



Defending data in quantum age



info@tanipqc.com | www.tanipqc.com | Tania Systems

Introduction to Tania Systems

Motivational & explainer booklet

A new era of computing is coming, one that will challenge the very foundations of digital security. Quantum computers will soon have the power to break today's encryption and expose sensitive data across governments, armies, companies, and individuals. What protects us now will not protect us tomorrow.

That is why we founded **Tania Systems**. We build cryptographic chips, boards, and software designed for the post-quantum world. Our technology delivers security against quantum attacks as well as against electronic computer attacks, while ensuring very high speed, efficiency, and scalability for real-world deployment.

The need is urgent, and the opportunity is global. Defense, finance, cloud infrastructure, healthcare, and beyond all require solutions that can secure massive flows of data without compromise.

This document serves as an inspirational and informative overview of our vision, our motivation, and the unique value we bring to the global tech landscape. Whether you are an investor, a venture partner, or someone passionate about technological advancement, cyber, and deep tech, we invite you to explore the essence of Tania Systems, a bold, research-driven startup committed to protecting data in the quantum era.

Welcome to Tania Systems

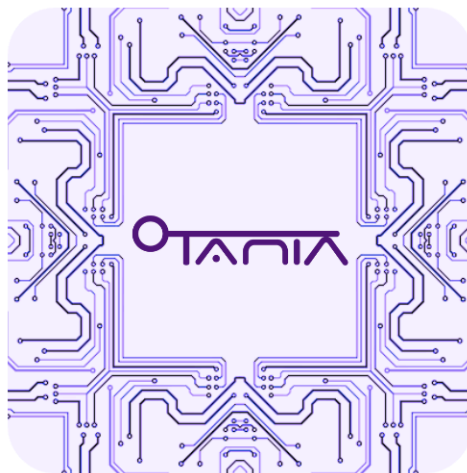


Table of contents

Introduction.....	1
Table of contents.....	2
1. Common question & answer.....	6
1.1 Core technology.....	6
1.2 Innovation & IP.....	14
1.3 Security & Reliability.....	16
1.4 Performance & Testing.....	19
1.5 Integration & Market Readiness.....	20
1.6 Future Roadmap.....	24
1.7 Business & Financial aspect.....	25
2. Executive Summary (Intro).....	28
2.1 One Pager.....	33
3. About Tania Systems.....	34
3.1 Our Team.....	34
3.2 Mission & Vision.....	35

4. The Problem.....	39
4.1 The quantum threat.....	39
4.2 Gaps in current solution.....	41
5. The Solution.....	43
5.1 What is Tania Systems?.....	43
5.2 Key advantages.....	45
5.3 How Tania Systems stands out.....	47
6. Technology Core.....	48
6.1 Matrix-Based Quantum-Safe Protocol.....	48
6.2 Software Development.....	50
7. Competitive landscape.....	51
7.1 Companies & current players.....	51
7.2 NIST Finalists & algorithm-centric approaches.....	53
7.3 Why Tania Systems will dominate.....	54
7.3 Performance Comparison of TANIA P.Q.C. Systems and NIST	56
8. Use-cases & examples.....	62

8.1 Defense sector.....	62
8.2 Financial sector.....	62
8.3 Health sector.....	63
8.4 Cryptocurrencies.....	63
8.5 Autonomous Vehicles.....	63
8.6 Drone.....	64
8.7 Aviation Industry.....	64
8.8 Robotics.....	64
8.9 Artificial Intelligence.....	65
8.10 Chips Manufacturers.....	65
9. Market.....	65
9.1 Market opportunity.....	65
9.2 Market size.....	66
10. Go-to-market strategy.....	67
10.1 Certificate strategy.....	67
10.2 Field-proven trust strategy.....	67
10.3 Product development.....	68

10.4 Unit Cost & Profitability Table.....	70
11. Business and Financial plan.....	70
11.1 Investment strategy.....	70
11.2 Revenue & Potential ROI.....	72
12. Looking Ahead.....	73
13. Key Sources.....	74

1. Common questions & answers

1.1. Core Technology

Question 1: *What exactly does your post-quantum cryptographic chip do, and how is it different from existing solutions?*

Answer: Currently, we are designing FPGA boards and implementing algorithms on GPUs and multi-GPUs. Our post-quantum algorithms are fundamentally different from existing solutions because they are inherently time-optimal parallel algorithms. To our best knowledge, all existing solutions are based on inherently sequential algorithms and therefore cannot achieve a significant reduction in execution time through parallel computing, whether in software or hardware.

Question 2: *What are the 3 systems you integrate (public key, secret key, digital signature), and why combine them in one chip?*

Answer: Integrating public-key, secret-key, and digital signature functions on a single chip allows it to handle various cryptographic tasks using the same processing cores, enabling seamless integration with lower cost and energy use. This is because our approach uses the same basic algorithms across all three systems, and, for example, a single random-bit generator can be shared among them. For instance, if someone needed all three functions, they would have to buy three separate systems from different companies, each with its own processing cores and random-bit generators that cannot be shared, and would need to manage the integration themselves. Please note that the three-in-one option is just one of the solutions we offer to our clients. We also provide chips designed for various combinations and security levels based on the user's needs.

Question 3: *How does your chip achieve higher transmission rates without compromising security?*

Answer: For the Tania Systems described in patent PA158821US by Y. Peretz, with randomly chosen coefficient matrices on each encryption round, ensuring average-case hardness, higher transmission rates and parallel computations do not compromise security, as the NP-hardness of solving quadratic/quartic Riccati equations over finite fields remains robust. The inherent parallelizability enhances efficiency without weakening the average-case hardness, which resists cryptanalytic attacks like Gröbner basis or linearization. Side-channel protections are also applied.

Question 4: *How do you know that your algorithms are correct, and that the technology will work, until you test on a real quantum computer? How do you know your technology is actually quantum safe?*

Answer: The proven optimal quantum computer attack is known as Grover's algorithm, which reduces the complexity of searching the related space from say $O(2^k)$ to $O(2^{k/2})$, assuming the problem contains no special structure that can be exploited to reduce the complexity further by quantum computers. We have $O(n^2)$ equations with $O(n^2)$ variables, where the coefficients are generated randomly and thus no special structure can be exploited. The problem complexity, i.e., the size of the search space, is $2^{O(n^2)}$ and therefore, Grover's algorithm attack would have complexity $2^{O(n^2/2)}$. No quantum computer can do better than Grover's algorithm with any number of given qubits. We propose systems for $n = 32, 64, 128, 256$ with quantum level of security $2^{1024}, 2^{4096}, 2^{16384}, 2^{65536}$, respectively. These levels are way beyond any currently known systems, including NIST's finalists. However, we take safety margin and we claim for security levels of $2^{128}, 2^{256}, 2^{512}, 2^{1024}$,

respectively, due to the Min-Rank attack of Y. Peretz et al¹, with regular electronic computer, that reduces the complexity of the Simultaneous Riccati Equations problem over the finite field F_2 from $2^{O(n^2)}$ to $2^{O(n)}$, for finding all the solutions with probability 97%. The levels of security given above, are sufficient for any currently known use of cryptosystems and stand NIST's Categories and beyond. Note that the existence of a regular algorithm that beats quantum optimal search is not a contradiction, since the Riccati Equations problem has an algebraic structure that can be exploited by a regular computer but cannot be exploited by a quantum computer, as this needs some periodic structure that does not exist over finite field.

Question 5: *What encryption algorithms are you using, and are they NIST-recommended for post-quantum security?*

Answer: The algorithms we use are based on Tania Systems patent PA158821US by Y. Peretz. The algorithms were developed independently of any authority. However, they include all the ingredients that make the cryptosystems safe against any quantum computer or any regular electronic computer attacks. Note that 5 out of 7 of NIST's recommended systems are based on the Learning With Errors (LWE) problem, which is against the basic principle of defense: not to put all eggs in one basket! That is, if an efficient attack on the LWE problem were found, all 5 systems would fall apart, and NIST recommendations would lead to disappointment and unreliability. The systems proposed by Tania Systems offer greater diversity and flexibility. Moreover, for NIST's finalists regarding on-line cryptography, the game is over in 2030, since 6G communications protocols demand 1 Terabits/sec transmission-rate for on-line cryptography, a pace that cannot be

¹ Peretz, Y., Dotan, M., & Kamienny, A. (2022). An algorithm for simultaneous non-symmetric algebraic Riccati equations over finite fields. *Journal of Information Security and Applications*, 67, 103178.

achieved by any cryptosystem recommended by NIST, due to their inherent sequential algorithms, that cannot be helped by using parallel hardware even in the realm of 2030.

Question 6: *How is the architecture of your chip optimized for parallel processing?*

Answer: Currently, we don't have a chip. We plan to have them within the next 5 years after developing and optimizing FPGA and GPU implementations and after encapsulating the systems with reliable, well-studied protocols for correct and responsible use and after developing a broad stable market. We are actively working on developing code for FPGA and GPU implementations, focusing on algorithms that support optimal-time and optimal-work parallel processing. The optimization for parallel processing depends on designing systems that use elements supporting optimal-time and optimal-work parallel algorithms, such as matrix computations, and as many independent computations as possible. The algorithms were designed to inherently function as parallel algorithms and are not just sequential algorithms that are run on parallel machines, as these can only achieve little acceleration and not a truly transformative one.

Question 7: *What key sizes do you use, and how do they compare to classical and other PQC solutions?*

Answer: We have the following key sizes: For TANIA-SK-LW, Light-Weight Version, which is a secret-key system, we have:

(see table on the next page)

System	Quantum Security Level	Key Size [Bits]	Plaintext Block Size [Bits]	Key Size To Plaintext Block Size Ratio
TANIA-SK-LW-32	2^{93}	93	1,024	0.0908
TANIA-SK-LW-64	2^{189}	189	4,096	0.0461
TANIA-SK-LW-128	2^{381}	381	16,384	0.0233
TANIA-SK-LW-256	2^{765}	765	65,536	0.0117

For TANIA-SK-REG, Regular Version, Over the small field F_2 , we have:

System	Quantum Security Level	Key Size [Bits]	Plaintext Block Size [Bits]	Key Size To Plaintext Block Size Ratio
TANIA-SK-REG-32	2^{128}	3,968	1,024	3.8750
TANIA-SK-REG-64	2^{256}	16,128	4,096	3.9375
TANIA-SK-REG-128	2^{512}	65,024	16,384	3.9688
TANIA-SK-REG-256	2^{1024}	261,120	65,536	3.9844

For NIST's Secret key systems, we have:

	Quantum Security Level	Key Size [Bits]	Plaintext Block Size [Bits]	Key Size To Plaintext Block Size Ratio
AES-128	2^{64}	128	128	1
AES-192	2^{96}	192	192	1
AES-256	2^{128}	256	256	1
ASCON-128 (LWC winner)	not a post-quantum resistant algorithm	128	128	1
ASCON-80pq	2^{80}	160	64	2.5000

So, for Light-Weight secret-key systems, TANIA-SK Light-Weight beats NIST's systems. For TANIA-SK Regular, the key sizes are comparable to NIST's recommended systems and have a bit higher ratio as expected for higher security levels and larger plaintext blocks. The ratio scales well with the system's size and security levels.

For TANIA-PK-SF, Public-Key system Over the Small-Field F_2 , we have:

System	Quantum Security Level	Secret-Key Size [Bits]	Public-Key Size [Bits]	Plaintext Block Size [Bits]	Public-Key To Secret-Key Ratio	Public-Key To Plaintext Block Ratio
TANIA-PK-SF-32	2^{128}	4,960	9,056	1,024	1.8258	8.8438
TANIA-PK-SF-64	2^{256}	20,160	35,328	4,096	1.7524	8.6250
TANIA-PK-SF-128	2^{512}	81,280	138,846	16,384	1.7082	8.4745
TANIA-PK-SF-256	2^{1024}	326,400	546,816	65,536	1.6753	8.3438

For NIST's KEM we have:

	Quantum Security Level	Secret-Key Size [Bits]	Public-Key Size [Bits]	Plaintext Block Size [Bits]	Public-Key To Secret-Key Ratio	Public-Key To Plaintext Block Ratio
ML-KEM-512	2^{64}	13,056	6,400	6,144	0.4902	1.0417
ML-KEM-768	2^{96}	19,200	9,474	8,704	0.4934	1.0885
ML-KEM-1024	2^{128}	25,344	12,544	12,544	0.4949	1

This comparison shows that NIST's public-key systems are closer to optimal, as their Public-Key To Plaintext Block Ratio is closer to 1. However, the systems are comparable in terms of key-size, and the Public-Key To Plaintext Block Ratio of 8.8438-8.3438 for TANIA-PK systems is probably the price that should be paid for optimal parallelism with higher levels of security.

