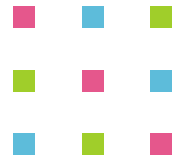
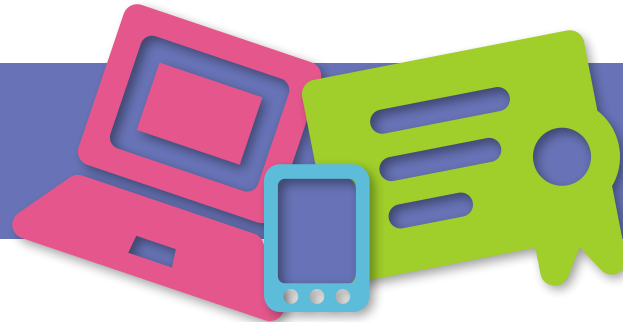


SECURITY 2015



23. ročník konference o bezpečnosti v ICT



Biometrics as Signal Detection Problem

Tomáš Rosa

Raiffeisenbank, a.s.



Signals Primer

- Let *a signal* be any detectable space-time varying quantity conveying information about physical phenomena.
- *Signal detection* is then an ability to discern between information-bearing patterns (signals) and random patterns (noise) that distract from the information.

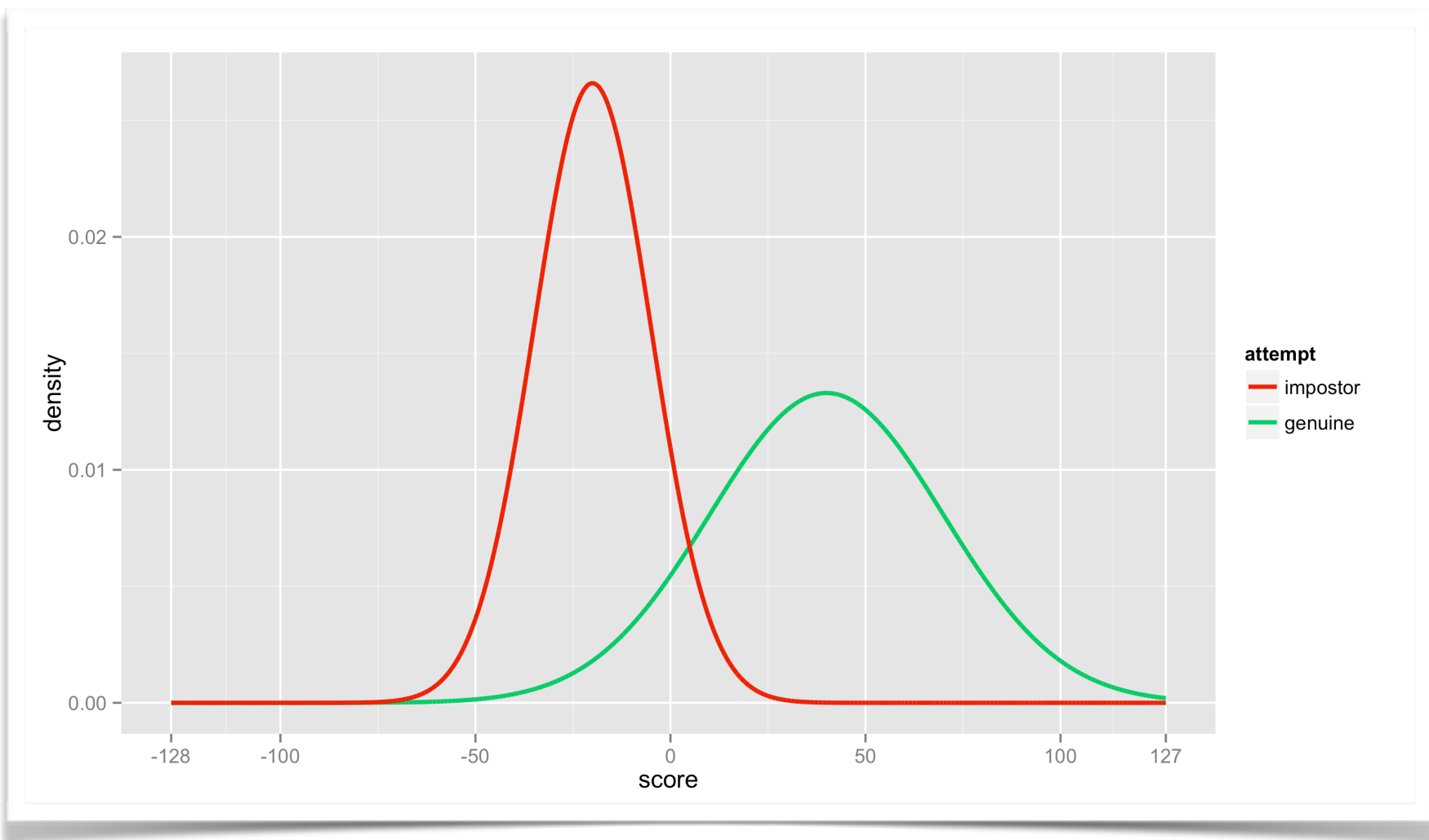


Match Score

- It would be nice if we had a simple **true-false** result.
 - As in conventional crypto.
 - But we cannot...
- All we have is a value of random variable X that follows two conditional distributions.
 - $f(x \mid \text{impostor})$
 - $f(x \mid \text{genuine})$

