23rd International Conference on
IT4P - Information Technology for Practice 2020

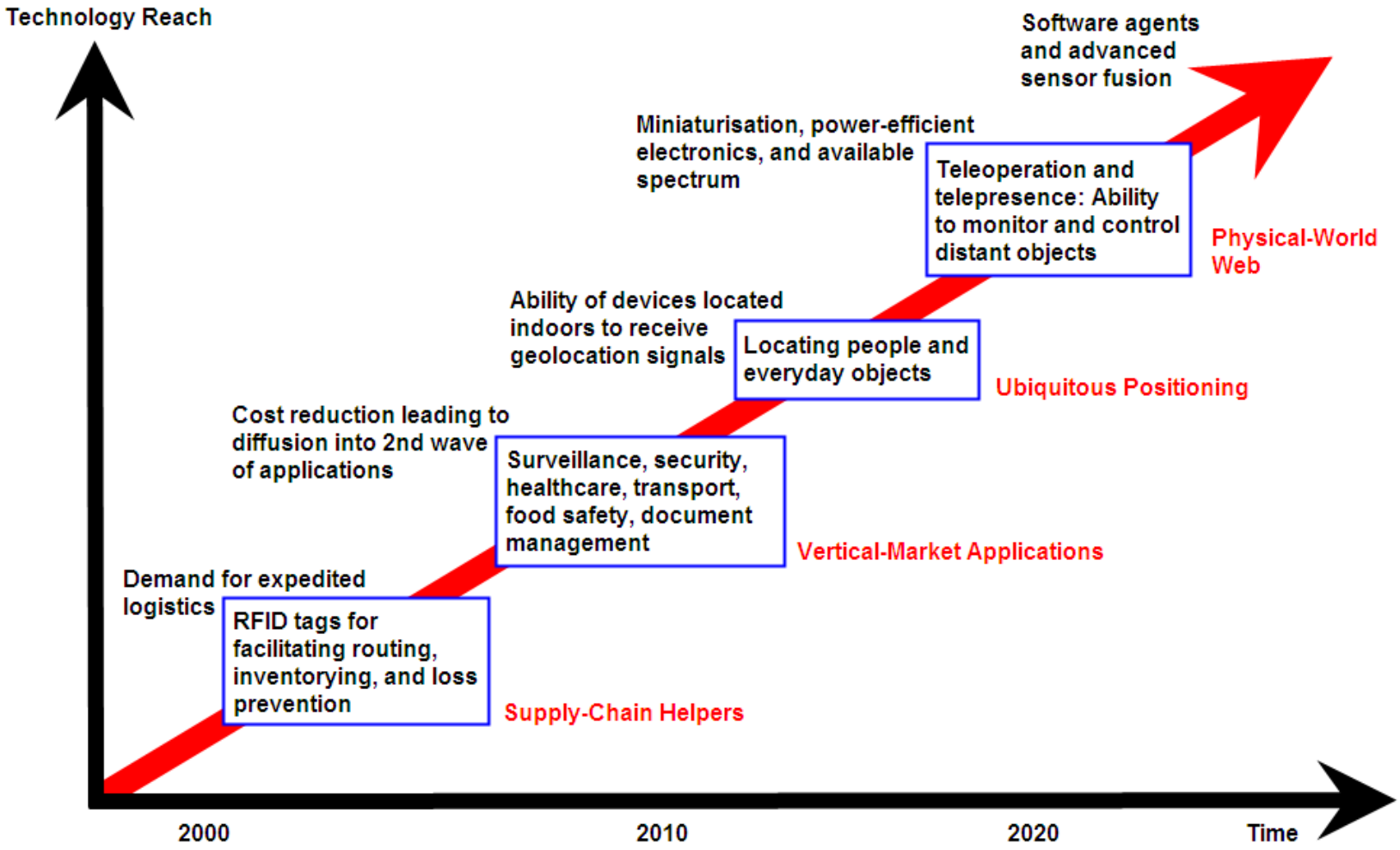
Thematic focus: Information security

Optimization of bit template in authentication problems

Elena Nyemkova [1], Morika Rusynko [2], Dmytro Kostyrko [3]

