



3. Hodnocení spolehlivosti a kvality biometrických systémů

→ Měření vzdálenosti

→ Vzdálenost

→ Metrika k rozlišování rysů / charakteristik

→ Důležité metriky pro biometrii

→ Minkowského metrika: $d_{ij} = \left[\sum |x_{ik} - x_{jk}|^r \right]^{\frac{1}{r}}$

→ pro $r = 1$ se jedná o „City-Block-Metric“

→ pro $r = 2$ se jedná o Eukleidovskou vzdálenost

→ Mahanalobisova metrika: $r^2 = (x - m_x)' \cdot C_x^{-1} \cdot (x - m_x)$

→ kde m_x je vlastní vektor všech referenčních vektorů a C_x je kovariační matice pro x

→ Normalizuje vzdálenosti

→ Jednotková matice $C_x \sim$ Eukleidovské vzdál.

→ Klasifikační rozhodnutí

→ Typy klasifikace

- Verifikace - patří množina rysů R k osobě O z celkového počtu osob N ?
- Identifikace - která množina rysů R z celkového počtu osob N patří k osobě O ?
- Rozpoznávání - které třídě patří sémantický obsah rysů R ?

→ Ideální stav: 0 chyb

→ Prakticky nemožné - M.I.

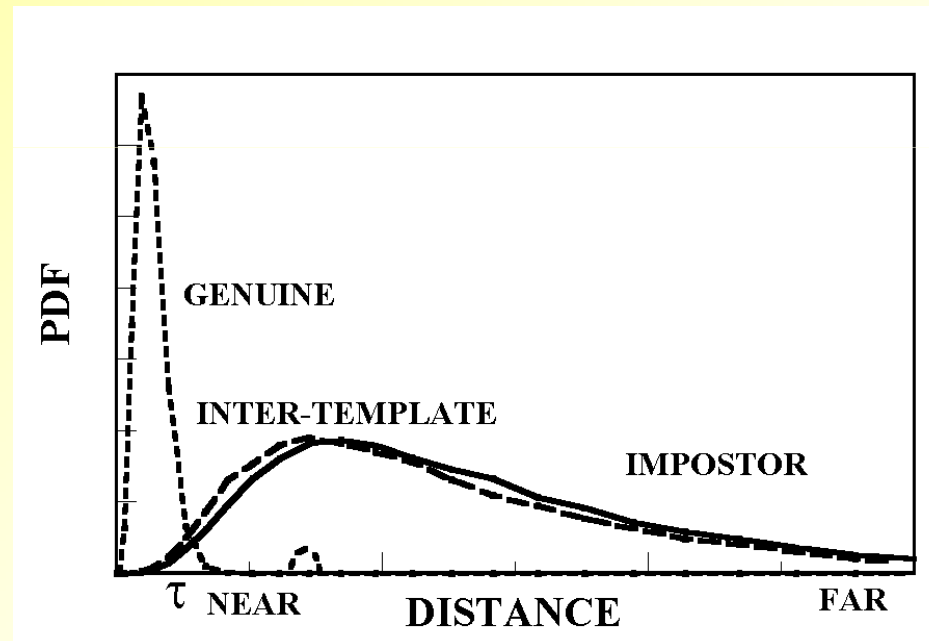
→ Problémem je změření přesnosti



→ Statistické základy (I.)

→ Problém: Distribuce vzdáleností rysů

- Genuine Distribution - Rozložení právoplatných rysů
- Impostor Distribution - Rozložení neprávoplatných rysů
- Inter-Template Distribution - Rozložení vzdáleností rysů mezi šablonami různých osob



- Problém při testování biometrických systémů
 - Kolik testů musí být provedeno, aby mohly být vysloveny signifikantní závěry?

- Binomické rozložení udává diskrétní rozdělení pravděpodobnosti $P_p(n, N)$ pro dosažení přesně n úspěchů z N Bernoulliho pokusů (*true* je s pravděpodobností p a *false* s $(1-p)$). Výpočet:

$$P_p(n, N) = \binom{N}{n} \cdot p^n \cdot q^{N-n} \quad \binom{N}{n} \text{ je binomický koeficient.}$$

→ Statistické základy (III.)

- U rozsáhlých databází může být binomické rozložení nahrazeno standardním normálním rozložením:

$$f_z(z) = \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{z^2}{2}}, \quad \text{kde } z = \frac{x - \hat{x}}{\sigma}$$

- K zajištění specifické úrovně důvěrnosti (chybovost menší než τ) se specifickou odchylkou σ pro hypotézu h (chyba $\leq h$) lze psát:
- $$n_\tau = \frac{z_\tau^2}{\sigma^2} \cdot h \cdot (1 - h)$$

Bezpečnostní třída	Horní hranice ($\sigma + \text{FAR}$) [%]	σ [%]	FAR [%]	n_τ
Nízká	15,0	5,0	10,0	138
	10,0	2,0	8,0	707
	5,0	1,0	4,0	1475
Střední	4,9	0,9	4,0	1821
	3,6	0,6	3,0	3105
	2,5	0,5	2,0	3012
Vysoká	1,9	0,4	1,5	3547
	1,5	0,5	1,0	1521
	1,0	0,3	0,7	2967
Velmi vysoká	1,0	0,2	0,8	7622
	0,5	0,1	0,4	15305
	0,3	0,1	0,2	30671

→ Entropie

- Kolik informace může obsahovat konkrétní biometrická vlastnost?
- Např. Kód duhovky (Daugmanův alg.) = 2048 bitů
- Např. Otisk prstu = 243 - 8075 bitů
- Teoreticky $3,23 \cdot 10^{616}$ / $6,57 \cdot 10^{2430}$ - a prakticky?
- Příklad: Pravděpodobnost shodnosti dvou různých
 - Duhovek $\sim 10^{-52}$
 - Otisků prstů $\sim 10^{-7}$ až 10^{-59} (závislé na modelu)

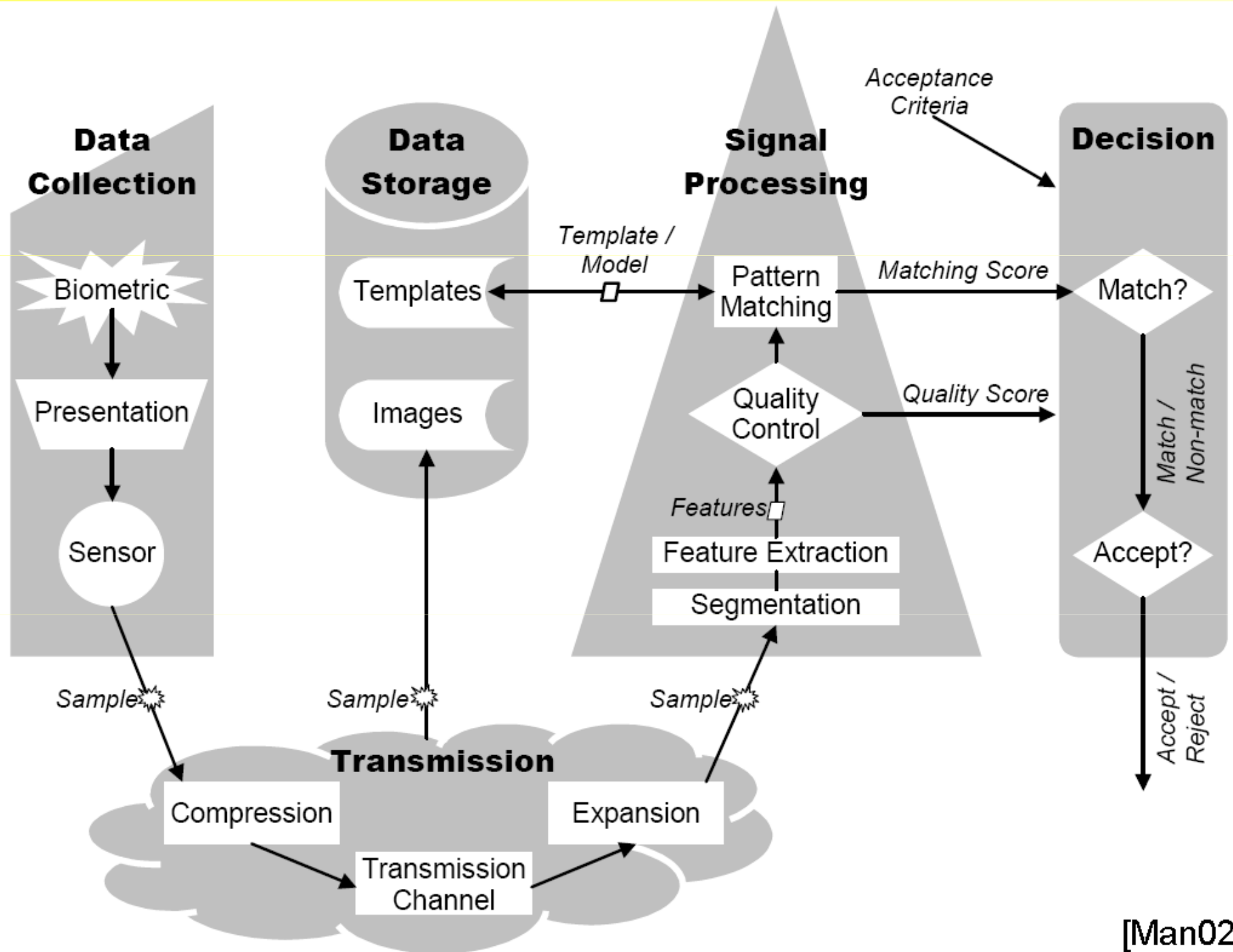
→ Statistické základy (V.)