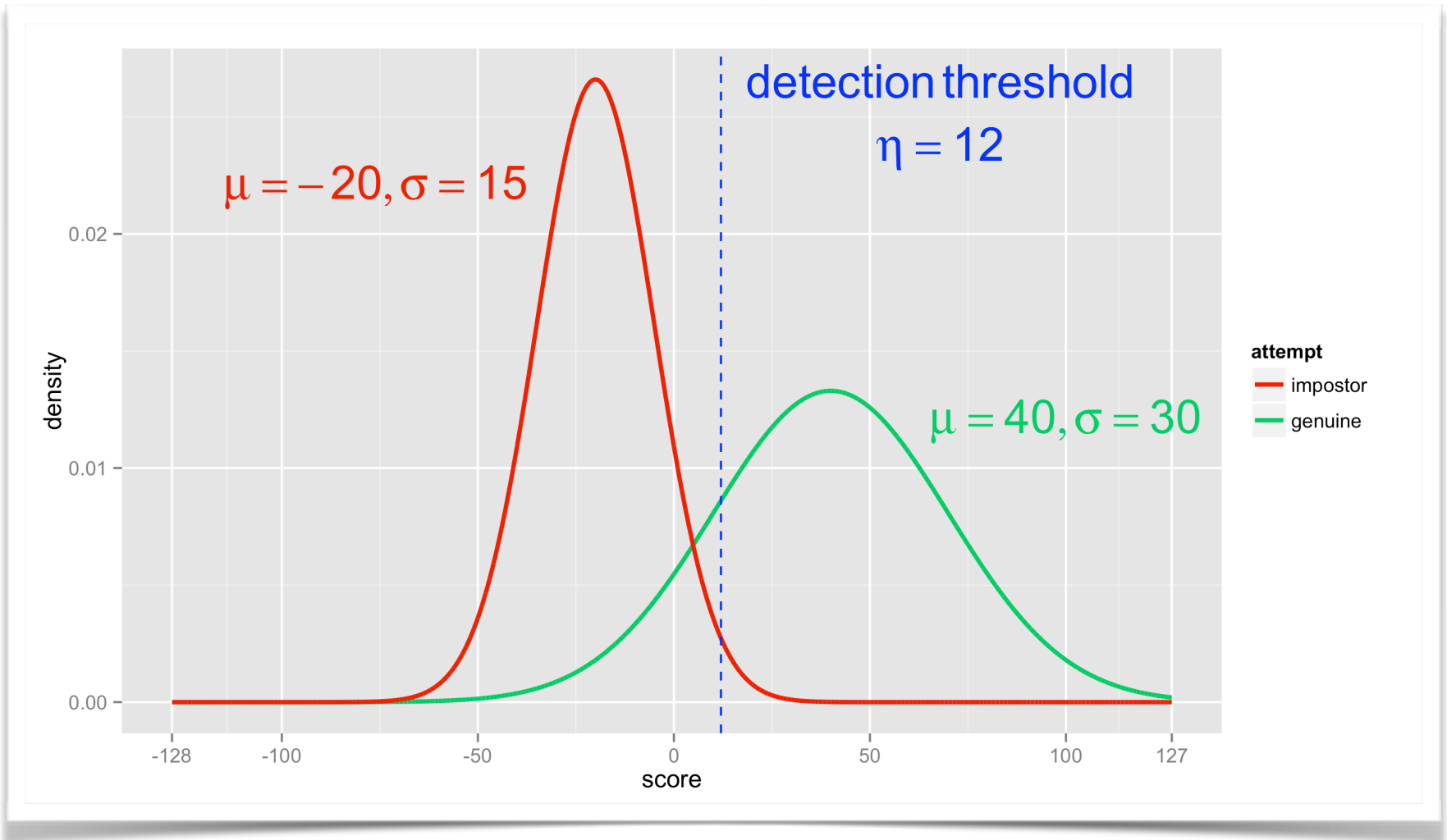


Base “Camel” Graph

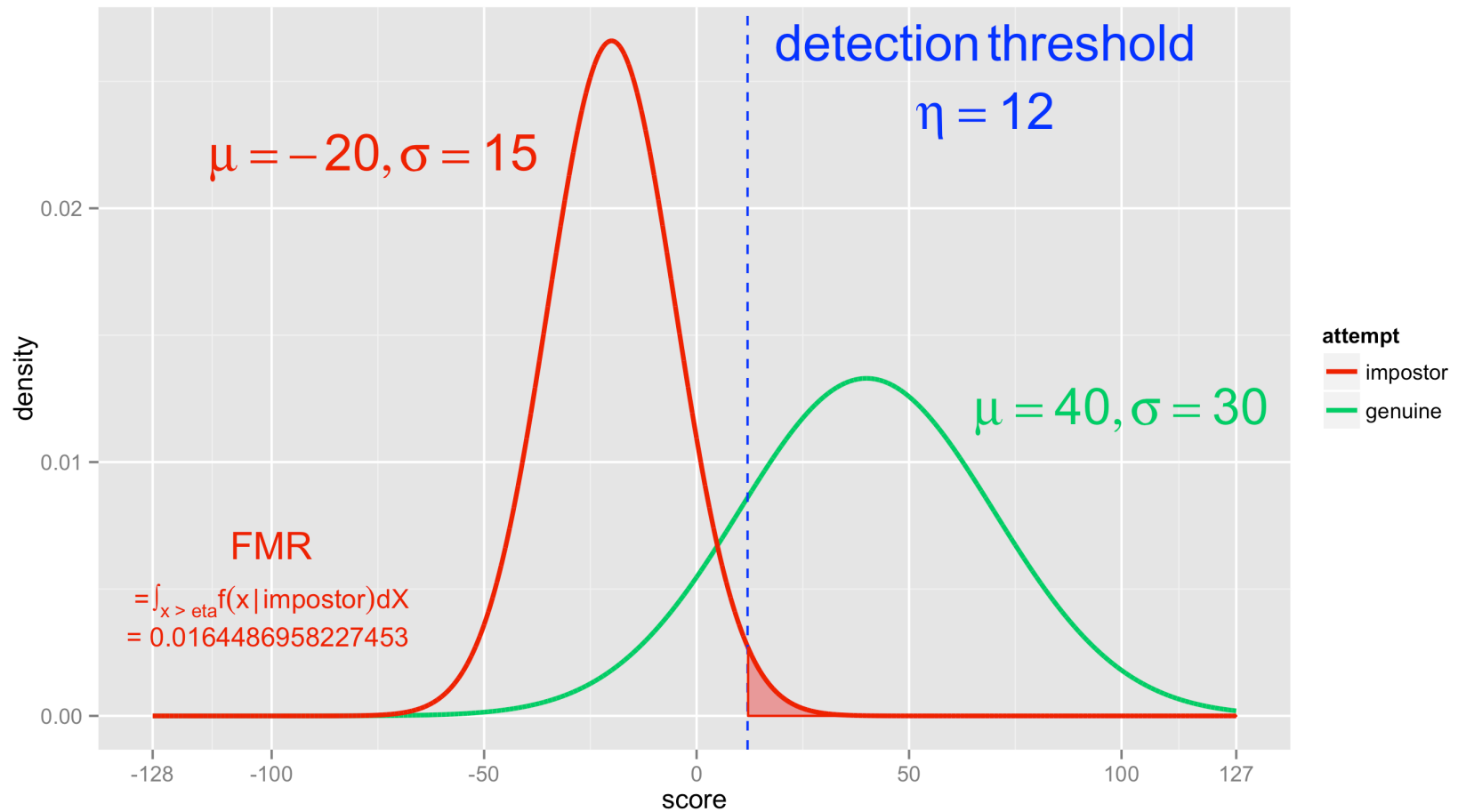




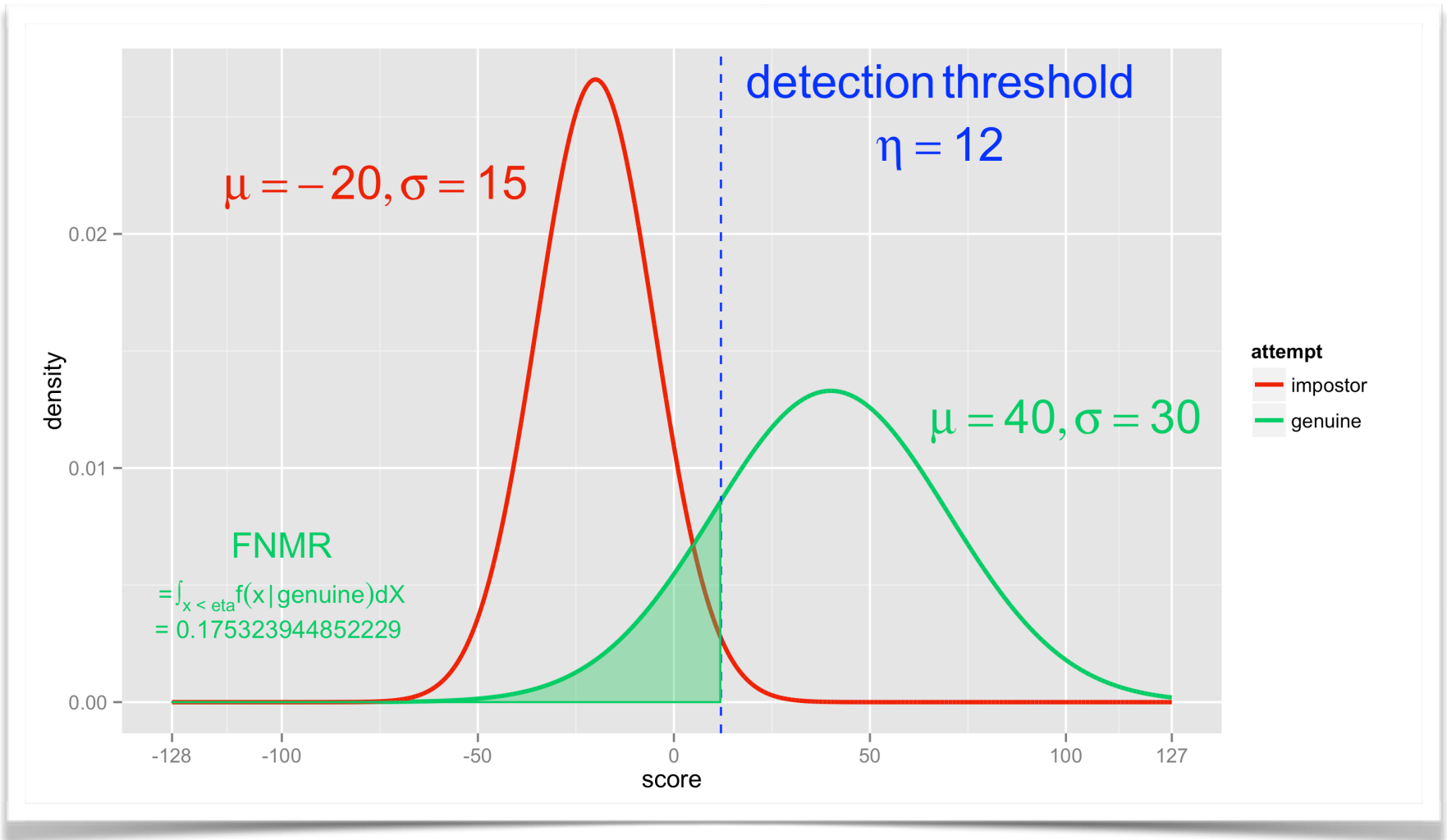
Signal Detection Approach



False Match Rate

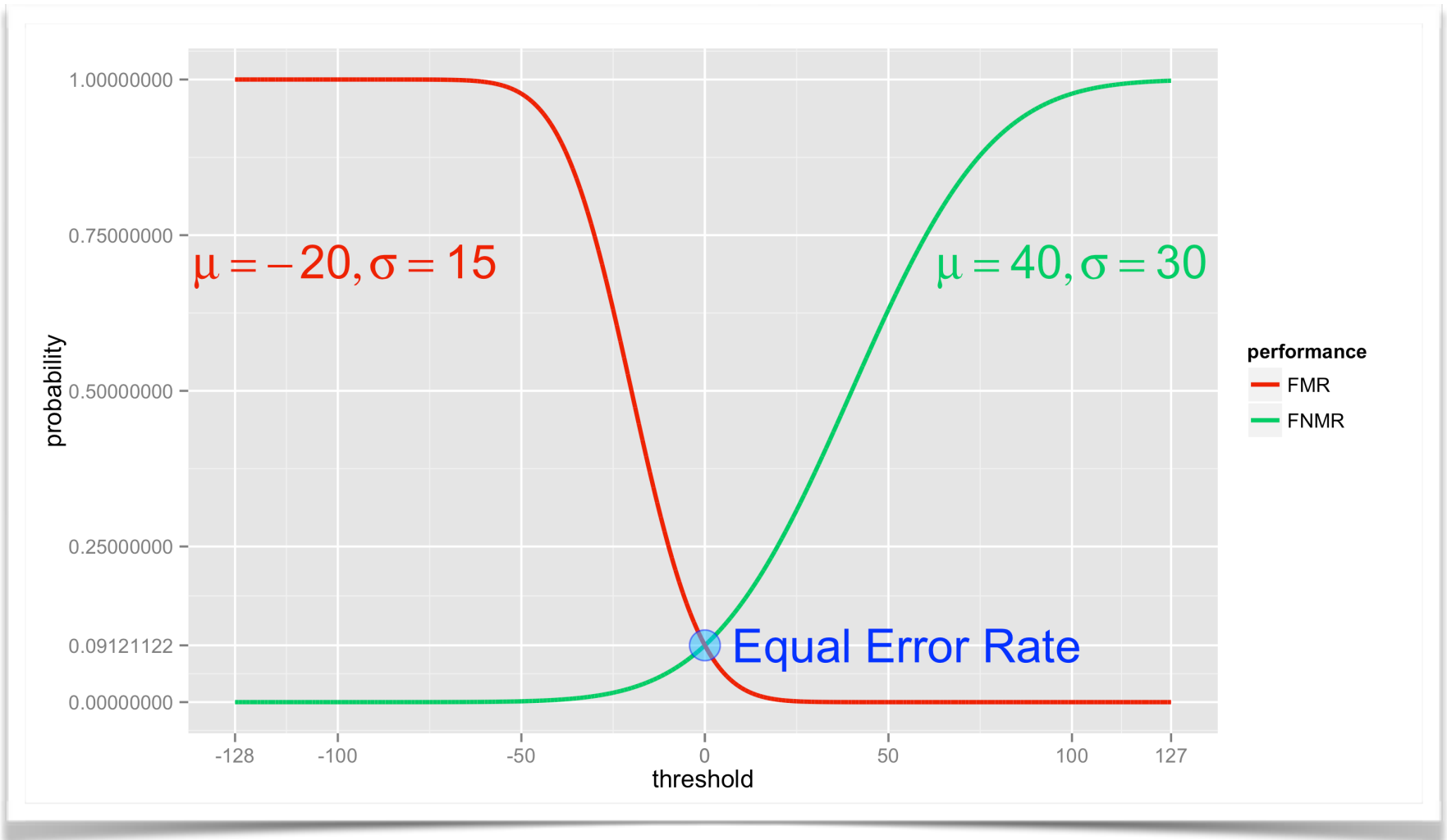


False Non-Match Rate



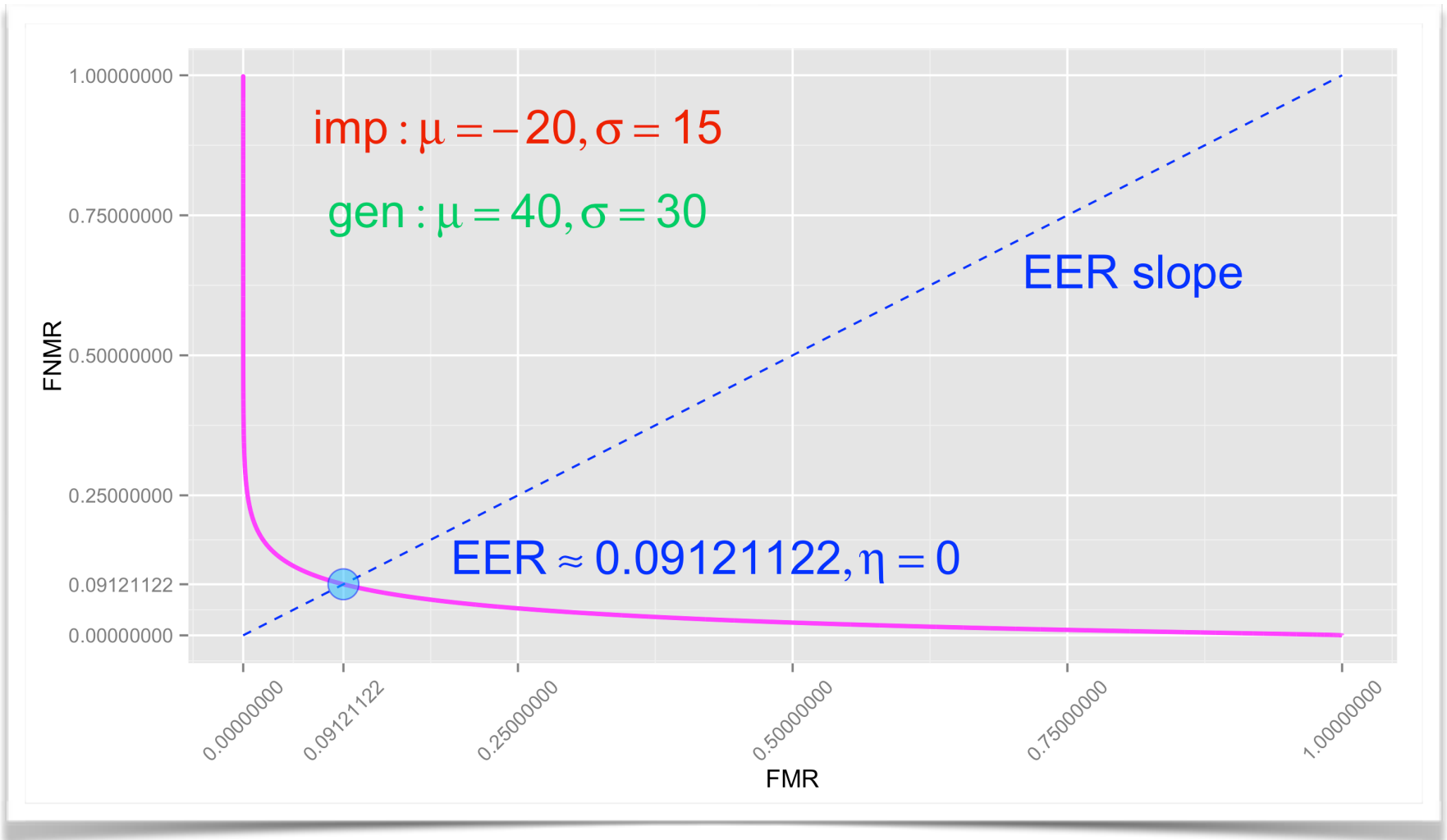


Error Distribution Functions



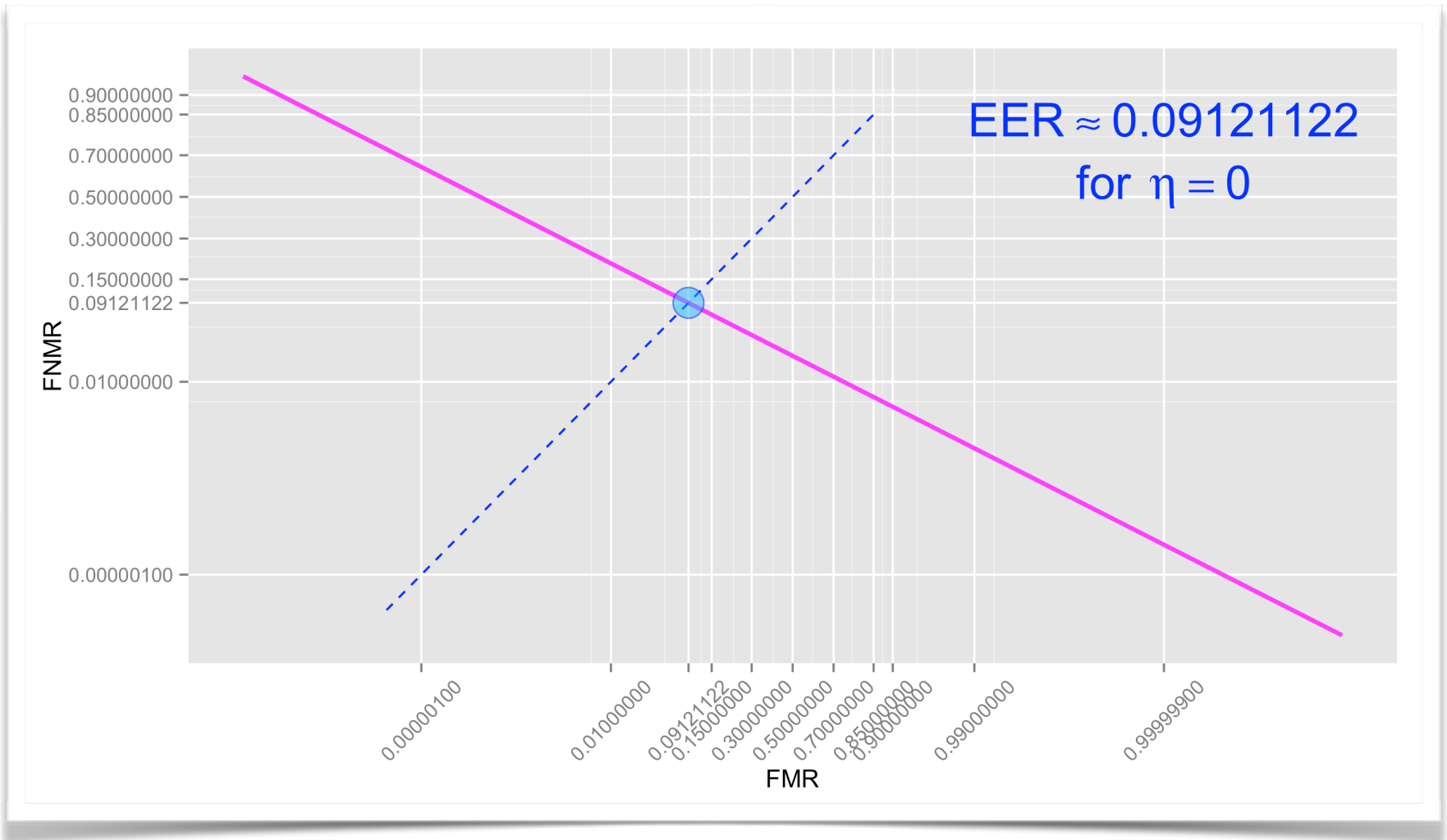


Receiver Operating Characteristics





Detection Error Trade-Off





ISO/IEC 19795

- Performance test methodologies for different life-cycle phases:
 - technology evaluation
 - scenario evaluation
 - operational evaluation
- We get comparable results with plausible confidence intervals.

