

PHILIPS



sense and simplicity

Aspects & System Performance for Helper-Data Systems: *Performance, Key Size, and Convenience*

Emile Kelkboom^a, Jeroen Breebaart^a, Koen de Groot^a, Raymond Veldhuis^b, Willem Jonker^b

^a Philips Research, The Netherlands

^b University of Twente, The Netherlands

Privacy and Security Risks

- Unprotected storage of the biometric data may lead to
 - Identify theft
 - Cross-matching
 - Limited renewability
 - Leaking medical information
 - Function creep

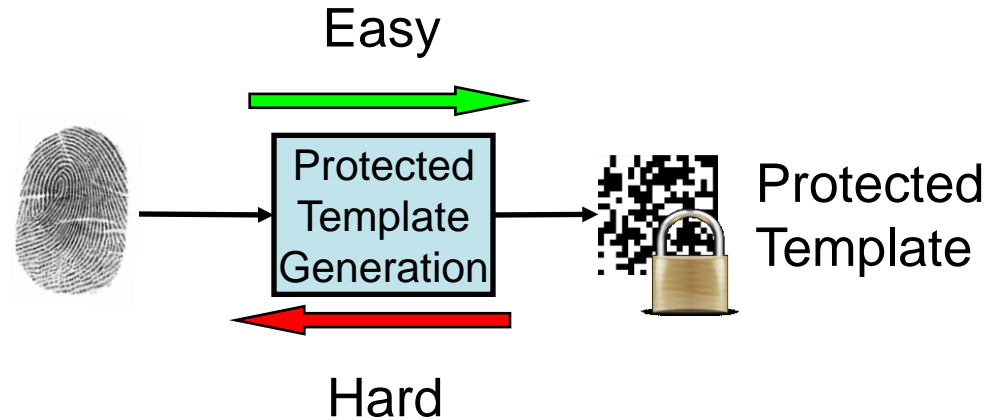
- Solution: **Template Protection (TP)**



Basic Properties of a Template Protection System

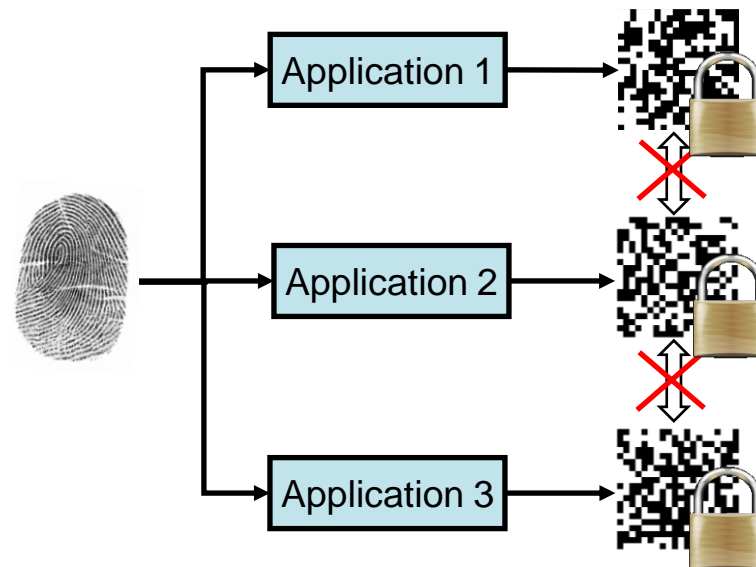
- Irreversibility

- Prevent identity theft
- Protect medical information
- Prevent function creep



- Unlinkability

- Enable renewability
- Prevent cross-matching



Key Binding/Release Notion

Key Binding (Enrolment)

Key Release (Verification)



Key Binding/Release as a Binary Symmetric Channel



- Effect of the **key size** $k_c=|K|$:
 - Determines the effort of guessing the key: $2^{k_c} - 1$
 - Defines the number of different protected templates: 2^{k_c}