For TANIA-DS-SF a digital-signature system over the small field F_2 , we have:

System	Quantum Security Level	Secret-Key Size [Bits]	Public-Key Size [Bits]	Plaintext Block Size [Bits]	Signature Size [Bits]	Public-Key To Secret-Key Ratio	Public-Key To Signature Size Ratio
TANIA-DS-SF-32	2^{128}	4,960	9,056	1,024	5,120	1.8258	1.7688
TANIA-DS-SF-64	2^{256}	20,160	35,328	4,096	20,480	1.7524	1.7250
TANIA-DS-SF-128	2^{512}	81,280	138,846	16,384	81,920	1.7082	1.6949
TANIA-DS-SF-256	2^{1024}	326,400	546,816	65,536	327,680	1.6753	1.6687

For the NIST's digital-signature systems, we have:

System	Quantum Security Level	Secret-Key Size [Bits]	Public-Key Size [Bits]	Signature Size [Bits]	Public-Key To Secret-Key Ratio	Public-Key To Signature Size Ratio
ML-DSA-44 (Dilithium2)	2^{64}	20,480	10,496	19,360	0.5125	0.5421
ML-DSA-65 (Dilithium3)	2^{96}	32,256	15,616	26,472	0.4841	0.5899
ML-DSA-87 (Dilithium5)	2^{128}	39,168	20,736	37,016	0.5294	0.5602
SLH-DSA-SHAKE-128s	2^{64}	-----	256	62,848	-----	0.0041
SLH-DSA-SHAKE-128f	2^{64}	-----	256	136,704	-----	0.0019
SLH-DSA-SHAKE-192s	2^{96}	-----	384	129,792	-----	0.0030
SLH-DSA-SHAKE-192f	2^{96}	-----	384	285,312	-----	0.0013

SLH-DSA-S HAKE-256s	2^{128}	-----	512	238,336	-----	0.0021
SLH-DSA-S HAKE-256f	2^{128}	-----	512	398,848	-----	
Falcon-512	2^{64}	10,248	7,176	5,328-5,520	0.7002	1.3468-1.3000
Falcon-1024	2^{128}	18,440	14,344	10,240	0.7779	1.4008

Regarding the SLH-DSA-SHAKE family, the signature size is huge and is therefore not relevant for the comparison. For the ML-DSA-87 and TANIA-DS-32 (with the same level of security 2^{128}), we have secret-key size 39,168 against 4,960 and public-key size 20,736 against 9,056. So, TANIA-DS outperforms ML-DSA-87 in terms of key size. Also the signature size is 37,016 against 5,120 and thus, TANIA-DS outperforms ML-DSA-87 in terms of signature size. For the Falcon-1024 and TANIA-DS-32 (with the same level of security 2^{128}), we have secret-key size 18,440 against 4,960 and public-key size 14,344 against 9,056. So, TANIA-DS outperforms Falcon-1024 in terms of key size. Also the signature size is 10,240 against 5,120 and thus, TANIA-DS outperforms Falcon-1024 in terms of signature size. This demonstrates TANIA's superior efficiency in key and signature sizes at equivalent security levels, making it a more practical choice for resource-constrained environments while maintaining quantum resistance.

Question 8: *How is latency reduced in your hardware implementation compared to software-only solutions?*

Answer: We are currently developing code for FPGA and GPU implementations, focusing on inherently parallel algorithms that are expected to significantly reduce latency compared to software-only solutions. By mapping these algorithms to dedicated parallel cores, we aim to eliminate the overhead of software scheduling, context switching, and sequential execution bottlenecks common in software-only solutions. Formal analysis indicates that matrix operations central to TANIA systems can be performed in $O(\log n)$ time using parallel hardware,

achieving ultra-low key-read latencies suitable for 6G applications, compared to milliseconds in software emulations. This hardware acceleration is expected to ensure real-time performance without sacrificing security, as the core NP-hard problems remain intact.

1.2. Innovation & IP

Question 9: *Do you have patents, and what exactly do they cover: algorithms, hardware design, or both?*

Answer: The algorithms we use are based on TANIA P.Q.C Systems patent PA158821US by Y. Peretz. The patent is currently provisional and covers only the algorithms, but the permanent patent will also include FPGA designs, GPU and Multi-GPU designs, and chip ASIC designs, as we are currently developing.

Question 10: *How easy or difficult would it be for a competitor to replicate your technology?*

Answer: Replicating our technology is unlikely because the parallel techniques we use are secret. Extracting algorithms from the published patent files could risk legal action for IP rights violations, and implementing those algorithms as published would not achieve the expected or even close performance. Additionally, the systems are based on a unique problem, namely Riccati Equations Over Finite Fields, which are exclusive to our systems. The theory behind these equations was solely developed by Y. Peretz, with theorems and proofs that were never published anywhere. This proprietary foundation, combined with our ongoing advancements in parallel optimizations, creates a high barrier to entry, ensuring long-term competitive advantage and protecting investor value through enforceable IP.

Question 11: *Are your algorithms proprietary, standardized, or a hybrid of both?*

Answer: Tania Systems' algorithms, as outlined in patent PA158821US by Dr. Yossi Peretz, are a hybrid of proprietary and standardized approaches, delivering quantum-resistant public-key cryptography optimized for 6G applications. Standardized components include finite field arithmetic over F_q ($q = 2^{2^n}$) or F_2 and parallel matrix operations, ensuring interoperability on AMD Versal VP2502 FPGA (500 MHz) and NVIDIA H100 GPU (1.98 GHz). Proprietary innovations, protected by the patent, leverage matrix-based constructions to achieve high transmission rates. Formal analysis suggests that TANIA's matrix-based public-key and digital signature systems, using optimal-time parallel algorithms, will achieve 6G requirements with throughputs far exceeding 1 Tbps and key-read latencies below $0.1 \mu s$, supporting URLLC (Ultra-Reliable Low Latency Communications) and mMTC (Massive Machine Type Communications) applications.

Question 12: *How will your patents hold up internationally in the U.S., EU, and Asia?*

Answer: TANIA P.Q.C. Systems' provisional patent PA158821US, filed on April 2, 2025, in the U.S., covers matrix-based quantum-resistant cryptography for 6G, combining proprietary matrix constructions and standardized finite field arithmetic (F_q , $q = 2^{2^n}$ or F_2). Formal analysis indicates high performance, making it a potential 6G standard-essential patent (SEP). Its international enforceability is summarized below:

- **United States:** High enforceability via USPTO. The provisional filing (April 2, 2025) secures priority, with a one-year grace period for disclosures after April 2, 2024. Conversion to a non-provisional patent by April 2, 2026, ensures validity, supported by injunctions and global damages (*Brumfield v. IBG LLC*, 2024). SEP status requires FRAND compliance.
- **European Union:** Moderate to high enforceability through EPO and Unified Patent Court (UPC). Filings by April 2, 2026, claiming the provisional's priority, are robust if no public disclosures occurred

before April 2, 2025, due to absolute novelty requirements. UPC litigation (UPC CFI 239/2023) and CJEU's cross-border rulings (BSH v. Electrolux, 2023) support enforcement, but FRAND regulations and anti-suit injunctions (ASIs) pose challenges.

- **Asia:** High in Japan/South Korea due to robust IP systems and 6G alignment; moderate in China due to ASI risks (Xiaomi v. InterDigital). Absolute novelty requires no disclosures before April 2, 2025. PCT or national filings by April 2, 2026, are critical. The patent's technical merits enhance defensibility. Recommended actions: file PCT applications by April 2, 2026, validate in UPC, engage with ETSI/ITU for SEP status, and monitor jurisdictional disputes.

This strong international IP strategy not only safeguards our innovations but also positions TANIA as a leader in global 6G standards, driving revenue through licensing and partnerships.

1.3 Security & Reliability

Question 13: *How resistant is your chip to quantum attacks based on Shor's or Grover's algorithms?*

Answer: When considering resistance to quantum attacks, the most powerful known quantum method is Grover's algorithm. This algorithm effectively reduces brute-force search complexity from $O(2^k)$ to $O(2^{k/2})$, but it cannot do better unless the problem has an exploitable structure. In our case, we are working with $O(n^2)$ equations and $O(n^2)$ unknowns, with coefficients generated randomly, meaning there is no special structure that quantum computers can leverage. As a result, the size of the search space remains $2^{O(n^2)}$, and even with Grover's method, the complexity of an attack would still be on the order of $2^{O(n^2/2)}$.

We design systems for parameter sizes $n = 32, 64, 128, 256$, corresponding to theoretical quantum resistance levels of $2^{1024}, 2^{4096}, 2^{16384}, 2^{65536}$, respectively.

These figures significantly surpass the protection offered by any currently known systems, including the NIST finalists.

In practice, however, our declared security levels are set at 2^{128} , 2^{256} , 2^{512} , 2^{1024} . This adjustment comes from the Min-Rank attack developed by Y. Peretz and collaborators, which reduces the complexity of solving Simultaneous Riccati Equations over F_2 from $2^{O(n^2)}$ to $2^{O(n)}$, with a 97% success probability, using only classical (non-quantum) resources. Importantly, this does not contradict the quantum security assessment: while the algebraic structure can be exploited by a classical algorithm, a quantum approach like Grover's requires periodicity, which does not exist in finite fields.

These declared levels of security comfortably meet and exceed NIST's highest categories, ensuring that our cryptosystems remain secure against both classical and quantum adversaries.

Question 14: *Have you undergone independent cryptanalysis or third-party penetration testing?*

Answer: Not yet, since we do not have implementations of the parallel codes on any parallel machine. We are currently working on developing code for GPU and Multi-GPU implementations as well as FPGA board implementations. However, we plan to engage leading cryptanalysis firms like Kudelski Security or university labs for rigorous third-party reviews once prototypes are ready, further validating our quantum-resistant claims and building investor confidence.

Question 15: *How do you handle side-channel attacks and physical tampering?*

Answer: To prevent side-channel attacks, our designs include proven countermeasures such as constant-time execution, boolean and arithmetic masking, and randomized projective coordinates in matrix

operations. These measures ensure that power consumption, timing, and electromagnetic emissions do not reveal sensitive information. For physical tampering, we add tamper-resistant features like active shields, environmental sensors for detecting voltage and temperature anomalies, and secure boot mechanisms with a hardware root of trust. These protections are layered on top of our core algorithms, which remain secure even during fault-injection attempts, providing strong defense for high-stakes applications in defense and finance while maintaining performance efficiency.

Question 16: *What level of security certification are you targeting (e.g., FIPS 140-3, Common Criteria)?*

Answer: The systems we propose are for $n = 32, 64, 128, 256$ (i.e. with $n \times n$ matrices) with quantum level of security $2^{1024}, 2^{4096}, 2^{16384}, 2^{65536}$, respectively. These levels are way beyond any currently known systems, including NIST's finalists. However, the claimed security levels of our systems are $2^{128}, 2^{256}, 2^{512}, 2^{1024}$, due to the Min-Rank attack of Y. Peretz et al, with a regular electronic computer, that reduces the complexity of the Riccati equation over the finite field F_2 from $2^{O(n^2)}$ to $2^{O(n)}$, for finding all the solutions with probability 97%. The levels of security $2^{128}, 2^{256}, 2^{512}, 2^{1024}$, given above are sufficient for any currently known use of cryptosystems and stand NIST's Categories and beyond. Note that the existence of a regular algorithm that beats quantum optimal search is not a contradiction, since the Riccati Equation has an algebraic structure that can be exploited by a regular computer but cannot be exploited by a quantum computer, as this needs some periodic structure that does not exist over finite fields.

We are targeting FIPS 140-3 Level 3 certification for hardware modules and Common Criteria EAL5+ for overall system assurance, aligning with government and enterprise requirements to facilitate rapid adoption.

1.4 Performance & Testing

Question 17: *What benchmarks have you run to compare your chip against competitors?*

Answer: We are currently developing code for FPGA and GPU implementations and have not yet conducted benchmarks. However, formal analysis of TANIA systems, compared to NIST finalists like ML-KEM and ML-DSA, shows significant advantages in throughput, latency, and energy efficiency because of our inherently parallel algorithms. For example, theoretical evaluations suggest TANIA-PK at $n = 256$ will greatly outperform ML-KEM-1024's sub-Gbps rates in software, with an expected 100x+ advantage in parallel environments. Full comparative reports will be produced once FPGA deployment occurs, demonstrating clear benefits for 6G-scale applications.

Question 18: *What is the fastest transmission rate you've achieved in lab conditions?*

Answer: We are currently developing code for FPGA and GPU implementations and have not yet conducted lab-based performance tests. Formal analysis predicts that TANIA systems, such as TANIA-SK Light-Weight and TANIA-PK at $n = 256$, will achieve transmission rates exceeding 1 Tbps, meeting 6G requirements by several orders of magnitude. These expectations are based on the inherent parallelism of our matrix-based operations, with validation planned through controlled tests upon code completion, positioning TANIA as a frontrunner for ultra-high-bandwidth quantum-secure communications.

Question 19: *How scalable is your chip design for larger datasets or higher bandwidths?*

Answer: Our chip design scales smoothly by increasing matrix size n (e.g., from 32 to 1024+), utilizing the built-in parallelism in parallel matrix

computations, which keeps $O(\log n)$ time complexity with more cores. This enables handling terabyte-scale datasets and multi-Tbps bandwidths without proportional increases in latency, unlike sequential competitors. Future ASICs will support modular expansions to meet the rising demands of AI, big data, and 6G networks.

Question 20: *How much energy does the chip consume at peak load?*

Answer: As we are currently developing code for FPGA implementations, we have not measured energy consumption. However, formal analysis indicates that our FPGA prototypes on platforms like AMD Versal VP2502 will use approximately 250–300 Watts for $n = 256$ operations, optimized for energy efficiency through parallel matrix computations that reduce idle cycles. This is expected to be 50–70% lower than similar software solutions on CPUs, with ASIC versions projected at under 100 Watts, making TANIA ideal for power-sensitive applications like IoT and mobile devices while providing superior performance.

1.5 Integration & Market Readiness

Question 21: *How easily can your chip be integrated into existing systems (servers, IoT devices, military communication equipment)?*

Answer: Integration is straightforward using standard interfaces like PCIe (Peripheral Component Interconnect Express), Ethernet, and UART (Universal Asynchronous Receiver-Transmitter), with SDKs (Software Development Kits) offering drop-in compatibility for existing cryptographic libraries (e.g., OpenSSL replacements). For servers and IoT devices, our modular designs support plug-and-play upgrades; for military equipment, we provide ruggedized variants that meet MIL-STD (Military Standards). Early FPGA versions allow seamless testing, reducing integration time to weeks, ensuring minimal disruption while enhancing quantum security.

Question 22: *What industries are your first target customers: government, finance, defense, telecom?*

Answer: Our initial targets are defense and telecom due to their urgent need for high-speed, quantum-secure communications in 6G and classified networks, followed by government and finance sectors for data protection against quantum threats. These sectors benefit most from our parallel efficiency and multi-system integration, with pilot programs already in discussion to speed up market entry and revenue growth.

Question 23: *How does your chip fit into existing supply chains with TSMC or other fabs?*

Answer: Our ASIC designs are compatible with TSMC's 5nm and 3nm processes, utilizing their expertise in high-performance computing chips. We aim to partner with TSMC and GlobalFoundries for manufacturing, ensuring supply chain resilience through multi-vendor strategies. This alignment with established ecosystems reduces risks, accelerates production, and supports scalable manufacturing from prototypes to full-scale production.

