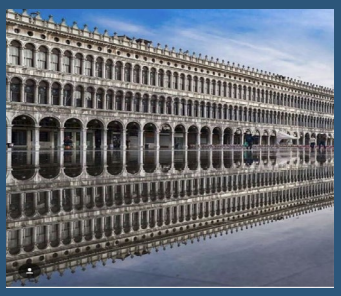


# *Is it better to remain silent and be thought a fool than to speak and remove all doubt?*

Abraham Lincoln?
Mark Twain?
Maurice Switzer ?
John Maynard Keynes ?
Confucius ?
Dalai Lama ?

# INDUCTION OF IMMUNITY FROM INTRUDERS? "VACCINE" STRATEGY AS A BIO-MEDICAL METAPHOR FOR DEVICE-AGNOSTIC CYBERSECURITY?

Shoumen Palit Austin Datta[1,2], Massachusetts Institute of Technology and Massachusetts General Hospital, Harvard Medical School
[1]MIT Auto-ID Lab, Dept of Mechanical Engineering, MIT and [2]MDPnP Lab, Dept of Anesthesiology, Massachusetts General Hospital

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

Billions or trillions of devices are in daily use without any consideration for cybersecurity even in critical applications, for example, in energy, infrastructure, healthcare. Can we add one or more hardware elements to devices in the post-market phase to endow a threat-proportionate dose of cybersecurity to uphold the basic tenets of availability, integrity, and confidentiality?

To deliver the value-added function, a symbiotic interaction between existing/embedded microprocessor/electronics (pre-market device design) and an externally (post-market delayed differentiation) added hardware (IC, SoC) is necessary, either directly or virtually.

The externally added hardware may be as simple as inserting the form factor of a flash drive in an USB-type port on the device to confer/deliver some form of hardware root-of-trust (HRoT). The externally introduced hardware may use TPM (trusted platform module) tools including TPM APIs to manage/control/supervise the internal microprocessor in the device.

Can HRoT, TPM, TEE, etc. help to protect/secure execution of commands/algorithm after authentication/verification/authorization? Can TPM use dynamic cryptographic keys and cascading non-deterministic random number generators (RNG) and other features to "vaccinate" the device? Can this protocol induce the device to acquire a layer of "immunity" from intruders?

Can this cybersecurity concept/abstraction serve as a generic "pill" (or a cocktail of pills and/or vaccines) for device-agnostic cybersecurity? Device-agnostic cybersecurity as a platform may be applicable in several verticals, for example, photovoltaic cells (distributed energy), medical devices (ventilators, plethysmograph), mobile edge devices (internet of things [IoT] is a design metaphor for devices, cyberphysical systems, mobile edge objects). Modular and/or reconfigurable device agnosticism enhances agile adaptability for niche applications, e.g.,alarms, which are in smoke detectors, vehicles, buildings and medical devices in hospitals and homes.

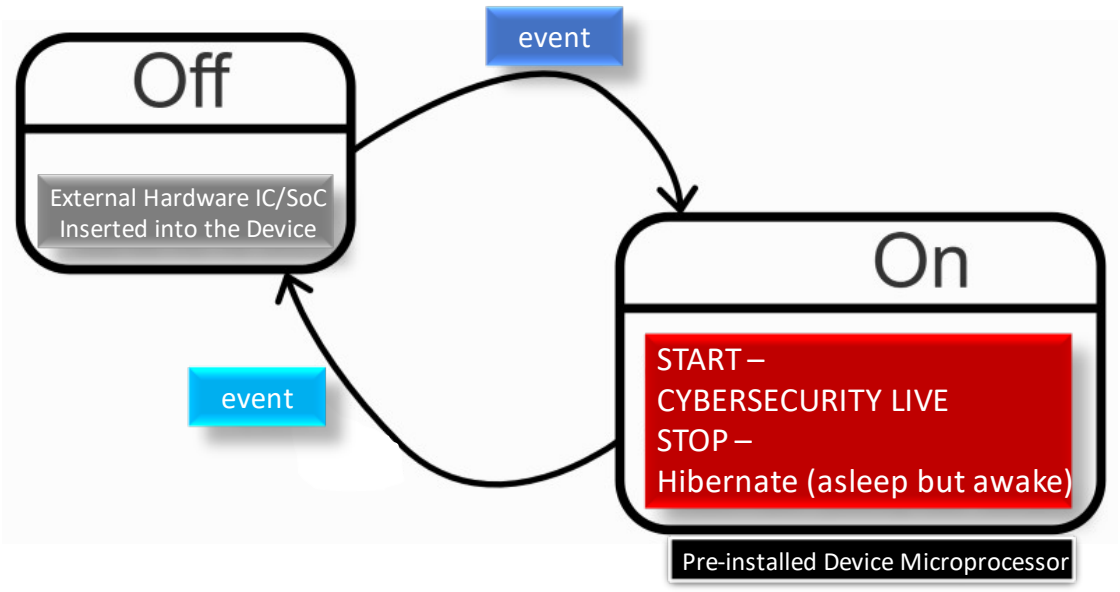



Figure 0: Cartoon of "on-off" state machine to illustrate the device-agnostic suggestion to "vaccinate" devices as an "immunization" step to protect from cybersecurity risks/threats.



Shoumen Datta ▪ shoumen@mit.edu ▪ sdatta8@mgh.harvard.edu ▪ https://dspace.mit.edu/handle/1721.1/140303

**ABSTRACT**

Integrating *ad hoc* objects/devices/things in a geospatially networked system introduces risks by violating trust boundaries. Poor attention to cybersecurity by design and complexity of standards influence device manufacturing in many sectors (energy, infrastructure, healthcare, transportation). Pre-market and post-market gaps in cybersecurity amplify vulnerabilities and potential for attacks.

The cybersecurity approach to mitigating risks when dealing with connected devices (internet of things) or adding things/objects to systems use sophisticated models with high precision (ATT&CK) as a guide to track and analyze characteristics of cyber intrusions.

This proposal is unfocused in its specificity. It advocates cybersecurity approaches as undifferentiated supplements. The biomedical metaphor of acquired immunity is simply a hand-waving generalization in this context. It is biologically inaccurate in terms of science. However, these words are a part of the common vernacular and conveys a sense of *protection*. Hence, the stretch to use these terms with respect to cybersecurity.

If any strand of this idea is successful, perhaps after modification by experts, it may mitigate risks from invasion and/or intrusion by external agents. The poor metaphor of immunity may help spring new ideas and convergence with other tools of cybersecurity in the context of medical devices (eg: ventilators). Ideally, a device-agnostic platform approach (universal vaccine, another poor metaphor) is preferred. Implementation of this tool will be measured in terms of quantifiable reduction of cybersecurity risks when *ad hoc* (IoT-type) devices are connected to systems in any vertical (energy, infrastructure, health).

A proof-of-concept using biomedical devices, such as life-support ventilators/respirators, may generate significant impact if the key performance indicator is the analysis of mortality and morbidity rates (instances where life-support devices were essential). The testbed for protection of infrastructure proof-of-concept may use photovoltaics (distributed energy resources) with bi-directional control features over the open internet (IoT-type devices) to optimize efficiency of micro-grids.

**BACKGROUND**

The spread of ransomware in healthcare[1] and hospitals[2] appears to be keeping pace[3] with the pandemic and the increasing epidemic[4] of cyberattacks, in general. Response from various agencies[5] indicate[6] that models[7] are necessary[8] but thinking outside conventional[9] culture[10] may also help since our lives[11] are rapidly and inextricably linked with the networked physical world[12] system[13]. The latter is an example of ubiquitous[14] computing which may include trillions of devices[15] manufactured by millions of companies, with geographically dispersed global supply chains which vary significantly in their competencies. It may be difficult for regulatory agencies[16] to provide oversight[17] for these devices which may connect to and communicate with the open internet using the principles of internet of things (IoT) as a digital-by-design metaphor.

Systems integration of devices, including IoT-type cyberphysical systems (CPS), often adds value to systems performance. Cybersecurity risks[18] after systems integration must be re-evaluated[19] and mitigation strategies updated if post-market systems integration violates the trust boundaries created during pre-market system design. Cybersecurity risks/threats introduced into systems due to integrating external devices may be dynamic, cryptic or volatile. Examples include sensors[20] in vehicles[21], digital diagnostics[22], medical devices[23], control-valve actuators in power plants[24] and photovoltaics in distributed energy resource optimization (micro-grids).

Cybersecurity by design, in general, is an aspirational goal due to lack of good security abstractions[25] as a guide. For device manufacturers the incorporation of cybersecurity is neither a core competency nor a business priority. Supply chain network planners relegate procurement functions to OEMs (original equipment manufacturers) mostly located in low-cost geographies who are less aware, ill-equipped and resource constrained even to consider cybersecurity in their design. Trillions of sub-systems, sub-components or spare parts are percolating globally without any form of cybersecurity or cybersecurity awareness.

Most businesses lack transparency, visibility and accountability with respect to supply chain assurance from their network of supply chain partners (Sarbanes-Oxley Act[26] of 2002). These actors source goods and services from sub-layers of the value network but businesses may be unaware of cryptology-based markers for supply-chain assurance. Hence, cybersecurity by design may be a delusional expectation for products with multi-tier supply chains extending into small and medium enterprises. The elusive quest to "build secure" during the pre-market phase may be worthy in principle but may remain an illusion for cybersecurity protagonists who may be irrationally optimistic about the global diffusion of cybersecurity, in practice.

Guidance for manufacturers[27] promotes the "build secure" adage but the glacial pace of change reflects how manufacturers may view or resist cybersecurity unless mandated, regulated, enforced or incentivized to better optimize specific outcomes, for example, end-point security[28]. Risks due to gaps[29] between principles (guidance) and practice (implementation at point of use) in mission critical operations (energy, power grid, infrastructure, hospitals, healthcare) could be fatal. Lack of cybersecurity may increase the risk of mortality and morbidity in healthcare[30], hospitals, telemedicine[31] for war fighters and medical devices for home health monitoring.

Programs to mitigate cybersecurity risks due to vulnerabilities arising from systems integration of devices may become an unsurmountable and unmanageable problem of gigantic proportions if a device-specific[32] approach was the only *modus operandi*. The lack of a panacea solution needs no over-emphasis.

This suggestion explores *device-agnostic cybersecurity platform(s)* with modular components and proof-of-concept (PoC) testbeds. Agility in variant configuration due to modularity may offer late-stage service level differentiation which may be catalytic for commercialization. Industrial adoption rates will vary widely depending on the level of acuity, granularity and maturity of different verticals. Due to heterogeneity of devices in different industries, market segmentation and domain-specific delayed differentiation may be necessary to accelerate adoption. Modularity by design will facilitate concurrent engineering to enable "mix and match" combinations of elements, structure and functions to create a branched decision tree of service level options. Modularity will also enable dynamic re-configuration if end-users choose to adapt versions of the product closer to the edge (for example, applications deploying IoT-type devices to meet or scale agile on-demand customer preferences).

One example of edge-dependent dynamic variant reconfiguration is the apt incorporation of digital twins[33] as a "mirage" for applications running *Shadow Figment*[34] where intruders are tracked[35] via *honeypots*[36] using a "digital shadow" (fake digital duplicate / digital twin) of the actual operation (which stays protected/secured). Digital twins can change depending on the application running the honey pot-esque project[37] "Shadow Figment" created by PNNL[38].

A platform approach includes the potential for dynamic aggregation and disaggregation of components and services if units are application-adaptive and multi-standard compliant. The modularity of design in device-agnostic cybersecurity is key to optimizing this "mix/match" versioning-on-demand. The accepted caveat in this hypothetical device-agnostic platform approach for a vast landscape (billions/trillions of devices) are the gaps of knowledge inherent in any experiment which attempts to create a new paradigm in a complex and competitive domain.

An optimistic outcome of this platform approach is to innovate complementary products ("pill"[39] or "universal"[40] or "*pan vaccine"*[41]) to endow devices with some level of "immunity" from cyber threats and risks irrespective of its pre-market status. The combination of these products may result in a convergence of hardware and software executing Agent-driven tasks[42] or something new or unknown or unanticipated. It is not expected to be easy[43].

The pillars of this hypothetical concept must be founded on scientific rationale, core engineering principles and rigorous metrics (measurements) to inform and re-inform design cycles to re-engineer or re-titrate key performance indicators (KPI). The preferred KPI (acceptable range of values, target metrics) may be established *a priori* and then work backwards to achieve that "target" in a retrosynthetic[44] approach, a principle borrowed from chemistry. This research accomplishment may provide one or more sets of criteria which may deliver the desired target of threat-proportionate level of device cybersecurity.

Insights from 1945[45] partially captured the concept of ubiquitous[46] computing in the 1990s. Progress[47] over a century has created computing which can sense, predict, plan, process data, execute complex applications and continuously compute across distributed systems for performance optimization, load-balancing, fault tolerance as well as a myriad of other functions but not without problems[48]. From the IC (integrated circuits) to the ICU (intensive care units) computing today is an inordinately complex orchestration of CPUs (central processing unit), GPUs (graphics processing unit) and NPUs (neural processing unit). Cybersecurity for devices on land (mobile edge devices) communicating with data centers under the sea[49] or cloud computing on MARS via the interplanetary internet[50] (interplanetary internet of things) must expect the unexpected. If the questions are correct, actionable, and down to earth, it may generate trustworthy data to inform our knowledge and advance the science of cybersecurity.

## OBJECTIVES AND GOALS

The central thrust of this hypothetical idea is to develop device-agnostic cybersecurity tool/platform to deliver cybersecurity features to a broad spectrum of devices (induction of immunity through administration of vaccines as a biomedical metaphor for cybersecurity). The objectives may include:

1. Demonstrate device "vaccination" as a pragmatic tool to confer immunity from intruders.
2. Demonstrate "vaccination" as a device-agnostic tool useful for general cybersecurity.
3. Challenge configured devices and analyze outcome with respect to uninterrupted *availability*, maintenance of *integrity* and inviolable *confidentiality* (AIC).
4. Evaluate security characteristics (e.g. degree of assurance) provided by "vaccination"
5. Quantify post-vaccination device capability with respect to deter, protect, detect, respond[51]
6. Develop proof of concept using one or more unsecured devices as templates to deliver components identified in a bill of materials (BOM[52]) including hardware, software, etc.

After attempting the exploratory objectives, evaluate if device cybersecurity can address the following (general) goals and/or if we can bridge one or more knowledge gaps and/or usher new understanding relevant to advancing the science and technology of cybersecurity:

1. Authentication of users, devices, systems during *ad hoc* integration/disintegration
2. Change/restore system trust boundary with respect to IoT-type devices / on-demand services
3. Access control efficiency / role-based access / privilege de-escalation or reduction
4. Encryption/decryption of data (local DB, transmission, in-network processing, tamper-proof)
5. Pervasive use of cryptographic keys for endpoint security control
6. Simulate different decision-support scenarios with respect to threat models, including attacker/defender strategies in CPS/IoT environments (edge, fog, cloud computing)

The following are aspirational / long term goals (not immediately germane to the PoC):

1. Develop methodologies and standards to support seamless, end-to-end security across interconnected networks of devices with multiple owners, trust domains, topologies, networking (wired, wireless, cellular, LTE, 5G, ultrawideband, mesh networks)
2. Develop new paradigms for effective and efficient risk management
3. Develop novel (effective and efficient) methods to deter/counter malicious cyber activities
4. Develop integrated safety-security-privacy framework in the context of systems integration
5. Develop frameworks compliant with architectures? (TOGAF[53]? DoDAF[54]? MoDAF[55]?)
6. Reverse-engineering resistant tools for management of software systems (model-based, data-informed, self-actuating "sense-&-respond" Agents for performance[56] optimization).

| Security Objectives | | | Functions and Techniques |
|---|---|---|---|
| Availability | Integrity | Confidentiality | Description |
| ✓ | ✓ | ✓ | Endpoint Physical Security |
| | ✓ | | Establish Roots of Trust |
| ✓ | ✓ | ✓ | Endpoint Identity |
| ✓ | ✓ | ✓ | Endpoint Access Control |
| | ✓ | | Endpoint Integrity Protection |
| ✓ | ✓ | ✓ | Data Protection |
| ✓ | ✓ | ✓ | Endpoint Monitoring & Analysis |
| ✓ | ✓ | ✓ | Endpoint Configuration & Management |
| | ✓ | ✓ | Cryptography Techniques for Endpoints |
| ✓ | ✓ | ✓ | Isolation Techniques for Endpoints |

Table 0: Cybersecurity Objectives for Endpoint Security: essential framework[57] for devices[58].



Shoumen Datta ▪ shoumen@mit.edu ▪ sdatta8@mgh.harvard.edu ▪ https://dspace.mit.edu/handle/1721.1/140303

**RESEARCH AND DEVELOPMENT**

Can we add one or more elements to a device to deliver a threat-proportionate dose of cybersecurity? Functional integration between the existing microprocessor/electronics and an externally added element (IC/SoC) is essential for the success of this exploration/experiment.

The central suggestion is to introduce an external piece of hardware (for example, in the form factor of a flash drive) to supervise/control the existing device processor (hardware) by establishing a hardware root-of-trust (HRoT) as a form of a *security gateway*[59] to deliver cybersecurity to elements it may control, in the device, thereafter. Software defined hardware[60] tools may be useful for control or reconfiguration. The limited number of instructions, logic layers and algorithms in devices (generally) may not need ASIC (application specific integrated circuits) level performance and suffice with FPGA (field programmable gate array) level outcomes even if they perform poorly compared[61] to ASICs but FPGAs offer algorithm agility.

The installed pre-market device microprocessor and operating systems may limit the choices and/or functionalities which can be modified. The latter will influence the type or degree of cybersecurity which may be delivered to the device in the post-market phase. Modularity, adaptability and scalability of this research approach will determine the efficiency, efficacy and feasibility of the cybersecurity "vaccination" strategy or if the biomedical metaphors are in vain.

The device-agnostic platform approach to device cybersecurity proposes an initial focus on a few but different domain-specific device types for PoC testbeds. An example is a ventilator, a medical device used in intensive care units (surgical SICU or neonatal NICU), emergency rooms as well as for home health[62]. Microprocessor (IC) controlled mechanical ventilators[63] have rudimentary computational needs. These devices have a limited set of functions regulated by handful of variables (Tables 1 & 2) with pre-loaded instruction sets (algorithms). Medical professionals may change parameters based on resource patient-centric variables.

Ventilators, like most devices, are potentially at risk from malicious events (unauthorized users/intruders). Vulnerabilities in design may become fatal without cybersecurity provisions because ventilators are not only a device for data acquisition but also a device that performs semi-autonomous or autonomous data-informed actuation in cases of acute respiratory care to maintain breathing functions. Monitoring the amount of oxygen (fraction of inspired oxygen, Fi[64]) delivered to the patient ($FiO_2$) is a critical data[65] element which must be secured to avoid hyperoxia or hypoxia. There is a glut of ventilator designs from engineers[66] and enthusiasts[67] in response to the pandemic in affluent nations[68] as well as low-cost ventilators[69] for resource-limited[70] settings. Cybersecurity by design does not appear to be a part of this response.

Malicious tampering with ventilators may induce oxygen toxicity[71] or oxygen poisoning[72] leading to cessation of breathing (respiratory arrest/failure). Hypoxemia, hypercapnia and hypoxia may result in brain injury[73] within 3-4 minutes. Severe brain damage and/or coma may lead to brain death[74] and clinical death. Cybersecurity of acute care medical devices is a life and death matter, in a span of a few minutes. However, after cessation of breathing the case/patient-centric time to death varies[75] widely.

**SCIENCE AND RATIONALE**

The question is whether an externally introduced co-processor (IC, SoC, microsystem) can act as a security gateway to deliver cybersecurity features and functions. For decades, co-processors have been used to execute tasks distinct from the central core processor[76] but in this case cybersecurity involves securing the activity of the microprocessor already in the device. Can a co-processor function in a cis-trans configuration at the hardware level to endow the factory installed processor (behind the "gateway") to acquire cybersecurity features from the add-on co-processor? Can the "master-slave" paradigm enslave the installed device processor to commands from the "master" co-processor? Can the external hardware/microprocessor securely communicate with the installed microprocessor? Does this symbiotic exchange reveal/create new cybersecurity vulnerabilities? Can the external element (form factor of a flash drive inserted in a USB port) supervise functions from the manufacturers device microprocessor in order to uphold the basic tenets of cybersecurity and assure device performance as intended (for example, performing the task of a trustworthy ventilator)?