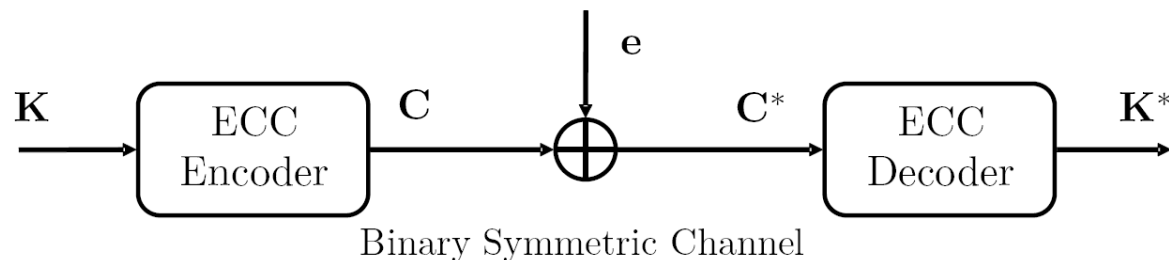
Performance, Key Size, and Convenience

- The **performance** of a biometric system can be expressed by
 - False match rate (FMR): same key at **imposter** comparison
 - False non-match rate (FNMR): different key at **genuine** comparison
- **Key size** $k_c = |K|$:
 - Determines the effort of guessing the key
 - Defines the number of unlinkable protected templates
- The **convenience** is influenced by
 - Operating FNMR: Annoying false rejections
 - Acquisition and queue time
 - The number of enrolment samples $N_e \rightarrow$ **only once**
 - The number of verification samples $N_v \rightarrow$ **at each verification session**

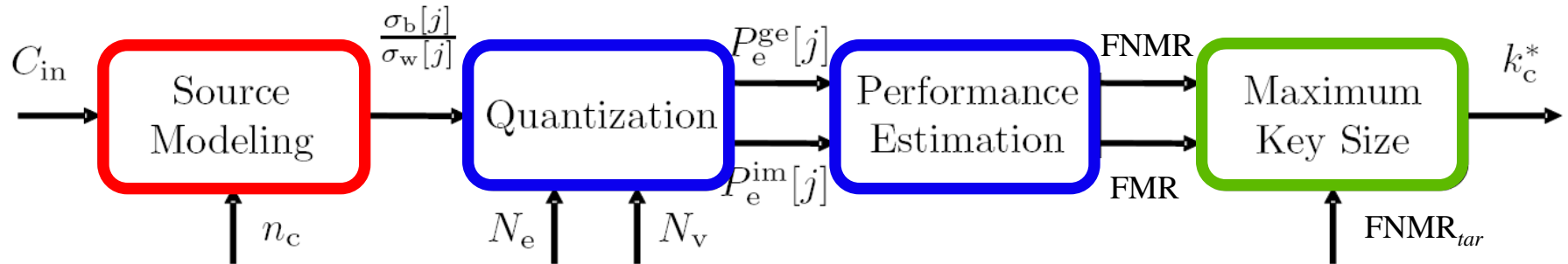


Research Questions:

- Given a binary symmetric channel
 - What is the performance?
 - What is the maximum key size?
 - How are both linked with respect to the convenience?



Analytical Framework



- Modeling the biometric feature vectors as a Gaussian source
 - Discriminating information indicated by the input capacity C_{in}
 - C_{in} is equally distributed among the n_c independent feature components

- Determine the template protection performance
 - Including the number of enrolment (N_e) and verification (N_v) samples

- Derive the maximum key size at targeted performance
 - Assuming an ECC at Shannon's bound

Biometric Source Modeling

- n_c independent feature components modeled by two Gaussian densities
 - Within-class
 - Biometric variability
 - Measurement noise
 - Between-class
 - Spread of mean across population

