BULLETPROOFS

BÜNZ BOOTLE BONEH POELSTRA WUILLE MAXWELL

Confidential Transactions

- Confidential Transactions: replacing output amounts with *Pedersen commitments*
- Publicly verifiable that transactions balance.
- Specific amounts are zero-knowledge.
- Amounts must be encoded as integers mod q, which can overflow. To prevent this we use a *rangeproof*.

Rangeproofs from Ring Signatures

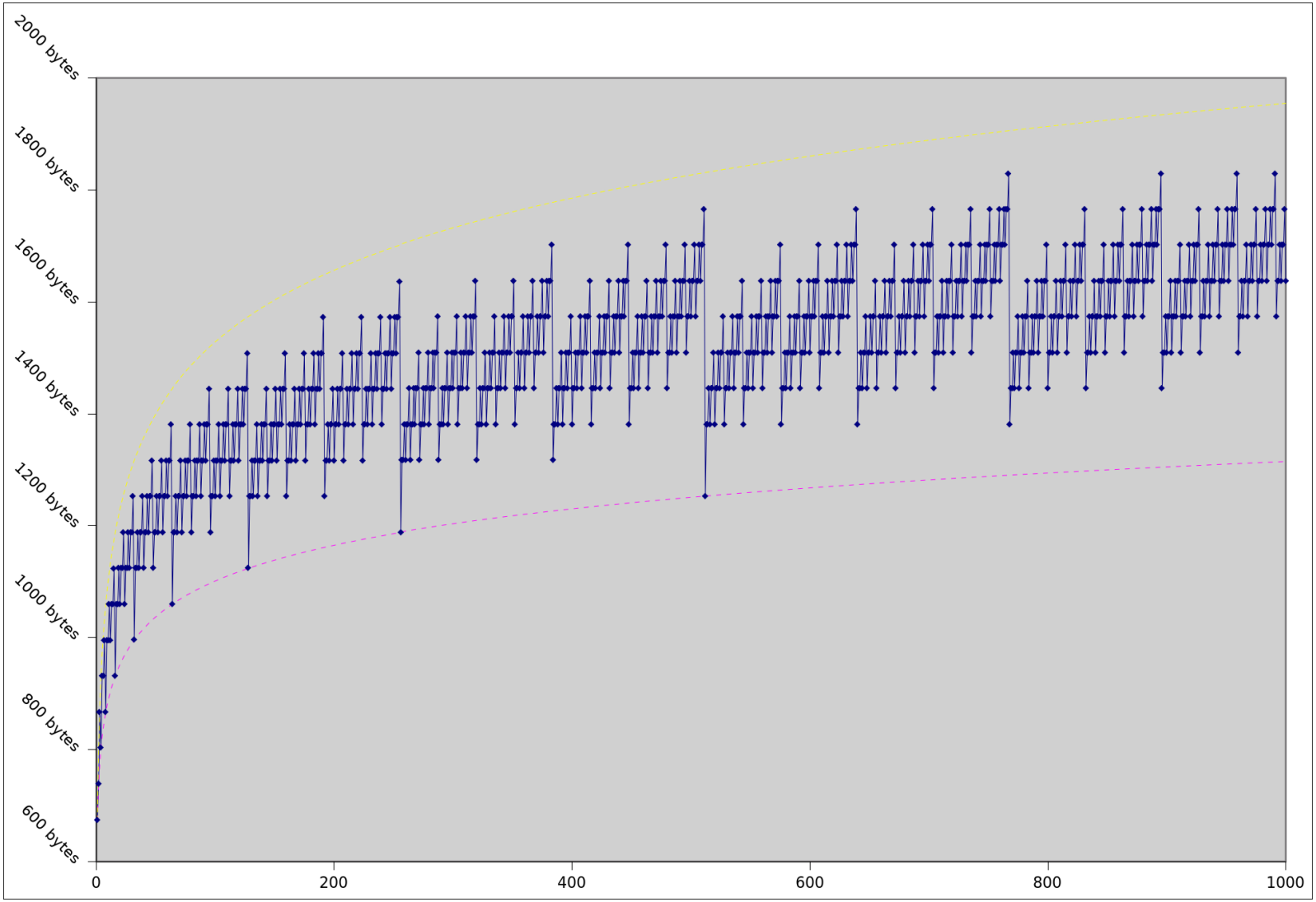
- Idea: split numbers into 64 bits. Hide the bits with more Pedersen commitments.
- Prove these commitments are actually bits.
- Do this with a *ring signature* on each bit commitment.
- Size: 80 bytes per bit. 5Kb for 64 bits.
- Verify time: 91μs per bit. 5.8ms for 64 bits.

Rangeproofs from Inner Products

- Idea: hide all the bits in a single *vector* Pedersen commitment.
- Prove each bit satisfies $x(x-1) = 0$. And that they sum to v.
- Express these conditions as an inner product.
- Take an efficient inner product argument (Bootle 2016), simplify it, shrink its size, make it work with Pedersen commitments.