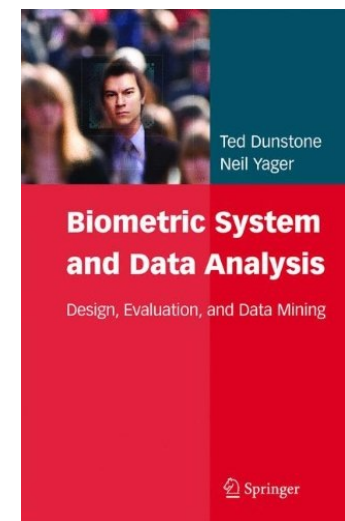


Bunch of Parameters

- False Match Rate / False Non-Match Rate
 - attempt oriented
- False Acceptance Rate / False Rejection Rate
 - transactional version of FMR/FNMR
- Failure To Acquire
- Failure To Enroll
 - both attempt and txn-oriented versions

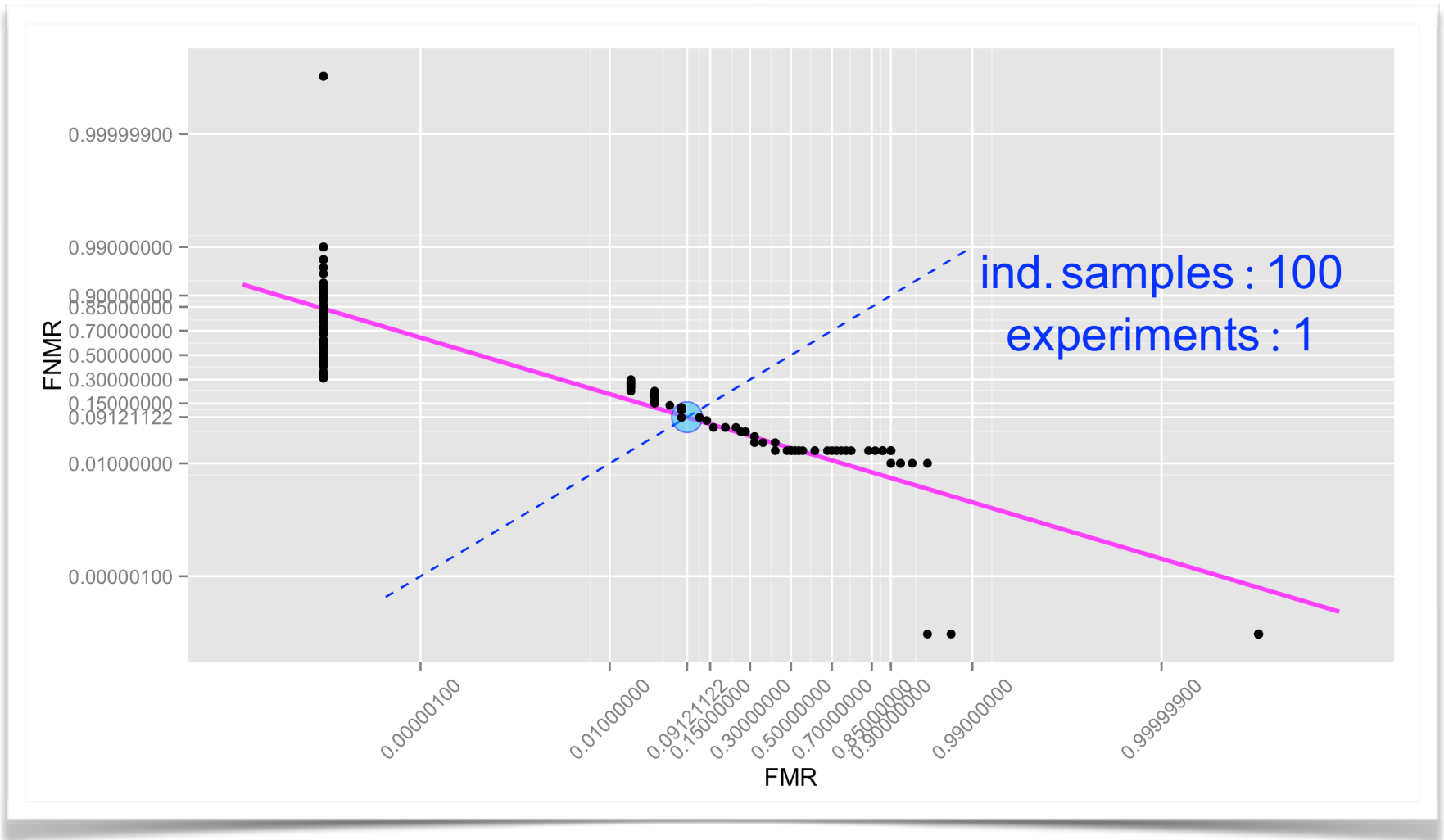
Biometric Data Mining

- In any life-cycle phase, we shall gather as much data as we can to estimate the performance or check we are still operating in expected margins.
- Anomalies may indicate a component malfunction or even a fraud.
- Again, be careful about confidence.
- Misleading statistics can be worse than none!