- **Variabilita** je měřítkem rozptylu statistické distribuce. Je-li μ střední hodnotou distribuce náhodné proměnné X , potom $V(X) = E[(X-\mu)^2]$. Tato hodnota může udávat jak blízko je odhadovaný výsledek skutečné hodnotě.
- **Interval důvěrnosti** (např. 95%) pro parametr x se skládá z dolní hranice L a horní hranice U tak, že pravděpodobnost skutečné hodnoty leží v tomto intervalu, tj. $p(x \in [L, U]) = 95\%$.
- **Chyba typu I**: Odmítnutí správné hypotézy.
- **Chyba typu II**: Přijetí chybné hypotézy

- Celková výkonnost biometrického systému je dána vlastnostmi jako univerzálnost, přesnost, rychlost a paměťové možnosti.
- Faktory jako cena a lehkost použití také samozřejmě ovlivňují celkovou výkonnost systému.
- Biometrické systémy nejsou perfektní - mohou chybně přijmout útočníka jako platného uživatele (chybné přijetí) a nebo odmítnout platného uživatele jako útočníka (chybné odmítnutí).

→ Struktura obecného biometrického systému



→ Tvrzení o identitě

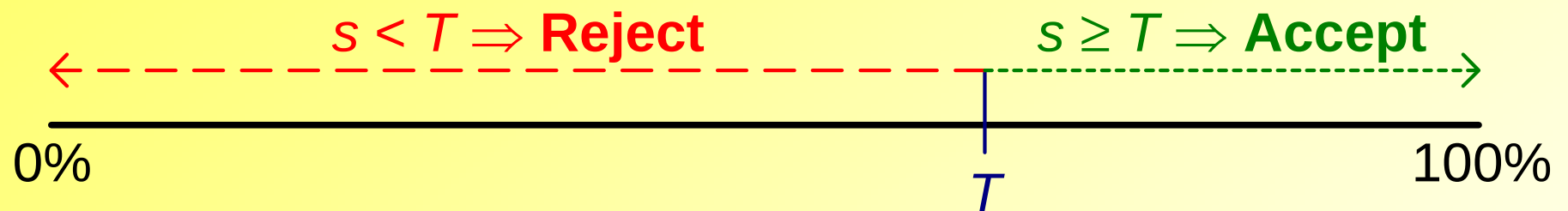


- Pozitivní tvrzení o identitě - uživatel tvrdí, že je již registrován v daném biometrickém systému. Např. se jedná o běžné přístupové systémy.
- Negativní tvrzení o identitě - uživatel tvrdí, že ještě není registrován v daném biometrickém systému. Např. se jedná o systémy sociální podpory / uprchlíků.
- Explicitní tvrzení o identitě - uživatel musí zadat svoji identitu (např. smart kartou) a ta je buď potvrzena a nebo vyvrácena. Porovnání 1:1.
- Implicitní tvrzení o identitě - identita uživatele je vyhledána a předložena. Porovnání 1:N.
- Tvrzení o identitě právoplatným uživatelem
- Tvrzení o identitě útočníkem

→ Porovnání („*Matching*“) (I.)

- Extrahovaný vzorek (množina rysů) je porovnán se šablonou - výsledkem je skóre porovnání („*Matching Score*“), tj. míra shody.
- Skóre porovnání udává kvantifikovanou podobnost mezi vzorkem a šablonou. Označujeme jako s .
- Metrika: $\langle 0, 1 \rangle \sim \langle 0\%, 100\% \rangle$, tedy $\langle \text{neshoda}, \text{shoda} \rangle$
- Porovnání uvnitř systému je založeno na prahu T .
 - If $(s) < (T)$ then Reject
 - If $(s) \geq (T)$ then Accept
 - Výsledkem je buď přijetí či odmítnutí ~ autorizace

→ Porovnání („Matching“) (II.)



→ Možné stavy při porovnání:

→ Dva vzory od dvou odlišných osob jsou rozpoznány (klasifikovány) jako shodné

→ Chybná shoda („*False Match*“)

→ Dva vzory (nasnímané ve dvou různých okamžicích) od stejné osoby jsou rozpoznány (klasifikovány) jako odlišné

→ Chybná neshoda („*False Non-Match*“)

→ Porovnání („*Matching*“) (III.)

- V literatuře se ujal pojmy:
 - „*False Match*“ ~ „*False Acceptance*“
 - „*False Non-Match*“ ~ „*False Rejection*“
- Projev na verifikaci (identifikaci):
 - Osoba A je přijata jako A.
 - Správné přijetí („*True Acceptance*“)
 - Osoba A je odmítnuta jako B.
 - Správné odmítnutí („*True Rejection*“)
 - Osoba A je přijata jako B.
 - Chybné přijetí („*False Acceptance*“)
 - Osoba A je odmítnuta jako A.
 - Chybné odmítnutí („*False Rejection*“)

→ Chyby - *False Acceptance Rate (FAR)*

- Míra chybného přijetí - **FAR**
- **FAR** je pravděpodobnost, že biometrický systém klasifikuje chybně dva odlišné biometrické vzory jako shodné a tím selže při odmítnutí možného útočníka.

$$\mathbf{FAR} = \frac{\text{Počet } \mathbf{shodných} \text{ porovnání } \mathbf{rozdílných} \text{ vzorů}}{\text{Celkový počet porovnání } \mathbf{rozdílných} \text{ vzorů}}$$

- Příklad: Provedli jsme 5.000 porovnání u technologie duhovky, přičemž byly vždy porovnávány páry, které nepochází od stejné osoby. Přesto jsme obdrželi 67 výsledků, které ležely v oblasti přijetí, tj. vykazovaly shodu.

$$\rightarrow \mathbf{FAR} = [67 / 5.000] * 100\% = 1,34\%$$

→ Chyby - *False Rejection Rate* (FRR)

→ Míra chybného odmítnutí - FRR

→ **FRR** je pravděpodobnost, že biometrický systém klasifikuje chybně dva biometrické vzory od stejné osoby jako odlišné a tím selže při přijetí oprávněného uživatele.

$$\text{FRR} = \frac{\text{Počet porovnání vzorů osoby A vedoucích k neshodě}}{\text{Celkový počet porovnání vzorů osoby A}}$$

→ Příklad: Provedli jsme 200 porovnání u technologie otisků prstů, přičemž byly vždy porovnávány páry, které pochází od stejného uživatele. Přesto jsme obdrželi 53 výsledků, které ležely v oblasti odmítnutí, tj. vykazovaly neshodu.

→ **FRR** = $[53 / 200] \cdot 100\% = 26,5\%$

→ Chyby - *False Match Rate (FMR)*

→ Míra chybné shody - **FMR**

→ **FMR** udává podíl chybně akceptovaných osob. Na rozdíl od **FAR** nejsou do celkových součtů brány v potaz pokusy, které byly neúspěšné ještě před samotným porovnáním (tj. **FTA**, **FTE**).

$$FMR(T) = \int_T^1 p_i(s | H_i) ds$$

→ T je rozhodovací práh,

→ H_i je výrok „rozdílné“ (vzor a šablona pochází od různých osob),

→ p - pravděpodobnostní hustota, že výrok v závorce je pravdivý,

→ s je skóre porovnání.

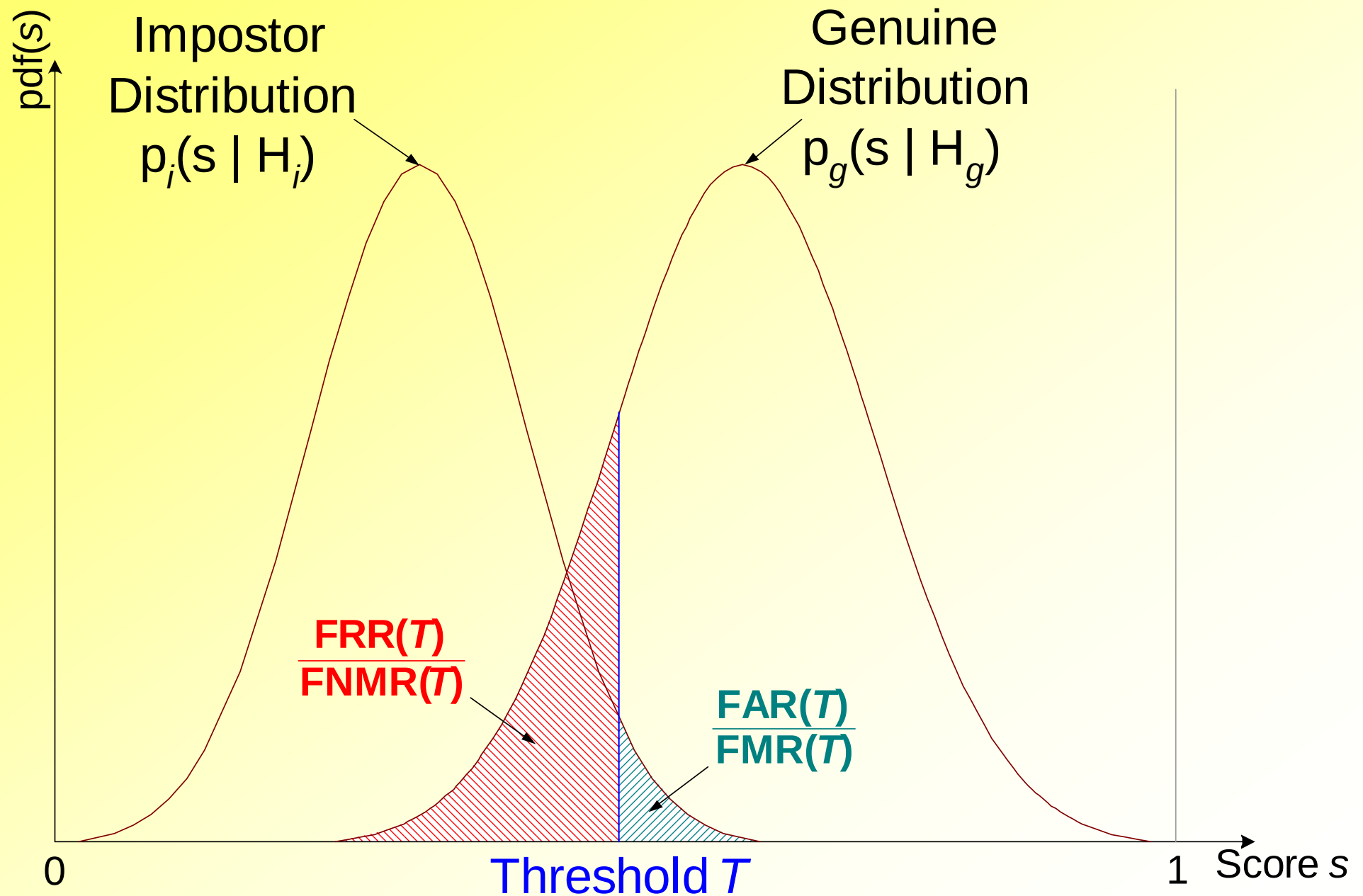
→ Chyby - *False Non-Match Rate (FNMR)*

- Míra chybné neshody - FNMR
- **FNMR** udává podíl chybně neakceptovaných osob. Na rozdíl od **FRR** nejsou do celkových součtů brány v potaz pokusy, které byly neúspěšné ještě před samotným porovnáním (tj. **FTA**, **FTE**).

