Performance Evaluation of an Advanced Man-in-the-Middle Attack Against Certain HB Authentication Protocols

Miodrag Mihaljević, Siniša Tomović and Milica Knežević
Mathematical Institute of
Serbian Academy of Sciences and Arts, Belgrade, Serbia

- COST CRYPTACUS Workshop -
16-18 November 2017, Nijmegen - Netherlands

Roadmap

- **Part I**:

  - Motivation for the Work

  - Summary of the Results

- **Part II**: Key Technical Elements

  - Advanced Recovery of the Noise Bits

  - Advanced Construction & Solving the System of Equations

- **Part III:**

  A number of Numerical Illustrations

- **Concluding Notes**

Part I

- Motivation for the work
- Summary of the Results

Basic References

[1] H. Gilbert, M. J. B. Robshaw, and Y. Seurin, "HB$^{\#}$: increasing the security and efficiency of HB^{+}," in Advances in Cryptology - EUROCRYPT 2008, N. Smart, Ed., vol. 4965 of Lecture Notes in Computer Science, pp. 361-378, Springer, Heidelberg, Germany, 2008.

[2] K. Ouafi, R. Overbeck, and S. Vaudenay, "On the security of HB$^{\#}$ against a man-in-the-middle attack," in Advances in Cryptology - ASIACRYPT 2008, J. Pieprzyk, Ed., vol. 5350 of Lecture Notes in Computer Science, pp. 108-124, Springer, Heidelberg, Germany, 2008.

HB# Authentication Protocol

$\mathcal{P}$		$\mathcal{V}$
(тајни $\mathbf{X}, \mathbf{Y}$)		(тајни $\mathbf{X}, \mathbf{Y}$)
$\mathbf{e} \leftarrow \mathrm{B}er_{\tau}^{m}$		
$\mathbf{b} \xleftarrow{\$} \mathbb{Z}_2^{k_Y}$	$\xrightarrow{\mathbf{b}}$	
	$\xleftarrow{\mathbf{a}}$	$\mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^{k_X}$

$$\mathbf{z} = \mathbf{a}\mathbf{X} \oplus \mathbf{b}\mathbf{Y} \oplus \mathbf{e} \xrightarrow{\mathbf{z}} ? \ \|\mathbf{a}\mathbf{X} \oplus \mathbf{b}\mathbf{Y} \oplus \mathbf{z}\| \leq thr$$

Man-in-the-Middle Attack Against HB# Authentication Protocol

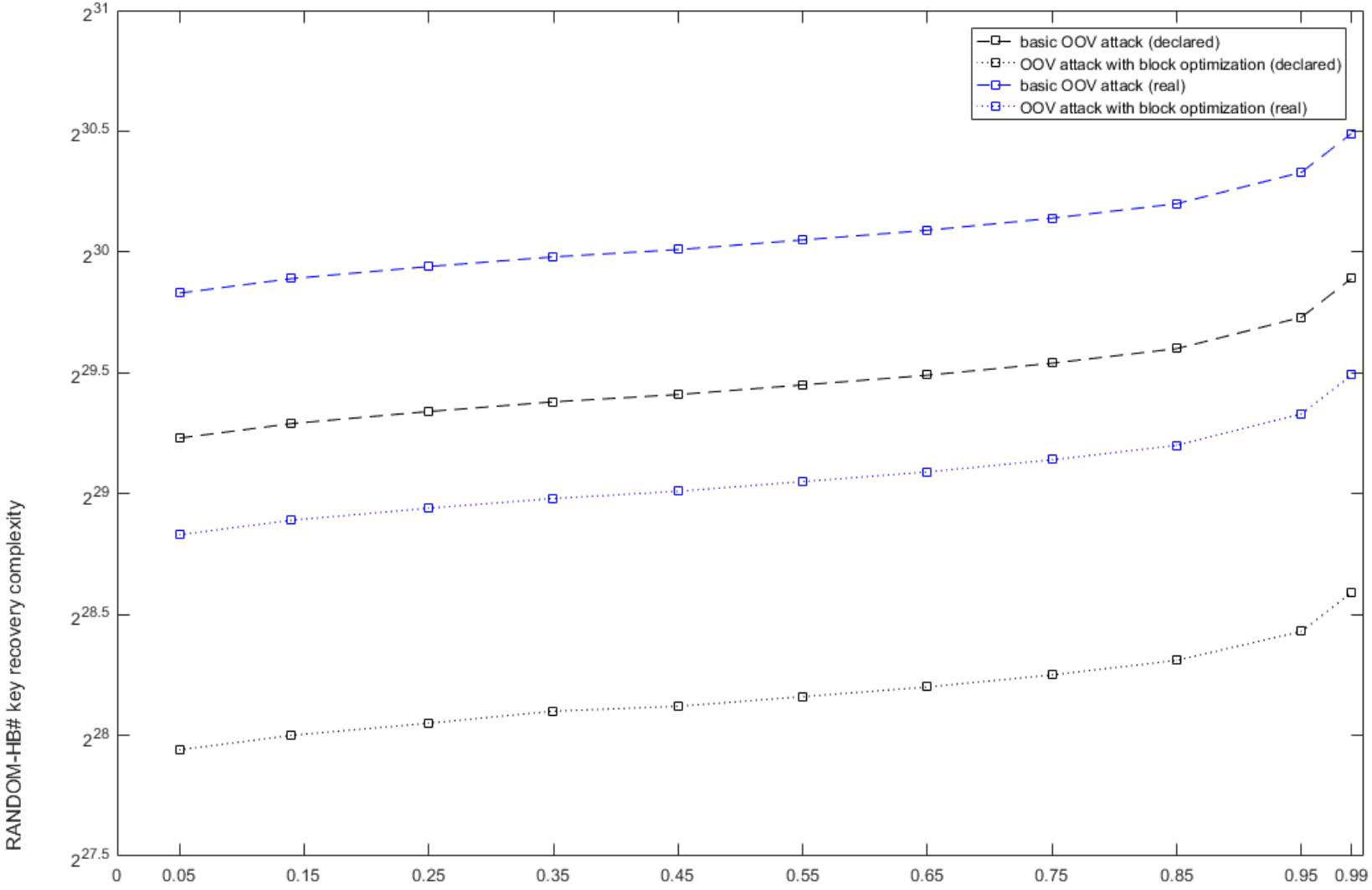
$\mathcal{P}$	$\mathcal{A}$	$\mathcal{V}$
(тајни $\mathbf{X}, \mathbf{Y}$)	триплет $(\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}})$	(тајни $\mathbf{X}, \mathbf{Y}$)
$\mathbf{e} \leftarrow Ber_{\tau}^{m}$		
$\mathbf{b} \xleftarrow{\$} \mathbb{Z}_2^{k_Y}$	$\xrightarrow{\hat{\mathbf{b}} = \mathbf{b} \oplus \bar{\mathbf{b}}}$	
	$\xleftarrow{\hat{\mathbf{a}} = \mathbf{a} \oplus \bar{\mathbf{a}}}$	$\mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^{k_X}$
$\mathbf{z} = \hat{\mathbf{a}}\mathbf{X} \oplus \mathbf{b}\mathbf{Y} \oplus \mathbf{e}$	$\xrightarrow{\hat{\mathbf{z}} = \mathbf{z} \oplus \bar{\mathbf{z}}}$	$? \ \lVert \mathbf{a}\mathbf{X} \oplus \hat{\mathbf{b}}\mathbf{Y} \oplus \hat{\mathbf{z}} \rVert \leq thr$