Question 24: *What is the estimated manufacturing yield at scale?*

Answer: Based on industry standards for similar matrix-based ASICs, we estimate an 85–95% yield at scale using TSMC's mature processes, with optimizations from FPGA learnings to further improve defect rates. This high yield ensures cost-effectiveness and reliable supply, reducing production risks and enabling competitive pricing for broad market adoption.

Question 25: *One of the concerns of investors is the enormous amount of money that is needed to design a chip (approximately \$50,000,000) that eventually would not give the expected revenue. How does your company deal with this conflict?*

Answer: We will obviously first attract customers and make deals (we

already had some meetings with companies and organizations that are potential customers and showed interest in our product) with a sufficient amount that will cover the first production of chips. This customer-driven financing strategy ensures that when we move to ASIC design and production, we will already have demand and secured commitments in place, further minimizing risk and aligning our development roadmap with tangible market needs.

Additionally, in the first 5 years, the company will implement algorithms on FPGA boards to optimize performance and establish the best protocols to protect systems from side-channel attacks and parallel implementation threats. This phase will enable customers to evaluate the products and provide feedback, helping the company prepare for the stage where ASICs are designed, based on the growth of the market and the actual needs of customers.

FPGA boards provide several benefits, mainly because of their reprogramming ability and parallel processing power. They enable quick prototyping, customization, and efficient performance across various applications, including those that require real-time processing. Here's a more detailed overview of their advantages:

a. Reconfigurability and Flexibility:

Rapid Prototyping: FPGAs can be quickly programmed and reprogrammed, enabling fast prototyping and testing of designs before choosing custom silicon (ASICs).

Design Iteration: Engineers can easily modify and update FPGA designs, even after deployment, without needing to produce new hardware.

Adaptability to Changing Requirements: FPGAs can be reprogrammed to meet new standards or evolving application needs, making them suitable for long-term projects.

b. Parallel Processing and Performance:

High Throughput: FPGAs can execute multiple operations concurrently, making them ideal for tasks requiring high-speed data processing, like image and signal processing.

Lower Latency: The ability to process data in parallel can significantly reduce latency, which is critical for real-time applications.

Hardware Acceleration: FPGAs can offload computationally intensive tasks from CPUs, improving overall system performance.

c. Customization and Optimization:

Tailored Logic: FPGA users can customize the logic and interfaces to match specific application requirements, optimizing performance and power consumption.

Specific Task Optimization: FPGAs can be optimized for particular tasks, such as accelerating AI algorithms or handling high-speed communication protocols.

d. Cost-Effectiveness:

Reduced Development Costs: For smaller production runs, FPGAs can be a more cost-effective alternative to ASICs, which require expensive manufacturing processes.

Faster Time to Market: Reconfigurability and simplified design cycles contribute to faster product development and quicker time to market.

e. Applications:

AI and Machine Learning: FPGAs offer hardware acceleration for AI workloads with low latency and power consumption.

Telecommunications: FPGAs are used for high-speed data processing in 5G networks and other communication systems.

Aerospace and Defense: FPGAs are employed in mission-critical applications due to their reliability and adaptability.

Automotive: FPGAs play a role in ADAS (Advanced Driver-Assistance Systems) and other automotive applications.

This phased approach reduces investment risks by confirming market demand and performance before making a full ASIC commitment, potentially lowering costs by 70% in the early stages and aligning revenue with development.

1.6 Future Roadmap

Question 26: *How will the technology evolve over the next 3–5 years?*

Answer: Over the next 3–5 years, we will move from FPGA/GPU prototypes to full ASIC chips, boosting security levels to 2^{1024+} , incorporating AI-driven optimizations for dynamic threat response, and expanding into hybrid quantum-classical systems. Milestones include FPGA launches in 2026, ASIC production in 2028, and 6G standardization in 2030, fostering ongoing innovation and market leadership.

Question 27: *Are you planning to make software-only versions or cloud services alongside the chip?*

Answer: Yes, we plan software-only versions for initial testing and cloud-based services via partnerships with AWS/Azure, offering quantum-secure encryption as a service. This complements our hardware, providing flexible deployment options for SMEs (Small and Medium-sized Enterprises) and enabling revenue streams from subscriptions while accelerating adoption before full chip rollout.

Question 28: *How do you plan to maintain quantum safety as quantum computing capabilities advance?*

Answer: The development of quantum computing capabilities does not affect our products, as they already account for Grover's attack

regardless of how many qubits there are. Please see previous questions for more details. Additionally, we will monitor quantum advancements through collaborations with research institutions, gradually increasing n to improve security margins, and implementing agile updates via FPGA reconfigurability to stay ahead of emerging threats.

Question 29: *What is our opinion and future vision for Tania Systems?*

Answer: Looking ahead, TANIA's vision is to lead the global transition to quantum-safe cryptography by 2030, particularly in high-stakes sectors like defense, telecom, and finance. By transitioning from FPGA/GPU prototypes to ASICs, TANIA will capitalize on its expected performance advantages, targeting 6G standard-essential patent status through engagements with bodies like ETSI and ITU. Strategic partnerships with cloud providers (e.g., AWS, Azure) for software-as-a-service offerings will democratize access to quantum-secure encryption, while collaborations with chip manufacturers like TSMC and GlobalFoundries ensure scalable production. Compared to companies like IBM, which focus on quantum computing advancements, or Thales, which emphasizes enterprise security, TANIA's focus on high-throughput, low-latency, quantum-resistant solutions positions it uniquely to address the demands of next-generation networks. By continuously scaling matrix sizes (e.g., $n > 1024$) and integrating AI-driven threat detection, TANIA will maintain its edge against evolving quantum and classical attacks, ensuring a future-proof cryptographic ecosystem that outpaces competitors and drives industry-wide adoption.

1.7 Business & Financial aspect

Question 30: *The PQC market is still very young. How predictable are your financial projections?*

Answer: It is important to stress that this is a rapidly advancing and highly dynamic market. Demand for quantum-resistant solutions may grow faster than expected as adoption accelerates, or it may stabilize depending on regulatory drivers and ecosystem readiness. For that reason, while our financial projections provide a clear growth path,

actual numbers may vary depending on how urgently customers need our systems. We are already engaging with organizations who have expressed concrete interest, which gives us confidence in our ability to capture early market share.

Question 31: *How much revenue do you expect to generate over the next years? (check section 10 for more details)*

Answer: Based on our current roadmap and market entry assumptions:

- 2026: ~\$600K from early adopters (40 units)
- 2027: ~\$2.25M (150 units)
- 2028: ~\$6.75M (500 units)
- 2029: ~\$16.5M (1,500 units)
- 2030: ~\$30M (3,000 units)

That totals over **\$56M** cumulative revenue in the first 5 years of commercialization.

Question 32: *When do you expect to become profitable?*

Answer: We anticipate running at a loss during the initial development and validation period (2025–2027) as we prioritize adoption and technology refinement. Profitability is projected starting 2028, with gross margins improving steadily as unit costs decline due to economies of scale and design optimization. By 2030, our gross margin is expected to exceed 70%.

Question 33: *What level of investment are you seeking?*

Answer: We offer 2 clear investment paths depending on investor appetite:

1. **\$600K seed investment → covers the first year of development (FPGA prototyping, R&D, early customer pilots).**

2. \$3M strategic investment → funds a longer-term horizon of research and development, accelerating ASIC design and positioning us for faster market capture.

Both paths are structured to align investor returns with the expected exponential growth of quantum-safe hardware demand.

Question 34: *How will you keep costs under control while scaling?*

Answer: In the early years, units will be more expensive due to manual assembly and testing, with COGS around \$27K per unit in 2026. However, as designs standardize and volume increases, costs drop sharply to ~\$2K per unit by 2030. This cost optimization, combined with strategic pricing, allows us to transition from penetration pricing to high-margin profitability while staying competitive.

2. Executive Summary (Intro)

Quantum computing is set to disrupt the foundations of cybersecurity. Algorithms that protect global communication, finance, defense, and critical infrastructure today will soon be vulnerable to quantum attacks. The threat is real, urgent, and already driving governments and corporations worldwide to search for quantum-safe solutions.

Tania Systems is developing post-quantum cryptographic chips, boards and software that provide unmatched speed, scalability, and resilience. By implementing advanced cryptographic algorithms directly in hardware and software, we deliver protection that software alone cannot match. Our technology is designed to secure massive data flows across sectors where reliability and speed are mission-critical.

The market opportunity is immense. With cybersecurity already exceeding \$200B globally and the post-quantum segment projected to surpass \$10B by 2030, adoption will be accelerated by regulatory mandates, defense needs, and corporate urgency. Early adoption in government and defense will pave the way for enterprise and consumer markets.

Our founding team brings together expertise in mathematics, cryptography, and entrepreneurship. Backed by this unique mix of technical depth and business drive, Tania Systems is positioned to lead the transition into the post-quantum security era.

We are building more than technology. We are building trust, resilience, and the backbone of tomorrow's digital security.

Key Advantages of Tania include:

Proven Quantum-Resilience

Tania's core algorithms are based on NP-complete problems and on average-case hard problems (specifically, quadratic matrix equations, with randomly changing coefficients, over finite fields), a class of problems believed to be intractable even for quantum computers. This provides a strong theoretical security foundation beyond the reach of known quantum attacks. In contrast to some post-quantum schemes that were later found vulnerable (e.g., the Rainbow signature scheme was broken by a key recovery attack), Tania's approach emphasizes well-vetted complexity assumptions and rigorous proof techniques. It aligns with NIST's goal of "encryption algorithms designed to withstand cyberattacks from a quantum computer" and even employs NIST-recommended cryptographic primitives (such as secure hash functions of 1008-bit output for signatures) to reinforce its design. The matrix computations over finite fields allow the use of optimal-time parallel algorithms that can be implemented on existing FPGA boards and GPUs to achieve a Transmission Rate of more than 1 Teabits/sec with 0.1-1 microseconds latency, ensuring the encryption of massive data online, in the realm of 6G communications protocols.

a. All-in-One Integration

Each Tania chip will contain three subsystems: TANIA-SK (Secret Key encryption), TANIA-PK (Public-Key encryption), and TANIA-DS (Digital Signature) - implemented together on a single platform. This integrated design is unique. It means one piece of hardware can seamlessly handle confidential data encryption, quantum-safe key exchanges, and digital signatures for authentication. Organizations no longer need to deploy and manage separate solutions for each cryptographic need. The result is a simpler architecture and lower cost of ownership, since the same chip covers multiple security functions. Notably, the chip can

also be configured to separate these systems on different chips if needed (for example, deploying only the signature module in a specialized device), giving flexibility in implementation without sacrificing the benefits of a common core technology.

b. Uncompromising Performance

Security often comes at the expense of speed, but Tania's hardware is built for high throughput and low latency. The design exploits massive parallelism. Most operations are simple bit-level matrix operations (XOR and AND over $GF(2)$), which can run concurrently at scale. As a result, encryption, decryption, and key generation can be performed with optimal efficiency. The chip's architecture uses ~262k logic gates (in its base security configuration) working in parallel across dozens of cycles for each operation, enabling gigabit to terabit-scale encryption speeds. In fact, Tania is targeting data transmission rates on the order of 1 Tbps (terabits per second) per chip—performance that is orders of magnitude beyond typical software-based encryption and suitable for even the most data-intensive online and real-time applications. Even at higher security settings (with larger key sizes), the design remains scalable. This high speed means that adopting quantum-safe encryption with Tania will not bottleneck network throughput or user experience, a critical requirement for sectors like defense, finance, and telecom.

c. Forward Security & Long-Term Protection

Every encryption operation in Tania uses refresh randomness at each execution, ensuring that even if the same plaintext is encrypted multiple times, it yields different ciphertexts. This property, known as forward security, means that past communications remain safe even if one

message is compromised in the future. Keys do not get weaker with reuse because the system never relies on static deterministic encryption patterns. In principle, this allows Tania's keys to remain secure indefinitely, so data meant to stay confidential for 50+ years (e.g. state secrets or personal health records) can indeed be kept secret for that long. Moreover, Tania's digital signature scheme is designed so that for each message, there is exactly one valid signature solution, eliminating the risk of an attacker finding alternative valid signatures to forge documents without the secret key. This one-to-one mapping of signature to message provides strong protection against collision and forgery attacks that have plagued other schemes.

d. **Reliability and Robustness**

Many advanced cryptosystems that introduce randomness (such as specific lattice-based PQC algorithms, e.g., schemes like Kyber and Dilithium, which were selected by NIST, are designed to tolerate a small amount of noise, allowing for a low probability of decryption failure, while others incorporate error-correcting codes for greater resilience) suffer a slight chance of decryption errors or failures, requiring complex error-correcting steps. This is particularly critical for applications that require immediate action, as in the case of decryption failure, where the user cannot afford a second chance, while waiting for the data to be resent (e.g., a drone that waits for a "Shoot" order or a distant surgery robot that waits for the orders from the surgery doctor). Tania's algorithms avoid this pitfall. They are constructed to be perfectly reversible, establishing a one-to-one relationship between plaintext and ciphertext. In practice, this means no failed decryptions. If you have the correct key, and the transmitted data was not corrupted (by thermal noise and interference in the transmission channel, leading to data corruption or signal distortion, which are treated by error correcting codes and are part of standard communication protocols),

you always recover the exact original data, every time. This reliability is crucial for real-world deployment, where even a tiny failure rate is unacceptable for mission-critical systems. Tania achieves this by careful mathematical design that introduces randomness for security without sacrificing determinism in the overall encryption/decryption process.

