

Security Analysis of a Fingerprint Fuzzy Vault

Patrick Perry

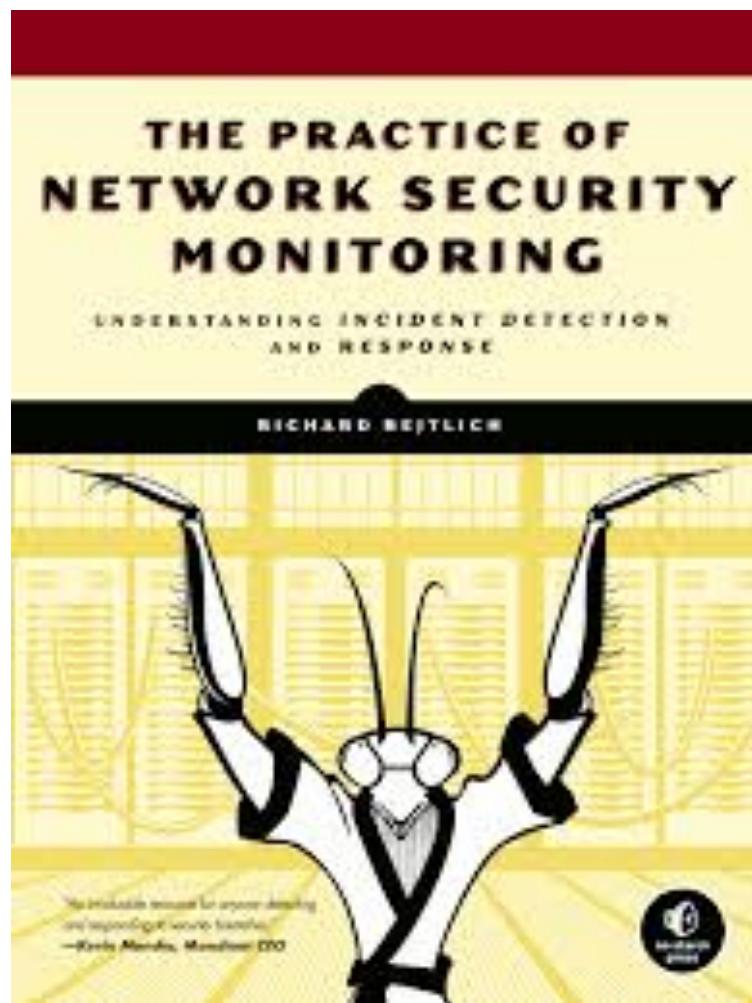
@pjberry

#FFVSEC





The Mandiant logo consists of a dark red square icon followed by the word "MANDIANT" in a bold, uppercase, sans-serif font. A registered trademark symbol (®) is located at the top right of the "T".



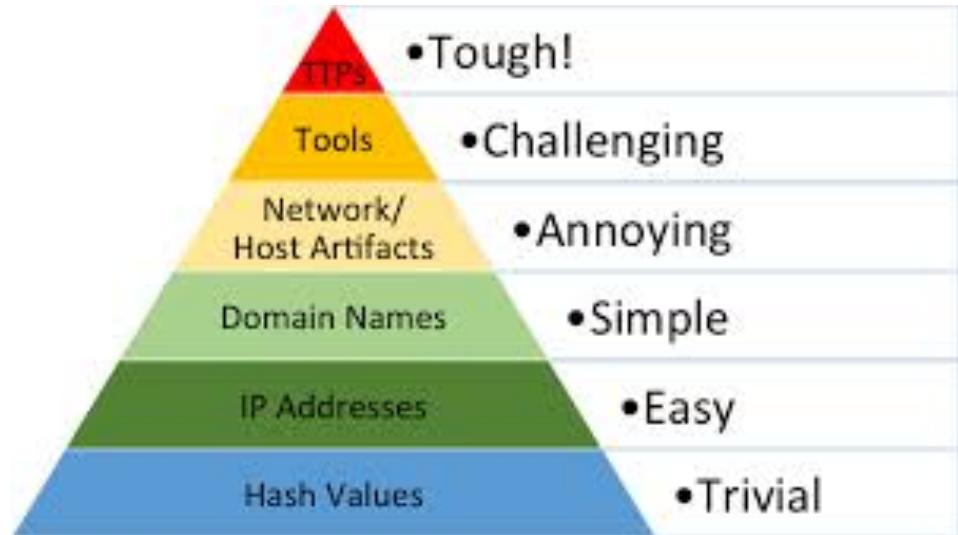
<http://taosecurity.blogspot.com/>



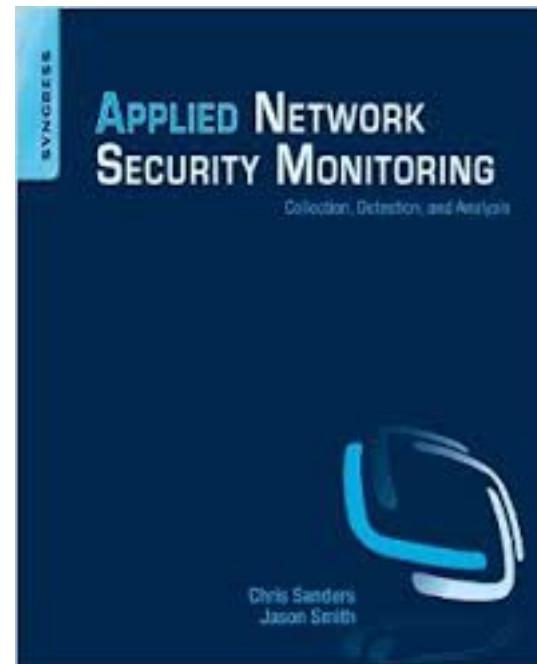
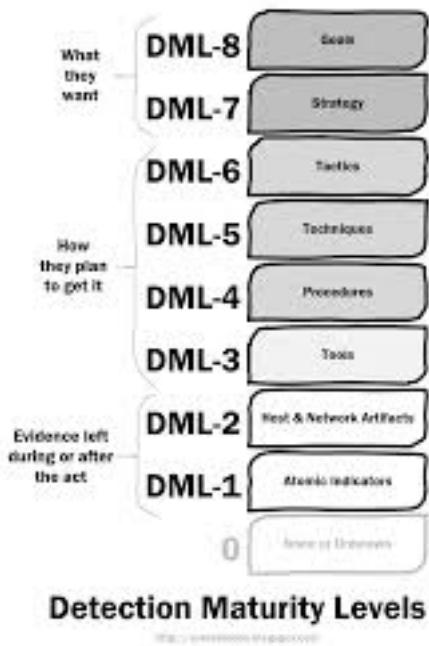
[http://bammv.github.io/
sguil/index.html](http://bammv.github.io/sguil/index.html)