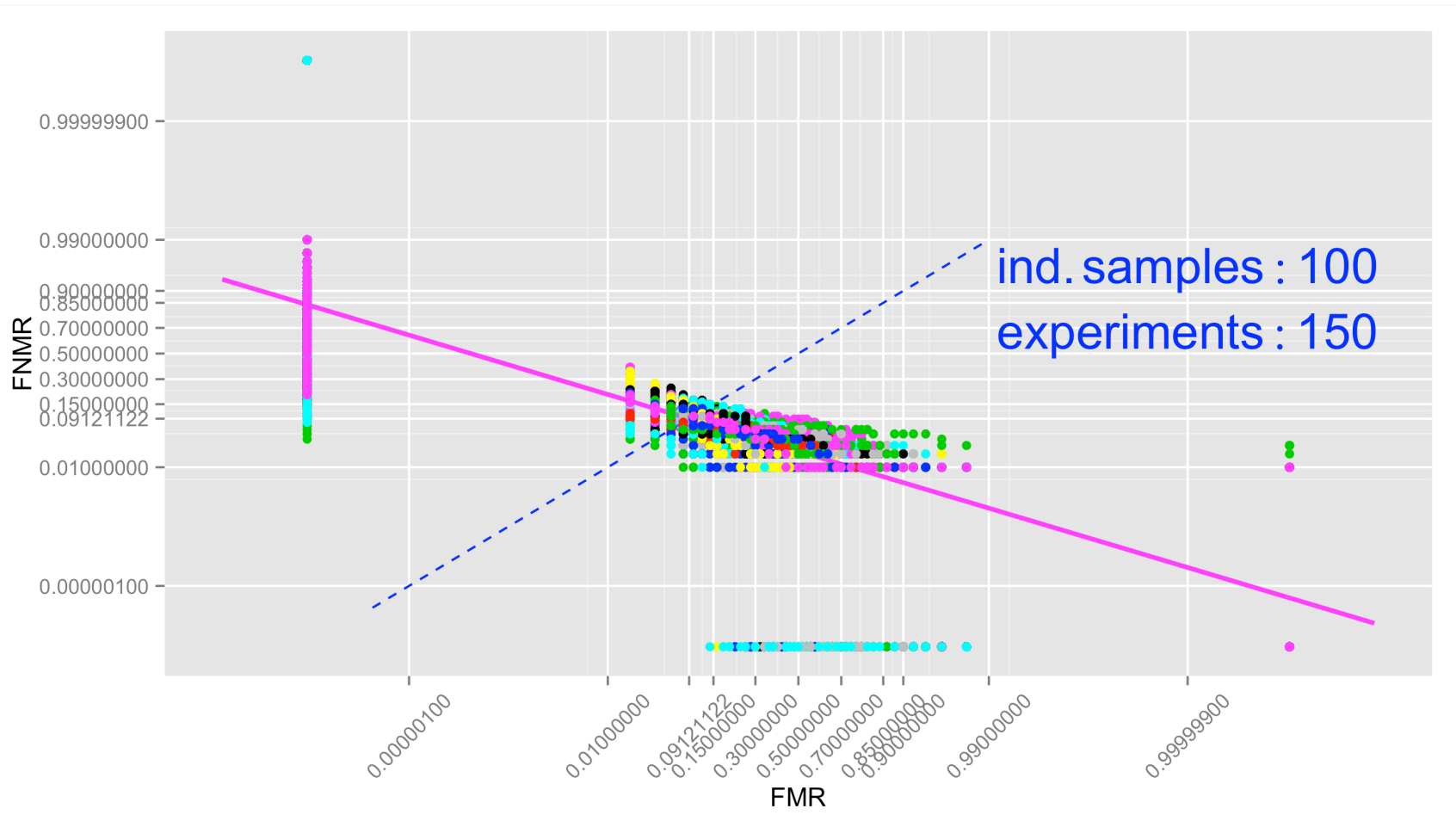




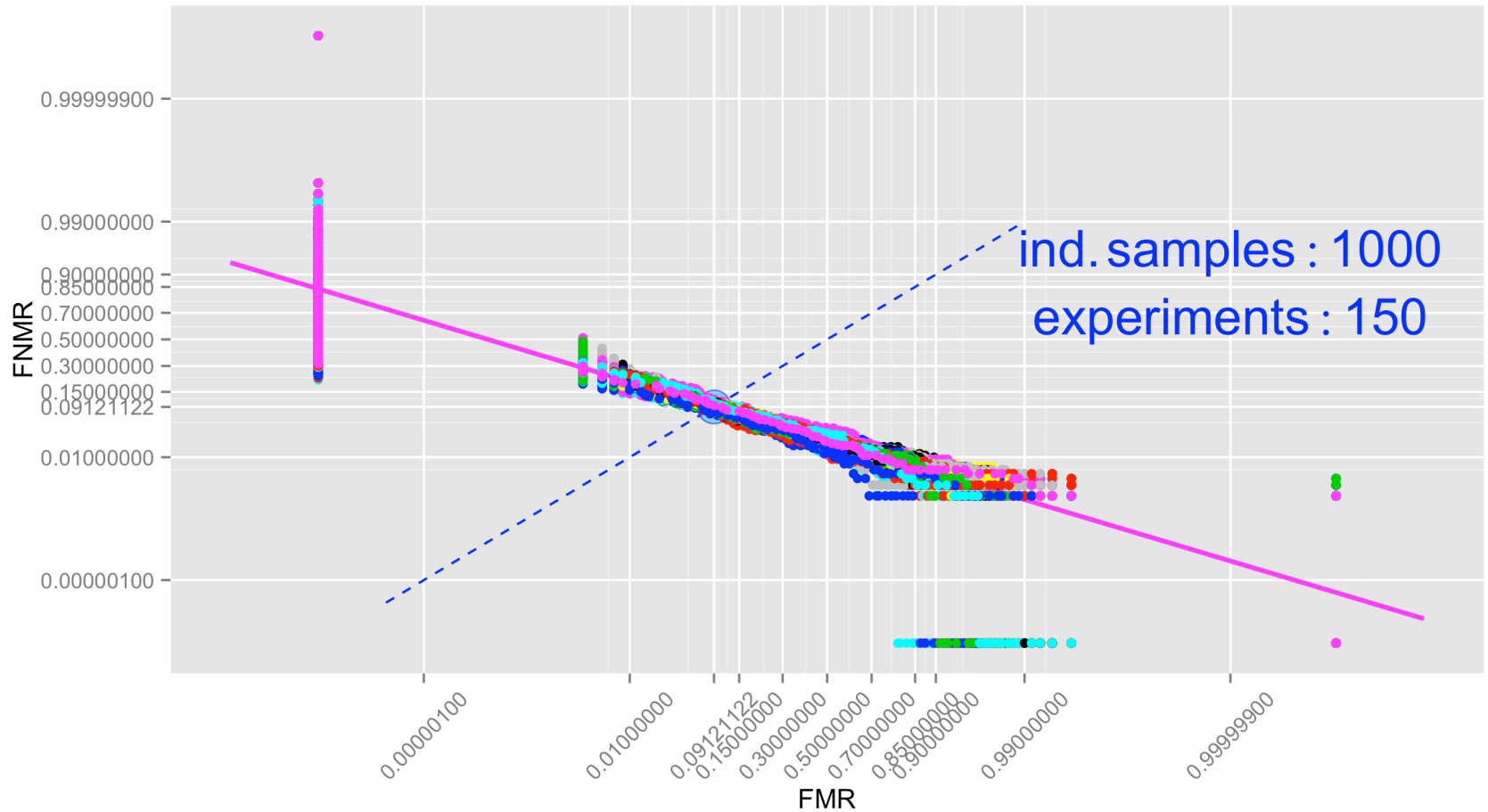
DET Estimation Simulation



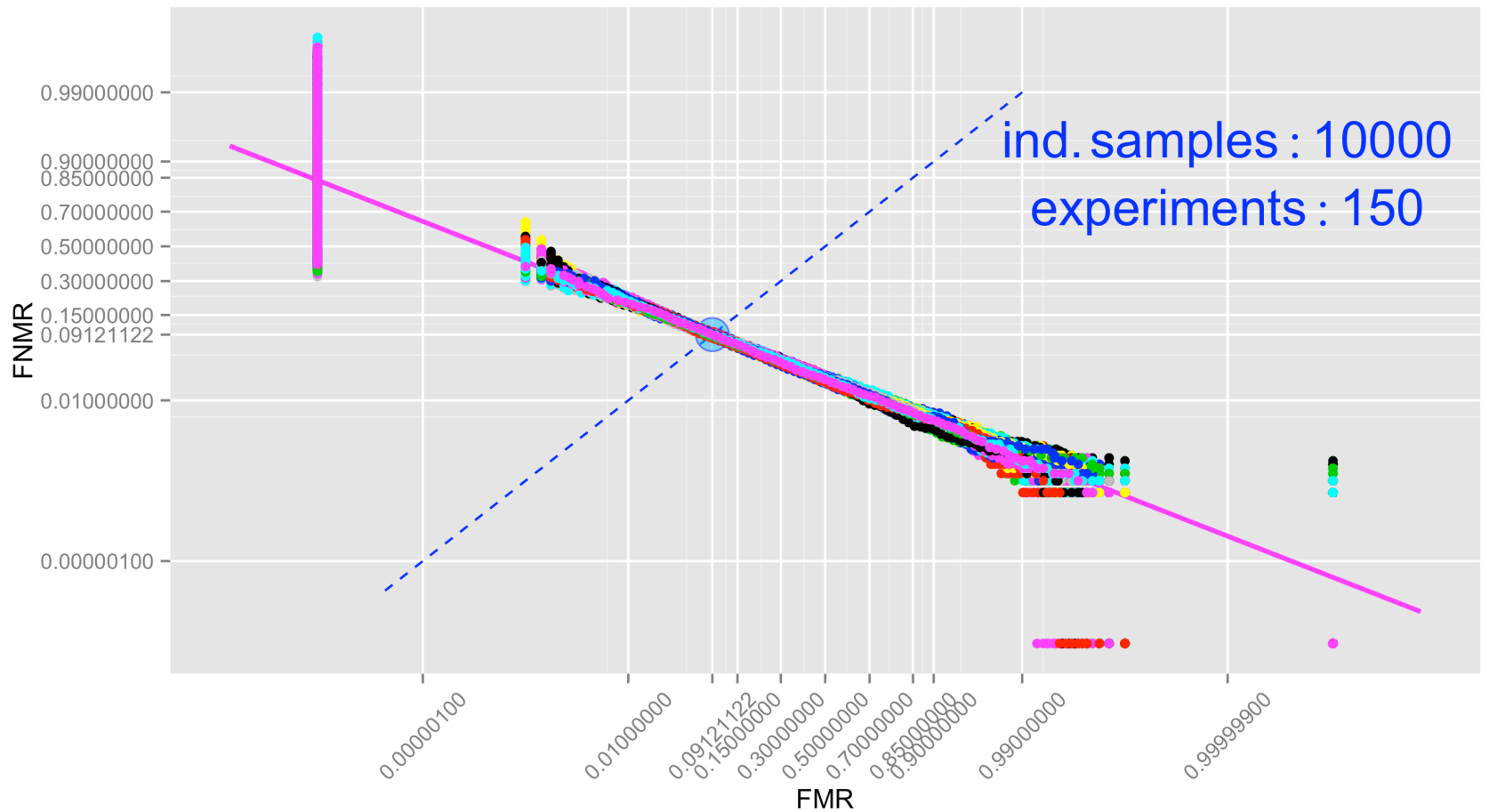
Confidence Intervals?!



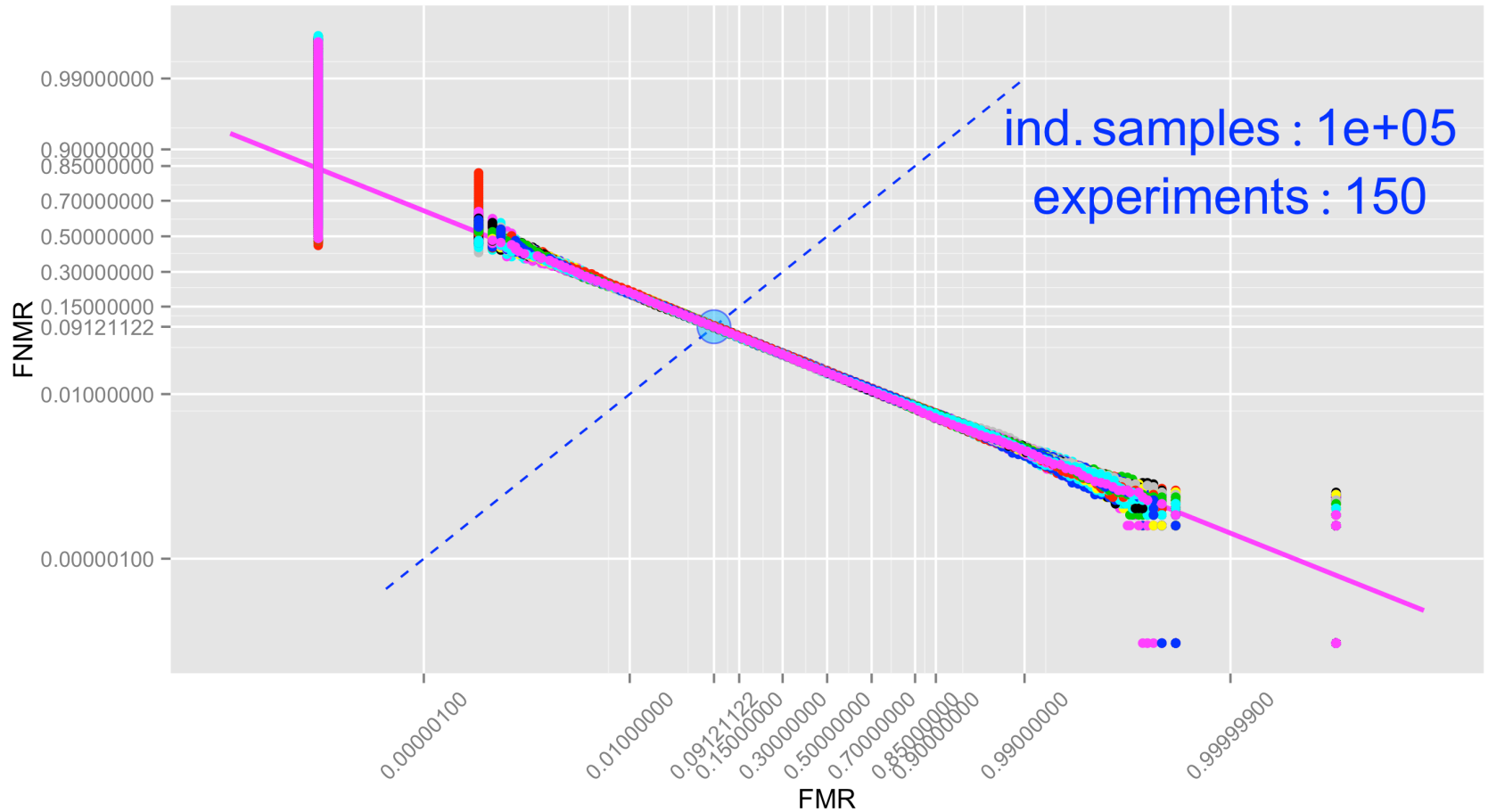
Any Confidence, Yet?



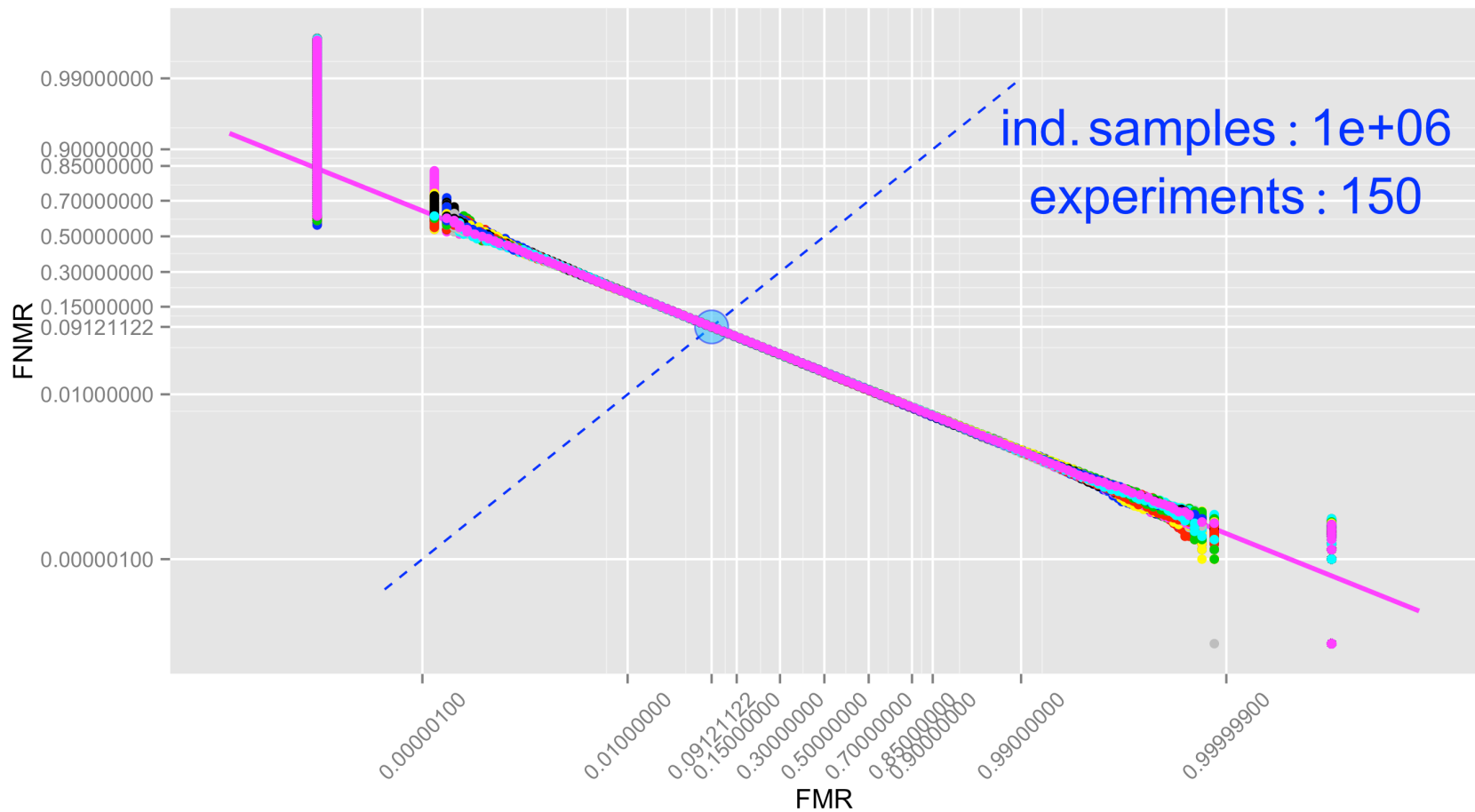
Fair Confidence



We Can be Proud



Just a Dream...