[1,2] Lviv Polytechnic National University, Ukraine
[3] Ukrainian Academy of Printing, Ukraine

TECHNOLOGY ROADMAP: THE INTERNET OF THINGS

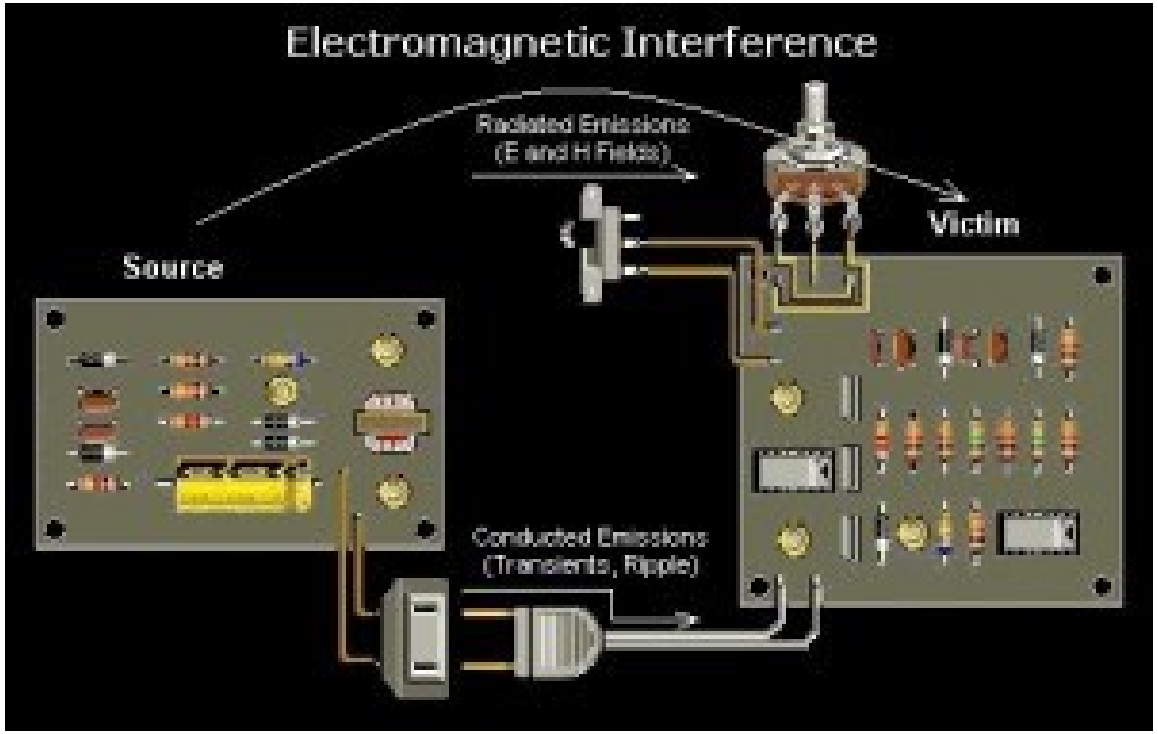


Source: SRI Consulting Business Intelligence

Principles of authentication

Password authentication (What I know)	• MAC-,IP-addresses, Kerberos, RADIUS, Cookie, HTTPS, OpenID, OpenAuth, OAuth, IMSI, IMEI
External authenticator (What I have)	• Tokens, USB-key, RFID, QR-code
Authentication by properties (What I am)	• Physically Unclonable Functions for IoT, Spontaneous electromagnetic radiation from working devices (mobile telephones, notebooks, Wi-Fi)

Electromagnetic interference (noise)



Source:
RADIOING.com

All electronic devices cause some electromagnetic interference (EMI). The EMI should be measured inside the device.