<https://snorby.org/>



[http://detect-respond.blogspot.com/
2013/03/the-pyramid-of-pain.html](http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html)



[http://
ryanstillions.blogspot.co
m/2014/04/the-dml-
model_21.html](http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html)

<http://www.appliednsm.com/>





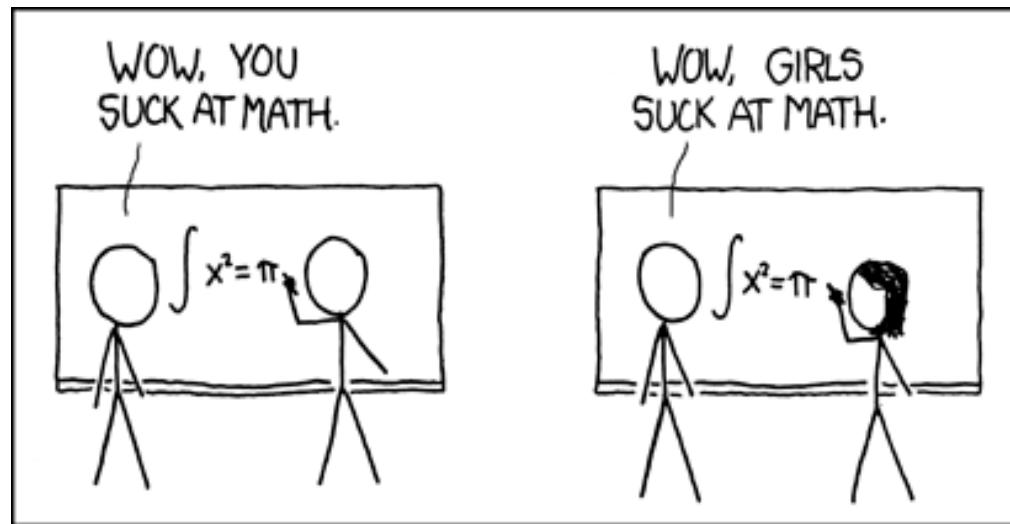
www.infosec.jmu.edu



xunhua wang

213
OFFICE

COMPUTER SCIENCE
DR. STEVE WANG

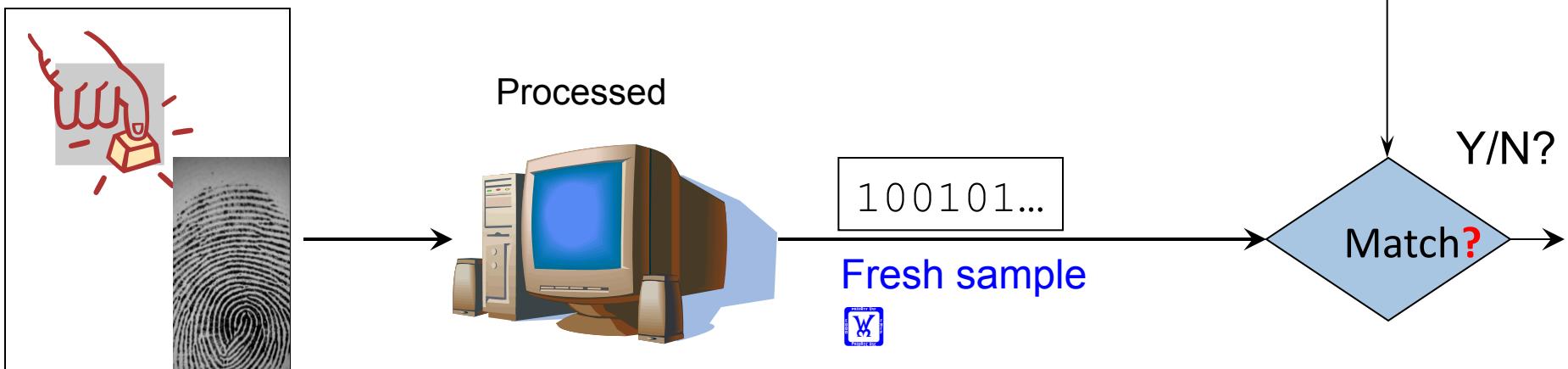
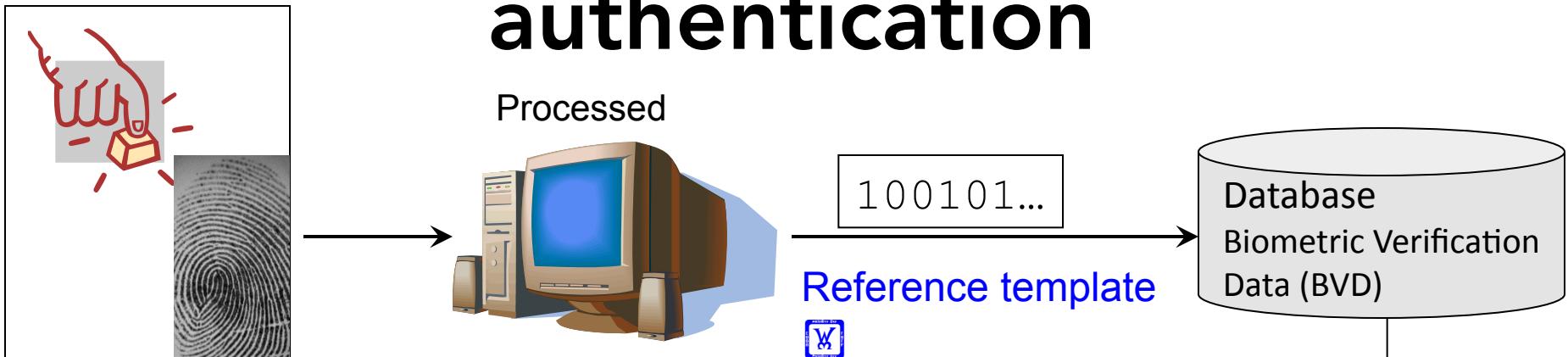