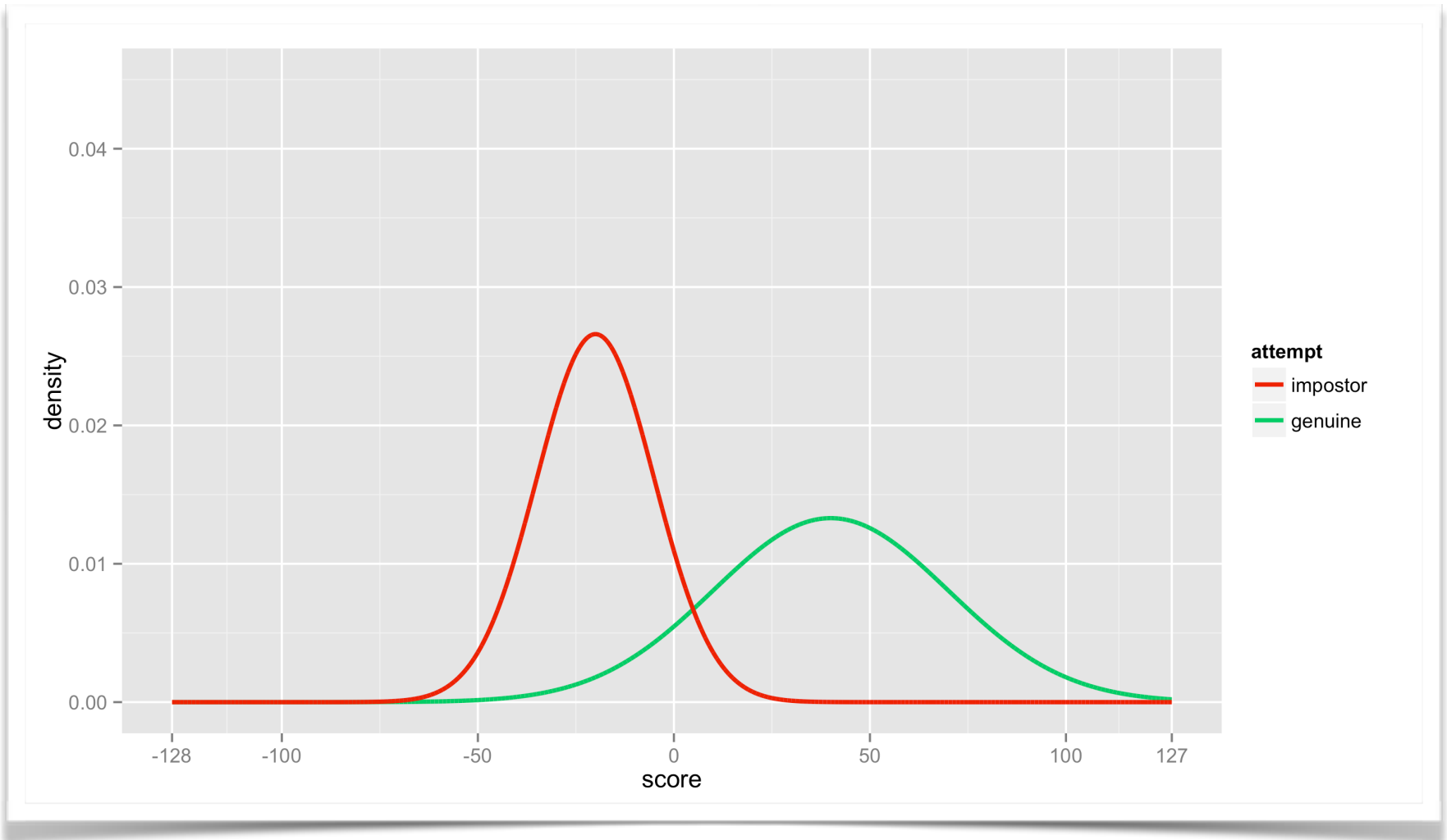


Biometric Menagerie

- To further complicate biometrics testing, those score distributions are usually *not* person-independent.
 - That means the performance is *not* the same for all people.
- There are *plenty of anomalies* out there we shall be aware of to interpret the system behaviour correctly.