The advantages of this approach:

- ✓ significant reduction in the influence of the electromagnetic background;
- ✓ elimination of a systematic error caused by an external meter;
- ✓ unlimited device mobility to the location of a third-party meter.

Arm of study

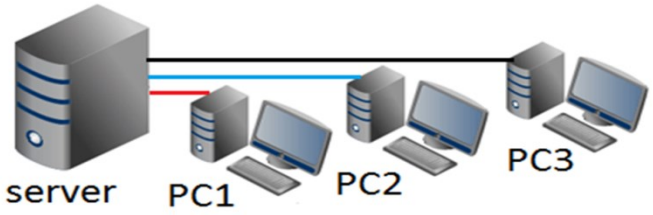
Comprehensive information about the individual characteristics of the device can be obtained by measuring the noise using the built-in ADC. In this case, the influence of the electromagnetic background of the environment is minimized. Therefore, it can be expected that authentication errors will be less when using internal electrical noise.

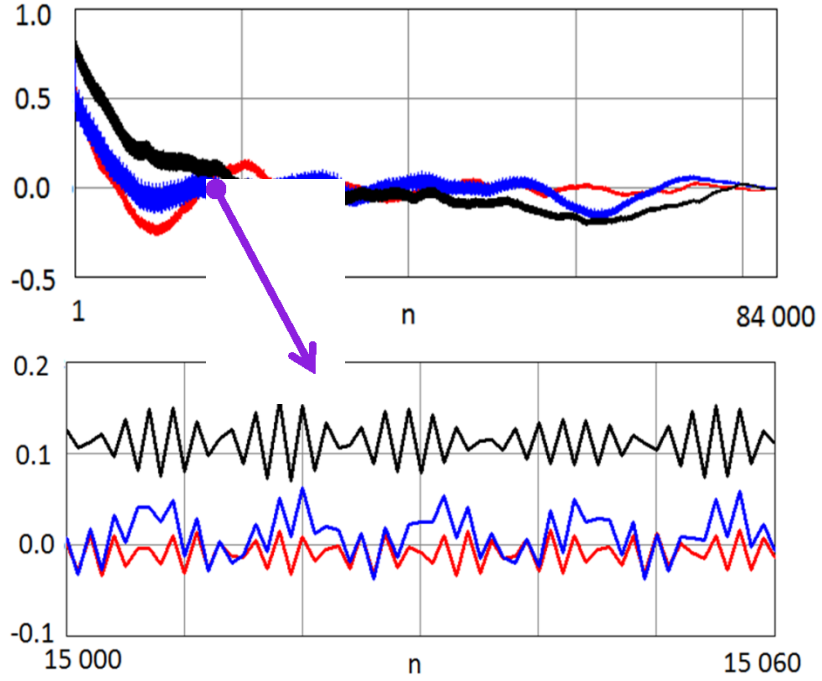
The purpose of this study is to establish the possibility of reducing the length of the bit template noise of an electronic device on the example of personal computers while maintaining inter- and intra-Hamming distances between templates.

