Abstract

This document describes how to use the el-author.cls file and how to format your LaTeXsubmissions correctly for *Electronics Letters*. It also serves as a template, so that you can simply copy the text from this example .tex file and replace it with your own. We have tried to cover the basic tools and commands you might need, but there may be some more unusual fields, etc, not described. Do not hesitate to contact us if you encounter any problems. The structure is as follows: we introduce the basic notations and preamble, and then provide some example text, followed by the references. For simplicity we have left the source code out of this document and refer the reader to the sample.tex file itself, from which to copy and paste.

Onderzoek naar de cyberaanval op *Oekraine* en de impact voor security van SCADA systemen

G. Bartes

12th April 2023

0.1 Introduction

this model, depicted in Fig. 1 and described in Section 2, has been used successfully in the development of safety-critical systems in industry and helps to clarify the behaviors of, and the boundaries between, the environment, sensors, actuators, and software. To be implementable, the system requirements must be feasible with respect to the environment (i.e., should specify only behaviors that obey the environmental constraints) and acceptable software behaviors must be possible given the chosen input/output devices. sciencedirect.com/science/article/pii/S0167642315001033fg0010 https://shemesh.larc.nasa.gov/fm/pa

`el-author.cls` is used in a similar fashion to the standard `article.cls` file. However, the `el-author.cls` file must be copied into the same directory as the .tex file you wish to compile for submission. Most of the preamble needed for including packages for mathematics or for displaying images is included within the `.cls` file itself, whereas more exotic packages will have to be included manually.

If you prefer to review your document in single column format or double spaced you can include this in the options of the document class with the command - inside the square brackets - `[doublespace, onecolumn]`.

Tables are straightforward to include (check the `.tex` file for details), and will format automatically:

Coefficients and remainders for distribution KK ($k = 0.05$, $v = 3$, $c_1 = 1.5$, $c_2 = 4.5$)

n	a_n^2	$r_k(1)$
0	3.602576748428	1.493719547999
1	1.384791111989	0.108928436101
2	0.108600438794	0.000327997399
3	0.000275794597	0.000052202814
4	0.000027616892	0.000024585922
5	0.000018178621	0.000006407300

Note that we used `[h]` after the `\begin{table}` command to force the table to be included exactly at that location. The same can be done for all tables and figures:

[width=60mm]imagefile1a

Figure 1: The Keldysh contour before extension of the real axis to infinity

In the next section we provide a short example manuscript, which includes images and their captions. In `sample.tex` we have added some com-

ments explaining how to use `\source{...}` to include subcaptions, and how to format equations over more than one line. For more information on submitting and *Electronics Letters* house style, see the author guide at http://www.theiet.org/resources/journals/eletters/authors.cfm.

0.2 Situatie

Starting at 3:30 p.m. on December 23, 2015, the Kyiv, Prykarpattia, and Chernivtsi electric control center HMIs began opening and closing circuit breakers without input from operators. The resulting unauthorized operations resulted in the loss of power to approximately 225,000 customers across Ukraine [1] [2]. Operators at the three operations centers were unable to regain remote control of more than 50 substations affected by the incident. After six hours and the loss of over 130 MW of load, operators restored power by sending technicians to the substations and manually controlling the power system [3] [4] [5]. Complicating the situation and reducing operator communications, the malicious actors also launched a telephony-based denial of service attack, using automated systems to overload the phone systems of the utilities. Post-power outage analysis found that firmware was corrupted on serial-to-Ethernet converters at substations, uninterruptible power supplies (UPS) for both the server room and the telephony system were remotely turned off, and the hard drives of numerous computers were corrupted. This event was the first successful cyber-induced power outage that disrupted an electric power grid. To mitigate future attempts at disruption of electrical power by cyber means, it is critical that other electric power organizations learn from the Ukraine incident. source: https://na.eventscloud.com/file$_u ploads/aed4bc20e84d2839b83c18bcba7e2876_O wens1.pdf https$: $//www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf https$: $//theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802 Deaanvalisslimopgezethttps$: $//www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/Cyberaanvalleninhetalgemeenhtt$ $//www.ifri.org/sites/default/files/atoms/files/desarnaud_c yber_a ttacks_e nergy_i nfrastructures_2$ $//jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/Attacking IEC-60870-5-104 SCADA Systemshttps$: $//www.researchgate.net/publication/333671061_A ttacking_I EC-60870-5-104_S CADA_S ystems$

