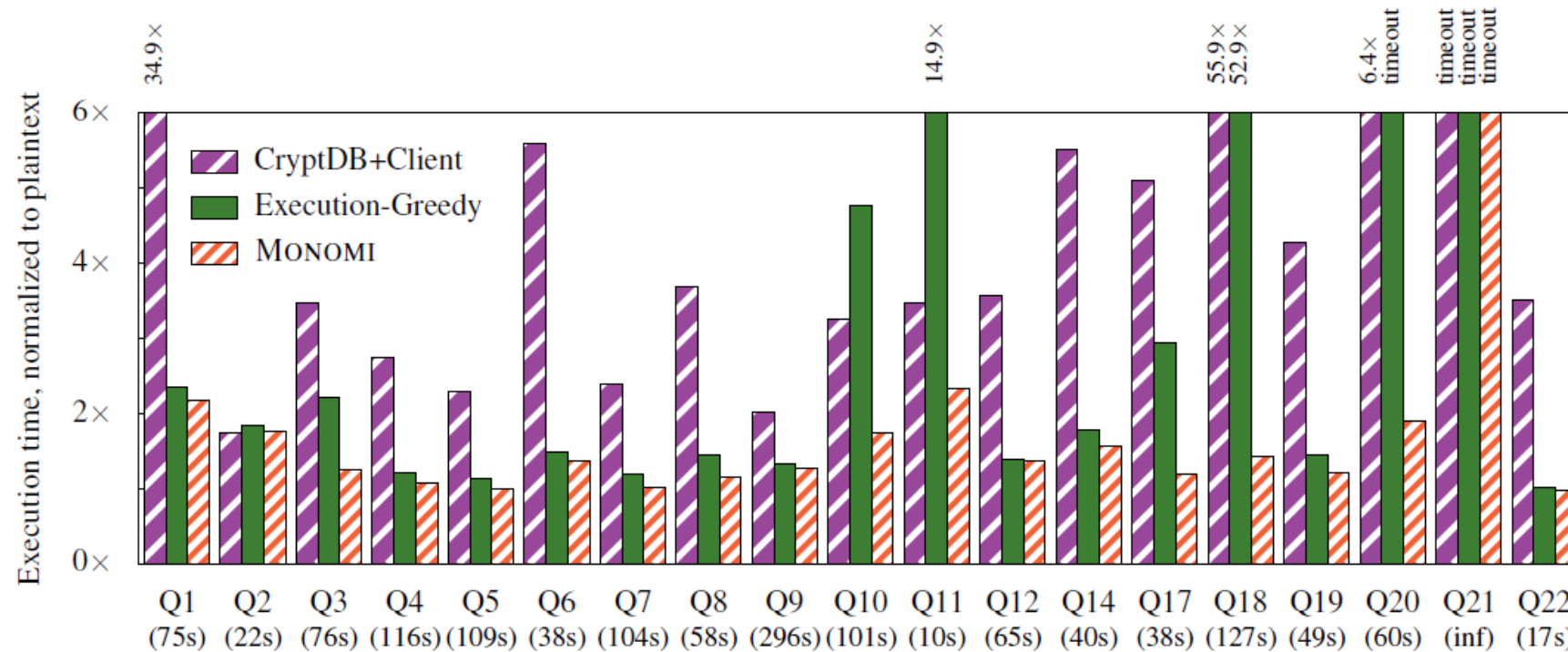
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

MONOMI – نتایج ارزیابی



S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich, "Processing analytical queries over encrypted data," in *Proceedings of the VLDB Endowment*, 2013, vol. 6, no. 5, pp. 289–300.

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

SDB

- استفاده از نقش مالک داده جهت پردازش برخی قسمت ها
- **ارایه اپراتورهای بهینه و قابل ترکیب**
- امکان استفاده از اپراتور ها برای داده های رمز شده و غیر رمز شده
- امکان اعمال روی هر نوع پایگاه داده
- ارایه اثبات برای امنیت شمای رمزنگاری آن
- بر مبنای تسهیم راز
- **تنها بر روی داده های عددی قابل اعمال**