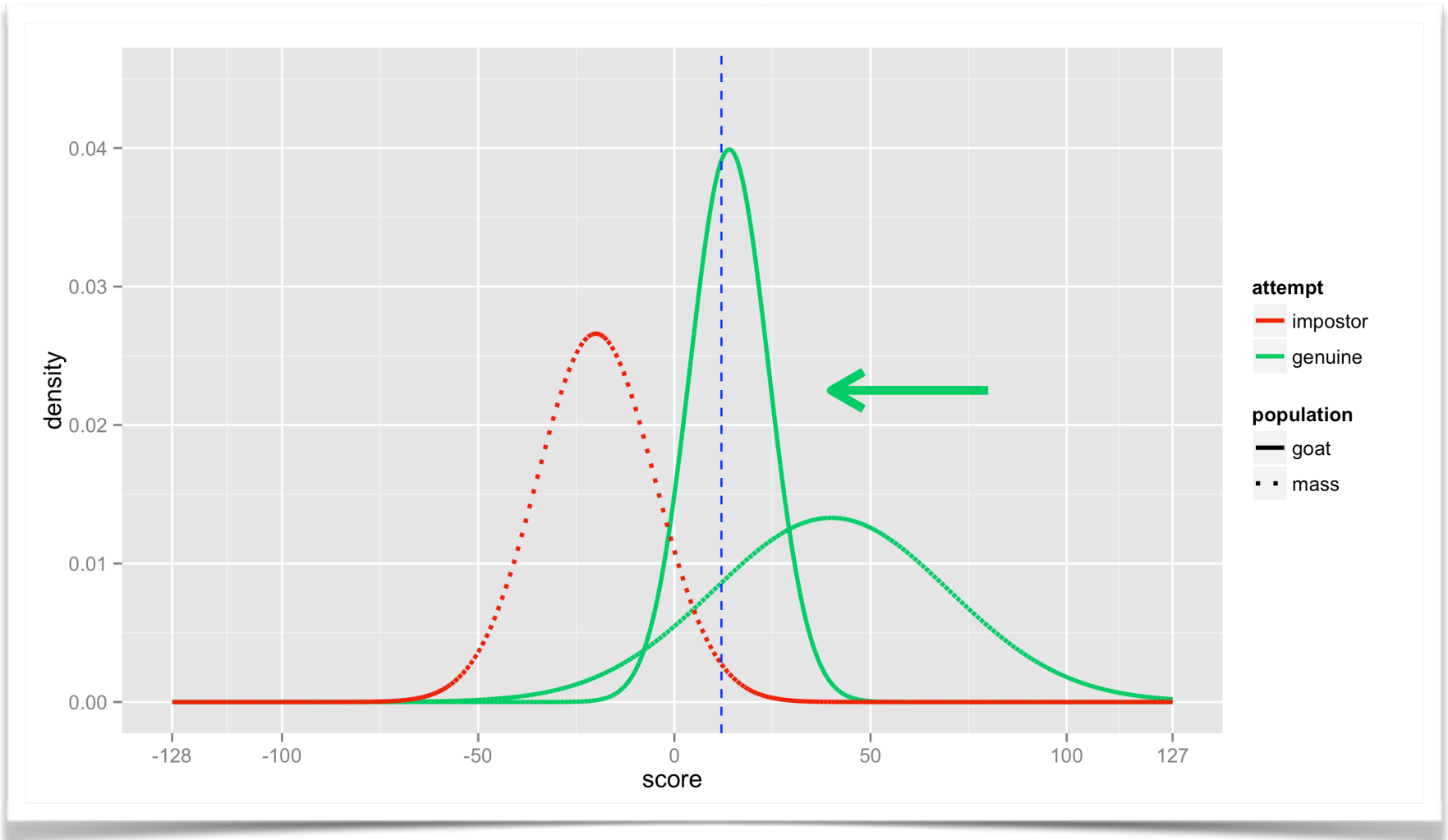


Sheep: An Ordinary User

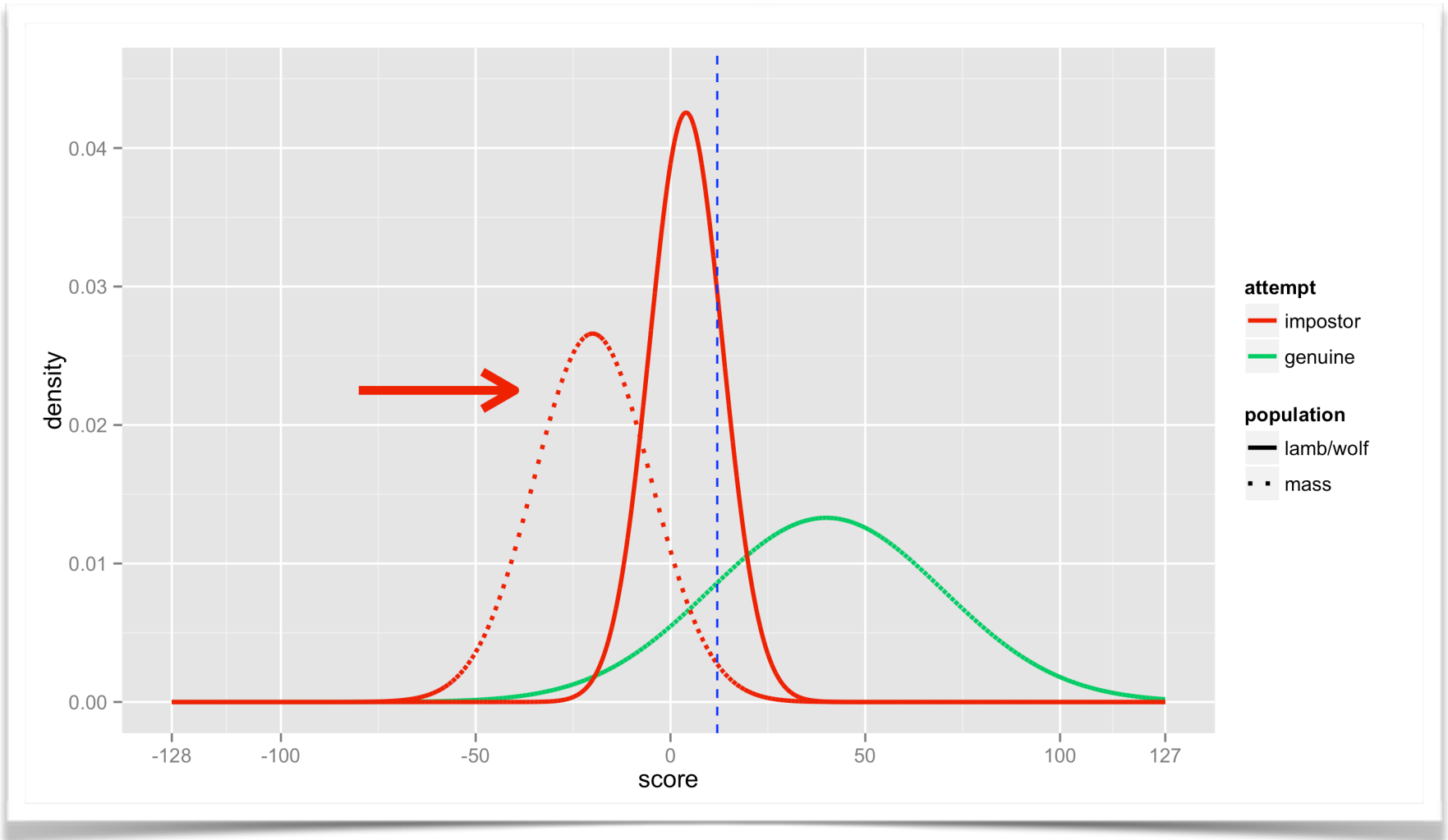




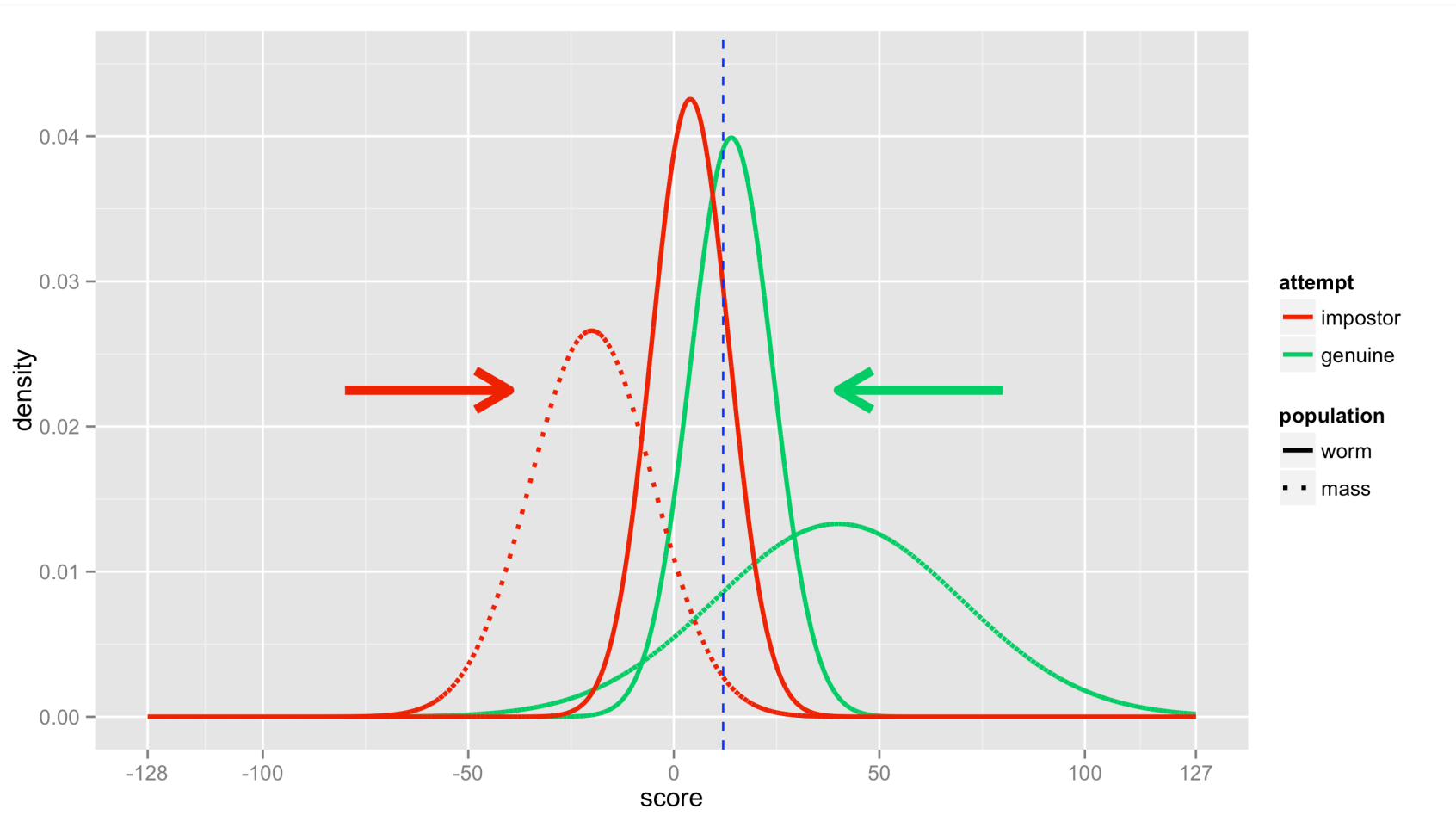
Goat: Problematic FNMR



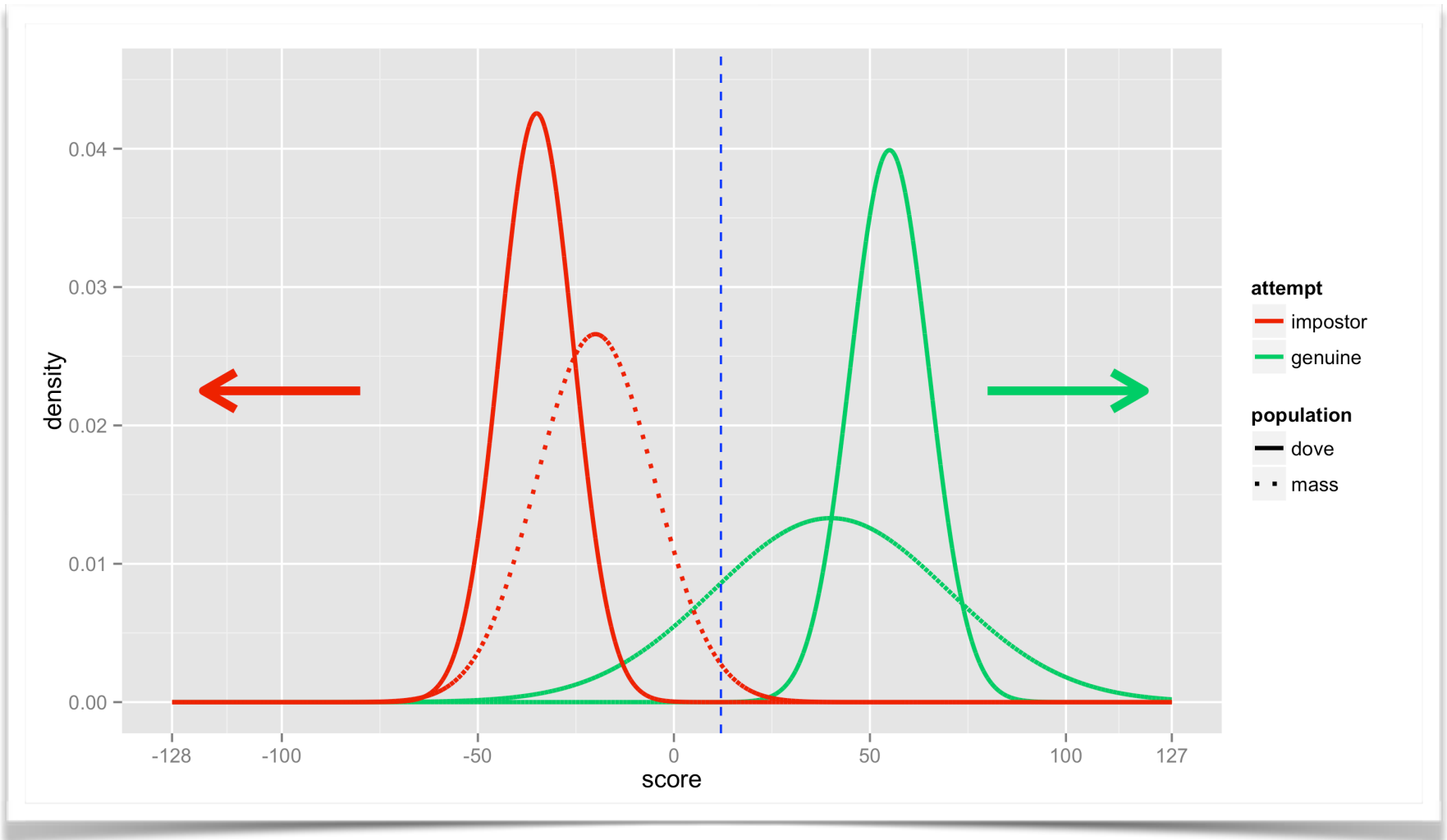
Lamb/Wolf: Easy Target and-or Effective Predator



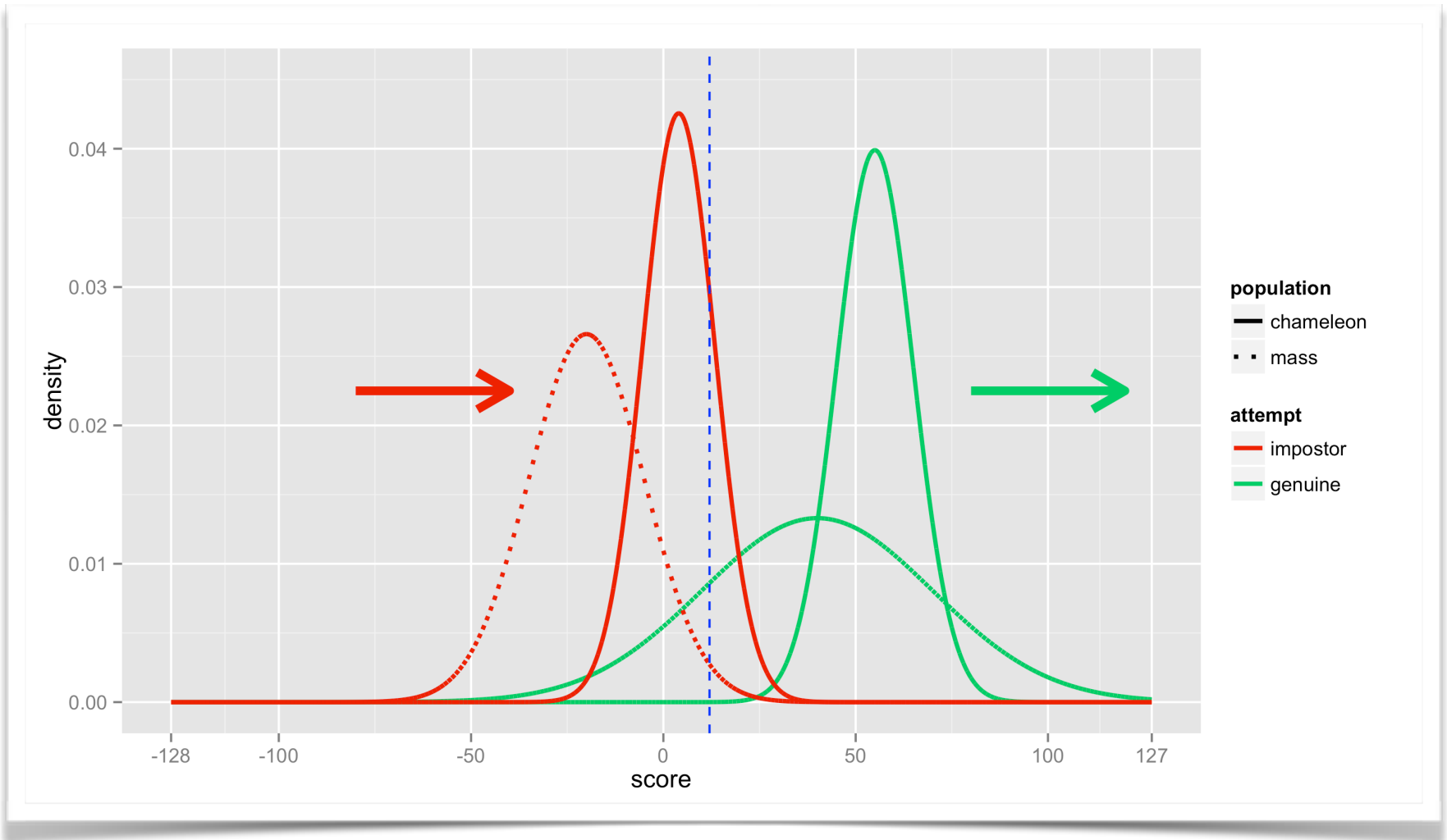
Worms: Both FNMR and FMR Increased



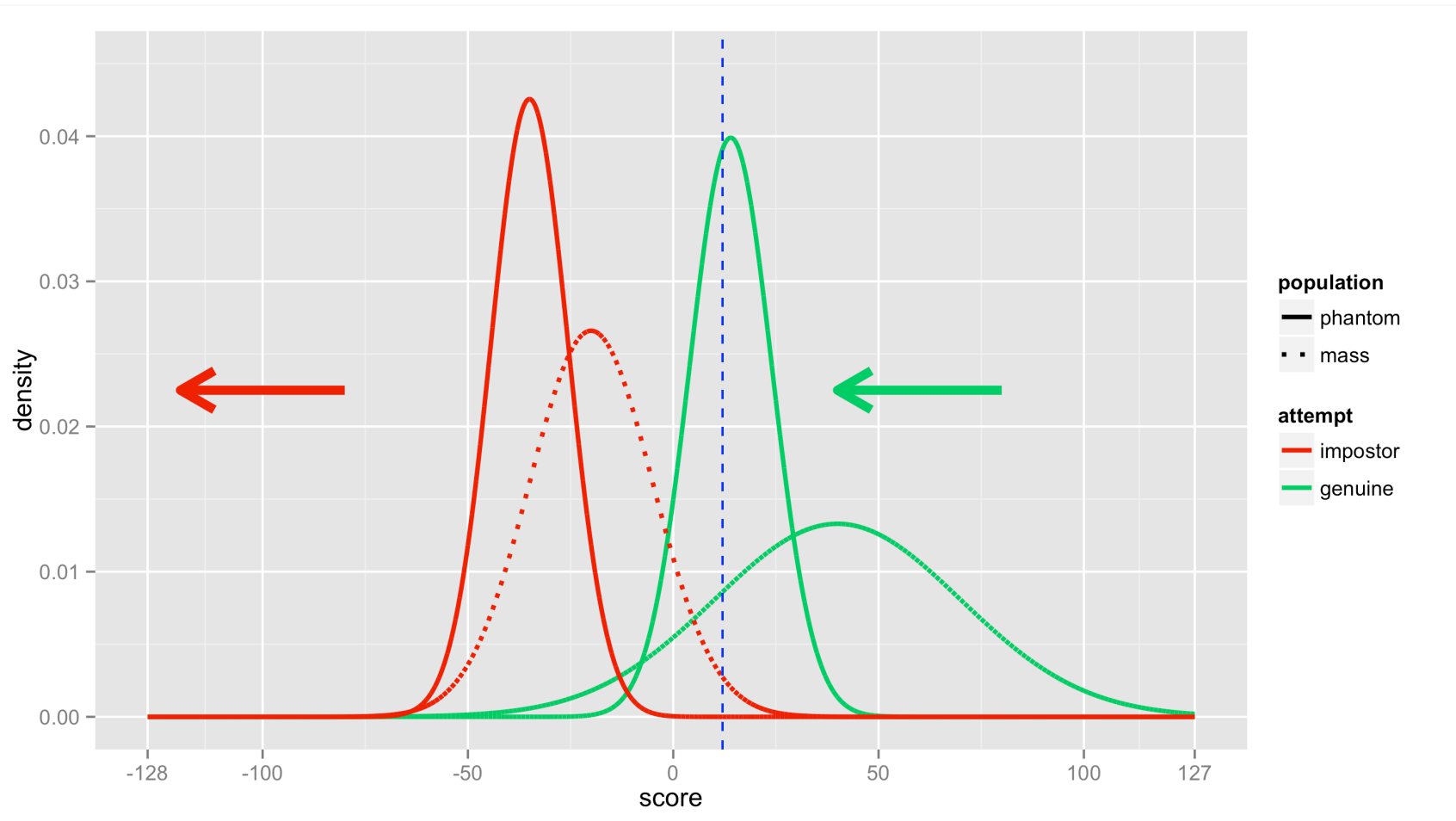
Dove: Excellent User



Chameleon: Excellent Scores, Anyway(!)



