# معرفی اهداف و برنامه‌های دومین مدرسه زمستانه انجمن رمز ایران

هادی سلیمانی

پژوهشکده فضای مجازی دانشگاه شهید بهشتی

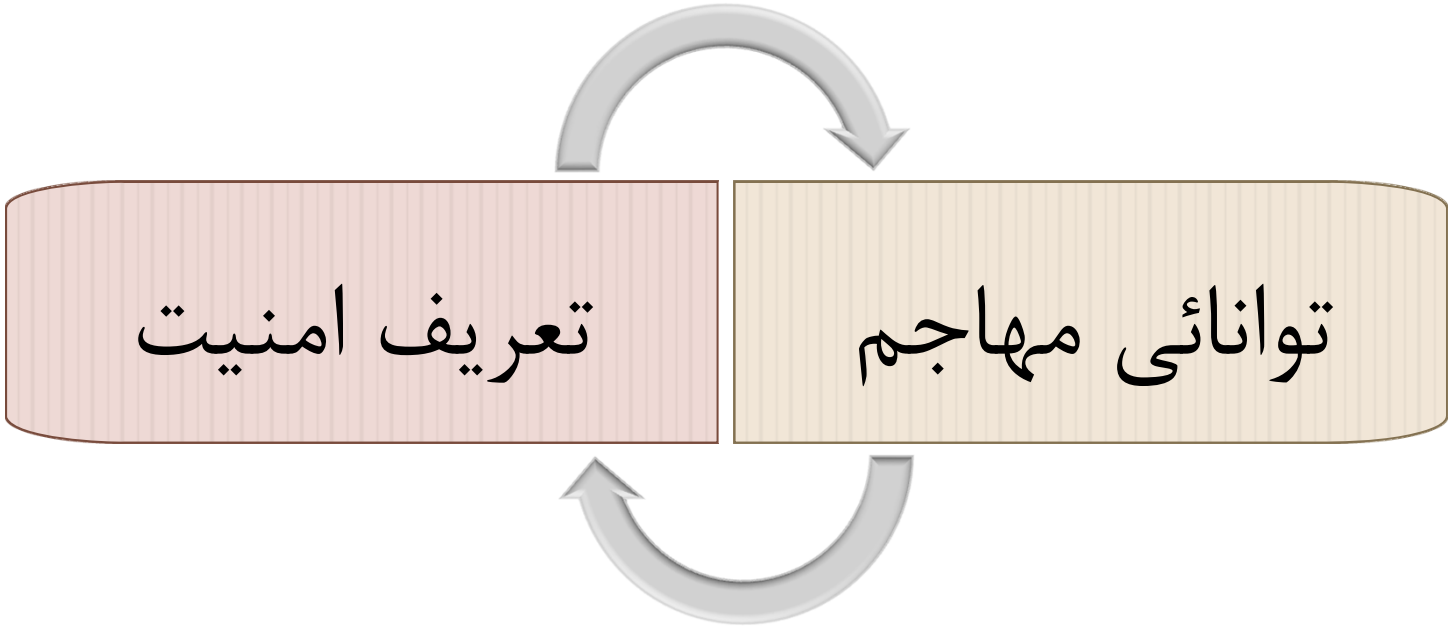
Email: h_soleimany@sbu.ac.ir

# طرح ارائه

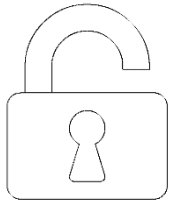
- آشنایی با تعاریف اولیه
  - دسته بندی حملات
  - مدل جعبه سیاه، جعبه خاکستری، جعبه سفید
- معرفی محورهای سخنرانی به همراه معرفی سخنرانان
  1. پیاده سازی کارای الگوریتم‌های رمزنگاری
  2. حملات القاء خطا
  3. حملات کانال جانبی تحلیل توان
  4. حملات کانال جانبی زمان
  5. رمزنگاری جعبه سفید
- جمع‌بندی

# مقدمه‌ای بر تعاریف اولیه

# دسته‌بندی حملات براساس توانائی مهاجم



# دسته‌بندی حملات (و تعریف امنیت) از منظر دسترسی مهاجم



- مدل جعبه سیاه: مهاجم به مجموعه‌ای از متون اصلی و رمزشده معادل آنها دسترسی دارد.
- مدل جعبه خاکستری: مهاجم دسترسی (بعضا فیزیکی) به ابزاری که رمزنگاری را انجام می‌دهد.
- مدل جعبه سفید: مهاجم درون سیستم است و به مقادیر میانی و ... دسترسی دارد!

ممکن است الگوریتم در مدل جعبه سیاه امن باشد اما در مدلهای جعبه خاکستری یا سفید امن **نباشد**.

تمرکز این کارگاه و دومین مدرسه زمستانه بر روی مدل‌های **جعبه خاکستری** و **جعبه سفید** می‌باشد.

# دسته‌بندی حملات مدل جعبه خاکستری

گران تر و موثرتر

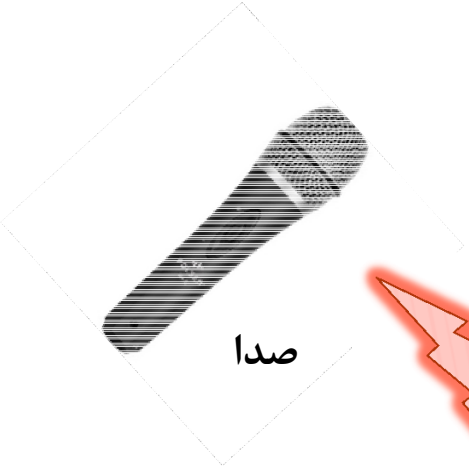
| | فعال | غیرفعال |
|---|---|---|
| تهاجمی | Permanent Faults | Probing |
| نیمه تهاجمی | Radiation Attack | Optical Inspection |
| غیرتهاجمی | Fault Attacks | Side-channel Attacks |

ارزان تر، قابلیت اجرا در کابردهای بیشتر

- تفاوت تعریف در برخی متون دیده می‌شود.
- به عنوان مثال، بعضا حملات فعال را به صورت کلی حملات القاء خطا نام گذاری می‌کنند.

تمرکز این کارگاه و دومین مدرسه زمستانه حملات **غیرتهاجمی** می‌باشد.

# انواع کانالهای جانبی



صدا

تشعشعات
الکترومغناطیس

زمان اجرا

...

توان مصرفی

تمرکز این کارگاه و دومین مدرسه زمستانه مبتنی بر حملات کانال جانبی **تحلیل توان مصرفی** و **زمان** خواهد بود.