If co-processors (or other hardware/software combinations) can assume control of the device microprocessor, can it also provide a shared hardware root-of-trust? The suggestion is to create (induce?) a hardware root-of-trust (HRoT) in the device, using a TPM chip (trusted platform module with embedded key) as a part of this external element. Keys and certificates generated and stored on the TPM may secure device health (boot code, authorizations), maintain integrity, availability and confidentiality of device data.

A combinatorial mix of dynamic cryptographic keys using non-deterministic random number generators (the RNG process may be off-loaded to microcontrollers to reduce processor overload) may be used as primers to seed cryptographic operations (authorizations, trusted boot). This "seeding" function to initiate authorization may be made even more dynamic (fluid) by using ndRNG strings and a TPM-embedded algorithm to further select a sub- or super-string from stored ndRNGs by combining/selecting/mixing string-related elements from TPM memory. For example, combine current and past ndRNG strings [$5^{th}$, $7^{th}$ and $12^{th}$] to create a superstring but choose every $3^{rd}$ number to form a new string (with embedded cryptoperiod) as the new crypto key to seed authorization. TPM may transmit (IP security?) encrypted variations of an alphanumeric sequence based on some combination of that *just-created* dynamic key (short half-life per cryptoperiod) to an authorization app on a chip display card and smartphone. Authorized users must synchronize (key exchange protocol?) the chip display and designated smartphone (encrypted mobile device) using KHA[77] (know, have, are) authentication scheme to begin the multi-factor authorization (MFA) to permit (authorize) synchronization using encrypted near-field communication (NFC). APIs (part of the software bill of materials[78]) associated with the external tool for TPM management may be used for this purpose.

Hence, TPM APIs may enable authorized medical professionals or trusted end-users to approve/disapprove state changes by providing additional authorized confirmations (using off-the-shelf cocktail of secure and searchable crypto-seeding algorithms[79]) during the boot/re-boot process to maintain device integrity. In hospitals, this process can be executed by professionals who are in proximity of the device but home health users may request remote changes to the device (ventilator) depending on the physiological status of the patient.

This introduces cybersecurity issues for remotely monitored devices. Such devices require additional stringency with respect to endpoint identity[80], device user identification and IP security. Using IP-based identification[81] with security and routing[82] controls are necessary for trust in asset management, authentication, authorization, and remote maintenance/activities.

Traditionally, one or more passwords may be used to authenticate the patient receiving services at home and the medical professional authorized to deliver/delivering the services. In an open networking environment, beyond firewalls, a tool such as MIT-Kerberos[83] authentication[84] server uses a coded format of passwords which are compared to a time-stamped code string but the actual passwords are never sent across open networks. After authentication is complete only then traditional IP transport layer security (TLS[85]) is established.

Oher hardware[86] security modules (HSM) in addition to or in combination with TPM, for example, Trusted Execution Environment[87] (TEE), may boost the vaccination for cybersecurity. Assuming that the device processors are resource constrained, can we run hypervisor[88] based security monitoring[89] software directly on the hardware if the externally introduced co-processor delivers more processing power? In this context virtual machine hosted processes are possible with hosted hypervisors which can be installed on the co-processor before it is inserted in the device. Software-based[90] TEE[91] could run on a hypervisor. Hypervisor-based security and/or virtualized instance for security can run honeypots with digital twins, eg, *Shadow Figment*.

The modularity (TPM, TEE, hypervisors, etc. may be viewed as modules) and portability (virtualization[92]) of the 'vaccination' method must be compatible between tools and devices with respect to software/hardware architecture, networks, operating systems and access to data ports (for securing data and distributed data management). HRoT with hardware-protected crypto keys are difficult to forge and preferred as a foundation for device-agnostic "vaccine" strategy. However, offshore hardware supply chains carries risk, such as, hardware Trojans or backdoors for data/information exfiltration.

The rationale for advocating device-agnostic cybersecurity "vaccine" strategy is based on a systems perspective. From 50,000 feet[93] the cartoon of connections of a microgrid[94] resembles the connectivity pattern of post-surgical PCA (patient-controlled analgesia[95]). Most devices are sensing or collecting (loggers) or transmitting or using data analytics in data- or information-informed semi-autonomous actuation. External commands and data fusion may also catalyze and commence auto-actuation. From a systems perspective, the connectivity view of the forward supply chain of Procter & Gamble's (Cincinnati, OH) consumer retail goods (Tide detergent) is similar at the cartoon level to the backward supply chain (reverse logistics) for DoD's (US Army Materiel Command[96] and Defense Logistics Agency) repair process for Sikorsky Black Hawk helicopters at Corpus Christi, TX (co-located with DoD's NAVFAC southeast). With greater diffusion of analytics, these connected pathways and networks may need new nodes (devices) to collect/monitor data for decision support systems (DSS). Several types of devices may be included in these systems to sense (S) the environment (E) and use the data from these percepts (P) to actuate (A) processes. Devices added to green-field and brown-field systems may benefit from PEAS data to optimize system performance. Hence, device cybersecurity is synonymous with data integrity, confidentiality and availability. Device-agnostic cybersecurity "vaccine" strategy offers a *plug-n-play* cybersecurity platform wherever applicable, whenever needed.

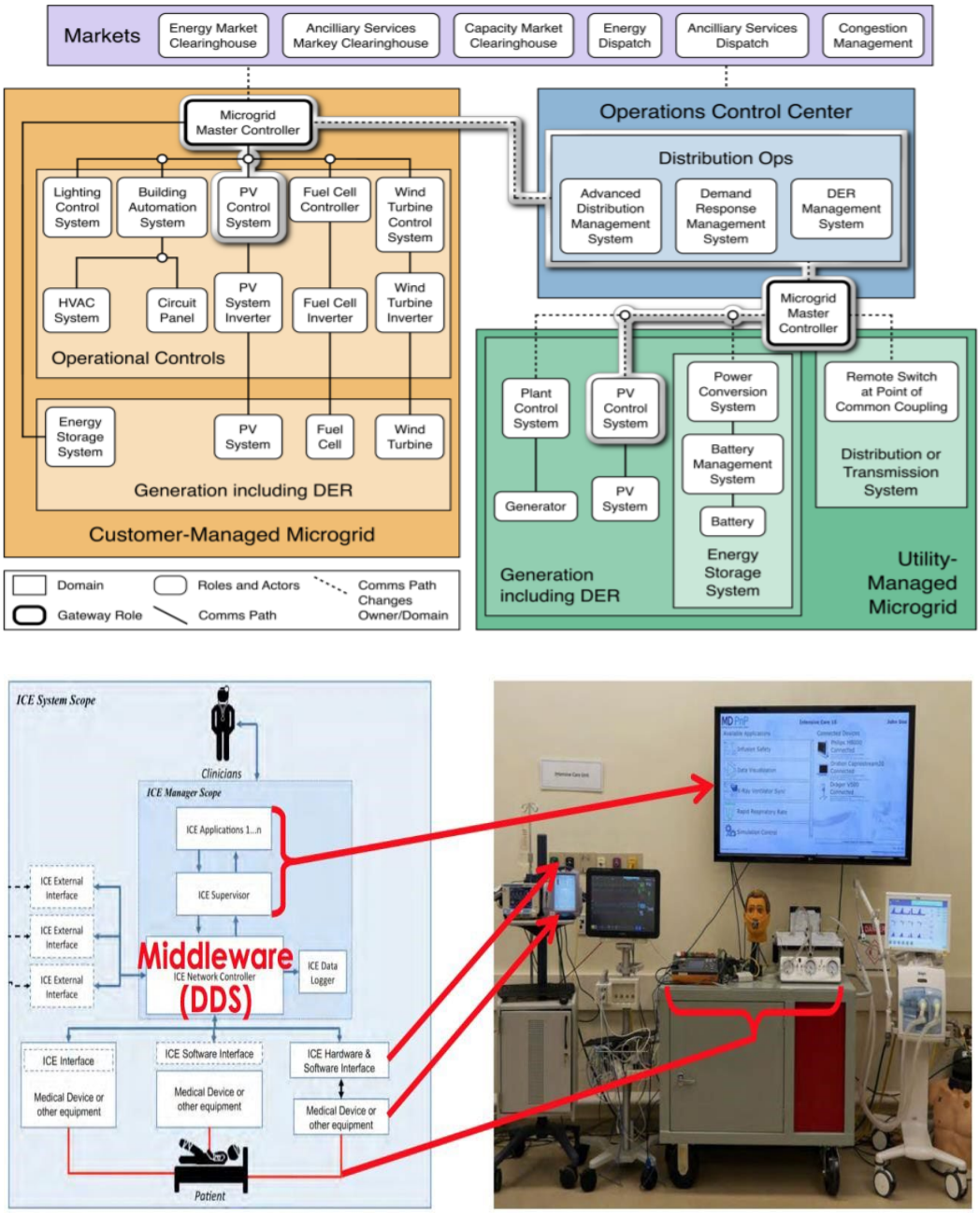



Figure 1: Cartoon of microgrid (ref. 94) and PCA (ref. 95). Both are device-dependent and data interoperability[97] is essential. Application of PEAS[98] paradigm (PEAS is a mnemonic from agent-based systems) may depend on data interoperability to improve systems performance through convergence of data and analytics from percepts (P), environment (E), actuators (A), and sensors (S). PEAS combined with OODA[99] and data fusion[100] tools may improve our understanding with respect to relational semantics between data, information, and knowledge in the context of the DIKW[101] pyramid. Data security may depend on device cybersecurity.

**DESIGN AND METHODS**

The "quick and dirty" round one experiment may use Raspberry Pi[102] (Rπ) with IC/SoC on a motherboard with ports (microUSB). Assume Rπ has no cybersecurity features (not even multi-factor authorization). An external hardware (IC/processor running HSM, TPM, TEE) is inserted into Rπ with the "expectation" to connect with the Rπ processor installed on the board.

Is it possible to direct/supervise the pre-installed Rπ processor using the externally added processor to deliver instructions? Can these instruction sets "induce" cybersecurity features to secure Rπ? For example, can Rπ be made to provide access control using cryptographic keys? Can the crypto keys be generated/delivered from the newly introduced hardware using TPM management tools (APIs) or other tools, such as, techniques used in software defined hardware? Can we use HAT (hardware attached on top) to add functionalities to installed microprocessor or co-processor? Is it appropriate to ask whether a microprocessor (Rπ) can be programmed in a manner similar to a microcontroller (Arduino) in the context of conferring cybersecurity? For example, Arduino IDE offers plug-and-play programming functions (plug Arduino board to a computer USB and upload). If Rπ can be configured as a microcontroller will it install the necessary cybersecurity features? If the Rπ experiment offers any sign of success then the real device of choice for this R&D effort is the ventilator. However, it may not be a Raspberry Pi *only* experiment but a combination of elements (SoCs/microprocessors/microcontrollers) available in various microsystems (Raspberry Pi, Arduino, BeagleBone, etc.).

Ventilators assist with improving pulmonary perfusion which requires certain design criteria and performance indicators (Table 1 & 2). For patients who are unable to breath on their own it provides mechanical "lung assist" and delivers a mixture of oxygen to improve perfusion. Various types of ventilators[103] provide different types of assisted breathing functions[104] (volume assist/control; pressure assist/control; pressure support ventilation; volume SIMV (synchronized intermittent mandatory ventilation); and pressure SIMV). From a cybersecurity perspective the microprocessor is involved in the execution of a simple set of algorithms for machine trigger variables and machine cycle variables as well as some compensatory mechanisms (SIMV) for respiratory optimization (Figure 2, Table 2).

Cybersecurity attacks may disrupt mechanical assistance or oxygen concentration, which, if undetected, may lead to severe brain damage, coma and/or clinal death (for example, lack of brain-stem responses). Simple "bit dribbling" by malicious intruders can slightly increase or decrease the range of values (low/high) to induce cessation of assisted breathing or alter the gaseous composition of inhaled breath leading to brain death and congestive heart failure (CHF).

The cybersecurity "vaccine" design is not intended to focus on device operation (vaccine is supposed to be device agnostic) but aimed at preventing any attempt to change any parameter (pressure, cycle time, concentration) unless the change is executed by an authorized user. The device-agnostic "vaccine" is supposed to uphold the cybersecurity characteristics: availability, integrity, confidentiality (AIC). Threat-proportionate versions of cybersecurity are necessary for ventilators, photovoltaic cells, car alarms, etc. The "vaccine" strategy for devices must remain cognizant that these devices, when and if necessary, may be operated over the open internet (IoT) for access and remote control of functions to modify device performance or operation.

Table 1:
Desired design features for ventilators (right). Performance criteria/indicators[105] to maintain physiological breathing in adults (bottom panel).

| Desired design features | |
|---|---|
| **Input criteria** | **Pneumatic:** medical flowmeters attached to 50 psig source connected to ventilator with high pressure hoses<br>**Air:** inspiratory flow and bias flow; control signal for exhalation manifold<br>**Oxygen:** inspiratory flow and bias flow<br>**Electrical:** power for exhalation manifold control circuit |
| **Output criteria** | Adjustable $FiO_2$<br>Adjustable breath rate and inspiratory time<br>Adjustable PEEP<br>Adjustable tidal volume<br>Disposable single-limb patient circuit |
| **Control circuit** | Electrical control of pneumatic pulse train to exhalation manifold<br>Digital display of<br>• inspiratory time<br>• breath rate<br>• peak airway pressure<br>• PEEP<br>Safety features<br>• disconnect alarm<br>• high pressure alarm<br>• electrical failure alarm |

| | Range | Accuracy | Settings |
|---|---|---|---|
| **Tidal volume** | 0–800 mL | ± 50 mL or < 10% | Result of flow and inspiratory time settings |
| **Respiratory rate** | 8–30 bpm | ± negligible | Continuous knob adjustment |
| **Inspiratory time** | 0–2 s | Assessed by tidal volume accuracy | Continuous knob adjustment |
| **Peep valve** | 3–30 cm $H_2O$ | ± 0.5 cm $H_2O$ | Continuous knob adjustment |
| **High pressure valve** | 60 cm $H_2O$ | ± 0.5 cm $H_2O$ | Preset |
| **$FiO_2$** | 40%–100% | ± 5% | Result of air and oxygen flowmeter settings |
| **High pressure sensor + shutoff** | >70 cm $H_2O$ | ± 2 cm $H_2O$ | Preset in software |
| **Low pressure sensor** | <3 cm $H_2O$ | ± 1 cm $H_2O$ | Preset in software |
| **Oxygen flow** | 0–15 L/min | Assessed by tidal volume and $FiO_2$ accuracy | Continuously adjustable |
| **Air flow** | 0–15 L/min | Assessed by tidal volume and $FiO_2$ accuracy | Continuously adjustable |

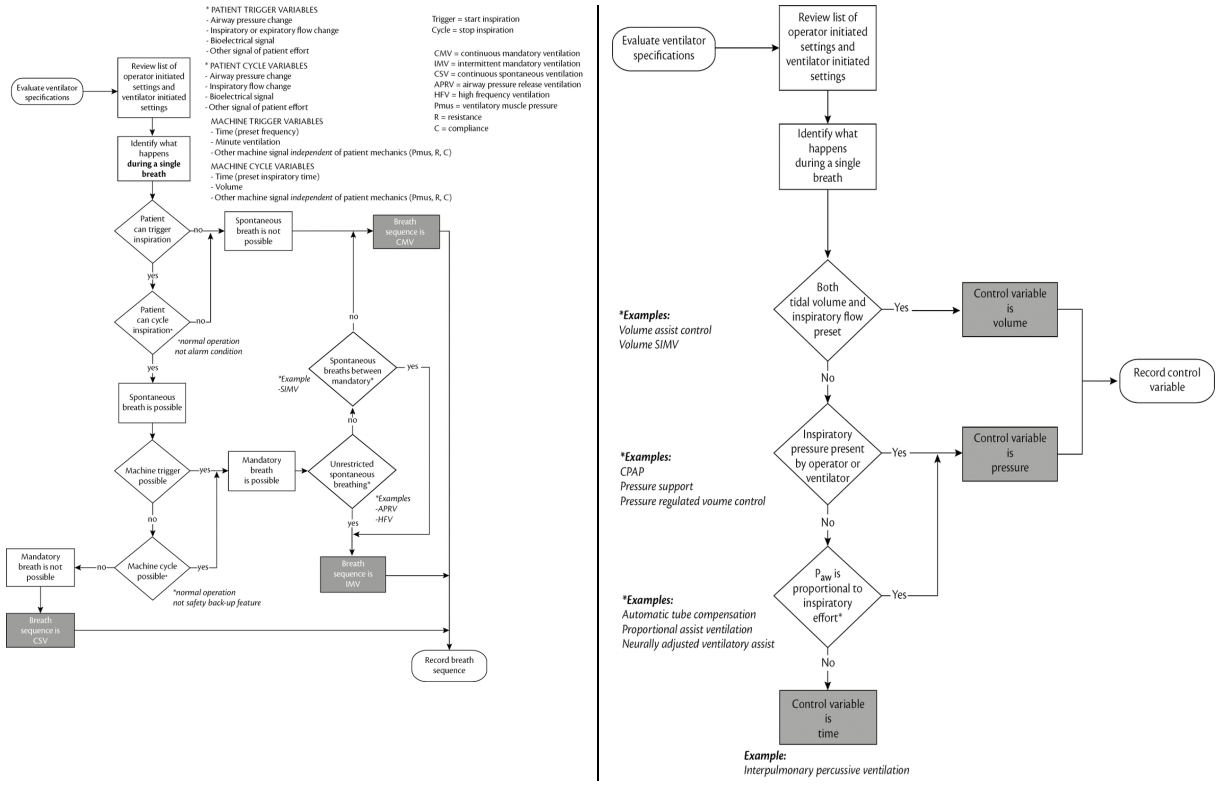



Figure 2: Decision tree for ventilators (ref 103) are guided by patient-centric data and feedback.

| Ventilator Variables | What happens/comments if changed/altered. Nodes where cybersecurity may be essential. |
|---|---|
| Respiratory Rate (RR) (breaths per minute) between 6 – 40 (normal).<br><br>I/E Ratio (inspiratory/expiration time ratio) recommended start 1:2; range of 1:1 – 1:4. | |
| Assist Control is based on a ***Trigger*** Sensitivity (trigger variables, see Figure 2). When a patient tries to inspire, they can cause a dip (2 to 7 cm $H_2O$) with respect to PEEP pressure (not necessarily equal to atmospheric pressure).<br>Airway pressure must be monitored continually (units in cm $H_2O$)<br>Maximum pressure: 40<br>Plateau pressure: 30<br>Passive mechanical blow-off valve: 40<br>PEEP* 5–15 cm (required)<br>Patient-centric need 10–15 | Respiratory Rate (RR) of 6-9 are applicable to Assist Control. |
| *Positive end-expiratory pressure (PEEP) is a value set up in patients receiving invasive or non-invasive mechanical ventilation.<br><br>Tidal Volume (TV) (air volume pushed into lung) between 200 – 800 mL (patient-centric, based on patient weight) | Failure conditions must result in an alarm and permit conversion to manual clinician override. If automatic ventilation fails, the conversion to manual ventilation must be ***immediate.*** |
| $etCO_2$ (end-tidal $CO_2$ is the amount of carbon dioxide in exhaled air**)** assesses ventilation (35-45 mmHg or 4.0-5.7kPa, kiloPascals) and perfusion (gaseous exchange in the lungs). High $etCO_2$ signals good ventilation, while low $etCO_2$ signals hypoventilation. | Capnometric data (partial pressure of $CO_2$ in exhaled air, etCO2, generated as waveform data - capnograph) is the fastest indicator to assess ***if ventilation is compromised***. ***Immediate*** action is recommended without waiting for pulse oximetry data which may be subject to some degree of phase equilibration since pulse oximetry assesses the amount of *oxygen bound to RBC* (red blood cells). |

Table 2: Nodes of control in ventilators which, if altered, may affect mortality and morbidity. Ventilator settings and values are obtained from MGH ICUs relative to CoVID-19 patients.