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی

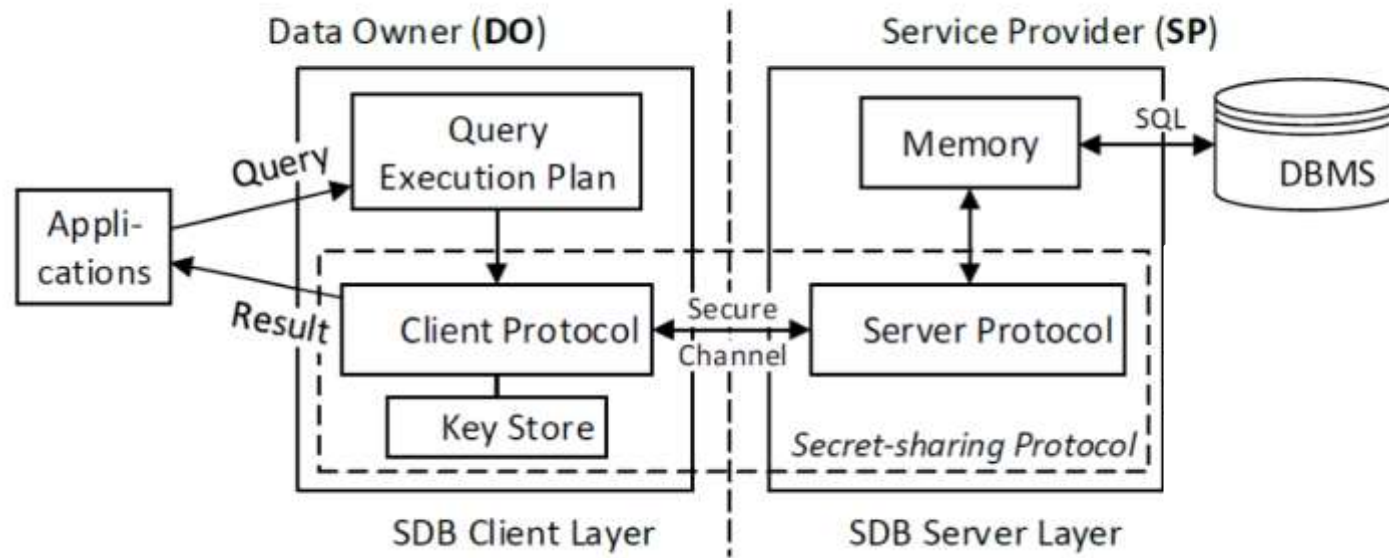
وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر

مروری بر محصولات موجود در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در رایانش ابری

SDB – معماری کلی



Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, "SDB: a secure query processing system with data interoperability," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