I.2 Motivation for our work

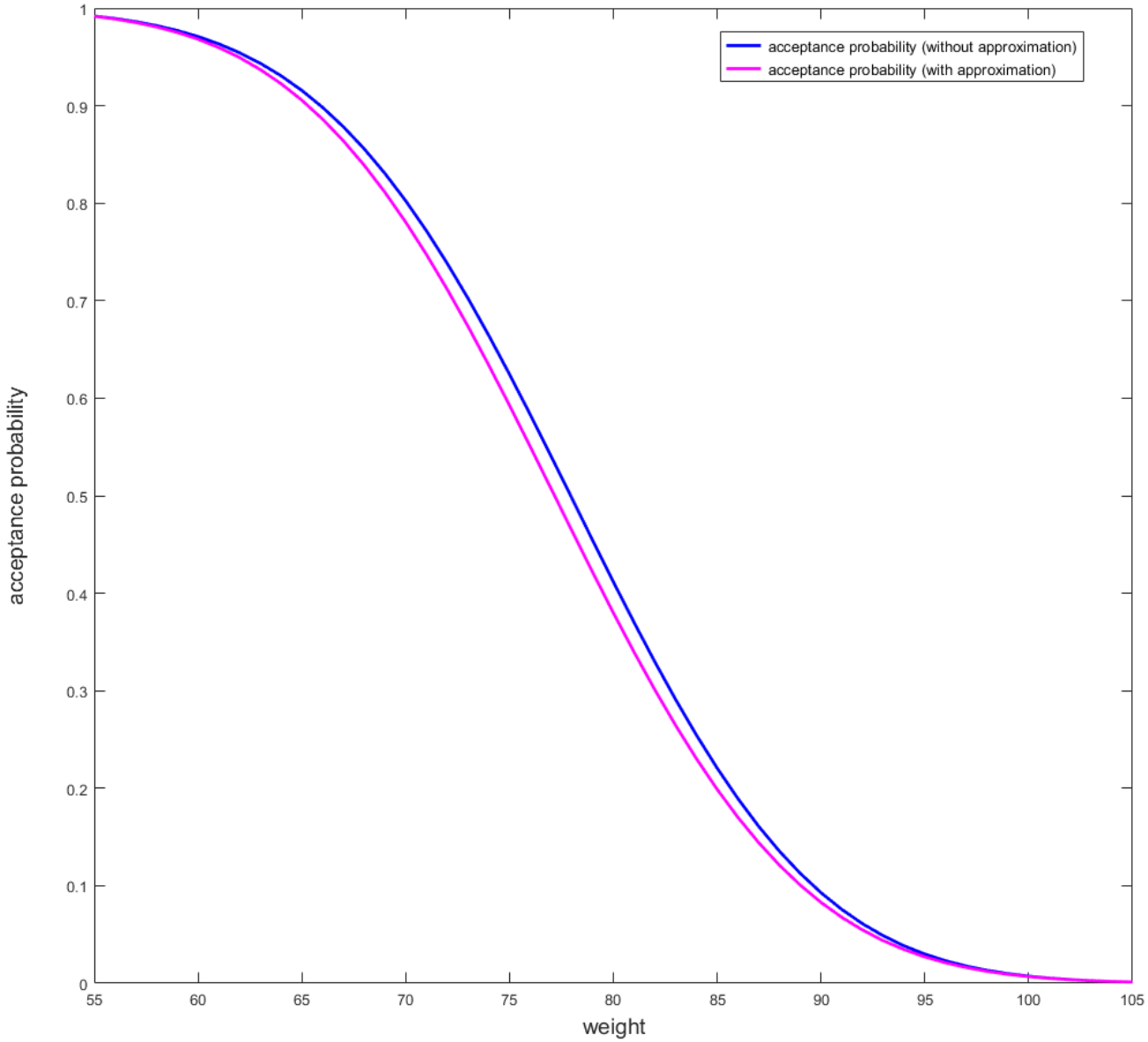
A problem with OOV [2] MIM attack

Experimental Evaluation of OOV MIM

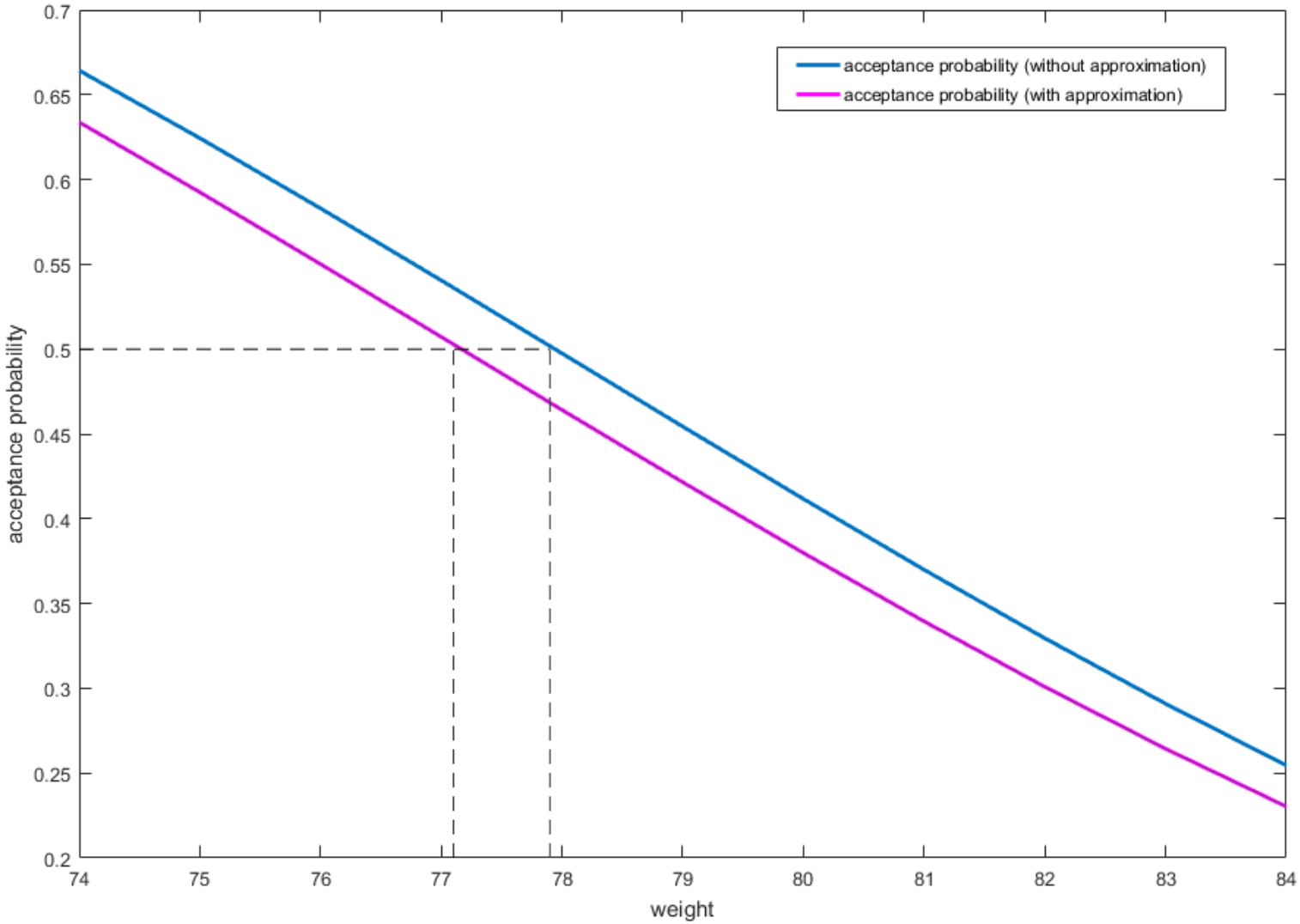
Complexity of the key recovery: Declared versus Experimentaly Evaluated



The Probability of Acceptance: Approximation & Real (1)



The Probability of Acceptance: Approximation & Real (2)



I.2 An Improved MIM Attack Against HB# Authentication Protocols

Summary of our approach and achieved results

The MIM attack proposed in [2] consists of the following main steps:

(i) estimation the weight of $\bar{\mathbf{e}}$ based on the acceptance rate after number of modified authentication sessions;

(ii) recovering i-th bit of $\bar{\mathbf{e}}$ based on the estimated weight of $\bar{\mathbf{e}}$ and the acceptance rate after an additional number of modified authentication sessions where i-th position of $\bar{\mathbf{e}}$ is flipped, $i = 1, 2, ..., m$;