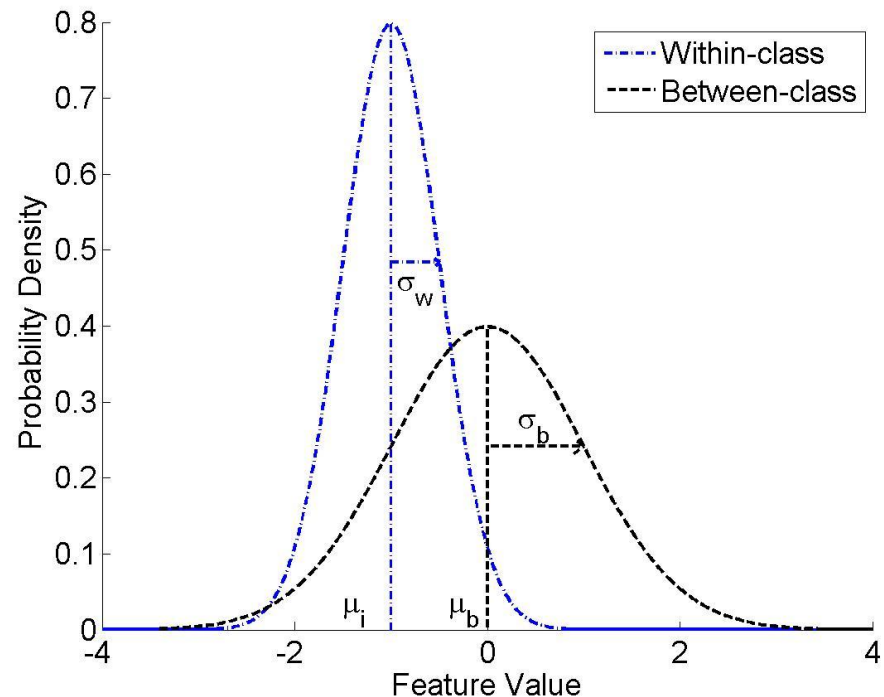
• Feature quality is $\frac{\sigma_b[j]}{\sigma_w[j]}$

• Gaussian channel capacity

$$C_G[j] = \frac{1}{2} \log_2 \left(1 + \left(\frac{\sigma_b[j]}{\sigma_w[j]} \right)^2 \right)$$

• Input capacity

$$C_{in} = \sum_{j=1}^{n_c} C_G[j]$$

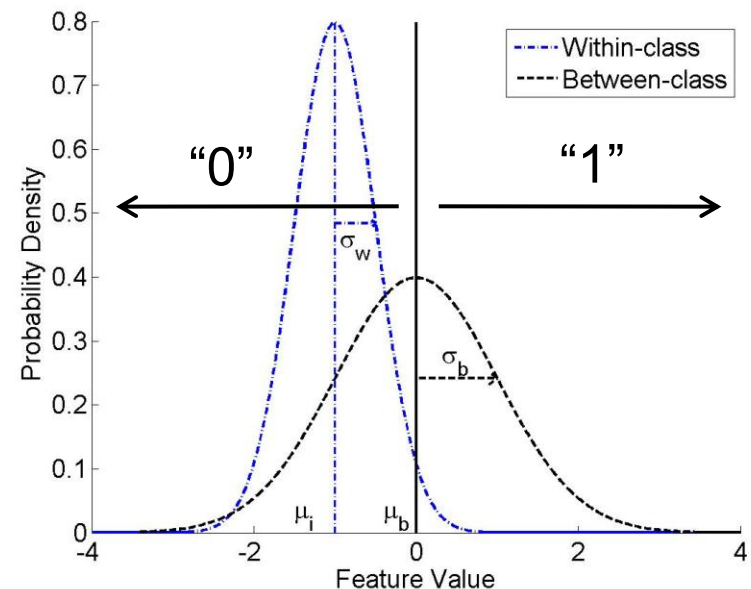


Quantization: Bit-Error Probabilities, $P_e[j]^*$

- A single-bit quantization scheme based on thresholding
 - When multiple samples are used we take the average
- Imposter comparisons
 - Each bit value is equal likely; $P_e^{im}[j] = 0.5$

