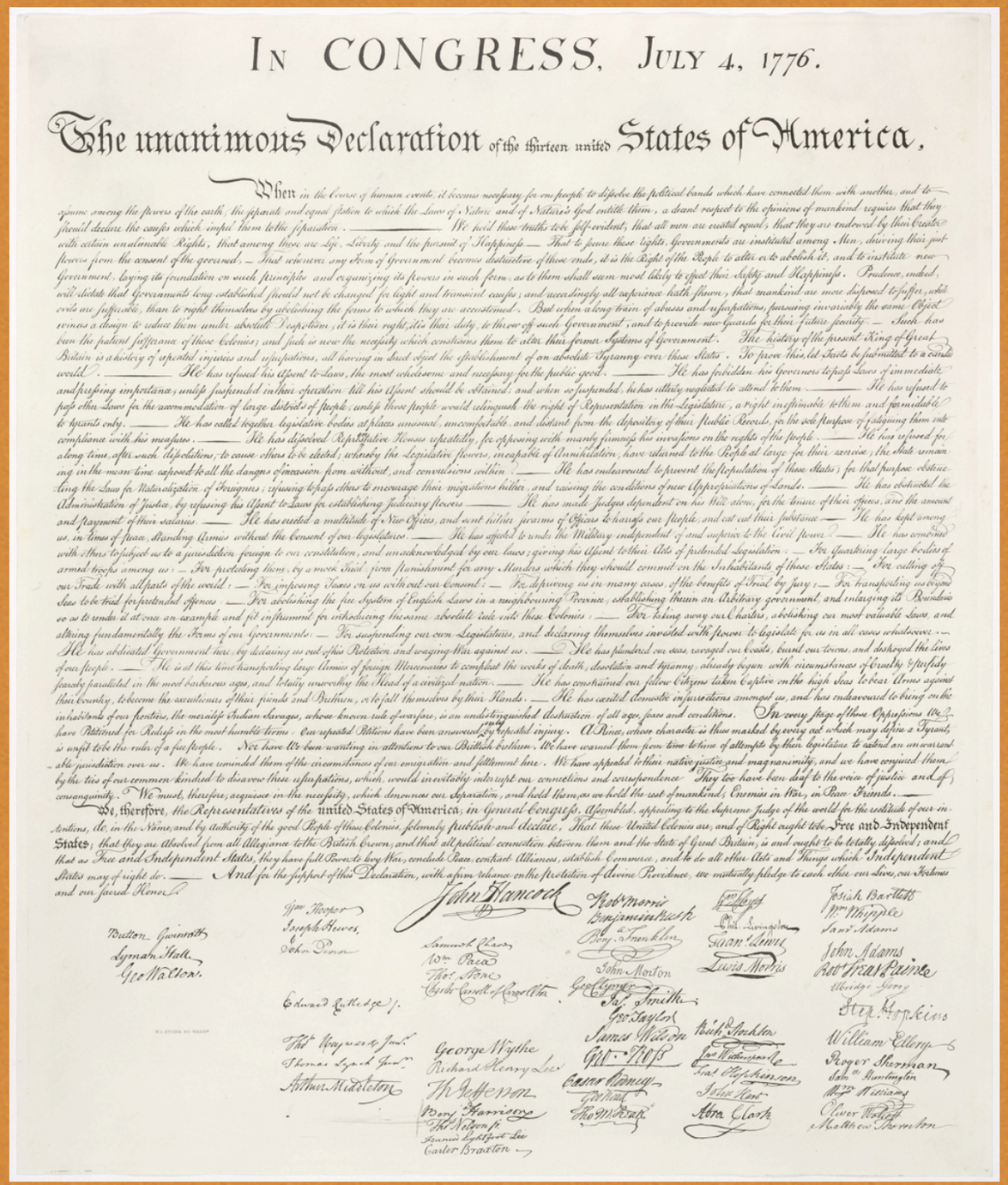
ORDERED MULTISIGNATURES AND IDENTITY-BASED SEQUENTIAL AGGREGATE SIGANTURES

Alexandra Boldyreva (Georgia Tech)
Craig Gentry (Stanford)
Adam O'Neill (Georgia Tech)
Dae Hyun Yum (POSTECH, Korea)

- When people sign a document, *order can matter*.