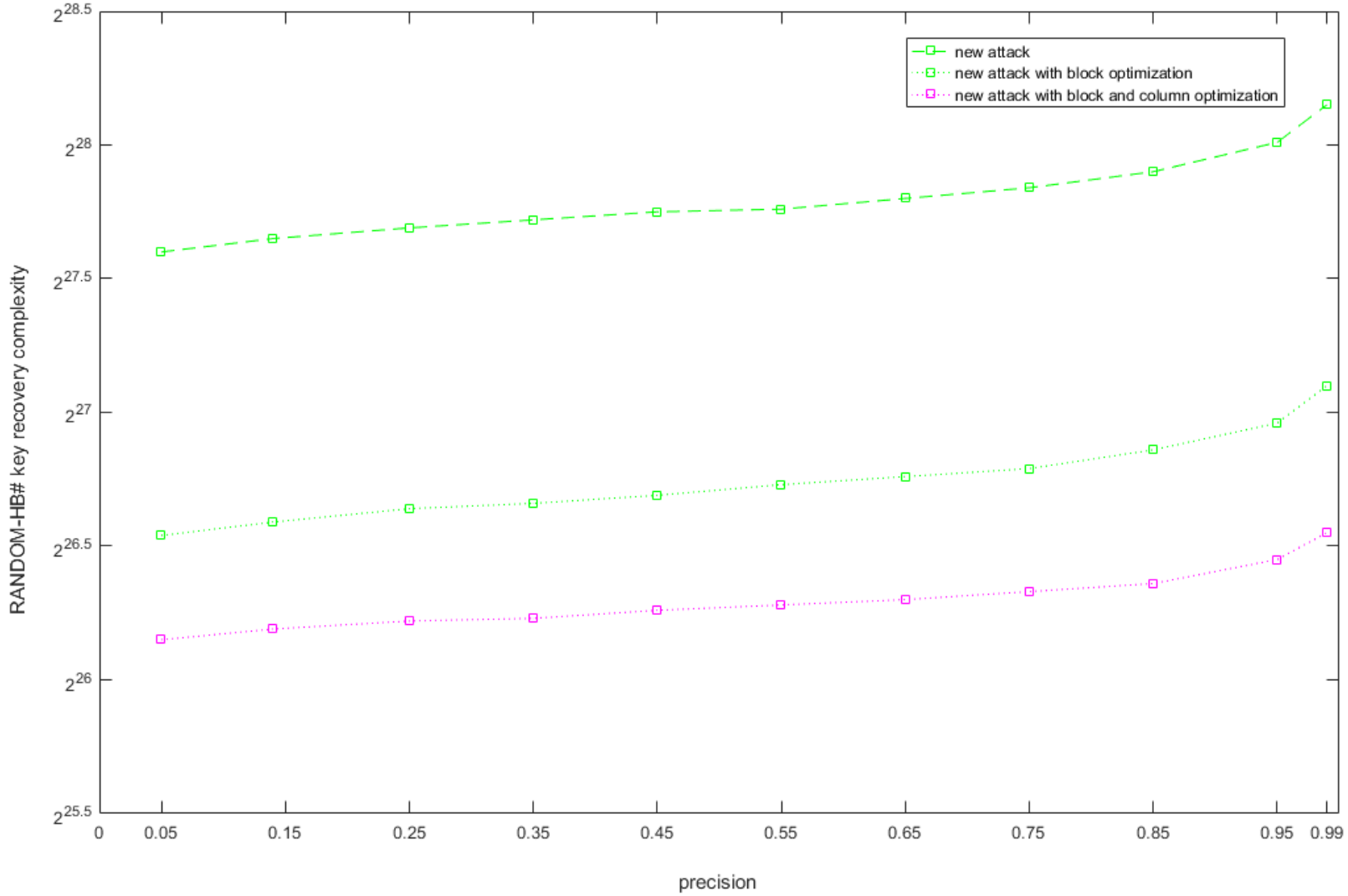
(iii) construction and solving a system of linear equations where unknowns are the secret key bits.

In this talk we point out that all three steps (i)-(iii) could be improved resulting in a significantly reduced complexity of the secret key recovery. The main underlying ideas for improvement of the attack are the following ones.

Comparison of OOV MIM and the Proposed One

	OOV MIM Attack ASIACRYPT 2008	Advanced Approach
Phase I: Evaluation of the acceptance rate after modification	same	same
Phase II: Recovering bits of the error vector	Employing inversion of the Gaussian function	Employing optimal Bayesian decision which minimizes the probability of error
Phase III: Recovering secret key bits	Employing a straightforward solving of the system of equations	Part-by-part solving the system of equations

Experimental Evaluation of Advanced MIM Attacks – Three Variants



Comparison of the Advanced and OOV MIM Attacks

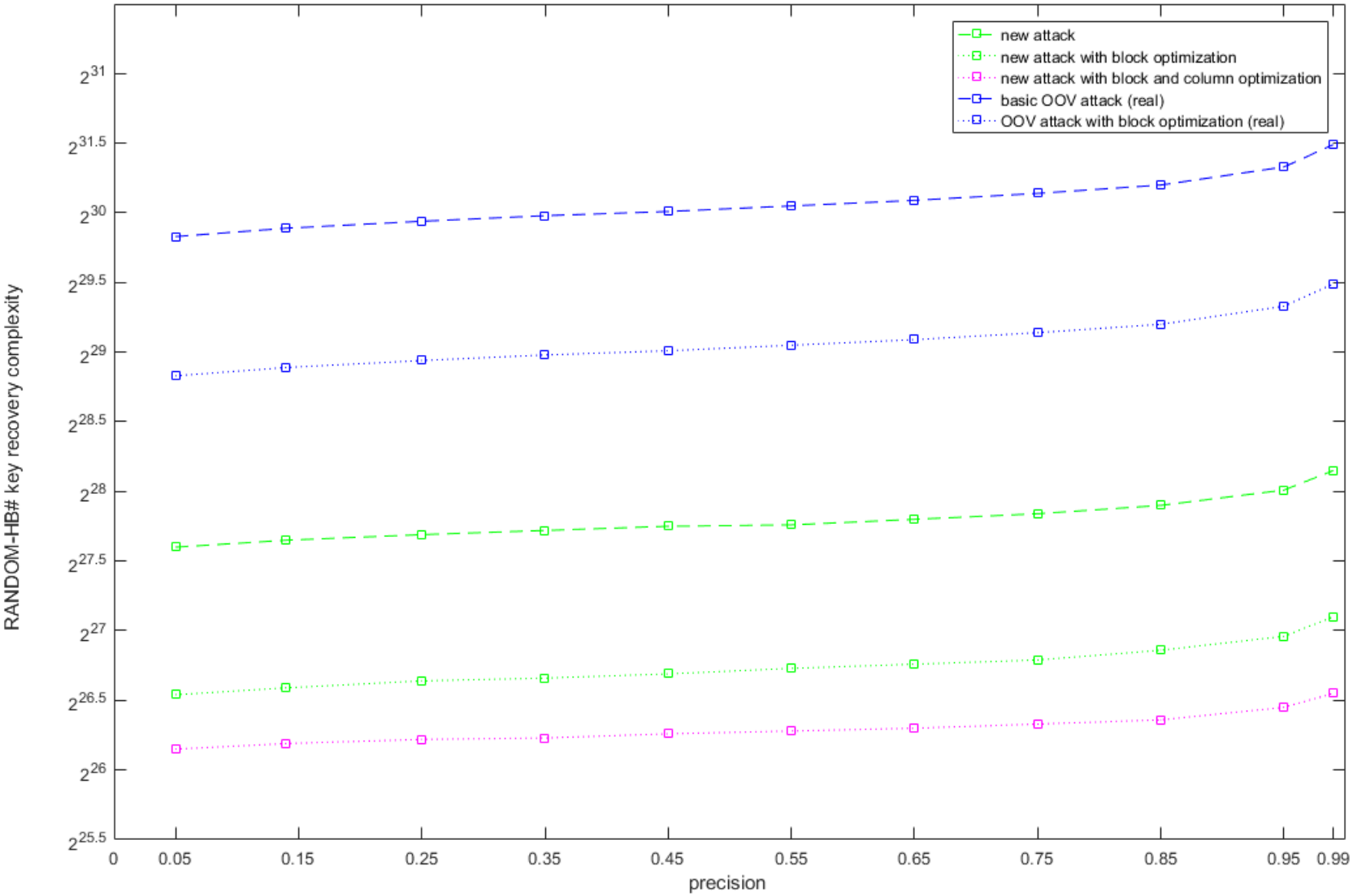


Table 1: Comparison of the complexities of Secret Key recovery

	Random HB#	**HB#**
Experimentally evaluated complexity of the MIM attack [2]	$\mathbf{2^{29.5}}$	$\mathbf{2^{20.7}}$
Experimentally evaluated complexity of the proposed improved MIM attack	$\mathbf{2^{26.5}}$	$\mathbf{2^{18.5}}$

Part II

- **Advanced Recovery of the Noise Bits**
- **Advanced Construction & Solving the System of Equations**

Advanced Recovery of the Noise Bits

Let $p_{\bar{\mathbf{a}},\bar{\mathbf{b}},\bar{\mathbf{z}}}$ denote the probability of succesfull authentication after MIM modification $(\bar{\mathbf{a}},\bar{\mathbf{b}},\bar{\mathbf{z}})$, and $S_{n,\bar{\mathbf{a}},\bar{\mathbf{b}},\bar{\mathbf{z}}}$ the random variable counting successfull authentications after repeating that MIM modification n times. Suppose that $(\bar{\mathbf{a}},\bar{\mathbf{b}},\bar{\mathbf{z}} = \bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{e}})$ is a triplet of exchanged messages during a HB# protocol session, and $w = \|\bar{\mathbf{e}}\|$. Then:

$$p_{\bar{\mathbf{a}},\bar{\mathbf{b}},\bar{\mathbf{z}}} = pb(w, thr) = \sum_{l=0}^{thr} \sum_{\alpha=0}^{\min\{l,w\}} \binom{w}{\alpha}\binom{m-w}{l-\alpha}\tau^{w+l-2\alpha}(1-\tau)^{m-(w+l-2\alpha)}$$

$$P(S_n^w = c) := P(S_{n,\bar{\mathbf{a}},\bar{\mathbf{b}},\bar{\mathbf{z}}} = c) = \binom{n}{c} pb(w, thr)^c (1-pb(w, thr))^{n-c}$$