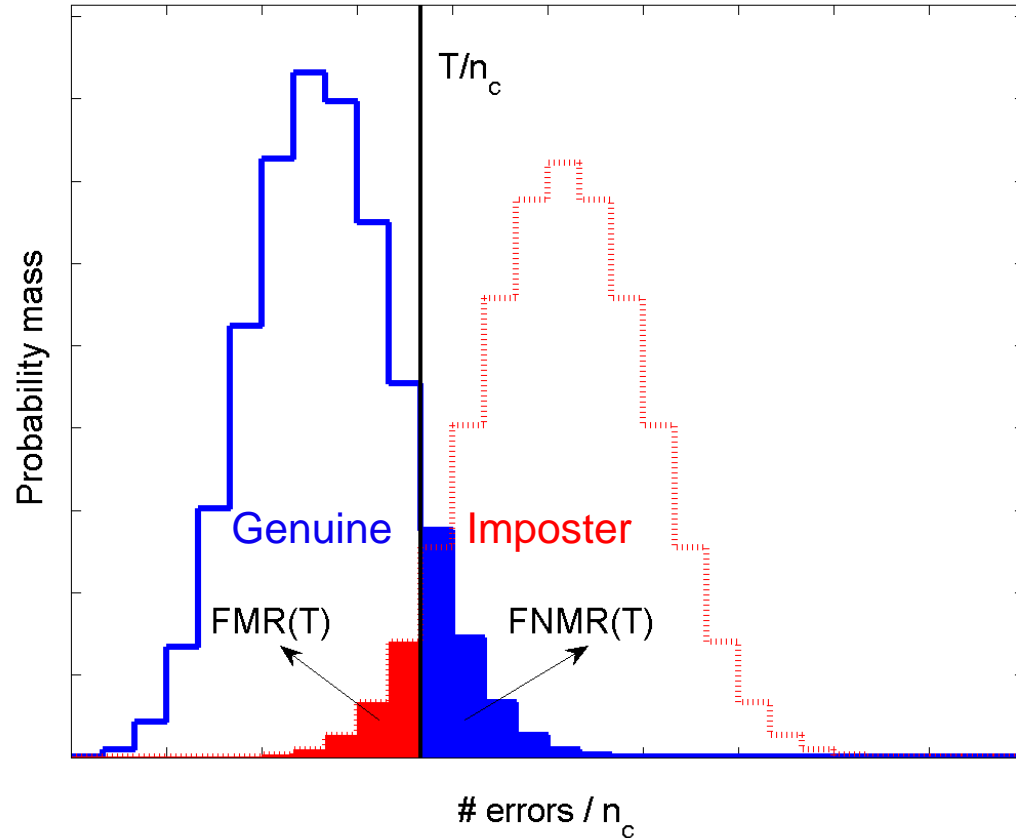
- Genuine comparisons

$$P_e^{ge}[j] = \frac{1}{2} - \frac{1}{\pi} \arctan \left(\frac{\sigma_b[j] \sqrt{N_e N_v}}{\sigma_w[j] \sqrt{N_e + N_v + \left(\frac{\sigma_b[j]}{\sigma_w[j]}\right)^{-2}}} \right)$$



* Published in: E.J.C. Kelkboom et al. "Binary Biometrics: An analytic framework to estimate the bit-error probability under Gaussian assumption", BTAS, Washington DC, 2008.