In summary, Tania Systems offers a bold and comprehensive solution to the quantum threat: a secure, high-performance chip that organizations can deploy with confidence that their data will remain safe today and in the post-quantum realm far into the future. Backed by cutting-edge research and aligned with NIST's post-quantum standards efforts, Tania is positioned to become a foundational technology for security in the quantum age. The market timing is ideal. Global cybersecurity spending is soaring (projected to exceed \$300 billion by 2026), and within that, the demand for quantum-safe cryptography is growing at over 30% annually as industries prepare for the coming quantum revolution. According to market analyses, the quantum cryptography market (encompassing PQC and quantum key distribution) is expected to grow from about \$1.16 billion in 2024 to \$7.59 billion by 2030 (36.8% CAGR). Early adopters in defense, finance, government, healthcare, and other sectors are already searching for practical solutions to deploy now, ahead of the threat curve. Tania's team, technology, and strategy position it to capture this opportunity and become a leader in quantum-safe security. We are currently seeking a pre-seed investment to continue our prototype development and engage with strategic partners to bring this solution to the market. In the following sections, we detail Tania's vision, technology, use cases, and roadmap, demonstrating why it's a compelling investment for those looking to secure the future of digital information.

2.1 One Pager



Defending Data in Quantum Age

<https://www.taniaapp.com/>
info@taniaapp.com
Tania Systems

Our Mission

Tania is a quantum-safe cryptographic chip algorithm, combining public key, secret key, and digital signature technologies, to be implemented in parallel hardware ensuring super fast transmission rates and robust security.

Problem	Solution
No Quantum Proof Solution	→ Tania's Quantum Safe Algorithms
Low Safety If High Transmission Rate	→ High Transmission Rate with Robust Security

Problem Example

Imagine a national power grid managing vast amounts of sensitive data and commands across multiple locations. If a quantum computer could intercept and decrypt these transmissions, it could potentially disrupt operations, leading to power outages, economic losses, and security risks.

Solution

With Tania's quantum-safe chip, the power grid's data transmissions are secured with advanced encryption that withstands even quantum-level threats. The chip's high-speed processing ensures real-time data protection without slowing down operations, making it a critical safeguard for essential infrastructure.

Value Proposition

Tania offers a groundbreaking, quantum-safe cryptographic chip that integrates secret key, public key, and digital signature functions into one streamlined design. This all-in-one solution provides unmatched data security, cost efficiency, and ease of integration, safeguarding systems against current and future quantum threats while reducing operational complexity. Ideal for industries needing high-level, future-proof security, Tania ensures resilience in a rapidly evolving digital landscape.

Tania's Team



Dr. Y. Peretz
CEO, CTO & Co-founder




Kevin Chami
CPO & Co-founder



Hilal Primack
COO & Co-founder

Tania's Revenue Model



Patent Licensing



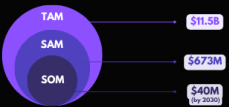
Direct Chips Sales



Customized Algorithm use

Market Size

With global spending on cybersecurity projected to exceed \$500 billion by 2026, Tania is positioned to capture significant market share, particularly in sectors where data security is paramount – such as finance, healthcare, autonomous vehicles, and defense.



TAM → \$11.5B
SAM → \$673M
SOM → \$40M (by 2026)

Competition Comparison

Tania leads in cryptographic transmission speeds, combining encryption and signing into a single chip. It achieves 0.1059 Tbps for secret key encryption (vs. AES12's 0.0698), 0.6756 Tbps for public key encryption (vs. 0.00032 and 0.000016), and excels in digital signatures with 1.2047 Tbps for generation and 6.8089 Tbps for verification (vs. 0.000192, 0.000125, and 0.0000038). With 3 systems in 1, Tania delivers unmatched speed, robust security, and seamless performance.

	SECRET KEY ENCRYPTION (Tbps)	PUBLIC KEY ENCRYPTION (Tbps)	DIGITAL SIGNATURE GENERATION (Tbps)	DIGITAL SIGNATURE VERIFICATION (Tbps)
TANIA	✓	0.1059	0.6756	1.2047
AES128	×	-	-	0.0000093
RIPEMD	×	-	0.000032	-
AES-256	×	0.0698	-	-
SHA-256	×	-	0.000008	-
SHA-512	×	-	-	0.0000125
SPHINCS	×	-	-	0.0000038

Pre-Seed:

Covers initial R&D, MVP development, team setup, first production, testing, and advanced research to reach proof of concept.

Seed:

Supports full product development, market entry, early partnerships, establishing revenue and validating product-market fit.

Series A:

Funds scaling production, expanding sales, marketing and customer support.

Series B:

Focuses on product and geographic expansion, advanced R&D, and market leadership.

(The above is a synthesized summary of Tania's one-page pitch. The following sections will expand on each aspect in detail.)

3. About Tania Systems

3.1 Our Team

Tania Systems is driven by a team of experienced innovators in cryptography, hardware engineering, and business strategy. The company's leadership brings together the multidisciplinary expertise needed to build a cutting-edge security hardware startup:

Dr. Yossi Peretz – CEO, CTO & Co-Founder: A leading expert in cryptography and applied mathematics and parallel algorithms, Dr. Peretz is the inventor of Tania's core post-quantum algorithms. Holding a **Ph.D. in mathematics and computer sciences**, he brings over three decades of research experience, including pioneering contributions to multivariate encryption schemes. His academic work, such as solving simultaneous algebraic Riccati equations over finite fields, randomized and parallel algorithms, formed the foundations for Tania's systems approach. As **CEO and CTO**, Dr. Peretz oversees our **R&D efforts**, ensuring our technology is not only cutting-edge but also mathematically sound and provably secure.



Kevin Chami – CPO & Co-Founder: Kevin brings a strong foundation as a software engineer with a **Bachelor's degree in Computer Science**. At Tania Systems, he leads **software and algorithms** implementation, with a focus on optimizing cryptographic performance for **GPU and cloud** environments. As a founding partner with a solid technological background, Kevin plays a key role in translating mathematical innovations into high-performance systems. Beyond the technical side, he is actively involved in **product strategy, investor relations, and coordination** with external technology partners to support the company's growth.



Hillel Primack – COO & Co-Founder: Hillel holds a **Bachelor’s degree in Business and Entrepreneurship** and brings a proven track record of building and managing ventures across multiple industries. With hands-on experience



in startups, sales, and business development, he combines **strategic thinking** with practical execution. His entrepreneurial drive and strong **network of connections** give Tania Systems a competitive edge in forming partnerships, engaging investors, and navigating global markets. As COO, Hillel oversees business operations, strategy, and growth initiatives, ensuring that technical

innovation is matched with **clear market opportunities**. His leadership focuses on building sustainable structures, driving partnerships, and positioning Tania as a trusted player in the cybersecurity and semiconductor industries.

Together, our founding team brings deep expertise across **cryptography, software engineering, and business strategy**. From pioneering post-quantum algorithms to optimizing real-world implementations and leading market execution, we cover the full spectrum needed to build and scale transformative cybersecurity technology. Backed by advisors with experience in information security, semiconductor manufacturing, and defense procurement, Tania is uniquely positioned to turn advanced cryptographic research into a robust, scalable product. United by a shared mission to protect global data infrastructure against the quantum threat, **we have both the vision and the capabilities to make it a reality.**

3.2 Mission & Vision

Mission

Tania Systems exists to protect the foundations of our digital world in an era where traditional security can no longer be trusted. The rise of quantum

computing presents a direct threat to the confidentiality, integrity, and reliability of global communications, finance, defense, and everyday digital life. Our mission is to ensure that governments, organizations, and individuals remain secure by building the next generation of quantum-resilient security solutions.

We are driven by the belief that trust in digital systems is not optional. It's essential for progress, stability, and freedom. From safeguarding national defense and critical infrastructure to enabling secure commerce and private communication, our mission is to provide the protection that societies need to thrive in the quantum age.

Vision

We envision a future where quantum resilience is the foundation of global trust in digital systems. Tania Systems aims to become the global standard for quantum-safe security, empowering every sector to confidently embrace the future of computing. We see a world where every critical system, from national defense and government communications to banking networks, hospitals, connected vehicles, and personal devices, is secured by quantum-resistant cryptography. In this future, Tania's technology stands as a cornerstone of digital trust, much like AES and RSA shaped the pre-quantum era. Our long-term goal is to democratize access to quantum-proof security so it becomes as seamless and universal as encryption is today. By collaborating on international standards, advancing our algorithms, and scaling our hardware globally, we will ensure that the quantum threat is neutralized and digital life remains secure, private, and trusted.

Values

Our core values reflect what Tania Systems stands for, guiding both our technology development and business practices:

- **Security First:** We place utmost priority on security and privacy in every decision. This means no compromise on cryptographic strength or integrity. From algorithm design to chip fabrication, every step will be executed with rigorous security standards. We follow industry best practices and beyond, for example: adhering to NIST recommendations for cryptographic primitives and undergoing thorough testing and validation. We are committed to maintaining trust: our products will do what we claim – protect data, and we will be transparent about their capabilities and limitations.
- **Innovation & Excellence:** Tania was born from cutting-edge research, and we continue to foster a culture of innovation. We tackle complex problems (like NP-complete and average-case hard problems based cryptography) with creativity and scientific rigor. The team continuously pushes the envelope of what's possible in cryptographic performance, often inventing new techniques (such as novel parallel processing methods) to meet our goals. We aim for excellence in execution as well. Whether it's producing a high-quality silicon chip or providing top-notch support to a customer, we strive for the best. This value drives us to keep learning, iterating, and staying ahead of adversaries.
- **Integrity & Trustworthiness:** Trust is the bedrock of security. At Tania Systems, we conduct business with integrity, ensuring honesty with customers, partners, and investors. This means making realistic claims rather than overpromising, submitting our technology to third-party audits, and protecting our intellectual property through our patent, while still committing to transparency. **With our patent in place**, we will continue to subject our methods to peer review under appropriate confidentiality, reinforcing confidence in our solutions. Internally, we uphold strict ethical standards, from secure development practices to safeguarding sensitive data we handle. Our goal is for everyone who

depends on Tania Systems to have complete confidence in our reliability.

- **Democratizing Security:** We believe quantum-grade security should not be reserved only for the largest governments or corporations. Every person and every organization deserves protection from advanced threats. This belief comes from recognizing that in the early years, quantum computers will likely be controlled by powerful entities such as nation-states or major technology companies, leaving others exposed and vulnerable. Our commitment to democratizing security means designing solutions that can be deployed widely, with a focus on cost-effectiveness, ease of integration, and broad compatibility. As production scales, our goal is to make Tania Systems chips accessible for consumer devices and open platforms, extending quantum-safe protection to individuals and communities worldwide.
- **Collaboration & Standards:** We value working with the broader community, whether in academia, industry, or government. Security is strongest when experts come together, as demonstrated by NIST's collaborative post-quantum cryptography project. At Tania Systems, we actively seek to contribute to standards and interoperability, ensuring our solutions enhance global efforts in post-quantum security rather than compete against them. We already collaborate with **ENICS-Labs at Bar-Ilan University**, a leading research center in Israel, to strengthen our development and validation efforts. Beyond academia, we build partnerships with security infrastructure providers and participate in standards bodies so that our technology integrates seamlessly into the ecosystems our customers depend on. This collaborative spirit also defines how we work internally, where problems are solved collectively and every team member's expertise is respected.

By living these values, Tania Systems builds not only superior technology but also a reputation as a trusted leader in security. They guide us as we grow in the fast-changing cybersecurity landscape, keeping us true to our mission of protecting data in the quantum era.

4. The Problem

4.1 The quantum threat

For decades, the security of our digital world has relied on a handful of cryptographic algorithms. Standards such as RSA, ECC, and Diffie-Hellman have been the backbone of secure communication, banking, government networks, and global commerce. Their strength has always rested on one assumption: that no computer could efficiently solve the mathematical problems at their core.

Quantum computing will change this assumption forever. Once quantum machines reach sufficient scale, they will be able to break RSA and ECC within hours or even minutes. What currently takes classical supercomputers thousands of years, will be reduced to trivial computations. The result is that nearly all of today's encryption, the same encryption protecting everything from military communications to online payments, will become obsolete.

This threat is not theoretical or distant. Leading technology companies and national laboratories are investing billions into quantum computing. Progress in this field is accelerating faster than most security experts predicted, and the first machines capable of breaking modern encryption could arrive within the next decade. Security standards bodies such as NIST, NATO, and the European Union are already sounding alarms and rushing to establish quantum-safe cryptography guidelines.

The challenge goes even deeper. Nation-states and advanced threat actors are already conducting what is known as harvest now, decrypting later

operations. Encrypted data intercepted today, including classified government communications, banking records, and personal information, can be stored until quantum computers mature. At that point it will be decrypted and exposed. This means that information we believe to be secure today may already be compromised for the future.

Adding to the urgency is the exponential growth of data. The rise of 5G and 6G networks, the explosion of IoT devices, AI-driven platforms, and cloud-based infrastructures have created an environment where massive volumes of sensitive information move every second. These networks demand not only stronger security but also solutions that can operate at extremely high speeds without slowing down global data flows. Current systems already strain to balance performance with security against classical threats, and when the quantum threat arrives the gap will widen into a full-scale crisis.

The implications are severe. Governments risk losing control over secure military and intelligence communications. Financial institutions face exposure of transactions and long-term data, leading to systemic instability. Healthcare systems could see medical records compromised, and entire industries built on confidentiality, from legal to defense contractors, could lose trust overnight. Even consumer technology, from smartphones to connected vehicles, would be exposed to threats that today's protections cannot withstand.

In short, the digital infrastructure that underpins modern society is vulnerable. Without a fundamental shift in security, the arrival of quantum computing will trigger a collapse in the systems of trust that enable communication, commerce, and defense in the digital age.

4.2 Gaps in current solution

Given the severity of the quantum threat, one might ask: *‘what solutions exist today and why are they not sufficient?’* Several approaches are being explored, but each leaves critical gaps that prevent true readiness.

One approach is legacy cryptography and incremental fixes. For symmetric ciphers such as AES, doubling key sizes to AES-256 or AES-512 can encounter Grover’s algorithm, which only halves effective security. While this helps on the symmetric side, it does nothing for public-key cryptography. RSA and ECC are fundamentally broken by Shor’s algorithm, and our entire public-key infrastructure – digital certificates, TLS handshakes, secure email, is built on algorithms that cannot simply be patched. They require full replacement with new mathematics. Even for symmetric encryption, longer keys do not address authentication and integrity challenges in a post-quantum world.