# محورهای کارگاه مقدماتی و دومین مدرسه زمستانه انجمن رمز

# محورهای کارگاه مقدماتی و دومین مدرسه زمستانه

۱ پیاده‌سازی الگوریتم‌های رمزنگاری

۲ حملات القاء خطا

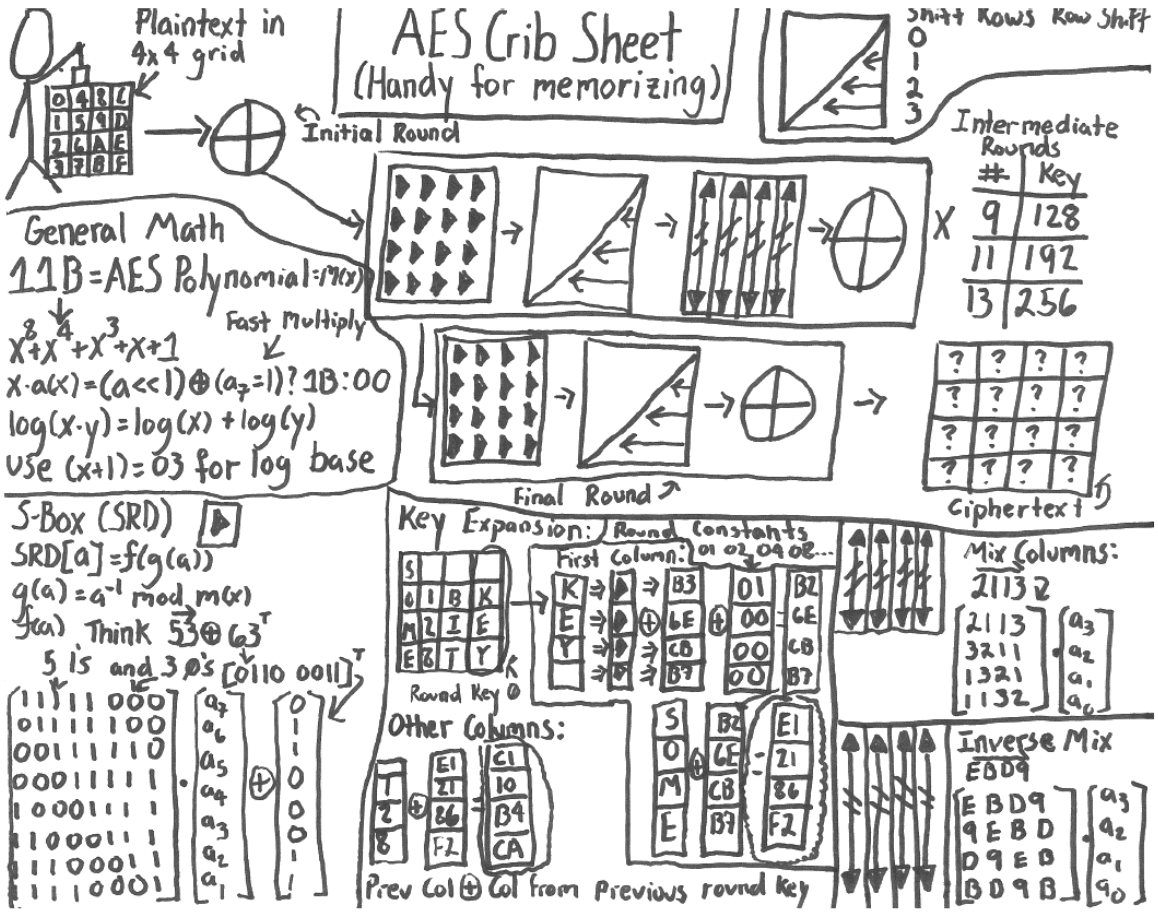
۳ حملات کانال جانبی تحلیل توان

۴ حملات کانال جانبی مبتنی بر زمان

۵ رمزنگاری جعبه سفید

# ۱- پیاده سازی کارای الگوریتم های رمزنگاری

# آشنایی با مقدمات ریاضی




- برای پیاده‌سازی (به خصوص سخت افزاری) اولیه‌های رمزنگاری، شناخت و فهم تعاریف ریاضی آنها الزامی است.



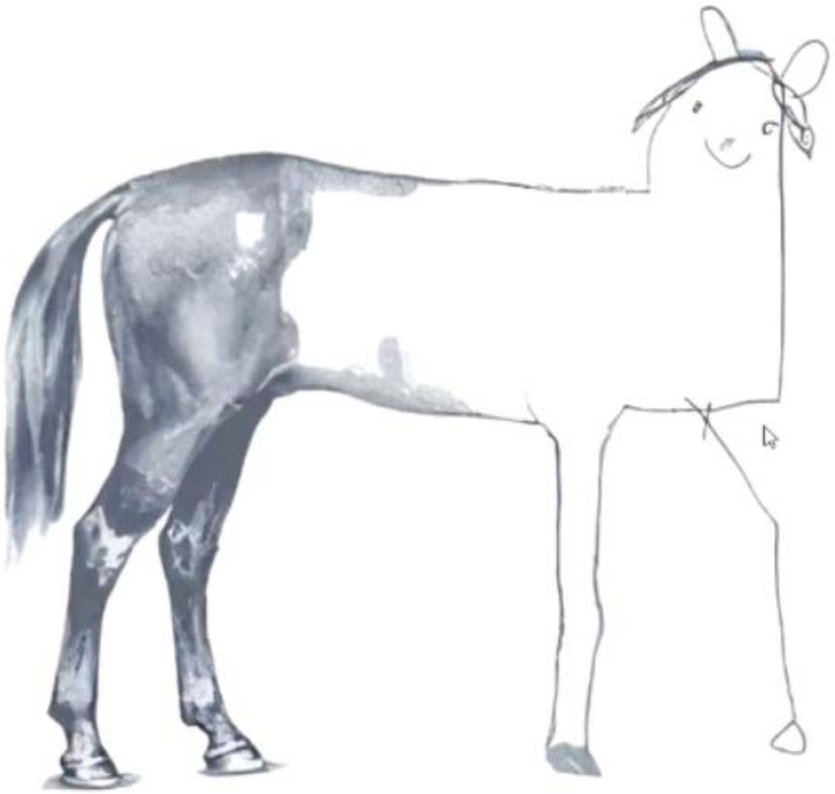
The slide is courtesy of Tim Güneysu.

# آشنایی با مقدمات ریاضی

**آشنایی با**
**مقدمات ریاضی**

- دکتر فرخ لقا معظمی؛ استادیار پژوهشکده فضای مجازی دانشگاه شهید بهشتی
- مقدمه‌ای بر نظریه گروه‌های متناهی و کاربردهای آن در پیاده‌سازی الگوریتم‌های رمزنگاری
  - کاربرد در پیاده‌سازی AES
  - کاربرد در پیاده‌سازی الگوریتم‌های خم بیضوی

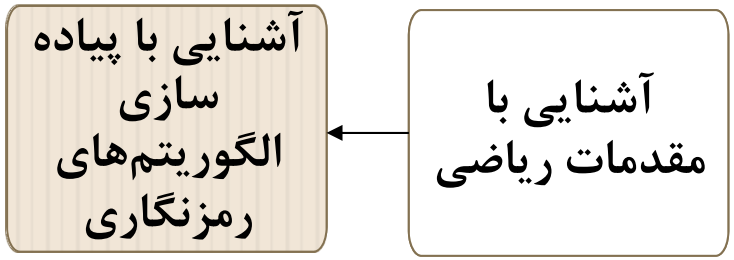
# آشنایی با پیاده‌سازی الگوریتم‌های رمزنگاری



Design Implementation

The picture is courtesy of Reza Sohizadeh.