Performance: FMR and FNMR



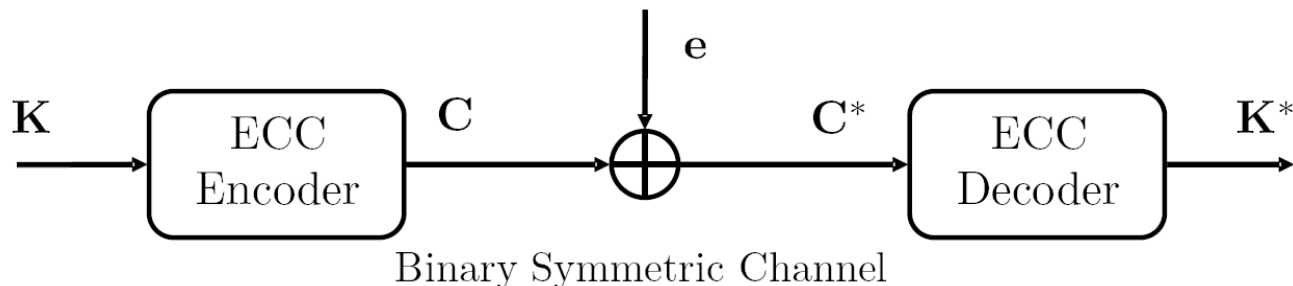
Maximum Key Size

- With the coderate $R = k_c/n_c$ and bit-error probability p , Shannon's theory dictates that there **exists** a decoding technique with an **arbitrary small decoding error** as long as