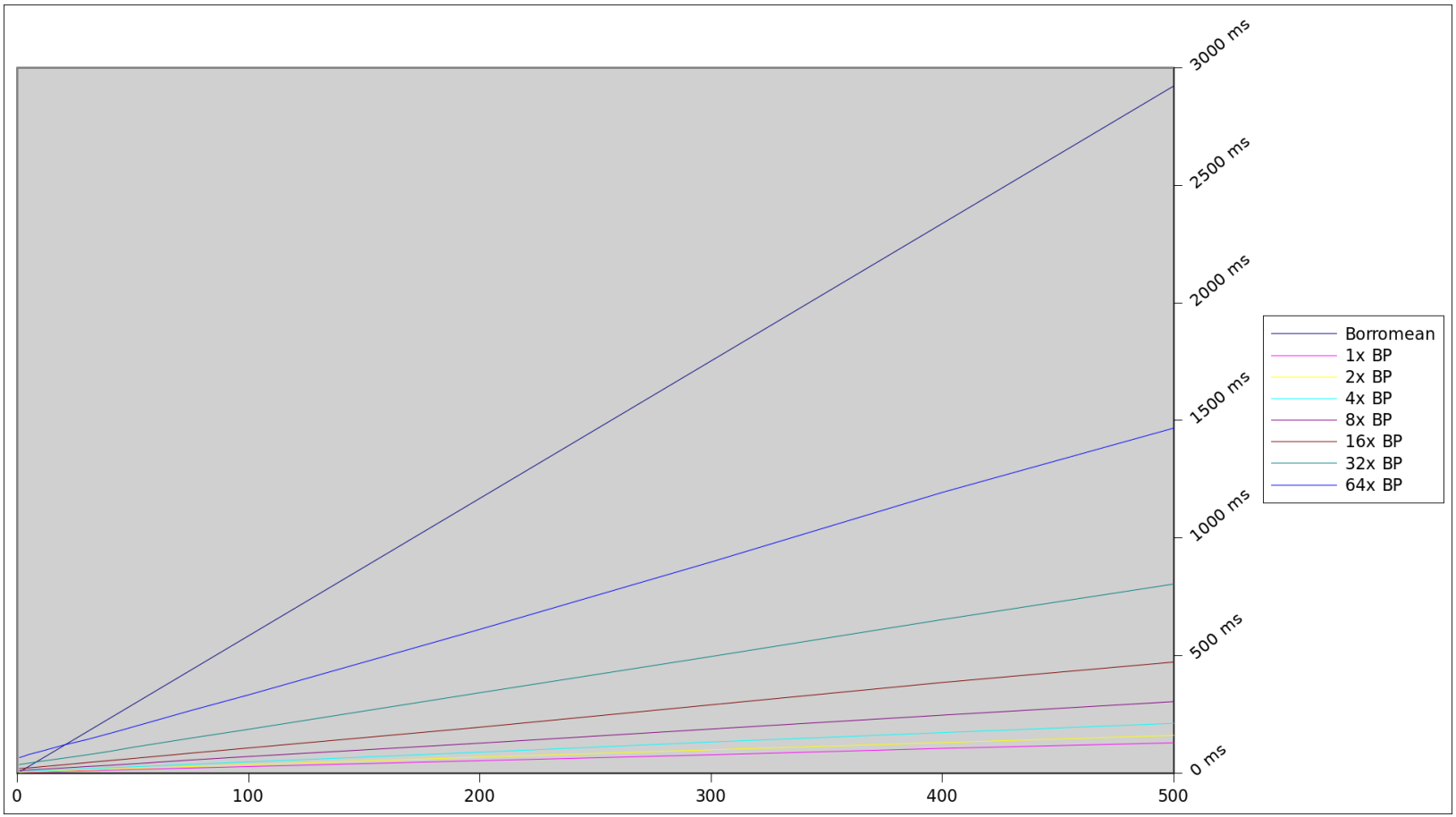
Bulletproofs: size

Size: logarithmic in the number of bits; can be aggregated.



Bulletproofs: size

Verify time: sublinear in the number of bits; can be batch verified



Arithmetic Circuits

- Inner products can prove much more than just ranges.
- Any algorithm with known running time.
- As expressive as SNARKs, STARKs, ZKBoo, etc.
- Small proofs (couple kb), fast-ish verification, fast-ish proving

Hash Preimages

- SHA-256 (512 bits): 21s to prove, 441ms to verify, 39ms to batch-verify
- Pedersen Hash (a la ZCash) (768 bits): 1.35s to prove, 72ms to verify, 5ms to batch-verify
- $\sim$ 2Kb for both these proofs

Applications

- Rangeproofs, of course
- Merkle proofs
- Proof of solvency
- Multisig with deterministic nonces
- Scriptless Scripts (with ECDSA in some cases)
- Assets / smart contracts / crypto-derivatives

Thank You

Andrew Poelstra <grindelwald@wpsoftware.net>