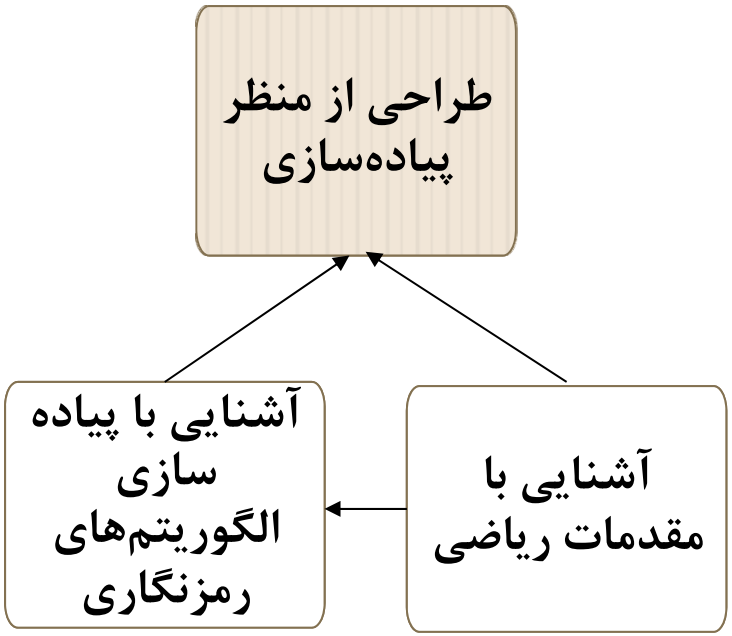
# آشنایی با پیاده‌سازی الگوریتم‌های رمزنگاری




- دکتر راضیه سالاری فرد؛ استادیار دانشکده کامپیوتر دانشگاه شهید بهشتی
- پیاده‌سازی کارای رمزنگاری خم بیضوی در نرم‌افزار و سخت‌افزار
- پیاده‌سازی کارای رمزنگاری AES در نرم‌افزار و سخت‌افزار

# طراحی از منظر پیاده‌سازی

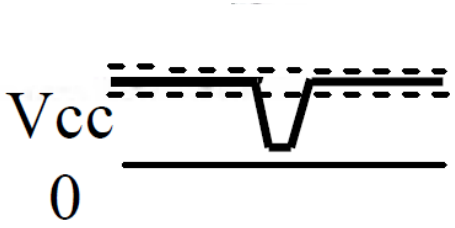
# طراحی از منظر پیاده‌سازی

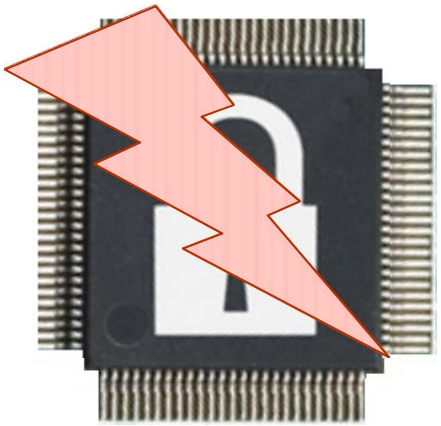


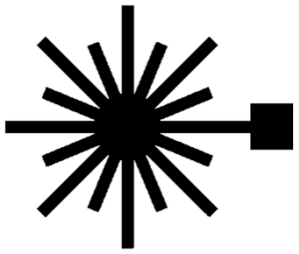

- پروفسور Joan Daemen؛ استاد دانشگاه Radboud هلند
- بیش از بیست سال سابقه طراحی اولیه‌های رمزنگاری در دانشگاه و صنعت
- از طراحان الگوریتم‌های رمزنگاری استاندارد AES و SHA-3
- برنده جایزه Levchin
- در حال اجرای پروژه تحقیقاتی ERC در زمینه طراحی اولیه های رمزنگاری

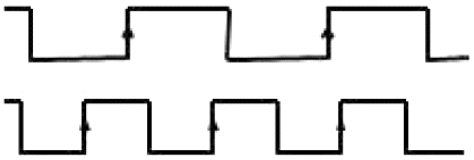
# ٢- حملات القاء خطا

# حملات القاء خطا





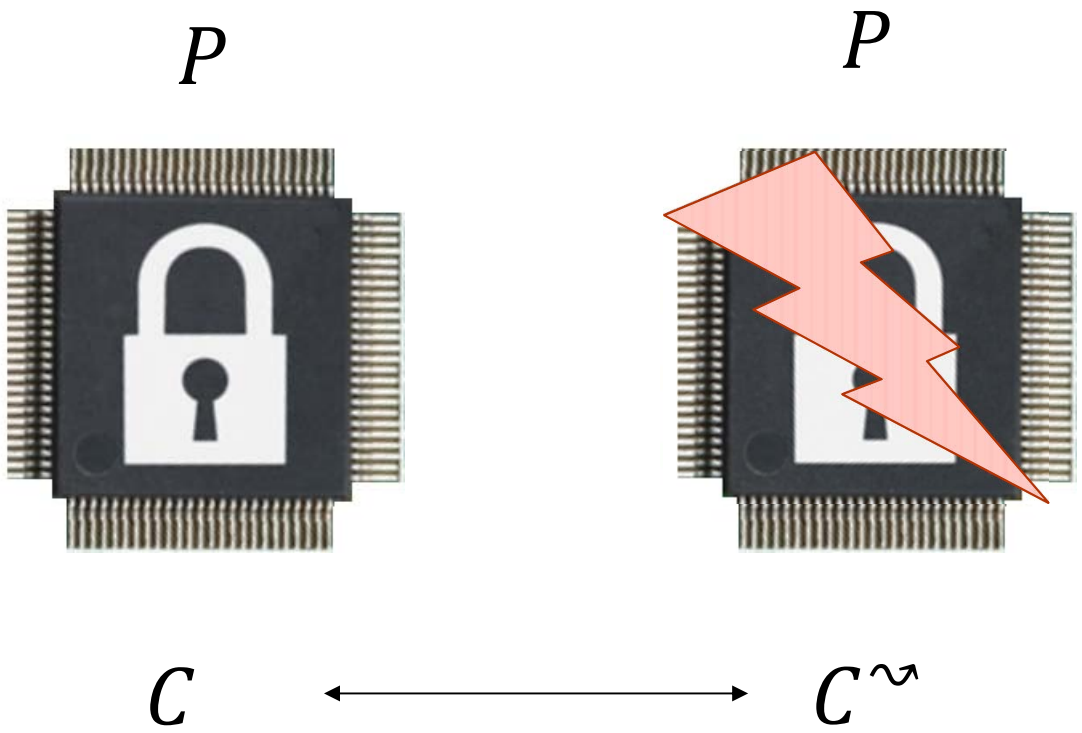


# حملات القاء خطا

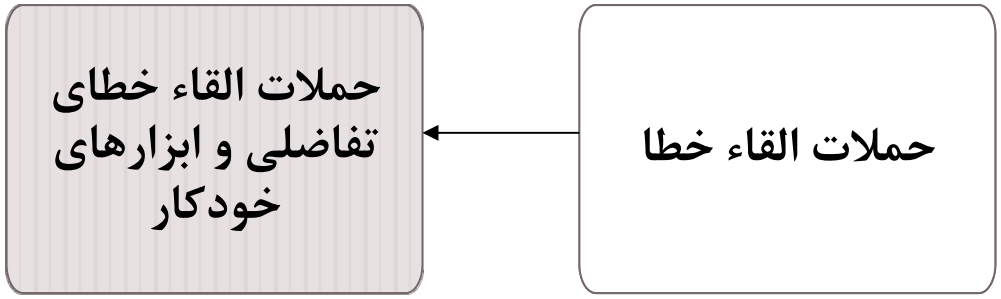
**حملات القاء خطا**

- دکتر محمد علی ارومیه‌چی‌ها؛ استادیار پژوهشگاه خواجه نصیرالدین طوسی
- دکتر علوم کامپیوتر تخصص رمزنگاری از دانشگاه Macquarie استرالیا
- پانزده سال سابقه تحقیق و توسعه در زمینه رمزنگاری