Theorem 1. Let $p_{\bar{a},\bar{b},\bar{z}}$ denote the probability of succesfull authentication after MIM modification $(\bar{a},\bar{b},\bar{z})$, and $S_{n,\bar{a},\bar{b},\bar{z}}$ the random variable counting successfull authentications after repeating that MIM modification n times. Suppose that $(\bar{a},\bar{b},\bar{z}=\bar{a}\mathbf{X}\oplus\bar{b}\mathbf{Y}\oplus\bar{e})$ is a triplet of exchanged messages during a HB# protocol session, and $w=\|\bar{e}\|$. Then:

$$p_{\bar{a},\bar{b},\bar{z}} = pb(w,thr) = \sum_{l=0}^{thr}\sum_{\alpha=0}^{\min\{l,w\}}\binom{w}{\alpha}\binom{m-w}{l-\alpha}\tau^{w+l-2\alpha}(1-\tau)^{m-(w+l-2\alpha)}$$

$$P(S_n^w=c) := P(S_{n,\bar{a},\bar{b},\bar{z}}=c) = \binom{n}{c}pb(w,thr)^c(1-pb(w,thr))^{n-c}$$

Let $J\subset\{1,\ldots,m\}$, $|J|=k$ be a set of bit positions in some vector $\bar{e}$. $\bar{e}[J]$ is the block made of bits $\bar{e}[J[1]],\ldots,\bar{e}[J[k]]$, $w_J=\|\bar{e}[J]\|$ and $\bar{z}_J=\bar{z}\oplus\mathbf{1}_J$, where $\mathbf{1}_J\in\mathbb{Z}_2^m$ such that $\mathbf{1}_J[i]=1 \iff i\in J$. Then:

$$p_{\bar{a},\bar{b},\bar{z}_J} = pb(w+|J|-2w_J,thr)$$

$$\begin{aligned}P(S_n^{w,|J|}=c) &:= P(S_{n,\bar{a},\bar{b},\bar{z}_J}=c)\\ &= \binom{n}{c}\sum_{k=0}^{|J|}pb(w+|J|-2k,thr)^c(1-pb(w+|J|-2k,thr))^{n-c}\binom{|J|}{k}\tau_*^k(1-\tau_*)^{|J|-k}, \tau_*=\frac{w}{m}\end{aligned}$$

$$\begin{aligned}P(w_J=i\,|\,S_n^{w,|J|}=c) &:= P(w_J=i\,|\,S_{n,\bar{a},\bar{b},\bar{z}_J}=c)\\ &= \frac{pb(w+|J|-2i,thr)^c(1-pb(w+|J|-2i,thr))^{n-c}\binom{|J|}{i}\tau_*^i(1-\tau_*)^{|J|-i}}{\sum_{k=0}^{|J|}pb(w+|J|-2k,thr)^c(1-pb(w+|J|-2k,thr))^{n-c}\binom{|J|}{k}\tau_*^k(1-\tau_*)^{|J|-k}}, \tau_*=\frac{w}{m}\end{aligned}$$

Implications

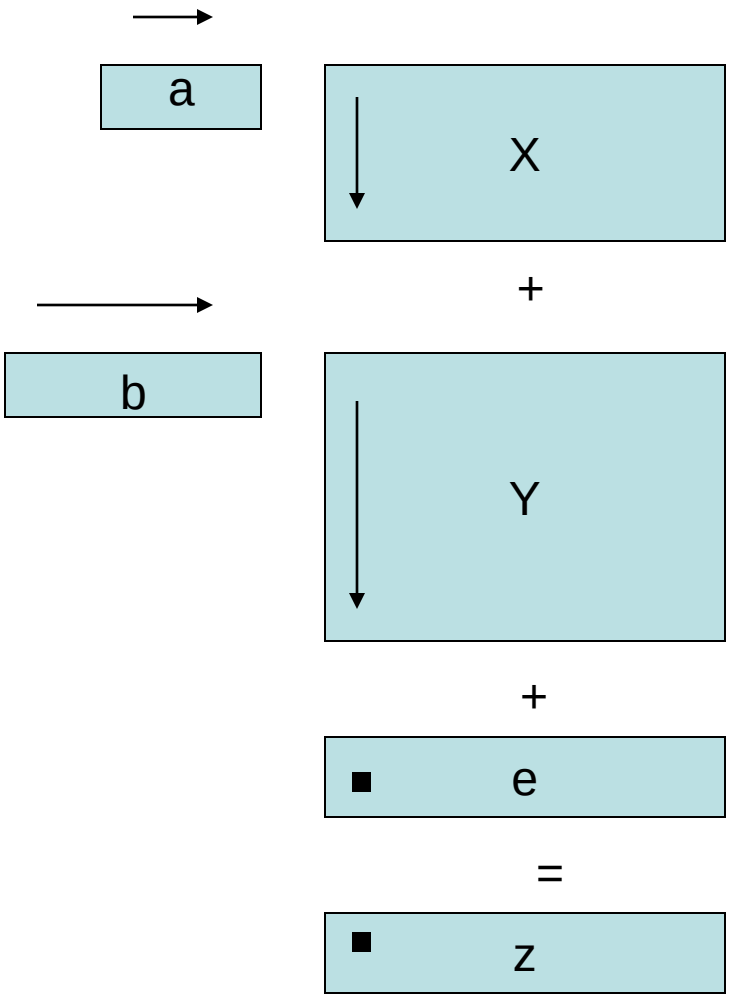
- Theorem 1 provides the background for optimal Bayesian estimation of the noise vector bits.
- Accordingly, the probability of error in estimation (for given sample) of the noise bits is minimized, and so **the probability is maximized that the correct system of equations is constructed.**

Modules for the Cryptanalysis

- Algorithm 1: Measuring the weight of a single block in the error vector of known weight
- Algorithm 2: High-precision measuring of the error vector weight whose expected weight is optimal
- Algorithm 3: The construction of the MIM triplet with low weight of error vector
- Algorithm 4: Recovery of a single block of known weight in the error vector
- Algorithm 5: Recovery of the system with m linear equations $\bar{\mathbf{a}}\mathbf{X} + \bar{\mathbf{b}}\mathbf{Y} = \bar{\mathbf{c}}$
- Algorithm 6: Recovery of the secret keys $\mathbf{X}, \mathbf{Y}$

Advanced Construction & Solving the System of Equations

System of the Equations



$$\mathbf{a\,X + b\,Y + e = z}$$

Part-by-Part Solve & Check

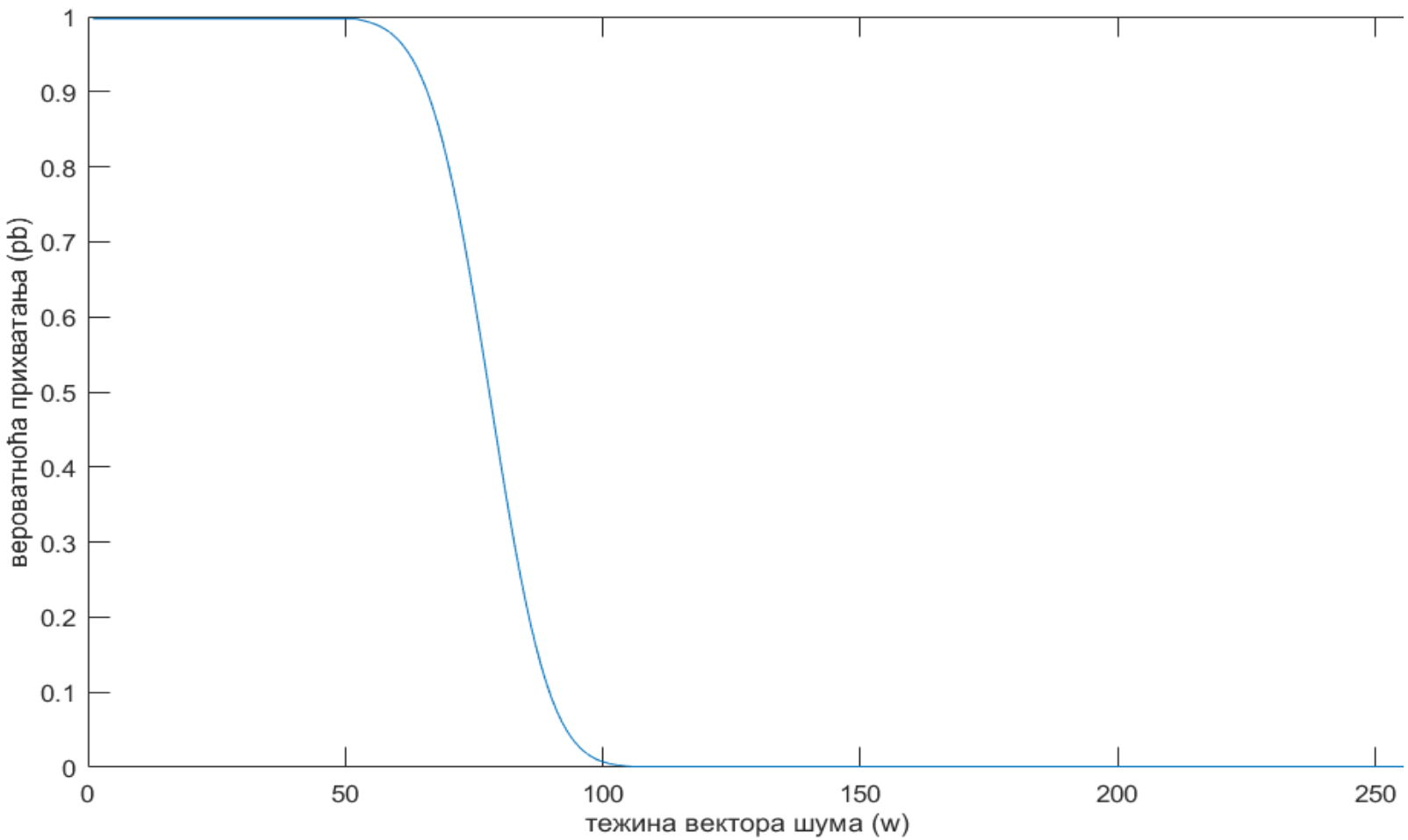
- Entire system of equations could be split into subsystems, and each subsystem could be solved and checked independently.
- Independent solving and checking the solutions provides that higher probability of error in estimation of bits in the vector of noise is tolerated.
- The above provides reduction of the attack complexity.