In the typical quantum dot set-up, as described in the introduction, the dot weakly connects together two electron seas, the leads. It is understood

that the phenomenon of the Coulomb blockade limits conductance through the dot unless the charge induced on the dot by the gate is $\mathrm{Q}=\left(N+\frac{1}{2}\right)e$ Consequently, we find sharp peaks in the conductance of the dot at these degeneracy points. However, for $T < T_K$ new behaviour is observed, as in Fig. 2. The original conduction peaks of figure of the classic Coulomb blockade exist when the occupancy is effectively half integer. Hence, we expect at integer occupancy *suppression* of the conductance. This is indeed observed if N is even. However, for $T < T_K$ and N odd, we see that the conductance is not *fully* suppressed. The difference is clear: for even occupancy, the spin of the dot will be zero, as there will be as many up as down electrons. However, for odd filling, the $N+1$th electron will contribute a spin-half, causing the dot to behave as a Kondo-like impurity. We will discuss what consequences the Kondo-nature of the dot has, but first we will explain exactly *how* it acquires this nature.

0.3 Oorzaken

1. An initial email spear phishing attack lures recipients into opening an attached Microsoft® document with a macro that installs Black Energy 3 (BE3) onto corporate workstations. 2. BE3 and other tools perform reconnaissance and enumeration of the network and provide an initial backdoor for the hackers into the corporate network. 3. As a result of network reconnaissance, the malicious actors discover and access the oblenergos' Microsoft Active Directory® servers that contain corporate user accounts and credentials. 4. With the harvested credentials, the malicious actors use an encrypted tunnel from an external network to get inside the oblenergo network, establishing a presence on the oblenergo control system networks. 5. Malicious actors discover and access the control center supervisory control and data acquisition (SCADA) human-machine interface (HMI) servers and substations. While a router separates corporate and SCADA networks, the firewall rules are improperly configured. 6. On December 23, 2015, at 3:30 p.m., the malicious actors begin their power outage attacks by entering operations and SCADA networks through backdoors on the compromised SCADA workstations. The malicious actors take control away from HMI operators and then open breakers. 7. The malicious actors perform several other actions with the intent of complicating the responses of control operators and increasing the effort required to return the system to normal operating conditions. These actions include: a. Launching a coordinated Telephony Denial of Service (TDoS) attack that floods call centers to prevent

legitimate calls from getting through. b. Disabling the UPSs for the control centers. c. Corrupting the firmware on a remote terminal unit (RTU) HMI module and serial-to-Ethernet port servers. 8. Malicious actors execute KillDisk malware in an attempt to wipe out the control center HMIs and pivotpoint workstations. http://web.mit.edu/smadnick/www/wp/2016-22.pdf

0.4 4 variabelen model

0.4.1 Monitored ie. sensors

0.4.2 Controlled ie. actuators

0.4.3 Input

intrusion usingb phishing mail blz 4 install malware on the system blz 5 create a communication channel to the adversary's command and control. reconnaissance by collecting credentials and moving through the network to eventually pivot into the network segments where Supervisory Control and Data Acquisition (SCADA) dispatch workstations and servers existed. reconfiguredthe uninterruptible power supply (UPS) coded malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations to prevent rebooting to support recovery blz 9 take out the converters so that it would prevent operators from sending remote commands to re-close breakers once the shutdown happened tap into the SCADA networks through the hijacked VPNs and send commands to deactivate the UPS system they had already reconfigured. I an internal telephone communications server was targeted effectively cutting off all internal communications with regional offices and distribution substations actor used the local UPS to schedule a power shutdown of the main datacenter to occur a few hours later. In addition to standard consequences of power loss, a reboot caused the full impact of the KillDisk efforts to take effect. The hackers had flooded customer call centers with thousands of fake calls, to prevent legitimate callers from being able to report the outage. Once they neared the end of their assault, the hackers used KillDisk to wipe the files off the operator station's causing them to be inoperable. KillDisk is a piece of malware that wipes or overwrites data in essential system files that causes a computer to crash. The infected computers are unable to reboot because KillDisk also overwrites the master boot record blz 9 source http://web.mit.edu/smadnick/www/wp/2016-22.pdf

[width=60mm]imagefile2a

Figure 2: Quantum dot resistance for $T \ll T_K$ and $T \gg T_K$ For high temperatures (dashed line) the Coulomb blockade remains For lower temperatures (solid line) the Coulomb blockade is overcome