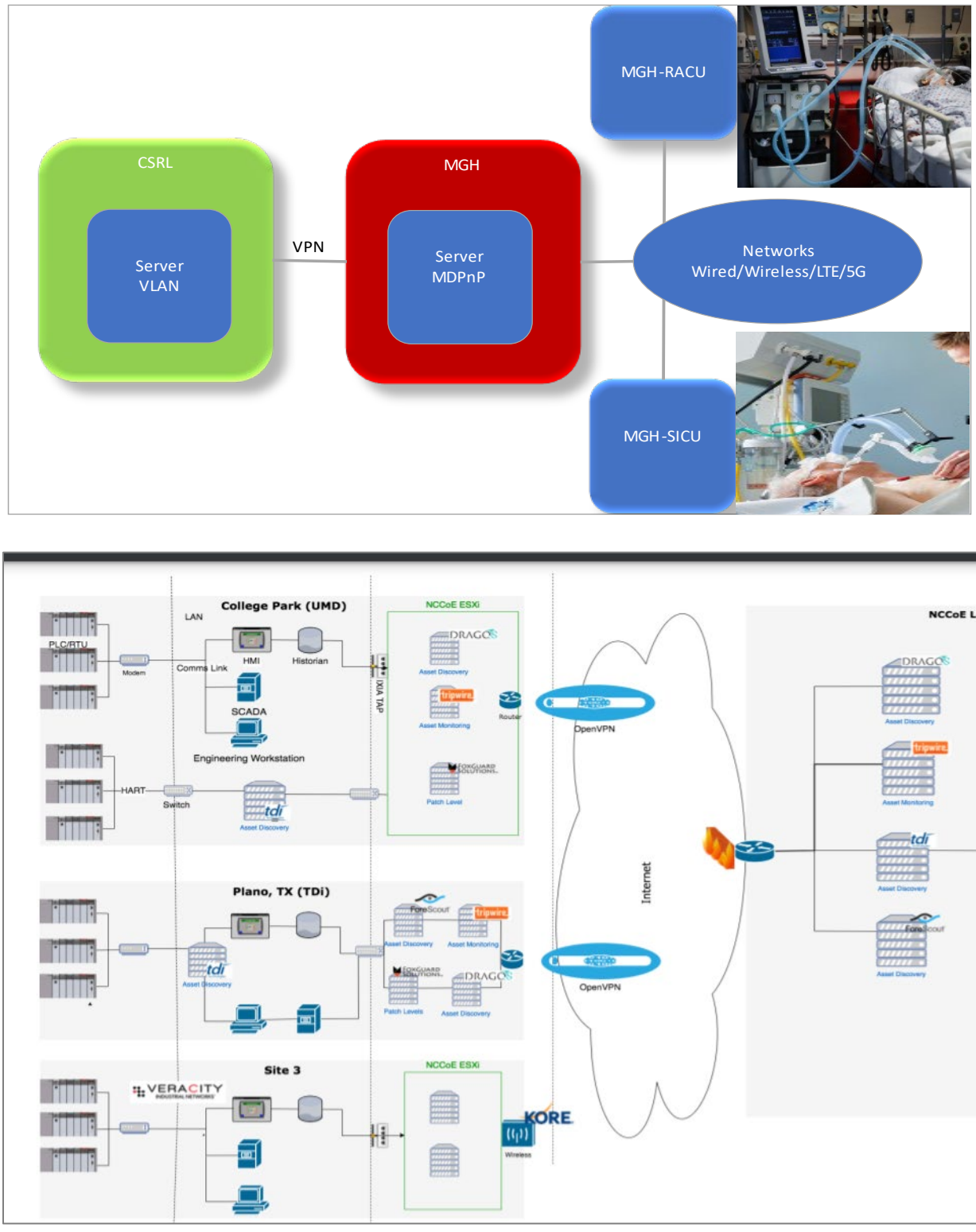



Figure 3: Cartoon for experimental testbed for cybersecurity vaccine strategy (top) is a model based on a testbed[106] used for distributed energy resources using photovoltaic cells (NCCoE).

In the context of medical devices, a "by-product" is the proliferation of device-specific (status) alarms[107] triggered when values (data/measurement/metrics) falls above or below the threshold/range (pre-set, hard-coded). Altering values may perturb thresholds/ranges and trigger automatic alarms. Cybersecurity attacks could trigger tens or hundreds of alarms in a hospital setting to deliberately sow debilitating confusion. Reduction[108] of alarm events[109] is a thorny issue. What if it was a false positive or what if the alarm caused a fatal distraction.

Performance of alarms and the criteria governing their on/off status are complex and legal problems at the heart of patient safety. Table 1 indicates "***disconnect alarm***" is a required "safety feature" but Table 2 emphasizes the ***need for alarm***. Alarms are linked to a network of physiological variables (Table 1, bottom panel) which are measured and communicated in near real-time to determine the status of the patient. It may require continuous data analytics by combining data from various devices (manufactured by different device manufacturers). The analysis of data from physiological monitoring and its outcome follows embedded/coded routines for triggering safety protocols, including alarms, which are essential elements of patient safety. Alarms in the context of patient safety should be secured and cannot be selectively turned on/off without medical authorization. Breach of cybersecurity in any device with an alarm may be as simple as to turn-on or turn-off the alarm (why "on-off" state machine [Figure 0] security is not trivial and the consequences may be fatal). Acuity of alarms may be a niche function for healthcare but essential for patient safety, hence, essential for medical device cybersecurity.

## EXPECTATIONS AND ECOSYSTEMS

If cybersecurity "vaccine" strategy succeeds (challenged by active intrusion) then the analytics may quantify "vaccine" performance with respect to the "immunity" acquired. This result may be a minor milestone because cybersecurity of devices are a part of an ecosystem.

The *physical* device-centric cybersecurity "vaccine" strategy must be viewed with respect to the system or systems connected to the device, locally and geospatially. The integrity of data in the device (Figure 1), integrity/confidentiality of the data during transmission, as well as the availability/integrity/confidentiality of the data stored at a remote database or cloud are highly significant.

Data analysis, feedback and decision support at the point-of-use are *cyber* components linked with the ecosystem of the *physical* device. The supply chain of this closed loop *cyberphysical* system[110] (CPS[111]) must be secured. The weakest link may be a penetration point to corrupt data or exfiltrate data and information.

Corrupt data, if stored and when analyzed, may lead to harmful decisions, including death (healthcare/biomedical devices) and destruction (infrastructure, energy). Lateral persistence and lateral movement of intruders exploiting the gaps in defense (eg ATT&CK) may be catastrophic. Intruders may "tunnel" from an edge device to a storage device, for example, from the ventilator to the electronic health records or electronic medical records (EHR/EMR).

Tunneling through routers (wired/wireless networks) to access devices and gain special privileges to data stores are a part of the ecosystem where the reality of threats from ransomware could become deadly. Ransomware at the device level is annoying (device replaced) but databases are the Achilles heel for systems unless dynamic redundancy is practiced daily.

In the ecosystem-centric view, if the network is compromised, device cybersecurity becomes exponentially more significant to prevent data tampering at the point of use. Can sensor devices store data (data persistence?) rather than transmitting the data if the network is not secure? Ubiquity of sensors makes this a serious problem with life and death consequences in certain cases. For example, oxygen sensors[112] in ventilators are vital to prevent hyperoxia or hypoxia by using $FiO_2$ data (Figure 2, left) to adjust the composition of the inhaled gaseous mix.

Low cost sensors without cybersecurity characteristics may introduce higher risks. It is an open question whether sensors without "local cache" or tiny databases are suitable for critical operations. It may be useful to revisit advances from DARPA Smart Dust[113] with respect to sensor networks (tinyOS[114] and tinyDB[115]), cybersecurity of data, *data acquisition* from devices[116] in hospitals, industry and the edge (IoT-type wearable photoplethysmography[117]).

Devices which generate/collect continuous waveform data[118] are vulnerable to minor changes. Intermittent sampling periods (see Figure 6) for continuous variables (gaps in time series data[119]) could change the data profile and alter the data-informed analytical outcome. Storage[120] of waveform data "samples" (sampling time) in patient records (EHR[121]) may be detrimental to long term healthcare due to errors in diagnosis, prognosis, treatment and medication. Deliberate artefacts[122] introduced[123] into data under the guise of efficacy[124] further degrades the data and corrupted data are stored in electronic medical records. Errors also arise due to proprietary restrictions in data handling enforced by device manufacturers. Preventing data interoperability between devices makes medical errors the 3rd leading cause of death[125] in the US. Patient safety[126] is a very complex task even without cybersecurity risks and threats.

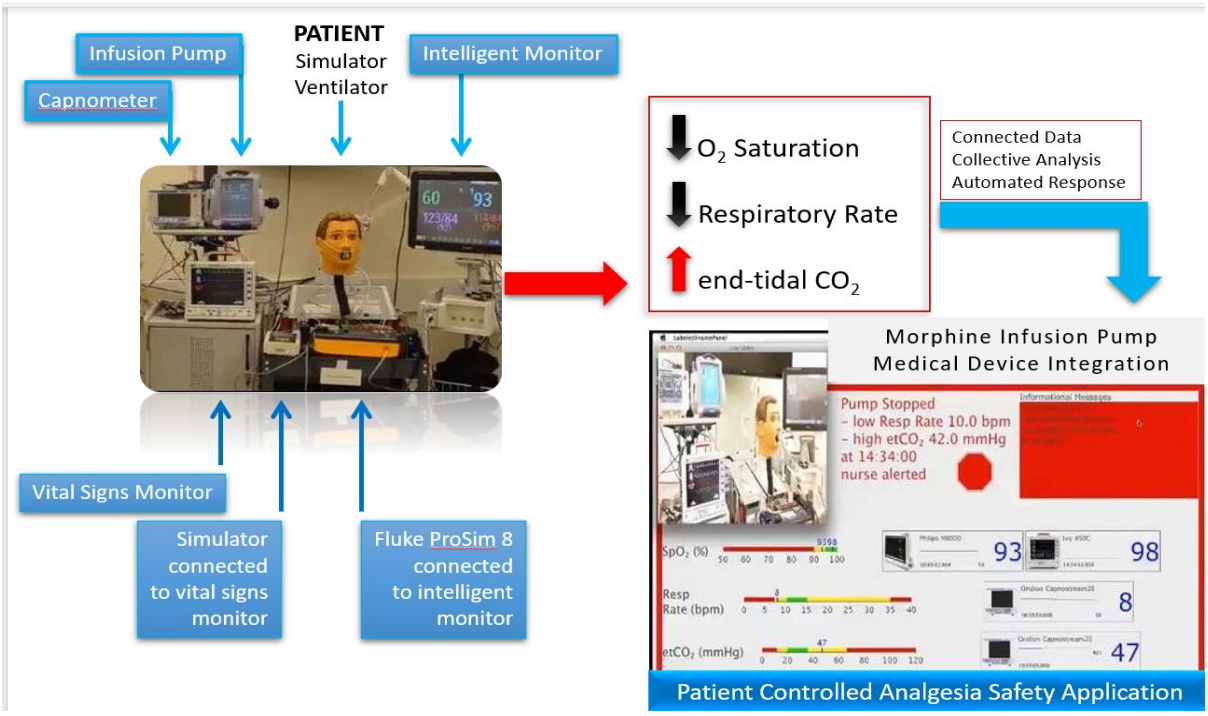



Figure 4: PCA simulation (MDPnP Lab, MGH, ref 95). Devices manufactured by different corporations are required for a post-surgical patient to self-administer morphine for pain control.

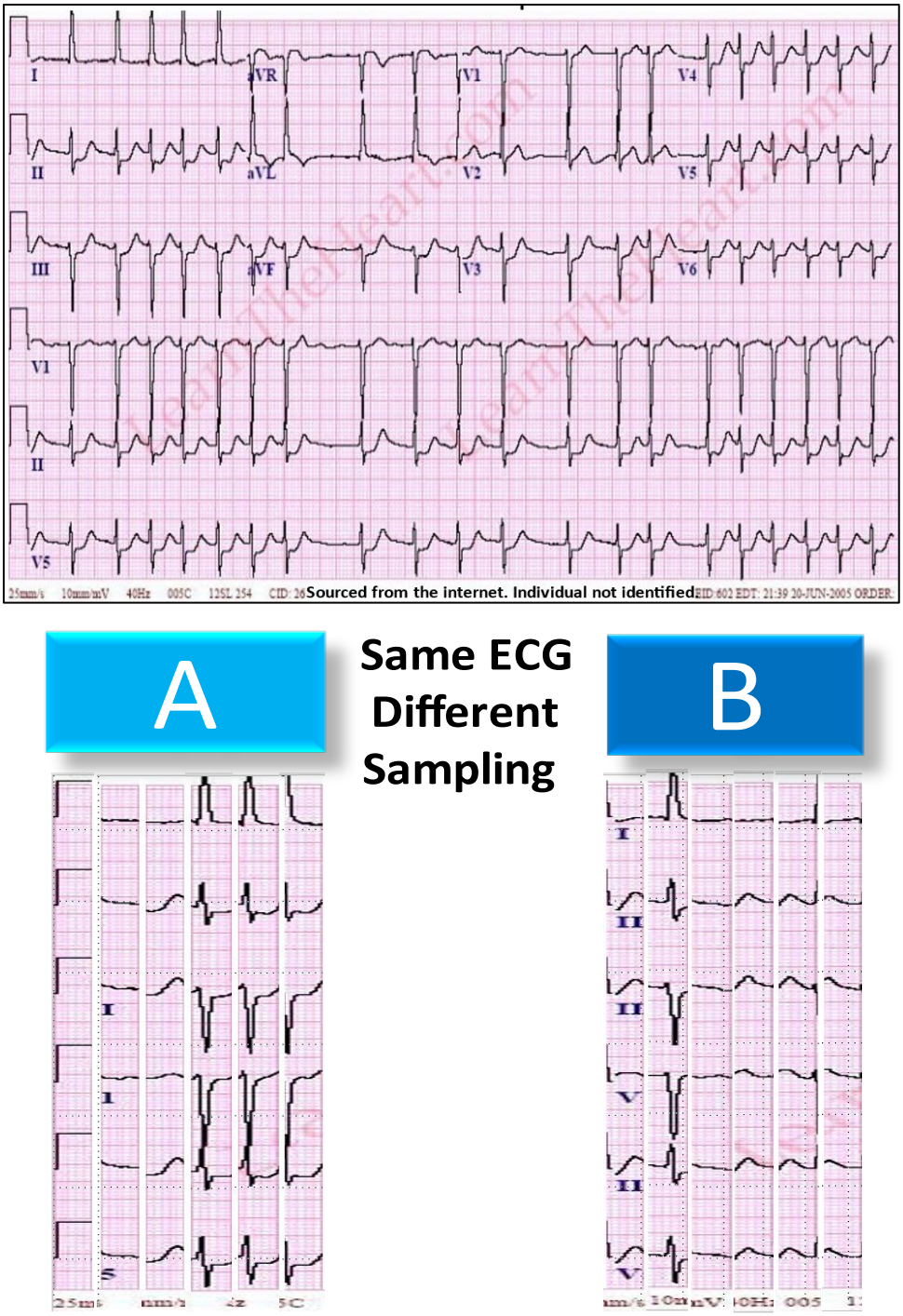



Figure 5: Atrial fibrillation with rapid ventricular rate is common[127] in cardiovascular diseases. An example of the complete waveform data (top) may be "sampled" by the instrument (ECG) for storage[128] in electronic health records (EHR). Depending on sampling time interval, this patient-specific critical time series data is sampled, corrupted and stored (bottom) as shown in panels A and B (see page 77 of 94 in reference[129]) for future misdiagnosis. Cybersecurity for data integrity is essential to store unaltered waveform data (patient-specific time series data).

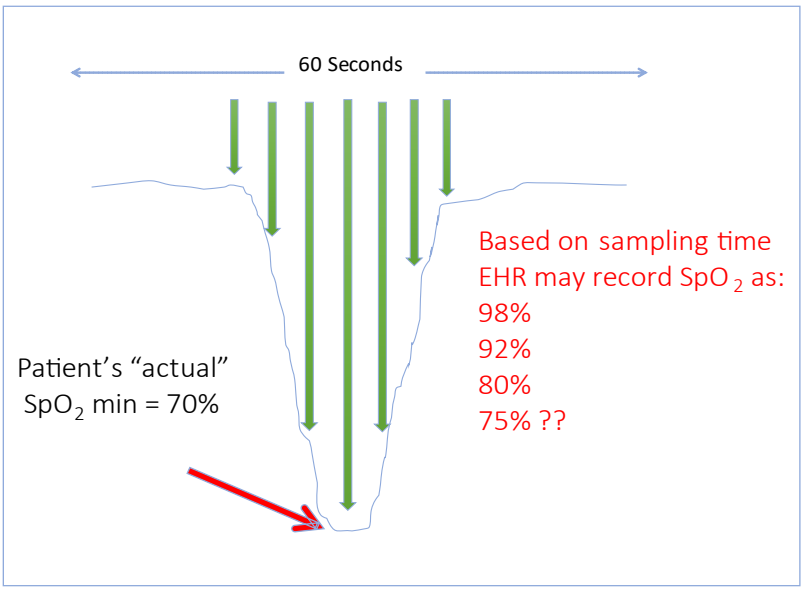



Figure 6: Error prone EHR documentation (storage) due to sampling time selection (sample points for 1-minute period). Which value will be recorded by the electronic health record (EHR) database? This example shows data from pulse oximetry which reports pulse rate (PR) blood oxygen levels via an oxygen saturation measurement called peripheral capillary oxygen saturation, or $SpO_2$ (percentage of oxygen in blood). Malicious intruders can exploit the sampling point vulnerability (sampling frequency, time between samples) of any data (but especially waveform data) to create massive errors in cumulative time series data which can be either device-centric or patient-specific (or both, depending on the target of cyber attackers). Device cybersecurity may be one but crucial layer of protection to maintain data integrity and confidentiality. Please see page 63 of 94 in "DATA" (for URL see reference number 129). The context of the raw data is vital to make sense of the analytics[130] for micro-decisions (patient-specific, precision medicine) as well as gain a macro-understanding (i.e. the *value*[131] network).

**DELIVERABLES AND IMPACT**

[1] A turn-key solution in the form factor of a flash drive which can be inserted in the device USB type port to induce cybersecurity functions and uphold the principal tenets (CIA).

[2] An update-by-wire version of the cybersecurity "vaccine" strategy (booster doses).

[3] Map device vulnerabilities to cybersecurity frameworks (expectations) and map "vaccinated" device cybersecurity capabilities, establish metrics for level of acquired immunity.

SCENARIO

Adversary targets TATRC[132] field operations where war fighters are on ventilators. Intruder lowers the range/threshold value for oxygen concentration and mutes alarms: patients suffer brain damage due to hypoxia (oxygen deprived due to low oxygen concentration) or are clinically dead in about 5 minutes (cessation of brain-stem responses).

SOLUTION

Inventory of "over-the-counter" (OTC) device-agnostic cybersecurity "vaccine" flash drives. Medic[133] GI Jane inserts "vaccine" in devices to commence "immune" functions *prior* to operations. GI Jane (not a cybersecurity expert or a computer scientist) delivers instructions via TPM management API using drag-and-drop commands on a digital twin interface embedded with Scratch[134] tools[135]. GI Jane received online[136] Lego MindStorm tutorials[137] and other entry level[138] training before joining the cybersecurity team at TATRC.

## CONTEXTS AND CLARIFICATIONS

Vaccine and immunity are used in this proposal as biological metaphors, not biomimicry. The use of "vaccine" is a hand-waving metaphor because it doesn't quite fit. In future *biological processes* of conferring immunity may be analyzed at a granular level to explore whether we can advance the *science* of cybersecurity by creating tools using the immune system as a template. The later may be true biomimicry. However, use of biological behaviors (ants, birds, "swarm intelligence") are often referred to as biomimicry (these may be behavior models, at best).

The use of biomedical metaphors (vaccine, immunity, booster) are laissez-faire, at best, but tested, tried and true natural processes. The principle of immunity is not unique for higher animals but exists in fungi[139], bacteria[140] and even works *between* kingdoms, in terms of taxonomy. Cross-kingdom delivery of immunity from plants to fungal pathogens[141] is an example of mobile[142] genetics[143] using microRNA[144] to silence or interfere[145] with gene expression. The principle of immunity is a Natural Law.

Advancing the science of cybersecurity based on natural laws provides uncompromising rigor. The transformation of biomimicry to inform cybersecurity must explore the *granularity* of *molecular* principles that underlie biological processes. We may wish to abstract the later and choose processes which may offer insights for offensive or defensive cybersecurity. There is ample room for innovation if we choose to explore biomimicry for cybersecurity.

It remains to be observed whether the outcome (if any) from this metaphorical treatment is just a drop in the ocean or a pebble in the pond. The lack of success in *this* use of biological metaphor should not affect the pursuit of biomimicry to advance the science of cybersecurity.

## OPINION AND CONCLUSION

Conventional wisdom suggests that deciding whether this project should be undertaken may depend on a few traditional questions and answers:

1. Is there a need for this solution?
2. Are there other technologies that can address the challenge more simply?
3. Could a significant part of the industry or sector benefit from the solution?
4. Is it practical?
5. Can it be built without having to rip out and replace existing infrastructure?
6. Is it a replacement for what already exists?
7. Is there a reasonably good chance an industry or sector may adopt the solution?
8. If the answers are affirmative, then, are there resources available to support the project?