IN CONGRESS, JULY 4, 1776.

The unanimous Declaration of the thirteen united States of America.

When in the Course of human events, it becomes necessary for one people to dissolve the political bands which have connected them with another, and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation. — We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. — That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, — That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn, that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security. — Such has been the patient sufferance of these Colonies; and such is now the necessity which constrains them to alter their former Systems of Government. The history of the present King of Great Britain is a history of repeated injuries and usurpations, all having in direct object the establishment of an absolute Tyranny over these States. To prove this, let Facts be submitted to a candid world. — He has refused his Assent to Laws, the most wholesome and necessary for the public good. — He has forbidden his Governors to pass Laws of immediate and pressing importance, unless suspended in their operation till his Assent should be obtained; and when so suspended, he has utterly neglected to attend to them. — He has refused to pass other Laws for the accommodation of large districts of people, unless those people would relinquish the right of Representation in the Legislature, a right inestimable to them and formidable to tyrants only. — He has called together legislative bodies at places unusual, uncomfortable, and distant from the depository of their public Records, for the sole purpose of fatiguing them into compliance with his measures. — He has dissolved Representative Houses repeatedly, for opposing with manly firmness his invasions on the rights of the people. — He has refused for a long time, after such dissolutions, to cause others to be elected; whereby the Legislative powers, incapable of Annihilation, have returned to the People at large for their exercise; the State remaining in the mean time exposed to all the dangers of invasion from without, and convulsions within. — He has endeavoured to prevent the population of these States; for that purpose obstructing the Laws for Naturalization of Foreigners; refusing to pass others to encourage their migrations hither, and raising the conditions of new Appropriations of Lands. — He has obstructed the Administration of Justice, by refusing his Assent to Laws for establishing Judiciary powers. — He has made Judges dependent on his Will alone, for the tenure of their offices, and the amount and payment of their salaries. — He has erected a multitude of New Offices, and sent hither swarms of Officers to harass our People, and eat out their substance. — He has kept among us, in times of peace, Standing Armies without the Consent of our Legislatures. — He has affected to render the Military independent of, and superior to, the Civil power. — He has combined with others to subject us to a jurisdiction foreign to our constitution, and unacknowledged by our laws; giving his Assent to their Acts of pretended legislation: — For quartering large bodies of armed troops among us: — For protecting them, by a mock Trial, from punishment for any Murders which they should commit on the Inhabitants of these States: — For cutting off our Trade with all parts of the world: — For imposing Taxes on us without our Consent: — For depriving us in many cases, of the benefits of Trial by Jury: — For transporting us beyond Seas to be tried for pretended offences. — For abolishing the free System of English Laws in a neighbouring Province, establishing therein an Arbitrary government, and enlarging its Boundaries so as to render it at once an example and fit instrument for introducing the same absolute rule into these Colonies: — For taking away our Charters, abolishing our most valuable Laws, and altering fundamentally the Forms of our Governments: — For suspending our own Legislatures, and declaring themselves invested with Power to legislate for us in all cases whatsoever. — He has abdicated Government here, by declaring us out of his Protection and waging War against us. — He has plundered our seas, ravaged our Coasts, burnt our towns, and destroyed the lives of our people. — He is at this time transporting large Armies of foreign Mercenaries to compleat the works of death, desolation and tyranny, already begun with circumstances of Cruelty & Perfidy scarcely paralleled in the most barbarous ages, and totally unworthy the Head of a civilized nation. — He has constrained our fellow Citizens taken Captive on the high Seas to bear Arms against their Country, to become the executioners of their friends and Brethren, or to fall themselves by their Hands. — He has excited domestic insurrections amongst us, and has endeavoured to bring on the inhabitants of our frontiers, the merciless Indian Savages, whose known rule of warfare, is an undistinguished destruction of all ages, sexes and conditions. In every stage of these Oppressions We have Petitioned for Redress in the most humble terms: Our repeated Petitions have been answered only by repeated injury. A Prince, whose character is thus marked by every act which may define a Tyrant, is unfit to be the ruler of a free people. Nor have We been wanting in attentions to our British brethren. We have warned them from time to time of attempts by their legislature to extend an unwarrantable jurisdiction over us. We have reminded them of the circumstances of our emigration and settlement here. We have appealed to their native justice and magnanimity, and we have conjured them by the ties of our common kindred to disavow these usurpations, which, would inevitably interrupt our connections and correspondence. They too have been deaf to the voice of justice and of consanguinity. We must, therefore, acquiesce in the necessity, which denounces our Separation, and hold them, as we hold the rest of mankind, Enemies in War, in Peace Friends.