<http://xkcd.com/385/>



biometric authentication

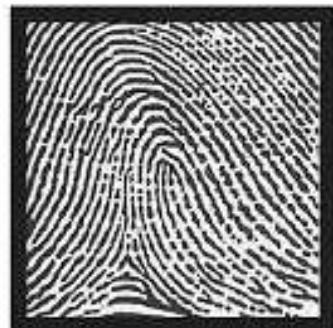
traditional fingerprint authentication



beyond simple authentication: fingerprint applications – vault



variation



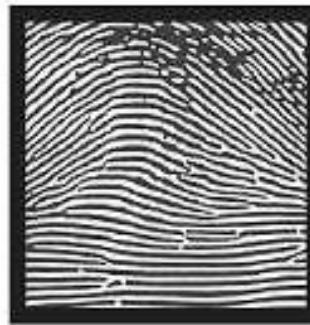
Right Loop



Left Loop



Whorl



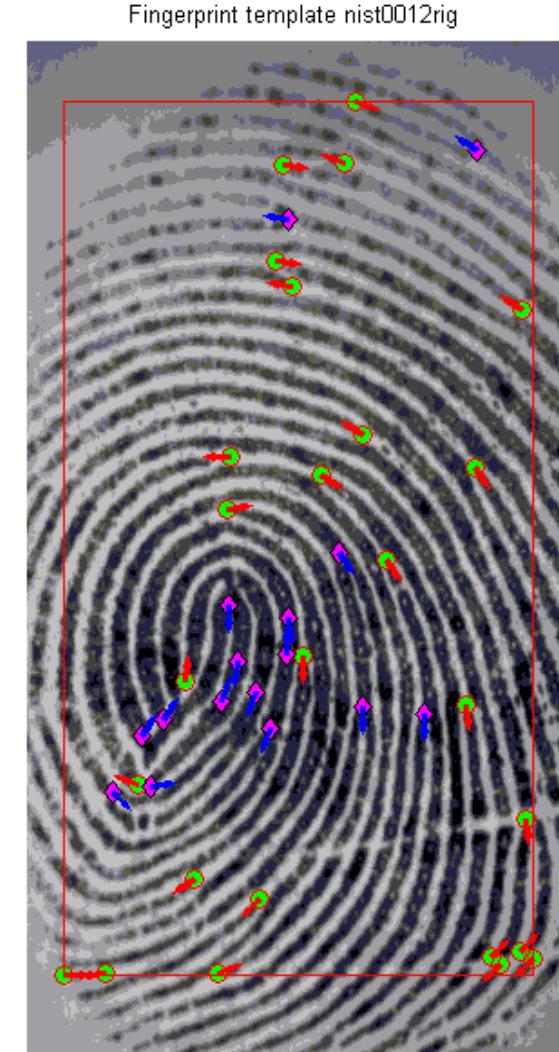
Arch



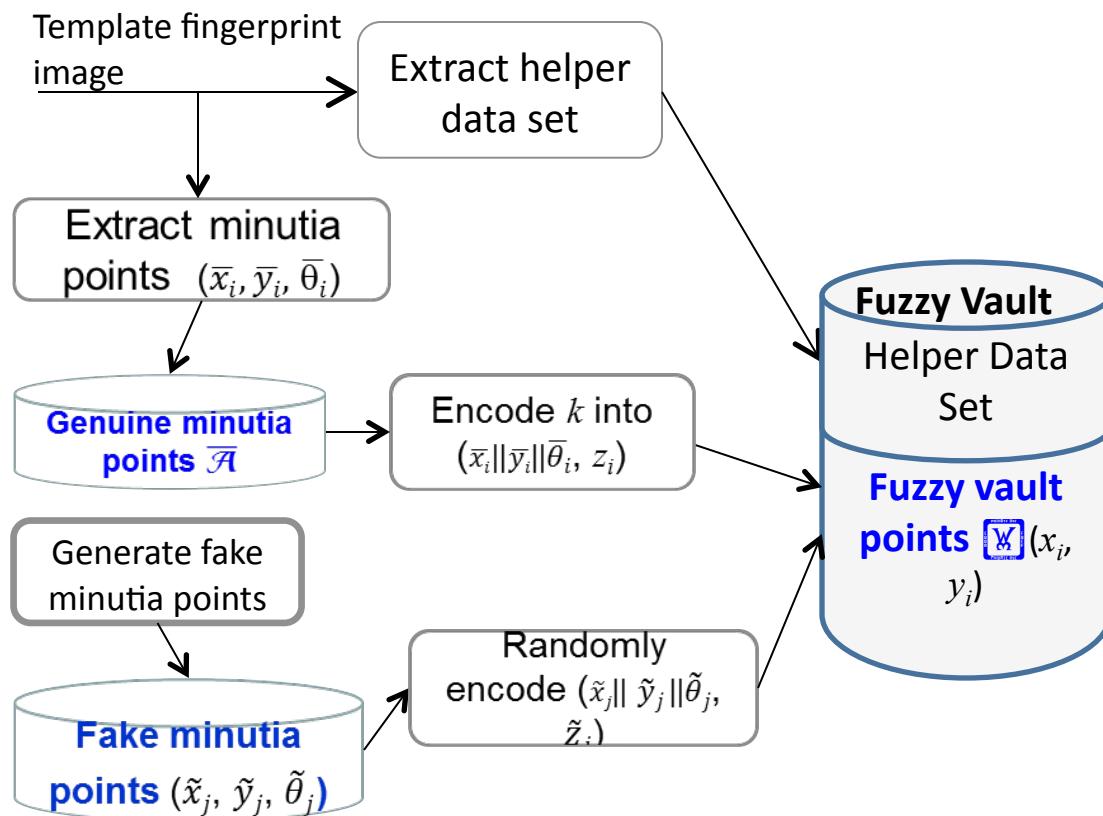
Tented Arch

identifiers

- ridge, valley
- minutia points
 - ridge ending
 - bifurcation
 - (x,y,theta)