Phantom: Problematic Matching, Anyway



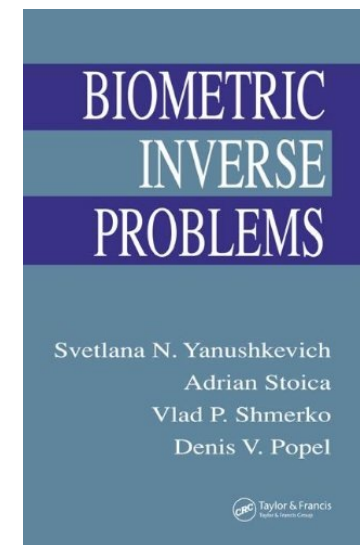
Secret Files on Biometrics





BIO Brute Force Attack

- Randomly generate plausible circa $1/FMR$ samples and put them to the test.
 - Also termed “Zero-Effort”, denoting that the attacker makes no special effort to imitate the original person characteristic.
- Synthetic samples generation is quite feasible today.





Cryptanalysis-Like Attacks

- **Masquerade attacks**, can be a variant of “**Hill-Climbing**” denoting the attacker iteratively improves the BIO sample data based on:
 - **scoring feedback** (*side channels*)
 - **stolen template** (*pre-image attacks*)
 - **independent template trained from intercepted BIO samples** (*correlation attacks*)
 - **known scoring anomaly** (*differential analysis*)
 - **implementation faults** (*general hacking*)



Spoofting

- *The process of defeating a biometric system through the introduction of fake biometric samples.*
 - *(Schuckers, Adler et al., 2010)*
- Particular modus operandi on how to deploy the attacking data vectors.
 - Can be seen as being orthogonal to the aforementioned ways of gaining fake samples.

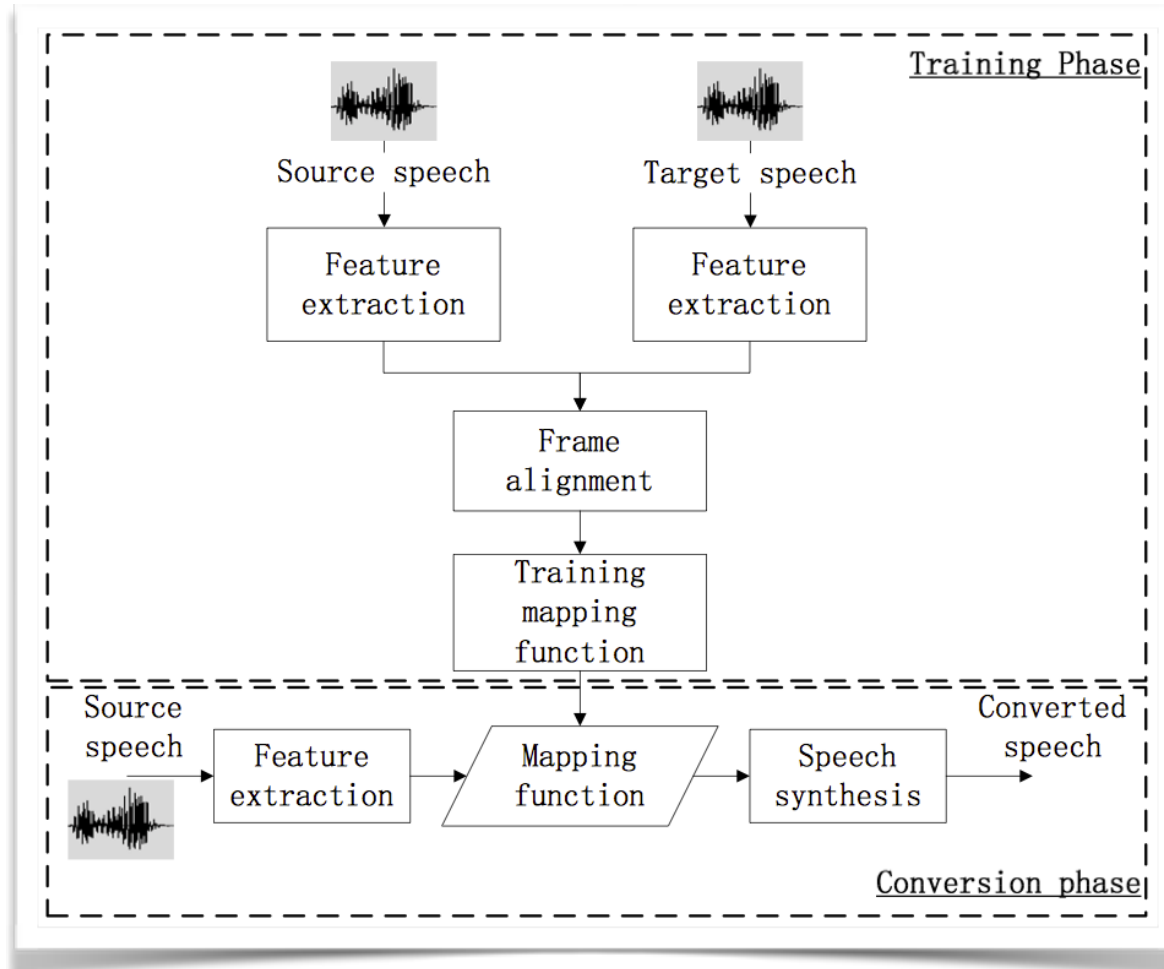


Sensor-Bypass Attacks

- Do not expose API service for unrestricted automated sample verification!
 - Recall the **zero-effort** attack complexity is often trivial.
 - Furthermore, **masquerade** attacks can shift FMR significantly.