$$FNMR(T) = \int_0^T p_g(s | H_g) ds$$

- T je rozhodovací práh,
- H_g je výrok „shodné“ (vzor a šablona pochází od stejné osoby),
- p - pravděpodobnostní hustota, že výrok v závorce je pravdivý,
- s je skóre porovnání.

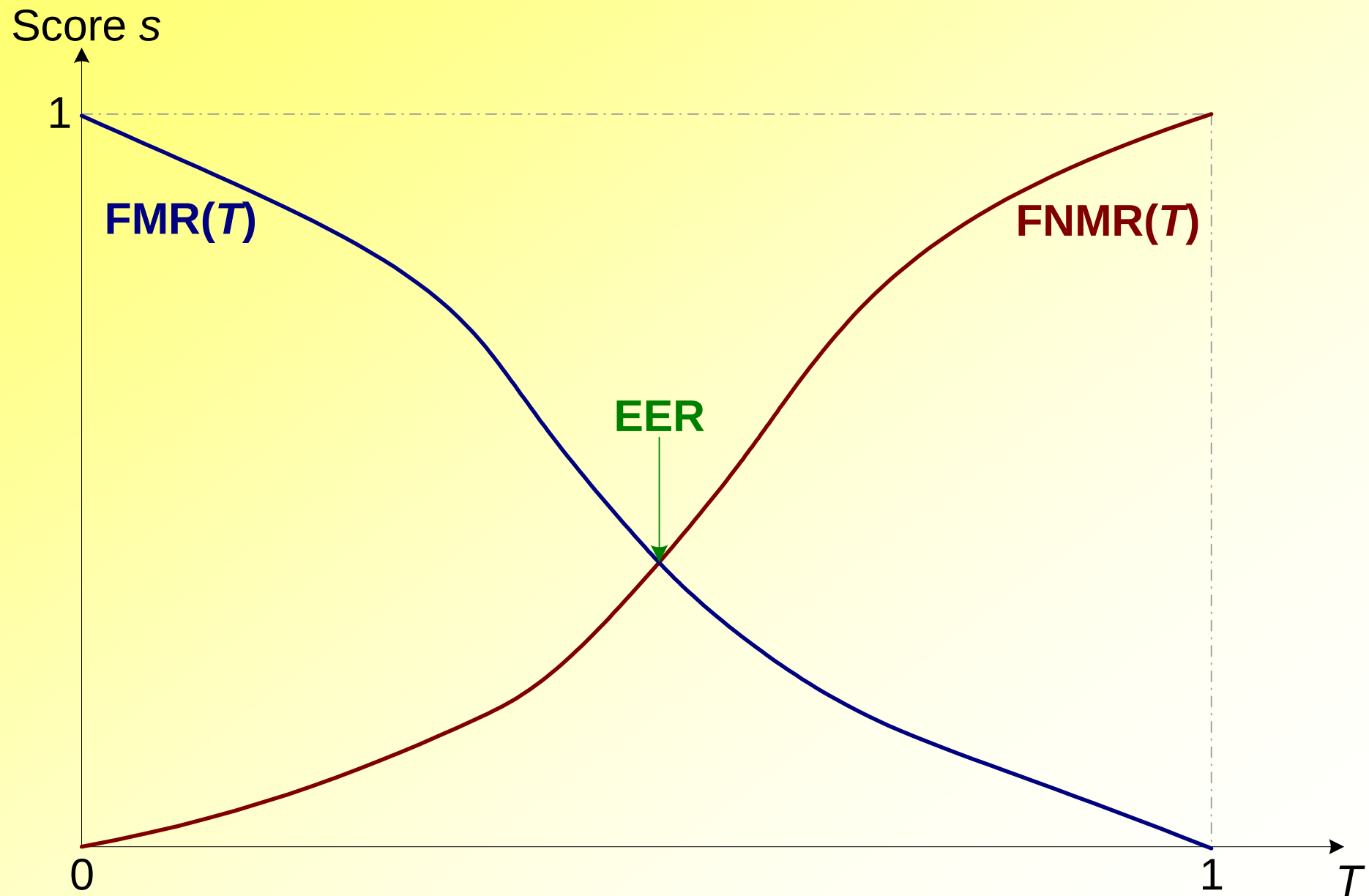
→ Chyby - FMR vs. FNMR / FAR vs. FAR



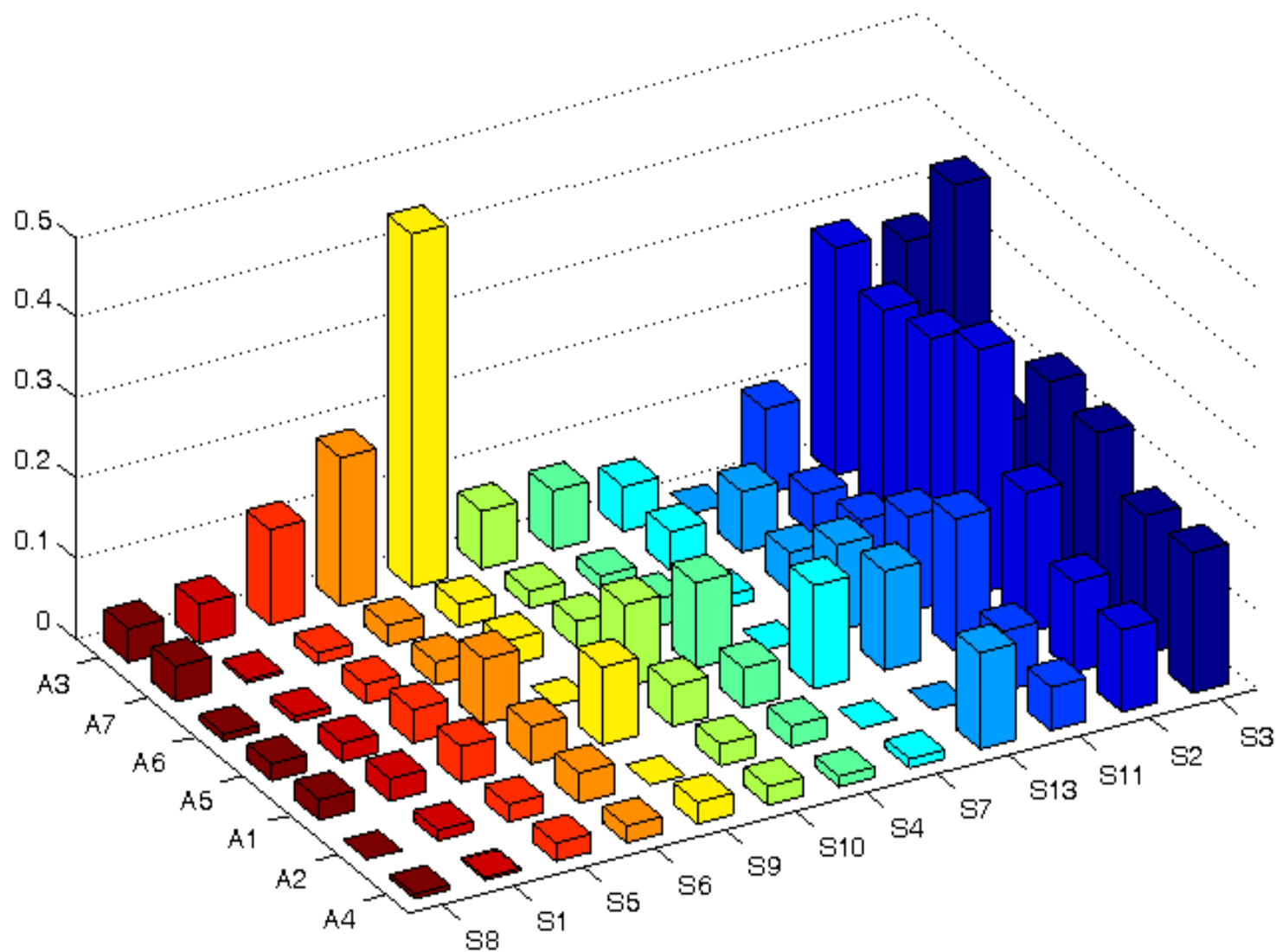
→ Chyby - *Equal Error Rate (EER)* (I.)

- Míra vyrovnaní chyb - **EER**
- **EER** je definována podmínkou $\mathbf{FMR}(T) = \mathbf{FNMR}(T)$. V praxi se u **FMR** a **FNMR** křivek jedná o diskrétní funkce, tj. přesné určení **EER** není možné. Je tedy možné udat oblast, ve které se obě chybové míry shodují. Při nastavení porovnávacího prahu T na **EER** bude chybně akceptován stejně jako chybně odmítnut stejný počet osob. Tím je tedy možné nastavit práh tak, aby hodnoty **FMR** / **FNMR** odpovídaly požadavkům (dle způsobu použití systému).