fingerprint fuzzy fault NJP07

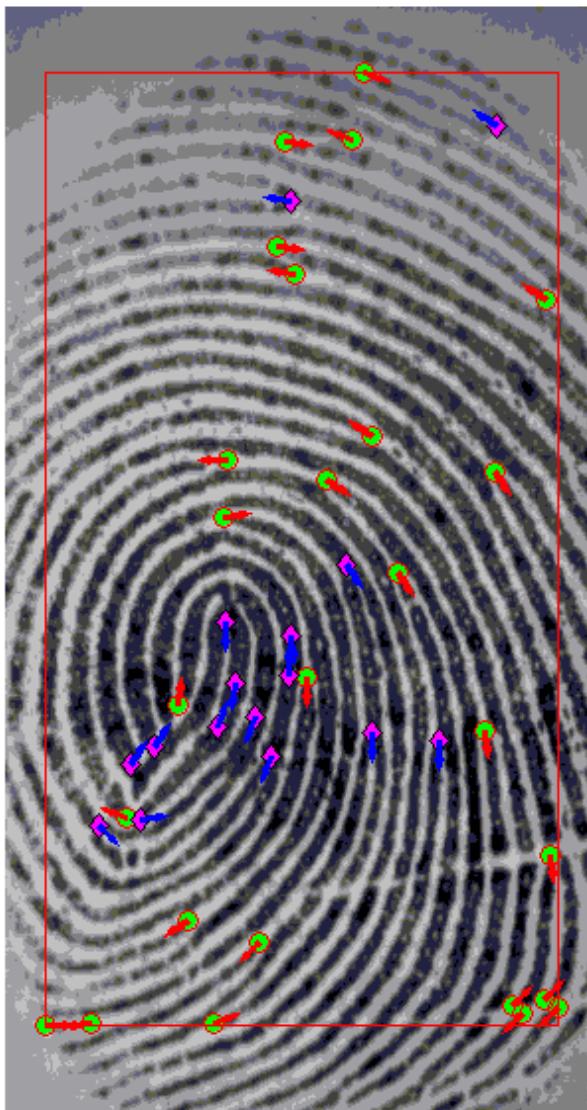


- **fingerprint minutia points are **not** integers**
- **minutia point comparison is **not** exact**

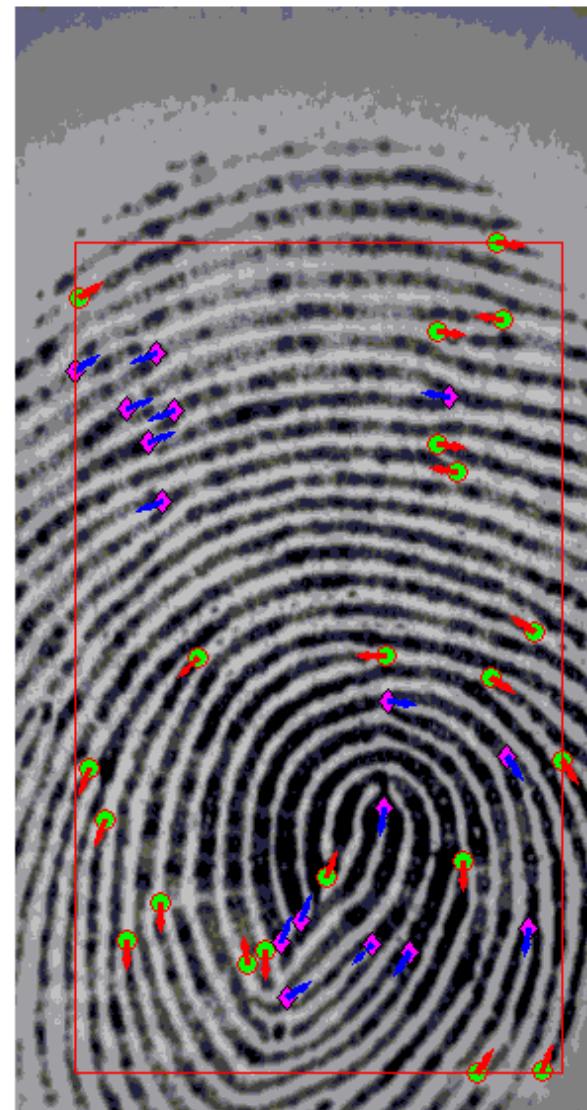


alignment is a bitch

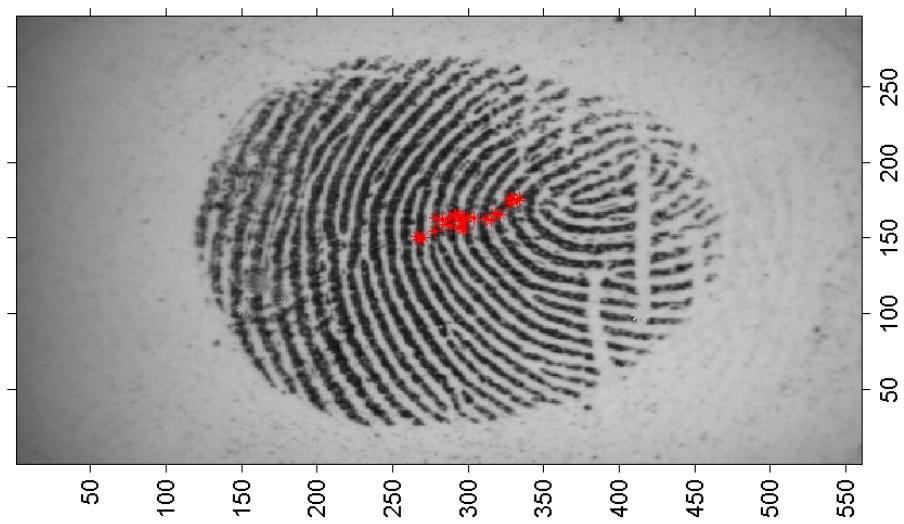
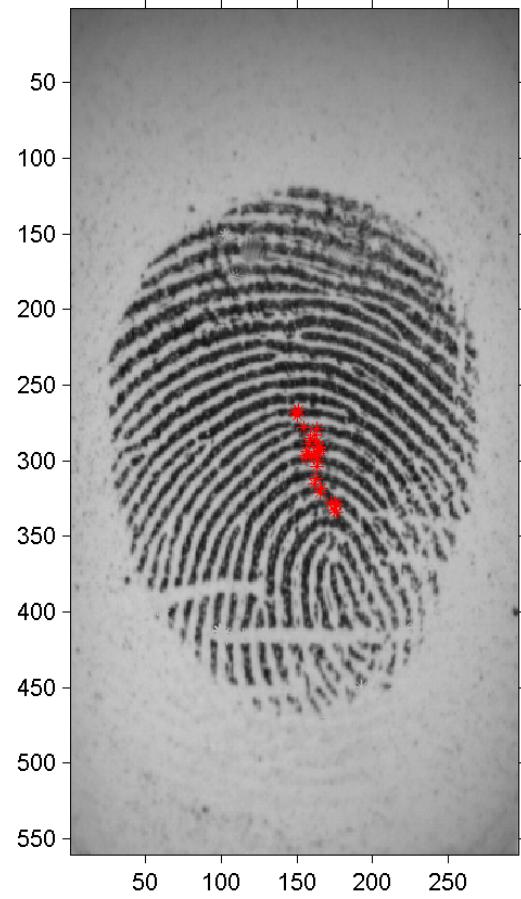
Fingerprint template nist0012rig