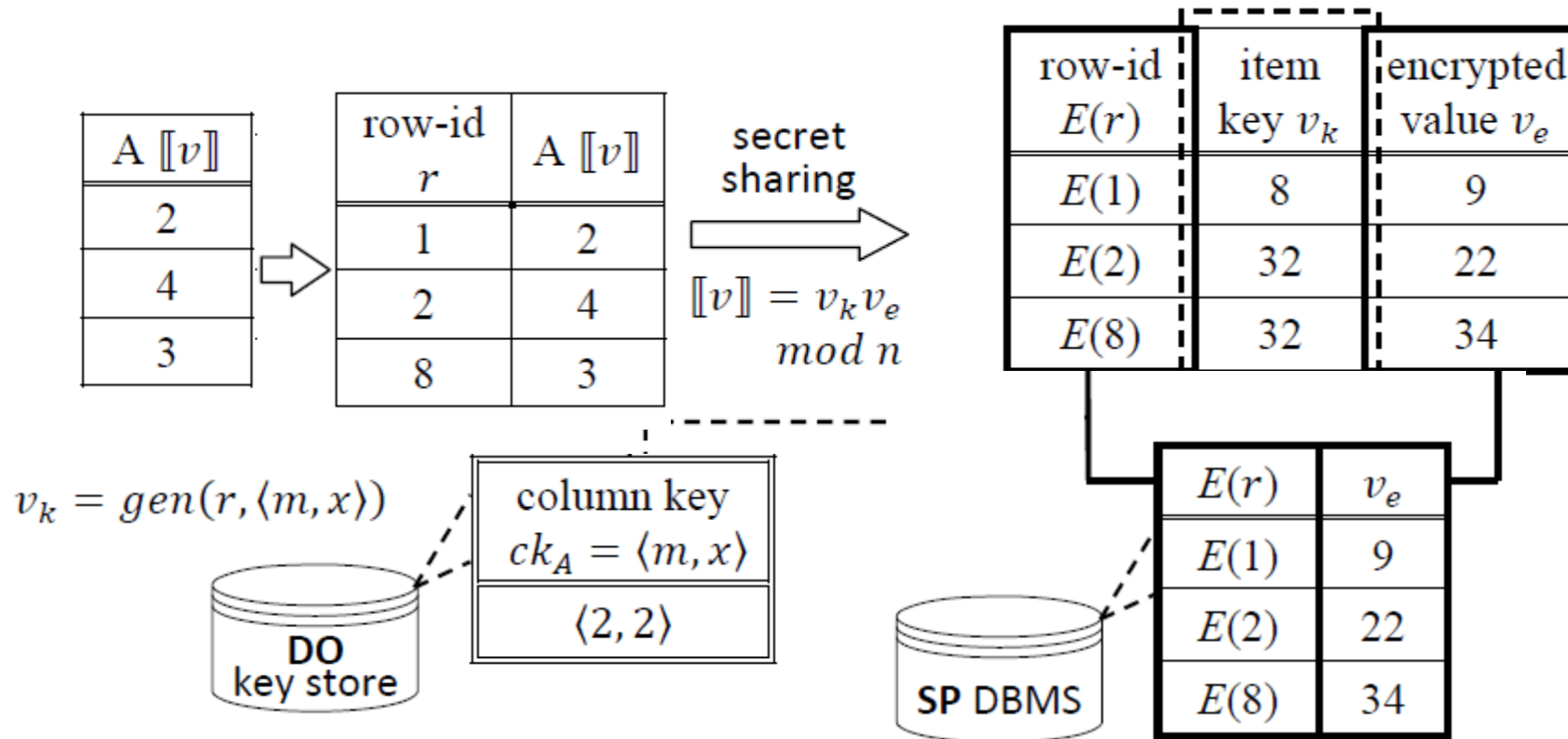
رایانش ابری

SDB – نحوه رمز کردن داده ها

$$v_k = gen(r, \langle m, x \rangle) = mg^{(rx \bmod \phi(n))} \bmod n.$$

$$v_e = \mathcal{E}([v], v_k) = [v]v_k^{-1} \bmod n,$$

$$(g = 2, n = 35)$$



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

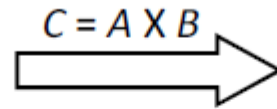
Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, "SDB: a secure query processing system with data interoperability," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.

SDB – نحوه پیاده سازی ضرب کردن

$$C = A \times B \quad (g = 2, n = 35)$$

Plaintext values

A	B
2	3
4	1

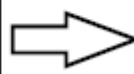


C
6
4

$$c_e = a_e \cdot b_e$$

DO

$ck_A = \langle 2, 2 \rangle$
$ck_B = \langle 1, 3 \rangle$



$ck_C = \langle 2, 5 \rangle$

SP

$E(r)$	A_e	B_e
$E(1)$	9	31
$E(2)$	22	29



C_e
34
8

$$ck_C = \langle m_C, x_C \rangle = \langle m_A m_B, x_A + x_B \rangle$$

$$c_k = m_C \cdot g^{r x_C} = m_A \cdot m_B \cdot g^{r(x_A + x_B)} = a_k b_k \pmod{n}$$

$$[c] = c_e c_k = a_e b_e c_k = [a] a_k^{-1} [b] b_k^{-1} a_k b_k = [a] [b]$$

Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, "SDB: a secure query processing system with data interoperability," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