→ Chyby - *Equal Error Rate (EER)* (II.)

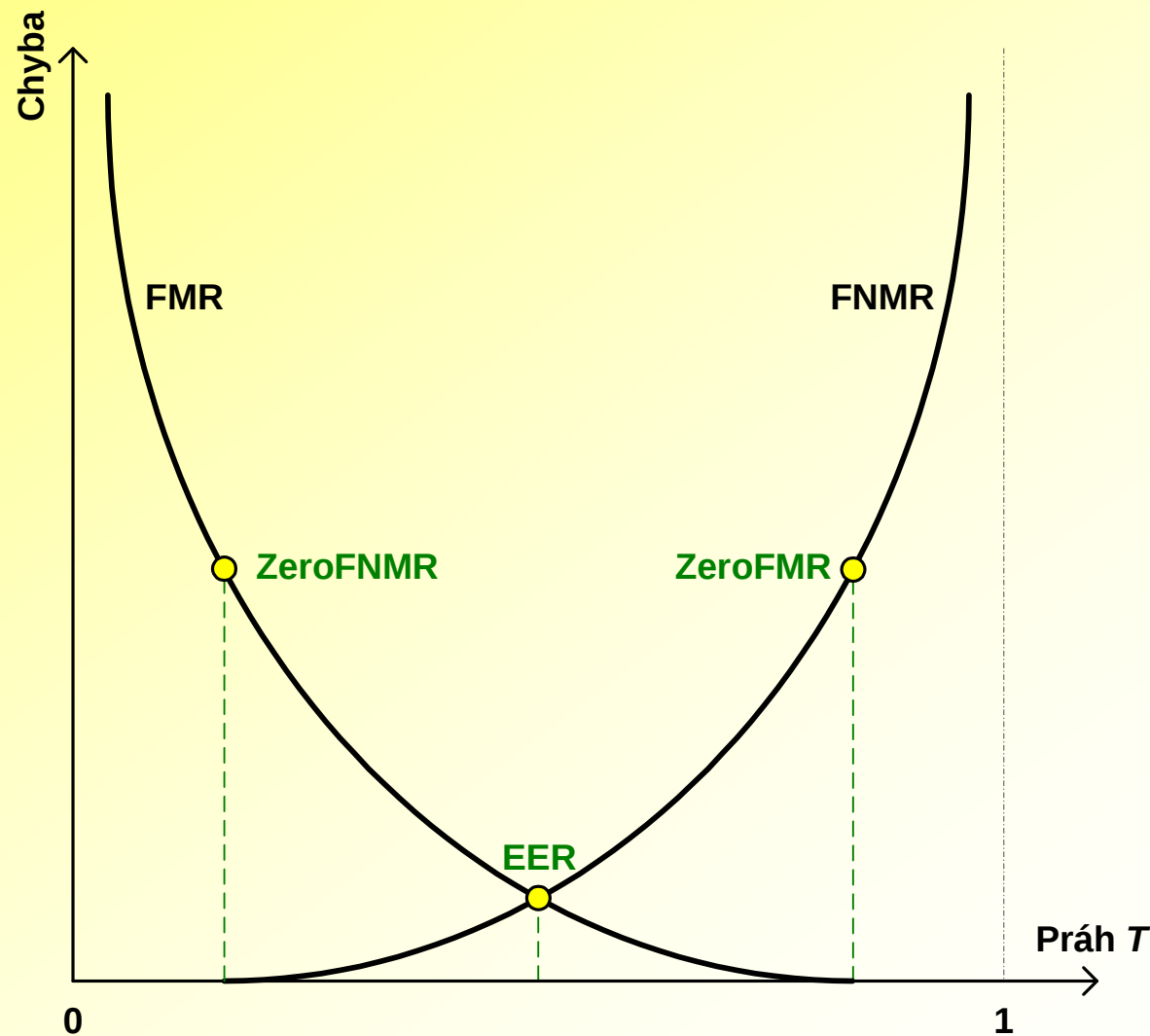


→ Chyby - *Equal Error Rate (EER)* (III.)



→ Chyby - *ZeroFMR* / *ZeroFNMR*

- **ZeroFMR** je dolní hranice **FNMR**, tj. **FMR** = 0.
- **ZeroFNMR** je dolní hranice **FMR**, tj. **FNMR** = 0.



→ Chyby - *Failure To Acquire Rate (FTA)*



- **Míra neschopnosti nasnímat - FTA**
- **FTA** udává podíl chybných záznamů v automatickém módu záznamu daného senzoru. Tj. zaznamenání biometrické charakteristiky je odmítnuto, ačkoliv je biometrická charakteristika přítomna. Čím vyšší je tato hodnota, tím méně je daný senzor vhodný pro záznam uvedené biometrické charakteristiky. Tím pádem slouží tato míra k hodnocení kvality senzorů.
- **Příklad:** Z celkového počtu 50 pokusů o nasnímání sítnice oka se nepodařilo získat data ze senzoru celkem 3×. Tedy **FTA** = $3 / 50 = 6\%$.

→ Chyby - *Failure To Enroll Rate (FTE)*



- Míra neschopnosti zaregistrovat - **FTE**
- **FTE** udává procentuální podíl uživatelů, které není systém schopen se naučit. Míry **FTE** se často vyskytují u systémů, které mají kontrolu kvality biometrické charakteristiky. Tj. biometrické charakteristiky s nedostatečnou kvalitou nejsou systémem naučeny. V tomto smyslu představuje **FTE** údaj, který ohodnocuje schopnost algoritmu pracovat i s nekvalitními biometrickými charakteristikami.
- Příklad: Z celkového počtu 200 pokusů o nasnímáním hlasu se nepodařilo z důvodu velkého hluku v pozadí rozpoznat řečový signál z mikrofonu celkem 9×. Tedy **FTE** = $9 / 200 = 4,5\%$.

→ Chyby - *Failure To Match Rate (FTM)*

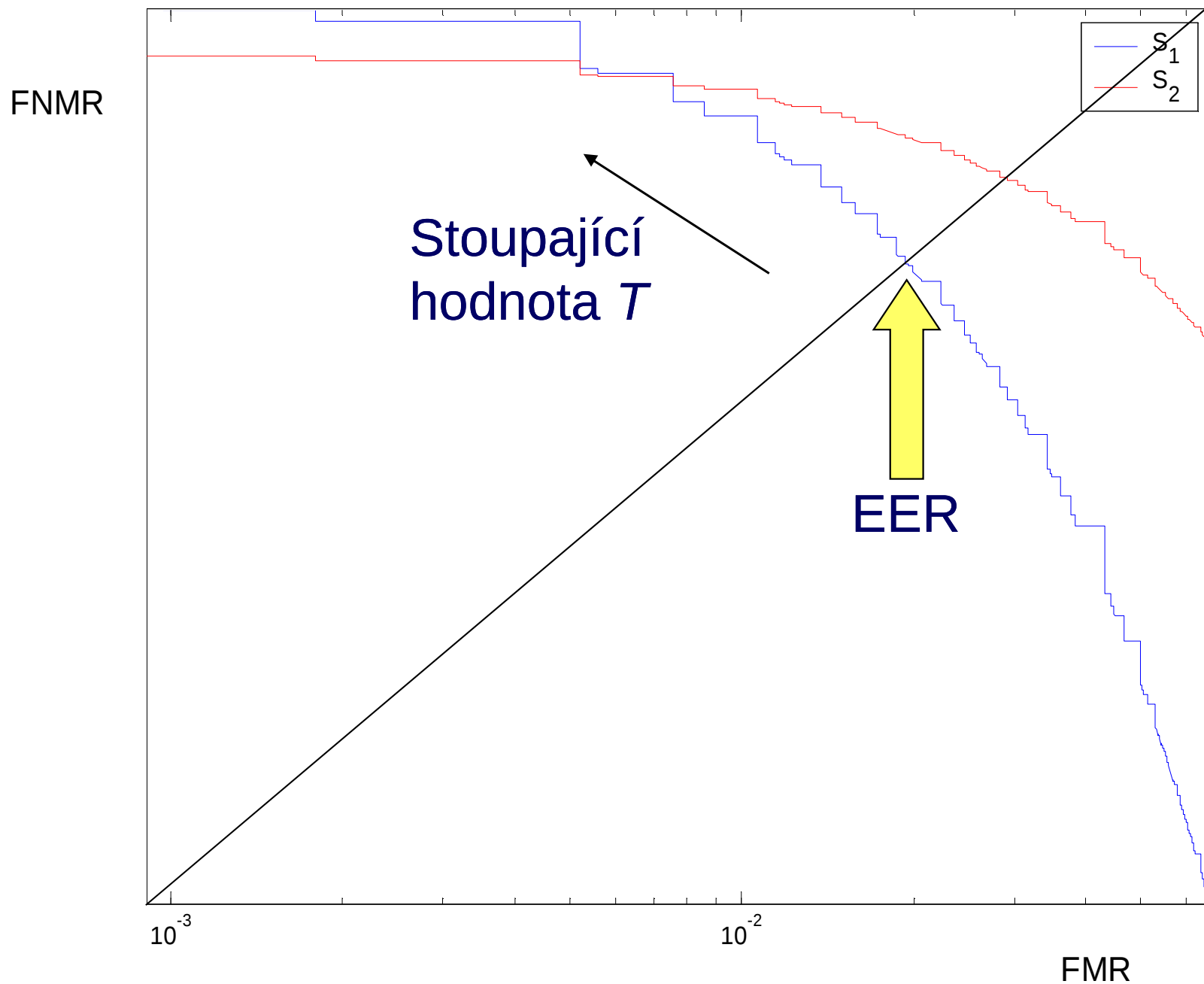
- Míra neschopnosti porovnat - **FTM**
- **FTM** udává procentuální podíl biometrických charakteristik, které nemohly být porovnány se šablonou a nebo jakkoliv jinak zpracovány (po procesu zaregistrování). Tato míra poukazuje na neschopnost systému učinit rozhodnutí, tj. porovnání nepřinese žádný výsledek.
- Příklad: Z celkového počtu 3000 pokusů o porovnání zaregistrovaných otisků prstů se nepodařilo z důvodu nedostatečného počtu markantů srovnat celkem 25 z nich. Tedy **FTM** = $25 / 3000 = 0,83\%$.