Fingerprint template nist0017rig



helper data





**an attack predicated on
occam's razor**

does the helper data leak?

"Since high curvature points are global features in the fingerprint pattern, they do not reveal any information about the minutia attributes which are local characteristics in the fingerprint. Moreover, the helper data do not contain sufficient information to estimate the orientation field or reconstruct the complete fingerprint pattern.... Therefore, the proposed helper data do not affect the security of the fuzzy vault."

No, because we said so.





now what?



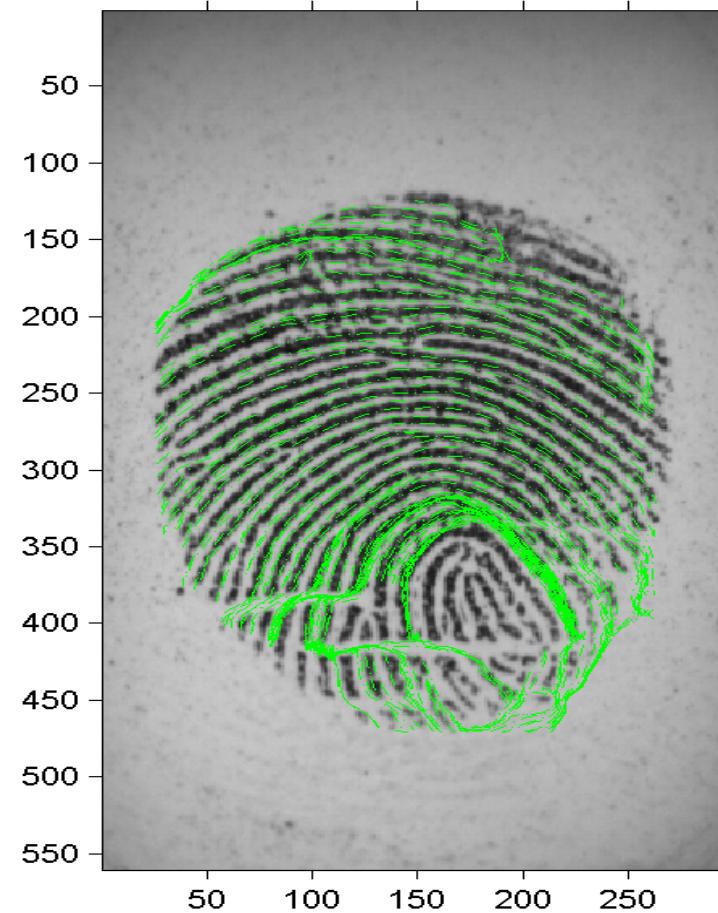
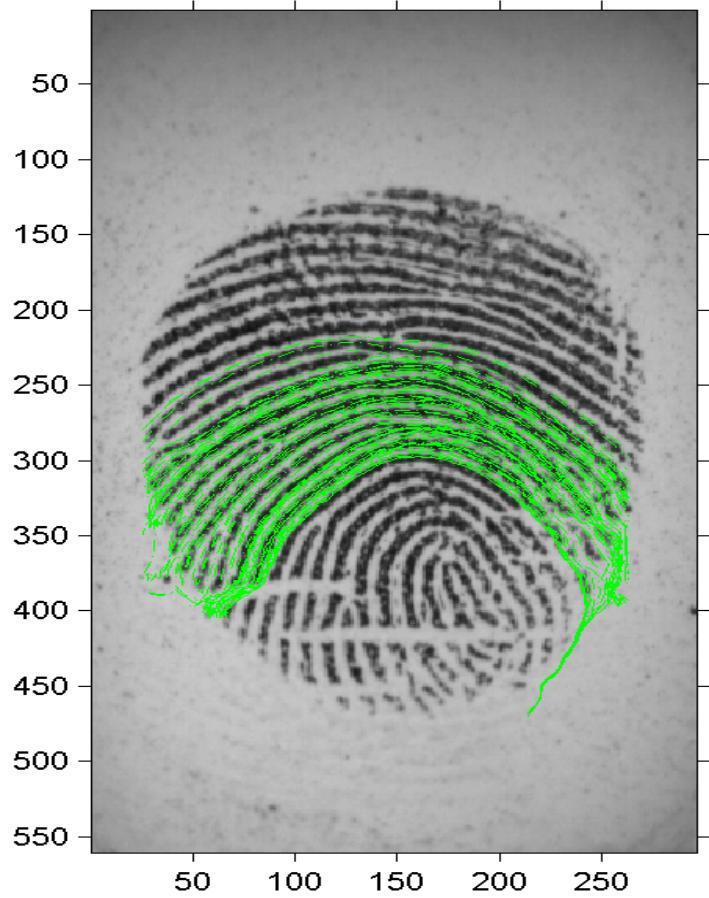
screw it, i'll do it myself

- get a large sample of fingerprints
- model the fingerprints (trace the ridges)
- find the high curvature points (helper data)
- analysis (does the helper data leak?)
- profit