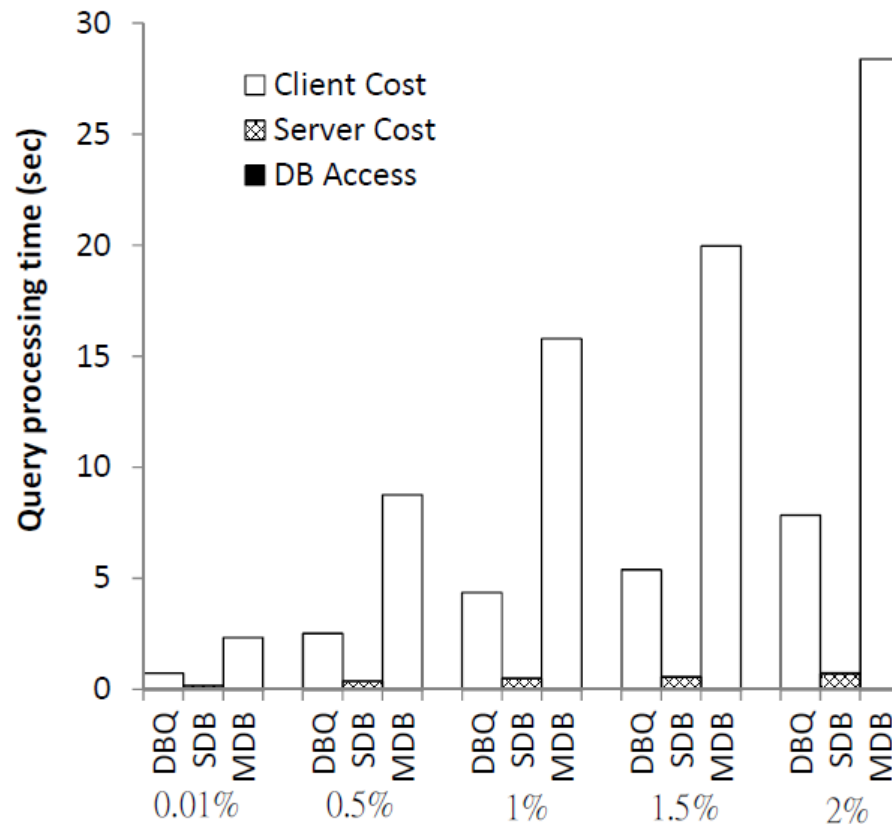
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

مقایسه کارایی



Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, "SDB: a secure query processing system with data interoperability," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

جمع بندی

- فعلا نمی توان از توابع FHE برای ایجاد رمزنگاری کاربردی استفاده کرد
- لازم است از توابع خاص منظوره استفاده کرد
- برای ایجاد قابلیت اجرای پرس و جو های پیچیده نیاز به وجود Planner است
- برای تامین امنیت، داده خام نباید وارد/ خارج کارگزار شود
- باید تا جای ممکن پردازش ها را در سمت کارگزار قرار داد تا از منابع آن استفاده کرد

□ نیاز به یک محصول امن و کارای برون سپاری در حوزه تجاری و تحقیقاتی وجود دارد

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت خطر در

رایانش ابری

ارجاعات

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و
رویکردهای تامین محرمانگیوارسی صحت پاسخ پرسمان روی
پایگاه داده برون سپاری شدهروشهای ذخیره سازی داده های
رمز شده غیر تکراری در ابرمروری بر محصولات موجود
در زمینه برون سپاری امن دادهامنیت داده و مدیریت خطر در
رایانش ابری

- ❑ <https://azure.microsoft.com/en-us/documentation/articles/sql-database-security/>
- ❑ <http://aws.amazon.com/rds/aurora/details/#security>
- ❑ R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Processing queries on an encrypted database," *Commun. ACM*, vol. 55, no. 9, pp. 103–111, 2012.
- ❑ S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich, "Processing analytical queries over encrypted data," in *Proceedings of the VLDB Endowment*, 2013, vol. 6, no. 5, pp. 289–300.
- ❑ W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, and S. M. Yiu, "Secure query processing with data interoperability in a cloud database environment," *Proc. 2014 ACM SIGMOD Int. Conf. Manag. data - SIGMOD '14*, pp. 1395–1406, 2014.
- ❑ Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, "SDB: a secure query processing system with data interoperability," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.
- ❑ V. Gadepally, B. Hancock, B. Kaiser, J. Kepner, P. Michaleas, M. Varia, and A. Yerukhimovich, "Computing on Masked Data to improve the Security of Big Data," 2015.
- ❑

باتشکر از توجه شما



امنیت داده در رایانش ابری

رمزنگاری جستجوپذیر متقارن

رمزنگاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون‌سپاری امن پایگاه داده و
رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی
پایگاه داده برون‌سپاری شده

روشهای ذخیره سازی داده های
رمز شده غیر تکراری در ابر

مروری بر محصولات موجود
در زمینه برون‌سپاری امن داده

امنیت داده و مدیریت خطر در
رایانش ابری