→ Chyby - ROC křivka (I.)

- **FMR** i **FNMR** jsou závislé na hodnotě prahu T
- Se změnou prahu T se zvyšuje či zmenšuje hodnota **FMR** a **FNMR** (vždy obě hodnoty naráz opačnými směry)
- Výkonnost systému se proto udává pomocí tzv. **ROC** křivky (**ROC** = *Receiver Operating Curve*)
- **ROC** křivky představují v současné době standard při popisu vlastností daného systému
- **ROC** křivky představují detekční schopnost funkce **FMR** vzhledem k **FNMR** (příp. **FAR** / **FRR**), tj.

$$\text{FNMR} = f(\text{FMR})$$

→ Chyby - ROC křivka (II.)

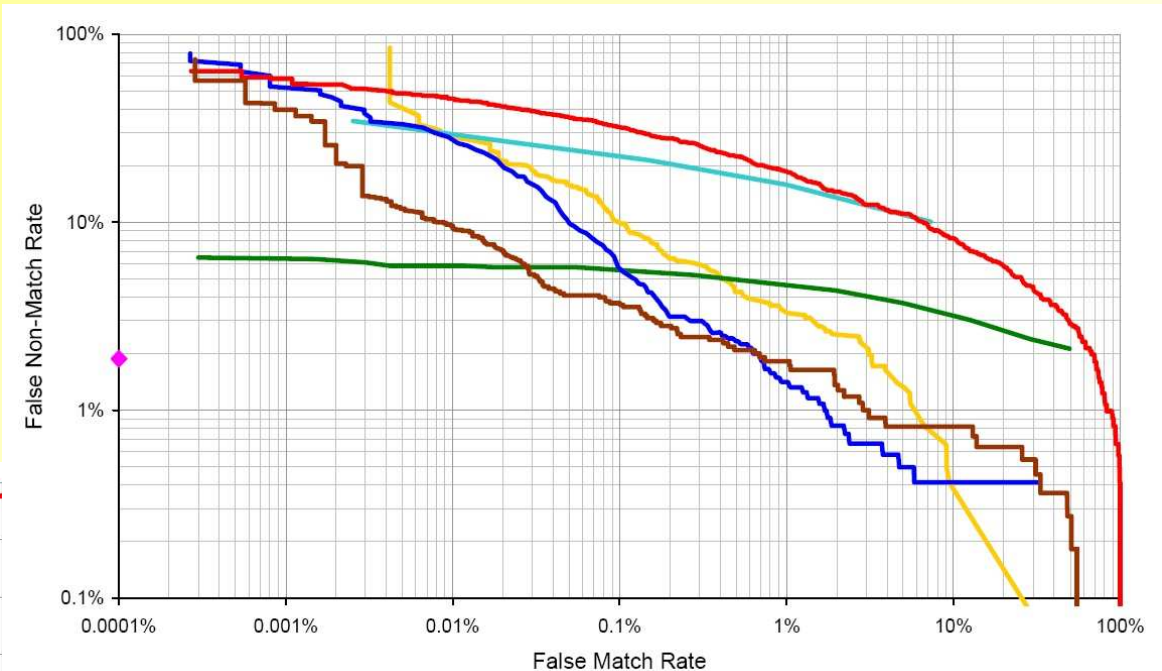
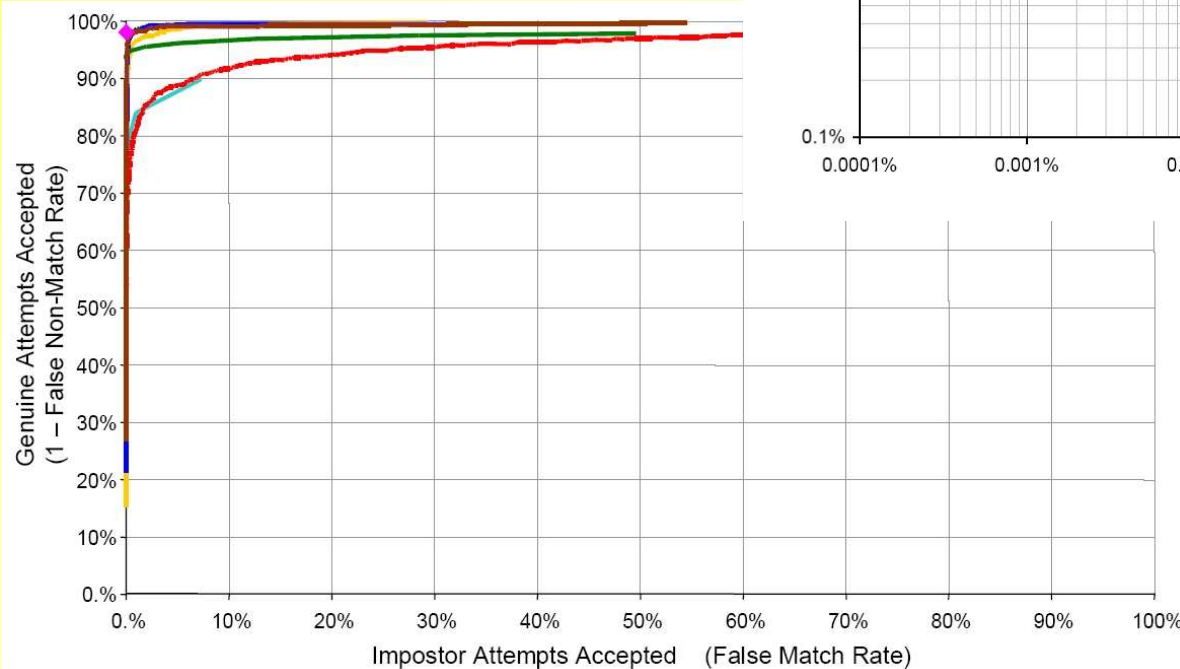


→ Chyby - ROC / DET křivka (II.)

→ ROC = *Receiver Operating Curve*

→ DET = *Detection Error Trade-off*

DET →



← ROC

→ Chyby - Souvislosti FAR / FRR (I.)

- **FTA** udává počet biometrických vlastností, které nemohly být nasnímány. Vyšší **FTA** zvyšuje **FRR** a snižuje naopak **FAR**. Počet biometrických vlastností, které nasnímány být mohly je $(1 - \text{FTA})$.
- **FTE** udává počet biometrických vlastností, které nemohly být daným algoritmem registrovány / naučeny. Vyšší **FTE** zvyšuje **FRR** a naopak snižuje **FAR**. Počet biometrických vlastností, které mohly být naučeny / zaregistrovány je $(1 - \text{FTE})$.

→ Chyby - Souvislosti FAR / FRR (II.)

- Dále lze zapsat tyto souvislosti:
 - $(1 - \mathbf{FTA}) \times \mathbf{FTE}$: odpovídá podílu biometrických vlastností, které byly nasnímány, ale nemohly být naučeny / zaregistrovány.
 - $(1 - \mathbf{FTA}) \times (1 - \mathbf{FTE})$: odpovídá podílu biom. vlastností, které byly nasnímány a zároveň naučeny / zaregistrovány.
- Jako hraniční podmínky lze psát:
 - $\mathbf{FMR}(0) = 1, \mathbf{FMR}(1) = 0$
 - $\mathbf{FNMR}(0) = 0, \mathbf{FNMR}(1) = 1$

→ Chyby - Počet porovnání

- Pro vytvoření **FMR** křivky (*Impostor Distribution*) je třeba provést následující počet porovnání:

$$N_{FMR} = \sum_{i=1}^{N_{DB}-1} (N_{DB} - i) = \frac{N_{DB} \cdot (N_{DB} - 1)}{2}$$

kde N_{DB} představuje celkový počet vzorů dané biometrické vlastnosti v databázi.

- Pro vytvoření **FNMR** křivky (*Genuine Distribution*) je třeba provést následující počet porovnání:

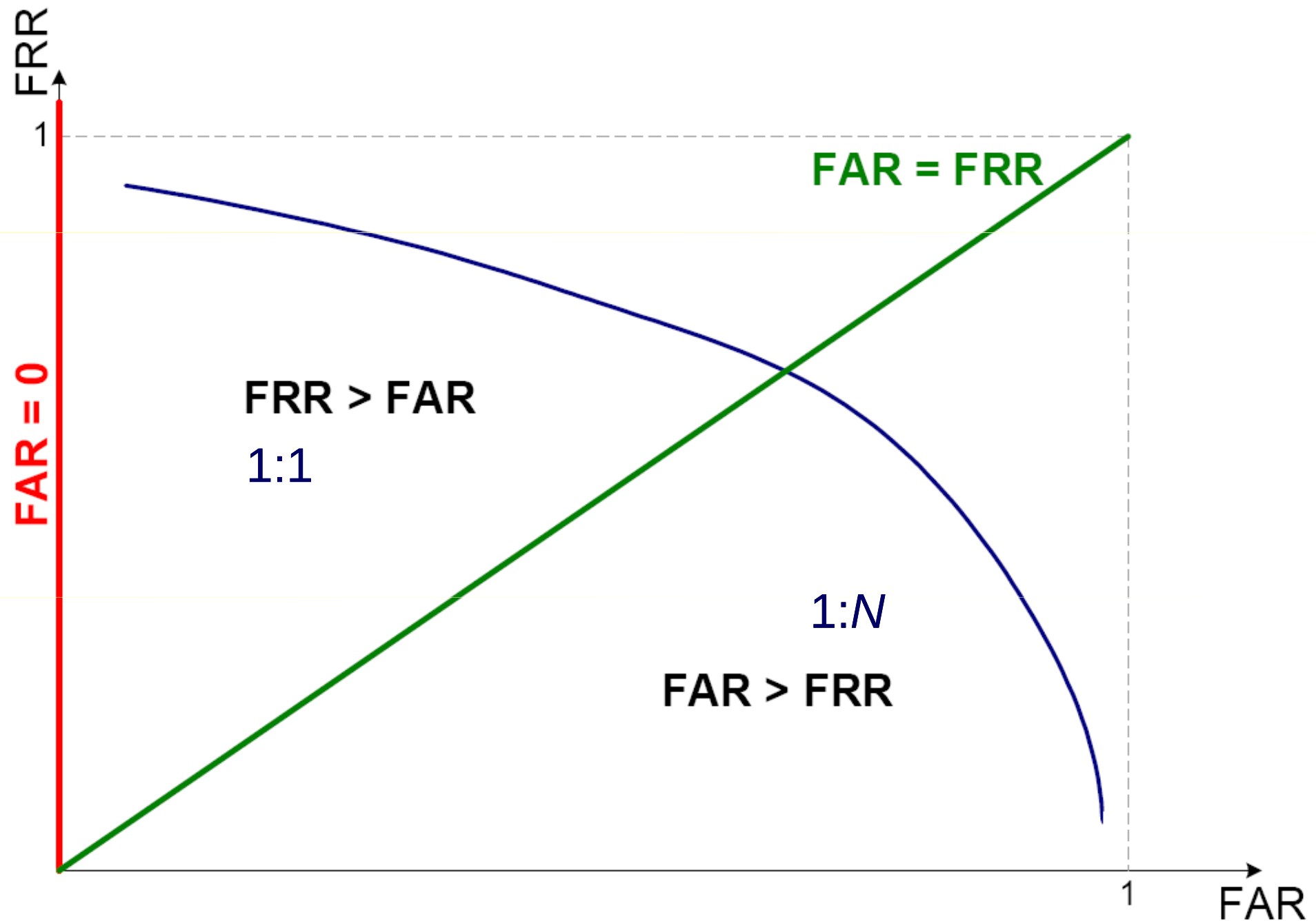
$$N_{FNMR} = \sum_{i=1}^{N_P} (N_P - i) \cdot N_{DB} = \frac{N_P \cdot (N_P - 1)}{2} \cdot N_{DB}$$

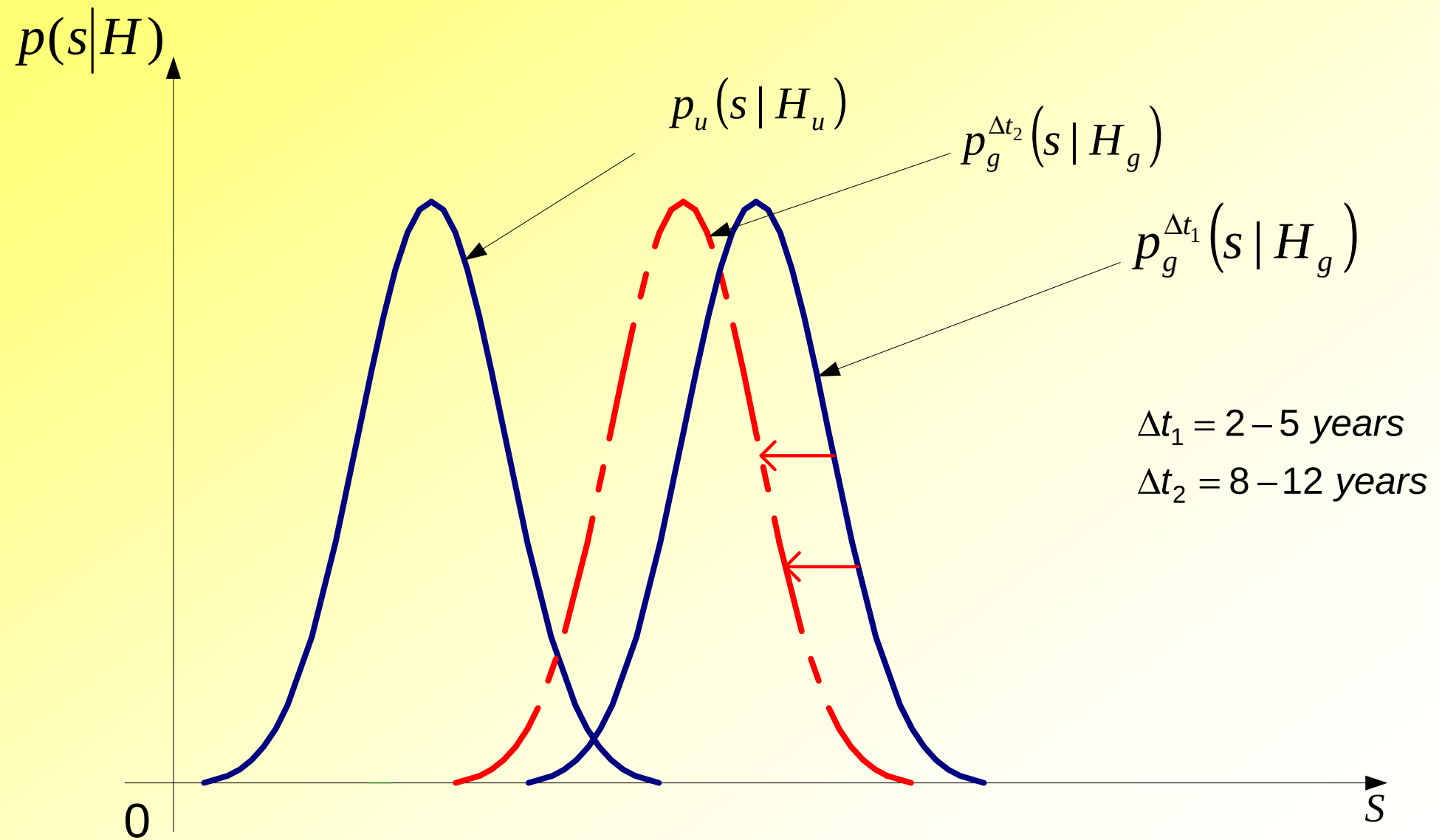
kde N_{DB} představuje celkový počet vzorů biometrické vlastnosti a N_P je počet záznamů od stejného nosiče biometrické vlastnosti (např. od téhož prstu)

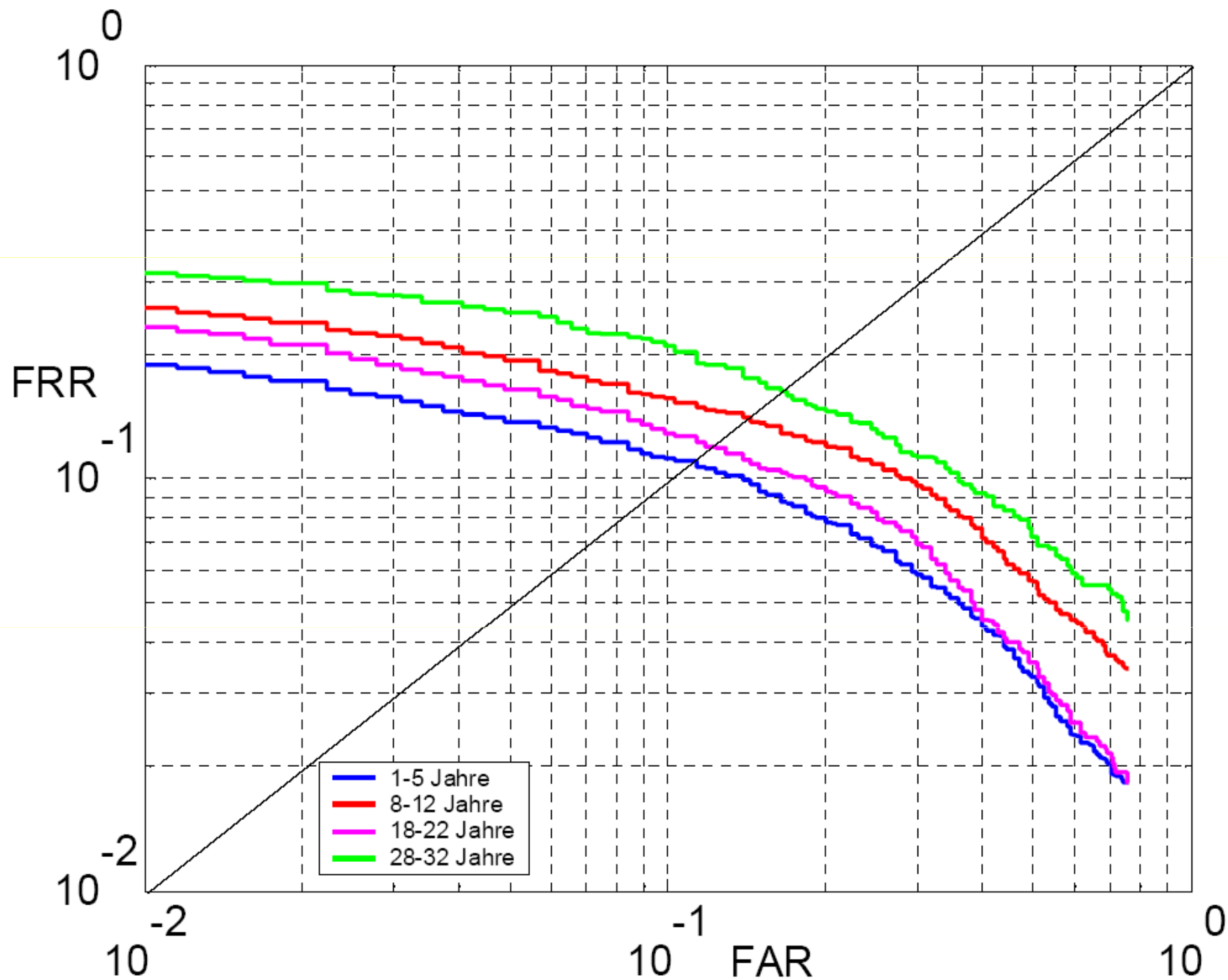
→ Chyby - Scénáře chyb (I.)