Another area of focus is post-quantum algorithms in software. The NIST process has produced promising candidates such as Kyber and Dilithium, but deploying them at scale is non-trivial. Many lattice-based schemes rely on heavy matrix multiplications and produce ciphertexts and signatures that are significantly larger than their RSA or ECC equivalents. This creates inefficiencies in bandwidth and storage and slows down operations. Organizations face a massive integration burden in updating every device and every system to handle these new cryptosystems. Pure software implementations introduce latency and high computational costs, and without acceleration or optimization they are impractical for wide deployment.

A further gap comes from the lack of comprehensive solutions. Current efforts often address only specific functions, such as key exchange or digital signatures, while leaving others unchanged. A company might adopt a lattice-based scheme for secure connections but continue using AES for bulk encryption and another algorithm for signatures. This creates a patchwork of

tools that complicates operations and increases risks. What is missing is a unified, streamlined approach that provides confidentiality, authentication, and integrity in a single package.

Quantum Key Distribution (QKD) has also been presented as a quantum-proof option. While it is promising for very specialized applications, it remains impractical for general use. QKD requires expensive infrastructure such as dedicated fiber-optic or satellite links and only solves the problem of key exchange. Once the key is exchanged, another algorithm is still needed for encryption, and QKD does nothing for digital signatures or stored data. For governments and enterprises looking for broad, scalable adoption, QKD is too limited in scope.

Another stop-gap measure comes from hardware security modules and FPGA retrofits. In sectors such as government and finance, HSMs and FPGA-based accelerators are already common. Some vendors have introduced firmware updates or loaded PQC cores onto FPGAs, but these are piecemeal solutions. They may accelerate a lattice-based key exchange for a VPN but leave signing or authentication to separate systems. The result is a fragmented landscape requiring multiple devices, multiple vendors, and higher complexity. These retrofits were not designed from the ground up for post-quantum needs, and as such they increase costs and expand the attack surface rather than simplifying security.

Finally, there is the uncertainty surrounding post-quantum schemes themselves. Not all candidates have proven resilient. The Rainbow digital signature, once a NIST finalist, was broken in 2022. Many schemes rely on mathematical assumptions that are newer and less time-tested than RSA or ECC once were. Organizations hesitate to commit fully to a single algorithm when confidence in its long-term security is not absolute. What is needed is not only strong mathematics but also designs that provide assurance even if individual schemes are challenged in the future.

In summary, while the world is actively working on quantum-safe security, current measures remain fragmented, inefficient, and incomplete. Organizations face a choice between patching together diverse algorithms, investing in exotic technologies like QKD that solve only part of the problem, or waiting and risking exposure. There is no comprehensive, high-performance, quantum-safe cryptographic system available off the shelf today. The gap is clear, and it highlights the need for a solution that is unified, scalable, and trusted.

5. The Solution

5.1. What is Tania Systems?

Tania Systems is the solution to one of the greatest vulnerabilities of our time: the collapse of modern encryption under the power of quantum computing. For decades, digital security has relied on mathematical assumptions that worked in a classical world but are destined to fail once quantum computers reach maturity. Governments, corporations, and entire industries know the threat is coming, yet the tools available today remain partial and incomplete. Tania Systems was created to bridge this gap by delivering a solution that is both future-proof and practical for the real-world challenges of today.

At its core, Tania Systems develops **post-quantum cryptographic chips**, hardware designed from the ground up to resist attacks from quantum machines. These chips provide a unified security framework by combining encryption, authentication, and digital signatures in one integrated platform. Instead of relying on fragmented solutions or patchwork updates, Tania offers a complete package that ensures confidentiality, integrity, and trust across digital systems.

What sets Tania apart is not only our quantum resistance, but also our **unmatched performance**. While many players in the market are developing

PQC solutions, we are among the very few capable of achieving **1 terabit per second (Tb/s)** throughput even for **public key operations**, a milestone that surpasses even AES, long considered the gold standard of symmetric encryption. This is made possible by our architecture's massive parallelism, which allows data to be encrypted and transmitted at speeds that no software-based or retrofitted hardware approach can match.

This breakthrough is not just a performance luxury; it is a **requirement for the future**. With the upcoming arrival of **6G networks**, the volume and velocity of global data traffic will skyrocket to unprecedented levels. The U.S. National Institute of Standards and Technology (NIST), which is finalizing PQC standards, has already indicated that all finalist algorithms will need to scale to **1 Tb/s** to remain viable in real-world adoption. Tania is ahead of this curve since we have designed for these requirements from day one.

By embedding our mathematically robust algorithms directly into silicon, we ensure speed, reliability, and energy efficiency in environments where delays or bottlenecks are unacceptable. This makes our chips suitable for a wide spectrum of applications: from embedded IoT devices, to hyperscale data centers handling billions of secure transactions, to defense networks transmitting real-time intelligence across the globe.

Tania Systems is built for those who cannot afford failure. Governments and armies require secure channels to protect state secrets and military operations. Financial institutions must safeguard trillions of dollars in value and maintain trust in global markets. Healthcare providers need to protect sensitive patient records and critical hospital systems. Enterprises and cloud platforms must ensure that data-driven infrastructure continues to function securely in an era where the very foundation of encryption is at risk. In each of these areas, Tania Systems provides a single, reliable solution to protect against the quantum threat while also delivering the **performance needed for the data-driven world of tomorrow**.

Beyond technology, Tania Systems represents a new approach to digital trust. Security is not only about algorithms and chips; it is about confidence. Our solution is designed to inspire confidence not just in its cryptographic strength, but also in its usability, scalability, and adaptability. By creating a platform that is both technically sound and practically deployable, we give organizations the ability to act now rather than wait and risk exposure later.

In essence, Tania Systems is more than a product. It is the answer to a problem that threatens the very core of modern society: how to ensure that the digital infrastructure powering governments, economies, daily life can survive in the quantum age. Our solution is designed to be comprehensive, high-performance, and future-ready, ensuring that trust in digital systems endures no matter what computing power the future brings.

5.2. Key advantages

Tania Systems was built to close the critical gaps left by today's post-quantum security efforts. Our solution is not a patch, not a retrofit, and not a niche experiment. It is a purpose-built platform designed for long-term trust in the quantum era. Several key advantages define why Tania stands out as the future of digital security.

Quantum-Resilient by Design

Our cryptography is built on NP-complete problems and randomized structures that resist both classical and quantum attacks. Unlike retrofitted systems or incremental fixes, Tania's architecture is designed from the ground up to withstand the computing power of tomorrow. This ensures that the protection we provide is not temporary but future-proof.

Hardware-Level Speed and Efficiency

By embedding post-quantum algorithms directly into silicon, we deliver performance that software-only implementations cannot match. Tania's

chips process massive volumes of data in real time, enabling secure communication at the scale of cloud providers, financial markets, defense networks, and beyond. Low latency, high throughput, and energy efficiency make our solution practical for deployment across industries.

Integrated All-in-One Security

Where current solutions require organizations to combine multiple algorithms and systems for different functions, Tania provides a unified framework. Our chips integrate public-key encryption, secret-key encryption, and digital signatures into one cohesive architecture. This reduces complexity, lowers cost, and ensures consistency across systems.

Scalability Across Sectors

From embedded IoT devices and connected vehicles to national defense infrastructures and global data centers, Tania's solution is built to scale. Our technology adapts to diverse environments without losing reliability or performance, making it equally valuable for governments, enterprises, and consumer-facing industries.

Trusted and Standardized

Security depends on confidence. Our technology is protected by patents and developed in collaboration with leading research partners such as ENICS-Labs at Bar-Ilan University. By engaging with international standards bodies and pursuing third-party audits, we ensure that Tania's solutions are not only secure but also trusted and interoperable on a global scale.

First-Mover Advantage in a Growing Market

With NIST standards finalized and adoption cycles beginning, the race to implement quantum-safe security has started. Tania is positioned at the forefront of this transition, offering governments, corporations, and organizations a solution that is both ready for deployment and designed to scale as demand explodes.

5.3. How Tania Systems stands out

The global race toward post-quantum security has already begun, but most of today's approaches remain partial or impractical. Some focus only on software, others retrofit existing hardware, and some rely on niche technologies that cannot scale. Tania Systems stands out by offering a complete, purpose-built solution that bridges these gaps and delivers security that is both powerful and deployable.

Our chips ensure real-time protection without slowing down communication or overwhelming energy budgets, making them viable for defense networks, financial markets, and global cloud infrastructure.

Unlike retrofit solutions such as firmware upgrades to HSMS or FPGA add-ons, which cover only single functions like key exchange or signatures, Tania integrates encryption, authentication, and digital signatures into a single architecture. This eliminates the patchwork of devices and vendors that organizations would otherwise be forced to manage, reducing cost and minimizing attack surfaces.

Unlike Quantum Key Distribution, which requires specialized and expensive infrastructure while solving only the key exchange problem, Tania offers a universal, flexible, and scalable platform. Our chips protect not only key exchange but also stored data, digital signatures, and everyday communication — all within one system that can be deployed broadly.

Tania Systems also stands out in trust and maturity. Many proposed PQC algorithms are unproven and some have already collapsed under scrutiny, such as Rainbow. Our design does not depend on a single fragile mathematical assumption. Instead, it leverages NP-complete problems and randomized structures, giving resilience even if individual schemes face future challenges. Combined with our patent, peer-review process, and collaboration with ENICS-Labs at Bar-Ilan University, we offer a solution

backed by rigorous science, independent validation, and legal protection.

Competition in this field exists, but it has not solved the performance and scalability requirements demanded by the coming 6G era, nor has it fully aligned with the NIST post-quantum standards that will govern adoption worldwide. Tania Systems was designed from the outset to address both. We will discuss the competitive landscape in more detail in the dedicated competition section of this booklet.

Finally, Tania's approach stands out for its practicality and vision. We aren't building a lab experiment or a temporary patch. We are building a solution that governments, armies, enterprises, and individuals can actually deploy at scale. By combining mathematical innovation, silicon-level engineering, and a focus on real-world usability, Tania Systems delivers what others can't.

6. Technology Core

6.1 Matrix-Based Quantum-Safe Protocol

Note: The following section contains advanced mathematical explanations and calculations. If the content is unclear, we strongly recommend consulting a professional mathematician with relevant expertise to properly understand the material:

Let F_q be a finite field, for example F_2 with the elements $\{0, 1\}$ and XOR and AND operations as the operations of addition and multiplication. All elements and computations are over the chosen field.

Assume that Alice and Bob want to communicate secretly over a public channel. Then, they choose n sufficiently large, considering the computational capabilities of a potential eavesdropper.

They choose random $2n \times 2n$ invertible matrix $U = \begin{bmatrix} U_{1,1} & U_{1,2} \\ U_{2,1} & U_{2,2} \end{bmatrix}$ partitioned to $n \times n$ blocks. They also choose two random $n \times n$ matrices \hat{A} and \hat{D} such that \hat{D} is invertible and \hat{A} and \hat{D} have co-prime minimal polynomials. They also choose two random $n \times n$ matrices P and Q where P is invertible.

The shared secret of Alice and Bob is $(U_{1,1}, U_{2,1}, U_{2,1}, U_{2,2}, \hat{A}, \hat{D}, P, Q)$.

Assume that Alice wants to send a secret message to Bob through the public channel. Then, she encodes the message into an $n \times n$ matrix M . She chose a random $n \times n$ matrix Z such that $\det(U_{2,1}Z + U_{2,2}) \neq 0$. Next, she computes

$\hat{B} = Z\hat{D} - \hat{A}Z$. She sets $\hat{T} = \begin{bmatrix} \hat{A} & \hat{B} \\ 0 & \hat{C} \end{bmatrix}$ and computes $T = U^{-1}\hat{T}U$, which she divide to four $n \times n$ blocks $T = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$. Next, she computes $X = f_U(Z) = (U_{1,1}Z + U_{1,2}) \cdot (U_{2,1}Z + U_{2,2})^{-1}$.

Finally, she computes $\tilde{Z} = PZ + Q$ and $\tilde{Y} = M \cdot (CX + D) - (A - XC) \cdot M$. She sends the couple (\tilde{Z}, \tilde{Y}) to Bob through the public channel.

Bob receives the couple (\tilde{Z}, \tilde{Y}) from Alice. Bob computes $Z = P^{-1} \cdot (\tilde{Z} - Q)$.

Bob computes $X = f_U(Z) = (U_{1,1}Z + U_{1,2}) \cdot (U_{2,1}Z + U_{2,2})^{-1}$.

Bob computes $\hat{B} = Z\hat{D} - \hat{A}Z$. Bob sets $\hat{T} = \begin{bmatrix} \hat{A} & \hat{B} \\ 0 & \hat{C} \end{bmatrix}$ and computes $T = U^{-1}\hat{T}U$, which he divide into four $n \times n$ blocks $T = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$.

Finally, Bob solves the equation $\tilde{Y} = M \cdot (CX + D) - (A - XC) \cdot M$ for M and recovers the message from Alice.

The equation $\tilde{Y} = M \cdot (CX + D) - (A - XC) \cdot M$ is a linear equation for Bob since he knows X, A, B, C, D and \tilde{Y} . This equation has a unique solution for M , since \hat{A} and \hat{D} have co-prime minimal polynomials.

For a possible eavesdropper, the equation $\tilde{Y} = M \cdot (CX + D) - (A - XC) \cdot M$ is a quadratic matrix equation since $M, (CX + D)$, and $(A - XC)$ are unknown to

him. He can't compute X, A, B, C, D from \tilde{Z} since he doesn't know $(U_{1,1}, U_{2,1}, U_{2,1}, U_{2,2}, \hat{A}, \hat{D}, P, Q)$.

Note that the equation $\tilde{Y} = M \cdot (CX + D) - (A - XC) \cdot M$ has random coefficients, namely $(CX + D)$ and $(A - XC)$ that depend on the randomly chosen Z matrix such that $\det(U_{2,1}Z + U_{2,2}) \neq 0$. It means that for any other messages or in any other sessions, the coefficients will be totally different and nothing would be learnt from the history. This provides a strong security against any possible attack. Moreover, it says that, at least theoretically, the lifetime of the secret key is infinite.