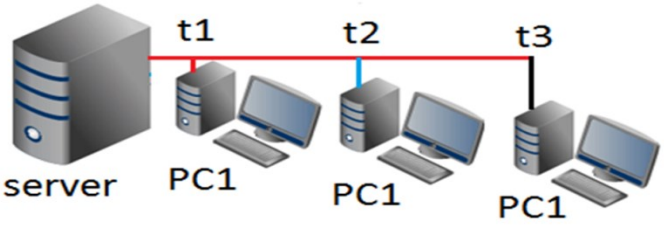
Experiment equipment and settings

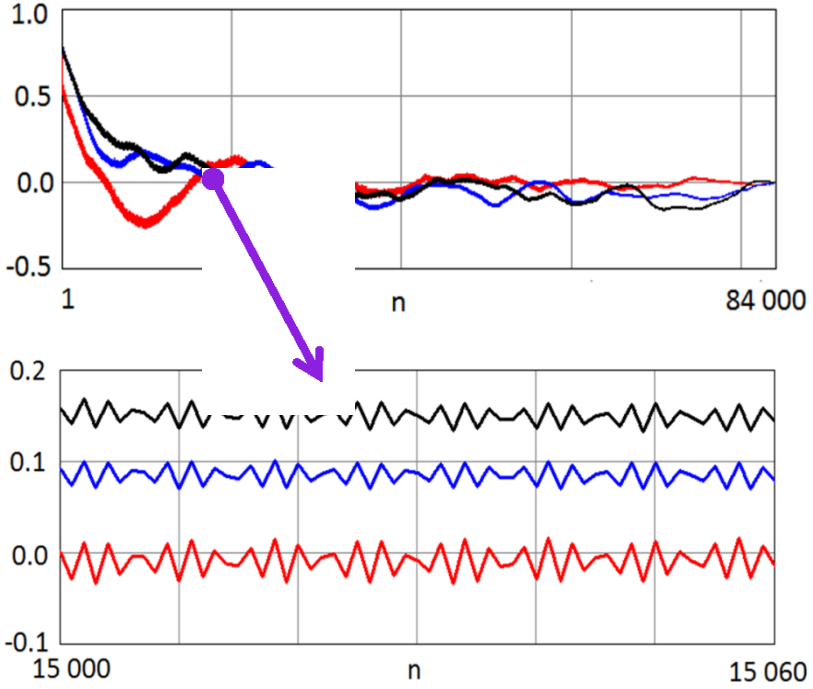
- Personal computers (PC) of one batch (AMD A-series, case STM Soho 112, ATX, Mid Tower) with embedded sound card Realtek (16-bit ADC),
- Windows7,
- program «OscilloMeter» - hardware-software multimeter (recording results from ADC were recorded into the ".wav" file),
- all sound card recorders (such as microphones, line-in), except for the mixer, are turned off using the sound control panel on the computer,
- in the Windows sound scheme customization "No Sounds" is selected.