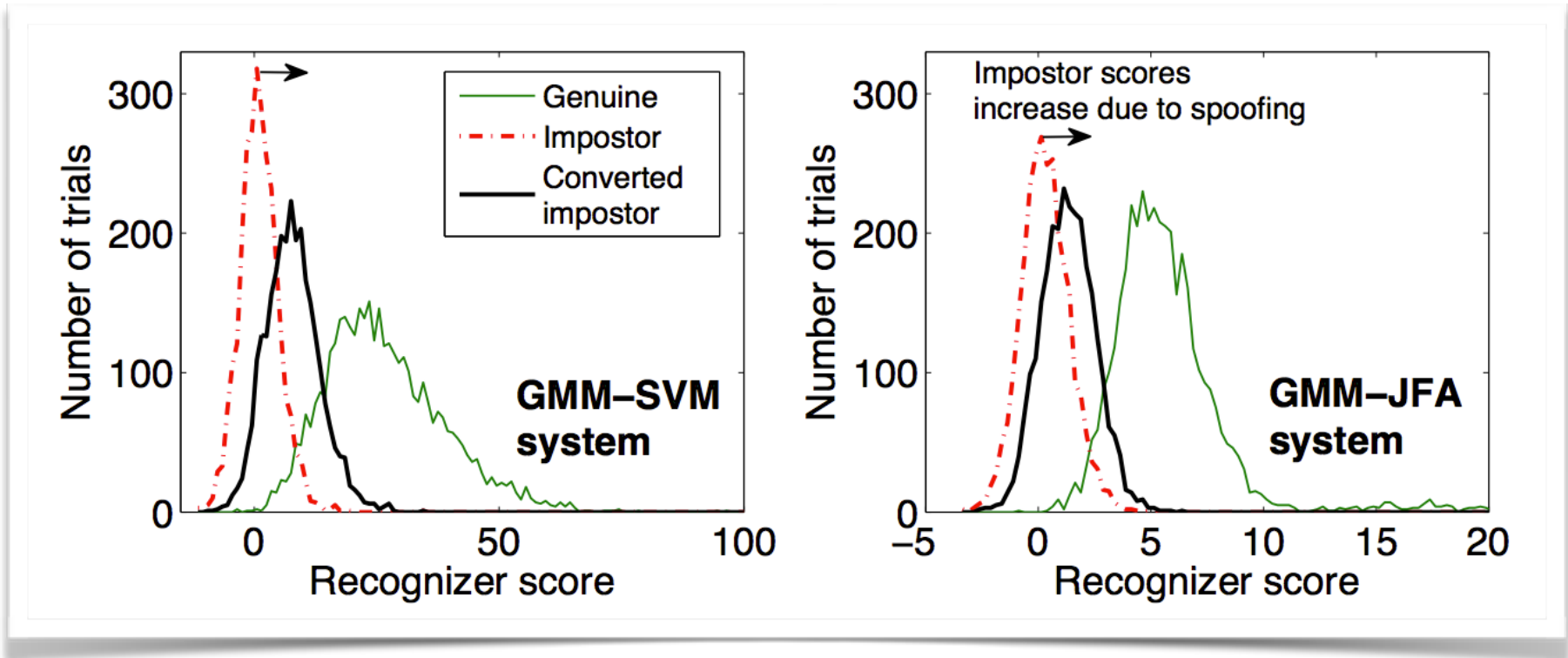
Conversion Attack Example



Kinnunen et al., ICASSP 2012



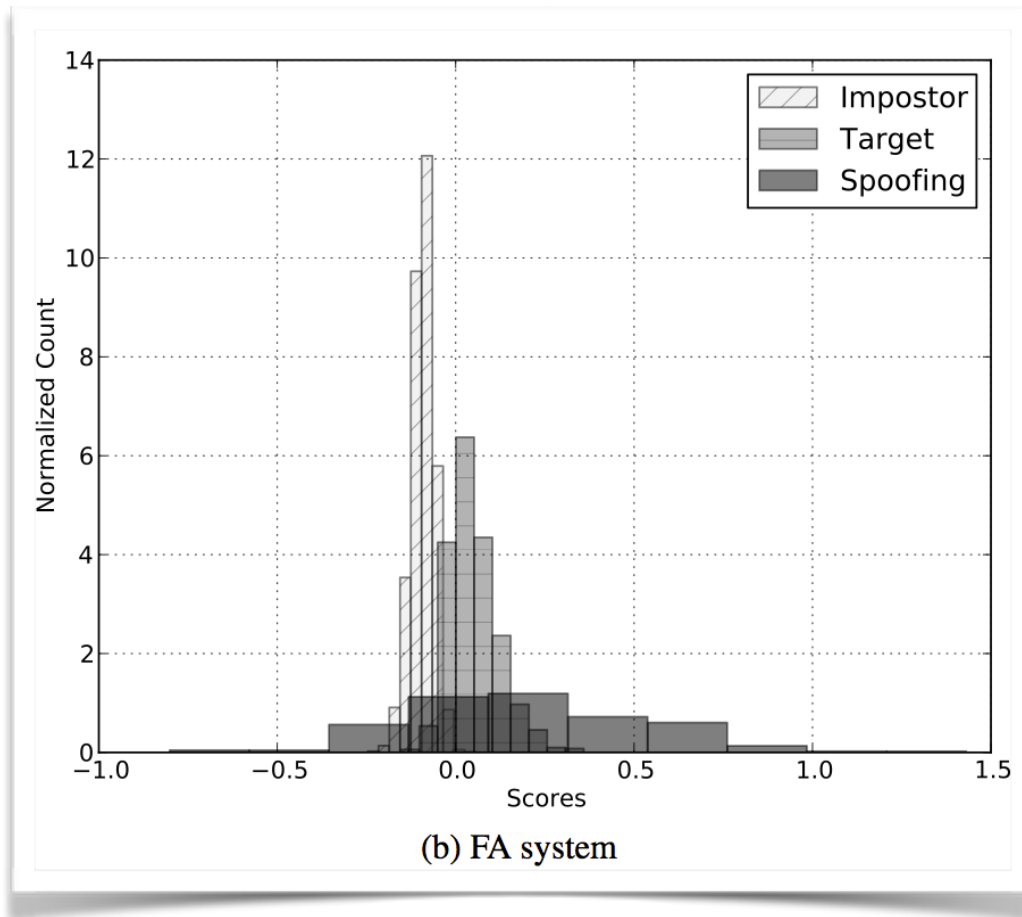
Reporting Attack Impact



Kinnunen et al., ICASSP 2012



Artificial Signals Impact



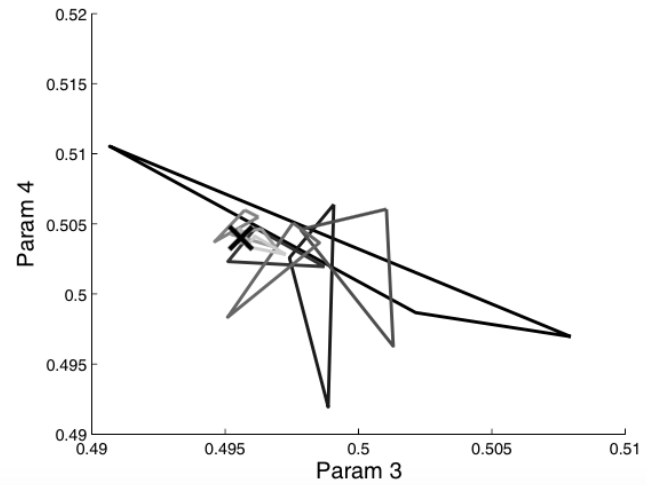
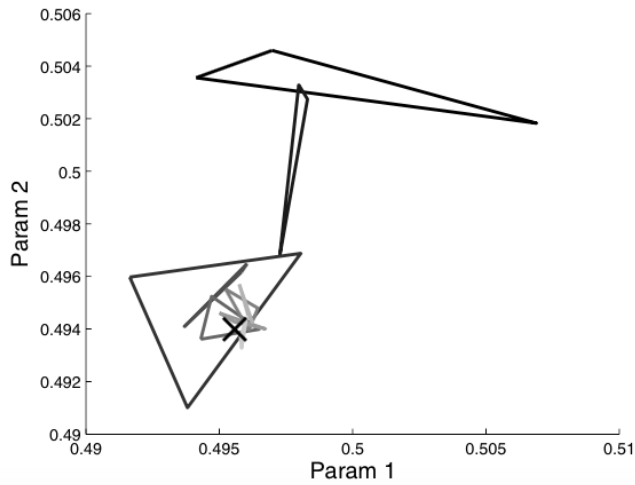
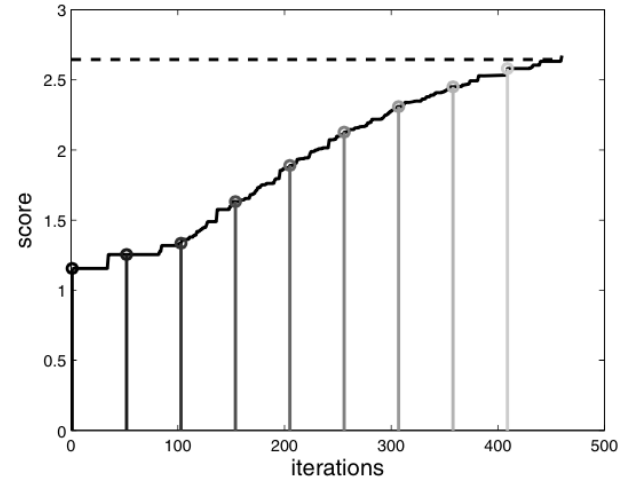
Alegre et al., EUSIPCO 2012-13

Biometric Signature Masquerade

- Hill-Climbing attack based on the Uphill Simplex algorithm and its application to signature verification
 - Gomez-Barrero, M., Galbally, J., Fierrez, J., and Garcia, J.-O. at Biold 2011

<i>FMR 0-effort</i>	$\phi(\#trials)$ <i>0-effort</i>	<i>FMR' US masq.</i>	$\phi(\#iters)$ <i>US masq.</i>
0.05%	2 000	91.76%	1 556
0.01%	10 000	89.58%	1 678
0.0025%	40 000	87.82%	1 805

Subspace Convergence Illustrated





X-talk Signal Leakage

- Furthermore, there is *a certain* link in between online (sign-pad made) and offline (pen-and-paper made) signatures.
 - Btw., we also hope to exploit this link should it come to a trial.
 - On the other hand, the amount of information being cross-transferred in between these two signal forms is *yet to be discovered!*



PDF Signature Leakage

- When signing a PDF using online signature data, we often put a human readable picture into the PDF annotation.
 - This is just to make the technology more user-friendly.
- This is, however, usually an offline plaintext projection of the (encrypted) online signature data.
 - How much information is leaking this way?



Offline Projection Example



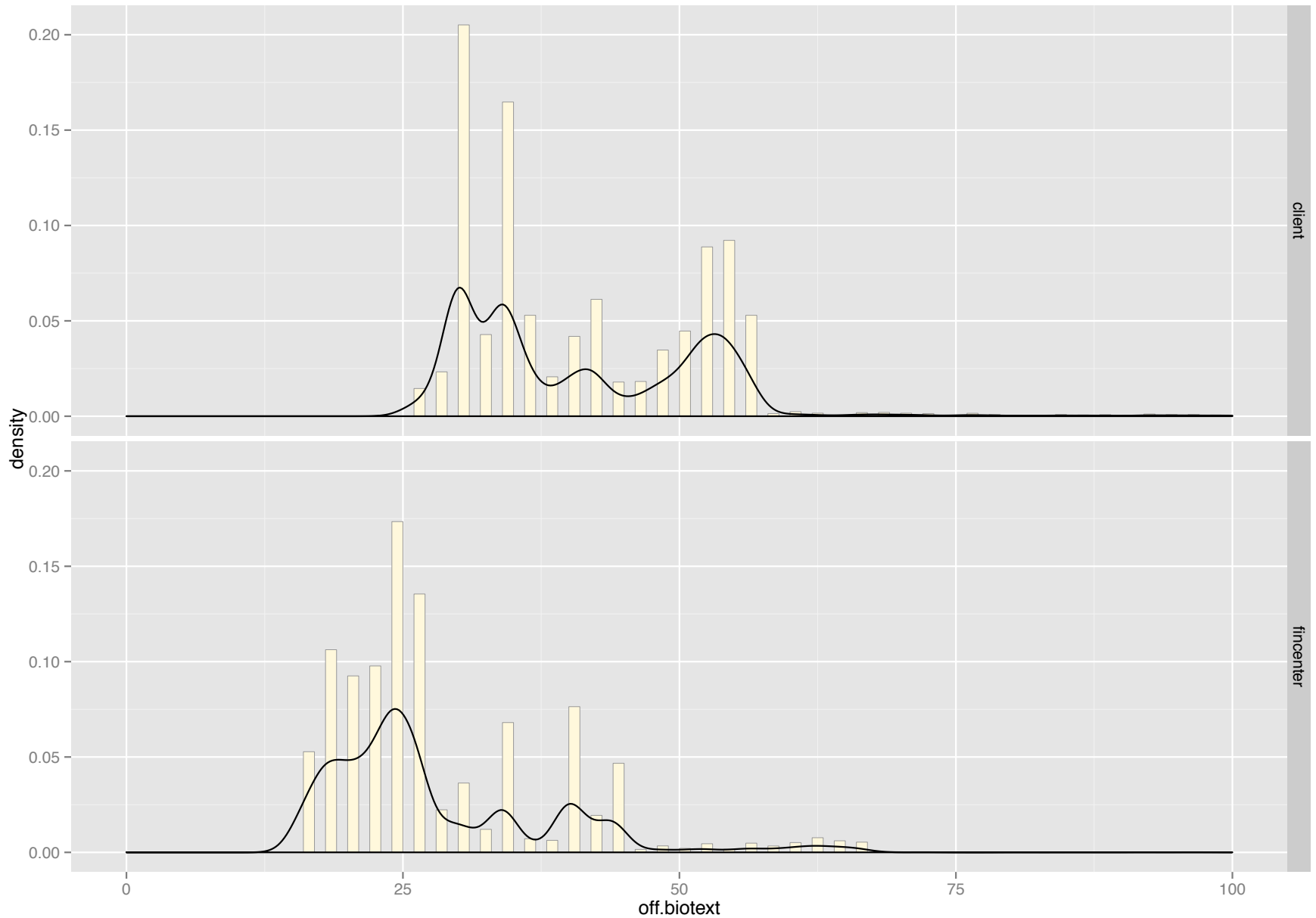
fincenter



client



Offline Signal Brief - There *is* Something!



ISO/IEC 24745 Requirements

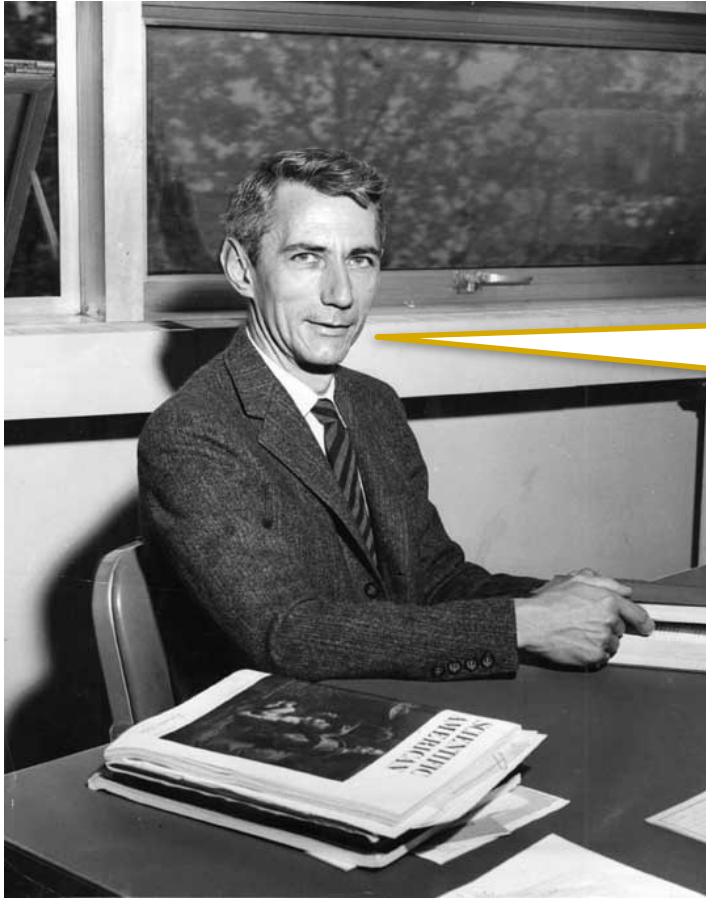
- **Renewability**
 - allows multiple independent *biometric references* created ad hoc
 - a particular leaked template does not compromise the other ones (provably!)
- **Revocability**
 - user can revoke the ability of being successfully verified by a particular template from now on
- Biocryptography is an effective way on how to achieve these goals.

Biometric Cryptography?





Back To the Origin



1. analyse the entropy gain from inter-class variation
2. use an error-correction code to cope with intra-class noise

Claude Elwood Shannon, 1948-49



Is It Enough?

- Template protection in contemporary systems is often quite questionable (*to be polite*).
- On the other hand, is it the only one problem?
 - **No.** We shall not push the concept of bio-keys too hard anyway.



Bio-Skimming

- Once biometric systems become ubiquitous, this will be a fruitful attack vector.
 - Attackers use a fake sensor (or hack into an original one) to skim the “bio-master-key”.
 - At the end of the day, how many eyes, fingers, faces, vocal tracts (etc.) do we have?
 - It is like having few master-keys for a whole life.
 - Furthermore, we prove the master-key possession by simply handing it over to almost any device that asks so (again, again, ...and again).



Spoofting Still Matters!

- That said, liveness detection will be always important!
 - Remember, biometrics is a signal detection.
 - It all works as long as we can assume the signal is coming from a particular human being!
 - *Apparently, the biometric signal detector output shall be just one out of many inputs into an authentication process (itself being another multidimensional signal detection problem).*



Tamper-Resistant Sensor

- It signs the biometric signal samples with its private key to indicate it already has sampled that signal from a living individual.
 - Furthermore, the sample shall be then processed as soon as possible.
 - Otherwise, we have to mitigate the risk of a sensor compromise in the intermediate time by a further time-stamping: Long Term Validation of bio-samples.
 - This concept is all too often neglected in the emerging handwritten signature biometrics!

Anyway, do the Pentest!





Conclusion

- We shall **require ISO 19795 methodology** during biometric application selection, comparison, and operation testing.
- Use an **independent penetration test** to verify:
 - zero-effort attack complexity
 - *beware of automated APIs!*
 - masquerade attacks
 - spoofing possibilities
 - template security
 - system security in general
 - *threshold settings, template tampering*

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Tomáš Rosa

Raiffeisenbank, a.s.

tomas."my_last_name"@rb.cz