# حملات القاء خطای تفاضلی

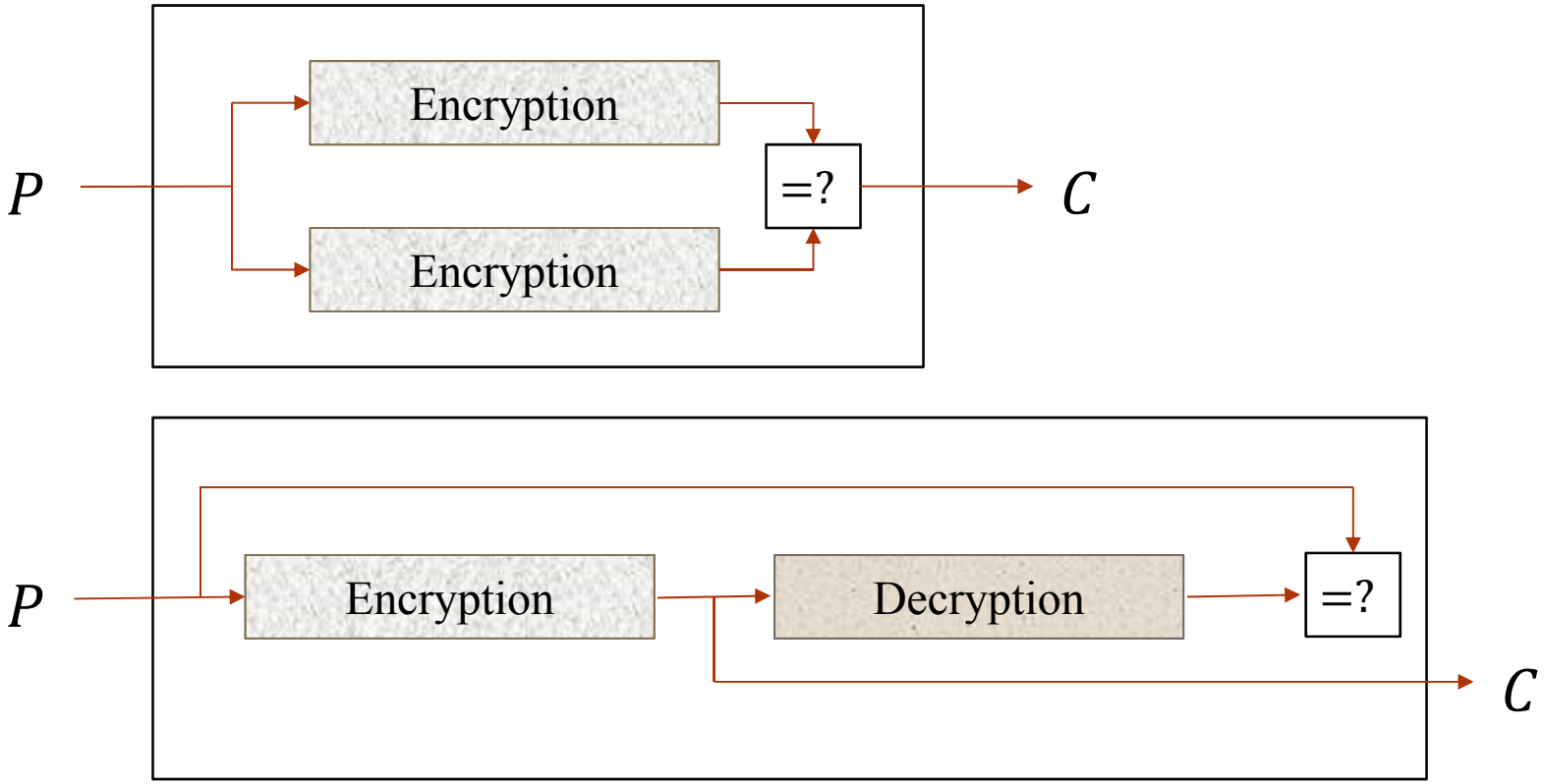


# حملات القاء خطای تفاضلی



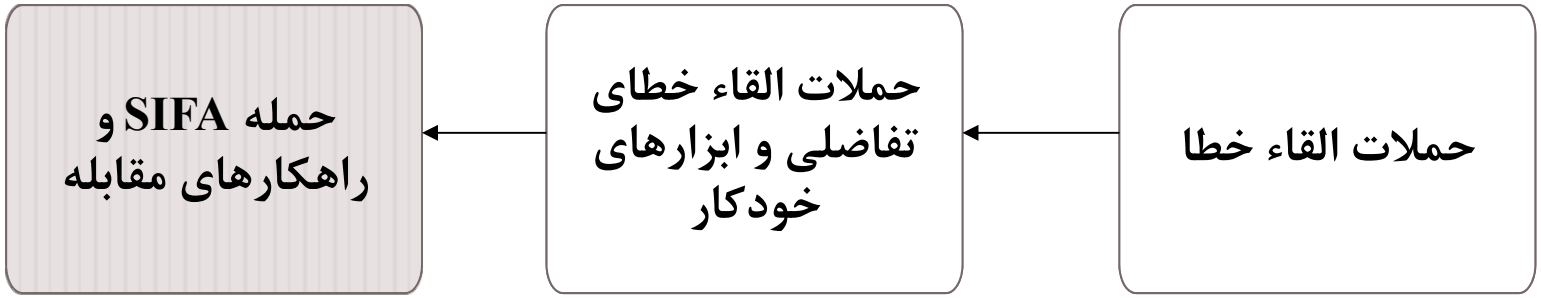

- دکتر Chester Rebeiro؛ استادیار دانشگاه IIT Madras هند
- فعالیت‌های گسترده تحقیقاتی ـ آزمایشگاهی در حوزه پیاده‌سازی امن

# مقابله با حملات القاء خطای تفاضلی




- با روش‌های متنوع می‌توان اعمال حملات القاء خطا را سخت‌تر کرد.
- یک از روش‌های معمول استفاده از افزونگی است: مثلا پیاده‌سازی موازی رمزگذاری یا رمزگشایی (مضاعف)

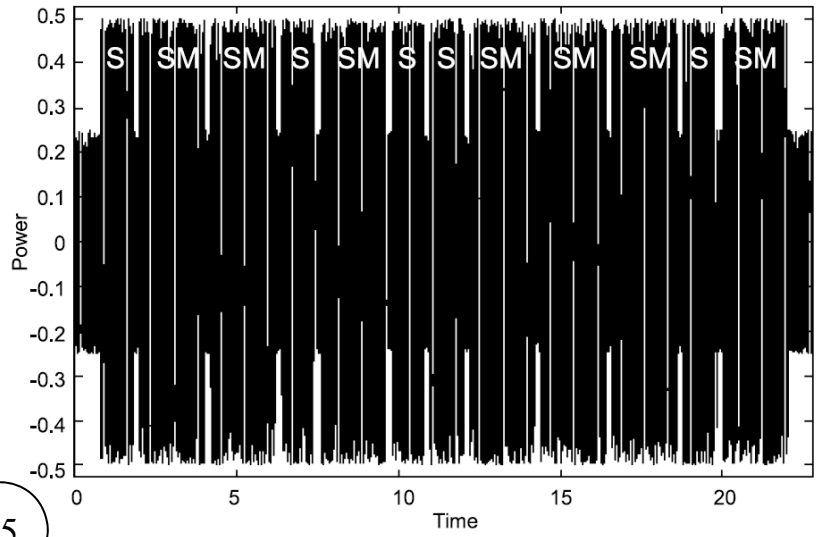
# حمله SIFA

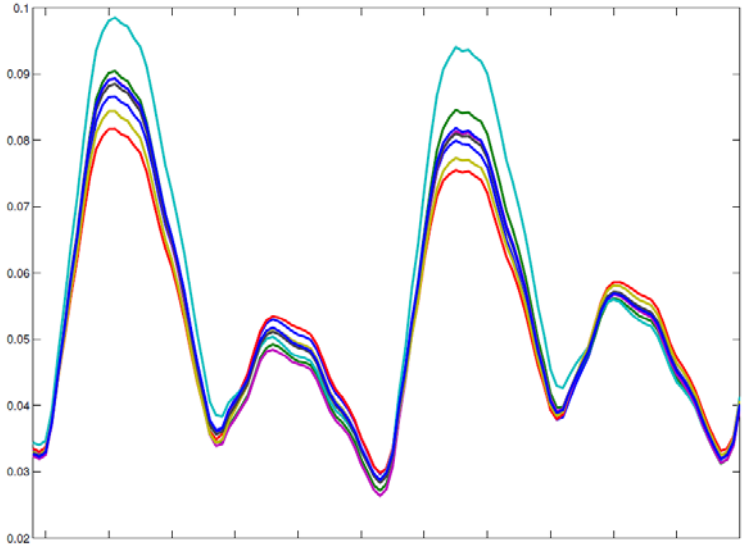



- دکتر Maria Eichlseder؛ استادیار دانشگاه Graz اتریش
- تحقیقات اخیر: ارتباط بین تحلیل‌های رمزنگاری و حملات القاء خطا
- جزء ارائه دهندگان حمله SIFA که قابل اعمال به طیف وسیعی از پیاده سازی‌ها می باشد.