- **FRR > FAR** (**FAR** $\cong 0$) : použití různých biometrických systémů ke kontrole identity - verifikaci (1:1). Např. hraniční kontrola.
- **FRR < FAR** : použití různých biometrických systémů ke zjištění identity - identifikaci (1:N). Např. automatické rozpoznávání obličejů a jejich porovnání s databází pachatelů, mobilní použití scannerů otisků prstů a vyhledání v databázi otisků prstů trestanců, identifikace již trestaných pachatelů na základě jejich hlasu, chůze...
- Bezpečnostní síla biometrického systému dle **FAR**:
 - Základní (ISO/IEC 15408): **FAR** $\leq 10^{-2}$
 - Střední (ISO/IEC 15408): **FAR** $\leq 10^{-4}$
 - Vysoká (ISO/IEC 15408): **FAR** $\leq 10^{-6}$

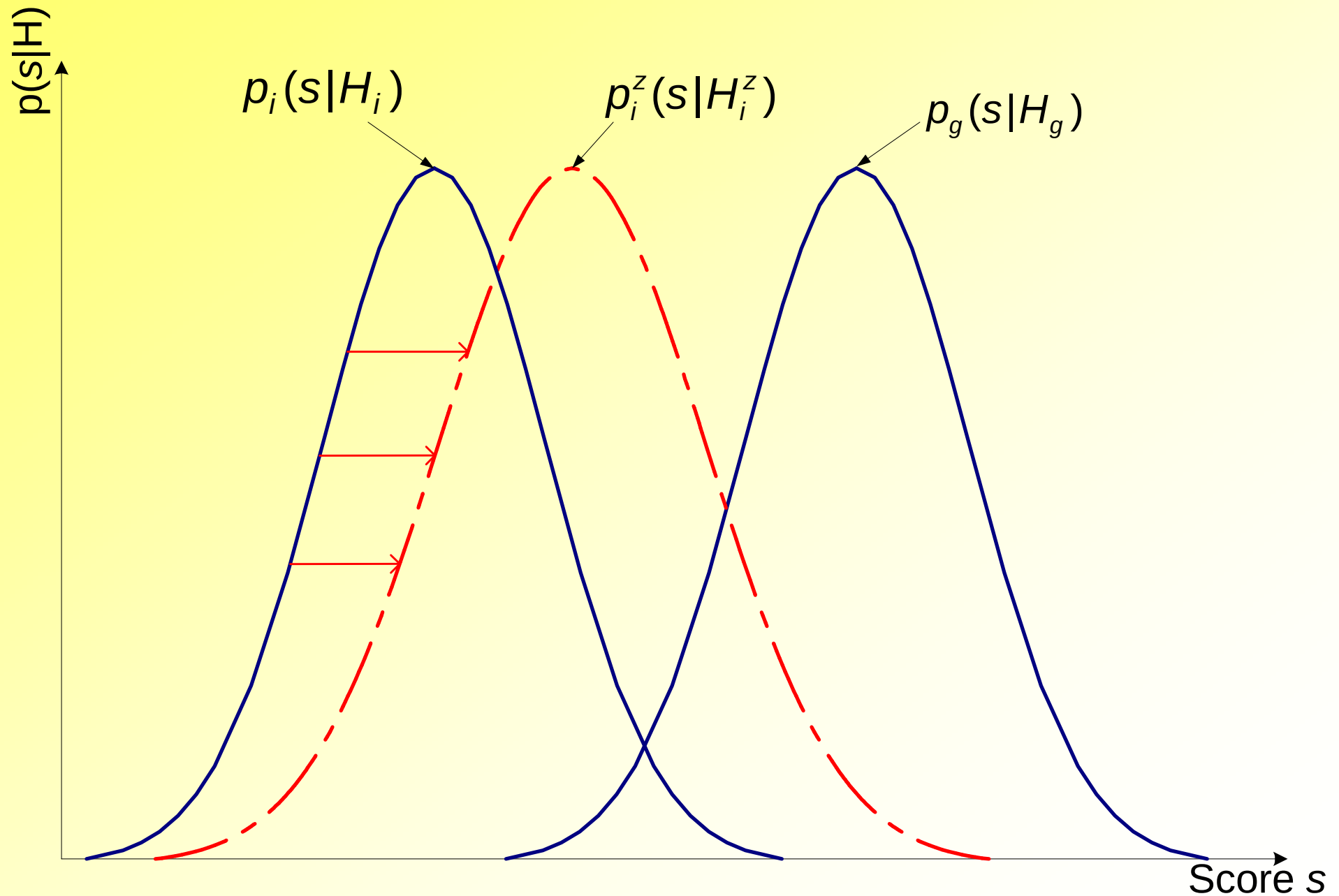
→ Chyby - Scénáře chyb (II.)