Internal electrical noise of Personal Computers









Statistical properties of PC noise

Sampling frequency 44.1 kHz

Level of internal electrical noise ≈200 μV

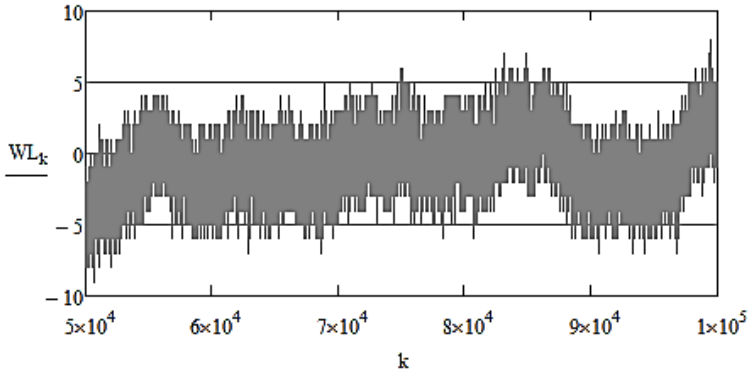
Recording time from 0.5 second

$$mean(x) = \frac{1}{n}\sum_{i=0}^{n-1} x_i$$

$$Var(x) = \frac{1}{n-1}\sum_{i=0}^{n-1} (x_i - mean(x))^2$$

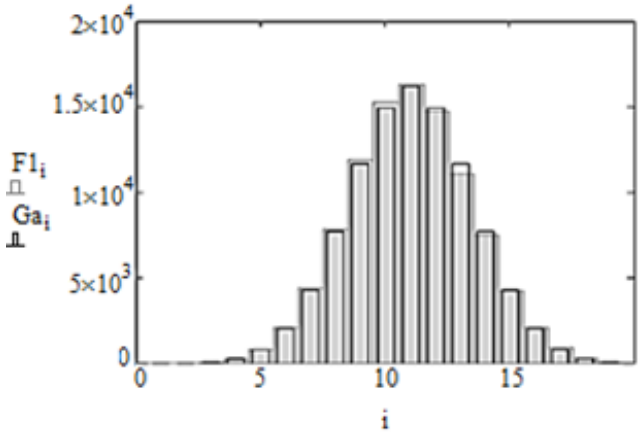
$$Stdev(x) = Var^{0.5}(x)$$

Oscillogram of noise

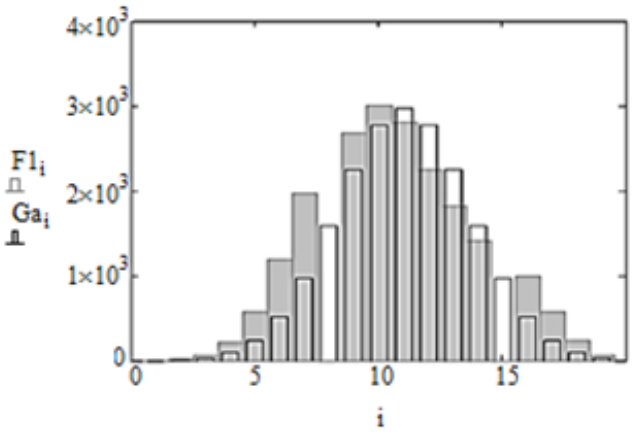