$$R < C(p)$$

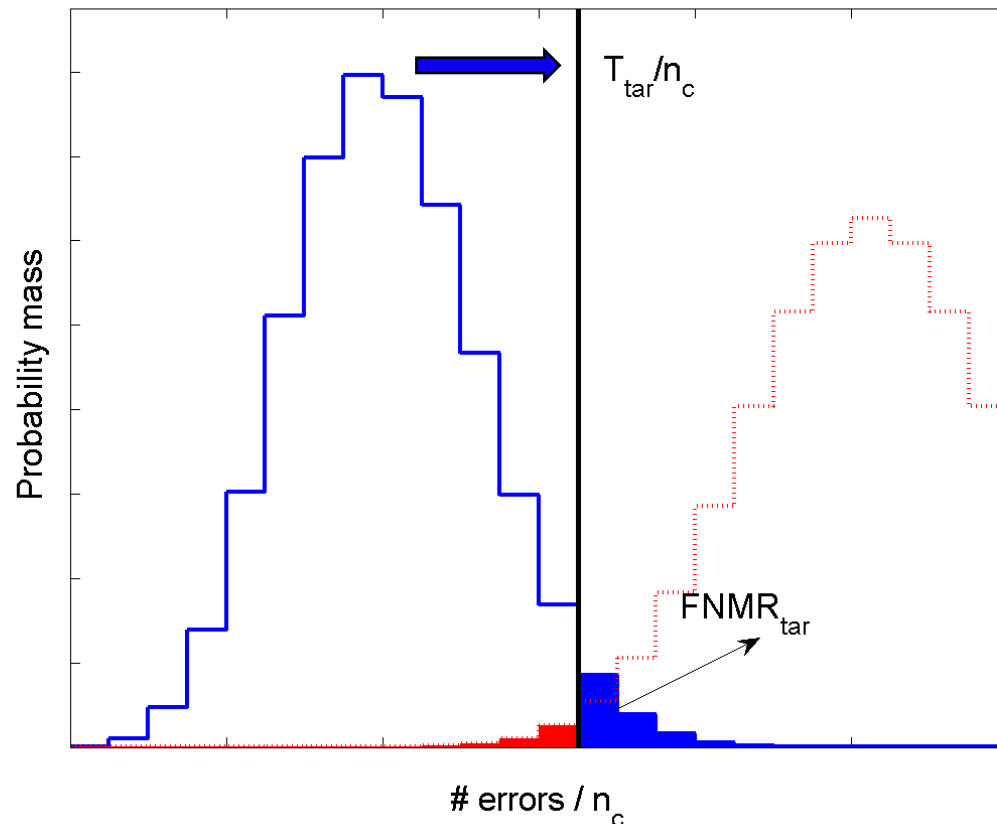
and n_c is large enough

- The maximum key size is thus $k_c = n_c R < n_c C(P_e^{ge})$



Maximum Key Size

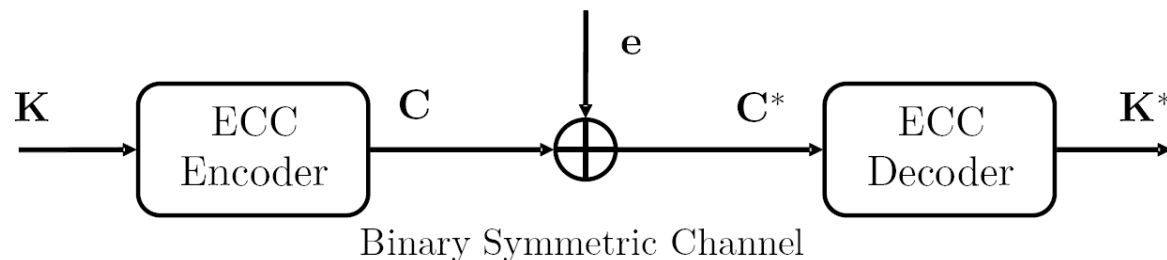
- Codeword is not large enough \rightarrow high FNMR
- Instead we take the operating point T_{tar} where $FNMR_{tar}$ is obtained
 - The maximum key size thus becomes: $k_c^* \stackrel{\text{def}}{=} n_c C\left(\frac{T_{tar}}{n_c}\right)$





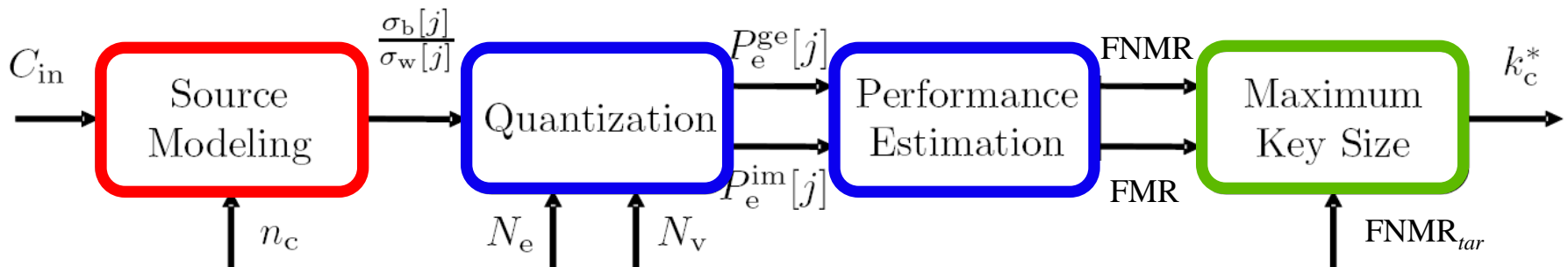
Research Questions:

- Given a binary symmetric channel
 - What is the performance?
 - What is the maximum key size?
 - How are both linked with respect to the convenience?