Solving a matrix quadratic equation is NP-hard in general, and having a random coefficient makes the problem even more difficult, as it becomes hard on average. This means the likelihood of encountering an easy-to-solve equation is negligible. These features make TANIA Systems quantum-resistant and quantum-safe.

The parameter n was selected by TANIA Systems to be sufficient to withstand attacks from quantum computers, regardless of their number of qubits.

The actual systems were designed for efficient implementations and parallel optimal-time algorithms for matrix operations. The actual chosen n in values of 32,64,128,256 reflects the need for flexibility, supplying various levels of security (also against electronic computer attacks) and making the computations efficient.

For more details, see TANIA P.Q.C Systems patent PA158821US by Y. Peretz.

6.2 Software Development

At Tanya Systems, we are building the GPU-accelerated implementation of TANIA-SK-Light-Weight, a post-quantum secret-key cryptosystem designed for ultra-low latency and extreme throughput. Our software core translates advanced algebraic constructions into high-performance GPU pipelines running on NVIDIA A100 hardware.

The core pillars of our technology are built around several key elements. First, GF(2) arithmetic acceleration ensures that all cryptographic operations are executed over GF(2) with bit-packed representations and custom CUDA kernels optimized through popcount parity, coalesced memory access, and shared memory tiling. Second, high-speed encryption and decryption are achieved by fusing companion matrix transformations (CCF and ICCF) into steady pipelines that minimize host-to-device transfers while leveraging CUDA Graphs to reduce launch overhead. Third, our scalable multi-GPU design uses MPI and CUDA multi-device APIs, allowing the system to scale seamlessly across multiple NVIDIA A100 GPUs. Finally, profiling-driven optimization ensures maximum performance by using Nsight Systems and Nsight Compute to analyze kernel occupancy, memory efficiency, and instruction throughput.

7. Competitive landscape

7.1. Companies & current players

The race to secure data against quantum threats has drawn in both established technology giants and specialized startups. While this shows that the market is real and urgent, none of these players offers a complete solution that addresses the full scope of the challenge.

Firms like IBM, Google, and Microsoft are investing heavily in post-quantum cryptography. Their efforts are focused mainly on software integration — adding PQC algorithms into existing cloud platforms, VPNs, and browsers. For example, Google has piloted Kyber in Chrome, and Microsoft is testing PQC protocols for its enterprise services. While these initiatives are valuable, they remain limited to software updates. They do not solve the performance and scalability challenges that will arise in 5G, 6G, or large-scale defense systems.

Several startups have emerged, including:

- PQShield (UK) – Offers software libraries for PQC and embedded cryptography, targeting chipmakers and OEMs.
- ISARA (Canada) – Provides toolkits to help companies migrate to PQC-ready software and hybrid cryptographic solutions.
- Quantinuum (US/UK) – Focused on both quantum computing hardware and quantum-safe cryptography, with an emphasis on software solutions.
- CryptoNext Security (France) – Develops software suites for post-quantum encryption in enterprise environments.

These companies are advancing awareness and integration but are primarily software players. Their solutions require organizations to update software stacks, protocols, and systems, often at the cost of performance, energy efficiency, and integration complexity.

Traditional hardware security module (HSM) vendors like Thales and Entrust have begun to offer firmware updates to support PQC algorithms. FPGA manufacturers such as Xilinx (AMD) and Intel (Altera) are being used to prototype PQC accelerators. These are important steps, but they are retrofits, not purpose-built solutions. They typically handle only one function (for example, accelerating key exchange) and require organizations to combine multiple devices or vendors to cover all their needs.

Players like ID Quantique (based in Switzerland) are focused on Quantum Key Distribution, using entangled photons for secure key exchange. While interesting for very specialized use cases, QKD requires expensive

infrastructure, solves only the key exchange problem, and does not address signatures, stored data, or broad-scale communication. It is not a practical or generalizable solution for governments, enterprises, or consumer applications.

So in short: competitors are fragmented. Big tech is doing software integration, startups provide PQC toolkits, hardware vendors are doing retrofits, and niche players are pursuing experimental physics approaches like QKD. None of them delivers a unified, scalable, hardware-based solution like Tania Systems.

7.2. NIST Finalists & algorithm-centric approaches

In response to the quantum threat, the U.S. National Institute of Standards and Technology (NIST) has been leading the effort to define post-quantum cryptographic standards. After years of evaluation, NIST announced its first set of finalists in 2022, with Kyber selected for encryption and key establishment, Dilithium and Falcon for digital signatures, and SPHINCS+ as an additional option for signatures. These algorithms form the backbone of the coming generation of quantum-safe security.

While they are essential, deploying them in practice reveals serious limitations. Post-quantum algorithms are significantly more complex than RSA or ECC. Ciphertexts and signatures can be several times larger, and many operations involve heavy matrix multiplications. In software, this creates slower performance, higher latency, and greater energy consumption. For environments where speed is critical, such as financial exchanges, 6G mobile networks, or defense systems, these inefficiencies are unacceptable.

Another issue is integration. NIST has recommended different algorithms for different tasks: Kyber for key exchange, Dilithium or Falcon for signatures, AES for bulk encryption, and so on. Organizations adopting them must piece

together multiple systems, each with its own requirements and implementation details. This patchwork creates complexity, raises costs, and opens the door to misconfigurations or vulnerabilities.

There is also the challenge of maturity. While the NIST finalists are strong candidates, they remain relatively new compared to standards like RSA and AES that have been studied for decades. Some once-promising algorithms have already collapsed under scrutiny, such as Rainbow, a former NIST finalist that was broken in 2022. This uncertainty makes governments and enterprises cautious about fully committing to a single scheme.

Competitors in the field generally focus on implementing these algorithms in software libraries, enterprise tools, or VPNs. Their contributions are important but do not solve the performance bottleneck or provide a unified framework. Adoption in this model requires updating every device, protocol, and service independently, which is costly, complex, and difficult to scale.

In short, the NIST process has given the world the algorithms it needs, but the way they are delivered today is not enough. What is missing is a unified, hardware-accelerated platform that makes these standards practical, scalable, and trustworthy for real-world deployment.

7.3. Why Tania Systems will dominate

While many companies and research groups are contributing to the post-quantum field, they remain limited in scope. Big technology firms are integrating algorithms like Kyber and Dilithium into browsers and cloud platforms, but these remain software updates that add latency and complexity without addressing the scale required for 5G and 6G networks. Startups such as PQShield, ISARA, and CryptoNext Security provide valuable toolkits, but they focus almost entirely on software libraries and migration support. Hardware vendors retrofit existing HSMs and FPGAs with PQC cores, but these piecemeal solutions only cover single functions and increase cost

and operational complexity. Niche players in quantum key distribution pursue highly specialized approaches that cannot be deployed broadly.

This fragmented landscape highlights the absence of a comprehensive, scalable solution. Tania Systems is positioned to fill that gap. Our platform is built from the ground up as a unified hardware solution that integrates encryption, key exchange, and digital signatures into one chip. By accelerating post-quantum algorithms directly in silicon, we eliminate the performance bottlenecks of software-only approaches. By providing a complete framework, we avoid the patchwork complexity of mixing multiple tools and vendors. By designing for scalability, we ensure our solution can meet the unprecedented demands of data-driven sectors, from IoT and cloud to defense and finance.

Another key differentiator is future readiness. Current competitors are not prepared for the performance and bandwidth requirements of the 6G era, nor are their solutions fully aligned with NIST's post-quantum standards. Tania has been engineered from the outset with both in mind, ensuring that our platform is not only secure but also compliant and deployable at scale once governments and enterprises begin the mandatory transition.

Our advantage lies in three factors: performance, integration, and trust. Performance comes from hardware acceleration that delivers real-time protection for massive data flows. Integration comes from combining all core cryptographic functions into one solution, reducing cost and attack surfaces. Trust comes from our patent, our collaboration with ENICS-Labs at Bar-Ilan University, and our commitment to third-party review and international standards.

For these reasons, while others deliver pieces of the puzzle, Tania Systems is positioned to dominate the market by delivering the first truly comprehensive, scalable, and future-proof solution for post-quantum security.

7.4. Performance Comparison of TANIA P.Q.C. Systems and NIST Finalists

Note: The following tables contain mathematical formulas and technical units that may be unfamiliar. If any part of the content is unclear, we recommend consulting a professional with expertise in mathematics or engineering to ensure proper understanding.

This section compares the performance of TANIA Post-Quantum Cryptography (P.Q.C.) Systems and NIST finalists (ML-KEM, ML-DSA, Falcon, SLH-DSA, AES, ASCON) on a 1 GHz FPGA and the AMD VCK190 FPGA (Versal AI Core VC1902, 600 MHz AI Engine, $\approx 2\text{M}$ LUTs, 112 Gbps transceivers), targeting 6G requirements (greater than 1 Tbps throughput, sub-millisecond latency). TANIA leverages matrix addition (1 cycle), multiplication ($\log_2(n)$ cycles: 5, 6, 7, 8 for $n=32, 64, 128, 256$), and inversion ($\log^2(n)$ cycles: 25, 36, 49, 64), optimized for the AI Engine's 400 tiles (512-bit SIMD, 124 TOPS for int8 at 600 MHz, 165 TOPS at 1 GHz). The AI Engine provides 12–20x parallelism for TANIA and 3–9x for NIST, but VCK190's 112 Gbps transceivers (0.112 Tbps) limit I/O for high-throughput algorithms.

For ML-KEM (CRYSTALS-Kyber), performance is evaluated for full key generation, encapsulation (encryption), and decapsulation (decryption), which include matrix-vector operations, hashing, sampling, and error correction. Throughputs are reported in Terabits per second (Tbps), based on data sizes (e.g., ML-KEM-512: 768-byte ciphertexts for Encapsulation, 32-byte shared secrets for Decapsulation). ML-DSA (CRYSTALS-Dilithium) throughputs are reported for full signing, based on signature sizes (e.g., ML-DSA-44: 2,420 bytes). These align with TANIA's full cryptographic processes (e.g., SK-Light de-cryption, SK-Regular/PK encryption, DS signing). The VCK190's programmable logic (PL) supports 300–600 MHz, with 1,979,404 LUTs and 3,958,808 FFs. TANIA's gate counts (e.g., 8.59 billion for PK-LF-256) require optimization. Throughputs for TANIA and NIST algorithms are calculated as $Tbps = (Data\ Size\ [Bits] \times Operations\ per\ Second) / 10^{12}$, capped at 0.112 Tbps by VCK190 transceivers at 600 MHz, and scaled from 220 MHz (Artix-7). By 2030, 1–2 GHz FPGAs with over 500 tiles and optical interconnects (e.g.,

400 Gbps) will support uncapped Tbps-scale PQC for 6G.

Table 1: Summary of TANIA P.Q.C. Systems Performance

System Level	Operation	Quantum [Bits]	Sec. Cycles/Depth	Block/Sig. Size	Throughput [Tbps] at 1 GHz	Throughput [Tbps] at 600 MHz (VCK190)
SK-Light-32	Decryption	2^{93}	24	1,024	0.0427 (0.512–0.854)	0.0256 (0.307–0.512)
SK-Light-64	Decryption	2^{189}	27	4,096	0.1517 (1.820–3.034)	0.0910 (1.092–1.820)
SK-Light-128	Decryption	2^{381}	30	16,384	0.5461 (6.553–10.922)	0.3277 (3.932–6.553)*
SK-Light-256	Decryption	2^{765}	33	65,536	1.9859 (23.831–39.718)	1.1915 (14.298–23.83)*
SK-Regular-32	Encryption	2^{128}	62	1,024	0.0165 (0.198–0.33)	0.0099 (0.119–0.198)
SK-Regular-64	Encryption	2^{256}	79	4,096	0.0518 (0.622–1.036)	0.0311 (0.373–0.622)
SK-Regular-128	Encryption	2^{512}	98	16,384	0.1672 (2.006–3.344)	0.1003 (1.204–2.006)*
SK-Regular-256	Encryption	2^{1024}	119	65,536	0.5507 (6.608–11.014)	0.3304 (3.965–6.608)*
PK-LF-32	Encryption	2^{128}	291	65,536	0.2252	0.1351
PK-LF-64	Encryption	2^{256}	395	524,288	1.3273	0.7964*
PK-LF-128	Encryption	2^{512}	515	4,194,304	8.1443	4.8866*
PK-LF-256	Encryption	2^{1024}	651	33,554,432	51.5429	30.9257*
PK-SF-32	Encryption	2^{128}	110	1,024	0.0093	0.0056
PK-SF-64	Encryption	2^{256}	128	4,096	0.0320	0.0192
PK-SF-128	Encryption	2^{512}	148	16,384	0.1107	0.0664
PK-SF-256	Encryption	2^{1024}	168	65,536	0.3901	0.2341*
DS-LF-32	Signing	2^{128}	816	327,680	0.4016	0.2409*
DS-LF-64	Signing	2^{256}	1,155	2,621,440	2.2696	1.3618*
DS-LF-128	Signing	2^{512}	1,568	20,971,520	13.3747	8.0248*
DS-LF-256	Signing	2^{1024}	2,061	167,772,160	81.4033	48.8420*
DS-SF-32	Signing	2^{128}	193	5,120	0.0265	0.0159
DS-SF-64	Signing	2^{256}	224	20,480	0.0914	0.0549
DS-SF-128	Signing	2^{512}	257	81,920	0.3188	0.1913*
DS-SF-256	Signing	2^{1024}	290	327,680	1.1299	0.6780*

Table 1: TANIA Performance on 1 GHz FPGA vs. VCK190 at 600 MHz AI Engine. Throughput = (Transmission Rate [Bits/Cycle] × Frequency) / 1000. SK-Light/SK-Regular with 12–20x parallelism (parentheses) reach 3–24 Tbps (1 GHz) and 3–18 Tbps (600 MHz). * indicates capping at 0.112 Tbps by VCK190's 112 Gbps transceivers.