# ۳- حملات کانال جانبی تحلیل توان

# حملات تحلیل توان

# حملات کانال جانبی تحلیل توان

**حملات کانال جانبی**
**تحلیل توان**

- دکتر علی جهانیان؛ دانشیار دانشکده کامپیوتر دانشگاه شهید بهشتی
- مسئول گروه تحقیقاتی امنیت سخت‌افزار
- تجربیات گسترده در تحقیقات نظری و آزمایشگاهی در حوزه امنیت سخت‌افزار و حملات کانال جانبی
- مفاهیم پایه در حملات کانال جانبی تحلیل توان؛ مبانی الکترونیک، الگوریتم‌ها و ابزارها

# Profiling Attacks

## Non Profiled attacks

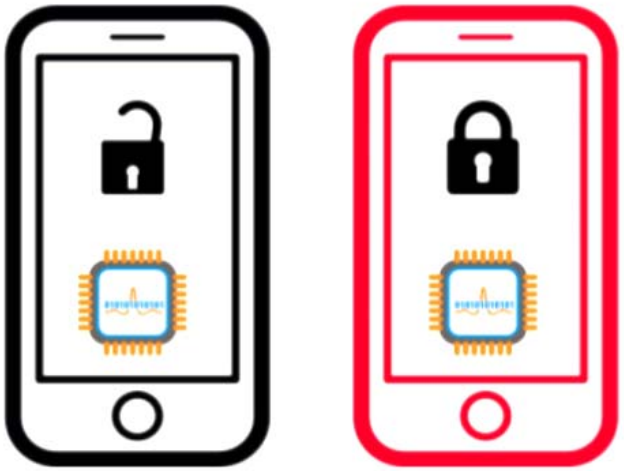
Target device
(closed)

- Differential Power Analysis (DPA)
- Correlation Power Analysis (CPA)
- Mutual Information Analysis (MIA)

## Profiled attacks

Profiling device
(open)

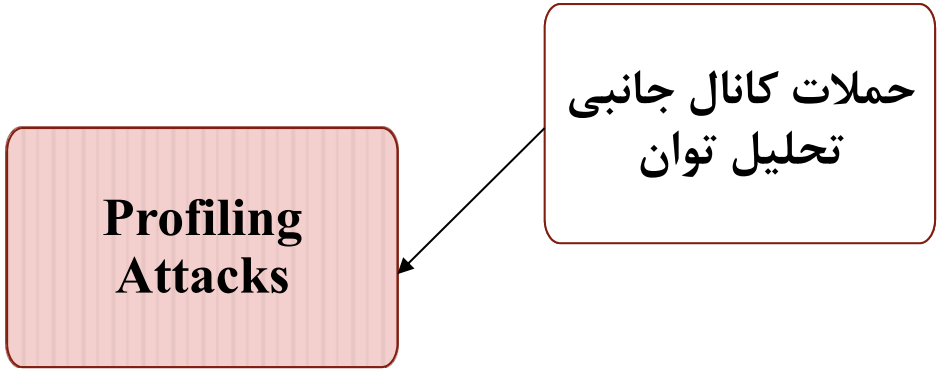
Target device
(closed)



- Template attacks
- Support Vector Machine
- Random Forests
- Deep Learning

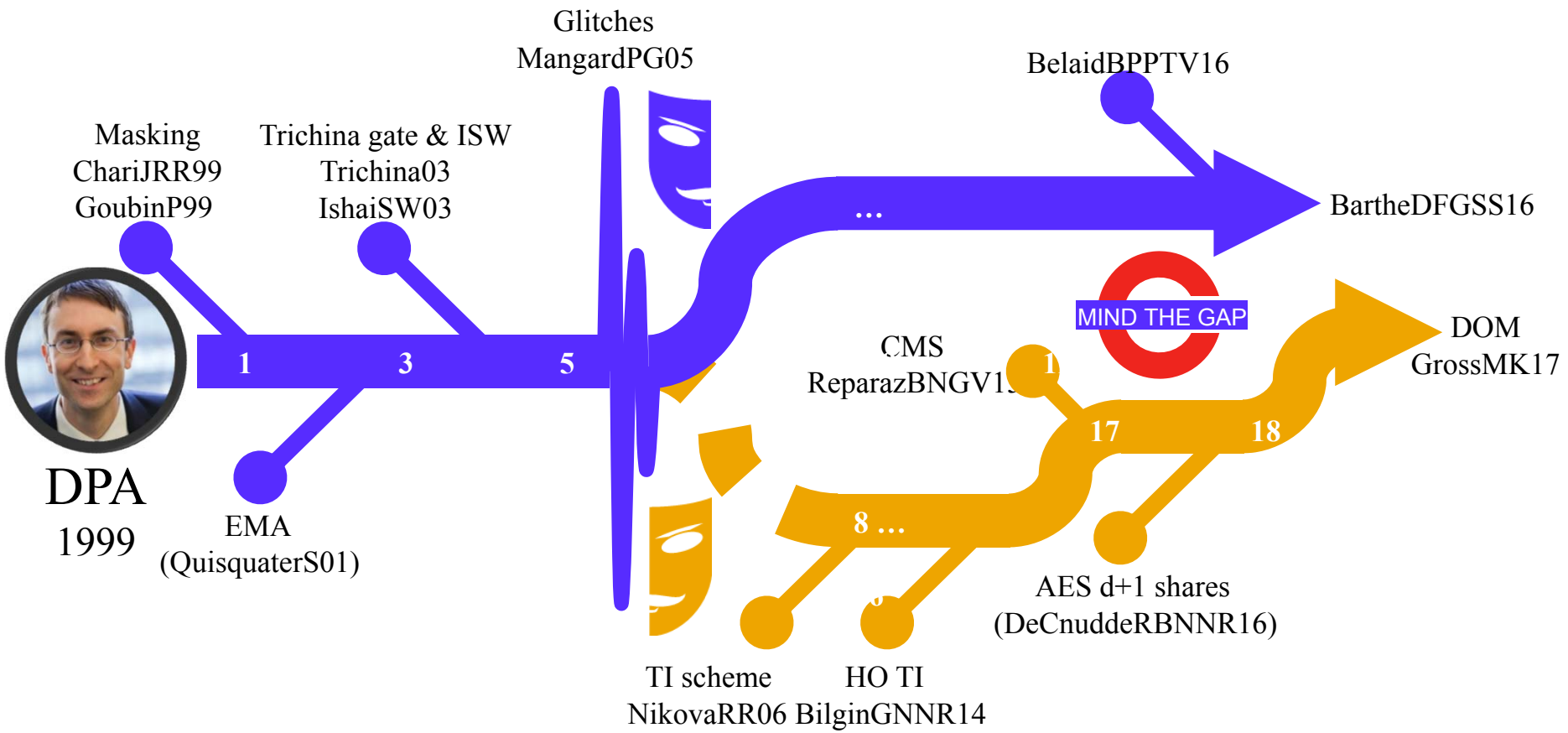
The picture is courtesy of Benjamin Timon