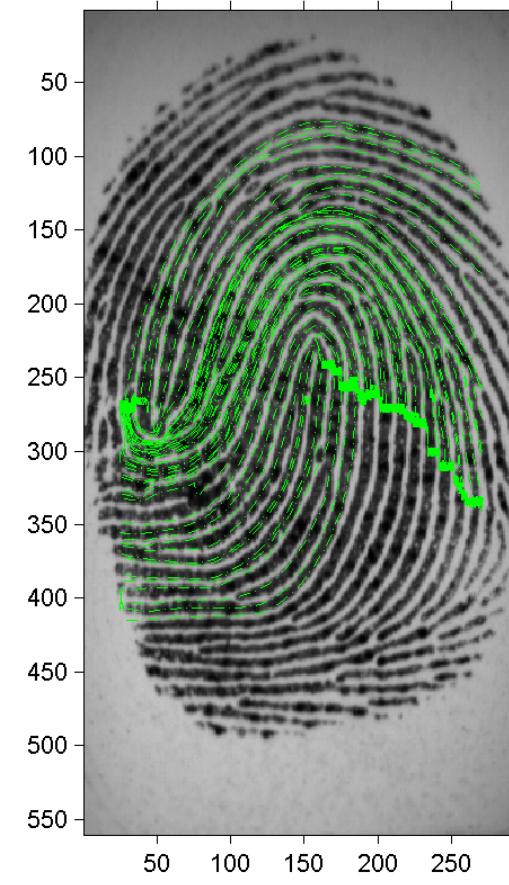
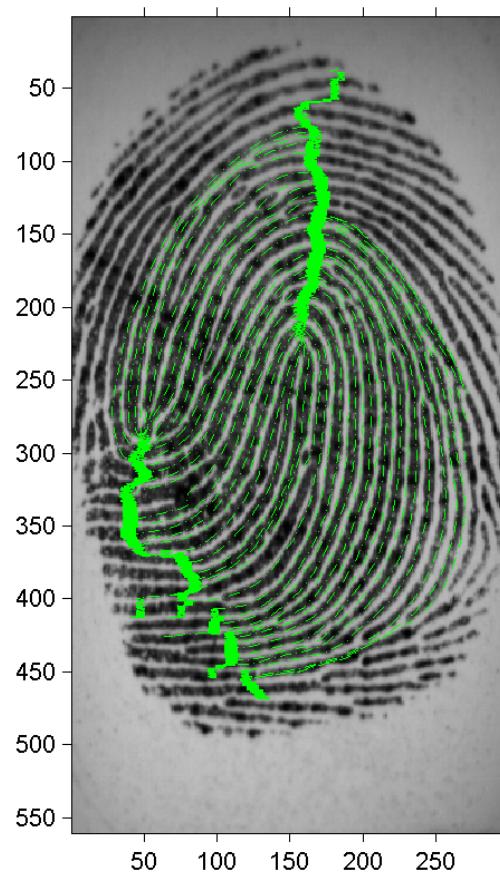
hobos



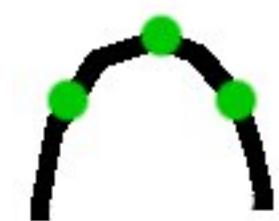
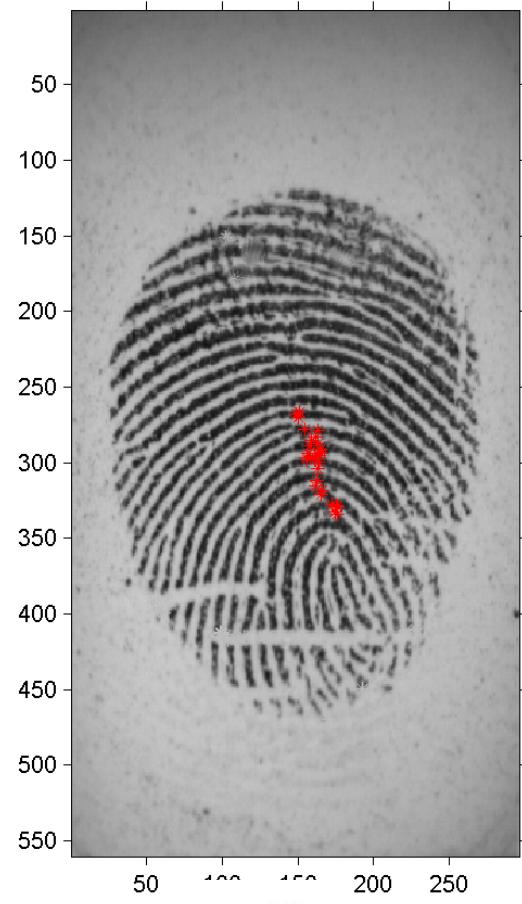
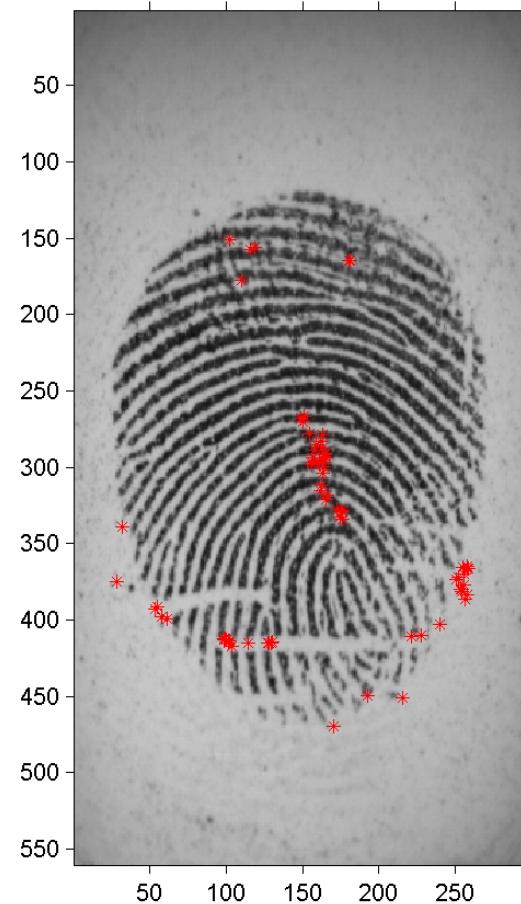
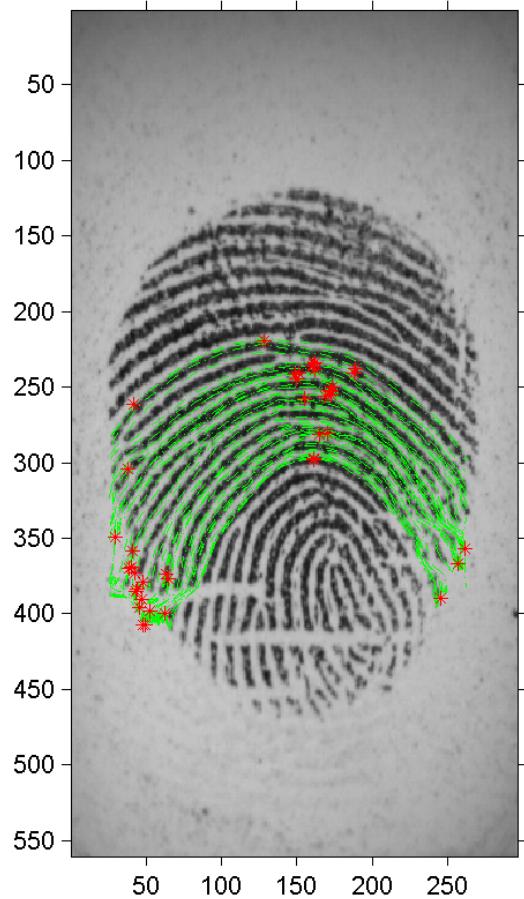
walk the line