Comparison with NIST Finalists on FPGA

Table 2: Symmetric and Lightweight: AES Pipelined and ASCON

System	Device	Resources (LUTs/FFs/BRAM/DSP)	Freq (MHz)	Throughput [Tbps] at 1 GHz AI Engine	Throughput [Tbps] at 600 MHz AI Engine (VCK190)
High-Speed AES Variants					
AES-128	Xilinx Spartan-III	17,425 slices / - / - / -	196	0.1279	0.0767
AES-192	Xilinx Spartan-III	17,425 slices / - / - / -	196	0.1279	0.0767
AES-256	Xilinx Spartan-III	17,425 slices / - / - / -	196	0.1279	0.0767
Low-Area AES Variants					
AES-128	Xilinx Spartan-II	124 slices / - / - / -	67	0.0328	0.0197
AES-192	Xilinx Spartan-II	124 slices / - / - / -	67	0.0328	0.0197
AES-256	Xilinx Spartan-II	124 slices / - / - / -	67	0.0328	0.0197
ASCON Variants					
ASCON-128 (Enc+Tag)	Xilinx Kintex-7	944 / 734 / - / -	181	-	-
ASCON-128 (Dec+Verify)	Xilinx Kintex-7	1058 / 735 / - / -	181	-	-

Table 2: AES and ASCON Performance, scaled to 1 GHz and VCK190 at 600 MHz AI Engine. AES block sizes: 128 bits (AES-128), 192 bits (AES-192), 256 bits (AES-256). AI Engine boosts throughput 2–3x (e.g., 25.1 Gbps to 127.9 Gbps at 1 GHz, 76.7 Gbps at 600 MHz).

Table 3: KEM: ML-KEM (CRYSTALS-Kyber)

Variant	Operation	Resources (LUTs/FFs/BRAM/DSP)	Cycles	Throughput [Tbps] at 1 GHz AI Engine	Throughput [Tbps] at 600 MHz AI Engine (VCK190)
ML-KEM-512 KeyGen		9,457 / 8,543 / 4.5 / 2,200	4	0.0019	0.00114
ML-KEM-512 Encapsulation		9,457 / 8,543 / 4.5 / 3,200	4	0.0019	0.00114
ML-KEM-512 Decapsulation		9,457 / 8,543 / 4.5 / 4,500	4	0.000079	0.000047
ML-KEM-768 KeyGen		10,530 / 9,837 / 6.5 / 2,600	/ 6	0.0027	0.00162
ML-KEM-768 Encapsulation		10,530 / 9,837 / 6.5 / 3,700	/ 6	0.0027	0.00162
ML-KEM-768 Decapsulation		10,530 / 9,837 / 6.5 / 4,900	/ 6	0.000065	0.000039

Table 3: ML-KEM Performance (full operations) on Artix-7 (220 MHz), scaled to 1 GHz and VCK190 at 600 MHz AI Engine. Throughputs in Tbps based on data sizes: ML-KEM-512 (768-byte public key/ciphertext for KeyGen/Encapsulation, 32-byte shared secret for Decapsulation), ML-KEM-768 (1,088-byte public key/ciphertext, 32-byte shared secret). Equivalent to 100–500 Mbps on PL-only (220 MHz). Not capped by transceivers.

Table 4: Digital Signatures: ML-DSA, Falcon, SLH-DS

System	Operation Resources	Cycles (LUTs/FFs/BRAM/DSP)	Throughput	
			[Tbps] at 1 GHz AI Engine	[Tbps] at 600 MHz AI Engine (VCK190)
ML-DSA-44	Signing	3,821 / 2,970 / 5 258,000 / 20	0.000075	0.000045
Falcon	Sampler (Sign)	15,400 / 9,300 / 22 7.5 / 254	-	-
SLH-DSA-SHAKE-128f	Signing	14,428 / - / 32 / - 4,903,978	Low	Low
SLH-DSA-SHAKE-128f	Verification	14,428 / - / 32 / - 440,636	Low	Low
SLH-DSA-SHAKE-128s	Signing	14,428 / - / 32 / - 102,346,701	Very low	Very low
SLH-DSA-SHAKE-128s	Verification	14,428 / - / 32 / - 179,603	Low	Low

Table 4: NIST Signature Schemes on Zynq UltraScale+ (131–322 MHz) and Artix-7 (100 MHz), scaled to 1 GHz and VCK190 at 600 MHz AI Engine. ML-DSA-44 Signing throughput in Tbps based on 2,420-byte signatures, scaled from ≈852 ops/sec at 220 MHz. Throughputs not capped by transceivers (below 0.112 Tbps).

Table 5: AES Regular Performance Details

System	Theo.	Quantum	Sec. Actual	Quantum	Sec. Cycles/Depth	Block Size [Bits]	Throughput [Tbps] at 1 GHz
Throughput [Tbps] at 600 MHz (VCK190)							
AES-128 0.00006 (0.00072–0.0012)	2 ⁶⁴		2 ⁸¹	1,280	128	0.0001 (0.0012–0.002)	
AES-192 0.00005 (0.0006–0.001)	2 ⁹⁶		2 ¹¹³	2,304	192	0.0000833 (0.001–0.0017)	
AES-256 0.0000428 (0.00051–0.00084)	2 ¹²⁸		2 ¹⁴⁵	3,584	256	0.0000714 (0.00086–0.0014)	

Table 5: AES Performance on 1 GHz FPGA and VCK190 at 600 MHz AI Engine. Block sizes: 128 bits (AES-128), 192 bits (AES-192), 256 bits (AES-256). Throughput = (Transmission Rate [Bits/Cycle] × Frequency) / 1000. AI Engine parallelism (12–20x) boosts throughput (parentheses).

Tables conclusion

The performance comparison between a 1 GHz FPGA and the AMD VCK190, operating at 600 MHz with an AI Engine, approximately 2 million LUTs, and 112 Gbps transceivers, reveals significant throughput differences for Tania

Post-Quantum Cryptography Systems and NIST finalists. These differences are driven by clock speed, AI Engine parallelism, and transceiver limitations, which are critical for meeting 6G requirements of over 1 Tbps throughput and sub-millisecond latency.

Tania systems leverage highly parallelizable matrix operations, including addition in 1 cycle, multiplication in 5 to 8 cycles, and inversion in 25 to 64 cycles. On a 1 GHz FPGA, TANIA-SK-Light decryption achieves 0.0427 to 1.9859 Tbps for 32 to 256-bit blocks, scaling to 3 to 24 Tbps with 12 to 20x AI Engine parallelism. For example, SK-Light-256 reaches 23.831 to 39.718 Tbps. TANIA-SK-Regular encryption delivers 0.0165 to 0.5507 Tbps, scaling to 1 to 12 Tbps, with SK-Regular-256 achieving 6.608 to 11.014 Tbps. TANIA- PK-LF and DS-LF provide up to 51.5429 Tbps for encryption and 81.4033 Tbps for signing with large block sizes, ranging from 65,536 to 33,554,432 bits. On the VCK190 at 600 MHz, throughputs are reduced by 0.6x: SK-Light achieves 0.0256 to 1.1915 Tbps base, scaling to 3 to 18 Tbps (e.g., SK-Light-256: 14.298 to 23.83 Tbps); SK-Regular achieves 0.0099 to 0.3304 Tbps base, scaling to 1 to 9 Tbps (e.g., SK-Regular-256: 3.965 to 6.608 Tbps). PK-LF-256 and DS-LF-256 yield 30.9257 Tbps and 48.842 Tbps, respectively. However, the VCK190's 112 Gbps transceivers cap high-throughput variants, such as SK-Light-128/256, PK-LF, and DS-LF, at 0.112 Tbps, requiring multiple transceivers or internal buffering to approach 6G targets.

NIST algorithms are limited by their sequential designs. On a 1 GHz FPGA, ML-KEM's full key generation, encapsulation, and decapsulation yield 0.0019 to 0.000079 Tbps for ML-KEM-512 and 0.0027 to 0.000065 Tbps for ML-KEM-768, based on 768-byte and 1,088-byte public keys/ciphertexts for Key-Gen/Encapsulation and 32-byte shared secrets for Decapsulation. At 600 MHz on the VCK190, these drop to 0.00114 to 0.000047 Tbps for ML-KEM-512 and 0.00162 to 0.000039 Tbps for ML-KEM-768, equivalent to 100 to 500 Mbps on PL-only FPGAs at 220 MHz. ML-DSA-44 full signing achieves approximately 0.000075 Tbps at 1 GHz and 0.000045 Tbps at 600 MHz, based on 2,420-byte signatures, significantly below TANIA's Tbps-scale throughputs. Falcon benefits from AI Engine-accelerated sampling, but its full signing throughput remains low. SLH-DSA's high cycle counts, in the millions per signature, make it impractical for 6G. AES with 128 to 256-bit blocks achieves 0.0000714 to

0.0001 Tbps base at 1 GHz, scaling to 0.00086 to 0.002 Tbps with 12 to 20x parallelism, and 0.0000428 to 0.00006 Tbps base at 600 MHz, scaling to 0.00051 to 0.0012 Tbps, all far below 6G requirements.

The Versal AI Engine, with 400 tiles, 512-bit SIMD, 165 TOPS at 1 GHz, and 124 TOPS at 600 MHz, provides 12 to 20x speedups for TANIA's matrix operations and 3 to 9x for NIST's vector processing and hashing. TANIA's high parallelism, such as SK-Light-256 achieving 23.831 to 39.718 Tbps at 1 GHz and 14.298 to 23.83 Tbps at 600 MHz, far exceeds NIST's capabilities, with ML-KEM and ML-DSA remaining in the Mbps range when expressed as Tbps.

The VCK190's 112 Gbps transceivers limit high-throughput algorithms, such as TANIA-PK-LF-256, DS-LF-256, and ML-DSA, to 0.112 Tbps, a significant constraint compared to the 1 GHz FPGA's uncapped potential, such as 51.5429 Tbps for PK-LF-256. Multiple transceivers or advanced buffering are needed to fully utilize TANIA's computed throughputs on the VCK190.

Achieving 1 to 2 GHz FPGAs by 2030 is feasible with 3nm to 2nm process nodes, over 500 AI Engine-like tiles, and optical interconnects, such as 400 Gbps transceivers, eliminating the 112 Gbps bottleneck. The FPGA market's projected growth to 20 billion \$ by 2030, driven by AI and 6G demands, supports this scalability. TANIA's throughputs of 3 to 24 Tbps for SK-Light, 1 to 12 Tbps for SK-Regular, and up to 81.4033 Tbps for DS-LF at 1 GHz, alongside NIST's low Tbps-scale ML-KEM and ML-DSA, will be fully realizable with future hardware, meeting 6G requirements. At 600 MHz, the VCK190 delivers significant but capped performance, necessitating advancements.

Real-world TANIA implementations require validation to confirm Tbps claims. NIST algorithms, particularly ML-KEM and ML-DSA, need optimization, such as parallelizing sequential steps, to approach 6G targets. Hybrid designs combining TANIA's high throughput with NIST's standardized security offer a promising path for quantum-resistant 6G network.

8. Use-cases & examples

8.1 Defense Sector

National defense and intelligence agencies rely on secure communication, data protection, and mission-critical systems. Quantum-vulnerable encryption exposes armies, intelligence agencies, and counterterror operations to severe risks if adversaries intercept classified data. Tania's chip ensures real-time, quantum-resilient communication and secure storage of sensitive information.

Example: Imagine an IDF soldier in the field transmitting live drone footage and coordinates to his commander. Even if the enemy intercepts the data, with Tania's chip the communication remains quantum-proof. Now picture a Mossad agent in a foreign country gathering highly sensitive intelligence. Traditionally, transferring gigabytes of encrypted files back to headquarters could expose the agent to detection or, worse, allow adversaries to harvest the data for future decryption. With Tania's chip, the agent can instantly transfer massive amounts of classified data at ultra-high speeds. Even if the transmission is intercepted, not even the most advanced quantum computer could break it, ensuring the agent remains undetected and the mission uncompromised.

8.2 Financial Sector

Banks and financial institutions manage trillions in daily transactions. Quantum attacks on authentication systems, trading platforms, or payment infrastructures could destabilize entire economies. Tania's chip delivers secure, high-speed, low-latency quantum-safe encryption for financial networks and ATM infrastructures.

Example: Imagine a bank customer logging into their account to transfer money. Without post-quantum protection, that transaction could be harvested and stolen once quantum computers mature. With Tania Systems, the customer's login, transfer request, and confirmation remain fully secure, protecting both the individual and the bank from catastrophic fraud.

8.3 Health Sector

Hospitals and health organizations store sensitive medical records and operate life-critical systems that cannot be compromised. Post-quantum security ensures data confidentiality, patient safety, and secure operation of connected devices.

Example: Imagine a hospital doctor pulling up a patient's digital file during an emergency surgery. With Tania's chip securing the hospital's servers, there is no risk that this sensitive medical data could be stolen today and revealed years later. Even connected medical devices like pacemakers remain safe from outside interference.

8.4 Cryptocurrencies

Blockchain systems rely heavily on public-key cryptography. A quantum computer could break digital signatures and steal funds or rewrite entire blockchains. Tania's chip enables quantum-resistant wallets, exchanges, and consensus protocols.

Example: Imagine a cryptocurrency trader holding millions in Bitcoin. A hacker could one day use a quantum computer to break his wallet's keys and drain the account instantly. Google's Willow chip, despite being a research breakthrough, has already demonstrated computational capabilities that raise alarms around the future of blockchain security. With Tania Systems embedded into wallets and exchanges, digital assets remain locked and secure, no quantum attacker can touch them.

8.5 Autonomous Vehicles

Self-driving cars rely on constant secure communication with cloud systems, sensors, and infrastructure. A quantum attack could manipulate or take over vehicles remotely. Tania's chips secure these communications and onboard systems against both classical and quantum threats.

Example: Imagine an autonomous car driving through Tel Aviv, communicating with traffic lights, GPS satellites, and other cars. If a hacker intercepted or manipulated those signals, the results could be deadly. With Tania's chip, every

command and update is secured, keeping passengers safe from quantum-age hijacking.