# Profiling Attacks



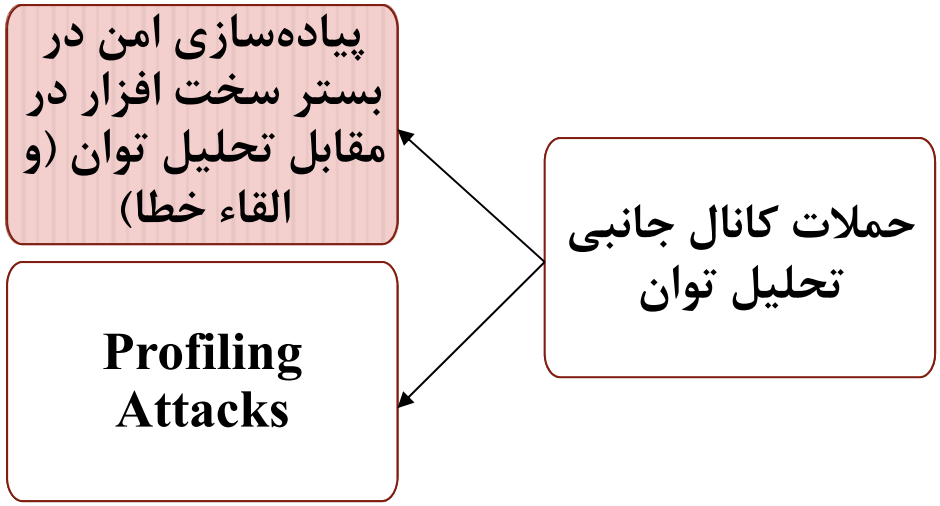

- پروفسور Elisabeth Oswald؛ استاد دانشگاه Klagenfurt اتریش
- از نویسندگان کتاب Power Analysis Attacks
- مسئول کمیته علمی Eurocrypt 2014، Eurocrypt 2015، CHES 2008
- اجرای پروژه‌های متعدد صنعتی و تحقیقاتی نظیر پروژه تحقیقاتی ERC

# مقابله با حملات تحلیل توان در پیاده سازی های سخت افزاری



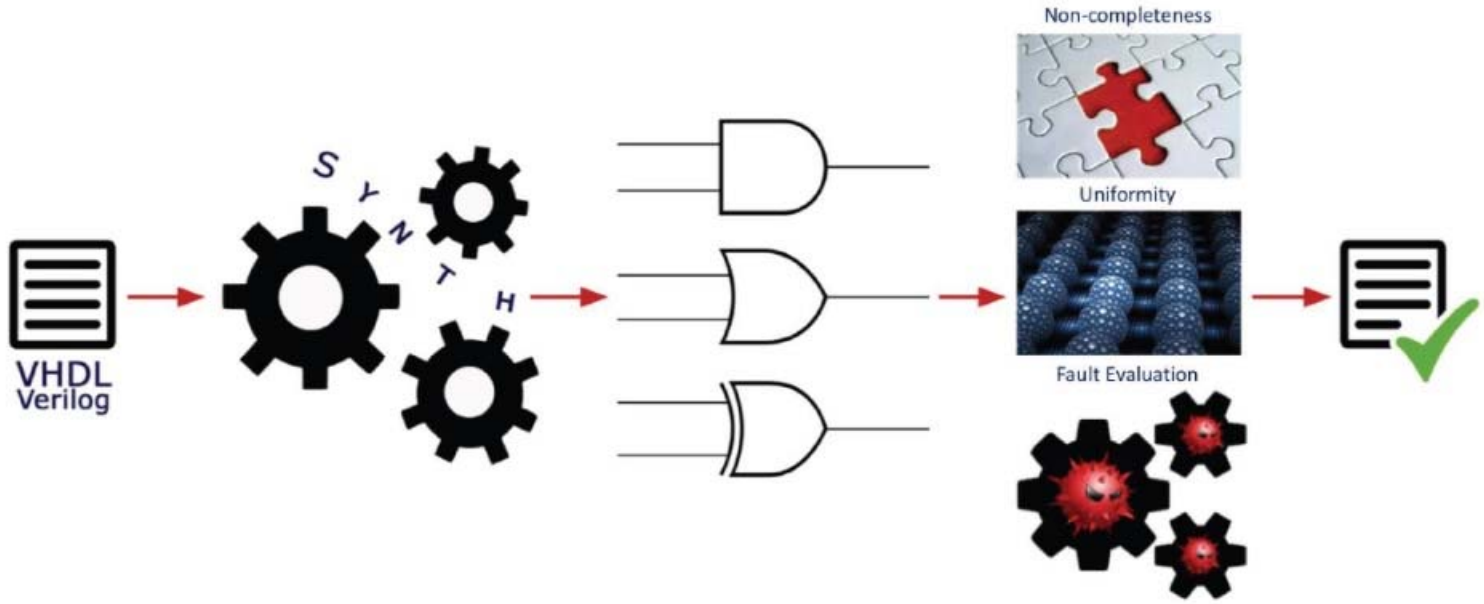

The picture is courtesy of Hannes Gross

# حملات کانال جانبی تحلیل توان



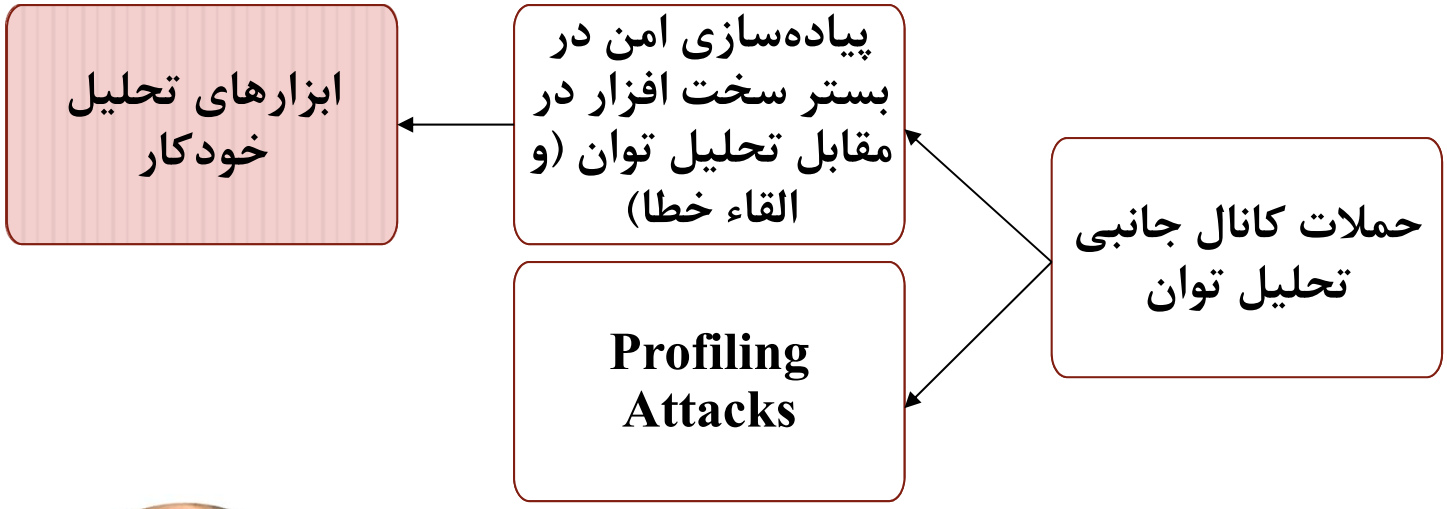

- دکتر Svetla Nikova، محقق ارشد دانشگاه KUL بلژیک
- راهنمائی ۱۰ پایان نامه در حوزه پیاده سازی امن
- از ارائه دهندگان پیاده سازی آستانه
- اجرای پروژه‌های متعدد اروپائی و بین‌المللی (پروژه NIST)
- پیش نیاز دیگر: آشنایی با حملات القاء خطا