Part III

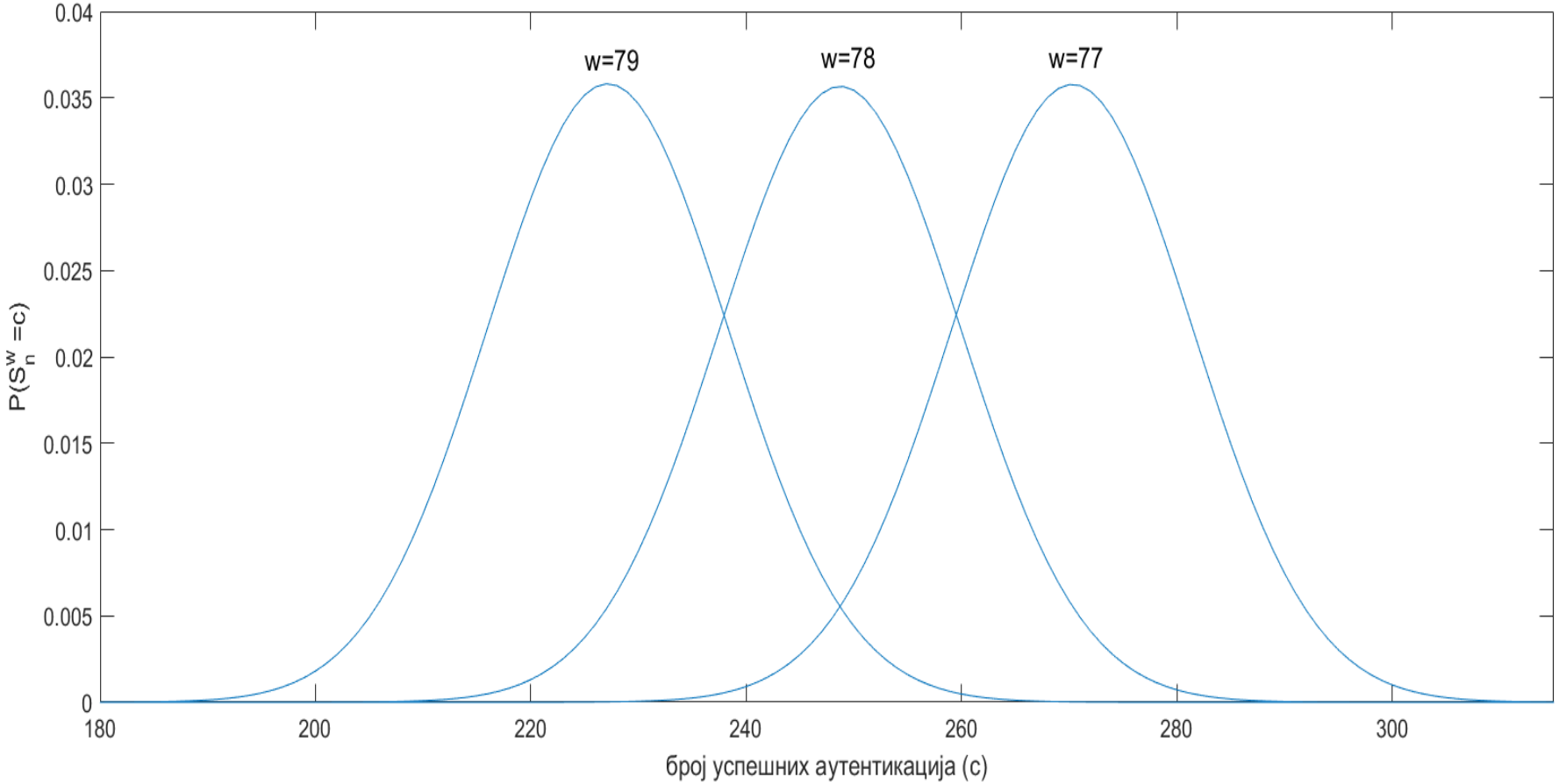
A Number of Numerical Illustrations

Numerical Illustrations on the Noise Bits Recovery

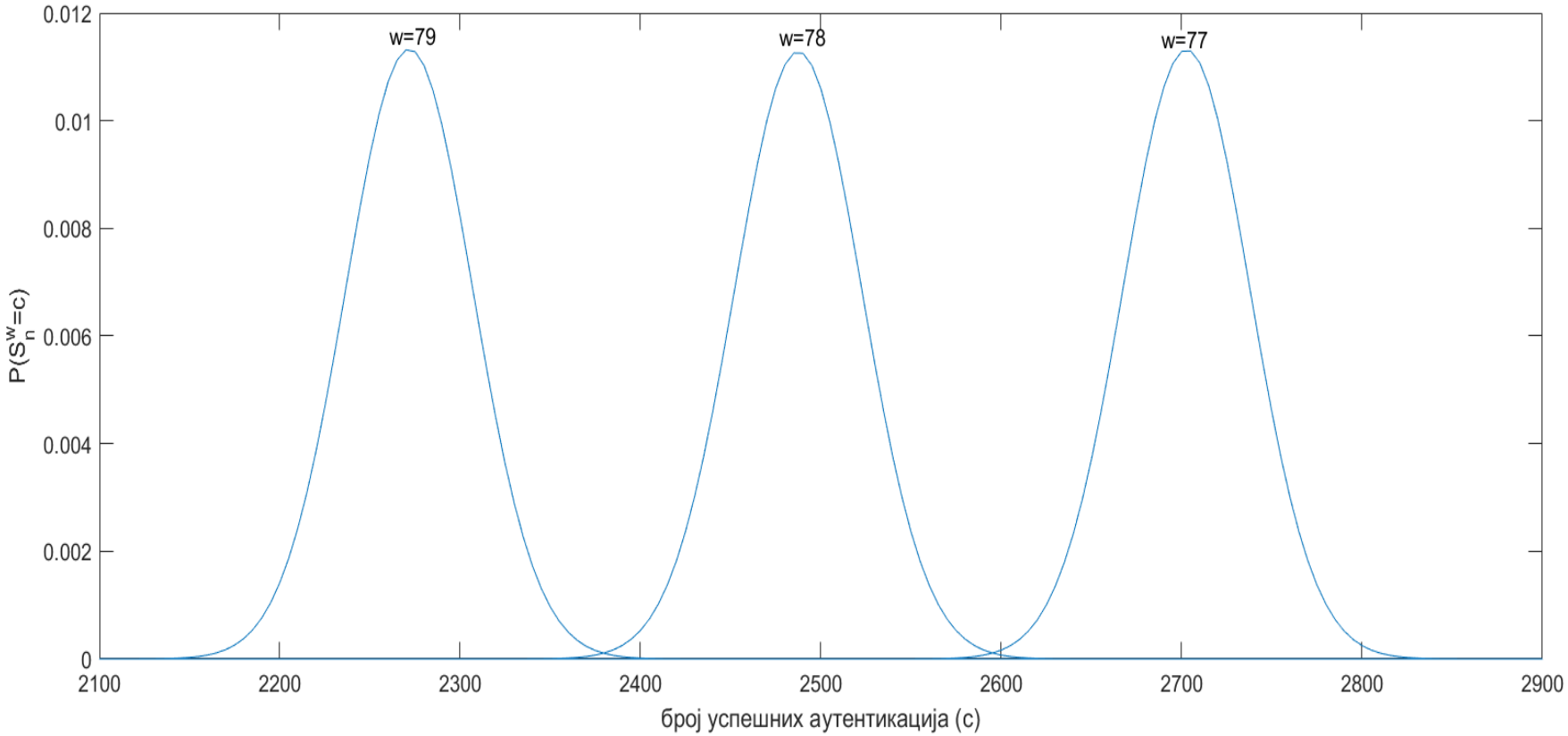
Acceptance rate as a function of the modification noise vector weight when thr = 113, m=441, $\tau = 0.125$