**COMMENTS AND CRITICISMS**

Submitted for review to a few individuals (personal communication only).

**REFERENCES AND NOTES**

[1] *The State of Ransomware in Healthcare 2021*. SOPHOS Whitepaper. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf

[2] *Ransomware in Hospitals 2022* https://www.cybertalk.org/2021/08/10/best-practices-to-avoid-ransomware-attacks-on-hospitals-in-2022/

[3] Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). Joint Cybersecurity Advisory. *Ransomware Activity Targeting the Healthcare and Public Health Sector*, October 28, 2020. https://www.cisa.gov/uscert/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf

[4] *4000 Attacks a Day Since CoVID-19 Pandemic*. August 11, 2020. https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html

[5] *Cybercrime: CoVID-19 Impact*. INTERPOL, 2020 (Lyon, France) https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

[6] Federal Bureau of Investigation, Cyber Division (February 4, 2022) Flash CU-000162-MW *Indicators of Compromise Associated with LockBit 2.0 Ransomware* https://www.ic3.gov/Media/News/2022/220204.pdf

[7] *MITRE ATT&CK vs Cyber Kill Chain vs Diamond Model* https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f

[8] Nickels, Katie and and Ryan, Kovar (2019) *MITRE ATT&CK: The Play at Home Edition 2.0* https://i.blackhat.com/webcasts/2019/11-21-black-hat-webcast-mitre-attack-by-k-nickels-and-r-kovar.pdf

[9] National Academies of Sciences, Engineering, and Medicine (2017) *Additional Observations on Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions*: An Annex: Unclassified Abbreviated Version of a Classified Report. National Academies Press, Washington, DC. https://doi.org/10.17226/24949

[10] Georgiadou, A., Mouzakitis, S., Askounis, D. *Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework.* Sensors 2021, 21, 3267. https://doi.org/10.3390/s21093267 https://www.mdpi.com/1424-8220/21/9/3267/pdf

[11] Thomasian, Nicole M., and Eli Y. Adashi. "Cybersecurity in the Internet of Medical Things." *Health Policy and Technology*, vol. 10, no. 3, Sept. 2021, p. 100549 https://doi.org/10.1016/j.hlpt.2021.100549 https://fardapaper.ir/mohavaha/uploads/2021/12/3-Cybersecurity-in-the-Internet-of-Medical-Things.pdf

[12] Sanjay Sarma, David Brock and Kevin Ashton (1999) *"The Networked Physical World - Proposals for Engineering the Next Generation of Computing, Commerce, and Automatic-Identification,"* MIT Auto-ID Center White Paper. MIT-AUTOID-WH001, 1999. https://autoid.mit.edu/publications-0 https://pdfs.semanticscholar.org/88b4/a255082d91b3c88261976c85a24f2f92c5c3.pdf

[13] Daniel W. Engels, Sanjay E. Sarma, Laxmiprasad Putta, David Brock: The *Networked Physical World System*. International Conference WWW/Internet 2002 (ICWI): pages 104-111 https://www.researchgate.net/profile/Daniel-Engels-2/publication/220969017_The_Networked_Physical_World_System/links/0c96052aba0920de0e000000/The-Networked-Physical-World-System.pdf

[14] Max Mühlhäuser and Iryna Gurevych (2008) Introduction to Ubiquitous Computing. IGI Global. https://pdfs.semanticscholar.org/ab0e/b44c7c81a1af3fc2d23fa03f8f04f9e4ca2d.pdf

[15] Anandaraj S.P., Poornima S., Vignesh R., Ravi V. (2022) *Industrial Automation of IoT in 5G Era.* In: Velliangiri S., Gunasekaran M., Karthikeyan P. (eds) Secure Communication for 5G and IoT Networks. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-79766-9_6

[16] Murrin, Suzanne (2018) *FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices* (OEI-09- 16-00220) September 2018. Office of the Inspector General (OIG), US Department of Health and Human Services, Washington, DC. https://oig.hhs.gov/oei/reports/oei-09-16-00220.pdf

[17] *Medicare Lacks Consistent Oversight of Cybersecurity for Networked Medical Devices in Hospitals* (2021) US Department of Health & Human Services Office of Inspector General. Issue Brief June 2021, OEI-01-20-00220 www.oig.hhs.gov/oei/reports/OEI-01-20-00220.pdf

[18] Elaine Bochniewicz, Melissa Chase, Steve Christey Coley, Kyle Wallace, Matt Weir and Margie Zuk (202) Playbook for Threat Modeling Medical Devices. THE MITRE CORPORATION and the Medical Device Innovation Consortium (MDIC) https://www.mitre.org/sites/default/files/publications/Playbook-for-Threat-Modeling-Medical-Devices.pdf

[19] Committee on Cyber Resilience Workshop Series, et al. *Beyond Spectre: Confronting New Technical and Policy Challenges: Proceedings of a Workshop*. Edited by Anne Johnson and Lynette I. Millett, National Academies Press, 2019. https://doi.org/10.17226/25418

[20] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam and P. Ranganathan. *"Cybersecurity Attacks in Vehicular Sensors,"* in IEEE Sensors Journal, vol. 20, no. 22, pp. 13752-13767, November 15, 2020. doi: 10.1109/JSEN.2020.3004275 https://ieeexplore.ieee.org/document/9122502

[21] X. Sun, F. R. Yu and P. Zhang. *"A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs),"* in IEEE Transactions on Intelligent Transportation Systems. doi: 10.1109/TITS.2021.3085297 https://ieeexplore.ieee.org/document/9447840

[22] World Health Organization (July 31, 2020) *Guidance for post-market surveillance and market surveillance of medical devices, including in-vitro-diagnostics*. https://www.who.int/docs/default-source/essential-medicines/in-vitro-diagnostics/draft-public-pmsdevices.pdf?sfvrsn=f803f68a_2&download=true

[23] US Food and Drug Administration (December 22, 2021) Cybersecurity Alert: Fresenius Kabi Agilia Connect Infusion System https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

[24] Hossein Motlagh N, Mohammadrezaei M, Hunt J, Zakeri B. Internet of Things (IoT) and the Energy Sector. *Energies*. 2020; 13(2):494. https://doi.org/10.3390/en13020494 https://www.mdpi.com/1996-1073/13/2/494/pdf

[25] US Department of Defense (2018) Summary of the National Defense Strategy: Sharpening American Military's Competitive Edge https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

[26] US Senate and House of Representatives of the United States of America in Congress [H.R.3763, July 30, 2002] *Sarbanes-Oxley Act of 2002*. Public Law 107–204 107th Congress https://pcaobus.org/About/History/Documents/PDFs/Sarbanes_Oxley_Act_of_2002.pdf Amendment https://www.govinfo.gov/content/pkg/COMPS-1883/pdf/COMPS-1883.pdf Study https://www.sec.gov/news/studies/2009/sox-404_study.pdf

[27] Murugiah Souppaya Karen Scarfone Donna Dodson (February 2022) *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.* Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), US Department of Commerce. https://doi.org/10.6028/NIST.SP.800-218 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

[28] Karayi, Sumir (May 11, 2020) *3 Ways to Get Endpoint Security Back Under Control in the New Remote World of Work* https://www.securitymagazine.com/articles/92362-ways-to-get-endpoint-security-back-under-control-in-the-new-remote-world-of-work

[29] Adam Pennington, Andy Applebaum, Katie Nickels, Tim Schulz, Blake Strom and John Wunder (2019) *Getting Started with ATT&CK*. MITRE Corporation (attack.mitre.org) https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf

[30] Newman, Lily Hay (July 16, 2019) *These Hackers Made an App That Kills to Prove a Point: Medtronic and the FDA left an insulin pump with a potentially deadly vulnerability on the market - until researchers who found the flaw showed how bad it could be.*WIRED. https://www.wired.com/story/medtronic-insulin-pump-hack-app

[31] U.S. Army Telemedicine & Advanced Technology Research Center (TATRC) *OpTMed Lab Conducts 4th Annual Field Evaluations at Communications-Electronics Research, Development and Engineering Center (CERDEC) Ground Activity.* 2019. https://www.tatrc.org/www/docs/news/16_9_OpTMedVisitors.pdf

[32] Burke G, Saxena N. *Cyber Risks Prediction and Analysis in Medical Emergency Equipment for Situational Awareness.* Sensors. 2021 August 6; 21(16):5325. doi: 10.3390/s21165325 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8398009/pdf/sensors-21-05325.pdf

[33] Datta, Shoumen (2016) Digital Twins https://arxiv.org/ftp/arxiv/papers/1610/1610.06467.pdf

[34] Thomas W. Edgar (2020) *SHADOW FIGMENT - Model Driven Deception for Cyber-Physical System Defense.* Pacific Northwest National Lab. https://apps.dtic.mil/sti/pdfs/AD1128044.pdf

[35] Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. Doubleday, 1989 http://bayrampasamakina.com/tr/pdf_stoll_4_1.pdf

[36] Lance Spitzner (September 13, 2002) *Honeypots: Tracking Hackers.* Addison-Wesley ISBN: 0-321-10895-7 http://www.it-docs.net/ddata/792.pdf

[37] Spitzner, Lance (2003) *"The Honeynet Project: trapping the hackers". IEEE Security & Privacy* **1** (2): 15 - 23 doi:10.1109/MSECP.2003.1193207 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.121.7750&rep=rep1&type=pdf

[38] *Shadow Figment* (Battelle Number 31305) https://www.pnnl.gov/available-technologies/shadow-figment-model-driven-cyber-defense-control-systems

[39] Bethany Halford (January 14, 2022) *How Pfizer scientists transformed an old drug lead into a COVID-19 antiviral: Behind the scenes of the medicinal chemistry campaign that led to the pill Paxlovid.* Chemical & Engineering News (C&EN) volume 100 issue 3. ISSN 0009-2347 American Chemical Society https://cen.acs.org/pharmaceuticals/drug-discovery/How-Pfizer-scientists-transformed-an-old-drug-lead-into-a-COVID-19-antiviral/100/i3

[40] Carolyn Beans (January 26, 2022) Researchers getting closer to a "universal" flu vaccine Proceedings of the National Academy of Sciences 119 (5) e2123477119 DOI: 10.1073/pnas.2123477119 https://www.pnas.org/content/pnas/119/5/e2123477119.full.pdf

[41] US Military Health System (MHS) *Development of WRAIR's Pan-Coronavirus Vaccine Shows Promise.* Walter Reed Army Institute of Research (WRAIR) December 28, 2021 https://www.health.mil/News/Articles/2021/12/28/Development-of-WRAIRs-PanCoronavirus-Vaccine-Shows-Promise

[42] Datta, Shoumen (2016) *Cybersecurity: Personal Security Agents as Modular Models representing People, Process, Atoms and Bits.* European Union (EU) Agenda. https://euagenda.eu/upload/publications/cybersecurity.pdf

[43] Kim Tingley (December 8, 2021) We're Getting Close to 'Universal' Vaccines. It Hasn't Been Easy. The New York Times. https://www.ncbi.nlm.nih.gov/search/research-news/15155

[44] Corey, E.J., Ohno, Masaji, Mitra, Rajat B., and Vatakencherry, Paul A. (February 1, 1964) Total Synthesis of Longifolene. *Journal of the American Chemical Society* 1964, 86, 3, 478–485 https://doi.org/10.1021/ja01057a039

[45] Bush, Vannevar "As We May Think." *The Atlantic*. July 1, 1945. https://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/

[46] Weiser, M. (1991) *The Computer for the 21st Century.* Scientific American, 265, 94-104. http://dx.doi.org/10.1038/scientificamerican0991-94 https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf

[47] Helena Parmask, Christina Jaegering, Maarja Pärnpuu. *The History of Ubiquitous Computing* https://www.sutori.com/en/story/the-history-of-ubiquitous-computing--SMuA4RazAxWSKRXHENnAGSx2

[48] Leonardo B. Oliveira, Fernando Magno Quintão Pereira, Rafael Misoczki, Diego F. Aranha, Fábio Borges, Michele Nogueira, Michelle Wangham, Min Wu and Jie Liu (2018) The computer for the 21st century: present security & privacy challenges. *Journal of Internet Services and Applications* **9,** 24 (2018). https://doi.org/10.1186/s13174-018-0095-2 https://jisajournal.springeropen.com/track/pdf/10.1186/s13174-018-0095-2.pdf

[49] Roach, John (June 5, 2018) *Under the sea, Microsoft tests a datacenter that's quick to deploy, could provide internet connectivity for years.* MICROSOFT https://natick.research.microsoft.com/

[50] Burleigh S, Cerf V, Durst R, Fall K, Hooke A, Scott K, Weiss H. *The Interplanetary Internet: a communications infrastructure for Mars exploration.* Acta Astronaut. 2003 August-November 53(4-10): 365-373 DOI: 10.1016/s0094-5765(03)00154-1 https://www.sciencedirect.com/science/article/abs/pii/S0094576503001541

[51] Executive Office of the President of the United States (2019) *Federal Cybersecurity Research and Development Strategic Plan.* Cyber Security and Information Assurance (CISA) InterAgency Working Group, Subcommittee on Networking & Information Technology Research & Development (NITRD), Committee on Science & Technology Enterprise of the National Science & Technology Council (December 2019) https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf

[52] National Telecommunications and Information Administration (NTIA): *NTIA Multistakeholder Process on Software Component Transparency - Software Bill of Materials (SBOM).* https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf

[53] The Open Group. *TOGAF Standard*, Version 9.2 Part V - Enterprise Continuum and Tools: Architecture Repository https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap37.html

[54] US Department of Defense (DoD). *The DoD Architecture Framework (DoDAF) Version 2.02* DoD Office of the CIO https://dodcio.defense.gov/library/dod-architecture-framework/

[55] Object Management Group. *The Unified Profile for DoDAF/MODAF (UPDM).* US DoD Architecture Framework (DoDAF) and UK Ministry of Defence Architecture Framework (MODAF). https://www.omg.org/updm/

[56] Datta, Shoumen Palit Austin, Tausifa Jan Saleem, Molood Barati, María Victoria López López, Marie-Laure Furgala, Diana C. Vanegas, Gérald Santucci, Pramod P. Khargonekar and Eric S. McLamore (April 2, 2021) *Data, Analytics and Interoperability between Systems (IoT) is Incongruous with the Economics of Technology: Evolution of Porous Pareto Partition (P3).* Chapter 2 in "*Big Data Analytics for Internet of Things*" 1st ed. Editors Tausifa Jan Saleem and Mohammad Ahsan Chishti. Wiley. ISBN: 9781119740759 DOI: 10.1002/9781119740780 https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119740780.ch2

[57] Industrial Internet Consortium (IIC) *Industrial Internet of Things Volume G4: Security Framework* https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

[58] Martin, Bob (2016) *Industrial Internet of Things Security Framework* https://csrc.nist.gov/csrc/media/projects/supply-chain-risk-management/documents/ssca/2016-fall/wed_am1-industrial_internet_of_things_security_framework_bob_martin.pdf

[59] Tselios C., Tsolis G., Athanatos M. (2020) *A Comprehensive Technical Survey of Contemporary Cybersecurity Products and Solutions.* In: Fournaris A. et al. (eds) Computer Security. IOSEC 2019, MSTEC 2019, FINSEC 2019. Lecture Notes in Computer Science, vol 11981. Springer, Cham. https://doi.org/10.1007/978-3-030-42051-2_1

[60] Shen, Wade. (2018) *Software Defined Hardware*. DARPA. ERI Summit, San Francisco. https://eri-summit.darpa.mil/docs/20180725_1030_SDH.pdf

[61] Keshavarzi, Ali (2018) *Software Defined Hardware*. Defense Advanced Research Projects Agency (DARPA) https://www.darpa.mil/program/software-defined-hardware

[62] Ambrosino N, Pierucci P. *Using Telemedicine to Monitor the Patient with Chronic Respiratory Failure.* Life (Basel). **2021** October 20; 11(11):1113. doi: 10.3390/life11111113. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8620445/pdf/life-11-01113.pdf
Farré R, Navajas D, Prats E, Marti S, Guell R, Montserrat JM, Tebe C, Escarrabill J. *Performance of mechanical ventilators at the patient's home: a multicentre quality control study.* Thorax. **2006** May; 61(5):400-404. doi: 10.1136/thx.2005.052647. Epub 2006 February 7. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2111198/pdf/400.pdf https://thorax.bmj.com/content/thoraxjnl/61/5/400.full.pdf
Bassett, M R. *Passive ventilators in New Zealand homes. Part 1: Numerical studies and Part 2: Experimental trials.* United Kingdom, **1994** https://www.osti.gov/etdeweb/biblio/80807

[63] Sanborn WG. *Microprocessor-based mechanical ventilation.* Respiratory Care. 1993 January; 38(1):72-109

[64] Fuentes S, Chowdhury YS. *Fraction of Inspired Oxygen*. [Updated 2021 January 17]. In: StatPearls [Internet]. StatPearls Publishing https://www.ncbi.nlm.nih.gov/books/NBK560867

[65] Balasamy, K., Krishnaraj, N., Ramprasath, J. and Ramprakash, P. (2022). *A Secure Framework for Protecting Clinical Data in Medical IoT Environment.* In Smart Healthcare System Design (eds S.H. Islam and D. Samanta). https://doi.org/10.1002/9781119792253.ch9

[66] Massachusetts Institute of Technology (2020) *MIT Emergency Ventilator Design Toolbox* https://e-vent.mit.edu/mechanical/

[67] Tischer, Eric (2020) *Open source DIY Ventilator PLC control system* http://etischer.com/ventilator/ https://e-vent.mit.edu/user/etischer/?profiletab=main

[68] El-Hadj A, Kezrane M, Ahmad H, Ameur H, Bin Abd Rahim SZ, Younsi A, Abu-Zinadah H. *Design and simulation of mechanical ventilators*. Chaos Solitons Fractals. 2021 September; 150:111169. doi: 10.1016/j.chaos.2021.111169. Epub 2021 June 25. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8226155/pdf/main.pdf

[69] DeBoer B, Barari A, Nonoyama M, Dubrowski A, Zaccagnini M, Hosseini A. *Preliminary Design and Development of a Mechanical Ventilator Using Industrial Automation Components for Rapid Deployment During the COVID-19 Pandemic.* Cureus. 2021 December 13; 13(12):e20386. doi: 10.7759/cureus.20386 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8752376/pdf/cureus-0013-00000020386.pdf https://assets.cureus.com/uploads/technical_report/pdf/75218/20220112-32222-oo35ov.pdf

[70] Madekurozwa M, Bonneuil WV, Frattolin J, Watson DJ, Moore AC, Stevens MM, Moore J Jr, Mathiszig-Lee J, van Batenburg-Sherwood J. *A Novel Ventilator Design for COVID-19 and Resource-Limited Settings.* Frontiers in Medical Technology. 2021 October 4; 3:707826. doi: 10.3389/fmedt.2021.707826 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8757831/pdf/fmedt-03-707826.pdf https://www.frontiersin.org/articles/10.3389/fmedt.2021.707826/pdf

[71] Chawla A, Lavania AK. *Oxygen Toxicity*. Medical Journal of the Armed Forces India. 2001 April; 57(2):131-3. doi: 10.1016/S0377-1237(01)80133-7. Epub 2011 July 21. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4925834/pdf/main.pdf

[72] Donald, K.W. (1947) *Oxygen poisoning in man; signs and symptoms of oxygen poisoning.* British Medical Journal 1947 May 25; 1(4507):712-7. doi: 10.1136/bmj.1.4507.712 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2053400/pdf/brmedj03782-0008.pdf

[73] Moll, Vanessa (2021) *Overview of Respiratory Arrest* in Critical Care Medicine, Merck Manual Professional Edition https://www.merckmanuals.com/professional/critical-care-medicine/respiratory-arrest/overview-of-respiratory-arrest

[74] *A definition of irreversible coma.* Report of the Ad Hoc Committee of the Harvard Medical School to Examine the Definition of Brain Death. JAMA. 1968 August 5; 205(6):337-340 https://jamanetwork.com/journals/jama/article-abstract/340177

[75] Cooke CR, Hotchkin DL, Engelberg RA, Rubinson L, Curtis JR. *Predictors of time to death after terminal withdrawal of mechanical ventilation in the ICU.* Chest. 2010 August; 138(2):289-297. doi: 10.1378/chest.10-0289. Epub 2010 April 2. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2913765/pdf/100289.pdf