# ابزارهای تحلیل خودکار




The slide is courtesy of Victor Arribas

# حملات کانال جانبی تحلیل توان




- دکتر Pascal Sasdrich، محقق پسادکتری دانشگاه Ruhr آلمان
- از ارائه‌دهندگان ابزار SILVER

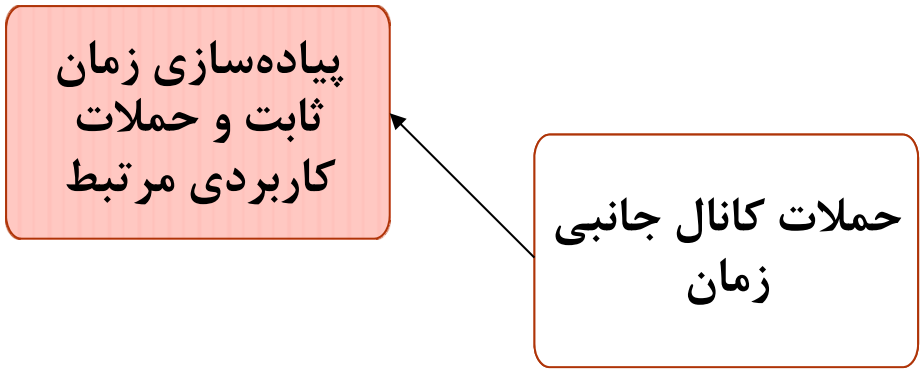
# ۴- حملات کانال جانبی زمان

# حملات کانال جانبی زمان

**حملات کانال جانبی زمان**

- دکتر سیده عاطفه موسوی، محقق پسادکتری آزمایشگاه امنیت و ایمنی نرم‌افزار و سیستم دانشگاه صنعتی شریف
- متخصص امنیت سیستم‌ها و سامانه‌های رایانشی

# حملات کانال جانبی زمان

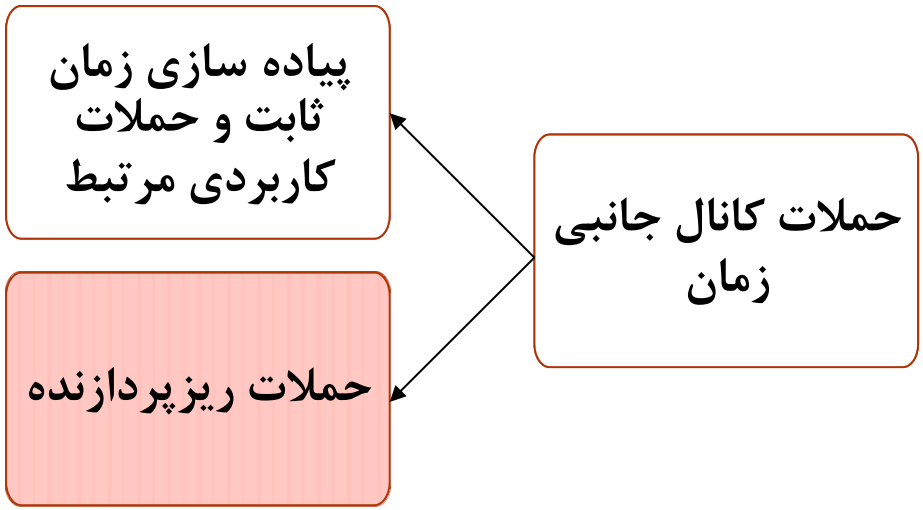



- دکتر Billy Brumley، دانشیار دانشگاه Tampere فنلاند
- تخصص در زمینه پیاده‌سازی امن نرم افزاری الگوریتم‌های رمزنگاری در مقابل حملات زمان
- در حال اجرای پروژه ERC در حوزه حملات کانال جانبی زمان

# حملات ریزمعماری؛ بازتاب گسترده در رسانه های خبری


The slide is courtesy of Daniel Gruss

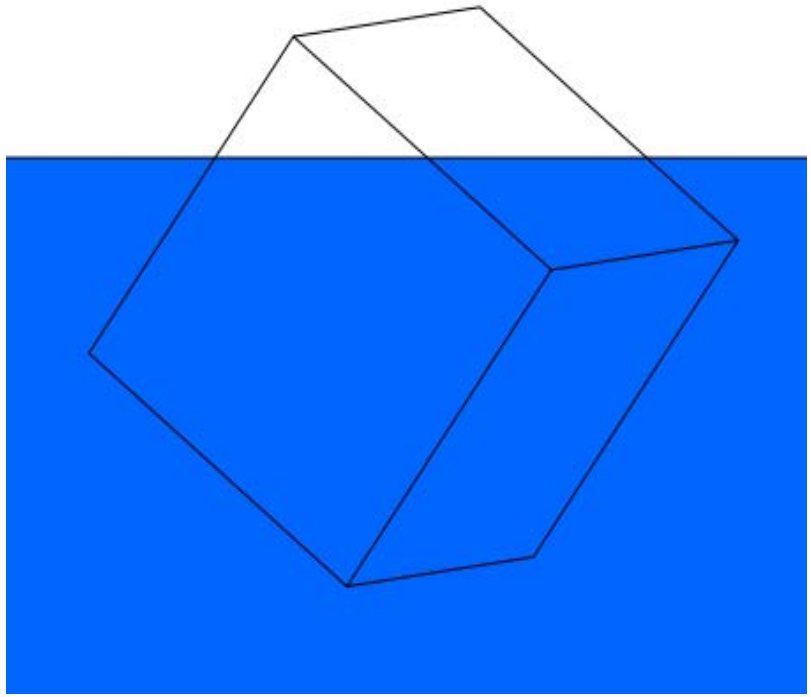
# حملات کانال جانبی زمان




- دکتر Daniel Gruss، استادیار دانشگاه Graz اتریش
- دانشنامه برتر دانشگاه Graz
- از جوانترین اساتید برجسته در حوزه حملات کانال جانبی
- از اعضای تیم کشف کننده حملات Meltdown، Spectre و PLATYPUS

# ۵- رمزنگاری جعبه سفید

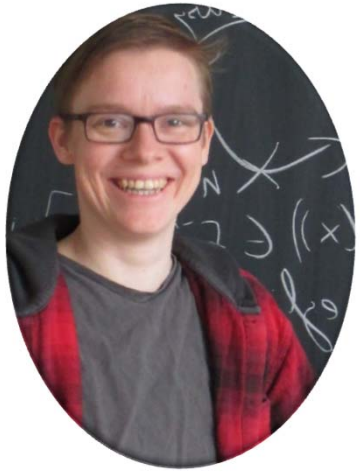
# رمزنگاری جعبه سفید



- رمزنگاری جعبه سفید در کاربردهای مختلف به کار می رود.
- نیاز به این مدل با توجه به فن‌آوری NFC بیشتر احساس شده است.
  - شروع مجدد فعالیت‌های آکادمیک
- عموما روش‌های به کارگرفته شده در صنعت منتشر نشده‌اند.