mean(*x*)=0.06,
Var(*x*)=6.039,
Stdev(*x*)=2.457

mean(*x*)=0.18,
Var(*x*)=7.203,
Stdev(*x*)=2.684



a) 100 000 samples

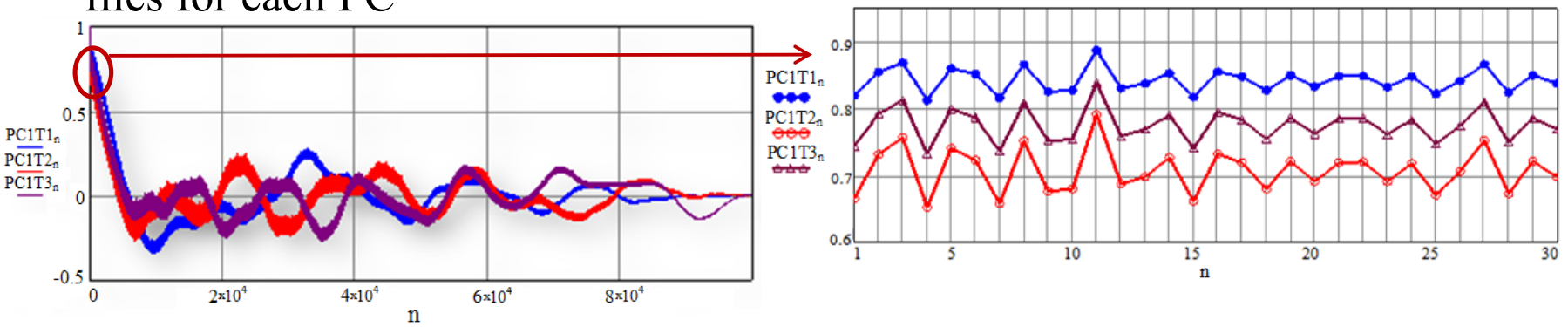


b) 20 000 samples

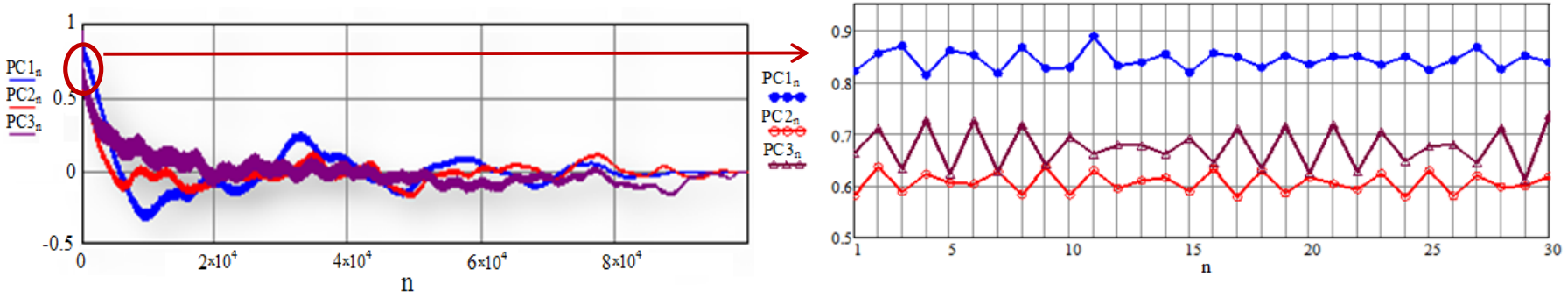
Autocorrelation function

$$a_k(x,x) = \frac{1}{\mathrm{var}(x)(N+1)} \sum_{i=1}^{N} (x_{k+i} - m(x))(x_i - m(x))$$

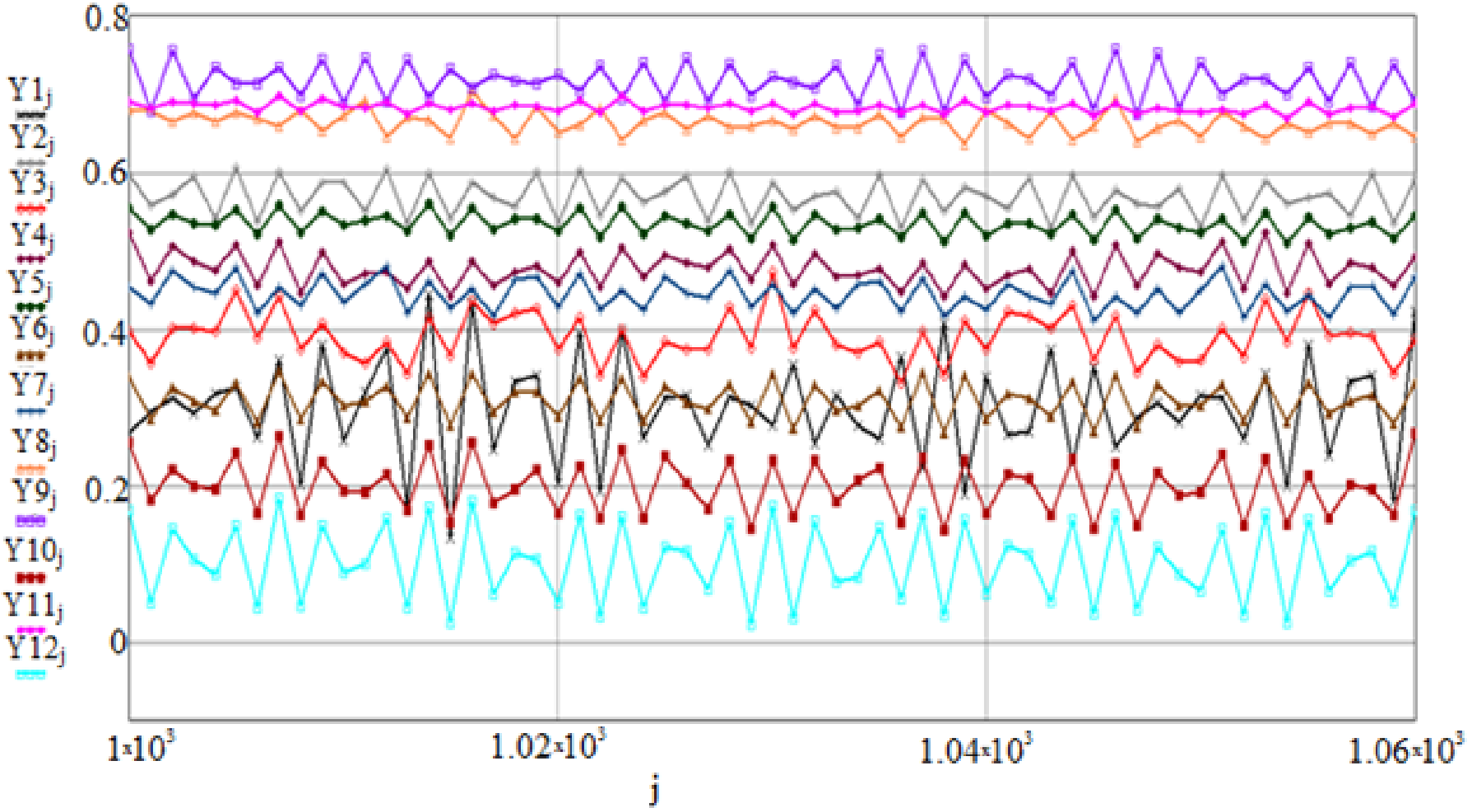
The correlogram's detail form is almost unchangeable for different record files for each PC