[76] Allen Bradley (1994) PLC-3 High Speed Interface and Diagnostic Software 2.0 (Installation Data) https://literature.rockwellautomation.com/idc/groups/literature/documents/in/1775-in001_-en-p.pdf
NASA Conference on Intelligent Robotics in Field, Factory, Service, and Space (CIRFFSS '94) https://ntrs.nasa.gov/api/citations/19940026021/downloads/19940026021.pdf

[77] Schneider, Fred B. *Something You Know, Have, or Are* https://www.cs.cornell.edu/courses/cs513/2005fa/NNLauthPeople.html

[78] *The Minimum Elements For a Software Bill of Materials (SBOM)* (July 12, 2021) Executive Order 14028, National Telecommunications and Information Administration (NTIA), US DoC https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
*NTIA Software Transparency Healthcare POC* https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf

[79] Antonio Regalado (February 4, 2022) *How Pfizer made an effective anti-covid pill*. MIT Technology Review https://www.technologyreview.com/2022/02/04/1044714/pfizer-covid-pill-paxlovid-pandemic/

[80] Skopik, Florian, Max Landauer, and Markus Wurzenberger. *"Blind Spots of Security Monitoring in Enterprise Infrastructures: A Survey."* IEEE Security & Privacy, 2022, pp. 2–10. https://doi.org/10.1109/MSEC.2021.3133764

[81] Cheekiralla, Sivaram, and Daniel W. Engels. *"An IPv6-Based Identification Scheme."* 2006 IEEE International Conference on Communications, vol. 1, 2006, pp. 281-286. doi:10.1109/ICC.2006.254741 https://ieeexplore.ieee.org/document/4024131

[82] Datta, Shoumen (2007) *Unified Theory of Relativistic Identification of Information in a Systems Age: Proposed Convergence of Unique Identification with Syntax and Semantics through Internet Protocol version 6* (MIT Engineering Systems Working Paper Series 2007 ESD-WP-2007-17, School of Engineering, Massachusetts Institute of Technology, Cambridge) *International Journal of Advanced Logistics* **1** 66-82 http://dspace.mit.edu/handle/1721.1/41902

[83] Massachusetts Institute of Technology. *Creating and Using Your MIT Kerberos Identity.* MIT Information Systems and Technology (IST). https://ist.mit.edu/start/kerberos

[84] Thomas Hardjono (2014) *Kerberos for Internet-of-Things.* MIT Kerberos and Internet Trust Consortium February, 2014 https://kit.mit.edu/sites/default/files/documents/Kerberos_Internet_of%20Things.pdf

[85] E. Rescorla (2018) Transport Layer Security (TLS) Protocol Version 1.3 ISSN: 2070-1721 https://datatracker.ietf.org/doc/html/rfc8446

[86] Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano (2019) *A comprehensive survey of hardware-assisted security: From the edge to the cloud*. Internet of Things, vol 6, 2019. ISSN 2542-6605 https://doi.org/10.1016/j.iot.2019.100055 https://www.sciencedirect.com/science/article/pii/S2542660519300101

[87] Valero J.M.J. *et al.* (2022) *Trusted Execution Environment-Enabled Platform for 5G Security and Privacy Enhancement.* In: Abd El-Latif A.A., Abd-El-Atty B., Venegas-Andraca S.E., Mazurczyk W., Gupta B.B. (eds) Security and Privacy Preserving for IoT and 5G Networks. Studies in Big Data, vol 95. Springer, Cham. https://doi.org/10.1007/978-3-030-85428-7_9

[88] Erick Bauman, Gbadebo Ayoade, and Zhiqiang Lin (2015) *A Survey on Hypervisor-Based Monitoring: Approaches, Applications, and Evolutions.* ACM Comp. Survey 48, 1, Article 10 (September 2015), 33 pages. DOI: https://doi.org/10.1145/2775111

[89] Yacine Hebbal (2017*) Semantic monitoring mechanisms dedicated to security monitoring in IaaS cloud. Computation and Language.* Thesis. Ecole nationale supérieure Mines-Télécom Atlantique, 2017. https://tel.archives-ouvertes.fr/tel-01797056/document

[90] Meiyu Zhang, Qianying Zhang, Shijun Zhao, Zhiping Shi, Yong Guan (2019) *"SoftME: A Software-Based Memory Protection Approach for TEE System to Resist Physical Attacks",* Security & Communication Networks, vol 2019 https://doi.org/10.1155/2019/8690853

[91] Shijun Zhao, Qianying Zhang, Yu Qin, Wei Feng, and Dengguo Feng (2019) *SecTEE: A Software-based Approach to Secure Enclave Architecture Using TEE.* In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. ACM (Association for Computing Machinery) New York, NY, USA. Pages 1723–1740. https://doi.org/10.1145/3319535.3363205

[92] Jakub Szefer and Ruby B. Lee. 2012. *Architectural support for hypervisor-secure virtualization.* In Proceedings of the Seventeenth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS XVII). Association for Computing Machinery, New York, NY, USA, pages 437–450. https://doi.org/10.1145/2150976.2151022

[93] Hoffman, W. (2004). The view from 50,000 feet. *PM Network, 18*(7), pages 26–33 https://www.pmi.org/learning/library/business-dashboard-continuous-feedback-process-4219

[94] Jim McCarthy, Eileen Division, Don Faatz, Nik Urlaub, John Wiltberger and Tsion Yimer (February 2022) *Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity.* National Institute of Standards and Technology (NIST), National Cybersecurity Center of Excellence (NCCoE), US Department of Commerce. https://doi.org/10.6028/NIST.SP.1800-32 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-32.pdf

[95] Datta, S. and Goldman, J.M. (2017) *Healthcare - Digital Transformation of the Healthcare Value Chain: Emergence of Medical Internet of Things (MIoT) may need an Integrated Clinical Environment, ICE*. https://arxiv.org/ftp/arxiv/papers/1703/1703.04524.pdf Cornell University https://arxiv.org/abs/1703.04524 MIT Library https://dspace.mit.edu/handle/1721.1/107893

[96] General Paul Kern, Former Commanding General, US Army Materiel Command, Fort Belvoir. *Personal Communication*. https://apps.dtic.mil/sti/pdfs/ADA601375.pdf

[97] Weininger S, Jaffe MB, Rausch T, Goldman JM. (2017) *Capturing Essential Information to Achieve Safe Interoperability.* Anesthesia and Analgesia 2017 January; 124(1):83-94. doi: 10.1213/ANE.0000000000001351 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5161571/pdf/nihms772191.pdf

[98] Artificial Intelligence - *Intelligent Agents* (2017) https://courses.edx.org/asset-v1:ColumbiaX+CSMM.101x+1T2017+type@asset+block@AI_edx_intelligent_agents_new__1_.pdf

[99] William S. Angerman (2004) *Coming Full Circle With Boyd's OODA Loop Ideas: An Analysis Of Innovation Diffusion And Evolution* (Thesis). https://apps.dtic.mil/dtic/tr/fulltext/u2/a425228.pdf

[100] Castanedo, Federico. "A Review of Data Fusion Techniques." *The Scientific World Journal*, 2013. doi:10.1155/2013/704504 http://downloads.hindawi.com/journals/tswj/2013/704504.pdf

[101] Henry, Nicholas L. (May–June 1974). *"Knowledge Management: A New Concern for Public Administration".* Public Administration Review **34** (3): 189–196. doi:10.2307/974902 https://www.jstor.org/stable/974902

[102] C. Severance. *"Eben Upton: Raspberry Pi,"* in Computer, vol. 46, no. 10, pp. 14-16, October 2013. doi: 10.1109/MC.2013.349

[103] Chatburn, Robert L., and Eduardo Mireles-Cabodevila. *Design and Function of Mechanical Ventilators*. In Oxford Textbook of Critical Care (2 ed.). Oxford University Press, 2016. https://doi.org/10.1093/med/9780199600830.003.0092

[104] Lei, Yuan (2017). *Ventilator System Concept*. In Medical Ventilator System Basics: A clinical guide. Oxford University Press, Oxford, UK. July 2017. ISBN-13 9780198784975 DOI: 10.1093/med/9780198784975.001.0001 https://oxfordmedicine.com/view/10.1093/med/9780198784975.001.0001/med-9780198784975-chapter-4 https://oxfordmedicine.com/view/10.1093/med/9780198784975.001.0001/med-9780198784975

[105] Knorr JM, Sheehan MM, Santana DC, Samorezov S, Sammour I, Deblock M, Kuban B, Chaisson N, Chatburn RL. Design and performance testing of a novel emergency ventilator for in-hospital use. Can J Respir Ther. 2020 Sep 28;56:42-51. doi: 10.29390/cjrt-2020-023. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7521602/pdf/cjrt-2020-023.pdf

[106] NIST National Cybersecurity Center of Excellence (November 13, 2018) *Energy Provider Community Update* www.nccoe.nist.gov/sites/default/files/legacy-files/es-coi-20181113.pdf

[107] Borowski M, Görges M, Fried R, Such O, Wrede C, Imhoff M. *Medical device alarms.* Biomed Tech (Berlin) 2011 April; 56(2):73-83. doi 10.1515/BMT.2011.005 Epub 2011 March 3 https://www.degruyter.com/document/doi/10.1515/BMT.2011.005/html

[108] Koomen E, Webster CS, Konrad D, van der Hoeven JG, Best T, Kesecioglu J, Gommers DA, de Vries WB, Kappen TH. *Reducing medical device alarms by an order of magnitude: A human factors approach.* Anaesth Intensive Care. 2021 January; 49(1):52-61. doi: 10.1177/0310057X20968840 Epub 2021 February 2. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7905747/pdf/10.1177_0310057X20968840.pdf

[109] Chambrin MC. *Alarms in the intensive care unit: how can the number of false alarms be reduced?* Crit Care. 2001 August; 5(4):184-8. doi: 10.1186/cc1021. Epub 2001 May 23. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC137277/pdf/cc1021.pdf).

[110] Yaacoub JA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. *Cyber-physical systems security: Limitations, issues and future trends.* Microprocessors and Microsystems 2020 September; 77:103201. doi: 10.1016/j.micpro.2020.103201. Epub 2020 July 8. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7340599/pdf/main.pdf

[111] *NIST Framework for Cyber-Physical Systems*
Volume 1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
Volume 2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-202.pdf

[112] Draeger Oxygen Sensor 6850645 https://www.draeger.com/Products/Content/sensors-oxygen-flow-pi-9071248-en-us.pdf

[113] Pister, Kris. *SMART DUST: Autonomous sensing and communication in a cubic millimeter.* https://people.eecs.berkeley.edu/~pister/SmartDust/

[114] Jason Hill, Robert Szewczyk, Alec Woo, Seth Hollar, David Culler, Kristofer Pister (2000) *System Architecture Directions for Networked Sensors.* In Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS IX). Association for Computing Machinery, Cambridge, Massachusetts. https://pdos.csail.mit.edu/archive/6.097/readings/tinyos.pdf

[115] Sam Madden, Joe Hellerstein, and Wei Hong (2003) *TinyDB: In-Network Query Processing in TinyOS* Version 0.4 September, 2003 http://telegraph.cs.berkeley.edu/tinydb/tinydb.pdf

[116] Samuel R. Madden, Michael J. Franklin, Joseph M. Hellerstein, and Wei Hong (2005) *TinyDB: an acquisitional query processing system for sensor networks.* ACM Transactions on Database Systems 30, 1 (March 2005), 122–173 https://doi.org/10.1145/1061318.1061322

[117] Castaneda D, Esparza A, Ghamari M, Soltanpur C, Nazeran H. *A review on wearable photoplethysmography sensors and their potential future applications in health care.* Int J Biosens Bioelectron. 2018; 4(4):195-202. doi: 10.15406/ijbsbe.2018.04.00125 Epub 2018 Aug 6 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6426305/pdf/nihms-984963.pdf

[118] Goodwin AJ, Eytan D, Greer RW, Mazwi M, Thommandram A, Goodfellow SD, Assadi A, Jegatheeswaran A, Laussen PC. *A practical approach to storage and retrieval of high-frequency physiological signals.* Physiological Measurement 2020 April 20; 41(3):035008. doi: 10.1088/1361-6579/ab7cb5 https://iopscience.iop.org/article/10.1088/1361-6579/ab7cb5/pdf

[119] Blalock, Davis, Madden, Samuel and Guttag, John (2018*) "Sprintz: Time Series Compression for the Internet of Things."* Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 2, no. 3, September 2018, pp. 1–23. https://doi.org/10.1145/3264903 https://dl.acm.org/doi/pdf/10.1145/3264903 https://arxiv.org/pdf/1808.02515.pdf

[120] Brinkmann BH, Bower MR, Stengel KA, Worrell GA, Stead M. (2009*) Large-scale electrophysiology: acquisition, compression, encryption, and storage of big data.* J Neurosci Methods. 2009 May 30; 180(1):185-92. doi: 10.1016/j.jneumeth.2009.03.022 Epub 2009 April 1 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2720128/pdf/nihms106959.pdf

[121] Charlton PH, Villarroel M, Salguiero F. *Waveform Analysis to Estimate Respiratory Rate.* 2016 September 10. In: MIT Critical Data, editor. Secondary Analysis of Electronic Health Records [Internet]. Cham (CH): Springer; 2016. Chapter 26 https://www.ncbi.nlm.nih.gov/books/NBK543644/ https://www.ncbi.nlm.nih.gov/books/NBK543644/pdf/Bookshelf_NBK543644.pdf https://www.ncbi.nlm.nih.gov/books/NBK543630/pdf/Bookshelf_NBK543630.pdf

[122] Edinburgh T, Smielewski P, Czosnyka M, Cabeleira M, Eglen SJ, Ercole A. *DeepClean: Self-Supervised Artefact Rejection for Intensive Care Waveform Data Using Deep Generative Learning.* Acta Neurochir Suppl. 2021;131:235-241. doi: 10.1007/978-3-030-59436-7_45

[123] Silva P, Luz E, Silva G, Moreira G, Wanner E, Vidal F, Menotti D. *Towards better heartbeat segmentation with deep learning classification.* Science Rep. 2020 November 26; 10(1):20701. Doi: 10.1038/s41598-020-77745-0 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7692498/pdf/41598_2020_Article_77745.pdf

[124] Bizzego A, Gabrieli G, Neoh MJY, Esposito G. *Improving the Efficacy of Deep-Learning Models for Heart Beat Detection on Heterogeneous Datasets.* Bioengineering. 2021 Nov 28; 8(12):193. doi: 10.3390/bioengineering8120193. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8698903/pdf/bioengineering-08-00193.pdf

[125] Makary MA, Daniel M. *Medical error-the third leading cause of death in the US.* BMJ. 2016 May 3; 353:i2139 https://doi.org/10.1136/bmj.i2139

[126] Luke Slawomirski, Ane Auraaen and Niek Klazinga (2017) *The Economics Of Patient Safety: Strengthening a value-based approach to reducing patient harm at national level.* Organisation for Economic Co-operation and Development (OECD), Health Division. https://www.oecd.org/els/health-systems/The-economics-of-patient-safety-March-2017.pdf

[127] Shettigar UR. *Management of rapid ventricular rate in acute atrial fibrillation*. International Journal of Clinical Pharmacology and Therapeutics 1994 May; 32(5) pages 240-245

[128] Moskowitz A, Chen KP, Cooper AZ, Chahin A, Ghassemi MM, Celi LA. *Management of Atrial Fibrillation with Rapid Ventricular Response in the Intensive Care Unit: A Secondary Analysis of Electronic Health Record Data.* Shock. 2017 October; 48(4) pages 436-440. doi: 10.1097/SHK.0000000000000869 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5603354/pdf/nihms860354.pdf

[129] Page 77 of 94 in "DATA" – please download "DATA" PDF from the MIT Library DSpace https://dspace.mit.edu/handle/1721.1/140303 (Note: Page 63 of 94 is also in this "DATA" PDF).

[130] Datta, Shoumen and Granger, Clive (2006) Advances in Supply Chain Management: Potential to Improve Forecasting. MIT Engineering Systems Division Work Paper Series (ESD-WP-2006-11) https://dspace.mit.edu/handle/1721.1/102799
Datta, S., Granger, C. W. J., Barari, M. and Gibbs, T. (2007) Management of Supply Chain: an alternative modeling technique for forecasting. *Journal of the Operational Research Society* 58 1459-1469 http://www.tandfonline.com/doi/full/10.1057/palgrave.jors.2602419 http://dspace.mit.edu/handle/1721.1/41906

[131] Shoumen Datta, Bob Betts, Mark Dinning, Feryal Erhun, Tom Gibbs, Pinar Keskinocak, Hui Li, Mike Li, and Micah Samuels (2003) *Adaptive Value Network* pages 3-67 (Chapter 1). In Evolution of Supply Chain Management: Symbiosis of Adaptive Value Networks and ICT (Information Communication Technology). Chang, Yoon Seok, Makatsoris, Harris C., and Richards, Howard D., eds. Print ISBN 978-1-4020-7812-5 https://doi.org/10.1007/b110025 2004 Kluwer Academic Publishers, Boston. https://link.springer.com/book/10.1007/b110025 http://eprints.stiperdharmawacana.ac.id/68/1/%5BYoon_Seok_Chang%2C_Harris_C._Makatsoris%2C_Howard_D._%28BookFi%29.pdf

[132] Telemedicine & Advanced Technology Research Center www.tatrc.org

[133] OpTMed Lab Conducts 4th Annual Field Evaluations at CERDEC Ground Activity https://www.tatrc.org/www/docs/news/16_9_OpTMedVisitors.pdf

[134] Sylvan, Elisabeth Amy (2008) *The sharing of wonderful ideas: influence and interaction in online communities of creators.* Doctoral Thesis (PhD), Massachusetts Institute of Technology, School of Architecture and Planning, Program in Media Arts and Sciences (MIT Media Lab) February 2008 https://dspace.mit.edu/handle/1721.1/42404

[135] SCRATCH https://scratch.mit.edu/projects/editor/?tutorial=getStarted

[136] MIT Open Learning https://openlearning.mit.edu

[137] Lifelong Kindergarten Group, MIT Media Lab. Massachusetts Institute of Technology. https://www.media.mit.edu/groups/lifelong-kindergarten/overview

[138] MIT App Inventor https://appinventor.mit.edu

[139] Daskalov A, Mitchell PS, Sandstrom A, Vance RE, Glass NL. *Molecular characterization of a fungal gasdermin-like protein.* Proceedings of the National Academy of Sciences, USA. 2020 August 4; 117(31): 18600-18607 doi: 10.1073/pnas.2004876117 Epub 2020 July 23. https://www.pnas.org/content/pnas/117/31/18600.full.pdf https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7414189/pdf/pnas.202004876.pdf

[140] Johnson AG, Wein T, Mayer ML, Duncan-Lowey B, Yirmiya E, Oppenheimer-Shaanan Y, Amitai G, Sorek R, Kranzusch PJ. *Bacterial gasdermins reveal an ancient mechanism of cell death.* Science. 2022 January 14; 375(6577) pages 221-225. doi: 10.1126/science.abj8432.