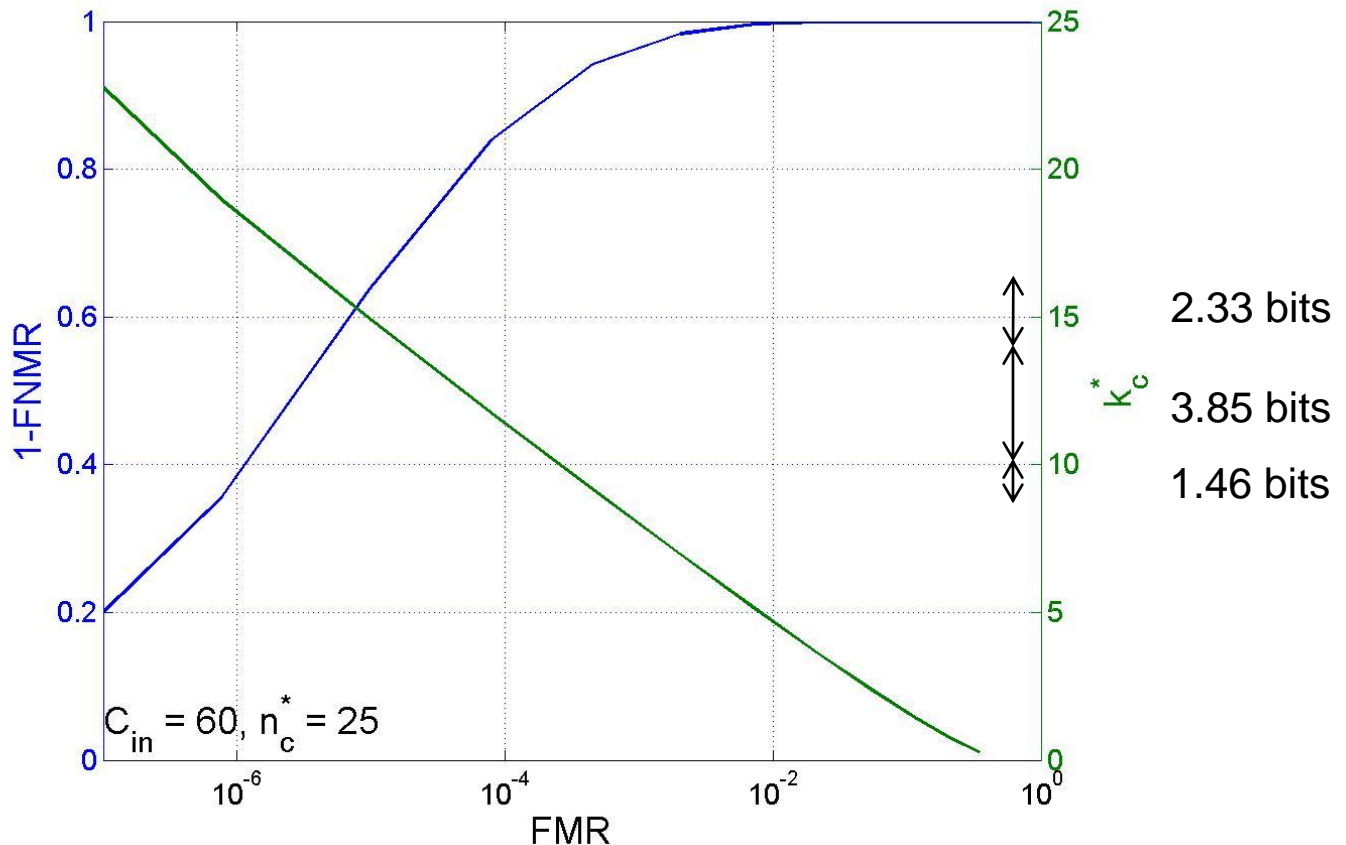
Numerical Analysis of the Maximum Key Size

