On one definition of bit security for decision problems*

* The report is based on a set of quotations from the paper:


Sergey Kyazhin
CryptoPro LLC
• “It is common in cryptography to describe the level of security offered by a ... cryptographic primitive \( P \) by saying that \( P \) provides a certain number of bits of security” [MW18]

• “... in many cases cryptographers seem to have an intuitive (at least approximate) common understanding of what “n bits of security” means: ... for any attack with cost \( T \) and success probability \( \varepsilon \), it must be \( T/\varepsilon > 2^n \)” [MW18]
Two types of problems in cryptography

Search problems

• “adversary is trying to recover some secret information from a large search space, as in a key recovery attack” [MW18]

• “the traditional notion of bit security, as the logarithm of the ratio $T/\epsilon$” [MW18]

Decision problems

• “adversary is trying to decide if a secret bit is 0 or 1, as in the indistinguishability games” [MW18]

• new notion of bit security
“the amount of information that the adversary is able to learn about the secret” [MW18]:

\[ I(X;A) = 1 - \beta \log_2(1/\beta) - (1 - \beta) \log_2(1/(1 - \beta)) = \\
= (2\beta - 1)^2/(2 \ln 2) + O((2\beta - 1)^4) \leq \\
\leq (2\beta - 1)^2 \]

- \( X, A \) – “random variables ... modeling the secret and ... the adversary output” [MW18] (values from \{0,1\})
- \( \beta \) – “probability ... that the [adversary] output correctly identifies the secret” [MW18]

“The reasoning is that the inverse ... provides a lower bound on the number of times this adversary needs to be run in order to extract the entire secret” [MW18]
Search problems

• “adversary is trying to recover some secret information from a large search space, as in a key recovery attack” [MW18]

• “the traditional notion of bit security, as the logarithm of the ratio $T/\varepsilon$” [MW18]

Decision problems

• “adversary is trying to decide if a secret bit is 0 or 1, as in the indistinguishability games” [MW18]

• the bit security is the logarithm of $T/(2\beta – 1)^2$ [MW18]
Thank you for your attention!