[141] Cai Q, Qiao L, Wang M, He B, Lin FM, Palmquist J, Huang SD, Jin H. (2018) *Plants send small RNAs in extracellular vesicles to fungal pathogen to silence virulence genes.* Science. 2018 June 8; 360(6393):1126-1129. doi: 10.1126/science.aar4142. Epub 2018 May 17. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6442475/

[142] Creighton HB and McClintock B (1931) A correlation of cytological and genetical crossing-over in Zea Mays. Proc Natl Acad Sci USA 17 (8):492–497 https://www.pnas.org/content/pnas/17/8/492.full.pdf
McClintock B (1950) The origin and behavior of mutable loci in maize. Proc Natl Acad Sci USA 36 (6):344–355 https://www.pnas.org/content/pnas/36/6/344.full.pdf

[143] Johanna Wong-Bajracharya, Vasanth Singan, Remo Monti, Krista L. Plett, Vivian Ng, Igor V. Grigoriev, Francis M. Martin, Ian C. Anderson and Jonathan M. Plett (2022) *The ectomycorrhizal fungus* Pisolithus microcarpus *encodes a microRNA involved in cross-kingdom gene silencing during symbiosis.* PNAS 2022, 19 (3) e2103527119 https://doi.org/10.1073/pnas.2103527119 www.pnas.org/content/119/3/e2103527119

[144] Zhang L, Hou D, Chen X, Li D, Zhu L, Zhang Y, Li J, Bian Z, Liang X, Cai X, Yin Y, Wang C, Zhang T, Zhu D, Zhang D, Xu J, Chen Q, Ba Y, Liu J, Wang Q, Chen J, Wang J, Wang M, Zhang Q, Zhang J, Zen K, Zhang CY. *Exogenous plant MIR168a specifically targets mammalian LDLRAP1: evidence of cross-kingdom regulation by microRNA.* Cell Res. 2012 Jan; 22(1):107-26. doi: 10.1038/cr.2011.158. Epub 2011 September 20. Erratum in: Cell Res. 2012 Jan; 22(1): 273-4. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3351925/pdf/cr2011158a.pdf

[145] Fire A, Xu S, Montgomery MK, Kostas SA, Driver SE, Mello CC. *Potent and specific genetic interference by double-stranded RNA in Caenorhabditis elegans.* Nature. 1998 Feb 19;391(6669):806-11. doi: 10.1038/35888 https://www.nature.com/articles/35888.pdf

Ideas are like chessmen moved forward. They may be beaten, but they may also start a winning game. - *Johann Wolfgang von Goethe*

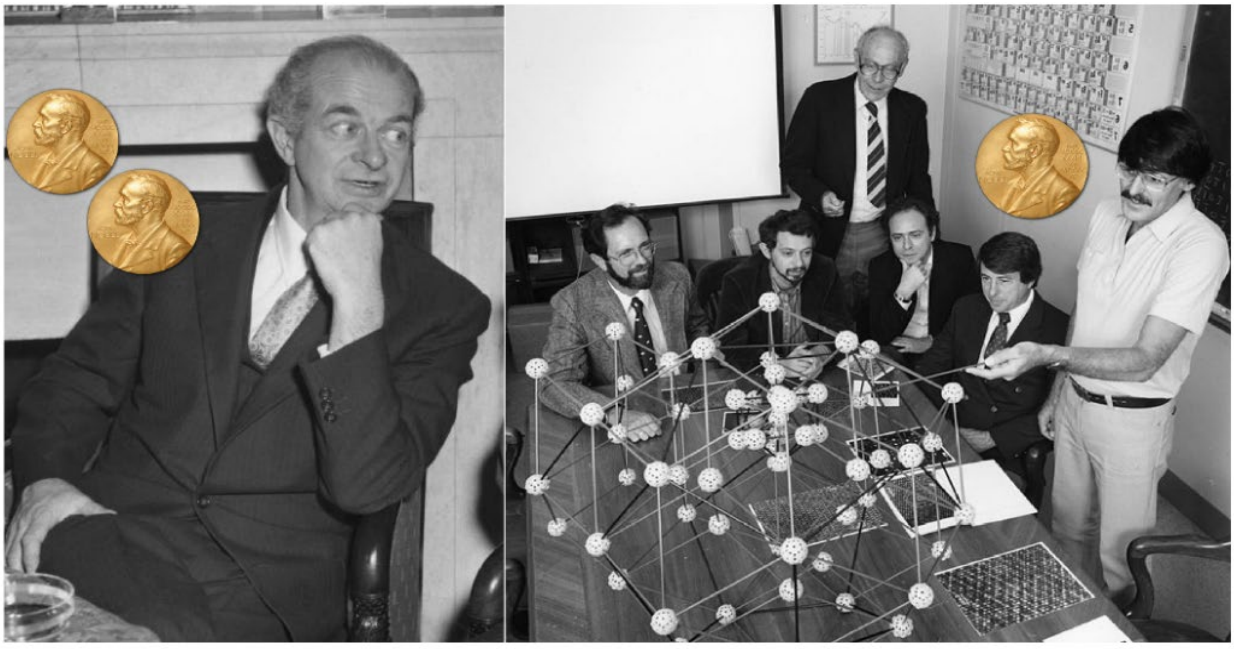
When Shechtman first presented his data and conclusions in his research group at NIST, the head of his group told this 40-years-old scientist (who was at the same time also a professor Israel Institute of Technology Technion):

*"Go back and read the textbook."*

A few days later, he asked Shechtman to leave NIST, as he was "bringing a disgrace to the team." From the available resources, it wasn't completely clear to me whether, at the time when he published results two years later, he was fired from NIST or just on a sabbatical.

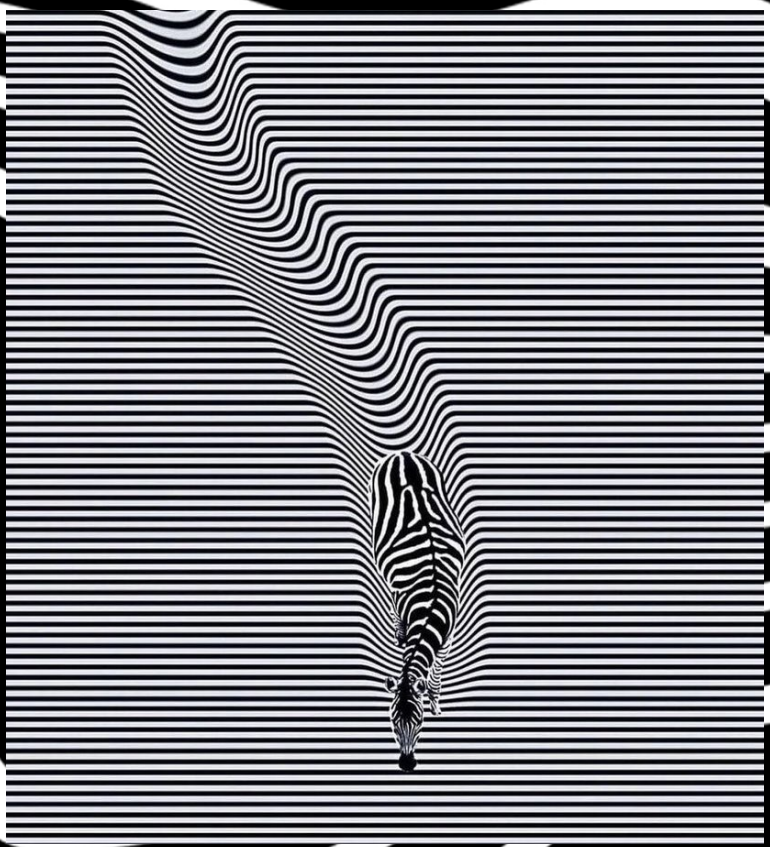
Shechtman didn't give up and was still confidently presenting his finding at conferences, Pauling is now famously quoted for exclaiming in front of hundreds of other scientists: [6]

*"There are no such things as quasicrystals, there are only quasi-scientists."*



Linus Pauling (left) and Dan Shechtman (right)

https://www.cantorsparadise.com/nobel-prize-to-guy-who-another-laureate-said-is-not-a-real-scientist-654b50a85aed



Research Article Vol. 9, No. 10 / October 2022 / Optica 1121

# Fully integrated four-channel wavelength-division multiplexed QKD receiver

Fabian Beutel,[1,2,3] Frank Brückerhoff-Plückelmann,[1,2] Helge Gehring,[1,2] Vadim Kovalyuk,[4,5] Philipp Zolotov,[5,6] Gregory Goltsman,[4,5,6] and Wolfram H. P. Pernice[1,2,7,8,*]

[1]University of Münster, Institute of Physics, 48149 Münster, Germany
[2]Center for Nanotechnology (CeNTech), 48149 Münster, Germany
[3]Pixel Photonics GmbH, Heisenbergstr. 11, 48149 Münster, Germany
[4]Department of Physics, Moscow Pedagogical State University, Moscow, Russia
[5]Russian Quantum Center, Skolkovo 143025, Moscow, Russia
[6]National Research University Higher School of Economics, Moscow 101000, Russia
[7]Center for Soft Nanoscience (SoN), 48149 Münster, Germany
[8]Kirchhoff-Institut für Physik, Heidelberg University, 69120 Heidelberg, Germany
*Corresponding author: wolfram.pernice@uni-muenster.de

Received 27 June 2022; revised 12 August 2022; accepted 31 August 2022; published 30 September 2022

**Quantum key distribution (QKD) enables secure communication even in the presence of advanced quantum computers. However, scaling up discrete-variable QKD to high key rates remains a challenge due to the lossy nature of quantum communication channels and the use of weak coherent states. Photonic integration and massive parallelization are crucial steps toward the goal of high-throughput secret-key distribution. We present a fully integrated photonic chip on silicon nitride featuring a four-channel wavelength-division demultiplexed QKD receiver circuit including state-of-the-art waveguide-integrated superconducting nanowire single-photon detectors (SNSPDs). With a proof-of-principle setup operated at a clock rate of 3.35 GHz, we achieve a total secret-key rate of up to 12.17 Mbit/s at 10 dB channel attenuation with low detector-induced error rates. The QKD receiver architecture is massively scalable and constitutes a foundation for high-rate many-channel QKD transmission.** 

https://doi.org/10.1364/OPTICA.468982

## 1. INTRODUCTION

Quantum key distribution (QKD) as a means to distribute secret keys among two distant parties in a provably secure way has come a long way since its first publication [1], with various protocols and experimental demonstrations for both continuous variables and discrete variables [2,3]. In order to sustain the security promise of the original idea, the generated keys should be used as a one-time pad [4,5], thereby implying that the length of the generated secret key must match the length of the data to be transmitted. While data rates for classical communication are continuously increasing, achieving high secret-key rates remains a challenge due to the lossy nature of fiber links and the lack of suitable quantum repeaters.

Multiple speedup strategies are available to further scale up secret-key rates: Optimizations of the underlying protocols and the right set of parameters for a given transmission setup can significantly increase efficiency. The recent development of twin-field QKD [6] is one example of progress toward higher key rates at large channel attenuation, which, however, comes with strongly increased experimental complexity [7–9]. Continuous-variable QKD (CV-QKD), on the other hand, is a promising candidate for achieving higher key rates, yet practical implementations suffer from complex and slower post-processing as well as excess noise in the quantum channel and are, therefore, limited to shorter distances than discrete-variable QKD (DV-QKD) in practice [10,11].

Optimizing the properties of the devices and setups, such as the signal-to-noise ratio of the sending module and the loss of the measurement circuitry, as well as signal-to-noise ratio of the single-photon detectors is another approach. However, with detection efficiencies beyond 90% and dark count rates (DCRs) below 10 Hz [12], headspace for further improvements in the underlying detector technology is rather limited. Alternatively, an increase in the clock rate can translate to a linear increase in the secret-key rate and, therefore, significantly improved data rates. However, when operating beyond 10 GHz, the challenges in realizing low-noise signal generation, synchronization, and dispersion control grow dramatically and subsequently lead to stark increase in hardware cost.

A promising option for significant speedups is massive parallelization of the quantum communication bandwidth via signal multiplexing, analog to well-established concepts in classical signal processing. Wavelength-division multiplexing (WDM) is attractive as it allows for a large number of multiplexed channels (unlike polarization-division multiplexing) and can be realized using

single-mode fiber optic cables and components (unlike mode-division multiplexing). While multiple previous implementations use WDM to mix a classical synchronization and communication channel over the same fiber as the quantum channel [13,14], WDM can also be used to combine multiple quantum channels [15,16]. So far, however, limiting factors have been the number of single-photon detector channels, which are a key requirement for the implementation of DV-QKD experiments, as well as the growing complexity of a many-channel circuitry.

Photonic integration plays a crucial role in overcoming these challenges, as it allows for alignment-free and stable readout circuits while keeping the overall footprint of the setup at a minimum and could, therefore, lead to monolithic chips implementing all the functionality needed for parallel multi-channel QKD signal generation and detection [15,17–20]. While the integration of the sender side and partially the receiver side on active platforms such as InP has shown significant progress [21], we have only recently demonstrated the first fully integrated photonic receiver module, which includes waveguide-integrated single-photon detectors on the chip and eliminates the need for additional interfaces between the readout circuitry and the photon detection [22]. In this work, we demonstrate the first fully integrated multi-channel QKD receiver by combining highly efficient fiber-to-waveguide couplers, low-loss wavelength-division demultiplexing, a delay-line interferometer (DLI), and waveguide-integrated superconducting nanowire single-photon detectors (SNSPDs) on a single silicon nitride ($Si_3N_4$) chip. We achieve Mbit/s secret-key rates even at channel attenuations corresponding to more than 100 km of fiber and, therefore, demonstrate the suitability of QKD for securing sensitive and bandwidth-intensive communication channels.

## 2. RESULTS

### A. Protocol and Implementation

QKD protocols that encode information in the degrees of freedom of time and relative phase between pulses are well suited for implementing wavelength-division multiplexed QKD schemes because the wavelength does not directly bear any information as part of the underlying protocol. A multiplexed scheme, as shown in Fig. 1(a), can be realized by utilizing multiple signal generators, which can, for example, consist of a CW laser, intensity modulator (IM), phase modulator (PM), and attenuators, and combining them into a single channel. The need for explicit WDM components can be circumvented by using a well-characterized $1 \times n$ fiber splitter since the loss on the sender side is typically irrelevant due to the strong attenuation that needs to be applied to the signal before leaving Alice's safe environment.

For this work, we use a three-state time-bin protocol, in which the generated signal consists of a random sequence of states $Z_0$, $Z_1$, $X_+$, where $Z_0$ and $Z_1$ are a pulse in the early and late half of a time slot, respectively, and $X_+ = \frac{1}{\sqrt{2}}(Z_0 + Z_1)$ is the superposition state. Each symbol is sent with a randomly chosen mean photon number $\mu \in \{\mu_1, \mu_2\}$.

On the receiver side, a single DLI can be shared among the channels as long as the interferometric visibility over the spanned wavelength range is sufficiently high. In this configuration, wavelength-division demultiplexers (DEMUXs) can be placed at the Z-output of the passive basis-selection splitter and at the output of the DLI. It has been shown that monitoring only the destructive interference output of the DLI is sufficient to generate secret keys [23]; therefore, only two identical demultiplexers are needed, as shown in Fig. 1(a). The output of each demultiplexer channel is connected to a single-photon detector, and signal going through the DLI is used to gather statistics on the interference behavior of transmitted pulses and allows the deduction of information about the presence of a potential eavesdropper; the bit string is typically collected by the main detector.

For the experimental implementation in this work, all the optical components needed for the receiver device are realized on an integrated $Si_3N_4$ platform with an overall footprint of $1.5 \times 1.5\ mm^2$ as shown in Fig. 1(b). Light is coupled into waveguides via 3D total internal reflection (TIR) couplers, which offer vertical coupling and have previously shown to be wavelength insensitive and highly efficient [24]. Via a directional coupler acting as a passive basis selection splitter, about 85% of the incoming light is forwarded directly into the on-chip DEMUX and then fed to a SNSPD, which is used to measure the data bits of the transmitted key.

The remaining 15% of the incoming light is tapped and forwarded into a DLI, where one arm contains a delay line. By choosing an appropriate clock rate, when a superposition state is sent, part of the early pulse will be delayed such that it arrives at the output at the same time as the non-delayed part of the late pulse, thereby yielding destructive interference at one of the output ports in the minimum wavelength.

The resulting signal is then forwarded through the DEMUX onto a second SNSPD. In this way, only one DLI is used for all four wavelength channels. Because the free spectral range (FSR) of the DLI is much smaller than the channel spacing and width, the operating wavelength within each channel can be chosen such that optimal destructive interference at the output channel of the DLI is achieved.

For realizing the DEMUX, we choose serially coupled ring resonators and an add-drop configuration, as described in the next section. Because each of the resonator structures has four ports (input, through, add, drop) and behaves completely reciprocal, one ring resonator chain can serve as a single demultiplexer for both the main detection channel and the DLI detection channel, where the through-port acts as input port for the DLI channel. Thereby, the overall footprint is reduced, and the signal paths experience exactly the same filter spectrum and are, therefore, insensitive to slight fabrication variations that would otherwise create discrepancies between the main and DLI path.

The chip is fabricated in a multi-step electron-beam lithography (EBL) process on a 330 nm $Si_3N_4$ on insulator substrate. To minimize waveguide loss, the sample is annealed at 1100°C for four hours before a superconducting NbN layer with a nominal thickness of 4 nm is sputter-deposited. The gold contact pads and alignment markers are deposited via physical vapor deposition (PVD) and patterned using a lift-off process. Nanowires are subsequently patterned and etched in a CF4 atmosphere and passivated with a thin HSQ protection layer in order to protect the surface and sidewalls during subsequent fabrication steps. Photonic waveguides are reactive-ion etched in a CHF3 atmosphere. Finally, an 800 nm thick HSQ cladding is applied to the waveguide structures for reduced propagation loss. Finally, the 3D TIR fiber-to-chip couplers are printed in a direct-laser writing step, where $Si_3N_4$ markers act as alignment structures.

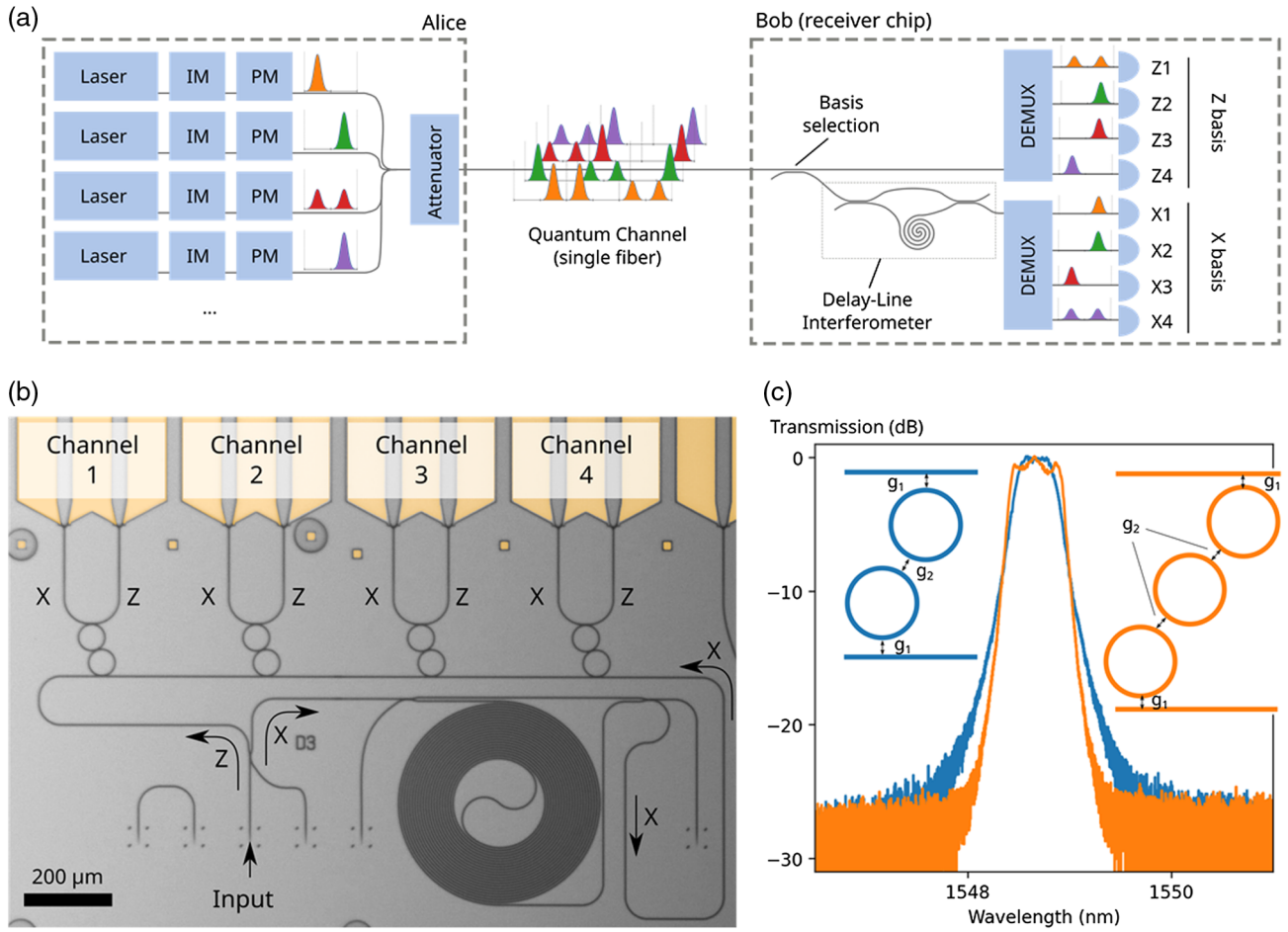



**Fig. 1.** *Protocol and receiver chip*. (a) Time-based QKD protocols are well suited for wavelength-division multiplexing. A single delay-line interferometer (DLI) on the receiver side can be shared among many wavelength channels, thereby greatly reducing the needed overall footprint and complexity. (b) False-color microscope image of the receiver chip for four-channel time-bin QKD protocols. The DLI is shared among all for wavelength channels. We further utilize the symmetry of ring resonators in an add-drop configuration; therefore, only a single wavelength filter is needed per channel. (c) Comparison of the transmission spectrum of serially coupled two- and three-ring filters.