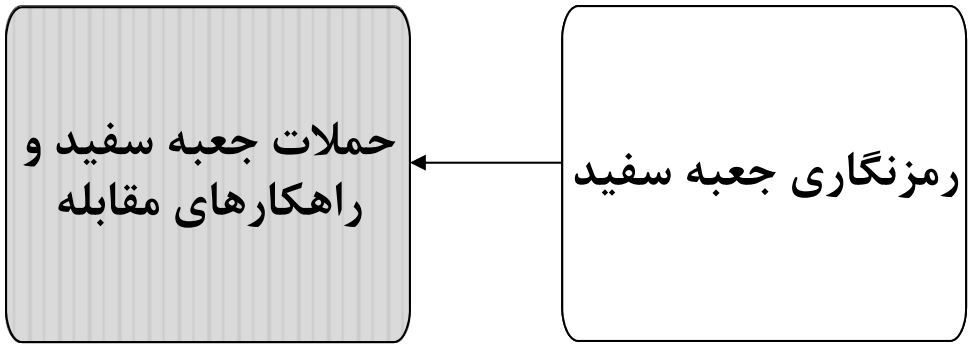
# رمزنگاری جعبه سفید

**رمزنگاری جعبه سفید**

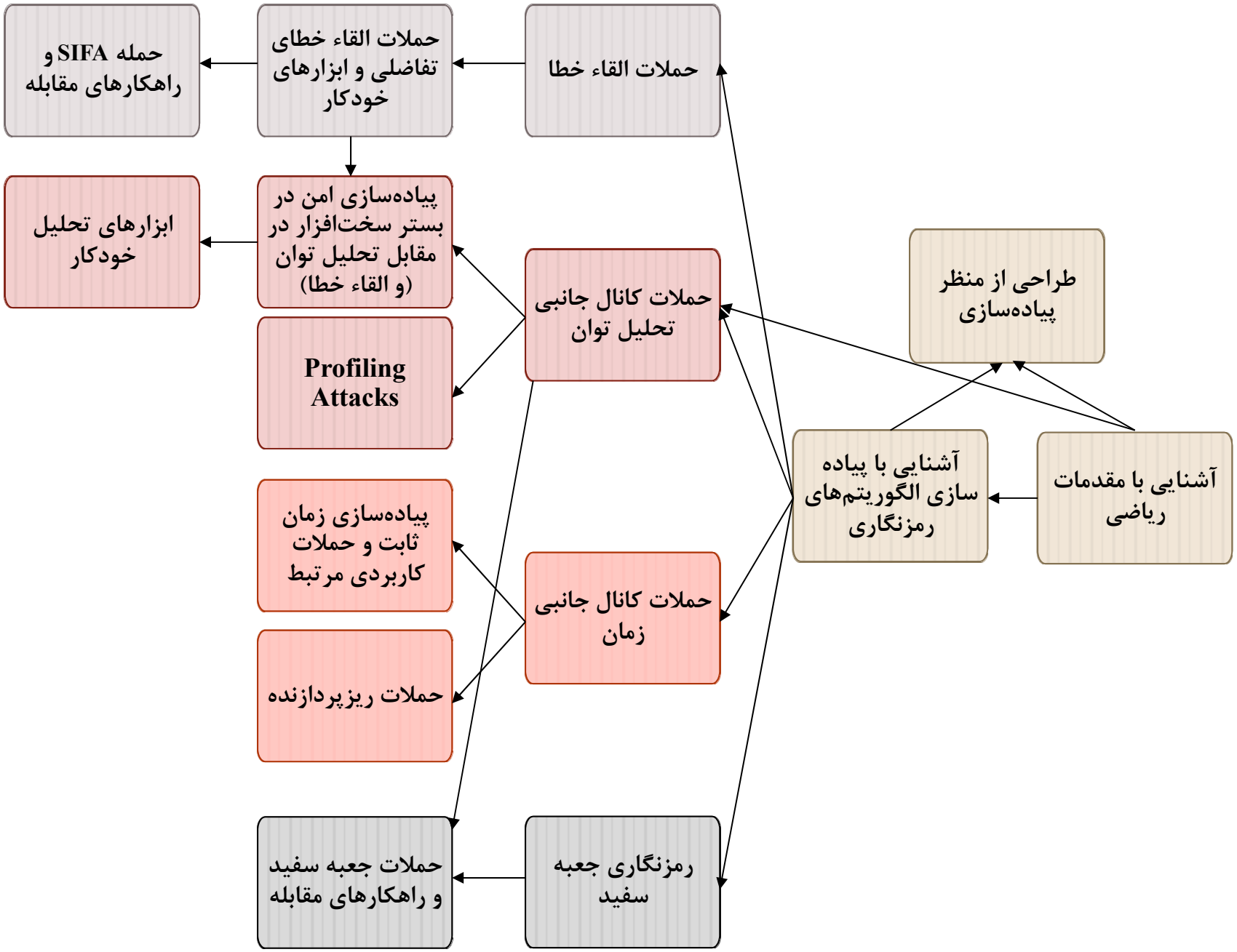


- دکتر Chris Brzuska، استادیار دانشگاه Aalto فنلاند
- نوآوری‌های مهم در حوزه نظری و عملی رمزنگاری جعبه سفید

# رمزنگاری جعبه سفید




- دکتر Alpirez Bock Estuardo؛ محقق پسادکتری دانشگاه Aalto فنلاند
- رمزنگاری جعبه سفید، موضوع دانشنامه دکتری ایشان بوده است.
- هم اکنون هم موضوع تحقیقاتی ایشان در دوره پسادکتری است.
- نوآوری‌های متعدد در حوزه‌های کاربردی رمزنگاری جعبه سفید
- پیش‌نیاز اضافه: آشنایی با حملات تحلیل توان تفاضلی


حملات القاء خطا
حملات القاء خطای تفاضلی و ابزارهای خودکار
حمله SIFA و راهکارهای مقابله
پیاده‌سازی امن در بستر سخت‌افزار در مقابل تحلیل توان (و القاء خطا)
ابزارهای تحلیل خودکار
حملات کانال جانبی تحلیل توان
Profiling Attacks
طراحی از منظر پیاده‌سازی
آشنایی با پیاده سازی الگوریتم‌های رمزنگاری
آشنایی با مقدمات ریاضی
پیاده‌سازی زمان ثابت و حملات کاربردی مرتبط
حملات کانال جانبی زمان
حملات ریزپردازنده
رمزنگاری جعبه سفید
حملات جعبه سفید و راهکارهای مقابله

# نشست‌های جانبی

# نشست پرسمان آزاد (Ask Me Anything)

- دکتر امیر مرادی؛ دانشیار دانشگاه Ruhr آلمان
- مسئول کمیته علمی کنفرانس CHES 2020
- محقق برجسته بین‌المللی در حوزه پیاده‌سازی امن و به طور خاص حملات کانال جانبی توان و القاء خطا

# نشست آشنایی با آزمایشگاه های فعال در صنعت

- در این نشست، مسئولین آزمایشگاه-های فعال در صنعت تجارب خود در حوزه پیاده‌سازی امن الگوریتم‌های رمزنگاری را به اشتراک خواهند گذاشت.
- دکتر بشیرپور، محقق ارشد شرکت متیران
- مهندس مهری یحیایی، مدیر آزمایشگاه‌های فناوری اطلاعات مرکز تحقیقات صنایع انفورماتیک

# نکات پایانی

- فیلم‌های نشست‌های کارگاه مقدماتی و مدرسه زمستانه در کانال آپارات انجمن قرار خواهند گرفت. با عضویت در کانال می توانید از آخرین به روزرسانی‌ها مطلع شوید.

  https://www.aparat.com/Irancrypt

- اسلایدها در سایت‌های کارگاه مقدماتی و مدرسه زمستانه قرار خواهند گرفت.
- در صورت داشتن هرگونه سوال و یا هرگونه مشکل، تیم برگزار کننده آماده پاسخگوئی هستند.
  - ایمیل: iscwsisc2021@sbu.ac.ir
  - شماره تماس: ۰۲۱۲۹۹۰۵۴۷۵

# با تشکر از توجه شما

The picture is courtesy of Lejla Batina