The correlogram's detailed form for noise of each PC is uniqueness



Fragments of normalized autocorrelation functions of noises of 12 PC

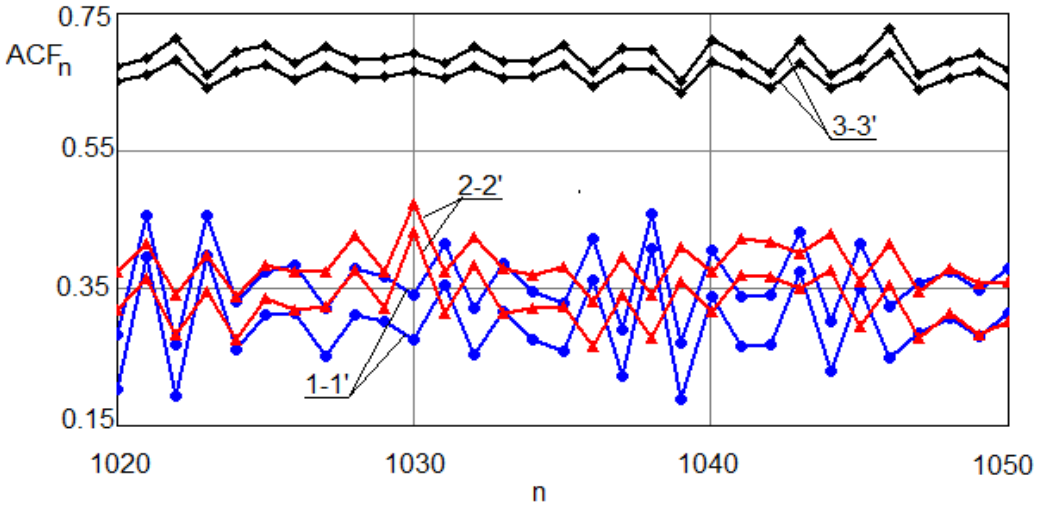


Bit template

Bit template is binary code, that characterizes the increase or decrease of the normalized value ACF $\{a_n\}$ for two consecutive lag values n and n+1. For comparing pair of bit templates the Hamming distance is used.

$$B^I{}_n = \begin{cases} 1, a_{n+1} \geq a_n \\ 0, a_{n+1} < a_n \end{cases}$$

$$H(B^I, B^J) = \sum_{n=1}^{N-1} \left| B^I{}_n - B^J{}_n \right|$$



11010100101001010010010110110

10101101001010010101011010110 1

10101011010101101010010101 01

The length of the bit templates required to reliably identify computers is 1000 bits.