### B. Photonic On-Chip Components

While single ring resonators already offer wavelength-selective filtering, it has been shown that coupling multiple resonator structures serially or in parallel can significantly improve the filter characteristics, where the filter quality grows with the number of coupled rings [25–28]. However, concatenating many rings bears challenges due to fabrication inaccuracies and can lead to additional instabilities.

The gaps between the rings are optimized by experimentally sweeping parameters for devices on a separate chip prior to implementation of the final sample.

Figure 1(c) shows the comparison of two serially coupled ring resonator filters with two ($g_1 = 170$ nm, $g_2 = 550$ nm) and three ($g_1 = 150$ nm, $g_2 = 450$ nm) rings, respectively, where the rings in each chain are completely identical. A minimal insertion loss of $0.9 \pm 0.2$ dB (two rings) and $0.9 \pm 0.3$ dB (three rings) was measured in the sample devices. While the three-ring variant shows steeper filter characteristic, it is more challenging to achieve a flat top and, therefore, low loss over the full channel width, as can be seen from the ripples around the maximum. Depending on the requirements of the protocol and other components involved, the use of three- and higher-order ring resonator chains might be warranted. Moreover, steeper falloff of the filter edges allows the wavelength channels to be packed more tightly. For our proof-of-principle implementation with relatively large channel spacing, both variants have been fabricated and evaluated for use in a QKD measurement.

The FSR and channel width are directly influenced by the ring radius $r$, with the relation $\mathrm{FSR} \approx \lambda^2/(2n_g\pi r)$ [29], where $n_g$ is the effective group index. The relative positioning of the channels to each other is achieved by slightly increasing the ring radius for each channel by 40 nm, yielding a wavelength channel spacing of approximately 1.8 nm.

The top (bottom) of Figure 2(a) shows the system detection efficiency (SDE) of the single-photon detectors behind each filter channel in the final device 1 (device 2) with two rings (three rings) when CW light is sent through the input port. The SDE includes the insertion loss from all receiver components as well as the fiber-to-chip coupling interface and, therefore, directly translates to the achievable secret-key rate of the device.

The single-photon detectors on the chip consist of superconducting NbN nanowires deposited on top of the $Si_3N_4$ waveguides. By tuning the geometric parameters of the nanowires, they can be optimized for the targeted operating conditions: while a long and relatively narrow nanowire yields high absorption as well

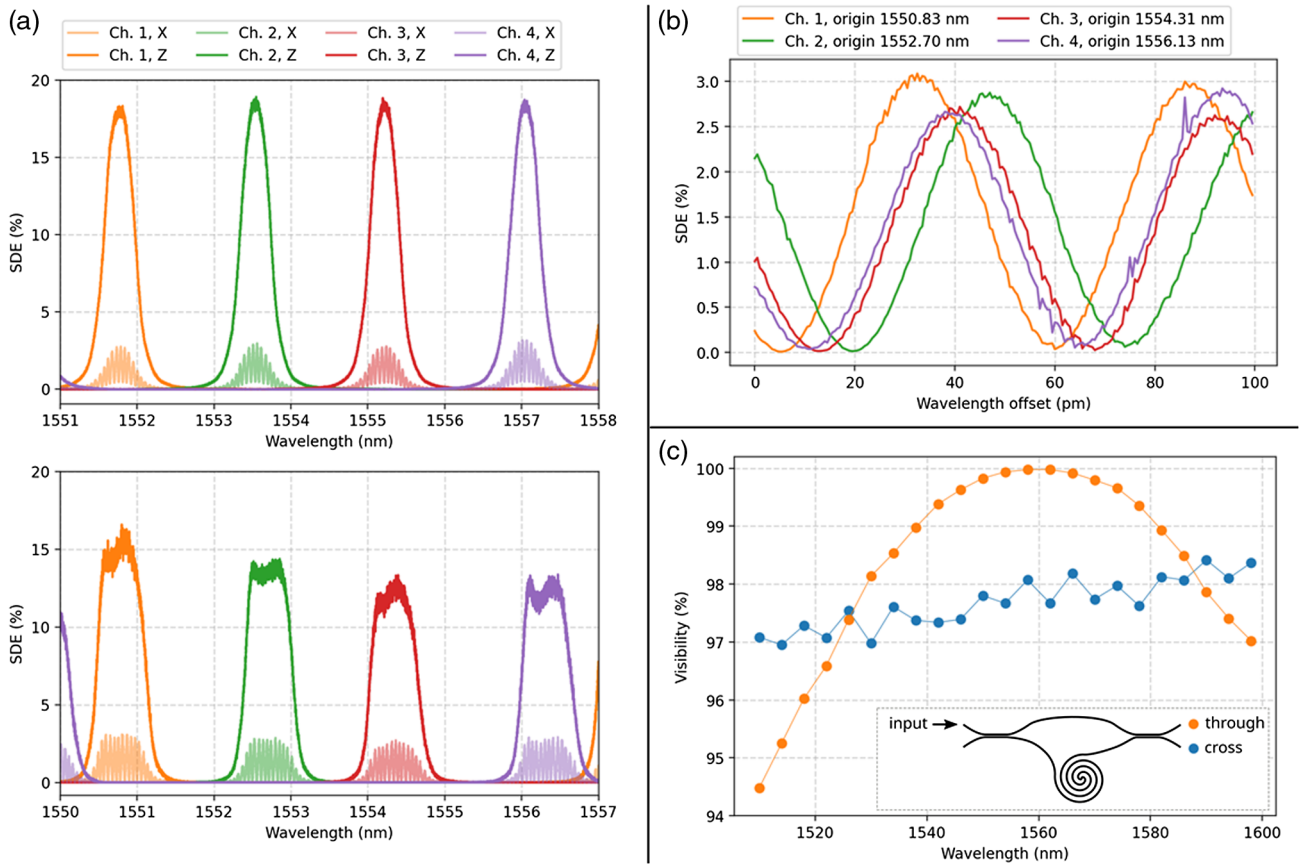



**Fig. 2.** *Filter and DLI characteristics*. (a) System detection efficiency (SDE) of the eight detectors versus wavelength for a device with two rings (device 1, top) and three rings (device 2, bottom). The main channel detectors (Z) feature system detection efficiencies between 13% and 19%. This includes all loss accumulated through the fiber-to-chip couplers as well as all optical elements on the chip. SDE of the X basis detectors is considerably lower because the passive basis selection splitter only forward about 15% into the DLI. (b) SDE versus wavelength for the X basis SNSPDs of device 2. (c) Visibility of the DLI as measured through the characterization ports. The cross port (diagonal to the input of the DLI) only shows a weak wavelength dependence compared to the through port. All QKD measurements are performed with the cross port.

as high internal quantum efficiencies, it suffers from longer reset times than a shorter and wider nanowire [30].

For the purpose of this work, we chose nanowire lengths of 120 μm and a wire width of 90 nm for all detectors. For each nanowire, the critical current is characterized, and the detector is subsequently operated at around 80% of the critical current during the QKD measurements. This ensures that dark counts are at mostly negligible levels of below 40 Hz for all channels. For the devices under test, we find optimal bias currents between 16 and 21 μA.

As shown in Fig. 2(a), the maximum SDE for each $Z$ channel SNSPD is between 13% and 19%. For the detectors receiving the signal from the DLI ($X$ basis), the maximum SDE is between 2.5% and 3.1%. The much lower SDE in this case is consistent with the on-chip basis selection splitter after the input coupler, which only forwards about 19% into the DLI and the non-negligible waveguide loss caused by the on-chip delay line. All reported numbers are measured at a wavelength where constructive interference inside the DLI occurs.

QKD protocols such as the coherent one-way protocol or the three-state time-bin protocol [31,32] utilize a Mach–Zehnder DLI in order to overlay consecutive pulses for interference measurements. If the packing of symbols, each consisting of an early and a late time slot, is dense in the time domain, then the needed delay time is exactly half of the symbol length. Therefore, the needed delay line length decreases with increasing clock rate. In this way, the footprint and also the propagation loss in the DLI are reduced, making higher clock rates attractive for a fully integrated solution. The delay line in our case is designed for a group delay of 150 ps, which corresponds to approximately 2 cm and yields a FSR of $54.3 \pm 0.8$ pm [Fig. 2(b)].

The final operating clock rate for the QKD transmission is experimentally optimized by varying the frequency of a sinusoidal laser signal set to the destructive interference wavelength of the DLI. Minimum count rates at the X-basis detectors were observed for a signal frequency of 6.71 GHz (6.70 GHz) for device 1 (device 2), and the symbol rate for the QKD protocol was chosen accordingly.

With an estimated waveguide loss of around 0.4 dB/cm, a spiral length of 2 cm leads to a significant reduction in the extinction ratio of the DLI. Therefore, the splitting ratio of the input splitter is slightly adjusted such that more light is coupled into the delay line arm of the DLI. In this setup, the extinction ratio of the output diagonal to the input ("cross") only weakly depends on the absolute splitting ratios of the DLI splitters, as shown in Fig. 2(c), while the other DLI output ("through") exhibits a much stronger wavelength dependence due to the wavelength-sensitive directional couplers. As long as the operating wavelength of each channel is

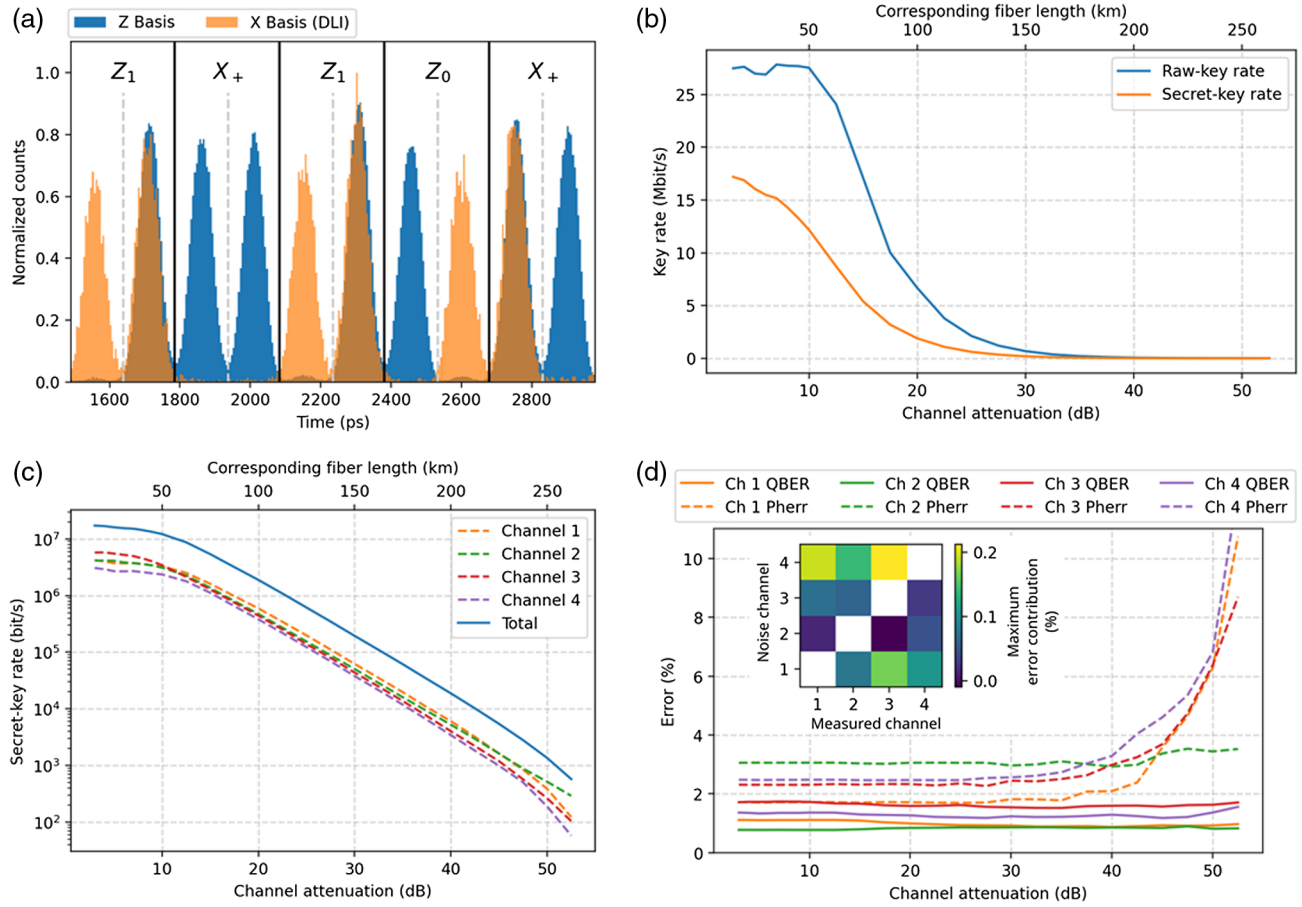



**Fig. 3.** *QKD results*. (a) Excerpt of the recorded histogram of the Z-SNSPD (blue) and the X-SNSPD (orange) for channel 1. Destructive interference can be seen when two consecutive pulses are sent ($X_+$ or a $Z_1$, $Z_0$ sequence). (b) Total raw-key rates and secret-key rates of the system. The key rates are not monotonically decreasing for low attenuation levels because at high incident count rates the detectors for channels 3 and 4 latch at lower rates than channels 1 and 2. (c) Logarithmic plot of the secret-key rate for all channels individually as well as the total secret-key rate of the system. A maximum secret-key rate of 6.84 Mbit/s is achieved at 7 dB channel attenuation and 4.97 Mbit/s at 10 dB. (d) Quantum bit-error rate (QBER) and phase error rate (Pherr) for each channel. QBER is below 2.1% for all channels until 55 dB channel attenuation. The phase error is significantly higher due to the imperfect interferometric visibility of the DLI. Inset, maximum increase of QBER when a QKD transmission on a channel is performed ("measured channel") while noise on a different wavelength channel ("noise channel") with an intensity corresponding to a real QKD signal is sent. The maximum error contribution is 0.2% and well within the uncertainty levels of the reported QBER.

freely tunable within the FSR of the DLI, both outputs can be used as destructive interference output. On the one hand, using the through output, therefore, would allow countering inaccuracies in the loss estimation or fabrication by moving the operating wavelength to the point with the best extinction ratio. For the purpose of this work, however, the cross output proved to be sufficient and was used for the sake of greater wavelength independence over a broad bandwidth.

The maximum visibility around 1550 nm when measured with the SNSPDs was $(92.1 \pm 0.9)\%$ for device 1 and $(97.8 \pm 0.5)\%$ for device 2. The difference can be attributed to fabrication variations. The QKD measurements were conducted for device 2, as the better visibility allows for the achievement of lower phase error rates.

### C. Experimental QKD Transmission

We perform several proof-of-principle measurements with the receiver module by sending a pseudo-random 512-bit pattern signal onto the chip. The signal is generated on Alice's side using a bit-pattern generator (BPG) connected to electro-optical IMs acting on a CW laser signal at the operating wavelength.

The BPG bit rate is set to a bit rate double that of the symbol rate such that each sample point corresponds to a time slot with two time slots per symbol. The separate CLOCK output of the BPG produces a sinusoidal signal with the frequency equal to the bit rate of the BPG. By setting an appropriate delay between CLOCK and DATA output and modulating the optical with a second EOM driven by the CLOCK output, light will only pass through the second EOM in the center of a time slot when the sine function reaches its maximum. Thereby, a good extinction ratio and signal quality are achieved.

The signal is then strongly attenuated to the decoy intensities of $\mu_1 \in [0.1, 0.8]$ and $\mu_2 \in [0.02, 0.17]$ photons per symbol, respectively. A global channel attenuation between 0 and 60 dB is simulated using a fiber attenuator.

For each channel attenuation, a histogram is recorded for all channels, an excerpt of which is shown in Fig. 3(a). The histogram is triggered by the start of the bit pattern, and an artificial delay is adjusted for each detector signal individually. From this, the

quantum bit-error rate (QBER) and the phase error rate can be calculated by comparing the histogram with the original pattern, and the achievable secret-key rate under the given operating conditions and channel attenuation can be measured. By summing the rates of the individual channels, a total raw-key rate of up to 27.51 Mbit/s (where the raw-key rate denotes the rate after sifting, but before post-processing) and a secret-key rate of 12.17 Mbit/s at 10 dB channel attenuation was demonstrated [Fig. 3(b)]. This number is obtained by considering contributions from histograms corresponding to the same channel attenuation but different mean photon number per pulse $\mu_1$ and $\mu_2$, weighted with the probability to select the corresponding decoy intensity. In our calculations, we also consider and correct for finite-key effects with an assumed block size of $10^9$ and a security parameter $\varepsilon = \varepsilon_{\mathrm{sec}} = \varepsilon_{\mathrm{cor}} = 10^{-9}$.

The maximum achievable key rates saturate toward lower channel attenuations as the detectors limit the maximum count rate. However, while the raw-key rate is already fully saturated at 7 dB with a maximum value of 27.83 Mbit/s, the secret-key rate increases to a maximum of 17.19 Mbit/s at 3 dB channel attenuation. This is driven by the use of lower $\mu_1$ and $\mu_2$, which benefits the secret fraction, which can be extracted from the sifted key.

QBER and phase error rate are measured and evaluated for each channel individually, as plotted in Fig. 3(d). The QBER is below 2% for the entire measurement range with a slight increase at very low and very high attenuation levels. The phase error rate is slightly higher for all channels with a mean value of $(2.4 \pm 0.5)\%$ for attenuation below 40 dB, which can be attributed to the imperfect interferometric visibility of the DLI itself.

While only one channel is characterized at a time, we also study cross talk behavior by mixing the generated signal with a second CW laser set to the wavelength of a different channel and with the power set to a level as would be the case in a multiplexed QKD setup. The combined signal then leaves Alice's setup, and the same simulated channel attenuation is applied. Any cross talk should, therefore, exhibit no relation to the actual pattern and yield perfectly random noise characteristics, which would not be the case when the same pattern would be sent to different channels at the same time. No significant effect on the error rates of the other channels has been measured, which is consistent with the good extinction ratio between the channels for a CW signal as seen in Fig. 2(a). For obtaining upper bounds on the effect, we plot the maximum contribution to the QBER over all measured channel attenuation levels for each combination of two channels in the inset of Fig. 2(d). The maximum contribution was measured to be 0.25% and can be considered to be well within the uncertainty levels.

The system's long-term stability was tested in a long-term measurement by repeatedly sweeping the wavelength and measuring the visibility of the interferometer over the course of 24 h in the same cryogenic temperature-controlled environment at $(1.32 \pm 0.2)$ K as was used for the QKD measurements. Small fluctuations of the visibility of $\pm 1\%$ can be observed. The shift of the optimum destructive interference wavelength is also monitored and shows a maximum offset of 6 pm relative to the starting wavelength over the full measurement time, which is a small deviation compared to the FSR of the spiral. The effect can easily be countered by regularly optimizing the transmission wavelengths every few hours during the run of an experiment.

## 3. DISCUSSION

The device presented in this work combines several optimized photonic components to achieve high key rate QKD over a wide range of channel attenuations: first, we utilize broadband and highly efficient fiber-to-chip couplers, which allows operation of the device far beyond the optical bandwidth that was demonstrated in this work, thereby allowing hundreds of wavelength channels to be packed onto a single chip.

By using only a single DLI, which is the single largest photonic component on the chip, shared among all channels, the overall size of the device can be kept as small as possible. Furthermore, because of the long waveguide contained in the DLI, the potential for fabrication defects is significantly reduced if only one delay line is necessary per device and, therefore, beneficial for the overall yield. Similarly, by only monitoring one output of the DLI and utilizing the add-drop configuration of the ring resonators, only one filter is needed per channel, bringing similar benefits.

Finally, waveguide-integrated single-photon detectors have been shown to offer excellent timing resolution (jitter) below 20 ps [33] together with high efficiency over a broad bandwidth and low DCR [24]. A low average QBER of $(1.1 \pm 0.3)\%$ over the full measurement range and a maximum channel QBER of only 2.1% for channel 4 at 55 dB channel attenuation particularly indicates that the DCR plays no significant role in the error. At very low channel attenuations below 10 dB, on the other hand, a small increase in QBER can be observed for some channels, as can be seen in Fig. 3(d).

