Project 90

LATEST — 04 DEC 2025

Squeezing Every Millisecond: A Practical Guide to TLS Optimization

You've done everything right. You've built a sleek application, containerized it, and deployed it behind a robust service mesh. But something feels... off. Your services are secure, but they feel just a little sluggish. That tiny bit of latency can be a real killer, and the culprit might be hidin...

5 MIN READ

MORE ISSUES

Could LLVM Finally Fix Crypto's Nagging Side-Channel Problem?

In the world of cryptography, some of the most devastating attacks don't break the math—they exploit the hardware it runs on. Timing attacks, a sneaky type of side-channel vulnerability, can leak secret keys just by measuring how long a computer takes to perform a calculation. For years, develope...

03 DEC 2025 4 MIN READ

Rethinking Remainder: Could a Simple Math Trick Supercharge Modern Crypto?

A developer recently sparked a fascinating debate by proposing a new take on modular arithmetic, a cornerstone of digital security. Dubbed 'REIST Division,' this method promises a staggering 6x speedup for polynomial additions, a critical operation in modern lattice-based cryptography like Kyber ...

01 DEC 2025 4 MIN READ

Is the NSA Hiding a Backdoor in Our Quantum-Proof Future? The ML-KEM Debate

The crypto world is on edge. As we race to build defenses against quantum computers, a new standard called ML-KEM is taking center stage. But with it comes a heavy dose of paranoia, and for good reason. History has taught us to be wary of government involvement in encryption standards, with the i...

30 NOV 2025 5 MIN READ

Crypto's Civil War: Why the Fight Over New Standards Is About Old Ghosts

A storm is brewing in the world of cryptography, and it's not just about complex math or the looming threat of quantum computers. It's about trust. A heated debate is unfolding around the standardization of post-quantum cryptography (PQC), the next generation of encryption meant to keep us safe. ...

26 NOV 2025 4 MIN READ

The Uncrowned King: Why Isn't ChaCha20 NIST-Approved?

Ever noticed that little padlock in your browser? Behind it are powerful encryption algorithms working tirelessly. One of the big names is ChaCha20, used by tech giants and securing countless connections every second. So, you'd assume it has the official stamp of approval from the U.S. National I...

24 NOV 2025 4 MIN READ

Oops, We Lost the Votes: The Digital Election Fiasco and Crypto's Human Problem

Imagine casting your vote in a local election, confident in the security of a modern, encrypted system. Now imagine getting a notification that the entire election is being redone... because someone lost the digital key. It sounds like a plot from a sitcom, but it's a real story that has people a...

22 NOV 2025 4 MIN READ

Can you profit on the sports card marketplace?

The sports card marketplace has re-emerged as a mainstream digital economy The sports card marketplace has re-emerged as a mainstream digital economy where collectors, flippers, and investors meet. Over the past five years, the hobby has exploded online, driven by celebrity endorsements, pandemic-era collecting, and new platforms that make buying

22 NOV 2025 5 MIN READ

What Can AI activism Change Today?

AI Activism: A Rising Movement AI activism is rising fast, and it matters more than ever. Across cities and online forums, citizens, researchers, and workers are pushing for safer, fairer, and more transparent artificial intelligence. They demand accountability for algorithms, protections for jobs and privacy, and clear rules for powerful

22 NOV 2025 6 MIN READ

Go, Rust, and the Secret Hardware Tricks Making Your Crypto Safer

Ever wonder what's happening behind the scenes to keep your digital life secure? It's not always about flashy new apps. Sometimes, the most important changes are deep in the code and silicon. We're taking a look at the latest in Go's cryptography, including the huge move to make RSA signing 'cons...

22 NOV 2025 4 MIN READ

Load more issues

ABOUT

Project 90

Cryptocurrency innovations, blockchain advancements, and Web3 trends. Stay updated with expert insights on DeFi, NFTs, smart contracts, and emerging crypto tech shaping the future of finance.

FEATURED

Squeezing Every Millisecond: A Practical Guide to TLS Optimization

You've done everything right. You've built a sleek application, containerized it, and deployed it behind a robust service mesh. But something feels... off. Your services are secure, but they feel just a little sluggish. That tiny bit of latency can be a real killer, and the culprit might be hidin...