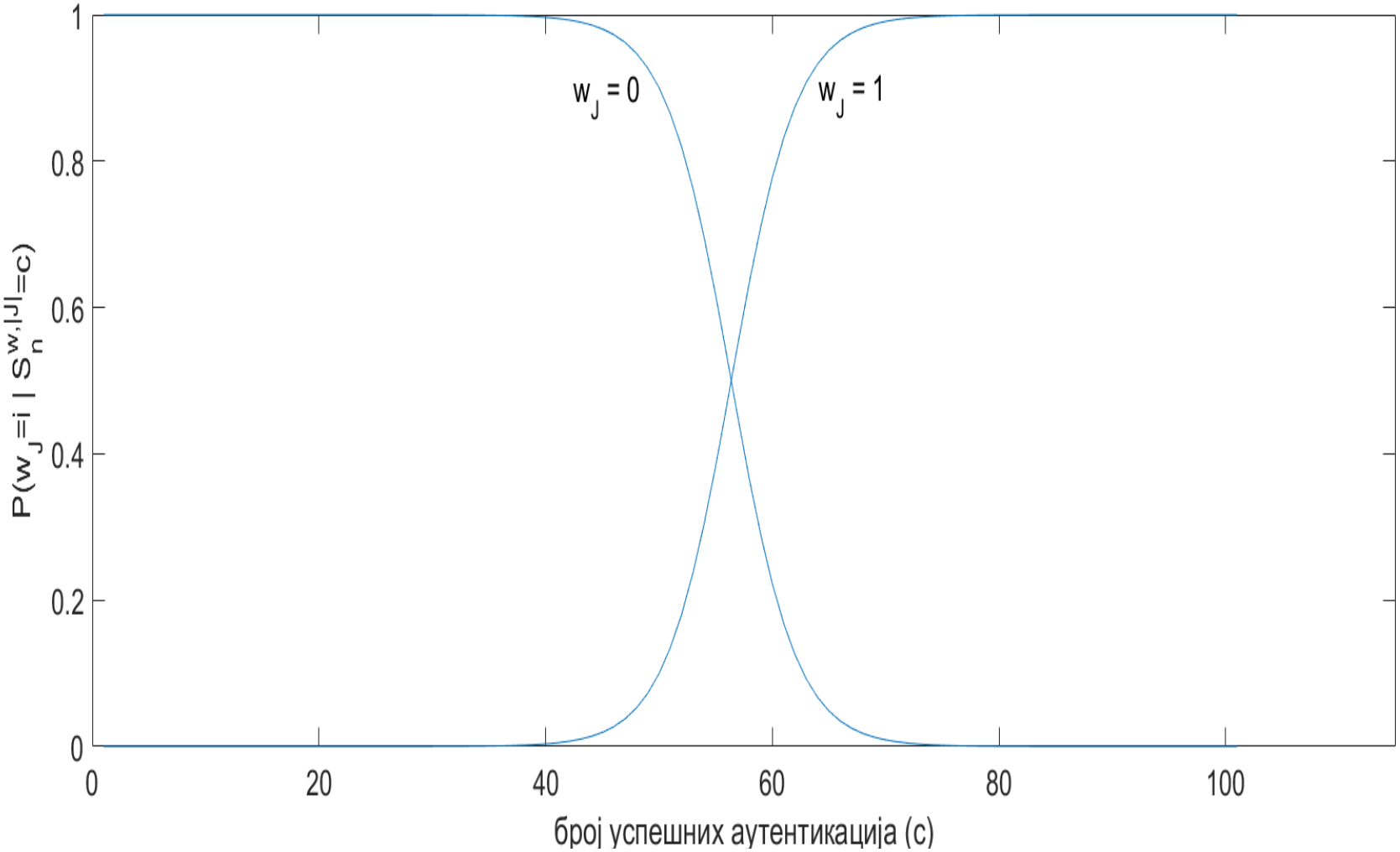
Probability distributions of the acceptance rate for three different weights ***w*** of the noise vector after 500 authentication attempts



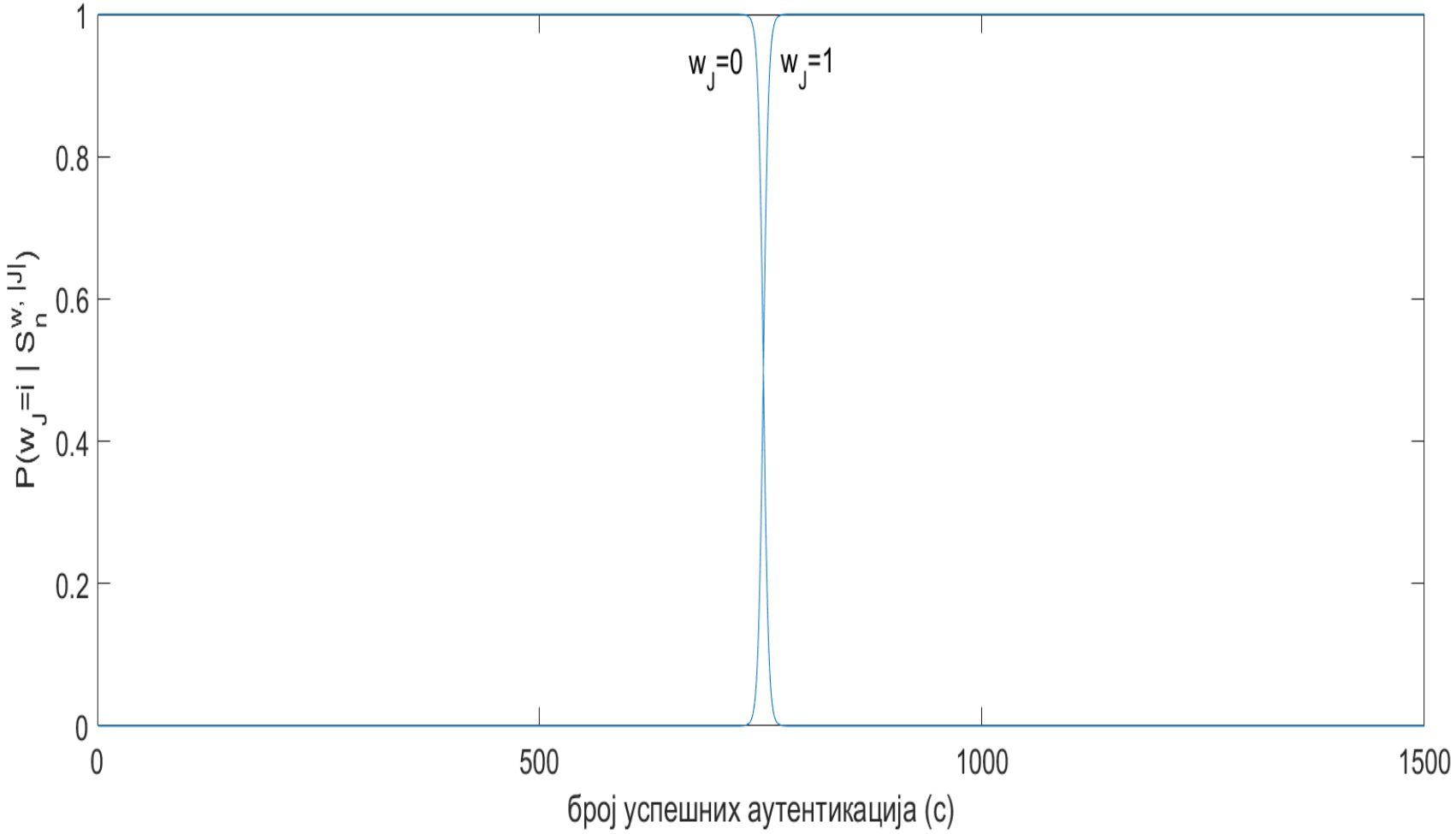
Probability distributions of the acceptance rate for three different weights ***w*** of the noise vector after 5000 authentication attempts