We attribute this to an increase in the number of events with temporal spacing smaller than the full recovery of a detector. At that point, consecutive pulses of the SNSPD will overlap, and the electrical signal arriving at the time tagger has a different shape; therefore, the trigger level and operating point are not optimal anymore, leading to a small but measurable increase in the error rate.

Below 40 dB, a mean phase error rate of $(2.4 \pm 0.5)\%$ was measured. Unlike the QBER, the phase error shows a significant increase for all channels for attenuation levels beyond 40 dB. This can likely be attributed to the much lower number of events that count toward the calculation of the phase error rate due to the splitting ratio of the basis selection splitter and the additional waveguide loss caused by the DLI. The signal-to-noise ratio is, therefore, lower than for the Z basis measurements, and the effect of detector dark counts becomes significant at lower attenuation levels as compared to the QBER. The phase error rate could be further improved by optimizing the DLI, as described above, or by connecting the through-port of the DLI and operating at an optimized wavelength [see Fig. 2(d)].

For all QKD measurements in this work, a physical quantum channel was realized using a fiber attenuator instead of a field-deployed fiber. While this gives the flexibility to easily measure for many different attenuation levels, it neglects further effects that are expected from deployed fiber links of the corresponding length, such as dispersion effects and polarization drift [34]. However, polarization-maintaining fibers or active stabilization have previously been implemented in the context of QKD and can also be added per wavelength channel, if necessary. As the sender requires active per-channel modulation (as opposed to the receiver) and on-chip polarization modulation has been previously demonstrated [18], active polarization stabilization can be best included on the sender side.

The dead time of the single-photon detectors typically imposes an upper limit on the achievable key rates. In the case of SNSPDs, the nanowires can enter a latching state when the incident photon rate becomes too big. While the mean photon number per symbol is well below 1 for all measurements, the high clock rate of 3.35 GHz leads to a significant photon influx when the applied channel attenuation is low. The use of relatively short waveguide-integrated SNSPDs with low dead times of around 10 ns is, therefore, a key advantage as compared to meander-shaped SNSPDs or other single-photon detector technologies, which often exhibit much smaller maximum count rates [30]. This is especially attractive for metropolitan networks or relatively short fiber and free-space links. For the results reported in this work, significant detector saturation was only observed below 10 dB. For measurements below 10 dB, where latching reduced the achieved transmission rates significantly, the results from higher-attenuation measurements with maximum key rates are projected instead. This is equivalent to artificially applying additional attenuation when the quantum channels are so low that detector saturation would otherwise occur and can be easily implemented in a real-word QKD setup.

While the secret-key rates reported in this work are, to the knowledge of the authors, already higher than any previously reported results utilizing wavelength-multiplexed DV-QKD, the receiver architecture presented herein also is an important foundation for further up-scaling toward GHz key rates. The realization and operation of large-scale waveguide-integrated SNSPD arrays has been demonstrated, and a massive increase in the number of channels is, therefore, realistic [35].

While the FSR of the ring filters used in this work prevents the use of more than four channels with the current parameters and without additional components, several options are available for increasing the number of channels of the QKD demultiplexer: because the FSR of the DLI is much smaller than the channel spacing, the latter could be further reduced in order to fit more channels into the same wavelength range. However, as discussed above, an increase in the clock rate is attractive for achieving even higher per-channel key rates. This leads to an increase of the DLI's FSR and, thus, also increases the lower limit for the channel spacing. Alternatively, by changing the ring parameters and possibly including different-sized rings within a chain of serially coupled or parallel coupled rings, wavelength-selective filters with much larger FSR are possible [36], albeit requiring high fabrication precision and reproducibility.

The approach we propose instead is the use of a hybrid multiplexing scheme, where additional Bragg gratings are used as coarse pre-filter, as shown in Fig. 4(a). Apodized Bragg gratings

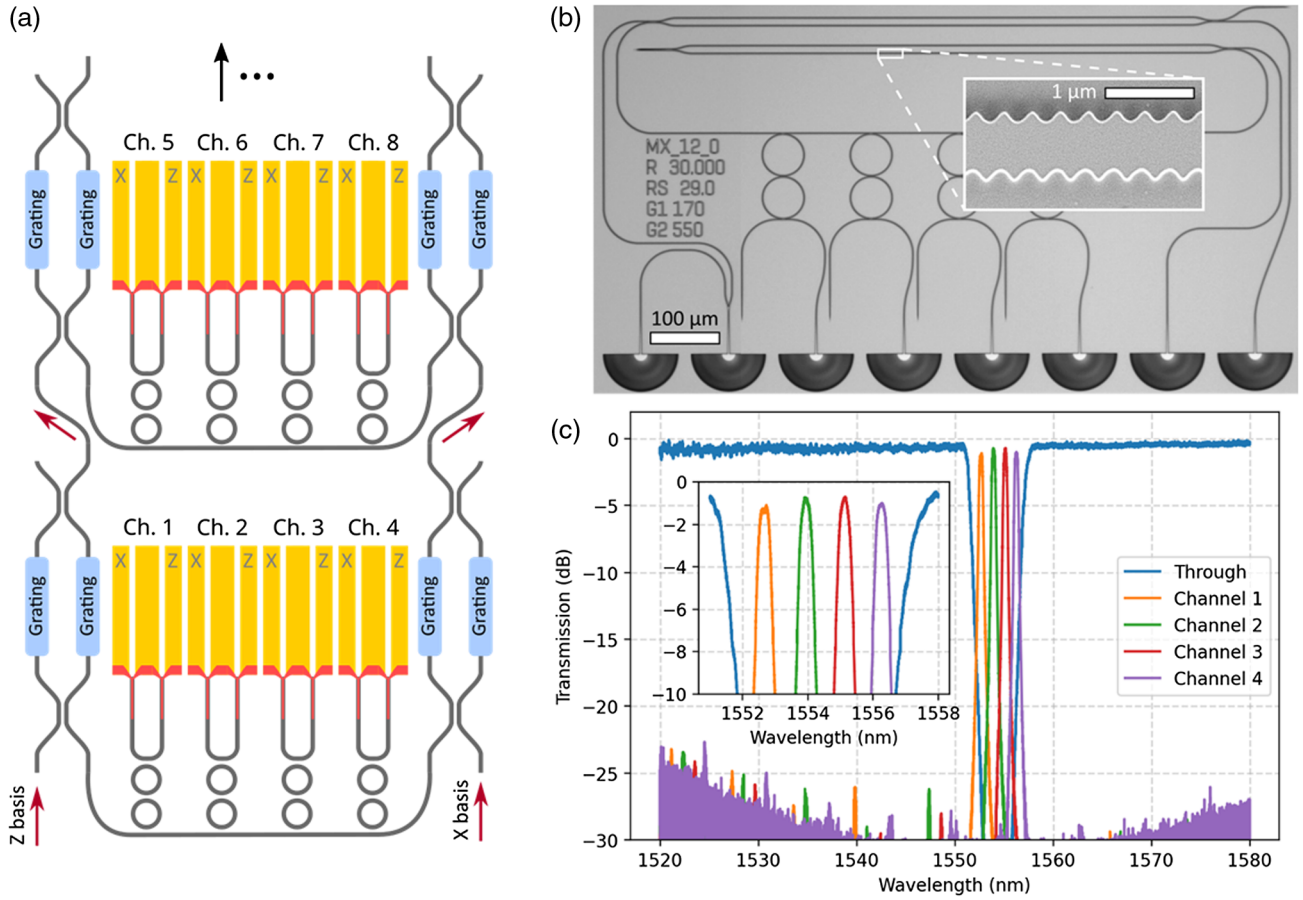



**Fig. 4.** *Up-scaling to many channels.* (a) Ring resonator filters can be combined with apodized Bragg gratings in a Mach–Zehnder configuration as a hybrid multiplexing scheme. The light passes through the coarse Bragg filters before the dense wavelength demultiplexing is performed by the ring resonators. A high number of channels can be realized in this way, where the delay-line interferometer and basis selection can be shared among all channels. (b) Microscope image of a test structure implementing a hybrid demultiplexer. The gratings are 735 µm long. Inset, SEM image of the grating. (c) Measured spectrum of the test device. Insertion loss of less than 1.5 dB for all channels is maintained (inset), while suppression of side peaks of the ring resonators is better than 23 dB over a range of 60 nm.

are positioned in a Mach–Zehnder configuration and act as bandpass filters, as described in more detail in previous works [37]. The Bragg multiplexers divide the full wavelength range in coarse channels, where the bandwidth is similar to that of the FSR of the ring resonators. Dense wavelength-division demultiplexing is subsequently performed by cascaded ring resonators as described above. We characterize a proof-of-principle implementation of the scheme with the photonic circuit depicted in Fig. 4(b) and achieve a maximum insertion loss of 1.5 dB while a suppression of side peaks of more than 23 dB over a wavelength range from 1520 to 1580 nm is maintained [Fig. 4(c)].

## 4. CONCLUSION AND OUTLOOK

With the implementation presented in this work, we demonstrate a viable way forward toward increased secret-key rates by parallelizing QKD using WDM and operation at GHz clock speed. We demonstrate a four-channel fully integrated detector module, where all photonic components needed for the state measurement and wavelength-division demultiplexing are realized on chip. This drastically reduces the complexity and allows for greater scalability as compared to the use of discrete components. A set of benchmark measurements is used to quantify the maximum throughput of the QKD receiver, and secret-key rates of more than 10 Mbit/s at more than 10 dB channel attenuation are demonstrated. The novel WDM-QKD architecture presented here employs ring resonators for wavelength filtering and an on-chip DLI, as well as state-of-the-art waveguide-integrated superconducting single-photon detectors, allowing for high count rates at extremely low noise levels.

Furthermore, we show that the architecture can be easily scaled up to higher channel numbers with the use of a hybrid multiplexing scheme where Bragg gratings are utilized as broad pre-filters. The architecture is, therefore, a promising candidate for the realization of miniaturized, massively scalable high-performance QKD receivers.

## APPENDIX A: METHODS

### A.1. Fabrication

The base substrate consists of a 500 μm Si/3.3 μm $SiO_2$/330 nm $Si_3N_4$ stack, which is annealed at 1100°C for four hours. Subsequently, a 4 nm NbN layer is sputter-deposited. Preliminary optimization of the deposition process allowed us to obtain the critical temperature $T_c = 9.7$ K, with a sheet resistance $R_s = 420\,\Omega/\mathrm{Sq}$ and residual resistivity ratio (RRR) of 0.74. Gold structures (markers and contact pads) are fabricated using a 350 nm PMMA mask, which is patterned with a 100 kV EBL system (Raith EBPG5150), which is used for all subsequent fabrication steps as well. 5 nm Cr (adhesion layer) and 80 nm Au are deposited using physical vapor deposition and shaped in a lift-off process. Nanowires are written in 120 nm HSQ on top of a 5 nm $SiO_2$ adhesion layer. Photonic structures are exposed using arN-7520.12 with a thickness of 320 nm. Finally, a HSQ layer of 800 nm is spin-coated and exposed with a buffer of 10 μm around all photonic structures except for the areas around the fiber-to-chip interface, where 3D-printed coupling structures are fabricated using a direct-laser writing process (Nanoscribe Professional GT) in the last step.

### A.2. Measurement Setup

The sample is mounted on a XYZ-movable cryo-compatible stage (Attocube) inside a 1.32 K closed-cycle helium cryostat. A standard single-mode fiber array (SMF-28) is used for the optical interface, while an eight-port RF probe (Cascade Microtech Unity Probe) is used for the electrical contacts. All ports are connected to the outside using stainless-steel RF lines, where each detector is connected to the electrical readout and biasing circuit: a bias-tee (ZFBT-6GW+, 100 kHz–6 GHz) separates the DC bias current input from the RF path. The fast voltage pulses generated by the SNSPDs propagate through the RF path through two cascaded low-noise amplifiers (2 × ZFL-1000LN+) and are forwarded to a time tagger (Swabian Instruments Time Tagger Ultra), where events from each channel are recorded as described in the main text.

On the sender side, a bit-pattern generator (BPG, Agilent 81141A) is used to generate a repeating pattern consisting of 512 bits with a bit rate of 6.7 GHz. A trigger signal is generated at the start of each pattern and connected to a free port of the time tagger.

The CLOCK output of the BPG, which produces a sinusoidal signal with a frequency matching the bit rate, is connected to an amplifier (ZX60-83LN-S+) and a bias-tee (ZFBT-6GW+) such that a separate DC bias can be applied to the electro-optical modulator (EOM, Optilab IML-1550-40-PM-V). The DATA output with a signal amplitude of 1.8 V is not amplified in order to protect the lower frequency components of the signal, but it is sent through a bias-tee (ZFBT-6GW+) and to a second EOM (Optilab IML-1550-40-PM-V). A time delay is set between the clock and data such that each maximum of the clock signal falls on a sample point of the bit pattern.

The optical signal is generated by a tunable CW laser (Santec TSL-710) and propagates through a polarization controller, which is used to optimize transmission through the EOMs. Both EOMs are connected via polarization-maintaining fibers. Finally, the signal is attenuated to the targeted signal intensity and then combined with a secondary CW laser signal, which is used to quantify the channel cross talk as described in the main text. The combined signal is sent through another polarization controller for optimizing the fiber-to-chip coupling, passes through a second attenuator for simulating the channel attenuation, and is then split by a 50:50 splitter. One arm of the signal is going to a calibrated power meter (HP 81635A), while the other output is connected to the input fiber going into the cryostat. See Supplement 1 for a more detailed description of the sender setup.

### A.3. QKD Measurements

For the estimation of the achievable secret-key rates, each channel is initially characterized individually. First, a fine wavelength sweep is conducted while recording the count rate in both detectors of each channel in order to find the optimal operating wavelength yielding high SDE and strongest destructive interference of the DLI. The bias current for the SNSPDs for each channel is swept while monitoring the count rate to find the optimum operating current. The sender setup is optimized by sweeping the clock rate around the expected optimum while recording the phase error rate for channel 1. Similarly, the bias voltages for the two EOMs are optimized by monitoring the bit- and phase error rates. Settings

of the sender setup are reused for all channels. The QKD measurement is then conducted by recording a 30 s histogram for each channel attenuation level, with the mean photon number set to $\mu = 0.1$. Higher (lower) values for $\mu$ can be obtained by using the corresponding recordings with lower (higher) applied channel attenuation during post-processing. The secondary, unmodulated CW laser is set to the operating wavelength of a different channel and attenuated such that its signal power corresponds to $\mu = 0.1$ photons per pulse and passes through the same channel attenuator as the primary laser, thereby simulating the operation of a different channel with random signal. Histograms are recorded for each combination of primary and secondary channels as well as without the secondary channel active. Calculation of the secret-key rate then follows the process as described in [38].

**Funding.** H2020 Future and Emerging Technologies (101017237); HORIZON EUROPE European Research Council (724707); Russian Science Foundation (21-72-10117).

**Acknowledgment.** V. K., Z. P., and G. N. acknowledge support of the RSF (NbN films deposition, optimization, and testing). W. P. acknowledges funding from ERC and EU H2020.

**Disclosures.** The authors declare no conflicts of interest. The authors declare no competing interests.

**Data availability.** Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

**Supplemental document.** See Supplement 1 for supporting content.

## REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: quantum key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.
2. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
3. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
4. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**, 656–715 (1949).
5. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
6. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
7. Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution through sending or not sending," Phys. Rev. Lett. **123**, 100505 (2019).
8. S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," Phys. Rev. X **9**, 021046 (2019).
9. X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," Phys. Rev. Lett. **123**, 100506 (2019).
10. M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," NPJ Quantum Inf. **4**, 21 (2018).
11. X. Wang, S. Guo, P. Wang, W. Liu, and Y. Li, "Realistic rate–distance limit of continuous-variable quantum key distribution," Opt. Express **27**, 13372–13386 (2019).
12. F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," Nat. Photonics **7**, 210–214 (2013).
13. I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, H. Griesser, M. Eiselt, C. Chunnilall, G. Lepert, A. Sinclair, J.-P. Elbers, A. Lord, and A. Shields, "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," Opt. Express **22**, 23121–23128 (2014).
14. N. Walenta, A. Burg, D. Caselunghe, *et al.*, "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," New J. Phys. **16**, 013047 (2014).
15. D. Bunandar, N. Harris, Z. Zhang, C. Lee, R. Ding, T. Baehr-Jones, M. Hochberg, J. Shapiro, F. N. Wong, and D. Englund, "Wavelength-division multiplexed quantum key distribution on silicon photonic integrated devices," presented at APS March Meeting 2018, Los Angeles, California (5-9 March 2018).
16. A. B. Price, P. Sibson, C. Erven, J. G. Rarity, and M. G. Thompson, "High-speed quantum key distribution with wavelength-division multiplexing on integrated photonic devices," in *Conference on Lasers and Electro-Optics* (OSA, 2018), paper JTh2A.24.
17. Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," NPJ Quantum Inf. **3**, 25 (2017).
18. C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).
19. H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," Optica **7**, 238–242 (2020).
20. P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**, 172–177 (2017).
21. A. Orieux and E. Diamanti, "Recent advances on integrated quantum communications," J. Opt. **18**, 083002 (2016).
22. F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, and W. Pernice, "Detector-integrated on-chip QKD receiver for GHz clock rates," NPJ Quantum Info. **7**, 40 (2021).
23. D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, "Security proof for a simplified BB84-like QKD protocol," Phys. Rev. A **98**, 052336 (2018).
24. M. A. Wolff, F. Beutel, J. Schütte, H. Gehring, M. Häußler, W. Pernice, and C. Schuck, "Broadband waveguide-integrated superconducting single-photon detectors with high system detection efficiency," Appl. Phys. Lett. **118**, 154004 (2021).
25. T. Barwicz, M. A. Popovic, P. T. Rakich, M. R. Watts, H. A. Haus, E. P. Ippen, and H. I. Smith, "Microring-resonator-based add-drop filters in SiN: fabrication and analysis," Opt. Express **12**, 1437–1442 (2004).
26. G. Griffel and S. Arnold, "Synthesis of variable optical filters using meso-optical ring resonator arrays," in *Conference Proceedings. LEOS '97. 10th Annual Meeting IEEE Lasers and Electro-Optics Society 1997 Annual Meeting* (IEEE, 1996), Vol. **2**, p. 165.
27. B. E. Little, S. T. Chu, H. A. Haus, J. Foresi, and J.-P. Laine, "Microring resonator channel dropping filters," J. Lightwave Technol. **15**, 998–1005 (1997).
28. A. Melloni, "Synthesis of a parallel-coupled ring-resonator filter," Opt. Lett. **26**, 917–919 (2001).
29. W. Bogaerts, P. De Heyn, T. Van Vaerenbergh, K. De Vos, S. Kumar Selvaraja, T. Claes, P. Dumon, P. Bienstman, D. Van Thourhout, and R. Baets, "Silicon microring resonators," Laser Photon. Rev. **6**, 47–73 (2012).
30. S. Ferrari, C. Schuck, and W. Pernice, "Waveguide-integrated superconducting nanowire single-photon detectors," Nanophotonics **7**, 1725–1758 (2018).
31. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," Appl. Phys. Lett. **87**, 194108 (2005).
32. A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," Appl. Phys. Lett. **112**, 171108 (2018).
33. W. H. P. Pernice, C. Schuck, O. Minaeva, M. Li, G. N. Goltsman, A. V. Sergienko, and H. X. Tang, "High-speed and high-efficiency travelling

wave single-photon detectors embedded in nanophotonic circuits," Nat. Commun. **3**, 1325 (2012).
34. J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, "Stability of high bit rate quantum key distribution on installed fiber," Opt. Express **20**, 16339–16347 (2012).
35. M. Häußler, R. Terhaar, M. A. Wolff, H. Gehring, F. Beutel, W. Hartmann, N. Walter, M. Tillmann, M. Ahangarianabhari, M. Wahl, T. Röhlicke, H.-J. Rahn, W. H. P. Pernice, and C. Schuck, "Scaling waveguide-integrated superconducting nanowire single-photon detector solutions to large numbers of independent optical channels," arXiv:2207.12060 (2022).
36. G. Griffel, "Vernier effect in asymmetrical ring resonator arrays," IEEE Photon. Technol. Lett. **12**, 1642–1644 (2000).
37. F. Brückerhoff-Plückelmann, J. Feldmann, H. Gehring, W. Zhou, C. D. Wright, H. Bhaskaran, and W. Pernice, "Broadband photonic tensor core with integrated ultra-low crosstalk wavelength multiplexers," Nanophotonics 4063–4072 (2022).
38. D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis on the 1-decoy state QKD protocol," Appl. Phys. Lett. **112**, 171104 (2018).