0.4.4 Output

To set up the non-equilibrium Kondo problem - formally - we introduce the two-channel Anderson Hamiltonian $\mathrm{H}_{2C} = \sum_{\alpha k\sigma} \epsilon_{\alpha k} \hat{c}^\dagger_{\alpha k\sigma} \hat{c}_{\alpha k\sigma} + U \hat{d}^\dagger_\uparrow \hat{d}_\uparrow \hat{d}^\dagger_\downarrow \hat{d}_\downarrow$ $+ \sum_\sigma \epsilon_d \hat{d}^\dagger_\sigma \hat{d}_\sigma + \sum_{\alpha k\sigma} [t_\alpha \hat{c}^\dagger_{\alpha k\sigma} \hat{d}_\sigma + h.c.]$ The subscript α is the channel label, for the dot case left and right. The physical idea is that the dot is already at half-integer occupancy. The Hubbard U is recognized as the charging energy (the energy required to add another electron) which we assume to be much larger than the mean level spacing in the dot, so that we may consider only one level, ϵ_d. The hybridization, t_α is the tunneling energy through the potential barriers connecting the dot to the leads, and is assumed to be point like. It is clear that the dot behaves exactly as the original Anderson impurity model, with the addition of lead indices, and this Hamiltonian has been studied *perturbatively*. However, the Schrieffer-Wolff transformation can be performed exactly as before: $\mathrm{H}_{2K} = \sum_{\alpha k\sigma} \epsilon_{\alpha k} \hat{c}^\dagger_{\alpha k\sigma} \hat{c}_{\alpha k\sigma} + \sum_{\alpha\beta\sigma\tau} \underbrace{\frac{t^*_\alpha t_\beta}{U}}_{J_{\alpha\beta}} \hat{c}^\dagger_{\alpha\sigma}(r = 0) \sigma^a_{\sigma\tau} \hat{c}_{\beta\tau}(r = 0) S^a$ In the following we will assume that the coupling to the left and right leads is identical, $J_{\alpha\beta}$, we may perform the sum over leads, giving $\mathrm{H}_{2K} = \sum_{\alpha k\sigma} \epsilon_{\alpha k} \hat{c}^\dagger_{\alpha k\sigma} \hat{c}_{\alpha k\sigma} + J\{[\hat{c}^\dagger_{L\sigma}(r = 0) + \hat{c}^\dagger_{R\sigma}(r = 0)]$
$\times \sigma^a_{\sigma\tau} [\hat{c}_{L\tau}(r = 0) + \hat{c}_{R\tau}(r = 0)]\} S^a$

0.5 Veiligheidsissues

0.6 Maatregelen

III. CREATING A ROBUST CONTROL SYSTEM ARCHITECTURE To create a robust control system architecture with a solid defense, an organization should consider three concepts. • Identify risk and develop a plan for managing that risk. • Implement effective controls to manage the risk. • Create a defense-in-depth model that allows effective and efficient security controls.

Risk assessment has the following objectives: • Identify assets and their

value • Identify vulnerabilities and threats • Calculate threat probability and business impact • Balance threat impact with security control cost

ls. Asset value includes: • Value of replacement • Cost to maintain • Damage in cost if lost • Penalties or fines if lost

Oplossingen 1) Isolate Control Systems 2) Baseline, Log, and Continuously Monitor Control Systems 3) Patch, Update, and Maintain 4) Have Contingency Plans 5) After Action Reports and Lessons Learned 6) Ensure Physical Security 7) Ensure Complex Passwords source: https://na.eventscloud.com/file$_u$*ploads/ae*

Detection of the BlackEnergy malware should be conducted using the latest published YARA signature https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

requiremnts en de rol van de politiek/statelijke actoren https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108 https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN

There may be no better place to witness cyber conflict in action than Ukraine today. Open warfare with Russia, a highly skilled, computer-literate pool of talent and a uniquely vulnerable political, economic and IT environment have made the country the perfect sandbox for those looking to test new cyberweapons, tactics and tools.

Even as Russian tanks crossed the physical border into eastern Ukraine in the spring of 2014, Russian-affiliated hackers were sending malicious code onto Ukraine's IT systems, providing political chaos as a smokescreen.

The goal, say experts, is to test the West's defenses. The U.S. and other intelligence agencies have responded by moving into the Ukrainian networks to pick up the signals.

https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ First Malware Designed Solely for Electric Grids Caused 2016 Ukraine Outage

https://www.darkreading.com/threat-intelligence/first-malware-designed-solely-for-electric-grids-caused-2016-ukraine-outage

Systeem https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0513EED48102FDAD1BD9

If we assume that the kinetic term takes the same form for the left lead as the right lead (in equilibrium), a simple (Bogoliubov) rotation of basis will transform H_{2K} into the standard one channel Kondo model: $\hat{H}^1_{2K} = \sum_k \varepsilon_k \hat{c}^\dagger_{\alpha k\sigma} \hat{c}_{\alpha k\sigma} + J \sum_\alpha \hat{s}(0) \cdot \hat{S}$ such that the new Hamiltonian is diagonal in the lead index, and so α behaves as an additional degeneracy. This procedure is justified if we wish to *perturbatively* analyze the conductance of the dot. For bias voltages, V much lower than the Kondo temperature, this seems

reasonable, as the only true energy scale for the Kondo model is T_K.