- Influence of C_{in} and $FNMR_{tar}$
- Influence of N_e and N_v



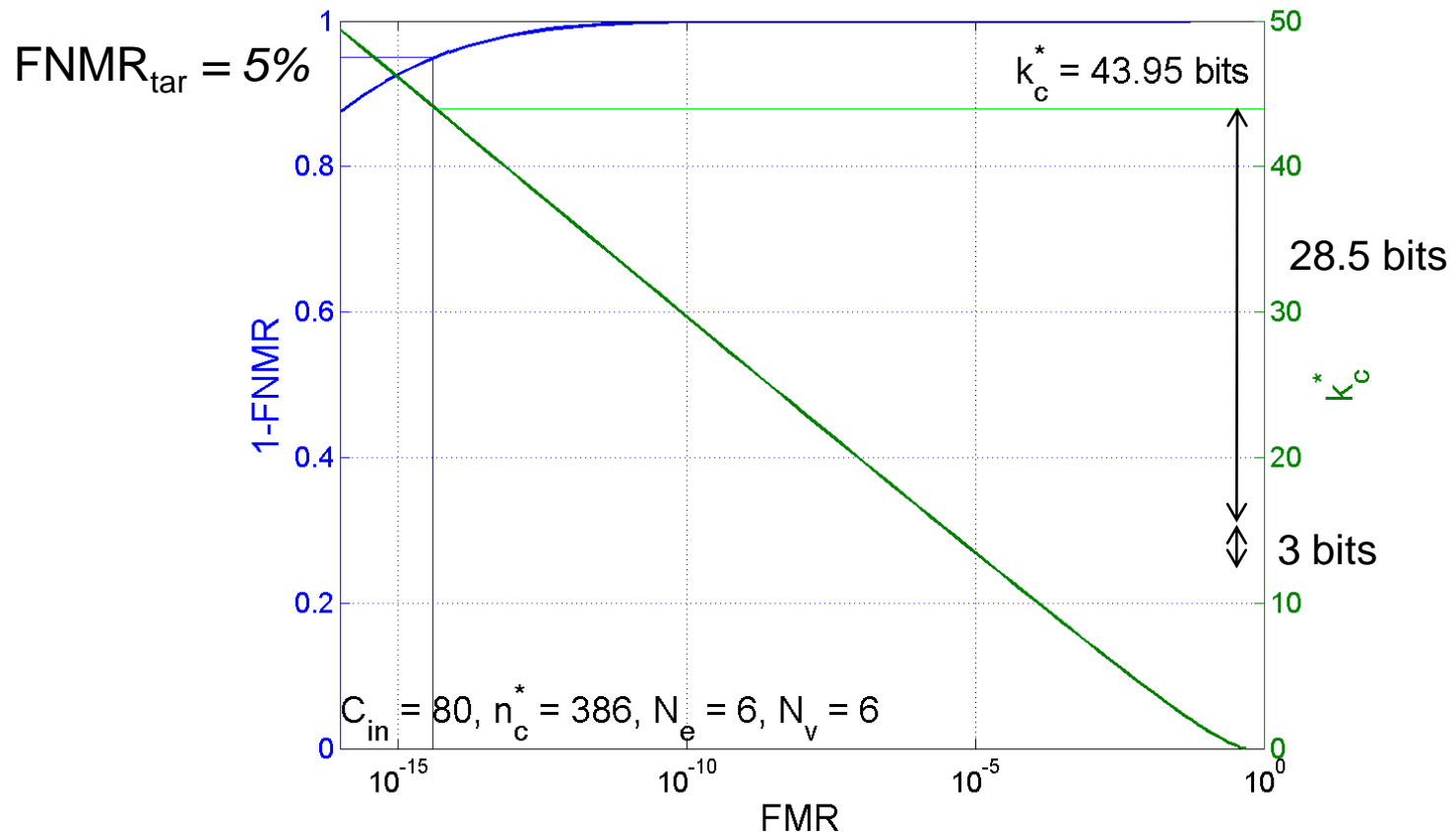
Influence of C_{in} and $FNMR_{tar}$

- Increasing either C_{in} or $FNMR_{tar}$ increases the maximum key size k_c^*
 - Doubling $FNMR_{tar}$ increases k_c^* with 1 or 2 bits



Influence of N_e and N_v

- Increasing the number of samples increases the maximum key size k_c^*
- Greatest improvement when increasing **both** N_e and N_v
 - When $N_e=N_v=6$ the key size increased with 32 bits
 - Increasing N_v has a greater impact on the convenience than N_e



Conclusions

- We have analytically determined the template protection performance and maximum key size for a
 - Key binding and release system modeled as a binary symmetric channel
 - Gaussian modeled biometric source
 - Single-bit quantization scheme based on thresholding
 - N_e enrolment and N_v verification samples
 - ECC at Shannon bound
- Sacrificing some convenience can lead to a significant improvement of the performance and key size!
 - Doubling FNMR_{tar} adds 1 to 2 bits
 - Using 6 enrolment and verification samples adds 32 bits to the key

Thank you for your attention. Any questions?