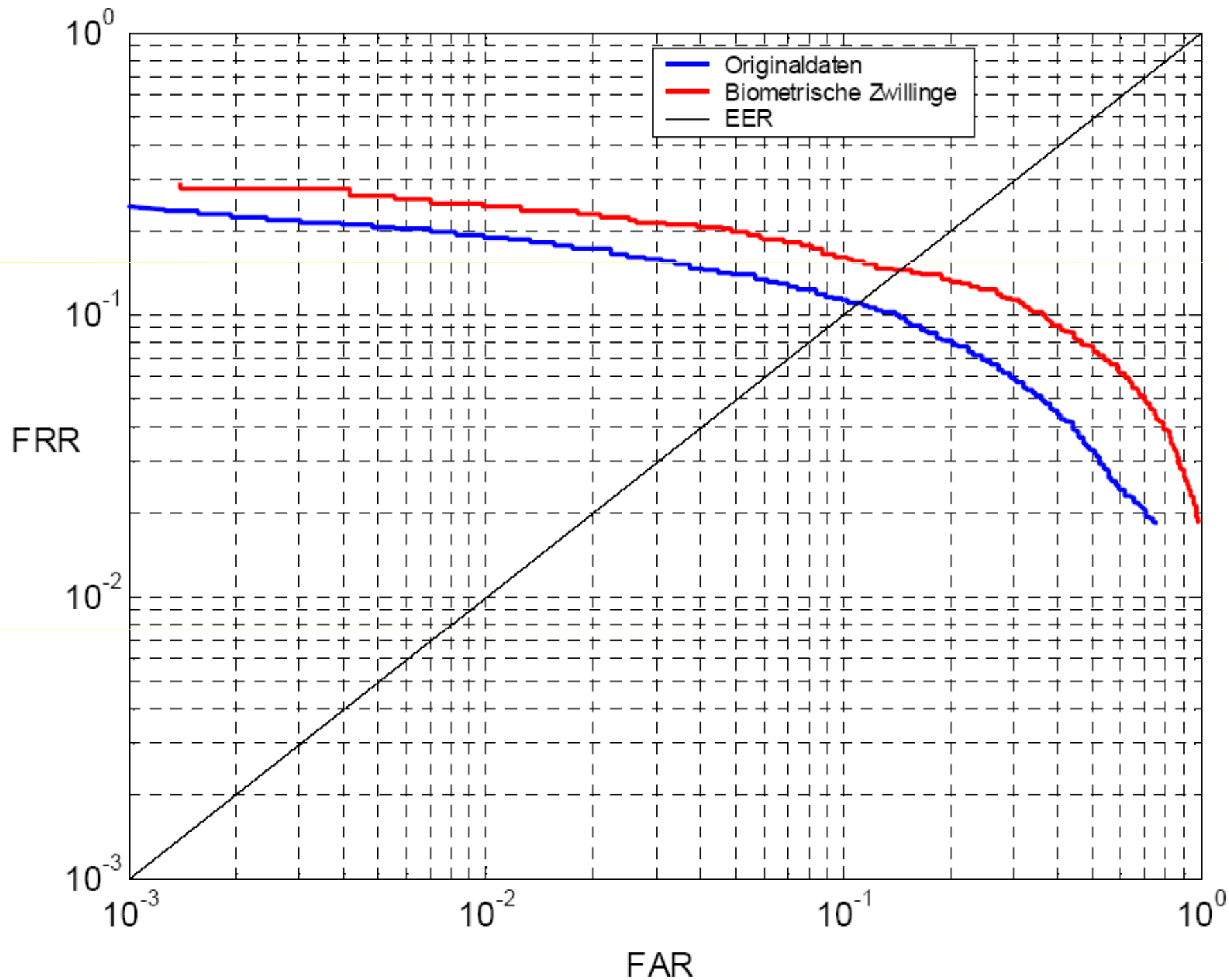




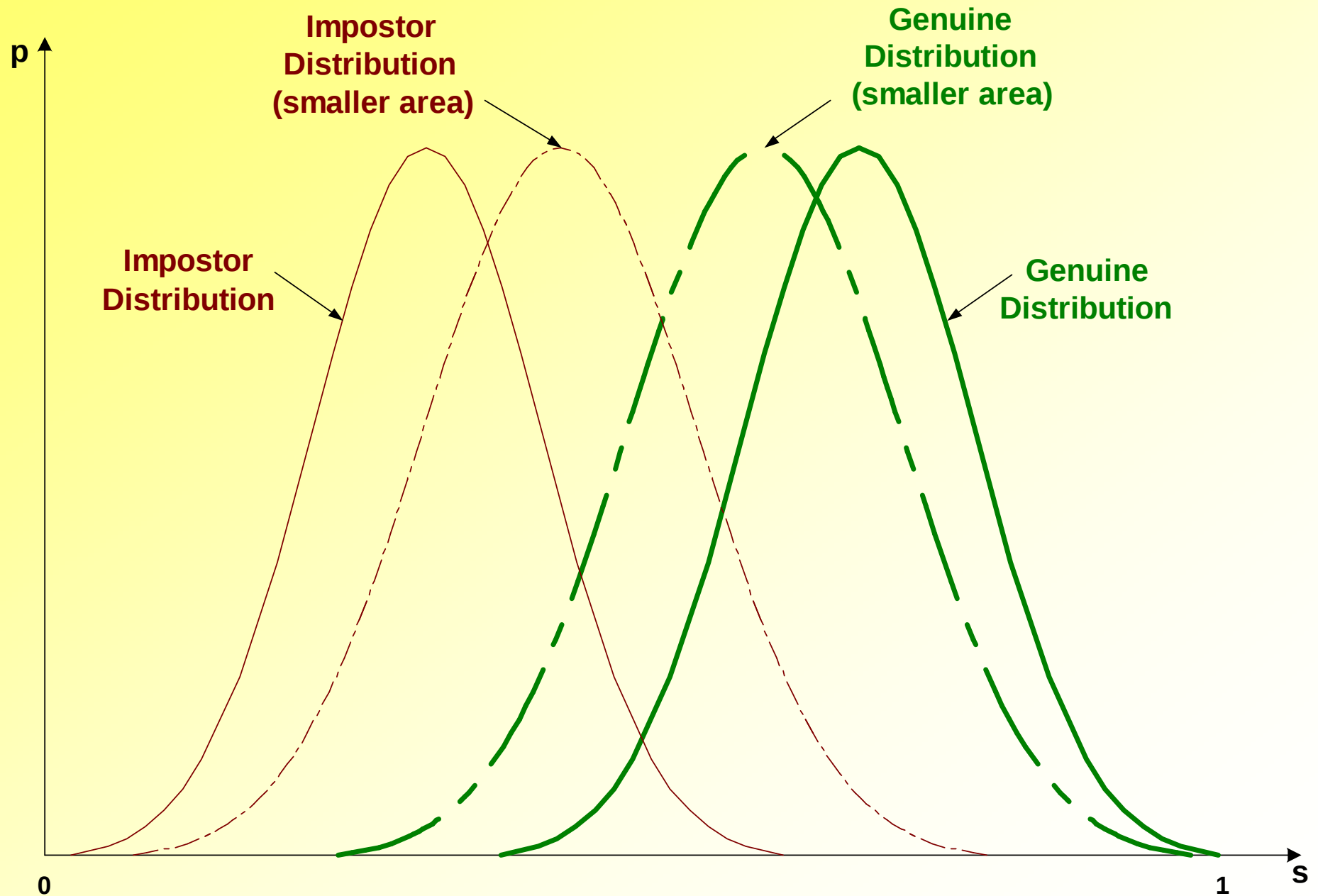
→ Dvojčata (I.)



→ Dvojčata (II.)



→ Příklad - Zmenšení plochy senzoru



→ Typy evaluace



- Evaluace technologie spočívá v testování vybraných algoritmů, které používá daný biometrický systém a jsou obvykle provedeny v laboratorních systémech či prototypch budoucích systémů.
- Evaluace scénáře testuje celkovou výkonnost a spolehlivost daného biometrického systému v prototypových situacích. Tato evaluace obsahuje snímání biometrické vlastnosti, provedení registrace a porovnání, vč. generování a předání výsledku.
- Provozní evaluace spočívá v testování zvoleného biometrického systému pro nějakou konkrétní specifickou aplikaci. Tím pomáhá určit, zda daný systém bude pracovat v reálném světě v daném konkrétním prostředí.

→ Plánování testování



- Co chceme testováním dokázat?
- Který typ scénáře evaluace máme použít?
- Určení informací o systému (log soubory, šablony, SDK, kvalita vstupu, ...).
- Kontrola faktorů ovlivňujících výkonnost (vlivy prostředí, chybná volba dobrovolníků, ...)
- Velikost testových dat
 - Pravidlo „*Rule of 3*“
 - Pravidlo „*Rule of 30*“
- Opakované testy se stejnými daty za jiných podmínek.

→ Plánování testování - Pravidlo „*Rule of 3*“

→ Pravidlo „*Rule of 3*“

→ Otázka - Jaká je nejmenší chybová míra, která může být statisticky určena na základě určitého počtu N porovnání?

→ Touto hodnotou je chybová míra p , pro kterou je pravděpodobnost žádné chyby v N pokusech (zcela náhodných), 5%. Potom

$$p \approx 3 / N \text{ pro } 95\% \text{ úroveň jistoty}$$

→ Příklad: O testu 300 nezávislých vzorků nevykazujících chyby může být vyřčeno s 95% jistotou, že chybová míra p leží pod 1%.

→ Plánování testování - Pravidlo „*Rule of 30*“



→ Pravidlo „*Rule of 30*“

- Toto pravidlo slouží k určení velikosti dat
- Abychom si byli jisti na 90%, že skutečná chybová míra leží v rozsahu $\pm 30\%$ zjištěné chybové míry, musí se vyskytnout nejméně 30 chyb.
- Příklad: Máme-li 30 chybných NM výsledků ve 3000 nezávislých pokusech oprávněných uživatelů, můžeme říct s 90% jistotou, že skutečná chybová míra leží v rozsahu $<0,7\%; 1,3\%>$.

→ Sběr dat a vyhodnocení



- Zamezení vzniku chyb při sběru dat!
- Ukládat záznamy ke každému nasnímání.
- Ukládat log-soubory pro registrování uživatelů do systému a veškeré provedené transakce.
- Evaluační scénáře různé pro
 - Transakce právoplatných uživatelů (*Genuine*)
 - Transakce útočníků (*Impostor*)
- Rozdíl pro on-line a off-line systémy
- Po provedení testů je nutné vyjádřit **FTA**, **FTE**, **FTM**,
dále **FMR+FNMR** / **FAR+FRR** a **ROC** křivky

→ Variabilita FMR

→ Musí být proveden kompletní počet porovnání všech biometrických vlastností od různých uživatelů!

→ Potom je zjištěná **FMR** (US notace): $\hat{q} = \frac{\sum_{ij} b_{ij}}{mn(n-1)}$

→ Variabilita zjištěné **FMR** může být spočtena:

$$\hat{V}(\hat{q}) = \frac{\sum_i (c_i + d_i)^2 - \sum_i \sum_{j \neq i} (b_{ij}^2 + b_{ij}b_{ji})}{m^2 n(n-1)(n-2)(n-3)} - \frac{(4n-6)}{(n-2)(n-3)} \cdot \hat{q}^2$$

→ n - počet uživatelů (šablon)

→ m - počet vzorků jednoho uživatele

→ b_{ij} - počet vzorků i -tého uživatele FM j -tou šablonu

→ $c_j = \sum_i b_{ij}$ - počet chybných shod (FM) vůči j -té šabloně

→ $d_i = \sum_j b_{ij}$ - celkový počet chybných shod u uživatele i

→ Variabilita FNMR - jeden pokus 1 uživatele

→ Pro případ, že každý z oprávněných uživatelů provede pouze jeden pokus o srovnání.

→ Potom je zjištěná **FNMR** (US notace): $\hat{p} = \frac{1}{n} \sum_i a_i$

→ Variabilita zjištěné **FNMR** může být spočtena:

$$\hat{V}(\hat{p}) = \frac{\hat{p}(1 - \hat{p})}{n - 1}$$

→ n - počet uživatelů (šablon)

→ $\hat{p}$ - zjištěná **FNMR** pro všechny uživatele

→ $\hat{V}(\hat{p})$ - zjištěná variabilita **FNMR** pro všechny uživatele

→ a_i - počet FNM pro i -tého uživatele

→ Variabilita FNMR - více pokusů 1 uživatele

- Pro případ, že každý z oprávněných uživatelů provede více pokusů o srovnání (všichni stejný počet!).
- Potom je zjištěná **FNMR** (US notace): $\hat{p} = \frac{1}{n} \sum_i p_i = \frac{1}{mn} \sum_i a_i$
- Variabilita zjištěné **FNMR** může být spočtena:

$$\hat{V}(\hat{p}) = \frac{\sum (p_i - \hat{p})^2}{n(n-1)} = \frac{1}{(n-1)} \cdot \left(\frac{\sum a_i^2}{m^2 \cdot n} - \hat{p}^2 \right)$$

- n - počet uživatelů (šablon)
- m - průměrný počet šablon na uživatele
- $\hat{p}$ - zjištěná **FNMR** pro všechny uživatele
- $\hat{V}(\hat{p})$ - zjištěná variabilita **FNMR** pro všechny uživatele
- a_i - počet FNM pro i -tého uživatele
- p_i - podíl neshodných porovnání vzorků i -tého uživ.

→ Příklady provedených testů

→ CESG - Best Practices

www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf

→ Face Recognition Vendor Test

www.frvt.org

→ FVC 2004

bias.csr.unibo.it/fvc2004

→ BioFinger

www.bsi.de/literat/studien/BioFinger

→ BioFace

www.bsi.de/literat/studien/BioFace

→ NIST SG

www.nist.gov/speech/tests/spk

→ Děkuji za pozornost!

→ Přednáška: 4. Rozpoznávání podle otisků prstů

→ Použitá literatura: [BIF04], [Dit04], [Dra05], [Jai04],
[Jai04], [Mac04], [Man02]

http://www.natasafety1st.org/posters/2001_Mission_Impossible.jpg

http://www.angel-investor-news.com/ART_Biometric.htm

<http://mathworld.wolfram.com/BinomialDistribution.html>