Given that $\hat{H}^1_{2K}$ is diagonal in lead index, the same techniques as are used for the equilibrium case apply. Indeed, performing the poor man's scaling procedure and using Fermi's golden rule, it is straightforward to recover the result, for $T \gg T_K$: $\mathrm{G}_1 \sim G_0 \nu_0 J$
$G_0 \sim \ln^2(T/T_k)$ A full and more careful treatment, recovers the numerical factors: $\mathrm{G}_1 = \frac{2e^2}{h} \frac{4\Gamma_L\Gamma_R}{(\Gamma_L+\Gamma_R)^2} \frac{3\pi^2/16}{\ln^2(T/T_k)}$
$\equiv G_0 \frac{3\pi^2/16}{\ln^2(T/T_k)}$ We emphasize that this is valid *only* for $T \gg T_K \gg V$.

At temperatures below T_K, the coupling diverges, so that the dominant term in equation (0.6) is $\hat{H}_{coup} = J \sum_\alpha \hat{s}(0) \cdot \hat{S}$ As was discussed for the one channel problem, the ground state is a singlet, with zero spin, and we expect the scattering in the dot to be suppressed, and so to leading order, the the conductance reduces to $G_2 = G_0$. Perturbative corrections have been found, [3], which yield $\mathrm{G}_2 = G_0 \left[1 - \left(\frac{\pi T}{T_K}\right)^2\right]$ Thus, we can define two regions for the conductance, both for $V \ll T_K$:

$$\begin{array}{ll} G_1 = G_0 \frac{3\pi^2/16}{\ln^2(T/T_k)}, & T \gg T_K \\ G_2 = G_0, & T \ll T_K \end{array}$$

So, we see that as we lower the temperature below T_K, for an odd-integer Coulomb blockade valley, the conductance is no longer exponentially suppressed.

As we have stressed, these results are valid *only* for $V \ll T_K$. The next step is to introduce an arbitrary voltage via the kinetic term in equation (0.6): $\hat{H}^1_{2K} = \sum_{k\sigma}(\varepsilon_k - eV)\hat{c}^\dagger_{Lk\sigma}\hat{c}_{Lk\sigma} + \sum_{k\sigma}\varepsilon_k \hat{c}^\dagger_{Rk\sigma}\hat{c}_{Rk\sigma} + J\sum_\alpha \hat{s}(0)\cdot\hat{S}$ If we assume that $V \gg T$, we can again divide into two regions: $\tilde{G} = \begin{cases} \tilde{G}_1, & V \gg T_K \\ \tilde{G}_2, & V \ll T_K \end{cases}$ Here, the previous work is based on the idea that eV now plays the same role as temperature. That is, in the R.G. flow, we cut at eV, and the perturbation analysis of [3] is now for low voltage, so we find
$\tilde{G}_1 = G_0 \frac{3\pi^2/16}{\ln^2(eV/T_k)}$
$\tilde{G}_2 = G_0 \left[1 - \left(\frac{\pi eV}{T_K}\right)^2\right]$ However, we argue that the approximations used are not entirely reasonable. From the work of N. d'Ambrumenil and B. Muzykantskii, on the non-equilibrium x-ray problem (to which the Kondo problem can be related), it is *not* sufficient to decouple the leads, rotate basis and then simply reintroduce the voltage. It is clear (in the very least as a precaution), that a full treatment of the *true* two lead Kondo Hamiltonian of equation (0.4.4) is required. With this in mind, in the next chapter, we will be following the calculation of Anderson, Yuval and Hamann, in which

they map the Kondo Hamiltonian onto a two dimensional Coulomb gas.

0.7 Conclusion

We have derived some results for the two lead Kondo problem in various limits. We have shown the suppression of the Coulomb blockade, and observed that this suppression can be viewed as a kind of delocalisation caused by the Kondo singlet across the dot. The above treatment required us to neglect the bias potential and then to rotate our two lead problem to a diagonal basis. However, it is not clear that this is a controlled or reasonable approach. In fact, the presence of voltage in the non-diagonal Green's function of related x-ray problems implies that the voltage cannot be treated perturbatively, and that a generalisation of non-eequilibrium Riemann-Hilbert techniques may be necessary.