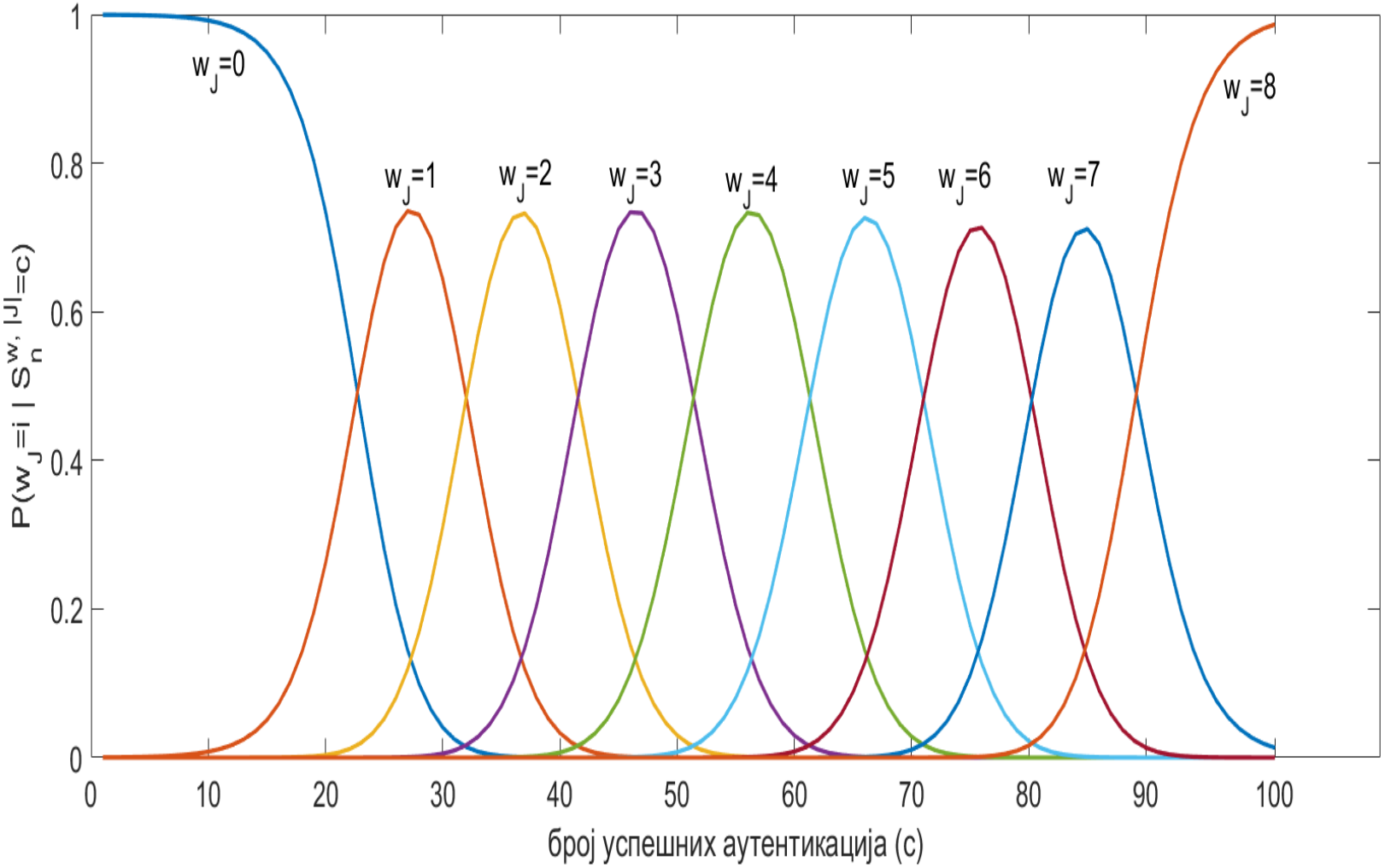
Probability distribution of the Acceptance Score when the flipped bit is “1” and “0”, respectively, when **n=100** modified authentication sessions are considered



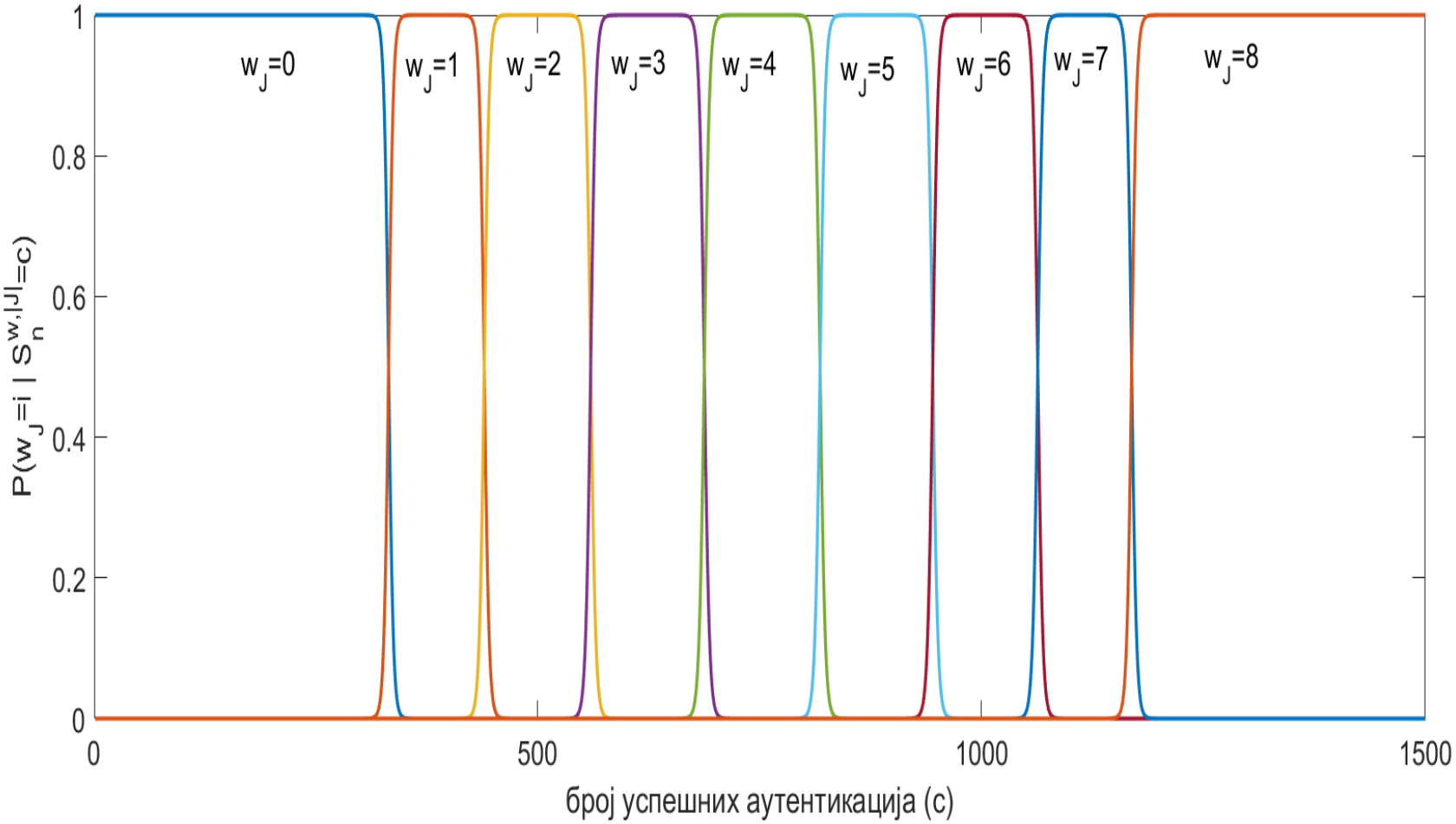
Probability distribution of the Acceptance Score when the flipped bit is “1” and “0”, respectively, when **n=1500** modified authentication sessions are considered