8.6 Drones

Military and civilian drones transmit sensitive video feeds and navigation data. Without quantum-safe security, intercepted drone communications could be manipulated or weaponized. Tania provides resilient, low-latency encryption for drones operating in critical missions.

Example: Imagine a surveillance drone flying over the Gaza border, sending real-time video back to its operator. Without quantum security, an adversary could intercept or alter the feed. With Tania's chip, the video remains tamper-proof and the mission stays uncompromised.

8.7 Aviation Industry

Airlines and aviation systems rely on secure communications, from air traffic control to aircraft avionics. Quantum vulnerabilities could threaten passenger safety and logistics. Tania's chips secure cockpit communication, flight data, and aviation networks.

Example: Imagine a pilot flying a packed passenger jet. The aircraft is in constant communication with ground control. A single compromised channel could cause chaos. With Tania's chip embedded in aviation systems, both pilots and passengers are protected from quantum-era sabotage.

8.8 Robotics

Robotics in manufacturing, healthcare, and defense depend on secure command-and-control systems. If compromised, robots can be manipulated to disrupt production, harm patients, or undermine operations. Tania ensures commands and data remain tamper-proof.

Example: Imagine a robotic arm in a car factory building vehicles. A hacker interfering with its instructions could halt production or cause dangerous malfunctions. With Tania Systems, every instruction is verified and secure, ensuring the robots only follow trusted commands.

8.9 Artificial Intelligence

AI systems process massive datasets, including sensitive personal, financial, or national security information. A quantum attack could compromise model integrity, data privacy, or decision-making systems. Tania's chips safeguard both data pipelines and AI model parameters.

Example: Imagine a defense AI system analyzing incoming satellite data to detect threats. If an adversary tampered with the AI's input, it could miss critical warnings. With Tania's chip, the data feeding the AI remains intact and trustworthy, ensuring accurate real-time decisions.

8.10 Chip Manufacturers

As semiconductor companies adopt post-quantum standards, integrating Tania's patented cryptographic architecture into their designs gives them an advantage in compliance and performance.

Example: Imagine a global chipmaker embedding Tania's architecture directly into next-generation processors. Every device built with those chips — from smartphones to servers, would have built-in quantum-resistant security, creating a new standard across industries.

9. Market

9.1 Market opportunity

The demand for post-quantum cryptography (PQC) is about to follow the same trajectory as artificial intelligence did in 2015. Back then, AI was considered experimental, and few believed it would disrupt entire industries so quickly. Those who invested early became the global leaders once AI exploded into the mainstream. The same shift is about to happen here.

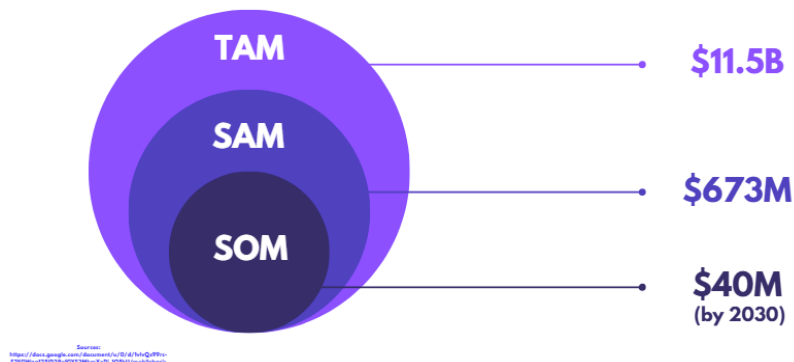
Quantum computing is not a theoretical threat, it is inevitable. Once these machines reach maturity, the entire foundation of RSA and ECC will collapse instantly. Governments, banks, healthcare providers, and enterprises will have no choice but to adopt PQC solutions. Standards bodies such as NIST, NATO, and the

EU are already preparing for this shift, and with the arrival of 6G networks, encryption at 1 Tb/s speeds will become mandatory. Companies that position themselves early will dominate a market that is destined to become a global necessity.

9.2 Market size

According to research, the global **Total Addressable Market (TAM)** for quantum-safe security is **\$11.5 billion**, covering all industries worldwide that require post-quantum protection. The **Serviceable Available Market (SAM)**, which focuses specifically on hardware acceleration and PQC-ready infrastructures, is valued at **\$673 million**. Within this segment, Tania Systems is targeting a **Serviceable Obtainable Market (SOM)** of **\$40 million by 2030**, driven by our unique ability to deliver chip-level, high-throughput protection that surpasses software-only competitors.

This may appear modest at first glance, but like cloud computing or AI in their early days, PQC hardware will grow rapidly as adoption becomes inevitable. Regulations, industry standards, and the increasing need for ultra-fast, quantum-proof security will transform this market into one of the most critical technology stacks of the decade.



10. Go-to-market strategy

10.1 Certificate strategy

A core part of Tania Systems' roadmap is achieving official recognition and certification from the U.S. National Institute of Standards and Technology (NIST). Certification will position Tania as a globally trusted provider not only of quantum-safe cryptography but also of high-performance solutions capable of meeting the massive transmission demands of the future.

Our plan is structured in phases. First, we will initiate the multi-year NIST PQC standardization process by submitting Tania's algorithms and hardware implementations for review. This process involves rigorous peer evaluation, independent testing, and alignment with global standards. Our long-term goal is to secure certification that ensures wide adoption in civil, commercial, and government infrastructures worldwide. By combining quantum safety with proven 1 Tb/s throughput, we will stand out from competitors who may achieve security but not the performance required for 6G and beyond.

10.2 Field-proven trust strategy

While NIST certification is the formal recognition pathway, we also know that companies, governments, and defense agencies demand field-proven trust before widespread adoption. Tania Systems will build credibility by showing that our systems not only resist quantum attacks but also handle extreme data volumes without performance loss.

This strategy has three components. First, we will openly publish Tania's algorithms for global review, demonstrating transparency and academic rigor. Second, we will engage external cybersecurity experts to test and validate both the security strength and the throughput capacity of our systems. Third, we will focus on early adoption by high-trust sectors such as the Israel Defense Forces (IDF), Rafael, and Elbit. Real-world use by these organizations will prove that Tania can secure critical data at unprecedented speeds, creating confidence for other sectors to follow.

By pursuing both certification and field-proven validation, Tania Systems builds a dual track of credibility. Certification ensures long-term recognition on the global stage, while early adoption in demanding environments demonstrates immediate reliability and speed. Together, these strategies create a pathway for Tania to become the recognized global standard in quantum-safe, high-throughput cryptography.

10.3 Product development

Tania Systems' product development roadmap is designed to ensure a fast, reliable, and scalable transition from research to commercial deployment. Our approach begins with proving the technology on existing platforms, then refining it into proprietary hardware and full-stack solutions.

Phase 1: Hardware Prototyping (0–12 months)

During the first **6 to 12 months**, we will focus on implementing our algorithms on **FPGA boards and GPUs**. These platforms allow rapid iteration, real-time testing, and performance benchmarking of our cryptographic designs. In parallel, we will launch our **SaaS API model**, integrating Tania's solutions into **cloud environments** so early partners and customers can easily experiment with quantum-safe acceleration at scale. This usage-based approach provides immediate access, lowers adoption barriers, and begins generating recurring revenue from day one.

This hybrid phase, combining FPGA/GPU prototyping with SaaS delivery, offers both flexibility and speed, while avoiding the high upfront costs of custom silicon fabrication. It allows Tania to validate technology, prove market demand, and establish early revenue streams before transitioning into large-scale hardware and ASIC production.

Phase 2: Adding custom chips production & sales (12–24 months)

Once our FPGA, GPU, and software implementations are validated, we will

begin **chip production and sales** of custom **post-quantum cryptographic hardware**. This step involves close collaboration with semiconductor manufacturing partners to translate our parallelized designs into silicon. The result will be purpose-built chips capable of delivering both quantum resistance and 1 Tb/s throughput at lower power consumption and higher efficiency than any software-based solution.

Phase 3: Full-Stack Ecosystem (24+ months)

In parallel with chip development, we will continue building the **software and board ecosystem that surrounds our hardware**. This includes SDKs for easy integration, cloud-ready implementations, and development boards for partners in defense, finance, healthcare, and telecommunications. By providing not just chips but complete platforms, we ensure that organizations can adopt Tania's technology seamlessly into their infrastructure.

Commercialization Timeline

Sales of initial products will begin once our FPGA/GPU-based prototypes are validated, targeting early adopters in high-trust sectors such as defense and financial institutions. These early deployments will generate field-proven results that strengthen our credibility with both NIST and global commercial markets. As we transition into custom silicon, sales will expand into larger enterprise and consumer markets, supported by our certification and partnership strategy.

10.4 Unit Cost & Profitability Table

Phase	Price per Unit	Cost Unit	per Gross Margin	Goal
2026–2027, Penetration	\$15,000	\$14,700	~2%	Adoption & Validation
2028–2029, Optimization	\$13,500–11,000	\$8,000–4,100	~60%	Scaling with better unit economics
2030, Profitability	\$10,000	\$1,948	~80%	Strategic profitability at volume

11. Business and Financial plan.

11.1 Investment strategy

a. Cost of Goods Sold (COGS)

A significant portion of the investment will go directly into the technical foundation of our prototype development:

- **FPGA Development Kit & Programmer Tools:** Purchase of Intel Agilex 7 F-Series kit and programming hardware to build, test, and refine the first prototypes.
- **FPGA/Hardware Engineering:** Covering RTL design, synthesis, and integration for a twelve-month period to ensure optimal performance.
- **Software Engineering:** Investment in cloud infrastructure and computational resources required for large-scale testing, algorithm simulations, and integration into SaaS environments. This includes costs for cloud hosting, GPU instances, storage, and security layers necessary to support development and deployment of our quantum-resistant

solutions.

- **Founders' Salary:** Compensation for the founders, who are leading, dedicated to building and promoting the startup while driving its technical and business growth.

This ensures we have both the hardware and engineering manpower required to create and test the first fully functional FPGA and software-based system.

b. Operating Expenses (OPEX)

We are also investing in the operational backbone needed to run as a company:

- **General Operations:** Core administrative, sales, marketing, and operational expenses to support day-to-day activities and early business development.
- **Legal & Accounting:** Costs for incorporation, legal entity setup, audit, and annual reporting.
- **Facilities:** Rental of a shared office/lab environment for twelve months to host the team and equipment.

These expenses establish the formal, legal, and technical framework to operate as a company while keeping overhead lean.

c. Capital Expenditures (CAPEX)

The investment will also cover specialized hardware and infrastructure:

- **Power, Cooling & Peripherals:** High-speed fans, heat sinks, power supplies, and cables needed to ensure stability of prototypes under

testing conditions.

- **Development Workstation:** A high-performance PC for simulation, design runs, and synthesis tasks.

This ensures that the team has the physical infrastructure required to handle heavy computational loads and long testing cycles.

d. Contingency Fund (10%)

Finally, we are setting aside a cash buffer for unexpected costs, such as additional components, licensing updates, or unforeseen integration challenges. This adds flexibility and reduces risk during the prototype stage.

In summary: Investor funds in 2025 will be carefully distributed across prototype development (COGS), operational setup (OPEX), lab equipment (CAPEX), and contingency reserves. This allocation ensures we can deliver a working FPGA and software prototype, validate our algorithms, and lay the groundwork for scaling into ASIC production.

11.2 Revenue & Potential ROI

Tania Systems is projecting a total revenue of **\$56.1 million USD between 2025 and 2030**.

Monetization begins in **2026** with the sale of **40 units** (physical FPGA boards with our algorithms implemented), generating **\$600,000 in revenue**. In parallel, our software will follow a usage-based subscription model (per request / per throughput tier), creating a recurring revenue stream. By the end of **2028**, we anticipate reaching **break-even**, supported by rapid revenue scaling, growing from **\$600K in 2026 to \$30M annually by 2030**.

By 2030, this growth trajectory delivers an estimated **ROI of ~35.8x (3580%)**.

To realize this potential, we are currently seeking an investment of **\$600,000**

USD, which will directly support our path toward adoption, scaling, and profitability at volume.

12. Looking Ahead

At Tania Systems, we believe the future of cybersecurity is not only about protecting data, it is about building the foundation for trust in a quantum world. The challenges ahead are vast, but so is the opportunity. With every line of code, every prototype, and every step toward silicon, we are shaping technology that will safeguard nations, industries, and individuals for decades to come.

Our vision is bold: to lead the transition to post-quantum security at scale, delivering unmatched speed, efficiency, and resilience. With the right partners and investors by our side, Tania Systems will not only capture a global market, we will set a new standard for security in the digital age.

The journey is just beginning, and we invite you to be part of building the future!

13. Key Sources

<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards#:~:text=The%20three%20new%20standards%20are,individuals%2C%20organizations%20and%20entire%20nations>

<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards#:~:text=The%20standards%20%E2%80%94%20containing%20the,it%20carries%20threats%20as%20well>

<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards#:~:text=current%20encryption%20that%20provides%20security,are%20ready%20for%20immediate%20use>

<https://www.cryptomathic.com/blog/nist-pqc-finalists-update-its-over-for-the-rainbow#:~:text=published%20a%20practical%20key%20recovery,against%20the%20Rainbow%20signature%20scheme>

<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards#:~:text=GAITHERSBURG%2C%20Md,cyberattacks%20from%20a%20quantum%20computer>

<https://www.marketsandmarkets.com/Market-Reports/quantum-cryptography-market-45857130.html#:~:text=The%20global%20quantum%20cryptography%20market,based%20quantum>

<https://www.marketsandmarkets.com/Market-Reports/quantum-cryptography-market-45857130.html#:~:text=The%20global%20quantum%20cryptography%20market,IoT%20devices%20and%20digital%20technologies>

<https://www.statista.com/statistics/1332857/quantum-security-market-revenue/>

<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-communication-growth-drivers-cybersecurity-and-quantum-computin>

g

<https://www.precedenceresearch.com/post-quantum-cryptography-market>

<https://www.alliedmarketresearch.com/hardware-encryption-market#:~:text=The%20global%20hardware%20encryption%20market,used%20for%20securing%20digital%20data.>

<https://straitsresearch.com/report/hardware-encryption-market>