0.8 Verder lezen

https://ris.utwente.nl/ws/files/6028066/3-s2$_0$$-$$B$9780128015957000227.$pdfhttps$: $//repositorio-aberto.up.pt/bitstream/$10216/119066/2/315683.$pdfhttps$: $//www.diva-portal.org/smash/get/diva$2 : 1046339/$FULLTEXT$01.$pdfhttps$: $//www.semanticscholar.org/paper/Cybersecurity-analysis-of-a-SCADA-system-under-and-Rocha/dfa$7c12551$ebe$7b24$da$8d806$e$87e946051$a57cb$9https$: $//dreamlab.net/en/blog/post/fuzzing-ics-protocols/https$: $//www.connectivity4ir.co.uk/artic$ 62351$--Secure-communication-in-the-energy-industry.aspxhttps$: $//www.win.tue.nl/$ $setalle/$2017$_f auri_e ncryption.pdfhttps$: $//blog.nettedautomation.com/$2017/$ta$ $//arxiv.org/pdf/$2001.02925.$pdfhttps$: $//www.dragos.com/wp-content/uploads/CrashOverride$ 01.$pdfhttps$: $//www.welivesecurity.com/wp-content/uploads/$2017/06/$Win32_I ndustroyer.pdfht$ $//www.cybersecurityintelligence.com/blog/attack-on-ukraines-power-grid-targeted-transmission-stations-$4530.$htmlhttps$: $//arstechnica.com/information-technology/$2017/06/$crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet/https$: $//www.vice.com/en/article/zmeyg8/ukraine-power-grid-malware-crashoverride-industroyerhttps$: $//www.dragos.com/resource/crashov$ $analyzing-the-malware-that-attacks-power-grids/https$: $//en.wikipedia.org/wiki/Industr$ $//en.wikipedia.org/wiki/Crash_O verride_N etworkhttps$: $//www.nixu.com/blog/crashoverride-threat-electricity-networkswatkaneenbackdoorallemaalhttps$: $//www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/crashoverridehttps$: $//www.incibe-cert.es/en/blog/crashoverride-malware-ics-back-againindustroyerhttps$: $//rhebo.com/en/service/glossar/industroyer-$ 25114/$https$: $//www.paloaltonetworks.com/blog/$2017/06/$crashoverrideindustroyer-$

protections−palo−alto−networks−customers/https : *//search.abb.com/library/Download.aspx*?
9*AKK*107045*A*1003*amp*; *LanguageCode* = *en*

crashoverride in december 2016 https://www.dragos.com/wp-content/uploads/CRASHOVERRI
https://www.csoonline.com/article/3200828/crash-override-malware-that-took-down-a-power-grid-may-have-been-a-test-run.html https://www.powermag.com/why-crashoverride-is-a-red-flag-for-u-s-power-companies/ https://www.webopedia.com/definitions/crash
industroyer-malware/

https://www.msspalert.com/cybersecurity-breaches-and-attacks/u-s-dept-of-homeland-securitys-crashoverride-malware-warning-to-utilities/ https://blog.checkpoint.com/res
https://thehill.com/policy/cybersecurity/337877-crash-override-malware-heightens-fears-for-us-electric-grid/ https://pylos.co/2018/11/03/crashoverride-when-advanced-actors-look-like-amateurs/ https://www.inguardians.com/dhs-fbi-warn-of-attacks-against-us-energy-manufacturing-companies-and-employees/
https://www.cyberthreatalliance.org/stuxnet-to-crashoverride-to-trisis-evaluating-the-history-and-future-of-integrity-based-attacks-on-industrial-environments/
https://rethinkresearch.biz/articles/industroyer-crashoverride-malware-behind-ukraine-utility-attack/

This work has been supported by The IET

J. Smith and A. N. Other (*The IET, Stevenage, UK*)

E-mail: jsmith@theiet.org

Bibliography

[1] Anderson, P.: 'A poor man's derivation of scaling laws for the Kondo problem', *J. Phys. C.*, 1960, **3**, p. 2436

[2] Coleman, P.: '1/N expansion for the Kondo lattice', *Phys. Rev. B*, 1983, **28**, pp. 5255-5262

[3] Ludwig, I. and Ludwig A. W. W.: 'Kondo effect induced by a magnetic field', *Phys. Rev. B*, 2001, **64**, p. 045328