04 DEC 2025 5 MIN READ

Could LLVM Finally Fix Crypto's Nagging Side-Channel Problem?

In the world of cryptography, some of the most devastating attacks don't break the math—they exploit the hardware it runs on. Timing attacks, a sneaky type of side-channel vulnerability, can leak secret keys just by measuring how long a computer takes to perform a calculation. For years, develope...

03 DEC 2025 4 MIN READ

Rethinking Remainder: Could a Simple Math Trick Supercharge Modern Crypto?

A developer recently sparked a fascinating debate by proposing a new take on modular arithmetic, a cornerstone of digital security. Dubbed 'REIST Division,' this method promises a staggering 6x speedup for polynomial additions, a critical operation in modern lattice-based cryptography like Kyber ...

01 DEC 2025 4 MIN READ

Is the NSA Hiding a Backdoor in Our Quantum-Proof Future? The ML-KEM Debate

The crypto world is on edge. As we race to build defenses against quantum computers, a new standard called ML-KEM is taking center stage. But with it comes a heavy dose of paranoia, and for good reason. History has taught us to be wary of government involvement in encryption standards, with the i...

30 NOV 2025 5 MIN READ

Crypto's Civil War: Why the Fight Over New Standards Is About Old Ghosts

A storm is brewing in the world of cryptography, and it's not just about complex math or the looming threat of quantum computers. It's about trust. A heated debate is unfolding around the standardization of post-quantum cryptography (PQC), the next generation of encryption meant to keep us safe. ...

26 NOV 2025 4 MIN READ

TOPICS

AES	2 issues
AI	20 issues
AMD	1 issue
API Changes	2 issues
Argon2id	1 issue

ARM	2 issues
Authentication	2 issues
Automation	2 issues
blockchain	6 issues
Blockchain Technology	1 issue
Business Ideas	16 issues
career advice	2 issues
CBDC	1 issue
centralization	1 issue
ChaCha20	2 issues
ChaCha20-Poly1305	1 issue
Chinese Remainder Theorem	1 issue
CIRCL	1 issue
Cloudflare	1 issue
community building	1 issue
Community Management	1 issue
computer science	2 issues
Constant-Time	2 issues
crypto	2 issues
Crypto Community	1 issue
crypto developer	1 issue
crypto-pragmatism	1 issue
Cryptocurrency	4 issues
cryptography	24 issues
cryptozoology	2 issues

Cybersecurity	17 issues
DAOs	1 issue
Data Security	2 issues
decentralization	3 issues
decentralized social media	1 issue
defense in depth	1 issue
DevOps	1 issue
Digital Euro	1 issue
digital migration	1 issue
Digital Privacy	1 issue
digital security	2 issues
Dilithium	1 issue
double ratchet	1 issue
Dual EC DRBG	1 issue
Dual_EC_DRBG	1 issue
ECB	1 issue
ECC	1 issue
Education	1 issue
Election Security	1 issue
Elon Musk	1 issue
encryption	11 issues
End-to-End Encryption	1 issue
Entropy	1 issue
ethereum	1 issue
European Union	1 issue

FEAT_DIT	1 issue
Financial Technology	1 issue
forward secrecy	1 issue
future of tech	1 issue
Go	1 issue
Groth16	1 issue
Halo2	1 issue
Hardware Security	1 issue
HMAC	1 issue
Human Error	1 issue
IETF	2 issues
internet culture	1 issue
Invalid Curve Attack	1 issue
Istio	1 issue
JavaScript	1 issue
Key Management	1 issue
Kyber	1 issue
language	1 issue
lattice-based cryptography	1 issue
layer-2	1 issue
Lemmy	2 issues
length-extension	1 issue
Linux	1 issue
Linux Kernel	1 issue
LLVM	1 issue

long-term thinking	1 issue
math	1 issue
mathematics	1 issue
Merkle-Damgard	1 issue
Mike Rosulek	1 issue
ML-KEM	1 issue
mls	1 issue
moderation	1 issue
modular arithmetic	2 issues
NEON	1 issue
networking	1 issue
Nginx	1 issue
NIST	3 issues
NSA	3 issues
Online Communities	2 issues
Open Access	1 issue
Open Source	2 issues
P2P	1 issue
p2p messaging	1 issue
passkeys	1 issue

Sign up

LInk 1

Powered by Ghost