We, therefore, the Representatives of the united States of America, in General Congress, Assembled, appealing to the Supreme Judge of the world for the rectitude of our intentions, do, in the Name, and by Authority of the good People of these Colonies, solemnly publish and declare, That these United Colonies are, and of Right ought to be Free and Independent States; that they are Absolved from all Allegiance to the British Crown, and that all political connection between them and the State of Great Britain, is and ought to be totally dissolved; and that as Free and Independent States, they have full Power to levy War, conclude Peace, contract Alliances, establish Commerce, and to do all other Acts and Things which Independent States may of right do. — And for the support of this Declaration, with a firm reliance on the protection of divine Providence, we mutually pledge to each other our Lives, our Fortunes and our sacred Honor.

John Hancock

Button Gwinnett
Lyman Hall
Geo Walton

Wm Hooper
Joseph Hewes
John Penn

Edward Rutledge
Thos Heyward Junr
Thomas Lynch Junr
Arthur Middleton

Samuel Chase
Wm Paca
Thos Stone
Chas Carroll of Carrollton

George Wythe
Richard Henry Lee
Th Jefferson
Benj Harrison
Thos Nelson jr
Francis Lightfoot Lee
Carter Braxton

Robt Morris
Benjamin Rush
Benj Franklin
John Morton
Geo Clymer
Jas Smith
Geo Taylor
James Wilson
Geo Ross

Caesar Rodney
Geo Read
Tho M:Kean

Wm Floyd
Phil Livingston
Frans Lewis
Lewis Morris

Richd Stockton
Jno Witherspoon
Fras Hopkinson
John Hart
Abra Clark

Josiah Bartlett
Wm Whipple

Saml Adams
John Adams
Robt Treat Paine
Elbridge Gerry

Step Hopkins
William Ellery

Roger Sherman
Sam Huntington
Wm Williams
Oliver Wolcott

Matthew Thornton

e united States of America, in General Congress, Assembled, appealing
People of these Colonies, solemnly publish and declare, That these United Colo
the British Crown, and that all political connection between them and the State
full Power to levy War, conclude Peace, contract Alliances, establish Commerce, and
port of this Declaration, with a firm reliance on the protection of divine Providen

John Hancock

Robt Morris
Benjamin Rush
Benj. Franklin

John Morton
Geo Clymer
Jas. Smith
Geo. Taylor
James Wilson
Geo. Ross

Hooper
Joseph Hewes,

Samuel Chase
Wm. Paca
Thos. Stone
Charles Carroll of Carrollton.

aid Rutledge

Geo. Wythe
Richard Henry Lee

Th. Heyward Junr.
nas Lynch Junr.

MULTISIGNATURES

- Multisignature: Compact signature that convices a verifier that a group of signers signed some message.
- What about verifiability of the order of signing?
- Where the need for this arises: Internet packet routing, troubleshooting.

AGGREGATE SIGNATURES

- Similar to multisignatures, but allows each signer to sign its own message.
- This functionality allows signers to sign their order as well.
- But constructions are *less efficient* than those for multisignatures.

OUR RESULTS

- We introduce *ordered multisignatures*: allows signers to attest to both a message and signing order.
- We define a security model.
- Very efficient, pairing-based, non-interactive construction (more efficient than all known aggregate schemes).
- We prove its security under standard assumptions.

OUR RESULTS (CONT.)

- We also treat *identity-based sequential aggregate signatures*.
- ID-based setting cuts out bandwidth and storage associated with PKI here.
- We define a new security model.
- We give an efficient, non-interactive pairing-based construction (signature size 3 group elts) and prove its security.

OUR RESULTS (CONT.)

- The construction does not rely on clock synchronization or a trusted first signer as in previous constructions.
- Applications include S-BGP route attestation.