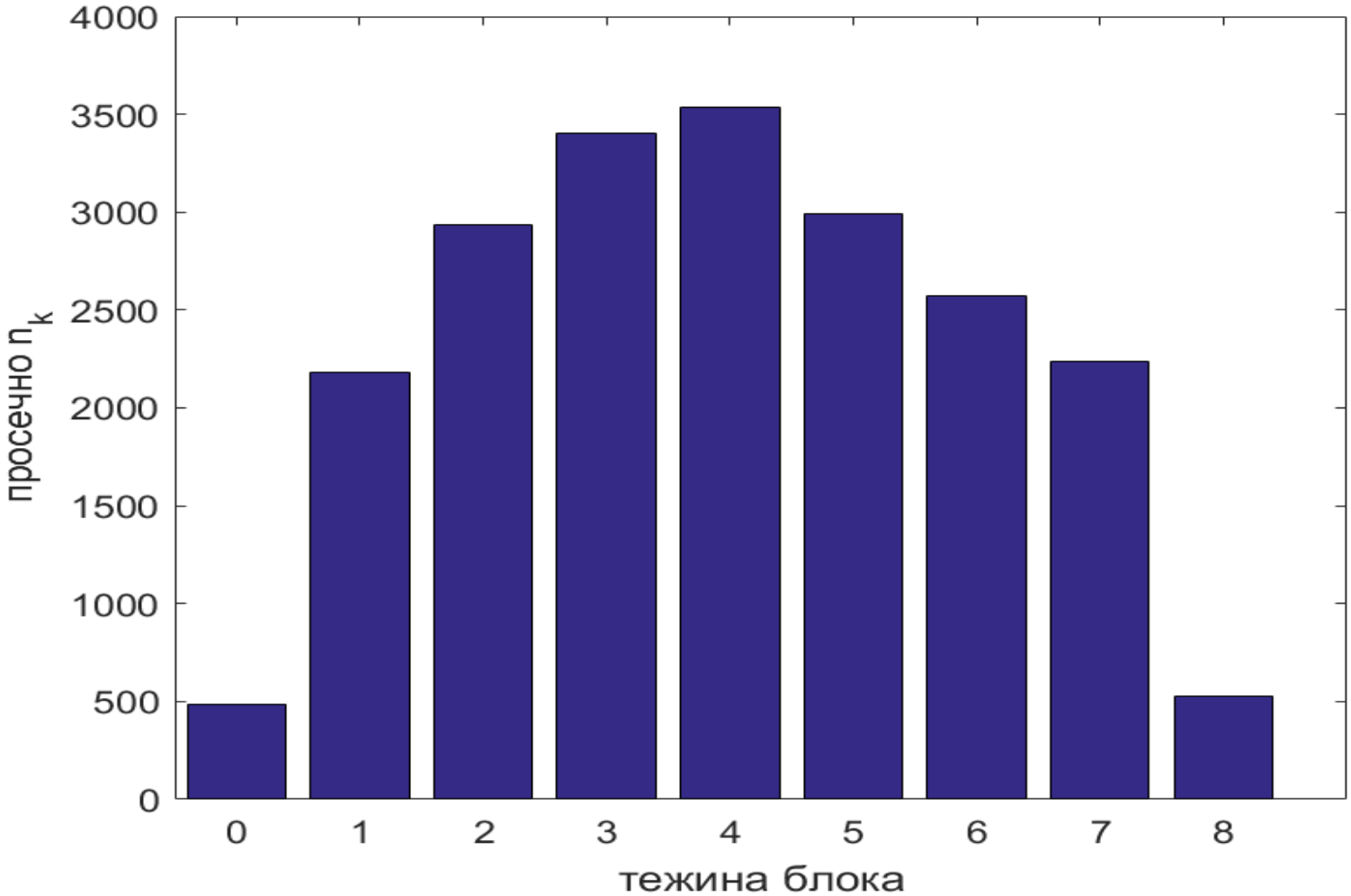
Probability distributions of 8-bit segment weights of the modification noise vector after **n=100** modified authentications



Probability distributions of 8-bit segment weights of the modification noise vector after **n=1500** modified authentications

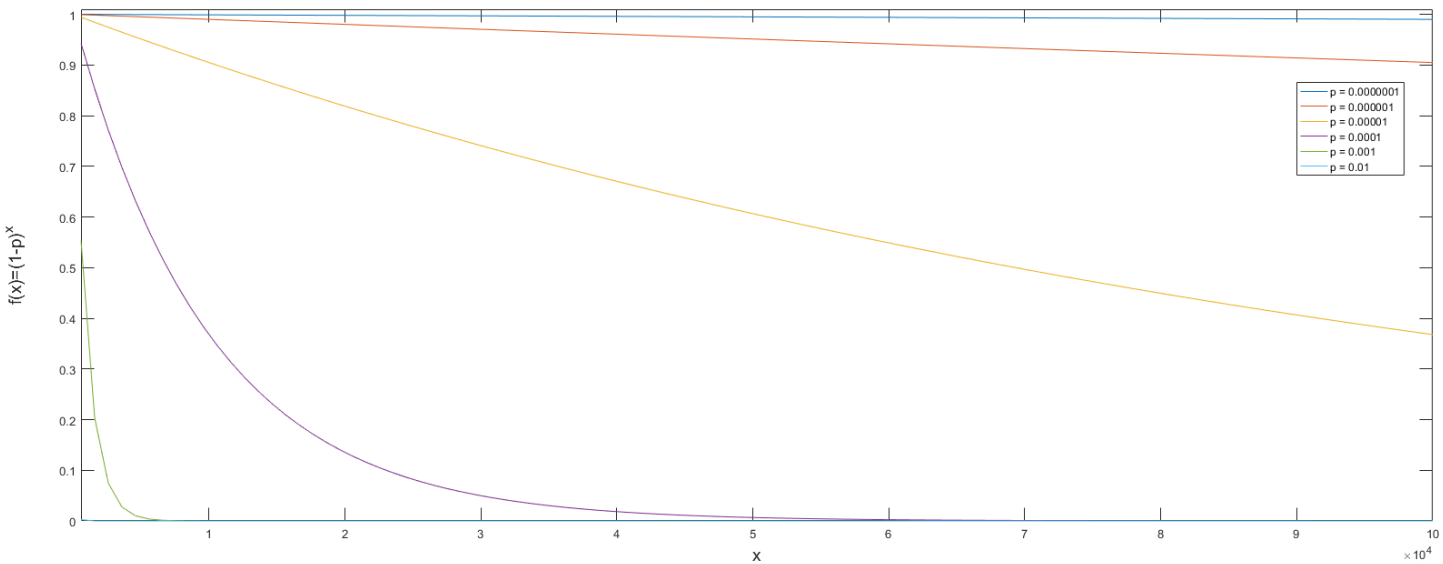


Histogram of required number of modified authentication for correct recovery an 8-bit noise-segment of certain weight

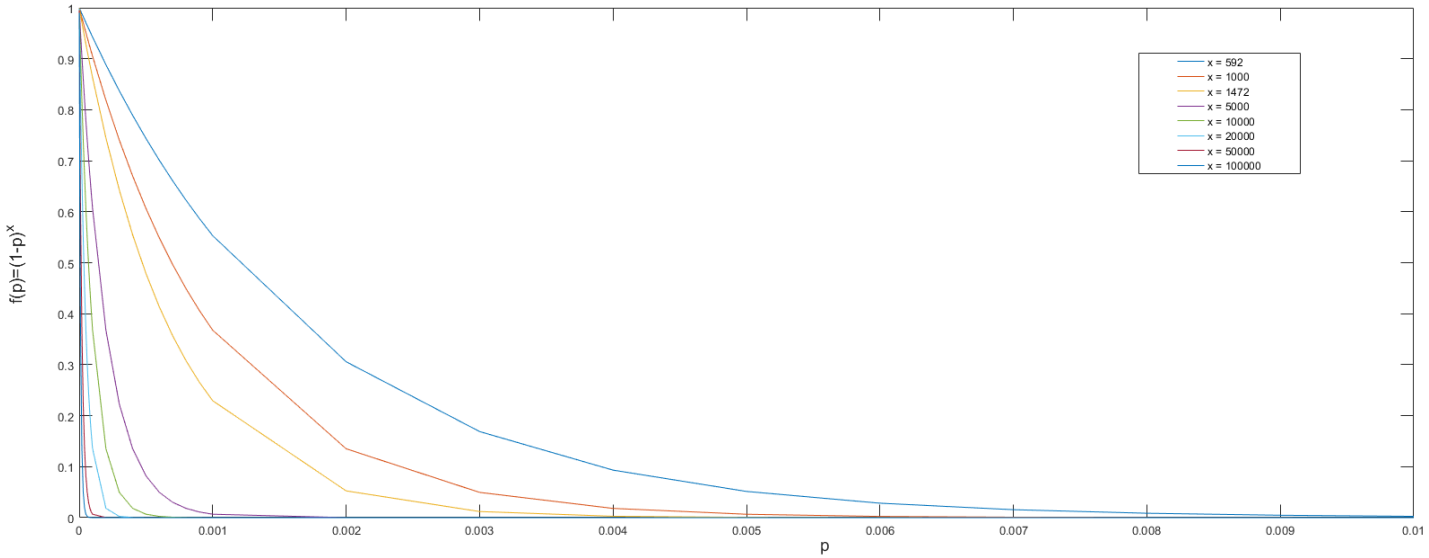


Numerical Illustrations of the Gain Implied by Advanced Solving System of the Equations

The probability of success recovery of x bits of noise when the bit error rate is a parameter



The probability of success recovery of x bits of noise as a function of the bit error rate



Concluding Notes

Main Messages of the Talk

- The **talk points out that advances in up to now known MIM attack** are possible making that the problem of designing lightweight and secure authentication protocols appears as additionally challenging one.
- **An improved MIM attack against HB# authentication protocols has been proposed and its main technical issues have been discussed**.

Thank You Very Much for the Attention,

and

QUESTIONS Please!