trip on the aforementioned line

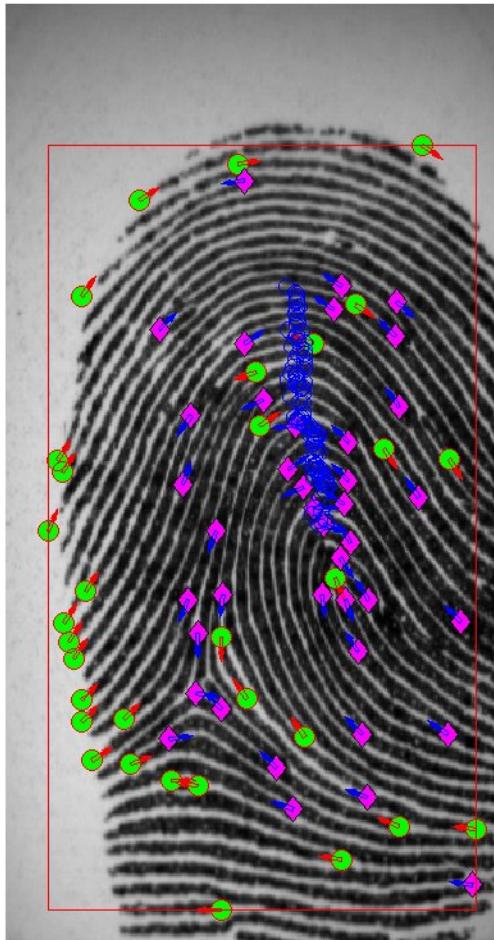


high curvature points/helper data

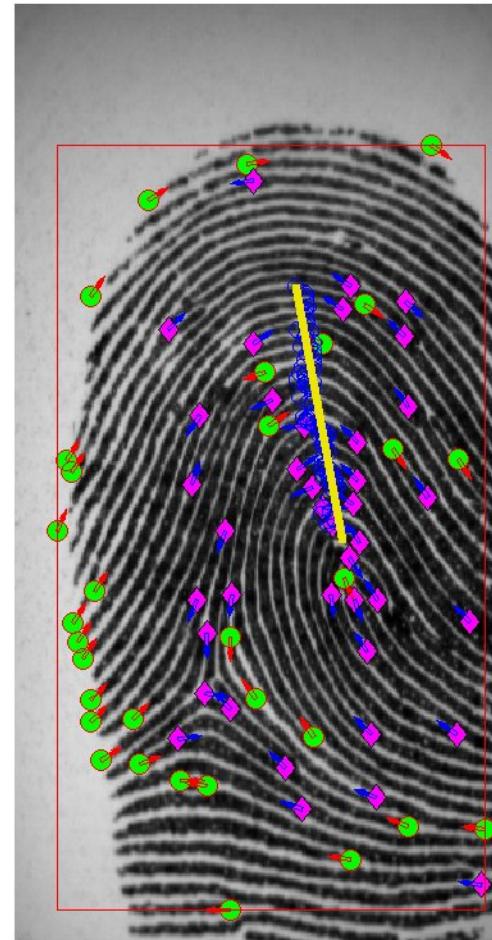


so, lets get started

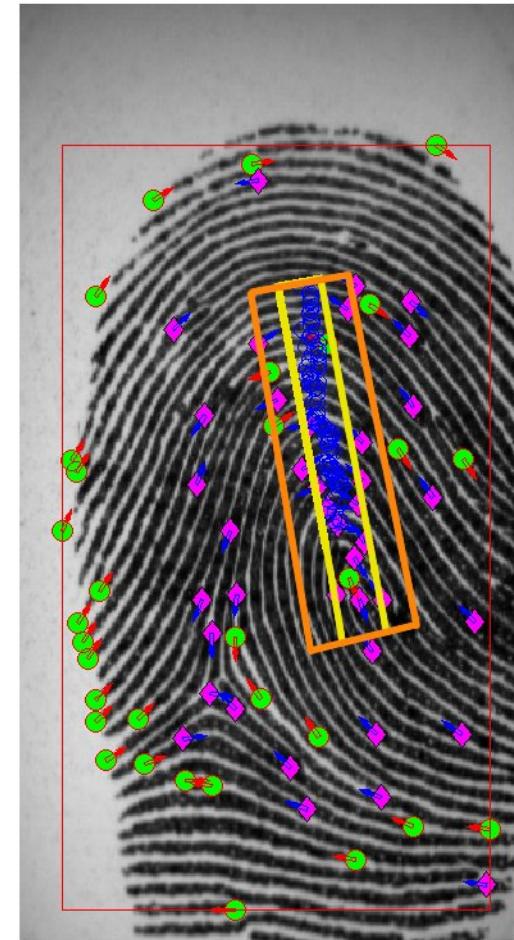
Fingerprint template nist0521rig



Fingerprint template nist0521rig



Fingerprint template nist0521rig



and boom goes the dynamite

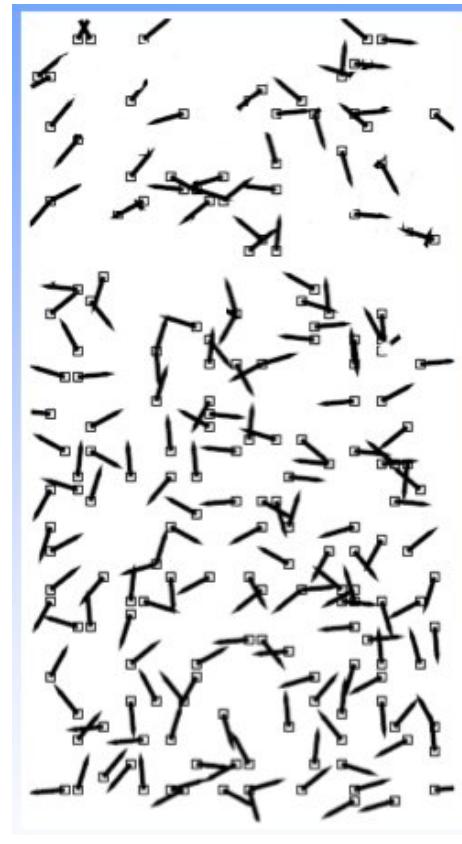
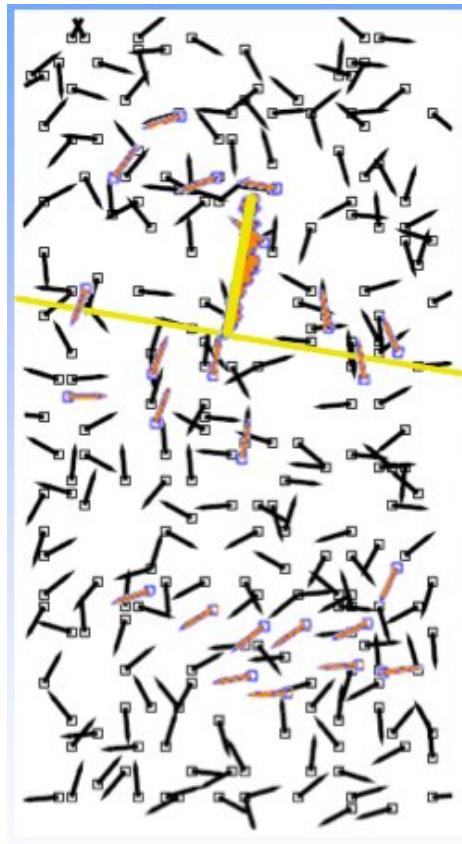
Results for 10% by 125%

	All fingerprints	Fingerprints with greater minutia points than expected	Fingerprints with fewer minutia points than expected
Chi-square	720.41	697.89	22.52
Degrees of freedom	199	148	50