Average accuracy of different types of electronic devices authentication

№	*Method*	*Type of device*	*Probability of correct authentication,%*	*Remarks*
1	Frequency identification by electromagnetic radiation	Notebooks MacBook Pro	94.6	Measurement by external measuring instrument
		LED screens DELL	94.7	
		Mobile telephones iPhone6	71.2	
		Wi-Fi modules with chip NRF24LE1	94.0	
2	Form of correlogram's internal electric noise	Personal stationary computers AMD A-series, case STM Soho 112, ATX, Mid Tower	98.1	Measurement by embedded instrument (these investigations)
3	Trajectory of phase error vector (GSM)	Mobile telephones Nokia 6100, Motorola C118	97.6	Measurement by embedded instrument

Optimization of bit template length

Positions of bit patterns with the identical values

5	65	99	254	288	306	348	390	391
412	418	437	438	439	464	465	484	485
486	511	530	531	532	537	569	578	579
615	616	630	719	756	757	758	759	793
802	803	804	805	806	809	810	840	841
849	850	851	852	855	856	886	887	888
889	893	897	898	899	901	902	903	904
932	933	934	935	940	945	949	950	980
981	982							

7.4% identical values over the length of bit patterns

Intra-Hamming distance matrix for average optimized / no optimized templates

i \ k	1	2	3	4	5	6	7	8	9	10	11	12
1	4 / 5	8 / 9	15	5	5 / 7	7 / 8	14	5 / 6	7	10 / 12	4	4
2	14 / 15	28	9 / 10	13	16 /19	12 / 13	12	15 / 17	13 / 14	19	15 / 16	13 / 14
3	23	29	23	34 / 35	26	36	35 / 37	26	27	28 / 30	28 / 29	36 / 37
4	17	23	15	20	25	16	27	14	10	15	13	17
5	26	21	12	12	21	19	19	16	17	20	16	20
6	12	15	13	19	11	16	16	11	98	16	18	13
7	14 / 15	17 / 19	18 / 19	12	8 / 9	21 / 23	10 / 11	19 / 22	13 / 15	15	93	12 / 15
8	1	3	6	2	1	5	3	10	3	5	8	7
9	10 / 13	7 / 10	16 / 20	11 / 16	8 / 12	15 / 20	17 / 24	16 / 21	423 /424	7 / 10	12 / 19	17 / 25
10	12	13	10	12	7	10	16	15	10	12	15	16
11	24	20	23 / 24	21 / 22	26	12	23 / 24	23	29 / 30	24 / 25	22	23
12	10	13	118 / 119	3	12	10	12	9	11	13	13	6

Inter-Hamming distance matrix for average optimized / no optimized templates

H11 =

	1	2	3	4	5	6	7	8	9	10	11	12
1	0	470	449	440	439	437	444	516	550	440	445	441
2	470	0	327	330	325	325	358	506	480	330	333	325
3	449	327	0	89	106	104	119	505	429	79	94	102
4	440	330	89	0	39	37	88	508	432	48	63	41
5	439	325	106	39	0	6	87	507	429	41	52	12
6	437	325	104	37	6	0	87	507	431	37	50	12
7	444	358	119	88	87	87	0	512	444	94	91	87
8	516	506	505	508	507	507	512	0	494	514	505	503
9	550	480	429	432	429	431	444	494	0	426	437	431
10	440	330	79	48	41	37	94	514	426	0	65	41
11	445	333	94	63	52	50	91	505	437	65	0	52
12	441	325	102	41	12	12	87	503	431	41	52	0

Conclusions

1. The internal noise approach provides an increase in the probability of correct authentication up to 98.1% compared to 94.6% for known analogs.
2. The using this approach will significantly complicate the execution of attacks by forging, intercepting and reusing authentication data.
3. The length of the bit templates of the noise of personal computers can be reduced by 74 bits with an initial pattern length of 1000 bits, which is 7.4% of the initial length of the templates.
4. The proposed reduction in length does not affect the intra- and inter-Hamming distance between bit templates.
5. Further development of the research is in applying the method to a wider range of devices, namely to intelligent sensors and devices of the Internet of Things, most of which have imbedded ADCs and microprocessors.

Our contacts

National University Lviv Polytechnic
Department of Information technology security
olena.a.niemkova@lpnu.ua

Thank you for your attention!