p-value	< 0.001	< 0.001	0.9997

Results for 25% by 125%

	All fingerprints	Fingerprints with greater minutia points than expected	Fingerprints with fewer minutia points than expected
Chi-square	506.97	492.84	14.13
Degrees of freedom	199	157	41
p-value	< 0.001	< 0.001	0.9999

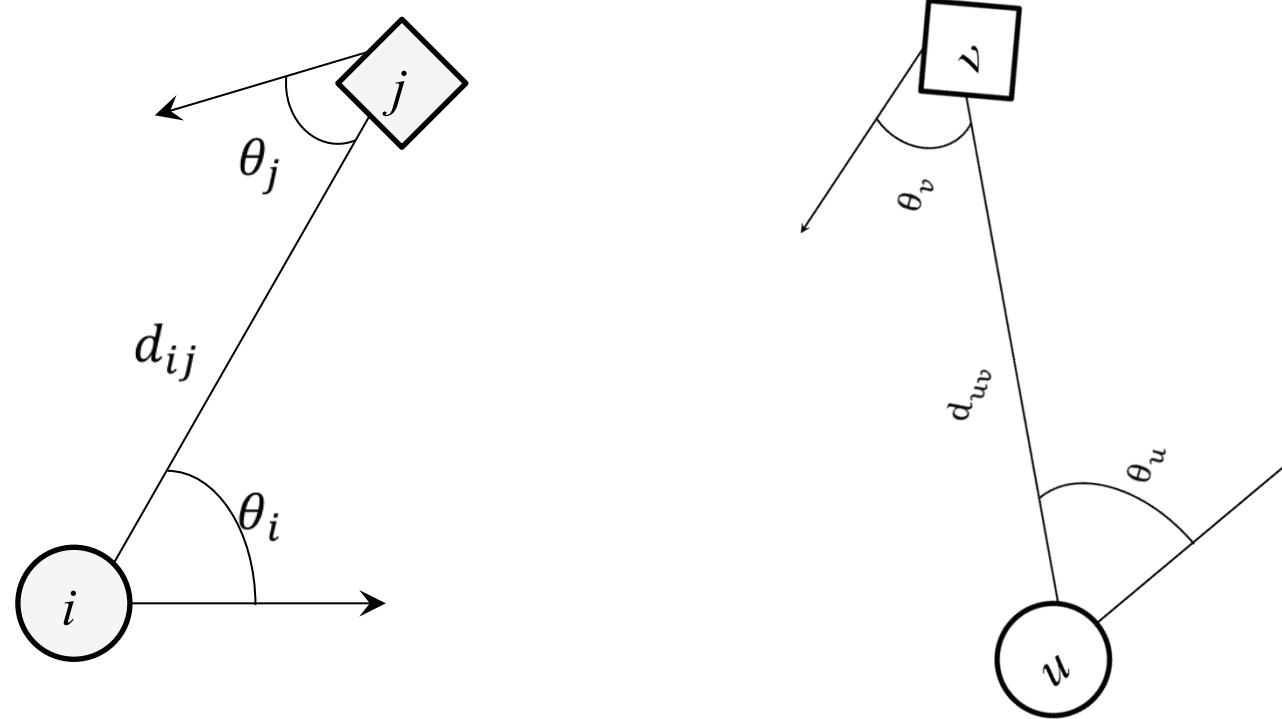
chaffe elimination attack



the fingerprint fuzzy vault is broken

“Since the helper data are stored as public information, it should not reveal any information about the template minutiae used for constructing the vault because any such leakage would compromise the security.”

proposed solution- bozorth





questions?

Patrick Perry
@pjberry
#FFVSEC